oesterreichs energie.

Endbericht des Expertenpools

Digitale Schnittstelle

Bidirektionale *Digitale Schnittstelle*

Version 1.0

22.12.2022

Inhaltsverzeichnis

A. Executive Summary

A.1 Motivation

Um die Klimaziele in Österreich erreichen zu können, muss unter anderem eine verstärkte Elektrifizierung des Energiesystems und damit auch eine Steigerung der Energieeffizienz erfolgen. Zum daraus resultierenden notwendigen Ausbau von erneuerbaren Energien kommt der Ersatz fossiler Brennstoffe hinzu, um die Dekarbonisierung voranzutreiben. Diese Entwicklung, verbunden mit der stärkeren Dezentralität und Volatilität der zukünftigen Energieerzeugung, führt in den Verteilernetzen bereits aktuell zu einer starken Änderung der Lastflüsse und einem signifikanten Anstieg der bereitzustellenden Spitzenleistung, beides Effekte, für welche die bestehende Netzinfrastruktur nicht ausgelegt wurde. Dieser Entwicklung Rechnung tragend, hat die Regulierungsbehörde E-Control im Dokument “Tarife 2.1” erstmals zusätzliche Modelle für Netztarife mit einer Steuerungsoption für Verteilernetzbetreiber (VNB) vorgestellt. Diese zielen darauf ab, Spitzenleistungen durch netztarifliche Anreize bei Erzeugungsanlagen oder Lastenbesser zu verteilen. Zum Beispiel können die Spitzenleistungen von E-Mobilität und Wärmepumpen (WP) zum Ausgleich der Netze dienen. Mit dieser Steuerungsoption soll die Anzahl der in die Bestandsnetze integrierbaren Erzeugungsanlagen und neuen Lasten erhöht werden. Dafür muss eine Kommunikationsmöglichkeit zwischen einem Steuerungssystem bei den Verteilernetzen und den betreffenden Kundenanlagen geschaffen werden.

Bei Oesterreichs Energie wurde vom Lenkungsausschuss Netze der Auftrag formuliert, das Projekt „*Digitale Schnittstelle*“ durchzuführen und dabei die verschiedenen Stakeholder einzubinden und deren Interessen zu berücksichtigen. Der Begriff "*Digitale Schnittstelle*" wurde im Projekt als Synonym für eine bidirektionale elektronische Schnittstelle definiert, die ein VNB zur Übermittlung von Leistungsvorgaben für eine Kundenanlage zur Verfügung stellt. Eine Darstellung der technischen Möglichkeiten für die Bereitstellung von solchen Kommunikationskanälen über geeignete Schnittstellen, Standards und Protokolle wurde im Rahmen dieses Projektes erarbeitet. Zusätzlich wurde der aktuelle rechtlich-regulatorische Rahmen auf noch fehlende oder anzupassende Vorgaben analysiert.

Die Ausgestaltung einer *Digitalen Schnittstelle* kann einen Beitrag zur Erreichung der Interoperabilität leisten, die in einem digitalisierten Stromnetz stark an Bedeutung gewinnt. Die Interoperabilität ist Kommunikationsfähigkeit unterschiedlicher Komponenten und Systemen und dem damit ermöglichten Zusammenspiel.

A.2 Projektdurchführung

Im ersten Schritt wurden sechs Use Cases erarbeitet. Der Fokus im Projekt richtete sich auf den Use Case 1 „Ansteuerung von Kundenanlagen durch VNB im Notzustand“. Aus diesen Use

Cases wurden speziell die Anforderungen an den Kommunikationskanal zwischen Verteilernetzbetreiber und Netzkunde abgeleitet. Der Verteilernetzbetreiber ermittelt pro Netzanschlusspunkt die erforderlichen Leistungsvorgaben, die über drei verschiedene Kommunikationsarchitekturen umgesetzt werden können:

- Ein Verteilernetzbetreiber kommuniziert über eine *zentrale Schnittstelle* mit einem Dritten, der mit seiner Infrastruktur für die Umsetzung der Leistungsvorgaben im Auftrag des VNB sorgt
- Ein Verteilernetzbetreiber kommuniziert direkt über eine *zentrale Schnittstelle* mit steuerbaren Anlagen bei Netzkunden
- Ein Verteilernetzbetreiber kommuniziert über einen beim Netzkunden installierten Funktionsblock[1] mit steuerbaren Anlagen beim Netzkunden

In einem zweiten Schritt wurden alle Erkenntnisse aus den Use Cases und den Architekturvarianten einem Expertenteam unter der Leitung des AIT (Austrian Institute of Technologie) mit dem Auftrag übergeben, bekannte Standards, Protokolle und Lösungen für diese Aufgabenstellung zu evaluieren und nach abgestimmten Kriterien zu bewerten.

A.3 Ergebnisse

Die Ergebnisse können wie folgt zusammengefasst werden:

- Die wesentlichen Anforderungen an eine Kommunikationsarchitektur zwischen Verteilernetzbetreiber und Netzkunden vor dem Hintergrund konkreter Anwendungen (Use Cases) liegen vor, müssen aber zu einem späteren Zeitpunkt ggf. ergänzt oder angepasst werden.
- Eine wissenschaftliche Analyse und eine Bewertung der für die gegenständliche Aufgabenstellung in Frage kommenden Standards, Protokolle und Lösungen liegt als Entscheidungsgrundlage vor. Hier muss allerdings angemerkt werden, dass die Bewertung in Bezug auf Security nur sehr generisch erfolgt ist, da noch eine Festlegung der erforderlichen Betriebsprozesse (z. B. Onboarding von Geräten) und darauf basierend eine Festlegung der für die Einhaltung der NIS-Gesetzgebung (Netz- und Informationssystemsicherheit) erforderlichen Maßnahmen fehlt.
- Eine tiefgehende Analyse der bestehenden rechtlich regulatorischen Rahmenbedingungen auf fehlende oder hinderliche Vorgaben wurde erstellt und im Kapitel F.4 dokumentiert.

[1] Der Funktionsblock ist eine funktionale Beschreibung einer lokalen Schnittstelle zwischen VNB und Kundenanlage. Die technische Ausgestaltung kann durch eine separate Hardware (z.B. eigenes Gateway inkl. Software) und/oder Software (Integration in bestehende Hardware wie beispielsweise Smart Meter) umgesetzt werden.

Es hat sich herausgestellt, dass sich die Lösungsfindung der Thematik in der Tiefe deutlich komplexer darstellt als ursprünglich angenommen. Deshalb ist eine weitergehende Bearbeitung des Themas über dieses Projekt hinaus erforderlich. Dafür wurde ein konkreter Vorschlag erarbeitet, der zwei Schwerpunkte umfasst:

- Erhebung der detaillierten Anforderungen und Erstellung einer Schnittstellenspezifikation für eine *Digitale Schnittstelle* zur Kommunikation mit Dritten, die Steuerungsmaßnahmen "im Auftrag" des VNB ausführen
- Ergänzung der Varianten in denen der VNB die Leistungsvorgaben direkt vorgibt

Details zur Fortführung des Projekts sind in Kapitel H.3 beschrieben. Handlungsempfehlungen für die betroffenen Stakeholder wurden in Kapitel H.2 zusammengefasst.

B. Ausgangslage & Motivation

Die Klimakrise und die zur Bewältigung erforderliche Elektrifizierung der Mobilität und der Raumwärme sowie die Strombereitstellung rein aus erneuerbaren Energieträgern waren in der Vergangenheit zwar bereits absehbar, sind nun aber mit einer deutlich höheren Dynamik, zusätzlich verstärkt durch den Ukrainekrieg, eingetreten.[2] Die bestehende Netzinfrastruktur und insbesondere die Verteilernetze werden allerdings zunehmend zum limitierenden Faktor für die Umsetzung der Energiewende. Demnach braucht es entsprechende Maßnahmen im Stromnetz um das Erreichen der Energie- und Klimaziele nicht zu behindern und dabei weiterhin das hohe Maß an Versorgungssicherheit zu gewährleisten.

Die Bereitstellung immer höherer Spitzenleistungen z.B. für Elektrofahrzeuge, Wärmepumpen und Photovoltaikanlagen und das damit einhergehende geänderte Nutzerverhalten stellt für die Verteilernetze eine Herausforderung dar. Eine wesentliche Maßnahme stellen der Ausbau und die Verstärkung der Verteilnetze dar, womit erhebliche Investitionen verbunden sind. Damit der Netzausbau möglichst kosteneffizient erfolgen kann, sind zusätzliche Maßnahmen für eine optimale Nutzung der Netzkapazitäten zu setzen. Einen wesentlichen Beitrag dazu können die Digitalisierung und die Nutzung von angebots- sowie nachfrageseitigen Flexibilitäten leisten. Auch die Umsetzung einer umfassenden Reform der Netzentgelte (Netztarife 2.1) ist von erheblicher Bedeutung.

B.1 Grundlagen der Netzinfrastruktur

Das solide Fundament des klassischen Netzausbaues beruht auf der sogenannten Primärtechnik (Kabel, Trafos) und ist auch für den Umbau des Energiesystems ein wesentlicher Bestandteil, welcher auch langfristig als solide Basis der Netzinfrastruktur bestehen bleiben soll. Da Netzausbaumaßnahmen zeit- und ressourcenaufwendig sind, ist die Ergänzung durch vermehrten Einsatz von Messtechnik („Transparente Netze“) und Intelligenz in den unteren Spannungsebenen notwendig, um die richtige Priorisierung von Maßnahmen vornehmen zu können. Dafür sind zukünftig umfangreiche Planungen erforderlich, die einen schrittweisen und branchenübergreifenden Aufbau von digitalen Schnittstellen zur bidirektionalen Ansteuerung ermöglichen.

B.2 Leistungszunahme im Verteilernetz

Bisher waren die Haushalte mit ihren durchschnittlichen Leistungswerten von typischen 1-2 kW (mit Gleichzeitigkeitsfaktor[3]) für die Systemauslegung im Rahmen der Netzplanung im niedrigen Leistungsbereich nicht systemrelevant. Die Veränderung hin zu Prosumer - also Haushalte, die

[2] Vgl. (BMK, 2021), (Europäische Kommission, 2022)

[3] Gleichzeitigkeitsfaktor: Die Wahrscheinlichkeit, dass Verbraucher oder Einspeiser zum gleichen Zeitpunkt Energie vom Netz beziehen oder einspeisen.

sowohl als Energiekonsumenten als auch als Energieerzeuger auf das Netz einwirken - hebt die Systemrelevanz in Verteilernetzen, vor allem in Niederspannungsnetzen maßgeblich an. Beispielsweise haben Photovoltaikanlagen typischerweise eine installierte Leistung von 5-10 kWp, Ladeeinrichtungen für Elektromobilität 11 kW oder 22 kW und Wärmepumpen mit Heizstab zwischen 4-10 kW. Durch die höhere Gleichzeitigkeit von Ladeeinrichtungen und Wärmepumpen im Vergleich zu Standardlasten wie z.B. einem Herd, erhöhen sich die durchschnittlichen Leistungen. Dadurch belasten diese Verbraucher bzw. Einspeiser die Netze in beide Energieflussrichtung stärker und erhöhen damit den Druck auf Netzertüchtigungen durch die VNB.[4] Nachfolgend beispielhaft der Gleichzeitigkeitsfaktor für Ladeinrichtungen mit unterschiedlichen Ladeleistungen, siehe Abbildung 1.

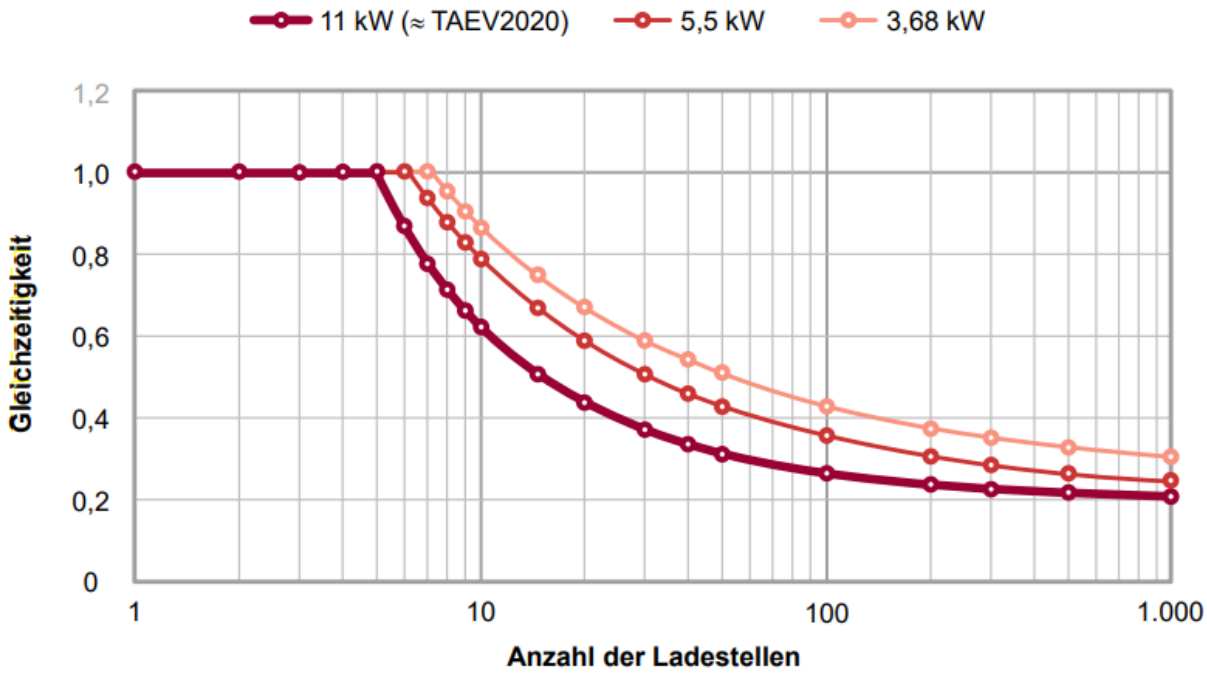

Abbildung 1: Ermittelte Gleichzeitigkeitsfaktoren für die Ladeleistungen von 11 kW, 5,5 kW und 3,68 kW (Oesterreichs Energie, 2020)

Zur Glättung dieser Leistungsspitzen können Netzbenutzer bei entsprechenden netztariflichen Anreizen einen Beitrag leisten und sollten deshalb stärker einbezogen werden. Durch netzdienliches Verhalten der Netzbenutzer können die Leistungsspitzen gedämpft, die vorhandenen Kapazitäten optimaler ausgelastet, und mehr Verbraucher und Einspeiser angeschlossen werden.[5] Durch die Nutzung von Flexibilitätspotenzialen von Ladeeinrichtungen oder Wärmepumpen kann ein netzdienlicher Betrieb der Anlagen sichergestellt werden, der zu einer Glättung der Lastprofile

[4] Vgl. (Kathan, J.;, 2019)

[5] Vgl. (Agora Verkehrswende, 2019)

führt. Darüber hinaus wird die Nutzung von Synergien mit intermittierenden erneuerbaren Energiequellen (Wind, Photovoltaik (PV)) und Speichern (Batterien) in der Stromerzeugung ermöglicht.[6]

B.3 Herausforderungen für die Verteilernetzbetreiber (VNB)

Die VNB in Österreich stellen eine durch die Dekarbonisierung des Energiesystems bedingte dynamische Erhöhung des Spitzenleistungsbedarfs auf Haushaltsebene fest, der zu Lasten der Netzkapazitäten geht. Diese schwinden rasch und ein schneller konventioneller Netzausbau wird durch Lieferengpässen bei der Primärtechnik (Kabel, Trafos) zunehmend zu einer Herausforderung. Darüber hinaus sind derzeit Netzkapazitäten wegen mangelnder Verfügbarkeit von Messdaten in den Niederspannungsnetzen (NE 6 und 7) nicht verlässlich ermittelbar. Doch gerade derartige Messdaten sind unabdingbar um Netzengpässe treffsicher zu ermitteln und somit für die Umsetzung einer *Digitalen Schnittstelle* dringend notwendig.

In einzelnen Regionen stoßen die Verteilernetze bereits heute an ihre Kapazitätsgrenzen, da der Netzausbau, die Digitalisierung sowie flankierende Maßnahmen zur Optimierung der Nutzung der Netzkapazitäten mit dem Tempo der fortschreitenden Elektrifizierung in der Mobilität, Wärmebereitstellung und dem Ausbau der dezentralen Stromerzeugung nicht mehr Schritt halten können, siehe nachfolgende Abbildungen.

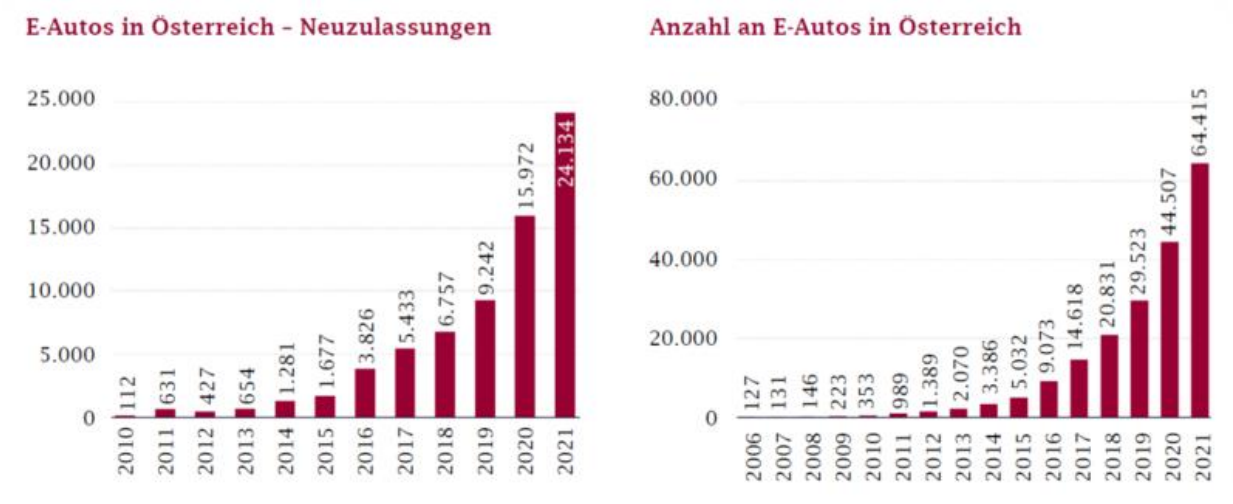

Abbildung 2: Neuzulassungen und Anzahl an Elektroautos in Österreich (Statistik Austria, 2022)

Die Europäische Union hat beschlossen die CO2-Emissionen von neuen PKW bis 2030 auf 37,5% zu senken. Um dieses Ziel in Österreich zu erreichen, muss der Anteil an Elektroautos in

[6] Vgl. (Kepplinger, P; Fässler, B.; Huber, G.; M.A.S.T, Ireshika; Rheinberger, K.; Preißinger, M.;, 2020)

diesem Mobilitätsszenario im Jahr 2030 bei 27,1% und im Jahr 2050 bei 100%, siehe nachfolgende Abbildung 2 und Abbildung 3.

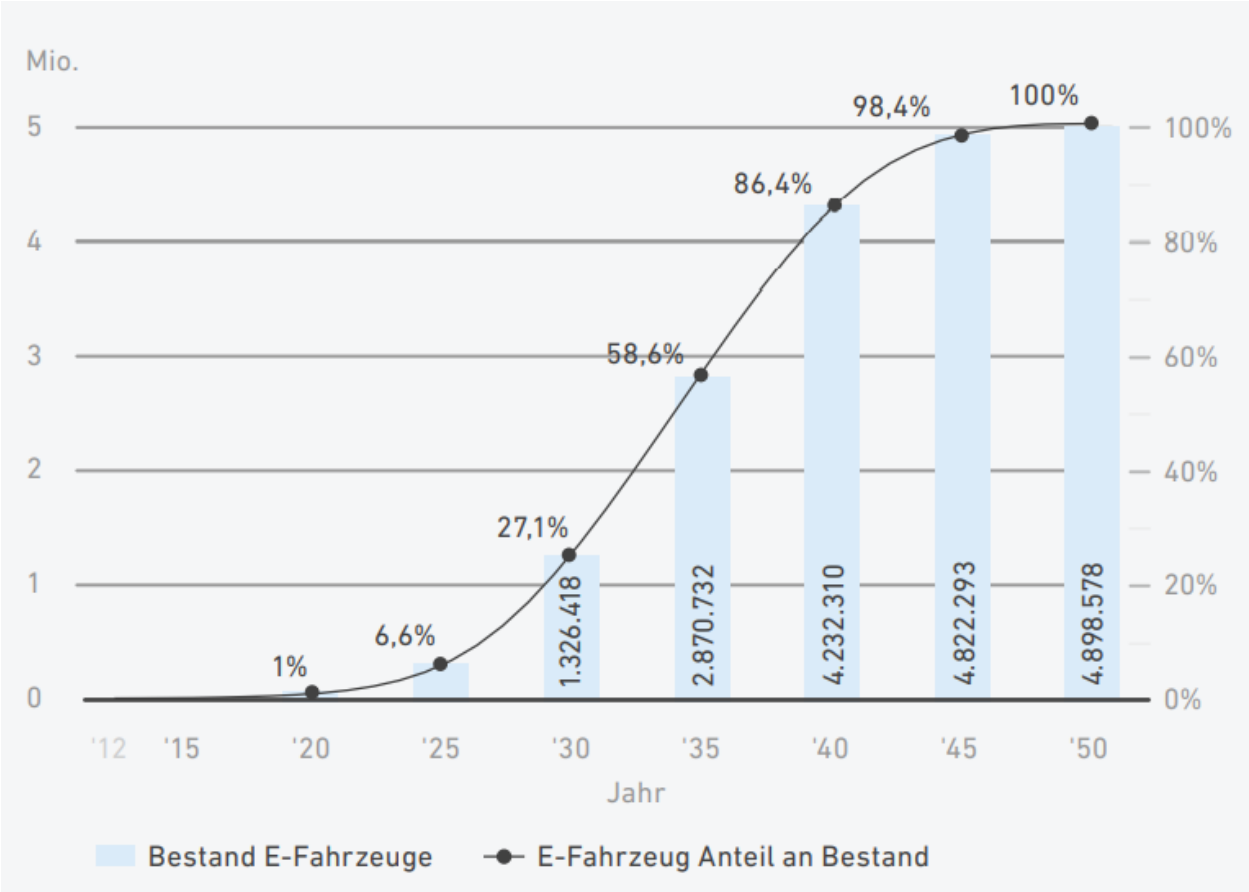

Abbildung 3: Prognostizierte Entwicklung des E-Fahrzeugbestandes in Österreich bis 2050 (Oesterreichs Energie, 2020)

Ein steigender Strombedarf aufgrund der Verbreitung der Elektromobilität führt zu zusätzlichem Kapazitätsbedarf im Verteilernetz. Bei einer flächendeckenden Integration von Elektroautos müssen bis 2040 ca. 40% der Netze verstärkt werden.[7]

[7] Vgl. (Forschungsgesellschaft für Energiewirtschaft FfE, 2022)

Nachfolgende Abbildung 4 und Abbildung 5 beschreiben den Zubau von Wärmepumpen und Photovoltaikanlagen.

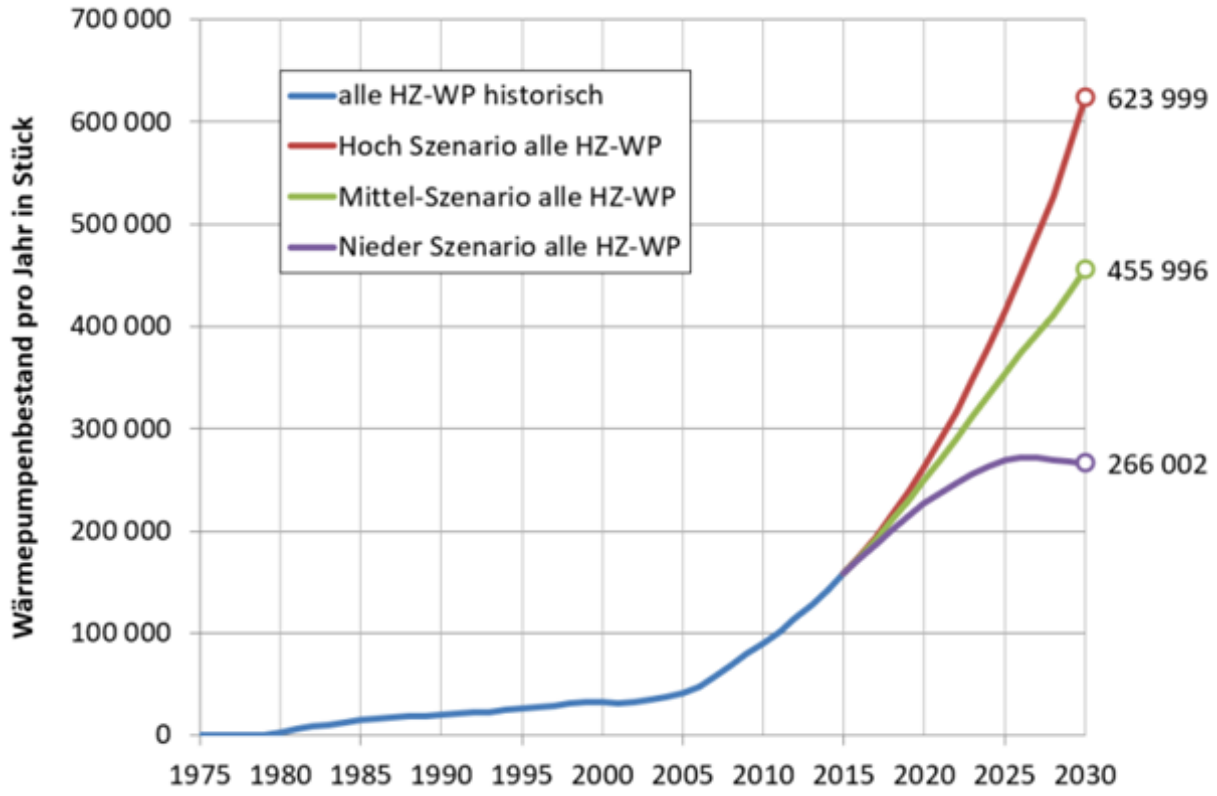

Abbildung 4: Historischer Bestand an Wärmepumpen in Österreich und Szenarien bis 2030 (Bundesministerium für Verkehr, Innovation und Technologie, 05-12-2022)

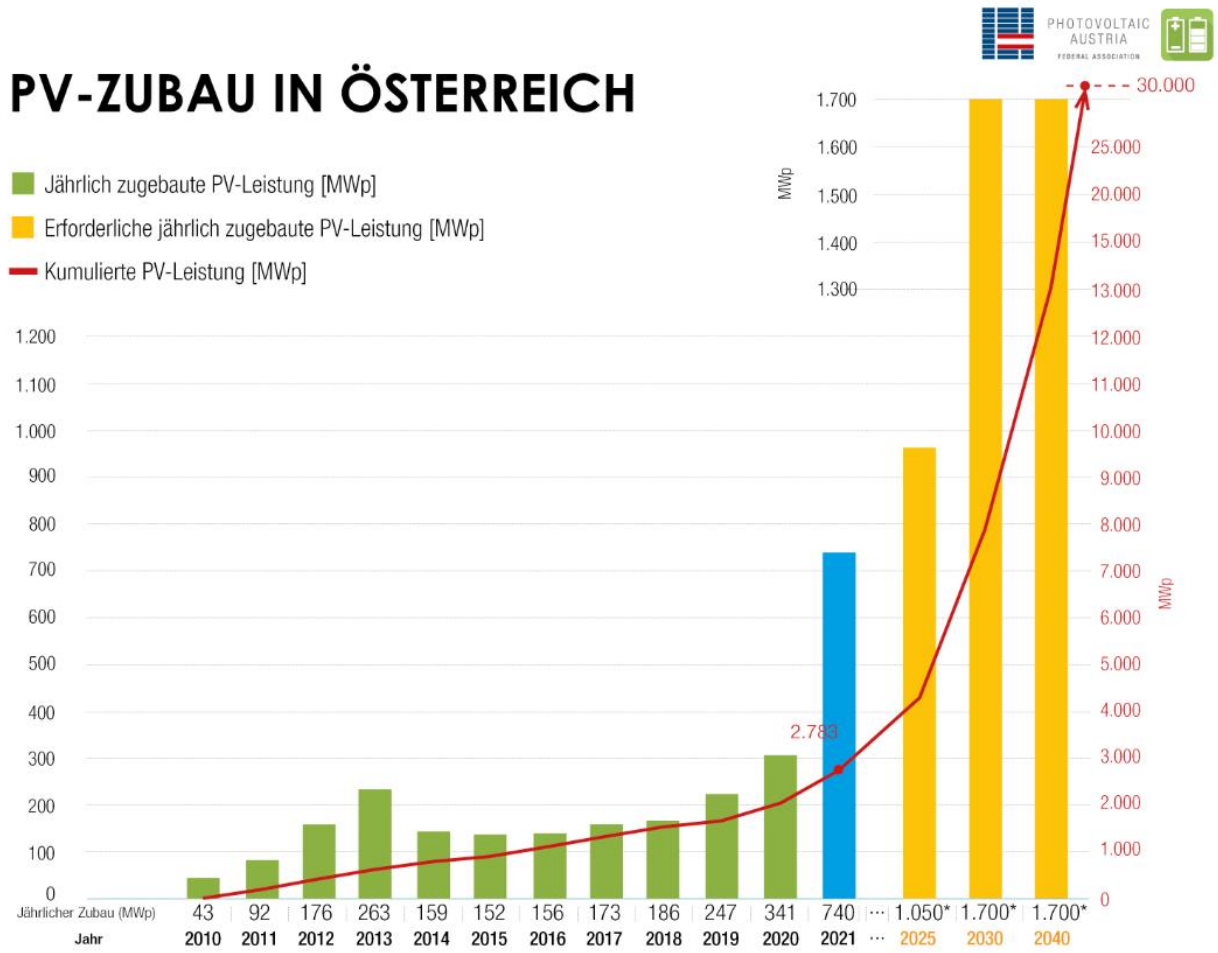

Abbildung 5: Jährlicher PV-Zubau in Österreich und kumulierte Leistung bis 2040(PV Austria, 2022), (Bundesminsterium für Klimaschutz, Umwelt, Energie, 2022)

Die für den Zubau von Ladeeinrichtungen, PV und Wärmepumpen notwendigen Netzverstärkungen können aufgrund äußerer Einflüsse wie z.B. langfristiger Genehmigungsverfahren und fehlenden Grundstücken oft nicht zeitgerecht durchgeführt werden. Zusätzlich verzögern in der jüngeren Vergangenheit pandemie- und kriegsbedingt zu Lieferengpässen diverser Betriebsmittel (z.B. Trafos, Niederspannungskabel) den Netzausbau zusätzlich. Aus diesem Grund kann der Netzausbau mit dem notwendigen Leistungsbedarf derzeit nicht Schritt halten.

Wie in der Studie „Netzberechnungen Österreich“[8] beschrieben, fallen für Österreich schon bis 2030 zu den Regelinvestitionskosten von 10,6 Mrd. Euro, für das untersuchte PV-Szenario Zusatzinvestitionen in Höhe von 2,8 Mrd. Euro und für das untersuchte Elektromobilitäts-Szenario, mit einer Elektromobilitäts-Durchdringung von 30 % des Pkw-Bestands im Jahr 2030 Zusatzinvestitionen in Höhe von 4,3 Mrd. Euro an. Das entspricht einer Erhöhung der Kosten um 27% für das PV-Szenario bzw. um 41% für das Elektromobilitäts-Szenario, wobei der Ausbaubedarf für

[8] (Oesterreichs Energie, 2020)

die beiden Technologien separat ermittelt wurde. Ein kumulativer Netzausbaubedarf für beide Technologien wurde nicht behandelt. Die Investitionskosten für Österreich bezüglich Elektromobilität- und PV-Szenarien sind in Abbildung 6 dargestellt.

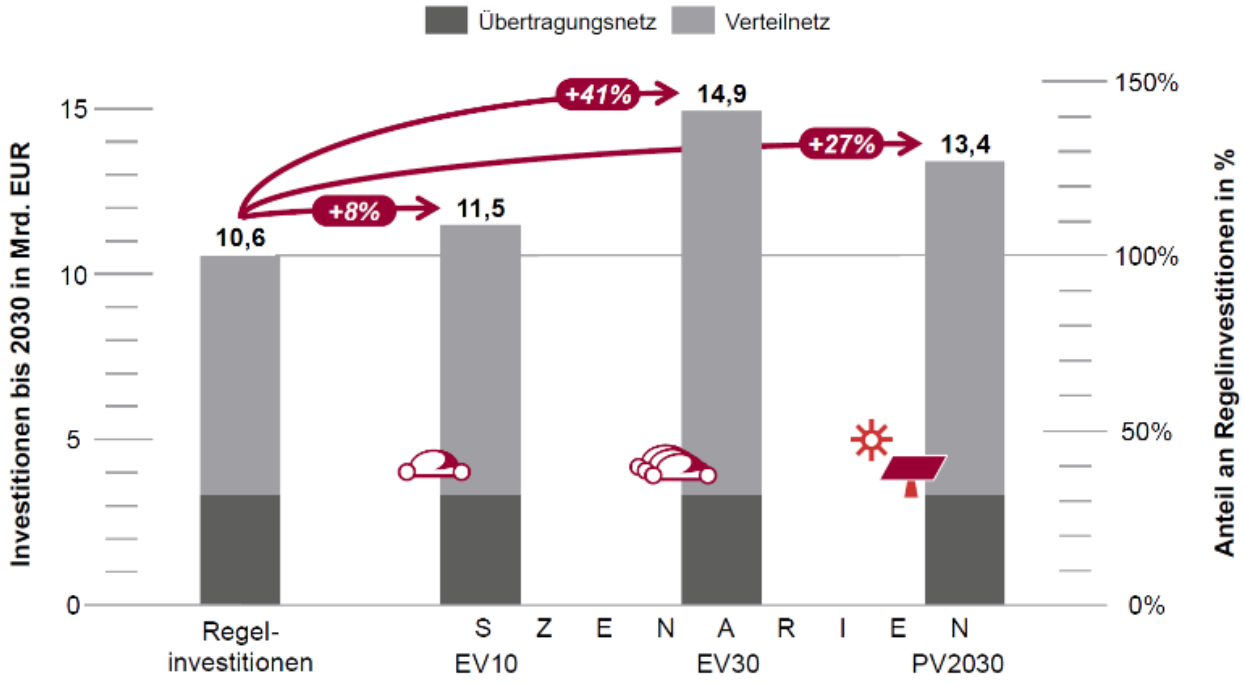

Abbildung 6: Investitionskosten für Elektromobilität- und PV-Szenarien (Oesterreichs Energie, 2020)

Diese Kosten entstehen durch folgende Maßnahmen[9]:

- notwendige Leitungsverstärkungen in der MS- und NS Ebene
- Erhöhung der Transformatornennleistungen in der NS/MS-Ebene bzw. etwaiger Zusatzkosten, durch notwendigen Neubau oder Leitungsverstärkungen in der MS-Ebene
- Verlegung von Netztrennstellen
- Neubau sowie Erweiterung bestehender MS-Schaltanlagen
- Austausch leistungsstärkerer Umspanner in der HS/MS-Ebene
- Neubau zusätzlicher Umspannwerke
- Neubau oder Leitungsverstärkungen in der HS-Ebene.

Damit wird klar, dass alle Maßnahmen zu nutzen sind, um Zeit für den Netzausbau zu gewinnen, damit dieser parallel stattfinden kann und eine Überlastung des Bestandnetzes nicht eintritt. Die dazu notwendige Leistungsvergleichmäßigung (zeitliche Verschiebung der Leistungsspitzen in bestehende Leistungstäler) gelingt nur durch Einbeziehung von Kundenanlagen. Die hohen Ladeleistungen können nur in Verbindung mit einer Lastflexibilisierung bereitgestellt werden, indem

[9] (Oesterreichs Energie, 2020)

Kunden durch zeitvariable Netztarife zu netzdienlichen Laden angeregt werden. Mit einem gesteuerten Laden (Verschiebung des Ladevorgangs während der Standzeit) kann im Vergleich zu ungesteuerten Laden der Netzausbau deutlich reduziert werden, siehe nachfolgende Abbildung 7.[10]

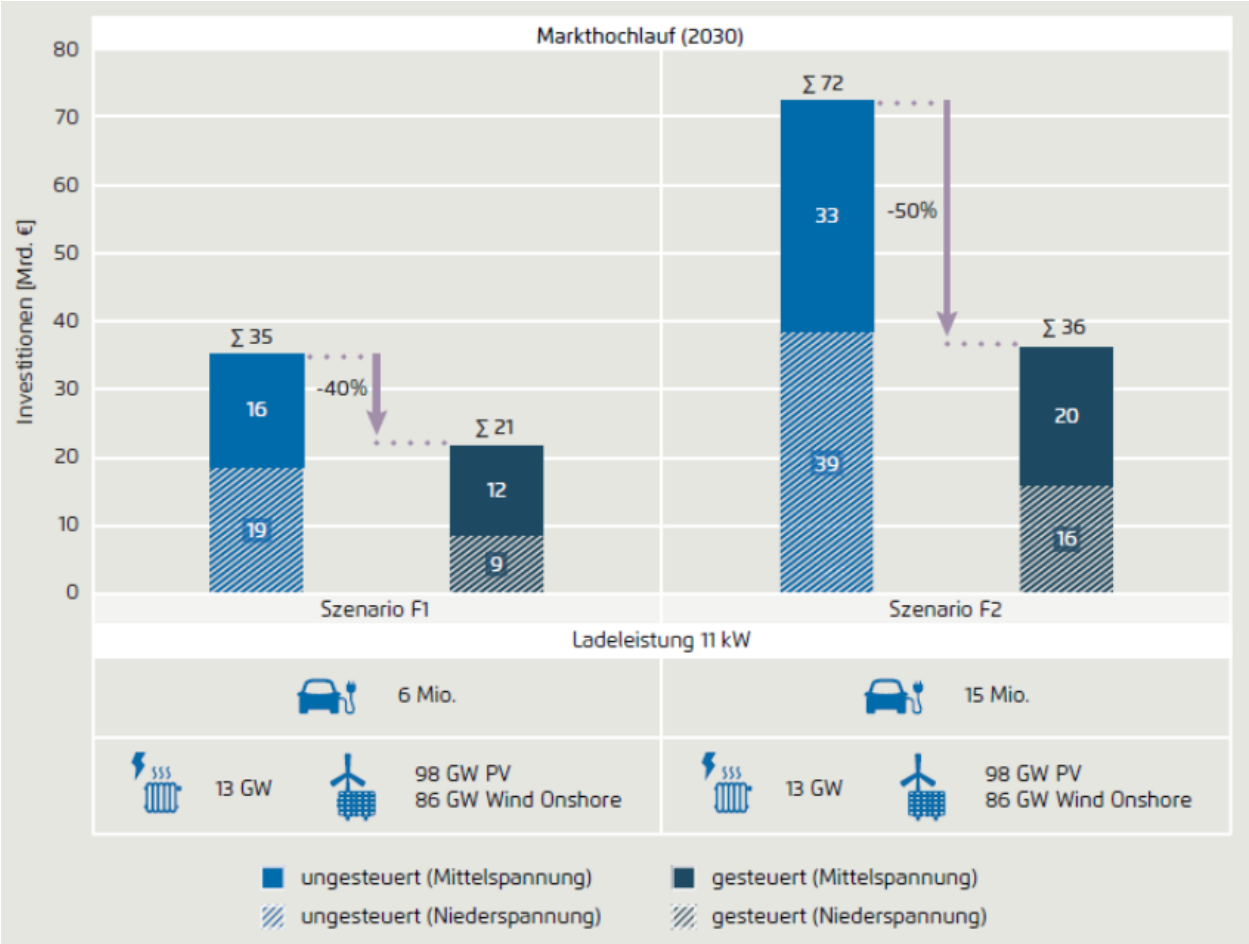

Abbildung 7: Reduktion des Investitionsbedarfs in deutsche Verteilernetze durch gesteuertes Laden (Agora Verkehrswende, 2019)

Für eine *Digitale Schnittstelle* ist eine technische Kommunikation zwischen den Systempartnern VNB und Kundenanlage notwendig. Die bisher für Steuerungseingriffe in Verteilernetzen eingesetzte Rundsteuerung erfüllt nicht die aktuellen Anforderungen, weil zunehmend selektiv auf Netzengpässe reagiert werden muss und für eine intelligente und zielgerichtete Steuerung eine bidirektionale Kommunikation erforderlich ist. Demnach sind im Rahmen der notwendigen Digitalisierung des Energiesystems “zukunftsfitte” Lösungen zu entwickeln. Damit erhöhen sich die

[10] Vgl. (Agora Verkehrswende, 2019)

Ansprüche an die Kommunikations- und Steuerungstechniken und es ergibt sich die Notwendigkeit einer Schnittstelle zur digitalen Ansteuerung von netzrelevanten steuerbaren Verbrauchseinheiten.

C. Zielsetzung, Fragestellung

Die Projektphase 1 startete am 20 April 2022 und endete am 7. Dezember 2022. Die Zielsetzung der Schaffung einer Entscheidungsgrundlage für die Einführung einer *Digitalen Schnittstelle* war in mehreren Phasen zu erarbeiten. Entsprechend sind in diesem Bericht die allgemeinen Ziele, Nicht-Ziele des Gesamtprojekts und die Ergebnisse der ersten Phase dokumentiert.

C.1 Ziele, Nicht-Ziele

Die nachfolgenden Punkte beschreiben die Ziele und Nicht-Ziele des Gesamtprojekts, die der Projektphase 1.0 als Leitfaden dienten und im Projekt bearbeitet wurden.

Ziele Phase 1 (2022)

- Eine zukunftssichere massenrolloutfähige *Digitale Schnittstelle* zwischen VNB und Kundenanlage für die Anbindung steuerbarer elektrischer Einrichtungen ist vom Projektteam funktional inhaltlich beschrieben, bei der der bidirektionale Informationsaustausch gewährleistet ist
- Geeignete Standards und Protokolle für eine *Digitale Schnittstelle* (lokale und zentrale Schnittstelle) sind objektiv evaluiert
- Der Haupt-Use Case „Notzustand“ ist beschrieben
- Use Cases für verschiedene Anwendungsfälle sind beschrieben, welche sich von der „Ausgangslage“ gem. Kapitel B ableiten
- Die infrage kommenden Architekturvarianten sind sowohl in Gegenüberstellung zur Erfüllbarkeit der technischen Rahmenbedingungen als auch in Bezug auf die Use Cases vom Projektteam evaluiert
- Die notwendigen IT-Security Anforderungen für die Architekturvarianten sind evaluiert bzw. zu klärende Aspekte spezifiziert
- Eine funktionale Weiterentwicklung der *Digitalen Schnittstelle* muss laufend möglich sein, um für zusätzliche Funktionen und Anwendungen offen zu bleiben
- Die *Digitale Schnittstelle* berücksichtigt die Anforderungen von Photovoltaik-Anlagen, elektrischen Speichern, Wärmepumpen, sowie Ladeeinrichtungen der Elektromobilität und deren Kombination (Prosumer-Haushalt)
- Der Betrieb der digitalen Schnittstelle sieht eine Leistungsvorgabe für einzelne Komponenten oder eine Kundenanlage bzw. ein Energiemanagementsystem (EMS) vor
- Rechtliche und regulatorische Lücken für eine Umsetzung einer *Digitalen Schnittstelle* sind beschrieben und Formulierungsvorschläge für Anpassungen der relevanten Regelwerke und Rechtsdokumente sind dokumentiert (keine rechtliche Umsetzung)
- Abgrenzung zwischen einer Steuerung in einem Notzustand durch den VNB und einer freiwilligen Ansteuerung ist beschrieben
- Beschreibung möglicher Anreize einer *Digitalen Schnittstelle* für den Kunden

- Alle erarbeiteten Ergebnisse des Endberichts der Projektphase 1.0 sind als Zwischenergebnisse des aktuellen Projektteams sowie als Momentaufnahme, entsprechend dem Bearbeitungsstand zu Redaktionsschluss, zu lesen und beinhalten offene Diskussionspunkte sowie fortführenden Evaluierungs- und Definitionsbedarf. Der Detaillierungsgrad ist dabei für eine Weiterführung 2023 ff auch mit anderen Akteuren geeignet, wobei die bestehenden Stakeholdergruppen bei weiterführenden Projektphasen miteinbezogen werden.

Nicht-Ziele Phase 1 (2022)

- Festlegungen oder Definition einer Hardware
- Genaue Verortung des Verantwortungsüberganges zwischen VNB und Netzkunde (Hausanschluss, im Zählerverteiler, im Endgerät)
- Festlegung des technischen Kommunikationsweges (z.B. LTE, GSM)
- Generierung von Steuerungssignalen und Algorithmen im System des VNB
- Ausarbeitung einer Logik bzw. Algorithmus zur Ansteuerung von Komponenten oder EMS
- Ausarbeitung / Diskussion von Netztarifmodellen
- Rechtliche Umsetzung einer digitalen Schnittstelle
- Definition eines Ampelmodells
- Technische Anbindung des Smart Meters zur Auslesung der Smart-Meter Daten
- Ausarbeitung / Diskussion von Beispielen für Netzanschlussverträge mit VNB-Steuerungsoptionen
- Entwicklung eines neuen Kommunikationsstandards nur für Österreich
- Konkrete Ausgestaltung von potenziellen Geschäftsmodellen von Stakeholder-Gruppen
- Koordination der geschäftlichen Interessen von Stakeholdern untereinander

C.2 Zielgruppe

Die *Digitale Schnittstelle* richtet sich vor allem an nachfolgende Stakeholder: (Liste nicht abschließend)

a) Politik
b) Regulierungsbehörde
c) Wissenschaftliche Partner
d) Normung/Standardisierung
e) VNB-Strom
f) Handel und Vertrieb Strom
g) Erzeuger
h) Wärmepumpenhersteller
i) Ladeeinrichtungshersteller (stationäre und mobile Ladeeinrichtungen)
j) Ladeeinrichtungsbetreiber
k) Hersteller von Photovoltaik Wechselrichtern und Speichern

l) Aggregatoren
m) Lösungsanbieter für Telekommunikation
n) IT Security Firmen
o) Fahrzeughersteller (OEM)
p) Industriehersteller von Steuerungseinrichtungen
q) Lösungsanbieter für Energiegemeinschaften
r) Hersteller von Industrieprodukten

D. Prozessbeschreibung

Die Initiative zum Projekt wurde am 16.12.2021 durch die Sparte Netze der Interessensvertretung Oesterreichs Energie mit dem Ziel initiiert, einen Ansatz für eine breit abgestimmte *Digitale Schnittstelle* zu entwerfen. Über Einladung der Sparte Netze versammelten sich bis zum Kickoff am 20.04.2022 Experten aus den verschiedensten Bereichen (z.B. VNB, CPO, Lieferanten, Industrie, Energiehandel, Wissenschaft) und erarbeiten in mehreren Arbeitsgruppen notwendige Anforderungen und Lösungsansätze. Die vollständige Liste der Teilnehmer:innen siehe Anhang J.1.

Das Projekt hat Herr Reinhard Nenning (vorarlberg netz, Leiter des Arbeitskreises Verteilernetze) geleitet. Die Projektassistenz seitens Oesterreichs Energie hat Herr Karl Scheida übernommen.

Arbeitsgruppen

Arbeitsgruppen	**Bezeichnung**	**Leitung**	**Bezeichnung**
AG 1	Aggregatoren	Alexander Schenk	Siemens
AG 2	Wärmepumpen	Richard Freimüller	Wärmepumpe Austria
AG 3	VNB	Reinhard Nenning	vorarlberg netz
AG 4	Regularien, Recht	Lukas Schober	vorarlberg netz
Red.	Redaktionsteam	Lukas Schober	vorarlberg netz
IT	IT-Experten	Reinhard Nenning	vorarlberg netz

Für allfällige Schwierigkeiten im Projektablauf wurde ein Kernteam eingerichtet, das von Reinhard Nenning geleitet wurde.

Kernteam	**Bezeichnung**
Fabian Bouda	TU Wien
Vera Fahrnberger	Oesterreichs Energie
Richard Freimüller	Wärmepumpe Austria
Reinhard Nenning	vorarlberg netz
Alexander Schenk	Siemens
Lukas Schober	vorarlberg netz

Die Erarbeitung der Ergebnisse erfolgte konsensorientiert und sie wurden in der Redaktion im Ergebnisbericht eingearbeitet, wo sie inhaltlich von den Arbeitsgruppenleitern verantwortet wurden. Im Bericht wurden neben dem Haupt-Use Case „Notzustand“ auch die fünf weiteren Zusatz-Use Cases eingearbeitet.

D.1 Arbeitsablauf

Nachfolgende Abbildung 8 beschreibt in 4 Schritten die Vorgehensweise zur Ermittlung der Ergebnisse.

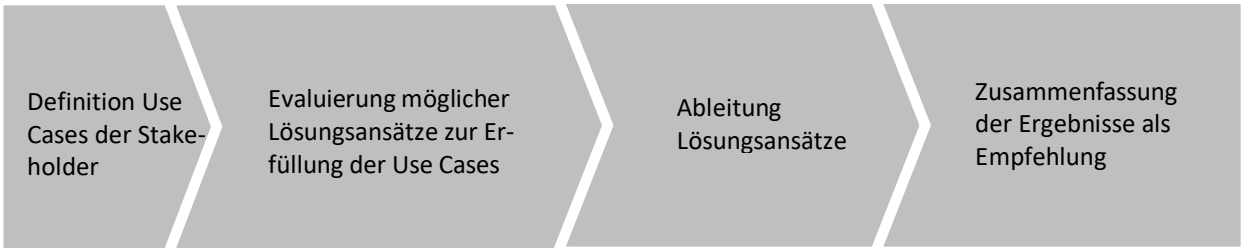

Abbildung 8: Arbeitsablauf – EP Digitale Schnittstelle

D.2 Zeitplan

Das Projekt *Digitale Schnittstelle* Phase 1 wurde am wurde am 20.04.2022 mit einem Kick-Off gestartet und am 7. Dezember 2022 abgeschlossen. Nachfolgende Abbildung 9 zeigt den durchgeführten Zeitplan von Phase I.

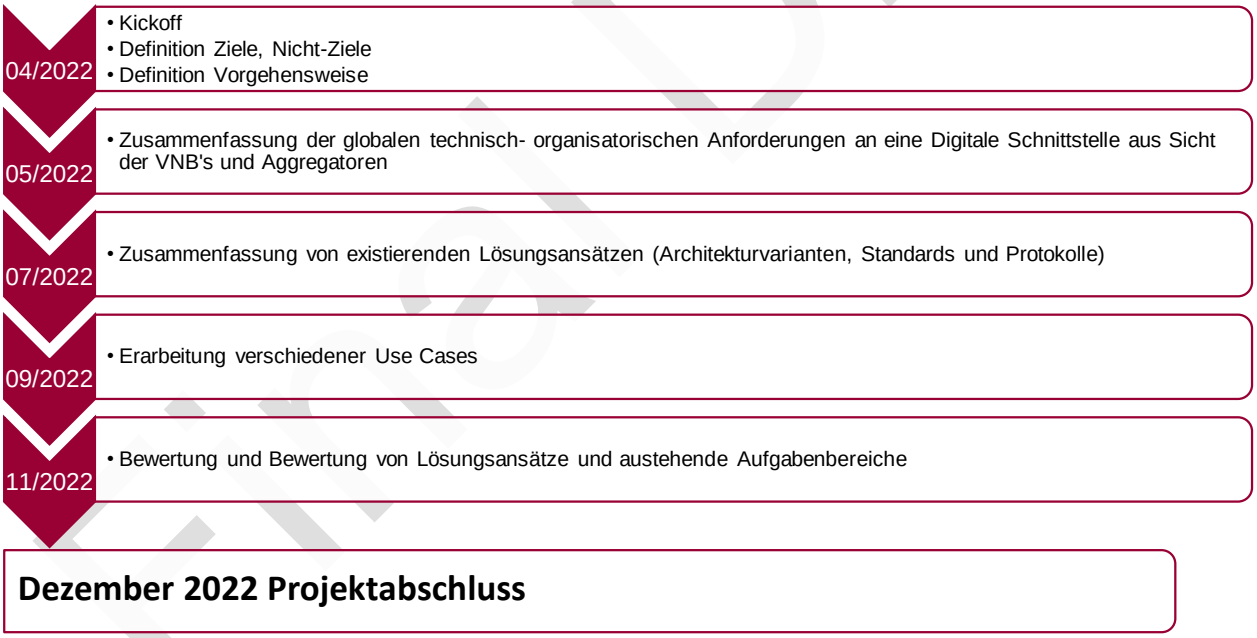

Abbildung 9: Zeitplan EP Digitale Schnittstelle

E. Technische Kommunikationsschnittstellen

E.1 Ausprägung von Architekturvarianten

In der Vergangenheit und bis heute erfolgten technische Steuerungseingriffe vom Verteilernetzbetreiber zu Kundenanlagen im Niederspannungsnetz lediglich unidirektional z.B. durch eine Rundsteuerung oder einen Schaltkontakt eines Smart Meters.

Für eine zukunftssichere Kommunikation zwischen VNB und Netzkunden ist eine bidirektionale *Digitale Schnittstelle* erforderlich, die den Austausch von Mess-, Steuer- und Kundeninformation ermöglicht. Bei der Umsetzung muss die Informationssicherheit (z.B. NIS-Gesetz, DSGVO) berücksichtigt werden.

Damit die VNB die Netzinfrastruktur effizienter nutzen kann, müssen bei Netzengpässen durch Flexibilitätsabrufe bei den Kundenanlagen Lasten und Erzeugungsanlagen entsprechend Leistungsvorgaben durchgeführt werden. Dafür ist eine Digitale Schnittstelle erforderlich, die aus Sicht der VNB eine Übermittlung von Informationen und Leistungsvorgaben an die Kundenanlage und die Übertragung von Messwerten in die Gegenrichtung erlaubt. Die Leistungsvorgabe durch den VNB muss von der Kundenanlage umgesetzt bzw. Grenzwert eingehalten werden. Bei der Leistungsvorgabe durch den VNB kann es sich im regelungstechnischen Sinn um eine Steuerung ohne Rückführung von Messwerten oder eine Regelung mit geschlossener Regelschleife handeln.

E.2 Der Schaltkontakt und die Rundsteuerung

Der von den VNB in A-CH-CZ im Frühjahr 2021 mit den Herstellern von Ladeeinrichtungen und in der Schweiz bereits umgesetzte potenzialfreie Schaltkontakt, ist eine einfache, rasch umsetzbare Maßnahme zur Behebung von Netzengpässen, die auch bezüglich IT-Security anspruchslos ist, sofern man ein Rundsteuersystem zur Ansteuerung der Kontakte verwendet. Zur Beherrschung von Lastspitzen ist der Schaltkontakt unter gewissen Voraussetzungen eine wirksame Ersthilfemöglichkeit für Netzstabilisierung, wenn der lokale VNB über ein Rundsteuerungssystem oder über Schaltuhren verfügt. Im Hinblick auf die beträchtliche Anzahl kleiner VNB, die noch mit einem Rundsteuerungssystem arbeiten, kann ein Schaltkontakt eine niedrige Umsetzungshürde haben. Ein Schaltkontakt bietet erstmalig bei den Ladeeinrichtungen eine standardisierte Ansteuerungsmöglichkeit. Ein Rundsteuersystem kann dabei eine verlässliche und verzögerungsfreie Signalübertragung ermöglichen.

Der Schaltkontakt hat im Vergleich zu einer *Digitale Schnittstelle* jedoch auch relevante Nachteile. Bei einem Schaltkontakt ist kein Rückkanal vorhanden, der über das Ergebnis einer Ansteuerungsmaßnahme oder Informationen zum Betriebszustand der Anlage Auskunft gibt. Des Weiteren ist am Beispiel von Ladeeinrichtungen für Elektroautos eine Verdrahtung vom Zählerverteiler hin zur Ladeeinrichtung erforderlich, die leicht manipuliert werden kann, um eine Ansteuerung zu

verhindern. Der Schaltkontakt wird derzeit auch bei Wärmepumpen mit unterbrechbarem Tarif angewendet, um zu bestimmten Zeiten die Leistung zu unterbrechen. Auch bei Wärmepumpen ist zukünftig eine *Digitale Schnittstelle* notwendig, um die Wärmepumpen flexibler betreiben zu können.

Da es sowohl bei einer Rundsteuerungslösung wie auch einer Digitalen Schnittstelle noch keine national etablierten technischen Standards für eine Komponentenansteuerung gibt, haben nur wenige Hersteller einen Schaltkontakt in den Komponenten eingebaut. Für die Nutzung von verschiedenen Flexibilitäten hat der Schaltkontakt im Vergleich zu einer digitalen Schnittstelle bezüglich der Steuerungsoptionen nur eingeschränkte Möglichkeiten. Der Schaltkontakt bietet eine erste einfache Ansteuerungsmöglichkeit, ist jedoch für die Nutzung zukünftiger Flexibilitäten und netzdienlicher Ansteuerungen langfristig nicht zielführend.

E.3 Herausforderungen einer Digitalen Schnittstelle

Die *Digitale Schnittstelle* ist in Gegenüberstellung zu Schaltkontakten eine wesentlich flexiblere und damit zukunftsfähigere Lösung und bietet Übertragungs- und Verteilernetzbetreibern neue Möglichkeiten für die Aufrechterhaltung der Versorgungsqualität. Die wesentlichen Herausforderungen für die Einführung einer *Digitalen Schnittstelle* in Österreich in ihren verschiedenen Ausprägungen können in einem D-A-CH Vergleich, wie folgt, zusammengefasst werden:

Regulatorische und rechtliche Herausforderungen:

- Rechtlich und regulatorisch Rahmenbedingungen für die Nutzung von Flexibilitäten sind in Deutschland (Energiewirtschaftsgesetz EnWG §14a) und in der Schweiz (im Stromversorgungsgesetz und in den Werkvorschriften) bereits geregelt, in Österreich (ElWOG) müssen diese Rahmenbedingungen noch geschaffen werden.
- Die Rollenverteilung und Verantwortlichkeiten bezüglich Leistungsvorgaben und Informationspflicht des VNB im Zusammenspiel mit Netzkund:innen und anderen Marktpartnern muss geklärt werden
- Es müssen Rahmenbedingungen für die Bereitstellung der erforderlichen Kommunikationsverbindung geschaffen werden.
- Die Kostentragung bzw. Kostenübernahme für Kommunikation, erforderliche Geräte und deren Installation und Wartung ist nicht geklärt
- Für die Umsetzung einer digitalen Schnittstelle sind standardisierte Betriebsprozess zu etablieren und zwischen VNB und Netzkund:innen vertraglich zu regeln. Es ist sinnvoll, die Möglichkeit vorzusehen, dass Netzkund:innen auch Dritte (z.B. Aggregatoren) mit der Abwicklung der Betriebsprozesse beauftragen können
- Rechtliche Ausgestaltung einer Ansteuerung in „Notsituation“ und einer freiwilligen Ansteuerung

- Sämtliche rechtlichen und regulatorischen Rahmenbedingungen zusammengenommen müssen alle genannten offenen Punkte so regeln, dass für Netzkunden ein nachvollziehbarer signifikanter Nutzen entsteht. Erst damit kann die notwendige große Nachfrage nach Netzzugangsverträgen mit Steuerungsoption für den VNB sichergestellt und die mit der digitalen Schnittstelle verbundenen Ziele über die Skalierung erreicht werden.

Solange hier von Politik und Regulator keine Klarstellungen bezüglich einer Ansteuerung im Notzustand und der Nutzung von Flexibilitäten Art. 32 RL (EU) 2019/944 erfolgt sind, ist eine frühzeitige technische Entwicklung durch Industriepartner nicht zu erwarten. Damit werden hier rasche Entscheidungen zum Schlüssel für einen Erfolg in Bezug auf

- eine zeitgerechte Umsetzung der Energiewende und damit verbunden auch eine Ausweitung des bestehenden Basisgeschäfts der Marktpartner im Energiesystem sowie die Schaffung neuer Geschäftssegmente und die Entwicklung neuer Angebote, speziell im Bereich der Dienstleistungen,
- die Sicherstellung der Versorgungsqualität auch in der Zukunft.

Herausforderungen der Sensorik und Erfassung des Netzzustandes:

Um eine *Digitale Schnittstelle* bedienen zu können, muss ein VNB ein geeignetes Steuerungssystem aufbauen, das folgende wesentliche Merkmale aufweist:

- Der VNB muss die Netzzustände im Verteilernetz laufend messtechnisch erfassen und bewerten. Dazu sind Messdaten von Sensoren und Smart Metern erforderlich.
- Erkennt der VNB drohende Netzengpässe werden Netzausbaumaßnehmen erforderlich. Nimmt man die Existenz einer *Digitale Schnittstelle* vorweg, dann wird in Zukunft der Netzausbau aus einer wirtschaftlichen Kombination aus einem Ausbau intelligenter Komponenten und Kupferinfrastruktur bestehen. Die intelligenten Komponenten können im laufenden Betrieb aktuell auftretende Netzengpässe feststellen und im Zusammenspiel mit einem IT-System zur Administration von Netzzugangsverträgen geeignete Steuerungsmaßnahmen bei Netzkunden mit VNB-Steuerungsoption festlegen. Diese werden dann über Aggregatoren oder den VNB selbst zur Umsetzung an die betreffenden Kundenanlagen übergeben.

  Im Falle netzkritischer Zustände muss der VNB transparent auf vorab mit dem Dienstleister vereinbarte „Phasen der Netzstabilität“ referenzieren (Notzustand, Kapitel G.2.2).

Herausforderungen der Kommunikation:

- Die *Digitale Schnittstelle* muss bei möglichst viele Netzkunden mit einem netzdienlichen Vorteil kommunikationstechnisch an ein VNB-Steuerungssystem angebunden werden können.

Die konkreten Anforderungen an solche Kommunikationsverbindungen müssen in einer zweiten Phase (anschließend an dieses Projekt) nach Festlegen der Betriebsprozesse und Security-Anforderungen und auf Basis der Lösungsevaluierung aus diesem Projekt festgelegt und spezifiziert werden. Aus heutiger Sicht werden hier Lösungen für alle 3 Varianten der Kommunikationsarchitektur gemäß Kapitel F.2 festzulegen sein.

- Der VNB muss erforderlich werdende temporäre Leistungsbegrenzungen pro Zählpunkt / Netzanschlusspunkt und übermitteln, diese entweder über einen beauftragten Dritten oder selbst an die betroffenen Netzkunden. Für die Einhaltung dieser Leistungsvorgaben ist der Netzkunde als Vertragspartner des VNB verantwortlich. Der VNB muss den Netzkunden oder ggf. sein beauftragter Dienstleister frühzeitig informieren, sofern dies technisch möglich und planbar ist.
- Das Zusammenspiel der Vielfalt an nicht interoperablen Protokollen und Kommunikations-Standards.

Wirtschaftliche Herausforderungen:

- Für eine Umsetzung einer *Digitale Schnittstelle* müssen auf VNB Seite dauerhaft genügend finanzielle und personelle Ressourcen (Lehrlinge, Fachkräfte, Ausbilder:innen, etc.) bereitgestellt werden. Aufgrund der aktuell knappen Ressourcen müssen dafür Kapazitäten geschaffen werden
- Ein flächendeckender Einsatz der *Digitalen Schnittstelle* muss effizient und im richtigen Ausmaß zwischen Netzverstärkung und Flexibilitätsnutzung erfolgen.
- Die Industrie kann bei Vorliegen konkreter Spezifikationen und einer entsprechenden nachvollziehbaren Marktperspektive Produkte entwickeln, und in Folge Lösungen liefern. Der Zeithorizont dafür wird nicht nur durch die Komplexität der zu schaffenden Lösungen, sondern auch von der Verfügbarkeit von Elektronikkomponenten und Bauteilen abhängen.

E.4 Möglichkeiten einer *Digitalen Schnittstelle*

Die Möglichkeiten und Anwendungen für eine *Digitale Schnittstelle* sind vielfältig und zukunftsweisend. Neben der Nutzung einer Digitalen Schnittstelle durch VNB besteht ihr wesentlicher Vorteil darin, dass verschiedenste Stakeholder (z.B. Lieferanten, CPOs, Aggregatoren) Dienstleistungen für Netzkund:innen anbieten können. Durch einen laufenden Informationsaustausch mit Steuerungsmöglichkeit können auch kleine Flexibilitäten im Haushaltsbereich bewirtschaftet werden. Optimierungspotenziale im Haushaltsbereich können z.B. durch eine Verschneidung der erhaltenen Daten mit zusätzlichen Informationen gefunden und ausgeschöpft werden. Darüber hinaus können zusätzliche Services im Bereich des Anlagenbetriebs und der Anlagenwartung angeboten werden. Weitere Synergieeffekte bieten sich bei der Integration von Energiegemeinschaften, um mehr Energie lokal zu erzeugen sowie zu verbrauchen und den Eigenverbrauchsanteil lokal zu optimieren. Über eine *Digitale Schnittstelle* können aggregierte Flexibilitäten aus

Kundenanlagen abgerufen werden und der Aufbau von Flexibilitätsmärkten unterstützt werden. Eine *Digitale Schnittstelle* kann somit einen großen Beitrag zur optimalen Nutzung der Netzkapazitäten leisten.

F. Rahmenbedingungen für eine *Digitale Schnittstelle*

Der Netzbetreiber ist lediglich für die Signalgebung der Leistungsvorgaben anhand einer *Digitalen Schnittstelle* verantwortlich.[11] Die technischen, wirtschaftlichen und rechtlichen Rahmenbedingungen werden zwischen dem VNB und dem Netzkunden im Netzzugangsvertrag vereinbart. Für die *Digitale Schnittstelle* selbst sind in zukünftigen Projektphasen neben der technischen Umsetzung standardisierte Marktprozesse zwischen VNB und Netzbenutzer:innen zu etablieren. Dabei übernimmt ausschließlich der Dienstleister (Lieferant, Energiehandel), den vertraglich vereinbarten Kontakt zu seinen Kunden. Hierbei wird der Dienstleister über Leistungsvorgaben proaktiv und frühzeitig informiert, soweit technisch möglich und planbar. Ein Anforderungskatalog kann den Netzkunden zur Verfügung gestellt werden, in dem u.a. die Netzanschlussanträge transparent gelegt werden. Im Falle einer eintretenden netzseitigen Leistungsvorgabe sollte anhand eines Anforderungskataloges die Nachweispflicht zur erfolgten Netzzugangssteuerung anhand der Parameter österreichweiter einheitlicher Standards und definierte Fristen dokumentiert werden.

F.1 Arbeitshypothese

Für die Formulierung der technischen Rahmenbedingungen wurde von folgender Arbeitshypothese ausgegangen:

Es werden rechtliche regulatorische und technische Rahmenbedingungen geschaffen, die es VNB ermöglichen, Lasten (z.B. Ladeeinrichtungen, Wärmepumpe) und Einspeiseanlagen (z.B. Wechselrichter) gemäß noch zu definierender Regeln (Kapitel G.2) im Bereich der Kundenanlage temporäre Leistungsvorgaben vorzugeben. Damit können drohende Überlastungen von Betriebsmitteln, Wirkleistungsreduzierungen bei hoher PV-Produktion und unzulässige Systemzustände der Spannungsqualität nach Norm EN 50160 (Definition Notzustand, Kapitel G.2.2) in Verteilernetzen vermieden werden. Der Notzustand muss rechtlich definiert und die Handlungsmöglichkeiten für die Akteure im Fall des Auftretens geregelt werden. Die Leistungsvorgabe im Notzustand wird als „ultima ratio“ angesehen, die immer dann zum Einsatz kommt, wenn vorgelagerte Maßnahmen zur Verhinderung von Netzengpässen seitens anderer Marktpartner (z.B. Energielieferanten, CPOs, Aggregatoren, etc.) nicht ausreichend wirksam werden. Die hier seitens der VNB relevanten elektrischen Größen sind die elektrische Leistung (P), die Blindleistung (Q) sowie die Spannung (U), die über eine zu definierende Schnittstelle zwischen Netzkunde und VNB auszutauschen sind.

Wird seitens der VNB ein Kommunikationsnetz zwischen VNB und Kundenanlage aufgebaut, sollte dieses aus Erwägungen der Kosteneffizienz auch für eine Verwendung durch berechtigte

[11] (E-Control, 2022)

Dritte geeignet und zugänglich sein. Bezogen auf die Schnittstelle zwischen VNB und Kundenanlage bedeutet dies, dass eine flexible Erweiterung des für VNB benötigten Datenmodells mit zusätzlichen Prozessgrößen möglich sein muss.

F.2 Technische Rahmenbedingungen

Ausgehend von der Arbeitshypothese und den betrieblichen Möglichkeiten der VNB können die nachfolgenden technischen Rahmenbedingungen abgeleitet werden. **Ziel ist es die infrage kommenden Schnittstellenkonzepte gegen die Erfüllbarkeit der technischen Rahmenbedingungen und der Use Cases zu evaluieren.**

F.2.1 Betriebliche Integration

Der VNB kann erforderliche Leistungsvorgaben mit seinem technischen System meist für (eine) einzelne Komponente(n) oder pro Netzanschlusspunkt ermitteln. Erfolgt die Vorgabe auf den Netzanschlusspunkt, so muss ein Energiemanagementsystem (EMS) beim Netzkunden vorhanden sein, das die Einhaltung der Leistungsvorgabe umsetzt, wobei dessen Verortung (z.B. physisch als Hardware in der Kundeanlage, in einer Cloud oder an einer anderen Stelle) noch nicht festgelegt ist. Ein EMS übergibt Leistungsvorgaben des VNB auf mehrere lokal verfügbare und steuerbare Komponenten, unter Berücksichtigung der individuellen Bedürfnisse der Kund:innen. Eine direkte Leistungsvorgabe an mehrere Komponente(n) hinter einem Netzanschlusspunkt durch den VNB wäre zwar möglich, wird aber nicht als zweckmäßig erachtet, weil individuelle Bedürfnisse der einzelnen Kund:innen vom VNB nicht sinnvoll administriert und gewartet werden können.

F.2.2 Sicherstellung wirtschaftlichen Betriebs und langfristiger Wartbarkeit

Die Typenvielfalt der zu steuernden Komponenten ist sehr groß und kommt darüber hinaus aus unterschiedlichen Marktdomänen, wie zum Beispiel der Elektromobilität und Gebäudetechnik (Wärmepumpen, dezentrale Erzeugungsanlagen und Speicher), in denen sich zum Teil bereits unterschiedliche Standards und Protokolle etabliert haben. Diese orientieren sich naturgemäß an den jeweiligen domänenspezifischen Anforderungen.

Als Beispiel kann hier für die Domäne Elektromobilität das Open Charge Point Protocol (OCPP) genannt werden. Dieses wurde für die Anbindung von Ladestationen (Charge Points oder CPs) an ein Charge-Point-Management entwickelt und ist heute in der Version 1.6 weit verbreitet. Die praktischen Erfahrungen mit dieser Version und zusätzliche Anforderungen haben zur Weiterentwicklung von OCPP geführt, sodass mit der Version OCPP 2.1 bereits die nächste Generation dieses Protokolls in den Startlöchern steht. Zudem wächst die Nachfrage nach bidirektionalem Laden stark, welches mit dem Standard IEC63110 vermehrt an Bedeutung gewinnt. Ähnliche Entwicklungen finden sich im Bereich der intelligenten Gebäude. Hier sind weitere Protokolle wie z.B. Modbus-SunSpec und Standards wie z.B. KNX im Einsatz. Als neuer Standard steht hier der

EEBUS zur Verfügung, welches derzeit ein paar Use Cases unterstützt und fortlaufend weiterentwickelt wird. Diesem Umstand stehen nun die Anforderungen der VNB gegenüber, die wie folgt zusammengefasst werden können:

- Die VNBs benötigen eine Möglichkeit Flexibilitäten bei Erreichen der Netzgrenzen sowohl angebots- (Erzeugung) als auch nachfrageseitig (Last) abrufen zu können. Dazu sollten die entsprechenden Komponenten aus allen Domänen (z. B. Ladestationen, PV-Anlagen, Wärmepumpen, Speicher etc.) beitragen können.
- Die Flexibilitätsabrufe müssen an ein technisches System bei den Netzkunden mit entsprechendem Netzzugangsvertrag kommuniziert werden.
- Die Flexibilitätsabrufe bestehen aus einer temporären Vorgabe einer Leistungsvorgabe. Dafür ist eine digitale Kommunikationsschnittstelle erforderlich. Aus Sicht der VNBs kann eine solche *Digitale Schnittstelle* aus einer zentralen Schnittstelle bestehen, über die die Leistungsvorgaben an Dritte (Aggregatoren) zur Umsetzung über ein von ihnen betriebenes technisches System übergeben werden oder aus einer Lösung bei der ein VNB direkt mit einem technischen System bei Netzkunden kommuniziert.
- Die VNB können nur eine Leistungsgrenze pro Zählpunkt/Netzanschlusspunkt konform zu dem entsprechenden Netzanschlussvertrag ermitteln, die dann von der Kundenanlage umzusetzen ist.

Legt man die Anforderungen der VNB über das durch unterschiedliche Domänen geprägte Szenario bei den Netzkunden, dann ergibt sich die Notwendigkeit eigene VNB-Schnittstellen festlegen zu müssen, um einen sicheren Betrieb und die langfristige Wartbarkeit eines Steuerungssystems sicherstellen zu können. Diese VNB-Schnittstellen müssen von den relevanten Komponenten aus den betroffenen Domänen entsprechend unterstützt werden. Die Gründe für diese Anforderung sind:

- Die Domänen Elektromobilität und intelligente Haushalte/Gebäude inklusive Energiegemeinschaften stehen vor einer signifikanten Weiterentwicklung mit zu erwartenden kurzen Innovationszyklen. Diese haben auch Rückwirkungen auf die jeweils benötigte Kommunikation / Standards und Protokolle
- Ein VNB muss ein domänenübergreifendes Steuerungssystem langfristig wirtschaftlich und sicher nach seinen Anforderungen betreiben. Damit scheiden Lösungen in denen ein VNB domänenspezifische Standards und Protokolle in ein Steuerungssystem integriert aus, denn in diesem Fall müsste der VNB alle Innovationszyklen aus den betroffenen Domänen mitmachen. Dies ist sowohl technisch als auch administrativ in der Masse nicht möglich. International ist diese Problematik bekannt, deshalb wurden eigene Schnittstellenlösungen für die Aggregation von Flexibilität meist unter dem Titel “Demand-Response” entwickelt, und bereits als Standard oder defacto-Standard verfügbar gemacht. Diese Lösungen decken sich gut mit

den Anforderungen der VNBs und sind in der Regel rückwärtskompatibel, d. h. neue Anforderungen werden so implementiert, dass Anlagen mit einer älteren Version in einem erweiterten System ohne Änderungen weiter betrieben werden können.

Ergänzend zu der Thematik “eigene VNB-Schnittstellen für die Steuerung von Kundenanlagen” sei die Smart Grid Ready Initiative[12] in der Schweiz erwähnt. Sie wird von der Schweizer Regierung finanziert und erarbeitet eine technische Basis, wie unterschiedlichen Geräten im Haushalt, wie z. B. Ladestationen, Wärmepumpen PV-Anlagen und ähnliches, in ein gemeinsames Steuerungssystem integriert werden können. Dafür entwickeln sie Verknüpfungen für diese Geräte, die deren grundsätzliche Funktionalität abbilden. Über Vorgaben können dann die Verknüpfungen an konkret am Markt verfügbaren Geräte angepasst werden. Darüber hinaus entwickeln und warten sie Schnittstellenadapter, die die wichtigsten domänenspezifischen Standards und Protokolle in einer Entwicklungsumgebung zusammenfassen. Damit können auf einfache Art und Weise zentrale Controller bzw. Energiemanagementsysteme entwickelt und Komponenten unterschiedlicher Hersteller in ein Heimsystem integriert werden. Dieser Ansatz lässt sich natürlich auch um ein Modell für ein VNB-Steuerungssystem und einen entsprechenden VNB-Schnittstellenadapter erweitern.

F.2.3 Sicherstellung eines deterministischen Systemverhaltens in Fehlerfall

Temporäre Leistungsvorgaben an Netzkunden mit entsprechenden Netzzugangsverträgen macht, ein VNB nur dann, wenn ohne diesen Eingriff eine Überschreitung der physikalischen Grenzen der Netzinfrastruktur oder eine Nichteinhaltung der Versorgungsqualität die Folge wäre. Im Umkehrschluss bedeutet dies, dass eine Nichteinhaltung dieser Leistungsvorgaben zu einer Schädigung oder im Extremfall zu einem Ausfall von Betriebsmitteln und damit zu einer Reduktion der Netzverfügbarkeit führt. Damit muss im Zusammenhang mit einer Schnittstellenimplementierung folgende Zusatzfunktionalität bereitgestellt werden:

- Auf Netzkundenseite muss die Verfügbarkeit des steuernden VNB-Systems inklusive der Kommunikationswege laufend überprüft werden. Dafür gibt es mehrere technische Lösungen, von denen eine passende im Zuge der Spezifikation eines VNB-Schnittstellenstandards festgelegt werden muss.
- Sollte ein Systemfehler auftreten, dann muss die empfangende Instanz auf Netzkundenseite automatisch einen Default-Leistungswert als maximal mögliche Leistung aktivieren. Dieser Default-Leistungswert ist vertragsspezifisch (Netzzugangsvertrag) und muss daher vom VNB administriert und angepasst werden können. Daher muss jeder Default-Leistungswert je nach

[12] www.smartgridready.ch

Lösungskonzept bei der Erstinbetriebnahme als Parameter vorgegeben werden können und falls der Kunde seinen Netzzugangsvertrag ändert, im laufenden Betrieb angepasst werden können. Der maximal mögliche Default-Leistungswert entspricht im Regelfall jener Leistung, die vom Netz auch bei Ausfall des Steuerungssystems oder der Kommunikationsverbindungen noch innerhalb zulässiger Systembetriebsgrenzen beherrscht werden kann.

F.2.4 Kommunikationsmedien

Für die Umsetzung einer *Digitalen Schnittstelle* muss ein geeignetes Kommunikationsmedium vorhanden sein, um die notwendigen Informationen zur Ansteuerung sicher übertragen zu können. Nachfolgend findet sich eine Auflistung beispielhafter Kommunikationsmedien, die für die Bewertung der Standards und Protokolle sowie Lösungskonzepte herangezogen wurden. Eine Evaluierung der Kommunikationsmedien, muss zu einem späteren Zeitpunkt vorgenommen.

- Internet
- GPRS / LTE / 5G
- LoRaWan
- LTE 450
- PLC

F.2.5 Provisionierung, Fehlermanagement

Die Anmeldung und Parametrierung (z.B. Default-Leistung, Kommunikationsparameter, Schutzzeiten) von Komponenten durch das VNB-System (Onboarding) muss unterstützt werden. Bezogen auf die nachfolgend beschriebenen Konfigurationen bezieht sich diese Anforderung vor allem auf den Funktionsblock und für die Variante der Bereitstellung einer zentralen *Digitalen Schnittstelle* auf die zu steuernde Komponente. Darüber hinaus müssen Fehlermeldungen erfasst und übertragen werden, damit Störungen zeitgerecht behoben werden können. Die Anforderungen für die Wartung und Betriebsführung von Schnittstellen und notwendigen Systemen müssen bei der Planung und Umsetzung berücksichtigt werden.

F.2.6 Security

Gemäß §45 Elektrizitätswirtschafts- und -organisationsgesetz (ElWOG) sind die Verteilernetzbetreiber für den sicheren Betrieb des Verteilernetzes verantwortlich. Bei einer Umsetzung einer *Digitalen Schnittstelle* ist weiterhin der VNB bzw. allfälligen Dritte oder Aggregatoren für die Übertragung von Messdaten und Signalen verantwortlich. Da es sich bei Verteilernetzen um eine kritische Infrastruktur handelt, gilt in Bezug auf die Security die NIS-Richtlinie. Die Einführung einer *Digitalen Schnittstelle* verbreitert nun die potenzielle Angriffsfläche auf das Gesamtsystem des VNB, womit diesem Thema eine besondere Bedeutung zukommt. Eine sehr ähnliche, vergleichbare Problemstellung wurde österreichweit für Smart Meter Systeme bereits gelöst und vielfach erfolgreich umgesetzt.

F.2.7 Architekturvarianten

Als weitere Rahmenbedingung wurde die Evaluierung dreier Architekturvarianten vorgegeben, siehe Abbildung 10:

Übersicht Architekturvarianten:

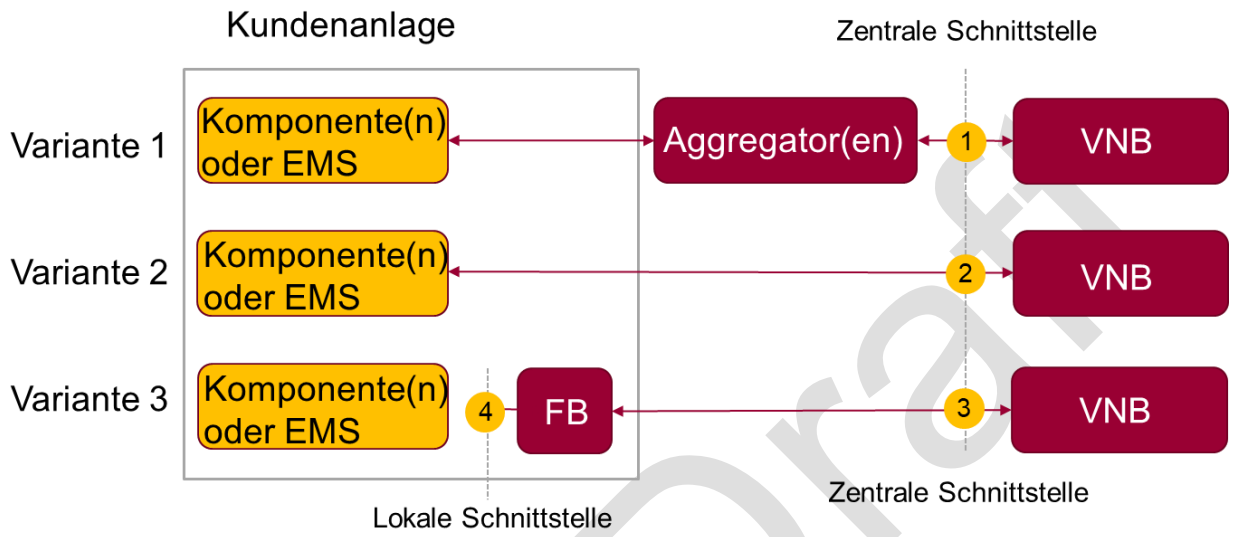

Abbildung 10: Übersicht Architekturvarianten

In Variante 1 ermittelt der VNB die erforderlichen Leistungsvorgaben pro Netzanschlusspunkt und übergibt sie über die zentrale Schnittstelle 1 einem oder mehreren Aggregator(en), der dann mit seiner technischen Infrastruktur für die Umsetzung der Leistungsvorgaben sorgt. Dabei können die Leistungsvorgaben auf eine oder mehrere Komponenten, sowie auf ein EMS erfolgen. Unter einer Komponente wird ein einzelnes Gerät (z.B. Ladeeinrichtung, Wärmepumpe, PV-Anlage) verstanden. Die sich hier ergebenden Kommunikationsbeziehungen werden im nachfolgenden Kapitel erläutert. Ein Onboarding-Prozess für Komponenten ist in dieser Variante (im Gegensatz zu den beiden anderen) für den VNB nicht erforderlich. Die NIS-Anforderungen müssen durch die technische Infrastruktur des Aggregators erfüllt werden.

In Variante 2 übermittelt der VNB die erforderlichen Leistungsvorgaben über die zentrale Schnittstelle 2 direkt auf eine oder mehrere Komponenten, sowie auf ein EMS erfolgen, wodurch sich immer eine 1:1 Kommunikationsbeziehung ergibt. Die NIS-Anforderungen müssen in der Komponente erfüllt werden.

In Variante 3 übermittelt der VNB die erforderlichen Leistungsvorgaben über die zentrale Schnittstelle 3 an ein beim Kunden definierten Funktionsblock, welcher über die lokale Schnittstelle 4 an eine oder mehrere Komponenten oder ein EMS zur Umsetzung weiterleitet. Die Variante 3 er-

möglicht eine Trennung der VNB-Security von der Security im Kundenbereich und eine Auslagerung der für die Netzverfügbarkeit erforderlichen Fall Back Funktionen in den Funktionsblock, womit sich starke Vereinfachungen für die Kommunikation mit den Komponente(n) ergeben. Auch hier ergibt sich eine 1:1 Kommunikationsbeziehung zwischen VNB und Funktionsblock sowie zwischen Funktionsblock und Komponente(n). Die NIS-Anforderungen müssen im Funktionsblock erfüllt werden, wodurch eine klare Trennung zwischen VNB und Kundenanlage geschaffen werden kann.

Zur Umsetzung der zentralen Schnittstelle bei allen drei Varianten benötigt es eine „Digitale Plattform“, welche die Koordinierungsfunktion zwischen VNB und Lieferanten, Aggregatoren bzw. Kund:innen übernimmt, um Messdaten, Leistungsvorgaben und Informationen auszutauschen.

Digitale Schnittstelle für Aggregator(en) (Variante 1)

Bei der Variante 1 wird die *Digitale Schnittstelle* über einen Aggregator ausgeführt. In dieser Variante stellt der VNB eine zentrale Schnittstelle für einen oder mehreren Aggregatoren bereit, womit sich die in der nachfolgenden Abbildung 11 dargestellten Kommunikationsbeziehungen ergeben:

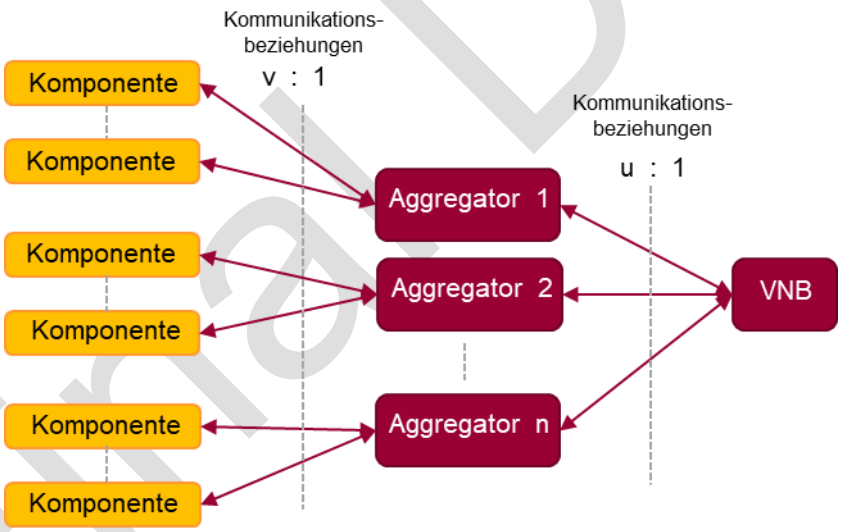

Abbildung 11: Kommunikationsbeziehung Variante 1

Der VNB ermittelt pro Netzanschlusspunkt eine Leistungsvorgabe, die er dem jeweils zuständigen Aggregator(en) zur Umsetzung über eine oder mehrere Komponenten oder einem EMS übergibt. Dabei sollten bestehende Infrastrukturen von Aggregatoren genutzt werden. Zusätzlich zu Leistungsvorgaben werden notwendige Messwerte in die Gegenrichtung zum VNB übermittelt, siehe Abbildung 12.

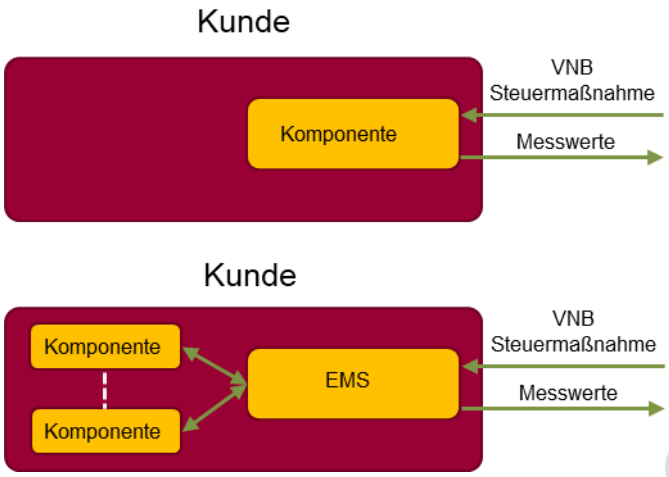

Abbildung 12: Variante 1 – Beziehung Kunde und Komponente

Hier wird die Leistungsvorgabe des VNB entweder direkt von einer Komponente ausgeführt oder ein kundenseitig bereitgestelltes EMS regelt die Vorgaben des Netzkunden.
Darüber hinaus besteht die Möglichkeit, dass Aggregatoren die Funktionen des EMS als Dienstleistung anbieten. In diesem Falle ergeben sich die folgenden Kommunikationsbeziehungen, siehe Abbildung 13.

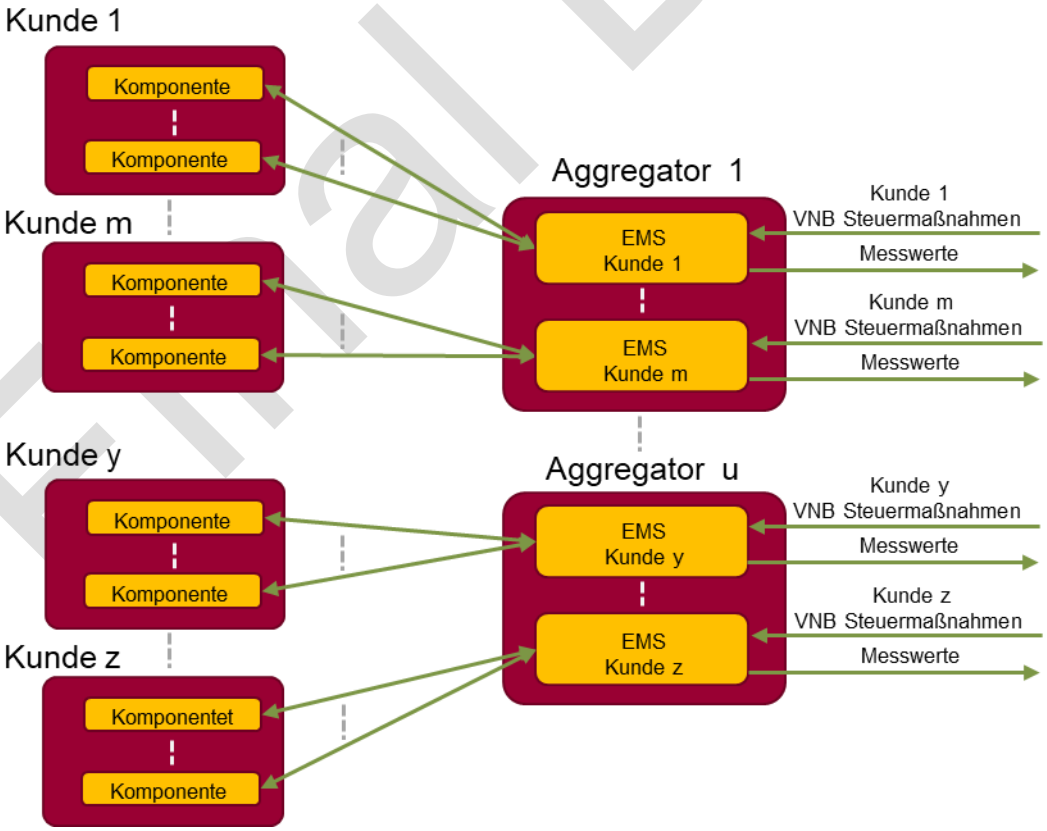

Abbildung 13: Variante 1 – Beziehung Kunde und Aggregator

Hier sind die Komponenten der Kunden direkt mit den Anwendungen der Aggregatoren verbunden. Der Aggregator kann die Funktionen des EMS in seinem Zuständigkeitsbereich umsetzen und die individuellen Bedürfnisse und Präferenzen der Kund:innen berücksichtigen.
Für beide Varianten benötigt der VNB eine Zuordnung an welchem Netzanschlusspunkt durch welche(n) Aggregator(en) Leistungsvorgaben durchgeführt werden. Darüber hinaus müssen die Aggregatorsysteme die Leistungsvorgaben, deren Rahmenbedingungen durch eine neue Tarifverordnung (Tarife 2.1 – Kapitel G.2) vorgegeben werden, einheitlich umsetzen. Da in der Variante 1 der Aggregator die Aufgaben der Leistungsvorgaben übernimmt, muss der Aggregator den Kunden über Leistungsbegrenzungen informieren. Durch die beschriebenen Beziehungen ergeben sich bei der Variante 1 die nachfolgenden Hardware-Architekturen, die am Beispiel von Ladestationen und Wärmepumpen dargestellt werden:

Bei der Variante 1 mit einem Aggregator ohne EMS übernimmt ein Aggregator(en) die Leistungsvorgabe für eine Komponente, z.B. eine Ladeeinrichtung, siehe Abbildung 14.

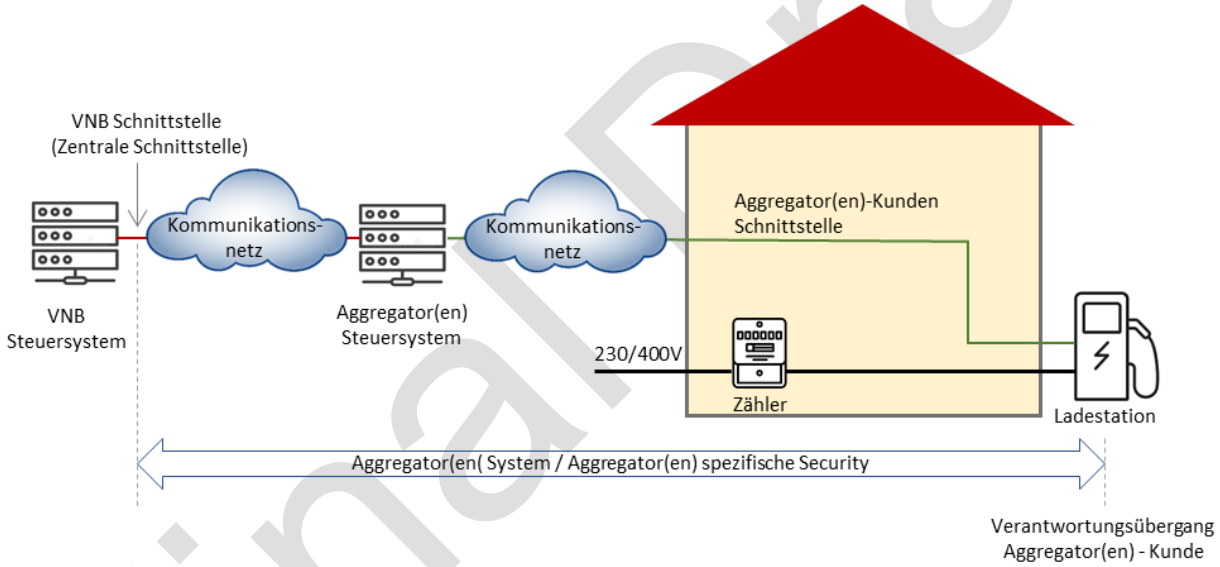

Abbildung 14: Variante 1 – Aggregator ohne EMS

Die Variante 1 mit einem Aggregator mit zentralem EMS betreibt der Aggregator ein EMS für mehrere Komponenten in einem zentralen Steuersystem, siehe Abbildung 15.

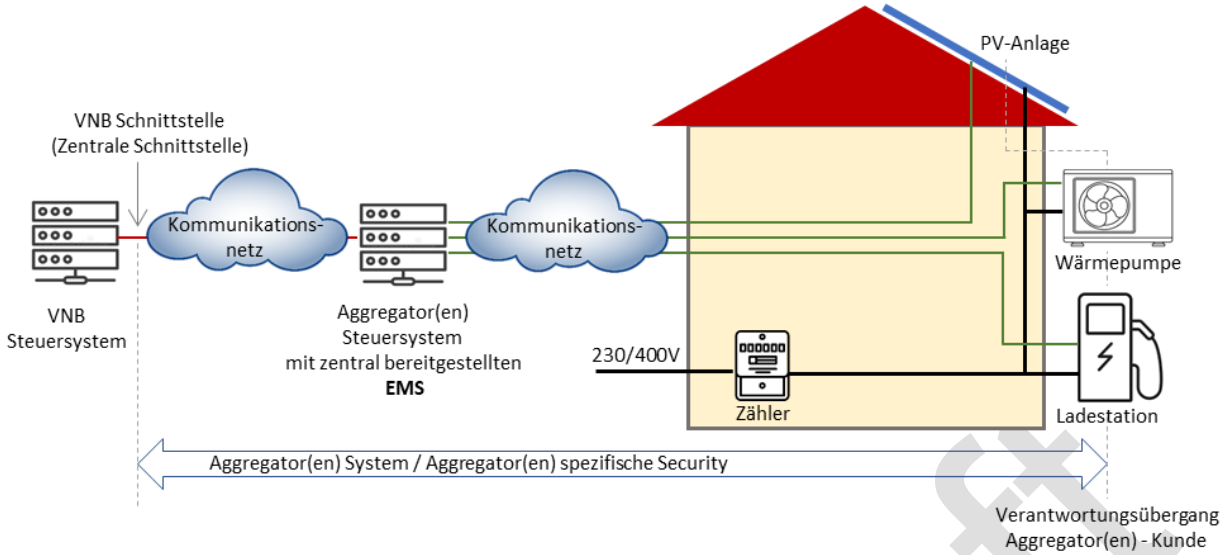

Abbildung 15: Variante 1 mit zentralem EMS

Der Aggregator hat weitere Möglichkeiten bestimmte Dienstleistungen für den Kunden zu übernehmen. Alternativ zu einem EMS als Cloud-Service kann dieses auch als eigenes beim Kunden installiertes Gerät ausgeführt sein. Beispielweise kann der Aggregator die Aufgaben für ein lokales EMS umsetzen, siehe nachfolgende Abbildung 16.

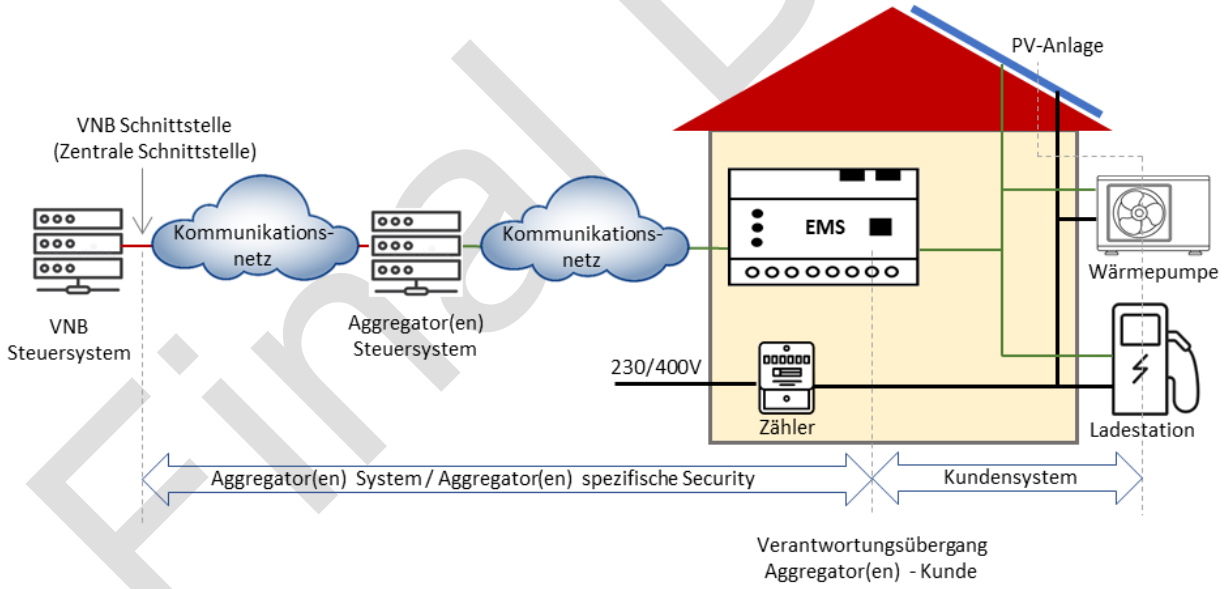

Abbildung 16: Variante 1 – Aggregator mit lokalem EMS

Zentrale Digitale Schnittstelle (Variante 2)

Bei der Variante 2 führt der VNB Leistungsvorgaben über eine zentrale digitale Schnittstelle pro Netzanschlusspunkt durch. Im dargestellten Fall erfolgt die Leistungsvorgabe an eine Komponente. Dabei ergibt sich eine n:1-Beziehung, siehe nachfolgende Abbildung 17.

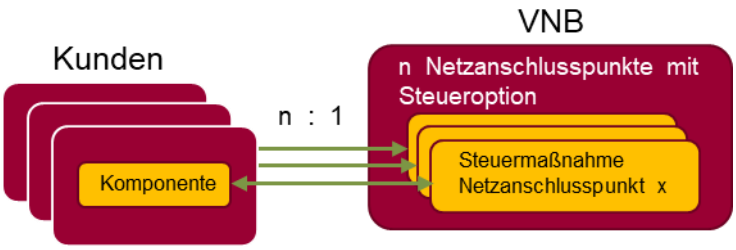

Abbildung 17: Variante 2 – Kommunikationsbeziehung – 1 Komponente

Verfügt der Kunde über mehrere Komponenten, kann ein kundenseitig bereitgestelltes EMS die erforderlichen Leistungsvorgaben unter Berücksichtigung der Kundenvorgaben umsetzen, siehe Abbildung 18.

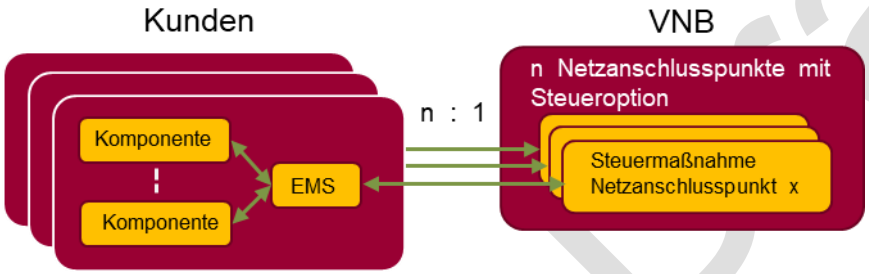

Abbildung 18: Variante 2 – Kommunikationsbeziehung – 2 Komponenten mit EMS

Da in der Variante 2 der VNB die Aufgaben der Leistungsvorgaben übernimmt, muss der VNB den Kunden über Leistungsbegrenzungen informieren, soweit technische möglich und planbar. Bei der Variante 2 ergeben sich nachfolgende technische Konfigurationen:

Der VNB übermittelt über eine zentrale *Digitale Schnittstelle* notwendige Leistungsvorgaben direkt an eine Komponente z.B. Wärmepumpe (Abbildung 19) oder bei mehreren Komponenten an ein EMS (Abbildung 20).

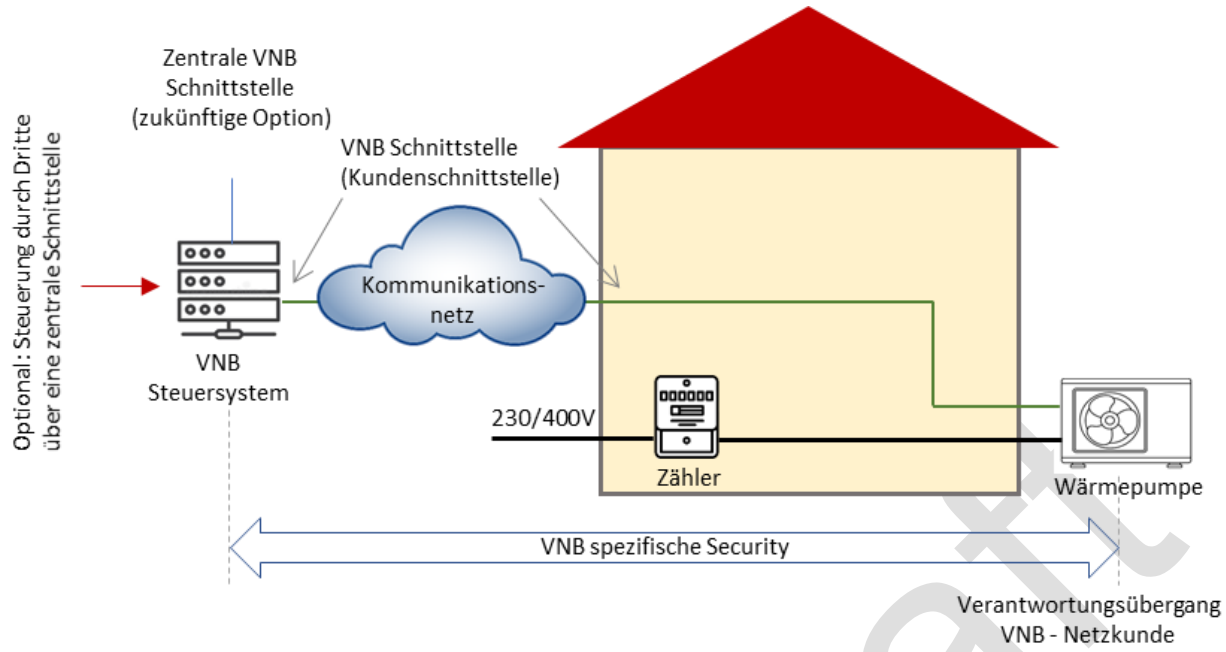

Abbildung 19: Variante 2 mit einer Komponente ohne EMS

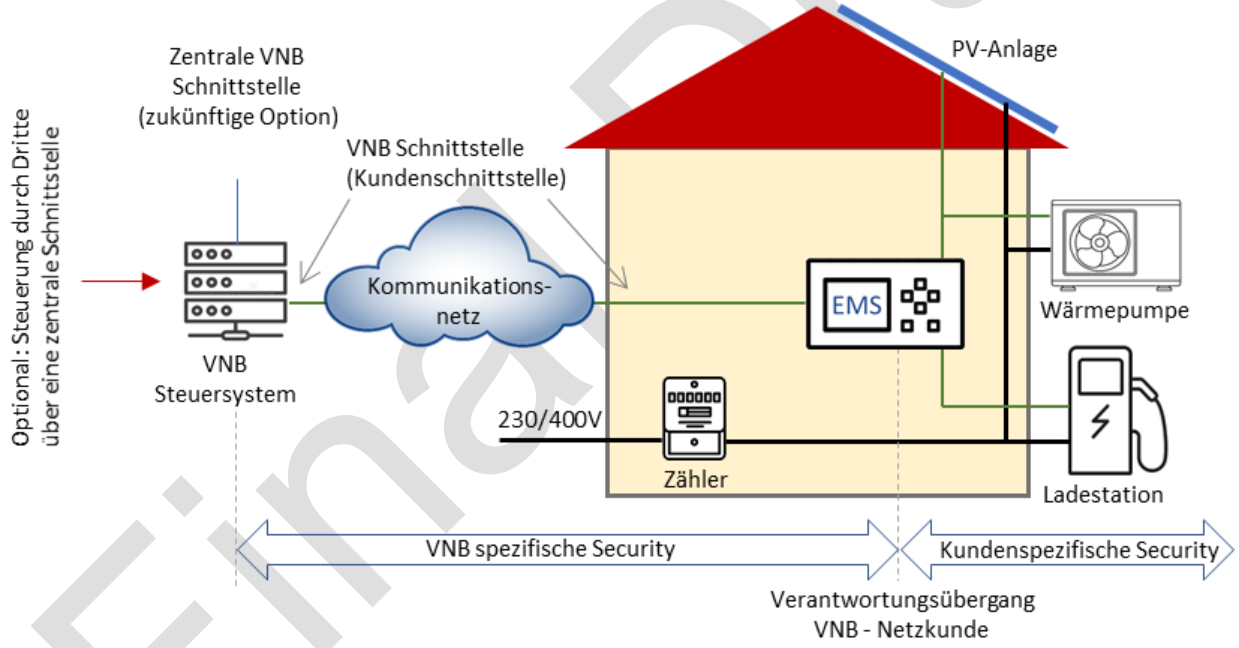

Abbildung 20: Variante 2 mit EMS und mehreren Komponenten

Digitale Schnittstelle mit Funktionsblock (Variante 3)

Bei der Variante 3 übermittelt der VNB die Leistungsvorgaben über einen Funktionsblock an eine Komponente oder ein EMS. Der Funktionsblock ist eine funktionale Beschreibung einer lokalen Schnittstelle zwischen VNB und Kundenanlage. Die technische Ausgestaltung kann durch eine separate Hardware (z.B. eigenes Gateway inkl. Software) und/oder Software (Integration in bestehende Hardware wie beispielsweise Smart Meter) umgesetzt werden. Der Funktionsblock hat dabei die Aufgabe aus Sicht des Schutzes gegen unbefugtes Eindringen das VNB System vom Kundensystem zu entkoppeln und Funktionen für die Sicherstellung der Netzverfügbarkeit (z. B.

Systemüberwachung, Default-Leistungswerte bei Systemstörungen...) zu übernehmen. In dieser Variante ergibt sich eine n:1 Kommunikationsbeziehung in der Leistungsvorgaben vom VNB zum Kunden und Messwerte in die Gegenrichtung übertragen werden, siehe Abbildung 21.

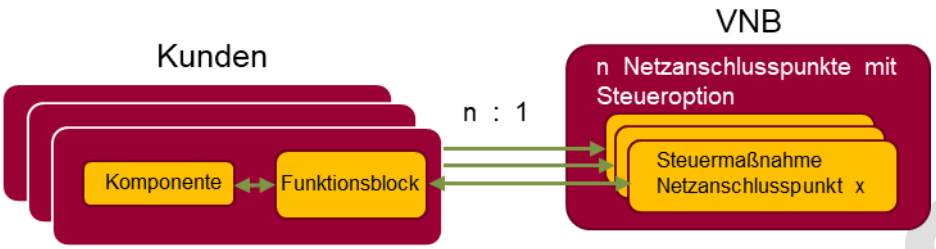

Abbildung 21: Variante 3 – Kommunikationsbeziehung – 1 Komponente

Sind mehrere Komponenten in der Kundenanlage vorhanden, ergibt sich mit einem EMS folgende Kommunikationsbeziehung, siehe Abbildung 22

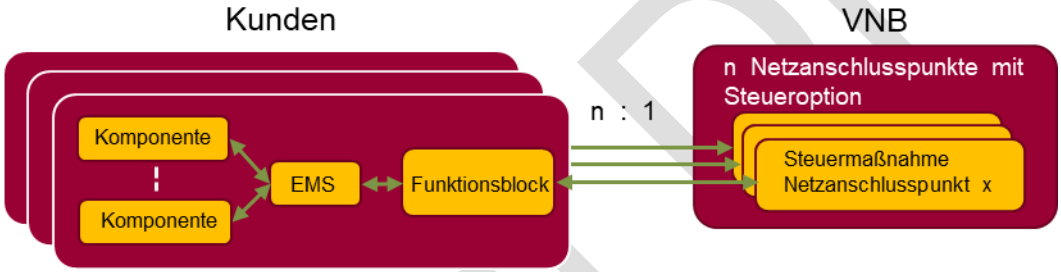

Abbildung 22: Variante 3 – Kommunikationsbeziehung – 2 Komponenten

Da in der Variante 3 der VNB die Aufgaben der Leistungsvorgaben übernimmt, muss der VNB den Kunden über Leistungsbegrenzungen informieren, soweit technische möglich und planbar. Bei der Variante 3 ergeben sich nachfolgende technische Konfigurationen:

Bei der Variante 3 mit Funktionsblock kommuniziert das Steuerungssystem des VNB mit einem beim Netzkunden installierten Funktionsblock. Optional ist hier eine zusätzliche Zählerschnittstelle möglich. Der Verantwortungsübergang zwischen dem VNB und Kundensystem wurde schematisch im Funktionsblock dargestellt, siehe Abbildung 23. Die Aufgaben und Rahmenbedingungen des Verantwortungsübergangs müssen in einer nächsten Phase genauer definiert werden.

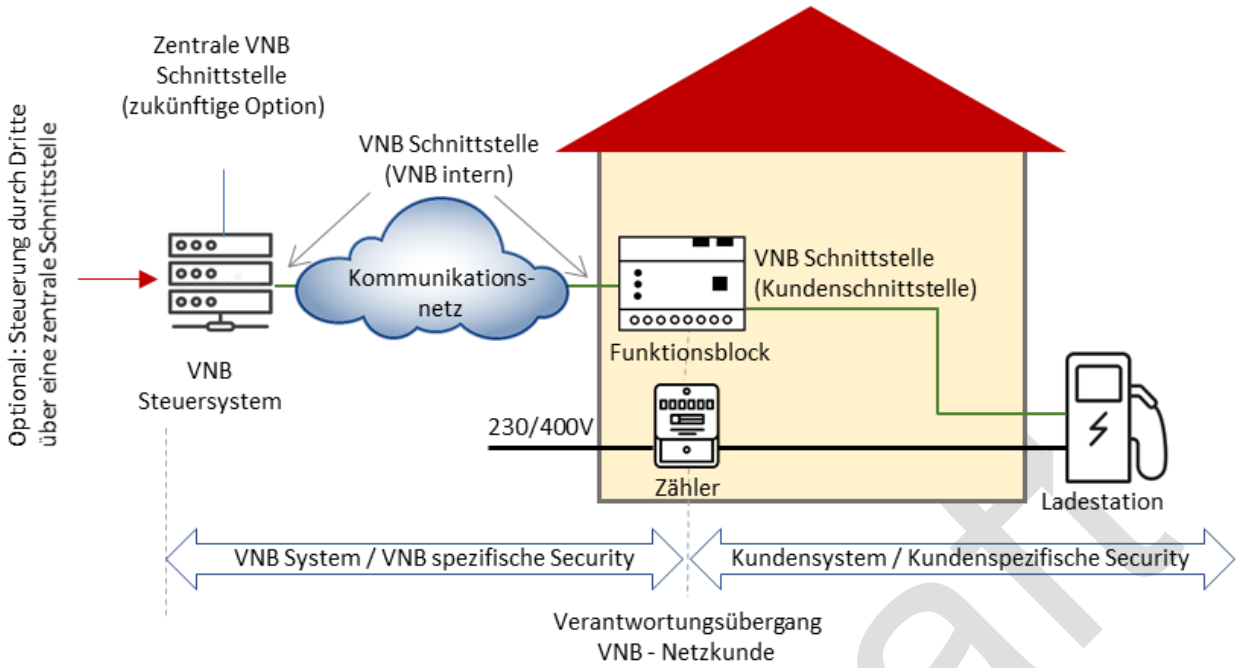

Abbildung 23: Variante 3 mit Funktionsblock

Sind in der Kundenanlage mehrere Komponenten installiert, kann ein EMS die Koordination mehrerer Komponenten übernehmen, siehe nachfolgende Abbildung 24.

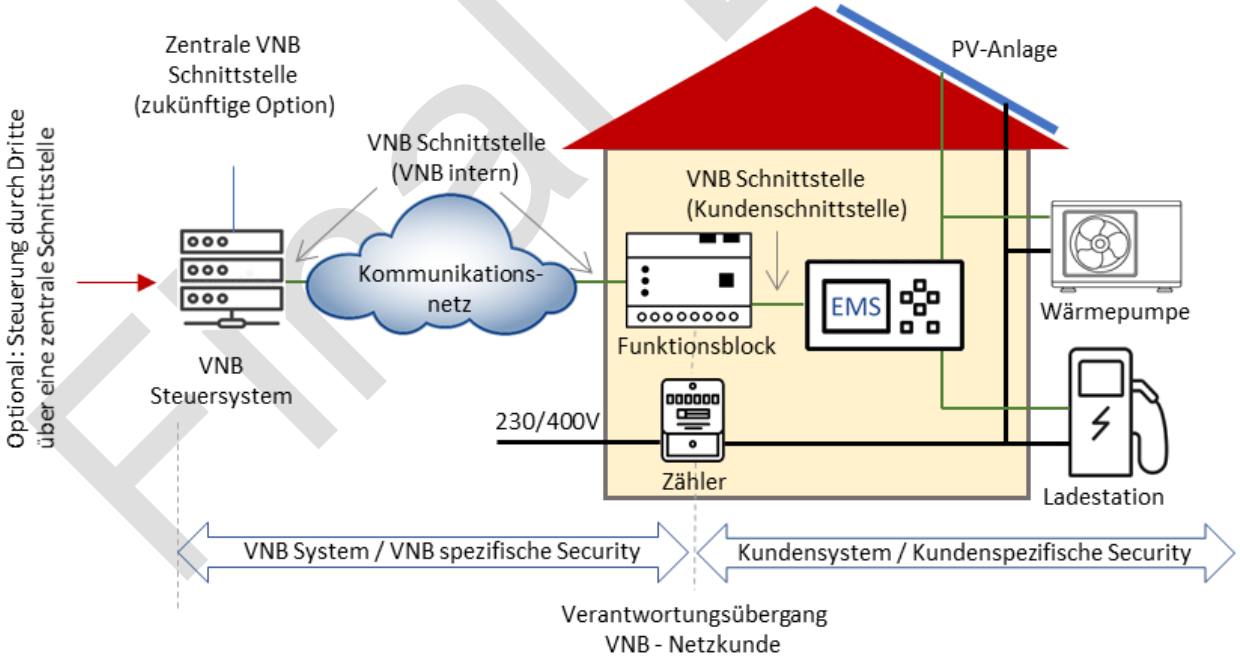

Abbildung 24: Variante 3 mit Funktionsblock und EMS

Bei den Architekturvarianten 2 und 3 ist auch eine Leistungsvorgabe der einzelnen Komponenten durch berechtigte Dritte, unabhängig vom VNB, möglich. In diesem Fall muss aber sichergestellt sein, dass Leistungsvorgaben des VNB Vorrang gegenüber allen anderen haben und vollständig ausgeführt werden müssen.

F.3 Use Cases

Neben der Arbeitshypothese und den allgemeinen technischen Rahmenbedingungen wurden folgende sechs exemplarische Use Cases für die Evaluierung von Schnittstellenlösungen ausgearbeitet, die einen Überblick verschaffen, welche Informationen über eine *Digitale Schnittstelle* auszutauschen sind und welche besonderen domänenspezifischen Rahmenbedingungen einzuhalten sind.

Nachfolgend werden die einzelnen Use Cases zusammenfassend dargestellt. Die vollständigen Beschreibungen der Use Cases finden sich in Anhang J.3.

F.3.1 Use Case 1 - Ansteuerung von Kundenanlagen durch VNB im Notzustand

Der Use Case 1 wurde von den VNB erstellt und geht davon aus, dass zusätzliche Verteilernetzkapazitäten für die Integration von dezentraler Erzeugung und zusätzlichen Lasten in die bestehenden Verteilernetze zur Verfügung gestellt werden können, wenn die Möglichkeit besteht, elektrische Einrichtungen im Falle des Erreichens von physikalischen Netzgrenzen netzentlastend zu beeinflussen. Dabei geht es um eine Begrenzung der Lastspitzen und ein Verschieben der durch die Begrenzung nicht übertragener Energie in Zeiten geringerer Auslastung. Ziel ist hier eine gleichmäßigere Verteilung der Netzbelastung und damit eine effizientere Nutzung der vorhandenen Infrastruktur. Für solche Lösungen sind insbesondere Netzkundenprozesse geeignet, die über Flexibilitätspotenziale verfügen. Dazu zählen vor allem thermische Prozesse, das Laden von Elektroautos und das Laden lokaler Batterien über PV-Anlagen.

Für diesen Use Case ist es notwendig, dass der VNB die Netze digitalisiert und durch Sensorik das Netzverhalten erfasst. Der VNB kann bei Erreichen von Leistungs- oder Spannungsgrenzwerten entsprechende Netzkapazitäten für Kundenanlagen ermitteln, um Entlastungen im Netz zu ermöglichen und umzusetzen. So wird eine Überlastung von Betriebsmitteln verhindert und ein normkonformen Systembetrieb ermöglicht. Grundsätzlich sieht Use Case 1 vor, dass die pro Netzanschlusspunkt ermittelten Leistungsvorgaben sowohl über eine *Digitale Schnittstelle* direkt an die elektrischen Einrichtungen übertragen werden oder, dass berechtigte Dritte über ein von ihnen betriebenes Steuerungssystem die erforderlichen Leistungsvorgaben an die elektrischen Einrichtungen weitergeben und umsetzen.

F.3.2 Use Case 2 - Laden von Elektroautos im Notzustand

Use Case 2 beschreibt das Laden von Elektroautos hinter einem Netzanschlusspunkt. Es wird davon ausgegangen, dass im Normalfall das Laden von Elektroautos uneingeschränkt erfolgen kann, und dass nur im Falle des Erreichens der VNB-Systemgrenzen priorisierte Leistungsvorgaben erforderlich werden, welche gegenüber kundenseitigen Vorgaben Vorrang haben. Diese werden dann über die *Digitale Schnittstelle* zwischen VNB und Netzkunde (gemäß Anschlussver-

trag) entweder an eine Ladeeinrichtung oder ein lokales Energiemanagementsystem, das mehrere Ladeeinrichtungen hinter dem Netzanschlusspunkt koordiniert, zur Umsetzung übertragen. Wenn es zu Leistungsvorgaben durch den VNB kommt, um eine Überschreitung der physischen Netzgrenzen zu vermeiden, haben diese die höchste Priorität. Darüber hinaus ist eine Informations-/Dokumentationspflicht durch den VNB notwendig. Netzkunden, Lieferanten und ggf. Behörden müssen rechtzeitig im Vorfeld über eine Leistungsvorgabe informiert werden, soweit technische möglich und planbar. Des Weiteren müssen Dritte, die im Auftrag des Netzkunden im Zusammenhang mit den betroffenen Ladepunkten Services und Leistungen erbringen (z.B. Aggregatoren) Auskunft über die Leistungsbegrenzung erhalten.

F.3.3 Use Case 3 - Ansteuerung von Ladeeinrichtungen durch CPO-Backend in Netznotsituation

Bei Use Case 3 handelt es sich um ein Angebot von Aggregatoren (z.B. CPO), steuerbare elektrische Einrichtungen (Kundenanlagen), die an das Steuerungssystem des Aggregator angebunden sind, nach den Vorgaben der VNB zu steuern, sofern Netzengpässe z.B. Notzustand auftreten. In diesem Fall sind die erforderlichen Leistungsvorgaben über eine *Digitale Schnittstelle* zwischen VNB und Aggregator an den Aggregator zur Umsetzung zu übertragen. Der Aggregator tritt bei diesem Use Case als Dienstleister auf.

Nachdem die CPOs bereits heute zahlreiche Ladeeinrichtungen betreiben und die Summe der Anschlussleistungen wächst, hat der Use Case 3 ein sehr hohes Potenzial, in Zukunft einen wesentlichen Beitrag zur Systemstabilität zu liefern. Da bei Use Case 3 keine zusätzliche Hardware bei den Kund:innen installiert werden muss, kann diese Variante vergleichsweise schnell umgesetzt werden.

F.3.4 Use Case 4 - Ansteuerung von Wärmepumpen in Netznotsituationen

Use Case 4 beschreibt die Ansteuerung von Wärmepumpen in Notsituationen. Wärmepumpen können einen Beitrag zu Beseitigung von Netzengpässen leisten, allerdings müssen die betroffenen Anlagen entsprechend ausgelegt und dimensioniert werden. Die wesentlichen Eingangsgrößen sind hier die bereitzustellende Flexibilität und die Anforderungen (in der Regel bauliche Eignung des Objektes und der Heizungsanlage, sowie Komfortanforderungen) des Anlagennutzers. Hinsichtlich der technischen Rahmenbedingungen für eine Steuerung ist folgendes zu beachten

- Um Schädigungen der Kompressoren von Wärmepumpen zu vermeiden, dürfen diese in der Regel nicht ohne Rücksicht von extern „hart“ geschaltet werden. Wird ein Abschaltbefehl empfangen, dann wird eine Abschaltzeit von bis zu 30 Minuten benötigt, um die Wärmepumpe herunterfahren zu können. Inverter gesteuerte Wärmepumpen reagieren auf Leistungsvorgaben innerhalb des spezifizierten min/max-Bereichs in der Regel sofort, allerdings ist der Maximalwert abhängig von den Umgebungsbedingungen nicht immer möglich.

- Der Heizstab von Wärmepumpen kann sofort geschaltet werden, allerdings wird er im Regelfall über das Jahr betrachtet nur in 1 bis 2% der Zeit benötigt und kann daher keinen wesentlichen Flexibilitätsbeitrag liefern.[13]

F.3.5 Use Case 5 – Ansteuerung durch Lieferanten und Aggregatoren

Use Case 5 erfasst den Umstand, dass, sofern der VNB eine eigene Infrastruktur zur Leistungsvorgabe von Kundenanlagen bei Erreichen der Netzgrenzen aufgebaut hat, diese auch für Aggregatoren und Lieferanten – sofern durch Netzkunden berechtigt – zugänglich ist. Der Aggregator tritt bei diesen Use Case als Bedarfsträger auf.

Die für den VNB verfügbaren Steuerungsoptionen pro Netzkunde müssen für die Aggregatoren und Lieferanten zur Verfügung stehen, sofern kein Netzengpass vorliegt, d. h. netzseitig keine Steuereingriffe erforderlich sind. Alle Prozessinformationen, die pro Netzkunde verfügbar sind, im Besonderen aktuelle Leistungs- und Verbrauchswerte müssen auch Aggregatoren und Lieferanten zugänglich gemacht werden. Darüber hinaus ist eine Informations-/Dokumentationspflicht durch den VNB notwendig. Netzkunden, Lieferanten und ggf. Behörden müssen rechtzeitig im Vorfeld über eine Leistungsvorgabe informiert werden, soweit technische möglich und planbar Der Betrieb der Schnittstelle erfolgt gemäß den vertraglichen Festlegungen zwischen den Partnern VNB und Netzkunde, der gewisse Rechte an Dritte übertragen kann (z.B. auch Regelung Informationsfluss). Sofern technisch machbar, müssen Prognosen von zukünftigen Netzengpässen erstellt und weitergeleitet werden, damit durch Setzen von marktseitigen Steuerungsmaßnahmen Eingriffe der VNB präventiv möglichst vermieden werden können.

F.3.6 Use Case 6 - Ansteuerung über eine Hersteller - und Aggregator Cloud

Use Case 6 basiert auf dem Umstand, dass eine Verbindung mit einer Cloud eines Industriepartners hergestellt wird. Wahlweise kann die Verbindung zusätzlich auch über einen Aggregator hergestellt werden. Der Verteilnetzbetreiber sendet die temporären Leistungsvorgaben entweder direkt an die Cloud des Herstellers oder an einen Aggregator, der diese Vorgaben an die Cloud des Industriepartners weitergibt. In der Cloud werden die Vorgaben verarbeitet und entsprechend den Vorgaben (VNB, Kunde) priorisiert. Die Cloud des Herstellers übermittelt die Vorgaben an die lokalen Einheiten. Der Aggregator tritt bei diesen Use Case als Bedarfsträger auf.

F.3.7 Use Cases – Lessons Learned: Zusätzliche Anforderungen

Aufgrund der dargestellten Use Cases können folgende zusätzliche Anforderungen an eine digitale Schnittstelle abgeleitet werden, die bei einer Modellierung berücksichtigt werden müssen:

[13] Annahme Wärmepumpen Austria

- Je nach zu steuernder Kundenanlage kann eine Schutzzeit zwischen zwei aufeinander folgenden Steuereingriffen erforderlich sein. Bei Ladestationen sollten hier 15 Minuten eingehalten werden.
- Es kann kundenprozesstechnische Minimalwerte geben, die nicht unterschritten werden dürfen. Bei AC-Ladestationen beträgt der minimale Ladestrom 6A. Darunter ist in der Praxis keine Ladung mehr möglich.
- Es kann erforderliche Nachlaufzeiten geben, d. h. ein gegebener Steuerbefehl darf erst nach der Nachlaufdauer umgesetzt werden (z. B. Abschalten einer klassischen Wärmepumpe.

Zur Durchführung der Use Cases müssen bestimmte Datenpunkte über die digitale Schnittstelle(n) übertragen werden können. Dabei wird unterschieden zwischen:

- Unveränderbare (statische) Standwerte von Einzelgeräte wie z.B. maximale Leistungswerte
- aktuelle Messwerte von der Übergabestelle, Zähler und Einzelgeräten
- Vorgabewerte für die Übergabestelle, Zähler und Einzelgeräte zur Beeinflussung der Leistung

Als Einzelgeräte (elektrische Einrichtungen) werden in der Datenpunktliste die Ladeeinrichtung, Wärmepumpe, Batteriespeicher und die PV-Anlage berücksichtigt, siehe Anhang J.2.

Zusätzlich gilt die Anforderung nach Erweiterungsmöglichkeiten des Datenmodells in Richtung Zeitreihen wie sie für den Lieferanten / Aggregator Use Case erforderlich werden und in Richtung zusätzlicher Datenpunkte die in Zukunft erforderlich werden könnten.

Darüber hinaus ist eine Informations-/Dokumentationspflicht durch den VNB notwendig. Netzkunden, Lieferanten und ggf. Behörden müssen rechtzeitig im Vorfeld über eine Leistungsvorgabe informiert werden, soweit technisch möglich und planbar. Die Schnittstelle wird zwischen VNB und Netzbenutzer:innen muss vertraglich vereinbart werden, jedoch durch die Kontaktstellen VNB und Dienstleister sowie Dienstleister und Endkunden:innen abgewickelt werden. Sofern technisch machbar, müssen Prognosen von zukünftigen Netzengpässen erstellt und weitergeleitet werden, damit durch Setzen von marktseitigen Steuerungsmaßnahmen Eingriffe der VNB präventiv möglichst vermieden werden können.

Zusätzlich zu den Anforderungen an die Modellierung der *Digitalen Schnittstelle* als auch des Datenmodells gibt es folgende Anforderungen zwischen Netz und Marktakteuren:

- Ein Anforderungskatalog wird den Netzkunden zur Verfügung gestellt, in den u.a. die Netzanschlussanträge transparent gelegt werden.
- Im Falle einer eintretenden netzseitigen Steuerung wird anhand eines Anforderungskataloges die Nachweispflicht zur erfolgten Netzzugangssteuerung anhand der Parameter österreichweiter einheitlicher Standards und definierte Fristen dokumentiert werden.

- Analog zum Prozess des „Netzzugangsvertrages“ wird die Schnittstelle zwischen VNB und Netzbenutzer vertraglich vereinbart, wobei die Umsetzung der Steuerung zwischen Aggregatoren und Netzbenutzer abgewickelt wird.

Durch die zunehmende Nachfrage nach Energiegemeinschaften muss zukünftig bei der Digitalen Schnittstelle nachfolgende Aspekte berücksichtigt werden:

- Komponenten innerhalb einer Energiegemeinschaft haben keine gemeinsame offene Schnittstelle, sondern eine proprietäre Kommunikation. Entsprechend können Geräte des gleichen Herstellers sehr gut miteinander kommunizieren, Geräte unterschiedlicher Hersteller aber nicht.
- Energiegemeinschaften könnten mit der Kombination aus der Architekturvariante 1 und 3 realisiert werden. Der Smart-Meter soll dabei nur für die Abrechnung verwendet werden und nicht zur Leistungsvorgabe von Komponenten.

Weitere Untersuchungen für Energiegemeinschaften sollten dazu in Phase II evaluiert werden.

F.3.8 Use Cases – Verknüpfung mit Architekturvarianten

Die ausgearbeiteten Use Cases beschreiben erste Anwendungsfälle (nicht abschließend) für die Umsetzung einer *Digitalen Schnittstelle*. Wie im Projekt ausgearbeitet, können die Use Cases mit nachfolgenden Architekturvarianten umgesetzt werden: (weitere Kombinationen möglich)

Use Case 1 (Ansteuerung von Kundenanlagen durch VNB im Netznotzustand) und Use Case 2 (Laden von Elektroautos im Netznormalzustand) werden über die Infrastruktur des VNB umgesetzt und benötigen keine Dienstleistungen von Aggregatoren. Aus diesem Grund kann Use Case 1 und 2 mit der Architekturvariante 2 (Zentrale *Digitale Schnittstelle*) und 3 (*Digitale Schnittstelle* mit Funktionsblock) umgesetzt werden.

Bei den Use Cases 3-6 (CPO, Wärmepumpe, Lieferanten, Hersteller) werden Dienstleistungen von einem Aggregator(en) in Anspruch genommen, deshalb können diese Use Cases mit der Architekturvariante 1 (*Digitale Schnittstelle* über Aggregator(en)) umgesetzt werden.

F.4 Rechtliche Rahmenbedingungen

Neben der technischen Ausarbeitung sind für den Einsatz einer digitalen Schnittstelle auch die rechtlichen und regulatorischen Rahmenbedingungen zu schaffen. Nach Einschätzung der Arbeitsgruppe gibt es derzeit keine rechtlichen Rahmenbedingungen für eine *Digitale Schnittstelle*. Für die Umsetzung einer *Digitalen Schnittstelle* wurden im Rahmen des Projekts notwendige Änderungen der Regelwerke erarbeitet, siehe Kapitel G.2.

F.5 Wirtschaftliche Rahmenbedingungen

F.5.1 Volkswirtschaftliche Sicht

Die vermehrte Nutzung erneuerbarer Energien und der großflächige Einsatz von neuartigen Lasten, wie Elektrofahrzeuge und Wärmepumpen, stellen die VNB vor neue Herausforderungen. Wegen der Umstellung von fossilen Energieträgern auf Strom aus Erneuerbaren besteht aktuell hoher Druck auf kurzfristige Netzverstärkungen, die mit entsprechenden Investitionen verbunden sind.

Im Regulierungsschema strebt der Regulator ein volkswirtschaftliches Optimum an. Dabei werden Kostenbelastungen der Kunden und der Netzbetreiber in Summe betrachtet. Damit stehen generell wirkende kostensenkende Lösungen im Fokus. Die Digitalisierung eröffnet – in einem sinnvollen Maße eingeführt – hier Kostensenkungspotenziale, die mit fortschreitender technischer und regulatorischer Entwicklung zunehmender attraktiver werden dürften – so die allgemeine Einschätzung. Entscheidend ist dabei aber die Wirkung der Digitalisierung auf die Optimierung des Netzbetriebes durch Leistungsvergleichsmäßigung. Der VNB hat die Pflicht, die Lastflüsse zu überwachen und den Systemzustand zu kennen, sowie zeitgerecht notwendige Verstärkungsmaßnahmen durchzuführen.

Ohne die Möglichkeit der Vorgabe von Leistungswerten durch die VNB für Kundenanlagen ist stets eine konventionelle Netzplanung und konventionelle Anschlussbeurteilung der Kundenanlagen nötig, bei denen die VNB von einem Worst-Case-Szenario ausgehen müssen. Eine *Digitale Schnittstelle* bietet die Möglichkeit, die Zunahme der Netzrestrukturierungsmaßnahmen und damit der Investitionskosten zu dämpfen. Die Netzinfrastruktur kann zu Zeiten geringer oder mittlerer Auslastung besser genutzt werden. Dafür ist jedoch eine Möglichkeit der Steuerung durch die VNB unerlässlich, um in Zeiten hoher Auslastung die Überlastung von Betriebsmitteln zu vermeiden und die Spannungsqualität aller Kunden sicherzustellen. Die bessere Ausnutzung der Netzinfrastruktur durch eine *Digitale Schnittstelle* ermöglicht es, mehr Kundenanlagen ans Netz anzuschließen. Dadurch kann das Netz aus volkswirtschaftlicher Sicht jedenfalls kosteneffizienter sein, zumal letztendlich die Netzkunden, und damit die gesamte Bevölkerung, für die Netzkosten aufkommen müssen. Es kann länger mit dem Bestandsnetz das Auslangen gefunden werden.

Über die Verringerung des Investitionsbedarfs hinaus bietet eine *Digitale Schnittstelle* die technische Möglichkeit, überhaupt Kundenanlagen zu genehmigen und anzuschließen, wenn die erforderlichen Netzrestrukturierungsmaßnahmen kurzfristig, etwa aufgrund von Personalmangel, aus organisatorischen Gründen oder wegen Lieferengpässen bei Betriebsmitteln - nicht durchgeführt werden können. Wie in Abbildung 25 zu sehen ist, nehmen die Kundenanfragen und die für den Anschluss erforderlichen Maßnahmen seitens der VNB zu.

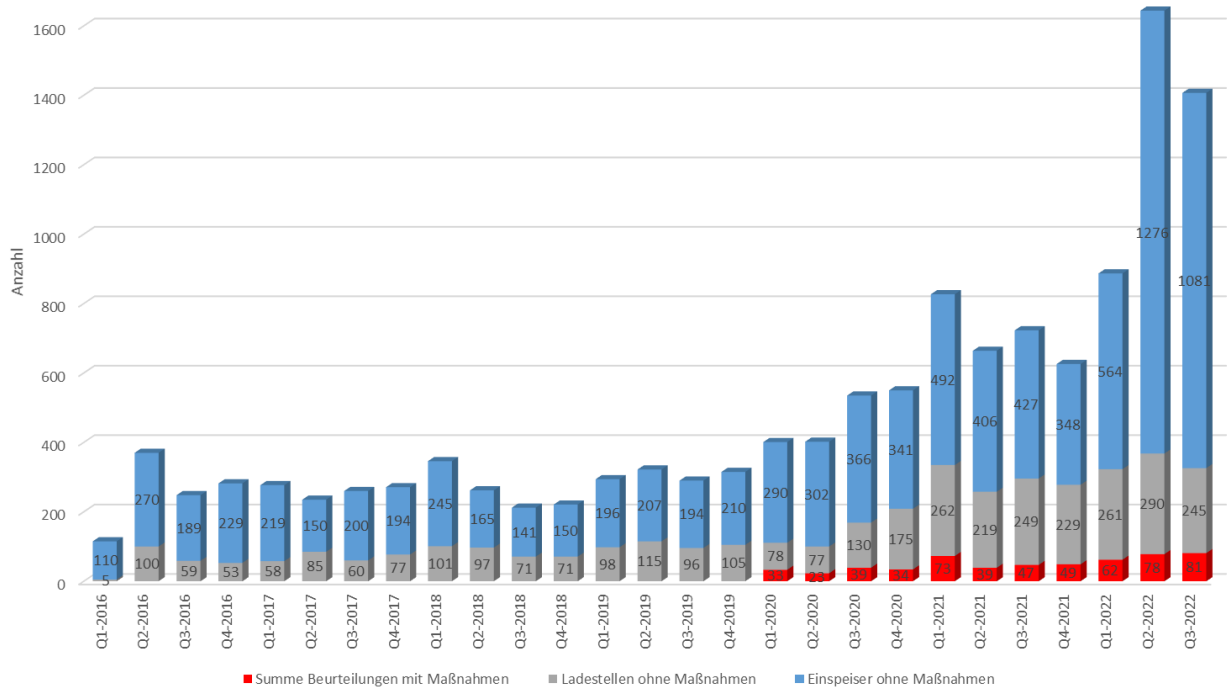

Abbildung 25: Kundenanfragen für Ladeeinrichtungen und Einspeiseanlagen bei Vorarlberger Energienetzen GmbH (Vorarlberger Energienetze)

Eine *Digitale Schnittstelle* kann dabei helfen, den steigenden Kundenanfragen länger gerecht zu werden, wobei es dem Betreiber selbst zufällt, die per Signal gemeldete Reduktionsanfrage umzusetzen. Das Bedeutet im Detail, dass die *Digitale Schnittstelle* zwischen VNB und Kundenanlage vertraglich vereinbart, jedoch durch die Aggregatoren abgewickelt werden kann. Das Marktsegment kann für den Kunden dafür lohnende Angebote schaffen.

Eine Erhöhung der Netzkapazität bedeutet, zusätzlich zur bereits erwähnten besseren Ausnutzung der Infrastruktur und somit volkswirtschaftliche Vorteile durch:

- höhere Investitionen in Kundenanlagen wie Ladestationen, Wärmepumpen und PV-Anlagen,
- höhere Investitionen in lokale Installationsunternehmen,
- mehr verfügbare Anlagen für die Bewirtschaftung durch EVU, CPOs und andere Aggregatoren sowie
- Erhöhung lokaler Stromproduktion bzw. eine verringerte Abhängigkeit von Energieimporten.

F.5.2 Betriebswirtschaftliche Sicht der Netzbetreiber

Die VNB sind zu einem kosteneffizienten Netzausbau und –betrieb gesetzlich und regulatorisch verpflichtet. Damit ist die permanente Suche nach den besten technischen Lösungen verbunden. Das ist ein laufender Orientierungsprozess, der neben den sich ändernden Anforderungen auch die jeweils aktuellen Handlungsoptionen einschließt. Ein angepasstes Leitungsnetz mit ausreichenden Trafokapazitäten stellt auch weiterhin allgemein eine solide Basis der Stromversorgung dar. Für die dynamischen Leistungszuwächse steht dem professionellen Netzplaner ein bunter

Blumenstrauß an elektrotechnisch anspruchsvollen Ergänzungsmaßnahmen zur Verfügung (z.B. wirkstromkompoundierte Spannungsregelung, Strangregler, regelbare Ortsnetztransformatoren, Wirk- und Blindleistungsmanagement usw.).

Für den VNB ist nun in Konkurrenz zu den angeführten Ertüchtigungsmaßnahmen die mittel- und langfristige Kosten-Nutzen-Relation von Digitalisierungsmaßnahmen zu bewerten. Dabei ist noch zwischen Investitionen in der Netzinfrastruktur und Maßnahmen in Kundenanlagen zu unterscheiden, die aber technisch nicht entkoppelt betrachtet werden können.

Gleichzeitig hat sich der Netzbetreiber auch im Benchmark-System der Regulierungsbehörde zu bewähren, indem Anreize zu erfolgreichem Wirtschaften gesetzt werden.

Maßnahmen in die Digitalisierung der öffentlichen Netze

Die meisten VNB haben insbesondere mit der Ausrollung zusätzlicher Messtechnik und sonstiger Optimierungsfunktionen in die Netzstationen (sog. intelligente Netzstationen „iONS“) begonnen. In Kombination mit der Nutzung von Smart-Meter-Daten könnte so eine spürbare Dämpfung der Zusatzkosten für Leistungssteigerungen erreicht werden, weil damit die jeweils lokal noch vorhandenen Netzkapazitäten erkannt und bewirtschaftet werden können. Hier ist leider die IONS-Ausbaugeschwindigkeit realistisch über einen längeren Zeitraum anzusetzen, da bei Montageaufwand, Finanzierung und Komponentenverfügbarkeit natürliche Grenzen wirken.

VNB-Digitalisierungsmaßnahmen in Kundenanlagen

Ergänzend oder alternativ kann der VNB auch Einrichtungen in Kundenanlagen installieren, um unter gewissen Voraussetzungen Messwerte abzuholen und Leistungsvorgaben an die Kundenanlagen zu übertragen. Soll dies zukünftig unter Nutzung technologischen Fortschrittes digital erfolgen, setzt dies Investitionen für Kunden und VNB voraus. Auch hier ist mittel- und langfristig zu bewerten, in welchem Gesamtanteil Digitalisierungskosten betriebswirtschaftlich zielführend sind.

Software- und Hardwarekosten

Für den laufen Betrieb der digitalen Schnittstelle (Serverinfrastruktur, Wartungen, Weiterentwicklung, Aufrechterhaltung der Sicherheit, etc.) werden in Zukunft bei den Netzbetreibern, Netzkunden, Herstellern und auch Aggregatoren Kosten anfallen. Eine vollständige Kostenbetrachtung und -abgeltung einer *Digitalen Schnittstelle* muss für die Umsetzung durchgeführt werden, was nicht Teil des Projekts (Phase I) war und in der Phase II evaluiert werden sollte. Nachfolgend ein paar Beispiele möglicher Kostenkriterien:

Software Kosten

Laufende Kosten: Betrieb (Verfügbarkeit, Security), Weiterentwicklung der Funktionalitäten, Datenverbindung (wenn kein Kundeninternet), 1st + 2nd Level Support, Hotline, Bereitschaft, Wartung für Standards und Protokolle, Updates, Fehlerbehebungen, Stabilität, Schulungskosten, Datenspeicherung, Hosting, Lizenzgebühren

Einmalige Kosten: Implementierung Softwareschnittstelle/Standards und Protokolle, Inbetriebnahme der Prozesse, Zertifizierung, Abnahmeverfahren (Standardisierter Prozess durch bspw. unabhängiges Institut zur Harmonisierung aller Netzbetreiber), Dokumentation

Hardware Kosten

Laufende Kosten: Kosten für eine zentrale EDA-Schnittstelle, Serverkosten, Datenverbindung, Energiekosten, Austausch bei Defekt, Recycling

Einmalige Kosten: Kosten für die Funktionsbox (Gateway, Backend, etc.), Kosten für eine zentrale EDA-Schnittstelle, Installationskosten vor Ort, Kosten für Hardwareentwicklung, Serverkosten, Zertifizierung der Geräte, Rolloutkosten

F.5.3 Betriebswirtschaftliche Sicht weiterer Partner

Für sämtliche weiteren Partner ist selbstverständlich ebenfalls eine Wirtschaftlichkeit Voraussetzung für ein Engagement. Einmalige und laufende Kosten müssen rentabel investiert sein.

Dafür sind geeignete Rahmenbedingungen (z.B. Netztarifmodell mit einer spürbaren Leistungspreiskomponente) entscheidend. Einmalige und laufende Kosten für den Kunden dürfen nicht zu hoch sein, damit die Use Cases und Anwendungsfälle auch wirtschaftlich darstellbar sind.

G. Ergebnisse

G.1 Zusammenfassung der AIT-Studie zur Bewertung der Standards und Protokolle

In diesem Abschnitt werden die Ergebnisse der Studie des *Austrian Institute Of Technology* (AIT) zur Untersuchung der relevanten Standards und Protokolle zusammengefasst. Zuerst wird auf die evaluierten Standards und Protokolle sowie die Methodik eingegangen. Aufbauend auf einer grundlegenden Bewertung werden Security-Aspekte von drei Architekturvarianten untersucht und eine SGAM-Modellierung (SGAM = Smart Grid Architecture Model) durchgeführt. Die Modellierung der Architekturvarianten im international anerkannten SGAM verbessert das gemeinsame Verständnis der Verortung von Akteur:innen und deren Interaktionen. Die vollständige Studie ist im Anhang J.5 zu finden.

G.1.1 Untersuchte Standards und Protokolle, Methodik

Für die Bewertung der verschiedenen Kommunikationsstandards und -protokolle zur Umsetzung einer digitalen Schnittstelle wurde eine Literaturrecherche von unterschiedlichen wissenschaftlichen Projektergebnissen und verfügbaren Quellen durchgeführt. Dieser Ansatz eignet sich gut, um bekannte Eigenschaften der Standards und Protokolle zu sammeln und vergleichend darzustellen. Implementierungsspezifische Kriterien lassen sich dadurch jedoch nur teilweise bewerten. Für die Bewertung von unterschiedlichen Standards und Protokolle wurde zuerst eine Vorauswahl getroffen. Die ausgewählten Standards und Protokolle wurden unter Berücksichtigung mehrerer Kriterien untersucht. Die Kriterien und deren Bewertungsklassifizierungen werden in den folgenden Absätzen genauer erläutert.

Auswahl der Kommunikationsstandards und -protokolle

Für die Auswahl der Standards und Protokolle wurde zuerst eine Vorauswahl durch die AIT-Experten getroffen. Diese Vorauswahl wurde daraufhin dem Expertenpool Digitale Schnittstelle vorgestellt und abgestimmt. Als Feedback auf diese Vorstellung wurden weitere relevante Standards und Protokolle erwähnt, insbesondere Modbus TCP, und die Auswahl der zu analysierenden Standards und Protokolle um diese erweitert.

Auswahl der Analysekriterien

Zur weiteren Analyse der Standards und Protokolle wurde zuerst definiert, welche Aspekte für die Einsetzbarkeit besonders relevant sind. Dafür wurde von den Experten ein Kriterienkatalog entwickelt und in vier Hauptkategorien gegliedert (Generelle Kriterien, Operative Kriterien, Technologiespezifische Kriterien und Security Kriterien). Zu jedem Kriterium wurde eine Klassifizierung definiert, um dem Aspekt einen numerischen Wert (von 1, schlecht, bis 5, sehr gut) zuzuordnen, wenn möglich. Diese numerischen Werte wurden rein aus Expertenwissen definiert und wurden zur Vergleichbarkeit der Standards und Protokolle eingeführt. Die Klassifizierungen aller bewerteten Kriterien sind im Anhang J.5.4 angeführt.

Die in Anhang J.5.4 vorgestellten Klassifizierungen der Kriterien wurden in weiterer Folge zur Analyse der unterschiedlichen Standards und Protokolle eingesetzt. Mit den numerischen Werten wurden in weiterer Folge gewichtete Mittelwerte für die einzelnen Gruppen von Kriterien berechnet, um ein Ranking für die Standards und Protokolle und ihre Eignung aufzustellen. Die Gewichtung der Kriterien, die in der finalen Analyse zum Einsatz gekommen ist, wurde von Mitgliedern aus dem Expertenpool vorgeschlagen und daraufhin in der Studie übernommen. Diese ist im Anhang J.5.6 zu

Analyse der Standards und Protokolle

Die Methodik der Analyse der Standards und Protokolle setzte sich aus zwei Vorgehensweisen zusammen. Erstens wurden veröffentlichte Standard- und Protokolltexte von AIT-Experten gesichtet und auf die, im Vorhinein definierten Aspekte, hin analysiert. Zweitens wurde dieses Wissen durch Gespräche mit weiteren Spezialisten vertieft. Die Bewertung der einzelnen Standards und Protokolle wurde von jenen Experten durchgeführt, welche die jeweiligen Standards und Protokolle analysiert haben.

Weitere Diskussionsrunden zu den Bewertungen wäre in einem nächsten Projektschritt ratsam, um die Ergebnisse noch belastbarer zu machen.

Architekturvarianten

Die Architekturvarianten, also die gesamte Umsetzung vom VNB bis zu den Kundenanlagen, gegebenenfalls durch mehrere Standards und Protokolle bzw. Schnittstellen, wurden parallel zur Bewertung der Standards und Protokolle konkretisiert. Die entwickelten Architekturvarianten sind im Kapitel F.2 in Abbildung 10: Übersicht Architekturvarianten dargestellt.

Limitierungen der Studie

Bei der Studie handelt es sich um eine theoretische Untersuchung relevanter Standards und Protokolle. Es wurde die generelle Eignung der Standards und Protokolle bewertet, um sichere Systeme zu entwerfen. In weiterer Folge wäre es ratsam, Demonstratoren mit geeigneten Kommunikationsstandards und -protokollen zu evaluieren, um genauere Aussagen über implementierungsspezifische Unterschiede treffen zu können.

Zum Zeitpunkt der Analyse war noch keine genaue Definition von Prozessen und Interaktionen zwischen den Kommunikationsteilnehmern vorhanden. In einem folgenden Schritt wäre es ratsam die genauen Datenübertragungsprozesse zu definieren und deren Umsetzbarkeit in den einzelnen Standards und Protokolle noch genauer zu beleuchten. Vor allem die Kriterien betreffend die Security müssen nochmals auf Prozessebene beleuchtet und analysiert werden.

G.1.2 Bewertung der Standards und Protokolle

Die Standards und Protokolle wurden entsprechend der Vorgehensweise aus Kapitel G.1.1 bewertet. Die Ergebnisse für eine zentrale Schnittstelle sind in Tabelle 1 zusammengefasst, jene für eine lokale Schnittstelle in Tabelle 2.

Eine umfangreiche textliche Beschreibung der Bewertung ist im Kapitel J.5.3 angeführt. Im Kapitel J.5.5 findet sich die Tabelle mit der vollen numerischen Bewertung aller Aspekte. Im Kapitel J.5.6 ist die benutzte Gewichtung angeführt, die verwendet wurde, um aus den Bewertungen der einzelnen Kriterien auf die Bewertung der Kategorien zu kommen.

Tabelle 1: Bewertung der Standards und Protokolle für die zentrale VNB-Schnittstelle, gewichtet

	Generell	Operativ	Technologie-spezifisch	Security	**Summe**
IEEE 2030.5	+	+	++	++	**++**
IEC 62746 (OpenADR)	+	+	++	++	**++**
IEC 61850	+	+	++	++	**+**
DNP3	+	++	+	+	**+**
IEC 60870-104	+	~	+	+	**+**

Tabelle 2: Bewertung der Standards und Protokolle für die lokale Schnittstelle, gewichtet

	Generell	Operativ	Technologie-spezifisch	Security	**Summe**
IEEE 2030.5	+	+	++	++	**++**
EEBus (IEC 63380)	++	+	+	++	**++**
Sunspec Modbus / REST	++	+	++	++	**++**
OCPP 2.0.1	+	+	+	++	**+**
KNX IoT	+	+	+	++	**+**
Modbus TCP	+	~	+	~	**~**

Für die Bewertung in Tabelle 1 und Tabelle 2 wurde folgende Skala benutzt:

++	+	~	-	--
Sehr gut geeignet	Gut geeignet	Ausreichend	Eher nicht ausreichend	Nicht ausreichend

Die Bewertung stellt eine Momentaufnahme dar. Sowohl im Smart Home Bereich als auch im Bereich der Steuerung von verteilten intelligenten Energieanlagen finden zurzeit mehrere, teilweise parallele, Entwicklungen statt. Ob sich ein einzelner Standard oder ein einzelnes Protokoll zur Kommunikation mit Endkundenanlagen international durchsetzt, ist noch nicht absehbar.

G.1.3 Fazit der AIT-Studie: Empfehlung zur Umsetzung

Im Rahmen der Studie wurden mehrere Standards und Protokolle aus dem Smart Grid Bereich beleuchtet, die bei einer bidirektionalen digitalen Schnittstelle (Kapitel G.1.1) vorgestellten Kriterien wurden bewertet und diese Kriterien dann in 4 Kategorien zusammengefasst.

Zu Beginn wurden alle Aspekte in den Kategorien gleichbehandelt und keine Priorisierung einzelner Kriterien vorgenommen. Die Resultate in Kapitel G.1.2 wurden mit der Rückmeldung der Stakeholder aus dem Expertenpool gewichtet und zeigen eine Favorisierung von IEEE 2030.5 und OpenADR für eine zentrale Schnittstelle. Für domänenunabhängige lokale Standards und Protokolle erweisen sich IEEE 2030.5 sowie EEBus als sehr gut geeignet, für domänenspezifische lokalen Standards und Protokolle OCPP und Sunspec Modbus.

Jene Standards und Protokolle, die auf Web-Technologien basieren, sind besser geeignet, unterschiedliche Architekturvarianten zu bedienen. Bei diesen Standards und Protokollen kann der notwendige Aufwand bei der Implementierung verringert sowie die Wartung und Erweiterung der Kommunikationsinfrastruktur erleichtert werden.

Eine weite Verbreitung von Applikationsprotokollen, vor allem im IT-Bereich, kann bedeuten, dass Sicherheitslücken schneller bemerkt und bereinigt werden. Ebenso sind Strategien diese Standards und Protokolle abzusichern oft schon in der Konzeption berücksichtigt und einfacher umzusetzen.

In den drei ausgewählten Architekturvarianten tauchen sowohl Schnittstellen auf, für die Standards und Protokolle aus dem OT (Operational Technology) Bereich zulässig wären, wie zum Beispiel die Verbindung des VNB zu den Funktionsblöcken im Kundenbereich, als auch Schnittstellen für die Standards und Protokolle aus dem IT (Information Technology) am besten geeignet wären, wie zum Beispiel der Verbindung zwischen Aggregator und VNB. Zusätzlich dazu wäre es aber vorteilhaft, wenn alle Architekturvarianten sich zumindest an der zentralen Schnittstelle des gleichen Standards und Protokolls bedienen würden. Unter diesem Hintergrund könnten sich Standards und Protokolle, die auf einem weit verbreiteten Applikationsprotokoll aus dem IT-Bereich basieren, als vorteilhaft erweisen.

Die Gefahr bei sehr spezifischen Protokollen, wie zum Beispiel der Applikationsprotokolle der IEC 61850 und IEC 60870, besteht darin, dass diese Protokolle sehr spezifisch sind und außerhalb

der Anwendungen nicht häufig eingesetzt werden. Bei Architekturen, die auf Standard-Webtechnologien, wie REST-APIs (HTTP) oder WebSockets aufbauen, ist die Gefahr geringer, dass die Verbreitung der Protokolle abnimmt.

Die umfangreichen Datenmodelle der IEC 61850 lassen sich eventuell auch nutzen, ohne auf den kompletten Standard zurückzugreifen. Sehr ähnlich wurde das bei der IEEE 2030.5 umgesetzt. Dort wurden eigene Datenstrukturen definiert, die sehr umfangreich sind und eine Übersetzung in das IEC 61850 Datenmodell erlauben. So eine Vorgehensweise wäre auch für eine Österreich Implementierung einer VNB-Schnittstelle denkbar, egal welche Standards oder Protokolle gewählt werden. Das Datenmodell könnte im Rahmen einer Demonstrationsimplementierung der *Digitalen Schnittstelle* entstehen, und in weiterer Folge erweitert bzw. wo nötig reduziert werden.

Für die lokale Schnittstelle ergeben sich viele potenzielle Optionen. Es gibt keinen klaren Favoriten zur Abdeckung aller Geräte aus verschiedenen Domänen. So hat zum Beispiel OCPP und Modbus TCP eine hohe Verbreitung im Bereich der Ladestationen, jedoch im Bereich der Speicher bzw. Photovoltaik Wechselrichter ist Sunspec (Modbus TCP) vorherrschend. In diesem Bereich versucht EEBus das verbindende Protokoll zwischen mehreren Domänen zu werden, ist aber noch nicht weit verbreitet. In Zukunft könnte sich diese Verbreitung aber erhöhen, und dann wäre es möglich mit nur einem lokalen Protokoll mehrere Geräte von unterschiedlichen Herstellern aus unterschiedlichen Domänen zu steuern.

In Anbetracht des komplexen Themenbereichs, der nur zum Teil untersucht wurde, wird eine Umsetzung von Architekturvarianten 1 bis 3 als Demonstration vorgeschlagen. Bei den Demonstrationen soll die Eignung der Standards und Protokolle praktisch untersucht und in Folge bewertet werden. Eine solche beispielhafte Umsetzung würde einen Kenntnisgewinn zu einer Implementierung ermöglichen, der über eine reine Literaturrecherche schwer greifbar ist.

Es gilt festzuhalten, dass das Resultat der Studie zwar richtungsweisend ist, aber nicht der alleinige Pfad zu einer Entscheidung für einen Standard bzw. ein Protokoll für eine *Digitale Schnittstelle* in Österreich sein kann.

G.2 Regulatorische Anforderungen und Änderungsvorschläge

Die Diskussionen haben gezeigt, dass die derzeitigen regulatorischen Rahmenbedingungen für eine praktische Umsetzung einer *Digitalen Schnittstelle* nicht ausreichend sind.

G.2.1 Anpassung der gesetzlichen und regulatorischen Regelwerke

Aus Sicht des Projektteams weisen nachfolgende Regularien einen Änderungsbedarf auf:

- Strommarktgesetz /ElWOG
- Technische und Organisatorische Regeln für Betreiber und Benutzer von Netzen (TOR) betreffend Verteilernetzanschluss (≤ 110 kV) (veröffentlicht – 01.11.22)
- Sonstige Marktregeln
- Systemnutzungsentgeltverordnung – Umsetzung der Tarife 2.1
- TOR-Systemschutzplan

G.2.2 Notwendige Änderungen für rechtliche und regulatorische Regelwerke

Das Elektrizitätswirtschafts- und Organisationsgesetz (ElWOG) regelt die generellen Rahmenbedingungen für alle Marktteilnehmer der Energiewirtschaft in Österreich. Derzeit enthält das ElWOG keine Regelungen zur Steuerung von Lasten in Kundenanlagen durch den Verteilernetzbetreiber. Der aktuelle Diskussionsprozess im Rahmen der umfassenden Überarbeitung und Neugestaltung des ElWOG bietet die Möglichkeit, Impulse und Vorschläge für die im Strommarktgesetz zu regelnden Inhalten und Beschreibungen für eine mögliche gesetzliche Festschreibung der Ansteuerung von elektrischen Einrichtungen im Fall des Netznotzustands.

Die nachstehenden Ansätze sind als Vorschläge und Basis für eine konkrete Ausgestaltung im Gesetz zu bewerten. Mangels eingehender juristischer Prüfung wird nicht der Anspruch erhoben, dass es sich dabei um fertige Vorschläge für die Formulierung als Gesetzestext handelt.

Vorschläge für Regelungen im Rahmen des neuen Strommarktgesetzes:

Adaptierung der grundlegenden Rechte und Pflichten, um den aktuellen Herausforderungen Rechnung zu tragen.

<u>Rechte und Pflichten der Verteilernetzbetreiber</u>

- Engpässe im Netz zu ermitteln und Handlungen zu setzen, um diese zu vermeiden.
- Zur Beherrschung von Notsituationen im Netz (Notzustand) unverzüglich alle angemessenen Maßnahmen zu ergreifen, um schnellstmöglich in einen sicheren Systemzustand zu gelangen. Dabei hat der VNB das Recht, steuerbaren Anlagen über die *Digitale Schnittstelle* Leistungsbeschränkungen vorzugeben.

- Diese Möglichkeit soll einerseits dazu beitragen, Lastabwürfe (Komplettabschaltungen von Netzabschnitten oder einzelnen Netzbenutzern) zu vermeiden, und andererseits einen rascheren Ausbau von Elektromobilität, strombasierten Heizsystemen etc. ermöglichen, da Netzbetreiber durch die Steuerungsmöglichkeit bei der Netzplanung geringere Sicherheitsmargen einkalkulieren müssen.
- Bei der Netzplanung und im Netzbetrieb haben VNB auch die vorausschauende Beschaffung von Flexibilitätsleistungen in Erwägung zu ziehen, die es ihnen ermöglichen, Laststeuerung in Kundenanlagen auch präventiv (vor Eintreten eines Notzustandes) durchzuführen.
- Die Beschaffung von Flexibilitätsleistungen sollte in der Regel mit marktbasierten Instrumenten (z.B. Ausschreibungen von ab- oder zuschaltbarer Leistung in bestimmten Netzabschnitten und Zeiträumen) erfolgen. Eine solche Leistungsvorhaltung durch Netzbenutzer/-kunden hat grundsätzlich auf freiwilliger Basis und gegen finanzielle Abgeltung zu erfolgen."
- Die technische Umsetzung der Leistungsvorgaben liegt in der Verantwortung des VNB bzw. allfälliger Vertragspartner oder Aggregatoren.
- Der VNB muss den Kunden ggf. Aggregator frühzeitig und angemessen (z.B. Wert der Leistungsbegrenzung) über den Eingriff zu informieren, soweit technisch möglich und planbar.

Definition von “Notzustand”

Für die Umsetzung des Use Case „Ansteuerung von Kundenanlagen durch VNB im Notzustand“ ist es notwendig den Begriff „Notzustand“ (im Netz) zu definieren und damit auch gesetzlich festzulegen, unter welchen Voraussetzungen der VNB eine Leistungsvorgabe an die steuerbaren Einrichtungen (z.B. Ladeeinrichtungen) vorgeben darf. Dabei kann auf bereits vorhandene Begriffsbestimmungen der TOR zurückgegriffen werden. Die TOR-Begriffe werden entlang physikalischer Messgrößen bestimmt und definiert den Notzustand wie folgt:[14]

Notzustand

- Zumindest ein definierter Sicherheitsgrenzwert wird nicht eingehalten
- Die Frequenz befindet sich im Emergency-Status (> 200 mHz)
- Mindestens eine Maßnahme des Systemschutzplans ist aktiviert
- Ausfall von Leitsystemen, Kommunikation, etc. > 30 min

[14] (E-Control, 2022)

Des Weiteren finden sich in den TOR-Begriffen noch Begriffsbestimmungen für “Normalzustand” und Gefährdeter Zustand”, als dem Notzustand vorgelagerte Situationen im Netz sowie “Black-out-Zustand" und Netzwiederaufbau-Zustand.

Normalzustand

- Frequenz ist im Normalbereich (Abweichung je nach Zeitdauer unter 50/100 mHz) und
- Wirkleistungs- und Blindleistungsreserven reichen für Ausfälle aus der Ausfallvarianten Liste von Betriebsmitteln aus

Gefährdeter Zustand

- Spannung und Leistungsflüsse sind unterhalb der betrieblichen Grenzwerte, aber mindestens ein Ausfall auf der Ausfallvarianten-Liste führt zu einer Überschreitung der betrieblichen Sicherheitsgrenzwerte des ÜNB, selbst wenn Entlastungsmaßnahmen aktiviert werden oder
- Frequenzabweichung im Alert State (> 100 mHz > 5 min oder > 50 mHz > 15 min)

Black-out-Zustand

- Verlust von mehr als 50 % der Last in der Regelzone des ÜNB; oder
- Spannungslosigkeit in der Regelzone des betreffenden ÜNB für mindestens drei Minuten, sodass Netzwiederaufbaupläne aktiviert werden

Netzwiederaufbau-Zustand

- Wiederaufbau der Versorgung entsprechend den überregionalen und regionalen Konzepten

Liegt ein Notzustand vor, muss der VNB bestimmte Notfallmaßnahmen ergreifen, um weitere Störungen und Ausfälle vermeiden zu können. Ist der Systemzustand außerhalb des Notzustandes können durch präventive Maßnahmen z.B. mit Flexibilitäten bereits erste Maßnahmen umgesetzt werden, um einen Notzustand zu verhindern. Die EU-Strombinnenmarktlinie 2019/944 sieht gemäß Artikel 32 vor, dass der VNB zukünftig Flexibilitäten zur Netzstabilisierung nutzen muss. Die Ausgestaltung der Flexibilitäten war in Phase I ein Nicht-Ziel, sollte aber in der Phase II bearbeitet werden.

Der EP DS empfiehlt demnach “Notzustand” wie folgt zu definieren:

Als „Notzustand“ wird bezeichnet, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- mindestens ein festgelegter betrieblicher Sicherheitsgrenzwert (thermischer Grenzstrom überschritten, Spannung zu hoch oder zu tief gem. EN 50160) wird trotz Einsatz aller Entlastungsmaßnahmen und vertraglich gebundener Wirk-/Blindleistungskapazitäten nicht eingehalten;
- relevante Instrumente, Mittel und/oder Anlagen für den ordentlichen Netzbetrieb und auch die vorgesehenen Backup-Systeme nicht zur Verfügung stehen;
- um eine unmittelbare, auch bloß vermutete Gefahr für Personen oder Sachen abzuwenden;
- bei einer durch höhere Gewalt oder sonstige, nicht in der Sphäre des VNB liegende, Umstände bedingten Verhinderung der Erbringung der Netzdienstleistungen;
- bei Setzung von Maßnahmen zur Vermeidung von Großstörungen und Begrenzung ihrer Auswirkungen gemäß TOR Systemschutzplan;
- bei einem drohenden oder bereits eingetretenen Netzzusammenbruch.

Die Leistungsvorgabe im Notzustand benötigt einen finanziellen Ausgleich bei Inanspruchnahme und erfolgt unabhängig von einem freiwilligen tariflichen Anreiz. Der VNB informiert den Lieferanten und den Netzbenutzer (ggf. Aggregatoren) über die Maßnahme, soweit technisch möglich. Im Notzustand besteht Gefahr, deshalb müssen ausreichend Ladeeinrichtungen reduziert bzw. abgeschaltet werden, um einen Lastabwurf vor einem unmittelbaren Zusammenbruch und weitere Schäden zu vermeiden. Der Notzustand ist kein üblicher oder gewünschter Netzzustand, wodurch eine allgemeine Abwendung der Schadensbegrenzung erfolgen muss. Bei der Ansteuerung darf nicht zwischen privat und öffentlich unterschieden werden. Bei der Ansteuerung im Notzustand darf der VNB nur so viel Einfluss nehmen, wie es nötig ist den stabilen Netzzustand wieder aufrecht zu halten. Nach Einschätzung des EP DS kann nicht definiert, wie oft, wie tief, wie lange abgeregelt werden, da in Notsituationen die dafür notwendige Ansteuerung notwendig ist. Deshalb können keine Qualitätskriterien vorgegeben werden. Möglicherweise könnte ein Richtwert angegeben, z.B. 3 Jahres Durchschnitt ~ 150 Minuten[15]. Wird dieser Richtwert überschritten, sollte ein priorisierter Netzausbau in diesem Netz durchgeführt werden.

Um eine generelle Ansteuerung im Notzustand von Wärmepumpen und Ladeeinrichtungen zu ermöglichen, müssten im diese eine Sonderstellung im ElWOG erhalten, da laut ElWOG jeder Verbraucher gleich zu behandeln ist.

[15] vgl. Richtwert EN 50160 Anzahl Spannungsunterbrechungen

TOR-Systemschutzplan: Einordnung der Ansteuerung im Netznotzustand als "manuellen Lastabwurf"

Der Systemschutzplan Österreich (auch „TOR-Systemschutzplan") beschreibt Maßnahmen zur Beherrschung von kritischen Netzzuständen, zur Vermeidung von Großstörungen bzw. zur Begrenzung ihrer Auswirkungen. Beilage 13.3 des Systemschutzplans beschreibt Grundsätze und Abläufe bei manuellem Lastabwurf. Darin ist geregelt, dass „für die Netzsicherheit und damit für die Einhaltung betrieblicher Grenzwerte (Lastfluss, Spannung und Kurzschlussstrom) – (..) der jeweilige Netzbetreiber (VNB oder ÜNB) zuständig" ist (Seite 4 der Beilage 13.3). Weiteres ist festgelegt, dass „die Auswahl und Umsetzung konkreter Abschaltungsmaßnahmen dem jeweiligen VNB" obliegt.

Eine Abschaltung von steuerbaren Betriebsmitteln ist aus Sicht von AG4 als manueller Lastabwurf bzw. konkreter Abschaltungsmaßnahmen im Sinne dieser Regelung zu werten. Um Rechtssicherheit zu schaffen, wird seitens AG4 empfohlen, die Möglichkeit der Abschaltung von steuerbaren Betriebsmitteln (anstelle oder zusätzlich zur Abschaltung einzelner Netzkunden) ausdrücklich zu erwähnen und als Lastabwurf im Sinne des Systemschutzplans zu definieren.

TOR Verteilernetzanschluss[16]

Einleitend ist festzuhalten, ist der VNB gemäß ElWOG grundsätzlich dazu verpflichtet ist, neue Anlagen anzuschließen. Die im Herbst 2022 veröffentlichen TOR Verteilernetzanschluss gestehen dem VNB allerdings das Recht zu, den Netzanschluss wegen begründeter Sicherheitsbedenken oder mangelnder Netzkapazitäten im Rahmen des § 46 Abs. 2 und 3 ElWOG und der auf dieser Basis ergangen Ausführungsgesetze vorübergehend zur weiteren Prüfung aussetzen. Der Netzbenutzer muss vom relevanten VNB binnen 4 Wochen nach vollständiger Meldung schriftlich über die Gründe des Aussetzens, die maximal mögliche netzwirksame (Summen-)Bemessungsleistung, die netzseitig notwendigen Maßnahmen (i.d.R. Netzverstärkung bzw. Netzausbau), den Zeitplan für deren Durchführung sowie unmittelbar mögliche Alternativen zu dem vom Netzbenutzer eingereichten Netzanschluss aufgeklärt. Solche Alternativen können bspw. die Änderung des Netzanschlusspunktes, das Vorsehen einer dynamischen Leistungsregelung zur Begrenzung der netzwirksamen Bezugsleistung oder der Anschluss über einen Netzanschlusspunkt mit unterbrechbarem Tarif sein. Kann eine Anlage aufgrund nicht ausreichender Netzkapazitäten nicht sofort angeschlossen werden, muss sichergestellt werden, dass der Netzausbau zeitgerecht umgesetzt wird, damit nicht alle Ladeeinrichtungen über den Notzustand angesteuert werden. Eine zentrale Rolle spielt dabei der Netzentwicklungsplan für Verteilernetze der alle 2 Jahre durchgeführt werden muss. Grundsätzlich gilt aber die Allgemeine Anschlusspflicht. Die Netze werden

[16] https://www.e-control.at/marktteilnehmer/strom/marktregeln/tor

also entsprechend den neuen Anforderungen (E-Mobilität, Wärmepumpen etc.) auszubauen sein. Abschließend ist nicht geklärt, welche Vorgehensweise der VNB wählen soll, wenn keine Netzkapazitäten vorhanden sind und mehrere Leistungsanfragen anstehen. Dabei stellt sich die Frage, welche Leistung zuerst bedient oder Leistungsreserven aufteilt werden sollen.

Mit Blick auf die rechtliche Einordnung der TOR ist darauf hinzuweisen, dass gemäß § 22 Z 2 E-Control Technische Organisatorische Regeln von der E-Control in Zusammenarbeit mit den Betreibern von Elektrizitätsnetzen im Zuge der Erledigung der Regulierungsaufgaben für die Betreiber und Nutzer von Netzen zu erarbeiten und diesen zur Verfügung zu stellen. Die TOR werden mit einem Abschluss eines Netzanschlussvertrages zwischen VNB und Netzkunde entfalten ihre Wirkung.

Die neuen TOR Verteilernetzanschluss[17] enthalten technische und organisatorische Mindestanforderungen für den Anschluss und Parallelbetrieb von Netzen und Lasten in der Hochspannung, Mittelspannung und Niederspannung. In diesem Regelwerk wurden die technischen Anforderungen für steuerbare elektrische Einrichtungen definiert. Nachfolgend die notwendigen technischen Anforderungen laut TOR Verteilernetzanschluss, welche für die Diskussion der Erarbeitung einer *Digitalen Schnittstelle* von Relevanz sind:

TOR-Verteilernetzanschluss, Kapitel 5.9.2: Kommunikationsfähigkeit, Steuerbarkeit und Programmierbarkeit von Ladeeinrichtungen[18]

Grundsätzlichen müssen alle Ladeeinrichtungen (mobile und festmontiert) > 3,68 bei VNB gemeldet werden.

Ladeeinrichtungen (mobile und festmontiert) > 3,68 kVA müssen über eine bidirektionale digitale Kommunikationsschnittstelle verfügen. Diese Schnittstelle kann kabelgebunden oder kabellos umgesetzt sein. Die Ladeeinrichtung muss über diese Schnittstelle mittels einem gängigen, auf einem offenen Standard basierenden Kommunikationsprotokoll (bspw. OCPP, EEBUS) mit anderen Komponenten des Energiesystems kommunizieren können und eine externe Ansteuerung (Beschränkung der Ladeleistung) ermöglichen. Die Kommunikationsfähigkeit kann wahlweise über die Ladeeinrichtung selbst oder eine mit der Ladeeinrichtung permanent verbundene Infrastruktur (wie Lade- bzw. Energiemanagementsysteme oder „Smart-Home-Systeme“) bewerkstelligt werden.

[17] gültig seit 01.11.22

[18] Vgl. TOR Verteilernetzanschluss

Befindet sich innerhalb einer Kundenanlage nur eine Ladeeinrichtung < 10 kVA und erfolgt der Netzanschluss vor dem 1. Jänner 2025, ist anstelle einer bidirektionalen digitalen Schnittstelle ein potenzialfreier Kontakt, der eine externe Ansteuerung (Abschaltung) ermöglicht, zulässig. Ladeeinrichtungen > 3,68 kVA, die ab dem 1. Jänner 2025 erstmals an das Netz angeschlossen werden, müssen jedenfalls über eine bidirektionale digitale Kommunikationsschnittstelle verfügen.

Ladeeinrichtungen > 3,68 kVA müssen über Ladeprogramme verfügen, die das Laden bei reduzierter Leistung sowie eine zeitliche Steuerung von Ladevorgängen (z.B. verzögerter Start des Ladevorgangs oder Vorgabe von Ladezeiten) ermöglichen. Bei Programmen, die einen Start des Ladevorgangs zu einer vom Benutzer festgelegten Uhrzeit vorsehen, ist eine Verzögerung des tatsächlichen Ladestarts um eine zufällige Zeitspanne von 0 bis 300 Sekunden umzusetzen.

Die Anforderungen treten ab dem 1. Jänner 2024 in Kraft. Diese Anforderungen begründen weder eine Verpflichtung zur Übermittlung von Daten aus der Ladeeinrichtung an den Netzbetreiber oder andere Marktakteure, noch ein generelles Recht auf Ansteuerung für den Netzbetreiber.

TOR Verteilernetzanschluss, Kapitel 5.10: Steuerbarkeit von Wärmepumpen in der Niederspannung[19]

Erfolgt der Anschluss einer Wärmepumpe über einen Netzanschlusspunkt mit unterbrechbarem Tarif oder wird eine anderweitige vertragliche Regelung zwischen dem Netzbenutzer und dem VNB getroffen, die es dem VNB erlaubt, den Leistungsbezug der Wärmepumpe temporär zu beeinflussen, so kann der VNB fordern, dass die Steuerung wärmepumpenseitig über eine SG-Ready-Schnittstelle realisiert wird.

Wärmepumpen mit einer maximalen Leistungsaufnahme (d.h. Verdichter + Heizstab) ≥ 10 kW müssen auf jeden Fall über eine SG-Ready-Schnittstelle verfügen.

Hinsichtlich der am österreichischen Markt verfügbaren Wärmepumpen mit SG-Ready-Schnittstelle wird auf die Produktdatenbank von Wärmepumpe Austria verwiesen (https://www.waermepumpe-austria.at/oesterreichische-produkt-datenbank). Die Anforderungen treten ab dem 1. Jänner 2024 in Kraft.

[19] Vgl. TOR Verteilernetzanschluss

Insgesamt kann festgehalten werden, dass durch die technischen Anforderungen für Ladeeinrichtungen und Wärmepumpen in der TOR-Verteilernetzanschluss eine technische Vorrausetzung für die Umsetzung einer *Digitalen Schnittstelle* geschaffen wurde.

Rahmenbedingungen für die Inanspruchnahme der Option einer freiwilligen Ansteuerung:

Nach Einschätzung des EP DS kann derzeit grundsätzlich der „unterbrechbare-Tarif mit zusätzlichem Zähler" auch für Ladeeinrichtungen verwendet werden. Die Ansteuerung muss in diesem Fall allerdings zu fixen Zeiten vorgegeben werden. Die Ladeleistung muss unterbrochen werden und darf nicht nur reduziert werden. Für die Installation muss die Ladeeinrichtung jedoch an einem separaten Zähler installiert werden, wodurch zusätzliche Kosten für den Kunden entstehen. Demnach bedarf es angemessenerer Lösungen um die Kapazitäten im Netz optimaler zu nutzen.

Zusätzlich sollen Netzbenutzer:innen die freiwillige Option erhalten, gegen eine netztarifliche Entlastung dem VNB ein Recht auf Ansteuerung einzuräumen. Die Netzbeutzer:innen sowie andere relevante Akteur:innen (Lieferant, CPO, Aggregator) werden über die Maßnahme informiert. Die Ansteuerung der Ladeeinrichtung ist unabhängig von Betriebsmitteln und Belastbarkeit bzw. realer Auslastung durchzuführen. Des Weiteren können die Netzbenutzer:innen ihre Kundenanlagen als Flexibilität vermarkten. Die Flexibilität wird durch einen Aggregator über den VNB beeinflusst. Der rechtliche und organisatorische Ablauf zur Nutzung von Flexibilitäten wird derzeit in diversen Gremien und Expertengruppen erarbeitet und zukünftig ermöglicht.

Für neue steuerbare elektrische Einrichtungen, die wegen ihrer Leistungsgröße, ihrem Gleichzeitigkeitsverhalten oder ihrer Betriebsweise maßgeblich Einfluss auf die Systemauslegung in ihrer oder den übergeordneten Netzebenen haben, könnte eine mögliche Option sein, dass zusätzlich im Netzzugangsvertrag vorgesehen wird, dass der VNB die maximale mit dem Verteilernetz ausgetauschte Leistung in beide Energieflussrichtungen vorgibt, wenn die Gefahr der Überlastung der Netzinfrastruktur oder der Nichterfüllung der vereinbarten oder allgemein geforderten Spannungsqualität besteht und diese damit vermindert oder vermieden werden kann. Die Ansteuerung von Ladeeinrichtungen über eine *Digitale Schnittstelle* kann in der Praxis durch die Leistungsvorgaben im Notzustand als generelle Verpflichtung und als freiwillige Option für Flexibilitäten verbreitet eingesetzt werden. Aktuell werden seitens der Umweltförderung bereits intelligente Wallboxen finanziell gefördert.

Über die Tarife 2.1 können zukünftig Anreize für flexible Lasten (steuerbare elektrische Einrichtungen) finanziell angeboten werden. Das bedeutet, dass der Kunde seine Ladeeinrichtung intelligent ansteuern kann, um Kosten einsparen zu können. Die Ansteuerung sollte über einen Anreiz erfolgen, indem dem der Kunde auf freiwilliger Basis einen flexiblen Tarif mit Ansteuerung wählen kann. Wie im Tarifmodell „Tarife 2.1" der E-Control beschrieben, wird es zukünftig neben dem Standardkunden einen regelbaren Kunden geben. Der regelbare Kunde kann für die Grundlast

(z.B. Beleuchtung, Kochen) eine garantierte Leistung beziehen und für regelbare Lasten (z.B. Wärmepumpe, Ladeeinrichtungen) eine eingeschränkte Leistung beziehen, siehe Abbildung 26.

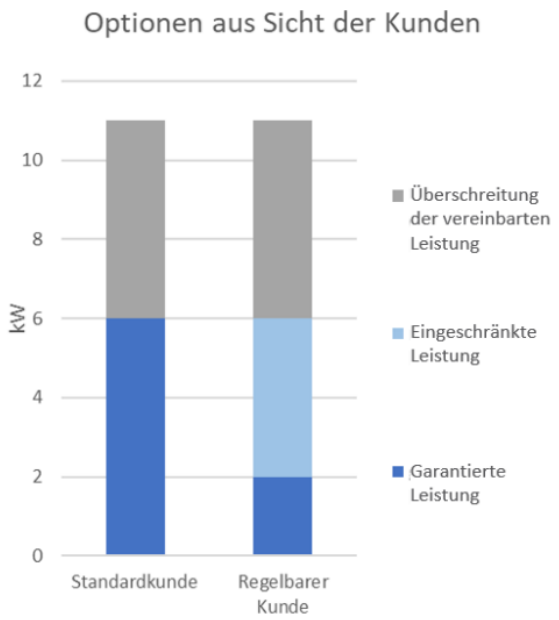

Abbildung 26: Flexibilitätsoptionen aus Sicht der Kunden, (E-Control, 2022)

Dabei sollen Kund:innen weiterhin die Wahlfreiheit haben, ob die Option der Ansteuerung durch den VNB gewährt wird oder nicht. Es muss sichergestellt werden, dass der Kunde ausreichende Mobilität, Wärme und Einspeiseleistung erhält, wenn der Kunde die freiwillige Ansteuerung nicht wählt. Im Fall eines Netzanschlussvertrages mit freiwilliger Ansteuerung ist den Kund:innen das Recht auf Ansteuerung auch mit einer entsprechenden Reduktion der Netzentgelte abzugelten.

G.2.3 Nutzung der Smart-Meter-Daten

Status Quo

Gemäß ElWOG § 84a (5) dürfen mittels intelligenter Messgeräte gemessene Verbrauchsdaten nicht für andere Zwecke als die in leg. cit. genannten verwendet werden. Dies sind hauptsächlich die Messung, Speicherung und Übertragung von Verbrauchswerten an VNB und Lieferanten zur Abrechnung, in begründeten lokalen Einzelfällen aber auch die Auslesung und Verwendung von Viertelstundenwerten ohne Kundenzustimmung, sofern dies zur Aufrechterhaltung eines sicheren und effizienten Netzbetriebes erforderlich ist.

Auslesen der Energiewerte durch VNB

- Standard-Einstellung: übermittelt täglich Tagesverbrauch am Folgetag
- Opt-In: übermittelt täglich die 15min-Werte am Folgetag
- Opt-Out: keine Speicherung von Verbrauchswerten. Auslesung des Zählerstandes nur für Abrechnungszwecke oder Verbrauchsabgrenzungen (Einzug/ Auszug/ Tarifwechsel).

Handlungsempfehlungen zum Auslesen der Netzspannung und Leistungswerte[20]

Handlungsempfehlungen zum Auslesen der Netzspannung im 10min-Raster durch VNB

- von vereinzelten Smart Metern entlang eines Stranges
  - d.h. nahe der Trafostation und nahe am Strangende
- darf die Netzspannung im 10min-Raster aufgezeichnet
- im Smart Meter für eine begrenzte Zeit (maximal 60 Tage) gespeichert
- und um Mitternacht übertragen werden
- BEACHTE: von Opt-Out-Zählern dürfen keine Messwerte ausgelesen werden!
- die Daten sind unmittelbar nach Verwendung, spätestens aber nach 3 Jahren zu löschen
- Aufzeichnung von Netzspannungswerten ist nur bei so wenigen Smart Metern wie nötig am Strang zulässig, dass hiermit keine Rückschlüsse auf das Verbrauchsverhalten der einzelnen Endverbraucher möglich sind
- Betroffene Personen sind über die Auslesung dieser Daten zu informieren!

Handlungsempfehlungen zur Auslesung und Verwendung von 15min-Werte in begründeten lokalen Einzelfällen durch VNB

- Lt. §84a Abs. (1) ElWOG dürfen Verteilernetzbetreiber Viertelstundenwerte
  - **in begründeten lokalen Einzelfällen** auch ohne Zustimmung des Endverbrauchers aus dem intelligenten Messgerät auslesen
  - soweit dies für den Zweck der Aufrechterhaltung eines sicheren und effizienten Netzbetriebes **unabdingbar ist**
  - diese Daten sind **unverzüglich zu löschen**, sobald sie für die Erfüllung des Zwecks nicht mehr benötigt werden
  - VNB haben **der Regulierungsbehörde jährlich einen Bericht** über die Anlassfälle für derartige Datenauslesungen zu legen
  - Der **Endverbraucher ist** im Falle einer Auslesung der Viertelstundenwerte ohne Einwilligung **zeitnah darüber zu informieren**

[20] Empfehlung basiert auf der Stellungnahme von Dr. Gerald Trieb, LL.M., im Auftrag von Österreichs E-Wirtschaft „Spannungsqualität/ Datenschutzrecht: Ihre Anfrage zur Zulässigkeit der Verarbeitung von Daten zur Spannungsqualität von Netzbenutzern“ vom 25. Juni 2020.

Handlungsempfehlungen zur Verwendung der Kundenschnittstelle

- die über die **Kundenschnittstelle** (Home-Area-Network - HAN) an ein externes Steuergerät übertragenen Werte (Netzspannung und Leistung) bei Haushalten mit Ladeeinrichtungen dürfen
    - nur im Steuergerät selbst verwendet werden und
- die **Auslesung** dieser Daten aus ggf. einem **Steuergerät** ist nur zu Zwecken der Fehleranalyse oder Anpassung des Steueralgorithmus zulässig
    - die Daten sind soweit wie möglich zu anonymisieren
    - Die Aufbewahrungsfrist beläuft sich auf mindestens 3 Jahre, da der Kunde 3 Jahre lang ein Recht auf Schadenersatz hat, wenn bei der Fehleranalyse oder bei Anpassungen ein Schaden entsteht

Empfehlung zur Nutzung der Smart-Meter Daten[21]

Die aufgezeigten Unwägbarkeiten bei der Netzplanung und im Netzbetrieb zeigen das zunehmende Erfordernis von mehr Informationen auch in den unteren Spannungsebenen auf. Die aktuellen gesetzlichen Rahmenbedingungen erlauben lediglich einen sehr eingeschränkten Zugriff sowie Verwendung der Smart-Meter Daten. Nur bei konsequenter Nutzung aller zur Verfügung stehenden Informationsquellen erscheint es möglich, die zusätzlichen Anforderungen an die Niederspannungsnetze kosteneffizient zu beherrschen. Die Nutzung der Messwerte aus Smart Metern (Verbrauchs-, Leistungs- und Spannungswerte, sowie Leistungsfaktor) zum Zwecke der Netzplanung und Netzbetrieb können dazu beitragen, einen sicheren und effizienten Netzbetrieb zu gewährleisten. Die Energie- und Klimaziele sowie die dazu erforderlichen Maßnahmen und Instrumente wie die Einführung von Energiegemeinschaften, die Verbreitung von Elektromobilität und der Erneuerbaren-Ausbau (insbesondere auch PV) können damit wirkungsvoll unterstützt werden.

Die volkswirtschaftlichen Investitionen von bisher etwa 1,7 Mrd. Euro[22] für die Smart Meter Einführung können damit für die gesamte Bevölkerung verstärkt nutzbar gemacht werden. Damit kann der Investitionsbedarf für den erforderlichen Umbau des Energiesystems und der dazu erforderliche Ausbau des Stromsystems optimiert werden. Eine Anpassung der rechtlichen Rahmenbedingungen für eine entsprechende Nutzung von Messdaten aus intelligenten Messgeräten erscheint angesichts der aufgezeigten Entwicklungen als erforderlich.

[21] Empfehlung Arbeitskreis Verteilernetze, Oesterreichs Energie

[22] https://www.diepresse.com/6202096/ausrollung-der-smart-meter-kommt-in-schwung

Der Smart-Meter-Rollout in Österreich verläuft regional sehr unterschiedlich. Gemäß der Intelligente Messgeräte-Einführungsverordnung (IME-VO) ist das Ziel, mindestens 95% der Haushalte bis Ende 2024 mit einem Smart Meter ausgestattet sind - siehe nachfolgende Abbildung 27.[23]

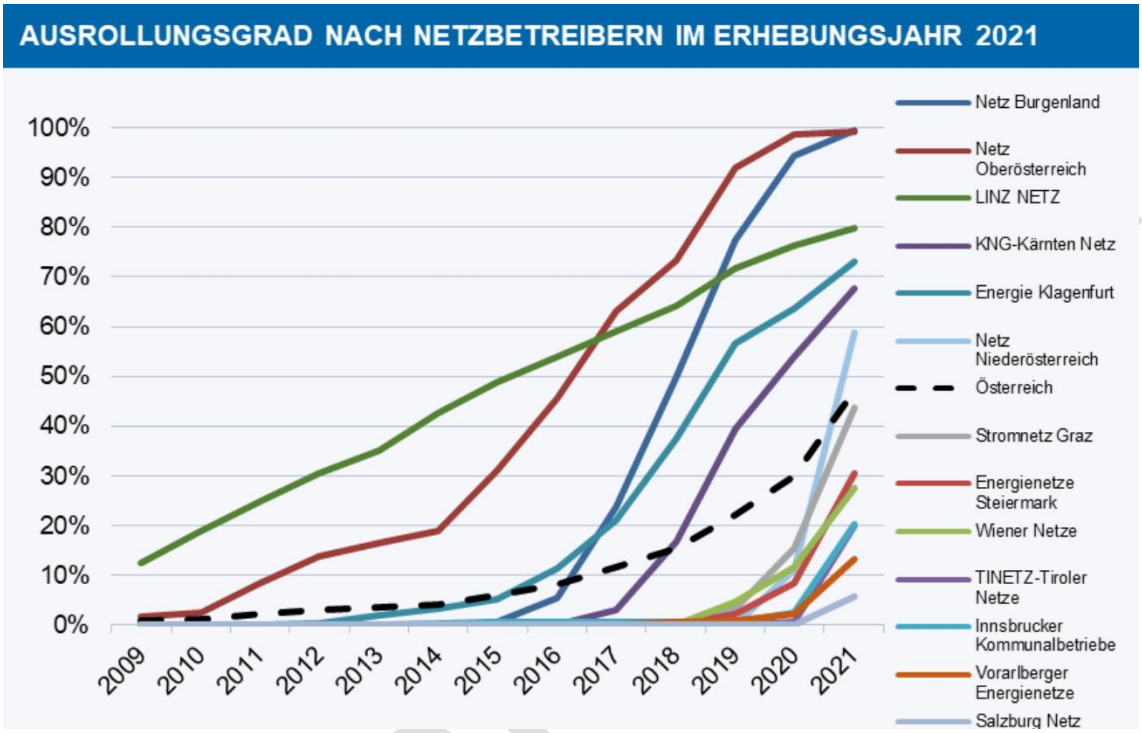

Abbildung 27: Ausrollungsgrad nach Netzbetreibern im Erhebungsjahr 2021(E-Control)

Im Rahmen einer umfassenden Überarbeitung des ElWOG werden auch rechtliche Änderungen diskutiert, die eine maximale Systemnutzung der Smart Meter Daten zur besseren Analyse und Planung der Netze bei gleichzeitiger Wahrung des Datenschutzes sicherstellen sollen. Die Regulierungsbehörde spricht sich dafür aus, dass zukünftig die Erfassung & Übermittlung von Viertelstundenwerte der Smart-Meter als neue Standardeinstellung vorgesehen wird.[24]

[23] BERICHT ZUR EINFÜHRUNG VON INTELLIGENTEN MESSGERÄTEN IN ÖSTERREICH 2022 BERICHTSJAHR 2021

[24] Vgl. Vortrag Dr. Kalt, „Ladeeinrichtungen für Elektrofahrzeuge in den neuen „TOR Verteilernetzanschluss“, Mobilitätstage OE, Wien

H. Fazit und Ausblick

H.1 Fazit

Die Annäherung an das Projektziel *Digitale Schnittstelle* erfolgte generisch und mit einer breiten Beteiligung relevanter Stakeholder. Für eine *Digitale Schnittstelle* wurde in einer ersten Stufe der Use Case „Ansteuerung von Kundenanlagen durch VNB im Notzustand“ und 5 weitere Use Cases beschrieben.

Für die Umsetzung konnten grundsätzlich 3 Architekturvarianten erarbeitet werden, bei denen eine Kommunikation zwischen Netzbetreiber und Kundenanlage entweder durch eine *Digitale Schnittstelle* über Aggregatoren, eine zentrale *Digitale Schnittstelle* oder eine *Digitale Schnittstelle* über einen Funktionsblock erfolgt. Die Leistungsvorgabe durch den VNB erfolgt dabei immer auf eine Komponente(n) oder ein EMS. Die exakte Verortung des Verantwortungsüberganges (z.B. Hausanschluss, Zählerverteiler, weitere Varianten) war nicht Gegenstand dieser Projektphase 1.

Die umfangreichen Bewertungen einer Reihe von internationalen Standards durch ein AIT-Expertenteam erbrachte bei einigen, dass sie grundsätzlich für den Einsatz geeignet wären (siehe Kap.G.1 Empfehlung zur Umsetzung – Fazit der AIT-Studie). Hierzu ist beabsichtigt, durch IKT-Experten der VNB in der nächsten Projektphase die wichtigsten VNB-Prozesse und deren Schutzlevel in einer vertiefenden Business Impact Analyse auszuwerten. Dies soll letztlich die Entscheidung über eine Auswahl der Standards und Protokolle auf eine solidere Basis stellen. Derzeit ist noch keine Festlegung auf einen bestimmten Standard möglich. Im Zuge des Projekts wurden aktuelle Praxisbeispiele vorgestellt, siehe Kapitel J.4.

In die Erarbeitung der Ergebnisse wurden verschiedene Stakeholder eingebunden und deren Anforderungen berücksichtigt. Bis zu einer Umsetzung einer *Digitalen Schnittstelle* gibt es noch viele offene Fragen zu klären und großen Abstimmungsbedarf. Die Weite des Handlungsfeldes eröffnete sich während des Projektfortschritts immer mehr. Dies zeigte sich auch dadurch, dass sich während der Arbeiten immer wieder neue Teilnehmer zur Mitwirkung einreihten, sodass am Ende deutlich mehr als 50 Personen im Projekt aktiv dabei waren. Deutlich spürbar ist auch das Interesse der Vertriebe, sich mit maßgeschneiderten Produkten an der Optimierung des Netzproblems beteiligen zu wollen. Die Herstellerindustrie und Verbände (Wärmepumpe, Photovoltaik) brachten sich stark gestaltend mit ein.

Rechtlich und regulatorisch konnten bereits eine Reihe von Unklarheiten aufgearbeitet werden. Insbesondere konnten Präzisierungen erarbeitet werden, wann der Zustand „Notzustand“ vorherrscht. Des Weiteren wurden während der Projektphase 1 durch die Veröffentlichung der neuen Marktregel TOR Verteilernetzanschluss am 17.10.2022 erste Umsetzungen auf dem Weg zu einer *Digitalen Schnittstelle* eingeleitet. Inhaltliche Ideen für ein neues ElWOG wurden formuliert.

Derzeit fehlende Regelungen wurden gelistet, etwa wie bei massiver Überforderung der Netze vorgegangen werden soll. Wichtig für die Weiterführung des Projektes werden Konkretisierungen des Regulators zum Positionspapier Netztarife V2.1 sein, da Netzzugangsverträge mit einer Steuerungsoption für den VNB noch detaillierter auszugestalten sind.

Insgesamt sehen alle Projektbeteiligten die Einführung einer Digitalen Schnittstelle als einen positiven Schritt für eine erfolgreiche Erreichung der Energie- und Klimaziele. Bilanziert man die gewonnenen Ergebnisse der Projektphase 1 (2022), ergeben sich in Richtung einer Umsetzung die nachfolgenden Handlungsempfehlungen. Parallel zur Ausgestaltung neuer Flexibilitätsmöglichkeiten muss der Netzausbau und die Verbesserung der Sensorik im Verteilernetz aktiv vorangetrieben werden.

H.2 Handlungsempfehlungen

Gesetzgeber / Regulator

Um eine möglichst rasche Bereitstellung einer *Digitalen Schnittstelle* zu ermöglichen, ist an erster Stelle rechtlich zu klären, welche Rechte und Pflichten der VNB im „Notzustand“ und bei einer freiwilligen Ansteuerung hat. Dazu gehört, dass der Netzzustand „Notzustand“ definiert wird.

Für Handlungen, die in einer Vorstufe vor einer Notsituation der Abwendung von unzulässigen Netzsituationen dienen, ist eine möglichst rasche Konkretisierung des Dokuments Tarife 2.1[25] gefolgt von einer Umsetzung in entsprechenden Verordnungen zu nennen. Speziell allfällige Vorgaben für die Ausgestaltung von Netzzugangsverträgen mit einer Steuerungsoption (Vorgabe von Leistungswerten) für den VNB sind wesentlich für:

- die Auslegung des technischen Systems zur Administration und Umsetzung solcher Netzzugangsverträge
- Gestaltung eines Marktprozesses zur Anwendung der Digitalen Schnittstelle
- die Adaptierung der bestehenden VNB-Betriebsprozesse und die Planung und Bereitstellung der erforderlichen Ressourcen
- die Markteinschätzung durch die Industrie, die die erforderlichen Systemkomponenten entwickeln und liefern muss. Hier steht der potenzielle Nutzen für die Netzkunden im Vordergrund, um die entsprechenden Investitionen in die erforderlichen Entwicklungen auszulösen.

Darüber hinaus muss berücksichtigt werden, dass eine erfolgreiche Einführung von Netzzugangsverträgen mit VNB-Steuerungsoption nur dann möglich sein wird, wenn die Industrie und

[25] https://www.e-control.at/marktteilnehmer/strom/netzentgelte/tarife-2-1

Lieferanten bzw. Energiedienstleister (z.B. auch Aggregatoren) „Plug and Play"-Lösungen anbieten können. Dafür ist es wesentlich, dass bei mehreren steuerbaren Anlagen wie „Dezentrale Erzeugung", „Wärmepumpen", „Ladeinfrastruktur" und „Speicher" für die Anwender einfach bedienbar ein Energiemanagementsystem (z.B. in Kundenanlage oder Cloud) zur Leistungsaufteilung nach Kundenvorgaben vorhanden ist. An einem Lösungsansatz, wie dies domänenübergreifend und herstellerübergreifend sichergestellt werden kann, arbeitet die herstellerunabhängige Smart Grid Ready Initiative[26] in der Schweiz. Daher ist zu überlegen, ob diese Initiative für Österreich auch zielführend ist.

Zu klären ist dabei auch der Verantwortungsübergang zwischen VNB und Kundenanlage mit und ohne Funktionsblock. Des Weiteren muss geklärt werden, wie die Kosten von den Partnern der Digitalen Schnittstelle finanziert und getragen werden. Ein weiterer wichtiger Punkt im Zusammenhang mit einer *Digitalen Schnittstelle* ist eine erweiterte Nutzung von Zählerdaten für die VNB-internen Prozesse im Bereich der Netzplanung und des Netzbetriebs, sowie einen diskriminierungsfreien Zugang für weitere Marktakteure. Sie ermöglicht eine frühzeitige Erkennung von potenziellen Netzengpässen und erlaubt eine Modellierung von Netzkunden, die betrieblich im Zusammenhang mit Netzengpassprognosen und der Ableitung von Steuerungsmaßnahmen hohe Relevanz haben kann.

Der Expertenpool empfiehlt, dass sich der Regulator mit der Mitgestaltung der zukünftigen *Digitalen Schnittstelle* aktiv einbringt und eine einheitliche Lösung für Österreich vorantreibt. Neben den rechtlichen und regulatorischen Rahmenbedingungen ist zudem wichtig, dass wirtschaftliche Rahmenbedingungen und Anreize für die Umsetzung einer Digitalen Schnittstelle für den VNB und die Stakeholder geschaffen werden.

Verteilernetzbetreiber

Im Bereich der Verteilernetzbetreiber ist eine Erweiterung / Weiterführung der bereits angedachten bzw. in Umsetzung befindlichen Digitalisierungskonzepte dringend erforderlich:

- Zentrale Erfassung von aktuellen und historischen Mess- Auslastungs- und Topologiedaten für die untersten Netzebenen bis zum Kundenanschluss als Basis für Trendanalysen, Prognosen, Ermittlung/Optimierung von wirtschaftlichen Betriebsmittelauslastungen und neuen Rahmenbedingungen für die Netzplanung

[26] https://smartgridready.ch/

- Adaptierung der Netzplanungsprozesse vorausschauend in Hinblick auf die Anforderungen der Energiesystemwende (stärker basierend auf aktuellen Daten, Data-Analytics, Einbeziehung von Laststeuerung als Baustein in der Netzplanung und der Lastflusssimulation…)
- Neben dem verstärkten Netzausbau ist die Ausrollung von intelligenten Trafostationen mit Sensorik erforderlich, sowie die Verarbeitung und Auswertung von Messdaten und daraus resultierende Ableitungen für Leistungsvorgaben
- Adaptierung der Netzbetriebsführung (dezentrale selbst organisierte Netzzellen versus zentrale Netzbetriebsführung über Leitsysteme, sowie ÜNB-VNB-Koordination im Netzbetrieb, insbesondere bei Systemdienstleistungen und Flexibilitätsleistungen), im Besonderen:
    - Wo werden im Betrieb Netzengpässe (netzebenenbezogen) festgestellt? Wie erfolgt die übergeordnete Koordination und die Ableitung von Steuerungsmaßnahmen?
    - Wie werden Steuerungsmaßnahmen dokumentiert und dritten Berechtigten zugänglich gemacht?
    - Wie erfolgt das Monitoring der Einhaltung der Bedingungen in den Netzzugangsverträgen und ggf. Berücksichtigung der Monitoring-Ergebnisse bei der Ableitung der Steuerungsmaßnahmen?
- Planung, Ausrollung und Betrieb der zusätzlich erforderlichen Sekundärtechnik in den untersten Netzebenen (z.B. Messtechnik, Steuerungs- und Überwachungseinrichtungen)
- Bereitstellung einer Digitalen Plattform zum Austausch zwischen VNB und externen Marktpartner:
    - für Aggregatoren zur Umsetzung von erforderlichen Steuerungsmaßnahmen und für den Empfang von aktuellen Messwerten
    - für das Ansprechen von Flexibilitäten für einen erweiterten Datenaustausch mit den Netzkunden
    - für den Datenaustausch mit Energiegemeinschaften, Kommunen, Ländern, Regierungsstellen, Regulator…
    - für den Bezug externer Daten (Datendienstleister wie Wetterdienste, Marktanalysten, Anbieter von statistischen Daten…)
- Aufbauend auf den Ergebnissen des Expertenpools „*Digitale Schnittstelle*":
    - Einschränken der vorgeschlagenen Varianten auf die in einem ersten Schritt zu realisierenden Varianten
    - Festlegung der Prozessdetails die mit dem Errichten und dem Betrieb von einer *Digitale Schnittstelle* verbunden sind (Geräteprovisionierung bzw. Onboarding, Fehlermanagement, Administration von Vertragsänderungen…)
    - Festlegen der Prozessdetails, die mit dem Betrieb einer zentralen Schnittstelle verbunden sind, hier speziell für die Kommunikation mit Dritten (Steuerungsfunktionen, Ist-Datenbereitstellung Zugangsberechtigungen, Zählpunktverwaltung…)

- Ableitung und Festlegung der Anforderungen für die Erfüllung der NIS-Gesetzgebung für die *Digitale Schnittstelle* und die zentrale Schnittstelle
- Erstellung einer Lösungsspezifikation, die die Entwicklung der ersten Prototypen erlaubt
- Durchführung von Feldtests zur Überprüfung der Funktionalität und der Optimierung der Betriebsprozessintegration

Eine möglichst frühzeitige Zusammenarbeit bei den vorgenannten Themen zwischen VNB, Lieferanten/CPO/Aggregatoren, Forschungsinstitutionen und der Industrie wird empfohlen, um die erforderliche Akzeptanz herzustellen, Stranded Investments zu vermeiden und frühzeitig zu skalierbaren Lösungskonzepten zu kommen.

Industrie

Industriehersteller, die Lösungen für VNB anbieten:

- Konsolidierung und ggf. Ergänzung der aus Forschungsprojekten bekannten Verfahren zur Ermittlung von Netzengpässen in Verteilernetzen
- Ermittlung der Anforderungen zur VNB-Prozessintegration zusammen mit den Verteilernetzbetreibern
- Entwicklung und Bereitstellung erster Prototypen für Feldtests

Industriepartner, die Geräte / Lösungen für Netzkunden anbieten:

- Entwicklung und Bereitstellung erster Prototypen von Geräten, die die Digitale Schnittstelle unterstützen
- Ggf. Unterstützung von „Smart Grid Ready Anforderungen“
- Entwicklung von interoperablen Geräten/Systemen
- Ggf. Unterstützung der IES-Methodik zur Spezifikation der Digitalen Schnittstelle unter Berücksichtigung der Interoperabilität

Lieferanten, CPO, Aggregatoren:

- Entwicklung von Geschäftsmodellen im Zusammenhang mit der beauftragten Umsetzung von Steuerungsmaßnahmen von Netzbetreibern und/oder einer Mitnutzung einer Steuerungsinfrastruktur, die von VNB betrieben wird.
- Einbringen von entsprechenden Anforderungen in die für die Ausgestaltung der zentralen VNB-Schnittstelle relevanten Diskussionen
- Mitwirkung bei Feldtests zur Überprüfung der Funktionalität und der Optimierung der Betriebsprozessintegration

H.3 Ausblick auf die Projektphase 2 (2023ff)

Die in diesem Bericht niedergeschriebenen Ergebnisse der Projektphase 1 (2022) dienen 2023ff als Ausgangsbasis für weitere Schritte zur Einführung einer Digitalen Schnittstelle. Die in Kapitel H.2 genannten Handlungsfelder sind in Arbeitspakete zusammenzufassen und in einem Projektablaufplan zu organisieren. Dabei wird für die drei Architekturvarianten ein Handlungspfad beschrieben, siehe nachfolgende Abbildung 28. Dabei wird empfohlen, dass die Netzbetreiber ein Strategieteam installieren, das die Ergebnisse der Phase 1 einer Diskussion innerhalb der VNB unterzieht, eine neue Projektorganisation mit neuer Projektleitung ernennt und die Weiterführung des Projektes in Angriff nimmt. Die Zusammenstellung der vorgeschlagenen Experten ist in Abbildung 29 ersichtlich.

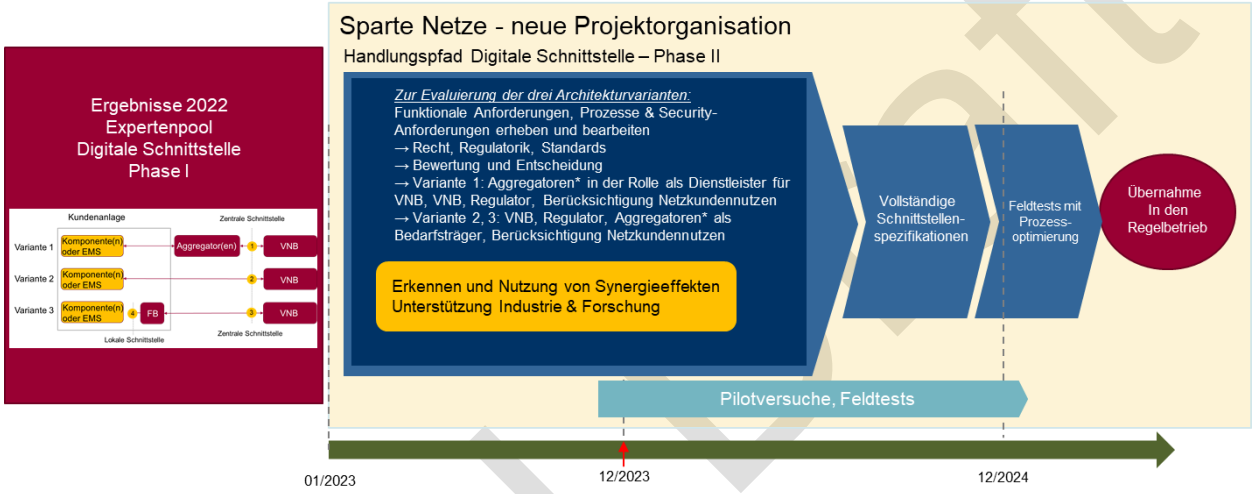

Abbildung 28: Fortführung 2023 ff, Handlungsempfehlungen

Abbildung 29: Zusammenstellung der vorgeschlagenen Experten für die Phase 2

Ergänzend zu diesen Maßnahmen ist technisch eine „Digitale Plattform“ für Aggregator-Lösungen zu erarbeiten. Ein weiterer Punkt, der in der Phase 2 betrachtet werden muss, sind alle Kosten, die aufgrund der digitalen Schnittstelle anfallen (vgl. Kapitel F.5) und wie diese Kosten abgegolten werden.

I. Literaturverzeichnis

Agora Verkehrswende. (2019). *Verteilnetzausbau für die Energiewende - Elektromobilität im Fokus.* Berlin: Agora Energiewende.

Bienert, R. (2022). *How OpenADR can Compare with IEEE 2030.5 for California Rule 21.* Webinar: OpenADR Alliance.

BMK. (2021). *Erneuerbaren-Ausbau-Gesetz.* Wien: Bundesministerium für Klimaschutz, Umwelt, Energie, Mobiltität, Innovation und Technolgie.

BMK. (2022). *Bestand an Wärmepumpen in Österreich.* Wien: Oesterreichs Energie.

Bundesministerium für Verkehr, Innovation und Technologie. (05-12-2022). *Österreichische Technologie-Roadmap für Wärmepumpen*. Von https://waermepumpe-izw.de/wp-content/uploads/2020/05/160600_-Austria-Technologieroadmap-WP.pdf abgerufen

Bundesminsterium für Klimaschutz, Umwelt, Energie. (2022). *Bestand PV Anlagen.* Wien: BMK.

CEN-CENELEC-ETSI Smart Grid Coordination Group. (2012). *Smart Grid Reference Architecture.* Von https://tinyurl.com/2ah9smw9 abgerufen

Darvish, S., Jahic, A., Schulz, D., Magdowski, A., & Wilmes, M. (2021). Projekt „ELBE“ – Erprobung und Analyse des. *Hamburger Beiträge zum technischen Klimaschutz.* Hamburg.

E-Control. (12. 10 2022). *TOR Begriffe.* Von https://www.e-control.at/marktteilnehmer/strom/marktregeln/tor abgerufen

E-Control. (2022). *TOR Erzeuger.* Von https://www.e-control.at/marktteilnehmer/strom/marktregeln/tor abgerufen

E-Control. (11. 10 2022). *Weiterentwicklung der Entgeltstruktur für den Stromnetzbereich - Tarife 2.1.* Von https://www.e-control.at/marktteilnehmer/strom/netzentgelte/tarife-2-1 abgerufen

Europäische Kommission. (2022). *Digitalisierung des Energiesystems - EU-Aktionsplan.* Straßburg: EU.

Forschungsgesellschaft für Energiewirtschaft FfE. (2022). *Netzbelastungen der Netzorienten Use Cases.* München: FfE.

Hoekstra, A., Bienert, R., Wargers, A., Singh, H., & Voskuilen , P. (2020). *Using OpenADR with OCPP.* openADR Whitepaper.

Kathan, J.;. (2019). *leafs - Integration of Loads and Electric Storage Systems into advanced .* Wien: AIT.

Kepplinger, P; Fässler, B.; Huber, G.; M.A.S.T, Ireshika; Rheinberger, K.; Preißinger, M.;. (2020). Autonomes Demand Side Management verteilter Energiespeicher. In *E Elektrotechnik Informationstechnik* (S. vol. 137, no, S. 52–58).

Kommunalkredit Public Consulting GmbH. (11. 10 2022). *Förderungsaktion Elektromobilität für private 2022 - Umweltförderung.* Von https://www.umweltfoerderung.at/privatpersonen/foerderungsaktion-e-mobilitaet-fuer-private-2022.html abgerufen

NIST National Institute of Standards and Technology. (2010). *Guidelines for Smart Grid Cyber Security (NISTIR 7628).*

Oesterreichs Energie. (2020). *Netzberechnungen Österreich - Einfluss der Entwicklungen von Elektromobilität und Photovoltaik auf das österreichische Stromnetz.* Wien: oesterreichs energie.

PV Austria. (2022). *Erforderlicher PV-Ausbau .* PV Austria.

Statistik Austria. (2022). *Anzahl an E-Autos in Österreich.* Wien: Oesterreichs Energie.

Thomas Eberhard, Christian Steger-Vonmetz. (2019). *Bestandszahlen von E-Fahrzeugen bis 2050.* Wien: Austria Tech.

United States Department of Commerce, National Institute of Standards and Technology,. (2004). *Standards for Security Categorization of Federal Information and Information Systems.*

VDE FNN. (2022). *Eckpunkte zum zukünftigen Netzbetrieb mit Flexibilitäten in der Niederspannung.* Berlin: VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

VDE, F. N. (2021). *Lastenheft Steuerbox - Funktionale und konstruktive Merkmale.* Berlin: VDE FNN.

J. Anhang

J.1 Teilnehmer der Expertengruppe Digitale Schnittstelle

Nachnahme	Vorname	Firma
Badstöber	Lena-Maria	Energie AG
Berger	Angela	Smartgrids Austria
Berger	Klaus	Verbund
Bertsch	Martin	OE
Bouda	Fabian	TU Wien
Brönnimann	Christoph	Smart Grid Ready CH
Eder	Gottfried	Viessmann
Eder	Ernst	TB Eder
Eichinger	Roman	OVE
Einfalt	Alfred	Siemens
Eugster	Christian	E-VO eMobility GmbH
Fahrnberger	Vera	OE
Freimüller	Richard	Wärmepumpe Austria
Gasteiger	Tobias	Tinetz
Grafendorfer	Christian	Energieallianz
Gruber	Micha	Wien Energie
Hamberger	Manfred	Wago
Hinrichs	Hauke	SMATRICS
Hirschbichler	Michael	E-VO eMobility GmbH
Hofer	Tobias	Fronius International GmbH
Hoschek	Pia	Wiener Netze
Huber	Anita Christine	Verbund
Janisch	Fabian	PV-Austria
Jerovcic	Patrick	Kelag
Kain	Philipp	Keba
Kaineder	Severin	Wärmepumpe Austria
Kalt	Gerald	E-Control
Katschinka	Klaus	Wien Energie
Kosovinc	Klemen	Kärnten Netz
Lackner	Herbert	SMATRICS

Ladinig	Thomas	Kelag
Lechner	Christian	EVN
Meister	Georg Florian	Stadtwerke Klagenfurt
Mucher	Christoph	Energie Netze Steiermark
Nenning	Reinhard	vorarlberg netz
Pawek	Lukas	IG Wind
Peck	Benjamin	Schrack
Peyreder	Markus	Energie Steiermark Technik
Pfeiffer	Lukas	SMATRICS
Praxmarer	Mario	Tinext
Raudaschl	Stephan	Salzburg Netz
Rechberger	Georg	Keba
Reihs	David	AIT
Resch	Paula	IG Windkraft
Scheida	Karl	Oesterreichs Energie
Scheidl	Patrick	Schrack
Schenk	Alexander	Siemens
Scheucher	Benjamin	Dinitech
Schober	Lukas	vorarlberg netz
Schuster	Andreas	ASCR
Selhofer	Armin	OE
Stefan	Mark	AIT
Taljan	Gregor	Energie Netze Steiermark
Wanzenböck	Christoph	Smartgrids Austria
Wimmer	Gerhard	Keba

J.2 Datenpunktlisten

Messwerte:

Messwerte - Smart Meter (Hausanschluss)

Elektrische Größe	Art	Messwertaktualisierung an der Zählerschnittstelle	Einheit
U1, U2, U3	Momentanwert	<5s	V
I1, I2, I3	Momentanwert	<5s	A
$I1_{max}$, $I2_{max}$, $I3_{max}$	Maximalwert, vgl. SM?, viel. 1 Jahr	<5s	A
P1, P2, P3	Momentanwert	100-200 ms (z.B. für AC-WR, Heizstäbe)	W
P+ (summiert)	Momentanwert, Summenwert 3~	<5s	W
P- (summiert)	Momentanwert, Summenwert 3~	<5s	W
Q+ (summiert)	Momentanwert, Summenwert 3~	<5s	VAR
Q- (summiert)	Momentanwert, Summenwert 3~	<5s	VAR
Leistungsfaktor pro Phase	Momentanwert, 1~	<5s	Cos Phi

Priorisierte Größen für Use Case „Netze in Not“

Messwerte – Ladeeinrichtung

Elektrische Größe	Art	Messwertaktualisierung an der Geräteschnittstelle	Einheit
U1, U2, U3	Momentanwert	<5s	V
I1, I2, I3 (angebotener maximaler Ladestrom der Ladestelle)	Maximalwert	<5s	A
I1, I2, I3 (tatsächliche genutzter Strom des EV)	Momentanwert	<5s	A
P+ (summiert)	Momentanwert, Summe 3~	<5s	W
P- (summiert)	Momentanwert, Summe 3~	<5s	W
Q+ (summiert)	Momentanwert, Summe 3~	<5s	Var
Q- (summiert)	Momentanwert, Summe 3~	<5s	Var
Leistungsfaktor pro Phase	Momentanwert, 1~	<5s	Cos Phi
Temperatur in Ladeeinrichtung*	Reduzierung der Ladeleistung wenn Temperatur zu heiß	<5s	Grad C
geladene Energie E_{kWh}*	Fortlaufend über alle Ladevorgänge	<5s	kWh

* als Information

Messwerte – Wärmepumpe

Elektrische Größe	Art	Messwertaktualisierung an der Geräteschnittstelle	Einheit
Aufnahmeleistung P_{WP}	statischer Wert gemäß WP Spezifikation	100-200 ms	W
Elektrische Zusatzheizung P_{EZH}	statischer Wert gemäß WP Spezifikation	<5s	W
Wärmeleistung $P_{wärme}$*	statischer Wert gemäß WP Spezifikation	<5s	W
Aufnahmeleistung im Nennpunkt P_N*	statischer Wert gemäß WP Spezifikation	<5s	W
Minimale Aufnahmeleistung P_{mA}*	statischer Wert gemäß WP Spezifikation	<5s	W

* als Information

Messwerte - PV Anlage

Elektrische Größe	Messwertaktualisierung an der Geräteschnittstelle	Einheit
Aktuelle Einspeiseleistung des Wechselrichter P+, P-, Q+, Q-	Momentanwert 3~	kVA

Messwerte – Batteriespeicher (AC/DC)

Elektrische Größe		Messwertaktualisierung an der Geräteschnittstelle	Einheit
Batteriekapazität	Aktueller Stand		kWh
Nutzbarer SOC-Bereich	Ladezustand		%
SOC	Ladezustand		%
Gerätespannung U1, U2, U3	Momentanwert		V
P+ (summiert)	Momentanwert, Summe 3~	<5s	W
P- (summiert)	Momentanwert, Summe 3~	<5s	W
Q+ (summiert)	Momentanwert, Summe 3~	<5s	Var
Q- (summiert)	Momentanwert, Summe 3~	<5s	Var

Vorgabewerte

Elektrische Größe	Art	Messwertaktualisierung an der Geräteschnittstelle	Einheit
Vorgabe auf Einzelgerät			
Maximaler Strom Ladeeinrichtung (aktuell)	Momentanwert	<5s	A
Maximale Leistung Ladeeinrichtung (Zukunft) +/- P, +/- Q (summiert, 3~)	Momentanwert	<5s	W, var
Maximale Leistung Wärmepumpe P1, P2, P3, Q1, Q2, Q3 (+/-)	Momentanwert	<5s	W, var
Maximale Leistung Wechselrichter P1, P2, P3, Q1, Q2, Q3 (+/-)	Momentanwert	<5s	W, var

Priorisierte Größen für Use Case „Netze in Not“

Elektrische Größe	Art	Messwertaktualisierung an der Geräteschnittstelle	Einheit
Vorgabe am Zählpunkt			
Maximale Einspeiseleistung P+Q (Zählpunkt Kunde)	1~, 3~	<5s	W, var
Maximale Bezugsleistung P+Q (Zählpunkt Kunde)	1~, 3~	<5s	W, var
Vorgabe auf Hausanschlusspunkt			
Maximale Einspeiseleistung P+Q (Hausanschlusspunkt)	1~, 3~	<5s	W, var
Maximale Bezugsleistung P+Q (Hausanschlusspunkt)	1~, 3~	<5s	W, var

Priorisierte Größen für Use Case „Netze in Not“

J.3 Use Cases

Use-Case 1
Ansteuerung von Kundenanlagen durch VNB im Notzustand

Use-Case Ziel (*kurze Beschreibung des Anwendungsfalls)*

- *Der Verteilernetzbetreiber versorgt unter anderen auch Kunden, die entweder einen Netzzugangsvertrag abgeschlossen haben, der einen steuernden Eingriff des VNB bei Netzengpässen vorsieht, oder es handelt sich um eine allgemeine Pflicht für gewisse Kundengruppen oder Geräte ggf. abhängig von der Leistungsgröße.*
- *Der VNB erkennt bzw. erleidet unmittelbar einen Netzengpass, der dadurch gekennzeichnet ist, dass entweder die Überlastung von Betriebsmitteln oder eine Nichteinhaltung der Versorgungsqualität droht oder bereits eingetreten ist.*
  Der VNB ermittelt auf Basis der Verortung des Netzengpasses und der betroffenen Netzebene die Netzkunden, die den Netzengpass aufgrund ihres Netzzugangsvertrags oder einer rechtlichen allgemeinen Verpflichtung vermeiden können und übermittelt ihnen eine entsprechende Information zur Aktivierung der Steueroption
- *Die Information zur Aktivierung der Steueroption bezieht sich auf den Netzzugangsvertrag und/oder allgemeine rechtliche Regelungen und die darin enthaltenen Optionen für den VNB durch Steuermaßnahmen Netzengpässe zu vermeiden oder zu beseitigen. Dies sind Direkteingriffe des VNB aufgrund einer rechtlichen Ermächtigung oder auch vertraglich vereinbarte Leistungsanpassungen in Kundenanlagen. Im Dokument Tarife 2.1 wären dies z.B. einerseits der unterbrechbare Tarif (schaltbare Vertragsleistung, entweder Vertragsleistung ein / aus oder Umschaltung zwischen bedingter und unbedingter Leistung) und andererseits Modelle mit bedingter und unbedingter Leistungsbereitstellung, bei denen die bedingte Leistung temporär bis auf die unbedingte Leistung reduziert werden kann.*
- *Die Kontrolle der Einhaltung von Steuermaßnahmen wird über das Smart Meter System sichergestellt.*
- *Globales UC-Ziel: Erhalt, Wiederherstellung und Sicherstellung der Netzstabilität und/oder der Netzverfügbarkeit (Vermeidung von Schäden an der Netzinfrastruktur) und Sicherstellung der Versorgungsqualität bei Einführung von Netzzugangsverträgen mit Steuermöglichkeit von Kunden-Assets durch den VNB.*

Use-Case Akteure (*beteiligte Personen, Einrichtungen, Unternehmen, etc.)*

- *Netzkunden mit Netzzugangsvertrag, der eine Steuermöglichkeit für den VNB vorsieht (Bereitstellung einer technischen Infrastruktur, die den oben beschriebenen Netzzugangsvertrag erfüllen kann)*
- *VNB (Owner des Use Cases)*
- *Optional Dritte (Energielieferanten / Aggregatoren / Anlagenbetreiber)*
- *Sie bekommen Informationen über die Aktivierung der Steueroption*
- *Sie generieren entsprechende Steuerbefehle und übermitteln diese an die Aktoren bei den Netzkunden.*

Trigger (*Wann wird der Use-Case ausgelöst oder ausgeführt?)*

Notzustand tritt ein:

- *Der Use Case wird mit der Erkennung eines Netzengpasses durch den VNB getriggert.*
- *Verhalten bei Systemstörungen: Im Falle einer Störung (Kommunikationsausfall, Störung im VNB-System …..) müssen die Aktoren auf Netzkundenseite automatisch auf eine vordefinierte Fall-Back Leistungsgrenze zurückfallen.*

Einzelne Schritte (*Wie ist der Ablauf des Use Case?)*

- Notzustand tritt ein: *Erkennung eines Netzengpasses*
- *Ermittlung der erforderlichen Aktoren (Zählpunktbezeichnung)*
- *Ermittlung und Aufteilung der Informationen zur Aktivierung der Steueroption (z.B. prozentuelle Reduzierung, Reduzierung auf Minimalleistung, der Leistungsgrenzwerte)*
- *Übertragung der Information zur Aktivierung der Steueroption zu den Aktoren auf Netzkundenseite und zusätzliche Information an Dritte (Aggregatoren, etc.)*
- *Überwachung der Ausführung durch die Aktoren (close to real time falls Strom oder Leistungswerte von z.B, Abgängen in der Trafostation bzw. den Aktoren vorliegen, sonst ex post mittels Smart Meter)*
- *Ende des Notzustandes*
- *Protokollierung des Steuereingriffs (zentral verfügbar)*

Systemstörung

- *Erkennen einer Systemstörung durch eine Instanz auf Netzkundenseite*
- *Aktivierung von vordefinierten Default-Werten*
- *Protokollierung der Systemstörung*

Voraussetzungen (*Welche Voraussetzungen müssen für den Use Case geschaffen werden? z.B. Hardware, Software, etc.)*

- *Abbildung der Netzzugangsverträge mit Steuereingriff durch den VNB nach den legistischen / regulatorischen Vorgaben im Kundenvertragsmanagement beim VNB (Steuergrenzen, Nachweispflichten……)*
- *Abgeleitet aus dem Kundenvertrag Verortung der Steuermöglichkeit mit den technischen Eigenschaften / Steuermöglichkeiten in der Netztopologie / dem Netzmodell*
- *Implementierung eines Monitoring-Systems zur Erfassung der Netzauslastung und Ermittlung von Netzengpässen*
- *Ermittlung der Stellgrößen für die Aktoren auf Netzkundenseite zur Vermeidung von Netzengpässen (z. B. durch hierarchisch organisierte Netz(zellen)regler oder ein zentrales System.)*
- *Übertragungskanal mit entsprechender Security für die Übermittlung der Informationen zur Aktivierung der Steuerungsoption*
- *Überwachung der gesetzten Maßnahmen, ggf. ergreifen von weiteren Maßnahmen, falls die erforderliche Netzentlastung nicht stattgefunden hat oder sie sich über der Zeit in die falsche Richtung bewegt (z. B. durch dezentrale Netzregler)*
- *Identifikation von Netzkunden, die sich nicht an Steuervorgaben gehalten haben, zumindest ex post mittels Smart Meter*
- *Dokumentation (z.B. Log-Files pro Zählpunkt oder zentral) aller Steuereingriffe / Vertragsverletzungen in einer Datenbank zum Nachweis der Konformität / Nichtkonformität zum Netzzugangsvertrag*

Abhängigkeiten (*Welche Abhängigkeiten bestehen zu anderen Anwendungsfällen, Stakeholder, Personen, Komponenten, etc.?)*

- *Alle Vertragsbeziehungen zwischen Netzkunden mit einem Netzzugangsvertrag mit VNB Steuermöglichkeit und Dritten, die zu einer bestimmten Zeit eine bestimmte Leistungsbereitstellung durch das Netz vorsehen – hier ist eine entsprechende Abstimmung der Verträge aufeinander erforderlich*

Messwerte (*Welche Messwerte / Informationen sind für Use Case notwendig?)*

Aktor auf Netzkundenseite

- *Vorgabe einer „Fall-Back-Leistung" die bei Systemstörungen einzuhalten ist.*
- *Entsprechend des Netzkundenzugangsvertrags bei Netzengpässen Vorgabe der für steuerbare Aktoren vereinbarten Information zur Aktivierung der Steuerfunktion durch den VNB. (z.B. Reduktion auf unbedingte Leistung, relative Reduktion in Bezug auf eine bedingte Leistung, ...).*
- *Erkennung und Protokollierung von Systemstörungen*
- *Aktuelle Wirkleistung eines Aktors (bezogen, geliefert)*

Zusätzliche Informationen für Vertragspartner der Netzkunden (für Prognosezwecke)

- *Leistungswerte (15 Minuten-Werte)*
- *Steuereingriffe der Netzbetreiber*

Auf VNB-Seite
Grob zusammengefasst:

- *Erkennung von Netzengpässen die eine Verletzung des Spannungsbandes und/oder eine Überlastung von Betriebsmitteln (Leitungen, Transformatoren, ...) verursachen*
- *Zählpunktspezifische Bereitstellung der Information zur Aktivierung der Steueroption*
- *Informationen zur Administration der Kundenverträge*

Use Case 2

Laden von Elektroautos im Notzustand

Use-Case Ziel (*kurze Beschreibung des Anwendungsfalls?)*

Verteilernetzbetreiber werden in Zukunft Netzzugangsverträge anbieten, die eine Steuermöglichkeit bei Netzengpässen vorsehen.
Dieser Use Case beschreibt Ladevorgänge für Elektroautos, bei der für die Ladeinfrastruktur ein solcher Netzzugangsvertrag abgeschlossen wurde. Die Ladeinfrastruktur kann aus einem oder mehreren Ladepunkten bestehen, wobei pro Netzanschlusspunkt immer eine technische Instanz für die betriebliche Abwicklung der Rahmenbedingungen aus dem Netzzugangsvertrag verantwortlich sein muss. In der Praxis bedeutet das:

- *Bei einem Ladepunkt an einem Netzanschluss muss dieser steuerbar sein*
- *Bei mehreren Ladepunkten an einem Netzanschluss und bei ggf. lokal vorhandenen Erzeugungs- / Speicheranlagen muss es eine Controllerinstanz geben, die auf der einen Seite die Vorgaben des Netzbetreibers aufnimmt und sie auf der anderen Seite durch entsprechende Steuerung der lokal vorhandenen Assets umsetzt.*

Ziel des Use Cases ist die Erfüllung der Netzzugangsverträge. Damit muss die Steuermöglichkeit durch den Netzbetreiber gegenüber allen anderen Steuer- und Regelfunktionen die oberste Priorität haben.

Use-Case Akteure (*beteiligte Personen, Einrichtungen, Unternehmen, etc.)*

- *Ladepunktnutzer*
- *Ladepunktbetreiber / CPO‘s*
- *E-Mobility Provider / EMP / MSP*
- *Zählpunktsinhaber (wählt den Netzzugangsvertrag)*
- *Verteilernetzbetreiber / Übertragungsnetzbetreiber*
- *Stromlieferant*
- *Ggf. Betreiber von Parkflächen und Energiegemeinschaften mit Ladepunkten*

Trigger *(Wann wird der Use-Case ausgelöst oder ausgeführt?)*

- *Beim Netzbetreiber ist ein Betriebszustand „Notzustand“ aufgetreten (gem. TOR)*

Einzelne Schritte (*Wie ist der Ablauf des Use Case?)*

- *Beim Netzbetreiber ist ein Betriebszustand „Notzustand“ aufgetreten (gem. TOR)*
- *Der Netzbetreiber ermittelt die erforderlichen Steuersignale pro Netzkunde oder Region und übermittelt sie über die digitale Schnittstelle an die betroffenen Netzkunden.*
- *Abregeln: Prozentuelle Reduktion von der Nennleistung, Reduktion auf Mindestleistung, Reduktion auf null.*
- *AC-Lader: 6A ist Mindestwert, darunter ist nur null möglich*
- *DC-Lader: kein Mindestwert erforderlich*
- *Vorschlag: Änderungen von Leistungsvorgaben wenn möglich im 15 Minuten Raster (beim Hinunterregeln ggf. schneller)*
- *Übermittlung der Steuereingriffe an berechtigte Dritte*
- *Priorisierung der Steuereingriffe privat vor öffentlich vor kritischer Infrastruktur für gesteuerte Elemente die auf Netzebene 7 angeschlossen sind*
- *Der Netzbetreiber erfasst alle Steuereingriffe bei seinen Kunden und stellt diese bei Bedarf im Rahmen der geltenden rechtlichen Rahmenbedingungen zur Verfügung*

Voraussetzungen (*Welche Voraussetzungen müssen für den Use Case geschaffen werden? z.B. Hardware, Software, etc.)*

- *Netzbetreiber müssen ihr Netz Monitoring auf die untersten Netzebenen erweitern*
- *Der Gesetzesgeber / Regulator muss die Rahmenbedingungen für die Eingriffe und zukünftigen Netztarife rechtlich umsetzen und Rahmenbedingungen für die entsprechenden Netzzugangsverträge festlegen.*
- *Die Netzbetreiber müssen Steuereingriffe ermitteln und dokumentieren können und sie über eine digitale Schnittstelle an die betroffenen Netzkunden übermitteln*
- *Für die praktische Realisierung der vorgenannten digitalen Schnittstelle gibt es 3 Varianten*

- *Das technische System des VNB ermittelt notwendige Steuereingriffe und übermittelt diese an ein zentrales System eines Dritten, der dann für die Umsetzung der Steuereingriffe über die in seiner Verantwortung stehende Infrastruktur sorgt. (z. B. Aggregator, Fast Track Use Case der CPO's)*
- *Die steuerbare Kundenanlage kommuniziert direkt mit einer Instanz des technischen Systems des VNB (kein Zusatzgerät bei den Netzkunden)*
- *Das technische System des VNB kommuniziert über eine Art Gateway, das bei den Netzkunden montiert wird, mit der steuerbaren Kundenanlage (Einzelgerät oder Energiemanagementsystem)*

Abhängigkeiten *(Welche Abhängigkeiten bestehen zu anderen Anwendungsfällen, Stakeholder, Personen, Komponenten, etc.?)*

Steuernde Eingriffe des VNB auf Ladevorgänge verlängern in der Regel die Ladezeit. Daher ist es wichtig, dass:

Netznutzer bei Abschluss eines Netzzugangsvertrags ein klares Bild vermittelt bekommen, in welchem Umfang und auf welche Art die Steuereingriffe erfolgen können.

Inhaltliche Abstimmung von Verträgen für Service- und Dienstleistungen mit Netzzugangsverträgen mit VNB Steuermöglichkeit. Ziel ist hier eine klare Abgrenzung der Verantwortlichkeiten.

Messwerte *(Welche Messwerte sind für Use Case notwendig?)*

Temporäre Vorgabe einer maximalen Ladeleistung

Übermittlung der aktuellen Ladeleistung

Use Case 3
Ansteuerung von Ladeeinrichtungen durch CPO-Backend in Notsituation

Use-Case Ziel (*kurze Beschreibung des Anwendungsfalls?)*

Annahme: Verteilernetzbetreiber werden in Zukunft in den Netzzugangsverträgen für NE7 vorsehen (ALTERNATIVE: in Netzanschlussanfrage), dass eine Steuermöglichkeit für definierte elektrische Verbraucher (Wallboxen, Wärmepumpen etc.) bei Netzengpässen vorzusehen ist, oder andernfalls Einschränkungen dieser Verbraucher vorzunehmen sind.
Dieser Use Case beschreibt die Steuerung von solchen Verbrauchern am Beispiel von Ladeinfrastruktur für E-Autos (auch anzuwenden auf andere Geräte mit ähnlichem Profil/Leistung) durch „zertifizierte Anbieter" auf Anweisung der Netzbetreiber, wenn die Ladeinfrastruktur unter die o.g. Regelungen/Anforderungen fällt. Die Ladeinfrastruktur kann aus einem oder mehreren Ladepunkten bestehen.
„Zertifizierte Anbieter" sind Aggregatoren (am Beispiel der Ladeinfrastruktur CPOs etc.), die elektrische Verbraucher gemäß festgelegter Vorgaben online angebunden haben und nach definierten Vorgaben der Netzbetreiber steuern können.

- *Ist ein Ladepunkt NICHT über einen „zertifizierten Anbieter" fernsteuerbar, so ist dieser auf einer vom Netzbetreiber festgesetzten eingeschränkten Leistung (bspw. Mindestleistung für Funktion) dauerhaft zu betreiben (z.B. max. 6 A 1- oder 3-phasig).*
- *Ist ein Ladepunkt über einen „zertifizierten Anbieter" ansteuerbar, so kann dieser bis zur maximalen Leistung, die vom Netzbetreiber festgelegt wird, betrieben werden, muss jedoch bei Einschränkungen im Netzbetrieb die Ladeleistung reduzieren. Bei Kommunikationsproblemen und Ausfällen muss der Ladepunkt auf die vom Netzbetreiber definierte reduzierte Leistung (bspw. 6 A) automatisch herunterregelt werden.*
- *Bei mehreren Ladepunkten, verhalten diese sich analog zum Verhalten eines Ladepunkts, jedoch kann die „freie Leistung" innerhalb der Ladepunktgruppe verteilt werden.*

Ziel des Use Cases ist die Erfüllung der Anforderungen bei Notzustand die in den Netzzugangsverträgen (ALTERNATIVE: Vorgaben aus der Netzanschlussanfrage) gefordert werden.
Durch die bereits bestehende Infrastruktur bei Aggregatoren ist eine frühzeitige Steuerungsmöglichkeit für Netzbetreiber, ohne dem notwendigen Rollout zusätzlicher physischer Geräte und lokalen Kommunikationsschnittstellen/-protokollen bzw. -standards, möglich.

Use-Case Akteure (*beteiligte Personen, Einrichtungen, Unternehmen, etc.)*

- *Ladepunktnutzer*
- *Ladepunktbetreiber / CPO*
- *Ladepunktbesitzer / CSO (Charging Station Owner)*
- *E-Mobility Provider / EMP / MSP*
- *Zählpunktinhaber (Vertragspartner Netzzugangsvertrag)*
- *Verteilernetzbetreiber*
- *Stromlieferant*
- *Ggf. Betreiber von Parkflächen und Energiegemeinschaften mit Ladepunkten*

Trigger (*Wann wird der Use-Case ausgelöst oder ausgeführt?)*

Der VNB gibt nach Feststellung des definierten Notzustandes eine Leistungsvorgabe an den Aggregator, der die Vorgaben dann an die Komponente oder das EMS überträgt.

Einzelne Schritte (*Wie ist der Ablauf des Use Case?)*

- *Beim Netzbetreiber ist ein Betriebszustand „Notzustand" aufgetreten (gem. TOR)*
- Über definierte Schnittstellen werden den „zertifizierten Anbietern" Vorgaben für die Ladeleistung der Ladeinfrastruktur in den betroffenen Netzgebieten/der betroffenen Zählpunkte übermittelt/zur Verfügung gestellt
- Entscheidung welcher Zählpunkt (und damit welche Ladeinfrastruktur) betroffen ist, liegt beim Netzbetreiber
- Priorisierung der Steuereingriffe privat vor öffentlich vor kritischer Infrastruktur für gesteuerte Elemente die auf Netzebene 7 angeschlossen sind erfolgt durch den Netzbetreiber
- Zertifizierte Anbieter führen Anpassung der Ladeleistung gemäß definierter Zustände durch
- Zertifizierte Anbieter stellen Messwerte (bzw. Zustandsinformationen) der Ladeinfrastruktur laufend über definierte Schnittstellen den Netzbetreibern zur Verfügung (Überprüfbarkeit)
- Der Netzbetreiber erfasst alle Steuereingriffe bei seinen Kunden und stellt diese bei Bedarf im Rahmen der geltenden rechtlichen Rahmenbedingungen zur Verfügung
- Bei weiteren Notwendigkeiten bzw. nach Ende „Notzustand" werden die Vorgaben über definierte Schnittstellen vom Netzbetreiber entsprechend angepasst

- Kaskadierungen / Rampen / Zeitabstände je ZP/Gerät sind vom Netzbetreiber zu managen
- Als Fallback wird bei Kommunikationsproblemen und ähnlichen Fällen die „eingeschränkte Leistung“ (Mindestleistung) definiert

Voraussetzungen (*Welche Voraussetzungen müssen für den Use Case geschaffen werden? z.B. Hardware, Software, etc.)*

- *Der Gesetzesgeber / Regulator muss die Rahmenbedingungen für die Eingriffe und rechtlich umsetzen und Rahmenbedingungen für die entsprechenden Netzzugangsverträge (ALTERNATIVE: Netzanschlussanfrage) festlegen und ein Anreizsystem für steuerbare Wallboxen/Geräte definieren (für NE7)*
- *Regulatorische Festlegung Priorisierung (privat/öffentlich/kritische Infrastruktur)*
- *Einheitliche Vorgaben (Netzzugang/Netzanschlussanfragen) für definierte Lasten (Wallboxen, Wärmepumpen) soweit möglich österreichweit (Klarheit für Kunden, einfacheres Management für zertifizierte Anbieter und Netzbetreiber)*
- *Schnittstelle Netzbetreiber und Zertifizierte Anbieter (Architektur)*
  - *Variante 1: zentrale „Aggregatoren – Netzbetreiber“ Hub – m:n Austausch*
  - *Variante 2: Anbindung je Netzbetreiber – 1:n Austausch*
  - *Variante 3: Anbindung je Netzbetreiber/Aggregator – 1:1 Austausch (ggf. für Proof of Concept)*
- *Vorgaben Ansteuerung (Ladeinfrastruktur, Wärmepumpen, sonstige Verbraucher)*
  - *Variante A – Zustandsdefiniert (Frei – Mindestleistung – Aus)*
  - *Variante B – Absolute Leistungsvorgabe (in kW/A)*
  - *Variante C - %-Vorgabe von aktueller/gemeldeter Leistung*
- *Rückmeldung der Aggregatoren*
  - *Aktuelle Leistungen/Stromstärken und ggf. Spannungen (zu definieren: je ZP, je Gerät, je Phase….)*
  - *Aktuelle Zustände (online, offline, Aus/Mindestleistung/Frei)*
- *„zertifizierte Anbieter“*
  - *Definition der Voraussetzungen (Security, Reaktionszeiten, Verfügbarkeiten etc.) und Prozesse*
- *Vollautomatisierte Anbindung/Einbindung und Matching steuerbare Verbraucher mit Zählpunkt*
- *Kontroll-/bzw. Sanktionsmöglichkeit des Netzbetreibers ggü. Kunden und Aggregatoren bei Nicht-Einhaltung der Vorgaben*

Abhängigkeiten (*Welche Abhängigkeiten bestehen zu anderen Anwendungsfällen, Stakeholder, Personen, Komponenten, etc.?)*

- Netznutzer bei Abschluss eines Netzzugangsvertrags (ALTERNATIVE: Netzanschlussanfrage) ein klares Bild vermittelt bekommen, in welchem Umfang und auf welche Art die Steuereingriffe erfolgen können, bzw. welche Einschränkungen bei nicht-steuerbarer Hardware einzuhalten sind.
- Inhaltliche Abstimmung von Verträgen für Service- und Dienstleistungen mit Netzzugangsverträgen mit VNB Steuermöglichkeit. Ziel ist hier eine klare Abgrenzung der Verantwortlichkeiten.
- Konzepterarbeitung für mehrere steuerbare Geräte (bspw. Ladepunkte und Wärmepumpe) mit unterschiedlichen zertifizierten Aggregatoren an einem Zählpunkt.

Messwerte (*Welche Messwerte sind für Use Case notwendig?)*

- *Siehe oben*

Sonstiges
Eine Nutzung des beschriebenen Kommunikationsweges ist auch für den Regelbetrieb für die Nutzung von marktgetriebenen Use Cases möglich (bspw. Lastverschiebung Preisoptimierung, Regelenergie). Jedenfalls ist aber sicherzustellen, dass bei „Notzustand“, die Vorgabe des Netzbetreibers „Vorrang“ hat.

Use Case 4
Ansteuerung von Wärmepumpen in Notsituationen

Use-Case Ziel (*kurze Beschreibung des Anwendungsfalls?)*
In bestimmten Notsituationen könnten Netzbetreiber bei Luft-Wärmepumpen Maßnahmen setzten damit die Leistungsaufnahme vorübergehend reduziert wird.
Das Ziel dieses UC ist es nicht, Wärmepumpen als alleinigen Lösungsansatz bei der Leistungsreduktion darzustellen. Vielmehr könnte dieser UC ein Teil von mehreren Maßnahmen sein. Der UC zielt darauf ab die technisch möglichen Rahmenbedingungen zum Schalten von Wärmepumpen festzuhalten. Dabei könne etwaige Komfort-Einbußen bei den Betreibern nur abgeschätzt werden. Welche Möglichkeiten tatsächlich im Rahmen der Komfort-Einbußen vertretbar sind, muss im Detail geklärt werden.
Die Wirksamkeit diese UC sollte in Verbindung mit anderen Maßnahmen verglichen und abgewogen werden. Der E-Heizstab stellt ca. 1-2% der notwendigen Energie an den kältesten Tagen im Jahr bereit, wodurch der Wirkungszeitraum dieser Maßnahme stark eingeschränkt ist.

Anmerkung: Außerhalb von der „Notzustand" Situation (z.B. bei flexiblen Tarifen) ist ein regelmäßiges Abschalten von Wärmepumpen durch externe Signale denkbar, wenn eine Mindestlaufzeit von 20min garantiert wird. Es ist auf die Abtauung bei Luft Wärmepumpen zu achten.

Use-Case Akteure (*beteiligte Personen, Einrichtungen, Unternehmen, etc.)*
- Nutznießer der erzeugten Wärme (Mieter, Untermieter)
- Wärmepumpen Betreiber (Privathaushalte wie Einfamilienhaus oder Reihenhaus, Miet- und Eigentums-Wohngemeinschaften im mehrgeschoßigen Wohnbau, Dienstleistungsgebäude wie Büros oder Verwaltungsgebäude, Industrie oder mit dem Betrieb beauftragte Dritte)
- Netzbetreiber
- Hersteller der Wärmepumpe
- Unternehmen welches die Wärmepumpe installiert (z.B. Installateur, Anlagenbauer)

Trigger (*Wann wird der Use-Case ausgelöst oder ausgeführt?)*

- *Der Use-Case wird durch den Netzbetreiber ausgelöst wenn,*
- *definierte Sicherheitsgrenzwerte nicht eingehalten werden (z.B.: gem. EN 50160)*

Einzelne Schritte (*Wie ist der Ablauf des Use Case?)*
- *Signal für* „Notzustand" *Situation*
- *Signalempfänger können den E-Heizstab für die maximale Ausschaltzeit ausschalten*
- *Nach der maximalen Ausschaltzeit muss der E-Heizstab wieder eingeschalten werden*

Voraussetzungen (*Welche Voraussetzungen müssen für den Use Case geschaffen werden? z.B. Hardware, Software, etc.)*

- *Hausinternes Energiemanagementsystem*
- *Kommunikationsschnittstelle zum Netzbetreiber*
- *Wenn eine Leistungsvorgabe für den Fall des UC1* „Notzustand" *ca. 1 mal jährlich und nicht öfter vorkommt, muss eine Mindestlaufzeit von 5 min eingehalten werden, um Schäden an den Wärmepumpen zu vermeiden.*

Abhängigkeiten (*Welche Abhängigkeiten bestehen zu anderen Anwendungsfällen, Stakeholder, Personen, Komponenten, etc.?)*
- *ev. Komforteinbußen beim Wärmepumpen Nutznießer*
- *Entscheidungsfreiheit für spezielle Bedürfnisse bei Betreibern*
- *Lebensdauer der Wärmepumpe*
- *Dauer des Notzustands*

Messwerte (*Welche Messwerte sind für Use Case notwendig?)*
Die Messwerte sind abhängig vom tatsächlichen Funktionsumfang der Schaltvorgänge. Parameter könnten folgende sein:

Variablenbeschreibung	**Variablendefinition**
Aufnahmeleistung [WP]	read write
Elektrische Zusatzheizung (EZH)	read only
Aufnahmeleistung im Nennpunkt	read only
minimale Aufnahmeleistung	read only

Use Case 5
Ansteuerung durch Lieferanten und -Aggregatoren

Use-Case Ziel (*kurze Beschreibung des Anwendungsfalls?)*

Die Beschreibung dieses Use Cases erfolgt unter den folgenden Annahmen (=Grundlage für den Use Case):

- *Netzzugangsverträge mit einer Steueroption für den VNB werden im rechtlich-regulatorischen Rahmen verankert und eingeführt*
- *Die VNB's errichten eine Infrastruktur die es ihnen ermöglicht, Informationen von Netzkundeneinrichtungen einzuholen, die zur Ermittlung von Netzengpässen dienlich sind und die es ihnen ermöglicht, die Steueroption im Falle von „Notzustand" auszuüben. Notzustand ist dann gegeben, wenn entweder Betriebsmittel des VNB gefährdet sind und/oder die Einhaltung der Spannungsqualität nach EN50160 an den Übergabepunkten zu den Netzkunden nicht mehr sichergestellt werden kann.*

In dem sich sehr dynamisch gestaltenden Marktumfeld ist es für Lieferanten und Aggregatoren wesentlich, möglichst viele Informationen zur Geschäftsoptimierung und Produktgestaltung zu erhalten. Deshalb soll eine von VNB's errichtete Infrastruktur gemäß vorhergehender Beschreibung auch für Lieferanten und Aggregatoren über eine zentrale Schnittstelle zugänglich gemacht werden. Die dafür erforderliche Vertragsbeziehung mit den betreffenden Netzkunden (bzw. Zustimmungserklärung, wenn es nur um den Datenaustausch geht) wird vorausgesetzt. Ein zukünftiges Ziel besteht darin, dass durch entsprechende Interaktionen (z.B. Austausch von Messdaten) und marktseitig getriebenen Steuermaßnahmen Notzustand Zustände möglichst vermieden werden. In diesem Szenario haben Steuermaßnahmen zufolge hat Notzustand Priorität gegenüber marktseitigen Steuermaßnahmen.

Anmerkung: Neben dem Netzbetreiber, der nur bei Notzustand eingreift, macht nur ein weiterer Stakeholder Sinn, der auf die Steueroption außerhalb von Notzustand zugreift. Kombinationen aus Lieferant und Aggregator, die beide auf die Steueroption eines Netzkunden zugreifen wollen können hier problematisch werden. → Thema für AG 4?

Unabhängig von der marktseitigen Nutzung der im Vorhergehenden beschriebenen VNB Infrastruktur müssen Steuereingriffe aufgrund von „Notzustand" dokumentiert und an Lieferanten und Aggregatoren gemeldet werden.

Use-Case Akteure (*beteiligte Personen, Einrichtungen, Unternehmen, etc.)*

- *Netzkunden*
- *VNB*
- *Lieferant / Aggregator*

Trigger (*Wann wird der Use-Case ausgelöst oder ausgeführt?)*

- *Dieser Use Case läuft permanent und wird nur durch „Notzustand" unterbrochen*

Einzelne Schritte (*Wie ist der Ablauf des Use Case?)*

- *Der Lieferant / Aggregator bezieht Informationen von Netzkunden (in der Regel Messwerte)*
- *Der Lieferant / Aggregator bezieht vom VNB sofern in Zukunft technisch machbar und verfügbar statistische Informationen über die Netzauslastung*
- *Der Lieferant / Aggregator ermittelt erforderliche Steuermaßnahmen in seinem Sinn und führt diese aus*

Voraussetzungen (*Welche Voraussetzungen müssen für den Use Case geschaffen werden? z.B. Hardware, Software, etc.)*

Festlegung einer zentralen Schnittstelle für den erforderlichen Informationsaustausch und die Ausübung der Steueroption

- *Technische, rechtliche und regulatorische Voraussetzungen, sowie Verträge zwischen den Parteien bestehen*

Abhängigkeiten (*Welche Abhängigkeiten bestehen zu anderen Anwendungsfällen, Stakeholder, Personen, Komponenten, etc.?)*

- *keine*

Messwerte (*Welche Messwerte sind für Use Case notwendig?)*

- *Informationen, die für Notzustand erhoben werden müssen und physikalische Größen und Zeitbereiche, die vorgegeben werden können*
- *Informationen die vorhanden sein können und die von der Digitale Schnittstelle unterstützt werden*
- *Zusätzliche Anforderungen an die Schnittstelle:*
- *Zeitreihen, die in der Vergangenheit oder der Zukunft liegen können (Basis für die Auswertung von Last- / Einspeiseverläufen und die Übermittlung von Forecasts oder Fahrplänen → wichtig für Energiemanagementsystemen bei Netzkunden)*
- *Informationstexte → zukünftige Kundeninformationen*

Use Case 6
Ansteuerung über eine
Hersteller- und Aggregator Cloud

Use-Case Ziel (*kurze Beschreibung des Anwendungsfalls?)*

- *Dieser Use Case zielt darauf ab, dass eine Verbindung mit der Herstellercloud hergestellt wird. Wahlweise kann die Verbindung auch über einen Aggregator hergestellt werden.*
- *Der Verteilnetzbetreiber sendet die temporären Leistungsvorgaben entweder an die Herstellercloud oder an einen Aggregator, der diese Vorgaben an die Herstellercloud weitergibt.*
- *Vorteile: Die Hersteller können bereits heute ihre Geräte über die Cloud steuern. Somit kann dieser Use Case schnell ausgerollt werden.*
- *Durch die Nutzung der vorhandenen Infrastruktur (wie z.B. existierender Kommunikationspfad über die Internetverbindung des Kunden) muss keine neue Infrastruktur ausgerollt werden.*

Use-Case Akteure (*beteiligte Personen, Einrichtungen, Unternehmen, etc.)*

- *Verteilnetzbetreiber*
- *Hersteller(-cloud)*
- *Ggf. Aggregator*
- *Endkunde*

Trigger (*Wann wird der Use-Case ausgelöst oder ausgeführt?)*

- *bei Vorherrschen des Netzzustandes „Notzustand“*

Einzelne Schritte (*Wie ist der Ablauf des Use Case?)*

- *Verteilnetzbetreiber erkennt einen Notzustand in seinem Netz*
- *Übermittlung der temporären Leistungsvorgaben in die Herstellerclouds der betroffenen Endkunden*
- *Empfang und Verarbeitung der Leistungsvorgaben in der Herstellercloud*
- *Weiterleitung der Leistungsvorgaben an die Endgeräte*
- *Auswertung des Netzzustandes durch den VNB*
- *Sobald der Notzustand überwunden ist, erhalten die Herstellerclouds der betroffenen Endkunden die Auflösung der temporären Leistungsvorgaben*
- *Aufhebung der temporären Leistungsvorgaben durch die Herstellerclouds*
- *Empfang und Verarbeitung der Aufhebung*

Voraussetzungen (*Welche Voraussetzungen müssen für den Use Case geschaffen werden? z.B. Hardware, Software, etc.)*

- *Verbindung zwischen Verteilnetzbetreiber und Herstellercloud muss geschaffen werden*
- *Wahlweise: Verbindung zwischen Verteilnetzbetreiber und Aggregator sowie Verbindung zwischen Aggregator und Endgeräten*

Messwerte (*Welche Messwerte sind für Use Case notwendig?)*

- Aktuelle Bezugsleistung
- Aktuelle Einspeiseleistung

Vorgabewerte (ergänzt)

- *Max. temporäre Bezugsleistung am Netzanschlusspunkt*
- *Max. temporäre Einspeiseleistung am Netzanschlusspunkt*

J.4 Praxisbeispiele einer *Digitalen Schnittstelle*

Im Rahmen des EP Digitale Schnittstelle wurden aktuelle Praxisbeispiele für eine *Digitale Schnittstelle* vorgestellt, die in einem separaten Dokument zur Verfügung stehen. Diese Beispiele dienten zur Veranschaulichung der Thematik, wurden jedoch nicht für die Bewertung der Architekturvarianten oder Standards und Protokolle herangezogen.

Vorgestellte Praxisbeispiele einer *Digitalen Schnittstelle*:

- Smart Grid Ready Schnittstelle (Schweiz) – Christoph Brönnimann – Smart Grid Ready
- Pilotprojekt IEEE 2030.5 (Australien) – Tobias Hofer – Fronius
- Technologielösungen für Ladeeinrichtungen – Dr. DI Michael Hirschbichler - E-VO eMobility
- Projekt „friendlyCharge“ - Markus Peyreder - Energie Steiermark Technik
- Smarte Netzintegration – Anreize und Koordination für intelligentes Laden – Dr. Michael Lehmann – MITNETZ Strom
- Sensor-Netzwerke: Status Quo und Trends – Mike Lange – Smart Home Deutschland
- Forschungsprojekt Car2Flex – Fabian Bouda – TU Wien

J.5 AIT-Studie zur Bewertung relevanter Standards und Protokolle

In diesem Abschnitt wird die vollständige Studie des *Austrian Institute Of Technology* (AIT) zur Untersuchung verschiedener Standards und Protokolle dargestellt. Zuerst wird auf die relevanten Standards und Protokolle sowie die Methodik eingegangen. Aufbauend auf einer grundlegenden Bewertung wird in der Studie eine SGAM-Modellierung (SGAM = Smart Grid Architecture Model) der drei Architekturvarianten und eine Beurteilung im Hinblick auf Security-Aspekte durchgeführt. Die Modellierung der Architekturvarianten im international anerkannten SGAM verbessert das gemeinsame Verständnis der Verortung von Akteuren und deren Interaktionen.

J.5.1 Untersuchte Standards und Protokolle, Methodik

Für die Bewertung der verschiedenen Kommunikationsstandards und -protokolle zur Umsetzung einer bidirektionalen digitalen Schnittstelle wurde eine Literaturrecherche von unterschiedlichen wissenschaftlichen Projektergebnissen und Standard- und Protokolltexten durchgeführt. Dieser Ansatz eignet sich gut, um bekannte Eigenschaften der Standards und Protokolle zu sammeln und vergleichend darzustellen. Implementierungsspezifische Kriterien lassen sich dadurch jedoch nur teilweise bewerten. Für die Bewertung von unterschiedlichen Kommunikationsstandards und -protokollen wurde zuerst eine Vorauswahl getroffen. Die ausgewählten Standards und Protokolle wurden unter Berücksichtigung mehrerer Kriterien untersucht. Die Kriterien und deren Bewertungsklassifizierungen werden in den folgenden Absätzen genauer erläutert.

Auswahl der Kommunikationsstandards und -protokolle

Für die Auswahl der Standards und Protokolle wurde zuerst eine Vorauswahl durch AIT-Experten getroffen. Diese Vorauswahl wurde daraufhin dem Expertenpool Digitale Schnittstelle vorgestellt und mit den involvierten Stakeholdern abgestimmt. Als Feedback auf diese Vorstellung wurden weitere relevante Standards und Protokolle erwähnt, insbesondere Modbus TCP, und die Auswahl der zu analysierenden Standards und Protokolle um diese erweitert.

Auswahl der Analysekriterien

Zur weiteren Analyse der Standards und Protokolle wurde zuerst definiert, welche Aspekte für die Einsetzbarkeit besonders relevant sind. Dafür wurde von den Experten ein Kriterienkatalog entwickelt und in vier Hauptkategorien eingeteilt (Generelle Kriterien, Operative Kriterien, Technologiespezifische Kriterien und Security Kriterien). Zu jedem Kriterium wurde eine Klassifizierung definiert, um dem Aspekt einen numerischen Wert (von 1 bis 5) zuzuordnen, wenn möglich. Diese numerischen Werte wurden rein aus Expertenwissen definiert und wurden zur Vergleichbarkeit der Standards und Protokolle eingeführt. Die Klassifizierungen aller bewerteten Kriterien sind im Anhang J.5.4 angeführt.

Die in Anhang J.5.4 vorgestellten Klassifizierungen der Kriterien wurden in weiterer Folge zur Analyse der unterschiedlichen Standards und Protokolle eingesetzt. Mit den numerischen Werten wurden in weiterer Folge gewichtete Mittelwerte für die einzelnen Gruppen von Kriterien berechnet, um ein Ranking für die Standards und Protokolle und ihre Eignung aufzustellen. Die Gewichtung der Kriterien, die in der finalen Analyse zum Einsatz gekommen ist, wurde von Mitgliedern aus dem Expertenpool vorgeschlagen und daraufhin in der Studie übernommen.

Analyse der Standards und Protokolle

Die Methodik der Analyse der Standards und Protokolle setzte sich aus zwei Vorgehensweisen zusammen. Erstens wurden veröffentlichte Standard- und Protokolltexte von AIT-Experten gesichtet und auf die, im Vorhinein definierten Aspekte, hin analysiert. Zweitens wurde dieses Wissen durch Gespräche mit weiteren Spezialisten vertieft. Die Bewertung der einzelnen Standards und Protokolle wurde von jenen Spezialisten durchgeführt, welche die jeweiligen Texte analysiert haben.

Weitere Diskussionsrunden zu den Bewertungen wäre in einem nächsten Projektschritt ratsam, um die Ergebnisse noch belastbarer zu machen.

Architekturvarianten

Die Architekturvarianten, also die gesamte Umsetzung vom VNB bis zu den Kundenanlagen, gegebenenfalls durch mehrere Standards und Protokolle bzw. Schnittstellen, wurden parallel zur Bewertung der Kommunikationsstandards und -protokolle konkretisiert. Die entwickelten Architekturvarianten sind in Abbildung 30 dargestellt.

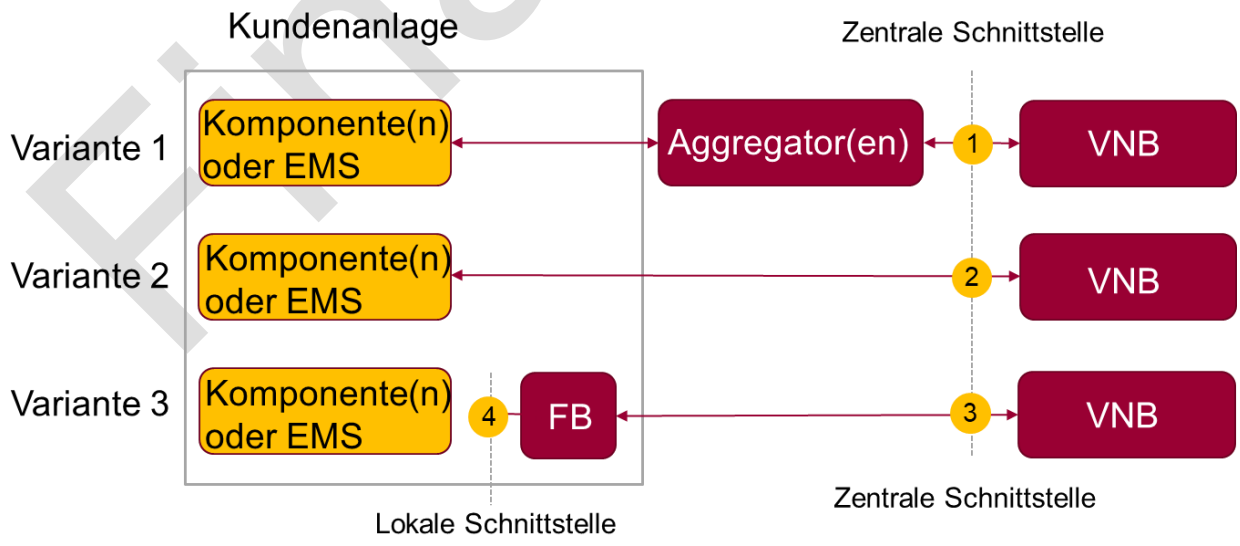

Abbildung 30: Architekturvarianten der Digitalen Schnittstelle

Architekturvariante 1 behandelt die Möglichkeit, bestehende oder neu aufgesetzte Verbindungen von Aggregatoren zu Endgeräten zu nutzen, und zur Umsetzung der *Digitale Schnittstelle* lediglich eine Schnittstelle zwischen VNB und Aggregatoren umzusetzen. In Architekturvariante 2, der sogenannten „IoT"-Lösung, wird eine direkte Schnittstelle zwischen VNB und Endkundengerät bzw. EMS umgesetzt. Architekturvariante 3 beschreibt die Umsetzung der *Digitale Schnittstelle* über einen Funktionsblock, der die Netzwerke des VNB und des Endkunden trennt und auf beide Seiten eine eigene Schnittstelle anbietet. Die Verortung des Funktionsblocks wurde in der Studie nicht genauer definiert.

Limitierungen der Studie

Bei der Studie handelt es sich um eine theoretische Untersuchung relevanter Standards und Protokolle. Es wurde die generelle Eignung der Standards und Protokolle bewertet, um sichere Systeme zu entwerfen. In weiterer Folge wäre es ratsam Demonstratoren mit geeigneten Kommunikationsstandards bzw. -protokollen zu evaluieren, um genauere Aussagen über implementierungsspezifische Unterschiede treffen zu können.

Zum Zeitpunkt der Analyse war noch keine genaue Definition von Prozessen und Interaktionen zwischen den Kommunikationsteilnehmern vorhanden. In einem folgenden Schritt wäre es ratsam die genauen Datenübertragungsprozesse zu definieren und deren Umsetzbarkeit in den einzelnen Standards bzw. Protokollen noch genauer zu beleuchten. Vor allem die Kriterien betreffend die Security müssen nochmals auf Prozessebene beleuchtet und analysiert werden.

J.5.2 Bewertung der Standards und Protokolle

Die Standards und Protokolle wurden entsprechend der Vorgehensweise aus Abschnitt G.1.1 bewertet. Die Ergebnisse für eine zentrale Schnittstelle sind in Tabelle 3 zusammengefasst, jene für eine lokale Schnittstelle in Tabelle 4.

Eine umfangreiche textliche Beschreibung der Bewertung ist im Kapitel 0 angeführt. Im Kapitel J.5.5 findet sich die Tabelle mit der vollen numerischen Bewertung aller Aspekte. Im Abschnitt J.5.6 ist die benutzte Gewichtung angeführt, die verwendet wurde, um aus den Bewertungen der einzelnen Kriterien auf die Bewertung der Kategorien zu kommen.

Tabelle 3: Bewertung der Standards und Protokolle für die zentrale VNB-Schnittstelle, gewichtet

	Generell	Operativ	Technologie-spezifisch	Security	Summe
IEEE 2030.5	+	+	++	++	++
IEC 62746 (OpenADR)	+	+	++	++	++
IEC 61850	+	+	++	++	+
DNP3	+	++	+	+	+
IEC 60870-104	+	~	+	+	+

Tabelle 4: Bewertung der Standards und Protokolle für die lokale Schnittstelle, gewichtet

	Generell	Operativ	Technologie-spezifisch	Security	Summe
IEEE 2030.5	+	+	++	++	++
EEBus (IEC 63380)	++	+	+	++	++
Sunspec Modbus / REST	++	+	++	++	++
OCPP 2.0.1	+	+	+	++	+
KNX IoT	+	+	+	++	+
Modbus TCP	+	~	+	~	~

Für die Bewertung in Tabelle 3 und Tabelle 4 wurde folgende Skala benutzt:

++	+	~	-	--
Sehr gut geeignet	Gut geeignet	Ausreichend	Eher nicht ausreichend	Nicht ausreichend

Die Bewertung stellt eine Momentaufnahme dar. Sowohl im Smart Home Bereich als auch im Bereich der Steuerung von verteilten intelligenten Energieanlagen finden zurzeit mehrere, teilweise parallele, Entwicklungen statt. Ob sich ein einzelner Standard oder ein einzelnes Protokoll zur Kommunikation mit Endkundenanlagen international durchsetzt, ist noch nicht absehbar.

J.5.3 Detaillierte Bewertung der Standards und Protokolle

In den folgenden Kapiteln wird die Bewertung der einzelnen Standards und Protokolle genauer beleuchtet und die numerische Bewertung textlich motiviert.

Für jeden Standard und jedes Protokoll wurde auf die 4 Hauptaspekte, (Generelle Kriterien, Operative Kriterien, Technologiespezifische Kriterien und Security Kriterien) im Detail eingegangen.

IEC 61850

Generelle Kriterien

Der Standard IEC 61850 kommt ursprünglich aus dem Bereich der Automatisierung von Umspannwerken. Dort hat sich der Standard etabliert und ist dort als herstellerunabhängiger Kommunikationsstandard sehr weit verbreitet. Als wichtigster offener Kommunikationsstandard in dem Bereich der Automatisierung von Umspannwerken gibt es viele wissenschaftliche Publikationen, die sich mit der Anwendung des Standards befassen. Die 61850 wird vom Technischen Komitee 57 des IEC herausgegeben und weiterentwickelt. Die Verbreitung des Standards ist gleichbleibend auf hohem Niveau, vor allem im Bereich der Mittelspannung und Hochspannung.

Es gibt 2 Nennenswerte Open Source Implementierungen der IEC 61850. Das erste Repository ist „libIEC61850" (https://libiec61850.com/), dass in C geschrieben ist und das letzte Release im März 2022 hatte. Das zweite Repository ist „IEC61850bean" (https://github.com/beanit/iec61850bean), dass in Java geschrieben ist und bei dem die letzten Änderungen im Mai 2021 veröffentlicht wurden. Beide Quellcodes sind somit mehr oder weniger aktiv.

Da die Applikationsprotokolle, die bei der IEC 61850 zum Einsatz kommen wenig weit verbreitet sind im IT-Bereich, wird die Einarbeitungszeit relativ hoch eingeschätzt und die zu erwartenden Kosten werden höher eingeschätzt als für Standards oder Protokolle, die auf sehr weit verbreiteten Web-Technologien aufbauen. Dieser Umstand könnte umgangen werden, wenn sich für die Implementierung voll auf open source Anwendungen gestützt werden würde, die Integration in andere Systeme wäre damit dann leichter umzusetzen. Diese Einschätzungen wurden unter der Annahme getroffen, dass die Implementierung ohne vorheriges Wissen zur IEC 61850 und deren Aufbau erfolgen würde.

Das Protokoll würde sich ausschließlich für die Implementierung einer zentralen VNB Schnittstelle eignen, da das Protokoll überhaupt nicht gängig ist im Bereich der verteilten Energieanlagen. Es würde auf Seiten der lokalen Schnittstelle einen großen Aufwand für Hersteller bedeuten, Geräte mit der IEC 61850 kompatibel zu machen.

Operative Kriterien

Die zeitliche Auflösung der Daten, die über IEC 61850 gesendet werden, ist sehr hoch, da der ursprüngliche Nutzen der Umspannwerkautomatisierung teilweise eine sehr schnelle Reaktionszeit von Komponenten erfordert. Es bietet die Möglichkeit bestimmte Nachrichten (in einem eigenen Netzwerk) zu priorisieren. Die Größe der Nachrichten, die versendet werden, ist normal bis eher klein, da der Standard unter anderem für den Einsatz mit einer Vielzahl an einfacheren Geräten entwickelt wurde. Eine sehr hohe Übertragungsfrequenz würde bei einer Verbindung zu

einer großen Zahl an Kunden schnell zu Überlastungen in Netz und Datenspeicher führen und ist für eine digitale Schnittstelle bei Endkunden voraussichtlich nicht notwendig.

Der Standard ist darauf ausgelegt eine Vielzahl von Geräten zu steuern, somit ist die Skalierbarkeit als gut einzustufen. Im Standard sind keine Funktionen zur Erhöhung der Fehlertoleranz definiert, die über die Funktionen von TCP auf der Transportebene hinaus gehen. Der Hauptteil des Standards definiert generelle Konzepte von Wartungsfunktionen, konkret wurde für verteilte Energieanlagen jedoch keine genauere Definition im relevanten Standardtext IEC 61850-7-420 gefunden.

Technologiespezifische Kriterien

Zur Abbildung von Daten definiert die IEC 61850 ein hierarchisches Datenmodell, dass aus physikalischen Geräten, Funktionen und logischen Knoten besteht. Funktionen können mehrere logische Knoten verbinden und deren Werte verändern. Funktionen können unterschiedliche Prioritäten zugeordnet werden, so dass mehrere Funktionen die gleichen logischen Knoten verändern können und lokal entschieden werden kann welche Funktionen tatsächlich umgesetzt werden sollen.

Die Erweiterbarkeit auf Datenpunktebene wird als einfach eingestuft, da alle notwendigen Datenobjekte im Datenmodell definiert sind, aber ein Großteil davon optional zum Einsatz kommt. Ebenso sollte ein System basierend auf der IEC 61850 relativ einfach erweiterbar sein, wenn neue Kommunikationsteilnehmer eingebunden werden müssen.

Auf Applikationsebene wird bei der IEC 61850 hauptsächlich MMS (Manufacturing Message Specification) eingesetzt. Bei MMS handelt es sich um eine eher ältere Kommunikationsspezifikation, die Ende der 1990er Jahre standardisiert wurde. Außerdem gibt es eine Abbildung der Kommunikation auf XMPP, das aber in der IEC 61850 nicht so häufig zum Einsatz kommt wie MMS. XMPP ist im IT-Bereich mehr verbreitet als MMS, hat jedoch den Nachteil, dass die meisten Ressourcen und Implementierungen von IEC 61850 nur für die MMS-Variante verfügbar sind.

Mit der Erweiterung IEC 61850-7-420 wurden Datenmodelle für verteilte Energieressourcen eingeführt und die Interaktion mit diesen genauer definiert. Für unterschiedliche Typen von Energieressourcen (EV, Batterie, etc.) wurden eigene Datenmodelle eingeführt, die alle technologiespezifischen Steuermöglichkeiten und vorhandenen Datenpunkte in hohem Detailgrad abbilden.

Die Komplexität bei einer erstmaligen Inbetriebnahme eines IEC 61850 Systems wird eher hoch eingeschätzt, da hier eher ausgewiesene Experten notwendig wären, um ein derartiges System aufzusetzen.

Security Aspekte

Der Standard IEC 61850 hat selbst keinen Teil der Security Aspekte berücksichtigt, sondern es werden Absicherungsmöglichkeiten für Leistungsmanagementsysteme im eigenen Standard IEC 62351 definiert und diese gelten auch für die IEC 61850.

Mit den Maßnahmen aus der IEC 62351 können Kommunikationsnetzwerke, die auf der IEC 61850 basieren abgesichert werden. Die Absicherungsmechanismen sind einerseits die Verwendung von Security auf der Transportebene (TLS) und Authentifizierungsmethoden durch digitale Signaturen.

Die Sicherheit der Kommunikation ist abhängig von der ordnungsgemäßen Umsetzung der Maßnahmen und bedarf sicher einer aktiven Betreuung durch Spezialisten. Genauere Aussagen über die Eignung der IEC 61850 für den Einsatz als Standard zwischen VNB und Endkunden sind erst nach einer weiteren Analyse der genauen Prozesse und deren Schutzbedarf möglich.

IEEE 2030.5

Generelle Kriterien

Der IEEE 2030.5 Standard ist aus dem Zigbee Smart Energy Profile (SEP) entstanden. Das SEP wurde entwickelt, um für Endverbraucher Energieversorgungsmamagent zu ermöglichen wie zum Beispiel Demand Response, Laststeuerung und Tageszeitpreisgestaltung zu ermöglichen. In der Industrie hat sich der Standard gut verbreitet, während die Verbreitung im wissenschaftlichen Bereich durchschnittlich ist. Der Standard wurde in Amerika von Standardisierungsgremium IEEE entwickelt mit der Unterstützung von Power Line Communications Committee. Zum Beispiel kommt die IEEE 2030.5 als Standard-Kommunikationskanal in Kalifornien von verfügbaren Kapazitäten an Endverbraucher zum Einsatz. Außerdem wird IEEE 2030.5 in mehreren Bundesstaaten in Australien verwendet, um Leistungskapazitäten an Endkunden bzw. Aggregatoren zu kommunizieren.

Zurzeit gibt es wenige open source Implementierungen vom IEE 2030.5. Auf github findet man nur wenige Repositorys für die Seite des Clients, und diese sind nicht mehr aktiv, da die letzten Änderungen einige Jahre zurück liegen. Von den verfügbaren Repositorys ist das von EPRI am ausgereiftesten.

Da die Kommunikationsprotokolle, die für IEE2030.5 verwendet werden, recht verbreitet sind, ist die Einarbeitung eher gering einzuschätzen, weil auf sehr weit verbreitete Web-Technoligen aufgebaut wird. Zusätzlich sind die erwarteten Kosten für die Implementierung auch eher gering eingeschätzt.

Da der Standard für den Bereich der dezentralen Energiesysteme entwickelt wurde, ist es sowohl für die Implementierung einer zentralen VNB Schnittstelle als auch für lokale Schnittstellen geeignet.

Operative Kriterien

Da der ursprüngliche Verwendungszweck von IEEE 2030.5 manchmal eine sehr schnelle Reaktionszeit der Komponenten erfordert, ist die zeitliche Auflösung der gesendeten Daten sehr hoch. Daten werden anhand von push/pull Methodik versendet oder eingefordert. Die Größe der verschickten Daten ist im Vergleich zu anderen Standards bzw. Protokollen im Mittelfeld. IEEE 2030.5 bietet auch die Möglichkeit, dass Nachrichten mit unterschiedlichen Prioritäten versendet werden.

Aufgrund der Tatsache das der Standard dafür entwickelt worden ist, dass viele Geräte im Netz miteinander kommunizieren und auch das immer wieder Geräte hinzugefügt werden oder entfernt werden, ist die Skalierbarkeit des Standards sehr gut.

Der Standard führt grundlegende Methoden für die Fehlertoleranz an die auf HTTP/TCP Funktionen basieren. Im Standard werden keine Ansätze für die Wartbarkeit angeführt.

Technologiespezifische Kriterien

IEEE 2030.5 ist für die Implementierung einer REST-Architektur konzipiert, basierend auf den HTTP Kernaktionen GET, HEAD, PUT, POST und DELETE. REST steht für „Representational State Transfer“. REST basiert auf Datenaustausch mit Fokus auf eine einfache Implementierung, Ressourcen und Zustandslosigkeit. Auch wenn schon 2000 der erste Ansatz für REST-Architekturen veröffentlich worden ist, ist der Ansatz im IT-Bereich heute sehr weit verbreitet.

Wenn Schnittstellen definiert werden, wird vom Verhalten nicht zwischen Server, Client und Geräten unterschieden. Dadurch wird vermieden das Komponenten unterschiedliches verhalten auf einem Server oder Client haben. Der Unterschied zwischen Client und Server ist ob Ressourcen zu Verfügung gestellt werden (Server) oder mit den Daten interagiert wird (Client).

Die Erweiterbarkeit auf Teilnehmerebene wird als sehr einfach eingestuft, da dies mithilfe von dem verbreiteten multicast Domain Name Service (mDNS) realisiert wird.

Zur Beschreibung von RESTfull Schnittstellen wird das weit verbreitete Web Application Description Language (WADL) verwendet, welches die Erweiterbarkeit auf Datenpunktebene erleichtert. Für die Beschreibung von Datenmodellen wird die Extensible Markup Language (XML) verwendet, welches auch weit verbreitet ist.

Die Komplexität bei einer erstmaligen Instandsetzung eines Systems wird eher gering eingeschätzt, da die verwendeten Mechanismen heutzutage weit verbreitet sind und nicht sehr komplex sind.

Security Aspekte

Der IEEE 2030.5 Standard definiert Sicherheitsaspekte nur auf der Anwendungsebene. Jedoch wird es den Entwickler offen gelassen dort weitere Sicherheitskonzepte zu implementieren.

Die Sicherheitsmechanismen, die im Standard angeführt werden, sind für Transportauthentifizierung und -verschlüsselung HTTP über TLS.

OpenADR

Generelle Kriterien

Der Standard OpenADR (IEC 62746) dient der Implementierung von Demand Response (DR) Programmen. Im wissenschaftlichen Bereich wird OpenADR oft als Teil von Smart Grids Systemen verwendet, um Simulationen und Algorithmen im Kontext von DR zu erforschen. OpenADR wird vom Technischen Komitee 118 des IEC herausgegeben und mit der OpenADR Alliance weiterentwickelt und verbreitet. Die Verbreitung des Standards ist in den USA fortgeschritten und es existieren Demonstratoren mit Beteiligung der Industrie. Die Verbreitung des Standards ist auf Ebene der EU und einigen Mitgliedsstaaten geplant und teilweise in Fallstudien mit Beteiligung der Industrie implementiert worden.

Die OpenADR Alliance publiziert einen Implementierungsleitfaden. Es gibt 2 nennenswerte Open Source Implementierungen des OpenADR, die jedoch beide noch keine stabilen Releases haben. Das erste Repository ist „OpenADR“ (https://github.com/avob/OpenADR) das in Java geschrieben ist und bei dem die letzten Änderungen im September 2021 veröffentlicht wurden. Es enthält bereits Informationen zum Deployment mit Docker und hat OpenADR 2.0b vollständig implementiert. Das zweite Repository ist „OpenLEADR“ (https://github.com/OpenLEADR/openleadr-python), welches in Python geschrieben ist und das letzte Release (0.5.27) im Oktober 2022 hatte. Es implementiert OpenADR 2.0b noch nicht vollständig, die Entwicklung steht jedoch unter dem Schirm der Linux Foundation.

Die Applikationsprotokolle, die bei OpenADR zum Einsatz kommen, sind im IT-Bereich weit verbreitet. Die Einarbeitungszeit wird deshalb niedrig eingeschätzt und damit die zu erwartenden Kosten geringer eingeschätzt als für Standards oder Protokolle, die auf weniger weit verbreiteten Technologien aufbauen. Diese Einschätzungen wurden unter der Annahme getroffen, dass die Implementierung ohne vorheriges Wissen zu OpenADR und dessen Aufbau erfolgen würde.

OpenADR würde sich prinzipiell sowohl für die Implementierung einer zentralen VNB-Schnittstelle als auch für die Implementierung einer lokalen Schnittstelle eignen. Da es auf der Endgeräteebene jedoch nicht verbreitet ist würde es sich vor allem für die Implementierung einer zentralen Schnittstelle eignen.

Operative Kriterien

Die zeitliche Auflösung der Daten, die über OpenADR gesendet werden, ist generell eher gering, da die Domäne des Demand Response eine tendenziell langsamere Reaktionszeit von Komponenten erfordert (mehrere Sekunden bis wenige Minuten). Die Größe der Nachrichten, die versendet werden, ist im Vergleich zu anderen Standards bzw. Protokollen eher groß, da der Standard hierarchische und relativ komplexe Datenmodelle unterstützt, weil ganze Demand Response Programme abgebildet werden können und die Payload als XML versendet wird.

Der Standard ist darauf ausgelegt einer Vielzahl von Geräten Events zu schicken, somit ist die Skalierbarkeit als gut einzustufen. Im Standard sind keine Funktionen zur Erhöhung der Fehlertoleranz definiert, die über die Funktionen von TCP auf der Transportebene und HTTP auf der Protokollebene hinaus gehen. Der Standard definiert keine Konzepte von Wartungsfunktionen.

Technologiespezifische Kriterien

Zur Abbildung von Daten definiert OpenADR mittels XML-Schemas (auf Basis von OASIS) ein hierarchisches Datenmodell, welches als wesentliche Komponenten Virtual Top Nodes (VTN) und Virtual End Nodes (VEN) beinhaltet. Die physikalischen Geräte oder die *Digitale Schnittstelle* würden als VENs und die Rolle des DSO als VTN gesehen werden. VTNs können von VENs bestimmte Services anfordern, wie beispielsweise einen Bericht (Messdaten) anfordern, oder einen Event (Sollwertvorgabe) schicken.

Die Erweiterbarkeit auf Datenpunktebene wird als einfach eingestuft, da alle notwendigen Datenobjekte im Datenmodell definiert sind. Ebenso sollte ein System basierend auf OpenADR relativ einfach erweiterbar sein, wenn neue Kommunikationsteilnehmer eingebunden werden müssen.

Auf Applikationsebene wird bei OpenADR HTTP oder XMPP eingesetzt. Beide Protokolle werden von der IETF spezifiziert und sind im World Wide Web sehr weit bis weit verbreitet.

Datenmodelle für verteilte Energieressourcen und -verbraucher sind im Standard nicht enthalten, stattdessen existieren Vorlagen um unterschiedliche Typen von Energieressourcen (Wechselrichter, Batterie, etc.) und -verbrauchern (Wärmepumpen, EV, etc.) zu implementieren.

Die Komplexität bei einer erstmaligen Inbetriebnahme eines Systems wird als moderat eingeschätzt, da einerseits zu den eingesetzten Protokollen und Technologien (HTTP, XMPP, XML)

generell genug Vorwissen und viel freie Dokumentation existiert, aber andererseits die DR Konzepte auf die Requirements umgelegt und die verteilten Energieressourcen auf Basis der Templates implementiert werden müssten.

Security Aspekte

Der Standard OpenADR definiert selbst keine Security Mechanismen.

Die nötigen Absicherungsmechanismen werden durch die Funktionen der eingesetzten Webtechnologien erfüllt. Hier sind von OpenADR beispielhaft die Security auf der Transportebene (TLS mit X.509 Zertifikaten, ECC und RSA Zertifikate) und Authentifizierungsmethoden durch digitale Signaturen oder die gängigen Protokollmechanismen angeraten.

Die Sicherheit der Kommunikation ist abhängig von der ordnungsgemäßen Umsetzung der Maßnahmen und bedarf sicher einer aktiven Betreuung durch Spezialisten. Genauere Aussagen über die Eignung von OpenADR für den Einsatz als Kommunikationsprotokoll zwischen VNB und Endkunden sind erst nach einer weiteren Analyse der genauen Prozesse und deren Schutzbedarf möglich.

OCPP / OSCP

Generelle Kriterien

Das “Open Charge Point Protocol” OCPP wurde für die Kommunikation zwischen Charging Station Management System (CSMS) und Charging Stations (CS) entwickelt, um Ladevorgänge von Elektrofahrzeugen zu automatisieren.

OCPP wird von der Open Charge Alliance entwickelt. Die Open Charge Alliance hat ihren Ursprung 2009 mit der E-Laad foundation in den Niederlanden, weshalb OCPP sich vor allem in Europa als de facto Standard etabliert hat. Auf anderen Kontinenten ist OCPP ebenfalls etabliert, aber hat nicht überall die gleiche Vormachtstellung wie in Europa.

Auf Github.com sind mehrere öffentliche aktive OCPP-Bibliotheken für Java und Python zu finden, welche aktiv bearbeitet werden und für Client- und Server-Implementierungen benutzt werden können. Aufgrund dessen wird der Aufwand für die Implementierung im Vergleich mit anderen Protokollen und Standards als eher gering eingeschätzt.

Das Protokoll wäre lediglich für eine lokale Schnittstelle geeignet. Eine direkte Kommunikation zwischen Verteilernetzbetreiber (VNB) und Endkunden mit OCPP wäre sehr umständlich in der Implementierung und entspricht nicht der ursprünglich geplanten Anwendung von OCPP. Das „Open Smart Charging Protocol“ OSCP wäre hierfür prinzipiell geeignet und wird unten in einem separaten Abschnitt behandelt.

Operative Kriterien

Nachdem OCPP bereits heute im großen Stil von CPOs benutzt wird, ist die Skalierbarkeit gegeben. Eine mögliche Architekturvariante wäre die Kommunikation vom Gateway bzw. Aggregator zu CS oder EMS (Energy Managment System).

Bei Version 2.0.1 wird die mögliche Topologie weiter gefasst. Es können auch andere Geräte als CS mittels dem „Device Model“ definiert werden. Nachdem es derzeit (10/2022) dafür jedoch keine vordefinierten Anwendungsfälle gibt und auf Nachfrage bei der Open Charge Alliance keine Projekte bekannt sind, welche andere Geräte als CS bzw. Elektrofahrzeuge einsetzen, wird diese Möglichkeit nicht untersucht. OCPP wird also nur im Hinblick auf eine lokale Schnittstelle für CS untersucht.

OCPP 2.0.1 bringt einige Verbesserungen gegenüber Version 1.6. Zu nennen sind hier Plug&Charge und Security Aspekte, aber auch die sogenannten „Advanced diagnostics“, welche die Möglichkeit bieten, diverse Zustände wie z.B. Temperaturen im Ladeequipment zu überwachen. Secure Firmware Updates bieten eine sichere Möglichkeit die Firmware zu aktualisieren. V2X-Funktionalitäten werden ab Version 2.1, die aktuell in der Entwurfsphase ist, im Detail erarbeitet.

Für den Anwendungsfall „Notzustand“ ist eine Datenübertragung mit geringer Latenz zwischen VNB und Kundenanlage erforderlich. Es müssen Sollwerte vom VNB zur Kundenanlage sowie Messwerte von der Kundenanlage zum VNB übertragen werden. In wie fern OCPP dafür geeignet ist, muss in Zusammenhang mit anderen Protokollen und Standards untersucht werden, welche für die Kommunikation zwischen VNB und Aggregator/Gateway eingesetzt werden. Für gewisse Anwendungen ist auch eine aggregierte Übertragung, beispielsweise der aggregierten Soll- und Ist-Wirkleistung, zwischen Aggregatoren und dem VNB denkbar.

Technologiespezifische Kriterien

Die Kommunikation mittels WebSockets ist Stand der Technik und bietet die Möglichkeit, dass vom Server, in diesem Fall dem CSMS, nach vorherigem Verbindungsaufbau durch den Client, in diesem Fall die CS, jederzeit Daten vom Server an den Client gesendet werden können, ohne dass der Client vorher wieder eine Verbindung aufbauen muss. Es ist daher nicht zwingend Polling seitens der CS erforderlich. Über WebSockets kann bidirektional kommuniziert werden.

Die Umstellung von Version 1.6 auf Version 2.0.1 bedeutet einen gewissen Implementierungsaufwand, weshalb bei vielen Anwendungen die Umstellung noch nicht durchgeführt wurde.

Die Erweiterbarkeit von Datenpunkten wird im Hinblick auf „Device Model“ und „Advanced diagnostics“ als „mittel“ eingestuft. Es sind verschiedene Zustände und Messwerte an den CS prinzipiell übertragbar. Die Erweiterbarkeit der Datenpunkte über CS bzw. Elektromobilitätstechnologie hinaus ist in der Praxis jedoch nicht erprobt.

Security Aspekte

OCPP 2.0.1 entspricht im Hinblick auf die Informationssicherheit dem neuesten Stand der Technik. Es wird “Transport Layer Security” (TLS) mit basic authentication und client side certificates unterstützt, wodurch nicht nur die Authentizität des CSMS, sondern auch die Authentizität der CS gewährleistet werden kann. Mit TLS 1.3 ist Perfect Forward Secrecy gewährleistet. Es ist zu erwähnen, dass nur eine korrekte Implementierung die volle Informationssicherheit gewährleistet.

Sofern die lokale Schnittstelle für andere Geräte wie Wärmepumpen und PV-Wechselrichter parallel mit anderen Protokollen oder Standards implementiert werden kann, und eine Kombination mit einem anderen vom VNB implementierten Protokoll bzw. Standard sinnvoll ist, wäre die Benutzung von OCPP für die lokale Schnittstelle prinzipiell denkbar.

OSCP

Das „Open Smart Charging Protocol“ OSCP ist für die Steuerung von flexiblen Ressourcen gedacht und beschränkt sich nicht nur auf Elektrofahrzeuge bzw. deren Equipment. OSCP wird ebenfalls von der Open Charge Alliance entwickelt. Das Protokoll dient dabei zur Kommunikation zwischen Capacity Provider, beispielsweise dem VNB, und einem Flexibility Provider, beispielsweise einem Charge Point Operator (CPO). OSCP ist für eine Fahrplan-Übermittlung mit Leistungsgrenzen an eine dritte Stelle gedacht, weshalb es für den, im ersten Schritt, primären Anwendungsfall der Digitalen Schnittstelle – „Notzustand“ – nicht weiter untersucht wird. Das Protokoll sollte jedoch bei Folgeuntersuchungen für andere Anwendungsfälle zur Steuerung von Flexibilitäten genauer betrachtet werden.

Sunspec REST / Modbus

Generelle Kriterien

Die Sunspec Initiative setzt sich aus mehreren Stakeholdern aus dem Bereich der verteilten Energieanlagen, insbesondere aus den Bereichen Photovoltaikanlagen (PV) und Speichersysteme. Die Initiative es sich zum Ziel gesetzt einen Informationsstandard für diese Bereiche zu erstellen der Interoperabilität zwischen Geräten unterschiedlicher Hersteller ermöglicht.

Die Sunspec Alliance hat ihren Ursprung in Amerika, der Informationsstandard hat mittlerweile jedoch international eine weite Verbreitung erlangt und ist quasi ein Industriestandard im Bereich der PV-Anlagen und Speicher.

Die Haupttechnologie auf die Sunspec setzt ist Modbus TCP, um lokale Steuerung von Geräten umzusetzen. Für eine genauere Bewertung des Einsatzes von Modbus TCP als Applikationsprotokoll im Bereich der Endkundenschnittstelle kann man die Bewertung von Modbus TCP auf Seite 108 heranziehen. Im Folgenden wird das Sunspec RESTful interface bewertet, dass das Datenmodell mit Sunspec Modbus teilt und interoperabel mit diesem ist. Dieser Teil des Standards befindet sich zurzeit im „Test“ Status.

Es gibt eine aktive open source Implementierung der Sunspec Modbus Spezifizierung von der Sunspec Alliance in Python (https://github.com/sunspec/pysunspec2). Außerdem ist die Spezifikation frei auf github erhältlich (https://github.com/sunspec/models).

Als Statuslose Implementierung einer API sind RESTful APIs sehr beliebt im IT-Bereich. Sie lassen sich außerdem recht einfach implementieren und ihre Anwendung skaliert gut auf viele Kommunikationsteilnehmer.

Die Sunspec Spezifikation würde sich vor allem für die lokale VNB Schnittstelle eignen. Es gibt für Sunspec außerdem eine Übersetzungsebene für IEEE 2030.5 und Profile, die über IEEE 2030.5 übertragen werden.

Operative Kriterien

Die zeitliche Auflösung der Daten, die mit der Sunspec Spezifizierung zu erreichen ist, wird als gut eingestuft. Die Datenintensivität wird ebenso als gering eingestuft. Die Sunspec Implementierung basierend auf REST skaliert sicher sehr gut, da die Technologie häufig im Webbereich, auch für große Projekt, zum Einsatz kommt.

Es gibt keine Fehlertoleranzfunktionen in der Spezifikation, jedoch kann sowohl bei Modbus TCP als auch bei REST auf die Fehlertoleranzfunktionen von TCP auf der Transportebene zurückgegriffen werden. Wartungsfunktionen werden ebenso nicht definiert.

Technologiespezifische Kriterien

Hauptsächlich wird in Sunspec ein Informationsmodell definiert, das auch eine gewisse Anlehnung an IEC 61850 Datenpunkte hat. Die Architektur (sowohl für Modbus als auch für REST) ist verbindungslos und statuslos, das heißt, dass der Client (hier das Endgerät) jegliche Statusinformation intern verwaltet wird und eine serverseitige Anfrage unabhängig von vorangegangener Kommunikation behandelt werden kann. Der aktuelle Status wird auf dem Gerät mittels Modbus

Registern oder REST Endpunkten zur Verfügung gestellt und kann von außen abgerufen bzw. verändert werden.

Die Spezifikation bietet einen großen Umfang an Datenpunkten für unterschiedliche Technologien und deckt voraussichtlich die benötigte Funktionalität für eine *Digitale Schnittstelle* ab.

Die Erweiterbarkeit auf Teilnehmerebene wird als einfach eingestuft, auf der Datenpunktebene ist die Erweiterbarkeit etwas komplizierter, da man bei Erweiterung der Datenpunkte beginnt von der standardisierten Spezifikation abzuweichen.

Security Aspekte

Vor allem auf der Security Ebene sind REST und Modbus sehr unterschiedlich zu bewerten. Modbus ist ein relativ simples, altes Protokoll, das schwer abzusichern ist. Eine REST API kommuniziert mittels HTTP als Applikationsprotokoll, das auf Grund seiner weiten Verbreitung im Webbereich als sehr gut und einfach abzusichern gilt.

Die Spezifizierung beinhaltet Cybersecurity Richtlinien für Modbus Implementierungen, jedoch nicht für REST Schnittstellen. Wahrscheinlich ist das auf Grund des „Test“ Status der Fall.

EEBus

Generelle Kriterien

Die EEBus Initiative e.V. ist 2012 aus einem Leuchtturmprojekt des deutschen Wirtschaft- und Technologieministeriums entstanden. Zusammen mit Industriepartnern ist ihr Ziel einen Kommunikationsstandard zu schaffen, der die Interaktion und das Management von unterschiedlichen Geräten ermöglicht. Zum jetzigen Zeitpunkt gibt es bereits Seriengeräte, wie Ladestationen und Wechselrichter, am Markt die eine EEBus Schnittstelle implementiert haben. Die aktuelle Entwicklung der Verbreitung ist, ohne eine genauere Analyse der Marktdurchdringung, jedoch schwer einzuschätzen, wird jedoch eher als steigend abgeschätzt.

Die EEBus Initiative hat die Definitionen eines „Smart Home Internetprotokolls“ (SHIP) für die Kommunikationsebene und eines Datenmodells namens „Smart Premises Interoperable Neutral-Message Exchange“ (SPINE) veröffentlicht. Das SPINE Datenmodell ist aus der „Smart Applications Reference“ (SAREF) Ontologie von ETSI abgeleitet und als XML-Schema veröffentlicht.

Für SHIP und SPINE lassen sich nicht ausgereifte Open Source Projekte finden, leider gibt es keine fertige, nutzbare Implementierung, die frei zugänglich ist. Das nennenswerteste Projekt ist das des Open Source Lademanagers „evcc“ (https://github.com/evcc-io/eebus), das in Go implementiert ist.

Die Einarbeitungszeit sowie die Integration in andere Systeme wird für EEBus eher gering eingeschätzt, da die eingesetzten Technologien (WebSockets) weitverbreitet sind.

Zum Einsatz kommen könnte der EEBus sowohl also zentrales Interface zwischen VNB und dritten Systemen, prädestiniert wäre es jedoch für eine lokale Schnittstelle hinter einem geeigneten Funktionsblock, der die Welten von VNB und Endkunde trennt. Die verfügbaren Use-Cases der EEBus Initiative befassen sich auch hauptsächlich mit dieser Anwendung.

Operative Kriterien

Sowohl Datenresolution und Datenintensität in für die Kommunikation wird als gering eingeschätzt. Die Skalierbarkeit der Lösung wird als gut eingeschätzt, da die eingesetzten Webtechnologien auch bei großen Projekten im IT-Bereich eingesetzt werden, wobei WebSockets (auf denen SHIP basiert), auf Grund ihrer durchgehenden TCP Verbindung, nicht so gut skalierbar sind wie zustandslose Anwendungen (z.B. REST Lösungen).

Technologiespezifische Kriterien

Die Erweiterbarkeit ist sowohl für Datenpunkte als auch für weitere Kommunikationsteilnehmer wird als sehr einfach eingeschätzt. Unterschiedliche Arten von Datentypen sind in SPINE definiert und können benutzt werden, um Messungen, Status und Einstellungen zu übertragen.

Als Teil des SHIP Spezifikation können außerdem mittels mDNS (Multicast Domain Name Server Protocol) Erkennungsfunktionen von Geräten, die eine EEBus Schnittstelle besitzen, genutzt werden. Das ermöglicht die automatische Erkennung von EEBus fähigen Geräten im lokalen Netzwerk und die Übertragung von angebotenen Funktionen an Managementanwendungen.

WebSockets, die die Grundlage von SHIP bilden, sind erstmals im Jahr 2010 standardisiert worden und stellen einen bidirektionalen Kommunikationskanal zwischen zwei Endpunkt, basierend auf einer persistenten TCP Verbindung, dar.

Die genauen Datenpunkte aus der Arbeitsgruppe müssten erst mit den vorhandenen Datentypen und Arten von Daten abgeglichen werden, um ein Set von Daten zu definieren, dass für den Use Case verwendet werden kann. Es ist möglich die gewollte Steuerung über EEBus durchzuführen.

Security Aspekte

In der Definition des SHIP Protokolls ist definiert, dass die Kommunikation über TLS 1.2 stattfinden muss. Zusätzlich ist eine Authentifizierung über TLS Zertifikate im Kommunikationsaufbau verpflichtend. Als Standard-Absicherungsmethode im IT-Bereich, wird die Verwendung von TLS hier als sehr sicher eingestuft. Die Sicherheit der Implementierung hängt stark von der Umset-

zung ab. Kommunikation über WebSockets kann als weit verbreitete Webtechnologie gut abgesichert werden und deren Security Aspekt wird als sehr gut bewertet. Weitere Analysen mit den genauen Prozessdefinitionen sind notwendig um eine eindeutigere Einschätzung zu ermöglichen.

Modbus TCP

Generelle Kriterien

Modbus ist ein Kommunikationsprotokoll das in den späten 70er Jahren zur Kommunikation mit „SPS“ (Speicherprogrammierbare Steuerungen) entworfen wurde. Veröffentlicht wurde das Modbus Protokoll von dem amerikanischen Unternehmen Modicon. Mittlerweile hat sich Modbus, vor allem Modbus TCP, in vielen Bereichen der Industrie zu einem „de facto“ Standard entwickelt und wird sehr weit verbreitet zur automatisierten Steuerung von intelligenten elektronischen Geräten eingesetzt.

Das Modbus Protokoll ist offen verfügbar und es gibt in einer Vielzahl von Programmiersprachen Pakete, die das Modbus Protokoll implementieren. Ein Beispiel dafür ist „pymodbus“ (https://github.com/riptideio/pymodbus) das eine volle Implementierung des Modbus Protokolls für Python veröffentlicht. Eine weitere open source Implementierung des Modbus Protokolls ist „libmodbus“ (https://github.com/stephane/libmodbus), das in C geschrieben ist.

Auf Grund der Einfachheit des Protokolls wird es sehr weit verbreitet eingesetzt, die Verbreitungsentwicklung wird jedoch als eher schrumpfend bewertet, da in einigen Einsatzbereichen neuere Kommunikationsprotokolle bzw. -standards Modbus ersetzen.

Wegen der aktuellen weiten Verbreitung werden die Einarbeitungszeit und der notwendige Aufwand als gering eingeschätzt, da es viele Beispiele für den Einsatz und mögliche Implementierung gibt. Die Kosten für die Implementierung einer Modbus Schnittstelle werden ebenfalls gering eingeschätzt.

Der Einsatz von Modbus wäre nur als lokales Interface ratsam, da das Protokoll als schwer abzusichern gilt und eine Verbindung über lokales Netzwerk hinaus, gegebenenfalls über das öffentliche Internet, nicht ratsam ist.

Operative Kriterien

Die zeitliche Auflösung, die mit einer Modbus Kommunikation zu erreichen ist, ist sehr gering, da das Protokoll sehr einfach aufgebaut ist und geringe Datenmengen übertragen werden. Es sind keine zusätzlichen zeitlichen Grenzen gesetzt. Der limitierende Faktor ist die Zeit, die gebraucht wird, um Daten in Register zu schreiben bzw. auszulesen.

Das Modbus Protokoll ist darauf ausgelegt mit einzelnen Befehlen einzelne Datenpunkte zu lesen bzw. zu schreiben. Zum Beispiel ist es mittels Modbus nicht möglich über einen einzelnen Befehl einen, nicht vordefinierten, Zeitverlauf für die Leistung einer Komponente zu setzen. Da mit jedem Befehl nur ein einzelnes Register beschrieben werden kann, wäre es notwendig die einzelnen Datenpunkte des Profils und deren relative zeitliche Verschiebung im Vorfeld statisch zu definieren, um einen Verlauf einer Variablen vorgeben zu können.

Technologiespezifische Kriterien

Auf Grund der langen Zeit, die Modbus bereits genutzt wird, ist es technologisch sehr stabil und es sind keine Änderungen an den Spezifikationen zu erwarten. Die Simplizität des Protokolls und der einfache Aufbau der Datenpakete machen Modbus sehr gut erweiterbar, sowohl in der Anzahl der Datenpunkte, die verändert werden können als auch in der Anzahl der angesprochenen Modbus Clients.

Die Grundlage von Modbus TCP sind Register, die mit Datenwerten beschrieben und/oder ausgelesen werden können. So kann der Modbus Client (Kundenseite) bestimmte Register anpassen, wenn sich ein Status ändert der daraufhin vom Server (VNB) abgefragt werden kann. Ebenso können Register vom Server gesetzt werden, um das Verhalten auf Client Seite zu verändern.

Datenpunkte und deren Struktur bzw. Registeradressen müssen bei reinem Modbus für die Anwendung eigens spezifiziert werden. Eine solche Spezifikation gibt es zum Beispiel für Sunspec Modbus. Beim Sunspec Protokoll sind Registeradressen und erwartetes Verhalten in Abhängigkeit des Status definiert.

Das Modbus Protokoll ist nicht mehr Stand der Technik, wird aber immer noch weit verbreitet eingesetzt. Die weite Verbreitung von Modbus Implementierungen zur Kommunikation mit Geräten aus unterschiedlichen Bereichen wäre ein Grund für die Nutzung von Modbus zur Nutzung von Modbus in einer lokalen Schnittstelle. Unterschiedliche Spezifikationen von Herstellern könnte hier aber zu weiteren Problemen in der Vereinheitlichung der Modbus Schnittstelle für den VNB führen.

Der Einsatz von Modbus TCP ist in allen IP basierten Netzwerken möglich, da TCP direkt über das Internet Protokoll kommuniziert werden kann.

Die verbundene Komplexität mit einer Kommunikation über Modbus wird als eher gering eingeschätzt, der Aufwand wäre vor allem in der Vereinheitlichung von Spezifizierung der Schnittstelle.

Security Kriterien

Auf Security Ebene gibt es mehrere Bedenken bezüglich des Einsatzes von Modbus TCP. Um Modbus abzusichern, gibt es Modbus Secure, dass die Kommunikation über sichere Transportkanäle ermöglicht. Auf Grund des Aufbaus der Technologie gibt es jedoch keine Möglichkeit einen Kommunikationspartner zu authentifizieren. Hier wäre es nicht möglich festzustellen wer ein Register ausliest oder beschreibt. Sollte ein Angreifer Zugriff zum Netzwerk erlangen ist Modbus sehr leicht angreifbar.

Um das Protokoll und die Schnittstelle abzusichern, müssten eine Vielzahl von Maßnahmen getroffen werden. Diese Vorkehrungen müssten an unterschiedlichen Stellen implementiert werden. Hersteller müssten hier zusammen mit VNB sichere Kommunikationskanäle aufsetzen. Auf Grund der mehreren Parteien, die in die Implementierung eingebunden werden müssen, wird der Prozess als fehleranfällig eingeschätzt und die Möglichkeit Modbus TCP abzusichern, als gering eingeschätzt.

IEC 60870-5-104

Generelle Kriterien

Die IEC 60870 ist ein Kommunikationsstandard im Bereich der Prozessautomatisierung, und wird von der IEC herausgegeben und betreut. Der Teil 60870-5-101 beschreibt die Möglichkeit der Kommunikation über serielle Datenübertragungskanäle. Dieser Teil wird vor allem in der Fernwirktechnik eingesetzt. Der Teil 60870-5-104 beschreibt die Übertragung der Datenpakete über TCP/IP, also Internetprotokoll-basierte Netzwerke. Dieser Standard ist weit verbreitet in der Prozessautomatisierung im Infrastrukturbereich. Ähnlich wie die IEC 61850 erlaubt die IEC 60870 direkte Kommunikation zwischen Partnern. Der Standard definiert jedoch keine ausführlichen Datenmodelle, sondern eher generelle Konzepte von Messdaten und Steuerbefehlen.

Es gibt mehrere open source Implementierung der IEC 60870, mehrere davon können als aktiv bezeichnet werden (z.B. https://github.com/mz-automation/lib60870).

Die notwendige Einarbeitungszeit, um mit der IEC 60870 umgehen zu können wird als gering eingeschätzt, da die Struktur der Datenübertragung simpel aufgebaut ist. Die erwarteten Kosten sind ebenfalls eher gering einzuschätzen. Die Integration in bestehende Systeme würde sich wahrscheinlich eher einfach gestalten.

Die IEC 60870-5-104 würde sich vor allem für die Implementierung einer zentralen Schnittstelle eignen, da die IEC 60870 üblicherweise nicht auf der Endgeräteebene implementiert ist.

Operative Kriterien

Die Kommunikation über 60870 ist sehr Dateneffizient gestaltet. Es werden keine großen Datenmengen übertragen, und die einzelnen Datenpakete sind relativ klein. Es können jedoch nur einzelne Datenpunkte übertragen werden. Das Übertragen von Profilen als Vorgabewerte mit einem gewissen zeitlichen Horizont ist nicht vorgesehen.

Die Skalierbarkeit von mehreren Datenverbindungen ist prinzipiell gut, nur stellt die Administrierung vieler gleichzeitiger Steuerungen einen hohen Aufwand dar.

Als Fehlertoleranzfunktionen wird auf die TCP Funktionalität zur Fehlererkennung und erneuten Übertragung zurückgegriffen. Der Standard beinhaltet keine genaueren Ansätze zur Wartung der Schnittstellen.

Technologiespezifische Kriterien

Die Architektur der IEC 60870 ist eine recht simpel gehaltene Server-Client Architektur, bei der der Server einzelne Datenpunkte abrufen und verändern kann, bzw. der Client bei Events bestimmte Informationen an den Server weiterreichen kann.

Die Erweiterbarkeit auf Teilnehmerebene wird als sehr einfach eingeschätzt, ebenso auf Ebene der Datenpunkte. Die Spezifizierung bzw. Standardisierung einer Spezifikation für Datenpunkte die vorhanden sein müssen für die gewollte *Digitale Schnittstelle*, gestaltet sich für die IEC 60870 schwieriger, da hier eine eigene Spezifikation entworfen werden muss. Die 60870 definiert nur bestimmte Datentypen, aber kein komplettes Datenmodell. Die Architektur ist eher veraltet, kommt aber noch häufig zum Einsatz.

Security Aspekte

Die Security Aspekte wurden bei der Konzeption der IEC 60870 nicht ausreichend beachtet. Deswegen hat die IEC den Cybersecuritystandard IEC 62351 herausgegeben, der sowohl für die IEC 60870 als auch für die IEC 61850 die notwendigen Maßnahmen zur Absicherung der Kommunikation beschreibt.

Die Absicherung eines Kommunikationskanals mit der IEC 60870 wird deswegen als schwieriger abzusichern eingeschätzt als ein Kommunikationskanal über einen Webstandard wie HTTPS.

Die genauen Anforderungen an die Prozesse müssen erst festgelegt werden, um Absicherungsmaßnahmen für eine Kommunikation über IEC 60870 definieren zu können und den Standard im Kontext genauer evaluieren zu können.

KNX-IOT

Generelle Kriterien

KNX ist ein offener Standard für gewerbliche und private Gebäudeautomation. Basierend auf den drei Standards Europäischer Installationsbus (EIB), BatiBus und European Home Systems (EHS) ist KNX der Nachfolger im Bereich Gebäudeautomation.

KNX IoT ist eine Drittanbieter IoT API, die noch nicht fertig spezifiziert ist. Laut KNX-Website ist der Open Source Stack verfügbar, jedoch führt der Link zu keiner Website. Für die Dokumentation ist bis jetzt nur ein leerer Platzhalter verfügbar. Ziel ist es sich an den Markt anzupassen damit auch nicht KNX Geräte mit KNX Geräten über eine REST API kommunizieren können.

Wahrscheinlich wird KNX IoT nur für die Kommunikation Gateway zu Kundenanlagen verwendbar sein, da aber KNX IoT noch nicht komplett definiert zugänglich ist, kann sich dies auch noch ändern.

Zumindest für die Implementierung von KNX gibt es von KNX eine standardisierten Software Engineering-Tool-Software (ETS) und auch viel Hardware welches bereits kompatibel mit dem KNX Standard ist. Dadurch lässt sich vermuten das KNX IoT auch leicht implementieren lässt, neben der Tatsache das REST Interfaces eher einfach zu implementieren sind.

Operative Kriterien

Aufgrund des Anwendungsbereiches von KNX IoT lässt sich vermuten das die Skalierbarkeit gut sein wird und die maximale Anzahl an Verbindungen auch eher überdurchschnittlich sein wird. Bezüglich der zeitlichen Auflösung, Fehlertoleranzen und Wartungsfunktionen muss man den endgültigen Standard abwarten.

Technologiespezifische Kriterien

KNX IoT soll es ermöglichen das KNX mit anderen Nicht-KNX-Geräten über standardisierte und nicht herstellerspezifische spezielle RESTful API kommunizieren können.

Für die Definition von Datenpunkten wird statt einem verbreiteten Format das KNX IoT das eigene ETS4 Format verwendet, welches die erstmalige Implementierung schwerer machen könnte.

Die KNX IoT API wird mit JSON-API definiert, welches eine Spezifikation für die Erstellung von APIs mit dem weit verbreitete JSON Format ist.

Security Aspekte

Bezüglich der Sicherheitsaspekte gibt es zurzeit keine Information zu KNX IoT.

DNP3

Generelle Kriterien

DNP3 (Distributed Network Protocol) ist ein Standard bzw. Protokoll aus dem Bereich der “Fernwirktechnik”. Allgemein wird dieses Protokoll zwischen Leitsystemen und Fernsteuerungsterminals angewendet. Es wurde im Jahr 1993 von der Firma *Harris* (heute GE Energy) spezifiziert und entwickelt, weil der internationale Standard IEC 60870-5 noch nicht fertig publiziert war. DNP3 ist sehr stark in den USA verbreitet. Der Trend scheint aber von DNP3 weg zu gehen, meist zu IEC61850 oder Standards bzw. Protokollen aus dem IT Bereich.

Es gibt nur eine bedeutende OSS Implementierung von *Step Function I/O* die das ursprüngliche Project opendnp3 von C++ auf Rust portiert haben und dies hier zur Verfügung stellen. Rein von der Anzahl der Commits gemessen kann man das Project als sehr aktiv einstufen. Es haben sich jedoch durch den Wechsel auf Rust Einschränkungen eingeschlichen (z.B. Compiler support) und das hat die *Usability* stark reduziert.

Operative Kriterien

Die Bewertung der operativen Kriterien für DNP3 ist sehr ähnlich wie für die IEC 61850. Da der Standard jedoch ursprünglich für Serielle/Dial-up Schnittstellen entwickelt wurde waren EMS Aspekte im Vordergrund. Auch in der neuen Iteration ist es als Layer-2 Standard zu sehen. Dies erfordert ein robustes Design – generell gilt DNP3 als einer der robustesten und effizientesten Standards in dessen Anwendungsbereich.

Technologiespezifische Kriterien

DNP3 ist auf dem SCADA (Supervisory Control and Data Acquisistion) <-> RTU (Remote Terminal Unit) Prinzip aufgebaut. Es kann sich über Modelle als auch einzelne Messages synchronisieren oder austauschen. Es ist hauptsachlich konzipiert für 1:N Operation; also 1 Master(SCADA) und mehrere Slaves(RTU). Es wird an einer Erneuerung gearbeitet mit der direkte Peer-to-peer Kommunikation, ohne zentralen Master, ermöglicht wird. Das DNP3 Protokoll kann genutzt werden um sowohl Push/Pull als auch Event basiertes Messaging zu implementieren. Das heißt, dass das SCADA aktiv Werte abfragen kann sowie die RTU’s Messages ungefragt verschicken können. Durch Message Klassifizierung werden Prioritäten für Nachrichten definiert und unterschiedliche Reaktionsschritte am RTU als auch am SCADA vorgesehen.

Generell ist das einsetzten des Standards trivial, solang die Architektur schon vorhanden ist. Wie oben schon gesagt wurde, ist mit der Portierung auf Rust einiges an Flexibilität verschwunden und erlaubt limitierten Einsatz bei IoT Geräten.

Da der Standard relativ unbekannt und in Europa fast nicht eingesetzt wird, könnte es Schwierigkeiten mit sich bringen DNP3 auszurollen.

Security Aspekte

DNP3 ist mit IEC 62351-5 konform. Das heißt es deckt alle Anforderungen an ein TC 57 Protokoll. Es wurde einiges an Arbeit aufgebracht um „Secure Authentication“ in das Protokoll zu bringen. OSI basierte Kommunikation kann über TLS verschlüsselt werden und ist auch standardmäßig Teil der Implementierung. Das gilt nicht für die serielle Implementierung des Protokolls. Neuerdings stellen manche Produzente BTW (Bump in the Wire) basierte Verschlüsselung zur Verfügung.

J.5.4 Klassifizierung der Analysekriterien

In diesem Abschnitt wird dargestellt, wie die Analysekriterien für die untersuchten Standards und Protokolle klassifiziert werden, um die Bewertung der Standards und Protokolle durchführen zu können. Die zusammengefassten Ergebnisse der Bewertung sind im Abschnitt J.5.2 zu finden, die vollständige numerische Bewertung im Kapitel J.5.5.

Tabelle 5: Klassifizierung der Analysekriterien

Aspekt	**1**	**2**	**3**	**4**	**5**
Generelle Kriterien					
Verbreitung *Industrie*	Gar nicht	Wenig	Mittel, Domänen-spezifisch	Hoch, Domänen-spezifisch	Hoch, Domänen-übergreifend
Verbreitung *Wissenschaft*	Länderspezifisch	Mehrere Länder	Kontinent spezifisch	Mehrere Kontinente	Global
Ursprung *Anwendungs-bereich*	Anderer Bereich	Automatisierung	Smart Grids	Incentivierung DER	Steuerung DER
Ursprung *Organisation*	Forschungs-projekt	Regierungs-projekt	Industrie-konsortium	Standard	Open Source
Ursprung *Region/Land*	Andere	Asien	Amerika	Europa	International
Anwendungs-bereiche *aktuell*	Anderer Bereich	Automatisierung	Smart Grids	Incentivierung DER	Steuerung DER
Verbreitungs-entwicklung	Stark schrumpfend	Schrumpfend	Gleich-bleibend	Wachsend	Stark Wachsend
Open Source Projekte	Keine	Ein nicht aktives / ausgereiftes	Mehrere nicht aktive	Ein aktives	Mehrere aktive
Umsetzung *Einarbeitungs-zeit*	Sehr lang	Eher lang	Mittel	Eher kurz	Sehr kurz
Umsetzung *Integration*	Sehr schwer	Eher schwer	Mittel	Eher leicht	Sehr leicht
Umsetzung *Kosten*	Sehr hoch	Eher hoch	Mittel	Eher niedrig	Sehr niedrig
Geeignete Interfaces	Definition Interfaces, kein numerischer Wert				
Offener Standard	Ausschlusskriterium, kein numerischer Wert				

Operative Kriterien					
Daten-resolution	Ungenügend	-	Genügend	-	Sehr gut
Daten-intensivität *Übertragungs-methodik*	-	Request	Single point	Push/Pull	Burst
Daten-intensivität *Kommunikation*	Sehr hoch	Eher hoch	Mittel	Eher niedrig	Sehr niedrig
Skalierbarkeit	Schlecht	-	Weniger gut	-	Sehr gut
Fehlerkorrektur	Keine	-	Fehler-erkennung	-	Gute Fehlerkorrektur
Wartungs-ansätze	Keine	-	-	-	Gibt Wartungs-ansätze
Technologiespezifische Kriterien					
Erweiterbarkeit *Teilnehmer*	Sehr schwer	Schwer	Mittel	Leicht	Sehr leicht
Erweiterbarkeit *Datenpunkte*	Sehr schwer	Schwer	Mittel	Leicht	Sehr leicht
Erweiterbarkeit *Asset Erkennung*	Keine Erkennung	-	-	-	Erkennungs-funktion
Architektur *Modernität*	Veraltet	-	State of the Art	-	Bleeding Edge
Verfügbarkeit *Protokolle/Standards*	Proprietär	-	Limitierte Lizenz	-	Frei verfügbar
Stabilität *Versions-Kompatibilität*	Schlecht	-	Weniger gut	-	Sehr gut
Datenmodell *Erweiterbarkeit*	Gar nicht	-	Mittel	-	Gut
Datenmodell EVSE *Anforderungs-überschneidung*	Nein	-	Teilweise	-	Ja
Datenmodell Wechselrichter	Nein	-	Teilweise	-	Ja

Anforderungs-überschneidung					
Datenmodell Batterie *Anforderungs-überschneidung*	Nein	-	Teilweise	-	Ja
Datenmodell Wärmepumpe *Anforderungs-überschneidung*	Nein	-	Teilweise	-	Ja
Datenmodell Smart Meter *Anforderungs-überschneidung*	Nein	-	Teilweise	-	Ja
Installations-komplexität	Hoch	-	Mittel	-	Niedrig
Securityspezifische Kriterien ***Absicherungskomplexität***					
Integrität	Schwer	Eher schwer	Mittel	Eher einfach	Einfach
Authentizität	Schwer	Eher schwer	Mittel	Eher einfach	Einfach
Verfügbarkeit	Schwer	Eher schwer	Mittel	Eher einfach	Einfach
Vertraulichkeit	Schwer	Eher schwer	Mittel	Eher einfach	Einfach

J.5.5 Detaillierte numerische Bewertung der Standards und Protokolle

In diesem Kapitel ist die detaillierte Bewertung aller untersuchten Standards und Protokolle zu finden, die in der kompakten Bewertung im Abschnitt J.5.2 zusammengefasst wurde.

	Kategorie	***Generell***					
	Aspekt	**Verbreitung**	**Verbreitung**	**Ursprung**	**Ursprung**	**Ursprung**	**Anwendungsbe-reiche**
	Beschreibung	*Gewerbe/Industrie*	*Wissenschaft*	*Anwendungsbereich*	*Organisation*	*Region/Land*	*Aktuell*
Kommunikationsstandard							
IEC 61850		4	5	3	4	4	3
IEEE 2030.5		4	3	5	4	3	5
IEC 62746 (OpenADR)		3	3	4	4,5	3	4
EEBus (IEC 63380)		3	3	5	2	4	5
Sunspec Modbus / REST		4	5	3	3	3	3
OCPP 2.0.1		4	4	3	4	4	2,5
KNX IoT		4	3	2	3	4	1,5
DNP3		5	1	5	4	3	4
IEC 60870-104		5	3	2	4	4	2
Modbus TCP		5	5	2	3	3	2

	Generell				
	Verbreitungs-entwicklung	**Open Source**	**Implementierung**	**Implementierung**	**Implementierung & Errichtung**
	Wachsend/ Schrumpfend	*Implementierungen Verfügbar*	*Einarbeitungszeit*	*Integration*	*Zu erwartende Kosten*
Kommunikationsstandard					
IEC 61850	3	4	2	2	2
IEEE 2030.5	4	2	4	4	5
IEC 62746 (OpenADR)	4	5	4	4	5
EEBus (IEC 63380)	4	2	4	4	5
Sunspec Modbus / REST	4	5	3	5	5
OCPP 2.0.1	4	5	4	4	5
KNX IoT	3	5	4	4	4
DNP3	2	1	2	4	3
IEC 60870-104	3	3	5	4	5
Modbus TCP	2	5	5	4	5

	Operativ					
	Datenresolution	**Datenintensivität**	**Datenintensivität**	**Skalierbarkeit**	**Fehlertoleranz**	**Wartbarkeit**
	Zeit	*Übertragungsmethodik*	*Kommunikation*	*Operativ*	*Operativ*	*Schnittstelle*
Kommunikationsstandard						
IEC 61850	5	4	4	5	2	1
IEEE 2030.5	5	4	3	5	3	1
IEC 62746 (OpenADR)	3	4	2	5	3	1
EEBus (IEC 63380)	5	4	4	5	3	1
Sunspec Modbus / REST	5	4	4	3	3	1
OCPP 2.0.1	3	4	3,5	5	3	2
KNX IoT	5	4	3	5	3	1
DNP3	5	4	2	5	5	5
IEC 60870-104	5	3	4	3	1	1
Modbus TCP	5	3	4	3	1	1

	Technologiespezifisch						
	Erweiterbarkeit	**Erweiterbarkeit**	**Erweiterbarkeit**	**Modernität**	**Verfügbarkeit**	**Stabilität (Versions-kompatibilität)**	**Installationskomplexität - Architekturvariante**
	Teilnehmer	*Datenpunkte*	*Asset Erkennung*	*Architektur*	*Lizenzfreiheit*	*Technologien*	*Inbetriebnahme - Varianten*
Standard/Protokoll							
IEC 61850	5	5	1	1	5	5	1
IEEE 2030.5	5	5	5	3	5	5	5
IEC 62746 (OpenADR)	5	5	5	3	5	5	3
EEBus (IEC 63380)	5	5	5	5	5	4	5
Sunspec Modbus / REST	5	5	1	3	5	5	3
OCPP 2.0.1	5	5	1	5	5	3	5
KNX IoT	5	5	1	3	5	3	5
DNP3	3	5	1	1	3	4	5
IEC 60870-104	5	5	1	1	5	4	5
Modbus TCP	5	5	1	1	5	4	5

	Technologiespezifisch					
	Datenmodell	**Datenmodell - EV**	**Datenmodell - Wechselrichter**	**Datenmodell - Batterie**	**Datenmodell - Wärmepumpe**	**Datenmodell – Smart Meter**
	Erweiterbarkeit	*Anforderungs-überschneidung*	*Anforderungs-überschneidung*	*Anforderungs-überschneidung*	*Anforderungs-überschneidung*	*Anforderungs-überschneidung*
Standard/Protokoll						
IEC 61850	3	5	5	5	3	5
IEEE 2030.5	5	5	5	5	3	5
IEC 62746 (OpenADR)	5	3	3	3	3	3
EEBus (IEC 63380)	5	1	1	1	1	1
Sunspec Modbus / REST	5	5	5	5	3	5
OCPP 2.0.1	3	5	1	1	1	1
KNX IoT	5	1	1	1	1	1
DNP3	3	3	5	1	1	5
IEC 60870-104	5	1	1	1	1	1
Modbus TCP	5	1	1	1	1	1

	Security			
	Integrität	**Authentizität**	**Verfügbarkeit**	**Vertraulichkeit**
Standard/Protokoll				
IEC 61850	5	4	5	4
IEEE 2030.5	5	5	5	5
IEC 62746 (OpenADR)	5	5	5	5
EEBus (IEC 63380)	5	5	5	5
Sunspec Modbus / REST	5	5	5	5
OCPP 2.0.1	5	5	5	5
KNX IoT	5	5	5	5
DNP3	5	4	3	4
IEC 60870-104	5	4	4	4
Modbus TCP	1	4	4	2

	Generell	Operativ	Technologie-spe-zifisch	Security	Summe
Standard/Protokoll					
IEC 61850	3,19	3,50	3,86	4,50	15,05
IEEE 2030.5	3,95	3,50	4,71	5,00	17,17
IEC 62746 (OpenADR)	4	3,00	4,00	5,00	16,00
EEBus (IEC 63380)	3,76	3,67	3,50	5,00	15,93
Sunspec Modbus / REST	3,86	3,33	4,29	5,00	16,48
OCPP 2.0.1	3,48	3,42	3,29	5,00	15,18
KNX IoT	3,43	3,50	3,00	5,00	14,93
DNP3	3,19	4,33	3,21	4,00	14,74
IEC 60870-104	3,67	2,83	2,79	4,25	13,54
Modbus TCP	3,67	2,83	2,79	2,75	12,04

J.5.6 Gewichtung der Bewertungskriterien

Im Abschnitt J.5.2 wurde die Bewertung der Standards und Protokolle kompakt zusammengefasst. Dabei wurde folgende Gewichtung durchgeführt, die mit den Stakeholdern im Expertenpool abgestimmt worden ist:

Generell							
Verbreitung	**Verbreitung**	**Ursprung**	**Ursprung**	**Ursprung**	**Anwendungsbereiche**	**Verbreitungsentwicklung**	**Open Source**
Gewerbe/Industrie	*Wissenschaft*	*Anwendungsbereich*	*Organisation*	*Region/Land*	*Aktuell*	*Wachsend/Schrumpfend*	*Implementierungen Verfügbar*
2	***1***	***1***	***0,5***	***0,5***	***2***	***2***	**2**

Generell			***Operativ***					
Implementierung	**Implementierung**	**Implementierung & Errichtung**	**Datenresolution**	**Datenintensivität**	**Datenintensivität**	**Skalierbarkeit**	**Fehlertoleranz**	**Wartbarkeit**
Einarbeitungszeit	*Integration*	*Zu erwartende Kosten*	*Zeit*	*Übertragungs-methodik*	*Kommunikation*	*Operativ*	*Operativ*	*Schnittstelle*
1	**1**	**2**	**0,5**	**0,5**	**1**	**2**	**2**	**1**

Technologiespezifisch						
Erweiterbarkeit	**Erweiterbarkeit**	**Erweiterbarkeit**	**Modernität**	**Verfügbarkeit**	**Stabilität (Versionkompabilität)**	**Installationskomplexität**
Teilnehmer	*Datenpunkte*	*Asset Erken-nung*	*Architektur*	*Lizenzfreiheit*	*Technologien*	*Inbetriebnahme - Szenarien*
2	**1**	**1**	**2**	**1**	**1**	**1**

Technologiespezifisch					
Datenmodell	**Datenmodell - EV**	**Datenmodell - Wechselrich-ter**	**Datenmodell - Batterie**	**Datenmodell - Wärmepumpe**	**Datenmodell - Smart Meter**

Erweiterbarkeit	*Anforderungsüberschneidung*	*Anforderungsüberschneidung*	*Anforderungsüberschneidung*	*Anforderungs-überschneidung*	*Anforderungsüberschneidung*
1	**1**	**1**	**1**	**1**	**1**

Security			
Integrität	**Authentizität**	**Verfügbarkeit**	**Vertraulichkeit**
1	1	1	1

J.5.7 Cyber-Security Anforderungen

Das *National Institute of Standards and Technology (NIST)* definiert Richtlinien für die Cybersicherheit von Smart Grids.[27] Hierfür wurde eine zusammengesetzte High-Level-Ansicht der Akteure innerhalb jeder der Smart-Grid-Domänen definiert und die möglichen Schnittstellen dieser Akteure aufgelistet (siehe Abbildung 31).

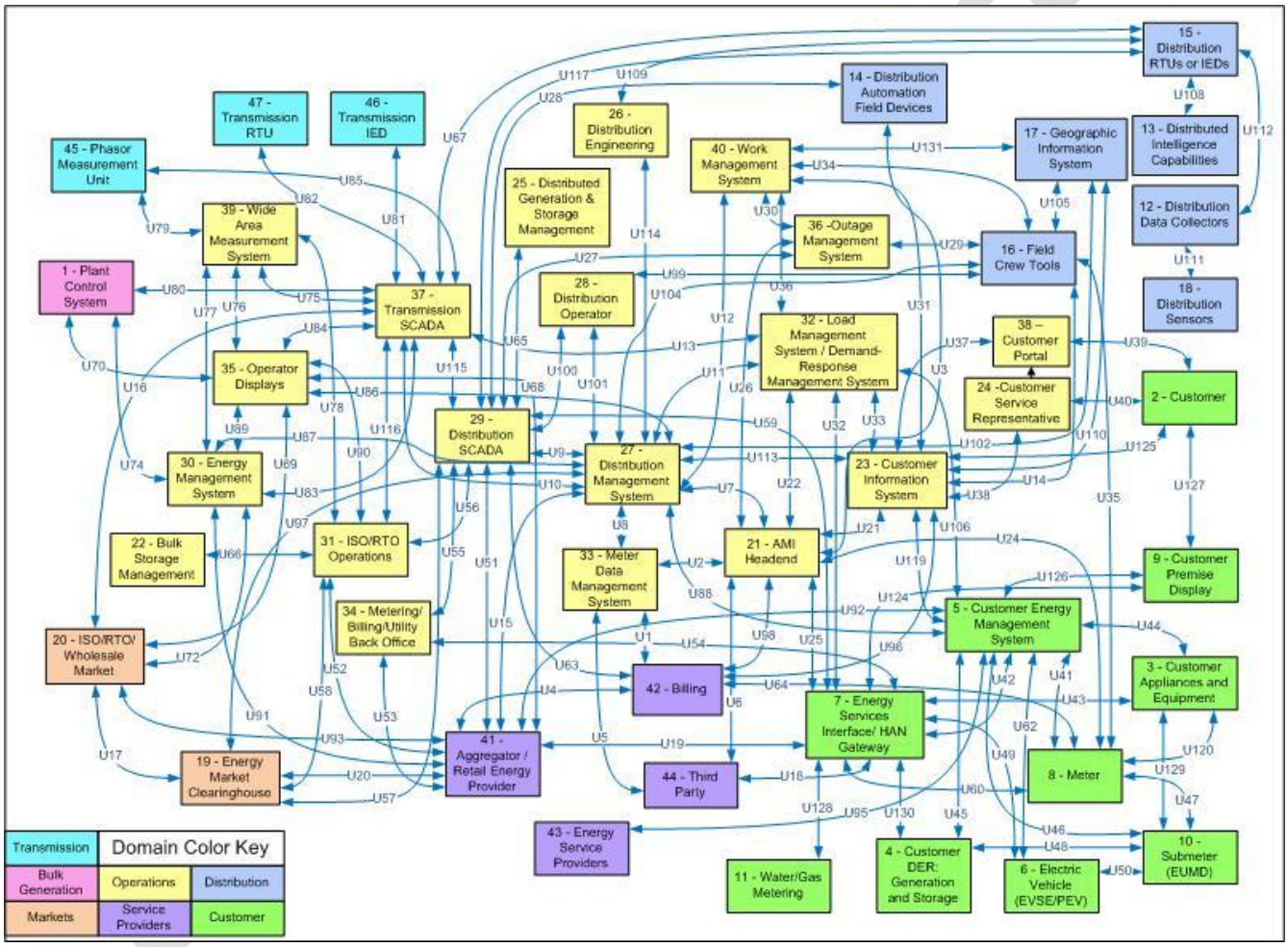

Abbildung 31: Logical Reference Model from NIST Guidelines for Smart Grid Cyber Security

Die Schnittstellen werden in 22 "logische Schnittstellenkategorien" eingeteilt. Für jede Kategorie wird die Bedeutung von Vertraulichkeit, Integrität und Verfügbarkeit festgelegt (*niedrig/low, mittel/moderate,*

[27] (NIST National Institute of Standards and Technology, 2010)

hoch/high). Für jede Schnittstelle werden, je nach Risikoeinstufung (*niedrig/low, mittel/moderate, hoch/high*), drei Arten von Anforderungen definiert:

- *Governance, risk, and compliance (GRC)* – Diese Anforderungen erfordern eine Behandlung auf der Organisationsebene.
- *Common technical requirements (CTR)* – Diese Anforderungen gelten für alle logischen Schnittstellenkategorien.
- *Unique technical requirements (UTR)* – Diese Anforderungen sind einer oder mehreren logischen Schnittstellenkategorien zugeordnet.

Cyber-Security Sicherheitsziele

Mit Smart-Grid-Technologien werden Millionen neuer Komponenten in das Stromnetz eingeführt. Viele dieser Komponenten sind für die Interoperabilität und Zuverlässigkeit von entscheidender Bedeutung, kommunizieren bidirektional und haben die Aufgabe, die für den Betrieb der Stromnetze unerlässliche **Vertraulichkeit/Confidentiality**, **Integrität/Integrity** und **Verfügbarkeit/Availability** (CIA) zu gewährleisten.

Verfügbarkeit (Availability)

Die **Verfügbarkeit** ist das wichtigste Sicherheitsziel für die Zuverlässigkeit des Stromnetzes. Die mit der Verfügbarkeit verbundene Latenzzeit kann variieren:

- Im Bereich von Millisekunden: Schutzrelais
- Unter einer Sekunde: Weiträumige Überwachung der Situation im Übertragungsbereich
- Sekunden: SCADA-Daten von Unterstationen und Abgängen
- Minuten: Überwachung unkritischer Geräte und einiger Marktpreisinformationen
- Stunden: Ablesung von Zählern und längerfristige Marktpreisinformationen
- Tage/Wochen/Monate: Erfassung langfristiger Daten wie Informationen zur Netzqualität.

Ein *Verlust der Verfügbarkeit* ist die Unterbrechung des Zugangs zu oder der Nutzung von Informationen oder eines Informationssystems.

Integrität (Integrity)

Die **Integrität** für den Betrieb des Stromnetzes umfasst die Gewährleistung, dass die folgenden Kriterien erfüllt sind:

- Die Daten wurden nicht unbefugt verändert.

- Die Quelle der Daten ist authentifiziert.
- Der mit den Daten verbundene Zeitstempel ist bekannt und authentifiziert.
- Die Qualität der Daten ist bekannt und authentifiziert.

Ein *Verlust der Integrität* ist die unbefugte Änderung oder Zerstörung von Informationen.

Vertraulichkeit (Confidentiality)

Die **Vertraulichkeit** ist für die Zuverlässigkeit des Stromnetzes am wenigsten entscheidend. Allerdings wird die Vertraulichkeit immer wichtiger, insbesondere mit der zunehmenden Verfügbarkeit von Kundeninformationen im Internet und umfasst folgende Informationen bzw. Anforderungen:

- Datenschutz von Kundeninformationen.
- Informationen über den Strommarkt.
- Allgemeine Unternehmensinformationen, wie Gehaltsabrechnungen, interne strategische Planung usw.

Ein *Verlust der Vertraulichkeit* ist die unbefugte Offenlegung von Informationen.

Auswirkungsstufen

Basierend auf diesen Definitionen werden die Auswirkungsstufen (*Impact Levels*) für jedes Sicherheitsziel (Vertraulichkeit, Integrität und Verfügbarkeit) als niedrig, mittel und hoch angegeben. Die Auswirkungsstufen werden bei der Auswahl der Sicherheitsanforderungen für jede logische Schnittstellenkategorie verwendet (siehe United States Department of Commerce, National Institute of Standards and Technology, 2004). Jede der drei Auswirkungsstufen (d. h. niedrig, mittel, hoch) basiert auf den erwarteten nachteiligen Auswirkungen einer Sicherheitsverletzung auf den Unternehmensbetrieb, organisatorische Vermögenswerte oder Einzelpersonen.

Tabelle 6: Übersicht der Auswirkungsstufen für die Sicherheitsziele

Sicherheitsziele/ Auswirkungsstufen	Niedrig	Mittel	Hoch
Vertraulichkeit	Begrenzte nachteilige Auswirkung auf den organisatorischen Betrieb, das Organisationsvermögen oder Einzelpersonen	Schwerwiegende nachteilige Auswirkungen auf den Geschäftsbetrieb, das Vermögen der Organisation oder Einzelpersonen	Schwerwiegende oder katastrophale nachteilige Auswirkungen auf den Geschäftsbetrieb, das Vermögen der Organisation oder auf Einzelpersonen

Integrität	Begrenzte nachteilige Auswirkung auf den organisatorischen Betrieb, die Vermögenswerte der Organisation oder Einzelpersonen	Schwerwiegende nachteilige Auswirkungen auf den Geschäftsbetrieb, die Vermögenswerte der Organisation oder Einzelpersonen	Schwerwiegende oder katastrophale nachteilige Auswirkungen auf den Geschäftsbetrieb, das Vermögen der Organisation oder Einzelpersonen
Verfügbarkeit	Begrenzte nachteilige Auswirkung auf den organisatorischen Betrieb, die Vermögenswerte der Organisation oder Einzelpersonen	Schwerwiegende nachteilige Auswirkungen auf den organisatorischen Betrieb, die Vermögenswerte der Organisation oder Einzelpersonen	Schwerwiegende oder katastrophale nachteilige Auswirkungen auf organisatorische Abläufe, Vermögenswerte der Organisation oder Einzelpersonen

Methode

Um die in (NIST National Institute of Standards and Technology, 2010) definierten Richtlinien auf die drei festgelegten Architekturvarianten anzuwenden, wurden die folgenden Schritte durchgeführt:

1. Identifikation und Verknüpfung der Akteure der Architekturvarianten und jenen im NIST Modell
2. Identifikation und Verknüpfung der Schnittstellen der Architekturvarianten und jenen im NIST Modell
3. Cyber-Security Anforderungen an die Architekturvarianten

Ad 1. Identifikation und Verknüpfung der Akteure der Architekturvarianten und jenen im NIST Modell

Im Folgenden sind, die Eigenschaften der im NIST Modell identifizierten Akteure (auf Basis der Architekturvarianten) beschrieben:

- #3 Customer Appliances and Equipment (Domäne: Customer):

  Ein Gerät oder Instrument, das eine bestimmte Funktion erfüllen soll, insbesondere ein elektrisches Gerät, wie z. B. ein Toaster, für den Hausgebrauch. Ein elektrisches Gerät oder eine Maschine, die überwacht, gesteuert und/oder angezeigt werden kann.

- #4 Customer Distributed Energy Resources: Generation and Storage (Domäne: Customer):

  Energieerzeugungsressourcen, wie z. B. Sonnen- oder Windenergie, die zur Erzeugung und Speicherung von Energie verwendet werden (am Standort des Kunden), um eine Schnittstelle zum Controller (HAN/BAN) zu bilden und eine energiebezogene Aktivität durchzuführen.

- #5 Customer Energy Management System (Domäne: Customer):

  Ein Anwendungsdienst oder ein Gerät, das mit Geräten im Haus kommuniziert. Der Anwendungsdienst oder das Gerät kann Schnittstellen zum Zähler haben, um Verbrauchsdaten abzulesen, oder zum Betriebsbereich, um Preis- oder andere Informationen zu erhalten, um automatische oder manuelle Entscheidungen zur effizienteren Steuerung des Energieverbrauchs zu treffen. Das EMS kann ein vom Versorgungsunternehmen abonnierter Dienst, ein von einem Dritten angebotener Dienst, eine vom Verbraucher festgelegte Richtlinie, ein Gerät im Besitz des Verbrauchers oder eine manuelle Steuerung durch das Versorgungsunternehmen oder den Verbraucher sein.

- #6 Electric Vehicle Service Element/Plug-in Electric Vehicle (Domäne: Customer):

  Ein Fahrzeug, das hauptsächlich von einem Elektromotor angetrieben wird, der von einer wiederaufladbaren Batterie gespeist wird, die durch Anschluss an das Stromnetz oder durch Aufladen über eine benzinbetriebene Lichtmaschine wieder aufgeladen werden kann.

- #7 Home Area Network Gateway (Domäne: Customer):

  Ein Fahrzeug, das hauptsächlich von einem Elektromotor angetrieben wird, der von einer wiederaufladbaren Batterie gespeist wird, die durch Anschluss an das Stromnetz oder durch Aufladen über eine benzinbetriebene Lichtmaschine wieder aufgeladen werden kann.

- #27 Distribution Management Systems (Domäne: Operations):

  Eine Reihe von Anwendungssoftware, die den Betrieb elektrischer Systeme unterstützt. Zu den Anwendungsbeispielen gehören Topologieprozessor, dreiphasiger, unsymmetrischer Online-Verteilungsstrom, Kontingenzanalyse, Studienmodusanalyse, Verwaltung von Schaltaufträgen, Kurzschlussanalyse, Spannungs/VAR-Management und Verlustanalyse. Diese Anwendungen stellen dem Betriebspersonal und den Technikern zusätzliche Informationen und Werkzeuge zur Verfügung, die ihnen helfen, ihre Ziele zu erreichen.

- #29 Distribution Supervisory Control and Data Acquisition (Domäne: Operations):

  Ein Steuersystem, das den Status der einzelnen Geräte überträgt, den Energieverbrauch durch die Steuerung konformer Geräte steuert und den Betreibern die Möglichkeit gibt, die Geräte des Stromnetzes direkt zu steuern.

- #32 Load Management Systems/Demand Response Management System (Domäne: Operations):

  Ein LMS gibt Befehle zum Lastmanagement an Geräte oder Anlagen beim Kunden aus, um die Last in Spitzen- oder Notsituationen zu verringern. Das DRMS gibt Preis- oder andere Signale an Geräte und Anlagen an Kundenstandorten aus, um die Kunden (oder ihre vorprogrammierten Systeme) aufzufordern, ihre Last als Reaktion auf die Signale zu verringern oder zu erhöhen.

- #41 Aggregator/Retail Energy Provider (Domäne: Service Provider):

  Jeder Vermarkter, Makler, jede öffentliche Einrichtung, jede Stadt, jeder Landkreis oder jeder Sonderbezirk, der die Lasten mehrerer Endverbraucher zusammenfasst und den Verkauf und Kauf von elektrischer Energie, die Übertragung und andere Dienstleistungen im Namen dieser Kunden erleichtert.

Ad 2. Identifikation und Verknüpfung der Schnittstellen der Architekturvarianten und jenen im NIST Modell

Im nächsten Schritt wurden auf Basis der zuvor identifizierten Akteure die jeweiligen Schnittstellen (und deren Kategorien) zwischen den Akteuren im NIST Modell ermittelt. In Tabelle 7 sind die Schnittstellen-Kategorien (#) mit den jeweils identifizierten logischen Schnittstellen (Uxx) angeführt. Weiteres sind die Auswirkungsstufen (L = low/niedrig; M = moderate/mittel; H = high/hoch) für die identifizierten Schnittstellen-Kategorien in der Tabelle angeführt (C = Confidentiality/Vertraulichkeit; I = Integrity/Integrität; A = Availability/Verfügbarkeit).

Tabelle 7: Identifizierte Schnittstellen-Kategorien, logische Schnittstellen und Auswirkungsstufen

#	Beschreibung	Logische Schnittstelle(n)	C	I	A
5	Schnittstelle zwischen Kontrollsystemen innerhalb desselben Unternehmens	U9, U11	L	H	H
8	Schnittstelle zwischen Back-Office-Systemen, die nicht einer gemeinsamen Verwaltungsbehörde unterstehen	U15	H	M	L
9	Schnittstelle zu B2B-Verbindungen zwischen Systemen, die in der Regel Finanz- oder Markttransaktionen umfassen	U51	L	M	M
10	Schnittstelle zwischen Kontrollsystemen und Nicht-Kontroll-/Firmensystemen	U59, U106	L	H	M
14	Schnittstelle zwischen Systemen, die das AMI-Netz mit hoher Verfügbarkeit nutzen	U32, U130	H	H	H
15	Schnittstelle zwischen Systemen, die Standortnetze von Kunden (Privathaushalte, Gewerbe und Industrie) nutzen	U42, U43, U44, U45, U49, U62	L	M	M

16	Schnittstelle zwischen externen Systemen und dem Kunden-standort	U88, U92	H	M	L

Die in Tabelle 7 aufgeführten Stufen betreffen die Auswirkungen auf das landesweite Stromnetz, insbesondere im Hinblick auf die Netzstabilität und -zuverlässigkeit. Folglich sind die Auswirkungen auf die Vertraulichkeit für diese logischen Schnittstellenkategorien gering. Die logischen Schnittstellenkategorien 8, 14 und 16 haben aufgrund der Art der zu schützenden Daten (z. B. sensible Energieverbrauchsdaten von Kunden, kritische Sicherheitsparameter und Informationen von einem HAN an eine dritte Partei) eine hohe Vertraulichkeitsstufe.

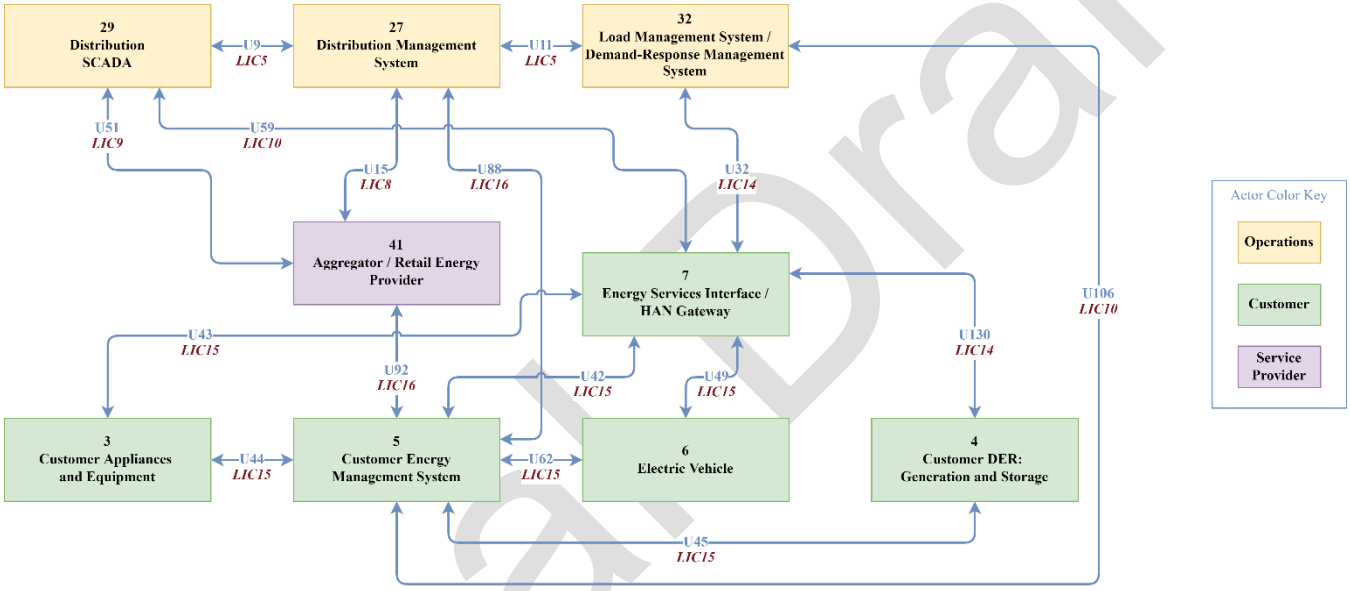

Abbildung 32: Akteure, Schnittstellen und Kategorien der drei Architekturvarianten

Abbildung 32 zeigt das Ergebnis der ersten beiden Schritte: Identifikation der möglichen Akteure sowie der logischen Schnittstellen und deren Kategorien.

Beispiel:

Distribution Management System (ID 27 im NISTIR Reference Model) in der Domäne *Operations* ist mit *Aggregator/Retail Energy Provider* (ID 41 im NISTIR Reference Modell) in der Domäne *Service Provider* über die logische Schnittstelle *U15* (Kategorie LIC8) verbunden.

Ad 3. Cyber-Security Anforderungen an die Architekturvarianten

Architekturvariante 1

Abbildung 31 zeigt die Darstellung der Verknüpfung der Akteure und Schnittstellen von Architekturvariante 1 und dem NISTIR Modell. Hierbei kann festgehalten werden, dass in Abhängigkeit des logischen Akteurs beim Verteilernetzbetreiber (entweder *27 Distribution Management System* oder *29 Distribution SCADA*) eine unterschiedliche Schnittstellenkategorie (mit unterschiedlichen Anforderungen an die Cyber-Security) eingesetzt werden kann. In dieser Architekturvariante wird angenommen, dass *5 Customer Energy Management System* durch Einzelkomponenten in der Kundendomäne ersetzt werden kann und die Anforderungen an die Cyber-Security bestehen bleiben. *Tabelle 8* enthält eine Übersicht über die verwendeten Schnittstellen und den Auswirkungsstufen für Architekturvariante 1.

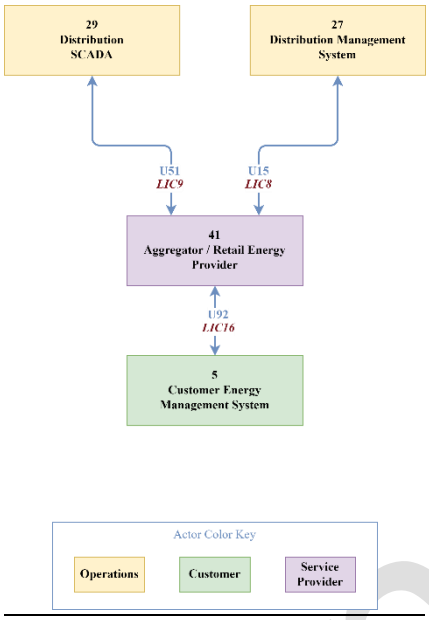

Abbildung 33: Darstellung des Architekturvariante 1.

Tabelle 8: Schnittstellen und Auswirkungsstufen für Architekturvariante 1.

#	Verbindung	Logische Schnittstelle	Kategorie	Auswirkungsstufen (C – I – A)
1	29 – 41	U51	LIC9	L – M – M
2	27 – 41	U15	LIC8	H – M – L
3	41 – 5	U92	LIC16	H – M – L

Auf Basis dieser Analyse und einer Risikobewertung konnten letztendlich die Anforderungen an die Cyber-Security abgeleitet werden. Tabelle 9, Tabelle 10 und Tabelle 11 zeigen die Ergebnisse dieser Bewertung (für GRC, CTR, UTR), jeweils einmal für ein geringes Risiko, ein mittleres Risiko sowie ein hohes Risiko. Die Risikobewertung ist eine Kombination aus der Wahrscheinlichkeit der Ausnutzung von Schwachstellen durch Bedrohungen und den Auswirkungen einer solchen Ausnutzung, einschließlich aller Unsicherheiten, die mit den Risikobestimmungen für den Betrieb der Organisation, die Vermögenswerte der Organisation oder Einzelpersonen verbunden sind. Eine Übersicht aller Anforderungen findet sich im Anhang, eine detaillierte Beschreibung dieser Anforderungen ist in (NIST National Institute of Standards and Technology, 2010) ersichtlich. Aufgrund des Platzbedarfs und der Lesbarkeit dieses Dokuments wurde auf die Darstellung aller Anforderungen und Details verzichtet.

Tabelle 9: Cyber-Security Anforderungen an die möglichen Schnittstellen von Architekturvariante 1 bei geringer Risikobewertung

#	Governance, risk, and compliance (GRC)	Common technical requirements (CTR)	Unique technical requirements (UTR)
1	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11, SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	SG.IA-6
2	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11, SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	-
3	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11, SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	-

Tabelle 10: Cyber-Security Anforderungen an die möglichen Schnittstellen von Architekturvariante 1 bei mittlerer Risikobewertung

#	Governance, risk, and compliance (GRC)	Common technical requirements (CTR)	Unique technical requirements (UTR)
1	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*,	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.AU-16, SG.IA-4, SG.SC-5, SG.SC-7, SG.SC-8, SG.SI-7

	SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*		
2	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.AU-16, SG.IA-4, SG.IA-5, SG.SC-3, SG.SC-7, SG.SC-8, SG.SI-7
3	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.AU-16, SG.IA-4, SG.SC-3, SG.SC-7, SG.SC-8, SG.SI-7

Tabelle 11: Cyber-Security Anforderungen an die möglichen Schnittstellen von Architekturvariante 1 bei hoher Risikobewertung

#	**Governance, risk, and compliance (GRC)**	**Common technical requirements (CTR)**	**Unique technical requirements (UTR)**
1	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	none
2	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-12, SG.IA-6, SG.SC-26
3	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.IA-6, SG.SC-9, SG.SC-26

Anmerkung: Der Eintrag “Alle gemeinsamen Anforderungen“ umfasst insgesamt 128 Anforderungen, die für jede Schnittstelle gelten, unabhängig von den verbundenen Akteuren und der Risikobewertung. Jene Anforderungen, die mit „*“ markiert sind unterscheiden sich in der konkreten Ausprägung von der jeweiligen Risikobewertung (siehe (NIST National Institute of Standards and Technology, 2010)).

Architekturvariante *2*

Abbildung 34 zeigt die Darstellung der Verknüpfung der Akteure und Schnittstellen von Architekturvariante 2 und dem NISTIR Modell. Hierbei kann festgehalten werden, dass in Abhängigkeit des logischen Akteurs beim Verteilernetzbetreiber (entweder *27 Distribution Management System* oder *32 Load Management System/Demand-Response Management System*) eine unterschiedliche Schnittstellenkategorie (mit unterschiedlichen Anforderungen an die Cyber-Security) eingesetzt werden kann. In dieser Architekturvariante wird angenommen, dass *5 Customer Energy Management System* durch Einzelkomponenten in der Kundendomäne ersetzt werden kann und die Anforderungen an die Cyber-Security bestehen bleiben. Tabelle 12 enthält eine Übersicht über die verwendeten Schnittstellen und den Auswirkungsstufen für Architekturvariante 2.

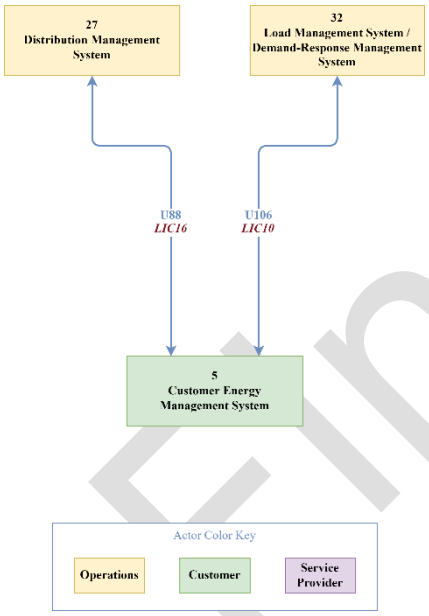

Abbildung 34: Darstellung des Architekturvariante 2

Tabelle 12: Schnittstellen und Auswirkungsstufen für Architekturvariante 2

#	Verbindung	Logische Schnittstelle	Kategorie	Auswirkungsstufen (C – I – A)
4	27 – 5	U88	LIC16	H – M – L
5	32 – 5	U106	LIC10	L – H – M

Die Tabelle 13, Tabelle 14 und Tabelle 15 zeigen die Ergebnisse dieser Bewertung (für GRC, CTR, UTR), jeweils einmal für ein geringes Risiko, ein mittleres Risiko sowie ein hohes Risiko.

Tabelle 13: Cyber-Security Anforderungen an die möglichen Schnittstellen von Architekturvariante 2 bei geringer Risikobewertung

#	Governance, risk, and compliance (GRC)	Common technical requirements (CTR)	Unique technical requirements (UTR)
4	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11, SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	-
5	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11, SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	SG.IA-6

Tabelle 14: Cyber-Security Anforderungen an die möglichen Schnittstellen von Architekturvariante 2 bei mittlerer Risikobewertung

#	Governance, risk, and compliance (GRC)	Common technical requirements (CTR)	Unique technical requirements (UTR)
4	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.AU-16, SG.IA-4, SG.SC-3, SG.SC-7, SG.SC-8, SG.SI-7
5	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.SC-5

Tabelle 15: Cyber-Security Anforderungen an die möglichen Schnittstellen von Architekturvariante 2 bei hoher Risikobewertung

#	Governance, risk, and compliance (GRC)	Common technical requirements (CTR)	Unique technical requirements (UTR)
4	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.IA-6, SG.SC-9, SG.SC-26

	10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*		
5	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.SC-7, SG.SC-8, SG.SC-29, SG.SI-7, SG.IA-4

Anmerkung: Der Eintrag “Alle gemeinsamen Anforderungen“ umfasst insgesamt 128 Anforderungen, die für jede Schnittstelle gelten, unabhängig von den verbundenen Akteuren und der Risikobewertung. Jene Anforderungen, die mit „*“ markiert sind unterscheiden sich in der konkreten Ausprägung von der jeweiligen Risikobewertung (siehe (NIST National Institute of Standards and Technology, 2010)).

Architekturvariante 3

Abbildung 35 zeigt die Darstellung der Verknüpfung der Akteure und Schnittstellen von Architekturvariante 3 und dem NISTIR Modell. Hierbei kann festgehalten werden, dass in Abhängigkeit des logischen Akteurs beim Verteilernetzbetreiber (entweder *27 Distribution Management System* oder *32 Load Management System/Demand-Response Management System*) eine unterschiedliche Schnittstellenkategorie (mit unterschiedlichen Anforderungen an die Cyber-Security) eingesetzt werden kann. In dieser Architekturvariante wird angenommen, dass *7 Energy Service Interface / HAN Gateway* den Funktionsblock darstellt und die Einzelgeräte oder das Energy Management System in der Kundedomäne über unterschiedliche Schnittstellen mit dem Funktionsblock verbunden sind. Tabelle 16 enthält eine Übersicht über die verwendeten Schnittstellen und den Auswirkungsstufen für Architekturvariante 3.

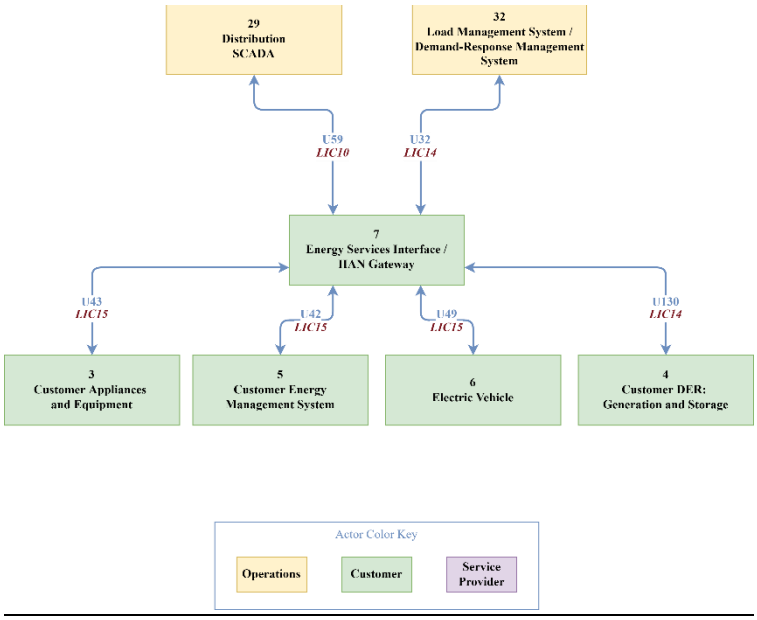

Abbildung 35: Darstellung des Architekturvariante 3.

Tabelle 16: Schnittstellen und Auswirkungsstufen für Architekturvariante 2.

#	Verbindung	Logische Schnittstelle	Kategorie	Auswirkungsstufen (C – I – A)
6	29 – 7	U59	LIC10	L – H – M
7	32 – 7	U32	LIC14	H – H – H
8	7 – 3	U43	LIC15	L – M – M
9	7 – 5	U42	LIC15	L – M – M
10	7 – 6	U49	LIC15	L – M – M
11	7 – 4	U130	LIC14	H – H – H

Die Tabelle 17, Tabelle 18 und Tabelle 19 zeigen die Ergebnisse dieser Bewertung (für GRC, CTR, UTR), jeweils einmal für ein geringes Risiko, ein mittleres Risiko sowie ein hohes Risiko.

Tabelle 17: Cyber-Security Anforderungen an die möglichen Schnittstellen von Architekturvariante 3 bei geringer *Risikobewertung*

#	Governance, risk, and compliance (GRC)	Common technical requirements (CTR)	Unique technical requirements (UTR)
6	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11, SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	SG.IA-6
7	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11,	-

		SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	
8	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11, SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	SG.IA-6
9	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11, SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	SG.IA-6
10	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11, SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	SG.IA-6
11	Alle gemeinsamen Anforderungen	SG.AC-8, SG.AC-9, SG.AC-16, SG.AU-3, SG.AC-4, SG.AU-15, SG.CM-7, SG.CM-8, SG.SA-11, SG.SC-12, SG.SC-15, SG.SC-18, SG.SC-19, SG.SC-20, SG.SC-21, SG.SI-9	-

Tabelle 18: Cyber-Security Anforderungen an die möglichen Schnittstellen von Architekturvariante 3 bei mittlerer Risikobewertung

#	Governance, risk, and compliance (GRC)	Common technical requirements (CTR)	Unique technical requirements (UTR)
6	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.SC-5
7	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	-
8	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.IA-4, SG.SC-3, SG.SC-5, SG.SC-7, SG.SC-8, SG.SI-7

	10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*		
9	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.IA-4, SG.SC-3, SG.SC-5, SG.SC-7, SG.SC-8, SG.SI-7
10	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.IA-4, SG.SC-3, SG.SC-5, SG.SC-7, SG.SC-8, SG.SI-7
11	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	-

Tabelle 19: Cyber-Security Anforderungen an die möglichen Schnittstellen von Architekturvariante 3 bei hoher Risikobewertung

#	**Governance, risk, and compliance (GRC)**	**Common technical requirements (CTR)**	**Unique technical requirements (UTR)**
6	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.SC-7, SG.SC-8, SG.SC-29, SG.SI-7, SG.IA-4
7	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.AU-16, SG.IA-4, SG.IA-6, SG.SC-3, SG.SC-5, SG.SC-6, SG.SC-7, SG.SC-8, SG.SC-9, SG.IA-26, SG.IA-29, SG.SI-7
8	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6,	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	-

	SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*		
9	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	-
10	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	-
11	Alle gemeinsamen Anforderungen, SG.CM-3, SG.CM-5, SG.CP-5, SG.MP-3, SG.SI-6, SG.AC-18*, SG.AU-5*, SG.AU-8*, SG.CP-7*, SG.CP-8*, SG.CP-9*, SG.CP-10*, SG.IR-10*, SG.MA-3*, SG.MA-6*, SG.PE-3*, SG.PE-5*, SG.PE-9*, SG.PE-12*, SG.RA-6*	SG.AC-6, SG.AC-7, SG.AC-17*, SG.SC-11*, SG.SC-16, SG.SC-22, SG.AC-30, SG.SI-8	SG.AC-14, SG.AU-16, SG.IA-4, SG.IA-6, SG.SC-3, SG.SC-5, SG.SC-6, SG.SC-7, SG.SC-8, SG.SC-9, SG.IA-26, SG.IA-29, SG.SI-7

J.5.8 SGAM-Modellierung der Architekturvarianten

Die Smart Grid Coordination Group/Reference Architecture Working Group entwickelte das Smart Grid Architecture Model (SGAM) (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012), um einen umfassenden Überblick über die gesamte Smart Grid (SG)-Architektur als Antwort auf das Normungsmandat M/4901 der Europäischen Kommission (EC) zu geben. Es ist ein Referenzmodell für die Analyse und Visualisierung von Smart-Grid-Anwendungsfällen, die technologieunabhängig sind. Es bietet einen methodischen Ansatz für den Umgang mit der Komplexität von Smart Grids und die Möglichkeit, mehrere SG-Lösungsmethoden zu vergleichen, um Unterschiede und Konvergenzen zwischen verschiedenen Paradigmen, Fahrplänen und Sichtweisen zu entdecken.

Durch die Berücksichtigung der Prinzipien Universalität, Lokalisierung, Konsistenz, Zuverlässigkeit und Interoperabilität bietet es außerdem eine systematische Methode zur Bewältigung der Komplexität von

Smart Grids, die eine Reflexion sowohl über den aktuellen Stand der Implementierung des Stromnetzes als auch über die Entwicklung potenzieller Smart-Grid-Szenarien ermöglicht.

Der Informationsaustausch zwischen verschiedenen Einheiten innerhalb der Smart-Energy-Branche kann mithilfe des SGAM modelliert werden, einem dreidimensionalen architektonischen Rahmen der aus Domains, Zonen und Layer besteht. Die Domains definieren fünf verschiedene Aspekte des intelligenten Stromnetzes, die sechs Zonen stellen die Verwaltungshierarchie des intelligenten Stromnetzes dar, während die (Interoperabilitäts-) Layer fünf verschiedene Gesichtspunkte des Informationsaustauschs und der Interoperabilität darstellen.

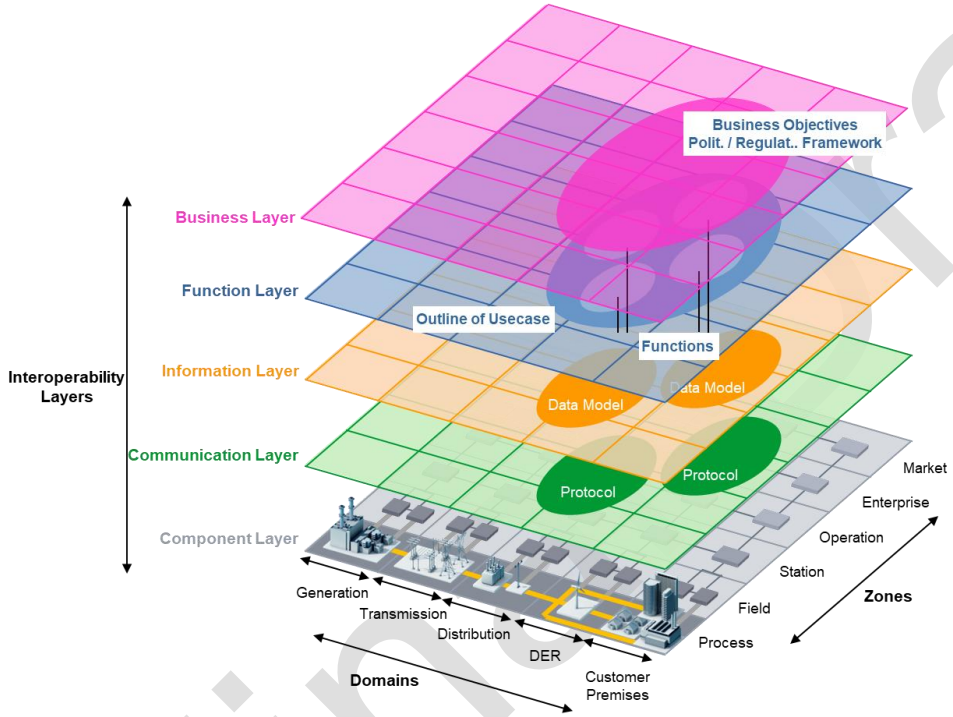

Abbildung 36: Das Smart Grid Architecture Model (SGAM) Framework

SGAM ist aufgrund seiner zahlreichen Vorteile ein beliebtes Werkzeug für die Modellierung von Smart-Grid-Anwendungsdesign und zur detaillierten Architekturdarstellung. Aus diesem Grund wird SGAM auch hier verwendet, um die High-Level-Modellierung und das Architekturdesign für die drei Architekturvarianten zu beschreiben. Dies ist zum einen für eine technologieneutrale Dokumentation nützlich und zum anderen erleichtert der harmonisierte Ansatz den Vergleich der vorgeschlagenen Architekturvarianten.

Die Modellierung wird im Folgenden zusammen mit einer zusammenfassenden Beschreibung in den einzelnen Unterabschnitten für die drei betrachteten Architekturvarianten dargestellt. Es ist zu beachten,

dass in dieser Studie nur die beiden Interoperabilitätsschichten (Funktions- und Informationsebene) modelliert werden und die Geschäfts-, Kommunikations- und Komponentenebene unberücksichtigt bleiben, da sie in der ersten Phase dieser Studie nicht berücksichtigt wurden. Bei der Modellierung der Informationsebene werden jedoch auch einige Aspekte der Komponentenebene unter architektonischen Gesichtspunkten behandelt.

Architekturvariante 1

In diesem Unterabschnitt wird das SGAM-Modell für die in Abbildung 30 dargestellte Architekturvariante 1 beschrieben. In dieser Architekturvariante wird der VNB von einem Aggregator bei der Aktivierung der Flexibilität im Kundenbereich unterstützt. In diesem Fall koordiniert der Aggregator sowohl mit dem VNB als auch mit dem Kunden die Erfassung der Messungen und die Aktivierung der Flexibilität. Im Folgenden werden die drei SGAM-Ebenen für diese Architekturvariante vorgestellt.

Der „SGAM Function Layer“

Der Function Layer in SGAM beschreibt die Anwendungsfälle, Funktionen und Dienste, die für die Realisierung der geplanten Geschäftsfälle erforderlich sind. Abbildung 37 zeigt den modellierten Function Layer für die erste Architekturvariante.

Im Modell ist zu erkennen, dass diese Architekturvariante die Domains Distribution, DER und Customer Premises abdeckt, während vier Zonen Process, Field, Operation und die Kombination von Enterprise/Market, im Kontext stehen. Darüber hinaus identifiziert das Modell vier High-Level-Funktionen oder primäre Anwendungsfälle (Primary Use Case, PUC), wie sie in der SGAM-Terminologie genannt werden, die für die Realisierung dieser Architekturvariante identifiziert wurden.

Wie aus dem nachstehenden Modell ersichtlich ist, gibt es vier Hauptfunktionen und primäre Anwendungsfälle. Die Aggregationsfunktion wird vom Aggregator ausgeführt, bei dem es sich um den Gerätehersteller oder eine andere dritte juristische Person handeln kann. Die Überwachungs- und Flexibilitätsaktivierungsanforderungsfunktion (“Monitoring and Flexibility Activation”) wird vom VNB ausgeführt, der eine Flexibilitätsaktivierungsanforderung sendet, sobald ein roter Netzzustand festgestellt wird. Bei den letzten beiden Funktionen geht es um die Erfassung der Messungen („Data Acquisition“) und die Erleichterung der Flexibilitätsaktivierung („Flexibility Activation“) durch die Kundengeräte. Nachfolgend wird jede dieser Funktionen mit Hilfe von entsprechenden UML-Diagrammen beschrieben.

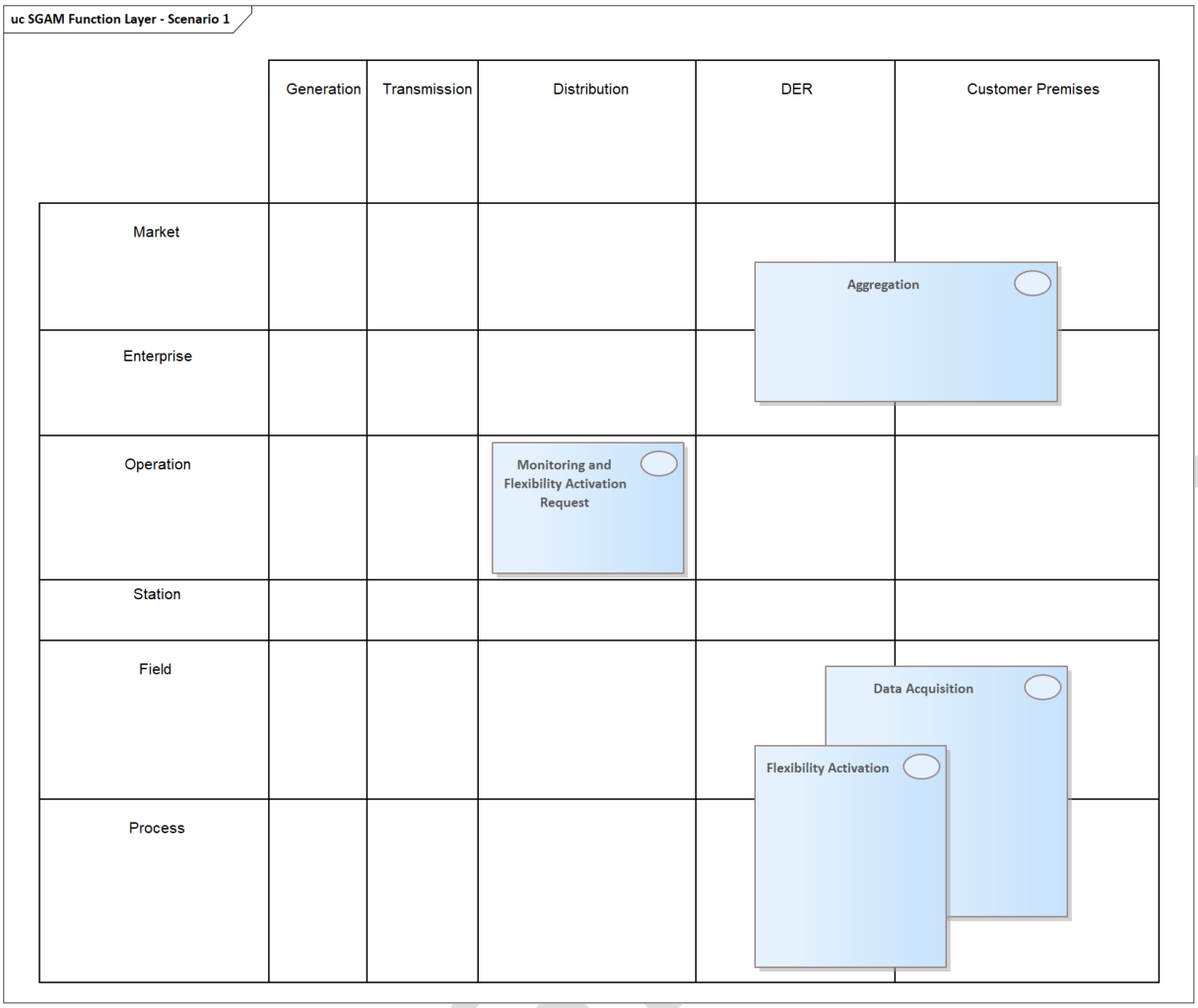

Abbildung 37: Architekturvariante 1, SGAM Function Layer

Die “Monitoring and Flexibility Activation” Funktion

Diese Funktion betrifft die VNB-Funktionalität, die mit der kontinuierlichen Überwachung des Netzzustands, z. B. mit Hilfe von SCADA oder einem DMS usw., beauftragt ist und eine Flexibilitätsaktivierungsanforderung an einen Aggregator sendet, sobald ein roter Zustand im Netz festgestellt wird. Der VNB interagiert in diesem Fall nicht direkt mit dem Kunden, sondern nutzt einen Aggregator als Vermittler, so dass keine direkte Schnittstelle zwischen VNB und Kunde implementiert werden muss. Abbildung 38 zeigt das Modell für diesen primären Anwendungsfall. Die Interaktion zwischen den Akteuren wird in einem Sequenzdiagramm dargestellt, wie in Abbildung 39 zu sehen ist. Eine weitere Ansicht der Funktion ist in Abbildung 40 mit einem Aktivitätsdiagramm dargestellt, das die wichtigsten Schritte in dieser Funktion hervorhebt.

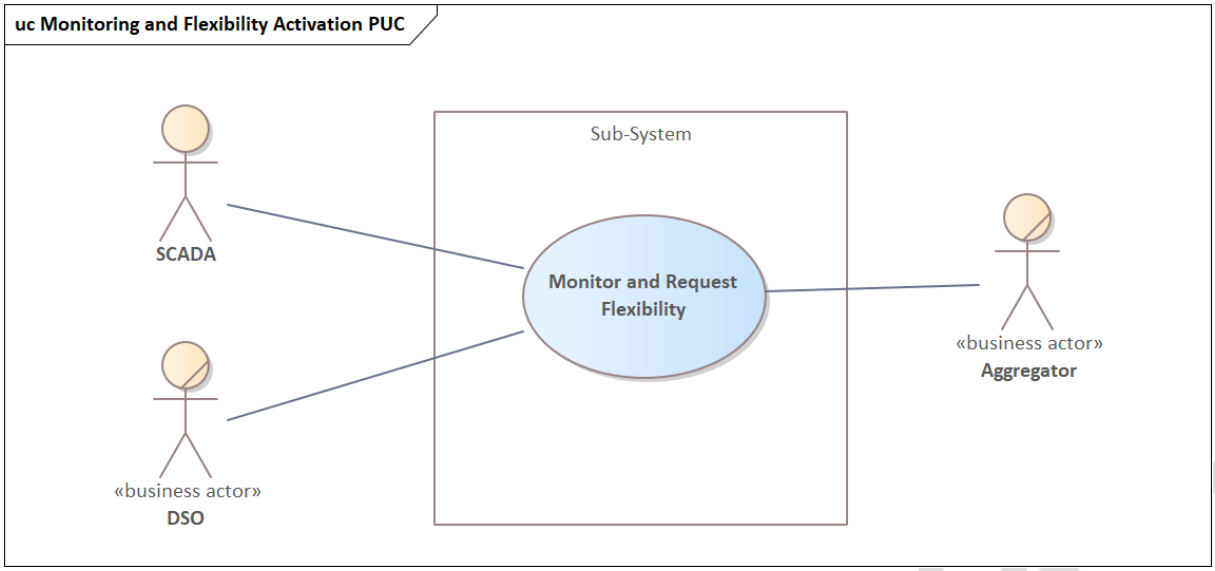

Abbildung 38: PUC Modell für die „Monitoring und Flexibility Activation“ Funktion.

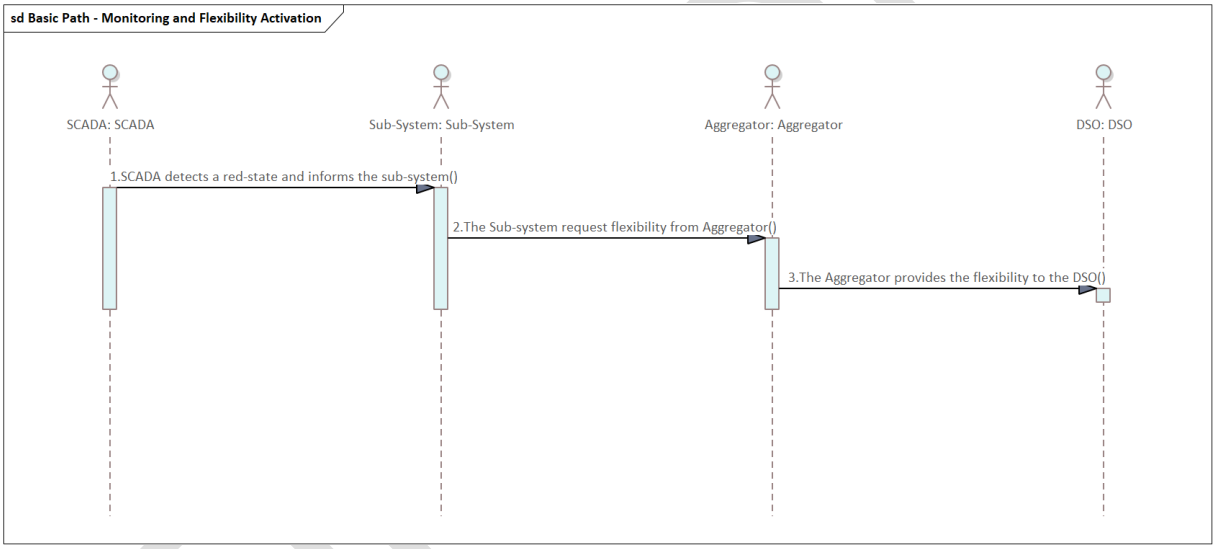

Abbildung 39: Sequenzdiagram für die Interaktionen der involvierten Akteure in der "Monitoring and Flexibility Activation" Funktion.

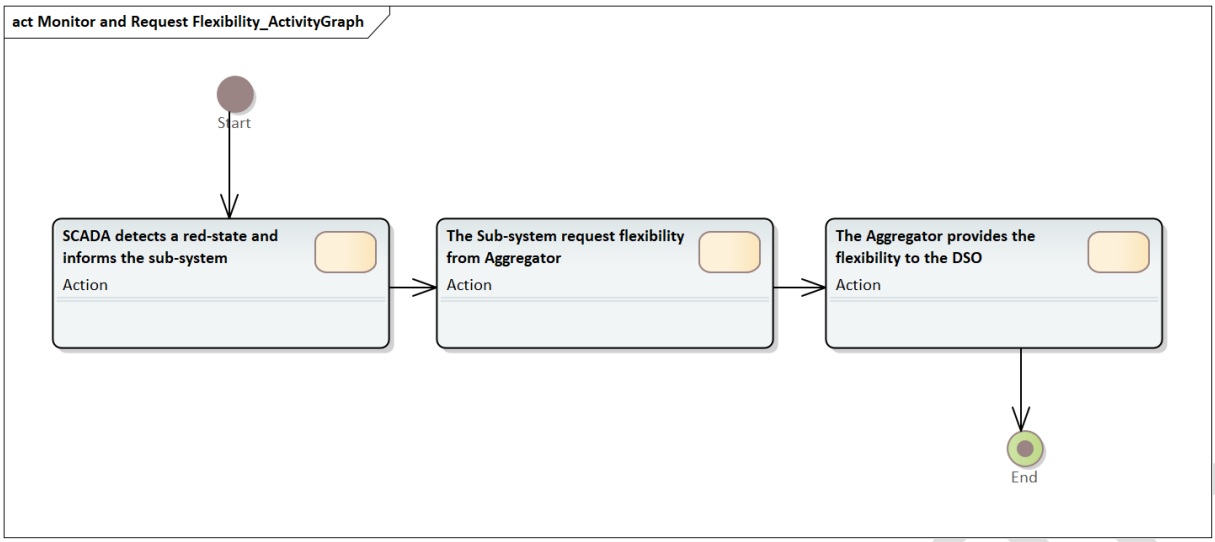

Abbildung 40: Aktivitätsdiagramm zur Beschreibung der Schritte in der "Monitoring and Flexibility Activation" Funktion.

Die „Aggregation“ Funktion

Diese Funktion ist vom Aggregator zu übernehmen. Sie soll die Koordinierung zwischen dem Kunden und dem VNB für die Flexibilitätsaktivierung, die Erfassung der Messungen der Kundenlasten und die Übermittlung der Sollwerte für die Kundenlasten übernehmen. Die nachfolgenden Abbildungen beschreiben die Aggregationsfunktion genauer.

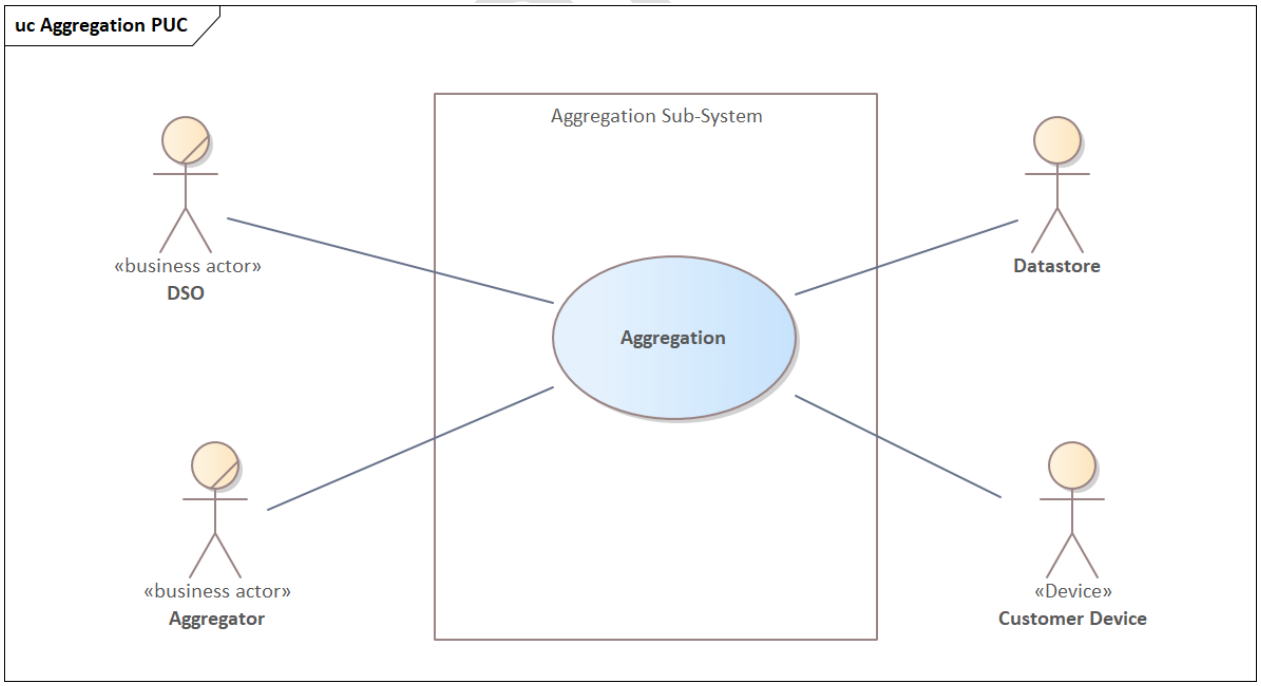

Abbildung 41: PUC-Modell für die „Aggregation“ Funktion

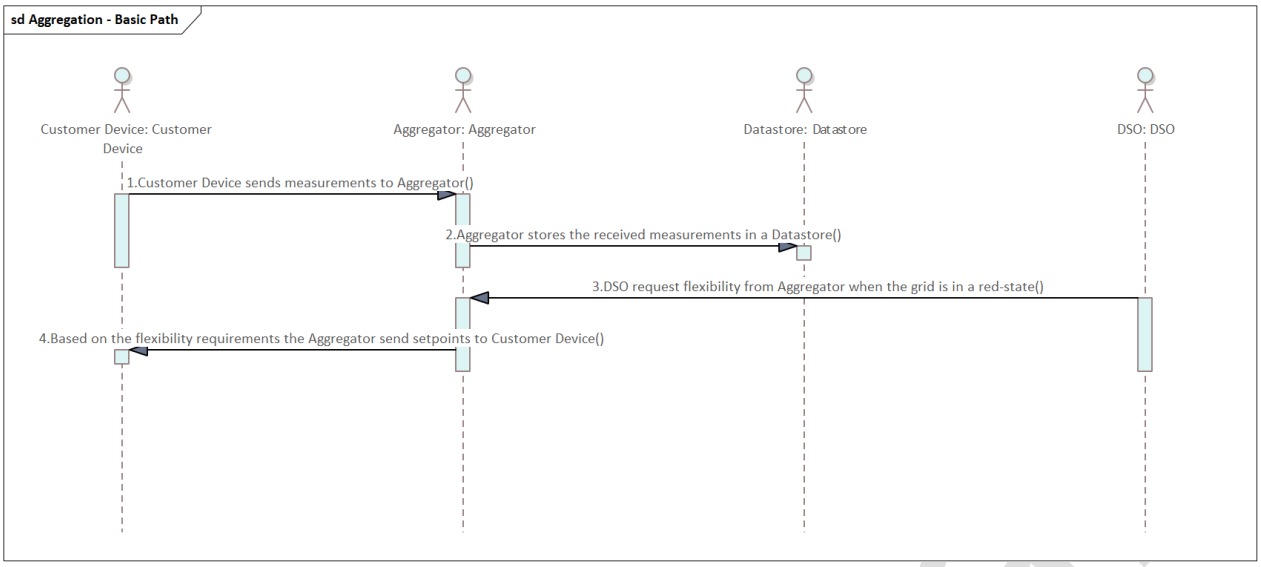

Abbildung 42: Sequenzdiagram für die Interaktionen der involvierten Akteure in der „Aggregation“ Funktion.

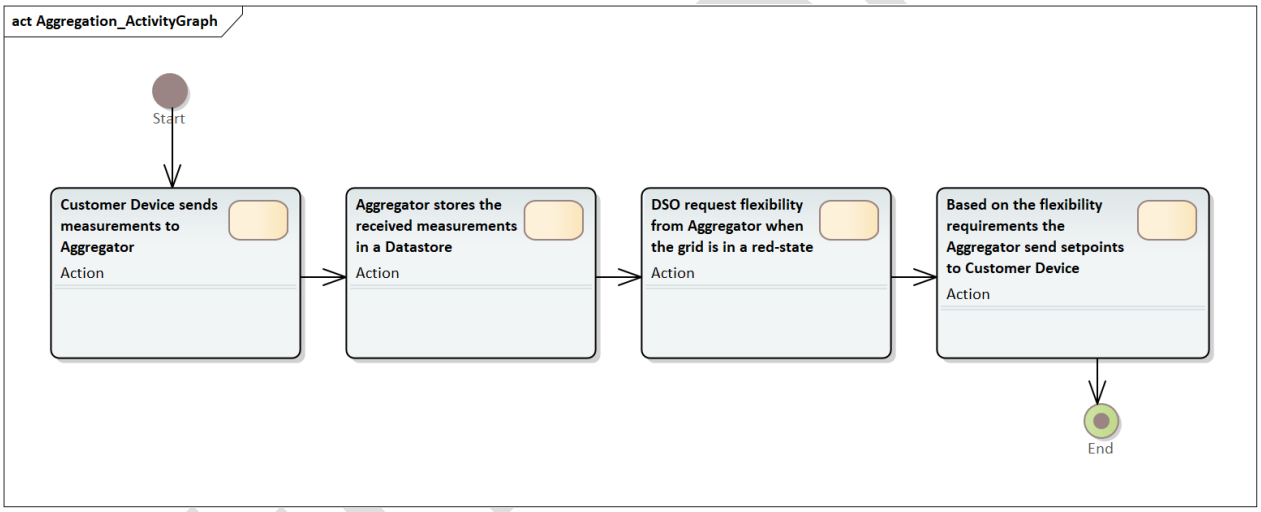

Abbildung 43: Aktivitätsdiagramm zur Beschreibung der Schritte in der „Aggregation“ Funktion

Die „Flexibility Activation“ Funktion

In dieser Architekturvariante muss diese Funktion vom Aggregator bereitgestellt und umgesetzt werden. Sobald der Aggregator eine Flexibilitätsaktivierungsanforderung vom VNB erhält, um das Netz im roten Bereich zu unterstützen, sendet der Aggregator Sollwerte an das Kundengerät. Nach Erhalt dieser Sollwerte ändert das Kundengerät sein Verhalten entsprechend. Als optionale Funktion bestätigt das Kundengerät dem Aggregator die Änderung seines Verhaltens. Diese zusätzliche Funktion ist nicht unbedingt erforderlich, da der Aggregator erkennen kann, wann das Gerät die Sollwerte übernommen hat. Für diese Funktion wird in Abbildung 44 ein Anwendungsfallmodell dargestellt, während die Interaktion

zwischen den Aktionen in Abbildung 45 mit einem Sequenzdiagramm gezeigt wird. In Abbildung 46 wird der Schritt zur Erfüllung der Funktionalität in dieser Funktion mit einem UML-Aktivitätsdiagramm skizziert.

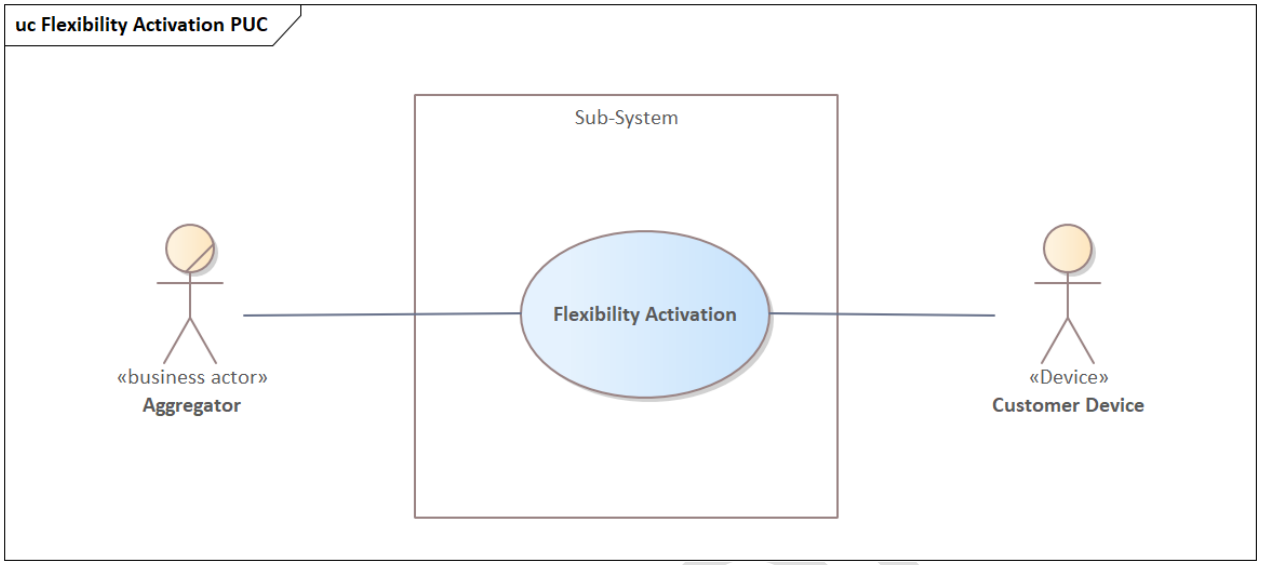

Abbildung 44: PUC Modell für die „Flexibility Activation“ Funktion.

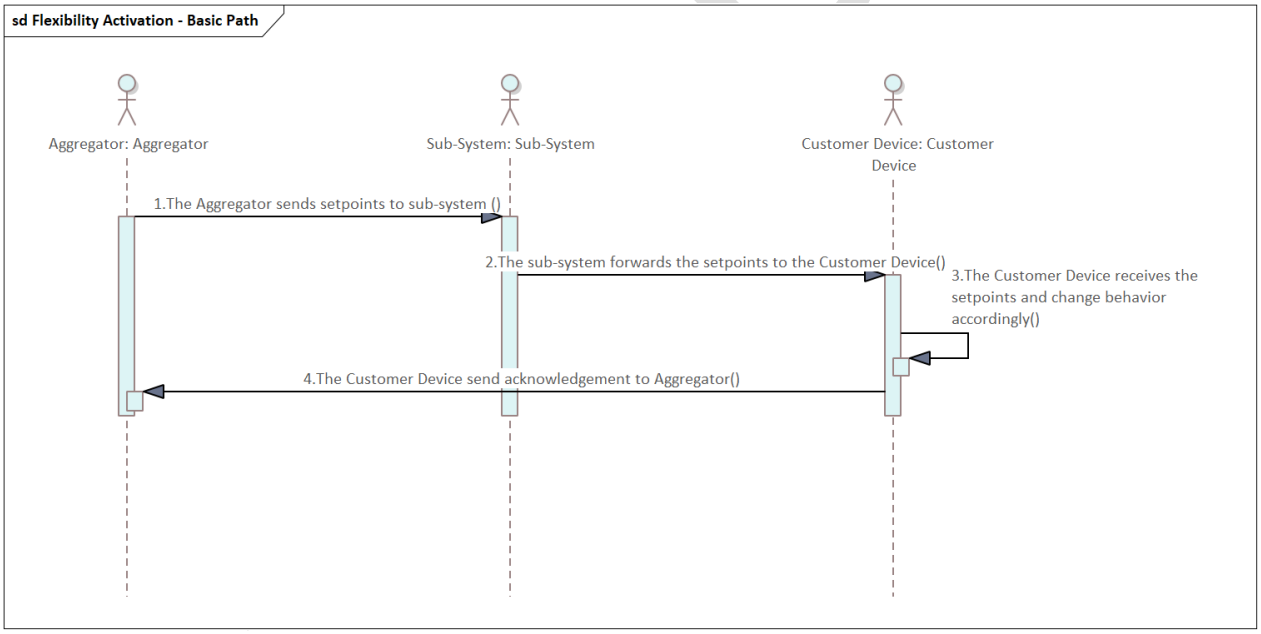

Abbildung 45: Sequenzdiagram für die Interaktionen der involvierten Akteure in der „Flexibility Activation“ Funktion.

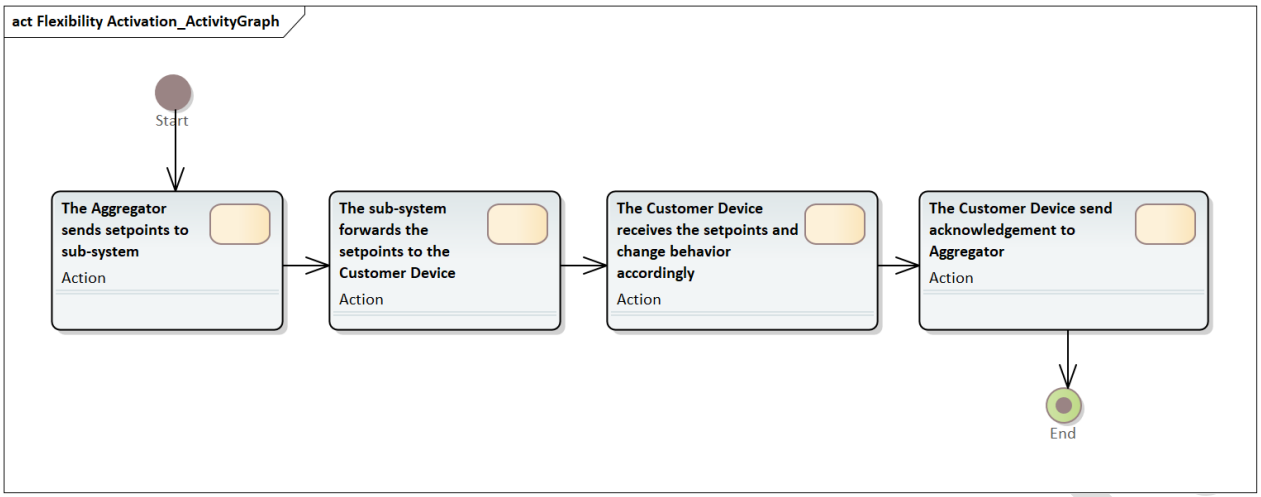

Abbildung 46: Aktivitätsdiagramm zur Beschreibung der Schritte in der "Flexibility Activation" Funktion.

Die „Data Acquistion“ Funktion

Diese Funktion erfordert die Übertragung der Messwerte von allen Kundengeräten wie EMS, PV, EV usw. an den Aggregator. Der Aggregator kann diese Daten dann für die Aggregationsfunktion verwenden und dem VNB Flexibilität bieten. Abbildung 47 zeigt einen Überblick über diese Funktion mit einem Anwendungsfallmodell. Einige weitere Details dieser Funktion werden mit einem Sequenzdiagramm in Abbildung 48 und einem Aktivitätsdiagramm in Abbildung 49 dargestellt. Diese Diagramme zeigen die Interaktion bzw. die Schritte.

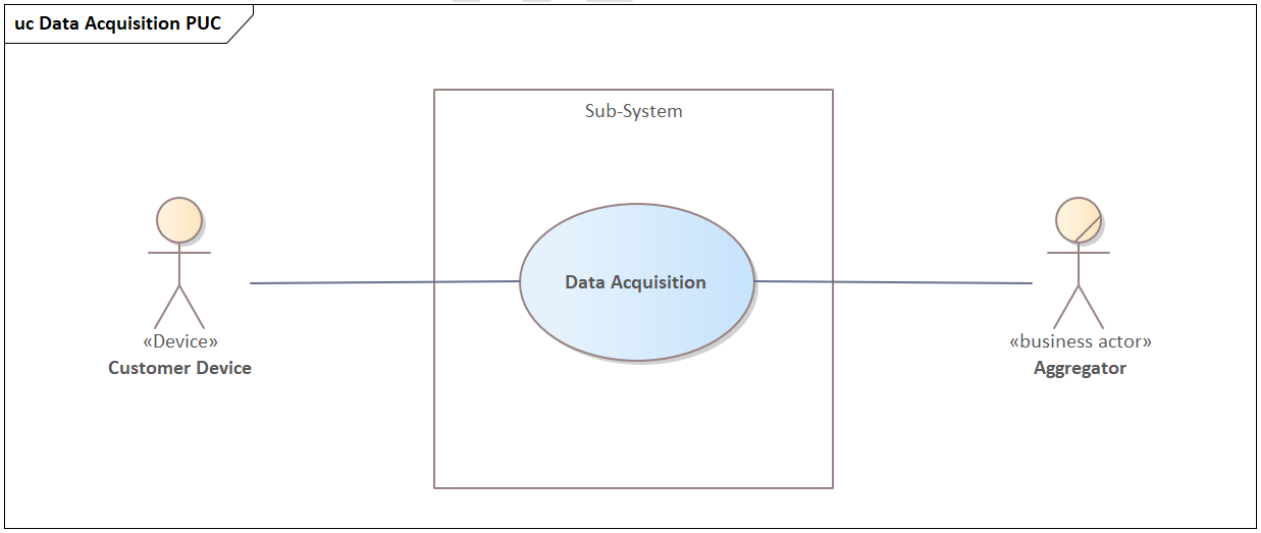

Abbildung 47: PUC Modell für die „Data Acquisition“ Funktion.

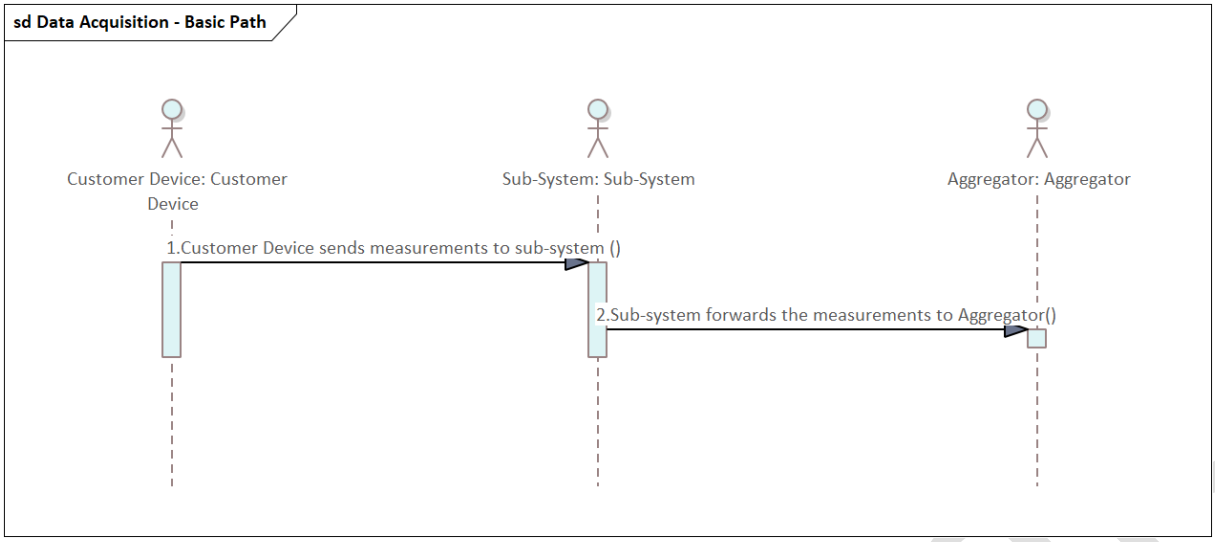

Abbildung 48: Sequenzdiagram für die Interaktionen der involvierten Akteure in der „Data Acquisition“ Funktion.

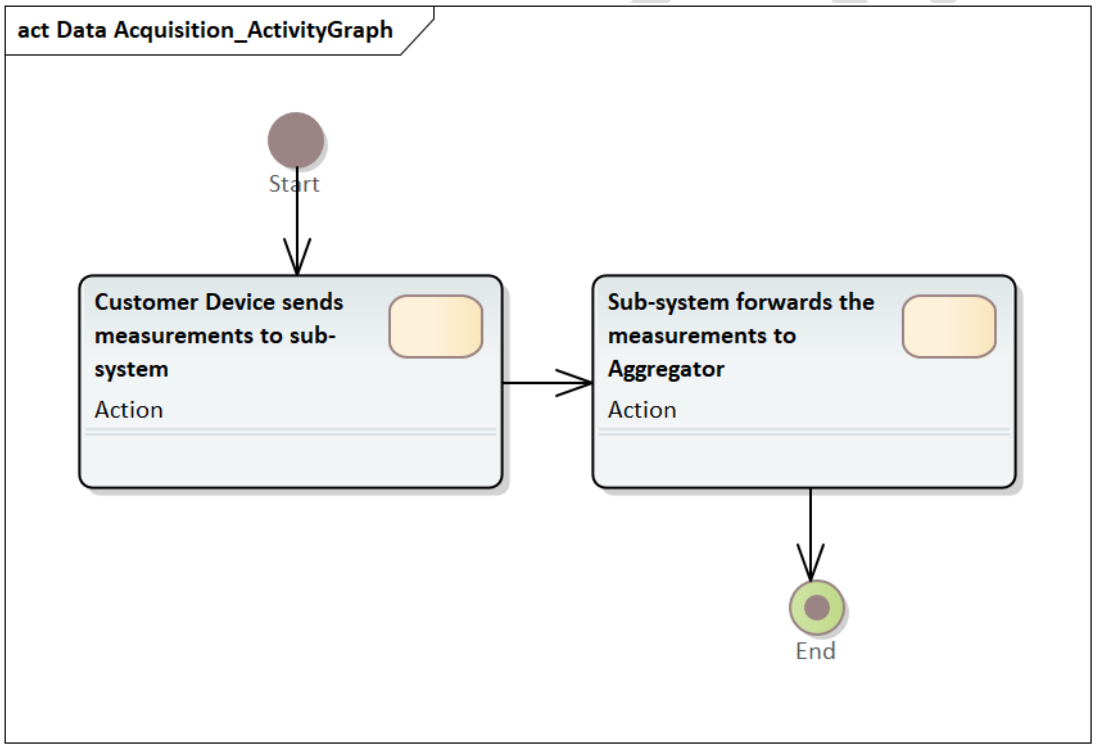

Abbildung 49: Aktivitätsdiagramm zur Beschreibung der Schritte in der "Data Acquisition" Funktion.

Der „SGAM Information Layer“

Die SGAM-Information Layer ist für die Modellierung des Informationsaustauschs zwischen verschiedenen Funktionen, Diensten und Akteuren vorgesehen. Da diese Architekturvariante in zwei weiteren Varianten realisiert werden kann, wurde für jede Variante eine Informationsschicht modelliert.

Die erste Variante ist in Abbildung 50 modelliert. In dieser Variante interagiert der Aggregator nicht mit dem einzelnen Kundengerät, sondern spricht stattdessen nur mit dem EMS des Kunden. In diesem Fall hat der Aggregator nur eine aktive Verbindung für alle Kundengeräte. Diese Variante setzt jedoch voraus, dass der Kunde ein EMS installiert hat, das den Zugang zu anderen Kundengeräten ermöglicht. In einigen Fällen wäre diese Variante besser skalierbar, da die Schnittstelle zu den Kundengeräten vom EMS des Kunden verwaltet wird.

Tabelle 20 fasst den Informationsaustausch in Variante 1 zwischen verschiedenen Akteuren an ihren spezifischen Schnittstellen zusammen. Daraus lässt sich ableiten, dass mehr Akteure und Informationsaustausche beteiligt sind als bei Variante 2.

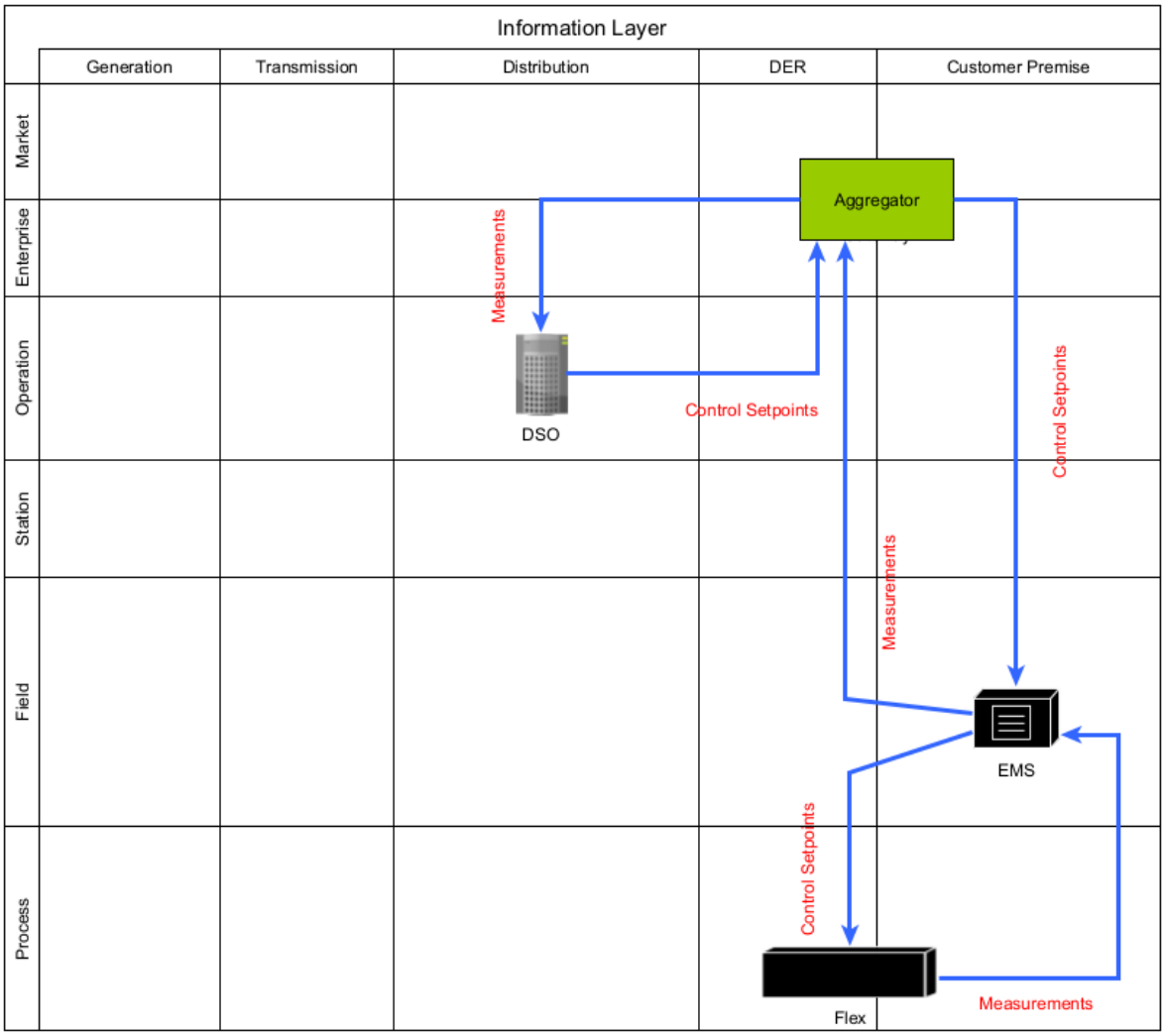

Abbildung 50: "SGAM Information Layer" der Variante 1 mit EMS im Kundenbereich.

Tabelle 20: Informationsaustausch in der Variante 1.

ID	Source Interface	Sink Interface	Information exchange
1	DSO	Aggregator	Flexibility activation request with control setpoints and network location
2	Aggregator	DSO	Measurements and aggregated available flexibilities
3	Aggregator	EMS	Control setpoints for flexibility activation
4	EMS	Aggregator	(Aggregated) Measurements and available flexibilities

5	EMS	Customer Device (Flex)	Control setpoints for flexibility activation
6	Customer Device (Flex)	EMS	Measurement and available flexibility

Die zweite Implementierungsvariante ist in Abbildung 51 dargestellt. Bei dieser Variante wird kein EMS beim Kunden benötigt. Vielmehr hat der Aggregator in diesem Fall eine eigene Schnittstelle zu jedem der Kundengeräte direkt. Das bedeutet, dass es eine Anzahl von n Verbindungen vom Aggregator zu n Kundengeräten gibt. Diese Variante ist daher mit einem höheren Verwaltungs- und Kontrollaufwand für den Aggregator verbunden, kann aber in einigen Fällen (Ad-hoc-Lösung, geringe Investitionen, geringe Anzahl von Geräten usw.) eine gute Wahl sein.

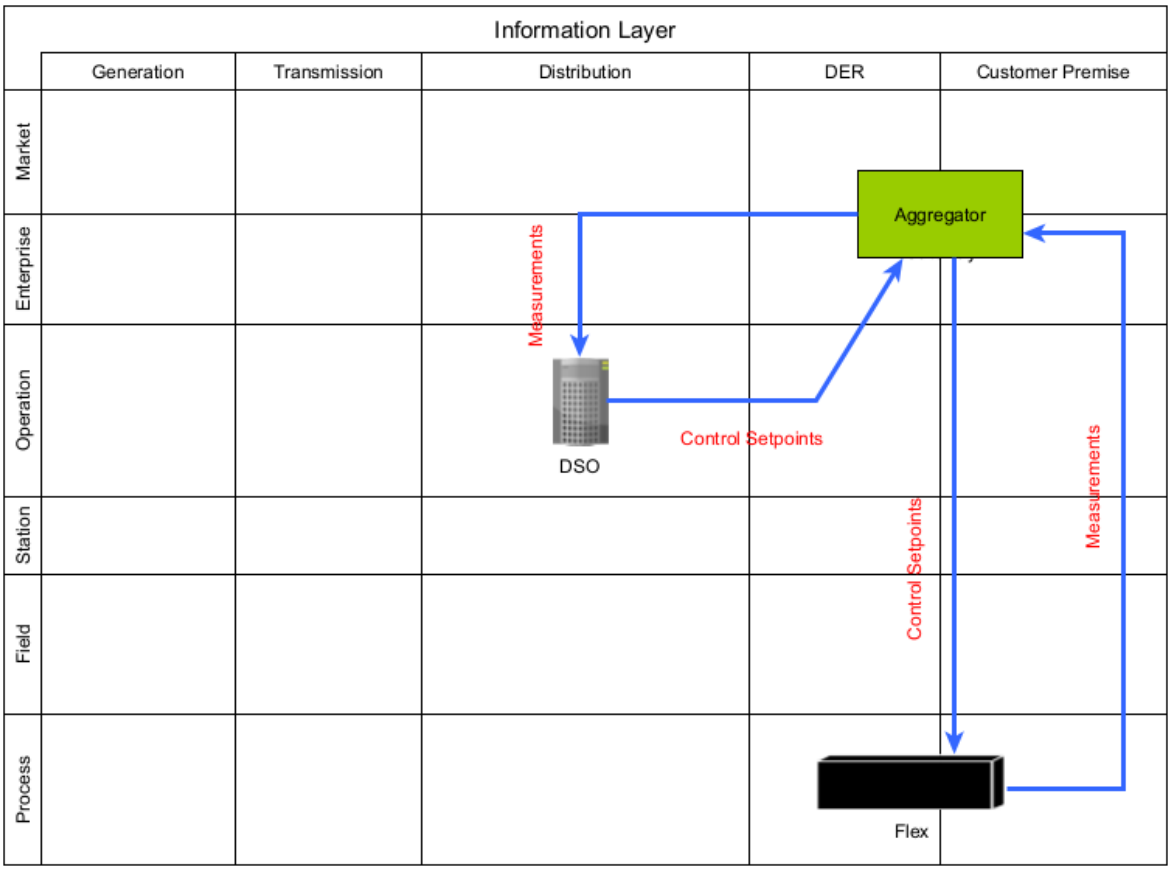

Abbildung 51: "SGAM Information Layer" der Variante 2 ohne EMS im Endkundenbereich.

Tabelle 21: Informationsaustausch in der Variante 2.

ID	Source Interface	Sink Interface	Information exchange
1	DSO	Aggregator	Flexibility activation request with control setpoints and network location
2	Aggregator	DSO	Measurements and aggregated available flexibilities
3	Aggregator	Customer Device (Flex)	Control setpoints for flexibility activation
4	Customer Device (Flex)	Aggregator	Measurement and available flexibility

Architekturvariante 2

In diesem Architekturvariante wird die Möglichkeit der direkten Interaktion zwischen dem VNB und dem Kunden untersucht. In diesem Fall werden alle wichtigen Funktionen und Dienste vom VNB betrieben. In diesem Fall wird keine zusätzliche Hardware installiert, und der Kunde nimmt an dem Prozess teil, indem er direkt über seine Kundengeräte oder über den intelligenten Zähler des VNB Zugang erhält. Dieser Unterabschnitt beschreibt einige der SGAM-Interoperabilitätsschichten, die für diese Architekturvariante modelliert wurden. Ein Überblick über diese Architekturvariante ist Abbildung 30 dargestellt.

Der „SGAM Function Layer“

Der „SGAM Function Layer“ wird, wie bereits erwähnt, zur Modellierung der Funktionen, Dienste und Anwendungsfälle verwendet, die für die Verwirklichung der geplanten Ziele erforderlich sind. Das Modell ist in Abbildung 52 auf der nachfolgenden Seite dargestellt.

Es gibt drei Hauptfunktionen, Dienste und primäre Anwendungsfälle (Primary Use Cases, PUC) für die Erreichung der geplanten Ziele. Die Überwachungs- und Flexibilitätsaktivierungsfunktion („Monitoring and Flexibility Activation“) sendet die Flexibilitätsanforderungen, wenn ein roter Netzzustand erkannt wird, die Flexibilitätsaktivierung („Flexibility Activation“) kümmert sich um die Aktivierung der Flexibilität, während die Datenerfassungsfunktion („Data Acquisition“) die Sammlung von Messungen für die verschiedenen Kundengeräte übernimmt. Nachfolgend wird jede der Funktionen mit Hilfe entsprechender UML-Diagramme näher erläutert.

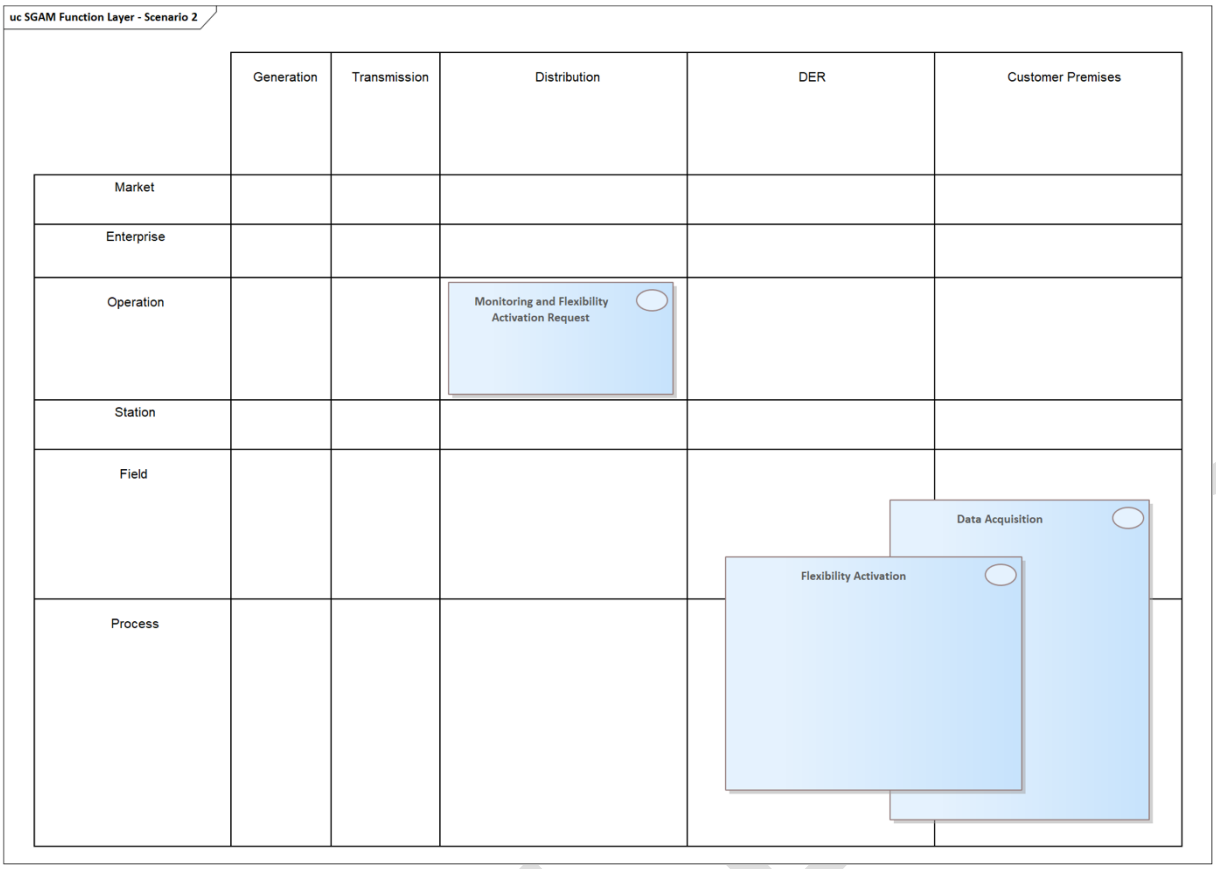

Abbildung 52: Architekturvariante 2, SGAM Function Layer

Die Funktionsschicht für diese Architekturvariante ist in Abbildung 52 dargestellt. Es wurden drei Funktionen identifiziert. Auf einer höheren Ebene sind einige dieser Funktionen der für Architekturvariante 1 identifizierten sehr ähnlich, unterscheiden sich jedoch in den Details. Im Folgenden wird eine kurze Beschreibung der einzelnen Funktionen mit Hilfe einiger UML-Modelle gegeben.

Die “Monitoring and Flexibility Activation” Funktion

Die „Monitoring and Flexibility Activation“ Funktion hat die Aufgabe, das Netz über SCADA/DMS zu überwachen, um jeden roten Zustand im Netz zu erkennen. Sobald ein solcher Zustand erkannt wird, beginnt der VNB mit der Aktivierung der Flexibilität, indem er Sollwerte direkt an die Kundengeräte sendet. Die Kundengeräte ändern daraufhin ihr Verhalten entsprechend und stellen dem Netz so die benötigte/verfügbare Flexibilität zur Verfügung, um es aus dem roten Netzzustand zu befreien. Die Hauptakteure, die an der Realisierung dieser Funktion beteiligt sind, sind der VNB, SCADA und das Kundengerät. Ein Überblick über das Anwendungsfallmodell ist in Abbildung 53 dargestellt. Darüber hinaus sind in Abbildung 54 und Abbildung 55 ein Sequenzdiagramm und ein Aktivitätsdiagramm dargestellt, die das Zusammenspiel bzw. die Abfolge der Schritte bei der Ausführung dieser Funktion zeigen.

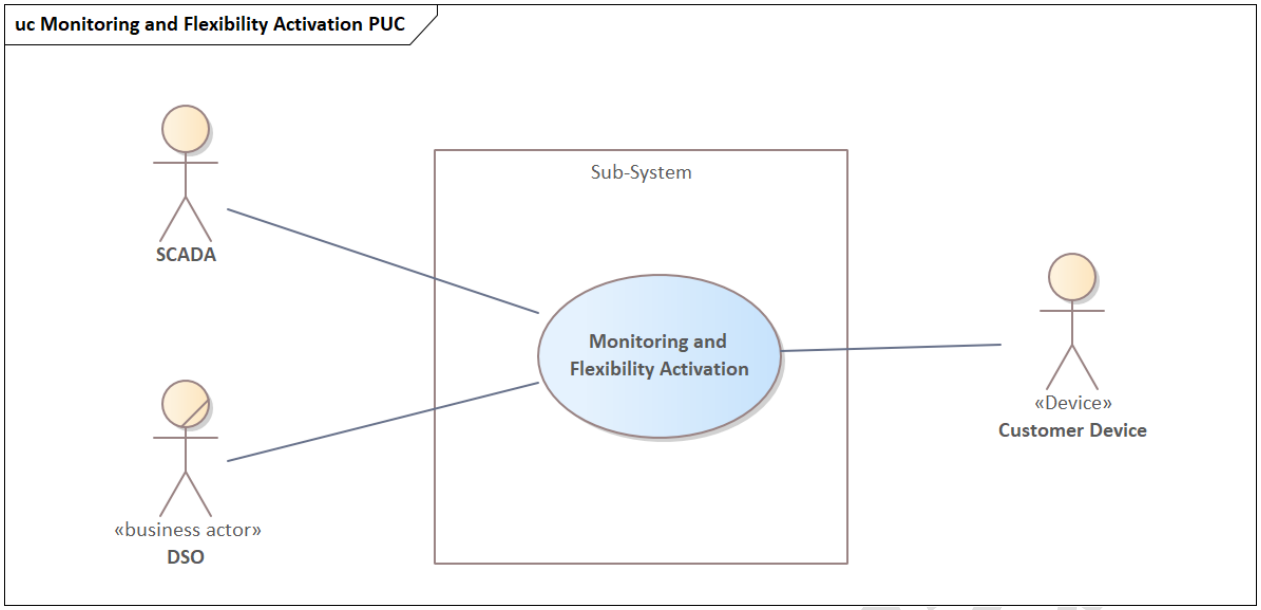

Abbildung 53: PUC Modell für die „Monitoring and Flexibility Activation“ Funktion.

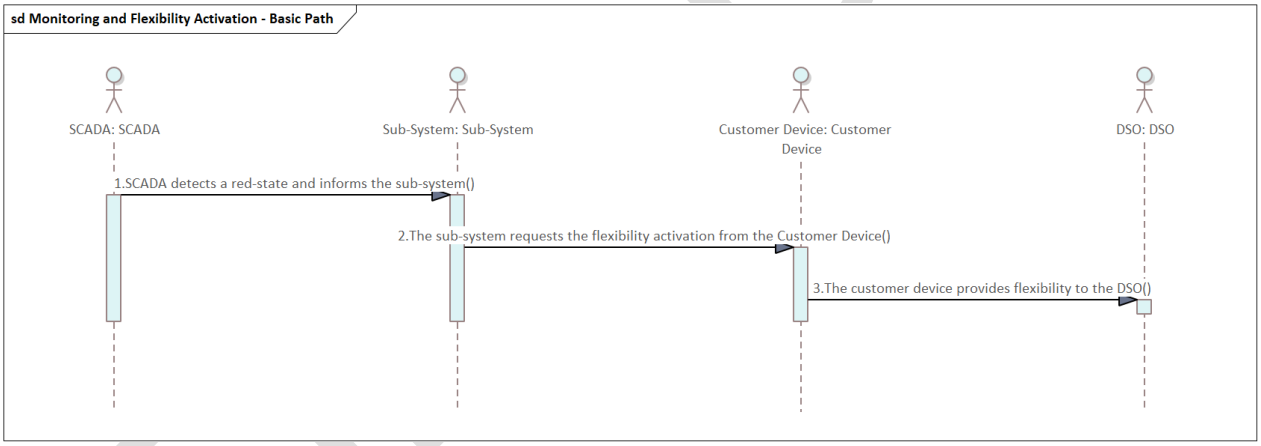

Abbildung 54: Sequenzdiagram für die Interaktionen der involvierten Akteure in der „Monitoring and Flexibility Activation“ Funktion.

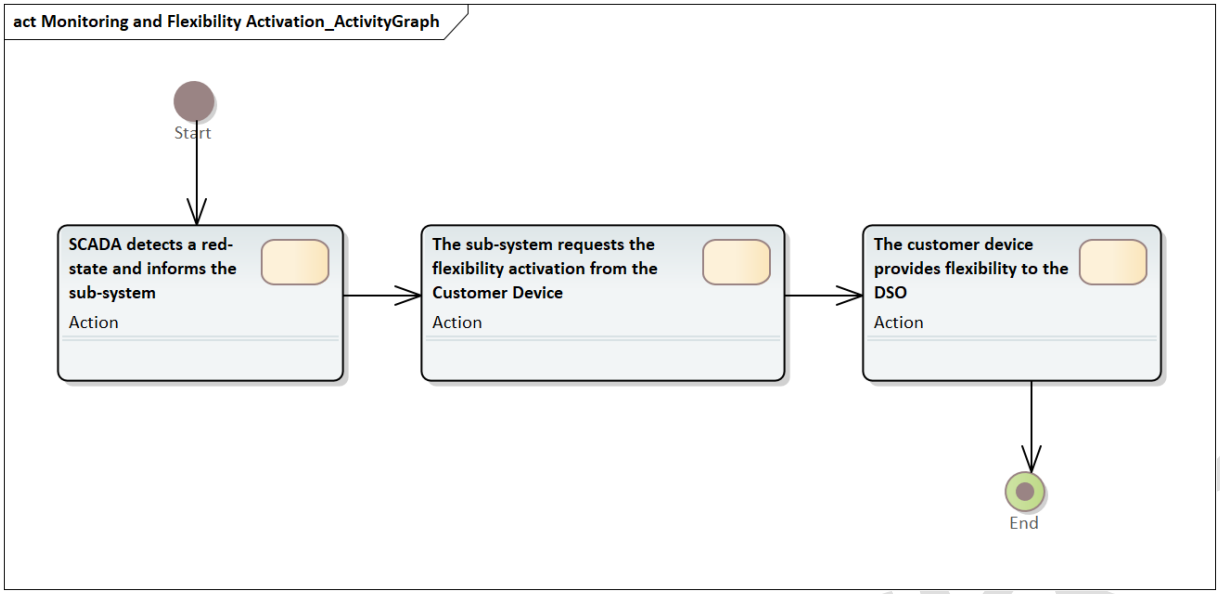

Abbildung 55: Aktivitätsdiagramm zur Beschreibung der Schritte in der "Monitoring and Flexibility Activation" Funktion.

Die „Flexibility Activation“ Funktion

Gemäß den Anforderungen zielt diese Funktion darauf ab, die Flexibilität zu aktivieren. In einer typischen Situation wird diese Funktion vom VNB ausgelöst, wenn ein roter Netzzustand von der Funktion „Monitoring and Flexibility Activation“ erkannt wird. Nach Erhalt des Signals werden die Sollwerte an das Kundengerät gesendet, das daraufhin sein Verhalten entsprechend ändert, so dass die Flexibilität aktiviert wird und dem VNB hilft, das Netz aus dem roten Zustand zu befreien. Ein Überblick über das Anwendungsfallmodell ist in Abbildung 56 dargestellt. Zusätzlich zeigt Abbildung 57 ein Sequenzdiagramm, das die Interaktionen zwischen den beteiligten Akteuren hervorhebt, während Abbildung 58 die wichtigsten Schritte während der Ausführung dieser Funktion darstellt.

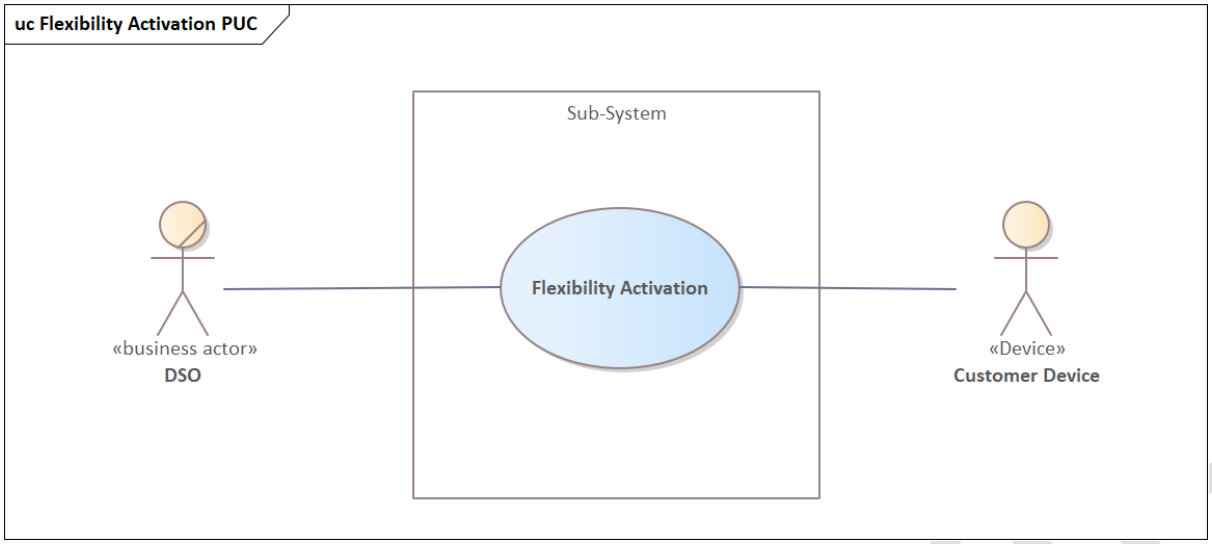

Abbildung 56: PUC Modell für die „Flexibility Activation“ Funktion.

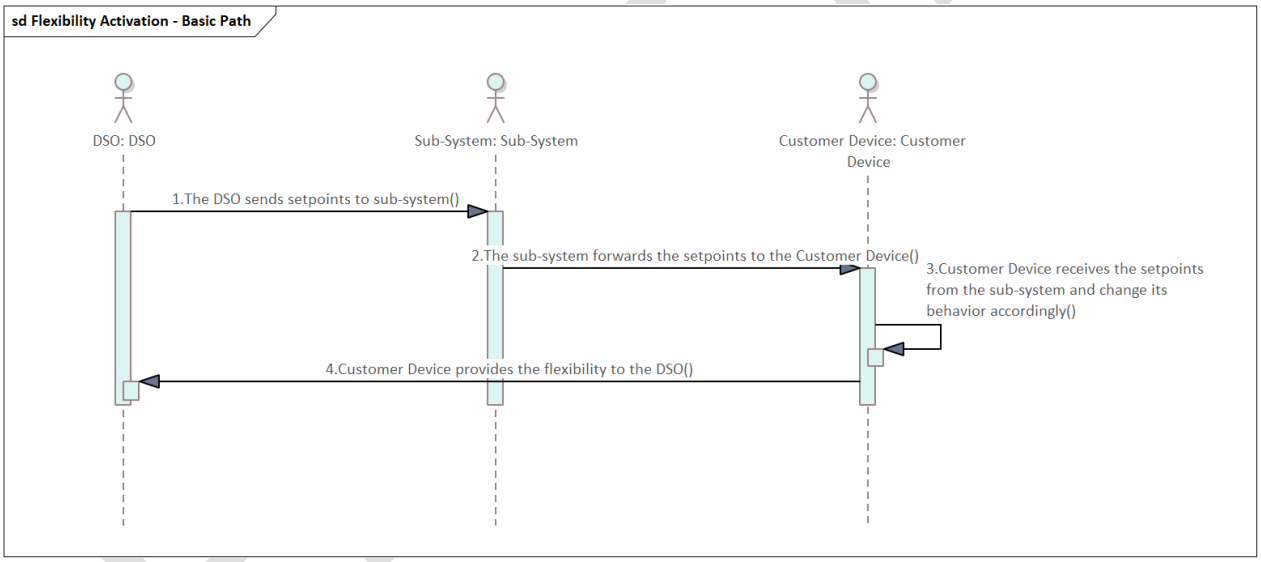

Abbildung 57: Sequenzdiagram für die Interaktionen der involvierten Akteure in der „Flexibility Activation“ Funktion.

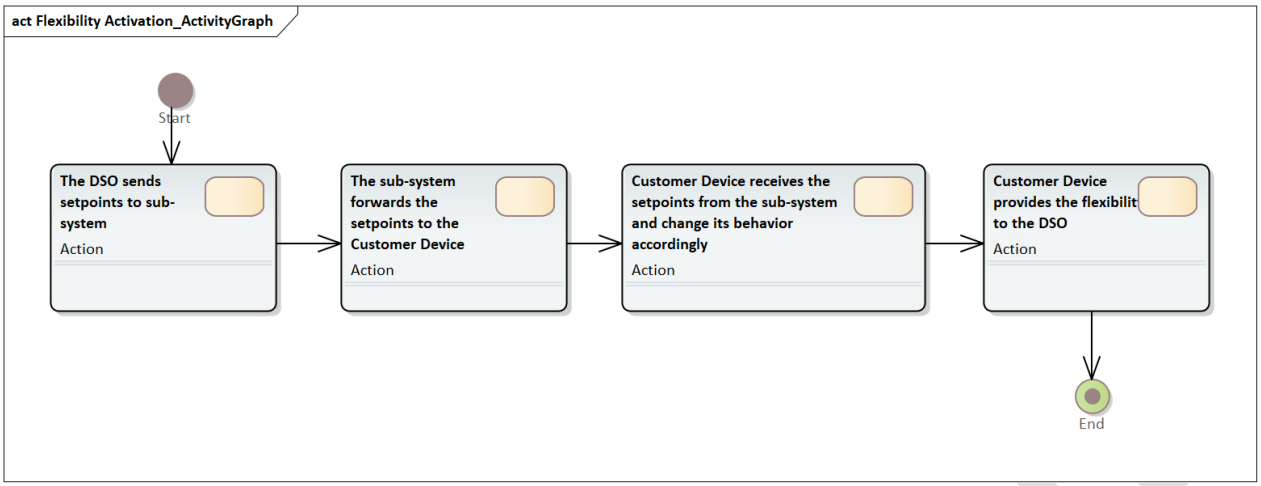

Abbildung 58: Aktivitätsdiagramm zur Beschreibung der Schritte in der "Flexibility Activation" Funktion.

Die „Data Acquisition“ Funktion

Diese Funktion soll helfen, Daten von den Kundengeräten zu sammeln und sie der VNB-Infrastruktur zur Verfügung zu stellen. Die Funktion kann entweder als Push-Funktion implementiert werden, bei der das Gerät nach einem festgelegten Zeitintervall Daten an das Backend System des VNB sendet, oder als Pull-Funktion, bei der die VNB-Infrastruktur eine Datenanforderung stellt, ebenfalls in einem festgelegten Zeitintervall. In beiden Fällen werden die Daten vom Kundengerät für die Speicherung und/oder Analyse zur Verfügung gestellt. Abbildung 59 gibt einen Überblick über das Anwendungsfallmodell für diese Funktion. Die Interaktionen zwischen den beteiligten Akteuren werden mit Hilfe eines Sequenzdiagramms dargestellt, das in Abbildung 60 zu sehen ist. Zusätzlich ist in Abbildung 61 ein Aktivitätsdiagramm dargestellt, das die Schritte während der Ausführung dieser Funktion skizziert.

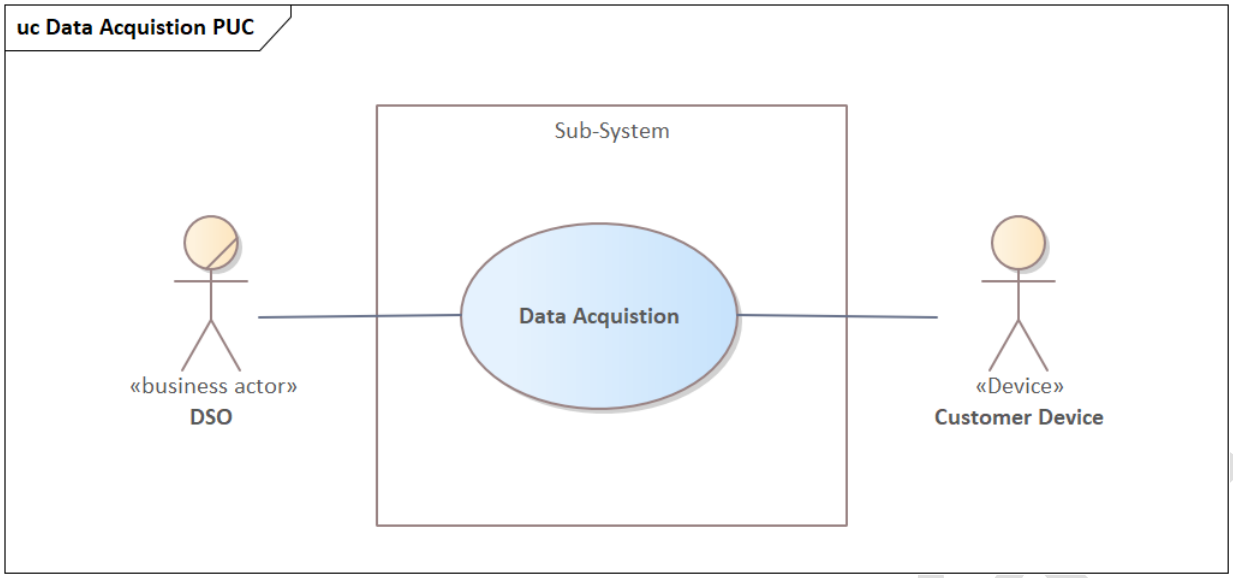

Abbildung 59: PUC Modell für die „Data Acquisition“ Funktion.

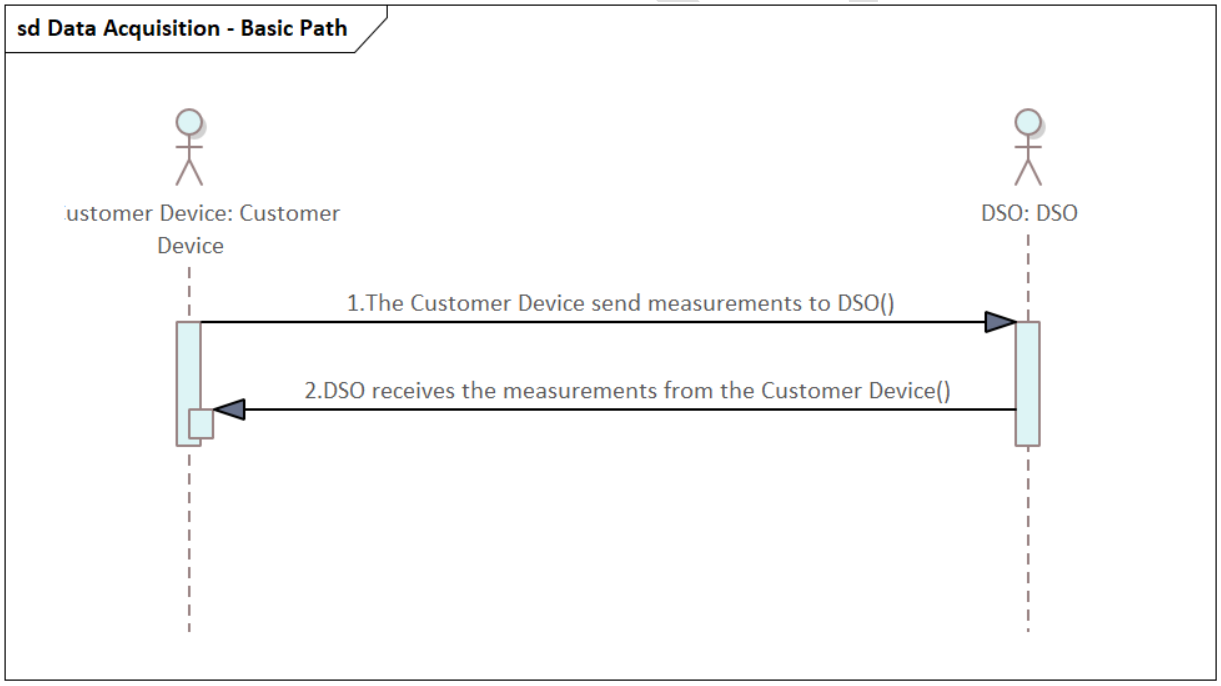

Abbildung 60: Sequenzdiagram für die Interaktionen der involvierten Akteure in der „Data Acquisition“ Funktion.

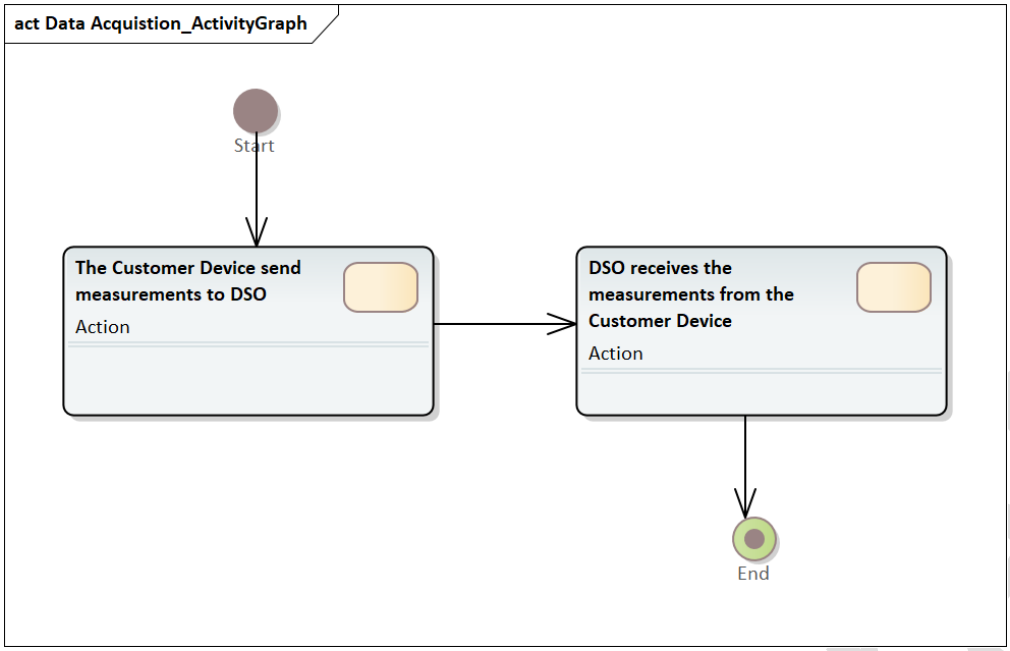

Abbildung 61: Aktivitätsdiagramm zur Beschreibung der Schritte in der „Data Acquisition" Funktion.

Der „SGAM Information Layer“

Die „SGAM Information Layer“ hebt den Informationsaustausch zwischen den verschiedenen Funktionen, Anwendungsfällen und/oder Akteuren hervor. Sie hilft bei der Definition und Betrachtung der möglichen Interaktionspunkte und der Abhängigkeiten. Für die Architekturvariante 2 ist die Informationsebene in Abbildung 62 dargestellt. Die Interaktionen zwischen den beteiligten Akteuren sind auch in Tabelle 22 zusammengefasst.

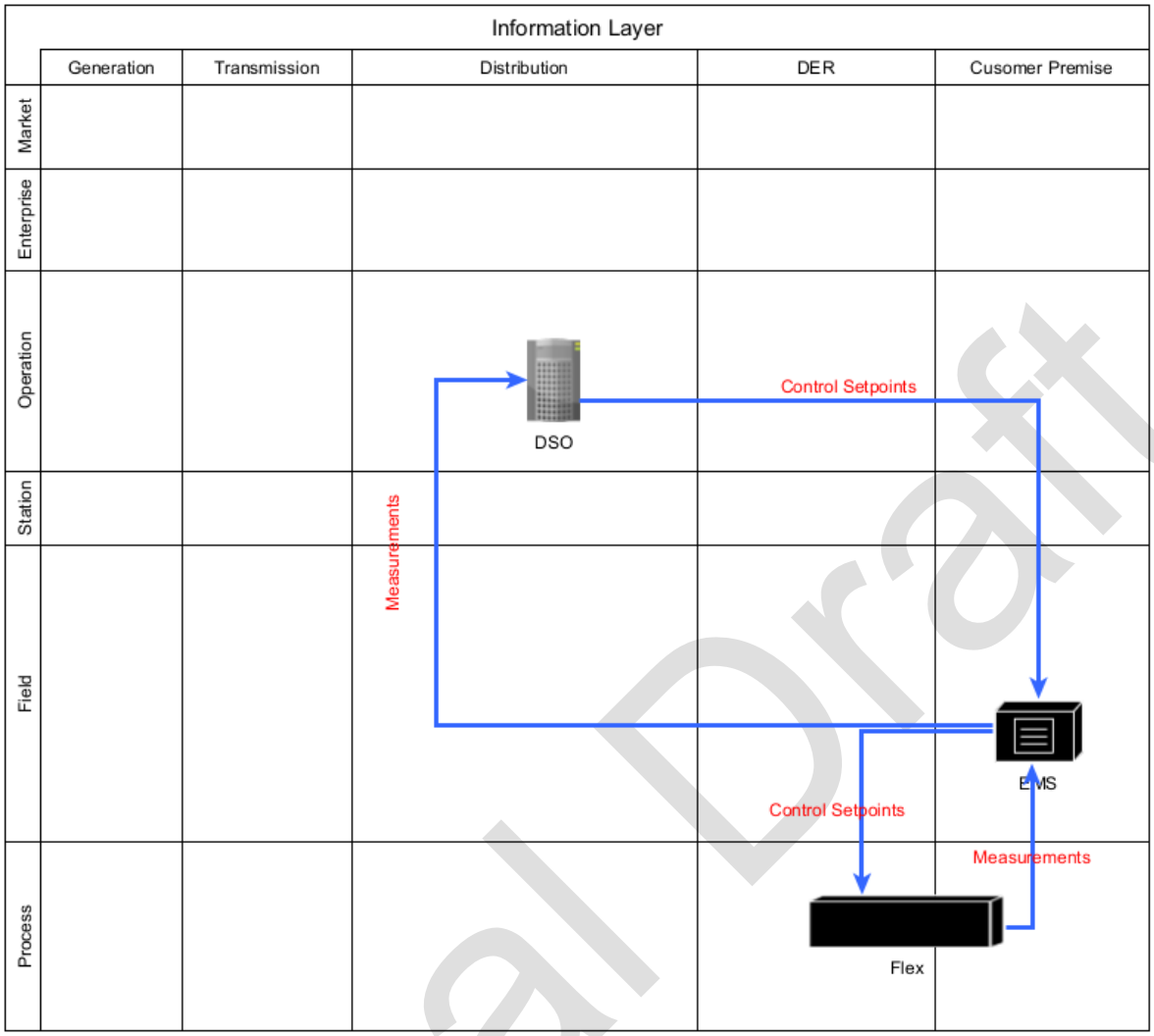

Abbildung 62: „SGAM Information Layer" für Architekturvariante 2.

Tabelle 22: Informationsaustausch in der Architekturvariante 2.

ID	Source Interface	Sink Interface	Information exchange
1	DSO	EMS	Flexibility activation request with control setpoints and network location
2	EMS	DSO	Measurements and aggregated available flexibilities
3	EMS	Customer Device (Flex)	Control setpoints for flexibility activation

4	Customer Device (Flex)	EMS	Measurement and available flexibility

Architekturvariante 3

In diesem Unterabschnitt wird die SGAM-Modellierung für die dritte Architekturvariante beschrieben. Ein Überblick über diese Architekturvariante ist in Abbildung 30 dargestellt. In dieser Architekturvariante wird die Möglichkeit untersucht, dass der VNB mit dem Kunden über ein in den Räumlichkeiten des Kunden installiertes Gateway-Gerät interagiert. Daher muss für diese Architekturvariante ein zusätzliches Hardware-Gerät entwickelt werden, dessen Funktionalität definiert und in jedem Haushalt installiert wird. Dieses Gerät übernimmt dann die Koordination zwischen dem VNB und dem Kunden. Alle wichtigen Funktionen und Dienste werden vom VNB betrieben und über das Gateway ausgeführt.

Der „SGAM Function Layer“

Der „SGAM Function Layer“ wird, wie bereits erwähnt, zur Modellierung der Funktionen, Dienste und Anwendungsfälle verwendet, die für die Realisierung der geplanten Ziele erforderlich sind. Aus funktionaler Sicht ähnelt das Modell für die Architekturvariante 3 der Architekturvariante 2, jedoch sind die Realisierung und die Verantwortlichkeiten dieser Funktionen sehr unterschiedlich. Das Modell ist in Abbildung 63 unten dargestellt. Es gibt drei Hauptfunktionen, Dienste und primäre Anwendungsfälle (Primary Use Cases, PUC) für die Erfüllung der angestrebten Ziele. Die Überwachungs- und Flexibilitätsaktivierungsfunktion („Monitoring and Flexibility Activation“) sendet die Flexibilitätsanforderungen, wenn ein roter Netzzustand erkannt wird, die Flexibilitätsaktivierung („Flexibility Activation“) kümmert sich um die Aktivierung der Flexibilität, während die Datenerfassungsfunktion („Data Acquisition“) die Sammlung von Messungen für die verschiedenen Kundengeräte übernimmt. In dieser Architekturvariante werden die letzten beiden Funktionen von der Gateway-Hardware ausgeführt. Im Folgenden wird jede der Funktionen mit Hilfe entsprechender UML-Diagramme näher erläutert.

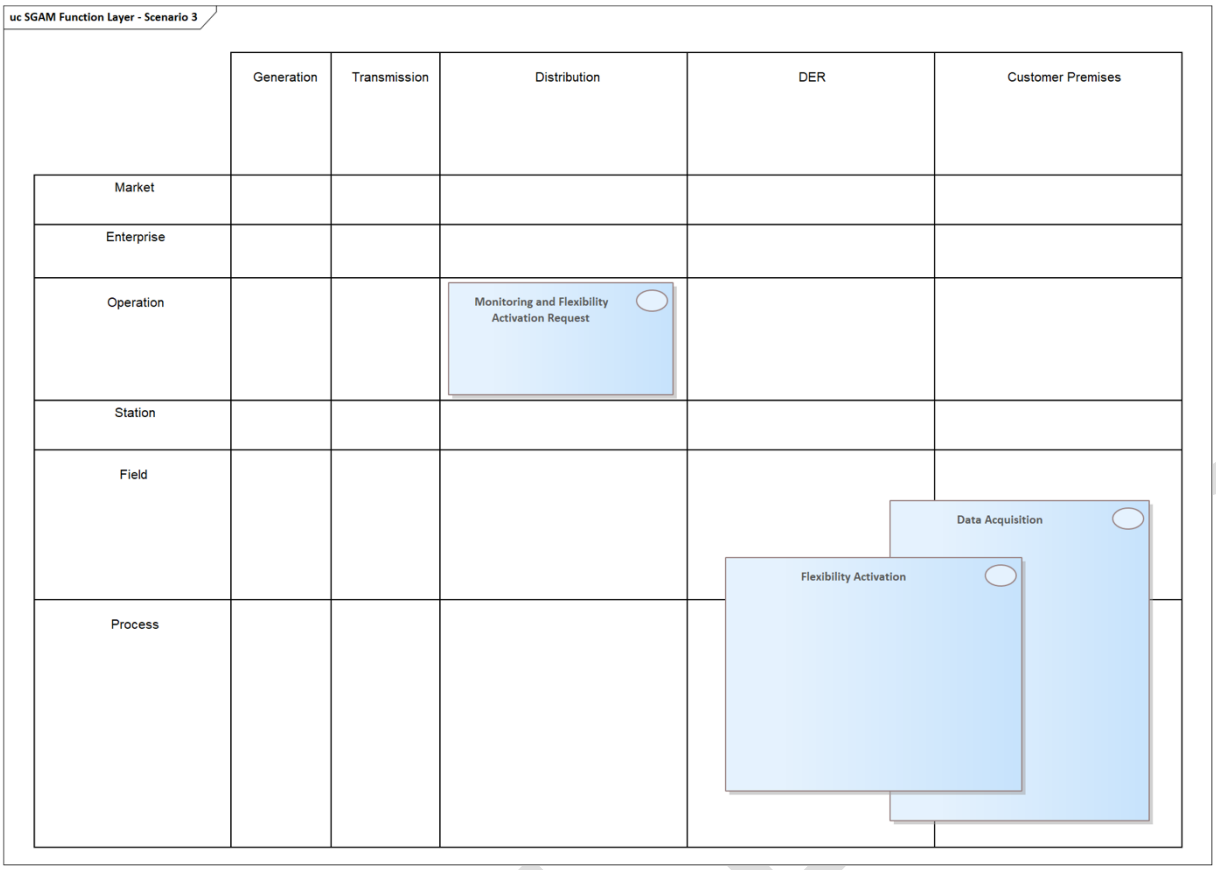

Abbildung 63: „SGAM Function Layer" für Architekturvariante 3

Die „Monitoring and Flexibility Activation" Funktion

Diese Funktion wird vom VNB ausgeführt und zielt darauf ab, eine Anforderung zur Flexibilitätsaktivierung zu stellen, sobald das VNB-Überwachungssystem einen roten Netzzustand feststellt. Sobald ein solcher Zustand erkannt wird, wird das Untersystem ausgelöst, das eine Anfrage an das Gateway-Gerät mit den berechneten Sollwerten stellt. Nach Erhalt der Anfrage leitet die Anfrage an einzelne Komponenten oder über das EMS des Kunden an das Kundengerät weiter. Das Kundengerät ändert sein Verhalten und bietet dem VNB Flexibilität. Ein Überblick über die Funktion ist in Abbildung 64 dargestellt.

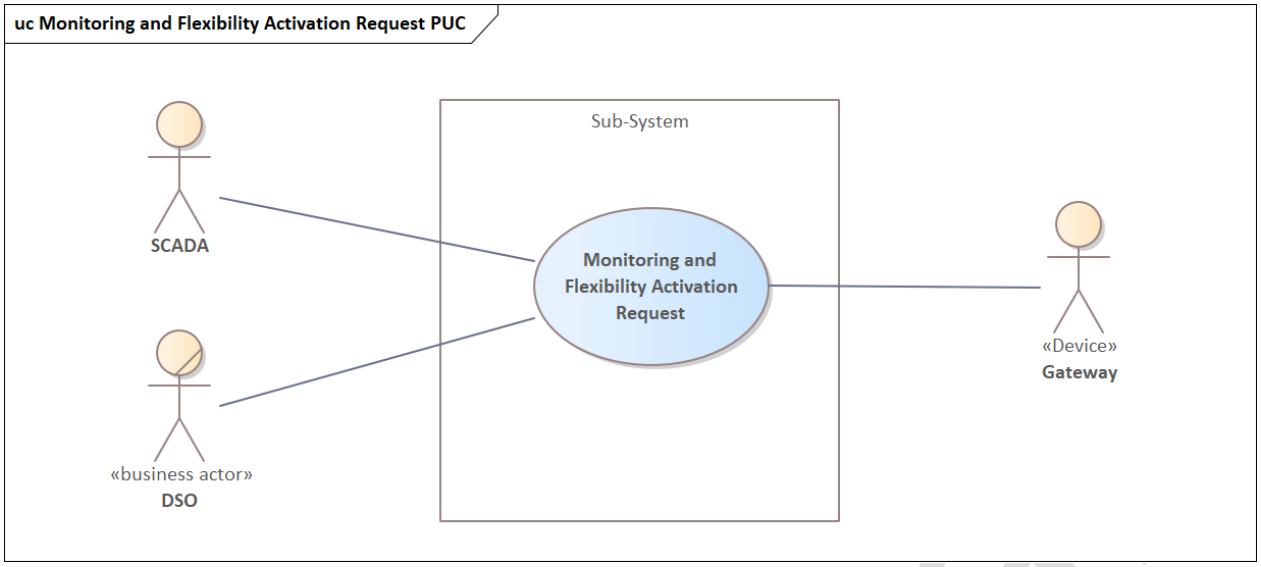

Abbildung 64: PUC Modell für die „Monitoring und Flexibility Activation“ Funktion

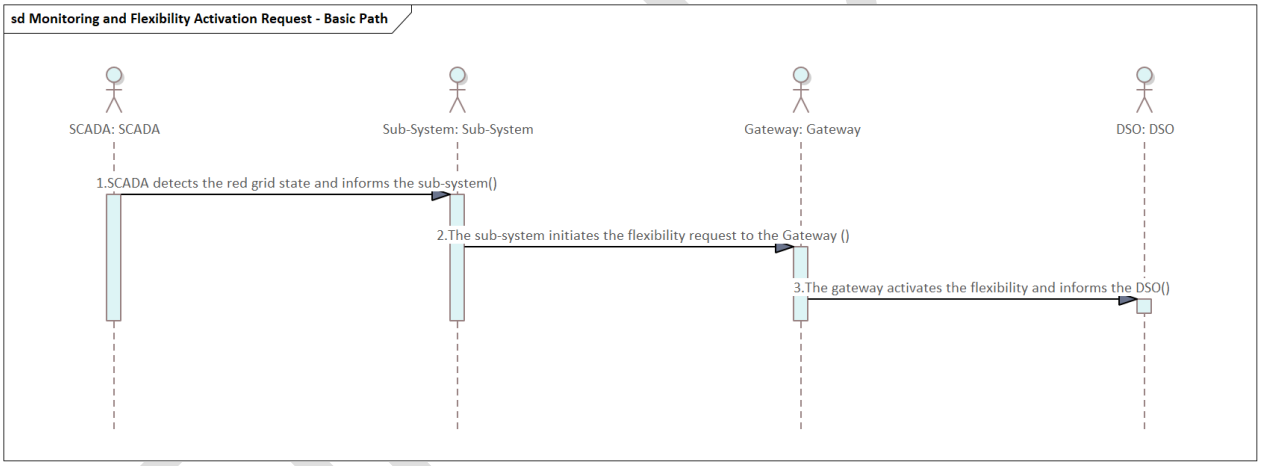

Abbildung 65: Sequenzdiagram für die Interaktionen der involvierten Akteure in der „Monitoring und Flexibility Activation“ Funktion

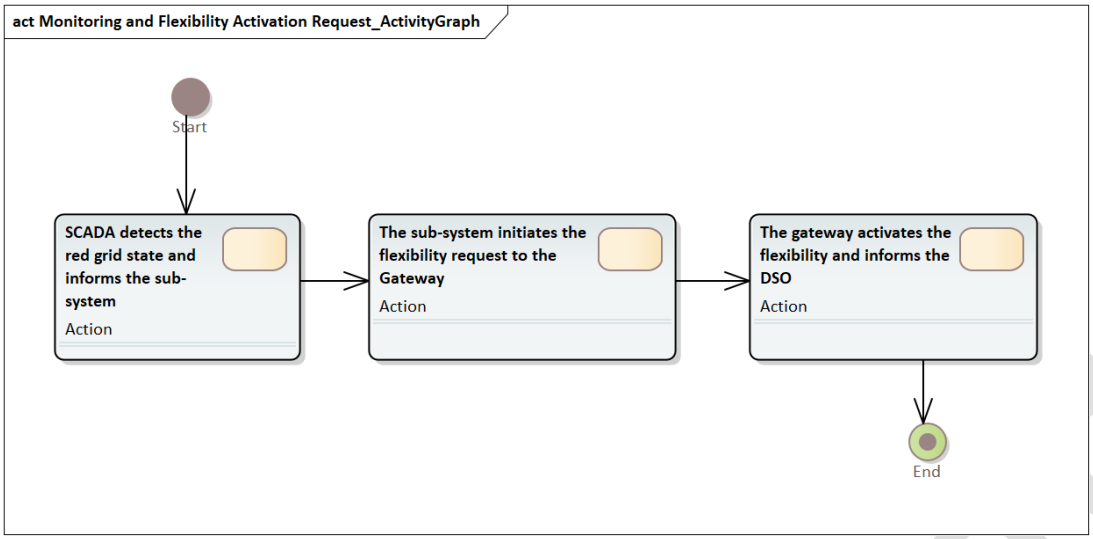

Abbildung 66: Aktivitätsdiagramm zur Beschreibung der Schritte in der "Monitoring und Flexibility Activation" Funktion

Die „Flexibility Activation“ Funktion

Diese Funktion wird vom Gateway-Gerät im Auftrag des VNB ausgeführt. Die Hauptfunktion besteht darin, die vom VNB empfangenen Sollwerte an die Komponenten oder über das EMS an die Komponente weiterzuleiten. Eine typische Ausführung wäre, dass der VNB eine Anforderung zur Flexibilität der Sollwerte an das Gateway-Gerät sendet, wenn ein roter Netzzustand festgestellt wird. Das Gateway-Gerät würde die Anforderung an das EMS weiterleiten, damit dieses die Sollwerte an ein Kundengerät weitergibt, das in der Lage ist, die erforderliche Flexibilität zu bieten. Nach Erhalt der Sollwerte würde sich das Kundengerät an den Sollwert anpassen, was wiederum dem VNB Flexibilität bietet und dem Netz hilft, sich von dem roten Zustand zu erholen. Ein Überblick über die Funktion mit einem Anwendungsfallmodell ist in Abbildung 67 dargestellt. Abbildung 68 zeigt die Interaktion zwischen den beteiligten Akteuren anhand eines UML-Sequenzdiagramms. Abbildung 69 skizziert die wichtigsten Schritte und ihre Abfolge anhand eines UML-Aktivitätsdiagramms.

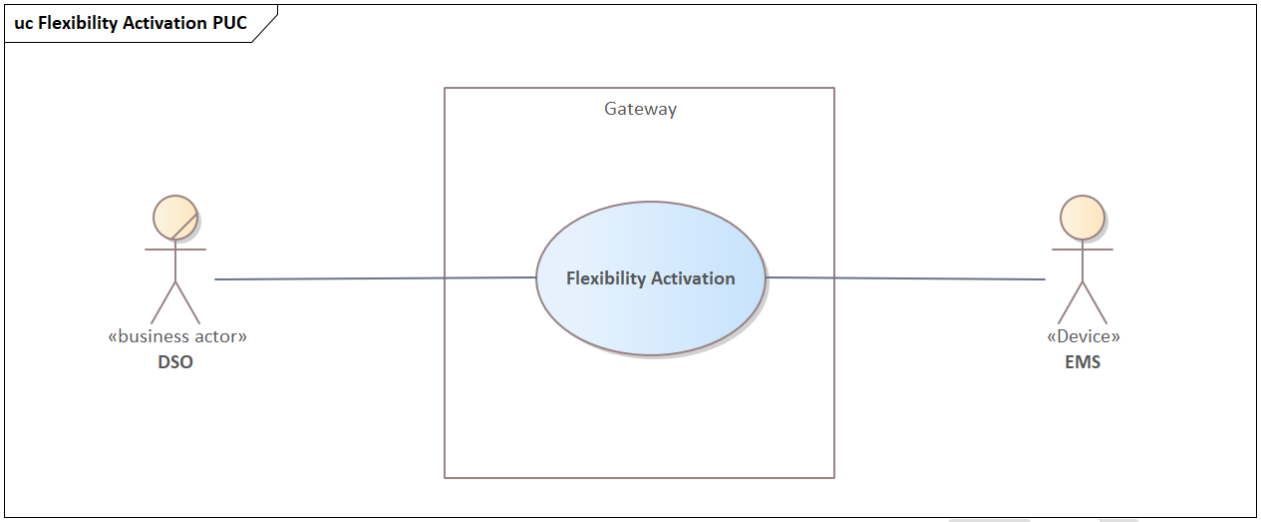

Abbildung 67: PUC Modell für die „Flexibility Activation“ Funktion.

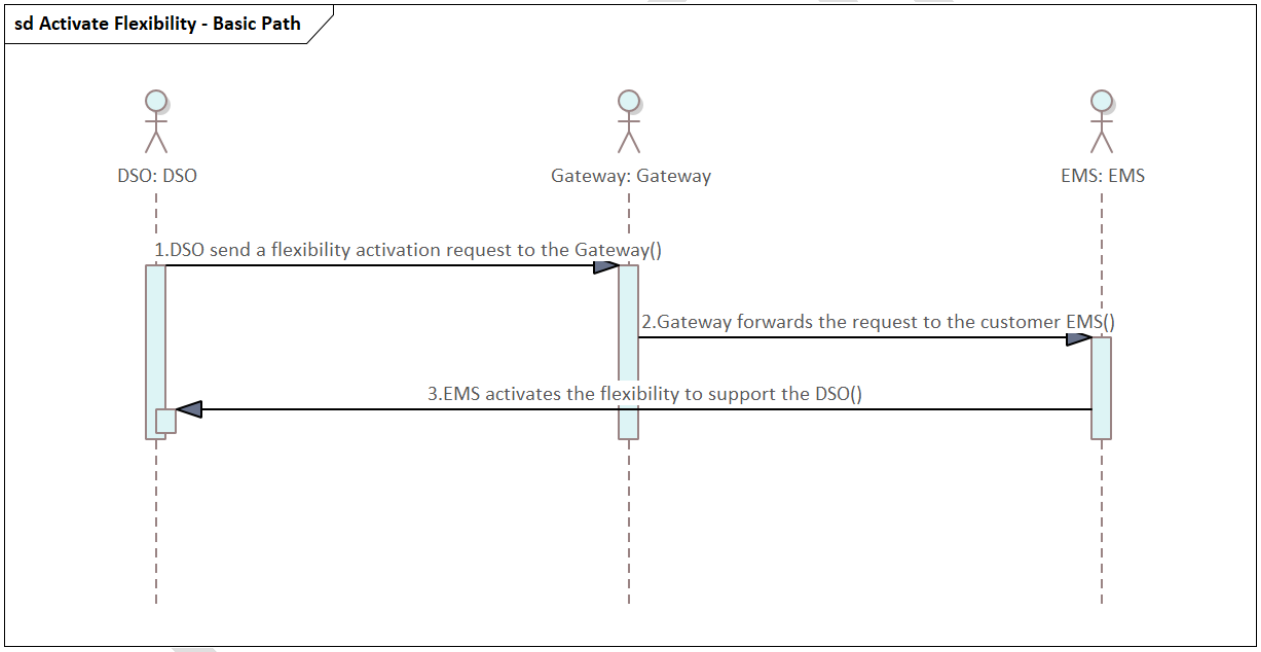

Abbildung 68: Sequenzdiagram für die Interaktionen der involvierten Akteure in der „Flexibility Activation“ Funktion.

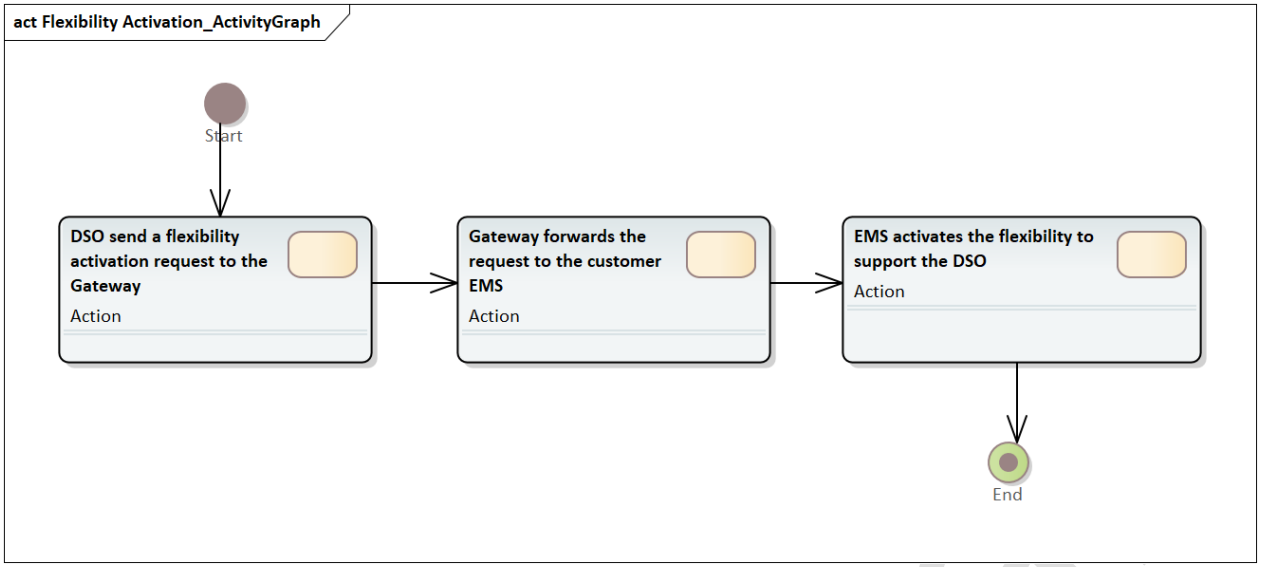

Abbildung 69: Aktivitätsdiagramm zur Beschreibung der Schritte in der "Flexibility Activation" Funktion.

Die „Data Acquisition“ Funktion

Die Funktionalität kann entweder als Pull- oder als Push-Funktion implementiert werden. Bei einer Pull-Implementierung sendet das Gateway die Messanfragen an das/die Kundengerät(e)/EMS in einem bestimmten Zeitintervall oder zu einem bestimmten Ereignis, auf das die Geräte reagieren. Bei einer Push-Implementierung senden die Kundengeräte die Messungen wiederum in einem bestimmten Zeitintervall an das Gateway. Das Gateway stellt die gesammelten Messungen dem DSO zur weiteren Analyse und Speicherung zur Verfügung. Ein Überblick über die Funktionalität ist in Abbildung 70 als Anwendungsfallmodell dargestellt. Abbildung 71 zeigt außerdem die Interaktion zwischen den beteiligten Akteuren, während Abbildung 72 die wichtigsten Schritte bei der Ausführung dieser Funktion skizziert.

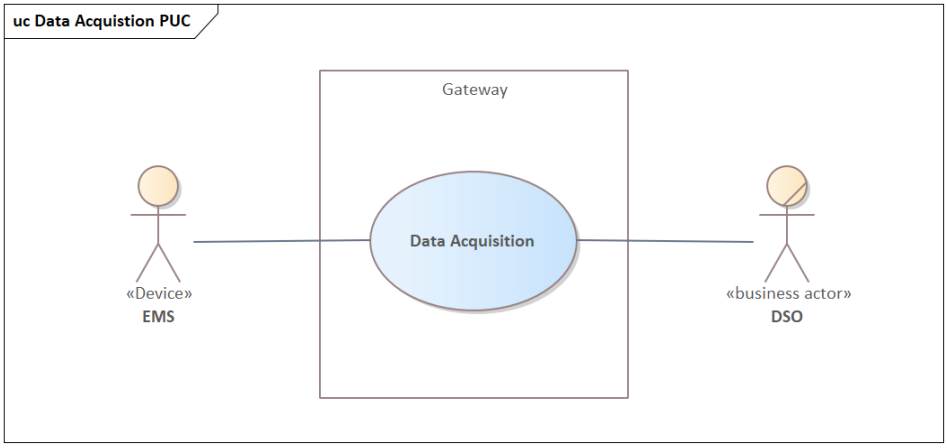

Abbildung 70: PUC Modell für die „Data Acquisition“ Funktion.

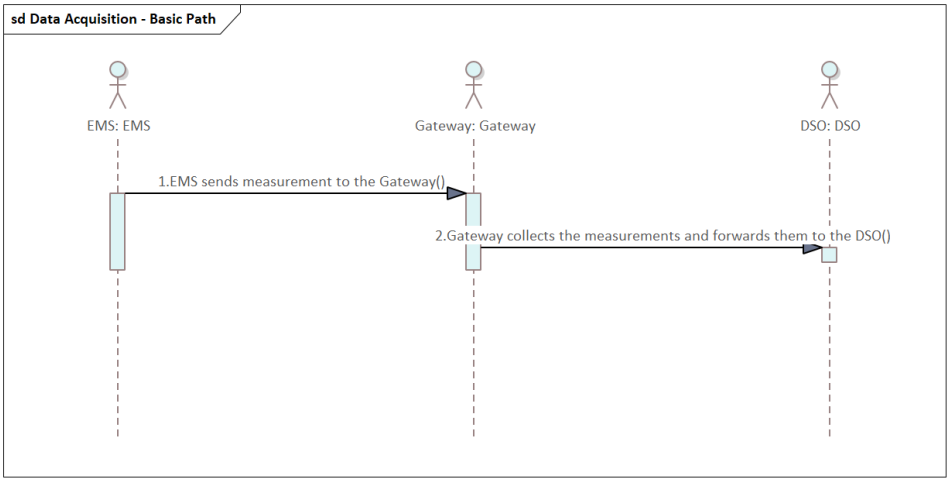

Abbildung 71: Sequenzdiagram für die Interaktionen der involvierten Akteure in der „Data Acquisition“ Funktion.

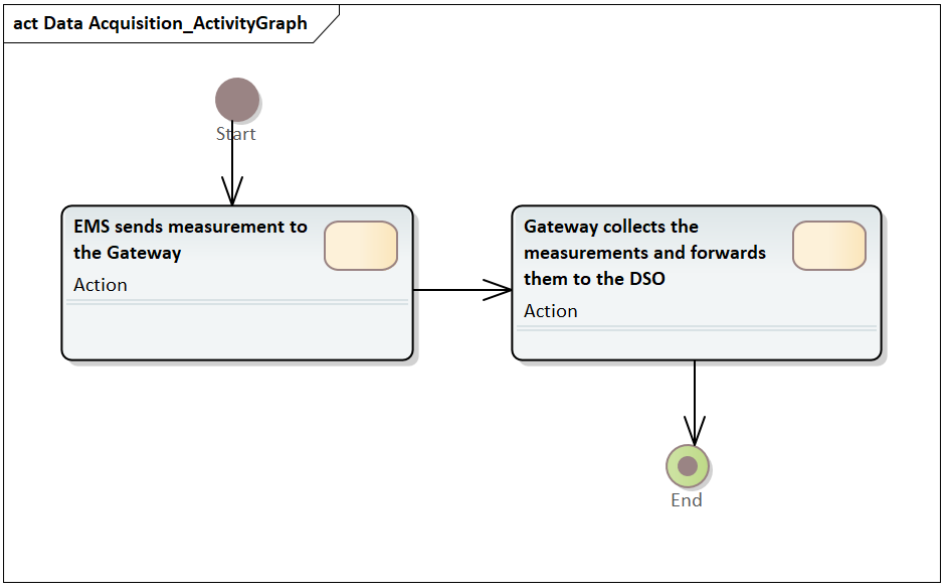

Abbildung 72: Aktivitätsdiagramm zur Beschreibung der Schritte in der "Data Acquisition" Funktion

Der „SGAM Information Layer“

Für die Architekturvariante 3 ist der „SGAM Information Layer“ in Abbildung 73 dargestellt. Wie im Modell zu sehen ist, gibt es zwei Hauptakteure (EMS, Kundengerät(e)) auf der Kundenseite, während die verbleibenden zwei (VNB und Gateway) auf der Verteilerseite liegen und vom VNB betrieben werden. Hier

wurde das EMS exemplarisch dargestellt. Es wäre auch denkbar, dass die Kundengeräte nicht über ein EMS mit dem Gateway verbunden sind.

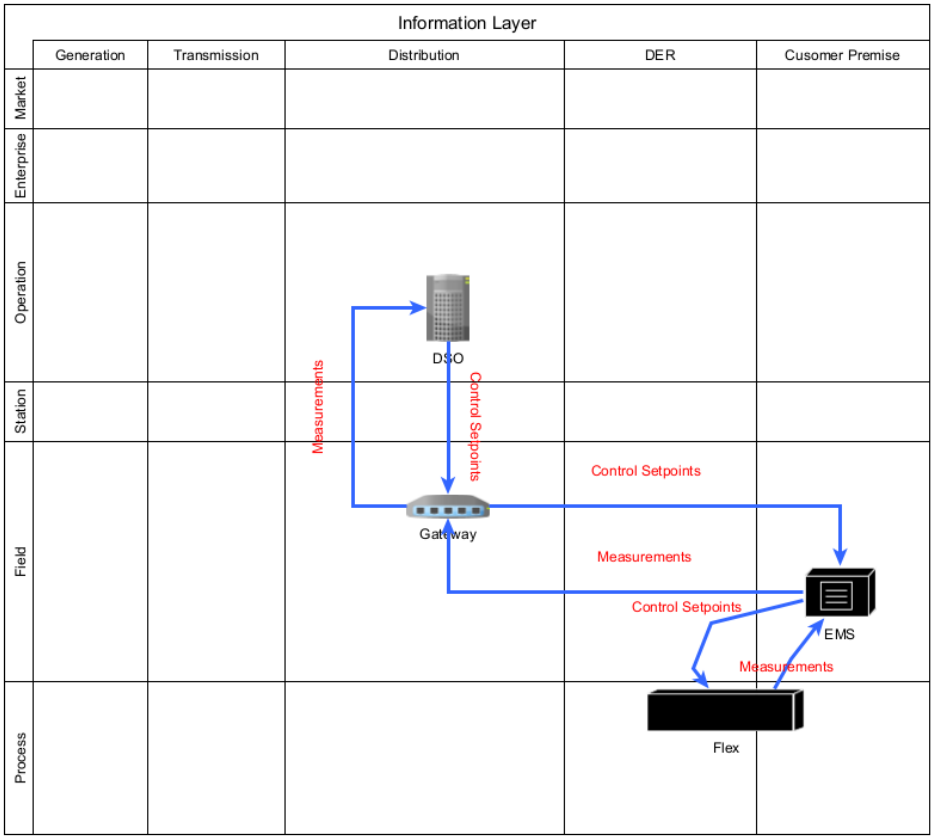

Abbildung 73: „SGAM Information Layer" für Architekturvariante 3

Tabelle 23 gibt einen Überblick über die Interaktionen und den Informationsaustausch zwischen den verschiedenen Schnittstellen der beteiligten Akteure während der Ausführung der Funktionen in der Architekturvariante 3.

Tabelle 23: Informationsaustausch bei der Architekturvariante 3

ID	Source Interface	Sink Interface	Information exchange
1	DSO	Gateway	Flexibility activation request with control setpoints
2	Gateway	DSO	Measurements and aggregated available flexibilities
3	EMS	Gateway	Measurements and aggregated available flexibilities
4	Gateway	EMS	Flexibility activation request with control setpoints

5	EMS	Customer Device (Flex)	Control setpoints for flexibility activation

J.5.9 Vergleich der Architekturvarianten

Um einen objektiven Vergleich der drei unterschiedlichen Architekturvarianten durchführen zu können, wurden mehrere Vergleichskriterien definiert und anschließend für die Architekturvarianten bewertet. Hierbei steht der Vergleich der unterschiedlichen Architekturvarianten im Vordergrund, auf eine detaillierte quantitative Bewertung der Kriterien wurde aufgrund des Projektrahmens verzichtet. Die Bewertung erfolgt in Abhängigkeit des Kriteriums mittels:

- - z.B. schnellste Umsetzung, geringster Aufwand
- - z.B. mittlere Umsetzung, mittlerer Aufwand
- - z.B. langsamste Umsetzung, höchster Aufwand

In der folgenden Aufzählung werden die Kriterien beschrieben, die Tabellen zeigen die jeweiligen Bewertungsergebnisse der Architekturvarianten anhand dieser Kriterien.

- *Schnelle Umsetzung:* Kann ein bereits bestehendes System direkt genutzt werden oder müssen neue Komponenten (Software, Hardware, Kommunikation) entwickelt, implementiert und getestet werden?

Variante	Schnelle Umsetzung	Bewertung
1	Bestehendes (Teil)System der Aggregatoren (Aggregator – Kunde/Kundenanlage) kann genutzt werden. Umsetzung der lokalen Schnittstelle notwendig (Verteilernetzbetreiber – Aggregator)	
2	Schnelle Umsetzung ist nicht möglich, da kein bestehendes (Teil)System genutzt werden kann, vollständige Umsetzung notwendig.	
3	Schnelle Umsetzung ist nicht möglich, da kein bestehendes (Teil)System genutzt werden kann, vollständige Umsetzung notwendig.	

- *Zusätzliche Hardware:* Wird zusätzliche Hardware und damit verbundener Installationsaufwand für die Umsetzung der Architekturvariante benötigt?

Variante	Zusätzliche Hardware	Bewertung
1	Keine zusätzliche Hardware für die Architekturvariante benötigt.	
2	Keine zusätzliche Hardware für die Architekturvariante benötigt.	
3	Zusätzliche Hardware ggf. benötigt oder Integration in bestehende Hardware (Funktionsblock)	

- *Anpassung Hardware:* Muss bereits bestehende Hardware für die Umsetzung der Architekturvariante angepasst werden (inkl. Spezifikations- und Umsetzungsaufwand)?

Variante	Anpassung Hardware	Bewertung
1	Keine Anpassung der bestehenden Hardware notwendig	
2	Anpassung der bestehenden Hardware erforderlich (Umsetzung der Schnittstelle auf Komponentenebene)	
3	Anpassung der bestehenden Hardware (z.B. Integration des Funktionsblocks) oder Entwicklung neuer Hardware (eigenes Gateway)	

- *Device-Management:* Entstehen dem Verteilernetzbetreiber Aufwände für Device-Management bestehender und Onboarding neuer Hardware?

Variante	Device-Management	Bewertung
1	Kein/Geringer Aufwand für den Verteilernetzbetreiber. Aufwand liegt beim Aggregator.	
2	Hoher Aufwand für Onboarding und Device-Management beim Verteilernetzbetreiber (für alle Geräte)	
3	Mittlerer Aufwand für Onboarding und Device-Management beim Verteilernetzbetreiber (1 Instanz hinter Funktionsblock)	

- *Zertifizierung Aggregator:* Ist eine Zertifizierung des Vertragspartners (hier Aggregator) notwendig (aus Sicht des Verteilernetzbetreibers)?

Variante	Zertifizierung Aggregator	Bewertung
1	Zertifizierung des Aggregators als Vertragspartner notwendig.	
2	Keine Zertifizierung notwendig (Kunde als Vertragspartner)	
3	Keine Zertifizierung notwendig (Kunde als Vertragspartner)	

- *Zertifizierung Hersteller:* Ist eine Zertifizierung des Vertragspartners (hier Hersteller von Soft- und Hardwarelösungen) notwendig (aus Sicht des Verteilernetzbetreibers)?

Variante	Zertifizierung Hersteller	Bewertung
1	Keine Zertifizierung notwendig (erfolgt über Aggregator)	
2	Zertifizierung des Herstellers (Kundenanlage mit direkter Anbindung an das System des Verteilernetzbetreibers) als Vertragspartner für den Verteilernetzbetreiber notwendig	
3	Zertifizierung des Herstellers (Funktionsblock mit Anbindung an das System des Verteilernetzbetreibers) als Vertragspartner für den Verteilernetzbetreiber notwendig	

- *Kontakt VNB:* Ist der direkte Ansprechpartner des Verteilernetzbetreibers ein Fachmann oder ein Laie?

Variante	Kontakt VNB	Bewertung
1	Kontakt bzw. direkter Ansprechpartner des Verteilernetzbetreibers ist ein Fachmann (hohe Kompetenz)	
2	Kontakt bzw. direkter Ansprechpartner des Verteilernetzbetreibers ist der Kunden (Laie, im Normalfall geringe Kompetenz)	
3	Kontakt bzw. direkter Ansprechpartner des Verteilernetzbetreibers ist der Kunden (Laie, im Normalfall geringe Kompetenz)	

- *Zugriff Komponente(n) oder EMS:* Besteht für den Verteilernetzbetreiber die Möglichkeit direkt auf die Komponente(n) oder EMS zuzugreifen (ohne weitere Instanz im Kommunikationsweg)?

Variante	Zugriff Komponente(n)/EMS	Bewertung
1	Direkter Zugriff durch den Verteilernetzbetreiber auf die Komponente(n) oder EMS nicht möglich (Aggregator als Instanz zwischen Verteilernetzbetreiber und Kundenanlage)	
2	Direkter Zugriff auf Komponente(n) oder EMS möglich	
3	Direkter Zugriff auf Komponente(n) oder EMS möglich (jedoch über Funktionsblock im Eigentum des Verteilernetzbetreibers)	

- *Rückkanal zur Kontrolle:* Wie ist die Implementierung des Rückkanals zum VNB zur Kontrolle der Umsetzung der Leistungsvorgaben durch die Kundenanlagen?

Variante	Rückkanal zur Kontrolle	Bewertung
1	Die Messwerte werden über den Aggregator an den VNB übertragen (weitere Instanz im Kommunikationsweg, Möglichkeit zur Veränderung/Verfälschung der Werte)	
2	Die Komponente(n) stellen ihre Messwerte direkt dem VNB zur Verfügung (keine weitere Instanz zwischen Komponente(n) und VNB, geringste Möglichkeiten zur Veränderung/Verfälschung der Werte)	
3	Die Messwerte werden über den Funktionsblock an den VNB übertragen (weitere Instanz im Kommunikationsweg, jedoch im Eigentum des Verteilernetzbetreibers)	

- *Ende-zu-Ende-Übertragungsgeschwindigkeit:* Wie kann die Ende-zu-Ende-Übertragungsgeschwindigkeit eingeschätzt werden, gibt es Einschränkungen in der Übertragung?

Variante	Ende-zu-Ende-Übertragungsgeschwindigkeit	Bewertung
1	Ende-zu-Ende-Übertragungsgeschwindigkeit durch Aggregator als Instanz (ggf. mit zusätzlichen Berechnungen) eingeschränkt	
2	Ende-zu-Ende-Übertragungsgeschwindigkeit maximal (direkte Kommunikation ohne weitere Instanz)	
3	Ende-zu-Ende-Übertragungsgeschwindigkeit durch Funktionsblock eingeschränkt	

- *Eigenes Kommunikationsnetz:* Besteht die Notwendigkeit ein zusätzliches Kommunikationsnetz beim Kunden einzurichten bzw. zu verwalten?

Variante	Eigenes Kommunikationsnetz	Bewertung
1	Kein zusätzliches Netzwerk notwendig (bestehendes Netzwerk kann genutzt werden)	
2	Kein zusätzliches Netzwerk notwendig	
3	Zusätzliches Netzwerk zwischen Funktionsblock und Kundenanlage notwendig	

- *Einbindung Dritter:* Ist die Einbindung weiterer Dienstleister möglich bzw. mit welchen Aufwänden ist zu rechnen?

Variante	Einbindung Dritter	Bewertung
1	Die Schnittstelle beim Aggregator kann für weitere Dienstleiter genutzt/angeboten werden (Aufwand beim Aggregator)	
2	Die Schnittstelle der Kundenanlage (inkl. Software; Hinterlegung: Priorität für Verteilernetzbetreiber) kann für weitere Dienstleister angepasst werden (Aufwand beim Hersteller)	
3	Hoher Aufwand für Verteilernetzbetreiber zur Bereitstellung der Schnittstelle des Funktionsblocks (Eigentümer des Funktionsblocks bzw. Verantwortung über Funktionsblock)	

- *Skalierbarkeit:* Wie kann die Skalierbarkeit (aus Sicht des Verteilernetzbetreibers) der Architekturvariante eingeschätzt werden, gibt es limitierende Faktoren?

Variante	Skalierbarkeit	Bewertung
1	Anzahl an Verbindungen für Verteilernetzbetreiber abhängig von der Anzahl der Aggregatoren (als Vertragspartner) und dadurch hohes Potential zur Skalierung der Lösung	
2	Anzahl an Verbindungen für Verteilernetzbetreiber abhängig von der Anzahl der Kunden (als Vertragspartner) und dadurch eingeschränkte Skalierbarkeit	

3	Anzahl an Verbindungen für Verteilernetzbetreiber abhängig von der Anzahl der Kunden (als Vertragspartner) und dadurch eingeschränkte Skalierbarkeit	

- *Fallback-Mechanismen:* Welche Fallback-Mechanismen (Anpassung der Leistung der Komponente auf definiertes Limit) stehen beim Ausfall der zentralen Schnittstelle zur Verfügung

Variante	Fallback-Mechanismen	Bewertung
1	Fallback-Mechanismus muss auf der Komponente implementiert werden. Zusätzlich können weitere Mechanismen beim Aggregator hinterlegt sein (Ausfall der zentralen Schnittstelle, aufrechte Verbindung zwischen Aggregator und Kundenanlage).	
2	Fallback-Mechanismus muss auf der Komponente implementiert werden. Keine weiteren Möglichkeiten bei Ausfall der zentralen Schnittstelle	
3	Fallback-Mechanismus muss auf der Komponente implementiert werden. Zusätzlich können weitere Mechanismen (z.B. lokales Management der Gesamtleistung mehrerer Komponenten) im Funktionsblock hinterlegt sein (Ausfall der zentralen Schnittstelle, aufrechte Verbindung zwischen Funktionsblock und Kundenanlage).	

J.5.10 Übersicht der Cyber-Security Anforderungen

ACCESS CONTROL (SG.AC)			
1	SG.AC-1	Access Control Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
2	SG.AC-2	Remote Access Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
3	SG.AC-3	Account Management	Common Governance, Risk, and Compliance (GRC) Requirements
4	SG.AC-4	Access Enforcement	Common Governance, Risk, and Compliance (GRC) Requirements
5	SG.AC-5	Information Flow Enforcement	Unique Technical Requirements
6	SG.AC-6	Separation of Duties	Common Technical Requirements, Integrity
7	SG.AC-7	Least Privilege	Common Technical Requirements, Integrity
8	SG.AC-8	Unsuccessful Login Attempts	Common Technical Requirements, Integrity
9	SG.AC-9	Smart Grid Information System Use Notification	Common Technical Requirements, Integrity
10	SG.AC-10	Previous Logon Notification	Unique Technical Requirements
11	SG.AC-11	Concurrent Session Control	Unique Technical Requirements
12	SG.AC-12	Session Lock	Unique Technical Requirements
13	SG.AC-13	Remote Session Termination	Unique Technical Requirements
14	SG.AC-14	Permitted Actions without Identification or Authentication	Unique Technical Requirements
15	SG.AC-15	Remote Access	Unique Technical Requirements
16	SG.AC-16	Wireless Access Restrictions	Common Technical Requirements, Confidentiality
17	SG.AC-17	Access Control for Portable and Mobile Devices	Common Technical Requirements, Confidentiality
18	SG.AC-18	Use of External Information Control Systems	Common Governance, Risk, and Compliance (GRC) Requirements
19	SG.AC-19	Control System Access Restrictions	Common Governance, Risk, and Compliance (GRC) Requirements
20	SG.AC-20	Publicly Accessible Content	Common Governance, Risk, and Compliance (GRC) Requirements
21	SG.AC-21	Passwords	Common Technical Requirements, Integrity
AWARENESS AND TRAINING (SG.AT)			
22	SG.AT-1	Awareness and Training Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
23	SG.AT-2	Security Awareness	Common Governance, Risk, and Compliance (GRC) Requirements
24	SG.AT-3	Security Training	Common Governance, Risk, and Compliance (GRC) Requirements
25	SG.AT-4	Security Awareness and Training Records	Common Governance, Risk, and Compliance (GRC) Requirements
26	SG.AT-5	Contact with Security Groups and Associations	Common Governance, Risk, and Compliance (GRC) Requirements
27	SG.AT-6	Security Responsibility Testing	Common Governance, Risk, and Compliance (GRC) Requirements

28	SG.AT-7	Planning Process Training	Common Governance, Risk, and Compliance (GRC) Requirements
AUDIT AND ACCOUNTABILITY (SG.AU)			
29	SG.AU-1	Audit and Accountability Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
30	SG.AU-2	Auditable Events	Common Technical Requirements, Integrity
31	SG.AU-3	Content of Audit Records	Common Technical Requirements, Integrity
32	SG.AU-4	Audit Storage Capacity	Common Technical Requirements, Integrity
33	SG.AU-5	Response to Audit Processing Failures	Common Governance, Risk, and Compliance (GRC) Requirements
34	SG.AU-6	Audit Monitoring, Analysis, and Reporting	Common Governance, Risk, and Compliance (GRC) Requirements
35	SG.AU-7	Audit Reduction and Report Generation	Common Governance, Risk, and Compliance (GRC) Requirements
36	SG.AU-8	Time Stamps	Common Governance, Risk, and Compliance (GRC) Requirements
37	SG.AU-9	Protection of Audit Information	Common Governance, Risk, and Compliance (GRC) Requirements
38	SG.AU-10	Audit Record Retention	Common Governance, Risk, and Compliance (GRC) Requirements
39	SG.AU-11	Conduct and Frequency of Audits	Common Governance, Risk, and Compliance (GRC) Requirements
40	SG.AU-12	Auditor Qualification	Common Governance, Risk, and Compliance (GRC) Requirements
41	SG.AU-13	Audit Tools	Common Governance, Risk, and Compliance (GRC) Requirements
42	SG.AU-14	Security Policy Compliance	Common Governance, Risk, and Compliance (GRC) Requirements
43	SG.AU-15	Audit Generation	Common Technical Requirements, Integrity
44	SG.AU-16	Non-Repudiation	Unique Technical Requirements
SECURITY ASSESSMENT AND AUTHORIZATION (SG.CA)			
45	SG.CA-1	Security Assessment and Authorization Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
46	SG.CA-2	Security Assessments	Common Governance, Risk, and Compliance (GRC) Requirements
47	SG.CA-3	Continuous Improvement	Common Governance, Risk, and Compliance (GRC) Requirements
48	SG.CA-4	Smart Grid Information System Connections	Common Governance, Risk, and Compliance (GRC) Requirements
49	SG.CA-5	Security Authorization to Operate	Common Governance, Risk, and Compliance (GRC) Requirements
50	SG.CA-6	Continuous Monitoring	Common Governance, Risk, and Compliance (GRC) Requirements
CONFIGURATION MANAGEMENT (SG.CM)			
51	SG.CM-1	Configuration Management Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
52	SG.CM-2	Baseline Configuration	Common Governance, Risk, and Compliance (GRC) Requirements
53	SG.CM-3	Configuration Change Control	Common Governance, Risk, and Compliance (GRC) Requirements
54	SG.CM-4	Monitoring Configuration Changes	Common Governance, Risk, and Compliance (GRC) Requirements
55	SG.CM-5	Access Restrictions for Configuration Change	Common Governance, Risk, and Compliance (GRC) Requirements

56	SG.CM-6	Configuration Settings	Common Governance, Risk, and Compliance (GRC) Requirements
57	SG.CM-7	Configuration for Least Functionality	Common Technical Requirements, Integrity
58	SG.CM-8	Component Inventory	Common Technical Requirements, Integrity
59	SG.CM-9	Addition, Removal, and Disposal of Equipment	Common Governance, Risk, and Compliance (GRC) Requirements
60	SG.CM-10	Factory Default Settings Management	Common Governance, Risk, and Compliance (GRC) Requirements
61	SG.CM-11	Configuration Management Plan	Common Governance, Risk, and Compliance (GRC) Requirements
CONTINUITY OF OPERATIONS (SG.CP)			
62	SG.CP-1	Continuity of Operations Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
63	SG.CP-2	Continuity of Operations Plan	Common Governance, Risk, and Compliance (GRC) Requirements
64	SG.CP-3	Continuity of Operations Roles and Responsibilities	Common Governance, Risk, and Compliance (GRC) Requirements
65	SG.CP-4	Continuity of Operations Training	Common Governance, Risk, and Compliance (GRC) Requirements
66	SG.CP-5	Continuity of Operations Plan Testing	Common Governance, Risk, and Compliance (GRC) Requirements
67	SG.CP-6	Continuity of Operations Plan Update	Common Governance, Risk, and Compliance (GRC) Requirements
68	SG.CP-7	Alternate Storage Sites	Common Governance, Risk, and Compliance (GRC) Requirements
69	SG.CP-8	Alternate Telecommunication Services	Common Governance, Risk, and Compliance (GRC) Requirements
70	SG.CP-9	Alternate Control Center	Common Governance, Risk, and Compliance (GRC) Requirements
71	SG.CP-10	Smart Grid Information System Recovery and Reconstitution	Common Governance, Risk, and Compliance (GRC) Requirements
72	SG.CP-11	Fail-Safe Response	Common Governance, Risk, and Compliance (GRC) Requirements
IDENTIFICATION AND AUTHENTICATION (SG.IA)			
73	SG.IA-1	Identification and Authentication Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
74	SG.IA-2	Identifier Management	Common Governance, Risk, and Compliance (GRC) Requirements
75	SG.IA-3	Authenticator Management	Common Governance, Risk, and Compliance (GRC) Requirements
76	SG.IA-4	User Identification and Authentication	Unique Technical Requirements
77	SG.IA-5	Device Identification and Authentication	Unique Technical Requirements
78	SG.IA-6	Authenticator Feedback	Unique Technical Requirements
INFORMATION AND DOCUMENT MANAGEMENT (SG.ID)			
79	SG.ID-1	Information and Document Management Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
80	SG.ID-2	Information and Document Retention	Common Governance, Risk, and Compliance (GRC) Requirements
81	SG.ID-3	Information Handling	Common Governance, Risk, and Compliance (GRC) Requirements
82	SG.ID-4	Information Exchange	Common Governance, Risk, and Compliance (GRC) Requirements
83	SG.ID-5	Automated Labeling	Common Governance, Risk, and Compliance (GRC) Requirements

INCIDENT RESPONSE (SG.IR)			
84	SG.IR-1	Incident Response Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
85	SG.IR-2	Incident Response Roles and Responsibilities	Common Governance, Risk, and Compliance (GRC) Requirements
86	SG.IR-3	Incident Response Training	Common Governance, Risk, and Compliance (GRC) Requirements
87	SG.IR-4	Incident Response Testing and Exercises	Common Governance, Risk, and Compliance (GRC) Requirements
88	SG.IR-5	Incident Handling	Common Governance, Risk, and Compliance (GRC) Requirements
89	SG.IR-6	Incident Monitoring	Common Governance, Risk, and Compliance (GRC) Requirements
90	SG.IR-7	Incident Reporting	Common Governance, Risk, and Compliance (GRC) Requirements
91	SG.IR-8	Incident Response Investigation and Analysis	Common Governance, Risk, and Compliance (GRC) Requirements
92	SG.IR-9	Corrective Action	Common Governance, Risk, and Compliance (GRC) Requirements
93	SG.IR-10	Smart Grid Information System Backup	Common Governance, Risk, and Compliance (GRC) Requirements
94	SG.IR-11	Coordination of Emergency Response	Common Governance, Risk, and Compliance (GRC) Requirements
SMART GRID INFORMATION SYSTEM DEVELOPMENT AND MAINTENANCE (SG.MA)			
95	SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
96	SG.MA-2	Legacy Smart Grid Information System Upgrades	Common Governance, Risk, and Compliance (GRC) Requirements
97	SG.MA-3	Smart Grid Information System Maintenance	Common Governance, Risk, and Compliance (GRC) Requirements
98	SG.MA-4	Maintenance Tools	Common Governance, Risk, and Compliance (GRC) Requirements
99	SG.MA-5	Maintenance Personnel	Common Governance, Risk, and Compliance (GRC) Requirements
100	SG.MA-6	Remote Maintenance	Common Governance, Risk, and Compliance (GRC) Requirements
101	SG.MA-7	Timely Maintenance	Common Governance, Risk, and Compliance (GRC) Requirements
MEDIA PROTECTION (SG.MP)			
102	SG.MP-1	Media Protection Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
103	SG.MP-2	Media Sensitivity Level	Common Governance, Risk, and Compliance (GRC) Requirements
104	SG.MP-3	Media Marking	Common Governance, Risk, and Compliance (GRC) Requirements
105	SG.MP-4	Media Storage	Common Governance, Risk, and Compliance (GRC) Requirements
106	SG.MP-5	Media Transport	Common Governance, Risk, and Compliance (GRC) Requirements
107	SG.MP-6	Media Sanitization and Disposal	Common Governance, Risk, and Compliance (GRC) Requirements
PHYSICAL AND ENVIRONMENTAL SECURITY (SG.PE)			
108	SG.PE-1	Physical and Environmental Security Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
109	SG.PE-2	Physical Access Authorizations	Common Governance, Risk, and Compliance (GRC) Requirements
110	SG.PE-3	Physical Access	Common Governance, Risk, and Compliance (GRC) Requirements

111	SG.PE-4	Monitoring Physical Access	Common Governance, Risk, and Compliance (GRC) Requirements
112	SG.PE-5	Visitor Control	Common Governance, Risk, and Compliance (GRC) Requirements
113	SG.PE-6	Visitor Records	Common Governance, Risk, and Compliance (GRC) Requirements
114	SG.PE-7	Physical Access Log Retention	Common Governance, Risk, and Compliance (GRC) Requirements
115	SG.PE-8	Emergency Shutoff Protection	Common Governance, Risk, and Compliance (GRC) Requirements
116	SG.PE-9	Emergency Power	Common Governance, Risk, and Compliance (GRC) Requirements
117	SG.PE-10	Delivery and Removal	Common Governance, Risk, and Compliance (GRC) Requirements
118	SG.PE-11	Alternate Work Site	Common Governance, Risk, and Compliance (GRC) Requirements
119	SG.PE-12	Location of Smart Grid Information System Assets	Common Governance, Risk, and Compliance (GRC) Requirements
PLANNING (SG.PL)			
120	SG.PL-1	Strategic Planning Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
121	SG.PL-2	Smart Grid Information System Security Plan	Common Governance, Risk, and Compliance (GRC) Requirements
122	SG.PL-3	Rules of Behavior	Common Governance, Risk, and Compliance (GRC) Requirements
123	SG.PL-4	Privacy Impact Assessment	Common Governance, Risk, and Compliance (GRC) Requirements
124	SG.PL-5	Security-Related Activity Planning	Common Governance, Risk, and Compliance (GRC) Requirements
SECURITY PROGRAM MANAGEMENT (SG.PM)			
125	SG.PM-1	Security Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
126	SG.PM-2	Security Program Plan	Common Governance, Risk, and Compliance (GRC) Requirements
127	SG.PM-3	Senior Management Authority	Common Governance, Risk, and Compliance (GRC) Requirements
128	SG.PM-4	Security Architecture	Common Governance, Risk, and Compliance (GRC) Requirements
129	SG.PM-5	Risk Management Strategy	Common Governance, Risk, and Compliance (GRC) Requirements
130	SG.PM-6	Security Authorization to Operate Process	Common Governance, Risk, and Compliance (GRC) Requirements
131	SG.PM-7	Mission/Business Process Definition	Common Governance, Risk, and Compliance (GRC) Requirements
132	SG.PM-8	Management Accountability	Common Governance, Risk, and Compliance (GRC) Requirements
PERSONNEL SECURITY (SG.PS)			
133	SG.PS-1	Personnel Security Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
134	SG.PS-2	Position Categorization	Common Governance, Risk, and Compliance (GRC) Requirements
135	SG.PS-3	Personnel Screening	Common Governance, Risk, and Compliance (GRC) Requirements
136	SG.PS-4	Personnel Termination	Common Governance, Risk, and Compliance (GRC) Requirements
137	SG.PS-5	Personnel Transfer	Common Governance, Risk, and Compliance (GRC) Requirements
138	SG.PS-6	Access Agreements	Common Governance, Risk, and Compliance (GRC) Requirements

139	SG.PS-7	Contractor and Third-Party Personnel Security	Common Governance, Risk, and Compliance (GRC) Requirements
140	SG.PS-8	Personnel Accountability	Common Governance, Risk, and Compliance (GRC) Requirements
141	SG.PS-9	Personnel Roles	Common Governance, Risk, and Compliance (GRC) Requirements
RISK MANAGEMENT AND ASSESSMENT (SG.RA)			
142	SG.RA-1	Risk Assessment Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
143	SG.RA-2	Risk Management Plan	Common Governance, Risk, and Compliance (GRC) Requirements
144	SG.RA-3	Security Impact Level	Common Governance, Risk, and Compliance (GRC) Requirements
145	SG.RA-4	Risk Assessment	Common Governance, Risk, and Compliance (GRC) Requirements
146	SG.RA-5	Risk Assessment Update	Common Governance, Risk, and Compliance (GRC) Requirements
147	SG.RA-6	Vulnerability Assessment and Awareness	Common Governance, Risk, and Compliance (GRC) Requirements
SMART GRID INFORMATION SYSTEM AND SERVICES ACQUISITION (SG.SA)			
148	SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
149	SG.SA-2	Security Policies for Contractors and Third Parties	Common Governance, Risk, and Compliance (GRC) Requirements
150	SG.SA-3	Life-Cycle Support	Common Governance, Risk, and Compliance (GRC) Requirements
151	SG.SA-4	Acquisitions	Common Governance, Risk, and Compliance (GRC) Requirements
152	SG.SA-5	Smart Grid Information System Documentation	Common Governance, Risk, and Compliance (GRC) Requirements
153	SG.SA-6	Software License Usage Restrictions	Common Governance, Risk, and Compliance (GRC) Requirements
154	SG.SA-7	User-Installed Software	Common Governance, Risk, and Compliance (GRC) Requirements
155	SG.SA-8	Security Engineering Principles	Common Governance, Risk, and Compliance (GRC) Requirements
156	SG.SA-9	Developer Configuration Management	Common Governance, Risk, and Compliance (GRC) Requirements
157	SG.SA-10	Developer Security Testing	Common Technical Requirements, Integrity
158	SG.SA-11	Supply Chain Protection	Common Technical Requirements, Integrity
SMART GRID INFORMATION SYSTEM AND COMMUNICATION PROTECTION (SG.SC)			
159	SG.SC-1	Smart Grid Information System and Communication Protection Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
160	SG.SC-2	Communications Partitioning	Unique Technical Requirements
161	SG.SC-3	Security Function Isolation	Unique Technical Requirements
162	SG.SC-4	Information Remnants	Unique Technical Requirements
163	SG.SC-5	Denial-of-Service Protection	Unique Technical Requirements
164	SG.SC-6	Resource Priority	Unique Technical Requirements
165	SG.SC-7	Boundary Protection	Unique Technical Requirements

166	SG.SC-8	Communication Integrity	Unique Technical Requirements
167	SG.SC-9	Communication Confidentiality	Unique Technical Requirements
168	SG.SC-10	Trusted Path	Unique Technical Requirements
169	SG.SC-11	Cryptographic Key Establishment and Management	Common Technical Requirements, Confidentiality
170	SG.SC-12	Use of Validated Cryptography	Common Technical Requirements, Confidentiality
171	SG.SC-13	Collaborative Computing	Common Governance, Risk, and Compliance (GRC) Requirements
172	SG.SC-14	Transmission of Security Parameters	Unique Technical Requirements
173	SG.SC-15	Public Key Infrastructure Certificates	Common Technical Requirements, Confidentiality
174	SG.SC-16	Mobile Code	Common Technical Requirements, Confidentiality
175	SG.SC-17	Voice-Over Internet Protocol	Unique Technical Requirements
176	SG.SC-18	System Connections	Common Technical Requirements, Confidentiality
177	SG.SC-19	Security Roles	Common Technical Requirements, Integrity
178	SG.SC-20	Message Authenticity	Common Technical Requirements, Integrity
179	SG.SC-21	Secure Name/Address Resolution Service	Common Technical Requirements, Integrity
180	SG.SC-22	Fail in Known State	Common Technical Requirements, Integrity
181	SG.SC-23	Thin Nodes	Unique Technical Requirements
182	SG.SC-24	Honeypots	Unique Technical Requirements
183	SG.SC-25	Operating System-Independent Applications	Unique Technical Requirements
184	SG.SC-26	Confidentiality of Information at Rest	Unique Technical Requirements
185	SG.SC-27	Heterogeneity	Unique Technical Requirements
186	SG.SC-28	Virtualization Techniques	Unique Technical Requirements
187	SG.SC-29	Application Partitioning	Unique Technical Requirements
188	SG.SC-30	Smart Grid Information System Partitioning	Common Technical Requirements, Integrity
SMART GRID INFORMATION SYSTEM AND INFORMATION INTEGRITY (SG.SI)			
188	SG.SI-1	Smart Grid Information System and Information Integrity Policy and Procedures	Common Governance, Risk, and Compliance (GRC) Requirements
189	SG.SI-2	Flaw Remediation	Common Technical Requirements, Integrity
190	SG.SI-3	Malicious Code and Spam Protection	Common Governance, Risk, and Compliance (GRC) Requirements
191	SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	Common Governance, Risk, and Compliance (GRC) Requirements
192	SG.SI-5	Security Alerts and Advisories	Common Governance, Risk, and Compliance (GRC) Requirements
193	SG.SI-6	Security Functionality Verification	Common Governance, Risk, and Compliance (GRC) Requirements
194	SG.SI-7	Software and Information Integrity	Unique Technical Requirements

195	SG.SI-8	Information Input Validation	Common Technical Requirements, Integrity
196	SG.SI-9	Error Handling	Common Technical Requirements, Integrity

J.5.11 Empfehlung zur Umsetzung – Fazit der AIT-Studie

Im Rahmen der Studie wurden mehrere Standards und Protokolle aus dem Smart Grid Bereich beleuchtet, die bei einer bidirektionalen digitalen Schnittstelle zum Einsatz kommen könnten. Die Im Abschnitt J.5.2 vorgestellten Kriterien wurden bewertet und diese Kriterien dann in 4 Kategorien zusammengefasst.

Zu Beginn wurden alle Aspekte in den Kategorien gleichbehandelt und keine Priorisierung einzelner Kriterien vorgenommen. Die Resultate in J.5.2 wurden mit der Rückmeldung der Stakeholder aus dem Expertenpool gewichtet und zeigen eine Favorisierung von IEEE 2030.5 und OpenADR für eine zentrale Schnittstelle. Für domänenunabhängige lokale Standards und Protokolle erweisen sich IEEE 2030.5 sowie EEBus als sehr gut geeignet, für domänenspezifische lokalen Standards und Protokolle OCPP und Sunspec Modbus.

Die Ergebnisse zeigen, dass Standards bzw. Protokolle einen Vorteil haben können, die auf Technologien aus der IT-Branche aufbauen. Die Kommunikationsarchitekturen der Standards und Protokolle, die auf Webtechnologien als Applikationsprotokolle setzen sind eher moderner und weiterverbreitet. Dieser Umstand kann den notwendigen Aufwand bei der Implementierung verringern, sowie die Wartung und Erweiterung der Kommunikationsinfrastruktur erleichtern.

Eine weite Verbreitung von Applikationsprotokollen, vor allem im IT-Bereich, kann bedeuten, dass Sicherheitslücken schneller bemerkt und bereinigt werden. Ebenso sind Strategien diese Protokolle abzusichern oft schon in der Konzeption berücksichtigt und einfacher umzusetzen.

In den drei ausgewählten Architekturvarianten tauchen sowohl Schnittstellen auf, für die Standards und Protokolle aus dem OT (Operational Technology) Bereich zulässig wären, wie zum Beispiel die Verbindung des VNB zu den Funktionsblöcken im Kundenbereich, als auch Schnittstellen für die Standards und Protokolle aus der IT (Information Technology) am besten geeignet wären, wie zum Beispiel der Verbindung zwischen Aggregator und VNB. Zusätzlich dazu wäre es aber vorteilhaft, wenn alle Architekturvarianten sich zumindest an der zentralen Schnittstelle des gleichen Standards bzw. Protokolls bedienen würden. Unter diesem Hintergrund könnten Standards oder Protokolle, die auf einem weit verbreiteten Applikationsprotokoll aus dem IT-Bereich basieren, als vorteilhaft erweisen.

Die Gefahr bei sehr spezifischen Protokollen, wie zum Beispiel der Applikationsprotokolle der IEC 61850 und IEC 60870 Standards, besteht darin, dass diese Protokolle sehr spezifisch sind und außerhalb der Anwendungen nicht häufig eingesetzt werden. Bei Architekturen, die auf Standard-Webtechnologien, wie REST-APIs (HTTP) oder WebSockets aufbauen, ist die Gefahr geringer, dass die Verbreitung der Protokolle abnimmt.

Die umfangreichen Datenmodelle der IEC 61850 lassen sich eventuell auch nutzen, ohne auf den kompletten Standard zurückzugreifen. Sehr ähnlich wurde das bei der IEEE 2030.5 umgesetzt. Dort wurden eigene Datenstrukturen definiert, die sehr umfangreich sind und eine Übersetzung in das IEC 61850 Datenmodell erlauben. So eine Vorgehensweise wäre auch für eine Österreich Implementierung einer VNB Schnittstelle denkbar, egal welcher Standard oder welches Protokoll gewählt wird. Das Datenmodell könnte im Rahmen einer Demonstrationsimplementierung der digitalen Schnittstelle entstehen, und in weiterer Folge erweitert bzw. wo nötig reduziert werden.

Für die lokale Schnittstelle ergeben sich viele potenzielle Kandidaten. Es gibt keinen klaren Favoriten zur Abdeckung aller Geräte aus verschiedenen Domänen. So hat zum Beispiel OCPP und Modbus TCP eine hohe Verbreitung im Bereich der Ladestationen, jedoch im Bereich der Speicher bzw. Photovoltaik Wechselrichter ist Sunspec (Modbus TCP) vorherrschend. In diesem Bereich versucht EEBus der verbindende Standard zwischen mehreren Domänen zu werden, ist aber noch nicht weit verbreitet. In Zukunft könnte sich diese Verbreitung aber erhöhen, und dann wäre es möglich mit nur einem lokalen Protokoll mehrere Geräte von unterschiedlichen Herstellern aus unterschiedlichen Domänen zu steuern.

In Anbetracht des überaus komplexen Themenbereichs der nur zum Teil untersucht wurde, wird eine Umsetzung von 1 bis 3 Varianten bzw. Standard- bzw. Protokollkombinationen als Demonstrationsimplementierungen vorgeschlagen. Eine solche Umsetzung würde einen Kenntnisgewinn zu einer Implementierung ermöglichen, der über eine reine Literaturrecherche schwer greifbar ist.

Es gilt festzuhalten, dass das Resultat der Studie zwar richtungsweisend ist, aber nicht der alleinige Pfad zu einer Entscheidung für einen Standard bzw. ein Protokoll für eine digitale Schnittstelle in Österreich sein kann.

K. Abbildungsverzeichnis

L. Tabellenverzeichnis

M. Abkürzungsverzeichnis

AIT	Austrian Institute of Technology
CIA	Confidentiality, Integrity, Availability
CPO	Charge Point Operator
CTR	Common technical requirements
EMS	Energiemanagementsystem
EV	Electric Vehicle
GRC	Governance, risk, and compliance
HAN	Home Area Network
LMS	Load Management System
NIS	Netz- und Informationssystemsicherheit
NIST	National Institute of Standards and Technology
PUC	Primary Use Case
PV	Photovoltaik
UTR	Unique technical requriements
VNB	Verteilernetzbetreiber
WP	Wärmepumpe

N. Begriffsbestimmungen

Aggregator

Aggregator bezeichnet Markteilnehmer:innen der mehrere Komponenten oder Kundenanlagen summiert bzw. aggregiert und diese gebündelt zum Kauf, Verkauf oder zur Versteigerung am Elektrizitätsmarkt anbietet. Bei der *Digitalen Schnittstelle* können Aggregatoren die Rolle als Dienstleister (z.B. ein CPO setzt Leistungsbegrenzungen im Auftrag des Verteilernetzbetreibers beim Netzkunden um) oder die Rolle als Bedarfsträger (z.B. ein Lieferant nutzt ein Steuerungs- und Kommunikationssystem eines Verteilernetzbetreibers mit) einnehmen.

Digitale Schnittstelle

Synonym für eine bidirektionale elektronische Schnittstelle, die ein VNB zur Übermittlung von Leistungsvorgaben für eine Kundenanlage zur Verfügung stellt.

Energiemanagementsystem (EMS)

Eine Instanz die mehrere Komponenten bei einem Netzkunden zusammenfasst und Vorgaben des Netzkunden und Netzbetreibers (über *Digitale Schnittstelle*) steuert. Es kann sich dabei um ein eigenes Gerät handeln, eine Implementierung in eine Komponente oder über einen Cloud-Service realisiert werden.

Funktionsblock

Der Funktionsblock ist eine funktionale Beschreibung einer lokalen Schnittstelle zwischen VNB und Kundenanlage. Die technische Ausgestaltung kann durch eine separate Hardware (z.B. eigenes Gateway inkl. Software) und/oder Software (Integration in bestehende Hardware wie beispielsweise Smart Meter) umgesetzt werden.

Gateway

Eigenes Gerät (Hardware) auf der der Funktionsblock implementiert ist.

Komponente

Ein steuerbares Gerät in der Kundenanlage (z. B. Ladestation, PV-Inverter, Wärmepumpe, Speicher …)

Steuerungsoption

Beschreibt die Vorgabe von temporär einzuhaltenden Leistungsgrenzen durch den Verteilernetzbetreiber und den damit zusammenhängenden Datenaustausch (z. B. Messwerte, Zeitreihen wie Lastprofile, Kundeninformationen). Es wird davon ausgegangen, dass die Details dazu in den entsprechenden Netzzugangsverträgen festgelegt werden.