Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Energie BFE
Sektion NE

Bericht vom 27. Juli 2016

Schutz- und Sicherheitsanalyse im Rahmen der Entwicklung von Smart Grids in der Schweiz

Datum: 27. Juli 2016
Ort: Bern

Auftraggeberin:
Bundesamt für Energie BFE
CH-3003 Bern
www.bfe.admin.ch

Auftragnehmer/in:
OFFIS – Institut für Informatik
Escherweg 2, 26121 Oldenburg, Deutschland
http://www.offis.de

Josef Ressel Zentrum FH Salzburg
Urstein Süd 1, 5412 Puch, Östrerreich
http://www.fh-salzburg.ac.at/

ecofys
Albrechtstraße 10 c, 10117 Berlin, Deutschland
http://www.ecofys.com/

Autor/in:
Dr.-Ing. Mathias Uslar, Offis, Mathias.Uslar@offis.de
Dipl.-Math. Marie Antoinette van Amelsvoort, Offis, Marie.vanAmelsvoort@offis.de
Dr. Christina Delfs, Offis, Christina.Delfs@offis.de

Prof. Dr. Dominik Engel, Josef Ressel Zentrum FH Salzburg, dominik.engel@fh-salzburg.ac.at
DI Christian Neureiter, Josef Ressel Zentrum FH Salzburg, christian.neureiter@fh-salzburg.ac.at

Dr. Christian Nabe, ecofys, C.Nabe@ecofys.com

BFE-Bereichsleitung: Bruno Le Roy, bruno.le-roy@bfe.admin.ch
BFE-Programmleitung: Matthias Gysler, matthias.gysler@nfe.admin.ch
BFE-Vertragsnummer: SI/200234-01

Bundesamt für Energie BFE
Mühlestrasse 4, CH-3063 Ittigen; Postadresse: CH-3003 Bern
Tel. +41 58 462 56 11 · Fax +41 58 463 25 00 · contact@bfe.admin.ch · www.bfe.admin.ch

OFFIS Energie
INSTITUT FÜR INFORMATIK

fhs Fachhochschule Salzburg University of Applied Sciences

ECOFYS

Abschlussbericht

Schutz- und Sicherheitsanalyse im Rahmen der Entwicklung von Smart Grids in der Schweiz

Untersuchung im Auftrag des

BFE- Bundesamt für Energie
3003 Bern

BFE Studie – Endbericht

Schutz- und Sicherheitsanalyse im Rahmen der Entwicklung von Smart Grids in der Schweiz – Fokus auf die Koordination an der Schnittstelle Markt und Netz

Oldenburg, den 27.07.2016

Autoren:

OFFIS – Institut für Informatik

Dr.-Ing. Mathias Uslar
Dipl.-Math. Marie Antoinette van Amelsvoort
Dr. Christina Delfs

Josef Ressel Zentrum FH Salzburg

Prof. Dr. Dominik Engel
DI Christian Neureiter

ecofys

Dr. Christian Nabe

Begleitgruppe BFE

Dipl. Ing. Ing. B. Le Roy (Koordinator)
Dr. M. Galus
Dr. C. Holzner
Dipl. Ing. H.-P. Binder

Executive Summary

Grundlagen, Definitionen und Zielsetzung

Innerhalb dieser Studie wird eine Schutz- und Sicherheitsanalyse für verschiedene, bereits vom BFE identifizierte Anwendungsfälle (engl.: Use Cases) im Smart Grid mit dem Fokus auf Flexibilitäten an der Schnittstelle Markt/Netz durchgeführt – die so genannten Koordinationsmodelle. Endergebnis ist dabei eine Modellierung dieser fachlichen Modelle, so dass konkrete Massnahmen gegen Risiken für die Infrsstruktur identifiziert und umgesetzt werden können.

Dabei stützt sich diese Studie fachlich auf die bereits dokumentierten Anwendungsfälle der beauftragten und abgeschlossenen Studien *„Koordination von Markt und Netz – Ausgestaltung der Schnittstellen*“ der Consentec und *„Datensicherheit und Datenschutz für Smart Grids: Offene Fragen und mögliche Lösungsansätze“* der AWK im Auftrag des BFE.

Diese bisherigen Studien hatten in ihrem Bearbeitungsfokus verschiedene Schwerpunkte, zum einen wurde in der AWK Arbeit eine Betrachtung des Datensicherheits- und des Datenschutzbedarfs einzelner, exemplarischer Anwendungsfälle im Smart Grid vorgenommen und daraus Bottom-Up eine Sicherheitsreferenzarchitektur zur Durchführung einer Sicherheitsanalyse verschiedenster Domänen des Smart Grids erstellt, zum anderen wurde durch die Consentec dediziert an der Schnittstelle zwischen Markt und Netz eine Betrachtung der möglichen Mechanismen mit einzelnen Anwendungsfälle bzgl. Engpässen im Netz und Engpassmanagement (Koordinationsmodelle) betrachtet.

Das Ziel der vorliegenden Studie ist, den Bedarf an Schutz und Sicherheit für die Informations- und Kommunikationstechnologien (IKT) der drei Koordinationsmodelle der Studie von Consentec zu identifizieren und konkrete Massnahmen für den Schutz der IKT-Infrastruktur in diesen Modellen unter einem Gesamtrisiko zu formulieren, um den Datenschutz und die Datensicherheit zu gewährleisten.

Dabei wird im Besonderen ein methodisches, reproduzierbares Vorgehen mittels der Verwendung von Standardmethodiken sowie die Einbeziehung existierender Vorarbeiten und der Studien von AWK und Consentec im Auftrag des BFE Schwerpunkt sein.

Die betrachteten Koordinationsmodelle sind dabei:

1. **Echtzeit-Engpassbeseitigung:** Dieses Modell sieht Prozesselemente zur Engpass-Vorhersage und -Beseitigung im Wesentlichen nur im unmittelbaren so genannten Echtzeitbetrieb des Netzes vor. Die Identifikation bestehender oder unmittelbar drohender Engpässe erfolgt hier auf Basis von Echtzeitmesswerten oder nicht-netzbezogenen Informationen etwa zur witterungsabhängigen Höhe der EE-Einspeisungen durch entsprechende Analysefunktionen des Netzleitsystems/SCADA. Wenn Probleme durch eine Netzzustandsvorhersage oder den Betriebsführer identifiziert werden, die Gegenmassnahmen erfordern, werden diese unmittelbar (heisst hier: im Rahmen des 15 Minuten Re-Dispatchfensters) veranlasst, sei es durch direkte Ansteuerung oder durch Anweisung eines Flexibilitätsanbieters, der dann die Steuerung übernimmt. Ein Beispiel für die Umsetzung dieses Modells ist der Einsatz des Einspeisemanagements durch VNB in Deutschland.

2. **Vorausschauende Engpassbeseitigung:** Dieses Modell sieht vor, dass zur Beseitigung möglicher Netzengpässe auch so genannte Flexibilitätsoptionen eingesetzt werden, die eine vorherige Abstimmung mit Marktteilnehmern erfordern, da sie grundsätz-

lich auch für andere Zwecke eingesetzt werden können und somit in einem Nutzungswettbewerb stehen. Dies könnten z.B. verbrauchsseitige Flexibilitäten (Industrie und (Haushalts-)Endkunden) oder der Einsatz von Speichern sein. Um die notwendige Abstimmung zu ermöglichen, setzt dieses Modell eine vorausschauende Engpass-Vorhersage voraus, die frühzeitige Entscheidungen ermöglicht, dafür allerdings auch umfangreiche, qualitativ hochwertige Eingangsdaten benötigt, aus denen eine Netzzustandsprognose im Leitsystem abgeleitet werden kann.

3. **Engpassbewirtschaftung:** Dieses Modell sieht vor, dass Netzbetreiber die marktseitigen Transaktionen durch Vorgabe von Einsatzbeschränkungen/ Restriktionen (analog der Vergabe von Transportkapazität im Übertragungssektor) so begrenzen, dass Engpässe im Idealfall gar nicht mehr auftreten, wofür die Marktteilnehmer dann allerdings Nutzeneinbussen beim Einsatz von Flexibilitäten hinnehmen müssen (z.B. Obergrenzen der Einspeisung bei Erneuerbaren). Um die dem Markt zur Verfügung stehende Kapazität zu ermitteln, ist eine vorausschauende Engpass-Vorhersage (ähnlich wie bei der vorausschauenden Engpassbeseitigung) notwendig.

Vorgehen und angewendete Werkzeuge

Die in der Consentec-Studie beschriebenen drei Koordinationsmodelle bestehen aus insgesamt fünf Prozesselementen. Die vorliegende Studie fokussiert auf den Schutzbedarf für die Prozesselemente und deren Schnittstellen. Dadurch wird auch der Fall sämtlicher Koordinationsmodelle (und eventuell weiterer Modelle, falls Prozesselemente neu artikuliert werden sollten) abgedeckt. Insgesamt lässt sich das Vorgehen der vorliegenden Studie abbilden wie in der Abbildung 1 unten dargestellt. Dieses Vorgehen stützt sich auf die Norm ISO 31000 zum Risikomanagement.

	Vorgehen im Rahmen der Studie	Angewendete Werkzeuge
a	Übertragung der AWK und Consentec Studien in die Use Case Template zur Vereinheitlichung von Struktur und Glossar	Anwendungsfalltemplate: IEC 62559
b	Modellierung der Anwendugsfälle	SGAM Toolbox und Übertragung in NISTIR 7628
c	Sicherheitsanalyse der Datenobjekte in den modellierten Anwendungsfällen	SGIS Toolbox aus dem M/490 EU Mandat
d	Gefahrenidentifikation und Schutzbedarf für die Schnittstellenklassen	SGIS Toolbox aus dem M/490 EU Mandat
e	Identifikation und Mapping der Schnittstellen in den modellierten Anwendungsfällen	NISTIR 7628
f	Gesamtrisikoanalyse für die jeweiligen Schnittstellen	SGIS Toolbox (Ermittlung des Risikofaktors) und NISTIR 7628 (Confidentiality, Integrity und Availability Analyse)
g	Identifikation der Schutzmassnahmen für die jeweiligen Schnittstellen	NISTIR 7628

Abbildung 1: Vorgehen im Rahmen der Studie – Gefahrenidentifikation und Definition der Sicherheitsanforderungen

a. Basis der Arbeiten dieser Studie ist die Konsolidierung der Texte und Modelle der Consentec und AWK in ein strukturiertes so genanntes Anwendungsfalltemplate mittels der IEC 62559. Dies erfolgt vor allem zum Zweck der Erfassung der relevanten Aspekte für eine Sicherheitsbetrachtung im Rahmen dieser Studie (dabei sind für die Koordinationsmodelle vor allem relevant: Systeme und Akteure, deren Schnittstellen, ihre ausgetauschten Daten, und die Verortung der Systeme in der Domäne Energie). Nach diesem Schritt liegt eine vereinheitlichte Sicht auf die zu betrachtenden Studien als Basis für alle weiteren Arbeiten in dieser Studie vor.

b. Im nächsten Schritt erfolgt eine Modellierung der Anwendungsfälle (d.h. der Prozesselemente) in einem Softwarewerkzeug (Smart Grid Architecture Model Toolbox der FH Salzburg[1]) zur Strukturierung und Detaillierung der Koordinationsmodelle und ihrer Prozesselemente im so genannten Smart Grid Architecture Model SGAM, welches als State-of-The-Art zur Dokumentation und Verortung von Smart Grid Lösungen und Technologien in Europa gilt. Dabei wird aus den verschiedenen Ebenen (Geschäfts-, Funktions-, Informations-, Kommunikations- und Komponentenebene, vgl. Abbildung 6 im Text) auf die Koordinationsmodelle geblickt, um unterschiedliche Aspekte von Sicherheit zu untersuchen. Die modellierten Anwendungsfälle werden dann für den Bedarf der Sicherheitsanalyse zur NISTR 7628 übertragen.

c. Eine Schutz- und Sicherheitsanalyse für die einzelnen Datenobjekte (d.h. generische Datentypen wie z.B. Messdaten) in den drei Koordinationsmodellen bzw. in den fünf Prozesselementen wird durchgeführt und die Ergebnisse dargestellt. Durch die Anwendung SGIS-Toolbox für diese Analyse wird geprüft, dass die Schlussfolgerungen der AWK Studie in der vorliegenden Studie übernommen werden können. Eine Risikoabschätzung kann für statische Daten (d.h. eine Analyse der Daten, wo sie bearbeitet sind, ohne die Datenaustausche zu berücksichtigen) jedoch nicht erfolgen, da ein Angriff nur über eine Schnittstelle oder ein Verlust nur in einem Prozess geschehen kann. Im Rahmen dieser Studie wird daher zusätzlich noch eine Sicherheitsanalyse für die Schnittstellen vorgenommen.

d. Für die Schnittstellenklassen wird zuerst der Schutzbedarf ermittelt. Die Gefahrenidentifikation erfolgt mit der Unterstützung der High-Level Security Guidance der SGIS M/490. Durch eine Zuordnung der jeweiligen Risk Impact Levels (RIL) wird somit ein Schutzbedarf für die einzelnen in den Prozesselementen integrierten Schnittstellen gezeigt.

e. Für die Sicherheitsanalyse in dieser Studie kommt die NISTIR 7628 als Analyseframework für Smart Grid Security zur Anwendung. Das allgemeine Ziel der NISTIR 7628 Guidelines ist die Entwicklung eines Frameworks für die Formulierung und Umsetzung einer effektiven Cyber Security Strategie. Deshalb müssen die Schnittstellen der jeweiligen Prozesselemente der Koordinationsmodelle in der NISTIR 628 identifiziert werden bzw. verortet werden. Für die jeweiligen Schnittstellen in den Prozesselementen wird ermittelt, welche Schnittstellenklassen der NISTIR 7628 zugrunde liegen.

f. In der Studie wird davon ausgegangen, dass ein System ist bedingt durch die Professionalität und Möglichkeiten der Angreifer nur so gut wie sein am schwächsten abgesichertes Interface („Weakest-Link" – Theorie). Deshalb wird für die sämtlichen Schnittstellenklassen, die im vorherigen Schritt als Bestandteile der Prozesselemente identifiziert wurden, durch die Anwendung SGIS-Toolbox eine Gesamtrisikoanalyse durchgeführt. Die Aspekte Vertraulichkeit, Integrität und Verfügbarkeit (CIA-Analyse) werden

[1] www.en-trust.at/NISTIR

untersucht und das Gesamtrisiko (ergibt sich aus den Aspekten des Schadensausmasses und der Eintrittswahrscheinlichkeit) der jeweiligen Schnittstellenklasse wird ermittelt.

g. Nach der vorstehenden Sicherheitsanalyse können durch ein Mapping der Schnittstellenklassen auf die unterschiedlichen Prozesselemente die Schutzziele für die jeweiligen Prozesselemente der Koordinationsmodelle identifiziert werden. Dabei werden dediziert Sicherheitsanforderungen (so genannte Cyber Security Requirements – benötigte Massnahmen zum Schutz der Schnittstellen) für einzelne Schnittstellen basierend auf dem NISTIR 7628 erhoben, die auf spezifischen Bedrohungsszenarien für einzelne Schnittstellenklassen (z.B. Kontrollsysteme zu dezentraler Anlage, Kommunikation zur Erzeugungsanlagen, Austausch von Messwerten) beruhen.

Durchführung der Analyse und Konsolidierung der Ergebnisse

Wie oben skizziert nutzt das Kapitel zur Risikoanalyse dieser Studie die aufbereiteten modellierten Anwendungsfälle, welche sich nach der Durchführung der konsolidierten NISTIR 7628 Modellierung ergaben, zu einer geeigneten Risikobewertung für die Schnittstellen der Koordinationsmodelle und ihre Prozesselemente auf Basis der SGIS Methodik aus dem M/490 EU Mandat.

Die SGIS-Methodik des M/490 unterscheidet dabei zwischen den Aspekten der Datensicherheit und des Datenschutzes (unter der Verwendung des so genannten Smart Grid Data Protection Class Concepts – SG-DPC) sowie eines Risikoimpacts für Smart Grid Lösungen (d.h. konkrete Systeme mit Prozessen und Datenaustausch) auf mehreren Sicherheitsebenen, die einen Grad für einen möglichen Schaden bieten. Grundsätzlich ist in der Studie eine sehr homogene Sicht auf die Daten in den Koordinationsmodellen zu erkennen, das Gefährdungspotenzial bei Verlust oder Offenlegung der Daten liegt jedoch zumeist im Bereich 3-4 (max. der Skala 5), falls Verletzungen bzgl. der Nutzung der Daten auftreten. Dabei ist zu beachten, dass die Risikoskala der SGIS eine europäische Dimension annimmt und an die Schweiz anzupassen bzw. zu relativieren ist. Gemäss ICT Continuity VSE Regel kann ab Gefährdungspotenzial 3 im Referenziell der SGIS-Methodik bereits eine Krise entstehen (ungeplantes Verhalten der elektrischen Energieversorgung mit über 50 MWh nicht zeitgerecht gelieferter Energie). Ein Verlust der Daten der einzelnen Koordinationsmodelle hat daher das Potenzial, durch eine geeignete Nutzung durch einen Angreifer theoretisch eine Krise auf lokaler Ebene auszulösen. Die entsprechenden Risiken, die in der Studie für die jeweiligen Schnittstellen eingeschätzt werden, sind in der Schweiz also generell hoch einzustufen.

Neben der Analyse des Datenschutzes und der Datensicherheit für statische Datenobjekte ist der zweite Schwerpunkt die Erstellung einer Schutzbedarfsanalyse auf Basis einer Gefahrenfelderidentifikation für die datentechnischen Schnittstellen in den Koordinationsmodellen und in ihren Prozesselementen.

Zuerst kann die Verortung der Schnittstellenklassen der Prozesselemente (EP) mithilfe der Tabelle 1 visualisiert werden. Diese Tabelle fast zusammen, welche Schnittstellenklassen des NISTIR 7628 in den Prozesselementen der Koordinationsmodelle zu finden sind.

Tabelle 1: Abbildung der Schnittstellenklassen auf die Anwendungsfälle EP01- EP05

Anwendungsfall	EP01: Echtzeit Engpassvorhersage	EP02: Vorrausschauende Engpassvorhersage	EP03: Echtzeit Engpassbeseitigung	EP04: Engpassbeseitigung durch Flexibilitäts-beschaffung	EP05: Engpass-bewirtschaftung
Schnittstellenklasse					
5	x	x	x	x	x
6		x	x	x	x
7			x	x	
8		x	x	x	x
9	x	x	x		
13			x	x	
14			x	x	
16	x	x	x	x	x
17	x				
18			x	x	
20	x	x	x	x	x

Im Anschluss wurde eine Gesamtrisikoanalyse durchgeführt, aus der sich eine Risikobetrachtung für die einzelnen Schnittstellenklassen der Prozesselemente ergeben. Die Risiken wurden dabei unter den Faktoren Schadensausmass und Eintrittswahrscheinlichkeit pro Schnittstelleklasse analysiert, diskutiert und priorisiert wie in Tabelle 2 dokumentiert. Für jede Schnittstellenklasse wird ein Risikofaktor (im Wertbereich 1-30, vgl. Tabelle 9 im Bericht) ermittelt.

Tabelle 2: Gesamtrisikobetrachtung im Rahmen der Studie

	Daten-dimension			Eintrittswahrscheinlichkeit				Schadensausmass		
Schnitt-stellen-klasse	C	I	A	Angreifer-motivation	Angreifbarkeit der Schnittstelle	Zugriffszahlen	API-Level	SGIS Security Level	Direkte Effekte im Betrieb	**Risiko**
5	L	H	H	1	1	1	1	4	1	**5**
6	L	H	M	1	1	2	1	4	1	**5**
7	H	H	L	2	1	2	2	3	1	**8**
8	H	H	L	2	2	2	3	3	1	**12**
9	H	H	M	3	3	3	5	2	0	**10**
13	H	H	L	3	2	3	5	2	1	**15**
14	H	H	H	2	2	3	4	3	1	**16**
16	L	M	M	3	3	3	5	2	1	**15**
17	L	H	M	1	2	2	2	3	1	**8**
18	M	H	L	3	3	3	5	1	1	**10**
20	L	H	M	1	2	1	1	2	0	**2**

Die Tabelle 2 zeigt dabei für die einzelnen in den Prozesselementen erforderlichen Schnittstellenklassen eine Analyse bzgl. der durch die Experten diskutierten und erarbeiteten Faktoren Angreifermotivation, physische Angreifbarkeit der Schnittstellen, Anzahl möglicher Angreifer, einem sich aus diesen Faktoren ergebenden Angriffswahrscheinlichkeitslevel sowie die Faktoren Schadensausmass und direkte Netzauswirkungen im Betrieb. Mittels einer Risikoformel ergibt sich auf Basis der Werte für die einzelnen Prozesselemente eine Risikoabschätzung pro Schnittstellenklasse, die im Kontext einer Risikomatrix mittels Ampelprinzip abgeschätzt wird.

Schliesslich wird mittels des NISTIR 7628 insgesamt 71 Massnahmen zum Schutz vor Schaden bei Angriffen auf diese Schnittstellenklasse identifiziert, die zu einer geeigneten Absiche-

rung der Koordinationsmodelle als Grundschutz umgesetzt werden sollten. Diese Massnahmen werden in der Tabelle 13 (im Text) präsentiert. Nicht alle 71 Massnahmen müssen jedoch in jeder Schnittstellenklassen umgesetzt werden. Die Tabelle 12 (im Text) gibt eine Überblick über die Schutzmassnahmen, die für jede Schnittstellenklasse –d.h. schlussendlich mittels Tabelle 1 für jedes Prozesselement umzusetzen sind. Diese Tabelle 13 stellt ein zentrales Element der Analyse dieser Studie dar, da sie den Schnittstellenklassen der Koordinationsmodelle Massnahmen zuweist, die zu deren Absicherung umgesetzt werden müssen bzw. sollten, wenn die Infrastruktur als geeignet abgesichert gelten soll.

Massnahmen und Empfehlungen

Basierend auf den Gesamtanalysenergebnissen und der Modellierung gibt die Studie abschliessend Empfehlungen zur Umsetzung und Etablierung von Massnahmen, falls die Koordinationsmodelle der Consentec auf dem Schweizer Energiemarkt umgesetzt werden.

Dabei sind vor allem die im Scope der Studie relevanten Felder Datensicherheit und Datenschutz der Datenobjekte ein Schwerpunkt der Empfehlungen.

Insgesamt gilt für diese Studie die Empfehlung, die Ergebnisse der AWK Studie, Kapitel 6, auch auf die hier in der Studie identifizierten Datenobjekte in den Koordinationsmodellen gemäss AWK anzuwenden und sie wie ihre Gegenstücke in der AWK Studie bzgl. der rechtlichen Situation zu behandeln. Bezüglich des Datenschutzes sind vor allem personenbezogene Daten (z.B. Lastgangmessungen oder kundenspezifische Informationen) kritisch und sollten im Hinblick auf das Datenschutzgesetz des Bundes geschützt werden. Zusätzlich ergänzt diese Studie die AWK um die Klassifizierung gemäss SGIS und eine Abschätzung des Schadensausmasses bei Verlust der in den Koordinationsmodellen ausgetauschten Daten, was in der AWK Studie bislang nicht etabliert war. Die vorliegende Studie stellt sicher, dass die abgestimmte Basis aus der AWK Studie auch im Kontext der Koordinationsmodelle gültig ist und somit eine geeignete Analyse für alle Datenobjekte vorliegt.

Für die Koordinationsmodelle gilt, dass die Ergebnisse der Consentec Studie erkennen lassen, dass die Koordinationsmodelle im Detail sehr unterschiedlich ausgestaltet werden können und sich aus den Gestaltungsdetails auch sehr unterschiedliche technische Anforderungen hinsichtlich Datenkommunikation und Systemkomponenten – und dadurch auch für ihren Datenschutz und die IT-Sicherheit - ergeben können. Die vorliegende Studie hat jedoch aufgezeigt, dass die Schnittstellenklassen und schlussendlich die Koordinationsmodelle grundsätzlich gefährdet sind und dementsprechend durch geeignete Schutzmassnahmen geschützt werden sollten. Es ergibt sich z.B., dass die Schnittstellenklassen 13 (Schnittstelle innerhalb der intelligenten Messinfrastruktur), 14 (Schnittstelle innerhalb der intelligenten Messinfrastruktur für den Netzbetrieb) und 16 (Schnittstelle zwischen dem Leitsystem und dem Flexibilitätsmanagement des Endverbrauchers), die die höchsten Risikoniveaus gemäss Tabelle 2 ausweisen, in den Prozesselementen 2 „Vorausschauende Engpassvorhersage“ und 3 „Echtzeit Engpassbeseitigung“ zu finden sind. Da diese Prozesselemente Bestandteil der drei Koordinationsmodelle sind, ergibt sich generell ein grosser Schutzbedarf für die Koordinationsmodelle.

Um dem Schutzbedarf entgegenzukommen wurden für die Koordinationsmodelle und die sich daraus ergebenden Anwendungsfälle insgesamt 71 Schutzbedarfe als so genanntes Grundschutzprofil und daraus abgeleitet auch passende Massnahmen gemäss NISTIR 7628 ermittelt. Da die Risikoanalyse für die Mehrzahl der Schnittstellenklassen und somit für die Koordinationsmodelle eine höhere Gefährdung ohne Umsetzung der identifizierten Massnahmen aus dem NISTIR 7628 ergab, wird empfohlen, diese bei einer Implementierung der Koordinationsmodelle als eine Art Grundschutz für das Smart Grid in diesem Umfeld auch umzusetzen und gemäss der Erkenntnisse der Risikoanalyse in ihrer Umsetzung zu priorisieren .

Unter Grundschutz wird im Rahmen der Studie die Erarbeitung von Massnahmen zum Erreichen eines mittleren, angemessenen und ausreichenden Schutzniveaus verstanden. Der Grundschutz stellt dabei einen Massnahmenkatalog zur Verfügung, der bei einer Gefährdung zum Einsatz kommt. Im Rahmen dieser Studie erfolgte die Risikoanalyse dazu, die gefährdetsten Schnittstellenklassen der Koordinationsmodelle zu identifizieren und damit für die Umsetzung der Massnahmen gleichsam zu priorisieren. Diese als sinnvoll zu erachtenden Massnahmen und ausführlich sind dediziert im Anhang (6.2) dieser Studie als Umsetzungsgrundlage aufgeführt.

Dadurch, dass die Erarbeitung von Schutzanforderungen für eine Grundschutz subsidiär auf Basis einer Schutzbedarfsanalyse, welche aus dieser Studie mit der kanonischen Methodik verfeinert werden kann, in der Branche erarbeitet werden sollte, ist zudem eine Angemessenheit, auch vor dem Hintergrund der Schweiz spezifischen Situation mit vielen heterogenen Netzbetreibern, gesichert. Ein ähnlicher Prozess wurde auch mit dem RASSA (Reference Architecture for Secure Smart Grids in Austria) Projekt in Österreich durch die Technologieplattform Smart Grid, die eControl, Österreich Energie und die Verteilnetzbetreiber verfolgt.

Eine formale Konformitätsprüfung gegen die individuell für die Schweiz erarbeiteten Schutzanforderungen bietet ein gutes Vertrauenswürdigkeits-Aufwands-Verhältnis. Zudem bietet ein Schutzprofil eine detaillierte Wegleitung für die Umsetzung der Koordinationsmodelle. Die individuell auf das nationale Schutzprofil ausgelegte Prüfung ermöglicht eine geeignete und schlanke Umsetzung der Konformitätsprüfung. Ein ähnlicher Ansatz zur Gewährleistung der Datensicherheit für intelligente Messsysteme bei Endverbrauchern wurde in einer vom BFE in Auftrag gegebenen Studie skizziert [45].

In dieser Studie wird also ein methodisches, gut dokumentiertes, und reproduzierbares Vorgehen, basierend auf der ISO 31000 und mittels der Verwendung von standardisierten Methodiken, angenommen. Dies stellt eine Reproduzierbarkeit der Ergebnisse unter anderen Anwendungsfällen sicher und ermöglicht, auch bei Veränderung der Koordinationsmodelle ohne extrem großen Aufwand eine Re-Evaluation der Situation vorzunehmen. Dieses Vorgehen, welches in der vorliegenden Studie auf die Koordinationsmodelle aus der Consentec Studie angewendet wird, kann daher auch für die IT-Sicherung von weiteren Smart Grid Anwendungsfällen mit anderen Schwerpunkten vorgenommen werden.

Résumé

Principes, définitions et objectifs

La présente étude réalise une analyse de la protection et de la sécurité pour divers cas d'utilisation (anglais : Use Cases) de réseaux intelligents, déjà identifiés par l'OFEN, portant sur la flexibilité des interfaces marché / réseau : les « modèles de coordination ». Elle aboutit à une modélisation de ces modèles spécifiques pour identifier et mettre en œuvre des mesures concrètes afin de lutter contre les risques menaçant l'infrastructure.

La présente étude se base sur les cas d'utilisation déjà documentés dans les études achevées « Koordination von Markt und Netz – Ausgestaltung der Schnittstellen » (coordination du marché et du réseau – Aménagement des interfaces) de Consentec et « Datensicherheit und Datenschutz für Smart Grids: Offene Fragen und mögliche Lösungsansätze » (sécurité et protection des données pour Smart Grids : questions ouvertes et solutions possibles) d'AWK et réalisées pour le compte de l'OFEN.

Les études réalisées jusqu'ici se concentraient sur divers points. L'étude d'AWK, d'une part, a examiné le besoin de protection et de sécurité des données dans certains cas d'utilisation ayant valeur d'exemple. L'étude d'AWK a ensuite élaboré une architecture de référence pour la sécurité avec une approche ascendante (« bottom-up ») afin d'effectuer une analyse de sécurité pour les domaines les plus divers des réseaux intelligents. L'étude de Consentec, d'autre part, a considéré les mécanismes possibles dans des cas d'utilisation relatifs à la congestion dans le réseau ainsi qu'à la gestion des congestions s'appliquant en particulier à l'interface entre réseau et marché (modèles de coordination).

L'objectif de cette étude est d'identifier le besoin de protection et de sécurité pour les technologies de l'information et de la communication (TIC) des trois modèles de coordination figurant dans l'étude de Consentec. Il s'agit ainsi de formuler des mesures concrètes pour la protection de l'infrastructure TIC de ces modèles, dans le cadre d'un risque global, afin de garantir la protection et la sécurité des données.

Pour cela, l'étude privilégie un procédé méthodique et reproductible par le biais de l'utilisation de méthodes standards ainsi que la prise en compte de travaux préliminaires existants et des études d'AWK et de Consentec pour le compte de l'OFEN.

Les modèles de coordination considérés sont:

1. **Suppression des congestions en temps réel :** ce modèle prévoit des éléments de processus pour l'anticipation et la suppression des congestions, en principe uniquement lors de l'exploitation directe du réseau (exploitation en temps réel). L'identification de congestions existantes ou imminentes intervient sur la base des valeurs de mesures en temps réel ou d'informations qui ne sont pas en relation avec le réseau, comme pour la quantité de l'injection d'énergies renouvelables qui varie en fonction des influences extérieures. Ces informations sont traitées par des fonctions d'analyse du système de conduite du réseau (SCADA). Si une prévision de l'état du réseau ou de l'exploitant identifie des problèmes exigeant que des mesures soient prisent, celles-ci seront immédiatement initiées (dans l'intervalle des 15 minutes de la fenêtre de redispatching), soit par une intervention directe ou par une intervention d'un prestataire de flexibilité qui reprendra alors le contrôle de la situation. La mise en œuvre de la gestion de l'injection par le gestionnaire de réseau de distribution (GRD) est un

exemple de mise en œuvre de ce modèle en Allemagne.

2. **Suppression des congestions par anticipation:** ce modèle prévoit des « options de flexibilité » pour la suppression d'éventuelles congestions sur le réseau. Ces options de flexibilité exigent une concertation préalable des acteurs du marché, car elles peuvent être utilisées en principe à d'autres fins et se trouvent ainsi dans une situation de concurrence pour leur utilisation. Ces options pourraient par exemple comprendre des flexibilités du côté du consommateur (industrie et clients privés/ménages) ou le recours au stockage. Pour permettre la concertation nécessaire, ce modèle prévoit une prévision des congestions par anticipation, facilitant les décisions en amont, mais nécessitant des données d'entrée exhaustives et de haute qualité pouvant générer une prévision de l'état du réseau dans le système de conduite.

	Approche dans le cadre de l'étude	**Outils utilisés**
a	Export des études d'AWK et de Consentec dans un modèle des cas d'utilisation pour une uniformisation de la structure et du glossaire	Type de modèle pour les cas d'utilisation: IEC 62559
b	Modélisation des cas d'utilisation	Boîte à outils SGAM et conversion dans NISTIR 7628
c	Analyse de sécurité des objets de données (types de données, par ex. données de mesure) dans les cas d'utilisation modélisés	Boîte à outils SGIS du mandat européen M/490
d	Identification des risques et besoins de protection pour les classes d'interfaces	Boîte à outils SGIS du mandat européen M/490
e	Identification et recensement des classes d'interfaces dans les cas d'utilisation modélisés	NISTIR 7628
f	Analyse globale des risques pour les classes d'interfaces concernées	Boîte à outils SGIS (détermination du facteur de risqué) et NISTIR 7628 (analyse de confidentialité, intégrité et disponibilité)
g	Identification des mesures de protection pour les classes d'interfaces concernées	NISTIR 7628

Figure 1 : Méthode dans le cadre de l'étude – Identification des dangers et définition des exigences de sécurité

3. **Gestion des congestions:** ce modèle prévoit une limitation des transactions du côté du marché par le GRD en imposant des contraintes d'utilisation ou des restrictions (comparable à l'affectation des capacités dans le secteur du transport) de sorte à éviter, dans le cas idéal, l'apparition de congestions. Les acteurs du marché doivent toutefois tolérer des pertes d'exploitation lors du recours à la flexibilité (par ex. limites supérieures de pour l'injection des énergies renouvelables). Une prévision par anticipation des congestions est nécessaire (tout comme une suppression des congestions

par anticipation) pour déterminer la capacité à la disposition du marché.

Approche et outils utilisés

Les trois modèles de coordination décrits dans l'étude de Consentec se composent au total de cinq éléments de processus. La présente étude se concentre sur le besoin de protection requis pour les éléments de processus et leurs interfaces. Par ce biais, les cas des divers modèles de coordination (et éventuellement d'autres modèles, si les éléments du processus doivent être à nouveau articulés) sont couverts. Dans l'ensemble, la méthode de la présente étude peut être représentée comme indiqué ci-après sur la figure 1. Cette méthode est basée sur la norme ISO 31000 relative à la gestion des risques.

a. La consolidation des études et des modèles de Consentec et d'AWK au sein d'un type de modèle structuré des cas d'utilisation selon la norme IEC 62559 constitue la base des travaux de cette étude. Elle intervient avant tout dans un objectif d'identification des aspects pertinents à prendre en compte pour la sécurité dans le cadre de cette étude. A cet égard, les aspects suivants sont intéressants pour les modèles de coordination : les systèmes et acteurs, leurs interfaces, les données échangées et la place des systèmes dans le domaine de l'énergie. Cette étape fournit une représentation uniformisée des cas d'utilisation qui constituent la base pour tous les autres travaux qui seront exécutés dans le cadre de cette étude.

b. Lors de l'étape suivante, une modélisation des cas d'utilisation (plus précisément des éléments de processus) interviendra à l'aide d'un logiciel (Smart Grid Architecture Model Toolbox de l'Ecole d'études supérieures de Salzbourg - FH Salzburg) afin d'obtenir une structure et une vue détaillée des modèles de coordination et de leurs éléments de processus dans le modèle d'architecture des réseaux intelligents « Smart Grid Architecture Model » (SGAM). Le SGAM est la référence en Europe en matière de documentation et de classification des solutions et des technologies de réseaux intelligents. Les modèles de coordination sont examinés sur différents niveaux (niveaux d'activité, de fonctions, d'information, de communication et de composant, cf. figure 6 dans le texte) pour déterminer les divers aspects relatifs à la sécurité. Pour les besoins de l'analyse de sécurité, les cas d'utilisation modélisés sont exportés dans le référentiel NISTIR 7628.

c. L'étude réalise une analyse de sécurité et de protection pour les divers objets de données (c'est-à-dire des types génériques de données, comme des données de mesure) au sein des trois modèles de coordination et des cinq éléments de processus, puis présente les résultats. Grâce à l'utilisation de la boite à outils « Smart Grid Information Security » (SGIS) pour cette analyse, les conclusions de l'étude d'AWK sont confirmées dans la présente étude. Une approche statique des données (c'est-à-dire une analyse des données là où elles sont traitées, sans considérer les échanges) ne permet toutefois pas d'effectuer une estimation des risques. En effet, une attaque ne peut intervenir que par le biais d'une interface ou une perte ne survient que lors d'un processus. Une analyse de sécurité supplémentaire sera donc effectuée pour les interfaces dans le cadre de cette étude.

d. On détermine d'abord le besoin de protection pour les classes d'interfaces. L'identification des dangers est effectuée en utilisant le document « High-Level Security Guidance » de SGIS du mandat européen M/490. En classifiant les différents niveaux d'impact de risques (« Risk Impact Levels » - RIL), l'étude met en évidence le besoin de protection pour chaque interface intégrée dans les éléments de processus.

e. Pour l'analyse de sécurité dans cette étude, la directive NISTIR 7628 sera utilisée comme cadre d'analyse pour la sécurité dans les réseaux intelligents. L'objectif général de la directive NISTIR 7628 est l'élaboration d'un cadre pour la formulation et la mise en œuvre d'une stratégie efficace de cyber-sécurité. Pour cela, les interfaces présentes dans les divers éléments de processus doivent être identifiées et ordonnées dans le référentiel NISTIR 7628. Pour chaque interface dans un élément de processus, on détermine quelle est la classe d'interface NISTIR 7628 correspondante.

f. La présente étude fait l'hypothèse qu'en fonction du professionnalisme et des possibilités des attaquants, un système est aussi bien sécurisé que l'interface la moins bien protégée (théorie du maillon le plus faible « Weakest-Link »). Pour cette raison, on procède à une analyse globale des risques en utilisant la boîte d'outils SGIS pour les diverses classes d'interfaces qui ont été identifiées lors de l'étape précédente comme faisant partie des éléments de processus. Les aspects relatifs à la confidentialité, à l'intégrité et à la disponibilité (analyse CIA) sont examinés et le risque global (découlant des aspects de l'ampleur des dommages et de la probabilité d'apparition) de chaque classe d'interface est déterminé.

g. De l'analyse de sécurité qui précède, on peut identifier et attribuer des objectifs de protection aux différents éléments de processus des modèles de coordination. Pour cela, l'étude répertorie les exigences de sécurité (« Cyber Security Requirements ») basées sur NISTIR 76287 pour les différentes classes d'interfaces. Ces mesures s'inspirent de scénarios de menace spécifiques aux différentes classes d'interface (par ex. les systèmes de contrôle pour les installations décentralisée, communication vers les installations de production, échange de valeurs de mesure).

Exécution de l'analyse et consolidation des résultats

Comme décrit ci-dessus, le chapitre de cette étude concernant l'analyse des risques utilise les cas d'utilisation modélisés grâce à l'exécution du modèle consolidé NISTIR 7628. Il s'agit ainsi d'aboutir à une évaluation appropriée des risques pour les interfaces des modèles de coordination et de leurs éléments de processus sur la base de la méthode SGIS du mandat européen M/490.

En utilisant le concept de classe de protection pour les données des réseaux intelligents « Smart Grid Data Protection Class » – SG-DPC, la méthode SGIS du mandat européen M/490 fait la différence entre les aspects de la sécurité et de la protection des données. Cette méthode différencie aussi les impacts des risques pour les solutions de réseau intelligent (à savoir des systèmes concrets avec des processus et des échanges de données) sur plusieurs niveaux de sécurité, proposant divers niveaux de dommages éventuels. Grâce à une l'analyse SGIS pour la protection et la sécurité des données, cette étude présente dans l'ensemble une vue très homogène des données dans les modèles de coordination. Le danger potentiel lors de la perte ou de la publication de données se situe principalement au niveau 3-4 (max. de l'échelle 5), en cas d'utilisation malveillante des données. Il faut tenir compte du fait que l'échelle de risques de SGIS revêt une dimension européenne et doit être adaptée et relativisée pour la Suisse. Conformément au document d'application *ICT Continuity* de l'AES, une crise peut survenir à partir du potentiel de mise en danger 3 dans le référentiel de la méthode SGIS (comportement imprévu de l'approvisionnement énergétique électrique avec plus de 50 MWh d'énergie non livrée à temps). Une perte de données des divers modèles de coordination peut pour cette raison déclencher théoriquement une crise au niveau local si les données sont

utilisées en conséquence par un attaquant. Les risques correspondants sont jugés élevés en général en Suisse pour les interfaces traitées dans l'étude.

Outre l'analyse de protection et de sécurité pour les données statiques, l'étude réalise une analyse des besoins de protection pour les interfaces où les données sont échangées. Cette analyse s'effectue sur la base d'une identification des champs de risques dans les modèles de coordination et dans les éléments de processus. La localisation des classes d'interfaces dans les éléments de processus (EP) est visualisée à l'aide du tableau 1. Ce tableau indique quelles classes d'interface de NISTIR 7628 figurent dans les éléments de processus des modèles de coordination.

Tableau 1 : Représentation des classes d'interface pour les cas d'utilisation EP01- EP05

Cas d'utilisation	EP01: prévision des congestions en temps réel	EP02: Prévision par anticipation des congestions	EP03: Suppression des congestions en temps réel	EP04: Suppression des congestions avec l'achat de flexibilité	EP05: Gestion des congestions
Classe d'interface					
5	x	x	x	x	x
6		x	x	x	x
7			x	x	
8		x	x	x	x
9	x	x	x		
13			x	x	
14			x	x	
16	x	x	x	x	x
17	x				
18			x	x	
20	x	x	x	x	x

Consécutivement, une analyse globale des risques a été réalisée sur la base d'une prise en compte des risques pour les diverses classes d'interface des éléments de processus. Les risques ont été analysés et discutés en tenant compte des facteurs que sont la probabilité d'apparition par classe d'interface et l'ampleur des dégâts. Un ordre de priorité a ensuite été établi comme indiqué dans le tableau 2. Un facteur de risque a été déterminé pour chaque classe d'interface (dans le domaine de valeur 1 à 30, cf. tableau 9 dans le rapport).

Tableau 2 : Considération globale des risques dans le cadre de l'étude

	Dimension relative aux données			Probabilite d'apparation				Ampleur des dégâts		
Classe d'interface	C	I	A	Motivation de l'attaquant	Possibilite d'attaque de l'interface	Nombre d'attaquants	Niveau API	SGIS Security Level	Effets directs dans l'exploitation	**Risque**
5	L	H	H	1	1	1	1	4	1	**5**
6	L	H	M	1	1	2	1	4	1	**5**
7	H	H	L	2	1	2	2	3	1	**8**
8	H	H	L	2	2	2	3	3	1	**12**
9	H	H	M	3	3	3	5	2	0	**10**
13	H	H	L	3	2	3	5	2	1	**15**
14	H	H	H	2	2	3	4	3	1	**16**
16	L	M	M	3	3	3	5	2	1	**15**
17	L	H	M	1	2	2	2	3	1	**8**
18	M	H	L	3	3	3	5	1	1	**10**
20	L	H	M	1	2	1	1	2	0	**2**

Le tableau 2 indique, pour les diverses classes d'interfaces figurant dans les éléments de processus des modèles de coordination, une analyse des facteurs élaborés et discutés par les experts : motivation de l'attaquant, possibilité physique d'attaque des interfaces, nombre d'attaquants possibles. Un niveau de probabilité d'attaque découlant de ces facteurs (API) ainsi que les facteurs de l'étendue des dégâts et les effets directs du réseau dans l'exploitation ont ainsi été déterminés. Pour les différents éléments de processus, une formule de risque permet de déterminer des valeurs pour estimer le risque par classe d'interface. Cette estimation est basée sur une matrice de risques avec le principe « des feux de signalisation ».

Finalement, 71 mesures visant à la protection contre des dommages en cas d'attaques sur les classes d'interfaces ont été identifiées à l'aide de NISTIR 7628. Ces mesures devraient être mises en œuvre comme protection de base, assurant ainsi une protection adéquate des modèles de coordination. Ces mesures sont présentées dans le tableau 3 (dans le texte). Il n'est toutefois pas impératif de mettre en œuvre toutes les 71 mesures sur chaque classe d'interface. Le tableau 12 (dans le texte) donne une vue d'ensemble de ces mesures de protection qui seront à appliquer pour chaque classe d'interface (c'est à dire finalement, avec le tableau 1, pour chaque élément de processus). Ce tableau 13 représente un élément central de l'analyse de cette étude car elle attribue aux classes d'interface des mesures qui doivent ou qui devraient être appliquées à titre de protection pour sécuriser l'infrastructure de manière adéquate.

Mesures et recommandations

Sur la base des résultats de l'ensemble de l'analyse et de la modélisation, l'étude donne finalement des recommandations pour la mise en œuvre et l'application de mesures, dans le cas où les modèles de coordination de Consentec sont à mettre en œuvre dans le marché de l'énergie suisse.

A ce titre, les sujets de la sécurité et protection des données des modèles de coordination sont pertinents pour le champ d'application de l'étude et sont en particulier au centre des recommandations.

Dans l'ensemble, il est recommandé dans cette étude d'appliquer les résultats de l'étude d'AWK (chapitre 6) également aux objets de données identifiés dans les modèles de coordination. Il est également recommandé de traiter ces données comme leurs pendants dans l'étude d'AWK en ce qui concerne la situation juridique, notamment au regard de la Loi fédérale sur la protection des données. En ce qui concerne la protection des données, ce sont avant tout les données personnelles (par ex. les mesures de courbe de charge ou les informations spécifiques aux clients) qui sont critiques et qui doivent être protégées. En outre, cette étude complète l'étude d'AWK avec la classification selon SGIS et avec une estimation de l'étendue des dommages en cas de perte des données échangées dans les modèles de coordination, ce qui n'était pas établi jusqu'ici dans l'étude d'AWK. La présente étude garantit que le cadre défini pour l'étude d'AWK et ses conclusions sont également valides dans le cas des modèles de coordinations, et que l'on dispose ainsi d'une analyse adéquate pour tous les objets de données.

Pour les modèles de coordination, les résultats de l'étude de Consentec montrent que les modèles de coordination peuvent être organisés en détail de manière très différente. Les détails relatifs à l'organisation peuvent générer des exigences techniques très différentes au niveau de la communication des données et des composants de système - et donc au niveau la protection et la sécurité informatiques. La présente étude a toutefois montré que les classes d'interfaces présentes dans les modèles de coordination sont en principe menacées et devraient être protégées par des mesures de protection adéquates. Il en résulte par exemple que les classes d'interface 13 (interface au sein de l'infrastructure de mesure intelligente), 14 (interface au sein de l'infrastructure de mesure intelligente pour l'exploitation réseau) et 16 (interface entre le système de contrôle et de supervision et le système de gestion de la flexibilité auprès du consommateur final), lesquelles présentent les niveaux de risques les plus élevés conformément au tableau 2, se trouvent dans les éléments de processus 2 « Prévisions par anticipation des congestions » et 3 « Suppression des congestions en temps réel ». Comme ces éléments de processus font partie des trois modèles de coordination, il en résulte un besoin de protection important pour les modèles de coordination.

Pour répondre au besoin de protection, 71 mesures au total ont été déterminées comme profil de protection de base pour les modèles de coordination. Des mesures adéquates selon NISTIR 7628 ont été définies. Comme l'analyse des risques a mis à jour une exposition élevée au danger pour la majorité des classes d'interfaces et donc pour les modèles de coordination si les mesures identifiées dans le NISTIR 7628 ne sont pas mises en œuvre, il est recommandé dans ce contexte d'appliquer ces mesures en cas de mise en œuvre des modèles de coordination à titre de protection de base pour les réseaux intelligents. Selon les renseignements fournis par l'analyse des risques, il est également recommandé de définir des priorités lors de la mise en œuvre.

La protection de base désigne, dans le cadre de cette étude, l'élaboration de mesures visant à atteindre à un niveau de protection moyen, adapté et suffisant. Elle représente un catalogue de mesures à prendre en cas d'apparition de menaces. Dans le cadre de cette étude, l'analyse de risques a entraîné une identification des classes d'interfaces les plus vulnérables dans les modèles de coordination et a généré une liste de priorités pour la mise en place des mesures. Les mesures jugées raisonnables sont indiquées en annexe (6.2) de la présente étude comme base pour la mise en œuvre.

Les exigences en matière de protection pour une protection de base devraient en principe être élaborées de manière subsidiaire, sur la base d'une analyse du besoin de protection, laquelle peut être raffinée en recourant à la méthode canonique utilisée dans cette étude. Ceci permet

de garantir un cadre adéquat, même pour la situation spécifique de la Suisse avec des gestionnaires de réseau nombreux et hétérogènes. Un processus semblable a été pratiqué avec le projet RASSA (Reference Architecture for Secure Smart Grids in Autria) en Autriche par la plateforme technologique Smart Grid, eControl, Österreich Energie et les gestionnaires de réseau.

Un contrôle de conformité formel par rapport aux exigences de protection propres à la Suisse garantit un bon rapport de fiabilité/efforts. En outre, un profil de protection propose une procédure détaillée pour la mise en place des modèles de coordination. Le contrôle conçu de manière individuelle pour le profil de protection national, permet une mise en place adaptée et allégée du contrôle de conformité. Une approche identique pour la garantie de la sécurité des données pour les systèmes de mesure intelligents chez les consommateurs finaux a été élaborée lors d'une étude commandée par l'OFEN [45].

La présente étude a adopté une approche méthodique, soigneusement documentée et reproductible sur la base de la norme ISO 31000, en utilisant des méthodes standardisées. Cela garantit une reproductibilité des résultats dans d'autres cas d'utilisation et permet, même en cas de modifications des modèles de coordination, de procéder à une réévaluation de la situation sans grand effort. Cette approche, utilisée dans la présente étude pour les modèles de coordination de l'étude de Consentec, peut être appliquée à la protection informatique des autres cas d'utilisation spécifiques à d'autres domaines des réseaux électriques intelligents.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Grundlagen, Definitionen und Zielsetzung

1.1 Grundlagen – Vorarbeiten der Studie

Innerhalb dieser Studie wird eine Schutz- und Sicherheitsanalyse für verschiedene, bereits in den Studien der Consentec [17] sowie der AWK [16] identifizierte Anwendungsfälle (engl.: Use cases) im Smart Grid mit dem Fokus auf Flexibilitäten an der Schnittstelle Markt/Netz durchgeführt. Dabei stützt sich diese Studie fachlich auf die bereits dokumentierten Anwendungsfälle der beauftragten und publizierten Studien *„Koordination von Markt und Netz – Ausgestaltung der Schnittstellen“* und *„Datensicherheit und Datenschutz für Smart Grids: Offene Fragen und mögliche Lösungsansätze“* im Auftrag des BFE.

Diese bisherigen Studien hatten in ihrem Bearbeitungsfokus verschiedene Schwerpunkte, zum einen wurde durch die AWK eine Betrachtung des Datensicherheits- und des Datenschutzbedarfs einzelner, exemplarischer Anwendungsfälle im Smart Grid vorgenommen und daraus Bottom-Up eine Sicherheitsreferenzarchitektur zur Erstellung einer Verfügbarkeits-, Vertraulichkeits- und Datenintegritätsanalyse verschiedenster Domänen (Bereiche im Smart Grid) erstellt, zum anderen wurde durch die Consentec dediziert an der Schnittstelle Smart Grid/Smart Market eine Betrachtung der möglichen Mechanismen mit einzelnen Anwendungsfälle bzgl. Engpässen im Netz und Engpassmanagement vorgenommen.

Innerhalb dieser Studie werden die Ergebnisse als Eingabegrössen für eine Schutz- und Sicherheitsanalyse herangezogen. Das genaue Untersuchungsumfeld wird im nächsten Abschnitt spezifiziert.

1.2 Definition des Untersuchungsumfeldes der Studie

Gemäss der Definition der Schweizer Smart Grid Roadmap [24, 25, 26] wird als ein Smart Grid in dieser Studie ein elektrisches System verstanden, das unter Einbezug von Mess- sowie meist digitaler Informations- und Kommunikationstechnologien den Austausch elektrischer Energie aus verschiedenartigen Quellen mit Konsumenten verschiedener Bedarfscharakteristika intelligent sicherstellt. Ein solches System soll den Bedürfnissen aller Marktakteure und der Gesellschaft Rechnung tragen. Die Nutzung und der Betrieb des Systems können dadurch optimiert und effizienter gestaltet werden, die Kosten und der Umwelteinfluss können minimiert und die Versorgungsqualität und -sicherheit in ausreichend hohem Masse gewährleistet werden [27].

Der Schwerpunkt der hier vorliegenden Studie liegt im Umfeld der Nutzung von Flexibilitäten im (Verteil-)Netz, um zum Einen den Netzbetrieb zu optimieren, zum Anderen aber auch Netzausbau durch eine intelligentere Nutzung vorhandener Assets zu vermeiden oder zu verzögern.

Die Arbeiten der Consentec diskutieren hierfür mögliche Marktmechanismen und -modelle, ohne jedoch eine abschliessende (technische) Implementierung mittels bestimmter Komponenten vorzuschreiben. Im Rahmen dieser Gemengelage ist das Ziel der Studie zu sehen, welches im folgenden Abschnitt detailliert wird.

1.3 Zielsetzung dieser Studie

Die hier vorliegende Studie hat den Anspruch, die bereits dokumentierten Anforderungen an Datenschutz- und Datensicherheit aus der AWK Studie weiter mit Schutzmassnahmen zu konkretisieren, die Vorarbeiten wo immer möglich wiederzunutzen und primär für die drei definierten Koordinationsmodelle der Consentec Studie zu verfeinern.

Das Ziel der im Rahmen dieses Auftrags zu erstellenden „Schutz- und Sicherheitsanalyse“ ist daher zusammenfassend, den Bedarf an Datenschutz und -Sicherheit in diesen drei Koordinationsmodellen zu identifizieren und konkrete Massnahmen für die Gewährleistung der Datenschutz und –Sicherheit in diesen Modellen zu formulieren. Dabei wird im Besonderen ein methodisches, reproduzierbares Vorgehen unter Berücksichtigung von Standards sowie die Einbeziehung existierender Vorarbeiten und Studien im Auftrag des BFE Schwerpunkt sein.

1.4 Verwendung der Koordinationsmodelle der Consentec Studie

In diesem Abschnitt werden die im Rahmen dieser Studie untersuchten Koordinationsmodelle (KM) exemplarisch und unter der Schwerpunktbildung dieser Studie vorgestellt und mit der dazugehörigen Prozesselementen (PE) als Basisbausteinen verknüpft. Sie basieren auf der Darstellung in Consentec [17].

Die Studie „Schnittstelle Markt-Netz“ präsentiert im Rahmen ihrer Mechanismenanalyse drei so genannte Hauptkoordinationsmodelle zwischen Netzbetreibern und Marktakteuren, die als Grundlage für weitere Arbeiten in dieser Studie im Bereich Datenschutz und Datensicherheit in Schweizer Smart Grids dienen sollen. Dabei handelt es sich um die folgenden drei grossen Koordinationsmodelle, welche untersucht wurden.

Abbildung 2 zeigt den prinzipiellen Ablauf der Koordinationsmodelle und deren Prozesselemente. Die Farben stehen dabei für die einzelnen Koordinationsmodelle, Pfeile zeigen deren feste Abhängigkeiten bzw. ein gestrichelter Pfeil eine optionale Abhängigkeit.

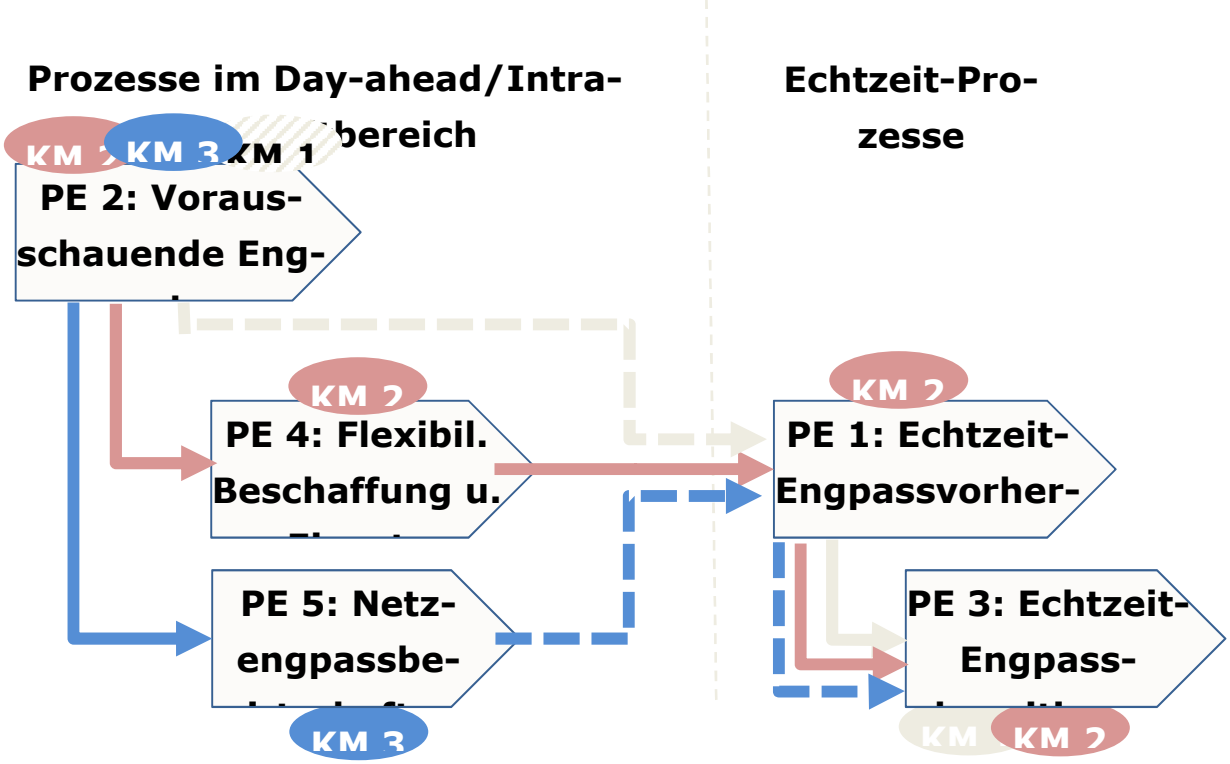


Abbildung 2: Übersicht über die untersuchten Koordinationsmodelle

Koordinationsmodell 1: Echtzeit-Engpassbeseitigung

Echtzeit-Engpassbeseitigung:
Dieses Modell sieht Prozesselemente zur Engpass-Vorhersage und -Beseitigung im Wesentlichen nur im unmittelbaren so genannten Echtzeitbetrieb des Netzes vor.

Die Identifikation bestehender oder unmittelbar drohender Engpässe erfolgt hier auf Basis von Echtzeitmesswerten oder nicht-netzbezogenen Informationen etwa zur witterungsabhängigen Höhe der EE-Einspeisungen durch entsprechende Analysefunktionen des Netzleitsystems/ SCADA. Wenn Probleme durch eine Netzzustandsvorhersage oder den Betriebsführer identifiziert werden, die Gegenmassnahmen erfordern, werden diese unmittelbar (heisst hier: im Rahmen des 15 Minuten Re-Dispatchfensters) veranlasst; sei es durch direkte Ansteuerung oder durch Anweisung eines Flexibilitätsanbieters, der dann die Steuerung übernimmt.

Die Basis für eine Entscheidung über die Notwendigkeit einer Echtzeit Engpassbeseitigung bildet eine Echtzeitvorhersage (PE1: Echtzeit-Engpassvorhersage[2]). Auf Basis von Online-Messwerten und kurzfristiger Extrapolation der Entwicklung von Messwerten hin zu kritischen Grenzwerten wird über die Notwendigkeit des Einsatzes von Massnahmen entschieden.

Die gezogene Massnahme (PE3: Echtzeit-Engpassbeseitigung) führt durch die Auslösung von Steuersignalen zur Steuerung der Flexibilität (z.B. Abregelung von Verbrauchern oder Erzeugern). Optional kann das Modell mit einer längerfristigen Engpassvorhersage kombiniert werden, die es ermöglicht, die Flexibilitätsanbieter über einen voraussichtlichen Einsatz der Flexibilität zu informieren.

In diesem Koordinationsmodell erfolgt der Eingriff auf Basis von gesetzlich definierten Eingriffsrechten und Entschädigungsregelungen. Es findet keine Koordination des Einsatzes der Flexibilität mit anderen, systemweiten Nutzungen in einem Day-ahead oder Intraday-Prozess statt.[3] Dieser Prozess ist beispielsweise in Deutschland in Form des *Einspeisemanagements* zu finden.

Koordinationsmodell 2: Vorausschauende Engpassbeseitigung

Vorausschauende Engpassbeseitigung:
Dieses Modell sieht vor, dass zur Beseitigung möglicher Netzengpässe auch so genannte Flexibilitätsoptionen eingesetzt werden, die eine vorherige Abstimmung mit Marktteilnehmern/ Dritten erfordern, da sie grundsätzlich auch für andere Zwecke eingesetzt werden können und somit in einem marktlichen Nutzungswettbewerb stehen. Dies könnten z.B. verbrauchsseitige Flexibilitäten (Industrie und (Haushalts-)Endkunden) oder der Einsatz von Speichern sein. Um die notwendige Abstimmung zu ermöglichen, setzt dieses Modell eine vorausschauende Engpass-Vorhersage voraus, die frühzeitige Entscheidungen ermöglicht, dafür allerdings auch umfangreiche, qualitativ hochwertige Eingangsdaten über den Netzzustand benötigt, aus denen eine Netzzustandsprognose im Leitsystem oder State Estimator abgeleitet werden kann.

Das bereits dargestellte Koordinationsmodell 1 kann durch vorgelagerte Prozesse erweitert werden, die ermöglichen, Flexibilitäten in marktlichen Prozessen zu beschaffen und mit anderen Anwendungen zu koordinieren. Im Koordinationsmodell 2 wird zunächst eine längerfristigere Engpassvorhersage eingefügt (PE 2: Vorausschauende Engpass-Vorhersage).[4] Diese ermöglicht eine marktliche Koordination des Flexibilitätseinsatzes im nachfolgenden Prozess Flexibilitätsbeschaffung und -einsatz (PE 4). In diesem Prozess kann der VNB unterschiedliche Flexibilitäten auswählen, kontrahieren und einsetzen. VNB können mit Flexibilitäten, die zur Engpassbeseitigung geeignet sind, Rahmenverträge abschliessen, in denen geeignete Flexibilitätsprodukte definiert sind. Beispielsweise können dies Einsatzverträge mit Speichern, Abregelungsverträge mit Betreibern von Erneuerbaren Energien oder Abschaltverträge mit unterbrechbaren Verbrauchseinrichtungen sein.

---

[2] Auch als Echtzeitmessung bezeichnet

[3] Vertiefend zu Koordinationsanforderungen: Ecofys/Swiss Economics (2015): Zukünftige Energiemärkte und die Rolle der Netzbetreiber. Studie im Auftrag des BfE

[4] Es ist auch möglich, dieses Prozesselement zusätzlich zur Echtzeit-Engpassvorhersage im Koordinationsmodell 1 zu verwenden.

Dieses Koordinationsmodell beruht auf freiwilligen Marktprozessen; es kann daher nicht sichergestellt werden, dass die Beseitigung des voraussichtlichen Engpasses erfolgreich ist. Weiterhin kann die Engpass-Vorhersage fehlerhaft sein und es kann zu nicht vorhergesehenen Engpässen kommen. Daher ist es notwendig, das oben beschriebene Koordinationsmodell 1 (Echtzeit-Engpassbeseitigung) zusätzlich anzuwenden, um in diesen Fällen den Engpass ggf. über gesetzlich definierte Eingriffsrechte zu beseitigen.

Koordinationsmodell 3: Engpassbewirtschaftung

Engpassbewirtschaftung:
Dieses Modell sieht vor, dass Netzbetreiber die marktseitigen Transaktionen durch Vorgabe von Einsatzbeschränkungen/Restriktionen (analog der Vergabe von Transportkapazität im Übertragungssektor) so begrenzen, dass Engpässe im Idealfall gar nicht mehr auftreten, wofür die Marktteilnehmer dann allerdings Nutzeneinbussen beim Einsatz von Flexibilitäten hinnehmen müssen (z.B. Obergrenzen der Einspeisung bei Erneuerbaren Energien). Um die dem Markt zur Verfügung stehende Kapazität zu ermitteln, ist eine vorausschauende Engpass-Vorhersage (ähnlich wie bei der vorausschauenden Engpassbeseitigung) notwendig.

Das Koordinationsmodell 3, Engpassbewirtschaftung, kann als Mischung von Elementen aus den beiden vorhergehenden Koordinationsmodellen betrachtet werden. Zunächst wird, wie in Koordinationsmodell 2 eine vorausschauende Engpassvorhersage durchgeführt (PE 2).

Aufbauend auf den Ergebnissen dieser Analyse werden Marktprozesse gezielt eingeschränkt, um Engpässe auszuschliessen. Dieser Prozess wird als PE 5 – Netzengpassbewirtschaftung bezeichnet. Die knappe Kapazität muss hier in geeigneter Weise auf die Akteure aufgeteilt werden, die die Kapazität nutzen wollen. Während im Koordinationsmodell 2 beispielsweise bei einer Überlastung einer Leitung durch einen Verbraucher eine Leistungsreduzierung vom VNB als Flexibilitätsprodukt kontrahiert wird, wird in diesem Modell der Bezug der Leistung verhindert.

In einer Ausgestaltungsmöglichkeit kann sogar von Verbrauchern eine Gebühr verlangt werden, wenn sie auf die Leistungsreduzierung nicht verzichten wollen. Dieses Modell weist damit Analogien zu der Bewirtschaftung von grenzüberschreienden Netzkuppelstellen auf Übertragungsnetzebene auf, bei denen in vielen Fällen die Kapazitätsvergabe durch Auktionen erfolgt. Auktionen sind jedoch nur bei einer hinreichend grossen Anzahl von Marktteilnehmern ein effizientes Allokationsinstrument, so dass in den Fällen von Engpässen im Verteilnetz auch auf andere Mechanismen zurückgegriffen werden muss (z.B. first-come, first served).

Wird die Aufteilung der Engpasskapazität den relevanten Flexibilitätsanbietern überlassen, so kann es zu Verhandlungsprozessen unter Bildung von Marktpreisen kommen, die der Marktpreisbildung im Koordinationsmodell 2 nahe kommen. Im Unterschied zu Koordinationsmodell 2 besteht im Falle der Engpassbewirtschaftung jedoch eine stärkere Eingriffsmöglichkeit des VNB, da eine zulässige Leistung vorgegeben wird. Damit ergibt sich nicht zwangsläufig die Notwendigkeit, das Koordinationsmodell 1 in Echtzeit anzuschliessen. Es kann jedoch *optional* vorgesehen werden, insbesondere wenn die vorausschauende Engpassvorhersage fehlerbehaftet ist oder die Rationierung des Engpasses nicht sicher kontrolliert werden kann.

Innerhalb der Studie der Consentec [17] wurden diese drei Anwendungsfälle, respektive Koordinationsmodelle bereits funktional und komponentenbasiert, grösstenteils auch prozessoral beschrieben. Die Studie bietet daher Input für die funktionale Analyse im SGAM, die für die Identifikation von Schnittstellen in bestimmten Domains/Zones für die Ermittlung von NISTIR 7628 Schnittstellenklassen relevant ist.

1.5 Verwendung der AWK Anwendungsfälle

Neben den drei Koordinationsmodellen werden auch die für den Aspekt Flexibilität relevanten AWK Anwendungsfälle 2 „Demand Side Response“, 5 „Regionale Flexibilitäten“, 8 „Steuerung Wirk- und Blindleistung“, 12 „Zeitliche Flexibilisierung Ein-/Ausspeisung“ aus der Gesamtheit dieser Studie sowie ihre Datenschutz- und Datensicherheitsaspekte herangezogen, um mittels einer standardisierten, durchgängigen Methodik [39, 42] ein wiederverwendbares und konsistentes Gesamtmodell für eine Analyse der Schutz- und Sicherheitsaspekte im Rahmen dieser Studie zu erhalten.

1.6 Aufbau der Studie – Leseanleitung

Abbildung 3 stellt den ISO 31000 konformen Prozess zum Risikomanagement innerhalb dieser Studie vor. Der Prozess ist dabei jedoch umfassender als das, was in dieser Studie geleistet werden kann. Diese Studie deckt die Aspekte Gefahrenidentifikation, Gefahrenfelder und Gefahrenanalyse sowie Risikobewertung und Massnahmenvorschläge ab. Weitere Aspekte des Prozesses sind organisatorisch durch die Branche oder den Regulator umzusetzen.

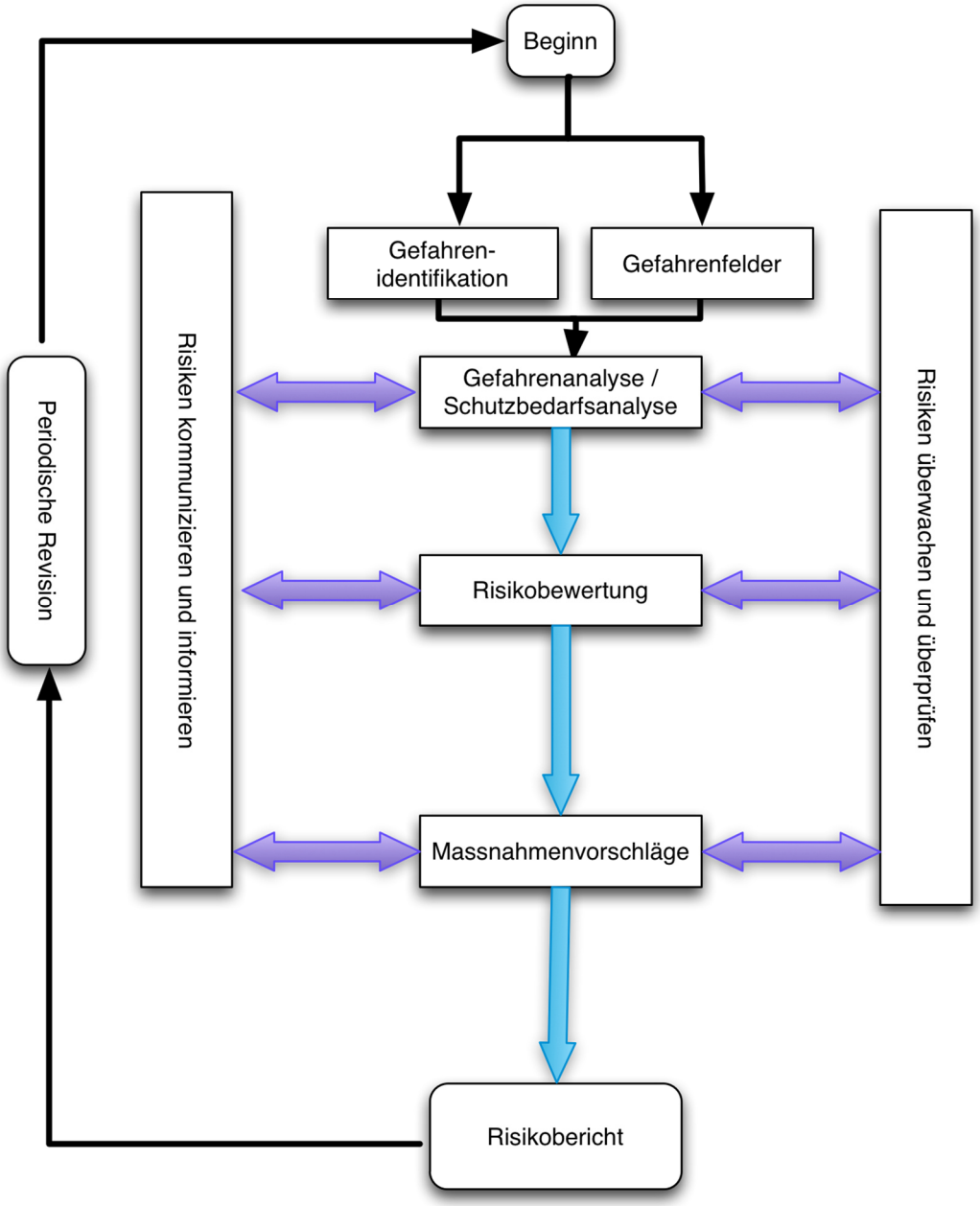


Abbildung 3: ISO 31000 konformer Risikomanagementprozess im Rahmen dieser Studie

Das Kapitel 1 dieser Studie bietet eine Zusammenfassung über den Rahmen der Studie und die generelle Zielsetzung aus Sicht von Auftraggeber und -nehmer. Daneben wird das Untersuchungsumfeld definiert und die Wiederverwendung der Ergebnisse der AWK und Consentec Studien kurz skizziert.

Ein Schwerpunkt ist dabei die Kurzdarstellung der Koordinationsmodelle. Diese Koordinationsmodelle werden in die IEC 62559 Vorlage [3, 4] überführt, um sie und die ausgewählten AWK Anwendungsfälle homogen zu strukturieren. Abschliessend wird kurz die Vorgehensweise zur Gefahren- und Risikoanalyse skizziert.

Dieses Kapitel ist geeignet für den Leser, der sich kurz einen detaillierteren Überblick über die Ziele und das Vorgehen der Studie als in der Executive Summary möglich machen will.

Kapitel 2 ist für den Leser geeignet, der die Motivation hinter der Anwendung der in dieser Studie genutzten Methodik und die dazugehörigen Grundlagen verstehen will. Neben der Motivation und Übersicht über existierende Referenzmodelle und Frameworks zur Smart Grid

Sicherheit bietet das Kapitel eine Übersicht über die durch Fachexperten empfohlenen technischen und organisatorischen Standards. Diese motivieren die Nutzung der IEC 62559 Anwendungsfallvorlage, technische Hintergründe zur Gefahrenanalyse mittels der NISTIR 7628 sowie die Übertragung dieser Methodik auf SGAM-Modelle.

Kapitel 3 stellt den Schwerpunkt dieser Studie dar. Das Kapitel 3 befasst sich mit der Auswertung der in der SGAM Toolbox modellierten Anwendungsfälle bzgl. Datensicherheit, Datenschutz und der Schnittstellensicherheit. Es nutzt die aufbereiteten Analysedaten, welche sich nach der Durchführung der konsolidierten NISTIR 7628 Modellierung aus Kapitel 2 ergeben, zu einer geeigneten Risikobewertung auf Basis der SGIS Toolbox [1, 2] aus dem M/490 EU Mandat. Konkret bietet Kapitel 3 eine Gesamtrisikoanalyse für die Studie samt dazugehöriger Priorisierung von Massnahmen, welche sich aus der Schnittstellenanalyse ergeben haben. Es ist der Kern der Studie und bietet eine Ergebnisübersicht, ohne jedoch zu tiefes methodisches Verständnis aus Kapitel 2 vorauszusetzen.

Kapitel 4 stellt die inhaltlich technische Zusammenfassung dieser Studie dar. Basierend auf der durchgeführten Analyse in Kapitel 3 samt der Einordnung der Koordinationsmodelle und ihrer Schnittstellen in Risikoklassen werden für die einzelnen Schnittstellen Massnahmen abgeleitet, diese präzisiert und Empfehlungen zur Umsetzung gegeben. Neben speziellen, IT-technisch orientierten Ansätzen werden auch Handreichungen und Motivationen für IT Sicherheit in der kritischen Infrastruktur diskutiert.

2 Verwandte Arbeiten und Methodik im Umfeld Smart Grids

Innerhalb dieses Abschnitts der Studie werden methodische Grundlagen der Studie mit den Schwerpunkten technische Standards und Roadmaps für Smart Grid Security, international anerkannte Standards für Smart Grid Sicherheit und verwandte Domänen sowie daraus abgeleitet methodische Grundlagen für diese Studie erklärt. Der Schwerpunkt der Methodik liegt dabei nicht im Schaffen eines tiefen Verständnisses für die einzelnen Technologien, sondern in der Vermittlung der Basistechnologien und Kernentscheidungen für die Analysemethodik dieser Studie und den damit erarbeiteten Ergebnissen in Kapitel 3.

Benötigt wird im Rahmen dieser Studie eine Methodik, die er erlaubt, die heterogenen Darstellungen der AWK und Consentec zu vereinheitlichen, die dort zu vorhandenen konzeptuellen Beschreibungen in eine technische Architektur zu überführen und diese dann bzgl. ihres Schutzbedarfs zu analysieren und zu bewerten und abschliessend standardisierte Massnahmen zu empfehlen, die eine spätere Umsetzung der Koordinationsmodelle berücksichtigen sollten. Mit Hilfe dieses „Fahndungsrasters“ wurden die folgenden Dokumente betrachtet.

2.1 Relevante Roadmaps und Standards

2.1.1 Smart Grid Architecture

Bei der Recherche zum stark wachsenden Thema im Kontext der IT/OT-Sicherheit (Informationstechnologien/ Operative Technologien) Systemsicherheit für das Smart Grid bzw. Anwendungsfälle des Smart Grids, sind die Auftragnehmer auf eine grosse Menge an genutzten, aber teilweise lückenhaft definierten Begrifflichkeiten wie „Referenzarchitektur“, „Sicherheitsreferenzarchitektur“, „Sicherheitsarchitekturmodell“, „Sicherheitsarchitekturframework“, „Sicherheitsleitfaden“, „Sicherheitstaxonomie“, „Security-by-Design-Architektur“ und weitere ähnliche Bezeichnungen gestoßen [6, 8].

Diese Suchwörter dienten dabei als Nukleus für die folgende Zusammenstellung an verwandten Arbeiten und Methodiken im Kontext dieser Studie, fassen diese jedoch mit einem engen Fokus nur kurz zusammen. Für weitere verwandte Arbeiten sei auf [9, 35, 38] verwiesen.

Die Smart Energy Reference Architecture (SERA) von Microsoft (2013) [29] und die Smart Grid Reference Architecture (SGRA) von IBM, Cisco und SOCAL Edison (2011) beispielsweise, wurden von der Industrie (IT und Versorger) bereitgestellt und beanspruchen das Thema einer so genannten Referenzarchitektur für Smart Grid Kommunikation und Technologien für sich. Dabei unterscheiden sich diese beiden sehr stark in ihrer thematischen Organisation sowie dem betrachteten Inhalt voneinander. Zum einen wird eine Umsetzung von Smart Grid Lösungen mittels Microsoftprodukten beschrieben, zum anderen eine in Schichten untergliederte Kommunikationsarchitektur zur Steuerung/ Kontrolle von Smart Grid Assets.

Analog zu diesen beiden Referenzarchitekturen definiert das NIST mit der NISTIR 7628 Reihe ein logisches Referenzmodell für das Smart Grid für den Fokus auf OT (engl. Operational Technology) Sicherheit, welches zwar vom Smart Grid Architecture Model (SGAM) (erstellt von der CEN-CENELEC-ETSI Reference Architecture Working Group (RAWG) [37] im Rahmen des M/490 Mandates) referenziert wird, sich aber konzeptionell sehr stark unterscheidet. Gemeinsam ist jedoch die Nutzung des so genannten GridWise Architecture Council Stacks zur Darstellung von Interoperabilität [7].

Die „E-Energy Referenz Architektur“ [8, 33] (eine Zusammenstellung der TU München der konsolidierten Architekturen aus den bundesdeutschen E-Energy Förderprojekten im Rahmen der E-Energy Begleitforschung) und das im FP 7 „DISCERN“-Projekt erstellte Deliverable

„D4.1 - Identification of Current System Architecture“ [31] stellen beide Ansätze zur Anwendung von SGAM als Reference Designation System [40] zur Verortung von systemischen Smart Grid Lösungen zur Verfügung.

Zur Vereinheitlichung dieser Quellen bietet sich der ISO/IEC 42010: Systems and software engineering — Architecture description [32] Standard an, er bietet eine wertvolle Perspektive auf die Ziele, Inhalte und Organisation von Referenzarchitekturen in Form eines standardisierten Meta-Modells und Begriffsraumes [36].

Wissenschaftliche Beiträge wie “IT-Architekturentwicklung im Smart Grid“ [8] schlagen Ansätze vor, welche sich sowohl mit der Notwendigkeit von Referenzarchitekturen im Smart Grid aus IKT Sicht befassen, als auch Diskrepanzen aufzeigen in und zwischen den existierenden Referenzarchitekturen und ihren Umsetzungen.

Im Rahmen der Betrachtung von Regulatoren sind die Arbeiten im Umfeld „RASSA“ in Österreich zu nennen. Ziel der RASSA (Reference Architecture for Secure Smart Grids in Austria) Initiative ist es, eine Referenzarchitektur für sichere Smart Grids in Österreich zu erarbeiten und zwischen den Akteuren abzustimmen. Für die Referenzarchitektur ist die Berücksichtigung von Sicherheitsaspekten wie Betriebssicherheit (Safety), Angriffssicherheit (Security) sowie Personen- und Anlagenschutz (Protection) notwendig. Privatsphärenaspekte (Privacy) sollen ebenfalls inhärent im Designprozess der Architektur beachtet werden. Aktuell wurde 2016 das Stakeholder-Projekt abgeschlossen [10].

Die bundesdeutsche Studie „Sichere Informations- und Kommunikationstechnologien für ein intelligentes Energienetz“ [23] (VS-NfD) hat eine sicherheitsspezifische Betrachtung aller absehbaren bzw. bekannten Glieder der zukünftigen Smart-Grid/ Smart-Energy-Wert-schöpfungskette (einschl. Strom-Gas-Kopplung) und deren Interdependenzen; u.a. Endgeräte in Wirtschaft und Haushalt mit Energiemanagement, Smart Meter, Mess-Stellenbetrieb, Verteilnetze, Erzeuger, Speicher, Aggregatoren, Elektromobilität, Marktplätze und Services im Fokus. Sie untersuchte die Erfassung und Auswertung wesentlicher deutscher, europäischer und internationaler Aktivitäten, Analysen und Studien sowie die Erfassung und Bewertung potentieller Risikoklassen (Datensicherheit, Datenschutz, Cyber Crime bei Hard- und Software und entsprechend der Funktion in der Wertschöpfungskette). Dabei wurden IEC 62559 basierte Use Cases und NISTIR 7628 Modelle angewendet.

Die infraprotect Studie „Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft“ ist das Ergebnis einer gemeinsamen, auf freiwilliger Basis stattgefundenen Kooperation zwischen dem österreichischen Bundeskanzleramt, sicherheitsrelevanter Ministerien, Branchenvertretern der österreichischen Energiewirtschaft und der Energie-Control Austria als zuständiger Regulierungsbehörde. Auslöser war die zum Teil zu emotional geführte Diskussion um Sicherheitsaspekte rund um die bevorstehende Einführung der Smart-Meter Technologie. Basierend auf einer NISTIR 7628 Analyse wurden zahlreiche Risiken identifiziert, aber auch Mitigationsstrategien entwickelt.

Zusammenfassend bieten Referenzarchitekturen, abhängig von dem spezifischen Kontext der Lösung im Smart Grid, beispielsweise Sicherheit, Kommunikation, Funktionalität, und Technologie, verschiedene relevante Sichten an.

Es existiert daher de-facto nicht *„DIE EINE“* Smart Grid Referenzarchitektur, die sämtliche dieser validen Sichten subsummiert. SGAM als Reference Designation [40] Werkzeug kann dennoch auch genutzt werden, verschiedene Referenzarchitekturen einheitlich zu dokumentieren und zu vergleichen. Die diversen Ansätze, welche die Terminologie der Referenzarchitektur beanspruchen, unterscheiden sich daher sehr stark im Fokus des Inhalts. Zusammenfassend lässt sich der Schwerpunkt der Quellen den im folgenden Abschnitt beschriebenen Zielen zuweisen.

Es sind vorrangige Ziele aus den Quellen im Gebiet der Referenzarchitekturen zu erkennen, welche unter anderem Organisationen (Regulatoren, Versorgern, Herstellern, ...) helfen sollen:

1. Verstehen und Adaptieren von etablierten Methoden, um einen effektiven und belastbaren Ansatz zur technischen Absicherung der Smart Grid Umgebungen zu erhalten. Darunter fallen beispielsweise Quellen wie „Smart Grid Information Security“ (SGIS), die eine Risikoanalyse ermöglichen.
2. Regulatorische Betrachtung der kritischen Infrastruktur elektrische Energieversorgung unter den neuen Rahmenbedingungen, um geeignete Massnahmen ableiten und festschreiben zu können (RASSA).
3. Definition von belastbaren und erprobten Architekturen (inklusive Technologien, Prozessen und “weichen“ Komponenten wie Organisationen), um das Smart Grid nachhaltig abzusichern. Darunter fallen beispielsweise das NISTIR 7628 als Analysewerkzeug für Schnittstellen und Schutzbedarfe, SGAM als Verortungswerkzeug und die Sandia „Microgrid Security Reference Architecture“ als fachliches Modell im Umfeld neue Flexibilitäten im Netzbetrieb.
4. Entwickeln von spezialisierten Entwürfen auf Basis der Architekturen. Dieser Bereich wird von Modellen wie der Microsoft „Smart Energy Reference Architecture - SERA“ adressiert.
5. Erzeugen von mathematischen und algorithmischen Modellen, Simulationen und Analysen dieser Entwürfe um diese Leistungstechnisch zu evaluieren oder Fehlervorhersagen zu erzeugen. Ein Beispiel hierfür ist etwa die Architektur für Flexibilitäten und verlässliche Systemdienstleistungen im Projekt „Smart Nord“ [41], welche auch Aspekte wie Reputation und Trust-Metriken umfasst.

Die genannten Ansätze sind komplementär und unterstützen durch ihre einzelnen Bausteine eine Organisation, welche versucht, eine robuste, dynamisch reagierende Smart Grid Umgebung zu schaffen, welche nicht nur Technologien, sondern auch die Prozesse und den menschlichen Einfluss auf Prozesse innerhalb von Organisationen berücksichtigt.

2.1.2 Für die vorliegende Studie berücksichtigte Standards und Vorgehensmodelle

Während der Studienrecherche erwiesen sich vor allem die folgenden Quellen als besonders hilfreich:

- Die US NISTIR 7628 - Reihe
- Quellen aus der Umgebung des M/490 Mandats – SGIS Risikoanalyse und RAWG SGAM Modellierung
- Studien aus dem D-A-Ch Umfeld wie die BMWi SIKT Studie, die infraprotect Risikoanalyse und die RASSA Initiative Österreichs

Dabei sind vor allem die ersten beiden Quellen besonders dazu geeignet die Architektur für eine definierte, abgeschlossene Smart Grid Umgebung zu definieren. Dabei bieten diese Arbeiten Werkzeuge als umfassende und komplementäre Methoden an, welche als zentrale Bestandteile bei der Erstellung von sicherheitsrelevanten Aspekten genutzt werden sollten.

2.1.3 Exkurs: Weitere Quellen mit Bezug zum Scope

In der Gesamtheit des Studienkontext sind noch andere Quellen zu beachten, welche sich zwar nicht direkt mit der Absicherung des Smart Grids beschäftigen, aber dennoch wichtige Ansätze zur Verfügung stellen, da sie z.B. technische Grundlagen für Kommunikationssicherheit definieren.

Darunter fallen beispielweise die technischen Standards der IEC Familien 61850, 62443, 62351 und noch weitere Standards aus diesem Bereich, welche normalerweise an die Technologielieferanten adressiert sind, und sich auch hauptsächlich mit der Absicherung der einzelnen Technologien befassen. Diese werden kurz im folgenden Abschnitt aufgezählt und benannt.

Das gleiche gilt für die IEEE Standards (z.B. P2030) für das Smart Grid. Als Sekundärquellen werden sie gerade auch vom NISTIR 7628 und den M/490 Quellen referenziert, weil sie unerlässlich für die Schaffung der wichtigen Querschnittseigenschaften Interoperabilität und Sicherheit im Smart Grid sind. Aber gerade weil diese Quellen so stark eingebunden wurden, ist es für Organisationen zumeist nicht notwendig, jeden einzelnen IEEE und IEC Standard zu beherrschen und zu beschaffen, sondern es reicht meist, sich auf das NISTIR 7628 und die M/490 Werkzeuge als zitierende Primärquellen zu verlassen.

Neben den genannten Hauptdokumenten in diesem Bereich existieren weitere Quellen. Dazu gehören unter anderem die ENISA „Appropriate Security Measures for Smart Grids“ [18, 20], welche auch für die Erstellung des NISTIR 7628 und des SGAM SGIS Modells herangezogen wurden und Bezüge zur ISO/IEC 27002 und ISO/IEC TR 27019 herstellen.

Am wichtigsten erscheinen im Studienzusammenhang gerade die verwandten Arbeiten und Methodiken, die sich mit der Unterstützung von Organisation befassen, um Smart Grid Sicherheitsmethoden zu adaptieren, umzusetzen und zu etablieren, um somit eine sichere Smart Grid Umgebung zu erschaffen.

Der ISO/IEC 42010 Standard [32] und die E-Energy Arbeiten sind dabei überaus nützlich für Standardisierungsorganisationen und ähnliche Gruppierungen, um solche Umsetzungsanleitungen als Blaupausen zu erstellen. Eine grosse Anzahl dieser Blaupausen beschäftigt sich aber eher mit direkten Anleitungen speziell für Netzbetreiber und andere Organisationen, die sich mit der Anwendung, Realisierung und dem Betrieb von Smart Grid Umgebungen befassen.

Als vorläufiges Fazit ist festzustellen, dass vor allem die folgenden beiden Quellen sowohl eine weite Verbreitung als auch Praxisrelevanz aufweisen, als auch die Ziele der methodischen Seite dieser Studie bzgl. der Aspekte Schutz- und Sicherheitsanalyse im Smart Grid unterstützen:

- Die „NISTIR 7628 User’s Guide“ und verwandte Quellen: Hierin werden Ansätze aufgezeigt, um das NISTIR 7628 bei der (System-)Entwicklung und Sicherung zu verwenden. Die nordamerikanische Privacybetrachtungen sind im einem extra Teil und müssen nicht genutzt werden, können also ersetzt werden
- Die „Smart Grid Information Security (SGIS)“ und verwandte Quellen aus dem M/490: Diese Dokumente beschreiben, wie das SGAM zur Entwicklung des Smart Grids im Umfeld Security Engineering genutzt werden kann und stellen eine europäische Perspektive auf die Bewertung von Datenschutz- und Datensicherheit bereit.

Beide Quellen referenzieren sich dabei gegenseitig und zeigen auf, wie das NISTIR 7628 und das SGAM/SGIS Toolbox zusammen verwendet werden können. Zusammen bieten sie eine sich ergänzende Anleitung für Organisationen, welche sich mit den Absicherungsmöglichkeiten für das Smart Grid befassen.

Weitere Dokumente beschreiben zumeist technische Standards von speziellen Smart Grid Implementierungen (inclusive Sicherheitsaspekten) in SGAM. Die „E-Energy Referenz Architektur“ erarbeitet zusätzlich noch eine Reihe von Anwendungsfälle für gerade solche technischen Modelle.

Des Weiteren sei erwähnt, das es derzeit drei zumeist so genannte Smart Grid Referenzarchitekturen gibt, welche aber eher Methoden für Standardisierungsprozesse und -gruppen liefern und sich eher weniger zu einer holistischen Umsetzung des Scopes „Sicherheit“ im Rahmen dieser Studie eignen.

Dies gilt zum Beispiel auch für die IEC 62357 „Seamless Integration Reference Architecture for Power System Exchange“ (SIA) [9], welche sich damit befasst, bestehende IEC Standards zu kartieren, um Lücken nachzuweisen und eine Vision für die zukünftige Normungsprojekte zu bieten. Die technischen TC 57 Standards im Umfeld „Power Systems and associated data exchange“ werden jedoch wiederum bei einer Umsetzung der Koordinationsmodelle bei Versorgern eingesetzt und müssen abgesichert werden.

Die gleiche Rolle der Lückenfindung in der technischen Normung fällt dabei auch anderen Teilen aus der IEC Standardfamilie zu, und auch die IEEE P2030 (Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads) [9] bezogenen Standards fallen in die Kategorie, um ein interoperables, abgesichertes Smart Grid zu erschaffen.

2.2 Cybersecurity-Normen, -Standards und -Richtlinien mit Smart-Grid-Bezug in dem Kontext der Studie

Die im Anhang aufgeführten Regularien, Standards, Technische Richtlinien und Normen sowie generischen Dokumente sind Standards, Regularien oder Normen, die im Rahmen der Arbeiten der so genannten First Set of Standards (FSS) Gruppe im M/490 für das Umfeld „Smart Grid Security“ identifiziert worden sind. Die Liste erhebt keinesfalls den Anspruch, vollständig zu sein, sondern nennt die aus Gutachtersicht relevantesten Dokumente zur Umsetzung von Smart Grid Security im Kontext der Massnahmen der Schutzbedarfsanalyse (SBA) dieser Studie. Eine ausführliche Beschreibung der einzelnen Dokumente bzw. Reihen findet sich jeweils in [6], [8] oder [9].

Zusammenfassend ergibt sich folgende Bewertung der Vorarbeiten für den Kontext dieser Studie in Tabelle 3:

Tabelle 3: Schwerpunkte der betrachteten Cybersecurity-Normen, -Standards und -Richtlinien mit Smart-Grid-Bezug - Klassifizierung

	Bedrohungs- und Risikoanalyse	Technologieanalyse und Forschungsbedarf	Domänenüber-greifende Betrachtung	Definition von Sicherheits-Anforderungen	Verwendung einer Referenz-architektur	Standardisierungs-bedarf
IEC 62351	O	O	O	O	O	O
ISO/IEC TR 27019			O	O		
IEC 62443 / SP 99			O	O		
IEC 15118			O	O		O
NERC CIP				O		
NISTIR 7628	O	O	O	O	O	O
NIST SP 800-39	O		O			
NIST SP 800-53	O		O	O		
NIST SP 800-82			O	O		
SGAM	O				O	O
ISO/IEC 42010			O		O	O
NIST Conceptual Model	O				O	O
RFC 6272				O	O	O
ENISA Recommendations	O			O		O
BDEW Branchen-richtlinien			O	O		

Die Tabelle 3 motiviert dabei vor allem den Nutzen der NIST 7628 Serie für den Betrachtungsgegenstand dieser Studie, da sämtliche relevanten Kategorien durch sie bereits abgedeckt werden. Eine besondere Herausforderung im Kontext des Smart Grid stellt hierbei die domänenübergreifende Natur dar, wodurch Arbeiten aus den Bereichen Elektrische Netze, Informations- und Kommunikationstechnologien (IKT), Automatisierungstechnik, sowie IT und Software relevant sind, aber nicht methodisch überbetont werden sollten.

2.3 Zusammenfassung Standards und verwandte Arbeiten

Die besondere Herausforderung für das Umfeld Smart Grids ergibt sich hierbei in der Vereinheitlichung der einzelnen Arbeiten und der Destillation eines Smart Grid spezifischen Gesamtkonzeptes. Spezifische Arbeiten wie etwa das M/490 SGAM oder die IEC 62559 hierzu liefern Ansätze, wie eine Vereinheitlichung erreicht werden kann. Auf hoher Abstraktionsebene existieren hierzu verschiedene Positionspapiere, die sich insbesondere den Themen „Schutzaspekte“ sowie „Strategie“ widmen.

Die in der vorliegenden Studie zusammengefassten Arbeiten stellen eine Methodik dar, die international erprobten Best Practice Ansätze wiederverwertbar macht. Dafür werden insbesondere verfügbare Anforderungs-Sammlungen mittels der IEC 62559 Anwendungsfallvorlage integriert. Daher sind insbesondere Arbeiten von Interesse, die nicht nur Konzepte, sondern vor allem auch umfassende Sammlungen an (Sicherheits-)Anforderungen zur Verfügung stellen. Insbesondere das „NISTIR 7628 Guidelines for Smart Grid Cyber Security“ (National Institute of Standards and Technology) ist von Interesse, da es als Quelle auch die europäischen ENISA Anforderungen berücksichtigt hat und diese als Untermenge besitzt.

Diese Arbeit zeichnet sich durch eine schlüssige Struktur für die Ermittlung der Anforderungen sowie eine direkte Abbildung zu modellierten Smart Grid Architekturen aus. Ausgehend von einem logischen Referenzmodell für Schnittstellen (LRM) des NISTIR 7628 werden hier Datenaustausche zwischen einzelnen Akteuren benannt, denen wiederum konkreten Security und Privacy Anforderungen zugeordnet werden. Die einzelnen Anforderungen werden wiederum zu grösseren Gruppen zusammengefasst. Insgesamt werden 198 Anforderungen (auf Englisch High Level Security Requirements) definiert und detailliert beschrieben. Durch die Struktur des NISTIR 7628 wird dieses Konzept als vielversprechendster Ansatz eingestuft. Um ein besseres Verständnis der den NISTIR 7628 Guidelines zu Grunde liegenden Konzepte zu ermöglichen, werden diese im folgenden Abschnitt zusammenfassend im Kontext des SGAM und des Konzept der Anwendungsfälle (engl. Use Cases) beschrieben.

Es wurden daher für die Studie die folgenden großen methodischen Blöcke gewählt:

- IEC 62559 Anwendungsfallmodellierung: Um geeignet die Vorarbeiten der AWK und der Consentec zu konsolidieren und auf eine gemeinsame Struktur zu übertragen, eigent sich die IEC 62559. Sie ist erprobt, es existieren kollaborative Werkzeuge zur Bearbeitung der Anwendungsfälle und das Meta-Modell ist mit dem SGAM harmonisiert. Die Anwendungsfälle werden dazu dienen, eine hypothetische Umsetzung zu betrachten und zu bewerten.
- Das SGAM dient als Möglichkeit, auf Basis einer Anwendungsfallbeschreibung eine umgesetzte Architektur zu verorten und unter verschiedenen Aspekten zu betrachten. In besonderen können Schnittstellen, Datenobjekte und Funktionen modelliert werden. Diese stehen auch im Fokus dieser Studie. Das SGIS im M/490 bietet für ein Datenobjekt, welches sich im SGAM verorten lässt eine Analyse bzgl. Datenschutz, Risiko und Privacy. Diese Analyse würde die vorherigen Arbeiten der AWK um die SGAM Dimension ergänzen.
- Die NISTIR 7628 bietet eine Übersicht über generische Gefahren für bestimmte Systeme, Funktionen und Schnittstellenklassen. Diesen Schnittstellenklassen lassen sich

Schutzbedarfe und Schutzmassnahmen zuweisen, die auf etablierten technischen Standards beruhen.

2.4 Methodik im Rahmen der Studie

Im Rahmen dieses Abschnitts der Studie wird die Wahl der Analysemethodik und der Vereinheitlichung der Inputergebnisse aus den Studien AWK [16] und Consentec [17] kurz dargestellt. Dabei steht vor allem die Nachvollziehbarkeit der Vorgehensweise im Fokus, *nicht jedoch* der Aspekt der Vollständigkeit einer methodischen Darstellung. Dem interessierten Leser wird [30, 39, 43] als vertiefendes Material zum Verständnis der individuellen Methodik empfohlen. Zum Einsatz kommen die methodischen Blöcke aus Abschnitt 2.3.

	Vorgehen im Rahmen der Studie	Angewendete Werkzeuge
a	Übertragung der AWK und Consentec Studien in die Use Case Template zur Vereinheitlichung von Struktur und Glossar	Anwendungsfalltemplate: IEC 62559
b	Modellierung der Anwendugsfälle	SGAM Toolbox und Übertragung in NISTIR 7628
c	Sicherheitsanalyse der Datenobjekte in den modellierten Anwendungsfällen	SGIS Toolbox aus dem M/490 EU Mandat
d	Gefahrenidentifikation und Schutzbedarf für die Schnittstellenklassen	SGIS Toolbox aus dem M/490 EU Mandat
e	Identifikation und Mapping der Schnittstellen in den modellierten Anwendungsfällen	NISTIR 7628
f	Gesamtrisikoanalyse für die jeweiligen Schnittstellen	SGIS Toolbox (Ermittlung des Risikofaktors) und NISTIR 7628 (Confidentiality, Integrity und Availability Analyse)
g	Identifikation der Schutzmassnahmen für die jeweiligen Schnittstellen	NISTIR 7628

Abbildung 4: Vorgehen im Rahmen der Studie – Gefahrenidentifikation und Definition der Sicherheitsanforderungen

Die Abbildung 4 präsentiert die sieben operativen Phasen im Vorgehen der Studie, deren Ergebnisse in Abschnitt 3: *Konsolidierung der Ergebnisse aus der Analyse dieser Studie* detaillierter im Kontext der fachlichen Ergebnisse vorgestellt werden.

Die folgenden Abschnitte der Studie befassen sich mit den drei als methodische Kernelemente identifizierten und motivierten Methodikbausteinen IEC 62559, SGAM/SGIS und NISTIR 7628. Diese Bausteine ermöglichen durch die Vereinheitlichung und Einordnung in der Anwendungsfallvorlage eine Wiedernutzung der Vorarbeiten in dem in Abschnitt 1 beschriebenen ISO 31000 konformen Risikomanagementprozess. Der Methodik der Studie deckt dabei die Felder Gefahrenidentifikation, Gefahrenfelder und Gefahrenanalyse/ Schutzbedarfsanalyse für die Anwendungsfälle ab.

2.5 IEC 62559 – IntelliGrid Methodology : Modellierung der Anwendungsfälle (International Electrotechnical Commission)

Anwendungsfälle (engl. Use Cases) werden erstellt, um das Verhalten eines Systems in Bezug auf dessen Anspruchsgruppen zu erfassen [4, 36].

Konkret sollen in der Smart Grid Standardisierung auf IEC Ebene mit der Anwendungsfallerstellung nach IEC 62559 bzw. IEC 62913 zukünftige Nutzungsszenarien von Energiesystemen (engl. Smart Grid Solutions) dokumentiert werden. Die einheitliche und strukturierte Dokumentation stellt zudem eine Kommunikationsgrundlage für die an der Systementwicklung beteiligten Akteure dar und die Analyse der Anwendungsfälle ermöglicht eine Ableitung von Anforderungen an die Systementwicklung (vgl. Abbildung 5).

Aufbauend auf den ermittelten Anforderungen kann schliesslich die Konzeption von Datenmodellen, Schnittstellen, Datenaustauschprozessen, Protokollen, aber selbstverständlich auch Sicherheitslösungen wie im Rahmen dieser Studie etc. erfolgen.

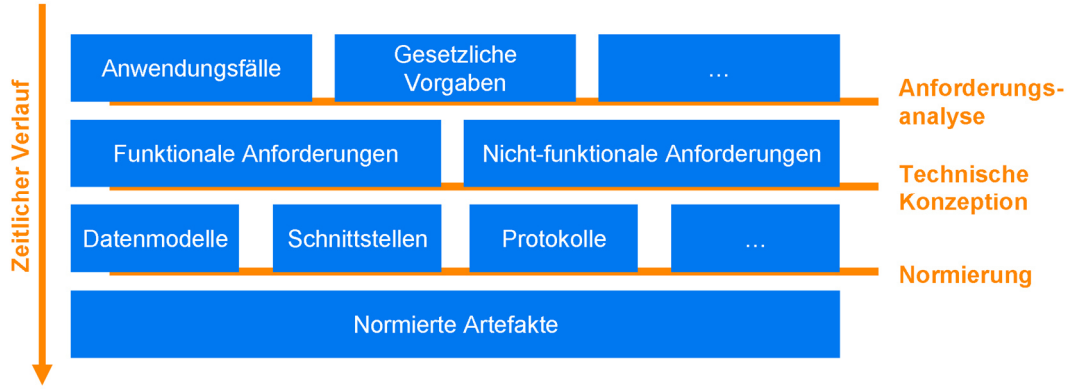


Abbildung 5: Vom Anwendungsfall zu normierten Artefakten

Mit einer soliden Basis von Anwendungsfällen, die normungsrelevante Bereiche des zukünftigen Energiesystems abdecken, und den daraus resultierenden Anforderungen wird die Basis geschaffen, um interoperable auch länderübergreifend technisch einheitliche Lösungen zu konzipieren. Aufgrund der Komplexität des Smart Grids, insbesondere aufgrund der verschiedenen Akteure und Systeme wie sie ja auch in dieser Studie betrachtet werden, sollen vereinheitlichte Anwendungsfallbeschreibungen zur Schaffung eines gemeinsamen Verständnisses sowie für die Entwicklung und Identifikation von Schnittstellen und Datenmodellen eingesetzt werden. Dieser Aspekt ist auch für die Integration der Ergebnisse der AWK und Consentec Studien höchst relevant. Aus Sicht der Normung spielt neben den genannten Zielen auch die Identifikation von Normungsbedarf oder auch Regulierungsbedarf eine entscheidende Rolle.

Anwendungsfallbeschreibungen sollen für unterschiedliche Zielgruppen wie

- Unternehmen in der Energiewirtschaft
- IT-Hersteller
- Gerätehersteller
- Normungsorganisationen
- Gesetzgeber/ Regulatoren
- Unternehmen aus anderen Branchen als der Energiewirtschaft
- Verantwortliche für IT-Sicherheit in Unternehmen und der Branche

konzipiert werden. Dies impliziert, dass Anwendungsfallbeschreibungen für ein so umfassendes Thema nur durch das Einbeziehen mehrerer Beteiligter mit unterschiedlichem Hintergrundwissen und Perspektiven zu realisieren sind. Anwendungsfallbeschreibungen stellen in

diesem Szenario das zentrale Element zur Beschreibung von Anforderungen und allgemeiner Funktionalität für Smart Grid Systeme dar, sie sollen die Zusammenarbeit zwischen verschiedenen Experten (bspw. Fach- und IT-Experten), Branchen, Organisationen und Komitees unterstützen. Weiterhin stellen Anwendungsfälle die Grundlage für die weitere Standardisierungsarbeit und den Entwurf von Interoperabilitätstests dar. Aufgrund der Komplexität wird eine klare Methodik und Klassifikation sowie eine entsprechende Werkzeugunterstützung gefordert.

Innerhalb dieser Studie wird für die Modellierung der Consentec Anwendungsfälle das so genannte Use Case Management Repository (UCMR) des OFFIS eingesetzt, um die Verwaltung einer Vielzahl von Anwendungsfallbeschreibungen zu ermöglichen. Dazu ist eine strukturierte, einheitliche Beschreibung zwingend erforderlich, um konsistente und strukturell ähnliche Beschreibungen zu erstellen. Gefordert ist ferner eine hohe methodische und inhaltliche Qualität sowie die Möglichkeit des Wiederauffindens von Anwendungsfällen, um den Aufwand der Dokumentation auch zu rechtfertigen.

Die IEC 62559 Vorlage (engl. Template) gliedert sich in zwei grosse Teile, einen Teil der als Basic Template bekannt ist und der Abschnitt 1 und 2 der Vorlage umfasst. Ein Ausfüllen dieses Teil des Formulars führt zu einer kurzen, wenig technischen Beschreibung des Anwendungsfall und wird typischerweise einen Umfang von maximal 4 Seiten an Ende der Anwendungsfalldokumentation erreichen. Die weiteren Abschnitt 3 und fortfolgend sind für eine detaillierte Beschreibung mit hohen Anforderungen an den technischen Detailgrad reserviert. Eine solche Anwendungsfallbeschreibung umfasst typischerweise, je nach Anzahl der Szenariovarianten, 35 Seiten. Für eine detaillierte Beschreibung und eine Ausfüllhilfe der Template ist [9, 36] als Quelle zu nennen. Im Rahmen dieser Studie steht das Template im Anhang (6.7) der Studie unkommentiert zur Verfügung, um aufzuzeigen, welche Informationen in welcher Struktur aus den Basisstudien konsolidiert worden sind.

2.6 Die SGAM/SGIS Toolbox

Vom Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Control[5] (JRZ) an der FH Salzburg wurde die "*SGAM-Toolbox*" entwickelt und unter der MIT Lizenz („free to use") veröffentlicht. Die Toolbox [43] ermöglicht *Model Driven Engineering (MDE)* für Smart Grid Systeme, d.h. eine Entwicklung einer Lösung basierend auf Modellen, die mittels eines Prozesses weiter und weiter auf dem Weg zur Implementierung verfeinert werden, ohne dabei die eigentlich Entwicklungsumgebung wechseln zu müssen. Kernelement ist eine *Domain Specific Language (DSL)*, d.h. einer branchenspezifischen Modellierungssprache, auf Basis des europäischen *Smart Grid Architecture Model (SGAM)*[6].

[5] www.en-trust.at

[6] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_reference_architecture.pdf

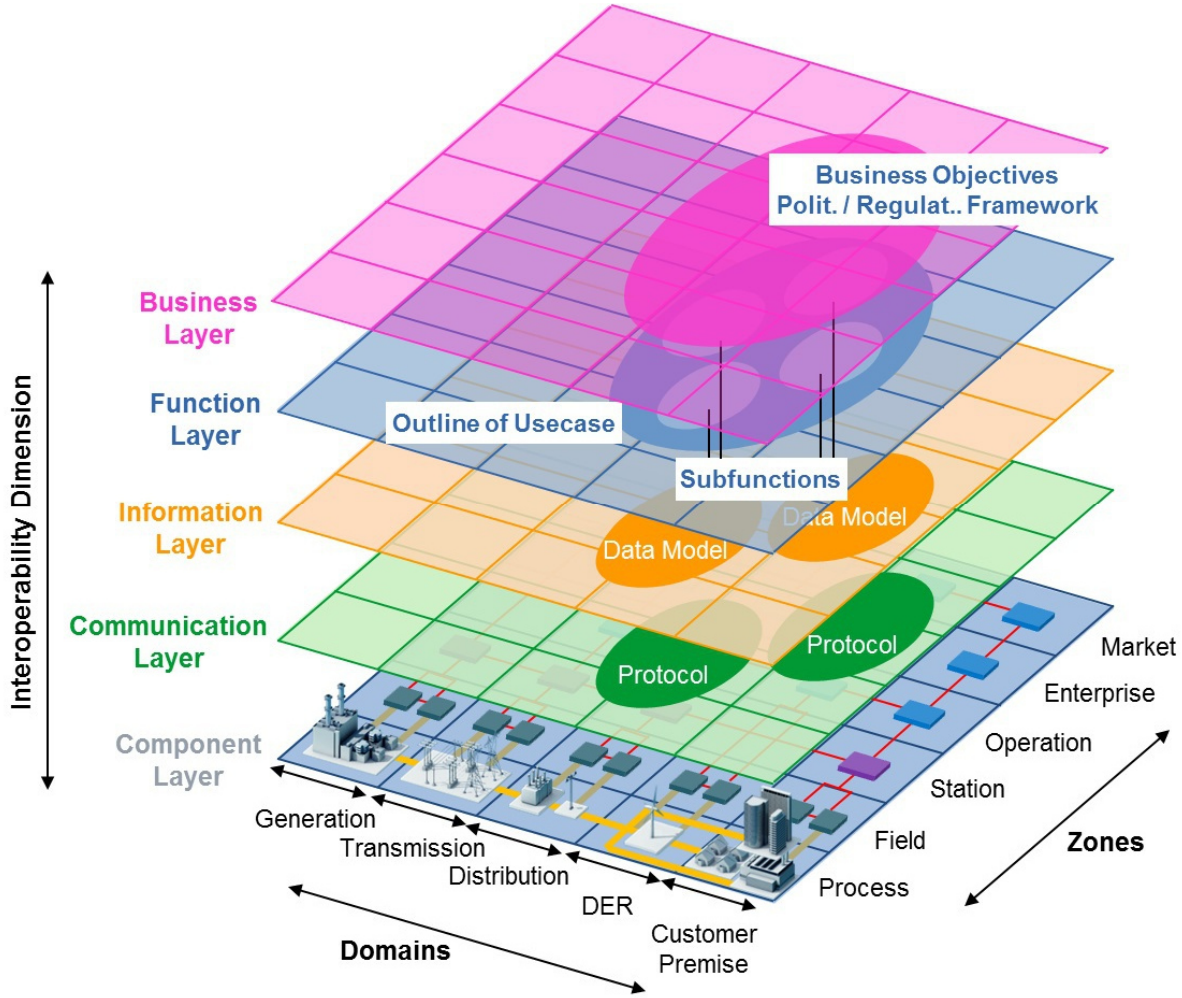


Abbildung 6: Das Smart Grid Architecture Model SGAM

Die SGAM-Toolbox der FH Salzburg ermöglicht eine durchgängige und konsistente, Modell-basierte Entwicklung und Integration komplexer Smart Grid Systeme. Zusätzlich stellen die Modelle eine gemeinsame Basis für den Austausch zwischen den beteiligten Stakeholdern aller Disziplinen und Domänen während des gesamten Entwicklungsprozesses dar.

Das Smart Grid Architecture Model (SGAM), das im Rahmen der Bearbeitung des EU-Mandats M/490 entwickelt wurde, dient der Konzeptualisierung von Smart Grids. In dem Modell werden Smart Grid Anwendungsfälle aus architektonischer Sicht betrachtet und das SGAM ist spezifisch und neutral in Hinblick auf Umsetzung und Technologie. Entsprechend können durch das SGAM Smart Grid Anwendungsfälle geprüft und deren Unterstützung durch Standards untersucht, sowie Lücken in den Anwendungsfällen identifiziert werden. Darüber hinaus kann die Entwicklung zu zukünftigen Smart Grid Szenarios geschildert werden, da das Modell den Prinzipien der Universalität, Lokalisierung, Konsistenz, Flexibilität, Skalierbarkeit, Erweiterbarkeit und Interoperabilität folgt.

Das SGAM wird auf den drei Achsen der Elektrische Domänen, Interoperabilitätsebenen und Energiemanagementzonen beschrieben. Bei der Modellierung wird auf fünf Interoperabilitätsebenen jeweils die Smart Grid Fläche abgedeckt, die durch die elektrischen Domänen mit der klassischen Energieflusskette und die Zonen des Energiemanagements mit der hierarchischen Struktur aufgespannt wird. Die elektrischen Domänen gehen von der Erzeugung (Generation) über die Übertragung (Transmission) und Verteilung (Distribution) der Energie bis hin zu den dezentralen Energieressourcen (DER) und dem gesondert betrachteten Kundenbereich (Customer Premise). Der Verteilnetzbetreiber und seine Betriebsmittel sind der Ver-

teilnetz-Domäne zuzuordnen, dezentrale Erzeugungsanlagen sind dezentrale Energieressourcen und die Verbraucher – unabhängig ob Gewerbe, öffentliche Einrichtungen oder Privatpersonen – gehören zur Kundendomäne. Die hierarchische Struktur des Energiemanagements beginnt in der Prozesszone (Process), dieser Zone werden die Stufenschalter und Wechselrichter der Geräte zugeordnet. Eine Stufe höher liegt die Feldzone (Field) mit dem Equipment der Feldgeräte wie den Sensoren und Kontrolleinheiten. Als Schnittstelle nach außen liegen in der Stationszone (Station) die Gateways der Feldgeräte zur Kommunikation sowie die Kommunikationsnetzwerke, die diese miteinander und mit dem System des Netzbetreibers verbinden. Die Systeme des Verteilernetzbetreibers liegen je nach Aufgabenbereich in der Betriebszone (Operation) und der Unternehmenszone (Enterprise).

Da die in dieser Studie betrachteten Systeme der Koordinationsmodelle für den Betrieb des Verteilernetzes zuständig sind, sind sie entsprechend meist der Betriebszone zuzuordnen. Über der Unternehmenszone befindet sich darüber hinaus im SGAM noch der Markt (Market).

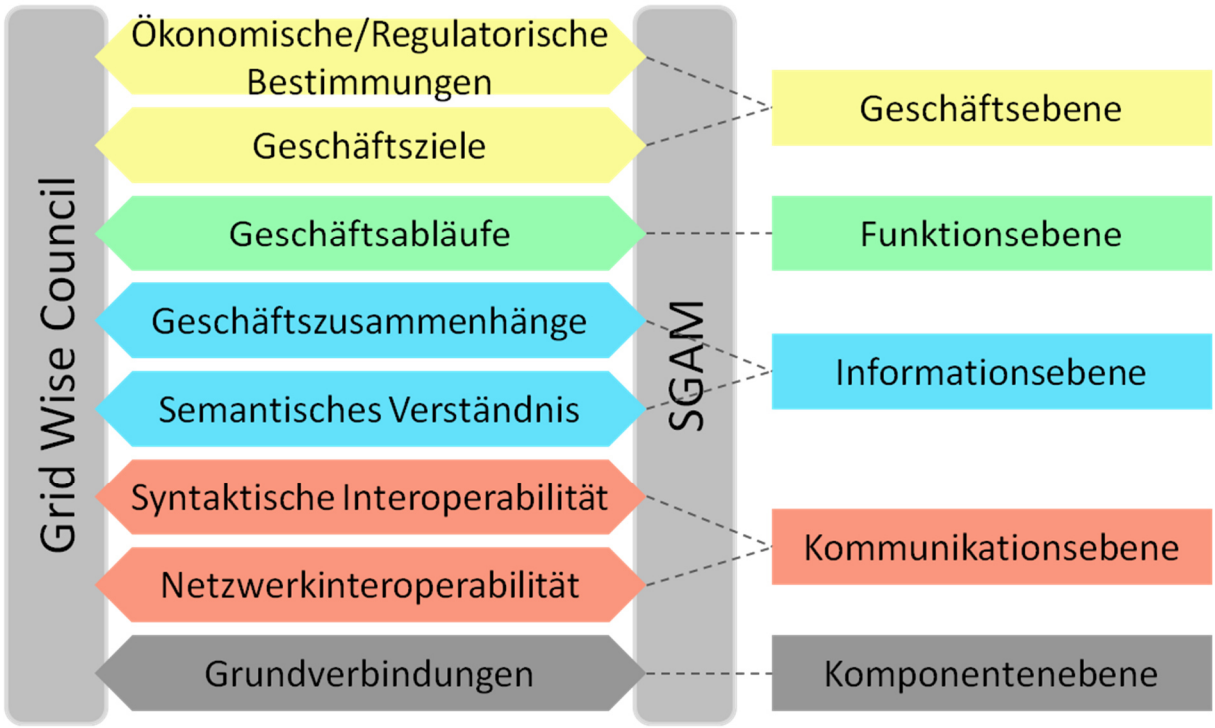


Abbildung 7: Interoperabilitätsebenen

Die dritte Dimension ist die der Interoperabilitätsebenen. Interoperabilität beschreibt die Fähigkeit zur Zusammenarbeit, wobei die Zusammenarbeit auf verschiedenen Ebenen anwendbar ist. Abbildung 7 zeigt in der linken Hälfte die acht Interoperabilitätskategorien des Grid Wise Architecture Council (GWAC), die im SGAM auf den rechts dargestellten fünf Interoperabilitätsebenen zusammengefasst werden. Auf der Geschäftsebene wird im SGAM die Interoperabilität zwischen den Geschäftszielen von Akteuren sowie ökonomischen und regulatorischen Bestimmungen dargestellt.

Das SGIS „Smart Grid Information Security“ ermöglicht die Durchführung von Risikoanalysen im Kontext des SGAM. Das SGIS im M/490 bietet für ein Datenobjekt, welches sich im SGAM verorten lässt, eine Analyse bzgl. Datenschutz, Risiko und Privacy. Ebenso ermöglicht das SGIS die Ermittlung der Risiken für die Schnittstellen in Smart Grid Systemen.

Die SGAM-Toolbox[7] wurde als Erweiterung für das Modellierungswerkzeug *Enterprise Architect* (EA) von *Sparx Systems*[8] entwickelt und um die Komponente des NISTIR 7628 LRM für diese Studie ergänzt.

2.7 NISTIR 7628 – Guidelines for Smart Grid Cyber Security

Neben der Modellierung der zu untersuchenden Fachlichkeit wird zusätzlich in dieser Studie bewährtes Fachwissen zur Analyse von Smart Grid Schnittstellen und Systemen aus der NISTIR 7628 [15] Serie genutzt, welche ein Schutzbedarfs- und Gefahrenanalysemodell für Smart Grid Systemlandschaften zur Verfügung stellt.

Das „National Institute of Standards and Technology" (NIST) ist eine sogenannte nicht-regulative Bundesbehörde innerhalb des US-Wirtschaftsministeriums. Als Ergänzung zu der „Roadmap für das Smart Grid" wurden die NISTIR 7628 Richtlinien von der „Cyber Security Working Group" (CSWG) des „Smart Grid Interoperability Panel" (SGIP) entwickelt, um einen Leitfaden für Informationssicherheit IT/OT im Smart Grid zu beschreiben.

Die NISTIR 7628 Guidelines [15] beschreiben einen Ansatz für die Identifikation von Cyber Security Aspekten sowie zur Auswahl und Adaption von Security Anforderungen, um den identifizierten Sicherheitsaspekten geeignet zu begegnen. Besonderer Fokus wird hierbei auf die Interoperabilität der individuellen Securitylösungen über die gesamte kritische Infrastruktur gelegt. Vom Selbstverständnis der Guidelines her dienen diese als flexibles Framework für die Absicherung von Smart Grids sowohl aus der Entwicklungs- als auch der Betriebsperspektive. Dies wird durch die unterschiedlichen Kategorien reflektiert.

Der Report unterteilt sich in die folgenden drei Hauptdokumente, wovon im Rahmen dieser Studie die Teile 1 und 3 zu Einsatz kamen:

Volume 1 mit dem Titel ***„Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements"*** beschreibt die genutzte Methode zur Identifikation von High-Level Security Anforderungen und ist damit für dieses Projekt die relevante Grundlage. Es werden Informationen zum Smart Grid und zu Cyber Sicherheitsstrategien vorgestellt. Das Ziel ist es, die Zuverlässigkeit des Netzes und die Vertraulichkeit von sensiblen Daten zu gewährleisten. Ein High-Level Diagramm mit einer Verortung der Systeme in den konzeptuelle Fokus des NIST wird beschrieben; es dient dazu, die Akteure in den Domänen (Operation, Service Provider, Markets, Transmission, Distribution, Customer und Generation) zu verorten. Darauf aufbauend entsteht ein übergreifendes Referenzmodell. Durch dieses werden 22 so genannte logische Interface-Kategorien (im weiteren Schnittstellenklassen genannt) – innerhalb und übergreifend über sieben Smart Grid Domänen – identifiziert und definiert. Daraus werden sogenannte Smart Grid Cyber Security Requirements (SG-CySecReq) abgeleitet.

Volume 2 mit dem Titel ***„Privacy and the Smart Grid"*** betrachtet verschiedene Arten von Datenschutz. Es wird beschrieben, welche Arten von zusätzlichem Informationsaustausch im Smart Grid stattfinden und es wird diskutiert, ob dies zu potenziellen Datenschutzproblemen führt. Dabei wird eine Nordamerikanische Sicht eingenommen. Im Rahmen dieser Studie wird dieser Teil daher ignoriert und in der Methodik durch die Analysen der AWK-Studie [16] sowie eine Analyse mittels SGIS Toolbox ersetzt.

Volume 3 mit dem Titel „***Supportive Analyses and References"*** beschreibt potentielle Schwachstellen aus verschiedenen Bereichen des Smart Grids. Ausserdem wurden mit Hilfe einer Bottom-Up Analyse spezifische so genannte Cyber Security Probleme und Risiken des

[7] www.en-trust.at/SGAM-Toolbox

[8] www.sparxsystems.com

Smart Grids im Betrieb ermittelt. Dabei wurden die Grenzen der aktuellen Standards und Normen identifiziert. Dieser Teil bietet einen technischen Background zur Umsetzung der Massnahmen zum Schutz der Schnittstellenklassen mittels verschiedener technischer Standrads, wie sie aus Sicht der M/490 auch im Anhang dieser Studie aufgeführt sind. Darauf basierend werden Forschungs- und Entwicklungsfragen vorgestellt sowie Aufgaben an das SGIP gespiegelt.

2.7.1 Methodik für die Erstellung der NISTIR 7628 Guidelines

Das Ziel der NISTIR Guidelines ist die Entwicklung eines Frameworks für die Formulierung und Umsetzung einer effektiven Cyber Security Strategie. Dies erfordert insbesondere einen ganzheitlichen Ansatz für die Beurteilung der möglichen Risiken. Eine effektive Risikobeurteilung wiederum erfordert systematisches Dokumentieren und Priorisieren bekannter und erwarteter Vulnerabilitäten (Bedrohungen) sowie deren potentieller Konsequenzen.

Risiko ist hierbei das Potential für ein unerwünschtes Ergebnis als Produkt aus Wahrscheinlichkeit des Eintretens und assoziierten Schadensausmasses. Dies ist auch die Arbeitsdefinition für diese Studie. Um ein Risiko berechnen und abschliessend bewerten zu können, müssen daher vorher beide Faktoren parallel ermittelt werden.

Die NISTIR 7628 Guidelines liefern hierfür ein generisches Analysemodell [39, 41].

Der Smart Grid-Risikoevaluierungsprozess, wie er von der Cyber Security Working Group (CSWG) (siehe Anhang) umgesetzt wurde, basiert auf existierenden Ansätzen sowohl aus dem privaten als auch öffentlichen Sektor. Er umfasst die Identifikation von Assets, Vulnerabilitäten und Gefährdungen sowie die Formulierung von potentiellen Konsequenzen. Wie eingangs geschildert umfasst das Smart Grid Systeme aus IT, Telekommunikation und Energieversorgungs-Technologie, wodurch der Risiko-Abschätzungsprozess auf alle drei Domänen angewendet wurde.

Die resultierende Methodik, die von der Cyber Security Working Group (CSWG) zur Ermittlung der in dieser Studie genutzten Massnahmen zur Absicherung der Schnittstellenklassen angewendet wurde, besteht aus fünf konkreten Schritten, welche detailliert für den interessierten Leser im Anhang dieser Studie zu finden sind.

2.7.2 Umsetzung der NISTIR 7628 Guidelines im Rahmen der Studie

Die Anwendung der NISTIR Guidelines wird mit einer Werkzeugunterstützung mittels der SGAM Toolbox der FH Salzburg[9] umgesetzt, so dass auf Basis der in den Anwendungsfällen identifizierten Schnittstellenklassen, Kommunikationsverbindungen und Datenobjekte eine Vertraulichkeits-, Integritäts- und Verfügbarkeits-Analyse vorgenommen werden kann, die in den folgenden Schritten durch eine Bedrohungsanalyse für eben diese Schnittstellen und Nennung von Massnahmen zum Schutz der Schnittstellen unterstützt wird.

Basierend auf diesen Bedrohungen, die auf ein Schadensausmass bei einem Angriff schliessen lassen, kann nach einer Abschätzung der Eintrittswahrscheinlichkeit ein Gesamtrisiko ermittelt werden, da sich Risiko als das Produkt von Schadensausmass und Eintrittwahrscheinlichkeit definiert. Dabei werden dediziert so genannte Cyber Security Requirements (Sicherheitsanforderungen) der NISTIR 7628 für einzelne Schnittstellen erhoben, die auf diese spezifischen Bedrohungsszenarien für Angriffe beruhen.

[9] www.en-trust.at/NISTIR

2.8 Das Smart Grid Architecture Model SGAM im Kontext der NISTIR 7628

Während der SGAM eine konsistente Modellierung Smart Grid Systeme ermöglicht, dient die NISTIR Richtlinie die Formulierung und die Umsetzung einer effektiven Cyber Security Strategie. Deshalb müssen die NISTIR 7628 und der SGAM im Rahmen dieser Studie verknüpft werden, damit Schutzmassnahmen für die modellierten Koordinationsmodelle definiert werden können und damit eine entsprechende Risikoanalyse durchgeführt werden kann. Die Verknüpfung der NISTIR 7628 und des SGAM soll neben der Realisierung des Security-by-Design-Prinzips auch Informationssicherheitsaspekte in das SGAM integrieren und das amerikanische Sicherheitsmodell im SGAM verorten. Dadurch kombiniert man die in der Methodenanalyse als zielführend identifizierten Ansätze. Das NIST weist eine sehr gute Analyse von existierenden, generischen Schnittstellen auf, während das SGAM eine Kombination mittels der SGIS Risikoanalyse auf europäischer Ebene ermöglicht und die Überführung von Anwendungsfällen in das SGAM aus der IEC 62559.

Bisherige Arbeiten innerhalb der M/490 SGIS Gruppe zielten vor allem auf den Aspekt der Informationssicherheit aus Sicht des Datenschutzes ab (siehe Kapitel 3 dieser Studie zu den so genannten Data Protection Classes SG-DPC - Datenschutzklassen). Die Nutzung der NISTIR 7628 Arbeiten führt dazu, dass ein bereits etabliertes Vorgehensmodell zur Absicherung und Analyse der Schnittstellen des Smart Grids auch im europäischen Kontext genutzt werden kann, während europäische Methoden der SGIS vor allem in den Bereichen Datenschutz und Datensicherheit sowie der Risikoanalyse zum Einsatz kommen.

Das NISTIR 7628 nimmt eine Einteilung in die Bereiche Operation, Service Provider, Markets, Transmission, Distribution, Customer und Generation vor. Da in dem SGAM einige identische Domänen und Zonen genutzt werden, lässt sich eine intuitive Einteilung in die SGAM Darstellung und damit eine Harmonisierung der beiden Ansätze auf der funktionalen Ebene (SGAM Function Layer) finden. In dem NISTIR 7628 werden auf Basis untersuchter Anwendungsfälle 46 repräsentative Akteure identifiziert, beschrieben und den einzelnen Domänen zugeordnet.

Die einzelnen Akteure (= die Systeme) des NISTIR 7628 Modells wurden in Rahmen der Verknüpfung im SGAM auf Grundlage der Beschreibungen in NIST LRM in der SGAM Toolbox der FH Salzburg verortet, vgl. Abbildung 8. Diese Abbildung ist ebenfalls im Anhang im grösseren Format zu finden.

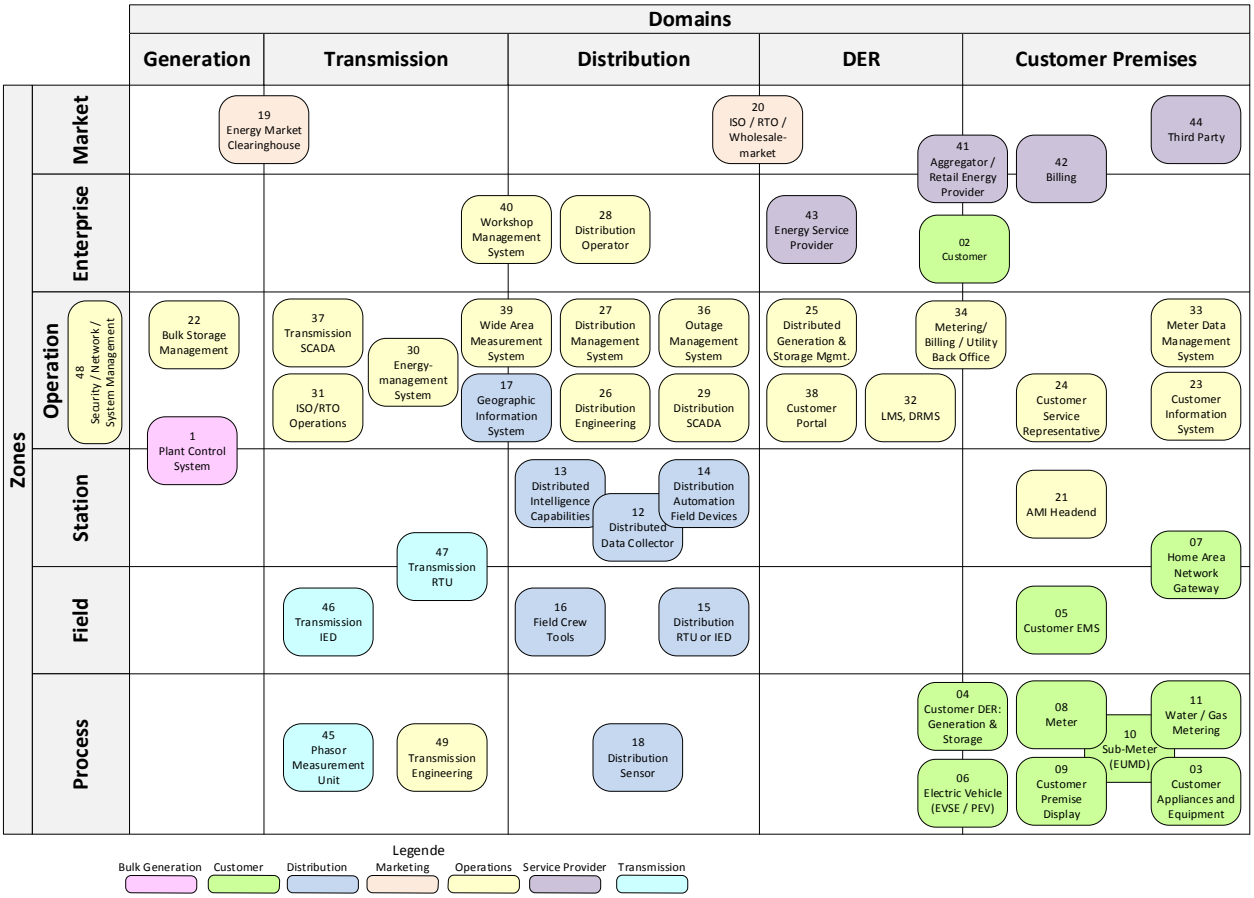


Abbildung 8: Verortung der Akteure des NISTIR 7628 im SGAM

Die Farben der einzelnen Akteure repräsentieren hier die jeweiligen Domänen der Akteure (Erzeugung – Verbraucher – Verteilung – Market – Betrieb – Dienstleistung – Übertragung) wie sie auch im NISTIR 7628 verwendet wurden.

In Abbildung 9 sind auch die logischen Interfaces aus dem NISTIR 7628, also die Schnittstellenklassen dieser Studie zu den Akteuren hinzugefügt und damit in das SGAM übertragen. Diese Abbildung veranschaulicht, wie tatsächlich die NISTIR 7628 und der SGAM verknüpft sind. Die Farbkodierung in der Legende entspricht dabei ebenso wie im Abbildung 8 den Systemen in den ursprünglichen NIST Domänen wie sie auch in der Legende genannt sind.

Diese Grafik ist eher als Symbolbild denn als operatives Modell zu sehen, da die Komplexität der Darstellung eine Auswertung nur in einem Werkzeug wie der SGAM-Toolbox ermöglicht, wie es in dieser Studie mit der FH Salzburg zum Einsatz kam. Sie zeigt aber, dass eine Abbildung der gesamten NIST System und Schnittstellensicht auf die Funtionsebene des SGAM möglich ist und, wenn nur Ausschnitte der Gesamtmodells genutzt werden müssen, diese Darstellung für eine Analyse mittels SGAM-Methoden geeignet ist. Diese Abbildung ist ebenfalls im Anhang im grösseren Format zu finden.

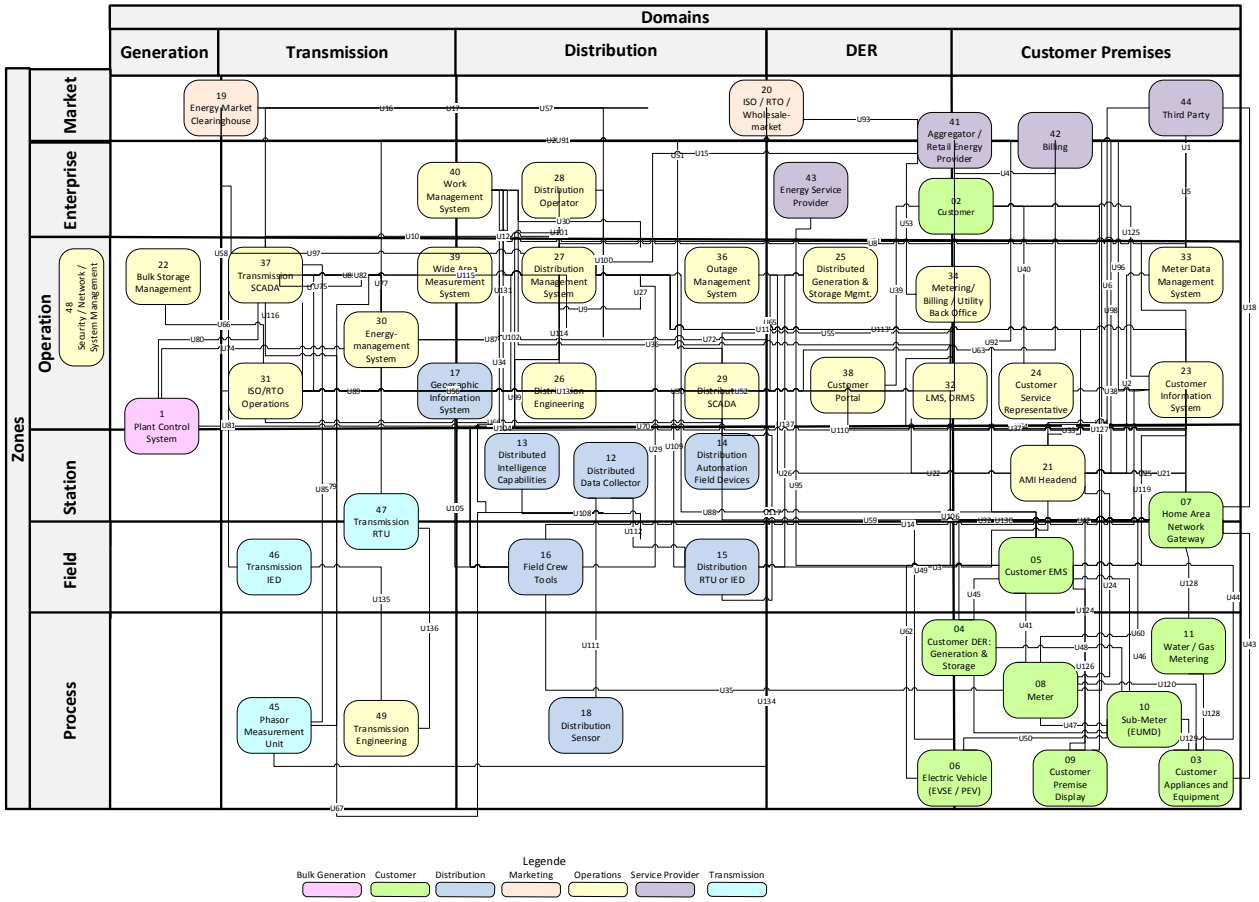


Abbildung 9: Verortung der Akteure des NISTIR 7628 ins SGAM mit logischen Interfaces

2.9 Zusammenfassung

Innerhalb dieses Kapitels wurden die Grundlagen motiviert, warum Referenzarchitekturen für ein sicheres Smart Grid nötig sind und welche Projekte hier bereits erste Ansätze geliefert haben. Dies wurde mittels eines schlagwortbasierten Desk-Research Ansatzes umgesetzt. Dabei werden mittels einer Internetrecherche über geeignete Suchmaschinen mit Hilfe der Schlagworte Quellen ermittelt, bewertet und für die Analyse herangezogen. Es konnte innerhalb dieses Schrittes die methodische Landschaft strukturiert und für die Studie einen Methodik ausgewählt werden (siehe Abbildung 4). Zumeist wird mit offenen, internationalen Standards gearbeitet.

Zur Harmonisierung der fachlichen Anwendungsfälle aus den vorherigen Studien der AWK und Consentec wird die IEC 62559 als Template eingesetzt. Diese Anwendungsfallvorlage ermöglicht es, die heterogenen Studien auf eine gemeinsame Struktur zu setzen und somit in die Methodik der Studie einfliessen zu lassen. Die Anwendungsfälle werden dann in das SGAM überführt. Dadurch können die verschiedenen Sichtweisen auf eine technische Lösung wie Funktionssicht, Datensicht, Schnittstellensicht, aber auch physische Komponenten explizierte werden. Diese IEC 62559 ermöglicht eine geeignete Modellierung der Eingabedaten in der SGAM Toolbox der FH Salzburg, um anschliessend eine Gefahren- und Risikoanalyse vornehmen zu können.

Die Literaturanalyse gab die Empfehlung, in diesem Studienprojekt die NISTIR 7628 als fachliches, logisches Referenzmodell zur Risikoanalyse zu nutzen. Das NISTIR 7628 bietet eine etablierte Basis, den Schutz einzelner Systeme und ihrer Schnittstellen zu ermitteln und später in eine Gesamtrisikobewertung einfliessen zu lassen. Ferner kann der Aspekt „Privacy“, welcher in Europa als Datensicherheit und Datenschutz geführt wird, durch eine europäische Sicht ersetzt werden. In dieser Studie wird also ein methodisches, gut dokumentiertes, und

reproduzierbares Vorgehen mittels der Verwendung von Standardmethodiken angenommen. Dieses Vorgehen, welches in der vorliegenden Studie auf die Koordinationsmodelle aus der Consentec Studie angewendet wird, kann für weitere Smart Grid Anwendungsfälle angenommen werden.

Ferner wurden in diesem Kapitel technische Standards, die später zu einer Anwendung in der Umsetzung der Massnahmen kommen werden, aus Sicht der M/490 SGIS Arbeitsgruppe identifiziert. Sie sind im Anhang (6.2) zu finden.

Abschliessend wurden die ausgewählten fachlichen Methodiken wurden kurz beschrieben, es wird der Zusammenhang von Anwendungsfällen als Eingabe für die Architekturbeschreibung im SGAM sowie der anschliessenden Sicherheitsanalyse mittels NISTIR 7628 im SGAM motiviert und kurz dokumentiert. Ausführliche Beispiele und ergänzendes Material findet sich im Anhang dieser Studie.

Der nächste Abschnitt befasst sich mit den Ergebnissen aus der Modellierung der Anwendungsfälle sowie der Auswertung der Analysen.

3 Durchführung der Analyse und Konsolidierung der Ergebnisse

Dieses Kapitel der Studie bietet eine konsolidierte Übersicht auf die Ergebnisse der Anwendungsfallanalyse mittel des NIST logischen Referenzmodell für Schnittstellen (NIST LRM) innerhalb der SGAM Toolbox. Basierend auf der Use Case Methodik aus Kapitel 2 dieser Studie wurden die Anwendungsfälle innerhalb eines SPARX Enterprise Architect Modells (Werkzeug für die Visualisierung der modellierten Use Cases) auf den verschiedenen SGAM Ebenen modelliert.

Aus Gründen der Übersichtlichkeit sind diese Anwendungsfallmodellierungen in dem hier vorliegenden Dokument jedoch nicht komplett enthalten, ein Reporting Export für jeden Anwendungsfall umfasst circa 80 Seiten. Zum Zweck der Ergebnisdokumentation sind vor allem die ausgetauschten Datenobjekte und die Informationsebene (engl. Information Layer) der jeweiligen SGAM Modellierung in der SGAM Toolbox von Bedeutung.

Basierend auf den SGAM Modellen wird ergänzend zu den Datenschutz- und Datensicherheitsresultaten eine Gefahrenanalyse auf Schnittstellenebene durchgeführt. Dabei ist zu beachten, dass Schutzklassen, wie sie in der NISTIR 7628 bezeichnet werden, auch stets schutzbedürftig sind, also auch Gefahrenklassen darstellen.

Analog zu der Methodik in der infraprotect Risikoanalyse für Österreich wird dies auch in dieser Studie entsprechend gehandhabt. Die Schnittstellenklassen (NISTIR Logical Interface Categories, LI-Categories) sind daher der Betrachtungsgegenstand der Gefahrenfelder, die Zuordnung der Schnittstellen zu den individuellen Anwendungsfällen ergibt die Gefahrenidentifikation.

Darauf basierend erfolgen im Rahmen dieses Kapitels Betrachtungen zu einer möglichen Risikoanalyse. Weil das NISTIR 7628 Schutzmassnahmen definiert, nicht aber die Eintrittswahrscheinlichkeit, wurden dazu aus dem M/490 die SGIS Security-Risk Impact levels (RIL) und die SGIS Security Levels (SL) herangezogen. Die SGIS Methodik umfasst 5 so genannte Security Level, denen entsprechend Ereignisse zu geordnet werden können, etwa lokale oder europäische Stromnetzausfälle (vgl. Tabelle 4). Ein Ausfall eines Assets hat Auswirkungen im Netzbetrieb, bestimmte Assets sind dabei kritischer als andere und erhalten dadurch bei Ausfall eine höhere Schadensausmasseinstufung. Diese Kritikalität wird auf Basis der Domäne/Zone Verortung ermittelt (vgl. Tabelle 5).

Eine Formel für die direkte Berechnung der Risiken liegt aus der SGIS Gruppe nicht vor, daher wurde eine Metrik verwendet, die aus jeweils gewichteten Faktoren für Eintrittwahrscheinlichkeit und Schadensausmass eine Risikomatrix mit einer normierten Zahl ermöglicht. Abschliessend werden Massnahmen für den Schutz der Schnittstellen und Daten der Koordinationsmodelle vorgeschlagen sowie eine informierte, aber subjektive Gesamtbewertung des Risikos vorgenommen.

Schliesslich ergibt sich der Schutzbedarf für die einzelnen Anwendungsfälle aus dem NISTIR 7628 Cyber-Security Requirements Katalog.

3.1 Vorgehen im Rahmen dieser Studie

Abbildung 10 zeigt das Vorgehen im Rahmen dieser Studie sowie den Scope des Betrachtungsraumes. Dabei werden die folgenden Schritte, teilweise parallel abgearbeitet:

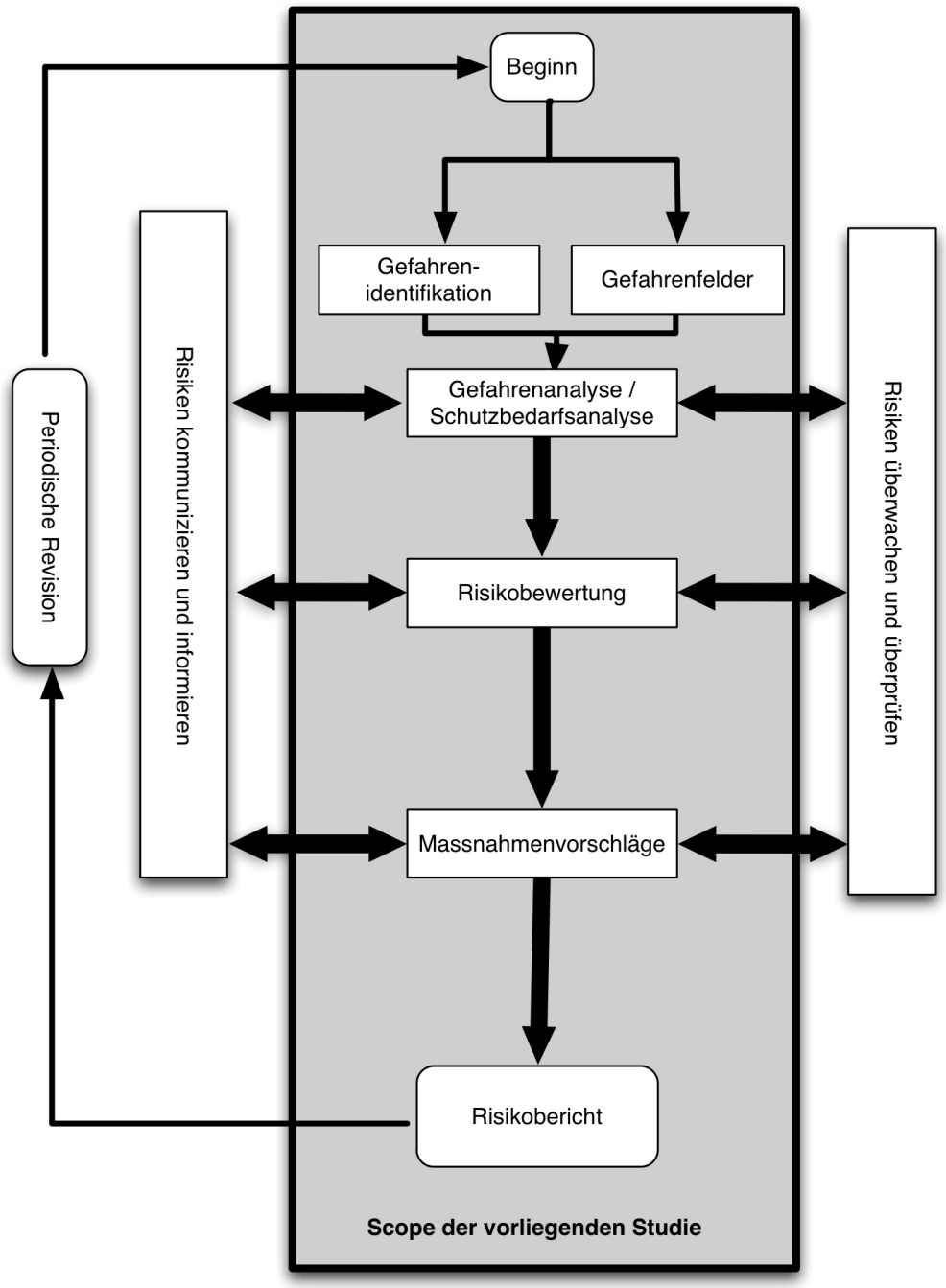


Abbildung 10: Vorgehen im Rahmen der Studie

Der Schritt „Beginn“ umfasst typischerweise den Bereich der Grunddatenerfassung, um den Risikomanagementprozess zu starten. Darunter wird eine Aufbereitung der nötigen (Eingabe-)Daten inklusive einer Datenqualitätssicherung, etwa aus einem revisionssicheren Dokumentenmanagementsystem verstanden. Innerhalb dieser Studie ist diese Ramp-Up Phase in der Modellierung und Vereinheitlichung der Anwendungsfälle mittels der IEC 62559 Vorlage zu verstehen, daher werden die einzelnen Untersuchungsgegenstände der AWK und Consentec in eine einheitliche Struktur überführt und können somit in die etablierten SGAM Toolbox/ NIS-TIR LRM der Auftragnehmer überführt werden.

Im nächsten Schritt „Gefahrenidentifikation und Gefahrenfelder“ wird die Modellierung der Anwendungsfälle in der SGAM Toolbox vorgenommen. Dabei werden Systeme, Akteure, Prozesse und Schnittstellen innerhalb des SGAM auf Ebene der Domains, Zones und der Layer verortet. Dadurch werden die Ergebnisse der Consentec und AWK Studien in einen Kontext gesetzt, für den es die Möglichkeit gibt, eine Sicherheitsanalyse auf Basis von generischen Anforderungen für bestimmte Koordinaten im SGAM vorzunehmen. Dies wird durch die Verortung der Best Practices des NISTIR 7628 Referenzmodells innerhalb des SGAM als Gefahrenfelderverortung ermöglicht – eine Zuordnung der Schnittstellen zu Koordinaten im SGAM ermöglicht es, die SGIS Zuordnung für das Security Level auf das jeweilige System abzubilden.

Im Schritt „Gefahrenanalyse und Schutzbedarfsanalyse“ werden die Anwendungsfälle im NIST LRM instantiiert, d.h. die generischen Systeme mit ihren Rollen, auf die konkreten Schweizer Anforderungen aus den IEC 62559 Anwendungsfällen (vier High-Level Anwendungsfälle und fünf primäre Anwendungsfälle) in ein „BFE“-NIST Modell überführt. Bestimmte Schweizer Rollen/ Systeme entsprechen dabei den US Pendants.

Fokus für die folgende Schutzbedarfsanalyse ist zum einen der Aspekt des Datenschutzes und der Datensicherheit, daher werden auf dem Information-Layer die ausgetauschten Datenobjekte für eine AWK und SGIS Analyse herangezogen um den Datenschutz und die Datensicherheit der ausgetauschten Datenobjekte zu ermitteln und zum anderen auf der Informationsebene die Schnittstellen der Anwendungsfälle, über die Daten ausgetauscht werden. Es müssen sowohl die Daten einzeln, als aus die Kommunikationskanäle zum Austausch der Daten betrachtet werden, da ein Datum statisch bei Veröffentlichung schon Schaden verursachen könnte, der Schutz der Kommunikation wiederum verhindern kann, dass ein Datum öffentlich wird. Die generischen Schnittstellen bieten dabei sowohl Schutzbedarf als auch natürlich Gefahrenpotenziale. Diese Studie wird daher die Schnittstellen mittels SGIS-RIL und einer CIA Analyse nach NIST LRM in Kombination mit den NIST Schutzbedarfen analysieren.

Der Schritt „Risikobewertung“ ermittelt für die Schnittstellenklassen der modellierten Consentec Koordinationsmodelle eine Risikozahl, die sich aus verschiedenen Faktoren für Eintrittswahrscheinlichkeit und Schadensausmass ergibt. Die Skala der Risikobewertung erfüllt dabei das Ampelprinzip und ordnet die jeweiligen Koordinationsmodelle ein. Dabei wird ein Angreiferszenario zugrunde gelegt, wie es auch in der AWK Studie genutzt wurde.

Der Schritt „Massnahmenvorschläge“ stützt sich auf die Ergebnisse der Schutzbedarfsanalyse und der Risikobewertung. Aus den Schutzbedarfen lassen sich Anforderungen und konkrete Massnahmen in verschiedenen Kategorien gemäss NISTIR 7628 ableiten.

Der Schritt „Risikobericht“ wird durch Kapitel 4 der Studie abgedeckt und setzt die identifizierten Massnahmen und Risiken nach Ampelprinzip in den Kontext der IT Sicherheit im Smart Grid für den Betrachtungsgegenstand der Studie.

3.2 Modellierung der AWK Anwendungsfälle

Die Modellierung der AWK Anwendungsfälle im Kontext dieser Studie verfolgte vor allem zwei grosse Ziele für die Umsetzung des Risikomanagements – die Ermittlung der Datensicherheit und des Datenschutzes für die ausgetauschten Daten der Koordinationsmodelle, auf der anderen Seite aber auch die technische Absicherung der Architektur der Koordinationsmodelle. Ein Fokus der Studie der AWK war die Untersuchung der Datenschutz- und Datensicherheitsaspekte für verschiedene Daten(-objekte) im Kontext von Smart Grid Systemen.

Dabei wurde eine ausführliche Analyse und Einschätzung für über 30 Datenobjekte vorgenommen, so dass diese Arbeiten auch im Kontext von Koordinationsmodellen wieder verwendet werden sollten. Es ist in dieser Studie zu prüfen, inwieweit die ermittelten Datenobjekte semantisch äquivalent zu denen der AWK Studie sind und daher gleiche Schutzeigenschaften bzgl. Vertraulichkeit, Integrität und Verfügbarkeit aufweisen, so dass die AWK Ergebnisse übernommen werden können. Dies wurde für die 16 identifizierten Datenobjekte der Koordinationsmodelle durchgeführt.

Um das zweite Ziel zu überprüfen, inwieweit das Verständnis der fachlichen Sicht auf „Flexibilitäten“ und „Koordinationsmodelle“ gleich ist, wurden ausgewählte AWK Anwendungsfälle mit Flexibilitätsbezug (schon identifiziert innerhalb der Consentec Studie, Nummern 2 „Demand Side Response“, 5 „Regionale Flexibilitäten“, 8 „Steuerung Wirk- und Blindleistung“, 12 „Zeitliche Flexibilisierung Ein-/Ausspeisung“) modelliert.

Bedingt durch die Modellierung auch dieser AWK Anwendungsfälle in der IEC 62559 konnte eine vereinheitlichte Darstellung für einen Vergleich erzielt werden, der positiv ausfiel, so dass für die Studie ein zwischen AWK und Consentec abgestimmtes Verständnis von „Flexibilitätskonzepten“ angenommen werden kann. Daher ist eine Übertragung der AWK Datenschutz und Datensicherheitsfachlichkeit auf Consentec Datenobjekte möglich und erfolgt in diesem Kapitel. Die Analyseergebnisse der AWK für die einzelnen Objekte sind daher auch für die auf die AWK Objekte abgebildeten Consentec Datenobjekte der Koordinationsmodelle gültig.

3.3 Modellierung der Consentec Anwendungsfälle

Dieser Abschnitt der Studie bietet kurz eine Übersicht auf die konsolidierten Modellierungen der Consentec Studie. Auf Basis der IEC 62559 Grundmodellierungen werden jeweils die Fälle:

- EP01: Echtzeit Engpassvorhersage
- EP02: Vorrausschauende Engpassvorhersage
- EP03: Echtzeit-Engpassbeseitigung
- EP04: Engpassbeseitigung durch Flexibilitätsbeschaffung und
- EP05: Engpassbewirtschaftung

in der SGAM Toolbox modelliert. Dadurch liegen in der Toolbox ausführliche Modelle zusätzlich zu den generischen NIST Analysekomponenten vor. Mittels Enterprise Architect können ausführliche Reports zu den einzelnen Fällen generiert werden[10]. Die Reports umfassen jeweils die exportierten SGAM Ebenen, die dazugehörigen Akteuer bzw. Systeme der Koordinationsmodelle, eine Aufstellung der dort genutzten Schnittstellen sowie die Anforderungen aus Sicht des NIST zur Absicherung der Schnittstellen.

Zum Verständnis der Ergebnisse im Rahmen dieser Analyse sind vor allem die grafischen Darstellungen der an den jeweiligen Koordinationsmodellen beteiligten Systeme und ihre passende Einordnung auf der Informationsebene im SGAM relevant, da sich so sowohl die Schnittstellen bzgl. einer SGIS Klassifizierung (d.h. Relevanz im SGAM bzgl. des Assets) als auch bzgl. der NISTIR 7628 Modellierung (d.h. Ableitung der Massnahmen zum Schutz eines Assets) identifizieren lassen.

Dieser Unterabschnitt der Studie enthält daher die fünf Informationsebenen der jeweiligen Anwendungsfälle, welche für die Koordinationsmodelle stehen. Die Abbildungen stellen jeweils eine Darstellung des jeweiligen Anwendungsfalls (EP01 bis EP05) da. Zu erkennen sind jeweils die Systeme, die ausgetauschten Daten sind an den Kanten annotiert. Auf Basis dieser

[10] Aus Gründen der Länge dieses Ergebnisdokuments der Studie sind die jeweils detailliert modellierten Anwendungsfälle der IEC 62559 sowie die generierten Analysereports aus dem SGAM Toolbox Werkzeug nicht in diesem Dokument verzeichnet, sondern liegen als extra Dateien in Form der ergänzenden Anwendungsfallmodellierung vor.

Modellierungen der Systeme wurde aus dem NIST eine Klassifizierung der Schnittstellen abgeleitet. Mittels dieser Schnittstellenklassen lassen sich nur den einzelnen Koordinationsmodellen Massnahmen zuordnen, wie im Folgenden zu sehen sein wird.

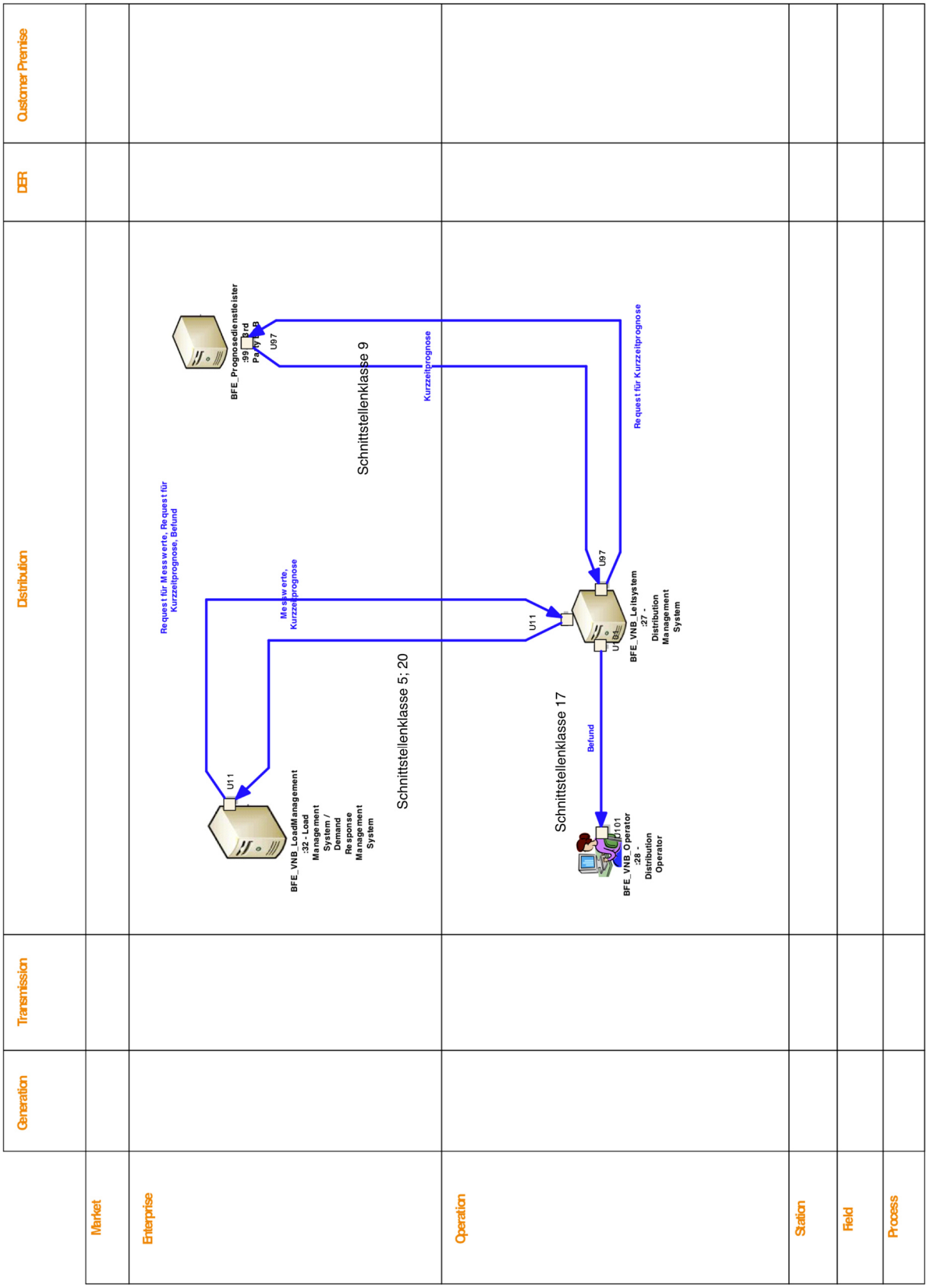


Abbildung 11: EP01 - Engpass Echtzeitprognose

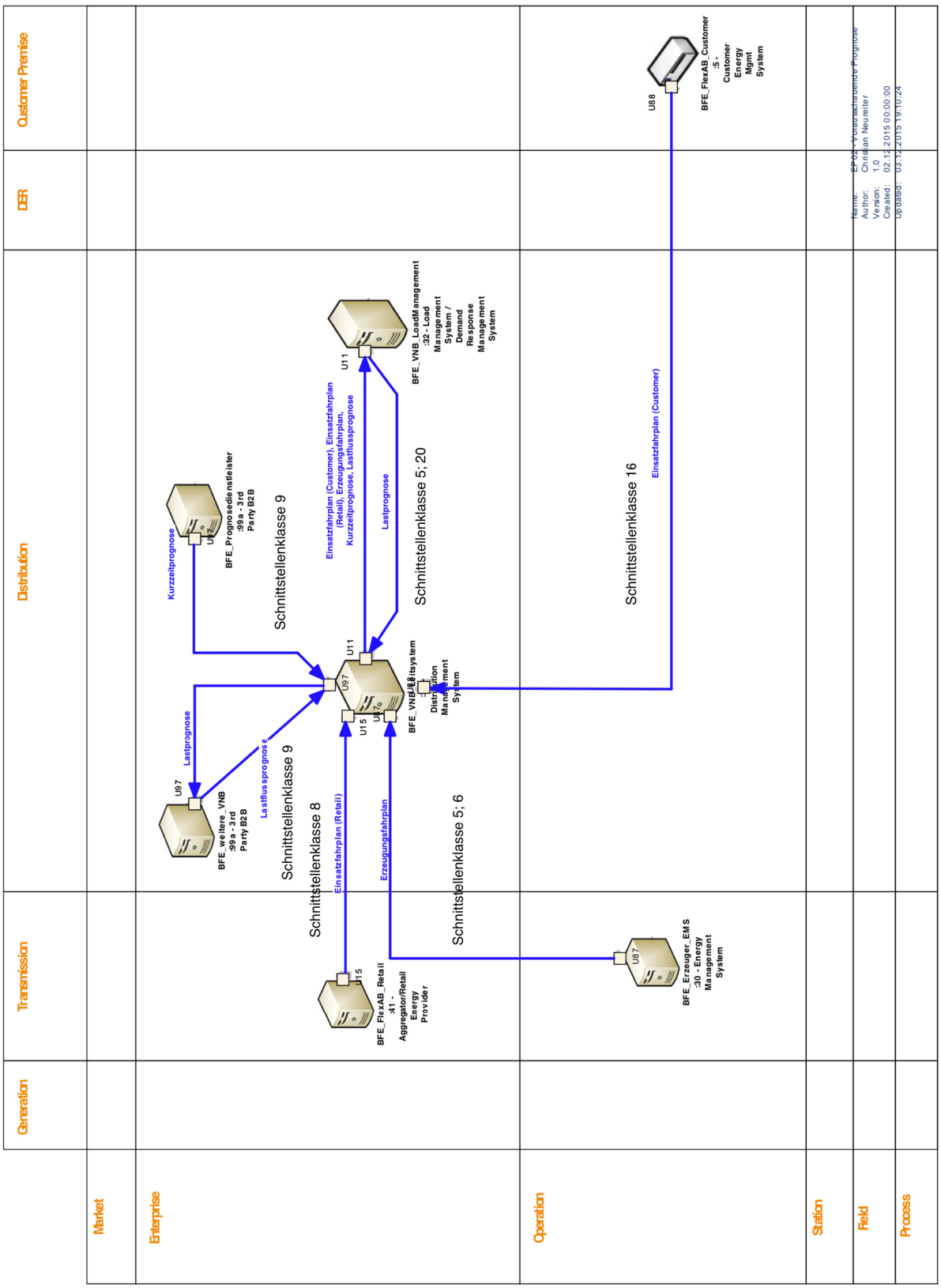


Abbildung 12: EP02 - Vorausschauende Engpassprognose

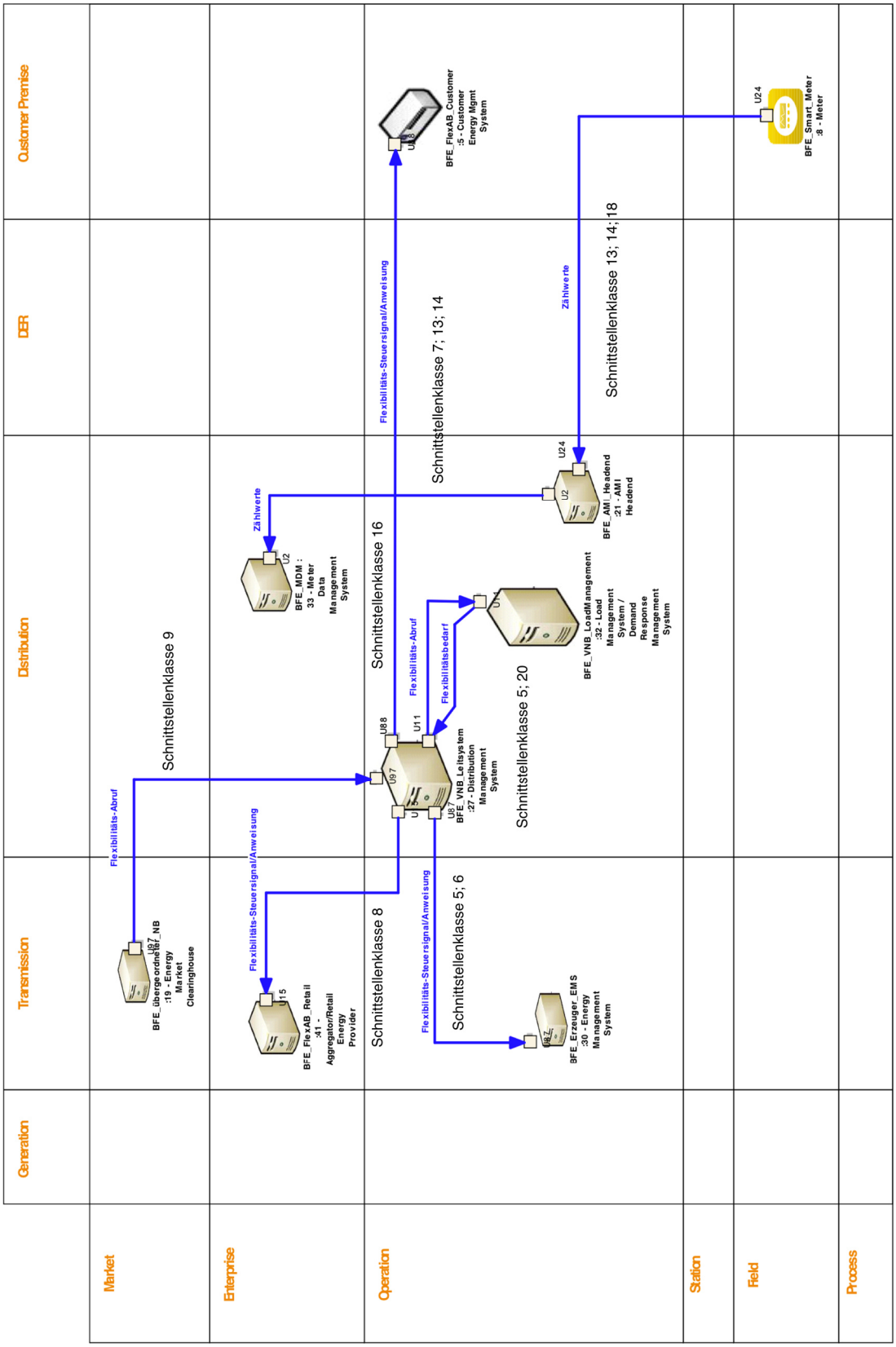


Abbildung 13: EP03 - Echtzeit Engpassbeseitigung

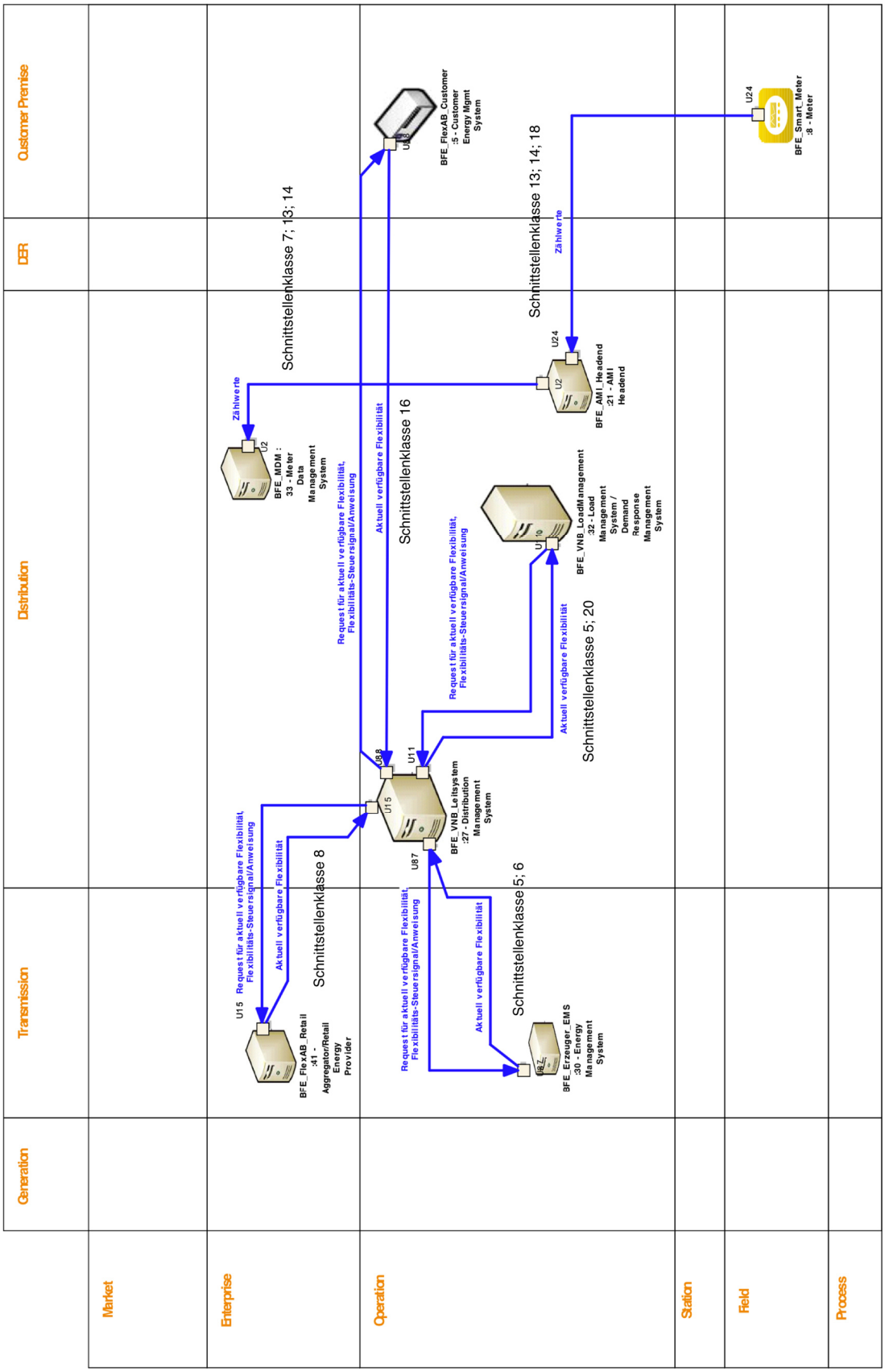


Abbildung 14: EP04 - Engpassbeseitigung durch Flexibilitätsbeschaffung

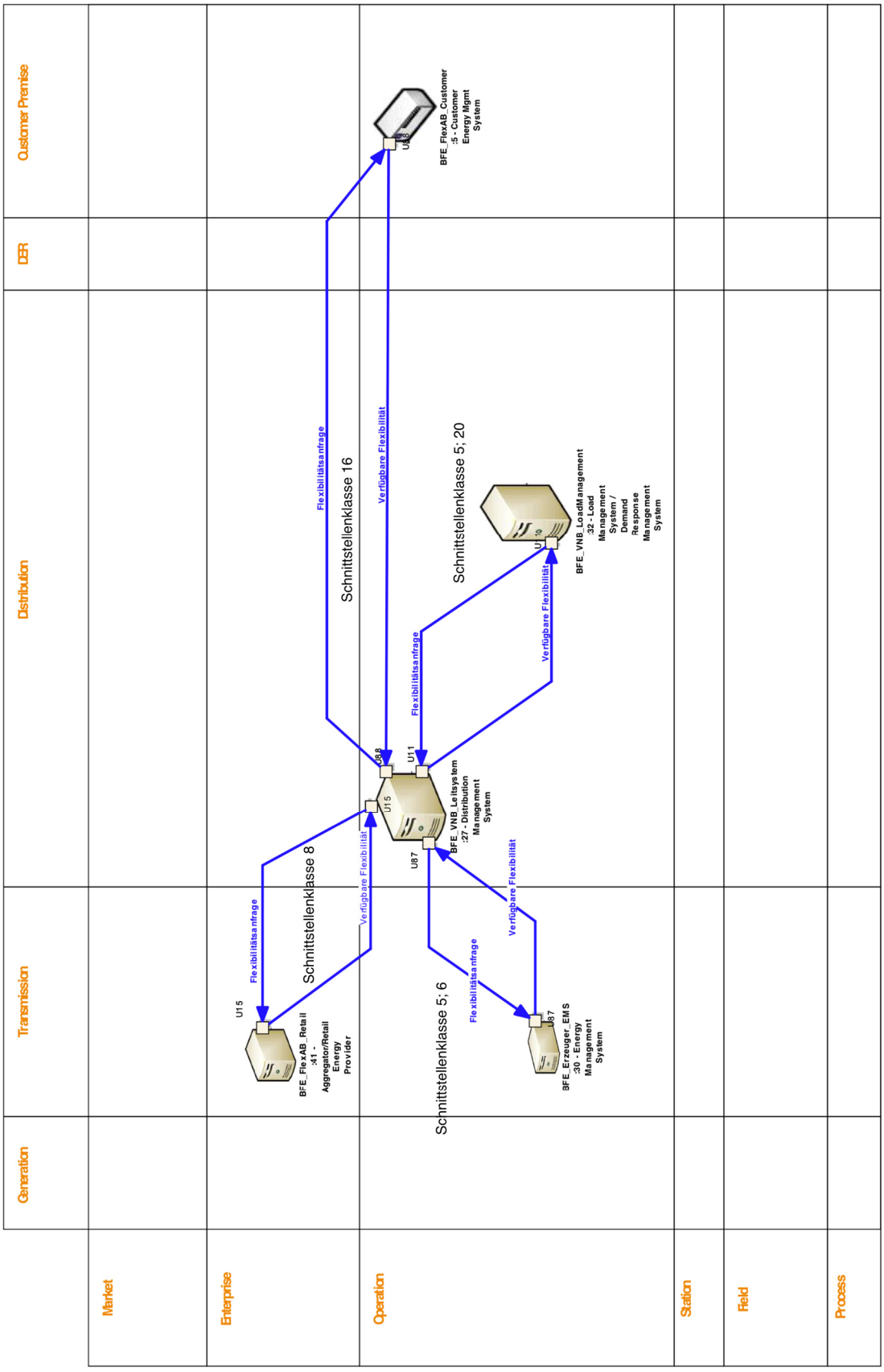


Abbildung 15: EP05 - Engpassbewirtschaftung

3.4 Kombination der Ergebnisse aus vorherigen Studien

Zusammenfassend kann bestätigt werden, dass eine Konsolidierung der Ergebnisse der AWK und Consentec Studien möglich ist und daher auf beiden Ergebnisberichten für eine Konsolidierung der Datenschutz, Datensicherheit und Massnahmenbildung im Rahmen dieser Studie aufgesetzt werden kann. Konkrete Ergebnisse dieser Konsolidierung sind in den nächsten Abschnitten dokumentiert.

3.5 Analyse Datenschutz und Datensicherheit für die Koordinationsmodelle

Innerhalb dieses Abschnitts der Studie wird eine Analyse für die einzelnen Datenobjekte in den drei Koordinationsmodellen bzw. den fünf Anwendungsfällen in der SGAM Toolbox, welche im Rahmen dieser Studie identifiziert worden sind, durchgeführt und die Ergebnisse dargestellt.

Tabelle 4 bietet eine Sichtweise der SGIS im M/490 auf verschiedene Risikolevel im Smart Grid. Diesen Risikoebenen ist jeweils ein Bezeichner zugeordnet, um auch eine Versprachlichung der jeweiligen Lage zu ermöglichen. Zur Schätzung eines Schadenausmasses orientiert sich die vorliegende Studie an der SGIS Toolbox. Es wird in der Basis SGIS Risikoabschätzung zwischen den Security Leveln hochkritisch, kritisch, hoch, mittel und gering unterschieden. Da wir jedoch nicht den Fokus UCTE Netz haben, ist entsprechend in dieser Studie eine leicht veränderte Bewertung in der Risikoanalyse getroffen worden wie im späteren Kapitel erläutert. Hauptgrund ist dabei, dass ein Krisenfall in der Schweiz im UCTE Netz ein so genannter lokaler Vorfall ist, in der Schweiz jedoch ein vollflächiger Krisenfall.

Die Schadenshöhe, die sich aus einer identifizierten Bedrohung ergeben kann, wird anhand der identifizierten Aspekte Energieversorgung, Energiefluss, Bevölkerung, weitere Infrastrukturen, Datensicherheit, Datenschutz, Leib und Leben, Reputation sowie finanzielle Auswirkungen geschätzt.

Nachfolgend werden die Einflussgrössen kurz beschrieben:

- **Energieversorgung:** Dieser Aspekt systematisiert den Schaden anhand des geographischen Umfangs eines Versorgungsnetzausfalls. Dieser Aspekt wird in dieser Studie berücksichtigt.
- **Energiefluss:** Hier wird der Schaden beschrieben, der sich durch die Einschränkungen des Stromflusses im Versorgungsnetz pro Stunde ergibt. Dieser Aspekt wird in dieser Studie gemäss VSE ICT Continuity Szenarien [11, 19] berücksichtigt. Da die SGIS eine Methodik auf die kontinentale europäische Netzebene ausgelegt ist, sind Krisen aus VSE Sicht (ein ungeplantes Verhalten der elektrischen Energieversorgung mit über 50 MWh nicht zeitgerecht gelieferten Energie) meist schon ab Security Level 3 der Tabelle 4 zu erwarten. Hauptgrund ist dabei, dass ein Krisenfall in der Schweiz im UCTE Netz ein pan-europäischer Vorfall ist, in der Schweiz jedoch ein vollflächiger Krisenfall. Daher wurde die Risikobewertung um einen Faktor ergänzt
- **Bevölkerung:** Dieser Aspekt ordnet den Schaden nach dem Umfang des betroffenen Bevölkerungsanteils ein. Dieser Aspekt wird in dieser Studie gemäss VSE Szenarien berücksichtigt.
- **Weitere Infrastrukturen:** Hier wird die Schadenshöhe nach ihren Auswirkungen auf andere Infrastrukturen, z.B. Wasserversorgung, bewertet. Dieser Aspekt wird in dieser Studie berücksichtigt.
- **Datensicherheit & Datenschutz:** Im Rahmen dieses Aspektes wird der Umfang des Schadens hinsichtlich Datensicherheit & Datenschutz bewertet. Hier wird zwi-

schen Offenlegung oder Manipulation von sensitiven oder personenbezogenen Daten unterschieden. Dieser Aspekt wird in dieser Studie durch die Anwendung der SGIS-DPC Analyse berücksichtigt.

- **Leib und Leben:** Dieser Aspekt beschreibt den Schaden für Leib und Leben nach Umfang betroffener Menschen. Dieser Aspekt wird in dieser Studie berücksichtigt.
- **Reputation:** Hier wird der Schadensumfang bewertet, der sich aus Imageverlust, z. B des Versorgers oder Flexibilitätsanbieters, ergibt. Dieser Aspekt wird in dieser Studie berücksichtigt.

Innerhalb dieses Abschnitts der Studie ist für uns die Einschätzung des Aspekts Datenschutz und Datensicherheit für die ausgetauschten Datenobjekte der Koordinationsmodelle relevant, um die Ergebnisse der AWK Analyse zu ergänzen bzw. zu bestätigen.

Security Level	Security Level Name	Security Level Beispiele
5	Hochkritisch	Pan-Europäischer Zwischenfall Assets, deren Ausfall eine Verlust von mehr als 10 GW Bilanz bedeuten Permanenter Verlust von Vertrauen Störung Energiefluss 10 GW/h
4	Kritisch	Europäischer / Ländervorfall Assets, deren Ausfall einen Verlust von mehr als 1 GW bedeuten Permanenter Verlust von Vertrauen in einem Land Störung Energiefluss 1 GW/h aufwärts
3	Hoch	Regionaler Vorfall Assets, deren Ausfall einen Verlust von mehr als 100 MW bedeuten Temporärer Verlust von Vertrauen Störung Energiefluss 100 MW/h aufwärts
2	Mittel	Städtischer Vorfall Assets, deren Ausfall einen Verlust von mehr als 1 MW bedeuten Temporärer lokaler Vertrauensverlust Störung Energiefluss 1 MW/h
1	Gering	Nachbarschaftvorfall Assets, deren Ausfall einen Verlust von unter einem 1 MW bedeuten Kurzzeitiger Vertrauensverlust Störung Energiefluss unter 1MW/h

Tabelle 4: SGIS M/490 Security Level mit korrespondierenden Impacts

Diese SGIS Security Level können nicht direkt operationalisiert werden, da es einen Bezug zu den Daten und ihrer Verortung in unterschiedlichen Schnittstellenklassen bzw. Wichtigkeit geben muss. Dieser Bezug wird in der Tabelle 5 hergestellt.

		Einschätzungen generischer Datentypen für die Zone "Operation" - SGIS-SL für SG-DPC					
SG-DPC 1: Personenbezogene Informationen	Sensitive Personenbezogenen Informationen	3 - 4	5	3 - 4	3	2 - 3	2 - 3
	Personenbezogene Informationen	3 - 4	5	3 - 4	3	2 - 3	2 - 3
	De-personalisierte, Pseudonomisierte Informationen	3 - 4	5	3 - 4	3	2 - 3	2 - 3
	Keine Personenbezogene Informationen	3 - 4	5	3 - 4	3	2 - 3	2 - 3
SG-DPC 2: Prozessdaten	Systemdaten Konfigurationsdaten Öffentliche und Private Schlüssel Rollen/Aktoren-Identitäten	3 - 4	5	3 - 4	3	2 - 3	2 - 3
	Governance- & Reporting Informationen Logs und Audit Daten	3 - 4	5	3 - 4	3	2 - 3	2 - 3
	Benötigte Informationen für Logs und Audits	3 - 4	5	3 - 4	3	2 - 3	2 - 3
	Informationen für Remotezugang	3 - 4	5	3 - 4	3	2 - 3	2 - 3
	Informationen für Remotebetrieb	3 - 4	5	3 - 4	3	2 - 3	2 - 3
	Geschäftsinformationen	3 - 4	5	3 - 4	3	2 - 3	2 - 3
	Messwerte	3 - 4	5	3 - 4	3	2 - 3	2 - 3
		Erzeugung	Übertragung	Verteilung	DER	Kunde	Im Kundenobjekt

Tabelle 5: Klassifikation der SGIS M/490 Gruppe für Data Protection Classes

Die folgenden 16 Daten-Objekte wurden innerhalb der Modellierung der Consentec Koordinationsmodelle [17] in der Modellierung identifiziert und gemäss der folgenden AWK Klassifizierung aus der Studie [16] eingeordnet.

Dabei wurden die bisherige Klassifikation der AWK um die M/490 SGIS Klassifikation aus Tabelle 5 ergänzt, damit im Rahmen der durchgängigen Studienmethodik auch diese Sicht auf den Betrachtungsgegenstand der statischen Datenobjekte der Koordinationsmodelle vorliegt.

Die SGIS-Methodik unterscheidet zwischen den Aspekten der Datensicherheit und des Datenschutzes (unter der Verwendung des so genannten Smart Grid Data Protection Class Concepts – SG-DPC) sowie eines Risikoimpacts eines Versagens von Smart Grid Lösungen mittels fünf Sicherheitsebenen. Bezüglich der Skala ist zu erkennen, dass bzgl. der Dataprotectionklassen (DPC-1 und DPC-2) eine Unterscheidung zwischen 1 und 2 vorgenommen wird. Dabei handelt es sich bei Klasse 1 um so genannte personenbezogene Daten, während es sich bei Klasse 2 um so genannte Prozessdaten handelt. Eine feinere Klassifikation ist in Tabelle 5 zu erkennen. Ein Verlust von personenbezogenen Daten bzw. eine Offenlegung hat meist keine direkten Auswirkungen im Netzbetrieb, wohl aber bzgl. der Reputation eines Unternehmens. Dies kann zu einem Vertrauensverlust unterschiedlicher Dauer führen, einem Reputationsverlust. Bei Prozessdaten kann es zu einer direkten Bedrohung der Assets bzw. des Netzbetriebs kommen. Sind Daten sowohl Prozessdaten als auch personenbezogenen Daten (z.B. Smart Metering Messwerte für die Nutzung im Netzbetrieb). So kann sich je nach Betrachtungswinkel ein unterschiedlicher Wert ergeben, da die Schäden bei Offenlegung unterschiedlich sein können.

Betrachten wir die Modellierungen der Koordinationsmodelle in den Anwendungsfällen EP01-EP05, so ist zu erkenn, dass die System, also auch die Prozessdatenschnittstellen, stets nach der Domain „Verteilung“ zu klassifizieren sind, zumeist auch in der Zone Operation, da hier das zentrale System angeordnet ist. Bzgl. der Einstufung 3-4 welche für diese Daten vorgeben ist, wird für einen genauen Wert empfohlen, fallweise bei einem Interface Richtung Übertragungsdomäne aufzurunden bzw bei einem Interface Richtung Kundendomäne abzurunden und somit die Werte 3 oder 4 zu nutzen. Aus Gründen der Übersicht ist passend zu den deckungsgleichen AWK Datenobjekten (hier fett markiert) *kursiv* die identischen Kurzbeschreibungstexte der Analyse aus der AWK Studie [16] eingefügt.

Rahmenvereinbarung (Kontrakt)

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	2	Smart Grid Information Security – Security Level	3

Entspricht AWK-Datenobjekt: *Abrechnungsdaten*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Für die Versorgungssicherheit sind die Abrechnungsdaten unkritisch.
Datensicherheit aus Gründen des Datenschutzes: Aus Datenschutzgründen ist die Vertraulichkeit und die Integrität der Abrechnungsdaten kritisch, da diese nicht anonymisiert werden.

Datenschutzrechtliche Qualifikation der Daten Bei Abrechnungsdaten handelt es sich um Daten für die Kundenrechnungsstellung wie Namen, Adressen, Angaben zur Bankverbindung usw. Sie stellen Informationen dar, welche eine Person bestimmen oder zumindest bestimmbar machen. Es handelt sich bei solchen Angaben um Personendaten gemäss Art. 3 lit. a DSG.

Messwerte

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	1 oder 2	Smart Grid Information Security – Security Level	4 bei DPC 2, 3 bei DPC 1

Entspricht AWK-Datenobjekt: *Messwerte Endgeräte*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Aus Sicht der Versorgungssicherheit kann die Integrität der Messwerte der Endgeräte kritisch sein, insbesondere wenn aufgrund deren an eine grössere Anzahl von Gebäudeautomationen gleichzeitig falsche Steuersignale gesendet werden.
Die Verfügbarkeit und Vertraulichkeit dieser Daten ist für die Versorgungssicherheit unkritisch. Datensicherheit aus Gründen des Datenschutzes: Für den Datenschutz sind die Messwerte der Endgeräte als kritisch einzustufen, hinsichtlich deren Vertraulichkeit und Integrität, da Rückschlüsse auf personenbezogene Daten möglich sind.

Buchung

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	1	Smart Grid Information Security – Security Level	3

Entspricht AWK-Datenobjekt: *Kundendaten*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Für die Versorgungssicherheit sind die Kundendaten unkritisch.

Datensicherheit aus Gründen des Datenschutzes: Aus Datenschutzgründen sind die Vertraulichkeit und die Integrität der Kundendaten kritisch, weil es sich um personenbezogene Daten handelt.

Datenschutzrechtliche Qualifikation der Daten Hierbei handelt es sich insbesondere um Angaben zu einer Person, Vertragsdaten, Messpunkte etc. Diese Daten scheinen zumindest die Bestimmbarkeit einer Person zu ermöglichen, in bestimmten Fällen können Personen auch direkt bestimmt werden. Es handelt sich dabei in der Regel um Personendaten gemäss Art. 3 lit. a DSG.

Befund

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	2	Smart Grid Information Security – Security Level	4

Entspricht AWK-Datenobjekt: *Netzauslastung*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Für die Versorgungssicherheit sind die Daten der Netzauslastung bezüglich Vertraulichkeit, Integrität und Verfügbarkeit kritisch. Da diese durch Fremde missbraucht werden könnten und die Netzstabilität beeinträchtigen könnten. Datensicherheit aus Gründen des Datenschutzes: Aus Datenschutzgründen ist die Netzauslastung nicht kritisch, da diese Daten nicht zwischen den Rollen ausgetauscht werden.

Datenschutzrechtliche Qualifikation der Daten: Die Zustandsdaten der Netzauslastung werden jeweils innerhalb der Netzgebiete überwacht, um regionale Flexibilitäten zu erkennen. Das Format ist hier noch offen, eine abschliessende Qualifikation der Personenbezogenheit der Daten ist somit noch nicht möglich. Normalerweise handelt es sich um rein interne Netzbetreiberdaten, es werden also keine Daten von anderen Personen bearbeitet. Das DSG gelangt, falls die Daten nur intern verwendet werden, nicht zur Anwendung.

Zählwerte

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	2	Smart Grid Information Security – Security Level	4

Entspricht AWK-Datenobjekt: *Systemzustandsdaten*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Für die Versorgungssicherheit ist die Verfügbarkeit und Integrität der Systemzustandsdaten als kritisch einzustufen. Mit falschen oder fehlenden Systemzustandsdaten könnten Schaltungen ausgelöst werden, welche die Netzstabilität beeinträchtigen und so die Versorgungssicherheit gefährden. Datensicherheit aus Gründen des Datenschutzes: Die Systemzustandsdaten sind aus Datenschutzsicht kritisch einzustufen, da diese Rückschlüsse auf geschützte personenbezogene Daten und Unternehmensdaten zulassen und unter den Rollen ausgetauscht werden.

Datenschutzrechtliche Qualifikation der Daten Systemzustandsdaten sind Daten über den Netzzustand, so dass der Verbraucher aktiv und zugunsten des Netzsystems agieren kann. Die Idee ist hier, dass diese Daten Anreizsignale an den Prosumer darstellen sollen. Inhalt und Form dieser Daten sind zurzeit jedoch noch offen. Ein Sammeln solcher Daten könnte Aufschluss über die generelle Versorgungsqualität des Netzes geben, womit Personendaten der Netzbetreiber vorliegen können.

Einsatzfahrplan

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	1 oder 2	Smart Grid Information Security – Security Level	4 bei DPC 2, 3 bei DPC 1

Entspricht AWK-Datenobjekt: *Flexibilitätsoptionen*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Die Flexibilisierungsoptionen sind für die Versorgungssicherheit tendenziell bezüglich deren Integrität kritisch, da falsche Daten (wenn z.B. grossflächig manipuliert) falsche Regelungen auslösen könnten und das Netz in einen Instabilen Zustand bringen könnte.

Datensicherheit aus Gründen des Datenschutzes: Die Flexibilisierungsoptionen sind aus Datenschutzsicht tendenziell kritisch, falls sie Rückschlüsse auf Personen zulassen. Insbesondere beim Prosumer ist denkbar, dass die Flexibilisierungsoptionen Rückschlüsse auf An- / Abwesenheiten und Grössenordnungen des Stromverbrauchs zulassen (z.B. mehr Flexibilität bei Abwesenheit oder mit einem Elektroauto / grossen Batterien).

Datenschutzrechtliche Qualifikation der Daten aus den gesammelten und aufbereiteten Daten können zeitlich flexible Energieflüsse (Ein- und Ausspeisepunkte) auf Grund des Netzzustandes optimiert werden. Die Optionen sollen Profile darstellen, wie die Lastflüsse gestaltet werden können. Auch hier handelt es sich um ein neues Format, die Ausgestaltung bzw. das Format der Daten ist also zurzeit noch offen, weshalb keine datenschutzrechtliche Qualifizierung vorgenommen werden kann.

Netzzustandsprognose
Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	2	Smart Grid Information Security – Security Level	4

Entspricht AWK-Datenobjekt: *Monitoringdaten*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Die Integrität der Monitoringdaten ist für die Versorgungssicherheit tendenziell kritisch, da falsche Daten in kritischen Situationen zu falschen Abrufsignalen führen könnten. Die Vertraulichkeit und Verfügbarkeit sind etwas weniger kritisch für die Versorgungssicherheit.

Datensicherheit aus Gründen des Datenschutzes: Die Monitoringdaten sind aus Sicht des Datenschutzes unkritisch, da es sich nicht um personenbezogene Daten handelt.

Datenschutzrechtliche Qualifikation der Daten Die Vorhaltung der SDL bei den teilnehmenden Anlagen soll vom SDV und dem Übertragungsnetzbetreiber laufend überwacht werden. Die hierfür benötigten Daten enthalten die aktuell abrufbare Leistung und je nach Regelleistung (primär, sekundär, tertiär) Angaben zum Arbeitspunkt und zur momentanen Leistung der teilnehmenden Erzeugungseinheit (bspw. einer Turbine). Die Überwachung solcher u.U. geschäftssensibler Unternehmensdaten durch den SDV und den Übertragungsnetzbetreiber stellt eine Bearbeitung von personenbezogenen Daten gemäss DSG dar.

Netzzustandsermittlung

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	2	Smart Grid Information Security – Security Level	4

Entspricht AWK-Datenobjekt: *Betriebsmittelzustand*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Für die Versorgungssicherheit könnte der Betriebsmittelzustand beim Verteilnetzbetreiber und beim Übertragungsnetzbetreiber tendenziell kritisch sein bezüglich Vertraulichkeit, Integrität und Verfügbarkeit. Schwachstellen in den Betriebsmitteln könnten durch Fremde genutzt werden, um die Versorgungssicherheit zu mindern.

Datensicherheit aus Gründen des Datenschutzes: Aus Sicht des Datenschutzes kann davon ausgegangen werden, dass diese Daten Rückschlüsse auf die Persönlichkeit im Sinne eines Unternehmens zulassen.

Datenschutzrechtliche Qualifikation der Daten: Die Zustandsdaten der Betriebsmittel werden jeweils innerhalb des Netzgebietes überwacht, um Fehler und den Netzzustand zu erkennen. Es handelt sich hier um Daten zu jedem Betriebsmittel und in welchem Zustand dieses ist wie Alter, Reparaturen etc. Bei den Daten zu den Betriebsmitteln könnte es sich allenfalls um personenbezogene Daten handeln, eine genaue Qualifikation setzt aber auch hier weitere Informationen voraus.

Empfangsquittung

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	2	Smart Grid Information Security – Security Level	4

Entspricht AWK-Datenobjekt: *Fehlerinformation*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Je nach Anwendungsfall können die Fehlerinformationen für die Versorgungssicherheit bezüglich der Vertraulichkeit, der Integrität und der Verfügbarkeit kritisch eingestuft werden. So sollten bei einem Bedrohungszustand (Use Case 6) oder bei grossflächigen Fehlern / Ausfälle (Use Case 7) die Fehlerinformationen korrekt und verfügbar sein. Zusätzlich ist sollte in einem Bedrohungszustand die Vertraulichkeit gegenüber fremden gewährleistet sein, um das Netz zusätzlich vor Angriffen zu schützen.

Datensicherheit aus Gründen des Datenschutzes: Die Relevanz der Fehlerinformationen aus Sicht Datenschutz ist bei den Daten von den Prosumern gegeben. Bei diesen Daten sollte die Vertraulichkeit und Integrität als kritisch eingestuft werden.

Datenschutzrechtliche Qualifikation der Daten: Die Fehlerinformationen müssen auch Informationen zu Daten enthalten, damit ein allfälliger Schwachpunkt erkennt werden kann.

Lastprognose

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security –	2	Smart Grid Information Security – Security Level	4

Data Protection class			

Entspricht AWK-Datenobjekt: *Prognosedaten Netz*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Für die Versorgungssicherheit sind die Prognosedaten tendenziell unkritisch, da ohnehin mit einer gewissen Unschärfe gerechnet werden muss und durch die heute angenommene Regelmässigkeit auch veraltete Daten für den stabilen Betrieb in der Regel ausreichen.

Datensicherheit aus Gründen des Datenschutzes: Die Prognosedaten für Netz und Energie sind in den meisten Fällen aggregiert und nicht personenbezogen und werden daher in diesen Fällen für die Datensicherheit als unkritisch eingestuft.

Datenschutzrechtliche Qualifikation der Daten:
Prognosedaten Netz: Hierbei handelt es sich um Daten für die Netznutzungskalkulation und Verlustbeschaffung. Zu beachten ist, dass auch die Daten der Verteilnetzbetreiber vom DSG erfasst sind, wenn sie personenbezogen sind, auch wenn Sie hier nicht im Fokus stehen. Im Netz sind es üblicherweise aggregierte Prognosen (über den gesamten Netzbereich zusammen), was dazu führt, dass die Daten keiner bestimmten bzw. bestimmbaren Person zugeordnet werden können.

Lastflussprognose

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	2	Smart Grid Information Security – Security Level	4

Entspricht AWK-Datenobjekt: *Prognosedaten*

Vgl. Lastprognose

Erzeugungsfahrplan

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	2	Smart Grid Information Security – Security Level	4

Entspricht AWK-Datenobjekt: *Flexibilitätsoptionen*

Vgl. Einsatzfahrplan

Flexibilitätssteuersignal

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection class	2	Smart Grid Information Security – Security Level	4

Entspricht AWK-Datenobjekt: *Abrufsignal*

Datensicherheitsbedarf
Datensicherheit aus Gründen der Versorgungssicherheit: Die Abrufsignale sind bezüglich Integrität und Verfügbarkeit für die Versorgungssicherheit kritisch, da diese genau für diesen Zweck verwendet werden und falsche oder nicht vorhandene Daten im kritischen Zeitpunkt das Netz instabil machen können. Bezüglich der Vertraulichkeit wird davon ausgegangen, dass diese Daten unkritisch sind.

Datensicherheit aus Gründen des Datenschutzes: Die Abrufsignale sind tendenziell nicht kritisch aus Sicht des Datenschutzes, da aus diesen Daten keine absoluten Nutzungsdaten eruiert werden können.

Datenschutzrechtliche Qualifikation der Daten: Die SDL Steuersignale werden heute zentral vom ÜNB übermittelt (Sekundärregelleistung, Tertiärregelleistung) oder direkt lokal eingestellt. Das Signal beinhaltet die Leistung, die im Kraftwerkt hoch-/runterzufahren ist. Damit das DSG anwendbar auf diesen Datentyp ist, müssten aus der hoch- bzw. runterzufahrenden Leistung Rückschlüsse auf bestimmte bzw. bestimmbare natürliche oder juristische Personen gezogen werden können. Dies ist grundsätzlich nicht auszuschliessen und wird von der konkreten Ausgestaltung des Use Cases abhängig sein.

Flexibilitätsgrenzen

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection Class	2	Smart Grid Information Security – Security Level	4

Entspricht AWK-Datenobjekt: *Monitoringdaten*

Vgl. Netzzustandsprognose

Flexibilitätsbedarf

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection Class	2	Smart Grid Information Security – Security Level	4

Entspricht AWK-Datenobjekt: *Flexibilitätsoptionen*

Vgl. Einsatzfahrplan

Verfügbare Flexibilität

Klassifikation im Rahmen dieser Studie:

Smart Grid Information Security – Data Protection Class	1	Smart Grid Information Security – Security Level	3

Entspricht AWK-Datenobjekt: *Angebot SDL*

Datensicherheitsbedarf:

Datensicherheit aus Gründen der Versorgungssicherheit: Die Vertraulichkeit und Integrität der SDL Angebote ist für die Versorgungssicherheit tendenziell kritisch, da falsche Daten in kritischen Situationen zu falschen Abrufsignalen führen könnten.

Datensicherheit aus Gründen des Datenschutzes: Die SDL Angebote sind tendenziell kritisch aus Sicht der Vertraulichkeit und der Integrität, da aus diesen Angeboten Rückschlüsse auf den zukünftigen Bedarf gemacht werden könnten (erhöhtes Angebot aufgrund von Abwesenheiten / Ferien der Bewohner).

Datenschutzrechtliche Qualifikation der Daten: Der SDL-Verantwortliche (SDV) unterbreitet dem ÜNB die SDL-Angebote (evtl. als Aggregator für virtuelle Kraftwerke) und hält die zugeschlagenen SDL-Scheiben zwecks Leistungsvorhaltung fest. Die Rolle des SDV wird häufig durch den Handel wahrgenommen. Heute beinhalten die Angebote und Zuschläge eine Leistungsscheiben- und Preiskomponente (bspw. wie viel MW zu welchem Preis). Die Angebote stellen somit geschäftssensible Daten dar, die der SDV dem ÜNB übergibt. Es handelt sich somit um personenbezogene Daten.

3.5.1 Zusammenfassung der Datenschutz- und Datensicherheitsanalyse

Die Ergebnisse der AWK Studie konnten durch eine vergleichbare Sicht auf den Betrachtungsgegenstand der Flexibilitäten innerhalb der Consentec Koordinationsmodellen übernommen werden.

Dabei wurden die in der Modellierung identifizierten Datenobjekte dieser Studie auf Datenobjekte der AWK Studie abgebildet. Es fand sich für jedes Objekt dabei ein passendes Gegenstück auf AWK Seite, das bereits bzgl. der Aspekte für Datensicherheit bzw. Datenschutz analysiert wurde. Diese bereits durch das BFE bestätigten Analysen der AWK können in dieser Studie übernommen werden, so dass auch für die 16 in dieser Studie zu betrachtenden Datenobjekte eine Datensicherheits- und Datenschutzeinstufung vorliegt.

Zusätzlich werden diese Datenobjekte in dieser Studie bzgl. ihrer Einstufung gemäss SGIS Methodik der so genannten Dataprotection Classes untersucht. Dabei werden sie gemäss dem Schema personenbezogene Daten (DPC-1) bzw. Prozessdaten (DPC-2) klassifiziert. Ein Verlust von personenbezogenen Daten bzw. eine Offenlegung hat meist keine direkten Auswirkungen im Netzbetrieb, wohl aber bzgl. der Reputation eines Unternehmens. Dies kann zu einem Vertrauensverlust unterschiedlicher Dauer führen, einem Reputationsverlust. Bei Prozessdaten kann es zu einer direkten Bedrohung der Assets bzw. des Netzbetriebs kommen, daher sind diese Daten grundsätzlich kritischer bzw. ein Umgang mit ihnen erfolgt auch grundsätzlich auf einem höheren Schutzniveau.

Grundsätzlich ist eine sehr homogene Sicht auf die Daten in den Koordinationsmodellen durch die SGIS-Analyse zu erkennen, das Gefährdungspotenzial jedoch zumeist im Bereich 3-4, falls Verletzungen bzgl. der Nutzung der Daten auftreten. Dabei ist jedoch zu beachten, dass gemäss ICT VSE Regel ab Sicherheitslevel 3 der SGIS Klassifikation bereits eine Krise entstehen kann, ein Verlust der Daten der Koordinationsmodelle hat daher das Potenzial, durch eine geeignete Nutzung durch einen Eingreifer theoretisch eine Krise auf lokaler Ebene auszulösen. Bei der Risikobewertung ist jedoch zumeist nicht nur das Schadensausmass zu betrachten, sondern auch die Eintrittswahrscheinlichkeit für das Gesamtprodukt Risiko.

Eine Risikoabschätzung kann für ein statisches Datum jedoch nicht erfolgen, da ein Angriff nur über eine Schnittstelle oder ein Verlust nur in einem Prozess geschehen kann. Im Rahmen dieser Studie wird daher zusätzlich noch eine Betrachtung der SGIS-Methodik für die Schnittstellen vorgenommen wie im folgenden Abschnitt zu erkennen ist.

3.6 Gefahrenidentifikation und Schutzbedarf für die Schnittstellenklassen

Dieser Abschnitt der Studie bietet eine Übersicht über die Gefahrenidentifikation auf Basis der High-Level Security Guidance der SGIS M/490 Arbeitsgruppe.

Tabelle 6 zeigt die Zuordnung der jeweiligen Risk Impact Levels (RIL) und somit einen Schutzbedarf für die einzelnen Domain/ Zone Kombinationen innerhalb einer SGAM-Ebene. Dazu wurden aus dem M/490 die SGIS Security-Risk Impact levels (RIL) und die SGIS Security Levels (SL) herangezogen.

Die SGIS Methodik umfasst fünf so genannte Security Level, denen entsprechend Ereignisse zu geordnet werden können, etwa lokale oder europäische Stromnetzausfälle (vgl. Tabelle 4). Ein Ausfall eines Assets hat Auswirkungen im Netzbetrieb, bestimmte Assets sind dabei kritischer als andere und erhalten dadurch bei Ausfall eine höhere Schadensausmasseinstufung. Diese Kritikalität wird auf Basis der Domäne/Zone Verortung ermittelt (vgl. Tabelle 6).

Diese Vorschläge zur Kritikalität werden später (in Abschnitt 3.8 dieser Studie) bei der Verortung der einzelnen Schnittstellen der Koordinationsmodelle im SGAM als Faktoren für die Gesamtrisikoanalyse herangezogen und stellen somit eine wichtige Eigenschaft der im SGAM verorteten Schnittstellenklassen dar.

SGIS-SL High-Level Guidance					
Generation	**Transmission**	**Distribution**	**DER**	**Customer**	
3 - 4	3 - 4	3 - 4	2 - 3	2 - 3	**Market**
3 - 4	3 - 4	3 - 4	2 - 3	2 - 3	**Enterprise**
3 - 4	5	3 - 4	3	2 - 3	**Operations**
2 - 3	4	2	1 - 2	2	**Station**
2 - 3	3	2	1 - 2	1	**Field**
2 - 3	2	2	1 - 2	1	**Process**

Tabelle 6: Klassifikation der M/490 Gruppe für Security Levels mit Bezug auf die SGAM Domänen und Zonen

Die SGIS Gruppe betrachtet die in Tabelle 7 definierten Risikokategorien. Innerhalb dieser Studie liegt der Fokus auf der primären Adressierung und Gewichtung der Kategorien Betrieb und Recht im Rahmen der Gesamtrisikoanalyse. Dazu wird in der Gesamtrisikoanalyse eine Datenschutz- und Datensicherheitsperspektive pro Schnittstellenklasse durch eine CIA Analyse eingeführt (diese Klassifizierung wird aus dem NISTIR 7628 Modell abgeleitet) sowie für den betrieblichen Aspekt eine detailliertere Formel angesetzt.

Es ist zu erwähnen, dass die SGIS Gruppe zwar die Analysemethodik zur Verfügung stellt, nicht jedoch ein dediziertes Verfahren zu Ermittlung einer Ordinalzahl für ein Gesamtrisiko. Daher wurde im Rahmen dieser Studie eine eigene Gewichtung mit Funktion erarbeitet und zur Befüllung der Risikomatrix genutzt. Abbildung 4 bietet eine detaillierte Sicht auf den Gefahrenidentifikationsprozess innerhalb dieser Studie sowie dessen einzelne Schritte.

Risikokategorien	
Kategorie	Unterkategorie
Betrieb	Energieversorgung
	Energiefluss
	Bevölkerung
	Infrastrukturen
Recht	Datenschutz
	Andere Rechte und Regulierungen
Angestellte	
Reputation	
Umwelt	
Finanzen	

Tabelle 7: Risikokategorien bzgl. Angreiferszenarien der SGIS Gruppe im M/490

3.7 Schnittstellenklassen aus NISTIR 7628 und Mapping der Schnittstellenklassen auf die Koordinationsmodelle

3.7.1 Schnittstellenklassen aus NISTIR 7628

Dieser Abschnitt bietet eine Aufzählung und Übersicht der Schnittstellenklassen aus der NISTIR 7628 Reihe und welche jeweiligen Bezeichner bzw. Kommunikationswege zur Systemvernetzung genutzt werden.

Dabei handelt es sich um eine Übersetzung der englischen Originalbezeichner, die sich im Anhang befinden.

- Schnittstellenklasse Nummer 1: Generische Schnittstelle zwischen Kontrollsystemen und hochverfügbaren Systemen, zusätzliche Bandbreiten- und/oder Berechnungskapazitätseinschränkungen

- Schnittstellenklasse Nummer 2: Schnittstelle zwischen Kontrollsystem und Systeme ohne Hochverfügbarkeit, aber mit Bandbreiten- und/oder Berechnungskapazitätseinschränkungen

- Schnittstellenklasse Nummer 3: Schnittstelle zwischen Kontrollsystem und Systemen mit Hochverfügbarkeit, aber ohne Bandbreiten- und/oder Berechnungskapazitätseinschränkungen

- Schnittstellenklasse Nummer 4: Schnittstelle zwischen Kontrollsystem und Systeme ohne Hochverfügbarkeits-, Bandbreiten- und/oder Berechnungskapazitätseinschränkungen

- Schnittstellenklasse Nummer 5: Schnittstelle zwischen Kontrollsystemen innerhalb einer Organisation

- Schnittstellenklasse Nummer 6: Schnittstelle zwischen Kontrollsystemen verschiedener Organisationen

- Schnittstellenklasse Nummer 7: Schnittstelle zwischen Back-Office-Systemen unter gemeinsamer Verantwortung

- Schnittstellenklasse Nummer 8: Schnittstelle zwischen Back-Office-Systemen unter getrennter Verantwortung
- Schnittstellenklasse Nummer 9: Schnittstelle mit B2B-Verbindungen zwischen Finanz- oder Marktsystemen
- Schnittstellenklasse Nummer 10: Schnittstelle zwischen Kontrollsystemen und Nicht-Kontrollsystemen/ Business-IT Systemen
- Schnittstellenklasse Nummer 11: Schnittstelle zwischen Sensoren und Sensornetzen zur Messung von Umweltparametern, typischerweise einfache Analogsensorik
- Schnittstellenklasse Nummer 12: Schnittstelle zwischen Sensornetzen und Kontroll-systemen
- Schnittstellenklasse Nummer 13: Schnittstelle zwischen Systemen die das AMI Netz nutzen
- Schnittstellenklasse Nummer 14: Schnittstelle zwischen Systemen die das AMI Netz für hochverfügbare Funktionen nutzen
- Schnittstellenklasse Nummer 15: Schnittstelle zwischen Systemen, die Kundennetze wie HAN und BAN nutzen (Haushalt, Kommerziell und Industriell)
- Schnittstellenklasse Nummer 16: Schnittstelle zwischen externen Systemen und dem Kundenanschluss
- Schnittstellenklasse Nummer 17: Schnittstellen zwischen Systemen und den mobilen Endgeräten der Crew im Feld
- Schnittstellenklasse Nummer 18: Schnittstellen im Zählerbereich
- Schnittstellenklasse Nummer 19: Schnittstellen zwischen operativen Entscheidungs-unterstützungssystemen
- Schnittstellenklasse Nummer 20: Schnittstelle zwischen Wartungs-/ Konfigurationssys-temen und Kontrollgeräten
- Schnittstellenklasse Nummer 21: Schnittstelle zwischen Kontrollsystemen und Ihren Herstellern für Standardwartung und -services
- Schnittstellenklasse Nummer 22: Schnittstelle zwischen Systemmanagementkonsolen und alle anderen Netzen und Systemen

3.7.2 Mapping der Schnittstellenklassen auf die Koordinationsmodelle

Angewendet auf die Prozesselemente der Koordinationsmodelle (vgl. Abbildung 2) innerhalb der Modellierung der SGAM Toolbox ergaben sich dabei die folgenden Schnittstellen, die ausgewählt werden für eine Gefahrenanalyse/Schutzbedarfsanalyse sowie eine abschliessende Risikoanalyse im Rahmen dieser Studie.

Für die Studie sind nach der Analyse der Koordinationsmodelle mittels der Modellierung in der SGAM Toolbox (Siehe Abschnitt 3.2 dieser Studie) die folgenden Schnittstellen relevant, da

sie sich aus der Analyse der logischen Schnittstellen und der Zuordnung zu den Kategorien der Schnittstellen im NISTIR 7628 ergaben (vgl. auch [15], Seite 27).

Diesen Schnittstellenklassen wurden im NISTIR 7628 verschiedene Eigenschaften zugewiesen, die zu einem jeweils spezifischen Schutzbedarf führen, welchen wir in dieser Studie nutzen werden, um die empfohlenen NISTIR 7628-Massnahmen auf die Koordinationsmodelle zu übertragen.

- Schnittstelle 5: Schnittstelle zwischen Kontrollsystemen innerhalb einer Organisation.

  Im Anwendungsfall EP01 handelt es dabei zum Beispiel um die Schnittstelle U11 des Lastmanagementsystemes des VNB zum Leitsystem des Verteilnetzes über das Messwerte und Kurzzeitprognosen ausgetauscht werden.

- Schnittstelle 6: Schnittstelle zwischen Kontrollsystemen verschiedener Organisationen

  Im Anwendungsfall EP02 handelt es sich zum Beispiel um die Schnittstelle U87 des Leitsystems zu einem lokalen Energiemanagementsystem eines Grosserzeugers. Dabei werden leittechnische Systeme verschiedener Parteien gekoppelt.

- Schnittstelle 7: Schnittstelle zwischen Back-Office-Systemen unter gemeinsamer Verantwortung

  Im Anwendungsfall EP03 handelt es sich hierbei z.B. um eine Schnittstelle wie U2 zwischen einem Zählermanagementsystem und dem Head-End einer Zählerinfrastruktur. Ausgetauschte Daten sind hierbei z.B. aggregierte Zählerwerte.

- Schnittstelle 8: Schnittstelle zwischen Back-Office-Systemen unter getrennter Verantwortung

  Im Anwendungsfall EP02 handelt es sich beispielsweise hier um die Schnittstellen U15 der Kategorie 8 zwischen einem Aggregator und seinem Abrechnungssysteme zum Netzmanagementsystem eines Verteilnetzbetreibers zum Austausch von Retail-Einsatzfahrplänen.

- Schnittstelle 9: Schnittstelle mit B2B-Verbindungen zwischen Finanz- oder Marktsystemen

  Im Anwendungsfall EP02 handelt es sich hier beispielsweise um das Interface U97 zwischen Marktteilnehmern und dem Energiemanagementsystem eines Verteilnetzbetreibers zur Übermittlung von Lastgangprognosen, etwa zur Netzauslastung in bestimmten Jahreszeiten.

- Schnittstelle 13: Schnittstelle zwischen Systemen die das AMI Netz nutzen

  Im Anwendungsfall EP03 handelt es sich hier beispielsweise um das Interface U2, welches Zählerdaten über einen Bus zwischen verschiedenen Teilen des AMI Netzes austauscht. Im Gegensatz zu Schnittstellenklasse 14 ist hier das Datum nicht relevant für den Netzbetrieb.

- Schnittstelle 14: Schnittstelle zwischen Systemen die das AMI Netz für hochverfügbare Funktionen nutzen

Im Anwendungsfall EP03 handelt es sich hier beispielsweise um das Interface U2, welches Zählerdaten über einen Bus zwischen verschiedenen Teilen des AMI Netzes austauscht. Im Gegensatz zu Schnittstellenklasse 13 ist hier das Datum relevant für den Netzbetrieb, zumeist also ein Prozessdatum.

- Schnittstelle 16: Schnittstelle zwischen externen Systemen und dem Kundenanschluss

  Im Anwendungsfall EP02 handelt es sich dabei zum Beispiel um die Schnittstelle U88 zwischen dem leittechnischen System zum Flexibilitätsmanagementsystem auf Endkundenseite an der (lokalen) Anlage über das Einsatzfahrpläne zur Kundenanlage übertragen werden.

- Schnittstelle 17: Schnittstellen zwischen Systemen und den mobilen Endgeräten der Crew im Feld

  Im Anwendungsfall EP01 handelt es dabei zum Beispiel um die Schnittstelle U101 des Leitsystems des Verteilnetzes zu einem Operatormonitor bzw. einer Workstation, die eine Manipulation des SCADA ermöglicht.

- Schnittstelle 18: Schnittstellen im Zählerbereich

  Bei dieser Schnittstelle handelt es sich zumeist um eine direkte Schnittstelle zu einem Endgerät im Zählerbereich zur Konfiguration oder zwecks HMI Interaktion, etwa im EP03 und EP04 mit dem U24. Diese ist implizit (da eine Abrechnung stets erfolgen muss) in jedem Anwendungsfall enthalten, da es sich hier meist um eine physische Schnittstelle zu einem Zähler handelt. Aus Gründen der Konsistenz zum NIST wurden die Schutzanforderungen jedoch nur in EP 03 und EP 04 ermittelt.

- Schnittstelle 20: Schnittstelle zwischen Wartungs-/ Konfigurationssystemen und Kontrollgeräten

  Im Anwendungsfall EP01 handelt es dabei zum Beispiel um die Schnittstelle U11 des Lastmanagementsystemes des VNB zum Leitsystem des Verteilnetzes über die Konfigurationsdaten im Sinne etwa von Basisnetzdaten zur Konfiguration an das Leitsysteme übermittelt werden.

Diese Schnittstellenklassen sind wie in der Tabelle 8 gezeigt den einzelnen Modellierungen der Koordinationsmodelle innerhalb der SGAM Toolbox zuzuordnen. Dadurch kann der Schutzbedarf für jede Schnittstellenklasse sowie die Massnahmen für den jeweiligen Schutzbedarf in den Koordinationsmodellen detailliert abgeleitet werden.

Anwendungsfall	EP01: Echtzeit Engpassvorhersage	EP02: Vorrausschauende Engpassvorhersage	EP03: Echtzeit Engpassbeseitigung	EP04: Engpassbeseitigung durch Flexibilitäts-beschaffung	EP05: Engpass-bewirtschaftung
Schnittstellenklasse					
5	x	x	x	x	x
6		x	x	x	x
7			x	x	
8		x	x	x	x
9	x	x	x		
13			x	x	
14			x	x	
16	x	x	x	x	x
17	x				
18			x	x	
20	x	x	x	x	x

Tabelle 8: Abbildung der Schnittstellenklassen auf die Anwendungsfälle EP01 bis EP05

3.8 Gesamtrisikoanalyse für die Koordinationsmodelle

Innerhalb dieses Abschnitts wird zusammenfassend aus den bisher dargestellten Ergebnissen eine Gesamtrisikoanalyse für die Schnittstellenklassen vorgenommen. Dabei wird wie bereits erwähnt davon ausgegangen, dass die „Weakest-Link" – Theorie valide ist – ein System ist bedingt durch die Professionalität und Möglichkeiten der Angreifer zur Recherche etwa in der ICS Cert Datenbank, nur so gut wie sein am schwächsten abgesichertes Interface. Ein Koordinationsmodell ist nur so sicher wie seine schwächste Schnittstelle.

Eine Analyse bzgl. der Aspekte Vertraulichkeit, Integrität und Verfügbarkeit (CIA-Analyse) verbleibt auf der Ebene einzelner Schnittstellen (Logical Interfaces), da sich ansonsten keine verwertbaren Ergebnisse in der Konsolidierung mehrerer (Einzel-)Analysen für einen Gesamtanwendungsfall ableiten lassen – alle konsolidierten EP 01 bis 05 hätten insgesamt die Klassifikation H, H, H, da zumeist sehr viele verschiedene Schnittstellen beteiligt sind.

Das Gesamtrisiko ergibt sich aus den Aspekten des Schadensausmasses und der Eintrittswahrscheinlichkeit. Im Rahmen dieser Studie ergeben sich die einzelnen beiden Faktoren aus jeweiligen Unterelementen gemäss folgender Formel:

Risiko = Schadensfaktor * API-Level
Ergebnis zwischen 1 und 30
Risiko ≤ 4 ist grün, ≥ 10 ist rot, Rest gelb

Dabei steht Risiko für das Gesamtrisiko auf einer Skala von 1-30.

Die einzelnen Faktoren der Formel sind dabei:

- SGIS-SL entspricht dem SGIS Guidance Level für die jeweilige Schnittstelle auf Basis ihrer Verortung im SGAM Modell durch die Experten (Wertebereich 1-5, vgl. Tabelle 6). Der Schadensfaktor ergibt sich wie folgt:

Schadensfaktor =	SGIS-SL	*ohne direkte Effekte im Betrieb*
	SGIS-SL + 1	*bei direkten Effekten im Betrieb*

  wobei *Direkte Effekte im Betrieb* mit Wert 1 bedeutet, dass direkte Effekte existieren

- API entspricht Attacker Probability Impact und ist definiert als die Summe der individuellen, gleichsensitiven Anteile Angreifermotivation (Wertebereich 1-3), Angreifbarkeit der Schnittstelle (Wertebereich 1-3) und Zugriffszahlen (Wertebereich 1-3) auf Basis einer Bewertung der Experten – dabei wird eine Risikoanalyse immer ohne Berücksichtigung möglicher Mitigationsstrategien, also ohne Anwendung von Gegenmassnahmen, wie sie für die Schnittstellen schon empfohlen worden sind, kalkuliert.

  Für das API-Level ergibt sich folgende Funktion:

API-Level =	1	*wenn ΣAPI ≤ 4*
	2	*wenn ΣAPI = 5*
	3	*wenn ΣAPI = 6*
	4	*wenn ΣAPI = 7*
	5	*wenn ΣAPI ≥ 8*

Dadurch ergeben sich bezüglich der zu erarbeitenden Risikomatrix folgende Bereiche, welche auch eine Priorisierung der nötigen Betrachtungen ermöglichen:

Tabelle 9: Risikomatrix: Bewertungsschema für die Ermittlung des Schadensfaktors

Risikomatrix: unter 4 grün, ab 10 rot		Schadensfaktor					
		1	2	3	4	5	6
API	gering	1	2	3	4	5	6
	eher gering	2	4	6	8	10	12
	mittel	3	6	9	12	15	18
	eher hoch	4	8	12	16	20	24
	hoch	5	10	15	20	25	30

Basierend auf dieser Matrix (Tabelle 9) als Bewertungsschema zur Zuordnung der Schnittstellenklassen ergibt sich die folgende Zuordnung der Schnittstellen der Koordinationsmodelle in der Tabelle 10:

Tabelle 10: Gesamtrisikobetrachtung im Rahmen der Studie

	Daten-dimension			Eintrittswahrscheinlichkeit				Schadensausmass		
Schnitt-stellen-klasse	C	I	A	Angreifer-motivation	Angreifbarkeit der Schnittstelle	Zugriffszahlen	API-Level	SGIS Security Level	Direkte Effekte im Betrieb	**Risiko**
5	L	H	H	1	1	1	1	4	1	**5**
6	L	H	M	1	1	2	1	4	1	**5**
7	H	H	L	2	1	2	2	3	1	**8**
8	H	H	L	2	2	2	3	3	1	**12**
9	H	H	M	3	3	3	5	2	0	**10**
13	H	H	L	3	2	3	5	2	1	**15**
14	H	H	H	2	2	3	4	3	1	**16**
16	L	M	M	3	3	3	5	2	1	**15**
17	L	H	M	1	2	2	2	3	1	**8**
18	M	H	L	3	3	3	5	1	1	**10**
20	L	H	M	1	2	1	1	2	0	**2**

Tabelle 11: Risikomatrix: Auswertung und Verortung der Schnittstellenklassen im Bewertungsschema des Schadensfaktors

Risikomatrix Verortung Kategorien		Schadensfaktor					
		1	2	3	4	5	6
API	gering		20			5, 6	
	eher gering				7, 17		
	mittel				8		
	eher hoch				14		
	hoch		9, 18	13, 16			

Betrachtet man also in Tabelle 10 die Ergebnisse der Gesamtrisikoanalyse, welche ohne die Umsetzung der Massnahmen zur Absicherung der Schnittstellen erstellt wurde, erkennt man,

dass 6 der Schnittstellenklassen als höher gefährdet gelten müssen, 4 der Schnittstellenklassen als mittel gefährdet und eine Klasse als weniger gefährdet. Da die Weakest Link Theorie wiederum zur Anwendung kommt und da die hoher gefährdeten Schnittstellenklassen in den 3 Koordinationsmodellen sind, gelten sämtliche Koordinationsmodelle als hoch gefährdet. Deshalb sollen die sämtlichen Schnittstellenklassen z.B. mittels der Grundschutzmassnahmen aus der NISTIR 7628 abgesichert werden (vgl. Abschnitt 3.9).

Für die einzelnen Schnittstellen lassen sich dabei folgende Charakteristiken und Gesamtrisikoeinschätzungen erkennen bzw. begründen:

Risiko Hoch

Schnittstellenklasse Nummer 8: Schnittstelle zwischen Back-Office-Systemen unter getrennter Verantwortung

Diese Schnittstelle ist nicht nur innerhalb eines Unternehmens, sondern Unternehmensübergreifend, etwa zwischen dem Lieferant, Erzeuger oder Aggregator und umfasst typischerweise Systeme, die im Intranet mehrerer Unternehmen hinter jeweils einer DMZ über eine WAN Verbindung miteinander interagieren, etwa zu Abrechnungszwecken. Hierbei kann es sich um Systeme handeln, die teilweise den Verteilnetzbetrieb als Sekundärsysteme unterstützen, teilweise aber auch lediglich eine Abrechnungsfunktion haben. Dadurch ist ein Schaden zwar im Ausmass hoch (Störung der Abrechnung, Störung der interner Prozesse, Sekundäreffekte im Workforcemanagement, etc.), die Angriffwahrscheinlichkeit aber höher als in Klasse 7, da hier mehr interne Angreifer in den Unternehmen (z.B: unzufriedene oder schlecht ausgebildete Mitarbeiter), aber auch externe wegen einer Kopplung über WAN in Frage kommen. Daher ist insgesamt eine höhere Gefährdung anzunehmen.

Schnittstellenklasse Nummer 9: Schnittstelle mit B2B-Verbindungen zwischen Finanz- oder Marktsystemen

Diese Schnittstelle ist eine B2B Schnittstelle, etwa zwischen Bilanzkreisverantwortlichen, die zumeist mit vielen Drittsystemen gekoppelt wird und vor allem zu Abrechnungs- oder Handelszwecken bedient wird. Dabei ist die Gefährdung vor allem in einem finanzielle Verlust bzgl. Energiehandel oder Abrechnung zu sehen, wenn hier ein Angriff bzw. ein Ausfall erfolgt. Dieser Schaden ist insgesamt im Verhältnis als eher mittel einzuschätzen, während durch die hohe Anzahl an exponierten Schnittstellen zu Dritten und die hohe Anzahl der möglichen Zugriffe sich aus dieser Kombination ein hohes Gefährdungsrisko ableiten lässt.

Schnittstellenklasse Nummer 13: Schnittstelle zwischen Systemen die das AMI Netz nutzen

Diese Schnittstelle zielt auf die Kopplung von Systemen in der so genannten Advanced Metering Infrastructure ab und ist höher gefährdet. Genau wie die Schnittstellen 14 und 18 ist sie für Messtellenbetreiber relevant. Dies liegt vor allem daran, dass das System insgesamt über mehr so genannte Endpoints in der Periphärie der primären Unternehmens-IT verfügt, zumeist sogar mit einem Endgerät mit einem Zähler bei vielen Kunden. Diese Endgeräte sind zumeist standardisiert, was sie anfälliger für Re-Engineering macht und sie auf dem Markt leicht verfügbar sind. Der Ausfall einzelner Zähler, selbst wenn diese als Messpunkte im Netz fungieren ist vom Schadensausmass her vertretbar, bedingt durch die große Menge an Zugriffen, die Verortung der Geräte und die hohe Motivation kommt es dennoch zu dieser Einschätzung.

Schnittstellenklasse Nummer 14: Schnittstelle zwischen Systemen die das AMI Netz für hochverfügbare Funktionen nutzen

Diese Schnittstelle zielt auf die Kopplung von Systemen, die hochverfügbare Funktionen nutzen, in der so genannten Advanced Metering Infrastructure ab und ist höher gefährdet. Genau

wie die Schnittstellen 14 ist sie für Messstellendienstleister, zusätzlich aber auch für Netzbetreiber relevant. Dies liegt vor allem daran, dass das System insgesamt über mehr so genannte Endpoints periphär zur primären Unternehmens-IT verfügt, zumeist sogar mit einem Endgerät mit einem Zähler oder steuerbaren Erzeuger bei vielen Kunden. Diese Endgeräte sind zumeist standardisiert, was sie anfälliger für Re-Engineering macht und sie auf dem Markt leicht verfügbar sind. Der Ausfall einzelner Kontrollierbarer Erzeuger oder Messpunkte für die Leittechnik vom Schadensausmass her vertretbar, bedingt durch die große Menge an Zugriffen, die Verortung der Geräte, die kontrollierbaren Lasten und die höhere Motivation kommt es dennoch zu dieser Einschätzung.

Schnittstellenklasse Nummer 16: Schnittstelle zwischen externen Systemen und dem Kundenanschluss

Bei dieser Schnittstelle handelt es sich typischerweise um Systeme, die Information oder Daten, etwa Tarife oder Updates für Erzeuger oder Zähler, für den Kunden zur Verfügung stellen, auch etwa Websysteme, in die er seinem aktuellen Zählerstand bei einem Umzug eintragen kann oder auch die Anbindung eines Homedisplays vor Ort. Diese Systeme sind durch Versorger schlecht kontrollierbar bzw. nicht überwachbar. Da sie nicht dem Primärbetrieb (d.h. dem reinen operativen Netzbetrieb) dienen, ist ein Ausfall vom Schaden her meist nur mit Reputationsverlust beim Kunden, ggf auch mit finanziellen Einbussen verbunden, durch ihre Exponiertheit sind sie jedoch ein leichtes Ziel für einen Angriff durch Dritte (z.B. dem Kunden, der seine Rechnung senken möchte oder Angreifer, die über das System in das Backend eindringen möchten). Daher ist eine höhere Gefährdung anzunehmen.

Schnittstellenklasse Nummer 18: Schnittstellen im Zählerbereich

Hierbei handelt es sich zumeist um einfache physische Schnittstellen vor Ort zum Auslesen durch das Backend des jeweiligen Zählers vor Ort, etwa durch den Messstellendienstleister (U24). Der Zähler wird hierbei nicht als netzdienliches Asset angesehen, hat also keine Funktionalität als Messpunkt für den kritischen Netzbetrieb oder eine Vorhersagekomponente. Dadurch ist der Schaden für den Ausfall oder die Manipulation eines einzelnen Zählers als überschaubar, wenn auch mit Auswirkungen im direkten Betrieb anzusehen (Rechnungslegung Kunde). Diese Endgeräte sind zumeist standardisiert, was sie anfälliger für Re-Engineering macht und sie auf dem Markt leicht verfügbar sind. Durch ihre Exponiertheit sind sie jedoch ein leichtes Ziel für einen Angriff durch Dritte (z.B. dem Kunden, der seine Rechnung senken möchte oder Angreifer, die über das System in das Backend eindringen möchten). Daher ist eine höhere Gefährdung anzunehmen.

Risiko Mittel

Schnittstellenklasse Nummer 5: Schnittstelle zwischen Kontrollsystemen innerhalb einer Organisation

Diese Schnittstelle als Schnittstelle einer leittechnischen Kontrollkomponente eine Verteilnetzbetreibers oder eines Flexibilitätsanbieters ist von der Gesamtrisikoverteilung im mittleren Gefährdungsbereich zu sehen. Zwar ist der Schaden bei einem tatsächlichen Eindringen sehr hoch und auch das Ausmass massiv mit Wirkung in die Zukunft und den Endkunden (Stromausfälle, ggf. mit Gefährdung von Personen), durch die Lage der Schnittstellen, typischerweise in einem dedizierten Netz ohne Kopplung zur Business-IT und an das Internet, ist aber die Angriffswahrscheinlichkeit für einen nicht hochgradig professionellen Angreifer (Budget/kriminelle Energie) eher gering.

Schnittstellenklasse Nummer 6: Schnittstelle zwischen Kontrollsystemen verschiedener Organisationen

Diese Schnittstelle als Schnittstelle einer leittechnischen Kontrollkomponente mit externen Systemen, etwa eines EMS zwischen einem Aggregator und einem Prognoseanbieter ist von der Gesamtrisikoverteilung im mittleren Gefährdungsbereich zu sehen. Zwar ist der Schaden bei einem tatsächlichen Eindringen sehr hoch und auch das Ausmass massiv mit Wirkung in die Zukunft und den Endkunden (Stromausfälle, ggf mit Gefährdung von Personen), durch die Lage der Schnittstellen, typischerweise pro Unternehmen in einem dedizierten Netz ohne Kopplung zur Business-IT und an das Internet, ist aber die Angriffswahrscheinlichkeit für einen nicht hochgradig professionellen Angreifer (Budget/kriminelle Energie) eher gering, jedoch höher als in Schnittstelle 5 anzusiedeln.

Schnittstellenklasse Nummer 7: Schnittstelle zwischen Back-Office-Systemen unter gemeinsamer Verantwortung

Diese Schnittstelle ist innerhalb eines Unternehmens und umfasst typischerweise Systeme, die im Intranet eines Unternehmens hinter einer DMZ (Demilitarised Zone) miteinander interagieren. Hierbei kann es sich um Billing oder auch Assetmanagementsysteme von Flexibilitätsanbietern, Lieferanten oder Bilanzkreisverantwortlichen handeln, die teilweise den Verteilnetzbetrieb als Sekundärsysteme unterstützen, teilweise aber auch lediglich eine Abrechnungsfunktion haben. Dadurch ist ein Schaden zwar im Ausmass hoch (Störung der Abrechnung, Störung der internen Prozesse, Sekundäreffekte im Workforcemanagement, etc.), die Angriffwahrscheinlichkeit aber gering, da vor allem interne Angreifer (z.B: unzufriedene oder schlecht ausgebildete Mitarbeiter) in Frage kommen. Daher ist insgesamt eine mittlere Gefährdung anzunehmen.

Schnittstellenklasse Nummer 17: Schnittstellen zwischen Systemen und den mobilen Endgeräten der Crew im Feld

Diese Schnittstelle ist innerhalb eines Unternehmens, etwa eines Verteilnetzbetreibers zu sehen und umfasst wie Schnittstelle 7 typischerweise Systeme, die im Intranet eines Unternehmens hinter einer DMZ, aber im Gegensatz zu 7 auch mit Systemen im Feld, etwa über UMTS miteinander interagieren. Hierbei kann es sich um Geoinformations- oder auch Assetmanagementsysteme handeln, die teilweise den Verteilnetzbetrieb als Sekundärsysteme unterstützen, teilweise aber auch lediglich eine Wartungsfunktion haben. Dadurch ist ein Schaden zwar im Ausmass hoch (Störung der Abrechnung, Störung der interner Prozesse, Sekundäreffekte im Workforcemanagement, etc.), die Angriffwahrscheinlichkeit aber gering, da vor allem interne Angreifer (z.B: unzufriedene oder schlecht ausgebildete Mitarbeiter) in Frage kommen. Daher ist insgesamt eine mittlere Gefährdung anzunehmen.

Risiko gering

Schnittstellenklasse Nummer 20: Schnittstelle zwischen Wartungs-/Konfigurationssystemen und Kontrollgeräten

Hierbei handelt es sich um die Wartungs- bzw. Konfigurationsschnittstelle für Endgeräte im Feld (IEDs), die durch einen Techniker für Verteilnetzbetreiber oder Aggregator projektiert werden. Bedingt durch die physische Verortung, typischerweise in einem verschlossenen Umspannwerk bzw. Schaltanlage sowie die Tatsache, dass nur Wartungstechniker nach Absprache und mit Rückprüfung mit dem Betriebsführers nach Freigabe Änderungen an der Konfiguration durchführen, ist hier von einem insgesamt eher geringen Risiko auszugehen, da Freigabeprozesse bereits schon jetzt ausreichend Kontrollen haben, um hier keine hohe Gefährdung zu besitzen.

3.9 Identifizierte Schutzmassnahmen für die Schnittstellenklassen

Bezüglich einer Analyse der Schutzmassnahmen (sprich Cyber Security Requirements der NISTIR 7628) ergeben sich folgende Ergebnisse aus den Schutzmassnahmen der jeweils einzelnen Schnittstellen als Ergebnis in der Tabelle 12. Ein „X“ in einer Spalte bedeutet dabei, dass der jeweiligen Schnittstellenklasse die Schutzmassnahmenanforderung aus der dazugehörigen Zeile zugewiesen ist.

Diese Tabelle stellt ein zentrales Element der Analyse dieser Studie dar, da sie den Schnittstellenklassen der Koordinationsmodelle Massnahmen zuweist, die zu deren Absicherung umgesetzt werden müssen bzw. sollten, wenn die Schnittstellen als geeignet abgesichert gemäss NISTIR 7628 gelten soll.

Durch die Verknüpfung der Generizität einer Schnittstellenklasse (d.h. allgemeingültiger Eigenschaften dieser Klasse) mit bestimmten Basisanforderungen kann eine geeignete scherenschnittartige Absicherung der einzelnen Schnittstellen bestimmt werden. Damit ist ein gewisses Grundschutzniveau zu definieren, ohne dass schon eine konkrete Implementierung bekannt sein muss.

Die ausführlichen Beschreibungen und mögliche Massnahmen zur Gefahrenabwehr als Mitigationsstrategie sind im Anhang (6.2) dieser Studie ausführlich dargestellt, dabei sind auch Vorschläge zu konkreten technischen Umsetzungen zu finden, wie sie jedoch für die Koordinationsmodelle aktuell noch nicht benötigt werden, da diese noch nicht final in ihrer Implementierung sind. Diese Vorschläge können aber schon in ein Design vor der Umsetzung einfliessen und somit das Paradigma Security-by-Design nutzen.

Dabei werden ausschliesslich die folgenden Kategorien von Schutzanforderungen mit Bezug zu Daten und Schnittstellen aus der NISTIR 7628 adressiert:

- ***Zugangskontrolle (SG-AC)*:** Der Fokus der Zugangskontrollen liegt darauf sicherzustellen, dass Personen, die Zugang zu den Ressourcen haben sollen, diesen auch bekommen. Diese Personen müssen korrekt identifiziert werden, ferner müssen die Zugangsaktivitäten überwacht werden.

- ***Prüfung und Verantwortlichkeit (SG-AU):*** Überprüfungen des Smart Grid Informationssystems, sowie Aufzeichnungen über diese, müssen regelmässig ausgeführt werden. Dies passiert um sicherzustellen, dass die Sicherheitsmechanismen, die während der Tests vorhanden waren, auch noch immer installiert sind und dass sie ordnungsgemäss arbeiten. Bei dieser Sicherheitsüberprüfung werden Aufzeichnungen und Aktivitäten überprüft um die festgelegten Sicherheitsvorgaben zu gewährleisten. Durch die Aufzeichnungen werden die Überprüfungen auch zum Aufspüren von Verletzungen der Sicherheitsanforderungen genutzt. Dabei sind die Aufzeichnungen für die Aufspürung von Anomalien, sowie für forensische Analysen notwendig.

- ***Identifikation und Authentifikation (SG-IA):*** Die Identifikation und Authentifikation ist der Prozess der Verifizierung eines Nutzers, eines Prozesses oder eines Gerätes, um Zugriff auf eine Ressource im Smart Grid Informationssystem zu bekommen.

- ***Absicherung der Smart Grid Informationssysteme und der Kommunikation (SG-SC):*** Die Absicherung des Informationssystems und der Kommunikation besteht aus Massnahmen, die getroffen werden, um Smart Grid Informationssysteme und die Nachrichtenverbindungen zwischen diesen vor Eindringlingen zu schützen.

- ***Integrität von Smart Grid Informationssystemen und Nachrichten (SG-SI):*** Durch die Aufrechterhaltung der Integrität von Smart Grid Informationssystemen und Datenintegrität, wird die Sicherheit, dass sensible Daten weder unautorisiert noch unbemerkt modifiziert oder gelöscht werden, erhöht. Die Sicherheitsanforderungen beinhalten

Richtlinien und Verfahren für die Identifizierung, Meldung und Korrektur von Mängeln. Ausserdem existieren Anforderung für das ausfindig machen von Schadcode. Es existieren Anforderungen für den Empfang von Sicherheitsalarmen und Vorschläge zur Verifikation von Sicherheitsfunktionen. Die Anforderungen dieser Kategorie finden unautorisierte Änderungen an Software und Daten und schützen gegen diese; schränken den Dateneingang und Ausgang ein; überprüfen die Fehlerfreiheit, Vollständigkeit, Korrektheit von Daten; und Handeln im Fehlerfall.

Tabelle 12: Zuordnung von Massnahmen zur Schutz der Schnittstellenklassen

Schutzmass-nahmen	Schnittstellenklassen der NISTIR 7628										
	5	6	7	8	9	13	14	16	17	18	20
SG.AC-01 bis SG.AC-04	X	X	X	X	X	X	X	X	X	X	X
SG.AC-06 bis SG.AC-09	X	X	X	X	X	X	X	X	X	X	X
SG.AC-11	-	-	-	-	X	-	-	-	X	-	-
SG.AC-12	-	-	X	X	X	-	-	-	X	-	-
SG.AC-13	-	-	-	-	X	-	-	-	X	-	-
SG.AC-14	X	X	X	X	X	X	X	X	X	X	X
SG.AC-15	-	-	-	-	X	-	-	-	-	-	X
SG.AC-16 bis SG.AC-21	X	X	X	X	X	X	X	X	X	X	X
SG.AU-01 bis SG.AU-15	X	X	X	X	X	X	X	X	X	X	X
SG.AU-16	-	-	X	X	X	X	X	X	-	-	X
SG.IA-01 bis SG.IA-04	X	X	X	X	X	X	X	X	X	X	X
SG.IA-05	-	-	X	X	X	-	-	-	X	-	X
SG.IA-06	X	X	X	X	-	X	X	X	X	X	X
SG.SC-01	X	X	X	X	X	X	X	X	X	X	X
SG.SC-03	-	-	X	X	X	X	X	X	-	X	X
SG.SC-04	-	-	X	X	-	X	X	X	-	-	-

Schutzmass-nahmen	Schnittstellenklassen der NISTIR 7628										
	5	6	7	8	9	13	14	16	17	18	20
SG.SC-05	X	X	-	-	X	-	X	-	-	-	-
SG.SC-07	X	X	-	X	X	X	X	X	-	X	X
SG.SC-08	X	X	X	X	X	X	X	X	-	X	X
SG.SC-09	-	-	-	-	X	X	X	X	-	-	-
SG.SC-11 bis SG.SC-13	X	X	X	X	X	X	X	X	X	X	X
SG.SC-15 und SG.SC-16	X	X	X	X	X	X	X	X	X	X	X
SG.SC-17	X	X	-	-	X	-	X	-	X	-	X
SG.SC-18 bis SG.SC-22	X	X	X	X	X	X	X	X	X	X	X
SG.SC-26	-	-	X	X	X	-	X	X	-	-	-
SG.SC-29	X	X	-	-	-	X	X	-	X	X	X
SG.SC-30	X	X	X	X	X	X	X	X	X	X	X
SG.SI-01 bis SG.SI-09	X	X	X	X	X	X	X	X	X	X	X

Die Tabelle 13 dokumentiert die Anforderungen und nötigen Schutzmassnahmen aus Sicht der NISTIR 7628. Diese Tabelle beschreibt ausführlich, welche Schutzmassnahmen für die Prozesselemente und schlussendlich für die Koordinationsmodelle umzusetzen sind. Wie bereits erwähnt sollten diese Anforderungen zur Sicherung der Schnittstellen der Koordinationsmodelle EP01-EP05 als eine Art Grundschutz umgesetzt werden.

Tabelle 13: Schutzmassnahmen aus den NIST Schnittstellenklassen 5-7, 13, 14, 16 bis 18 und 20

Bezeich-nung der Schutzmas-snahmen:	Name:	Beschreibung
SG.AC-1	Richtlinien und Vorge-hensweisen für Zugangs-kontrollen	Der Fokus der Zugangskontrollen liegt darauf sicherzustellen, dass Personen, die Zugang zu

		den Ressourcen haben sollen, diesen auch bekommen. Dabei werden Ziele, Rollen und Verantwortlichkeiten sowie der Umfang der Zugangskontrollen festgelegt.
SG.AC-2	Richtlinien und Vorgehensweisen für Zugangskontrollen zu Remote-Zugriffe	Der Remote Zugang ist jeder Zugang zu einem Smart Grid Informationssystem, der durch einen User oder Prozess über ein externes Netzwerk, welches nicht selbst kontrolliert wird, kommuniziert.
SG.AC-3	Account Management	Die Accounts für Smart Grid Informationssysteme werden verwaltet. Dazu gehören Autorisierung, Einrichtung, Aktivierung, Modifizierung, Sperrung und die Löschung von Accounts.
SG.AC-4	Durchführung des Zugangs	Autorisierten Accounts wird der Zugang zum Smart Grid Informationssystem im Einklang mit der Organisations-Policy gewährt.
SG.AC-6	Aufteilung der Pflichten	Die Aufteilung von Verantwortlichkeiten und die Trennung von Funktionen werden benötigt, um Interessenskonflikte zu eliminieren und damit die Unabhängigkeit der Verantwortlichkeiten und Funktionen von Individuen und Rollen zu gewährleisten. Dies geschieht durch zugeordnete Zugangskontrollen. Sicherheitsfunktionen werden nur einem möglichst kleinen Teil von Benutzern ermöglicht.
SG.AC-7	Minimum an Privilegien	Die Benutzer bekommen nur das Minimum an Rechten und Zugängen die sie benötigen.
SG.AC-8	Erfolglose Login Versuche	Für aufeinanderfolgende erfolglose Login Versuche in einer bestimmten Zeiteinheit wird ein Limit festgelegt.
SG.AC-9	Smart Grid Informationssystem Mitteilungen zur Systemnutzung	Bevor der Zugang zu einem Informationssystem gewährt wird, wird eine Mitteilung angezeigt, die Privatsphären- oder Sicherheitshinweise enthält.

SG.AC-11	Konkurrierende Sessions	Die Anzahl von konkurrierenden Sitzungen wird für jeden Nutzer eingeschränkt. Eine solche Einschränkung kann global, nach Account Typen, nach Accounts oder einer Kombination aus diesen erfolgen. Die Einschränkung bezieht sich auf konkurrierende Sitzungen eines Informationssystems und nicht auf konkurrierende Sitzungen eines Benutzers auf verschiedenen Informationssystemen.
SG.AC-12	Gesperrte Sitzungen	Nach einer festgelegten Zeitperiode, in der keine Aktivitäten stattfinden, wird die Sitzung gesperrt. Diese Sperrung bleibt bestehen, bis diese durch den dazugehörigen Identifikations- und Authentifikationsprozess aufgehoben wird.
SG.AC-13	Beendung von Remote-Sitzungen	Das Smart Grid Informationssystem beendet eine Remote-Sitzung am Ende der Sitzung oder nach einer vordefinierten Zeitperiode.
SG.AC-14	Zulässige Handlungen ohne Identifikation und Authentifikation	Es werden spezifische Handlungen identifiziert, die auf dem Informationssystem ohne Identifikation oder Authentifikation ausgeführt werden dürfen. Zusätzlich können auch Handlungen identifiziert werden, die normalerweise eine Identifikation und Authentifikation benötigen, aber unter bestimmten Umständen, wie zum Beispiel Notfällen, können diese umgangen werden.
SG.AC-15	Fernzugriff	Es werden alle Methoden des Fernzugriffs auf Smart Grid Informationssysteme autorisiert, überprüft und geregelt. Dabei ist ein Fernzugriff jeder Zugriff auf ein Informationssystem durch einen Benutzer (oder durch einen Prozess, der für einen Benutzer agiert), der über ein externes Netzwerk kommuniziert (z. B. Internet).

SG.AC-16	Einschränkungen des drahtlosen Zugangs	Der drahtlose Zugang zum Informationssystem muss autorisiert, überwacht und verwaltet werden. Es werden Nutzungseinschränkungen, sowie Implementierungsvorgaben für die WLAN Technologien festgelegt.
SG.AC-17	Zugangskontrollen für mobile Geräte	Es werden Nutzungseinschränkungen, sowie Implementierungsvorgaben für mobile Geräte vorgegeben. Verbindungen von mobilen Geräten zu Smart Grid Informationssystemen müssen autorisiert werden. Es wird auf unerlaubte Verbindungen überwacht.
SG.AC-18	Die Nutzung von externen Informationssystemen	Externe Informationssysteme sind Informationssysteme, oder Komponenten von diesen, die ausserhalb der autorisierten Grenzen liegen. Bei diesen hat das Unternehmen keine Kontrolle über die Anwendung von Sicherheitsanforderung, oder der Bewertung dieser.
SG.AC-19	Einschränkungen beim Zugang zu Kontrollsystemen	Es werden Mechanismen im Design und in der Implementierung eines Smart Grid Informationssystems eingesetzt, um den Zugang zu diesem vom unternehmenseigenen Netzwerk einzuschränken, z. B. read-only Zugänge.
SG.AC-20	Öffentlich erreichbare Daten	Es ist sicherzustellen, dass öffentlich zugängliche Informationen keine nichtöffentlichen Informationen enthalten. Dafür werden Individuen festgelegt, die diese Informationen posten dürfen und sie werden trainiert. Desweiteren werden die öffentlich zugänglichen Daten regelmässig geprüft.
SG.AC-21	Passwörter	Es werden Verfahren für die Erzeugung und Nutzung von Passwörtern entwickelt. Diese Vorgaben legen Regeln für die Komplexität der Passwörter für den Zugang zum Smart Grid Informationssystem fest. Passwörter müssen regelmässig geändert werden. Ausserdem

		werden diese nach einer festgelegten Zeit, in der sie nicht genutzt werden, widerrufen.
SG.AU-1	Vorgaben und Prozeduren für die Prüfung und Verantwortlichkeit	Die Prozeduren werden in einer vom Unternehmen festgelegten Häufigkeit entwickelt, umgesetzt, überprüft und aktualisiert.
SG.AU-2	Überprüfbare Ereignisse	Das Ziel dieser Anforderung ist es die Ereignisse zu identifizieren, die signifikant und relevant sind.
SG.AU-3	Inhalt von Prüfungsprotokollen	Das Informationssystem erzeugt Prüfungsprotokolle mit Datum, Zeitpunkt, Auftrittsort, Typ und Resultat des Ereignisses sowie der Nutzeridentität.
SG.AU-4	Speicherkapazität für Überprüfungen	Es werden extra Prüfungsprotokoll Speicherkapazitäten definiert und es wird überprüft, ob diese noch ausreichend ist um zu verhindern, dass die Kapazitäten überschritten werden.
SG.AU-5	Reaktion auf Fehler bei der Prüfung	Fehler bei der Prüfung beinhalten Software/Hardware Fehler, Fehler bei den Prüfungseinleitungsmechanismen und wenn Speicherkapazitäten erreicht oder überschritten werden. Das Informationssystem alarmiert die vorgesehenen Funktionäre über Fehler bei der Prüfung. Das Informationssystem führt eine vordefinierte Menge an Handlungen aus (z. B. Runterfahren des Informationssystems, Überschreibung des ältesten Protokolls, Stoppen der Erzeugung neuer Prüfungsprotokolle).
SG.AU-6	Überwachen, Analysieren und Berichten	Überprüfung und Analyse von Smart Grid Informationssystemen, sowie Überprüfung von Aufzeichnungen auf Anzeichen von unangemessenen oder ungewöhnlichen Aktivitäten in einer festgelegten Häufigkeit. Solche Funde

		werden an die zuständigen Personen berichtet.
SG.AU-7	Reduzierung der Überwachung und der Berichtserzeugung	Es wird eine Möglichkeit zur Reduzierung der Überwachung und der Berichtserzeugung bereitgestellt. Dies unterstützt die Realzeitanalyse und eine schnelle Untersuchung nach Sicherheitsvorfällen.
SG.AU-8	Zeitstempel	Es werden interne Systemuhren verwendet, um Zeitstempel für die Berichte der Überwachung zu erzeugen. Solche Zeitstempel vom Informationssystem enthalten sowohl das Datum als auch die Zeit und interne Systemuhren werden regelmässig in vorgegebenen Abständen synchronisiert.
SG.AU-9	Schutz von Überprüfungsinformationen	Das Informationssystem sichert aufgezeichnete Informationen und Werkzeuge für diese vor unautorisiertem Zugang, Modifizierung und Löschung.
SG.AU-10	Aufbewahrung von Aufzeichnungen	Aufzeichnungen werden für eine vordefinierte Zeit aufbewahrt, um Untersuchungen zu Sicherheitsunfällen zu unterstützen und regulatorische Anforderungen zur Informationsaufbewahrung zu erfüllen.
SG.AU-11	Durchführung und Häufigkeit von Anforderungen	Die Häufigkeit, in der Kontrollen durchgeführt werden, ist vom Unternehmen festgelegt, um die spezifizierten Sicherheitsanforderungen, sowie die entsprechenden Gesetze und Regulatorien zu erfüllen. Kontrollen können entweder interne Selbstkontrollen oder unabhängige Überprüfungen durch Dritte sein.

SG.AU-12	Qualifikation des Prüfers	Das Kontrollprogramm des Unternehmens spezifiziert die Qualifikationen des Prüfers.
SG.AU-13	Prüfungsprogramm	Es werden Regeln und Bedingungen für die Nutzung der Prüfungsprogramme spezifiziert. Der Zugang zu den Prüfungsprogrammen muss geschützt werden, um jede Möglichkeit des Missbrauchs oder der Kompromittierung zu verhindern.
SG.AU-14	Einhaltung der Sicherheitsrichtlinien	Die Einhaltung der Sicherheitsrichtlinien wird im Rahmen des Prüfungsprogramms des Unternehmens sichergestellt.
SG.AU-15	Initiierung der Prüfung	Es wird eine Möglichkeit bereitgestellt, die die Aufzeichnung für Kontrollen ermöglicht. Ausserdem werden, für eine vorgegebene Liste von Ereignissen, Aufzeichnungen erstellt.
SG.AU-16	Nichtabstreitbarkeit	Das Informationssystem soll dagegen geschützt sein, dass Individuen abstreiten bestimmte Handlungen ausgeführt zu haben.
SG.IA-1	Identifikations- und Authentifikationsrichtlinien und Vorgehen	Das Unternehmen entwickelt, implementiert, überprüft und aktualisiert in einer vom Unternehmen vorgegebenen Häufigkeit ein dokumentiertes Identifikations- und Authentifikationsvorgehen.
SG.IA-2	Identifizierungsmanagement	Das Unternehmen bekommt die Autorisierung von einer Management Authority, um den Identifikator eines Nutzers oder eines Gerätes zuzuweisen.
SG.IA-3	Authentifizierungs-management	Authentifizierungsdaten der Nutzer und Geräte werden verwaltet.
SG.IA-4	Nutzeridentifikation und Authentifikation	Es sollen Anwender, oder Prozesse die im Namen von Anwendern agieren, eindeutig identifiziert werden.

SG.IA-5	Geräteidentifikation und Authentifikation	Für eine festgelegte Liste von Geräten wird eine Verbindung dann zugelassen, wenn zuvor diese Geräte eindeutig identifiziert und authentifiziert wurden.
SG.IA-6	Authentifikation-Feedback	Der Authentifizierungsmechanismus verschleiert Authentifizierungsinformationen während der Authentifizierung, um diese Informationen vor einer möglichen Ausnutzung von unautorisierten Personen zu schützen.
SG.SC-1	Smart Grid Informations System und Kommunikationssystem Vorschriften	In einer vorgegebenen Häufigkeit entwickelt, implementiert, überprüft und aktualisiert das Unternehmen eine dokumentierte Strategie für die Absicherung der Smart Grid Informationssysteme.
SG.SC-3	Isolierung der Sicherheitsfunktionen	Es werden Sicherheitsfunktionen von nicht-Sicherheitsfunktionen isoliert.
SG.SC-4	Datenüberreste	Das Informationssystem verhindert unautorisierte oder ungewollte Datenübertragungen über geteilte Ressourcen.
SG.SC-5	Denial of Service Absicherung	Die Effekte von Denial of Service Attacken sollen begrenzt bzw. gemildert werden.
SG.SC-7	Grenzabsicherung	Es werden die Grenzen des Systems definiert. Ausserdem wird jegliche Kommunikation an der externen Grenze, sowie an den wichtigen internen Grenzen kontrolliert und überwacht.
SG.SC-8	Integrität der Kommunikation	Es wird mit Hilfe von kryptographischen Werkzeugen die Integrität von elektronisch übertragenen Daten sichergestellt. Das Informationssystem ist dabei auch für die Integrität bei der Erstellung, Verpackung und den Umwandlungen während der Vorbereitung zur Übertragung zuständig.

SG.SC-9	Vertraulichkeit der Kommunikation	Es wird die Vertraulichkeit von übertragenen Daten geschützt. Um eine unautorisierte Offenlegung von Daten zu verhindern, werden kryptographische Mechanismen verwendet.
SG.SC-11	Kryptographische Schlüsselerzeugung und Management	Das Unternehmen erzeugt und verwaltet kryptographische Schlüssel, die innerhalb des Informationssystems benötigt werden.
SG.SC-12	Nutzung von validierter Kryptographie	Alle kryptographischen und anderen Sicherheitsfunktionen (wie Hashes, Zufallsgeneratoren usw.) müssen anerkannt und erprobt sein.
SG.SC-13	Collaborative Computing	Das Unternehmen entwickelt, aktualisiert und überprüft regelmässig das Vorgehen für Collaborative Computing. Dazu gehören Möglichkeiten für Video und Audiokonferenzen oder auch Instant Messaging Technologien. Dabei werden dem Nutzer explizite Hinweise gegeben, wenn die Kamera oder das Mikrofon aktiviert sind.
SG.SC-15	Zertifikate für eine Public Key Infrastruktur	Für Smart Grid Informationssysteme, die eine Public Key Infrastruktur nutzen, werden unter Anwendung angemessener Richtlinien Public Key Zertifikate ausgegeben. Alternativ können die Zertifikate auch von einem anerkannten Dienstleister bereitgestellt werden.
SG.SC-16	Mobiler Code	Mobile Code Technologien beinhalten unter anderem Java, JavaScript, ActiveX, PDF, Postscript, Shockwave Movies und Flash Animations.
SG.SC-17	Voice-Over Internet Protocol	Für die Nutzung von Voice-over-IP gibt es Implementierungsvorgaben und Einschränkungen, basierend auf potentiellen Schäden die durch eine bösartige Nutzung entstehen können. Die Nutzung muss autorisiert, überwacht und kontrolliert werden.

SG.SC-18	Systemverbindungen	Alle externen Smart Grid Informationssysteme und Kommunikationsverbindungen werden identifiziert und vor Manipulation und Schäden geschützt. Externe Zugangspunkte zum Smart Grid Informationssystem müssen zum Schutz des Informationssystems abgesichert werden.
SG.SC-19	Sicherheitsrollen	Spezifische Sicherheitsrollen und Verantwortlichkeiten werden für die Nutzer des Smart Grid Informationssystems umgesetzt. Basierend auf der Sensibilität der Daten mit denen der Nutzer arbeitet wird die Rolle definiert, spezifiziert und implementiert. Solche Rollen können für bestimmte Jobs oder aber auch für Individuen festgelegt werden.
SG.SC-20	Authentizität von Nachrichten	Es werden Mechanismen zum Schutz der Authentizität von Gerät-zu-Gerät Kommunikation bereitgestellt. Dazu gehören der Schutz vor veränderten Nachrichten, falsch konfigurierten Geräten und bösartigen Entitäten.
SG.SC-21	Secure Name/Address Resolution Service	Die Organisation ist für die Name/Adressen-Auflösung verantwortlich, um die Herkunft von Daten und Integritätsartefakten zusammen mit den autorisierenden Daten bereitstellen zu können. Ebenso wird dies im Betrieb als Teil eines verteilten, hierarchischen Namensraums nötig, um den Sicherheitsstatus von Unter-Namensräumen zu identifizieren.
SG.SC-22	Rückfall in bekannten Zustand	Für definierte Fehler entsteht bei deren Eintritt ein Rückfall in einen bekannten Zustand. Dadurch kann ein Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit verhindert werden.
SG.SC-26	Vertraulichkeit von Daten im Ruhezustand	Die Sicherheitsfunktion beschreibt die Vertraulichkeit von Daten, die in dem Moment nicht

		genutzt werden. Das Informationssystem stellt kryptographische Mechanismen zum Schutz von kritischen Sicherheitsparametern (kryptographische Schlüssel, Passwörter, Sicherheitskonfigurationen,...) bereit. Dabei bezeichnen Daten im Ruhezustand User- oder Systemdaten, die auf Speichern verortet sind.
SG.SC-29	Partitionierung der Anwendungen	Funktionalitäten des Nutzers werden von Funktionalitäten des Systemmanagements getrennt. Zu den Funktionalitäten gehören unter anderem Funktionen zum Administrieren der Datenbanken, Netzwerkkomponenten und Server. Typischerweise benötigen diese Funktionen privilegierte Zugangsrechte. Die Separierung kann entweder physisch oder auch logisch erfolgen. Zusätzlich wird sichergestellt, dass es für normale Nutzer keine Möglichkeiten zum Administrieren gibt.
SG.SC-30	Partitionierung des Smart Grid Informationssystems	Das Informationssystem wird in Komponenten eingeteilt, die in separaten physischen oder logischen Domänen oder Umgebungen liegen.
SG.SI-1	Richtlinien und Verfahren für die Integrität von Smart Grid Informationssystemen und Nachrichten	In einer vorgegebenen Häufigkeit entwickelt, implementiert, überprüft und aktualisiert das Unternehmen eine dokumentierte Strategie für die Integrität von Smart Grid Informationssystemen und Nachrichten.
SG.SI-2	Korrektur von Mängeln	Es werden Soft- und Firmware identifiziert, die von bekannt gewordenen Mängeln betroffen sind und mögliche Schwachstellen, die sich daraus ergeben.
SG.SI-3	Schutz vor Schadcode und Spam	Es werden Mechanismen zum Schutz vor Schadcode implementiert. Diese Mechanismen werden, sobald es neue Versionen gibt, aktualisiert. Es wird verhindert, dass Nutzer diesen

		Schutz umgehen können und die Mechanismen werden zentral verwaltet. Es werden periodisch Scans auf dem Smart Grid Informationssystem durchgeführt. Diese dürfen aber die Performance nicht mindern.
SG.SI-4	Überwachungswerkzeuge und Techniken für Smart Grid Informationssysteme	Es werden Ereignisse auf dem Informationssystem überwacht, um Angriffe, unautorisierte Aktivitäten und nicht bösartige Fehler zu finden. Die Möglichkeiten der Überwachung können durch eine Vielzahl von Werkzeugen unterstützt werden. Dazu gehören: Systeme die ein Eindringen entdecken, Systeme die ein Eindringen verhindern, Software gegen Schadcode, protokollierende Überwachungssoftware und forensische Werkzeuge zur Netzwerkanalyse.
SG.SI-5	Sicherheitsalarm und Warnungen	Es werden Sicherheitsalarme und Warnungen von anderen Einrichtungen empfangen, sowie selber erzeugt und verbreitet, falls dies als notwendig erachtet wird. Automatismen für die Verbreitung des Sicherheitsalarms und der Warnungen werden im ganzen Unternehmen angewendet.
SG.SI-6	Verifizierung der Sicherheitsfunktionen	Der korrekte Betrieb der Sicherheitsfunktionen muss bei jedem Start, Neustart und in einer festgelegten Frequenz regelmässig verifiziert werden. Das System meldet, wenn Anomalien auftreten. Dazu gehört auch die Meldung falls ein automatischer Sicherheitstest fehlschlägt.
SG.SI-7	Integrität von Software und Daten	Unautorisierte Änderungen an Software und Daten werden festgestellt. Es werden Techniken für die Verifizierung der Integrität genutzt um Hinweise auf Manipulation von

		Daten oder Fehler zu finden. Durch regelmässige Integritätsüberprüfungen werden die Integrität der Software und der Daten beurteilt.
SG.SI-8	Validierung der Input Daten	Es werden Werkzeuge angewendet um Daten auf Genauigkeit, Komplettheit, Echtheit und Authentizität zu überprüfen. Um sicherzustellen, dass die Eingaben dem spezifizierten Format und Inhalt entsprechen, werden diese auf eine gültige Syntax hin überprüft. Beispiele sind Buchstabenmenge und Länge, numerischer Bereich, sowie akzeptierte Werte.
SG.SI-9	Fehlerhandhabung	Es werden die Umstände des Fehlers identifiziert. Es werden Fehlernachrichten erzeugt mit Informationen, die für die Fehlerbehebung notwendig sind, aber einem möglichen Gegner keine potentiell schädlichen Informationen preisgeben.

Aus den vorliegenden 71 Einzelempfehlungen lassen sich für die Schnittstelle Markt/Flexibilität zusammenfassend Empfehlungen für die Umsetzung von IT-Sicherheitsmassnahmen im Rahmen der Koordinationsmodelle in der Branche ableiten. Diese finden sich unter Berücksichtigung der Gesamtrisikoanalyse aus Kapitel 3.8 in Kapitel 4 dieser Studie.

4 Massnahmen und Empfehlungen

Dieser Abschnitt der Studie befasst sich allgemeinen Empfehlungen zu IT-Sicherheit, die sich im Kontext von Smart Grids als Vorbedingungen auch im Kontext der Absicherung der drei untersuchten Koordinationsmodelle aus Sicht der Experten ergeben. Daneben werden die konkreten Ergebnisse und Empfehlungen aus dieser Studie diskutiert und Massnahmen empfohlen.

4.1 Allgemeiner Nutzen von IT-Security und Anforderungen aus Sicht von Smart Grids

Der Nutzen von Massnahmen zur Erhöhung der IT-Sicherheit im Energiesektor besteht vor allem in der Minimierung wirtschaftlicher und volkswirtschaftlicher (Folge-)Schäden durch Angriffe auf unterstützende und primäre IKT-Systeme, um somit sowohl die Sicherheit aller kritischen Infrastrukturen (hier mit dem Fokus auf die Stromwirtschaft) stetig zu erhöhen als auch den Wohlstand und das Leib und Leben des einzelnen Schweizer Bürgers nachhaltig zu schützen [14].

Ein höheres Sicherheitsniveau insgesamt ist für die Kommunikation im Smart Grid nötig, da die kritische Infrastruktur erstens durch ihren hohen Vernetzungsgrad andere Schadensausmasse aufweist, und zweitens höherwertige Angriffe, wie beispielsweise durch semi-staatliche, professionelle Stellen bestehen muss, die über das Internet erfolgen können.

Zahlreiche Untersuchungen (z.B. [46]) zeigen, dass die Folgekosten für eine erfolgreiche Cyber-Attacke zumeist um ein Vielfaches höher als Investitionen sind, um sich dagegen zu schützen. Die Summe der Investitionen und dauernden Betriebskosten für das Umfeld IT-Security sollten daher gerade so hoch sein, dass sie geringer sind als mögliche Folgekosten. Mögliche Folgekosten können für jede Interessensdomäne auf Basis einer Gesamtrisikoanalyse der Versorger-Systemlandschaft, abgeschätzt werden. Ein Problem sowohl in der Kostenrechnung als auch in der Operationalisierung ist jedoch, dass die üblichen IT-Sicherheitsmassnahmen aus der klassischen Office-IT auf die Prozess-IT zur Steuerung von Energienetzen nicht 1:1 übertragbar sind und daher auch ein Kostenvergleich vor einer Einführung schwer fällt.

Die umzusetzenden Massnahmen (Organisatorische Mechanismen und Technologien) müssen andere Gewichtungen in Bezug auf Sicherheitsziele des Betriebs erfüllen. Bei der Office-IT (in dieser Studie IT genannt) liegt der Fokus darauf, beim Ausfall von IKT und dadurch fehlende Kontrolle etwa von Flexibilitäten vor allem finanzielle Schäden vom Unternehmen (z.B. Rechnungslegung von Bilanzkreisverantwortlichen, fehlende Zählerdaten zur Abrechnung, fehlende Prognosen etc.) abzuwenden. Bei der Prozess-IT (in dieser Studie auch OT, Operational Technology, genannt) geht es um den gesicherten Betrieb der kritischen Infrastruktur der elektrischen Energieversorgung 24 Stunden pro Tag, sieben Tage die Woche, 365 Tage im Jahr.

Deshalb hat das Schutzziel der Verfügbarkeit eine höhere Priorität und die Massnahmen sind auf dieses Schutzziel für den Erhalt des Primärbetriebs zu fokussieren, obwohl die anderen Schutzziele letztendlich nicht weniger wichtig sind. Dabei müssen teilweise auch hohe Anforderungen an Echtzeitfähigkeit der Systeme erfüllt werden, die jedoch anderen Schutzzielen wie etwa einer geeigneten Verschlüsselung konfligierend gegenüber stehen.

Die Nutzung der offenen IP-basierten Kommunikation über das Internet für die OT ist vielleicht im Ausnahmefall in einer abgesicherten Variante möglich. Für kritische Anwendungsfälle mit Echtzeitanforderungen ist eine Nutzung von anderen Kommunikationsnetzen nötig, die für den Anwendungsbereich separiert (geschlossene Benutzergruppe) sowie mit benötigter Bandbreite ausgestattet und hochverfügbar sind.

Sollten dabei die Kommunikationsnetze auch Schwarzfallfest, was im Sinne der Koordinationsmodelle sinnvoll wäre, bereitgestellt werden, müssen eben diese für folgende Funktionen geeignet sein:

- Bieten der technischen Voraussetzungen für einen erfolgreichen Wiederanlauf nach einem Schwarzfall
- Aufrechterhaltung der organisatorischen Kommunikation bei einem Grossschadensereignis mit Schwarzfall

Im ersten Fall liegt der Fokus auf reinen Steuerungsfunktionen. Das Smart Grid ist in einer für den zuverlässigen Wiederanlauf vorgesehene Konfiguration, am besten mittels lokalen Fallbackkonfigurationen, zu schalten. Dezentrale Erzeugungsanlagen (hier genutzt als Flexibilitäten) sind entweder im Inselbetrieb (Eigenversorgung) zu fahren oder abzuschalten und die Regler im Netz sind auf einen definierten (Normal-)Zustand festzusetzen, damit Ein- schwingvorgänge vermieden werden, die den Wiederanlauf der Netze gefährden können.

Durch die im zukünftigen Smart Grid zunehmende Vernetzung der Systemlandschaften steigt die Anforderung, die Systemlandschaft eines Versorgers sicherheitstechnisch im State-of-the-Art zu halten. Dies bedeutet zumeist im Gegensatz zur heutigen Situation, dass sichere Updatetechnologien und schnell verfügbare Patches zur kurzfristigen und störungsfreien Einspielung zur Verfügung stehen sollten. Schon heute ist etwa in der ICS Cert Datenbank[11] zu erkennen, dass immer mehr IED Geräte und SPS Geräte kritische Lücken haben, die mit Firmware Updates zeitnah korrigiert werden sollten, was vermutlich zahlreiche Versorger vernachlässigen, da es hierfür keinerlei Prüfung gibt. Die Technikräume in Umspannanlagen und Rechenzentren sind ein zentrales Elemente der IT-Infrastruktur, auch in den kritischen Infrastrukturen. Hier werden die erhobenen Daten und Informationen zusammengeführt und verarbeitet.

Daher erwarten Betreiber von IT-Infrastrukturen und Rechenzentren, dass sich Sicherheitsrisiken objektiv identifizieren und professionell bewerten lassen. Jedoch ist die Sicherheit nicht nur für die Systemlandschaft im Versorger selber, sondern auf für Systeme ausserhalb der unternehmensinternen Zone wie etwa im Kontext der Koordinationsmodelle zu gewährleisten.

Im Rahmen dieser Arbeiten in Kapitel 3.7 wurden für verschiedene Kategorien Massnahmen auf Basis der Schnittstellen der Koordinationsmodelle identifiziert. Diese Massnahmen umfassen die Dimensionen:

- Zugangskontrollmassnahmen zu den Systeme der kritischen Infrastruktur
- Prüfung und Verantwortlichkeit für das ISMS der kritischen Infrastruktur
- Identifikation und Authentifikation für einzelne Komponenten und Prozesse in der kritischen Infrastruktur
- Massnahmen zur Absicherung der Smart Grid Informationssysteme und der dazugehörigen Kommunikation
- Massnahmen zur Sicherstellung der Integrität der Daten von Energieinformationssystemen und Nachrichten.

Diese Massnahmen werden in den folgenden Abschnitten diskutiert und vorgestellt.

4.2 Datenschutz- und Datensicherheit – Empfehlungen

Die Ergebnisse der AWK Studie konnten durch eine vergleichbare Sicht auf den Betrachtungsgegenstand der Flexibilitäten innerhalb der Consentec Koordinationsmodellen übernommen und bestätigt werden. Dabei wurden die in der Modellierung identifizierten Datenobjekte dieser Studie auf Datenobjekte der AWK Studie abgebildet. Es fand sich für jedes Objekt dabei ein

[11] https://ics-cert.us-cert.gov/

passendes Gegenstück auf AWK Seite, das bereits bzgl. der Aspekte für Datensicherheit bzw. Datenschutz analysiert wurde. Diese bereits durch das BFE bestätigten Analysen der AWK können in dieser Studie übernommen werden, so dass auch für die 16 in dieser Studie zu betrachtenden Datenobjekte eine Datensicherheits- und Datenschutzeinstufung vorliegt.

Zusätzlich wurden diese Datenobjekte in dieser Studie bzgl. ihrer Einstufung gemäss SGIS Methodik der so genannten Dataprotection Classes untersucht. Dabei werden sie gemäss dem Schema Prozessdaten (DPC-2) bzw. personenbezogene Daten (DPC-1) klassifiziert.

Ein Verlust von personenbezogenen Daten bzw. eine Offenlegung hat meist keine direkten Auswirkungen im Netzbetrieb, wohl aber bzgl. der Reputation eines Unternehmens und bzgl. der Verletzung des kantonalen oder Bundesdatenschutzrechts. Dies kann zu einem Vertrauensverlust unterschiedlicher Dauer führen, einem Reputationsverlust. Bei Prozessdaten kann es zu einer direkten Bedrohung der Assets bzw. des Netzbetriebs kommen, daher sind diese Daten grundsätzlich kritischer bzw. ein Umgang mit ihnen erfolgt auch grundsätzlich auf einem höheren Schutzniveau.

Grundsätzlich ist in der Studie eine sehr homogene Sicht auf die Daten in den Koordinationsmodellen durch die SGIS-Analyse zu erkennen, das Gefährdungspotenzial jedoch zumeist im Bereich 3-4, falls Verletzungen bzgl. der Nutzung der Daten auftreten. Dabei ist jedoch zu beachten, dass gemäss ICT Continuity VSE Regel ab SL 3 bereits eine Krise entstehen kann (ungeplantes Verhalten der elektrischen Energieversorgung mit über 50 MWh nicht zeitgerecht gelieferter Energie). Ein Verlust der Daten der Koordinationsmodelle hat daher das Potenzial, durch eine geeignete Nutzung durch einen Angreifer theoretisch eine Krise auf lokaler Ebene auszulösen. Die entsprechenden Risiken, die in der Tabelle 10 für die jeweiligen Schnittstellen eingeschätzt werden, sind in der Schweiz also generell hoch einzustufen.

Insgesamt gilt für diese Studie die Empfehlung, die Ergebnisse der AWK Studie, Kapitel 6, auch auf die hier in der Studie klassifizierten Datenobjekte gemäss AWK anzuwenden und sie wie ihre Gegenstücke in der AWK Studie bzgl. der rechtlichen Situation zu behandeln. Dies stellt sicher, dass die abgestimmte rechtliche Basis aus der AWK Studie und die dazugehörigen Rechtsauffassung auch im Kontext der Koordinationsmodelle gültig ist.

Dadurch ist eine sehr detaillierte Analyse für diese Daten erfolgt, ohne dass dies im Rahmen dieser Studie erneut aufwändig erfolgen musste. Als zusätzlichen Mehrwert neben der konsolidierten Sicht des Datenschutzes und der Datensicherheit auf die Datenobjekte der Koordinationsmodelle wurde mittels der SGIS Datenschutzklasseneinstufung eine Klassifkation bzgl. der Kritikalität der Daten als personenbezogene Daten oder Prozessdaten durchgeführt. Darauf aufbauend wurde eine SGIS Einstufung vorgenommen, welche ein Schadensausmass bei Verlust oder Offenlegung der Datenobjekte der Koordinationsmodelle bietet. Diese ist konsistent zu der Risikoanalyse für die Schnittstellen und ermöglicht damit eine integrative Sicht, die vorher nicht existierte.

4.3 Massnahmen im Kontext der Schnittstellen der Koordinationsmodelle dieser Studie

Für die Consentec Koordinationsmodelle gilt, dass die Ergebnisse der Consentec Studie erkennen lassen, dass die Koordinationsmodelle im Detail sehr unterschiedlich ausgestaltet werden können und sich aus den Gestaltungsdetails auch sehr unterschiedliche Anforderungen hinsichtlich Datenkommunikation und Systemkomponenten – und dadurch auch für ihren Datenschutz und die IT-Sicherheit - ergeben können. Es erscheint der Consentec nicht sinnvoll, frühzeitig bestimmte Ausgestaltungsdetails universell festzulegen, da dann eine der jeweiligen Fallkonstellation angemessene Gestaltung kaum möglich ist. Diese Vorbedingung hat Auswirkungen auf die konkreten Empfehlungen dieser Studie, da eine direkte Implementierung und

Empfehlung dedizierter Standards für eine Datenformate und Schnittstellen auf Implementierungsebene nicht möglich ist. Es sind daher Massnahmen für die generischen Schnittstellen der Consentec Koordinationsmodelle mittels einer Anwendungsfallanalyse ermittelt worden.

Insgesamt wurden für die Koordinationsmodelle und die sich daraus ergebenden Anwendungsfälle 71 Schutzbedarfe und daraus abgeleitet auch passende Massnahmen gemäss NISTIR 7628 ermittelt. Da die Risikoanalyse für die Mehrzahl der Schnittstellen und somit für die Koordinationsmodelle eine höhere Gefährdung ohne Umsetzung der identifizierten Massnahmen aus dem NISTIR 7628 ergab, wird empfohlen, diese bei einer Implementierung der Koordinationsmodelle als eine Art Grundschutz für das Smart Grid in diesem Umfeld auch umzusetzen. Unter Grundschutz wird im Rahmen der Studie die Erarbeitung von Massnahmen zum Erreichen eines mittleren, angemessenen und ausreichenden Schutzniveaus verstanden. Basis eines Grundschutzkonzepts ist der initiale Verzicht auf eine detaillierte Risikoanalyse. Es wird von pauschalen Gefährdungen ausgegangen. Der Grundschutz stellt dabei einen Massnahmenkatalog zur Verfügung, der bei einer Gefährdung zum Einsatz kommt. Im Rahmen dieser Studie erfolgte die Risikoanalyse dazu, die gefährdetsten Schnittstellen der Koordinationsmodelle zu identifizieren und damit für die Umsetzung der Massnahmen gleichsam zu priorisieren. Diese als sinnvoll zu erachtenden Massnahmen sind dediziert im Anhang (6.2) dieser Studie aufgeführt.

4.4 Umsetzungsvorschläge

Die konkreten Umsetzungsvorschläge auf Technologien (nicht Instanzen, d.h. konkrete Systeme eines einzelnen Versorgers eines einzelnen Herstellers) und die organisatorischen Aspekten finden sich im Anhang der Studie, aufgeschlüsselt auf die individuellen Massnahmen. Zusätzlich ist eine Abbildung der im Rahmen dieser Studie empfohlenen NISTIR 7628 Massnahmen auf die ENISA „Appropriate Security Measures for Smart Grids“ im Anhang enthalten (6.3), da diese Massnahmen im Rahmen der AWK Studie im Fokus für die Datensicherheits- und Datenschutzaspekte standen.

Auf Basis des ENISA-Modells können in unterschiedlichen Sicherheitsdomänen in einer ersten Phase Implementierungstiefen klassifiziert werden (sophistication levels), für deren technischen Umsetzung ein Nachweis zu erbringen ist. Dieser Methodik folgend kann die Reihenfolge bzw. Priorisierung der durchzuführenden Maßnahmen auf Basis der „sophistication level“ durchgeführt werden. Eine solches Profil kann analog für die NISTIR 7628 Massnahmen etabliert und durch die Branche als eine Art Schutzprofil (definiert als implementierungs-unabhängige Menge von Sicherheitsanforderungen an eine Gruppe oder eine Kategorie von zu untersuchenden IT-Systemen) erarbeitet und umgesetzt werden. Die Erarbeitung eines Schutzprofils mit den detaillierten Anforderungen und deren Priorisierung wirkt sich vorteilhaft auf das Sicherheitsniveau der Koordinationsmodelle aus. Die Anforderungen können in der nötigen Breite und Tiefe definiert werden.

Dadurch, dass das Schutzprofil subsidiär auf Basis einer Schutzbedarfsanalyse, welche aus dieser Studie mit der kanonischen Methodik verfeinert werden kann, erarbeitet wird, ist zudem ihre Angemessenheit, auch vor dem Hintergrund der Schweiz spezifischen Situation mit vielen heterogenen Netzbetreibern, gesichert. Ein ähnlicher Prozess wurde auch mit dem RASSA Projekt und der infraprotect Studie in Österreich verfolgt.

Eine formale Konformitätsprüfung gegen das individuell für die Schweiz erarbeitete Schutzprofil bietet ein gutes Vertrauenswürdigkeits-Aufwands-Verhältnis. Zudem bietet ein Schutzprofil eine detaillierte Wegleitung für die Umsetzung der Koordinationsmodelle. Die individuell auf das nationale Schutzprofil ausgelegte Prüfung ermöglicht eine geeignete und schlanke Umsetzung der Konformitätsprüfung. Ein ähnlicher Ansatz zur Gewährleistung der Datensicherheit für intelligente Messsysteme bei Endverbrauchern wurde in einem vom BFE in Auftrag gegebene Studie skizziert [45].

Neben diese eher operativen Empfehlungen und Massnahmen an der Schnittstelle Markt und Netz sollten noch weitere Aspekte berücksichtigt werden, die eine Etablierung einer Sicherheitskultur für die kritische Infrastruktur und ihren Betrieb fördern könnte [etwa in 28]. Zudem ist zu betonen, dass in dieser Studie ein methodisches, gut dokumentiertes, und reproduzierbares Vorgehen mittels der Verwendung von robusten Methodiken angenommen wird. Dieses Vorgehen, welches in der vorliegenden Studie auf die Koordinationsmodelle aus der Consentec Studie angewendet wird, kann für weitere Smart Grid Anwendungsfälle angenommen werden.

Aus regulatorischer Sicht ist eine Kostenverteilung entsprechend der jeweiligen Interessensgruppen im Prozess der Koordinationsmodelle offensichtlich fair, d.h. die Kosten werden von dem Stakeholder übernommen, der ein originäres Interesse an der Umsetzung entsprechender Schutzmassnahmen hat. Gibt es jedoch wie zu erwarten mehrere Interessengruppen, sollten Kosten entsprechend aufgeteilt werden. Durch die Liberalisierung des Energiemarktes werden Netzbetreiber Energienetze in Zukunft so betreiben, dass sie prioritär wirtschaftliche Ziele erfüllen. Die Gefahr besteht, dass die Verfügbarkeit und Zuverlässigkeit der Daten somit nur als sekundäres Ziel verfolgt werden, d.h. es werden diejenigen Massnahmen umgesetzt, die erforderlich sind, um das wirtschaftliche Ziel im Rahmen der gesetzlichen Vorgaben sicherzustellen und nicht zu gefährden. Hierüber hinausgehende Risiken müssen aber in Zukunft ebenfalls adressiert werden, um die Sicherheit der kritischen Infrastruktur zu gewährleisten

Im Falle zu befürchtender volkswirtschaftlicher Schäden die durch ein Versagen der Koordinationsmodelle entstehen, sind folglich nicht nur Unternehmen in die Pflicht genommen, sich am Risikobudget und an Kosten für die Risikominimierung und geeigneten Massnahmen zu beteiligen, sondern ebenfalls der Staat. Es wird dem BFE empfohlen, ein Modell zur Kostenwälzung und Verantwortlichkeit, ggf. in Zusammenarbeit mit der Branche, zu erarbeiten. Dabei sollte für die Teildomäne der Koordinationsmodelle (immer im Falle einer Umsetzung gemäss Consentec) in Abstimmung mit der Branche ähnlich wie in Österreich erfolgt eine Umsetzung und Priorisierung der Massnahmen wie in der Studie vorgeschlagen diskutiert und Kostenverantwortlichkeiten klar definiert werden.

Glossar

Die im Glossar verwendeten Begriffe entsprechen wie die anderen innerhalb der Studie genutzten Definitionen den IEC Begriffen aus der Electropedia[12], wenn nicht anders gekennzeichnet.

Begriff	Definition
Aktor	Ein Akteur bezeichnet in der UML ein Element, das mit dem modellierten System interagiert. Meistens steht er in Beziehung zu einem Anwendungsfall: es ist der Akteur, der einen Anwendungsfall anstösst oder der die erwarteten Resultate eines Anwendungfalls entgegennimmt.
Anlage	Im elektrischen Netz an Mittel- und Niederspannung angeschlossener Energieerzeuger.
Anlagendatenbank	Statische Informationen zu integrierten Anlagen (Art der Anlage, Alter, Standort, installierte Leistung,…). Die Anlagendatenbank ist dabei eine Spezialisierung der Stammdatenbank.
Anwendungsfall (Use Case)	Liefern eine detaillierte Ablaufbeschreibung aus Sicht der Akteure und Komponenten.
BDEW Whitepaper	Anforderungen an sichere Steuerungs- und Telekommunikationssysteme des deutschen BDEW
Business Layer (SGAM) - Geschäftsebene	Die Geschäftsebene des SGAM stellt eine Geschäftsprozesssicht für die ausgetauschten Daten zur Verfügung. Sie wird zumeist dafür genutzt, Prozesse, Marktstrukturen, Produkte und Dienste, aber auch Fähigkeiten eines Unternehmens abzubilden.
Communication Layer (SGAM) - Kommunikationsebene	Der Schwerpunkt der Kommunikationsebene im SGAM ist die Darstellung der technischen Protokolle und Mechanismen für einen möglichst interoperablen Datenaustausch zwischen den Komponenten der tieferen Ebenen mit einem Bezug auf die zu erbringenden Anwendungsfälle.
Component Layer (SGAM) - Komponentenebene	Auf der Komponentenebene wird die physische Verteilung aller teilnehmenden Komponenten im Smart Grid Kontext dargestellt. Dies umfasst dabei Akteure, Anwendungen, Feldgeräte, Schutz- und Kontrolltechnik, Netzwerke und sonstige Arten von digitaler Verarbeitung.
Customer Premise Domain (SGAM) - Kundendomäne	Die Kundendomäne umfasst typischerweise die Endnutzer von elektrischer Energie, aber dadurch auch heutzutage Erzeuger mittels DER. Es kann sich jedoch um einen kommerziellen, industriellen oder privaten Kontext handeln.
DER Domain (SGAM) – EE-Domäne	Die EE-Domäne repräsentiert verteilte Energierzeuger mit direkter Verbindung zum Netz, typischerweise mit einer Kapazität von 3kW bis 10.000 kW. Diese können zumeist direkt gesteuert werden.
DER Gateway	Bildet die Schnittstelle zwischen einem möglicherweise komplexen und proprietären System von Erzeugungsanlagen und Verbrauchern bei einem Prosumer und den Systemen und Akteuren ausserhalb dieses Systems.

[12] www.electropedia.org

Dezentrale Energie Ressourcen (DER)	Energieerzeuger mit vergleichsweise geringer Leistung, die nicht zentral an das Übertragungsnetz, sondern dezentral und verbrauchernah am Mittel- oder Niederspannungsnetz angeschlossen sind.
DIN SPEC 27009 – ISO/IEC 27019	Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 (Referenz zum BDEW Whitepaper siehe Anlage Tabelle B.1)
Distribution Domain (SGAM) - Verteilnetzdomäne	Stellt die Infrastruktur und Organisation der elektrischen Energieverteilung zum Kunden zur Verfügung
Enterprise Zone (SGAM) - Unternehmenszone	Die Unternehmensebene umfasst geschäftliche und organisatorische Prozesse, Dienste und Infrastrukturen des Unternehmens, z.B. Assetmanagement, Ausbildung, Kundenmanagement, Rechnungswesen und Beschaffung.
Erneuerbare Energien (EE)	Energie aus schnell nachwachsenden Rohstoffen oder im Rahmen des menschlichen Zeithorizonts praktisch unerschöpflich verfügbaren Energieträgern.
Fahrplan	Ein Fahrplan gibt für jede Viertelstunde innerhalb der Dauer einer entsprechenden Übertragung an, wie viel Leistung zwischen Bilanzkreisen ausgetauscht bzw. am Einspeiseknoten/ Entnahmeknoten eingespeist/ entnommen wird.
Field Zone (SGAM) - Feldzone	Die Feldebene umfasst die Geräte zum Schutz, Steuerung und Überwachung der Prozesse im Stromnetz, z.B. also Schutzrelais, Abgangsfeldüberwachung sowie weitere IEDs zur Prozessdatenerfassung.
Fluktuierende Erzeugung/ Einspeiser	Stark schwankende, von äusseren Einflüssen wie Wetter abhängige Erzeugung von Strom.
Frequenzhaltung	Die Frequenzhaltung bezeichnet die Ausregelung von Frequenzabweichungen infolge von Ungleichgewichten zwischen Einspeisung und Entnahme (Wirkleistungsreglung) und erfolgt durch die Primär- und Sekundärregelung sowie unter Nutzung von Minutenreserven.
Frequenz-Leistungsregelung	Im Netz muss zu jedem Zeitpunkt die Leistungsbilanz zwischen Erzeugung und Abnahme (inkl. Netzverluste) ausgeglichen sein. Bereits kurzfristige Abweichungen in der Leistungsbilanz im Bereich von nur wenigen Sekunden führen zu spürbaren Veränderungen der Netzfrequenz.
Function Layer (SGAM) - Funktionsebene	Die Funktionsebene beschreibt die Funktionen und Dienste sowie deren Zusammenhang aus einer Architektursicht. Die Funktionen werden unabhängig von Akteuren und physischen Implementierungen in Anwendungen, Systeme oder auch Komponenten dargestellt. Sie werden aus Anwendungsfallbeschreibungen abgeleitet.
Generation Domain (SGAM) - Erzeugungsdomäne	Stellt die Erzeugung auf Grosskraftwerksebene da, etwa Kohle oder Kernkraftwerke, Off-Shore Windparks sowie grosse Solarparks.
Hausanschluss	Verbindungsstelle zwischen Elektrizitätsnetz und den Stromleitungen des Kunden.
IKT Gateway	Die Smart Grid „Fritz Box“ zur kommunikativen Anbindung der elektrischen Anlagen, inkl. Protokollumsetzer, usw.

Information Layer (SGAM) - Informationsebene	Die Informationsebene beschreibt die genutzten und ausgetauschten Informationen zwischen Funktionen, Diensten und Komponenten. Sie umfasst Informations-objekte und die dazugehörigen kanonischen Datenmodelle. Diese Objekte und Datenmodelle dienen der technischen Interoperabilität.
Intelligentes Messgerät	Der Begriff intelligentes Messgerät bezieht sich auf einen elektronischen Elektrizitätszähler - auch Smart Meter genannt. Seine Hauptaufgabe ist das Gewinnen von Messwerten des Elektrizitätsverbrauchs und der Elektrizitätsproduktion. Standardmässig sind diese Geräte mit weiteren Eigenschaften ausgerüstet, die sie auch zur Wahrnehmung weiterer Aufgaben befähigen. So können sie beispielsweise Spannungsabfälle messen, Störungen protokollieren oder Messwerte an dedizierte Tarifregister zuweisen. Diese weiteren Eigenschaften werden durch die technischen Mindestanforderungen an intelligente Messsysteme konkretisiert [44].
Interoperabilität	Bezeichnet allgemein die Fähigkeit unterschiedlicher technischer Systeme, zusammenarbeiten zu können. Die Zusammenarbeit umfasst dabei den syntaktisch und semantisch korrekten Austausch von Informationen mittels Kommunikation.
Lastmanagement	Ziel des Lastmanagements ist es, Spitzenlast zu verringern und den Lastgang zu verstetigen sowie den Leistungsbedarf, soweit möglich, angemeldeten Fahrplänen anzupassen.
Lastprofil	Gibt den Verlauf des elektrischen oder thermischen Verbrauchs einer Einheit innerhalb eines definierten Zeitraumes an. Für bestimmte Verbrauchergruppen gibt es sogenannte Standardlastprofile, die einen repräsentativen Verbrauch dieser Gruppe darstellen.
Leitwarte	Sammlung von Daten zur Überwachung und deren Verarbeitung zum optimierten Betrieb des zu leitenden Objekts (z.B. ein Kraftwerk oder ein Stromnetz).
Market Zone (SGAM) - Marktzone	Die Marktzone wird zur Darstellung der Marktmechanismen entlang der elektrischen Wertschöpfungskette genutzt, z.B. Energiehandel, Retail, Mass Market, …
Migrationspfade	Beschreiben Abhängigkeitsverhältnisse zwischen Technologien/ Technologiefeldern, die relevant sind für die Weiterentwicklung der Technologie.
Netzberechnungssystem	Programm, welches auf Basis physikalischer Zusammenhänge Lastfluss-/ Lastprofilberechnungen durchführt und dadurch den Zustand des Netzes (Knotenspannungen, Leistungsflüsse, etc.) ermittelt.
Netzbetreiber	Inhaber von Netzbetriebsmitteln und Leitungen zur Gewährleistung der Versorgung aller Verbraucher mit elektrischer Energie in vorgegebenen Spannungs- und Frequenzbereichen.
NISTIR 7628	Steht für das us-amerikanische “National Institute of Standards and Technology” (NIST) “Internal Report” (IR) – “Guidelines for Smart Grid Cyber Security” (7628)
Operation Zone (SGAM) - Netzbetriebszone	Steht für den Netzbetrieb und die dazugehörigen Systeme für Verteilnetzmanagement, Energiemanagement für Erzeugung und Übertragung, Microgridbetrieb, aber auch

	moderne Konzepte wie Virtuelle Kraftwerke, EV-Flotten-ladeinfrastruktur und mehr.
Plug & Automate	Systemlösung zur Netzautomatisierung, welches in der Lage ist, sich an Veränderungen der Einspeise- und Last-struktur, aber auch an Veränderungen der Netztopologie und der Sachdaten, selbstständig anzupassen.
Process Zone (SGAM) - Prozesszone	Umfasst sowohl das primäre Equipment wie Generatoren, Transformatoren, Schutz, Kabel als auch Lasten und die tatsächliche Energieumwandlung
Sensor	Quantitative Erfassung physikalischer Messgrössen.
Spannungsband	Toleranzbereich um die Nennspannung in einem Netz. Nach EN 50160 darf die Spannung in einem Stromnetz maximal um 10% nach oben und unten vom Sollwert ab-weichen. Hohe Last führt zum Spannungsabfall, hohe Einspeisung zur Spannungserhöhung.
Spannungshaltung	Die Spannungshaltung dient der Aufrechterhaltung eines akzeptablen Spannungsprofils im gesamten Netz. Dies wird durch eine ausgeglichene Blindleistungsbilanz in Ab-hängigkeit vom jeweiligen Blindleistungsbedarf des Net-zes und der Kunden erreicht.
Station Zone (SGAM) Stationszone	Bietet eine Aggregationsebene für Konzepte wie Schalt-anlagenautomation, Datenkonzentratoren etc.
Systemdienstleistun-gen (SDL)	Dienstleistungen, die für den Betrieb eines Elektrizitäts-versorgungssystems notwendig sind und vom Betreiber und/oder von Nutzern des Elektrizitätsversorgungssys-tems bereitgestellt werden
Transmission Domain (SGAM) - Übertra-gungsnetze	Stellt die Infrastruktur für die Modellierung der Übertra-gungsnetzkomponenten zur Verfügung.
Verbraucher	Abnehmer elektrischer Leistung.

5 Literatur

[1] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Information Security, Report, November 2012

[2] CEN-CENELEC-ETSI: Smart Grid Coordination Group technical report, Reference Architecture for the Smart Grid version 1.0 (draft) 2012-03-02, 2012

[3] IEC 62559 IntelliGrid Methodology for Developing Requirements for Energy Systems, 2008.

[4] A. Cockburn, Writing Effective Use Cases, Addison-Wesley Professional, 2001.

[5] DKE, The German Standardization Roadmap E-Energy/Smart Grid, VDE, 2010.

[6] J.M. González and H.-J. Appelrath, “"Energie-RMK" Ein Referenzmodellkatalog für die Energiewirtschaft,” GI-Modellierung 2010, 2010, pp. 319-334.

[7] NIST, NIST Framework and Roadmap for Smart Grid Interoperability Standards, 2010.

[8] Appelrath et al: IT-Architekturentwicklung im Smart Grid – Perspektiven für eine sichere markt- und standardbasierte Integration erneuerbarer Energien, Springer Gabler 2012

[9] M. Uslar et al: Standardization in Smart Grids: Introduction to IT-related methodologies, architectures and standards, Springer, 2012

[10] A. Berger et al.: Reference Architecture for Secure Smart Grids in Austria – RASSA. Stakeholderprojekt, Endbericht, 2016

[11] VSE, Beiträge der Erzeugungstechnologien zur Stromversorgung und Stabilität des elektrischen Systems, Oktober 2013

[12] C. Rupp, S. Queins, and B. Zengler, UML 2 Glasklar, Hanser Fachbuch, 2007.

[13] B. Schienmann, Kontinuierliches Anforderungsmanagement. Prozesse - Techniken - Werkzeuge, Addison-Wesley, 2001.

[14] Smart Grid Roadmap Schweiz: Wege in die Zukunft der Schweizer Elektrizitätsnetze BFE, 2015, http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06308

[15] NIST, NISTIR 7628 – „Guidelines for Smart Grid Cyber Security“, Volume 1-3, Edition 2, 2014

[16] Datensicherheit und Datenschutz für Smart Grids: Offene Fragen und mögliche Lösungsansätze AWK im Auftrag vom BFE, 2014 http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06012

[17] Consentec: Koordination von Markt und Netz – Ausgestaltung der Schnittstellen, Consentec im Auftrag vom BFE, 2015

[18] Smart Grid Security certification in Europe – Challenges and recommendations ENISA, December 2014 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and- services/smart-grids-and-smart-metering/smart-grid-security-certification/smart-grid-security- certification-in-europe

[19] VSE, Branchenempfehlung Strommarkt Schweiz: ICT Continuity – Umsetzungsempfehlungen zur Gewährleistung der ständigen Disponibilität der Informatik- und der Kommunikationstechnologie zwecks Sicherstellung der Versorgung, 2011

[20] ENISA, Appropriate Security Measures for Smart Grids, 2012

[21] Datenschutzgesetz (DSG) http://www.admin.ch/opc/de/classified-compilation/19920153/201401010000/235.1.pdf

[22] Fernmeldegesetz (FMG) http://www.admin.ch/opc/de/classified-compilation/19970160/201007010000/784.10.pdf

[23] Secunet: SIKT – Sichere Informations- und Kommunikationstechnologien für ein intelligentes Energienetz, Studie für das deutsche BMWi, 2013 – VS-nfD

[24] Bundesamt für Energie (BFE). (2013). Forschungsprogramm Netze. Bundesamt für Energie (BFE). (2010). Positionspapier zu "Smart Grids". Bern, Schweiz: UVEK.

[25] Bundesamt für Energie (BFE). (2012). Energieforschungskonzept des Bundesamts für Energie 2013- 2016.

[26] Bundesamt für Energie (BFE). (2012). Grundlagen Energieversorgungssicherheit. Bern.

[27] Bundesamt für Energie (BFE). (2013). Gesetzesentwurf und Botschaft zum 1. Massnahmenpaket der Energiestrategie 2050 vom 4. September 2013. Bern, Schweiz.

[28] Bundesamt für Energie (BFE). (2013). Pilot- und Demonstrationsprogramm - Konzept. Bern, Schweiz.

[29] Microsoft, Smart Energy Reference Architecture, 2012

[30] Consentec GmbH. (2013). Zustandsanalyse und Entwicklungsbedarf von Technologien für ein Schweizer Smart Grid. Bern, Schweiz.

[31] DISCERN, D4.1: Identification of Current System Architecture, www.discern.eu, 2015

[32] ISO IEC 42010, 2011

[33] M. Irlbeck at al.: Towards a Bottom-Up Development of Reference Architectures for Smart Energy, IEEE 2013

[34] Sandia National Laboratories: Micro-Grid Security Reference Architecture, 2012

[35] Sebastian Rohjans, Mathias Uslar, Robert Bleiker, Joée González, Michael Specht, Thomas Suding, Tobias Weidelt: Survey of Smart Grid standardization studies and recommendations, Smart Grid Communications (SmartGridComm), 583-588, IEEE

[36] J. Trefke, S. Rohjans, M. Uslar, S. Lehnhoff, L. Nordstrom, A. Saleem: Smart Grid Architecture Model use case management in a large European Project, Smart Grid Innovative Smart Grid Technologies Europe (ISGT EUROPE), 1-5, IEEE 2013

[37] H. Englert, M Uslar: Europäisches Architekturmodell für Smart Grids–Methodik und Anwendung der Ergebnisse der Arbeitsgruppe „Referenzarchitektur “des EU Normungsmandats M/490, VDE-Kongress 2012

[38] M. Uslar et al.: Untersuchung des Normungsumfeldes zum BMWi-Förderschwerpunkt" e-Energy-IKT-basiertes Energiesystem der Zukunft, Studie für das Bundesministerium für Wirtschaft und Technologie (BMWi), 2009

[39] M. Uslar, C. Rosinger, S. Schlegel, R. Santodomingo-Berry: Aligning IT Architecture Analysis and Security Standards for Smart Grids, Advances and New Trends in Environmental and Energy Informatics, 115-134, Springer 2016

[40] M. Uslar, Energy Informatics: Definition, State-of-the-Art and New Horizons, ComForEn 2015 - 6. Symposium Communications for Energy Systems, Vienna 2015

[41] C. Rosinger, M Uslar: Work Package 1.5: Information Security in Agent-Based Energy Management Systems, Smart Nord Final Report, 77-90, 2015

[42] M. Uslar, C. Rosinger, S. Schlegel: Security by Design for the Smart Grid: Combining the SGAM and NISTIR 7628, Computer Software and Applications Conference Workshops (COMPSACW), Västeras, IEEE, 2014

[43] C. Dänekas, C. Neureiter, S. Rohjans, M. Uslar, D. Engel, Towards a model-driven-architecture process for Smart Grid projects, Digital enterprise design & management, 47-58, Springer 2013

[44] BFE: Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz, Technische Mindestanforderungen und Einführungsmodalitäten,17.11.2014

[45] VZSecurity: Ansätze zur Gewährleistung der Datensicherheit für intelligente Messsysteme bei Endverbrauchern, Studie im Auftrag des BFE, 2015

[46] Untersuchungen und Studie der RSA Deutschland, 2013

6 Anhang

6.1 NISTIR 7628 Schnittstellen – englische Bezeichner der Logical Interfaces

- *Logical Interface Category 1: Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints*
- *Logical Interface Category 2: Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints*
- *Logical Interface Category 3: Interface between control systems and equipment with high availability, without compute or bandwidth constraints*
- *Logical Interface Category 4: Interface between control systems and equipment without high availability, without compute or bandwidth constraints*
- *Logical Interface Category 5: Interface between control systems within the same organization*
- *Logical Interface Category 6: Interface between control systems in different organizations*
- *Logical Interface Category 7: Interface between back office systems under common management authority*
- *Logical Interface Category 8: Interface between back office systems not under common management authority*
- *Logical Interface Category 9: Interface with business to business (B2B) connections between systems usually involving financial or market transactions*
- *Logical Interface Category 10: Interface between control systems and non-control/ corporate systems*
- *Logical Interface Category 11: Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements*
- *Logical Interface Category 12: Interface between sensor networks and control systems*
- *Logical Interface Category 13: Interface between systems that use the AMI network*
- *Logical Interface Category 14: Interface between systems that use the AMI network for functions that require high availability*
- *Logical Interface Category 15: Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs*
- *Logical Interface Category 16: Interface between external systems and the customer site*
- *Logical Interface Category 17: Interface between systems and mobile field crew laptops/equipment*

- *Logical Interface Category 18: Interface between metering equipment*
- *Logical Interface Category 19: Interface between operations decision support systems*
- *Logical Interface Category 20: Interface between engineering/ maintenance systems and control equipment*
- *Logical Interface Category 21: Interface between control systems and their vendors for standard maintenance and service*
- *Logical Interface Category 22: Interface between security/network/system management consoles and all networks and systems*

6.2 Beschreibung der Sicherheitsanforderungen und Massnahmen

Die Sicherheitsanforderungen der NISTIR 7628-Reihe lassen sich in eine der folgenden drei Gruppen einteilen:

- Steuerungs-, Risiko- und Konformitätsanforderungen;
- allgemein technische Anforderungen;
- und eindeutige technische Anforderungen.

Die allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen sind organisatorische Anforderungen und werden für alle Smart Grid Informationssysteme innerhalb eines Unternehmens angewendet. Sie werden typischerweise auf der Informationsebene implementiert und bei Bedarf erweitert. Die allgemeinen technischen Anforderungen werden auf alle Informationssysteme in einer Organisation im Smart Grid angewandt. Die eindeutigen technischen Anforderungen werden den logischen Interface Kategorien zugeordnet. Durch die Einteilung in die LI Kategorien wurden diese festgelegt. Die allgemeinen und die technischen Anforderungen sollen den Smart Grid Systemen und nicht unbedingt jeder einzelnen Komponente zugeordnet werden. Dies liegt daran, dass Sicherheit auf Systemebene und nicht speziell der Datenaustausch zweier Komponenten betrachtet wird. Zusätzlich sind die Anforderungen auch in Familien aufgeteilt. So gibt es beispielsweise eine Familie mit dem Bezeichner „Zugangskontrolle“ *(Access Control).* Die beinhaltet alle Anforderungen aus allen drei (Anforderungs-)Gruppen, die sich mit den Zugangskontrollen befassen.

Zugangskontrolle (AC): Der Fokus der Zugangskontrollen liegt darauf sicherzustellen, dass Personen, die Zugang zu den Ressourcen haben sollen, diesen auch bekommen. Diese Personen müssen korrekt identifiziert werden, ferner müssen die Zugangsaktivitäten überwacht werden.

SG.AC-1 Richtlinien und Vorgehensweisen für Zugangskontrollen

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen.

- Es wird eine selbstdefinierte Häufigkeit für die Entwicklung, Implementierung, Überprüfung und Aktualisierung festgelegt.
- Ziele, Rollen und Verantwortlichkeiten, Umfang der Zugangskontrollen werden festgelegt
- Eine enge Bindung an, sowie die Zustimmung des Managements sichert eine bessere Einhaltung der Anforderungen

- Es wird sichergestellt, dass die Vorgehensweise der Zugangskontrolle den aktuellen Vorschriften entspricht.

SG.AC-2 Richtlinien und Vorgehensweisen für Zugangskontrollen zu Remote-Zugriffe

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Der Remote Zugang ist jeder Zugang zu einem Smart Grid Informationssystem, der durch einen User oder Prozess über ein externes Netzwerk, welches nicht selbst kontrolliert wird, erfolgt.

- Die erlaubten Methoden für den Remote-Zugriff werden dokumentiert.
- Es werden Einschränkungen, sowie Implementierungsvorgaben für jede erlaubte Remote-Zugangsmethode festgelegt.
- Vor der Verbindung wird das Smart Grid Informationssystem autorisiert.

SG.AC-3 Account Management

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Die Accounts für Smart Grid Informationssysteme werden verwaltet. Dazu gehören Autorisierung, Einrichtung, Aktivierung, Modifizierung, Sperrung und die Löschung von Accounts.

- Spezifikation von Account Typen, Zugangsrechten und Privilegien
- Überprüfung von Accounts in regelmässigen Abständen. Es wird die Zustimmung von einer Zuständigen Person benötigt, bevor ein neuer Account eingerichtet werden darf.

SG.AC-4 Durchführung des Zugriffs

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen.

SG.AC-6 Aufteilung der Verantwortlichkeiten

Diese Anforderung gehört zu den allgemeinen technischen Anforderungen.

- Die Aufteilung von Verantwortlichkeiten und die Trennung von Funktionen werden benötigt, um Interessenskonflikte zu eliminieren und damit die Unabhängigkeit der Verantwortlichkeiten und Funktionen von Individuen und Rollen zu gewährleisten.
- Es wird die Aufteilung von Smart Grid Informationssystems Funktionen durch zugeordnete Zugangskontrollen ermöglicht.
- Sicherheitsfunktionen werden nur für einen möglichst kleinen Teil von Benutzern eingeschränkt um die Sicherheit des Informationssystems sicherzustellen. Umsetzungsmöglichkeiten: Sicherheitsmanagement (Daten, Eigenschaften, Funktionen, Rollenmanagement, Aufteilung der Pflichten)
- Rollenbasierte Zugriffskontrolle
- Training

SG.AC-7 Minimum an Privilegien

Diese Anforderung gehört zu den allgemeinen technischen Anforderungen.

Die Benutzer bekommen nur das Minimum an Rechten und Zugängen, die er benötigt. Umsetzungsmöglichkeiten hierfür sind:

- Sicherheitsmanagement (Daten, Eigenschaften, Funktionen, Rollenmanagement, Aufteilung der Pflichten)
- Sichere Domänen und Netzwerksegmentierung
- Rollenbasierte Zugriffskontrolle
- Training

SG.AC-8 Erfolglose Login-Versuche

Dies ist eine allgemeine technische Anforderung.

Für aufeinanderfolgende erfolglose Login-Versuche in einer bestimmten Zeiteinheit wird ein Limit festgelegt. Wenn die maximale Anzahl der Versuche ausgeführt ist, wird der Account automatisch gesperrt bis er von einem Administrator wieder freigeschaltet wird. Falls der Account nicht gesperrt werden kann, weil dieser unbedingt immer zugängig sein muss, trifft das System alternative Massnahmen.

Umsetzungsmöglichkeiten:

- Kenntnisnahme von Authentifizierungsfehlern.
- Anmeldungsbanner, oder Nachricht
- Aussperrung durch fehlgeschlagene Login Versuche

SG.AC-9 Smart Grid Informationssystem - Mitteilungen zur Systemnutzung

Dies ist eine allgemeine technische Anforderung. Bevor der Zugang zu einem Informationssystem gewährt wird, wird eine Mitteilung angezeigt, die Privatsphären- oder Sicherheitshinweise enthält.

Umsetzungsmöglichkeiten:

- Zugangshistorie
- Banner oder Nachricht zum Einloggen

SG.AC-11 Konkurrierende Sitzungen

Dies ist eine eindeutige technische Anforderung. Die Anzahl von konkurrierenden Sitzungen wird für jeden Nutzer eingeschränkt. Eine solche Einschränkung kann global, nach Account Typen, nach Accounts oder einer Kombination aus diesen erfolgen. Die Einschränkung bezieht sich auf konkurrierende Sitzungen eines Informationssystems und nicht auf konkurrierende Sitzungen eines Benutzers auf verschiedene Informationssysteme.

SG.AC-12 Gesperrte Sitzungen

Dies ist eine eindeutige technische Anforderung. Die Sicherheitsanforderung SC.AC-12 beschreibt „die Sperrung einer Sitzung“. Nach einer festgelegten Zeitperiode, in der keine Aktivitäten stattfinden, wird die Sitzung gesperrt. Diese Sperrung bleibt bestehen, bis diese durch den dazugehörigen Identifikations- und Authentifikationsprozess aufgehoben wird. Eine Sperrung einer Sitzung substituiert kein Lock Out.

SG.AC-13 Sperrung von Entfernten Sitzungen

Dies ist eine eindeutige technische Anforderung. Die Sicherheitsanforderung SC.AC-13 beschreibt „die Sperrung einer Sitzung“. Nach einer festgelegten Zeitperiode in der keine Aktivitäten stattfinden wird die Sitzung gesperrt. Diese Sperrung bleibt bestehen, bis diese durch

den dazugehörigen identifikations- und Authentifikationsprozess aufgehoben wird. Eine Sperrung einer Sitzung substituiert kein Lock Out.

SG.AC-14 Zulässige Handlungen ohne Identifikation und Authentifikation

Dies ist eine eindeutige technische Anforderung. Es werden spezifische Handlungen identifiziert, die auf dem Informationssystem ohne Identifikation oder Authentifikation ausgeführt werden dürfen. Zusätzlich können auch Handlungen identifiziert werden, die normalerweise eine Identifikation und Authentifikation benötigen, aber unter bestimmten Umständen, wie zum Beispiel Notfällen, umgangen werden dürfen.

SG.AC-15 Remote Access

Dies ist eine eindeutige technische Anforderung. Es werden alle Methoden des Fernzugriffs auf Smart Grid Informationssysteme autorisiert, überprüft und geregelt. Dabei ist ein Fernzugriff jeder Zugriff auf ein Informationssystem durch einen Benutzer (oder durch einen Prozess, der für einen Benutzer agiert), der über ein externes Netzwerk kommuniziert (z. B. Internet).

- Fernzugriffe auf Smart Grid Informationssysteme werden nur dann und nur für den benötigten Zeitraum zugelassen, wenn diese nötig, genehmigt und authentifiziert sind.
- Es werden automatisierte Mechanismen für die Unterstützung der Überwachung und die Kontrolle von Fernzugriffen genutzt.
- Der Fernzugriff muss authentifiziert werden. Ausserdem werden mit Hilfe von Kryptographie die Vertraulichkeit sowie die Integrität geschützt.
- Die Fernzugänge werden durch eine limitierte Anzahl von Zugangskontrollpunkten geleitet.
- Drahtloser Zugang wird, wenn er nicht unbedingt benötigt wird, deaktiviert.
- Drahtloser Zugang zum Informationssystem wird durch Authentifizierung und Verschlüsslung geschützt. Dabei authentifiziert sich der Nutzer, das Gerät oder falls nötig auch beide.
- Es wird auf unautorisierte Fernzugängen zum Informationssystem überprüft, Dies beinhaltet das Scannen nach unautorisierten Wireless Access Points in einer vordefinierten Häufigkeit sowie angemessene Massnahmen falls eine solche Verbindung gefunden wird.

SG.AC-16 Einschränkungen des drahtlosen Zugangs

Dies ist eine allgemeine technische Anforderung.

Es werden Nutzungseinschränkungen, sowie Implementierungsvorgaben für die WLAN Technologien festgelegt. Der drahtlose Zugang zum Informationssystem muss autorisiert, überwacht und verwaltet werden. Es wird Authentifizierung und Verschlüsselung zur Absicherung genutzt. In einem festgelegten Abstand wird auf unautorisierte Zugange überprüft und erforderliche Massnahmen werden getroffen.

Umsetzungsmöglichkeiten:

- Limitierung des Umfangs der auswählbaren Attribute
- Limitierung von konkurrierenden Sitzungen
- Systemzugangsbanner
- Systemzugangshistory
- Limitierung der Netzwerkzugangs
- Tunnel zur sicheren Kommunikation
- Authentifizierung

SG.AC-17 Zugangskontrollen für mobile Geräte

Dies ist eine allgemeine technische Anforderung.

Es werden Nutzungseinschränkungen, sowie Implementierungsvorgaben für mobile Geräte vorgegeben. Verbindungen von mobilen Geräten zu Smart Grid Informationssystemen müssen autorisiert werden. Es wird auf unerlaubte Verbindungen überwacht.

Umsetzungsmöglichkeiten:

- Limitierung des Umfangs der auswählbaren Attribute
- Limitierung von konkurrierenden Sitzungen
- Systemzugangsbanner
- Systemzugangshistory
- Limitierung des Netzwerkzugangs
- Tunnel zur sicheren Kommunikation
- Authentifizierung

SG.AC-18 Die Nutzung von externen Informationssystemen

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Externe Informationssysteme sind Informationssysteme, oder Komponenten von diesen, die ausserhalb der autorisierten Grenzen liegen. Bei diesen hat das Unternehmen keine Kontrolle über die Anwendung von Sicherheitsanforderung, oder der Bewertung dieser. Es werden die Einschränkungen und Konditionen für autorisierte Individuen festgelegt, um von einem externen Informationssystem Zugang zum Smart Grid Informationssystem zu bekommen. Es werden die Bedingungen für autorisierte Individuen festgelegt, um von einem externen Informationssystem die Verarbeitung, Speicherung und Übertragung von Informationen zu ermöglichen. Ausser in Ausnahmefällen wird der Zugang von externen Informationssystemen auf das Smart Grid Informationssystem, um Daten zu verarbeiten, speichern, oder zu übertragen, verboten. Ausnahmen können gewährleistet werden, wenn die Implementierung der geforderten Sicherheitsanforderungen des Unternehmens verifiziert werden kann oder wenn besondere Genehmigungen vorliegen.

SG.AC-19 Einschränkungen beim Zugang zu Kontrollsystemen

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Es werden Mechanismen im Design und in der Implementierung eines Smart Grid Informationssystems umgesetzt, um den Zugang zu diesem vom unternehmenseigenen Netzwerk einzuschränken, z. B. Read-only Zugänge.

SG.AC-20 Öffentlich erreichbare Daten

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen.

Informationen, die unter den Datenschutz fallen oder Informationen von Lieferanten sind Beispiele für nichtöffentliche Informationen. Die Anforderung betrifft Beiträge auf einem Informationssystem, das ohne Identifikation oder Authentifikation zugängig ist. Es werden Individuen festgelegt die öffentliche Informationen auf einen Informationssystem posten, das öffentlich zugängig ist. Autorisierte Personen werden trainiert, um sicherzustellen, dass öffentlich zugängliche Informationen keine nichtöffentlichen Informationen enthalten. Überprüfung des vorgestellten Inhalts der öffentlich zugänglichen Daten bevor diese auf das öffentliche Informationssystem gestellt werden. In einem definierten Abstand wird der Inhalt auf dem öffentlich

zugänglichen Informationssystem auf nichtöffentliche Informationen überprüft. Falls notwendig werden nichtöffentliche Informationen vom öffentlichen Informationssystem gelöscht.

SG.AC-21 Passwörter

Dies ist eine allgemeine technische Anforderung.

Es werden Verfahren für die Erzeugung und Nutzung von Passwörtern entwickelt Diese Vorgaben legen, basierend auf den Sicherheitslevels, Regeln für die Komplexität der Passwörter für den Zugang zum Smart Grid Informationssystem fest. Passwörter müssen regelmässig geändert werden. Ausserdem werden diese nach einer festgelegten Zeit, in der sie nicht genutzt werden, wiederrufen.

Umsetzungsmöglichkeiten:
- Authentifizierung
- Identifizierung
- Erzwingung von Passwörtern mit einer vorgegebenen Komplexität
- Salted Hashes
- Passwort cracking Tests

Prüfung und Verantwortlichkeit (AU): Überprüfungen des Smart Grid Informationssystems, sowie Aufzeichnungen über diese, müssen regelmässig ausgeführt werden. Dies passiert um sicherzustellen, dass die Sicherheitsmechanismen, die während der Tests vorhanden waren, auch noch immer installiert sind und dass sie ordnungsgemäss arbeiten. Bei dieser Sicherheitsüberprüfung werden Aufzeichnungen und Aktivitäten überprüft um die festgelegten Sicherheitsvorgaben zu gewährleisten. Durch die Aufzeichnungen werden die Überprüfungen auch zum Aufspüren von Verletzungen der Sicherheitsanforderungen genutzt. Dabei sind die Aufzeichnungen für die Aufspürung von Anomalien, sowie für forensische Analysen notwendig.

SG.AU-1 Vorgaben und Prozeduren für die Prüfung und Verantwortlichkeit

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Die folgenden Prozeduren werden in einer vom Unternehmen festgelegten Häufigkeit entwickelt, umgesetzt, überprüft und aktualisiert. Diese Anforderungen können innerhalb der generellen Sicherheitsvorgaben umgesetzt werden.

- Eine dokumentierte Überprüfungs- und Verantwortlichkeitsstrategie der Schutzziele, Rollen und Verantwortlichkeiten für das Sicherheitsprogramm und des Umfangs der Prüfungen und der Verantwortlichkeiten.
- Verpflichtungen des Managements stellen die Konformität mit den Sicherheitsvorgaben des Unternehmens, sowie anderen regulatorischen Anforderungen sicher.
- Es muss sichergestellt werden, dass diese Vorgaben auch den Regulatorien, wie Gesetzen usw. entspricht.

SG.AU-2 Überprüfbare Ereignisse

Dies ist eine allgemeine technische Anforderung. Das Ziel dieser Anforderung ist es die Ereignisse zu identifizieren, die signifikant und relevant sind. Auf Grundlage von Risikoabschätzungen wird regelmässig eine Liste mit überprüfbaren Ereignissen erstellt. In der Liste mit den Ereignissen werden auch bevorzugte Funktionen aufgeführt. Die Liste wird auf Grundlage aktueller Bedrohungen und Risikoabschätzungen regelmässig überarbeitet.

Umsetzungsmöglichkeiten:

- Standard Eventlogging
- Protokollierung des Management Programms
- Skalierbare Log Filter
- Zentralisierte Protokollierung an ein Security oder Network Operation Center
- Rund um die Uhr Echtzeit Prüfung und automatische Eventbenachrichtigung.

SG.AU-3 Inhalt von Prüfungsprotokollen

Dies ist eine allgemeine technische Anforderung. Das Informationssystem erzeugt Prüfungsprotokolle. Diese Protokolle enthalten:

- Datum und Zeitpunkt des Ereignisses
- Die Komponente, wo das Ereignis aufgetreten ist
- Typ des Ereignisses
- Nutzeridentität
- Resultat des Ereignisses

Ausserdem muss es die Möglichkeit geben, weitere detailliertere Informationen aufzuzeichnen.
Umsetzungsmöglichkeiten:

- Standard Eventlogging
- Sicherheitsprüfungseventauswahl
- Sicherheitsprüfung, Review und Analyse
- Aufzeichnungsmanagementprogramm
- Skalierbare Log Filter
- Zentralisierte Protokollierung an ein Security oder Network Operation Center
- Rund um die Uhr Echtzeit Prüfung und automatische Eventbenachrichtigung.

SG.AU-4 Speicherkapazität für Überprüfungen

Dies ist eine allgemeine technische Anforderung. Es werden extra Prüfungsprotokoll-Speicherkapazitäten definiert und es wird überprüft, ob diese noch ausreichend ist um zu verhindern, dass die Kapazitäten überschritten werden.

Umsetzungsmöglichkeiten:

- Standards und Anforderungen für die Aufbewahrung der Aufzeichnungen
- Regelmässige Archivierung und Management der Aufzeichnungen
- Zentralisierte Aufzeichnungen in einem Unternehmensaufzeichnungsmanagementsystem
- Befähigung zu automatischen Systemarchivierungschecks für Festplattenplatz.
- Aufzeichnungsmanagementprogramm

SG.AU-5 Reaktion auf Fehler bei der Prüfung

Dies ist eine allgemeine Steuerungs-, Risiko- und Konformitätsanforderung. Fehler bei der Prüfung beinhalten Software/Hardware Fehler, Fehler bei den Prüfungseinleitungsmechanismen und wenn Speicherkapazitäten erreicht oder überschritten werden. Das Informationssystem alarmiert die vorgesehenen Funktionäre über Fehler bei der Prüfung. Das Informationssystem führt eine vordefinierte Menge an Handlungen aus (z. B. Runterfahren des Informationssystems, Überschreibung des ältesten Protokolls, Stoppen der Erzeugung neuer Prüfungsprotokolle).

SG.AU-6 Überwachen, Analysieren und Berichten

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen.

Überprüfung und Analyse von Smart Grid Informationssystemen, sowie Überprüfung von Aufzeichnungen auf Anzeichen von unangemessenen oder ungewöhnlichen Aktivitäten in einer festgelegten Häufigkeit. Solche Funde werden an die zuständigen Personen berichtet. Wenn eine Änderung des Risikolevels für den Unternehmensbetrieb stattfindet, dann werden die Überprüfungslevels, sowie Analysen und die Berichte angepasst.

SG.AU-7 Reduzierung der Überwachung und der Berichtserzeugung

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Es wird eine Möglichkeit zur Reduzierung der Überwachung und der Berichtserzeugung bereitgestellt. Dies unterstützt die Realzeitanalyse und eine schnelle Untersuchung nach Sicherheitsvorfällen.

SG.AU-8 Zeitstempel

Die Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Es werden interne Systemuhren verwendet, um Zeitstempel für die Berichte der Überwachung zu erzeugen. Solche Zeitstempel vom Informationssystem enthalten sowohl das Datum als auch die Zeit. Das Informationssystem synchronisiert interne Systemuhren regelmässig in vorgegebenen Abständen.

SG.AU-9 Schutz von Überprüfungsinformationen

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen.

Das Informationssystem sichert aufgezeichnete Informationen und Werkzeuge für diese vor unautorisiertem Zugang, Modifizierung und Löschung. Zu den aufgezeichneten Informationen gehören unter anderem aufgezeichnete Überwachungen, Einstellungen und Berichte. Eine Möglichkeit zur Umsetzung ist die Aufzeichnung auf nur einmal beschreibbarer Hardware.
SG.AU-10 Aufbewahrung von Aufzeichnungen

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Aufzeichnungen werden für eine vordefinierte Zeit aufbewahrt, um Untersuchungen zu Sicherheitsunfällen zu unterstützen und regulatorische Informationsaufbewahrungsanforderungen zu erfüllen.

SG.AU-11 Durchführung und Häufigkeit von Audits

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Die Häufigkeit, in der Kontrollen durchgeführt werden, ist vom Unternehmen festgelegt, um die spezifizierten Sicherheitsanforderungen, sowie die entsprechenden Gesetzte und Regulatorien zu erfüllen. Kontrollen können entweder interne Selbstkontrollen, oder unabhängige Überprüfungen durch Dritte sein.

SG.AU-12 Qualifikation des Prüfers

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Das Kontrollprogramm des Unternehmens spezifiziert die Qualifikationen des Prüfers. Sicherheitsprüfer müssen das Smart Grid Informationssystem und die dazugehörigen Betriebspraktiken verstehen; die Risiken, die mit der Kontrolle zusammenhängen, verstehen und

die unternehmenseigene Sicherheitsrichtlinien, sowie Richtlinien für Smart Grid Informationssysteme und Verfahren verstehen. Der Prüfer und der Systemadministrator sollen verschiedene Personen sein.

SG.AU-13 Prüfungsprogramm

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Es werden Regeln und Bedingungen für die Nutzung der Prüfungsprogramme spezifiziert. Der Zugang zu den Prüfungsprogrammen muss geschützt werden, um jede Möglichkeit des Missbrauchs oder der Kompromittierung zu verhindern.

SG.AU-14 Einhaltung der Sicherheitsrichtlinien

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Die Einhaltung der Sicherheitsrichtlinien wird im Rahmen des Prüfungsprogramms des Unternehmens sichergestellt. Bei den regelmässig durchgeführten Prüfungen wird:

- Geprüft, ob die definierten Sicherheitsrichtlinien und die Verfahren, inklusive derer die Sicherheitsvorfälle feststellen, implementiert und befolgt werden.
- Die Einhaltung der Unternehmensstrategien dokumentiert und sichergestellt.
- Sicherheitsbedenken identifiziert. Es wird bestätigt dass das Informationssystem frei von Sicherheitsgefährdungen ist oder es werden erweiterte Informationen über Gefährdungen bereitgestellt, falls diese auftreten.
- Die Zuverlässigkeit und die Verfügbarkeit des Informationssystems sichergestellt, um einen sicheren Betrieb zu ermöglichen.
- Kontinuierlich die Leistung verbessert.

SG.AU-15 Initiierung der Prüfung

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Es wird eine Möglichkeit bereitgestellt, die die Aufzeichnung für Kontrollen ermöglicht. Ausserdem werden, für eine vorgegebene Liste von Ereignissen, Aufzeichnungen erstellt.

Autorisierte Nutzer können Ereignisse auswählen, die aufgezeichnet werden sollen. Solche Aufzeichnungen können von verschiedenen Komponenten im Smart Grid Informationssystem erzeugt werden.

SG.AU-16 Nichtabstreitbarkeit

Dies ist eine eindeutige technische Anforderung. Das Informationssystem soll dagegen geschützt sein, dass Individuen abstreiten bestimmte Handlungen ausgeführt zu haben. Nichtabstreitbarkeit schützt Individuen gegen spätere Ansprüche:

- Ein Autor hat ein bestimmtes Dokument nicht verfasst.
- Ein Sender hat eine bestimmte Nachricht nicht gesendet.
- Ein Empfänger hat eine bestimmte Nachricht nicht empfangen.
- Ein Unterzeichner hat ein bestimmtes Dokument nicht signiert.

Nichtabstreitbarkeitstechniken sind z. B. digitale Signaturen, digitale Nachrichten, Quittungen und Logging.

Identifikation und Authentifikation (IA): Die Identifikation und Authentifikation ist der Prozess der Verifizierung eines Nutzers, eines Prozesses oder eines Gerätes, um Zugriff auf eine Ressource im Smart Grid Informationssystem zu bekommen.

SG.IA-1 Identifikations- und Authentifikationsrichtlinien und Vorgehen

Die Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Das Unternehmen entwickelt, implementiert, überprüft und aktualisiert in einer vom Unternehmen vorgegebenen Häufigkeit ein dokumentiertes Identifikations- und Authentifikationsvorgehen das Folgendes vorgibt:

- Die Ziele, Funktionen, und Verantwortlichkeiten für das Identifikations- und Authentifikationssicherheitsprogramm.
- Der Umfang des Identifikations- und Authentifikationssicherheitsprogramms und wie es von Mitarbeitern, weiteren Unternehmen und third partys angewendet wird.
- Vorgehen zur Implementierung der Identifikations- und Authentifikationsvorgehen, sowie die zugehörigen Anforderungen für die Absicherung der Identifikation und Authentifikation.

Die Unterstützung vom Management stellt die Vereinbarkeit mit dem allgemeinen Sicherheitsvorgehen und anderen regulatorischen Anforderungen sicher. Das Unternehmen stellt sicher, dass die Vorgehen den Gesetzten und Regulatorien entsprechen. Das Identifikations- und Authentifikationsvorgehen kann als Teil des allgemeinen Sicherheitsvorgehens des Unternehmens umgesetzt werden. Dabei können Identifikations- und Authentifikationsverfahren für das allgemeine Sicherheitsvorgehen aber auch, falls benötigt, für spezielle Systeme entwickelt werden.

SG.IA-2 Identifizierungsmanagement

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Das Unternehmen bekommt die Autorisierung von einer Management Authority, um den Identifikator eines Nutzers oder eines Gerätes zuzuweisen. Das Unternehmen archiviert vorherige Nutzer- oder Geräteidentifikatoren. Es wird ein Identifikator gewählt, der eindeutig ein Individuum oder ein Gerät identifiziert.

SG.IA-3 Authentifizierungsmanagement

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Authentifizierungsdaten der Nutzer und Geräte werden verwaltet, indem

- Der Inhalt der Authentifizierungsdaten festgelegt wird, z.B. Festlegung der Token, Passwortlänge und Aufbau. Verfahren für die initiale Authentifizierung, für den Verlust, für kompromittierte oder beschädigte Zugangsdaten, sowie für die Entziehung von Zugangsdaten festgelegt werden.
- Zugangsdaten in einer vorgegebenen Frequenz erneuert werden.
- Massnahmen spezifiziert werden, um Authentifizierungsdaten zu schützen.

Dazu gehören der Besitz von individuellen Zugangsdaten und keine geteilten. Ausserdem müssen kompromittierte und verlorene Daten umgehend gemeldet werden. Es werden Programme angewendet, die feststellen ob die Passwörter ausreichend resistent gegen Attacken sind.

SG.IA-4 Nutzer Identifikation und Authentifikation

Dies ist eine eindeutige technische Anforderung. Die Sicherheitsanforderung SG.IA-04 beschreibt die „Identifizierung und Authentifizierung des Anwenders“. Dabei sollen Anwender, oder Prozesse die im Namen von Anwendern agieren, eindeutig identifiziert werden. Es werden Multifaktorauthentifizierungsmethoden für Fernzugriffe, sowie für lokale Zugriffe auf nicht vertrauliche, sowie auf vertrauliche Accounts verwendet. Auch bei Gruppenauthentifizierungen

müssen die Teilnehmer dieser Gruppe einzeln authentifiziert werden. Multifaktorauthentifizierungsmethoden werden für den Zugang zu Netzwerken verwendet und sollen resistent gegen Replay Attacken sein. Einer der Faktoren für die Multifaktorauthentifizierung soll von einem separaten System bereitgestellt werden. Für die Umsetzung dieser Anforderungen werden ein Passwort und ein Token verwendet. Dabei sollen die Passwörter mindestens zwölf Zeichen lang sein. Darüber hinaus sollen sie aus Gross- und Kleinbuchstaben sowie Sonderzeichen und Ziffern (?!%+…) bestehen und regelmässig geändert werden. Für das Sicherheitslevel M= Medium ist eine standartmässige Identifizierung und Authentifizierung mit dem SASL (Simple Authentication and Security Layer, RFC 4422) Framework mittels Passwort und TLS Verschlüsselung ausreichend.

SG.IA-5 Identifikation und Authentifikation von Geräten

Dies ist eine eindeutige technische Anforderung. Die Anforderung SG.IA-05 beschreibt die „Geräteidentifikation und Authentifikation“. Für eine festgelegte Liste von Geräten wird eine Verbindung dann zugelassen, wenn zuvor diese Geräte eindeutig identifiziert und authentifiziert wurden. In dieser Kategorie wird dabei zwischen zwei Sicherheitsleveln unterschieden. Für das Sicherheitslevel M= Medium ist eine standartmässige Identifizierung und Authentifizierung mit dem SASL (Simple Authentication and Security Layer, RFC 4422) Framework mittels Passwort und TLS Verschlüsselung ausreichend. Für das Sicherheitslevel H= High kann die Identifikation und Authentifikation wie im 61850-8-2 beschrieben durchgeführt werden. Dort wird beschrieben wie für XMPP eine Ende-zu-Ende Verschlüsselung mit Hilfe des 62351-4 ed.2 erstellt wird. Für die Authentifizierung werden X.509 Zertifikate verwendet.

SG.IA-6 Authentifikator Feedback

Dies ist eine eindeutige technische Anforderung Diese Anforderung hat das Sicherheitslevel L=Low. Der Authentifizierungsmechanismus verschleiert Authentifizierungsinformationen während der Authentifizierung, um diese Informationen vor einer möglichen Ausnutzung von unautorisierten Personen zu schützen. Ein Beispiel zur Umsetzung sind Sternchen bei der Passwort Eingabe, damit dieses keiner mitlesen kann. Zusätzlich kann auch die Länge des Passworts verschleiert werden.

Absicherung der Smart Grid Informationssysteme und der Kommunikation (SC): Die Absicherung des Informationssystems und der Kommunikation besteht aus Massnahmen, die getroffen werden, um Smart Grid Informationssysteme und die Nachrichtenverbindungen zwischen diesen vor Eindringlingen zu schützen.

SG.SC-1 Absicherung der Smart Grid Informationssysteme und der Kommunikation, Strategien und Vorgehen

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. In einer vorgegebenen Häufigkeit entwickelt, implementiert, überprüft und aktualisiert das Unternehmen eine dokumentierte Strategie für die Absicherung der Informationssysteme und deren Kommunikation, die Schutzziele, Rollen und Verantwortlichkeiten für das Sicherheitsprogramm, den Umfang der Strategien, das Vorgehen für die Umsetzung der Strategien und Anforderungen.

Verpflichtungen des Managements stellen die Konformität mit den Sicherheitsvorgaben des Unternehmens, sowie anderen regulatorischen Anforderungen sicher. Es muss sichergestellt werden, dass diese Vorgaben auch den Regulatorien, wie Gesetzen usw. entspricht. Diese Strategien können ein Teil der generellen Sicherheitsstrategien sein, oder, falls nötig, für spezielle Informationssysteme entwickelt werden.

SG.SC-3 Isolierung der Sicherheitsfunktionen

Dies ist eine eindeutige technische Anforderung. Die Sicherheitsanforderung SG.SC-03 beschreibt die „Isolierung der Sicherheitsfunktionen“. Dafür werden Sicherheitsfunktionen von nicht-Sicherheitsfunktionen isoliert. Das Kontrollsystem soll Sicherheitsfunktionen (z.B. Funktionen, die Zugriffe oder Informationsflüsse steuern) durch eine Isolationsgrenze von Funktionen ohne Sicherheitsaspekt trennen. So werden der Zugang zu den Sicherheitsfunktionen sowie die Integrität der Hardware, Software und Firmware, welche die Sicherheitsfunktionen ausführen, geschützt. Es gibt die Sicherheitslevel M= Medium und H= High.

Für die Umsetzung können Sicherheitsfunktionen als grosse unabhängige Module implementiert werden, die unnötige Interaktionen zu anderen Modulen vermeiden. Um eine Isolierung von Sicherheitsfunktionen von nicht Sicherheitsfunktionen zu ermöglichen, können Hardware Separierungsmechanismen, z.B. Isolierungsgrenzen via Partitionierung und Domänen, eingesetzt werden. Dies beinhaltet auch Sicherheitsfunktionen für die Durchführung von Zugangs- und Datenflusskontrollen und zur Absicherung der Integrität. Eine Separation der Hardware beinhaltet zum Beispiel Hardware Ring Architekturen, die im Allgemeinen durch Mikroprozessoren implementiert werden oder durch die Hardware durchgeführte Adresssegmentierung, um logisch getrennte Speicherbereiche mit unterschiedlichen Eigenschaften zu nutzen. Auch für die ausgeführten Prozesse kann eine separate Ausführungsdomäne, wie z.B. ein Adressbereich, genutzt werden.

SG.SC-4 Datenüberreste

Dies ist eine eindeutige technische Anforderung. Das Informationssystem verhindert unautorisierte oder ungewollte Datenübertragungen über geteilte Ressourcen. Bei einer geteilten Ressource wird verhindert, dass Daten für andere Nutzer, Rollen oder Prozesse verfügbar sind, nachdem diese wieder freigegeben ist.

SG.SC-5 Denial-of-Service Absicherung

Dies ist eine eindeutige technische Anforderung. Die Effekte von Denial of Service Attacken sollen begrenzt bzw. gemildert werden. In dieser Architektur gibt es die Sicherheitslevel M=Medium und H= High. Für die Umsetzung können Filter eingesetzt werden, die das Netzwerk abgrenzen und bestimmte Pakettypen herausfiltern. Dadurch können bereits einige Angriffe abgefangen bzw. abgeschwächt und die Geräte im Netzwerk geschützt werden. Ausserdem können die Möglichkeiten für Nutzer eingeschränkt werden, (z. B. durch Einschränkungen was verschickt werden kann und welche Grösse es haben darf) Denial of Service Angriffe gegen Smart Grid Informationssysteme zu starten. Ausserdem regelt das Informationssystem die Kapazität, Bandbreite oder andere Redundanzen, um die Effekte von Denial of Service Angriffen zu limitieren. Als Notfallplan ist zusätzlich eine Cloudbasierte Auslagerung von Dienstleistungen möglich, z. B. eine Amazon Cloud.

SG.SC-6 Priorisierung von Ressourcen

Dies ist eine eindeutige technische Anforderung. Die Sicherheitsfunktion SG.SC-06 beschreibt eine Priorisierung der Nutzung der Ressourcen. Es soll verhindert werden, dass niedriger priorisierte Prozesse die Ausführung von höher priorisierten Prozessen verzögern oder stören. Um dieses zu verhindern wird eine Priorisierung von Systemen, auf die mehrere Systeme gleichzeitig Zugriff haben, durchgeführt. Zusätzlich sollen Quoten verhindern, dass Prozesse mehr als eine festgelegte Grösse der Ressourcen erhalten.

SG.SC-7 Absicherung von Netzwerk-Grenzen

Dies ist eine eindeutige technische Anforderung. Die Sicherheitsfunktion SG.SC-07 beschreibt die „Grenzabsicherung“. Für die Umsetzung werden die Grenzen des Systems definiert. Ausserdem werden alle Kommunikationen an der externen Grenze, sowie an den wichtigen internen Grenzen kontrolliert und überwacht. Verbindungen zu externen Netzwerken bestehen nur

über verwaltete Interfaces, die die Grenzen absichern. Voreingestellt werden alle Verbindungen verweigert und nur in Ausnahmen welche zugelassen. Es wird die Anzahl der Zugänge zum Informationssystem so gering wie möglich gehalten. Bei eingehender Kommunikation wird immer überprüft, ob es sich um eine autorisierte Quelle handelt und ob die Kommunikation auch ein autorisiertes Ziel innerhalb der Grenzen hat. Ein solches Interface muss auch die Sicherheitsmassnahmen der Integrität und der Vertraulichkeit der übertragenden Informationen umsetzten. Die Interfaces nutzen Geräte zur Absicherung wie Proxys, Gateways, Router, Firewalls und verschlüsselte Tunnel. Es werden die Sicherheitslevel H=High und M= Medium in der Sicherheitsarchitektur benötigt.

SG.SC-8 Integrität der Kommunikation

Dies ist eine eindeutige technische Anforderung. Es wird mit Hilfe von kryptographischen Werkzeugen die Integrität von elektronisch übertragenen Daten sichergestellt. Das Informationssystem ist dabei auch für die Integrität bei der Erstellung, Verpackung und den Umwandlungen während der Vorbereitung zur Übertragung zuständig. Die Umsetzung kann wie im 61850-8-2 beschrieben erfolgen. Es wird für XMPP eine Ende-zu-Ende Verschlüsselung mit Hilfe des 62351-4 ed.2 erstellt. Um die Integrität zu gewährleisten, wird das A+ Profil aus der 62351-4 ed.2 verwendet.

SG.SC-9 Vertraulichkeit der Kommunikation

Dies ist eine eindeutige technische Anforderung. Es wird die Vertraulichkeit von übertragenden Daten geschützt. Um eine unautorisierte Offenlegung von Daten zu verhindern, werden kryptographische Mechanismen verwendet. Für die Umsetzung wird TLS, wie in RFC 6120 beschrieben, verwendet. Um ein TLS Profil zu erstellen, das TCP basierte Kommunikation absichert, sind die Einstellungen gemäss des 62351-3 ed.2 zu setzen, dies dient als Grundlage. Im 61850-8-2 wird beschrieben wie für XMPP eine Ende-zu-Ende Verschlüsselung mit Hilfe des 62351-4 ed.2 erstellt wird. Um hier zusätzlich die Vertraulichkeit zu gewährleisten, wird das Profil AE+ aus dem IEC 62351-4 ed.2 verwendet.

SG.SC-11 Kryptographische Schlüsselerzeugung und Management

Dies ist eine allgemeine technische Anforderung. Das Unternehmen erzeugt und verwaltet kryptographische Schlüssel, die innerhalb des Informationssystems benötigt werden. Zur Schlüsselerzeugung gehören ein Schlüsselerzeugungsprozess mit einem spezifischem Algorithmus und Schlüsselgrössen, basierend auf den angewendeten Standards. Für die Schlüsselerzeugung wird ein geeigneter Zufallsgenerator verwendet. Die Strategien für die Schlüsselverwaltung beinhalten periodischen Schlüsselaustausch, Schlüsselvernichtung und die Schlüsselverteilung. Für den Fall, dass ein Nutzer einen kryptographischen Schlüssel verliert, muss die Verfügbarkeit der Daten sichergestellt sein.

SG.SC-12 Nutzung von validierter Kryptographie

Dies ist eine allgemeine technische Anforderung. Alle kryptographischen und anderen Sicherheitsfunktionen (wie Hashes, Zufallsgeneratoren usw.) müssen anerkannt und erprobt sein. Eine Liste der im NIST empfohlenen Kryptographie ist im NISTIR 7628 im Kapitel 4 zu finden.

SG.SC-13 Collaborative Computing

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Das Unternehmen entwickelt, aktualisiert und überprüft regelmässig das Vorgehen für Collaborative Computing. Dazu gehören Möglichkeiten für Video und Audiokonferenzen oder

auch Instant Messaging Technologien. Dabei werden dem Nutzer explizite Hinweise gegeben, wenn die Kamera oder das Mikrofon aktiviert sind.

SG.SC-15 Zertifikate für eine Public Key Infrastruktur

Dies ist eine allgemeine technische Anforderung. Für Smart Grid Informationssysteme, die eine Public Key Infrastruktur nutzen, werden unter Anwendung angemessener Richtlinien Public Key Zertifikate ausgegeben. Alternativ können die Zertifikate auch von einem anerkannten Dienstleister bereitgestellt werden. Um ein Public Key Zertifikat zu erhalten wird die Autorisierung eines Zuständigen benötigt. Ausserdem muss ein Verfahren die Identität des Zertifikatsbesitzers eindeutig feststellen um sicherzustellen, dass das Zertifikat an die richtige Person ausgegeben wird. Für die Umsetzung wird eine kryptographische, sowie eine Key Management Unterstützung benötigt. Ausserdem werden sichere Vorgaben zur Austeilung der Zertifikate, die mit angemessenen Strategien auch die Autorisierungsstrategien erfüllen, benötigt.

SG.SC-16 Mobile Code

Dies ist eine allgemeine technische Anforderung. Mobile Code Technologien beinhalten unter anderem Java, JavaScript, ActiveX, PDF, Postscript, Shockwave Movies und Flash Animations. Für Mobile Code gibt es Implementierungsvorgaben und Einschränkungen, basierend auf potentiellen Schäden, die durch eine bösartige Nutzung entstehen können. Die Nutzung von Mobile Code wird dokumentiert, überwacht und verwaltet. Eine zuständige Person muss die Nutzung von Mobile Code autorisieren. Es werden Überprüfungsmechanismen umgesetzt, die unautorisierten Mobile Code identifizieren und angemessene Massnahmen ergreifen.

Für die Umsetzung wird benötigt:

- Prüfung des Codes
- Signierung des Codes und Verifikation für alle Mobile Codes
- Technologien um mobile Code zu finden
- Programme für die Software-Qualitätssicherheit

SG.SC-17 Voice-Over Internet Protocol

Dies ist eine eindeutige technische Anforderung. Für die Nutzung von Voice-Over IP gibt es Implementierungsvorgaben und Einschränkungen, basierend auf potentiellen Schäden die durch eine bösartige Nutzung entstehen können. Die Nutzung muss autorisiert überwacht und kontrolliert werden. NIST Special Publication 800-58 enthält Handlungsempfehlungen für Sicherheitsbetrachtungen von VoIP Technologien.

SG.SC-18 Systemverbindungen/-schnittstellen

Dies ist eine allgemeine technische Anforderung. Alle externen Smart Grid Informationssysteme und Kommunikationsverbindungen werden identifiziert und vor Manipulation und Schäden geschützt. Externe Zugangspunkte zum Smart Grid Informationssystem müssen zum Schutz des Informationssystems abgesichert werden.

Mögliche Technologien für die Umsetzung:

- Identifikation und Autorisierung
- Daten Klassifizierung
- Sichere Domänen- und Netzwerksegementierung
- Erlaubte/ verbotene Dienstleistungen

- Erlaubte/ verbotene Verbindungen

SG.SC-19 Sicherheitsrollen

Dies ist eine allgemeine technische Anforderung. Spezifische Sicherheitsrollen und Verantwortlichkeiten werden für die Nutzer des Smart Grid Informationssystems umgesetzt. Basierend auf der Sensibilität der Daten mit denen der Nutzer arbeitet wird die Rolle definiert, spezifiziert und implementiert. Solche Rollen können für bestimmte Jobs oder aber auch für Individuen festgelegt werden.

Mögliche Technologien für die Umsetzung:
- Sicherheitsmanagement (Daten, Eigenschaften, Funktionen, Rollenmanagement, Aufteilung der Pflichten
- Produkte die beim Treffen und Umsetzen von Entscheidungen helfen
- Rollenbasierte Zugriffskontrolle
- Training

SG.SC-20 Authentizität von Nachrichten

Dies ist eine allgemeine technische Anforderung. Es werden Mechanismen zum Schutz der Authentizität von Gerät-zu-Gerät Kommunikation bereitgestellt. Dazu gehören der Schutz vor veränderten Nachrichten, falsch konfigurierten Geräten und bösartige Entitäten.

Mögliche Technologien für die Umsetzung:
- Nichtabstreitbarkeit des Ursprungs
- Nichtabstreitbarkeit des Empfangs
- Integrität der Nachricht

SG.SC-21 Secure Name/Address Resolution Service

Dies ist eine allgemeine technische Anforderung.

Mögliche Technologie für die Umsetzung: Einschränkung der Transaktionsteilnehmer basierend auf IP Adressen.

SG.SC-22 Zustand nach Fehlern

Dies ist eine allgemeine technische Anforderung. Für definierte Fehler entsteht bei deren Eintritt ein bekannter Zustand. Dadurch kann ein Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit verhindert werden. Zusätzlich kann auch das Unternehmen weiterhin Erforderliches erfüllen.

Mögliche Technologien für die Umsetzung:
- Sicherer Zustand nach Fehler
- Sichere Wiederherstellung auf der Firmware und den Systemebenen
- Softwarequalitätssicherungsprogramm

SG.SC-26 Vertraulichkeit von Daten im Ruhezustand

Dies ist eine eindeutige technische Anforderung. Die Sicherheitsfunktion beschreibt die Vertraulichkeit von Daten, die in dem Moment nicht genutzt werden. Das Informationssystem stellt kryptographische Mechanismen zum Schutz von kritischen Sicherheitsparametern (kryptographische Schlüssel, Passwörter, Sicherheitskonfigurationen,…) bereit. Dabei bezeichnen Daten im Ruhezustand User- oder Systemdaten, die auf Speichern verortet sind. Eine Möglichkeit

diese zu schützen ist beispielsweise eine Verschlüsselung mittels „Advanced Encryption Standard“ (AES).

SG.SC-29 Partitionierung der Anwendungen

Dies ist eine eindeutige technische Anforderung. Funktionalitäten des Nutzers werden von Funktionalitäten des Systemmanagements getrennt. Zu den Funktionalitäten gehören unter anderem Funktionen zum Administrieren der Datenbanken, Netzwerk Komponenten und Server. Typischerweise benötigen diese Funktionen privilegierte Zugangsrechte. Die Separierung kann entweder physisch oder auch logisch erfolgen. Zusätzlich wird sichergestellt, dass es für normale Nutzer keine Möglichkeiten zum Administrieren gibt. Um diese nutzen zu können muss sich ein Nutzer beispielsweise erst mit Administratorrechten anmelden.

SG.SC-30 Partitionierung des Smart Grid Informationssystems

Dies ist eine allgemeine technische Anforderung. Das Informationssystem wird in Komponenten eingeteilt, die in separaten physischen oder logischen Domänen oder Umgebungen liegen.

Möglichkeiten für die Umsetzung:

- Programm zur Datenklassifizierung
- Zugangsverifikation zu und zwischen Prozessen
- Netzwerkbasierende physische Separation, Kennzeichnung
- Rollenbasierte Zugriffskontrolle
- Firewalls
- Betriebssystembasierte Separation der Prozessausführung

Integrität von Smart Grid Informationssystemen und Nachrichten (SI): Durch die Aufrechterhaltung der Integrität von Smart Grid Informationssystemen und Datenintegrität, wird die Sicherheit, dass sensible Daten weder unautorisiert noch unbemerkt modifiziert oder gelöscht werden, erhöht. Die Sicherheitsanforderungen beinhalten Richtlinien und Verfahren für die Identifizierung, Meldung und Korrektur von Mängeln. Ausserdem existieren Anforderung für das ausfindig machen von Schadcode. Es existieren Anforderungen für den Empfang von Sicherheitsalarmen und Vorschläge zur Verifikation von Sicherheitsfunktionen. Die Anforderungen dieser Kategorie finden unautorisierte Änderungen an Software und Daten und schützen gegen diese; schränken den Dateneingang und Ausgang ein; überprüfen die Fehlerfreiheit, Vollständigkeit, Korrektheit von Daten; und handeln im Fehlerfall.

SG.SI-01 Richtlinien und Verfahren für die Integrität von Smart Grid Informationssystemen und Nachrichten

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. In einer vorgegebenen Häufigkeit entwickelt, implementiert, überprüft und aktualisiert das Unternehmen:

- Eine dokumentierte Strategie für die Integrität von Smart Grid Informationssystemen und Nachrichten
- die Schutzziele, Rollen und Verantwortlichkeiten für das Sicherheitsprogramm zur Integrität von Smart Grid Informationssystemen und Nachrichten.
- den Umfang der Strategien
- ein Vorgehen für die Umsetzung der Strategien und Anforderungen

Verpflichtungen des Managements stellen die Konformität mit den Sicherheitsvorgaben des Unternehmens, sowie anderen regulatorischen Anforderungen sicher. Es muss sichergestellt

werden, dass diese Vorgaben auch den Regulatorien, wie Gesetzen usw. entsprechen. Diese Strategien können ein Teil der generellen Sicherheitsstrategien sein, oder, falls nötig, für spezielle Informationssysteme entwickelt werden.

SG.SI-02 Korrektur von Mängeln

Dies ist eine allgemeine technische Anforderung. Es werden Systemmängel identifiziert, berichtet und korrigiert. Es werden Softwareupdates, die zur Korrektur von Mängeln verwendet werden, auf Effektivität und auf potentielle Neben-/ Auswirkungen auf das Informationssystem getestet, bevor es installiert wird. Die Korrektur von Mängeln wird in den internen Managementprozess integriert. Es werden Soft- und Firmware identifiziert, die von bekannt gewordenen Mängeln betroffen sind und mögliche Schwachstellen, die sich daraus ergeben.

SG.SI-03 Schutz vor Schadcode und Spam

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Es werden Mechanismen zum Schutz vor Schadcode implementiert. Diese Mechanismen werden, sobald es neue Versionen gibt, aktualisiert. Es wird verhindert, dass Nutzer diesen Schutz umgehen. Die Mechanismen werden zentral verwaltet. Es werden periodisch Scans auf dem Smart Grid Informationssystem durchgeführt. Diese dürfen aber die Performance nicht mindern. Zusätzlich werden auch Massnahmen zum Schutz gegen Spam an Eintrittspunkten des Systems, Arbeitsplätzen und mobilen Geräten im Netzwerk umgesetzt.

SG.SI-04 Überwachungswerkzeuge und Techniken für Smart Grid Informationssysteme

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Es werden Ereignisse auf dem Informationssystem überwacht, um Angriffe, unautorisierte Aktivitäten und nicht bösartige Fehler zu finden.

Die Möglichkeiten der Überwachung können durch eine Vielzahl von Werkzeugen unterstützt werden. Dazu gehören: Systeme die ein Eindringen entdecken, Systeme die ein Eindringen verhindern, Software gegen Schadcode, protokollierende Überwachungssoftware und forensische Werkzeuge zur Netzwerkanalyse.

Es wird eine Liste mit verantwortlichen Personen festgelegt. Die Informationen aus den Überwachungen werden vor unautorisiertem Zugang, Modifizierung und Löschung geschützt. Die Überwachungswerkzeuge werden in einer festgelegten Zeitperiode ausgeführt und getestet. Es wird ein Realzeitalarm ausgelöst, wenn der Verdacht des Kompromittierens besteht. Es wird verhindert, dass Nutzer die Präventionen umgehen.

SG.SI-05 Sicherheitsalarm und Warnungen

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Es werden Sicherheitsalarme und Warnungen von anderen Einrichtungen empfangen. Es werden interne Sicherheitsalarme und Warnungen erzeugt und verbreitet, falls dieses als notwendig erachtet wird. Es werden Automatismen für die Verbreitung des Sicherheitsalarms und der Warnungen im ganzen Unternehmen angewendet.

SG.SI-06 Verifizierung der Sicherheitsfunktionen

Diese Anforderung gehört zu den allgemeinen Steuerungs-, Risiko- und Konformitätsanforderungen. Der korrekte Betrieb der Sicherheitsfunktionen muss bei jedem Start, Neustart und in einer festgelegten Frequenz regelmässig verifiziert werden. Das System meldet, wenn Anomalien auftreten. Dazu gehört auch die Meldung falls ein automatischer Sicherheitstest fehlschlägt.

SG.SI-07 Integrität von Software und Daten

Dies ist eine eindeutige technische Anforderung. Unautorisierte Änderungen an Software und Daten werden festgestellt. Es werden Techniken für die Verifizierung der Integrität genutzt um Hinweise auf Manipulation von Daten oder Fehler zu finden. Durch regelmässige Integritätsüberprüfungen werden die Integrität der Software und der Daten beurteilt.

SG.SI-08 Validierung der Input-Daten

Dies ist eine allgemeine technische Anforderung. Es werden Werkzeuge angewendet, um Daten auf Genauigkeit, Komplettheit, Echtheit und Authentizität zu überprüfen. Um sicherzustellen, dass die Eingaben dem spezifizierten Format und Inhalt entsprechen, werden diese auf eine gültige Syntax hin überprüft. Beispiele sind Buchstabenmenge und Länge, Numerischer Bereich, sowie akzeptierte Werte.

Umsetzungsmöglichkeiten:

- Absicherung der Nutzerdaten
- Datensicherung von internen Systemen
- Rollenbasierte Zugangskontrolle
- Aufteilung der Aufgaben
- Programm zur Softwarequalitätssicherung
- Nachweisbarkeit
- Authentifizierung
- Integrität des Datentransfers
- Vor dem Weiterverarbeiten eines Inputs von einem Nutzer, einer Datenquelle oder Komponente wird diese auf den Typ, Länge und Umfang hin überprüft.
- Übertragungen werden signiert
- Bevor eine Aktion ausgeführt wird, wird durch Zugangskontrollen überprüft ob der Nutzer dies auch darf

SG.SI-09 Fehlerhandhabung

Dies ist eine allgemeine technische Anforderung. Es werden die Umstände des Fehlers identifiziert. Es werden Fehlernachrichten erzeugt mit Informationen, die für die Fehlerbehebung notwendig sind, aber einem möglichen Gegner keine potentiell schädlichen Informationen preisgeben.

Umsetzungsmöglichkeiten:

- Programm zum Log Management
- Auslieferung von Fehlernachrichten über einen sicheren Kanal
- Softwarequalitätssicherungsprogramm

6.3 Abbildung von NISTIR 7628 Anforderungen auf ENISA Anforderungen der AWK

NISTIR 7628 Recommendations	ENISA Recommendations
SG.ID	SM 1.1.Information Security Policy
SG.AU-1	SM 1.2 Organisation of Information Security
SG.SA-1	SM 1.3 Information Security procedures
SG.RA-2	SM 1.4 Risk management Framework
SG.RA-4	SM 1.5 Risk Assessment
SG.RA-2	SM 1.6 Risk treatment plan
SG.SC-7	SM 10.1 Secure Network Segregation
SG.SC-18	SM 10.2 Secure Network Communications
SG.PS-7	SM 2.1 Third party agreements
SG.SA-2	SM 2.2 Monitoring third party services and validating solutions against predefined acceptance criteria
SG.CA-2	SM 3.1 Security Requirements analysis and specification
SG.ID	SM 3.2 Inventory of smart grid components/Systems
SG.CM	SM 3.3 Secure Configuration Management
SG.MA	SM 3.4 Maintenance of Smart Grid Components
SG.CM	SM 3.5 Software/firmware upgarde of smart grid components
SG.MP-6	SM 3.6 Disposal of Smart grid Components
SG.SI-6	SM 3.7 Security testing of smart grid components
SG.PS	SM 4-1 Personnel Screening
SG.PS	SM 4.2 Personnel changes
SG.PM	SM 4.2 Security and Awareness Programm
SG.PM	SM 4.4 Security Training and certification of personnel
SG.IR	SM 5.1 Incident response capabilities
SG.RA-6	SM 5.2 Vulnerability assessment
SG.RA-2	SM 5.3 Vulnerability management
SG.IR	SM 5.4 Contact with authorities and security interest groups
SG.AU	SM 6.1 Auditing capabilities
SG.CA-6	SM 6.2 Monitoring of Smart Grid Information Systems
SG.AU-1	SM 6.3 Protection of audit information
SG.CP	SM 7.1 Continuity of operations capabilities
SG.SC-1	SM 7.2 Essential communication Services
SG.PE-3	SM 8.1 Physical security
SG.PE-7	SM 8.2 Logging and monitoring physical access
SG.PE-1	SM 8.3 Physical security on third party premises
SG.SA	SM 9.1 Data Security
SG.AC	SM 9.2 Account management
SG.AC-1	SM 9.3 Logical Access Control
SG.MA-6	SM 9.4 Secure Remote Access
SG.SC	SM 9.5 Information Security on Information Systems
SG.MP-1	SM 9.6 Media Handling

6.4 Standards und Normen für das Umfeld Smart Grid Security aus dem M/490

Die hier aufgeführten Standards wurden im Rahmen der Arbeiten der First Set of Standards (FSS) und Smart Grid Information Security (SGIS) Gruppen des M/490 als die relevante technischen Standards für die Umsetzung von Kommunikationssicherheit und Schutz von Smart Grid Assets identifiziert.

Im Rahmen dieser Studie können sie konkret zur Umsetzung der Massnahmen genutzt werden, da die wegen der fehlenden Umsetzung der Koordinationsmodelle in der Praxis jedoch nicht sehr operativ sind, wurden einzelne Standards nicht direkt zugewiesen.

Eine Möglichkeit, diese Standards in den SGAM Bezug zu setzen, besteht mit dem IEC SmartgridMappingTool unter http://smartgridstandardsmap.com/ .

Advanced Security Acceleration Project – Smart Grid (ASAP-SG):

- Entwicklung von Security Anforderungen für das Smart Grid auf Systemebene (z.B. für Smart Metering, Verteilnetzautomatisierung) in Form von „Security-Profilen“:
  - Third Party Data Access
  - Advanced Metering Infrastructure (AMI)
  - Third Party Data Access Distribution Management
  - Wide-Area Monitoring, Protection, and Control (WAMPAC)
  - Substation Automation (under development)

International council on Large Electric Systems, CIGRE B5/D2.46:

- Anwendung und Management von Cybersecurity-Massnahmen für Schutz- und Kontroll-Systeme

Department of Homeland Security (DHS):

- Catalog of Control Systems Security

Department of Homeland Security (DHS):

- Cyber Security Procurement Language for Control Systems

Department of Energy (DOE) / Department of Homeland Security (DHS):

- Electric Sector Cyber Security Risk Management Maturity Initiative

Department of Energy (DOE) / National Institute of Standards and Technologie (NIST) / North American Electric Reliability Corporation (NERC):

- Electricity Subsector Cyber Security Risk Management Process Guideline

Department of Energy (DOE):

- Roadmap Achieve Energy Delivery Systems Cyber Security

CEN / CENELEC:

- EN 62056-5-3: beschreibt den COSEM Application Layer, inklusive Security

European Telecommunications Standards Institute (ETSI):

- ETSI TCRTR 029, Security Techniques Advisory Group (STAG); A directory of security features in ETSI standards
- ETSI ETR 332, Security Requirements Capture
- ETSI ES 202 382, ETSI ES 202 383, Security Design Guide; Method and proforma for defining Protection Profiles
- ETSI EG 202 387, Security Design Guide; Method for application of Common Criteria to ETSI deliverables
- ETSI TS 102 165-1, Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis
- ETSI TS 102 165-2, Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures
- ETSI EG 202 549, Design Guide; Application of security countermeasures to service capabilities
- ETSI TR 185 008, Analysis of security mechanisms for customer networks connected to TISPAN NGN R2
- ETSI TR 187 012, Report and recommendations on compliance to the data retention directive for NGN-R2
- ETSI TS 187 016, NGN Security; Identity Protection (Protection Profile)
- ETSI TR 102 419, Security analysis of IPv6 application in telecommunications Standards ETSI TS 101 456, ETSI TR 102 437, ETSI TS 102 042, ETSI TR 102 572, ETSI TS 102 573, Electronic signatures
- ETSI TS 102 689, M2M service requirements
- ETSI TS 102 690, M2M-Functional architecture
- ETSI TS 102 921, M2M-MLA, DLA and MLD interfaces
- ETSI TR 103 167, Threat analysis and counter-measures to M2M service layer
- ETSI TS 100 920, Communication, information for mobile (3GPP, GSM, CDMA ...) telecommunication infrastructures
- ETSI TS 133 203, Access security for IP-based services (3GPP TS 33.203)
- ETSI TS 133 210, Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)
- ETSI TS 133 234, Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234)
- ETSI TS 133 310, Network Domain Security (NDS); Authentication Framework AF) (3GPP TS 33.310)
- ETSI TS 102 225, Communication, information for mobile (3GPP, GSM, CDMA ...) telecommunication infrastructures. Secure packet protocol for remote administration of Security element
- ETSI TS 102 226, Communication, information for mobile (3GPP, GSM, CDMA ...) telecommunication infrastructures. Remote administration of Security element
- ETSI TS 102 484, Communication, information for mobile (3GPP, GSM, CDMA ...) telecommunication infrastructures. Local Secure Channel to Security element
- ETSI TS 187 001, Communication, information for fixed (IP based ...) telecommunication infrastructures. Security Requirements
- ETSI TS 187 003, Communication, information for fixed (IP based ...) telecommunication infrastructures. Threat Analysis
- ETSI TR 187 002, Communication, information for fixed (IP based ...) telecommunication infrastructures. Security Architecture

World Wide Web Consortium (W3C):

- W3C XML Digital Signature, Provide security features for XML encoded data
- W3C XML Encryption, Provide security features for XML encoded data

International Electrotechnical Commission (IEC):

- Normenreihe „IEC 62351 Teile 1–11 – Netzführungssysteme und ihr Informationsaustausch – Daten- und Kommunikationssicherheit“
- Normenreihe „IEC 62443 – Informationssicherheit in der Automatisierungstechnik“

Institute of Electrical and Electronics Engineers (IEEE):

- IEEE 1686-2007 – IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
- IEEE 802.11i Wireless security
- IEEE 802.1X Port based network access control
- IEEE 802.1AE MAC security
- IEEE 802.1AR Secure Device Identity

The Internet Engineering Task Force (IETF):

IETF Cyber Security RFCs:

- RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
- RFC 2759 EAP MS-CHAP2
- RFC 2865 RADIUS (Remote Authentication Dial In User Service)
- RFC 3711 Secure Real-time Transport Protocol (SRTP)
- RFC 3748 EAP Base Protocol (umfasst EAP MD5)
- RFC 4101, RFC 4102, RFC 4103 Base standards for IP Security (IPSec)
- RFC 4301, RFC 4302, RFC 4303 IPSec
- RFC 4764 EAP PSK (Pre-Shared Key)
- RFC 4962 Authentication, Authorization, and Accounting (AAA)
- RFC 5106 EAP IKEv2
- RFC 5216 EAP TLS
- RFC 5246 Transport Layer Security (TLS)
- RFC 5247 Extensible Authentication Protocol (EAP) Framework, Framework für Schlüsselmanagement
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Basis-Spezifikation für X.509-Zertifikate und -Zertifikatshandhabung
- RFC 5281 EAP TTLSv1.0
- RFC 6407 Group Domain of Interpretation (GDOI)
- RFC 6347 Datagram Transport Layer Security (DTLS)
- RFC 5746 Transport Layer Security (TLS) Renegotiation Indication Extension
- RFC 6272 Internet Protocols for the Smart Grid (identifiziert RFCs, die im Smart Grid Verwendung finden)
- RFC 6347 DTLS, Alternative zu TLS in UDP-basierten Netzen
- RFC 6407 Group Domain of Interpretation (GDOI), wird z.B. benutzt, um das Schlüsselmanagement bei der IEC 61850-90-5 zu realisieren
- RFC 6749 The OAuth 2.0 Authorization Framework

International Society of Automation (ISA):

- ISA 99 Standards Framework

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC):

- ISO/IEC 27000 Reihe

North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP) Programm:

- NERC-CIP Standards 002 bis 011

National Institute of Standards and Technologie (NIST):

- FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS) 140-2: Security Requirements for Cryptographic Modules
- Special Publication (SP) 500-267 Security profile for IPv6
- Special Publication (SP) 500-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
- NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards
- NIST Special Publication 800-39: Managing Information Security Risk: Organization, Mission and Information System View
- NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems
- NISTIR 7628 US-Guidelines for Smart Grid Cyber Security Part 1-3
- NISTIR 7823: Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework

6.5 Vorgehen der NIST CSWG zur Definition der NISTIR 7628

Der fünf schrittige Smart Grid-Risikoevaluierungsprozess, wie er von der CSWG umgesetzt wurde, basiert auf existierenden Ansätzen sowohl aus dem privaten als auch öffentlichen Sektor. Er umfasst die Identifikation von Assets, Vulnerabilitäten und Gefährdungen sowie die Formulierung von potentiellen Konsequenzen.

CSWG - Schritt 1 – Definition von Anwendungsfälle mit Cyber-Security Aspekten

Für die Identifikation von Smart Grid Anwendungsfälle mit Relevanz für Privacy und Security wurden verschiedene Sammlungen von Anwendungsfälle untersucht.

Konkret betrachtet wurden durch das NIST:

- IntelliGrid Anwendungsfälle: Diese Quelle stellt insgesamt über 700 Smart Grid Anwendungsfälle zur Verfügung. Für die vorliegenden Arbeiten im NISTIR 7628 wurden allerdings nur jene für den Betrieb von Elektrischen Systemen, für Demand Response (DR) und Advanced Metering Infrastructure (AMI) betrachtet. Die vollständige Liste wurde vom Electric Power Research Institute (EPRI) entwickelt und ist öffentlich verfügbar (IntelliGrid Architecture - Published Results)
- AMI Business Functions: Anwendungsfälle wurden aus Appendix B des Advanced Metering Infrastructure Security (AMI-SEC) System Security Requirements Dokuments entnommen. Dieses Dokument wurde von der AMI-SEC Task Force der Transmission and Distribution Domain Expert Working Group (T&D DEWG) erstellt.
- Benefits and Challenges of Distribution Automation: Use Case Szenarien aus dem California Energy Commission Document mit insgesamt 82 Anwendungsfälle.

- EPRI Use Case Repository: Eine Zusammenfassung der IntelliGrid und California Energy Commission (CEC) Anwendungsfälle mit zusätzlichen Ergänzungen.
- SCE Anwendungsfälle: Entwickelt von Southern California Edison (SCE) mit Unterstützung von EnerNex (vgl. Webseite SCE.com).

Die hier aufgeführten Use Case-Sammlungen stellten die Basis für das anschliessende Security Assessment (Schritt 2), die Entwicklung des Logical Reference Models (Schritt 3) sowie die Entwicklung der High-Level Security Requirements (Schritt 4) dar. Das logische NIST LRM (Logical Reference Model) Modell wurde aus dem Conceptual NIST-Modell und den konsolidierten Wissen über Schnittstellen aus den Anwendungsfallsammlungen abgeleitet.

CSWG - Schritt 2 – Durchführung einer Risiko Abschätzung

Auf Basis der in CSWG - Schritt 1 untersuchten Anwendungsfälle wurde eine Risiko Abschätzung durchgeführt. Jeder einzelne Use Case wurde aus einer High-Level Perspektive betrachtet, wobei spezifische Assets, Vulnerabilitäten, Bedrohungsszenarien und potentielle Konsequenzen identifiziert wurden. Das Ergebnis diente als Richtschnur für die Erstellung von Sicherheitsanforderungen sowie für die Identifikation von Gaps in den einschlägigen Standards und Guidelines.

Für die Untersuchung der Anwendungsfälle wurden sowohl Top-Down als auch Bottom-up Methodiken angewandt. Die Bottom-Up Ansätze fokussierten hierbei bekannte Probleme (z. B. Authentication und Authorisation). Ergänzend dazu wurden für die Top-Down Betrachtungen logische Interface Diagramme für sechs zu betrachtende Bereiche (so genannte Domänen) erstellt.

Diese sechs Bereiche umfassen

- Electric Transportation
- Electric Storage
- Wide Area Situational Awareness
- Demand Response
- Advanced Metering Infrastructure
- Distribution Grid Management

Die hierbei erstellten, logischen Interface-Diagramme wurden verwendet, um das so genannte Logical Reference Model (LRM) (Schritt 3) zu erstellen.

CSWG - Schritt 3 – Logical Reference Model: Entwicklung einer Security Architektur

Basis für das Erstellen des Logical Reference Model stellt das NIST Interoperability „Framework and Roadmap“ Dokument [7] dar, welches das Smart Grid in die sieben Domänen Transmission, Distribution, Operations, Bulk Generation, Marketing, Consumer und Service Provider unterteilt, wie in Abbildung 16 dargestellt.

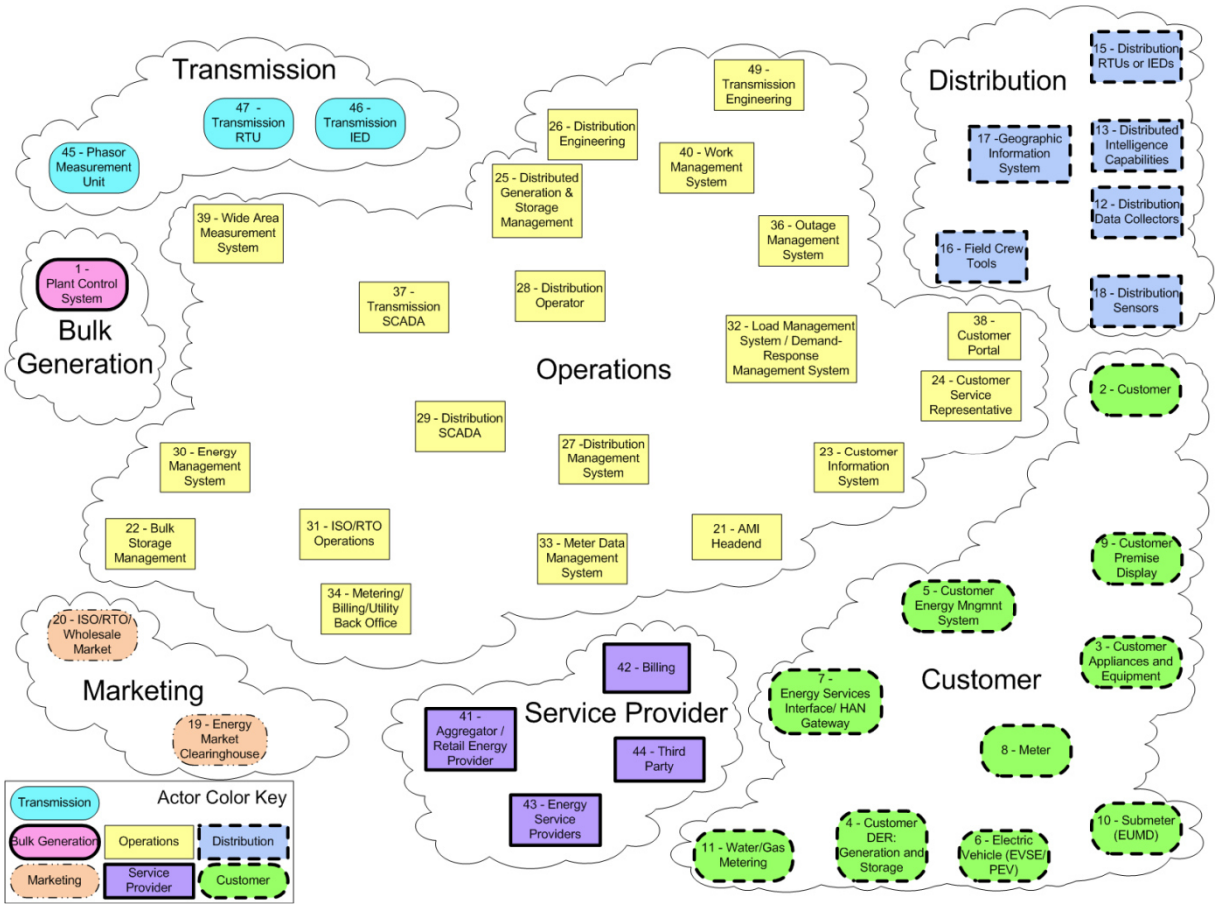


Abbildung 16: High Level View auf die Smart Grid Akteure in den jeweiligen Smart Grid Domänen

Eine Domäne fasst hierbei Akteure mit ähnlichen Zielen bzw. technischen Applikationen und Systemen zusammen.

Ausgehend von den Erkenntnissen aus Schritt 2 wurden insgesamt 46 Akteure für die Konzeption des Logical Reference Model ausgewählt. Diese 46 Akteure stellen keine abschliessende Menge an Akteuren dar, sondern stellen vielmehr ein repräsentatives Set an Akteuren für die weiteren Untersuchungen und Ergänzungen im Rahmen der Methodik dar.

Das Logical Reference Model definiert Schnittstellen (engl. Interfaces) zwischen diesen repräsentativen Akteuren, die wiederum einer konkreten Schnittstellenklasse zugeordnet werden können. Schnittstellenklassen (engl. Interface Categories) fassen hierbei Schnittstellen mit spezifischen Attributen zusammen und stellen somit die Grundlage für das anschliessende Anforderungsmanagement dar.

Insgesamt wurden über 130 Schnittstellen formuliert, die wiederum 22 Interface Categories repräsentieren.

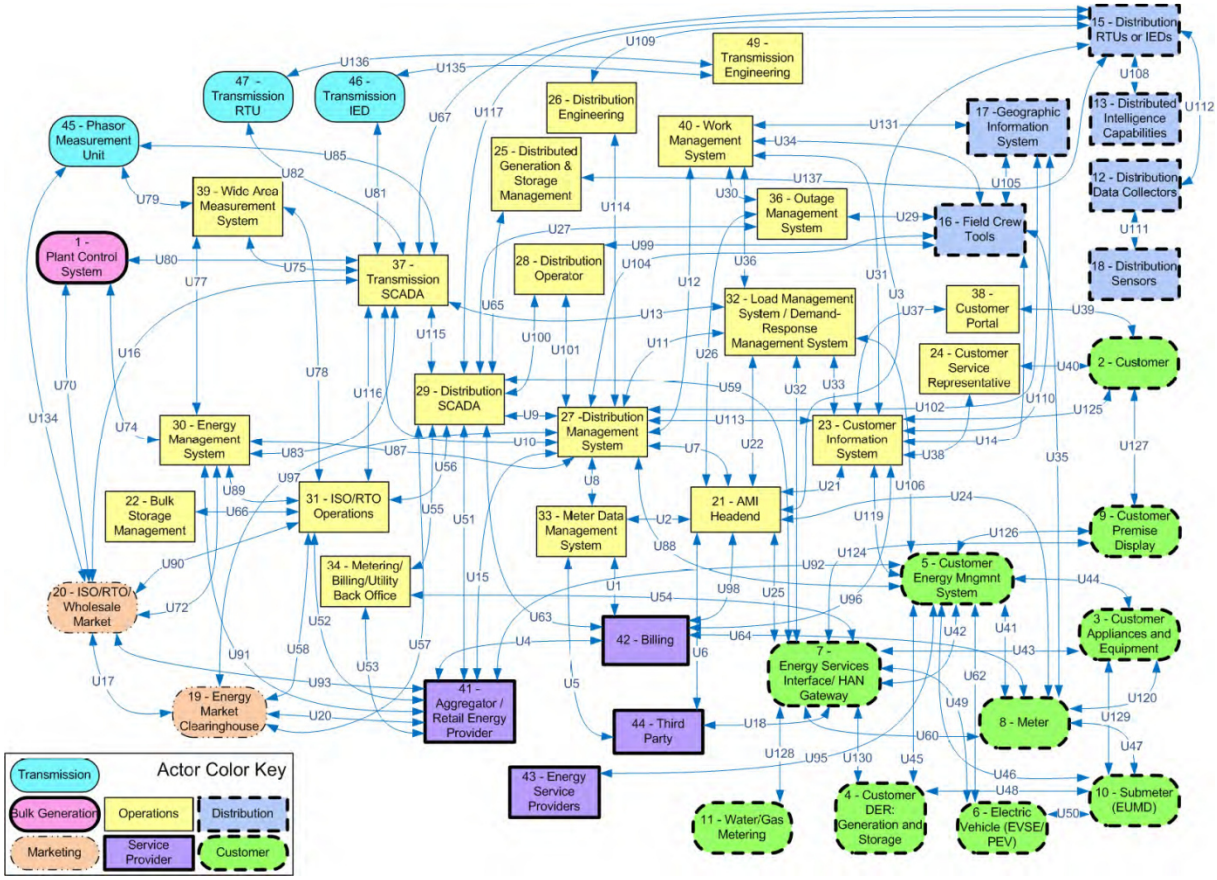


Abbildung 17: Logisches Referenzmodell

Eine beispielhafte Schnittstellenklasse ist in Abbildung 18 zu finden. Jede dieser Kategorien wurde speziell hinsichtlich der drei Sicherheitsaspekte Vertraulichkeit (engl. Confidentiality), Integrität (engl. Integrity) und Verfügbarkeit (engl. Availability) untersucht. Eine solche Analyse wird zumeist auch CIA Analyse genannt.

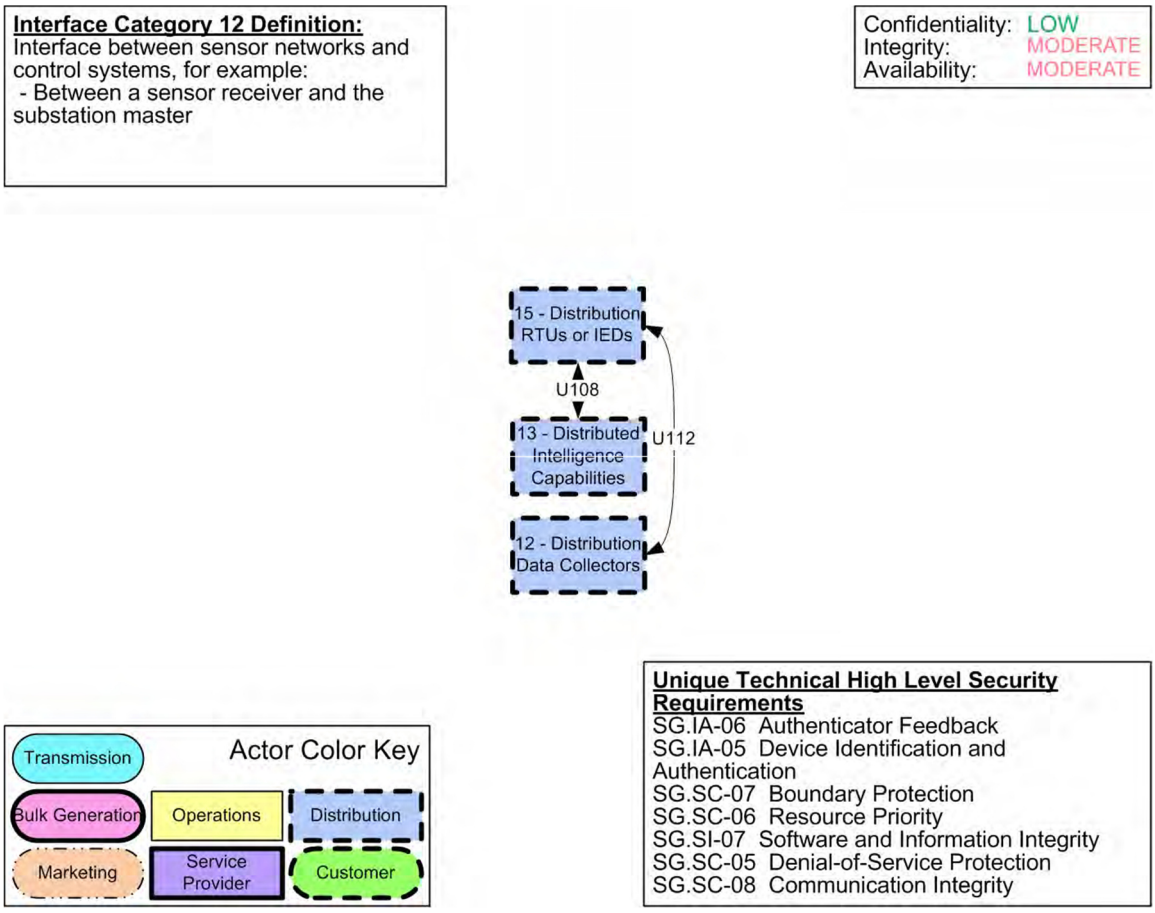


Abbildung 18: Beispiel Interface Category 12 aus dem NISTIR 7628

CSWG - Schritt 4 – Formulierung von High-Level Sicherheitsanforderungen

Im vierten Schritt wurden 198 Anforderungen (engl. High Level Security Requirements) entwickelt und detailliert beschrieben, die im Weiteren auf die zuvor spezifizierten Schnittstellenklassen abgebildet wurden. Diese Anforderungen basieren im Wesentlichen auf einem umfassenden Anforderungssatz aus dem „DHS Catalog of Control Systems Security“ (US Department of Homeland Security - Control Systems Security Program - National Cyber Security Division, 2011)

Die erarbeiteten so genannten Cyber Security Requirements wurden in 19 Gruppen (z. B. Access Control, Audit and Countability, Configuration Management) zusammengefasst und kategorisiert.

Für die Anwendung dieser Anforderungen im Entwurf und Betrieb (und der zuvor beschriebenen Ergebnisse) werden folgende Schritte vorgeschlagen:

- Identifikation der logischen Interface Kategorien
- Durchführen eines Risk Assessments
- Auswahl der initialen High-Level Security Requirements auf Basis der logischen Interface Kategorien

CSWG - Schritt 5 – Konformitäts-Tests und Zertifizierung

Neben den zuvor beschriebenen Schritten zur strukturierten Entwicklung von interoperablen Smart Grid Systemen mit den zugehörigen Sicherheitsanforderungen wird die Wichtigkeit eines Konformitäts- und Interoperabilitätstests betont.

Voraussetzung hierfür ist die Konsolidierung verschiedener Ansätze hin zu einem von breiter Basis getragenen Konzept. Entsprechende Arbeiten wurden initiiert, sind allerdings nicht mehr Teil der NISTIR 7628 Guidelines.

6.6 Beispiel für die Anwendung der NISTIR 7628

Im folgenden Abschnitt wird ein Minimalbeispiel für ein Mapping eines Anwendungsfalls auf das SGAM und die NISTIR 7628 Schnittstellenanalyse vorgestellt, um die Arbeiten an den Consentec Anwendungsfällen sowie den Ergebnissen in Kapitel 3 dieser Studie methodisch zu erläutern.

Beispielszenario für die Methodik „Steuerung von dezentralen Anlagen“

In einem Virtuellen Kraftwerk (VK) werden viele kleine Energie-Anlagen gebündelt, um durch das Erreichen einer „kritischen Masse“ den Handel an Strommärkten oder das Anbieten von Systemdienstleistungen (zu diesen gehört Frequenzhaltung, Spannungshaltung, Versorgungswiederaufbau und das Netzengpassmanagement) zu ermöglichen.

Ein VK-Betreiber trifft auf Basis von Potentialaussagen über Erzeugungsanlagen Handelsvereinbarungen und erstellt einen Einsatzplan für diese Anlagen. Zur Realisierung eines solchen Einsatzplans müssen Anpassungen an der Lasterzeugung bzw. dem Lastbedarf vorgenommen werden. Dies geschieht zum einen im Voraus durch das Geben von Anreizen sowie kurzfristig durch das direkte Steuern ausgewählter Anlagen.

Für das im vorherigen Abschnitt beschriebene CSWG-Vorgehensmodell ergeben sich für dieses Beispielszenario eines so genannten Virtuellen Kraftwerks folgende Arbeitsschritte:

UML-Sequenzdiagramm für das Minimalbeispiel

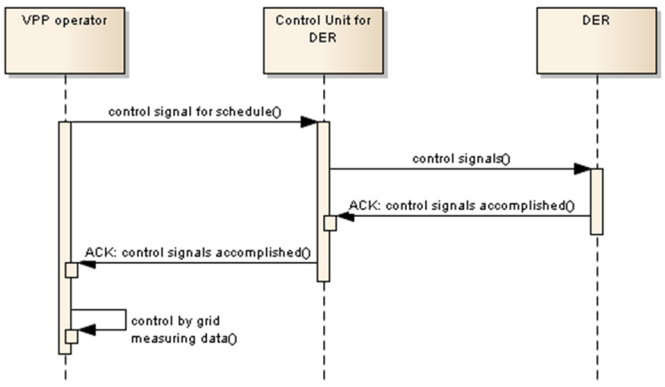


Abbildung 19: UML Sequenzdiagramm

A. Identifikation und Spezifikation des Anwendungsfall

- Verwendung der Beschreibung des Beispielszenarios für die Spezifikation des Anwendungsfall. Im Rahmen der Studie wird hier zumeist das IEC 62559 Template genutzt, für dieses Minimalbeispiel ist es jedoch nicht erforderlich.
- Identifizierte Akteure im Minimalbeispiel sind:
    - Dezentrale Energieanlagen,

  - VK-Betreiber,
  - System zur Steuerung der Energieanlage
- UML Sequenzdiagramm zur Darstellung des Prozessablaufs

B. Identifikation und Abgleich von logischen Knoten, Kommunikationsverbindungen und „Logical Interface Categories“ aus dem NISTIR 7628

Die im ersten Schritt beschriebenen Akteure und Kommunikationsbeziehungen müssen nun im NISTIR 7628 identifiziert und den Akteuren und Kommunikationsbeziehungen dort zugeordnet werden. Abbildung 20 zeigt das abgeleitete Szenario, das mittels des High-Level Diagramms aus dem NISTIR 7628 dargestellt ist. Die dezentrale Energieanlage entspricht dabei dem Customer DER, die Steuerung der Energieanlage erfolgt über das Customer EMS und der VK-Betreiber würde in diesem Anwendungsfall über das LMS/DRMS in den Prozess eingreifen. Zusätzlich wurden die Kommunikationsbeziehungen (U106 und U45) und entsprechend dazu die „Interface Categories 10 und 15“ identifiziert. Die Farben repräsentieren dabei die gleichen Domänen wie im NIST LRM SGAM Diagramm dargestellt.

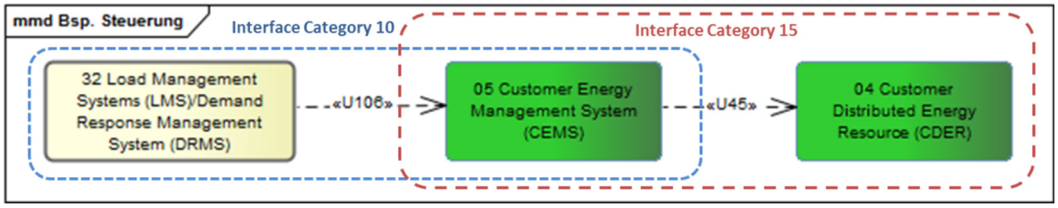


Abbildung 20: Steuerung von Anlagen dargestellt in der High-Level Interface Ansicht des NISTIR 7628

Genauer bedeutet dies für die Kommunikation in unserem Beispiel: Das System mit der Nr. 32 LMS/DRMS (gelb = Domäne „Operation“) sendet zwei verschiedene Arten von Signalen an das System Nr. 05 Customer EMS (grün = Domäne „Customer“). Es werden mit ausreichender Vorlaufzeit Tarifierungen ermittelt und übertragen, um je nach Bedarf die Last zu verringern oder zu erhöhen. Ist der Zeitpunkt gekommen, für den die Einsatzplanung erfolgte, so wird mit Echtzeit-Messdaten geprüft, ob die Vorgaben erfüllt werden. Sollte dies nicht der Fall sein, so wird mittels des zweiten Signals eine entsprechende direkte Steuerung von Lasten zur Erfüllung der Vorgaben initialisiert. Beide Signale werden an das CEMS gesendet. Dieses trifft manuell oder automatisiert Entscheidungen und sendet diese an das Customer DER. Die CDER sind Erzeugungsquellen, wie zum Beispiel Wind oder Solaranlagen, die beim Kunden verortet sind.

C. Integration der Logical Interfaces Systeme ins SGAM auf dem „Function Layer“

In diesem Schritt erfolgt nun die Integration ins SGAM auf dem „Function Layer“, dort sind die oben beschriebenen Akteure inkl. der Kommunikationsbeziehung im SGAM verortet. Diese Darstellung ermöglicht es nicht nur zu sehen, in welchen Domänen die Akteure liegen, sondern auch, welcher hierarchischen Zone innerhalb dieser Domänen sie zuzuordnen sind.

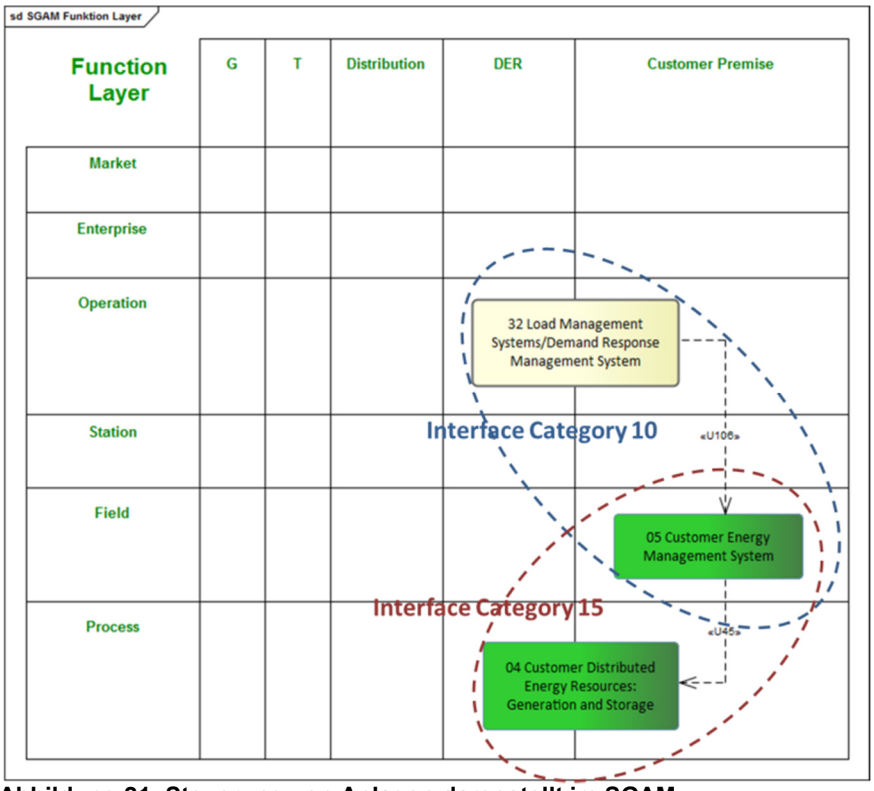


Abbildung 21: Steuerung von Anlagen dargestellt im SGAM

D. Verwendung von „Smart Grid Cyber Security Requirements“ (SG-CySecReq) zur Schutzzielpriorisierung sowie zur Identifikation von anwendbaren Sicherheitsstandards

Im vierten Schritt werden anhand der identifizierten „Logical Interface Categories“ die entsprechenden Anforderungen (SG-CySecReq) abgeleitet.

Damit ergibt sich eine vorläufige Schutzzielpriorisierung für den hier genannten Anwendungsfall, dargestellt in Tabelle 4. Zusätzlich gibt es hier die Möglichkeit aufgrund der SG-CySecReq aus dem NISTIR 7628 Sicherheitsstandards für den eigenen Entwurf zu identifizieren.

Tabelle 14: Beispielanalyse NISTIR

Logical Interface Category	Vertraulichkeit	Integrität	Verfügbarkeit	Smart Grid Cyber Security Requirements (Vgl. NISTIR 7628 Vol 3)
10	Niedrig	Hoch	Mittel	AC-14, IA-04, SC-05, SC-06, SC-07, SC-08, SC-26, SI-07
15	Niedrig	Mittel	Mittel	AC-14, IA-04, SC-03, SC-05, SC-06, SC-07, SC-08, SC-09, SC-26, SI-07
Gesamt	**Niedrig**	**Hoch**	**Mittel**	AC-14, IA-04, SC-03, SC-05, SC-06, SC-07, SC-08, SC-09, SC-26, SI-07

E. Abbilden der Elemente auf die weiteren Layer des SGAMs

Im fünften Schritt werden nun die in Schritt 4 identifizierten SG-CySecReq (Schutzanforderungen) zusammen mit den Akteuren und Kommunikationsbeziehungen auf die einzelnen SGAM-Layer abgebildet, um weitere Sicherheitsanforderungen abzuleiten und somit einer Gesamtsicherheitsanalyse zu unterziehen.

Um die Anwendungsfälle letztlich in das SGAM Toolbox Werkzeug einzupflegen, ist es nötig, geordnete und strukturierte Basisinformation zur Verfügung zu haben. Da im Rahmen dieser Studie auf zwei bereits existierende, heterogene Dokumente aufgesetzt wird, ist es nötig, die Anwendungsfälle der Consentec und AWK Studie in einer homogenen Anwendungsfallstruktur in einer Anwendungsfallvorlage abzubilden. Hierfür wurde die IEC 62559 gewählt, deren Vorlage im folgenden Abschnitt beschrieben wird.

6.7 IEC 62559 Anwendungsfallvorlage

1 Description of the Use Case

1.1 Name of use case

Use case identification		
ID	***Area Domain(s)/ Zone(s)***	***Name of use case***

1.2 Version management

Version management				
Version No.	***Date***	***Name of author(s)***	***Changes***	***Approval status***

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	
Objective(s)	
Related business case(s)	

1.4 Narrative of use case

Narrative of use case
Short description
Complete description

1.5 Key performance indicators (KPI)

Key performance indicators			
ID	***Name***	***Description***	***Reference to mentioned use case objectives***

1.6 Use case conditions

Use case conditions
Assumptions
Prerequisites

1.7 Further information to the use case for classification / mapping

Classification Information
Relation to other use cases
Level of depth
Prioritisation
Generic, regional or national relation
Nature of the use case
Further keywords for classification

1.8 General remarks

General remarks

2 Diagrams of use case

Diagram(s) of use case

3 Technical details

3.1 Actors

Actors			
Grouping		***Group description***	
Actor name	***Actor type***	***Actor description***	***Further information specific to this use case***

3.2 References

References						
No.	***References type***	***Reference***	***Status***	***Impact on use case***	***Originator / organisation***	***Link***

4 Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	***Scenario name***	***Scenario description***	***Primary actor***	***Triggering event***	***Pre-condition***	***Post-condition***

4.1 Steps – Scenarios

Scenario								
Scenario name :								
Step No.	***Event***	***Name of process/ activity***	***Description of process/ activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirements R-ID***

5 Information exchanged

Information Exchanged			
Information exchanged ID	***Name of information exchanged***	***Description of information exchanged***	***Requirements IDs***

6 Requirements (optional)

Requirements (optional)		
Categories ID	***Category name for requirements***	***Category description***
Requirement ID	***Requirement name***	***Requirement description***

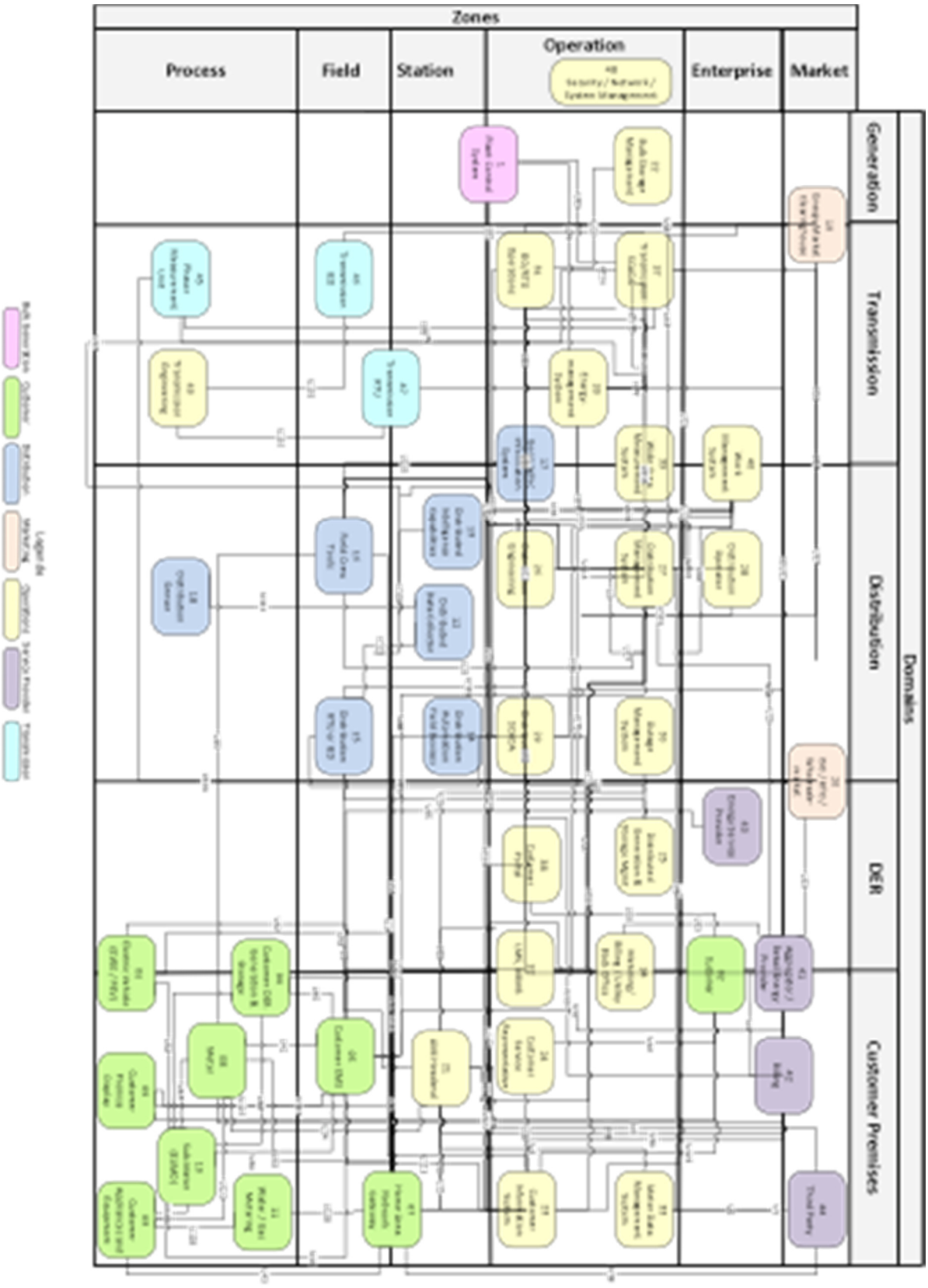
7 Common Terms and Definitions

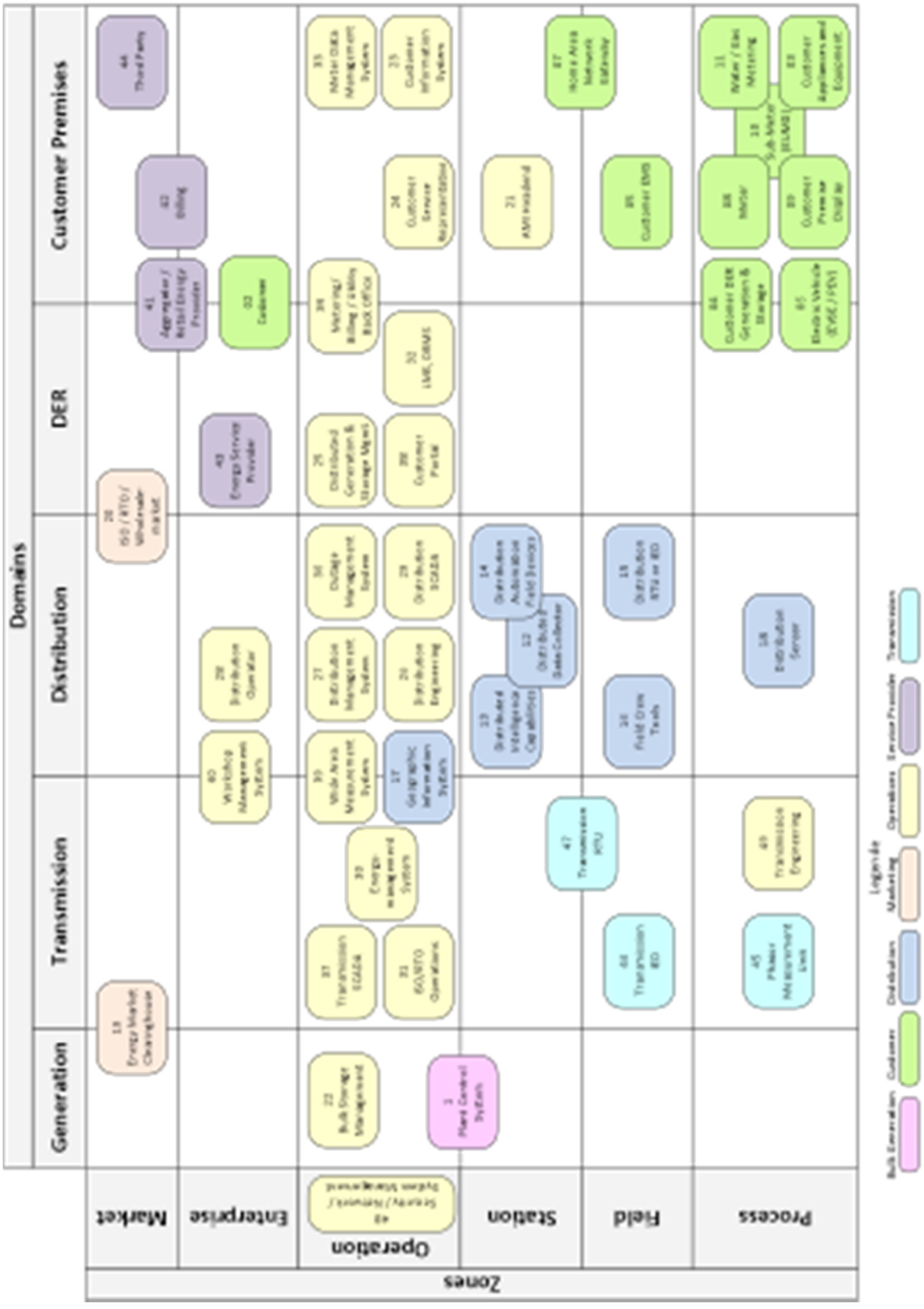
Common terms and definitions	
Term	***Definition***

8 Custom information (optional)

Custom information (optional)		
Key	***Value***	***Refers to section***

6.8 Detaillierte NISTIR 7628 zu SGAM Diagramme


Zones
Process
Field
Station
Operation
Enterprise
Market
Domains
Generation
Transmission
Distribution
DER
Customer Premises


Domains
Generation
Transmission
Distribution
DER
Customer Premises
Zones
Market
Enterprise
Operation
Station
Field
Process
Bulk Generation
Customer
Distribution
Markets
Operations
Service Provider
Transmission