Grundlagen der Massenfähigkeit

Teilprojekt 2 – Umfeldgestaltung

Arbeitspaket 2.8 - Massenfähigkeit durch Technische Regeln / Normen / Standards

C/sells – Großflächiges Schaufenster im Solarbogen Süddeutschlands

SINTEG - Förderprogramm
"Schaufenster intelligente Energie - Digitale Agenda für die Energiewende" (SINTEG)
des Bundesministeriums für Wirtschaft und Energie

Methoden und Modelle für Terminologie, Use Case- und Sicherheitsanalyse sowie Flexibilitätsmodellierung

Interoperabilität durch vereinbarte Regeln, Standards und Normen

Schutzmethodik anhand C/sells-Musterlösung und AutonomieLab Leimen

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

SINTEG
SCHAUFENSTER INTELLIGENTE ENERGIE

Version: **04/2020** (Aktualisierung vom 08.12.2020)

Verfasser: Andreas Kießling (energy design)
in Zusammenarbeit mit den mitwirkenden C/sells-Partnern im AP 2.8

Csells

Inhalt

Abbildungsverzeichnis 4
1 Methodik zur Erfüllung der Schutzbedürfnisse 5
1.1 Schutzbedürfnisse im intelligenten Energiesystem 5
1.2 Prozess zur Analyse und Erfüllung der Schutzbedürfnisse 10
1.2.1 Schritt 1 – Use Case-Analyse zur Ableitung von Schutzzielen 10
1.2.2 Schritt 2 – Risikoanalyse auf Basis von Schutzzielen 14
1.2.3 Schritt 3 - Bestimmung von Schutzanforderungen 18
1.2.4 Schritt 4 - Bestimmung von Schutzmaßnahmen 22
1.2.5 Schritt 5 - Spezifikation von Schutzrichtlinien und Implementierung 25
1.2.6 Schritt 6 - Beschreibung des Einsatzes und Konformitätsprüfung 25
2 C/sells: Musterlösung 26
2.1 Schutzbedürfnisse bei der Geräte- und Zellenintegration 26
2.2 Use Case-Analyse 27
2.3 Risikoanalyse – Integration Einzelanlagen und Gebäudezelle 35
2.4 Bestimmung von Schutzanforderungen 38
2.5 Bestimmung von Schutzmaßnahmen 43
3 Schutzbedarfsanalyse AutonomieLab Leimen 46
3.1 Schutzbedürfnisse in der autonomen Wohngebäudezelle 46
3.2 Use Case-Analyse 47
3.3 Risikoanalyse 55
3.4 Bestimmung der Schutzanforderungen 58
3.1 Bestimmung von Schutzmaßnahmen 62
4 Quellen 65

Abbildungsverzeichnis

Abb. 1: Schutzbedürfnisse im intelligenten Energiesystem 5
Abb. 2: Prozess der Schutzmethodik 10
Abb. 3: Beispiel Komponentenarchitektur C/sells 14
Abb. 4: Schutzanforderungen und Schutzmaßnahmen für Organisation und Technik, [SEG-CG/CSP (12/2016)]. 19
Abb. 5: Sicherheitsanforderungen, Bedrohungen, Gegenmaßnahmen und Management [Quelle: IEC 62351-1] 24
Abb. 6: Prozess der Schutzmethodik 26
Abb. 7: Komponenten der Schutzanalyse zur Musterlösung 34
Abb. 8: Schnittstellenarchitektur S1 bis S12 45
Abb. 9: Prozess der Schutzmethodik 46
Abb. 10: Komponentenarchitektur AutonomieLab Leimen 54
Abb. 11: Schnittstellenarchitektur S1 bis S9 64

1 Methodik zur Erfüllung der Schutzbedürfnisse

1.1 Schutzbedürfnisse im intelligenten Energiesystem

Um die **Schutzbedürfnisse (protection needs)** im intelligenten Energiesystem zu analysieren, wird die in nachfolgender Abbildung veranschaulichte Begriffsstruktur sowie das im EU-Mandat M/490 zur Standardisierung im Smart Grid vorgeschlagene Verfahren für **Smart Grid Informationssicherheit (SGIS)** [SEG-CG/CSP (12/2016)] zur Analyse der Schutzbedürfnisse benutzt. Ausgangspunkt sind dabei Use Cases, die Anwendungen im intelligenten Energiesystem definieren.

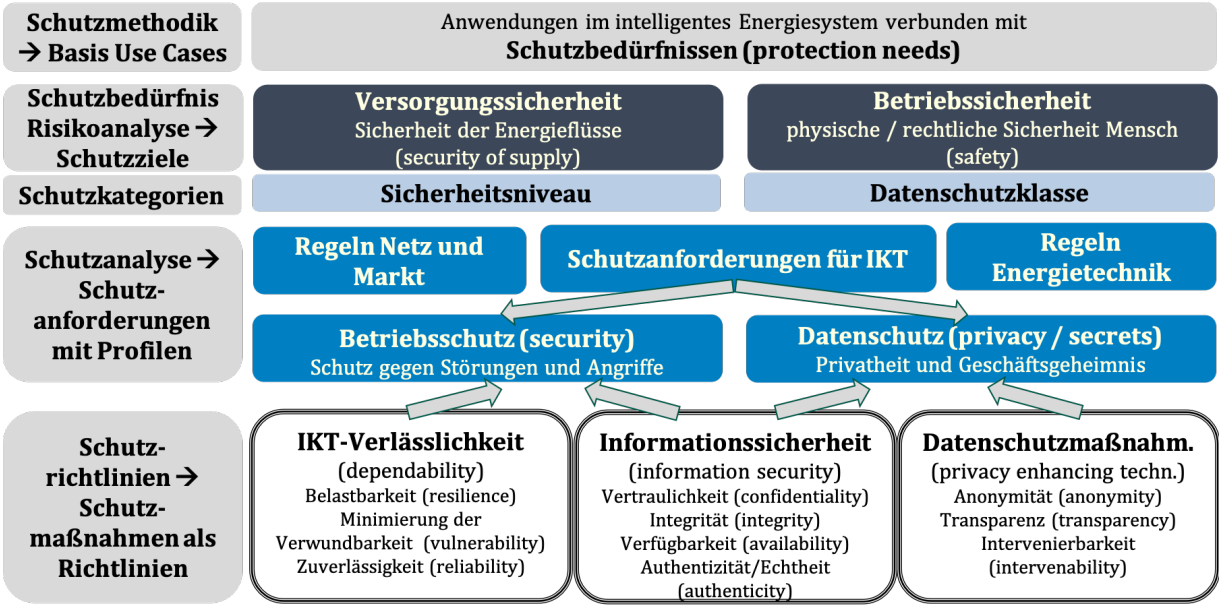

Abb. 1: Schutzbedürfnisse im intelligenten Energiesystem

Die Schutzbedürfnisse werden im Rahmen einer *Use Case-Analyse* als Schutzanforderungen der Systemanwender zur Sicherstellung der gewünschten Funktion formuliert und in zwei Gruppen untergliedert. Dies betrifft erstens die notwendige Sicherheit der korrekten Funktion des Energiesystems und zweitens die Anforderung zur sicheren Anwendung durch den Menschen.

Es gilt es also einen hohen Grad an **Versorgungssicherheit (security of supply)** zu erreichen, so dass weitgehend Ausfälle bei der Versorgung mit benötigter Endenergie vermieden werden. Anderseits bringen Energieflüsse mit den Medien Elektrizität, Wärme und Gas auch potentielle Gefahren für den Menschen und dessen Umwelt mit sich. Schutzbedürfnisse adressieren hier die notwendige hohe **Betriebssicherheit (safety)** bezüglich der physischen und rechtlichen Sicherheit der betroffenen Menschen und Umgebung.

Nun existieren **Bedrohungen**, die ein gewisses Risiko bewirken, dass die korrekte Funktion beeinträchtigt wird. Zur Erfüllung der Schutzbedürfnisse der Anwender sind deshalb mittels *Risikoanalyse* die Bedrohungen als potentielle Risiken zur Verletzung der Schutzbedürfnisse, die Risikoauswirkungen beim Eintreten sowie die Wahrscheinlichkeiten des Eintretens zu bewerten, um nachfolgend die notwendigen Anforderungen und Maßnahmen abzuleiten.

Dazu werden auf Basis der Use Case-Analyse messbare **Risikoauswirkungs-Kategorien** formuliert und mittels Risikobewertung zur Ableitung von **Schutzzielen** untersucht. Die Formulierung von Schutzzielen erfolgt dabei mit der Festlegung von **Sicherheitsniveaus (security level)** auf Basis der Bewertung von **Risikoauswirkungs-Niveaus** sowie von **Eintrittswahrscheinlichkeiten**.

Die mit der Risikoanalyse bestimmten Sicherheitsniveaus gehen in die nachfolgende Analyse der **Schutzanforderungen (protection requirements)** an Sicherheitsarchitekturen zur Gewährleistung der Schutzziele ein. Die **Schutzanforderungen der Anbieter** im Energiesystem können hierbei in die drei nachfolgenden Klassen eingeordnet werden:

- Regeln für Netz und Markt,
- Regeln an die Energietechnik sowie
- Schutzanforderungen an die Informations- und Kommunikationstechnik (IKT).

Mit dem ersten Punkt werden Schutzanforderungen zur Gewährleistung von Versorgungssicherheit durch technische und betriebswirtschaftliche **Regeln im Netz und Markt** definiert und umgesetzt. Sie sichern den Fluss an benötigter Energie. Diese Regeln stehen in dieser Betrachtung nicht weiter im Fokus.

Zweitens sorgen hier auch nicht weiter betrachtete **Regeln an die Energietechnik** dafür, dass das Schutzbedürfnis Betriebssicherheit gewährleistet wird. Dazu gehören funktionale Anforderungen an energietechnische Geräte und Anlagen sowie Transporteinrichtungen zur Sicherstellung der menschlichen Unversehrtheit im Betrieb der jeweiligen Einrichtungen.

Auf Basis der Schutzbedürfnisse Betriebssicherheit und Versorgungssicherheit ergeben sich drittens **Schutzanforderungen an die IKT**. Insbesondere diese Anforderungen werden mittels Schutzmethodik zur Smart Grid Informationssicherheit (SGIS) bestimmt.

Schutzanforderungen adressieren einerseits den **Betriebsschutz (security)** zur Sicherung der Verfügbarkeit und der Funktionalität des IKT-Betriebes. Anderseits handelt es sich auch um Anforderungen zum Schutz der Privatsphäre von Personen sowie von Geschäftsgeheimnissen rechtlicher Entitäten unter der Bezeichnung **Datenschutz (privacy, business secrets protection)**. Beide Anforderungskategorien unterstützen sowohl Betriebssicherheit des Energiesystems zur Minimierung des Einflusses auf Mensch und Umwelt als auch Versorgungssicherheit zur Sicherung der Energieflüsse. Aus der Schutzanalyse folgen somit Schutzanforderungen an die IKT zum Betriebsschutz und Datenschutz sowohl für die Ziele zur Versorgungssicherheit als auch für die Ziele zur Betriebssicherheit.

Der **Betriebsschutz** umfasst die Anforderungen an die IKT zur Sicherung der Verfügbarkeit und der robusten Funktionalität, um den Schutz der die energietechnischen Komponenten vernetzenden IKT-Systeme gegenüber Störungen und Angriffen zu gewährleisten. Unter Störungen werden hier ungeplante Fehlfunktionen von IKT-Systemen durch Hardwareausfälle, Softwarefehler oder menschliche, nicht vorsätzliche Fehlbedienungen verstanden, während Angriffe das vorsätzliche Verhalten von Menschen gegenüber den Systemen anderer Menschen beschreiben. Informationstechnische Angriffe können dazu gestartet werden,

- um Systemnutzern körperlichen Schaden durch beispielsweise elektrische Einwirkung oder technische Schäden zu bereiten (betrifft Schutzziele zur Betriebssicherheit)
- die Energielieferung durch Erzeugung eines Blackouts zu behindern (betrifft Schutzziele zur Versorgungssicherheit)

Dem **Datenschutz** zum Schutz der Privatsphäre und der Geschäftsgeheimnisse ist in besonderer Weise durch die zunehmende informations- und kommunikationstechnische Vernetzung im intelligenten Energiesystem Aufmerksamkeit zu widmen.

Verletzungen des Datenschutzes können dazu genutzt werden,

- um mit dem vernetzten System die persönlichen Grenzen des Menschen oder die Grenzen des Unternehmens durch den nicht ordnungsgemäßen Umgang mit den schützenswerten Informationen zu verletzen (betrifft Schutzziele zur Betriebssicherheit)

- oder durch Nichtbeachtung der Datenhoheit und durch Identitätsdiebstahl mit falscher Authentifizierung eine nicht ordnungsgemäße Versorgung zu initiieren (betrifft Schutzziele zur Versorgungssicherheit)

Datenschutz geht also der Frage nach, wie die missbräuchliche Datenverarbeitung gegen die Interessen der betroffenen Personen und Unternehmen verhindert werden kann.

Mit **Datenschutzklassen** werden Anforderungen für bestimmte Rollen gruppiert (siehe auch **Protection Profiles**), um hiermit die abzuleitenden Schutzmaßnahmen rollen- und funktionsabhängig definieren zu können.

Mit der Analyse der **Schutzmaßnahmen (protection measures)** auf Basis von Schutzanforderungen im Betriebsschutz und Datenschutz ergeben sich in drei Kategorien mit

- Datenschutzmaßnahmen,
- Informationssicherheit,
- IKT-Verlässlichkeit.

Auf der einen Seite wird die Einhaltung der Anforderungen zum Betriebsschutz durch Maßnahmen zur IKT-Verlässlichkeit und zur Informationssicherheit gewährleistet. Mit den zur Bestimmung von Betriebsschutzanforderungen ermittelten **Sicherheitsniveaus** können notwendige Maßnahmen gruppiert und den jeweiligen Anforderungsniveaus zugeordnet und damit **Sicherheitsrichtlinien** festgelegt werden.

Anderseits folgen aus Anforderungen zum Datenschutz entsprechende Datenschutzmaßnahmen als auch Maßnahmen zur Informationssicherheit. Hier gilt es ebenso, den zu **Datenschutzklassen** definierten und in Schutzprofilen gruppierten Schutzanforderungen notwendige Maßnahmen entsprechend den jeweiligen Niveaus oder Profilen Schutzmaßnahmen zuzuordnen und diese in **Sicherheitsrichtlinien** zu bündeln (siehe auch Technische Richtlinie).

In **Sicherheitsrichtlinien** zu Datenschutzklassen zur Gewährleistung bestimmter **Datenschutzanforderungen** werden entsprechende **Datenschutzmaßnahmen (privacy and business secrets enhancing technologies)** als auch weitere unterstützende Maßnahmen zur **Informationssicherheit (information security)** eingeordnet.

Zu **Datenschutzmaßnahmen** gehören neben rechtlich-organisatorischen Maßnahmen für die Umsetzung von Datenschutz auch eine Reihe technischer Schutzmaßnahmen. Dies betrifft insbesondere Maßnahmen zur Sicherstellung von **Anonymität, Transparenz** und **Intervenierbarkeit**. Technische Datenschutzmaßnahmen umfassen dabei sowohl IKT-Maßnahmen sowie auch organisatorische und bauliche Maßnahmen.

Maßnahmen zur **Informationssicherheit** beschäftigen sich mit dem eigentlichen Schutz von in IKT-Systemen vorhandener Daten (Datensicherheit) und der Informationsflüsse zur Sicherstellung von Datenschutz, aber auch mit dem Schutz des Betriebes. Eine scharfe Trennung von Schutzmaßnahmen bezüglich der Schutzaspekte (Safety) sowie Sicherheitsaspekte (Security) ist sicherlich schwierig.

Zur Kategorie der Informationssicherheit gehören Maßnahmen zur Gewährleistung von **Vertraulichkeit (confidentiality)**, **Integrität (integrity)**, **Verfügbarkeit (availability)** und **Authentizität/Echtheit (authenticity)**. Folgerichtig bedienen sich auch die Anforderungen zum Datenschutz der Methoden der Informationssicherheit zusätzlich zu organisatorischen und weiteren technischen Maßnahmen.

In **Sicherheitsrichtlinien** zur Gewährleistung bestimmter **Betriebsschutzanforderungen** werden ebenso sowohl Maßnahmen zur Sicherstellung der **IKT-Verlässlichkeit (dependability)** sowie auch entsprechende, oben aufgeführte Maßnahmen zur **Informationssicherheit** eingeordnet.

Maßnahmen zur Verlässlichkeit, insbesondere zur Gewährleistung des Betriebsschutzes, zielen dabei auf die Steigerung der **Belastbarkeit (resilience)** eines Systems, die Minimierung der **Verwundbarkeit (vulnerability)** sowie die Erhöhung der **Zuverlässigkeit (reliability)**. Verlässlichkeit wird insbesondere unter dem Aspekt betrachtet, der dem Schutz von Mensch und Umwelt durch zuverlässigen Erhalt des Energiesystems als kritische Infrastruktur dient.

Für die Spezifikation der Maßnahmen zur Erfüllung der Schutzbedürfnisse im Energiesystem sind somit zuerst nachfolgende vier Schritte zu beschreiten.

Mit der im Schritt 1 durchgeführte *Use Case Analyse* erfolgte die Formulierung von Schutzbedürfnissen.

Die im Schritt 2 folgende *Risikoanalyse* ermittelt Bedrohungen, die die Schutzbedürfnisse verletzen können. Mit der Bestimmung des Auswirkungsgrades bei Verletzungen sowie der Eintrittswahrscheinlichkeit werden Schutzziele in Form zu gewährleistender Sicherheitslevel abgeleitet.

Schritt 3 widmet sich der *Analyse von Schutzanforderungen*, um Schutzziele einhalten zu können.

Dies ist wiederum im Schritt 4 die Grundlage, um die *Analyse von Schutzmaßnahmen* durchzuführen, deren Umsetzung die Einhaltung der Anforderungen gewährleistet.

Grundlage der Use Case-Analyse ist dabei die in der Use Case-Beschreibung definierte Komponentenarchitektur mit jeweils zugehörigen Funktionen und Schnittstellen. Das Sicherheitsniveau für Komponenten korrespondiert dabei mit der Zuordnung dieser Komponenten zu Domänen und Betriebszonen im Smart Grid Architekturmodell.

Die nachfolgende Gliederung der Komponenten in vier Kategorien (A bis D) sowie die Bezeichnung der Komponentengruppen folgen dem Ansatz des DKE-Arbeitskreises Terminologie „Smart Energy“.

Backendsysteme von Markt- und Netzakteuren sowie Endkunden	**D**: Schnittstelle für Zugriffe und Anwendungen vielfältiger **Nutzer** bei hohem Grad der Partizipation, Eigengestaltung, Planungshoheit und eigener Wertschöpfung auf Basis von Smart Data in Smart Cells und Smart Grids

Leitsysteme, Betriebsführungssysteme und Energiemanagementsysteme	**C**: Zellulare (virtuelle) Regelkreise für Energieaustausch, Flexibilität und Energieeffizienz
	• **Beobachtung**
	  ○ Funktionen zum Datenmonitoring zu Energieflüssen und sonstigen, beeinflussenden Parametern
	• **Analyse**
	  ○ Funktionen zur Datenverarbeitung, Wissensgenerierung (lernende Systeme) und Entscheidungsvorbereitung
	• **Steuerung**
	  ○ Funktionen zur Ableitung von Reaktionen und zum Versand über IIS zur Steuerung des Verhaltens gewünschter Assets

Digitalisierungssysteme (Sensorik / Aktorik, Kommunikation und Plattformen)	**B**: Infrastruktur-Informationssystem (IIS) als Digitalisierungsschale für Energieinfrastruktur
	• **B1:** Geschützte **Zugriffskomponenten** an den Assets für
	  ○ Datenerhebung mit Messeinrichtungen (Sensorik) und Datenreaktionen über Steuereinrichtungen (Aktorik)
	• **B2:** Geschützte **Kommunikationssysteme** zur Datenübertragung
	  ○ lokal in Energiezelle und im Weiterverkehr zwischen Zellen sowie zu Diensten in der Cloud
	• **B3: Basiskomponenten** (**Plattformen**) zur Datenverwaltung, Datensicherung und Datenbereitstellung
	  ○ lokal in Energiezelle sowie zur Nutzung durch Nachbarn und andere Markt- und Netzakteure in der Cloud

Energieassets	**A**: Physikalische (reale) Assets als Datenquellen der Energieinfrastruktur jeder Zelle
	• **Energiewandler** zur Generierung und Nutzung von Energie als
	  ○ Erzeuger, Speicher und Verbraucher
	• **Energienetze** zur Ermöglichung der Energieflüsse mit
	  ○ Transportkanälen und Netzbetriebsmitteln

Das Begriffsmodell basiert auf [Kießling, A., Arndt, S. (01/2021)].

1.2 Prozess zur Analyse und Erfüllung der Schutzbedürfnisse

Die Schutzmethodik zur Analyse und Erfüllung der Schutzbedürfnisse im intelligenten Energiesystem nutzt in nachfolgender Abbildung dargestellten Prozess mit sechs Arbeitsschritten.

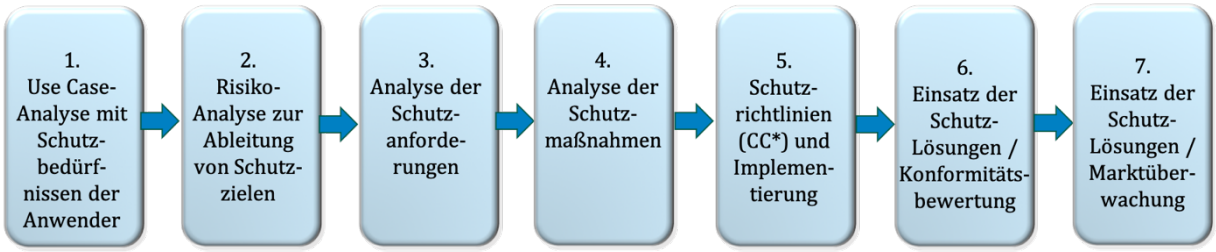

Abb. 2: Prozess der Schutzmethodik

1.2.1 Schritt 1 – Use Case-Analyse zur Ableitung von Schutzzielen

Schritt 1 der Schutzmethodik ist die Use Case-Analyse. Hierbei erfolgt die Untersuchung der mittels Use Case-Methodik beschriebenen Anwendungsfälle auf Schutzbedürfnisse der Anwender und mögliche Bedrohungen (Risiken zur Verletzung der Schutzbedürfnisse) für Anwender des Systems.

<u>Beispielliste für Schutzbedürfnisse und Bedrohungen</u>

(Listen sind je Use Case nach Bedarf zu erweitern)

Schutzbedürfnisse zur Versorgungssicherheit

- keine Störung der Energieversorgung in einer bestimmten Leistungshöhe in Watt
- keine Störung des Energieflusses über eine bestimmte Zeit in Watt pro Stunde
- keine Störung der Energieversorgung für eine bestimmte Bevölkerungsgröße (Bewohner der betroffenen Zelle)
- keine Störung weiterer Infrastrukturen

Schutzbedürfnisse zu Datenschutz und rechtlicher Sicherheit

- keine Verletzung des Datenschutzes
- keine Verletzung weiterer Gesetze und Regularien

Schutzbedürfnisse bezüglich Betriebssicherheit und Vertrauen

- keine Verletzungen und Unfälle durch den Betrieb des Energiesystems
- Hersteller oder Anbieter von Dienstleistungen wollen Vertrauensverlust vermeiden

Schutzbedürfnisse bezüglich finanzieller Sicherheit

- keinen finanziellen Verlust

Risiken zur Verletzung der Schutzbedürfnisse ergeben sich mit folgenden Beispielen zu Bedrohungen.

In der hier geführten Betrachtung werden ausschließlich Bedrohungen aus informations- und kommunikationstechnischer Sicht betrachtet. Bedrohungen durch Verletzung von Regeln (falsche Prozesse) oder von energetischen Komponenten (Assets) durch fehlerhafte Bauweise und absichtlich herbeigeführte technische Funktionsfehler der Assets sind hier ebenso wie Zerstörungen durch Naturkatastrophen (inkl. elektromagnetischer Strahlungsereignisse) nicht Bestandteil und somit gesondert mit der analogen Methodik zu untersuchen.

Bedrohungen bezüglich Verletzung der Schutzbedürfnisse

- **Vertraulichkeit (confidentiality)**: Unautorisierter Zugriff auf Informationen, d.h. Verletzung der Vertraulichkeit führt zur Verletzung des Datenschutzes und eventuell auch zu finanziellen Verlusten

- **Integrität (integrity)**: Unautorisierte Modifikation und Diebstahl von Informationen führt wiederum zur Verletzung des Datenschutzes, zum Verlust an Vertrauen und zu finanziellen Verlusten; kann aber mit Zugriffen auf Status- und Steuerungsdaten zu falscher Funktion oder zum Defekt von Assets des Elektrizitätssystems und davon abhängiger Infrastrukturen führen
- **Verfügbarkeit (availability)**: Dienstleistungsverhinderung oder die Verhinderung autorisierter Zugriffe (denial of services) kann die notwendige Bedienung von Assets verhindern sowie damit ebenso die korrekte Funktion des Elektrizitätssystems und davon abhängiger Infrastrukturen
- **Nicht-Abstreitbarkeit (repudiation)**: Verweigerung einer Aktion, die stattgefunden hat, oder Behauptung einer Aktion, die nicht stattgefunden hat (Bedrohung für die Rechenschaftspflicht), womit Vorgänge nicht bewiesen werden können und Schäden eventuell Gesetze und Regularien nicht ein
- **Verletzbarkeit (vulnerability)**: technische Ausfälle einer IKT-Komponente durch Defekt oder externe Einflüsse

Bedrohungen können durch folgende Akteure mit verschiedenen Eintrittswahrscheinlichkeiten ausgelöst werden (hier als Beispiele, kein Anspruch auf Vollständigkeit)**:**

- **Anwender** durch Fehlbetrieb oder Vandalismus
- **weitere Zugangsberechtigte** oder sich unerlaubt Zutritt verschaffende Personen vor Ort mit der Absicht zu Fehlbetrieb, Vandalismus oder Datendiebstahl
- **Mitarbeiter** externer Akteure durch fehlerhafte oder absichtliche Bedienung über Schnittstellen oder Datendiebstahl
- **Administratoren** externer Systeme durch fehlerhafte oder absichtliche Bedienung über Schnittstellen
- **Hacker**, die sich unerlaubt Zugang zu externen Systemen mit Schnittstellen zum Zielsystem oder direkt auf Zielsysteme zum Datendiebstahl oder zu unzulässiger Bedienung beschaffen
- **Terroristen**, die sich unerlaubt Zugang zu externen Systemen mit Schnittstellen zum Zielsystem oder direkt auf Zielsysteme zum Zwecke der Zerstörung verschaffen
- **IKT-Komponenten (technische Akteure)** erleiden Defekte durch Umwelteinflüsse oder durch den eigenen Ausfall

Grundlage zur Ermittlung der auf Use Cases bezogenen Schutzbedürfnisse und Bedrohungen ist die Kenntnis von

- Rollen mit verantwortlichen Akteuren
- zugehörige technische, legislative und regulatorische Rahmenbedingungen
- Komponenten mit Mapping auf die Komponentenarchitektur inklusive Zuordnung von Domänen und Zonen aus dem Smart Grid Architekturmodell sowie

Hierzu werden die entsprechenden Aufstellungen aus der Use Case-Beschreibung (Schritt 2 der Use Case Methodik, [C/sells – IOP Teil F. (03/2020)]) übernommen.

Rollen- und Akteursliste

Rollen	Verantwortlichkeiten (Übernahme von bestimmten Funktionen)	Akteure, die bestimmte Verantwortungen übernehmen (z.B. Individuen, Geräte, Anlagen, Softwaresysteme)	Schutzbedürfnisse
Anschlussnehmer	hat Anschlussvertrag mit Netzbetreiber bezüglich Bezugs- und Einspeiseleistungen	Betreiber von Erzeugungs- und Speichereinrichtungen sowie Betreiber oder Nutzer von Verbrauchseinrichtungen, deren **gemeinsamer Netzanschluss** im Quartier / Areal zeitweise gestört	Netzlösung, die Verbundenheit und Betrieb bei externen Störungen ermöglicht und damit

Rollen	Verantwortlichkeiten (Übernahme von bestimmten Funktionen)	Akteure, die bestimmte Verantwortungen übernehmen (z.B. Individuen, Geräte, Anlagen, Softwaresysteme)	Schutzbedürfnisse
		ist und hierfür Netzabschaltung, Netzweiterbetrieb und Wiederzuschaltung benötigen; müssen Netzverbindung zur Zuschaltung zwischen verschiedenen Betreibern herstellen lassen	Versorgungssicherheit erhöht
Verteilnetzbetreiber	natürliche oder juristische Personen oder rechtlich unselbständige Organisationseinheiten eines Energieversorgungs-unternehmens, die die Aufgabe der Verteilung von Elektrizität wahrnehmen	abschaltbarer und wiederzuschaltbarer Netzanschluss	erhalten sichere Netzabtrennung bei Netzausfall während Inselbetrieb sowie die Synchronisierung bei Aufhebung der Störung durch Signal vom VNB
Facility-Betreiber	Betreiber / Inhaber von Gebäudezelle mit verschiedenen technischen Ressourcen	Verbindung der Objekte von Betreibern von Erzeugungs- und Speichereinrichtungen sowie von Betreibern oder Nutzern von Verbrauchs-einrichtungen, um Notstrom-betrieb zu ermöglichen	Hausbetrieb mit höherer Versorgungssicherheit und evtl. finanzielle Anreiz für Systemdienstleistung im Quartier
…	…	…	…

Rahmenbedingungen (legislativ, regulatorisch und technisch):

Übernahme der Rahmenbedingungen aus der Use Case-Beschreibung zur Feststellung eventuell weiterer sicherheitsrelevanter Aspekte

Rahmenbedingungen (z.B. Datenschutz, Anschlussbedingungen, Zeitverhalten, Verfügbarkeit, Nutzergruppen, usw.)	Wirkung des Themas auf den Anwendungsfall	Verweise auf Gesetze und Regelungen
Gewährleistung von Datenschutz	Einsatz intelligenter Messsysteme	Digitalisierungsgesetz, Schutzprofil und techn. Richtlinie BSI
Gesetzliche und regulatorische Rahmenbedingungen	Beachtung der Netzampel, Koordinationsfunktion	EEG, EnWG, StromNEV
Messdatenbereitstellung in Echtzeit	aktuell nur über unzertifizierte iMSys	Weitere Zertifizierung von dazu notwendigen Tarifregistern in 2. Phase für Rollout Messsysteme
Steuerprozesse zu Anlagen	CLS-Kanal-Nutzung als aEMT: Übergabe des Steuerbefehls, Ausführen des Steuerbefehls, Übergabe von Statusinformationen, Interaktion mit GWA; CLS-Kanal-Management	Weitere dazu notwendiger Prozessspezifikationen in 2. Phase für Rollout Messsysteme im Rahmen der Normung in Verbindung mit BSI
Koordinationsrolle des Netzbetreibers	aktuell noch unklarer Rahmen	FNN-Position
…	…	…

Komponentenliste

Schutzbedürfnisse können durch Anwender (siehe Rollen) für Systeme oder Teilsysteme oder einzelne Komponenten definiert werden, die im Rahmen einer eventuellen Datenspeicherung sowie ihrer Funktionalitäten sowohl Aspekte der Versorgungssicherheit und der Betriebssicherheit betreffen.

Deshalb ist aus der Use Case-Beschreibung die Komponententabelle zu übernehmen (hier nur eine beispielhafte Aufführung von Komponenten).

Den Komponenten sind danach auf Basis der Betrachtung benötigter Funktionen Schutzbedürfnisse hinzuzufügen. Die weitere Detaillierung ist im Rahmen eines Zertifizierungsprozesse zum Informationssicherheits-Management vorzunehmen.
Der Fokus liegt dabei auf informationstechnischen und nicht auf elektrotechnischen Anforderungen.

Das Begriffsmodell der Kategorisierung von Komponenten (Kategorien A, B1 bis B3, C und D) basiert auf [Kießling, A., Arndt, S. (01/2021)].

Gliederung Komponenten in Kategorien A bis D **Komponenten** **Rolle des Betreibers**	**D: Domäne** **B: Betriebszone**	**Funktionen** **Schutzbedürfnisse**
A: Assets Verbraucher Anschlussnehmer, Konsument, Facility-Betreiber (EIV: Einsatzverantwortlicher)	D: Gebäude B: Prozess	Steuerbare Senke von Energieflüssen innerhalb der zwei Gebäude; Lieferung von Statusinformationen, Entgegennahme von Steueranweisungen (An/Aus); Betrieb von aEMT-Plattform und externem Energiemanagement-System darf nicht - den Assetbetrieb stören, - zu Beeinträchtigungen bei Endkunden führen, - nicht weitere Infrastrukturen des Endkunden stören, - Informationen zu Assets des Endkunden unerlaubt weitergeben, - zu Vertrauensverlusten gegenüber dem Betreiber führen und - zu keinen finanziellen Schäden beim Betreiber führen
…	…	…
B1: Sensorik / Aktorik Sensorik PV-Erzeugung und Batterieladezustand sowie Einzelverbräuche Anschlussnehmer, Prosument Facility-Betreiber (EIV: Einsatzverantwortlicher)	D: Gebäude B:Prozess	Messung der aktuellen PV-Einspeisung und des Ladezustandes der Batterie, um mögliche Maximallast für Gebäude zu bestimmen sowie Messung der Einzelverbräuche von Geräten und Anlagen im Gebäude, Übertragung Messwerte an GEMS; Daten dürfen nicht durch externe Akteure ermittelbar sein
B1: Sensorik / Aktorik moderne Messeinrichtung (mMe) Messstellenbetreiber (MSB)	D: Gebäude B: Feld	Messung und Erfassung der Energiedaten (Zweirichtungszähler als Hauptzähler am Netzanschluss sowie Einrichtungszähler Verbrauch für WP und für LP sowie Erzeugung PV-Anlage als auch Zweirichtungszähler für Batterie; Betrieb Plattform MSB soll nicht - zu Beeinträchtigungen der Messwerterfassung beim Endkunden führen, - Messung an weiteren Infrastrukturen des Endkunden stören, zu Verletzungen des Datenschutzes bezüglich der gemessenen Energieflüsse beim Endkunden führen,
…	…	…
C: Betriebskomponenten Energiemanagementsystem Energiedienstleister		**Betriebsfunktionen im Inselnetzbetrieb** …

Die Nutzung einer Abbildung zur Komponentenarchitektur auf Basis der SGAM-Komponentenebene ist hilfreich, die Verbindungen zwischen den genannten Komponenten zu verdeutlichen.

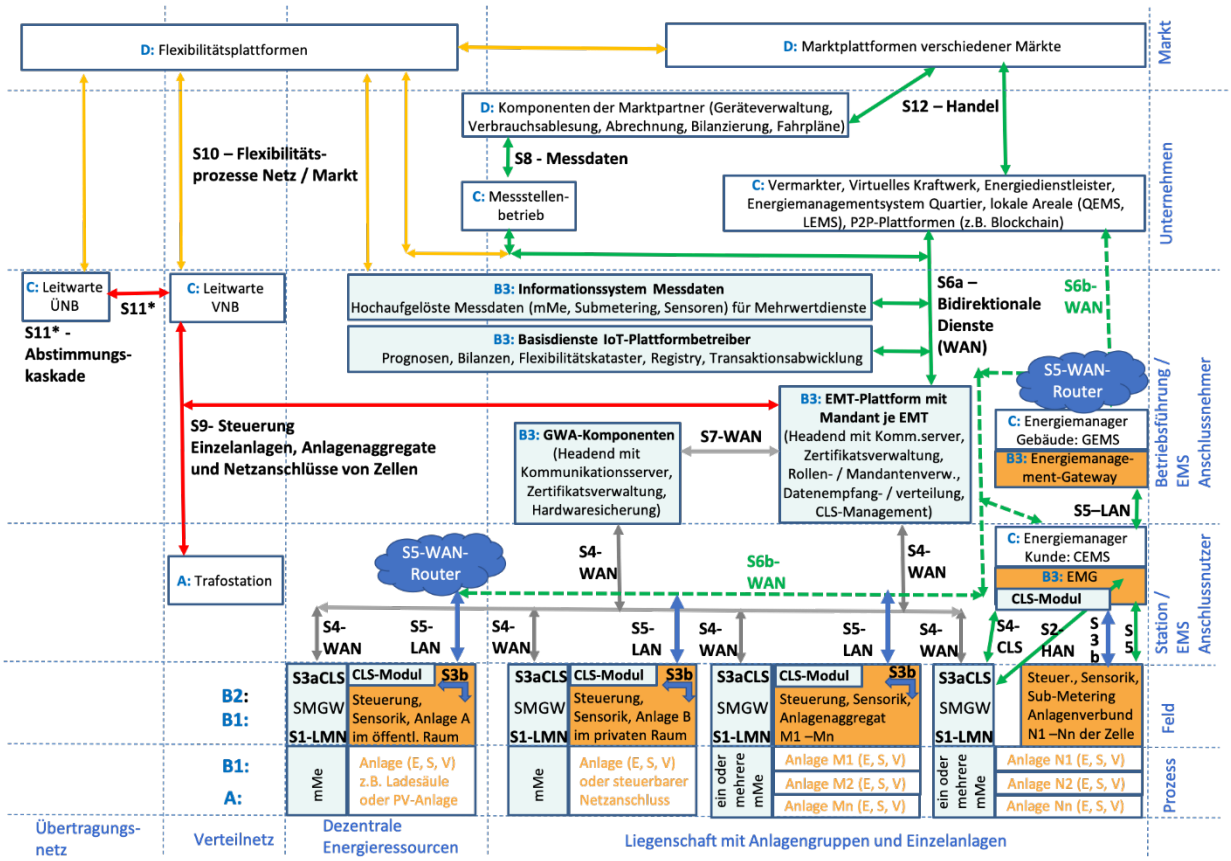

Abb. 3: Beispiel Komponentenarchitektur C/sells

1.2.2 Schritt 2 – Risikoanalyse auf Basis von Schutzzielen

Vorgehensweise

Die **Use Case-Analyse** formuliert zusätzlich zur gewünschten Funktion aus der Use Case-Beschreibung zugehörige **Schutzbedürfnisse**. Es geht darum, die korrekte Funktion zu schützen, also die Verfügbarkeit, den ordnungsgemäßen und ungefährlichen Ablauf sowie den Schutz der Daten zu gewährleisten.

Nun existieren verschiedene im Schritt 1 der Schutzmethodik – **Use Case Analyse** – zu ermittelnde **Bedrohungen**, die ein gewisses Risiko bewirken, dass die korrekte Funktion beeinträchtigt wird. Die möglichen Risiken, deren Auswirkungen sowie die Eintrittswahrscheinlichkeiten sind zu bewerten, um die notwendigen Anforderungen und Maßnahmen abzuleiten. Damit umfasst in Schritt 2 der Schutzmethodik die **Risikoanalyse**.

Die Risikoanalyse fügt den in der Use Case-Analyse ermittelten Schutzbedürfnissen mögliche Bedrohungen zu, die die Schutzbedürfnisse verletzen können.

Dabei werden zuerst den Schutzbedürfnissen bezüglich des Risikos ihrer Verletzung **messbare Risikoauswirkungs-Kategorien** sowie zugehörige **Risikoauswirkung-Niveaus** (**risk impact level**) zugeordnet. Es folgt die Bestimmung der **Eintrittswahrscheinlichkeit** (**likelihood**) einer Bedrohung mit dem Ergebnis einer bestimmten Risikoauswirkung.

Auf dieser Grundlage werden in Form von **Sicherheits-Levels** die **Schutzziele** bestimmt. Damit werden nur die Ziele benannt, aber noch nicht die dazu notwendigen **Schutzanforderungen** und **Schutzmaßnahmen**.

Verdeutlichen soll dies folgendes Beispiel:

- Die mittels Vorlage erstellte Use Case-Beschreibung umfasst die Vermarktung von Energie einer dezentralen Erzeugungsanlage auf dem Dach eines Gebäudes.

- Das mit der Use Case-Analyse erfasste Schutzbedürfnis seitens des Betreibers der Anlage besteht darin, dass diese Verbindung weder zu einer Unterbrechung des Betriebes der PV-Anlage für das Gebäude noch zu möglichen Verletzungen und Unfällen beim Betreiber führen dürfen.
- Mit der Use Case-Analyse werden weiterhin die möglichen Bedrohungen bei der Interaktion von Erzeugungsanlage und Energievermarkter festgestellt, die die obengenannten Schutzbedürfnisse verletzen können.
- Mit der Risikoanalyse wird das Schutzbedürfnis als messbare Risikoauswirkung-Kategorie formuliert – z.B. Ausfall PV-Anlage führt zu einer im Gebäude fehlenden Erzeugungsleistung.
- Dazu werden Risikoauswirkungs-Niveaus formuliert, die bestimmte quantitative und qualitative Grade der Auswirkung benennen (z.B. unterschiedliche Leistungs- oder Energieverluste).
- Am Schluss wird die Eintrittswahrscheinlichkeit abgeschätzt, dass z.B. ein Mitarbeiter beim Energievermarkter durch bewusste Fehlsteuerung den Einsatz der PV-Anlage korrumpiert.
- Risikoauswirkungs-Niveau und Eintrittswahrscheinlichkeit werden zu einem Sicherheits-Level zusammengefasst, dass als Schutzziel in den Folgeschritten Grundlage der Bestimmung von Schutzanforderungen und Schutzmaßnahmen ist.

Die das System nutzenden Akteure bestimmen mit dem Risikoauswirkungs-Niveau zuerst, in welcher Qualität eine bestimmte Bedrohung abzuwehren ist. Diese Qualität wird in die fünf Niveaus niedrig, mittel, hoch, kritisch und hoch kritisch gegliedert.

Die Bestimmung des Auswirkungsgrades erfolgt auf Basis der Zuordnung von Komponenten innerhalb der zum Use Case zugehörigen Systemarchitektur als Indikator für eine potentielle Einwirkung. Im zweiten Schritt werden die Gründe oder die Motivation zur Verletzung der Systemregeln bewertet und damit die Wahrscheinlichkeit des Eintrittes. Ein detailliertes Vorgehen kann aus [NIST SP 800-30] abgeleitet werden. Schlussendlich wird auf Basis dieser beiden Faktoren ein **Sicherheitsniveau** (**security level**) bestimmt, der das Schutzziel in Form eines bestimmten Grades vorgibt.

Die Vorgabe bestimmter Risikoauswirkungs-Niveaus und ihre Qualität ist abhängig vom Blickwinkel eines Akteurs, der die Auswirkungen möglicher Risiken für Versorgungs- und Betriebssicherheit einschätzt. Beispielsweise sind die nationalen oder sogar europäischen Risiken beim Ausfall mehrerer Kraftwerke aus Sicht eines Übertragungsnetzbetreibers mit einem höheren Risikoauswirkung-Niveau zu bewerten als beim Ausfall der PV-Anlage in einer Gebäudezelle.

Um hierzu eine strukturierte Betrachtung zu ermöglichen, werden zusammengehörige Auswirkungen auf die Versorgungs- und Betriebssicherheit definiert. Diese Auswirkungen werden für einen Use Case bezüglich der betroffenen Domänen und Zonen (siehe Use Case-Analyse) untersucht, in denen die zum System des Use Cases zugehörigen Komponenten installiert sind. Das Risikoauswirkungs-Niveau wird dann aus Sicht der Akteure innerhalb eines Use Cases betrachtet, wobei das dann von einem Akteur am höchsten eingeschätzte Niveau Grundlage für die weitere Risikoanalyse zur Bestimmung von Schutzzielen ist.

Wichtige Risikoauswirkungs-Kategorien:

Eine Risikoauswirkungs-Kategorie für Versorgungs- und Betriebssicherheit wird für die betriebliche Verfügbarkeit der Energieleistung gebildet.

In Abhängigkeit von der Domäne in der die Erzeugung stattfindet und transportiert wird (zentrale Erzeugung mit Übertragungsnetz, DER mit Verteilungsnetz und Liegenschaft mit privatem Netz) sowie der zugehörigen Zonen Prozess (stromerzeugende Anlagen) bis zur Betriebsführung werden unterschiedliche Risikoauswirkung-Niveaus dieser Klasse zugeordnet.

Beispielsweise werden dieser Kategorie in der Domäne zentrale Erzeugung und der zugehörigen Zone Prozess (stromerzeugende Anlagen) sowie auch in der Zone Betriebsführung folgende Risikoauswirkung-Niveaus zugeordnet.

- überregionale Netze mit Erzeugung über 10 GW → 5: hoch kritisches Auswirkungsniveau
- nationale Netze mit Erzeugung zwischen 1 und 10 GW → 4: (kritisches Auswirkungsniveau)
- Stadtnetze mit Erzeugung von 100 MW bis 1 GW → 3: hohes Auswirkungsniveau
- Nachbarschaftsnetze (Areale, Quartiere) von 10 – 100 MW → 2: mittleres Auswirkungsniveau
- Wohn- und Gebäudenetze unter 10 MW → 1: niedriges Auswirkungsniveau

Analoge Kategorien können nun auch für Schutzbedürfnisse der Versorgungs- und Betriebssicherheit zur betrieblichen Verfügbarkeit des Energieflusses (Leistung mal Zeit), für die Versorgung bestimmter Bevölkerungsdichten, für das Bestehen bestimmter anderer kritischer Infrastrukturen in Versorgungsgebieten gebildet werden.

Risikoauswirkungs-Kategorien sind aber auch für rechtliche Anforderungen der Anwender in bestimmten Regionen (Datenschutz, regulatorische Anforderungen) definierbar, aber auch Schutzbedürfnissen der durch Anlagen betroffenen Menschen, zum Erhalt von Vertrauen sowie bezüglich finanzieller Ziele.

Nachfolgende Tabelle umfasst dazu die Definition von fünf Risikoauswirkung-Niveaus sowie von neun Risikoauswirkungs-Kategorien [M490SE12 (07/2012)]. Die Kategorien messen, wie sich Sicherheitsverletzungen auf die Diensteverfügbarkeit auswirken. Weitere Kategorien können nach der IKT-Analyse der Use Cases bei Bedarf hinzugefügt werden, wobei die Bewertung nicht unbedingt die Fachspezialisten der Use Cases vornehmen können, sondern für eine zuverlässige Bewertung entsprechende Sicherheitsspezialisten benötigt werden.

Risikoaus-wirkung-Niveau risk impact level (	RA-Niveau auf Basis Größe und Typ Netz	RA-Niveau auf Basis Energie-fluss	RA-Niveau auf Basis betrof-fener Bevölke-rung	RA-Niveau auf Basis betrof-fener Infra-strukturen	RA-Niveau in Bezug zu Daten-schutz-direktiven	RA-Niveau auf Basis möglicher Strafen	RA-Niveau auf Basis Gefähr-dung Gesund-heit	RA-Niveau auf Basis Verlust an Vertrauen	RA-Niveau auf Basis direkter mone-tärer Verlust
hoch krtitisch	Trans-nationale Netze über 10GW	über 10GW/h	über 50% im Land über über 25% in mehreren Ländern	kritische Infra-strukt. betroffen in mehreren Ländern	noch keine Definition	Schlie-ßung od. Kollate-ralsch. bei Nicht-erfüllung	Direkte und höhere To-deszahlen in mehreren Ländern	alle Bereiche in mehreren Ländern betroffen	über 50% von EBITDA
kritisch	Nationale Netze von 1GW bis 10GW	von 1GW/h zu 10GW/h	von 25% bis 50% eines Landes	nationale, kritische Infra-strukt. betroffen	noch keine Definition	Betriebs-unter-brechung bei Nicht-erfüllung	Direkte und höhere To-deszahlen in einem Land	Perma-nent. Verlust in einem Land	von 33% zu 50% von EBITDA
hoch	Stadtnetze von 100MW bis 1GW	von 100MW/h zu 1GW/h	von 10% bis 25% eines Landes	essentielle Infra-strukt. betroffen	unautoris. Zugriff auf sensitive Daten	Gefängnis bei Nicht-erfüllung	Direkter Tod in einem Land	Tempo-rärer Verlust in einem Land	von 10% zu 33% von EBITDA
mittel	Nachbar-schafts-netze 1MW bis 100MW	von 1MW/h zu 100MW/h	von 2% bis 10% eines Landes	kostenlose Infra-strukt. betroffen	unautoris. Zugriff auf persönl. Daten	Geldstrafe bei Nicht-erfüllung	relevante Verletzung oder Behin-derung	Tempo-rärer Verlust in spezi-fischen Gebiet	von 1% zu 10% von EBITDA
niedrig	Wohn- oder Gebäude-netz unter 1MW	unter 1MW/h	unter 2% eines Landes	keine Infra-strukt. betroffen	keine persönl. od. sensitiven Daten	nur War-nungen bei Nicht-erfüllung	mindere Unfälle	Punktu-eller, tempo-rärer Verlust als Warnung	unter 1% von EBITDA

	Energie-versorgung (Leistung in W)	Energie-fluss (Leistung in Zeitdauer W/h)	Bevöl-kerung	Infra-strukturen	Daten-schutz	Andere Gesetze und Regularien	Menschen	Vertrauen	Finanzen
	Betrieblich				Gesetze				
	Schutzbedürfnisse (Schutzanforderungen Systemanwender) –> Messbare Risikoauswirkungs-Kategorien								

Tabelle 1: Risikoauswirkungs-Kategorien sowie zugehörige Bewertungsmöglichkeiten (Risikoauswirkungs-Niveau)

Insofern ist die Bestimmung des Risikoauswirkungs-Niveaus für einen Use Case in einer dieser Kategorien ein nicht eindeutig definierter Ausgangspunkt für die weitere Bewertung. Die Verfügbarkeit des Energieflusses vom Übertragungsnetz in ein Verteilnetz hat in einer Stadt mit geringer dezentraler Erzeugung bei hoher Bevölkerungsdichte und militärischen Standorten eine höhere Bedeutung als im Verteilnetz einer ländlichen Kleinstadt mit hohem Anteil eigener dezentraler Erzeugung. Das heißt, das höhere Niveau der Risikoauswirkung in der Spalte Bevölkerung gegenüber dem Niveau in der Spalte Energieversorgung bestimmt den Gesamtwert des Risikoauswirkung-Niveaus.

Auf dieser Grundlage sind zur Risikobewertung zum Schritt 2 der Use Case-Beschreibung zu entnehmen

- einerseits vollständig die Komponenten und benötigten Hauptfunktionen,
- sowie anderseits in der Tabelle zu den Rahmenbedingungen
  - Informationen zu Leistungen und Energiemengen,
  - zur Bevölkerung der betroffenen Zelle,
  - Angaben zu versorgenden, kritischen Infrastrukturen (z.B. Flughafen),
  - zu Datenschutz und regulatorischen Rahmen,
  - zur Gefährdungen für den Menschen bezüglich vorgesehener Komponenten,
  - aber auch evtl. zu weichen Faktoren wie Vertrauen und zu wirtschaftlichen Zielen.

Hieraus kann die Risikoauswirkungs-Tabelle analog abgeleitet werden. Zu bemerken ist aber auch Folgendes. Wie ausgeführt sind die Risikoauswirkungs-Kategorien in Abhängigkeit vom Use Case zu betrachten. Das Vorgehen bezogen auf überschaubare Use Cases hilft, die Komplexität der Risikoanalyse zu beherrschen. Hier können aber im zellularen System unterschiedliche Sichten der jeweiligen Akteure in den Zellen entstehen. Insofern ist die Risikoauswirkungs-Tabelle eventuell je nach Zelltypen, in denen der Use Case wirkt, um zusätzliche Kategorien zu erweitern.

Nun ist als zweiter Faktor die **Eintrittswahrscheinlichkeit** zu bestimmen. Die Wahrscheinlichkeit ist bezüglich des Angriffes auf die Kommunikation zwischen jeweils zwei Komponenten zu betrachten und dabei für unterschiedliche angreifende Akteure einzuschätzen. Dies wird mit nachfolgender Tabelle anhand eines Use Case-Beispiels für die Interaktion zwischen VNB-Einspeisemanagement und Energiemanagement eines Gebäudes veranschaulicht. Die Bildung von Gruppen potentieller Angreifer basiert wiederum auf [SEG-CG/CSP (12/2016)]. Grundsätzlich ist die Eintrittswahrscheinlichkeit für jede der in der Einleitung zur Use Case-Analyse genannten Bedrohungen zu bestimmen. Angewendet wird für die nachfolgende Bestimmung des Sicherheitslevels dann die jeweils höchste Eintrittswahrscheinlichkeit.

	vom Energiemanagement des Gebäudes zum VNB-Einspeisemanagement	vom VNB-Einspeisemanagement zum Energiemanagement des Gebäudes
unehrlicher Administrator	extrem hoch	sehr hoch
unehrlicher Beschäftigter (normaler Nutzer)	hoch	mittel

mit Vandalismus agierende Akteure	hoch	niedrig
Hacker	sehr hoch	mittel
Terrorist	mittel	sehr hoch

Tabelle 2: Bestimmung von Eintrittswahrscheinlichkeiten für Gruppen von potentiellen Angreifern

Die Kombination von Risikoauswirkungs-Niveau zwischen 1 und 5 und Grad der Eintrittswahrscheinlichkeit zwischen 1 und 5 ist Grundlage der Bestimmung des Sicherheitsniveaus (security level), die durch Addition mit Werten zwischen 2 bis 10 berechnet werden.

In nachfolgendem Beispiel, wo das Risikoauswirkungs-Niveau aus Sicht des VNB mit 4 und die höchste Eintrittswahrscheinlichkeit in der Stufe 5 bestimmt wurde, ergibt sich mit der Addition beider Werte das Sicherheitsniveau 9.

		Eintrittswahrscheinlichkeit (likelihood)				
		1: niedrig	2: mittel	3: hoch	4: sehr hoch	5: extrem hoch
Risiko-auswirkung-Niveau (risk impact level)	5: hoch krtitisch	6	7	8	9	10
	4: kritisch	5	6	7	8	9
	3: hoch	4	5	6	7	8
	2: mittel	3	4	5	6	7
	1: niedrig	2	3	4	5	6
		1	2	3	4	5
		Sicherheitsniveau (security level) und Datenschutzklassen				

Tabelle 3: Bestimmung der Sicherheits-Niveaus (security level)

Das Schutzziel für einen Use Case aus Sicht eines Systemanwenders wird somit über den Sicherheits-Level definiert.

Die bestimmten Schutzziele basieren im Rahmen der Risikoanalyse

- auf einer bestimmten Bedrohungslage in einem Use Case, also auf bestehenden Risiken,
- deren Eintreten zu bestimmten Auswirkungen (Risikoauswirkungs-Niveaus) führen kann
- sowie denen Eintrittswahrscheinlichkeiten auf Basis bestimmter Ursachen zugeordnet werden,
- um das Eintreten mit einer bestimmten Priorität zu verhindern.

Ein Schutzziel drückt also aus, mit welcher Qualität die Bedrohungen für definierte Schutzbedürfnisse abgewehrt werden sollen. Es benennt das Ziel, aber noch nicht die dazu notwendigen Anforderungen und Maßnahmen.

1.2.3 Schritt 3 - Bestimmung von Schutzanforderungen

Vorgehensweise

Die für Use Cases definierten Schutzziele und die resultierende Risikobewertung mit der Bestimmung von Risikoauswirkung-Niveaus, Eintrittswahrscheinlichkeiten sowie resultierenden Sicherheitsniveaus ist Grundlage für Schritt 3 der Schutzmethodik zur Ableitung von Schutzanforderungen.

Es sind Anforderungen zur Spezifikation technischer Details für alle Komponenten und Akteure in allen Domänen, Zonen und Ebenen eines Architekturmodells, in denen die betrachteten Use Cases wirken, zu spezifizieren. Grundlage für diesen Prozess sind existierende Sicherheitsstandards oder anderweitige technische und organisatorische Richtlinien.

Hier im Fokus befinden sich auf Basis der Schutzziele Betriebssicherheit und Versorgungssicherheit die **Schutzanforderungen an die IKT**. Hierbei handelt es sich einerseits um Anforderungen, die den **Betriebsschutz**

zur Sicherung der Verfügbarkeit und der Funktionalität des IKT-Betriebes adressieren. Anderseits handelt es sich auch um Anforderungen zum **Datenschutz** bezüglich der Sicherung der Privatsphäre von Personen sowie von Geschäftsgeheimnissen rechtlicher Entitäten. Beide Anforderungskategorien unterstützen sowohl Betriebssicherheit des Energiesystems zur Minimierung des Einflusses auf Mensch und Umwelt als auch Versorgungssicherheit zur Sicherung der Energieflüsse.

Nicht im Fokus sind im Rahmen dieser Methodik technische und betriebswirtschaftliche **Regeln im Netz und Markt** zur Gewährleistung von Versorgungssicherheit, aber auch nicht die **Regeln an die Energietechnik** zur Sicherstellung der Betriebssicherheit.

Zur strukturierten Erfassung von Schutzanforderungen können entsprechende Anforderungs-Standards oder rechtliche Anforderungs-Richtlinien genutzt werden. Dabei wird zwischen organisatorischen und technischen Anforderungen unterschieden. Die in einem späteren Schritt der Schutzmethodik beschriebene Spezifikation von Schutzmaßnahmen zur Erfüllung der Schutzanforderungen gliedert sich ebenso in organisatorische und technische Maßnahmen. Nachfolgende Abbildung mit vier Quadranten zu Anforderungen und Maßnahmen sowie zugehörigen beispielhaften Inhalten verdeutlicht das Vorgehen.

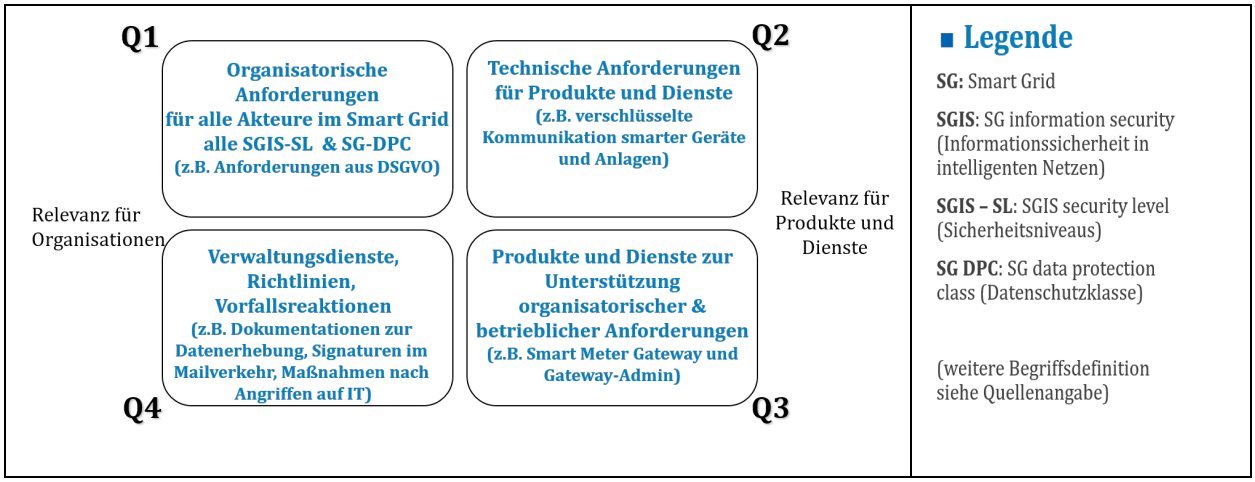

Abb. 4: Schutzanforderungen und Schutzmaßnahmen für Organisation und Technik, [SEG-CG/CSP (12/2016)]

Auf Basis der bestimmten Sicherheitsniveaus soll nun festgestellt werden, welche Schutzanforderungen sich an die Organisation und die Technik ergeben.

Ergab also die Risikoanalyse, dass keine persönlichen Daten, aber betriebliche Daten erhoben werden, sind keine entsprechenden organisatorischen Anforderungen zur Erhebung persönlicher Daten festzulegen. Die Anforderungs-Richtlinien der DSGVO wäre hier also nicht relevant. Trotzdem ergeben sich organisatorische Anforderungen auf Basis von Standards, die betriebliche Daten schützen, wobei diese Anforderungen in Abhängigkeit vom Risiko-Auswirkungsniveau variieren können. Unterstützt werden damit sowohl Schutzziele zur Betriebssicherheit (bei Zugriff auf betriebliche Daten eines Betreibers einer Erzeugungsanlage können falsche Informationen an den Markt übersendet werden und damit finanzielle Schäden für den Betreiber entstehen) als auch Schutzziele zur Versorgungssicherheit (bei Zugriff auf betriebliche Daten können falsche Bilanzierungsinformationen übersendet werden, was zu finanziellen Verlusten beim Betreiber bis hin bei großflächigen Angriffen zum Marktversagen führen kann).

Analog sind die technischen Anforderungen abzuleiten. Da z.B. eine Erzeugungsanlage mit einem Einspeisemanagementsystem des VNB interagiert und somit das entsprechend hohe Sicherheitsniveau abgeleitet wurde, ergeben sich besondere Anforderungen an eine verschlüsselte, authentifizierte und unveränderbare Kommunikation.

Ebenso wie Risikoauswirkungs-Kategorien bezüglicher der Schutzziele gebildet wurden, ergeben sich aus den Anforderungs-Standards entsprechende Bündel von organisatorischen und technischen Schutzanforderungen.

Die wichtigsten Normenreihen zur Ableitung der Schutzanforderungen (Was ist zu schützen?) umfasst nachfolgende Liste.

- ISO/IEC 27001 [10]: Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002 [11]: Information technology — Security techniques — Code of practice for information security management ISO/IEC TR 27001
- ISO/IEC TR 27019 [12]: Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- IEC 62443-2-4 [13]: Security for industrial automation and control systems – Network and system security – Part 2-4: Requirements for Industrial Automation Control Systems (IACS) solution suppliers
- IEC 62443-3-3 [14]: Security for industrial automation and control systems, Part 3-3: System security requirements and security levels
- IEC 62443-4-2 [15]: Security for industrial automation and control systems, Part 4-2: Technical Security Requirements for IACS Components
- IEEE 1686 [16]: Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities Smart Energy Grid Coordination Group Cyber Security and Privacy
- IEEE C37.240 [17]: Cyber Security Requirements for Substation Automation, Protection and Control Systems

Informationsobjekte und Kommunikationsanforderungen

Schutzanforderungen sind abhängig vom Wirkungsort installierter Komponenten (siehe Komponententabelle) und ihrer Schnittstellen sowie den dabei übertragenen Daten. Insofern ist die Übernahme und Betrachtung der Tabellen zu Informationsobjekten und zu Kommunikationsanforderungen aus der jeweiligen Use Case-Beschreibung (Schritt 2 der Use Case Methodik, [Kießling, A., Bogensberger, A., Köppl, S. & Faller, F. (03/2020)]) Grundlage der Ableitung von Schutzanforderungen.

Dabei sind zuerst zur Festlegung von Datenschutzklassen die im Use Case benötigten Daten zu klassifizieren. Dies erfolgt im Rahmen der zum Use Case ermittelten Informationsobjekte, d.h. von gespeicherten und im Rahmen von Nachrichten zwischen Akteuren ausgetauschten Daten.

Informationsobjekt	Teilobjekte	Inhalte	Schutzbedürfnisse und Datenklassifizierung
Steuerdaten	Wiederverbindungs-Signal	Einschaltsignal nach Störungsende	Zugriff auf und Manipulation von Steuerdaten verhindern, um die korrekte Funktion zu sichern sowie den persönliche Daten zu schützen → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betrieb-liche Daten, persönliche Daten
Messdaten	Leistungsgänge	Leistung Zeit	Zugriff auf und Manipulation von Messdaten verhindern, um die korrekte Funktion zu sichern sowie den persönliche Daten zu schützen → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
…	…	…	…

Im Weiteren sind die zum Use Case definierten Kommunikationsanforderungen zu betrachten. Untersucht wird, welche Daten von welchen Komponenten auf welche Weise ausgetaucht werden, um hierzu informationstechnische Schutzanforderungen hinzuzufügen (nachfolgend nur beispielhaft).

Kommunikationsschnittstelle			**Inhalt der Nachricht**	**Schutzanforderungen**
Von	Bis	**Schnitt-stelle**		
mMe SMGW	SMGW mMe	**S1**	Messdaten Energie und Leistung für Markt sowie Zählerstandsgänge Messdaten Netzqualität Konfigurationsdaten	definiert über BSI-Schutzprofil
SMGW HAN EMG	EMG SMGW CLS	**S2**	Messdaten mMe lokal vom SMGW an EMG Messdaten von Sub-Metering, Planungsdaten, Statusinformationen, Marktdaten	SMGW transportiert Daten von mMe's sicher über HAN-Schnittstelle an GEMS Messdaten vom GEMS (Sub-Metering) mit Nutzung und Abschluss des sicheren, transparenten Kommunikationskanals über SMGW
SMGW CLS CLS-Modul	CLS-Modul SMGW CLS	**S3a**	**Verschlüsselter und signierter Payload mit beliebigen Daten;** Kommunikationsdaten	Nutzung und Abschluss des sicheren, transparenten Kommunikationskanals über SMGW
CLS-Modul als Teil Steuerbox, Anlage oder EMG	Sub-Metering, Sensorik,	**S3b**	Anforderung Messdaten Sub-Metering, Messdaten und Status der Geräte, Anlagen sowie von Umwelt; Kommunikationsdaten	Nutzung und Abschluss des sicheren, transparenten Kommunikationskanals über SMGW
Komponente Leitwarte Flexibilitäts-prozesse	Flexibilitäts-plattform	**S10**	Planungs- und Marktdaten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen Netzpartnern außerhalb BSI-Schutzprofil; Unverfälschbarkeit der Flexibilitätsdaten sicherstellen, um Rückwirkung auf Netzbetrieb zu verhindern
Komponente Leitwarte Abstimmungs-kaskade VNB	Komponente Leitwarte Abstimmungs-kaskade ÜNB	**S11**	Planungsdaten, Steuerdaten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen Netzpartnern außerhalb BSI-Schutzprofil; Unverfälschbarkeit der Abstimmungsdaten sicherstellen, um Rückwirkung auf Netzbetrieb zu verhindern
Komponenten Energieliefer. Energiehandel	Marktplatt-formen	**S12**	Planungsdaten, Marktdaten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen Marktpartnern außerhalb BSI-Schutzprofil; Unverfälschbarkeit der Marktdaten (Handel, Fahrpläne, Abrechnungen, Transaktionen) sicherstellen

1.2.4 Schritt 4 - Bestimmung von Schutzmaßnahmen

Vorgehensweise

Folgender Prozess wurde bisher beschrieben.

Mit der im Schritt 1 durchgeführte **Use Case Analyse** erfolgte die Formulierung von Schutzbedürfnissen.

Die im Schritt 2 folgende **Risikoanalyse** ermittelt Bedrohungen, die die Schutzbedürfnisse verletzen können. Mit der Bestimmung des Auswirkungsgrades bei Verletzungen sowie der Eintrittswahrscheinlichkeit werden Schutzziele formuliert.

Schritt 3 widmet sich der **Analyse von Schutzanforderungen**, um Schutzziele einhalten zu können.

Dies ist wiederum im Schritt 4 die Grundlage, um entsprechende **Schutzmaßnahmen** festzulegen, deren Umsetzung die Einhaltung der Anforderungen gewährleistet.

Schutzmaßnahmen (protection measures) auf Basis von Schutzanforderungen im Betriebsschutz und Datenschutz sind in folgenden drei Kategorien abzuleiten:

- Datenschutzmaßnahmen,
- Informationssicherheit,
- IKT-Verlässlichkeit.

Die Einhaltung der Anforderungen zum Betriebsschutz wird durch Maßnahmen zur IKT-Verlässlichkeit und zur Informationssicherheit gewährleistet. Maßnahmen zur Verlässlichkeit zielen dabei auf die Steigerung der Belastbarkeit (resilience) eines Systems, die Minimierung der Verwundbarkeit (vulnerability) sowie die Erhöhung der Zuverlässigkeit (reliability). Verlässlichkeit wird insbesondere unter dem Aspekt betrachtet, der dem Schutz von Mensch und Umwelt durch zuverlässigen Erhalt des Energiesystems als kritische Infrastruktur dient.

Maßnahmen zur Informationssicherheit dienen dem Schutz von in IKT-Systemen vorhandener Daten (Datensicherheit) und der Informationsflüsse. Sie unterstützen sowohl die Anforderungen an den Betriebsschutz als auch die Sicherstellung von Datenschutz. Zur Kategorie der Informationssicherheit gehören Maßnahmen zur Gewährleistung von Vertraulichkeit (confidentiality), Integrität (integrity), Verfügbarkeit (availability) und Authentizität/Echtheit (authenticity).

Der Erfüllung der Anforderungen zum Datenschutz dienen wiederum die Datenschutzmaßnahmen als auch die Maßnahmen zur Informationssicherheit. Hier gilt ebenso, dass mit den zu Datenschutzanforderungen genannten Datenschutzklassen notwendige Maßnahmen gruppiert und den jeweiligen Niveaus der Datenschutzanforderungen zugeordnet und damit Sicherheitsrichtlinien werden können.

Zur Erfüllung der Anforderungen zum Schutz persönlicher Daten oder betrieblicher Geheimnisse werden entsprechende Datenschutzmaßnahmen (privacy and business secrets enhancing technologies) als auch weitere unterstützende Maßnahmen zur Informationssicherheit (information security) definiert. Zu Datenschutzmaßnahmen gehören neben rechtlich-organisatorischen Maßnahmen für die Umsetzung von Datenschutz auch eine Reihe technischer Schutzmaßnahmen. Dies betrifft insbesondere Maßnahmen zur Sicherstellung von Anonymität, Transparenz und Intervenierbarkeit. Technische Datenschutzmaßnahmen umfassen dabei sowohl IKT-Maßnahmen sowie auch organisatorische und bauliche Maßnahmen.

Die wichtigsten Normenreihen zur Ableitung der Schutzmaßnahmen (Wie ist zu schützen?) umfasst nachfolgende Liste.

- ISO /IEC 15118: Road vehicles – Vehicle-to-Grid Communication Interface, Part 8 [18]: Physical and data link layer requirements for wireless communication
- ISO / IEC 61850-8-2 [19]: Communication networks and systems for power utility automation - Part 8-2: Specific communication service mapping (SCSM) - Mapping to Extensible Messaging Presence Protocol (XMPP)

- IEC 62351-x [20] Power systems management and associated information exchange – Data and communication security
- IEC 62743 [21] Industrial communication networks – Wireless communication network and communication profiles - ISA 100.11a
- IETF draft-weis-gdoi-iec62351-9: IEC 62351 Security Protocol support for the Group Domain of Interpretation (GDOI) [22]
- IETF draft-TLS1.3 TLS Version 1.3 [25]
- Leitfaden für Informationssicherheits-Maßnahmen für Prozesssteuerungssysteme der Energieversorgung auf Grundlage der DIN ISO/IEC 27002 (Management)
    - Basis ist Standard DIN ISO/IEC 27002:2008 "Leitfaden für das Informationssicherheits-Management“
    - Erweiterung im DIN ISO/IEC 27009 mit Umsetzungsanleitungen zur Realisierung von Informationssicherheits-Maßnahmen im Rahmen eines Informationssicherheits-Managements für Prozesssteuerungssysteme der Energieversorgung.
    - Scope auf Prozessleit- und Automatisierungstechnik der Energieversorgung, um die Implementierung eines einheitlichen Informationssicherheits-Managementsystems (ISMS) auf Basis des Standards DIN ISO/IEC 27001:2008 (Anforderungen) von der Geschäfts- bis hin zu Prozessebene, zu ermöglichen.
    - Betrifft „Prozesssteuerungssysteme“ mit Systemen und Netzwerken zur Steuerung und Überwachung von Erzeugung, Übertragung und Verteilung von Strom, Gas und Wärme in Kombination mit der Steuerung von unterstützenden Prozessen. Dies umfasst die Leit- und Automatisierungssysteme, die Schutzsysteme sowie die Messtechnik inklusive der zugehörigen Kommunikations- und Fernwirktechnik.
    - Bezüglich Telekommunikationssysteme und Nachrichtentechnik im Umfeld der Prozesssteuerung Verweis auf Standard ISO/IEC 27011 „Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002:2005“

Nachfolgendes Beispiel gibt einen Überblick zum Zusammenhang von Bedrohungen, den aus IKT-Schutzzielen resultierenden Schutzanforderungen bezüglich Vertraulichkeit, Integrität, Verfügbarkeit und Nicht-Zurückweisbarkeit sowie einer Menge von Maßnahmen und des zugehörigen Sicherheitsmanagements.

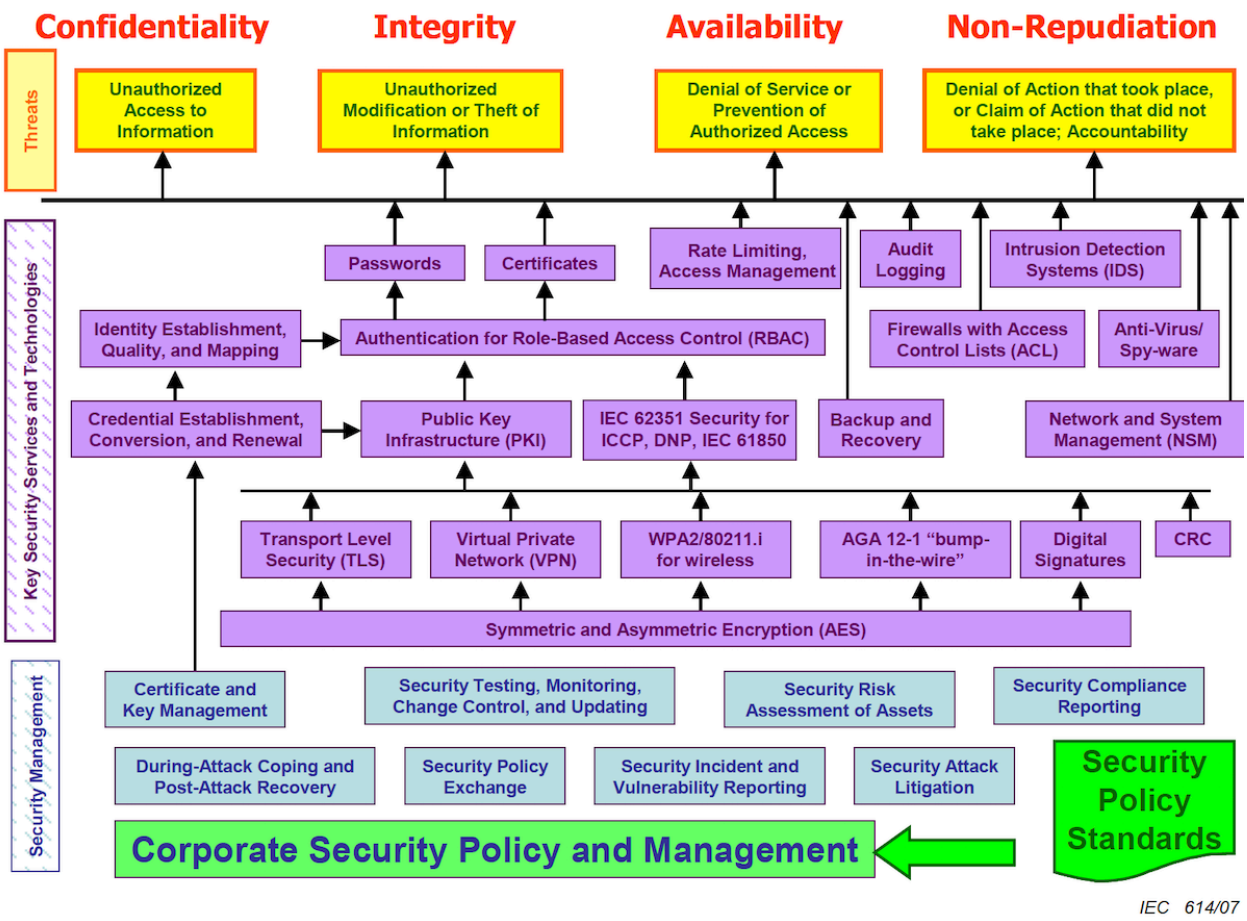

Abb. 5: Sicherheitsanforderungen, Bedrohungen, Gegenmaßnahmen und Management [Quelle: IEC 62351-1]

Schnittstellenliste und grundlegende Sicherheitsanforderungen (Beispiele)

Schutzmaßnahmen sind an jeder auszuprägenden Schnittstelle zwischen Komponenten zu definieren. Hierzu wird die Schnittstellentabelle aus Schritt 3 der Use Case Methodik [C/sells – IOP Teil F. (03/2020)] genutzt (hier nur beispielhaft).

SchnittstelleNr_ Nachricht-Nr	Absenderkomponente Zielkomponente	Informationen	Sicherheitsmaßnahmen
S01_01	mMe Gebäude Y und Z - SMGW Gebäude Y / Z	Messdaten Energie und Leistung für Markt sowie Anschlussnutzer	
S01_02	SMGW Gebäude Y / Z - mMe Gebäude Y und Z	Konfigurationsdaten	
S02_01	EMG – SMGW HAN	Schnittstelle für lokale Bereitstellung der Messdaten nicht genutzt	
S03a_01	SMGW CLS der Anschlussnutzer Gebäude Y / Z - CLS-Modul Anschluss-nehmer	Verschlüsselter und signierter Payload mit beliebigen Daten → im betrachteten Use Case Plim-Signal zur Einstellung einer Maximalleistung;	
S03a_02	CLS-Modul Anschlussnehmer - SMGW CLS der Anschlussnutzer Gebäude Y / Z	Statusdaten	
S03b_01	CLS-Modul als Teil Steuerbox – Aktorik an Netztrennschütz	Steuerdaten für Abschalten und Anschalten Netzanschluss	

S03b_02	CLS-Modul als Teil Steuerbox - EMG Gebäude Y	Steuerdaten mit Leistungsvorgabe (Plim-Signal des gemeinsamen Netzanschlusses)	
S03b_03	CLS-Modul als Teil Steuerbox - EMG Gebäude Z	Steuerdaten mit Leistungsvorgabe (Plim-Signal des gemeinsamen Netzanschlusses)	
S07_01	EMT-Plattform – GWA	Kommunikationsdaten	
S07_02	GWA – EMT-Plattform	Quittungsmeldungen, Statusdaten	
S09_01	Komponente Leitwarte Fernwirkung und Netzmonit. – EMT-Plattform	Leistungsbegrenzungssignal Plim; Wiederzuschaltungs-signal nach Netzwiederaufbau	

1.2.5 Schritt 5 - Spezifikation von Schutzrichtlinien und Implementierung

Vorgehensweise

Erstellung von Schutzrichtlinien auf Grundlage der festgelegten Schutzmaßnahmen sowie Dokumentation deren Implementierung

1.2.6 Schritt 6 - Beschreibung des Einsatzes und Konformitätsprüfung

Vorgehensweise

Einsatzdokumentation und Audits

2 C/sells: Musterlösung

2.1 Schutzbedürfnisse bei der Geräte- und Zellenintegration

Autonomie ist erstens legitimes Gestaltungsinteresse des Einzelnen und von Gemeinschaften sowie zweitens Grundlage für eine geringere Verletzlichkeit (Vulnerabilität) der Lebensfunktionen bei externen Störungen.

Gleichzeitig verfolgen Menschen als soziale Wesen gemeinschaftliche Interessen sowie zeigen die Fähigkeit zur gegenseitigen Unterstützung. Gerade bezüglich der Verfügbarkeit von Energie als Grundbedürfnis des menschlichen Lebens ist das solidarische Handeln im Energieverbundsystem so bedeutsam.

Die Gestaltung von Autonomie und Verbund erhöht die Widerstandsfähigkeit (Resilienz) eines Gesamtsystem als zellulärer Energieorganismus gegenüber ausschließlich zentral produzierenden und gesteuerten Systemen. Zwischen lokaler und regionaler sowie globaler Gestaltung ist das Optimum zu finden. Insbesondere erfordert die Notwendigkeit einer nachhaltige Stadtentwicklung die Erhöhung der Widerstandsfähigkeit durch Maßnahmen zur Klimaanpassung als auch zur Bereitstellung autonomer Infrastrukturfunktionen für Energie, Wasser, Ernährung und Logistik.

Die Corona-Krise zeigte eindrucksvoll, dass ein ausschließlich auf Globalisierung, Zentralisierung sowie Lean Management mit Lieferketten in Echtzeit und fehlender Speicherfähigkeit ausgerichteter Weg das System gegenüber unerwarteten Ereignissen sehr empfindlich reagieren lässt.

Die Systemflexibilität wird durch das Wechselspiel von Autonomie und Verbund erhöht, benötigt aber hierzu auch Speicherfähigkeit innerhalb autonomer Strukturen.

Die Betrachtung der Schutzbedürfnisse umfasst damit die Gewährleistung des autonomen Betriebs als auch der Systemdienlichkeit im Verbund inklusive der Steuerbarkeit zur Nutzung der Speicherfähigkeit in der Wohngebäudezelle.

Die Methodik zur Ableitung und Umsetzung von Schutzmaßnahmen umfasst die sechs Schritte der nachfolgenden Abbildung.

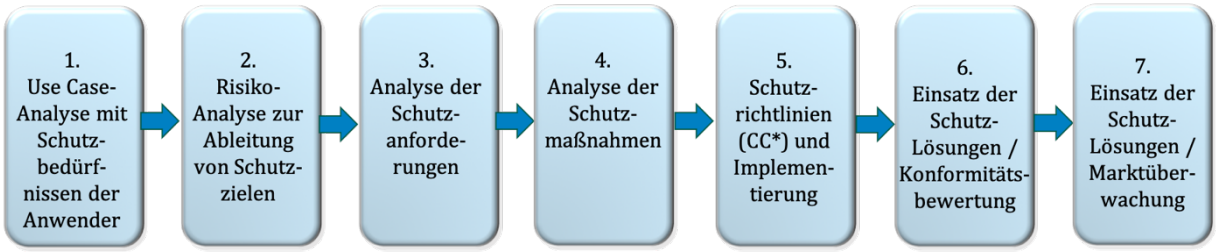

Abb. 6: Prozess der Schutzmethodik

Betrachtet werden im Rahmen der nachfolgenden Musterlösung nur die ersten vier Schritte beispielhaft bis zur Ableitung von Schutzmaßnahmen. Bezüglich der detaillierten Erläuterung des Use Cases sowie der genutzten Schutzmethodik (inklusive Beispiellisten für Schutzbedürfnisse und Bedrohungen) wird auf folgende Quelle verwiesen: Kießling, A. et al (05/2020).

2.2 Use Case-Analyse

Grundlage zur Ermittlung der auf Use Cases bezogenen Schutzbedürfnisse und Bedrohungen ist die Kenntnis von

- Rollen mit verantwortlichen Akteuren
- zugehörige technische, legislative und regulatorische Rahmenbedingungen
- Komponenten mit Mapping auf die Komponentenarchitektur inklusive Zuordnung von Domänen und Zonen aus dem Smart Grid Architekturmodell sowie

Hierzu werden die entsprechenden Aufstellungen aus der Use Case-Beschreibung „HLUCs 050G, 050H, 050I - Sichere Integration von Geräten/Anlagen/Zellen“ [Kießling, A. et al (03/2021)] übernommen (Erläuterungen siehe auch Schritt 2 Use Case Methodik, [Kießling, A., Bogensberger, A., Köppl, S. & Faller, F. (03/2020)]).

Rollen- und Akteursliste

Nachfolgende Akteursliste als Beispiel aus Sicht eines Betreibers der Infrastruktur eines Stadtquartieres mit Sektorkopplung von Strom und Wärme

Rolle / Akteur „wer?“	**Verantwortlichkeiten und Aufgaben „was?“**	**Nutzen und sonstige Wertversprechen für Akteure, „warum?“ Schutzbedürfnisse**
Energieanlageneigentümer (EAE)	Bereitstellung der PV-Anlagen, Power-to-Heat-Anlagen, Ladesäulen sowie zugehörige Sensorik, Aktorik und Kommunikationseinrichtungen	Anlageninvestition zur Optimierung Wärmenetz und Regelenergievermarktung; Sichere und wirtschaftliche Verfahren beim Einsatz der Einrichtungen in Objekten / Arealen → Verhinderung von Schäden gegenüber Anlagennutzern in Liegenschaft
Einsatzverantwortlicher (EIV); Energieanlagenbetreiber (EAB)	Betrieb der PV-Anlagen, Power-to-Heat-Anlagen, Ladesäulen sowie zugehörige Sensorik, Aktorik und Kommunikationseinrichtungen; Wahrnehmung vertraglich vereinbarter Pflichten ggü. Netzbetreiber, Marktakteuren und Akteuren in Liegenschaften, Quartieren, Arealen; technische Wartung; Sicherstellung Fernsteuerbarkeit;	Optimierung Wärmenetz und Regelenergievermarktung; Sichere und wirtschaftliche Verfahren beim Einsatz der Einrichtungen in Objekten / Arealen, Märkten und in Bezug auf Pflichten gegenüber Netzbetreiber und Marktakteuren → Vermeidung finanzieller Verluste bei Fehlfunktion
Prosument	Bewohner und Nutzer der Gebäude mit Bereitschaft Wärmespeicher in die Steuerung durch den Smart City-Betreiber einzubeziehen	Optimierung der Eigenversorgung; bei Stromausfall Weiterbetrieb notwendiger Geräte und damit auch Schutz von Geräten;
Flexibilitätsanbieter / -nutzer	Bewohner und Nutzer der Gebäude mit Bereitschaft Wärmespeicher in die Steuerung durch den Smart City-Betreiber einzubeziehen; Power-to-Heat-Anlagenbetreiber, der Flexibilität bereitstellt	Angebot von Flexibilität zur Erzielung wirtschaftlicher Vorteile im Wärmenetz; Gewährleistung der Lieferung vereinbarter Flexibilität, um finanzielle Verluste zu vermeiden;
Anschlussnehmer	hat Anschlussvertrag mit Netzbetreiber für Bezugs- und Einspeiseleistungen; Eigentümer vom Netzanschluss der PV- und P2H-Anlagen ist Smart City-Betreiber und Eigentümer der Wärmespeicher in den Gebäuden sind Gebäudeeigentümer verantwortlich für die Einhaltung der Netzanschlussbedingungen und der Netzverbindung zu internen Prosumenten für Strom- und Wärmenetz; Am Netzanschluss entstehen Bezug und Einspeisung der oder die im Objekt des Anschlussnehmers wirkenden Prosumenten.	Bessere Wärmeversorgung durch Vermeidung von Wärme-Schlechtpunkten; Betriebssicherheit der Wärmeversorgung im Gebäude trotz Einsatz Wärmespeicher für Flexibillität im Wärmenetz

Rolle / Akteur „wer?“	Verantwortlichkeiten und Aufgaben „was?“	Nutzen und sonstige Wertversprechen für Akteure, „warum?“ Schutzbedürfnisse
Anschlussnutzer	hat Anschlussbezugsvertrag oder -einspeisevertrag mit Lieferanten oder Vermarktern und ist Nutzer des Netzanschlusses; Bezüglich der PV- und P2H-Anlagen fallen Anschlussnehmer und -nutzer bei einem Akteur zusammen, während Anschlussnutzer im Gebäude die Bewohner sind und der Steuerung des Wärmespeichers zustimmen müssen	Bessere Wärmeversorgung durch Vermeidung von Wärme-Schlechtpunkten; Betriebssicherheit der Wärmeversorgung im Gebäude trotz Einsatz Wärmespeicher für Flexibillität im Wärmenetz
Facility-Betreiber	Bezüglich PV- und P2H-Anlagen fällt die Rolle des Einsatzverantwortlichen mit der Rolle des Facility-Betreibers zusammen; Bezüglich der Gebäude kann der Facility-Betreiber die Hausverwaltung sein, während der Anschlussnutzer der Mieter / Eigentümer ist Ein eventueller Betrieb eines Gebäude-Energiemanagementsystems liegt beim Anschlussnehmer, sowie eines Kunden-Energiemanagementsystems beim Anschlussnutzer, woraus auch die Verantwortlichkeit für Kommunikationsinfrastruktur folgt	Einsparungen beim Aufwand zur Betriebskostenabrechnung durch Einführung intelligenter Messsysteme; Sicherer Betrieb der Liegenschaften → Verhinderung von Schäden gegenüber Nutzern in Liegenschaft
Verteilnetzbetreiber (VNB)	Bereitstellen des Netzanschlusses, Ermöglichung der Nutzung des Stromnetzes, Sicherstellen der Versorgungssicherheit und Netzstabilität	Generierung von Einnahmen durch Bereitstellung der Netzinfrastruktur; Betriebsersparnisse im Wärmenetz durch Optimierung mit Energiemanagementsystem im Quartier sowie Steuerung Wärmenetz; Grundlegende Betriebssicherheit darf durch das Energiemanagementsystem nicht beeinflusst werden
Direktvermarkter / Aggregator	Vermarktung der durch PV-/P2H-Anlage angebotenen Flexibilität als Regelenergie oder auf anderen Märkten	neue Umsatzquelle aus der Anlagenvermarktung im Stadtquartier; Sicherstellung der Dienstleistung bei Kommunikationsausfall durch Grundzustandsbetrieb, Verhinderung von Datendiebstahl und -verlust
(wettbewerblicher) Messstellenbetreiber (MSB)	Einbau, Betrieb und Wartung von modernen Messeinrichtungen zur Ermittlung und Übermittlung von hochaufgelösten Messwerten über das SMGW Übertragung der Messdaten aus Erzeugung und Verbrauch an lokales EM-System sowie Weiterleitung der Daten an externe Akteure über Komponenten zur Messdatenverteilung und Messdatenverwaltung	Einnahmen durch regulierte Mess- und (unregulierte) Mehrwertdienste; Sicherstellung der Dienstleistung bei Kommunikationsausfall durch Grundzustandsbetrieb, Verhinderung von Datendiebstahl und -verlust; Einhaltung rechtlicher Anforderungen
Gateway-Administrator	Verwaltung der technischen Verbindung zu Smart Meter Gateway mit verschiedenen Stakeholdern; Betrieb eines Gateway-Administrationssystems als IIS-Komponente	Erlöse aus dem Betrieb einer sicheren Kommunikations-infrastruktur für Messdaten und Steuerungen; Sicherstellung der Dienstleistung bei Kommunikationsausfall durch Grundzustandsbetrieb, Verhinderung von Datendiebstahl und -verlust; Einhaltung rechtlicher Anforderungen
EMT-Plattform-Betreiber	Verantwortung für Kommunikationsdienste: Stellt Kommunikations-Infrastruktur mit Basisfunktionen für aktive, externe Marktteilnehmer als sichere Integrationsumgebung zu Zellen, Geräten, Anlagen, sowie Nutzung des Steuer- und Kommunikationskanals bereit;	Generierung von Einnahmen durch Bereitstellung von (Kommunikations-) Infrastruktur und Mehrwertdiensten; Sicherstellung der Dienstleistung bei Kommunikationsausfall durch Grundzustandsbetrieb, Verhinderung von

Rolle / Akteur „wer?“	Verantwortlichkeiten und Aufgaben „was?“	Nutzen und sonstige Wertversprechen für Akteure, „warum?“ Schutzbedürfnisse
		Datendiebstahl und -verlust; Einhaltung rechtlicher Anforderungen
Informationssystem-Betreiber	Verantwortung für weitere Informationsdienste in der Cloud: Betrieb diskriminierungsfreier IKT-Unterstützungsdienste (hochaufgelöste Messdaten, Prognosen, Flexibilitätsdaten für Regelenergiemarkt)	Einnahmen aus Informationsbereitstellung; Sicherstellung der Dienstleistung bei Kommunikationsausfall durch Grundzustandsbetrieb, Verhinderung von Datendiebstahl und -verlust; Einhaltung rechtlicher Anforderungen

Rahmenbedingungen (legislativ, regulatorisch und technisch):

Übernahme der Rahmenbedingungen aus der Use Case-Beschreibung zur Feststellung eventuell weiterer sicherheitsrelevanter Aspekte

Rahmenbedingungen (z.B. Datenschutz, Anschlussbedingungen, Zeitverhalten, Verfügbarkeit, Schutz, Koordination, usw.)	Wirkung des Themas auf den Anwendungsfall	Verweise auf Gesetze und Regelungen
Gewährleistung von Datenschutz	Einsatz intelligenter Messsysteme und Definition der Aufgaben beim MSB im Rahmen der IIS-Komponente zur Messdatenverwaltung	Digitalisierungsgesetz, Schutzprofil und techn. Richtlinie BSI, Datenschutzgrundverordnung
Gesetzliche und regulatorische Rahmenbedingungen	Vorrangregeln nac Ampelkonzept, Koordinationsfunktion,	BDEW, EEG, EnWG, StromNEV, Koordinationsfunktion bei FFN in Arbeit
Messdatenbereitstellung in Echtzeit	Aktuell in Zertifizierung SMGW nicht enthalten	
Steuerprozesse zu Anlagen	CLS-Kanal-Nutzung als aEMT: Übergabe des Steuerbefehls, Ausführen des Steuerbefehls, Übergabe von Statusinformationen, Interaktion mit GWA; CLS-Kanal-Management	Weitere dazu notwendiger Prozessspezifikationen in 2. Phase für Rollout Messsysteme im Rahmen der Normung in Verbindung mit BSI
Marktkommunikation	Festgelegte Prozesse und Anwendung Normen	Festlegungen BNetzA zur Marktkommunikation
Bewertung der Lösung aus Sicht der internen Quartiersenergielieferung	Geschäftsmodell und regulatorischen Rahmen bewerten	

Komponentenliste

Schutzbedürfnisse können durch Anwender (siehe Rollen) für Systeme oder Teilsysteme oder einzelne Komponenten definiert werden, die im Rahmen einer eventuellen Datenspeicherung sowie ihrer Funktionalitäten sowohl Aspekte der Versorgungssicherheit und der Betriebssicherheit betreffen.

Den Komponenten sind danach auf Basis der Betrachtung benötigter Funktionen Schutzbedürfnisse hinzuzufügen. Die weitere Detaillierung ist im Rahmen eines Zertifizierungsprozesse zum Informationssicherheits-Management vorzunehmen.
Der Fokus liegt dabei auf informationstechnischen und nicht auf elektrotechnischen Anforderungen.

Komponente (evtl. mit verantwortlicher Rolle)	D: Domäne B: Betriebszone	Funktionen Schutzbedürfnisse
A: Assets Geräte und Anlagen als Energiewandler (Erzeuger, Speicher, Verbraucher von Anlagenbetreibern) Energieanlagenbetreiber (Einsatzverantwortlicher) Anschlussnehmer	D: Liegenschaft, DER B: Prozess	**Gerätefunktionen als steuerbare Senke und Quelle von Energieflüssen aller Endenergieformen** - installiert innerhalb einer privaten Gebäudezelle sowie als dezentrale Energieanlage innerhalb eines öffentlichen Quartieres oder Areals; **Übertragung Statusinfos** (z.B. Prognosen, Fahrpläne, Flexibilitätsdaten, Kapazität), **Entgegennahme von zur Steuerung versendeten Informationen** **Einstellung der Leistung über definierte Zeitabschnitte** **Steuerbarkeit über IP direkt zu Anlage oder IP und Mapping zu jeweils ausgewählten Anlagen-Feldbus** Betrieb von aEMT-Plattform und externem Energiemanagement-System darf nicht - den Assetbetrieb stören, - zu Beeinträchtigungen bei Endkunden führen, - nicht weitere Infrastrukturen des Endkunden stören, - Informationen zu Assets des Endkunden unerlaubt weitergeben, - zu Vertrauensverlusten gegenüber dem Betreiber führen und - zu keinen finanziellen Schäden beim Betreiber führen **Gewährleistung von Netzanschlussbedingungen** Netzanschlussbedingungen dürfen nicht verletzt werden, um körperlichen und finanziellen Schaden zu verhindern
A: Assets Anlagenaggregat mit Systemmanager und gemeinsamen Netzanschluss (z.B. PV, Wechselrichter und Batterieb) Prosument Verteilnetzbetreiber	D: Gebäude B: Prozess	Bündelung von Gebäudestandardbezug sowie steuerbaren Einzelanlagen (PV, Batterie, WP, LP in einem Netzanschluss), wobei die Steuerbarkeit der Einzelanlagen darüber bereitgestellt werden kann; analog siehe oben (Assets: Geräte und Anlagen als Energiewandler) Gewährleistung Netzanschluss für Anlagenaggregat mit Leistungssteuerung am Netzanschluss des Aggregates und nicht zu Einzelanlagen, Vertrauensverlust in Netzbetreiber beim Anschlussnehmer durch Betriebsfehler, die den Assetbetrieb stören, verhindern
A: Assets Anlagen-Koppelschutz sowie Trenneinrichtung am Netzanschluss mit Inselfähigkeit über inselfähigen, dreiphasigen Wechselrichter Anschlussnehmer, Facility-Betreiber (EIV: Einsatzverantwortlicher)	D: Gebäude B: Prozess	Schutzeinrichtung und Erhaltung Netzfrequenz sowie Spannung (z.B. entsprechend ausgestatteter, gemeinsamer Wechselrichter für PV-Anlage und Batterie), abschaltbarer Netzanschluss von Gebäuden, Wiederzuschaltung durch Remote-Zugriff Netzbetreiber möglich; analog siehe oben (Assets: Geräte und Anlagen als Energiewandler)
B1: Sensorik / Aktorik Sensorik Energieanlagenbetreiber	D: Liegenschaft, DER B: Feld	**Messung interner Leistungsflüsse** an ausgewählten Anlagen (PV, Batterie) und Energie nutzenden Geräten sowie Übersendung der Daten an GEMS **Messung von Umweltparametern** **Bestimmung weiterer Status der Geräte und Anlagen** **Sichere Kommunikation der Messwerte im LAN** Daten dürfen nicht durch externe Akteure ermittelbar sein

Komponente (evtl. mit verantwortlicher Rolle)	D: Domäne B: Betriebszone	Funktionen Schutzbedürfnisse
B1: Sensorik / Aktorik Aktor einer Steuereinrichtung (z.B. FNN-Steuerbox oder in Verbindung SMGW oder abgesetztes Energiemanagement-Gateway mit Aktorik der Anlagen Energieanlagenbetreiber	D: Liegenschaft, DER B: Feld	**Einstellen der Leistung einzelner Anlagen** zu definierten Zeitpunkten über bestimmte Zeitdauern oder als aggregierte Leistung an ein EMS; **Erfassung der Statusinformation der Steuereinrichtung** (gestört / nicht gestört / Regelzustand) CLS-Modul zur **Terminierung des CLS-Kanales**, Entschlüsselung und zum Entpacken des Inhaltes innerhalb der Nachricht Betrieb Plattformen GWA/MSB/EMT soll nicht - zu Beeinträchtigungen der Steuerungsfähigkeit beim Endkunden führen, - sonstige Steuerungsfunktionen im Smart Building anderer Handlungssektoren des Endkunden stören, zu Verletzungen der Informationssicherheit oder der IKT-Zuverlässigkeit in den Systemen des Endkunden führen, Das Energiesystem im Gebäude darf nicht angreifbar sein, wenn Aktorik über EMS und Internetzugang des Gebäudes mit externen Energiedienstleistern verbunden ist.
B1: Sensorik / Aktorik moderne Messeinrichtung Messstellenbetreiber	D: Liegenschaft, DER B: Feld	**Messung der Leistungsflüsse zur externen Umgebung** (IST-Werterfassung) hinter Anschlusspunkt einer Liegenschaft, eines Unterobjektes in einer Liegenschaft oder einer Einzelanlage **Sichere Kommunikation der Messwerte im LMN;** Betrieb Plattform MSB soll nicht - zu Beeinträchtigungen der Messwerterfassung beim Endkunden führen, - Messung an weiteren Infrastrukturen des Endkunden stören, zu Verletzungen des Datenschutzes bezüglich der gemessenen Energieflüsse beim Endkunden führen,
B2: Kommunikations-komponenten Smart Meter Gateway Messstellenbetreiber Gateway-Administrator	D: Liegenschaft, DER B: Station Gebäude und Anlagensystem	**Speicherung der Abrechnungstarife** **Speicherung der Zählerstandsgänge** (Zählerstände pro Zeitpunkt als Basis der Bildung von Leistungskurven und Verbrauchszeitreihen Gewährleistung des Datenschutzes **Weitergabe der Messdaten an autorisierte pEMT** • **Öffnung CLS-Kanal zur sicheren Übertragung von Informationen externer aEMTs in die Zelle** (interne Managementsysteme und Einzelanlagen / Geräte) Gewährleistung der sicheren Kommunikation zwischen Geräten / Zellen und Außenwelt Betrieb externer Energiedienstleister, die Steuerbox bedienen, darf nicht zu Beeinträchtigungen des SMGW-Betriebs sowie zu konkurrierenden Zugriffen führen
B2: Kommunikations-komponenten Energiemanagement-Gateway Facility-Betreiber für Objekt des Prosument (CEMS) Gebäude (GEMS) Quartier / Areal (QEMS)	D: Liegenschaft, DER B: Feld	Gateway zur geschützten Weitergabe von Steuersignalen und zum Komm.mapping zwischen Steuereinrichtung / EMS sowie zu steuernden Anlagen / Geräten; CLS-Modul zur **Terminierung des CLS-Kanales**, Entschlüsselung und zum Entpacken des Inhaltes innerhalb der Nachricht; • **Direktsteuerung** der Anlage über externes Signal ohne Nutzung CLS-Kanal • **Direktsteuerung** der Anlage über externes Signal mit Terminierung des CLS-Kanales mit analogen Schaltsignalen • **Direktsteuerung** der Anlage über externes Signal mit Terminierung des CLS-Kanales mit digitaler Schnittstelle und Kommunikations-Mapping • **Indirekte Anlagensteuerung** durch Integration in das Energiemanagement-Framework von CEMS / GEMS / QEMS • **Gewährleistung der sicheren Kommunikation zwischen Geräten / Zellen und Außenwelt sowie auch von Datenschutz bei Verbindung über privaten Zugang in das Internet**

Komponente (evtl. mit verantwortlicher Rolle)	D: Domäne B: Betriebszone	Funktionen Schutzbedürfnisse
B2: Kommunikations-komponenten Lokales Kommunikationsnetz im Gebäude (LAN)	D: Liegenschaft, DER B: Betriebsführung	Betrieb der notwendigen lokalen Kommunikationssysteme in den Gebäuden hinter dem Anschlusspunkt (lokale Gebäudenetze sowie Kopplung von GEMS in Gebäuden zu iMSys sowie Sensorik und Aktorik); Verbindung HAN vom SMGW mit LAN zu Assets darf nicht - den Assetbetrieb stören, - zu Beeinträchtigungen bei Endkunden führen, - nicht weitere Infrastrukturen des Endkunden stören, - Informationen zu Assets des Endkunden unerlaubt weitergeben, - zu Vertrauensverlusten gegenüber dem Betreiber führen und zu keinen finanziellen Schäden beim Betreiber führen
B3: Kommunikations-komponenten GWA-System und zugehörige Teilkomponenten Gateway-Administrator	D: Liegenschaft, DER, Verteilnetz B: Betriebsführung	**Administration SMGW und Verbindung** Parametrierung und Konfiguration der Zertifikate der SMGWs für Verbindung zwischen Messystemen und pEMTs und aEMTs; Verbindungsaufbau für berechtigte Akteure; Datenempfang, Entschlüsselung und Weitergabe; **PKI-Infrastruktur** **Authentifizierung** der pEMTs und aEMTs • **Öffnung Komm.tunnel** für authentifizierten Partner Da Datenverteilung durch EMT-Plattform hat GWA-Komponente ausschließlich Funktionen zur Parametrierung sowie zur Freigabe der Kommunikationstunnel. Betrieb externer Energiedienstleister darf nicht zu Beeinträchtigungen des Betriebs beim GWA führen,
B2: Kommunikations-komponenten aEMT-Plattform und zugehörige Teilkomponenten IIS-Betreiber für aEMT-Plattform (z.B. VNB) Verteilnetzbetreiber Messstellenbetreiber	D: Liegenschaft, DER, Verteilnetz B: Betriebsführung (MSB)	**Administration aEMT-Funktionen und Verbindung über CLS-Tunnel** Bereitstellung einer Umgebung für verschiedene Energiedienstleister und Netzakteure zum steuernden Zugriff auf Anlagen über CLS-Tunnel inklusive CLS-Management und Koordinationsfunktion; Betrieb externer Energiedienstleister darf nicht zu Beeinträchtigungen des Betriebs beim GWA sowie der Prozesse zur Nutzung des sicheren CLS-Tunnels führen,
B3: Basiskomponenten Informationssystem Messdaten Messstellenbetreiber IoT-Plattformbetreiber	D: Liegenschaft, DER, Verteilnetz B: Betriebsführung	**Verwaltung von Messdaten** in jeweils benötigter Auflösung (**hochaufgelöste Messdaten – High resultion – HRM**) inkl. Submeter und Sensorik, Bereitstellen und Verwaltung von Historien der Zeitreihen; Betriebsschutz bezüglich Datenschutzfunktionen bei Weitergabe von Daten an externe Marktpartner gewährleisten (aktuell noch keine sternpunktförmige Datenweitergabe vom SMGW abgesichert über GWA, sondern Datenweitergabe über MSB und Messdatenplattformen mit bisherigen Prozessen der Marktkommunikation)
B3: Basiskomponenten Basisdienste IoT-Plattform IoT-Plattformbetreiber	D: Liegenschaft, DER, Verteilnetz B: Betriebsführung	**Eintragen von Stammdaten, Funktionslisten und von Kommunikationsprofilen in Registry** - durch Anlage, Gerät, Zelle oder über Dashboard eines Betreibers **Flexibilitätskataster, Prognosen, Bilanzen, Transaktionen** Betriebsschutz bezüglich Datenschutzfunktionen bei Weitergabe Messdaten sowie Versorgungssicherheit bei Weitergabe von Bilanzierungs-, Fahrplan- und Marktdaten an externe Marktpartner gewährleisten

Komponente (evtl. mit verantwortlicher Rolle)	D: Domäne B: Betriebszone	Funktionen Schutzbedürfnisse
C: Betriebskomponenten Fernwirkungsplattform der Leitwarte Verteilnetzbetreiber	D: Verteilnetz B: Betriebsführung	**Senden von Steuersignalen** – digital unter Nutzung des CLS-Kanales **Verwaltung Netzqualitätsdaten (f, U, I, cos Phi, …)** mit Lieferung der Daten intelligenter Messsysteme über Informationssystem Messdaten Störung der korrekten Netzfunktion durch Belieferung mit falschen Netzmessdaten verhindern
C: Betriebskomponenten Messstellenbetrieb Messstellenbetreiber	D: Liegenschaft, DER, Verteilnetz B: Unternehmen	**Lieferung von Geräteinformationen und Anschlussobjekten** (MeLo, MaLo) sowie **Messdaten** für Liefer- und Netzabrechnung **Einbau und Betrieb intelligenter Messeinrichtungen** mit modernen Messeinrichtungen (Strom, Wärme, Gas, Wasser) und SMGWs Betriebsschutz bezüglich Datenschutzfunktionen bei Weitergabe von Daten an externe Marktpartner gewährleisten
C: Betriebskomponenten Energiemanagement, Marktaggregation und Direktvermarktung Energiedienstleister Anbieter Energiemanagementsysteme Anbieter Systemdienstleistungen	D: Liegenschaft, DER B: Unternehmen	**Energieeffizienzdienstleistungen;** **Energiemanagement-Systeme für Prosumenten (CEMS), Gebäude (GEMS), Quartiere / Areale (QEMS);** **Virtuelle Kraftwerke;** **Direktvermarktung inklusive Peer-to-Peer-Umgebungen** Störung der korrekten Marktfunktionen durch Belieferung mit falschen Messdaten verhindern sowie Verletzung des Datenschutzes verhindern; Energiemanagementsystem beschafft Messwerte und muss hierbei die vorgegebenen Datenschutz-Kriterien einhalten, Das Energiemanagementsystem in Zellen darf nicht angreifbar sein, wenn EMS über Internetzugang der Liegenschaft mit externen Energiedienstleistern verbunden ist.
D: Marktkomponenten Energielieferung Energiehandel Lieferanten Händler	D: Liegenschaft, DER B: Unternehmen	**Geräteverwaltung,** **Verbrauchsablesung,** **Abrechnung,** **Bilanzierung,** **Fahrpläne** Direktvermarktung (Handelsgeschäfte mit Markt sowie Lieferung von Handelsergebnissen), Störung der korrekten Markt- oder Managementfunktionen durch Belieferung mit falschen Messdaten verhindern sowie Verletzung des Datenschutzes verhindern
D: Marktkomponenten Marktplattformen Flexibilitätsplattformen Marktplattformbetreiber Börsenbetreiber	D: ÜN, VN, DER, Liegenschaft B: Markt	**Marktfunktionen auf Plattformen verschiedener Märkte inklusive Großhandelsmarkt, Regionalmarkt, Flexibilitätsmarkt und Regelenergiemarkt** Störung der korrekten Markt- oder Managementfunktionen durch Belieferung mit falschen Messdaten verhindern sowie Verletzung des Datenschutzes verhindern

Die Nutzung einer Abbildung zur Komponentenarchitektur auf Basis der SGAM-Komponentenebene ist hilfreich, um die Verbindungen zwischen den genannten Komponenten zu verdeutlichen, wie nachfolgend dargestellt.

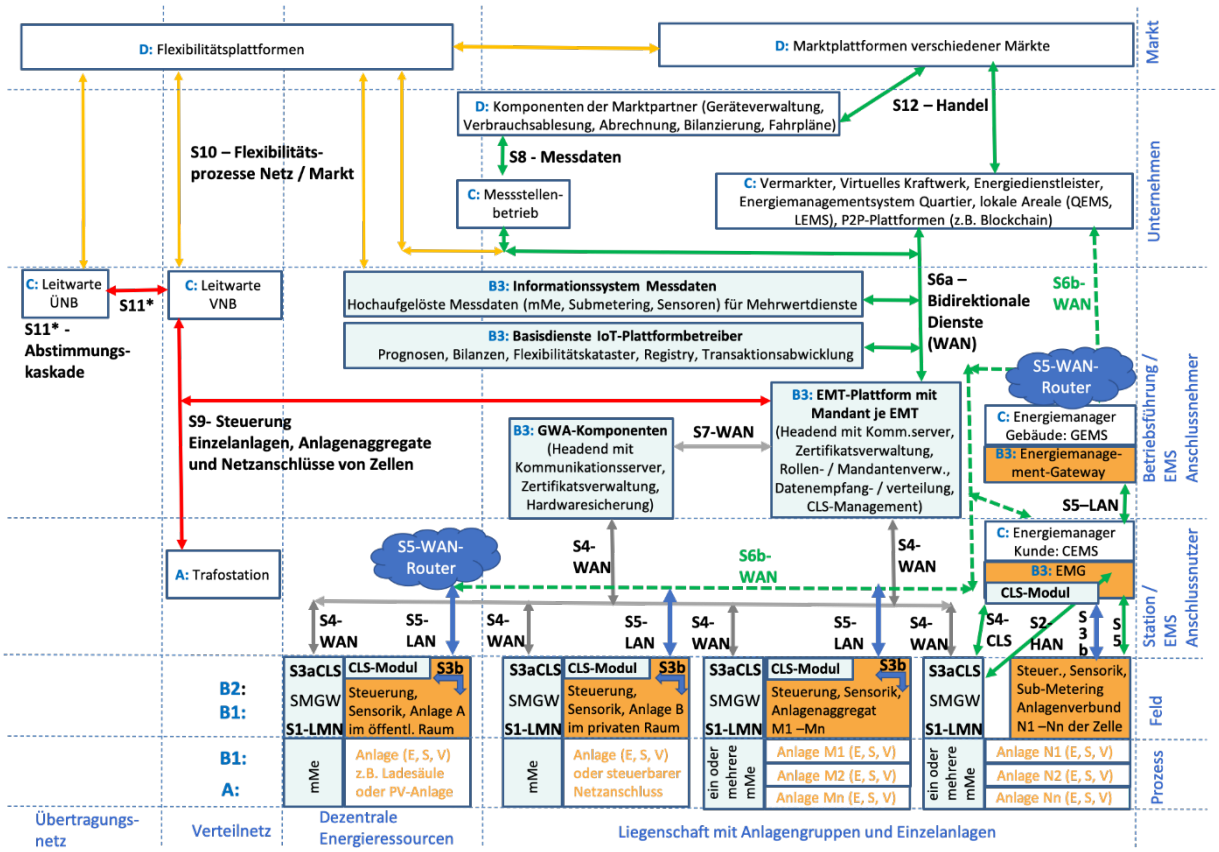

Abb. 7: Komponenten der Schutzanalyse zur Musterlösung

2.3 Risikoanalyse – Integration Einzelanlagen und Gebäudezelle

Risiken beim Betrieb des Energiesystems in einer Gebäudezelle beruhen auf dem Eintreten möglicher Bedrohungen. Um die Auswirkung eines Risikos zu begrenzen, formulieren Anlagenbetreiber und die Gebäudenutzer verschiedene Niveaus der Auswirkung und definieren für Schutzbedürfnisse eine bestimmte, maximal zulässige Auswirkung von eintretenden Risiken.

Folgende Schutzbedürfnisse wurden aus Sicht des Betreibers von Anlagen sowie Gebäuden mit zugehörigen Energieanlagen identifiziert.

Schutzbedürfnisse beim Betrieb des Energiesystems

- Fernsteuerbarer Netzanschluss im Gebäude darf nicht zur Störung der verfügbaren Leistung sowie einem Ausfall des Energieflusses am Netzanschluss führen.
- In ein Kommunikationsnetz eingebundene Sensorik und Aktorik im Gebäude an einzelnen Anlagen und Geräten dürfen nicht die Verfügbarkeit von Endgeräten und Teilbereichen des Gebäudes beeinträchtigen.
- In ein Kommunikationsnetz eingebundene Sensorik und Aktorik im Gebäude an einzelnen Anlagen und Geräten dürfen nicht die von anderen Infrastrukturen, wie Wasser- oder Wärmeversorgung beeinträchtigen.

Schutzbedürfnisse bezüglich der Einhaltung von Gesetzen und Regularien

- Die Übersendung von Messdaten an Energiedienstleister (z.B. zur Messdatenvisualisierung), die Messdaten speichern, darf nicht zur Verletzung des Datenschutzes führen.
- Die Übersendung von Daten sowie die Übertragung von Vermarktungsaufgaben an Energiedienstleister (z.B. Abrechnung von P2P-Stromverkäufen), die Unterstützungsdienstleistungen bieten, darf nicht zur Verletzung von Gesetzen und Regularien führen (z.B. Bilanzierungs- und Abrechnungspflicht).

Bedrohungen bezüglich der das Energiesystem nutzenden Menschen

- Fernzugriffe auf Steuerbox und Aktorik im Gebäude an einzelnen Anlagen und Geräten im Gebäude darf nicht zu körperlichen Verletzungen aufgrund Fehlbetriebes führen.

Bedrohungen für Finanzen

- Die Übersendung von Daten sowie die Übertragung von Vermarktungsaufgaben an Energiedienstleister (z.B. Abrechnung von P2P-Stromverkäufen), die Unterstützungsdienstleistungen bieten, darf keinen finanziellen Verlust der Gebäudenutzer und Anlagenbetreiber aufgrund fehlender Abrechnung oder Vermarktung bewirken.

Bei einer ausschließlich informations- und kommunikationstechnisch geführten Betrachtung (hier der Fokus im Beispiel) bestehen die Risiken, dass folgende Bedrohungen die Schutzbedürfnisse verletzen (siehe Einleitung zu Kapitel Use Case-Analyse).

- Vertraulichkeit(confidentiality) wird nicht eingehalten
- Integrität (integrity) der Daten wird durch unerlaubtes Verändern verletzt
- Verfügbarkeit (availability) nicht gewährleistet
- Nicht-Abstreitbarkeit (repudiation) durch Bedrohung der Protokollierungspflichten verletzt
- Verletzbarkeit (vulnerability) der technischen Funktion der IKT-Komponenten

Diese Bedrohungen werden den Risikoauswirkungs-Kategorien zugeordnet, die jeweils auf ein Schutzbedürfnis Bezug nehmen. Für das Eintreten der Bedrohung werden jeweils fünf zugehörige Risikoauswirkungs-Niveaus definiert und die jeweiligen Auswirkung wird mit einer farblichen Kennzeichnung zwischen den Werten niedrig, mittel, hoch, kritisch und hoch kritisch bewertet.

Grundsätzlich ist diese Bewertung für jede der genannten Bedrohungen zu bestimmen. Hier im Beispiel wird die Bewertung einmal für alle Bedrohungen geführt. In der Praxis wird bei getrennten Bewertungen als Ergebnis das am höchsten eingeschätzte Risikoauswirkungs-Niveau genutzt.

Risikoaus-wirkungs-Niveau risk impact level (	RA-Niveau auf Basis Leistungs-grenze am Netz-anschluss	RA-Niveau auf Basis Energie-fluss	RA-Niveau auf Basis betrof-fener Bevölke-rung	RA-Niveau auf Basis betrof-fener Infra-strukturen	RA-Niveau in Bezug zu Daten-schutz-direktiven	RA-Niveau auf Basis möglicher Strafen	RA-Niveau auf Basis Gefährdung Komfort / Gesundheit	RA-Niveau auf Basis direkter mone-tärer Schaden
hoch krtitisch	Leistungs-begren-zung 100 % der Maximal-leistung	Ausfälle im Bereich von Wochen	gesamtes Wohn-quartier ist betroffen	zusätzlich Wasser-ver-sorgung betroffen	noch keine Definition	Gebäude wird für unbenutz-bar erklärt	Todesfall	über 50% vom Jahresein-kommen
kritisch	Leistungs-begren-zung max. 80 % der Maximal-leistung	Ausfälle im Bereich von Tagen		zusätzlich Wärme-ver-sorgung betroffen	Noch keine Definition	Nutzungs-unter-brechung	Verletzung mit Folge-schäden	von 15% zu 50% vom Jahresein-kommen
hoch	Leistungs-begren-zung max. 60 % der Maximal-leistung	Ausfälle im Bereich von Stunden	Mehrere Familien sind betroffen	Gesamtes Stromnetz des Hauses betroffen	unautoris. Zugriff auf persön-liche Daten	Geld-strafen	Starke Verletzung	von 5% zu 15% vom Jahresein-kommen
mittel	Leistungs-begren-zung max. 40 % der Maximal-leistung	Ausfälle im Bereich von Minuten	Ganze Familie ist betroffen	Stromnetz in einzelnen Räumen betroffen	unautoris. Zugriff auf technische Daten	Probleme mit Nachbarn	Mindere Verletzung	von 1% zu 5% vom Jahresein-kommen
niedrig	Leistungs-begren-zung max. 20 % der Maximal-leistung	Kurze Span-nungs-schwan-kung - Sekunden	Einzelne Person ist betroffen	Nur eine Strom-phase betroffen	keine persönl. od. sensitiven Daten	nur War-nungen bei Nicht-erfüllung	Einschr. Komfort	unter 1% vom Jahresein-kommen
	Energie-versor-gung (Leistung in kW)	Energie-fluss (Leistung mal Zeitdauer kWh)	Bewohner	Infra-strukturen	Daten-schutz	Folgen durch Verletzung von Gesetzen / Verordn.	Menschen	Finanzen
	Funktional				Gesetze			

Tabelle 4: Risikoauswirkungs-Kategorien mit Bestimmung von Risikoauswirkung-Niveaus für AutonomieLab

Nun ist als zweiter Faktor die **Eintrittswahrscheinlichkeit** für die genannten vier Bedrohungen, deren Eintreten die genannten Risikoauswirkungen bewirken kann, zu bestimmen. Die Wahrscheinlichkeit kann auf

verschiedenen Wegen der Interaktion zwischen zwei Komponenten in Abhängigkeit vom Akteur, der Zugriff auf die Schnittstelle erhält, variieren. Die Wahrscheinlichkeit wird mittels der Level niedrig, mittel, hoch, sehr hoch und extrem hoch abgeschätzt. Da die Bedrohung über verschiedene Schnittstellen des Systems unterschiedlich hoch zu bewerten ist, aber der höchste Auswirkungsgrad durch das schwächste Glied der Kette – die am meisten bedrohte Schnittstelle – gegeben ist, wird der höchste Grad der Eintrittswahrscheinlichkeiten für die weitere Bestimmung der Anforderungen und Maßnahmen herangezogen.

Die folgende Tabelle verdeutlicht das Vorgehen zu Bestimmung der Eintrittswahrscheinlichkeit, wobei die angegebenen Wahrscheinlichkeiten hier nur beispielhaft aufgeführt sind und einer detaillierteren Risikobetrachtung bedürfen. Wiederum gilt, dass die Betrachtung für jede Bedrohung zu führen ist und dann die höchste Eintrittswahrscheinlichkeit für die Berechnung des Sicherheits-Levels gewählt wird. Hier im Beispiel wird von der gleichen Wahrscheinlichkeit für alle Bedrohungen ausgegangen.

Schnittstellen	**unehrlicher Administrator GWA- / aEMT-Plattform**	**unehrlicher Beschäftigter VNB**	**Vandalismus im Wohnquartier**	**Hacker**	**Terrorist**
aEMT-Komponente des VNB SMGW CLS-Kanal					
SMGW CLS-Kanal zu Steuerbox					
Steuerbox zu GEMS					
Sensorik zu GEMS					
App mobiles Endgerät zu GEMS					
Geräte/Anlagen zu WAN Gebäude					
GEMS zu externer P2P-Plattform					

Tabelle 5: Bestimmung von Eintrittswahrscheinlichkeiten für Gruppen von potentiellen Angreifern

Die Kombination von Risikoauswirkungs-Niveau zwischen 1 und 5 und Grad der Eintrittswahrscheinlichkeit zwischen 1 und 5 führt in folgender Tabelle zur Bestimmung des Sicherheitsniveaus (security level), die durch Addition mit Werten zwischen 2 bis 10 berechnet werden.

Genutzt wird jeweils das höchste ermittelte Risikoauswirkungs-Niveau und die höchste Eintrittswahrscheinlichkeit.

		Eintrittswahrscheinlichkeit (likelihood)				
		1: niedrig	2: mittel	3: hoch	4: sehr hoch	5: extrem hoch
Risiko-auswirkung-Niveau (risk impact level)	5: hoch krtitisch	6	7	8	9	10
	4: kritisch	5	6	7	8	9
	3: hoch	4	5	6	7	8
	2: mittel	3	4	5	6	7
	1: niedrig	2	3	4	5	6
		1	2	3	4	5
		Sicherheitsniveau (security level) und Datenschutzklassen				

Tabelle 6: Bestimmung der Sicherheits-Niveaus (security level) und Datenschutzklassen

2.4 Bestimmung von Schutzanforderungen

Vorgehensweise

Die für Use Cases definierten Schutzbedürfnisse und die resultierende Risikobewertung mit der Bestimmung von Risikoauswirkung-Niveaus, Eintrittswahrscheinlichkeiten sowie resultierenden Sicherheitsniveaus ist Grundlage für Schritt 3 der Schutzmethodik zur Ableitung von Schutzanforderungen.

Informationsobjekte und Kommunikationsanforderungen

Schutzanforderungen sind abhängig vom Wirkungsort installierter Komponenten (siehe Komponententabelle) und ihrer Schnittstellen sowie den dabei übertragenen Daten. Insofern erfolgt die Übernahme und Betrachtung der Tabellen zu Informationsobjekten und zu Kommunikationsanforderungen aus der Use Case-Beschreibung „HLUCs 050G, 050H, 050I - Sichere Integration von Geräten/Anlagen/Zellen“ [Kießling, A. et al (03/2021)] mit Erläuterungen zu Schritt 2 der Use Case Methodik [Kießling, A., Bogensberger, A., Köppl, S. & Faller, F. (03/2020)].

Dabei sind zuerst zur Festlegung von Datenschutzanforderungen die im Use Case benötigten Daten zu klassifizieren. Dies erfolgt im Rahmen der zum Use Case ermittelten Informationsobjekte, d.h. von gespeicherten und im Rahmen von Nachrichten zwischen Akteuren ausgetauschten Daten.

Informationsobjekt	Teilobjekte	Inhalte	Schutzbedürfnisse und Datenklassifizierung
Messdaten	Leistungsgänge	Leistung Zeit	Leistungsverläufe in der Zeit mit Auflösung im Sekundenbereich jeweils für Verbrauch und Erzeugung der benötigten Anlagen von iMSys oder Sensorik an Einzelgeräten; → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Messdaten	Mengen	Energie Zeitdauer	Energiemengen in Zeitabschnitten mit wählbarer Zeitdauer → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Messdaten	Powerqualität	Strom, Spannung, Frequenz, Phasenverschiebung	→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Planungsdaten	Prognose	Prognosemodell und Teilobjekte festlegen	→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Planungsdaten	Fahrplan	Fahrplanmodell und Teilobjekte festlegen	→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Planungsdaten	Flexibilität	Flexibilitätsmodell und Teilobjekte noch zu definieren	inkl. Randbedinungen wie Wartezeiten, Flex.intervalle, Gradienten, Abhängigkeiten) → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten

Marktdaten	Preise		→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Steuerdaten	Leistungsvorgaben	An- und Aussignale Zeit	Übersendung von Signalen zum An- und Abschalten von Geräten → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Steuerdaten	Statusinformationen	Zustände	Nachrichten von Steuerungs-einrichtungen über aktuelle Anlagenzustände → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Steuerdaten	Leistungsvorgaben	Leistung Zeit	Vorgabe Leistungsverläufe in der Zeit für Verbrauch / Erzeugung (**Leistungszeitreihen – P * t = Energie) oder Zeitreihen mit Leistungsänderungen zu Zeitpunkten – dP / dt = Flexibilität**) → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Konfigurationsdaten	Kommunikations-einstellungen, Programmdaten	Konfiguration SMGW, Software-Updates, Kommunikationsfreigaben	Prozesse des GWA nach Technischer Richtlinie BSI; → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Konfigurationsdaten	Zielvorgaben	Prioritäten, Regeln, Einsatzzeiten	Rahmenbedingungen der Anlagen und der Anwender → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Stammdaten	Gerätedaten	Standorte, Funktionen, Betreiber	→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Transaktionsdaten	Protokolle	Prozessschritte	Dokumentation der Prozessschritte für Protokollpflichten, Abrechnung und Nicht-Abtreitbarkeit → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Kommunikations-daten	Kommunikations-schemen; Protokolle	z.B. URI-Schemata	Hier nur Beispiel, zu definieren sind Schemata der Anwendungs-schnittstelle zur Nutzung des CLS-Kanales → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten

Im Weiteren sind die zum Use Case definierten Kommunikationsanforderungen zu betrachten. Untersucht wird, welche Daten von welchen Komponenten auf welche Weise ausgetaucht werden, um hierzu informationstechnische Schutzanforderungen hinzuzufügen.

Kommunikationsschnittstelle			**Inhalt der Nachricht**	**Schutzanforderungen**
Von	Bis	**Schnitt-stelle**		
mMe SMGW	SMGW mMe	**S1**	Messdaten Energie und Leistung für Markt sowie Zählerstandsgänge Messdaten Netzqualität Konfigurationsdaten	definiert über BSI-Schutzprofil
SMGW HAN EMG	EMG SMGW CLS	**S2**	Messdaten mMe lokal vom SMGW an EMG Messdaten von Sub-Metering, Planungsdaten, Statusinformationen, Marktdaten	SMGW transportiert Daten von mMe's sicher über HAN-Schnittstelle an GEMS Messdaten vom GEMS (Sub-Metering) mit Nutzung und Abschluss des sicheren, transparenten Kommunikationskanals über SMGW
SMGW CLS CLS-Modul	CLS-Modul SMGW CLS	**S3a**	**Verschlüsselter und signierter Payload mit beliebigen Daten;** Kommunikationsdaten	Nutzung und Abschluss des sicheren, transparenten Kommunikationskanals über SMGW
CLS-Modul als Teil Steuerbox, Anlage oder EMG Sub-Metering, Sensorik,	Sub-Metering, Sensorik, CLS-Modul als Teil Steuerbox, Anlage oder EMG	**S3b**	Anforderung Messdaten Sub-Metering, Messdaten und Status der Geräte, Anlagen sowie von Umwelt zu einem bestimmten Zeitpunkt; evtl. auch Anforderung zur Übermittlung von Prognosen, Fahrplänen, Flexibilität direkt aus den Anlagen; Kommunikationsdaten Bereitstellung von Messdaten Sub-Metering, Messdaten und Status der Geräte, Anlagen sowie von Umwelt zu einem bestimmten Zeitpunkt; Bereitstellung von Prognosen, Fahrplänen, Flexibilität direkt aus den Anlagen; Kommunikationsdaten	Nutzung und Abschluss des sicheren, transparenten Kommunikationskanals über SMGW Nutzung und Abschluss des sicheren, transparenten Kommunikationskanals über SMGW Informationssicherheit bei Verbindung zu CLS-Modul EMG über Kommunikation im Gebäudenetz (LAN) gewährleisten, Abspeicherung und Aggregation von Daten im EMG vor Weitergabe → Manipulationsfreiheit gewährleisten
CLS-Modul als Teil Steuerbox, Anlage oder EMG Aktorik	Aktorik CLS-Modul als Teil Steuerbox, Anlage oder EMG	**S3b**	Steuerdaten, Konfigurationsdaten inkl. der Vorgabe von Fahrplänen, Flexibilität an Anlagen; Statusdaten (Ereignisse)	Informationssicherheit bei Verbindung von CLS-Modul EMG zu Aktorik über Kommunikation im Gebäudenetz (LAN) gewährleisten, Abspeicherung von Daten im EMG vor Weitergabe → Manipulationsfreiheit der Steuerung gewährleisten
SMGW	GWA und EMT-Plattform	**S4**	Verschlüsselter und signierter Payload mit beliebigen Daten;	Anforderungen gemäß BSI-Schutzprofil;

GWA und EMT-Plattform	SMGW		Kommunikationsdaten	
EMG, S5-WAN-Router Sub-Metering, Sensorik,	Sub-Metering, Sensorik zu Anlagen und Umwelt EMG, S5-WAN-Router	**S5**	Anforderung Messdaten Sub-Metering, Messdaten und Status der Geräte, Anlagen sowie von Umwelt zu einem bestimmten Zeitpunkt; evtl. auch Anforderung zur Übermittlung von Prognosen, Fahrplänen, Flexibilität direkt aus den Anlagen; Kommunikationsdaten Bereitstellung von Messdaten Sub-Metering, Messdaten und Status der Geräte, Anlagen sowie von Umwelt zu einem bestimmten Zeitpunkt; Bereitstellung von Prognosen, Fahrplänen, Flexibilität direkt aus den Anlagen; Kommunikationsdaten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation über private Kommunikationsnetze; Rückwirkungsfreiheit zu HAN-Kommunikation des SMGW
EMG, S5-WAN-Router Aktorik	Aktorik EMG, S5-WAN-Router	**S5**	Steuerdaten, Konfigurationsdaten inkl. der Vorgabe von Fahrplänen, Flexibilität an Anlagen; Statusdaten (Ereignisse)	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation über private Kommunikationsnetze; Rückwirkungsfreiheit zu HAN-Kommunikation des SMGW
EMG CEMS EMG GEMS EMG GEMS, S5-WAN-Router S5-WAN-Router	EMG GEMS, S5-WAN-Router S5-WAN-Router EMG CEMS EMG GEMS	**S5**	Messdaten, Planungsdaten, Marktdaten, Steuerdaten, Konfig.daten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation über private Kommunikationsnetze; Rückwirkungsfreiheit zu HAN-Kommunikation des SMGW
S5-WAN-Router Betriebskomp. Markt und Netz	Betriebskomp. Markt und Netz S5-WAN-Router	**S6b**	Messdaten, Planungsdaten, Marktdaten, Steuerdaten, Konfig.daten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation über öffentliche Kommunikationsnetze;
EMT-Plattform	Betriebskomp. Markt	**S6a**	Messdaten, Planungsdaten, Marktdaten, Steuerdaten, Konfig.daten sicher weiter geleitet aus den Liegenschaftszellen	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen GWA/EMT-Infrastruktur und Marktpartnern – Anforderungen im BSI-Schutzprofil??
EMT-Plattform	Komponente Messstellen-betrieb	**S6a**	Messdaten, Gerätedaten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen GWA/EMT-Infrastruktur und Marktpartnern – Anforderungen im BSI-Schutzprofil??

EMT-Plattform	Basisdienste IoT-Plattform	**S6a**	Planungsdaten, Stammdaten, Transaktionsdaten, Kommunikationsschemen	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen GWA/EMT-Infrastruktur und Marktpartnern – Anforderungen im BSI-Schutzprofil??
EMT-Plattform	Infosystem Messdaten	**S6a**	Hochaufgelöste Messdaten von mMe und weiteren Submetern / Sensorik	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen GWA/EMT-Infrastruktur und Marktpartnern – Anforderungen im BSI-Schutzprofil??
EMT-Plattform GWA	GWA EMT-Plattform	**S7**	Kommunikationsdaten und Qittungsmeldungen	Anforderungen gemäß BSI-Schutzprofil;
Komponente Messstellen-betrieb	Komponenten Energieliefer. Energiehandel	**S8**	Messdaten, Gerätedaten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen Marktpartnern außerhalb BSI-Schutzprofil; Unverfälschbarkeit der Marktdaten (Handel, Fahrpläne, Abrechnungen, Transaktionen) sicherstellen
EMT-Plattform	Komponente Leitwarte Fernwirkung und Netzmonit.	**S9**	Planungsdaten, Konfigurationsdaten, Hochaufgelöste Messdaten der Powerqualität	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen GWA/EMT-Infrastruktur und Netzbetreiber – Anforderungen im BSI-Schutzprofil?? Unzulässige Manipulation zum Netzbetrieb sicherstellen
Komponente Leitwarte Flexibilitäts-prozesse	Flexibilitäts-plattform	**S10**	Planungs- und Marktdaten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen Netzpartnern außerhalb BSI-Schutzprofil; Unverfälschbarkeit der Flexibilitätsdaten sicherstellen, um Rückwirkung auf Netzbetrieb zu verhindern
Komponente Leitwarte Abstimmungs-kaskade VNB	Komponente Leitwarte Abstimmungs-kaskade ÜNB	**S11**	Planungsdaten, Steuerdaten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen Netzpartnern außerhalb BSI-Schutzprofil; Unverfälschbarkeit der Abstimmungsdaten sicherstellen, um Rückwirkung auf Netzbetrieb zu verhindern
Komponenten Energieliefer. Energiehandel	Marktplatt-formen	**S12**	Planungsdaten, Marktdaten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen Marktpartnern außerhalb BSI-Schutzprofil; Unverfälschbarkeit der Marktdaten (Handel, Fahrpläne, Abrechnungen, Transaktionen) sicherstellen
Betriebskomp. Markt	Marktplatt-formen	**S12**	Planungsdaten, Marktdaten	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen Marktpartnern außerhalb BSI-Schutzprofil; Unverfälschbarkeit der Marktdaten (Handel, Fahrpläne, Abrechnungen, Transaktionen) sicherstellen

2.5 Bestimmung von Schutzmaßnahmen

Vorgehensweise

Folgender Prozess wurde bisher beschrieben.

Mit der im Schritt 1 durchgeführte **Use Case Analyse** erfolgte die Formulierung von Schutzbedürfnissen.

Die im Schritt 2 folgende **Risikoanalyse** ermittelt Bedrohungen, die die Schutzbedürfnisse verletzen können. Mit der Bestimmung des Auswirkungsgrades bei Verletzungen sowie der Eintrittswahrscheinlichkeit werden Schutzziele formuliert.

Schritt 3 widmet sich der **Analyse von Schutzanforderungen**, um Schutzziele einhalten zu können.

Dies ist wiederum im Schritt 4 die Grundlage, um entsprechende **Schutzmaßnahmen** festzulegen, deren Umsetzung die Einhaltung der Anforderungen gewährleistet.

Schnittstellenliste und grundlegende Sicherheitsmaßnahmen

SchnittstelleNr_ Nachricht-Nr	Absenderkomponente Zielkomponente	Informationen	Sicherheitsmaßnahmen
S01_01	mMe - SMGW	Messdaten Energie und Leistung für Markt sowie Zählerstandsgänge, Messdaten Netzqualität	
S01_02	SMGW - mMe	Konfigurationsdaten	
S02_01	SMGW HAN – EMG	Messdaten mMe lokal vom SMGW an EMG	
S03a_01	SMGW CLS – CLS-Modul	Verschlüsselter und signierter Payload mit beliebigen Daten	
S03a_02	CLS-Modul – SMGW CLS	Kommunikationsdaten	
S03b_01	CLS-Modul als Teil Steuerbox, Anlage oder EMG – Sub-Metering, Sensorik	Anforderung von Messdaten zu Sub-Metering, zu Umwelt und Anlagen-Stati sowie bei Anlagen zu Prognosen, Flexibilität und Fahrplänen	
S03b_02	Sub-Metering, Sensorik - CLS-Modul als Teil Steuerbox, Anlage oder EMG	Lieferung von Messdaten zu Sub-Metering, zu Umwelt und Anlagen-Stati sowie bei Anlagen von Prognosen, Flexibilität und Fahrplänen	
S03b_03	CLS-Modul als Teil Steuerbox, Anlage oder EMG – Aktorik	Steuerdaten, Konfigurationsdaten inkl. der Vorgabe von Fahrplänen, Flexibilität an Anlagen	
S03b_04	Aktorik - CLS-Modul als Teil Steuerbox, Anlage oder EMG	Status- und Ereignisdaten	
S04_01	SMGW - GWA und EMT-Plattform	Verschlüsselter und signierter Payload mit beliebigen Daten	
S04_01	GWA und EMT-Plattform - SMGW	Kommunikationsdaten	
S05_01	EMG, S5-WAN-Router - Sub-Metering, Sensorik	Anforderung von Messdaten zu Sub-Metering, zu Umwelt und Anlagen-Stati sowie bei Anlagen zu Prognosen, Flexibilität und Fahrplänen	
S05_02	Sub-Metering, Sensorik - EMG, S5-WAN-Router	Lieferung von Messdaten zu Sub-Metering, zu Umwelt und Anlagen-Stati sowie bei Anlagen von Prognosen, Flexibilität und Fahrplänen	

S05_03	EMG, S5-WAN-Router - Sub-Metering, Aktorik	Steuerdaten, Konfigurationsdaten inkl. der Vorgabe von Fahrplänen, Flexibilität an Anlagen	
S05_04	Aktorik - EMG, S5-WAN-Router	Status- und Ereignisdaten	
S05_05	EMG CEMS - EMG GEMS, S5-WAN-Router oder EMG GEMS – S5-WAN-Router	Messdaten, Planungsdaten, Marktdaten, Steuerdaten	
S05_06	EMG GEMS, S5-WAN-Router – EMG CEMS oder S5-WAN-Router - EMG GEMS	Planungsdaten, Marktdaten, Steuerdaten	
S06a_01	EMT-Plattform - Betriebskomp. Markt	Messdaten, Planungsdaten, Marktdaten, Steuerdaten, Konfig.daten sicher weiter geleitet aus den Liegenschaftszellen	
S06a_02	EMT-Plattform - Komponente Messstellenbetrieb	Messdaten, Gerätedaten	
S06a_03	EMT-Plattform - Basisdienste IoT-Plattform	Planungsdaten, Stammdaten, Transaktionsdaten, Kommunikationsschemen	
S06a_04	EMT-Plattform - Infosystem Messdaten	Hochaufgelöste Messdaten von mMe und weiteren Submetern / Sensorik	
S06b_01	S5-WAN-Router – Betriebs-komp. Markt und Netz	Messdaten, Planungsdaten, Marktdaten, Steuerdaten, Konfig.daten	
S06b_02	Betriebskomp. Markt und Netz - S5-WAN-Router	Planungsdaten, Marktdaten, Steuerdaten	
S07_01	EMT-Plattform – GWA	Kommunikationsdaten	
S07_02	GWA – EMT-Plattform	Quittungsmeldungen, Statusdaten	
S08_01	Komponente Messstellen-betrieb - Komponenten Energieliefer. Energiehandel	Messdaten, Gerätedaten	
S09_01	EMT-Plattform - Komponente Leitwarte Fernwirkung und Netzmonit.	Hochaufgelöste Messdaten der Powerqualität	
S09_02	Komponente Leitwarte Fernwirkung und Netzmonit. - EMT-Plattform	Planungsdaten, Steuerdaten, Konfigurationsdaten,	
S10_01	Komponente Leitwarte Flex.prozesse – Flex.plattform	Planungs- und Marktdaten	
S10-0n			
S11_01	Komponente Leitwarte Abstimmungskaskade VNB – Abstimmungskaskade ÜNB	Planungsdaten, Steuerdaten	
S11_02	Komponente Leitwarte Abstimmungskaskade ÜNB – Abstimmungskaskade VNB	Planungsdaten, Steuerdaten	
S12_01	Komponenten Energieliefer. Energiehandel – Marktplattformen	Planungs- und Marktdaten	
S12_02	Marktplattformen - Komponenten Energieliefer. Energiehandel	Planungs- und Marktdaten	

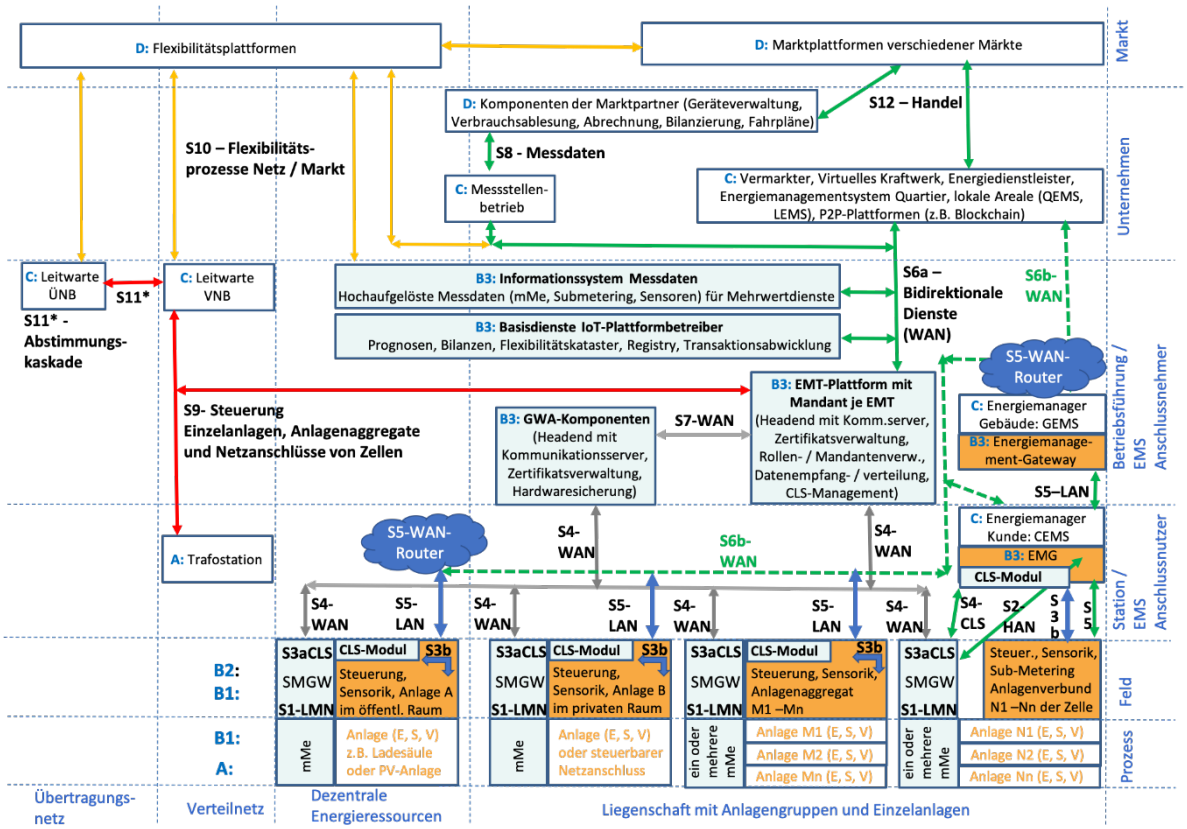

Abb. 8: Schnittstellenarchitektur S1 bis S12

3 Schutzbedarfsanalyse AutonomieLab Leimen

3.1 Schutzbedürfnisse in der autonomen Wohngebäudezelle

Autonomie ist erstens legitimes Gestaltungsinteresse des Einzelnen und von Gemeinschaften sowie zweitens Grundlage für eine geringere Verletzlichkeit (Vulnerabilität) der Lebensfunktionen bei externen Störungen.

Gleichzeitig verfolgen Menschen als soziale Wesen gemeinschaftliche Interessen sowie zeigen die Fähigkeit zur gegenseitigen Unterstützung. Gerade bezüglich der Verfügbarkeit von Energie als Grundbedürfnis des menschlichen Lebens ist das solidarische Handeln im Energieverbundsystem so bedeutsam.

Die Gestaltung von Autonomie und Verbund erhöht die Widerstandsfähigkeit (Resilienz) eines Gesamtsystem als zellulärer Energieorganismus gegenüber ausschließlich zentral produzierenden und gesteuerten Systemen. Zwischen lokaler und regionaler sowie globaler Gestaltung ist das Optimum zu finden. Insbesondere erfordert die Notwendigkeit einer nachhaltige Stadtentwicklung die Erhöhung der Widerstandsfähigkeit durch Maßnahmen zur Klimaanpassung als auch zur Bereitstellung autonomer Infrastrukturfunktionen für Energie, Wasser, Ernährung und Logistik.

Die Corona-Krise zeigte eindrucksvoll, dass ein ausschließlich auf Globalisierung, Zentralisierung sowie Lean Management mit Lieferketten in Echtzeit und fehlender Speicherfähigkeit ausgerichteter Weg das System gegenüber unerwarteten Ereignissen sehr empfindlich reagieren lässt.

Die Systemflexibilität wird durch das Wechselspiel von Autonomie und Verbund erhöht, benötigt aber hierzu auch Speicherfähigkeit innerhalb autonomer Strukturen.

Die Betrachtung der Schutzbedürfnisse umfasst damit die Gewährleistung des autonomen Betriebs als auch der Systemdienlichkeit im Verbund inklusive der Steuerbarkeit zur Nutzung der Speicherfähigkeit in der Wohngebäudezelle.

Die Methodik zur Ableitung und Umsetzung von Schutzmaßnahmen umfasst die sechs Schritte der nachfolgenden Abbildung.

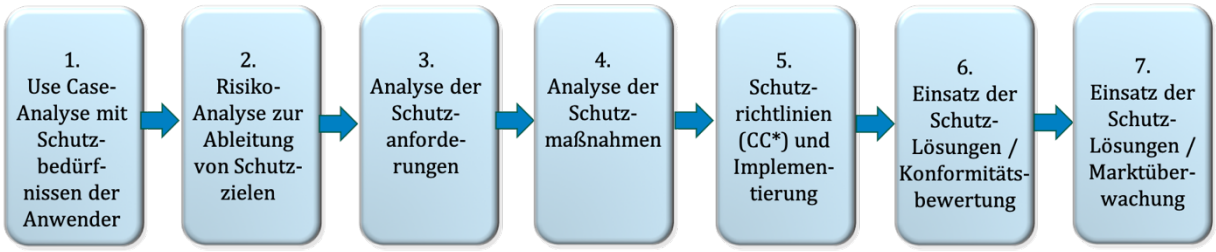

Abb. 9: Prozess der Schutzmethodik

Betrachtet werden im Rahmen der nachfolgenden Musterlösung nur die ersten vier Schritte beispielhaft bis zur Ableitung von Schutzmaßnahmen.

3.2 Use Case-Analyse

Grundlage zur Ermittlung der auf Use Cases bezogenen Schutzbedürfnisse und Bedrohungen ist die Kenntnis von

- Rollen mit verantwortlichen Akteuren
- zugehörige technische, legislative und regulatorische Rahmenbedingungen
- Komponenten mit Mapping auf die Komponentenarchitektur inklusive Zuordnung von Domänen und Zonen aus dem Smart Grid Architekturmodell sowie

Hierzu werden die entsprechenden Aufstellungen aus der Use Case-Beschreibung „HLUCs 050G, 050H, 050I - Sichere Integration von Geräten/Anlagen/Zellen“ [Kießling, A. et al (03/2021)] übernommen (Erläuterungen siehe auch Schritt 2 Use Case Methodik, [Kießling, A., Bogensberger, A., Köppl, S. & Faller, F. (03/2020)]).

Rollen- und Akteursliste

Rolle / Akteur „wer?“	Verantwortlichkeiten und Aufgaben „was?“	Schutzbedürfnisse
Energieanlageneigentümer (EAE)	Bereitstellung von Erzeugung- / Speicher- und Verbrauchseinrichtungen für Energie (Strom, Wärme, Gas); Aufgaben kann Prosument selbst übernehmen oder durch einen Energieanlagenbetreiber durchführen lassen;	bei Stromausfall Weiterbetrieb notwendiger Geräte und damit auch Schutz von Geräten;
Einsatzverantwortlicher (EIV); Energieanlagenbetreiber (EAB)	Betrieb von Erzeugungs- und Speichereinrichtungen in Objekten des Quartiers/Areals, die während Störungszeit des Netzes Strom zur Notversorgung der Verbrauchseinrichtungen in anderen Objekten des Quartiers / Areals liefern; Betrieb abschaltbarer Verbraucher in Form Smart-Grid-fähiger, elektrischer Geräte, Anlagen, Betriebs-mittel, damit Betrieb der wichtigsten Verbraucher im Notbetrieb priorisiert gewährleistet werden; hier identisch mit EAE	bei Stromausfall Weiterbetrieb notwendiger Geräte und damit auch Schutz von Geräten;
Prosument	Nutzung von Erzeugung- / Speicher- und Verbrauchseinrichtungen für Energie (Strom, Wärme, Gas) für Energielieferung und -bezug sowie Flexibilitätsleistung und -nutzung durch Nutzung von Speicher-, Verschiebepotentialen und Gerätepriorisierung, wobei sich das Gesamtsystem aus diesen Einrichtungen im Notfall auch selbst versorgt; Änderung von bezogener Wirk- und Bildleistung der Erzeugung- / Speicher- und Verbrauchseinrichtungen gegenüber einer anderen Planung oder Prognose Betreiber von Kunden-Energiemanagement-Systemen; hier identisch mit EAE	bei Stromausfall Weiterbetrieb notwendiger Geräte und damit auch Schutz von Geräten;
Anschlussnehmer	hat Anschlussvertrag mit Netzbetreiber für Bezugs- und Einspeiseleistungen; Eigentümer vom Netzan-schluss am jeweiligen Objekt oder Anlagensystem; verantwortlich für die Einhaltung der Netzanschluss-bedingungen und der Netzverbindung zu internen Prosumenten; Am Netzanschluss entstehen Bezug und Einspeisung der im Objekt des Anschlussnehmers wirkenden Prosumenten. Bei mehreren Prosumenten, d.h. mehreren Objekten mit einem gemeinsamen Netzanschluss, der zeitweise gestört sein kann, wird Einrichtung zur	Energiemanagementlösungen in einzelnen Reihenhäusern dürfen WEG-Gesamtsystem nicht beeinträchtigen

Rolle / Akteur „wer?“	Verantwortlichkeiten und Aufgaben „was?“	Schutzbedürfnisse
	Netzabschaltung, zum Netzweiterbetrieb und zur Wiederzuschaltung benötigt, wobei eine interne Netzverbindung zur Zuschaltung zwischen verschiedenen Prosumenten notwendig ist; hier gemeinsamer Netzanschluss der WEG im Quartier mit 7 Reihenhäusern als AN	
Anschlussnutzer	hat Anschlussbezugsvertrag oder -einspeisevertrag mit Lieferanten oder Vermarktern und ist Nutzer des Netzanschlusses zu Strombezug und -lieferung; hier 7 Reihenhäuser als 7 Anschlussnutzer des gemeinsamen WEG-Netzanschlusses	autonome Systemsicherheit trotz Verbund in WEG gewährleisten
Facility-Betreiber	Betreiber und/oder Inhaber einer Gebäudezelle oder eines Quartieres, wo Erzeugungs- / Speicher- und Verbrauchseinrichtungen installiert werden; Kommunikationsinfrastruktur für alle Anlagen / Geräte sowie Energiemanagement (EM)-Framework für ein lokales EM-System im Anlagenverbund Betreiber von Gebäude-Energiemanagement-systemen; hier 7 Eigentümer als Facility-Betreiber der 7 Reihenhäuser im AutonomieLab Leimen unter Verbindung von zwei Reihenhäusern als autonome, inselfähige Nachbarschaftszelle mit Notstrombetrieb bei externen Netzausfall	Hausbetrieb mit höherer Versorgungssicherheit und evtl. finanzielle Anreiz für Systemdienstleistung im Quartier
Verteilnetzbetreiber (VNB)	Bereitstellen des Netzanschlusses, Ermöglichung der Nutzung des Stromnetzes, Sicherstellen der Versorgungssicherheit und Netzstabilität mit abschaltbarem und wiederzuschaltbarem Netzanschluss	Kommunikation zum digitalen Netzanschluss darf keine Rückwirkungen auf den sicheren Netzbetrieb haben
Messstellenbetreiber (MSB)	Einbau, Betrieb und Wartung von modernen Messeinrichtungen zur Ermittlung und Übermittlung von Messwerten; Übertragung der Messdaten aus Erzeugung und Verbrauch an lokales EM-System über HAN-Schnittstelle an Energiemanagement-system und Anzeige; im Falle des Inselbetriebes sind Messdaten lokal zu speichern und nach Wiederherstellung der Verbindung an die externen Empfänger zu übertragen	Visualisierung Energieflüsse steht sicher auch lokal zur Verfügung, wenn externe Verbindung fehlt
Gateway-Administrator	Verwaltung der technischen Verbindung zu Smart Meter Gateway mit verschiedenen Stakeholdern; Betrieb eines Gateway-Administrationssystems als IIS-Komponente; Im produktiven Betrieb sichere Beendigung und Wiederherstellung der Funktionen des GWA mit Herstellung und Beendigung Inselbetrieb, da während Inselbetrieb Verlust der externen Kommunikation; u.U. identisch mit MSB	Sicherheit nach BSI-Schutzprofil und Technischer Richtlinie
EMT-Plattform-Betreiber	Verantwortung für Kommunikationsdienste: Stellt Kommunikations-Infrastruktur mit aEMT-Basisfunktionen als sichere Integrationsumgebung zu Zellen, Geräten, Anlagen, aufbereitete Markt- und Statusinformationen sowie Nutzung des Steuer- und Kommunikationskanals bereit; CLS-Management inklusive Koordination konkurierender Zugriffe	Sicherheit nach BSI-Schutzprofil und Technischer Richtlinie

Rolle / Akteur „wer?“	Verantwortlichkeiten und Aufgaben „was?“	Schutzbedürfnisse
Informationssystem-Betreiber	Verantwortung für weitere Informationsdienste: Betrieb diskriminierungsfreier IKT-Unterstützungsdienste (hochaufgelöste Messdatenverwaltung, Registry, Energiebilanzen, Prognosen, Flexibilitätskataster, Transaktionsabwicklung und -sicherung, Kommunikationsprofile)	
Kommunikationssystem-Betreiber	Sicherung der Kommunikation an Anschlusspunkten innerhalb der Zelle und Übertragung an lokalen Energiemanager; hier in Verantwortung bei Facility-Betreiber; Sicherung der externen Kommunikation in Verantwortung des MSB	Sicherung der internen Kommunikation bei Vorliegen eines privaten WAN-Zugangs umfasst auch Schutz von Komponenten gegen Angriffe im Internet der Dinge
Kunden-Energiemanagementsystem-Anbieter im Gebäude (GEMS)	Betrieb eines Gebäude-Energiemanagementsystems (GEMS) auf Basis der Plattform OGEMA (Energiemanagement-Gateway) mit Funktionen zur Regelung der Energieflüsse zwischen den Häusern und priorisierten Anlagen	Sicherung der internen Kommunikation zum GEMS bei Vorliegen eines privaten WAN-Zugangs umfasst auch Schutz von Komponenten gegen Angriffe aus dem Internet auf Energieanlagen
Energieanlageninstallateur	Elektrohandwerks für die Installation und Reparatur von elektrischen Anlagen	Remote bedienbare Service-Interfaces dürfen nicht zu Angriffen aus dem Internet auf Energieanlagen führen
Energienetzausrüstungs-hersteller	Bereitstellung von Netzkomponenten inkl. Mess- und Steuerungseinrichtungen zur Integration von Prosumenten, insbesondere von selbsttätiger Schaltstelle, Koppelschutz und Netzersatzeinrichtung zur Erhaltung Power-Qualität sowie Herstellung Verbindung zu VNB zur Wiederherstellung der Verbindung	Remote bedienbare Service-Interfaces dürfen nicht zu Angriffen aus dem Internet auf Energieanlagen führen
Systemdienstleistungs-anbieter	Betrieb einer technischen Ressource, die Energie nutzt oder erzeugt mit Wechselrichter mit Funktionen zur sicheren Netzabtrennung für Inselbetrieb, Erhaltung Netzqualität in den Gebäuden während Inselbetrieb und Wiedersynchronisierung mit Ende Netzstörung; hier durch Wechselrichter eines Gebäudes der Nachbarschaftszelle sowie durch Relais im Objekt zur Netzab- und Inselzuschaltung sowie Herstellung Gebäudeverbund im Inselfall sowie Umkehrung	Remote bedienbare Service-Interfaces dürfen nicht zu Angriffen aus dem Internet auf Stromverfügbarkeit im Gebäudeverbund führen

Rahmenbedingungen (legislativ, regulatorisch und technisch):

Übernahme der Rahmenbedingungen aus der Use Case-Beschreibung zur Feststellung eventuell weiterer sicherheitsrelevanter Aspekte

Rahmenbedingungen (z.B. Datenschutz, Anschlussbedingungen, Zeitverhalten, Verfügbarkeit, betroffene Nutzergruppen, usw.)	Wirkung des Themas auf den Anwendungsfall	Verweise auf Gesetze und Regelungen
Gewährleistung von Datenschutz	Einsatz intelligenter Messsysteme	Digitalisierungsgesetz, Schutzprofil und techn. Richtlinie BSI
Gesetzliche und regulatorische Rahmenbedingungen	Beachtung der Netzampel, Koordinationsfunktion	EEG, EnWG, StromNEV
Messdatenbereitstellung in Echtzeit	aktuell nur über unzertifizierte iMSys	Weitere Zertifizierung von dazu notwendigen Tarifregistern in 2. Phase für Rollout Messsysteme
Steuerprozesse zu Anlagen	CLS-Kanal-Nutzung als aEMT: Übergabe des Steuerbefehls, Ausführen des Steuerbefehls, Übergabe von Statusinformationen, Interaktion mit GWA; CLS-Kanal-Management	Weitere dazu notwendiger Prozessspezifikationen in 2. Phase für Rollout Messsysteme im Rahmen der Normung in Verbindung mit BSI
Koordinationsrolle des Netzbetreibers	aktuell noch unklarer Rahmen	FNN-Position
Bewertung der Lösung aus Sicht der internen Quartiersenergielieferung	Geschäftsmodell und regulatorischen Rahmen bewerten	
Bewertung der Lösung aus Sicht der Backendsysteme von Energiedienst-leistern und Netzbetreibern	Sicherheit und Datenschutz an den Schnittstellen zwischen zertifizierter Umgebung und den Systemen weitere Akteure	
Scope des Use Cases ist das Wohngebäude und damit sind betroffene Nutzergruppe die darin wohnenden Familien	Schutzbedürfnisse aus Sicht der Bewohner formulieren	Privatrechtliche Haftungsfragen bezüglich der Betroffenheit weiterer Gebäude-Infrastrukturen

Komponentenliste

Schutzbedürfnisse können durch Anwender (siehe Rollen) für Systeme oder Teilsysteme oder einzelne Komponenten definiert werden, die im Rahmen einer eventuellen Datenspeicherung sowie ihrer Funktionalitäten sowohl Aspekte der Versorgungssicherheit und der Betriebssicherheit betreffen.

Den Komponenten sind danach auf Basis der Betrachtung benötigter Funktionen Schutzbedürfnisse hinzuzufügen. Die weitere Detaillierung ist im Rahmen eines Zertifizierungsprozesse zum Informationssicherheits-Management vorzunehmen.
Der Fokus liegt dabei auf informationstechnischen und nicht auf elektrotechnischen Anforderungen.

Gliederung Komponenten in Kategorien A bis D **Komponenten** **Rolle des Betreibers**	**D: Domäne** **B: Betriebszone**	**Funktionen** **Schutzbedürfnisse**
A: Assets Verbraucher inkl. Ladepunkt in den Gebäuden Y und Z Anschlussnehmer, Konsument, Facility-Betreiber (EIV: Einsatzverantwortlicher)	D: Gebäude B: Prozess	Steuerbare Senke von Energieflüssen innerhalb der zwei Gebäude; an- und ausschaltbar über externe Schaltgeräte; Betrieb von aEMT-Plattform und externem Energiemanagement-System darf nicht - den Assetbetrieb stören, - zu Beeinträchtigungen bei Endkunden führen, - nicht weitere Infrastrukturen des Endkunden stören, - Informationen zu Assets des Endkunden unerlaubt weitergeben, - zu Vertrauensverlusten gegenüber dem Betreiber führen und - zu keinen finanziellen Schäden beim Betreiber führen
A: Assets Speicher (Batterie) im Gebäude Y	D: Gebäude B: Prozess	Steuerbare Senke und Quelle von Energieflüssen innerhalb der zwei Gebäude; Lieferung von Statusinformationen (**aktuelle Kapazität**), Entgegennahme von Steueranweisungen;

Gliederung Komponenten in Kategorien A bis D Komponenten Rolle des Betreibers	D: Domäne B: Betriebszone	Funktionen Schutzbedürfnisse
Anschlussnehmer, Prosument, Facility-Betreiber (EIV: Einsatzverantwortlicher)		Siehe Verbraucher
A: Assets Erzeuger im Gebäude Y als PV-Anlage Anschlussnehmer, Produzent, Facility-Betreiber (EIV: Einsatzverantwortlicher)	D: Gebäude B: Prozess	Steuerbare Quelle von Energieflüssen innerhalb der zwei Gebäude; Lieferung von Statusinformationen; Siehe Verbraucher
A: Assets PV-Schutzeinrichtung sowie Schütz am Netzanschluss zur Netzabtrennung sowie inselfähiger, einphasiger Wechselrichter Anschlussnehmer, Facility-Betreiber (EIV: Einsatzverantwortlicher)	D: Gebäude B: Prozess	Schutzeinrichtung und Erhaltung Netzfrequenz sowie Spannung (z.B. entsprechend ausgestatteter, gemeinsamer Wechselrichter für PV-Anlage und Batterie), abschaltbarer Netzanschluss von Gebäuden, Wiederzuschaltung durch Remote-Zugriff Netzbetreiber möglich; Siehe Verbraucher
A: Assets Ein gemeinsamer Netzanschluss für Bezug Haus Y und Z (inkl. Wärmepumpe, Ladepunkt im Haus Y) sowie Einspeisung im Haus Y Verteilnetzbetreiber	D: Gebäude B: Prozess	Bündelung von Gebäudestandardbezug sowie steuerbaren Einzelanlagen (PV, Batterie, WP, LP in einem Netzanschluss), wobei die Steuerbarkeit der Einzelanlagen darüber bereitgestellt werden kann; Siehe Verbraucher
A: Assets USV am gemeinsamen Netzanschluss Anschlussnehmer, Facility-Betreiber (EIV: Einsatzverantwortlicher)	D: Gebäude B: Prozess	am gemeinsamen Netzanschluss unterbrechungsfreier Weiterbetrieb der Mess- / Komm.- und Steuereinrichtungen beim Übergang von Netz- zu Inselbetrieb in der Phase der Abschaltung vom externen Netz bis zur Umschaltung auf Inselbetrieb; Siehe Verbraucher
B1: Sensorik / Aktorik Sensorik PV-Erzeugung und Batterieladezustand sowie Einzelverbräuche Anschlussnehmer, Prosument Facility-Betreiber (EIV: Einsatzverantwortlicher)	D: Gebäude B:Prozess	Messung der aktuellen PV-Einspeisung und des Ladezustandes der Batterie, um mögliche Maximallast für Gebäude zu bestimmen sowie Messung der Einzelverbräuche von Geräten und Anlagen im Gebäude, Übertragung Messwerte an GEMS; Daten dürfen nicht durch externe Akteure ermittelbar sein
B1: Sensorik / Aktorik moderne Messeinrichtung (mMe) Messstellenbetreiber (MSB)	D: Gebäude B: Feld	Messung und Erfassung der Energiedaten (Zweirichtungszähler als Hauptzähler am Netzanschluss sowie Einrichtungszähler Verbrauch für WP und für LP sowie Erzeugung PV-Anlage als auch Zweirichtungszähler für Batterie; Betrieb Plattform MSB soll nicht - zu Beeinträchtigungen der Messwerterfassung beim Endkunden führen, - Messung an weiteren Infrastrukturen des Endkunden stören, zu Verletzungen des Datenschutzes bezüglich der gemessenen Energieflüsse beim Endkunden führen,
B1: Sensorik / Aktorik Steuereinrichtung (entsprechend Anschlussbedingungen (FNN) – Steuerbox (digitales CLS-Modul) Verteilnetzbetreiber und/oder Einsatzverantwortlicher	D: Gebäude B: Feld	Digitale Steuerbox am Netzanschluss zum Einstellen der Leistung der Gebäude (Plim-Signal) als Zelle zu definierten Zeitpunkten über bestimmte Zeitdauern zur Umsetzung und Disaggregation der Gesamtleistung zu Einzelleistungen an Geräten / Anlagen in den Häusern Y und Z über die EMS der Gebäude,

Gliederung Komponenten in Kategorien A bis D Komponenten Rolle des Betreibers	D: Domäne B: Betriebszone	Funktionen Schutzbedürfnisse
		Erfassung der Statusinformation der Steuereinrichtung (gestört / nicht gestört / Regelzustand), Einrichtung zum VNB am Anschlusspunkt zur Entgegennahme des Signals zur Wiederverbindung; Betrieb Plattform MSB soll nicht - zu Beeinträchtigungen der Steuerungsfähigkeit beim Endkunden führen, - sonstige Steuerungsfunktionen im Smart Building anderer Handlungssektoren des Endkunden stören, zu Verletzungen der Informationssicherheit oder der IKT-Zuverlässigkeit in den Systemen des Endkunden führen,
B1: Sensorik / Aktorik Aktorik an Netztrennschütz sowie an Einzelanlagen und Geräten jeweils als Schaltgeräte 1 bis N in den Gebäuden Y und Z Einsatzverantwortlicher	D: Gebäude B: Feld	Steuern der Leistung der Einzelanlagen, Betrieb der Steuerungseinrichtungen darf die Sicherheit des Anlagenbetriebs nicht beeinträchtigen, Das Energiesystem im Gebäude darf nicht angreifbar sein, wenn Aktorik über EMS und Internetzugang des Gebäudes mit externen Energiedienstleistern verbunden ist.
B2: Kommunikations-komponenten Smart Meter Gateway (SMGW) jeweils für Haus Y und Haus Z SMGW-Administrator	D: Gebäude B: Feld	**Funktionen SMGW** WAN-Kommunikation zu SMGW, LMN-Komm. zu Smart Meter (mMe) sowie CLS-Komm. zu Geräten/Anlagen sowie Speicherung von Zählerstandsgängen und Tarifen; Betrieb externer Energiedienstleister, die Steuerbox bedienen, darf nicht zu Beeinträchtigungen des SMGW-Betriebs sowie zu konkurrierenden Zugriffen führen
B2: Kommunikations-komponenten WAN-Router VNB beim Anschlussnehmer Verteilnetzbetreiber	D: DER / Liegenschaft B: Station des Anschlussnehmers	**Funktion WAN-Router:** Verantwortung WAN-Kommunikation beim VNB, Komm.anschluss und Router Bestandteil des digitalen Netzanschlusses; Komm.einrichtung zu allen SMGWs der Anschlussnutzer sowie zur digitalen Steuerbox am Anschluss des Anschlussnehmers Kommunikationssicherheit im privaten Netz ist durch VNB sicherzustellen
B2: Kommunikations-komponenten Lokale Kommunikationsnetze in den Gebäuden Y und Z (HAN) Anschlussnutzer	D: DER / Liegenschaft B: Feld der Anschlussnutzer	Betrieb der notwendigen lokalen Kommunikationssysteme in den Gebäuden hinter dem CLS-Modul am digitalen Netzanschluss (lokale Gebäudenetze sowie Kopplung von GEMS in Gebäuden zu iMSys sowie Sensorik und Aktorik); Verbindung HAN mit Assets darf nicht - den Assetbetrieb stören, - zu Beeinträchtigungen bei Endkunden führen, - nicht weitere Infrastrukturen des Endkunden stören, - Informationen zu Assets des Endkunden unerlaubt weitergeben, - zu Vertrauensverlusten gegenüber dem Betreiber führen und zu keinen finanziellen Schäden beim Betreiber führen
B2: Kommunikations-komponenten S5-WAN-Router in den Gebäuden Y und Z Anschlussnutzer	D: DER / Liegenschaft B: Station der Anschlussnutzer	**Funktion:** Private WAN-Kommunikation des Anschlussnutzers mit Verbindung zu EMS sowie Geräten und Anlagen der Gebäude Betriebs- und Zugangssicherheit zum privaten WAN-Router ist zu garantieren, um Versorgungssicherheit und Geräteschutz zu gewährleisten
B3: Basiskomponenten Energiemanagement-Gateways in den Gebäuden Y und Z Anschlussnutzer	D: DER / Liegenschaft B: Station der Anschlussnutzer	**Funktion EMG:** Plattform und Laufzeitumgebung für lokale Energiemanagementsysteme (Edge-Computing beim Anschlussnutzer)

Gliederung Komponenten in Kategorien A bis D Komponenten Rolle des Betreibers	D: Domäne B: Betriebszone	Funktionen Schutzbedürfnisse
		Betriebs- und Zugangssicherheit zur Plattform ist zu gewährleisten
B3: Basiskomponenten GWA-System und zugehörige Teilkomponentgen SMGW-Administrator	D: DER / Liegenschaft B: Betriebsführung	**Administration SMGW und Verbindung**, Kommunikations-Headend-Funktionen, Messdatensicherung, Parametrierung und Konfiguration der Zertifikate der SMGWs, Messdatenverteilung und Verbindung von Messsystemen zu passiven und aktiven EMTs; Betrieb externer Energiedienstleister darf nicht zu Beeinträchtigungen des Betriebs beim GWA führen,
B3: Basiskomponenten aEMT-Plattform und zugehörige Teilkomponenten IIS-Betreiber für aEMT-Plattform (z.B. VNB)	D: DER / Liegenschaft B: Betriebsführung (MSB)	**Administration aEMT-Funktionen und Verbindung über CLS-Tunnel** Bereitstellung einer Umgebung für verschiedene Energiedienstleister und Netzakteure zum steuernden Zugriff auf Anlagen über CLS-Tunnel inklusive CLS-Management und Koordinationsfunktion; Betrieb externer Energiedienstleister darf nicht zu Beeinträchtigungen des Betriebs beim GWA sowie der Prozesse zur Nutzung des sicheren CLS-Tunnels führen,
B3: Basiskomponenten Informationssystem Messdaten Messstellenbetreiber IoT-Plattformbetreiber	D: Liegenschaft, DER, Verteilnetz B: Betriebsführung	**Funktion: in 2. Phase AutonomieLab Leimen noch nicht eingesetzt** **Verwaltung von Messdaten** in jeweils benötigter Auflösung (**hochaufgelöste Messdaten – High resultion – HRM**) inkl. Submeter und Sensorik, Bereitstellen und Verwaltung von Historien der Zeitreihen; Betriebsschutz bezüglich Datenschutzfunktionen bei Weitergabe von Daten an externe Marktpartner gewährleisten (aktuell noch keine sternpunktförmige Datenweitergabe vom SMGW abgesichert über GWA, sondern Datenweitergabe über MSB und Messdatenplattformen mit bisherigen Prozessen der Marktkommunikation)
B3: Basiskomponenten Basisdienste IoT-Plattform IoT-Plattformbetreiber	D: Liegenschaft, DER, Verteilnetz B: Betriebsführung	**Funktion: in 2. Phase AutonomieLab Leimen noch nicht eingesetzt** **Eintragen von Stammdaten, Funktionslisten und von Kommunikationsprofilen in Registry** - durch Anlage, Gerät, Zelle oder über Dashboard eines Betreibers **Flexibilitätskataster, Prognosen, Bilanzen, Transaktionen** Betriebsschutz bezüglich Datenschutzfunktionen bei Weitergabe Messdaten sowie Versorgungssicherheit bei Weitergabe von Bilanzierungs-, Fahrplan- und Marktdaten an externe Marktpartner gewährleisten
C: Betriebskomponenten Fernwirkungsplattform der Leitwarte Verteilnetzbetreiber	D: Verteilnetz B: Betriebsführung	**Funktion: Versand Plim-Signal** **Senden von Steuersignalen** – digital unter Nutzung des CLS-Kanales **Verwaltung Netzqualitätsdaten (f, U, I, cos Phi, …)** mit Lieferung der Daten der iMsys über Informationssystem Messdaten Störung der korrekten Netzfunktion durch Belieferung mit falschen Netzmessdaten verhindern
C: Betriebskomponenten Energiemanagement-Systeme (EMS) in den Gebäuden Y und Z Anschlussnutzer	D: DER / Liegenschaft B: Station der Anschlussnutzer	**Funktion EMS:** Lokales Energiemanagement in der Zelle des Anschlussnutzers Betriebs- und Zugangssicherheit zum Energiemanagementsystem ist zu garantieren, um Versorgungssicherheit und Geräteschutz zu gewährleisten
C: Betriebskomponenten Energiemanagementsystem Quartier		**Betriebsfunktionen im Inselnetzbetrieb** Monitoring sowie Steuerung der Energieflüsse hinter Anschlusspunkt der Gebäude als auch an ausgewählten Anlagen und Geräten (PV, Batterie, ausgewählte Verbraucher);

Gliederung Komponenten in Kategorien A bis D Komponenten Rolle des Betreibers	D: Domäne B: Betriebszone	Funktionen Schutzbedürfnisse
Energiedienstleister (EMS in der Cloud von FhG IEE)		um Steuerungsanliegen an Verbraucher bei der Regelung zur Einhaltung der Maximalleistung im Notbetrieb abzuleiten; Prognosen zur Erzeugung und in Verbindung mit Batteriekapazität, Vorgabe Maximalleistung zur Sicherstellung Notbetrieb über bestimmte Zeitspanne im Inselfall sowie Einhaltung der Leistungsgrenzen bei Vorgabe des Netzbetreibers, Priorisierung des Gerätebetriebes; Energiemanagementsystem beschafft Messwerte und muss hierbei die vorgegebenen Datenschutz-Kriterien einhalten, Das Energiesystem im Gebäude darf nicht angreifbar sein, wenn EMS über Internetzugang des Gebäudes mit externen Energiedienstleistern verbunden ist.
C: Betriebskomponenten Messstellenbetrieb Messstellenbetreiber	D: Liegenschaft, DER, Verteilnetz B: Unternehmen	**Funktion: in 2. Phase AutonomieLab Leimen noch keine Funktion** **Lieferung von Geräteinformationen und Anschlussobjekten** (MeLo, MaLo) sowie **Messdaten** für Liefer- und Netzabrechnung **Einbau und Betrieb intelligenter Messeinrichtungen** mit modernen Messeinrichtungen (Strom, Wärme, Gas, Wasser) und SMGWs Betriebsschutz bezüglich Datenschutzfunktionen bei Weitergabe von Daten an externe Marktpartner gewährleisten

Eine Abbildung zur Komponentenarchitektur auf Basis der SGAM-Komponentenebene ist hilfreich, um die Verbindungen zwischen den genannten Komponenten zu verdeutlichen, wie nachfolgend für den Use Cases zum AutonomieLab Leimen.

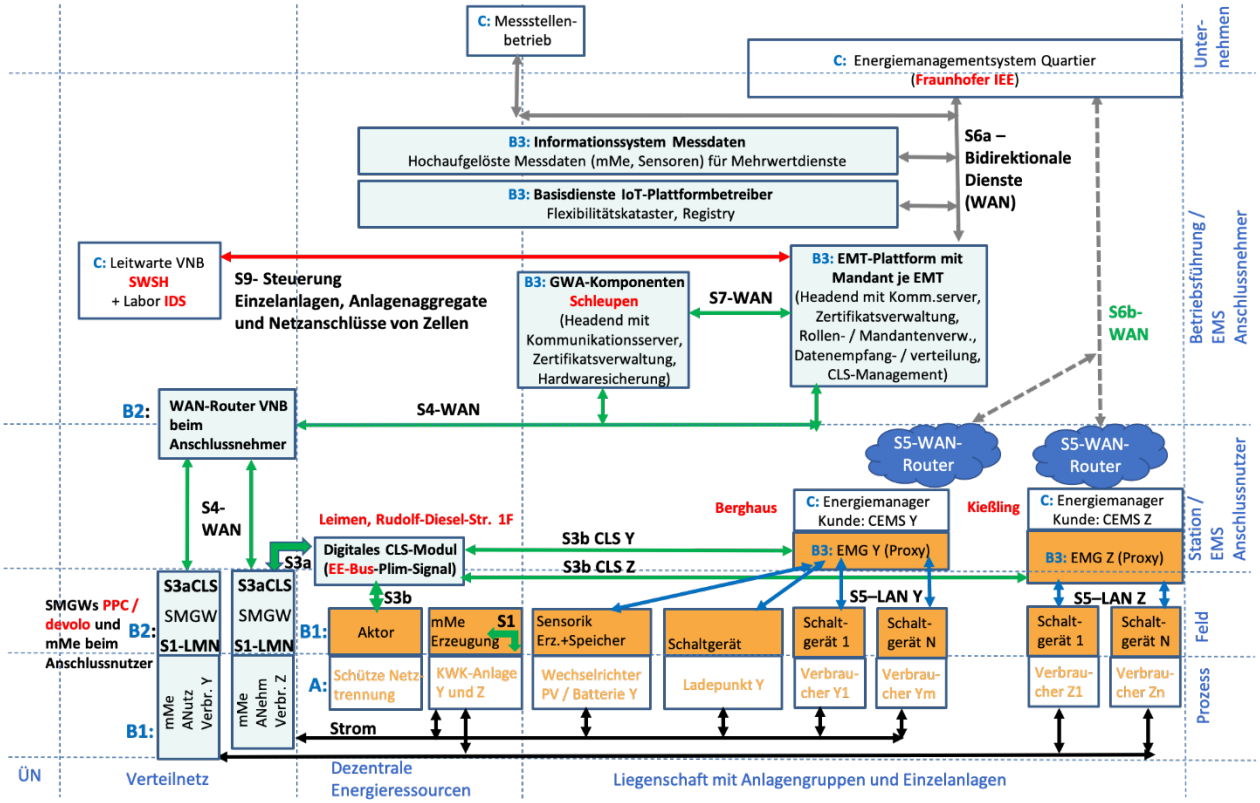

Abb. 10: Komponentenarchitektur AutonomieLab Leimen

3.3 Risikoanalyse

Risiken beim Betrieb des Energiesystems in einer Gebäudezelle beruhen auf dem Eintreten möglicher Bedrohungen. Um die Auswirkung eines Risikos zu begrenzen, formulieren die Gebäudenutzer verschiedene Niveaus der Auswirkung und definieren für Schutzbedürfnisse eine bestimmte, maximal zulässige Auswirkung von eintretenden Risiken.

Folgende Schutzbedürfnisse wurden aus Sicht des Gebäudenutzers inklusive der zugehörigen Energieanlagen identifiziert.

Schutzbedürfnisse beim Betrieb des Energiesystems

- Fernsteuerbarer Netzanschluss im Gebäude darf nicht zur Störung der verfügbaren Leistung sowie einem Ausfall des Energieflusses am Netzanschluss führen.
- In ein Kommunikationsnetz eingebundene Sensorik und Aktorik im Gebäude an einzelnen Anlagen und Geräten dürfen nicht die Verfügbarkeit von Endgeräten und Teilbereichen des Gebäudes beeinträchtigen.
- In ein Kommunikationsnetz eingebundene Sensorik und Aktorik im Gebäude an einzelnen Anlagen und Geräten dürfen nicht die von anderen Infrastrukturen, wie Wasser- oder Wärmeversorgung beeinträchtigen.

Schutzbedürfnisse bezüglich der Einhaltung von Gesetzen und Regularien

- Die Übersendung von Messdaten an Energiedienstleister (z.B. zur Messdatenvisualisierung), die Messdaten speichern, darf nicht zur Verletzung des Datenschutzes führen.
- Die Übersendung von Daten sowie die Übertragung von Vermarktungsaufgaben an Energiedienstleister (z.B. Abrechnung von P2P-Stromverkäufen), die Unterstützungsdienstleistungen bieten, darf nicht zur Verletzung von Gesetzen und Regularien führen (z.B. Bilanzierungs- und Abrechnungspflicht).

Bedrohungen bezüglich der das Energiesystem nutzenden Menschen

- Fernzugriffe auf Steuerbox und Aktorik im Gebäude an einzelnen Anlagen und Geräten im Gebäude darf nicht zu körperlichen Verletzungen aufgrund Fehlbetriebes führen.

Bedrohungen für Finanzen

- Die Übersendung von Daten sowie die Übertragung von Vermarktungsaufgaben an Energiedienstleister (z.B. Abrechnung von P2P-Stromverkäufen), die Unterstützungsdienstleistungen bieten, darf keinen finanziellen Verlust der Gebäudenutzer und Anlagenbetreiber aufgrund fehlender Abrechnung oder Vermarktung bewirken.

Bei einer ausschließlich informations- und kommunikationstechnisch geführten Betrachtung (hier der Fokus im Beispiel) bestehen die Risiken, dass folgende Bedrohungen die Schutzbedürfnisse verletzen (siehe Einleitung zu Kapitel Use Case-Analyse).

- Vertraulichkeit(confidentiality) wird nicht eingehalten
- Integrität (integrity) der Daten wird durch unerlaubtes Verändern verletzt
- Verfügbarkeit (availability) nicht gewährleistet
- Nicht-Abstreitbarkeit (repudiation) durch Bedrohung der Protokollierungspflichten verletzt
- Verletzbarkeit (vulnerability) der technischen Funktion der IKT-Komponenten

Diese Bedrohungen werden den Risikoauswirkungs-Kategorien zugeordnet, die jeweils auf ein Schutzbedürfnis Bezug nehmen. Für das Eintreten der Bedrohung werden jeweils fünf zugehörige Risikoauswirkungs-Niveaus definiert und die jeweiligen Auswirkung wird mit einer farblichen Kennzeichnung zwischen den Werten niedrig, mittel, hoch, kritisch und hoch kritisch bewertet.

Grundsätzlich ist diese Bewertung für jede der genannten Bedrohungen zu bestimmen. Hier im Beispiel wird die Bewertung einmal für alle Bedrohungen geführt. In der Praxis wird bei getrennten Bewertungen als Ergebnis das am höchsten eingeschätzte Risikoauswirkungs-Niveau genutzt.

Risikoaus-wirkungs-Niveau risk impact level (	RA-Niveau auf Basis Leistungs-grenze am Netz-anschluss	RA-Niveau auf Basis Energie-fluss	RA-Niveau auf Basis betrof-fener Bevölke-rung	RA-Niveau auf Basis betrof-fener Infra-strukturen	RA-Niveau in Bezug zu Daten-schutz-direktiven	RA-Niveau auf Basis möglicher Strafen	RA-Niveau auf Basis Gefährdung Komfort / Gesundheit	RA-Niveau auf Basis direkter mone-tärer Schaden
hoch krtitisch	Leistungs-begren-zung 100 % der Maximal-leistung	Ausfälle im Bereich von Wochen	gesamtes Wohn-quartier ist betroffen	zusätzlich Wasser-ver-sorgung betroffen	noch keine Definition	Gebäude wird für unbenutz-bar erklärt	Todesfall	über 50% vom Jahresein-kommen
kritisch	Leistungs-begren-zung max. 80 % der Maximal-leistung	Ausfälle im Bereich von Tagen		zusätzlich Wärme-ver-sorgung betroffen	Noch keine Definition	Nutzungs-unter-brechung	Verletzung mit Folge-schäden	von 15% zu 50% vom Jahresein-kommen
hoch	Leistungs-begren-zung max. 60 % der Maximal-leistung	Ausfälle im Bereich von Stunden	Mehrere Familien sind betroffen	Gesamtes Stromnetz des Hauses betroffen	unautoris. Zugriff auf persön-liche Daten	Geld-strafen	Starke Verletzung	von 5% zu 15% vom Jahresein-kommen
mittel	Leistungs-begren-zung max. 40 % der Maximal-leistung	Ausfälle im Bereich von Minuten	Ganze Familie ist betroffen	Stromnetz in einzelnen Räumen betroffen	unautoris. Zugriff auf technische Daten	Probleme mit Nachbarn	Mindere Verletzung	von 1% zu 5% vom Jahresein-kommen
niedrig	Leistungs-begren-zung max. 20 % der Maximal-leistung	Kurze Span-nungs-schwan-kung - Sekunden	Einzelne Person ist betroffen	Nur eine Strom-phase betroffen	keine persönl. od. sensitiven Daten	nur War-nungen bei Nicht-erfüllung	Einschr. Komfort	unter 1% vom Jahresein-kommen
	Energie-versor-gung (Leistung in kW)	Energie-fluss (Leistung mal Zeitdauer kWh)	Bewohner	Infra-strukturen	Daten-schutz	Folgen durch Verletzung von Gesetzen / Verordn.	Menschen	Finanzen
	Funktional				Gesetze			

Tabelle 7: Risikoauswirkungs-Kategorien mit Bestimmung von Risikoauswirkung-Niveaus für AutonomieLab

Nun ist als zweiter Faktor die **Eintrittswahrscheinlichkeit** für die genannten vier Bedrohungen, deren Eintreten die genannten Risikoauswirkungen bewirken kann, zu bestimmen. Die Wahrscheinlichkeit kann auf

verschiedenen Wegen der Interaktion zwischen zwei Komponenten in Abhängigkeit vom Akteur, der Zugriff auf die Schnittstelle erhält, variieren. Die Wahrscheinlichkeit wird mittels der Level niedrig, mittel, hoch, sehr hoch und extrem hoch abgeschätzt. Da die Bedrohung über verschiedene Schnittstellen des Systems unterschiedlich hoch zu bewerten ist, aber der höchste Auswirkungsgrad durch das schwächste Glied der Kette – die am meisten bedrohte Schnittstelle – gegeben ist, wird der höchste Grad der Eintrittswahrscheinlichkeiten für die weitere Bestimmung der Anforderungen und Maßnahmen herangezogen.

Die folgende Tabelle verdeutlicht das Vorgehen zu Bestimmung der Eintrittswahrscheinlichkeit, wobei die angegebenen Wahrscheinlichkeiten hier nur beispielhaft aufgeführt sind und einer detaillierteren Risikobetrachtung bedürfen. Wiederum gilt, dass die Betrachtung für jede Bedrohung zu führen ist und dann die höchste Eintrittswahrscheinlichkeit für die Berechnung des Sicherheits-Levels gewählt wird. Hier im Beispiel wird von der gleichen Wahrscheinlichkeit für alle Bedrohungen ausgegangen.

Schnittstellen	**unehrlicher Administrator GWA- / aEMT-Plattform**	**unehrlicher Beschäftigter VNB**	**Vandalismus im Wohnquartier**	**Hacker**	**Terrorist**
aEMT-Komponente des VNB SMGW CLS-Kanal					
SMGW CLS-Kanal zu Steuerbox					
Steuerbox zu GEMS					
Sensorik zu GEMS					
App mobiles Endgerät zu GEMS					
Geräte/Anlagen zu WAN Gebäude					
GEMS zu externer P2P-Plattform					

Tabelle 8: Bestimmung von Eintrittswahrscheinlichkeiten für Gruppen von potentiellen Angreifern

Die Kombination von Risikoauswirkungs-Niveau zwischen 1 und 5 und Grad der Eintrittswahrscheinlichkeit zwischen 1 und 5 führt in folgender Tabelle zur Bestimmung des Sicherheitsniveaus (security level), die durch Addition mit Werten zwischen 2 bis 10 berechnet werden.

Genutzt wird jeweils das höchste ermittelte Risikoauswirkungs-Niveau und die höchste Eintrittswahrscheinlichkeit.

		Eintrittswahrscheinlichkeit (likelihood)				
		1: niedrig	2: mittel	3: hoch	4: sehr hoch	5: extrem hoch
Risiko-auswirkung-Niveau (risk impact level)	5: hoch krtitisch	6	7	8	9	10
	4: kritisch	5	6	7	8	9
	3: hoch	4	5	6	7	8
	2: mittel	3	4	5	6	7
	1: niedrig	2	3	4	5	6
		1	2	3	4	5
		Sicherheitsniveau (security level) und Datenschutzklassen				

Tabelle 9: Bestimmung der Sicherheits-Niveaus (security level) und Datenschutzklassen

3.4 Bestimmung der Schutzanforderungen

Vorgehensweise

Die für Use Cases definierten Schutzziele und die resultierende Risikobewertung mit der Bestimmung von Risikoauswirkung-Niveaus, Eintrittswahrscheinlichkeiten sowie resultierenden Sicherheitsniveaus ist Grundlage für Schritt 3 der Schutzmethodik zur Ableitung von Schutzanforderungen.

Informationsobjekte und Kommunikationsanforderungen

Schutzanforderungen sind abhängig vom Wirkungsort installierter Komponenten (siehe Komponententabelle) und ihrer Schnittstellen sowie den dabei übertragenen Daten. Insofern ist die Übernahme und Betrachtung der Tabellen zu Informationsobjekten und zu Kommunikationsanforderungen aus der jeweiligen Use Case-Beschreibung (Schritt 2 der Use Case Methodik, C/sells – [Kießling, A., Bogensberger, A., Köppl, S. & Faller, F. (03/2020)]) Grundlage der Ableitung von Schutzanforderungen.

Dabei sind zuerst zur Festlegung von Datenschutzklassen die im Use Case benötigten Daten zu klassifizieren. Dies erfolgt im Rahmen der zum Use Case ermittelten Informationsobjekte, d.h. von gespeicherten und im Rahmen von Nachrichten zwischen Akteuren ausgetauschten Daten.

Nachfolgende Tabelle umfasst Informationsobjekte für den Zielzustand von AutonomieLab Leimen und werden nicht vollständig in der 2. Phase der Demonstration im AutonomieLab benötigt. Die Klassifikation der Daten bezüglich des Datenschutzes ist dabei für einen produktiven Einsatz noch zu spezifizieren.

Informationsobjekt	Teilobjekte	Inhalte	Kurzbeschreibung Schutzbedürfnisse und Datenklassifizierung
Messdaten	Leistungsgänge	Leistung Zeit	Leistungsverläufe in der Zeit mit Auflösung im Sekundenbereich jeweils für Verbrauch und Erzeugung der benötigten Anlagen von iMSys oder Sensorik an Einzelgeräten; → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Messdaten	Mengen	Energie Zeitdauer	Energiemengen in Zeitabschnitten mit wählbarer Zeitdauer → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Messdaten	Powerqualität	Strom, Spannung, Frequenz, Phasenverschiebung	→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Planungsdaten	Prognose	Prognosemodell und Teilobjekte festlegen	→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Planungsdaten	Fahrplan	Fahrplanmodell und Teilobjekte festlegen	→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Planungsdaten	Flexibilität	Flexibilitätsmodell und Teilobjekte noch zu definieren	inkl. Randbedinungen wie Wartezeiten, Flex.intervalle, Gradienten, Abhängigkeiten)

			→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Marktdaten	Preise		→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Steuerdaten	Leistungsvorgaben	An- und Aussignale Zeit	Übersendung von Signalen zum An- und Abschalten von Geräten → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Steuerdaten	Statusinformationen	Zustände	Nachrichten von Steuerungs-einrichtungen über aktuelle Anlagenzustände → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Steuerdaten	Leistungsvorgaben	Leistung Zeit	Vorgabe Leistungsverläufe in der Zeit für Verbrauch / Erzeugung (**Leistungszeitreihen – P * t = Energie) oder Zeitreihen mit Leistungsänderungen zu Zeitpunkten – dP / dt = Flexibilität**) → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Konfigurationsdaten	Kommunikations-einstellungen, Programmdaten	Konfiguration SMGW, Software-Updates, Kommunikationsfreigaben	Prozesse des GWA nach Technischer Richtlinie BSI; → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Konfigurationsdaten	Zielvorgaben	Prioritäten, Regeln, Einsatzzeiten	Rahmenbedingungen der Anlagen und der Anwender → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Stammdaten	Gerätedaten	Standorte, Funktionen, Betreiber	→ Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Transaktionsdaten	Protokolle	Prozessschritte	Dokumentation der Prozessschritte für Protokollpflichten, Abrechnung und Nicht-Abtreitbarkeit → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten
Kommunikations-daten	Kommunikations-schemen; Protokolle	z.B. URI-Schemata	Hier nur Beispiel, zu definieren sind Schemata der Anwendungs-schnittstelle zur Nutzung des CLS-Kanales → Daten klassifizieren: nicht sensible technische Daten, sensible technische Daten, betriebliche Daten, persönliche Daten

Im Weiteren sind die zum Use Case definierten Kommunikationsanforderungen zu betrachten. Untersucht wird, welche Daten von welchen Komponenten auf welche Weise ausgetauscht werden, um hierzu informationstechnische Schutzanforderungen hinzuzufügen.

Kommunikationsschnittstelle			**Inhalt der Nachricht**	**Schutzanforderungen**
Von	Bis	**Schnitt-stelle**		
mMe Gebäude Y und Z SMGW Gebäude Y / Z	SMGW Gebäude Y / Z mMe Gebäude Y und Z	**S1**	Messdaten Energie und Leistung für Markt sowie Anschlussnutzer Konfigurationsdaten	definiert über BSI-Schutzprofil
SMGW HAN EMG	EMG SMGW HAN	**S2**	Schnittstelle nicht genutzt in Phase 2 des AutonomieLab Leimen	SMGW transportiert Daten von mMe's sicher über HAN-Schnittstelle an GEMS
SMGW CLS der Anschlussnutzer Gebäude Y / Z CLS-Modul	CLS-Modul Anschluss-nehmer SMGW CLS	**S3a**	**Verschlüsselter und signierter Payload mit beliebigen Daten → im betrachteten Use Case Plim-Signal zur Einstellung einer Maximalleistung;** Statusdaten	Nutzung und Abschluss des sicheren, transparenten Kommunikationskanals über CLS-Kanal des SMGW zum CLS-Modul der Steuerbox nach BSI-Schutzprofil
CLS-Modul als Teil Steuerbox des Anschluss-nehmers	Aktorik an Netz-trennschütz des Anschluss-nehmers	**S3b**	**Im betrachteten Use Case setzt Steuerbox verschlüsselten und signierten Payload um in digitales Signal an Schütz vom Netzanschluss des Anschlussnehmers zur Netztrennung und Wiederverbindung**	Nutzung der Sicherheitskonzept der Steuerbox mit Direktverbindung zum Aktor des Netztrennschützes
CLS-Modul als Teil Steuerbox des Anschluss-nehmers	EMG Gebäude Y und Z	**S3b**	**Im betrachteten Use Case sendet Steuerbox verschlüsselten und signierten Payload weiter an EMGs der Anschlussnutzer Y und Z zur Übergabe des Plim-Signales;** **EMG als Proxy zwischen CLS-Modul und Gebäude-LAN**	Informationssicherheit bei Verbindung von CLS-Modul zu EMG durch Netzwerktrennung LAN CLS-Modul und LAN im Gebäudenetz (Proxyfunktion) gewährleisten, Abspeicherung von Daten im EMG vor Weitergabe → Manipulationsfreiheit der Steuerung gewährleisten
WAN-Router VNB	SMGWs der Anschlussnutzer Gebäude Y / Z	**S4**	**Transport von Informationen zu und von SMGWs**	Sicherheitsanforderungen definiert über BSI-Schutzprofil
WAN-Router VNB GWA und EMT-Plattform	GWA und EMT-Plattform WAN-Router VNB	**S4**	Verschlüsselter und signierter Payload mit beliebigen Daten; Kommunikationsdaten	Anforderungen gemäß BSI-Schutzprofil;
EMG	Aktorik: Schaltgeräte 1 bis N je Gebäude Y / Z und von Ladepunkt	**S5**	Übermittlung von Ein- und Ausschaltsignalen im privaten LAN der Gebäude entsprechend der Prioritätenregelung der EMS	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation über private Kommunikationsnetze; Rückwirkungsfreiheit zu HAN-Kommunikation des SMGW
Sensorik Erzeuger und Speicher	EMG	**S5**	Messdaten von Wechselrichter für PV und Batterie (Monitoring IPLON)	Gewährleistung von Informationssicherheit und

				Datenschutz für Kommunikation über private Kommunikationsnetze; Rückwirkungsfreiheit zu HAN-Kommunikation des SMGW
EMGs der Gebäude Y / Z S5-WAN-Router der Anschluss-nutzer	S5-WAN-Router der Anschluss-nutzer EMGs der Gebäude Y / Z	**S5**	Messdaten, Steuerdaten, Konfig.daten; **EMG als Proxy zwischen CLS-Modul und Gebäude-LAN**	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation über private Kommunikationsnetze; Rückwirkungsfreiheit zu HAN-Kommunikation des SMGW
S5-WAN-Router EMS Quartier in der Cloud	EMS Quartier in der Cloud S5-WAN-Router	**S6b**	Messdaten, Steuerdaten, Konfig.daten;	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation über öffentliche Kommunikationsnetze;
EMT-Plattform	EMS Quartier in der Cloud	**S6a**	Schnittstelle nicht genutzt in Phase 2 des AutonomieLab Leimen	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen GWA/EMT-Infrastruktur und Marktpartnern
EMT-Plattform	Komponente Messstellen-betrieb	**S6a**	Schnittstelle nicht genutzt in Phase 2 des AutonomieLab Leimen	wie S6a oben
EMT-Plattform	Basisdienste IoT-Plattform	**S6a**	Schnittstelle nicht genutzt in Phase 2 des AutonomieLab Leimen	wie S6a oben
EMT-Plattform	Infosystem Messdaten	**S6a**	Schnittstelle nicht genutzt in Phase 2 des AutonomieLab Leimen	wie S6a oben
EMT-Plattform GWA	GWA EMT-Plattform	**S7**	Kommunikationsdaten und Qittungsmeldungen	Anforderungen gemäß BSI-Schutzprofil;
Komponente Leitwarte Fernwirkung und Netzmonit.	EMT-Plattform	**S9**	Versand eines Leistungsbegrenzungssignales an gemeinsamen, digitalen Netzanschluss des Gebäudeverbundes Y und Z als Plim-Signal	Gewährleistung von Informationssicherheit und Datenschutz für Kommunikation zwischen GWA/EMT-Infrastruktur und Netzbetreiber – Anforderungen nach BSI-Schutzprofil

3.1 Bestimmung von Schutzmaßnahmen

Vorgehensweise

Folgender Prozess wurde bisher beschrieben.

Mit der im Schritt 1 durchgeführte **Use Case Analyse** erfolgte die Formulierung von Schutzbedürfnissen.

Die im Schritt 2 folgende **Risikoanalyse** ermittelt Bedrohungen, die die Schutzbedürfnisse verletzen können. Mit der Bestimmung des Auswirkungsgrades bei Verletzungen sowie der Eintrittswahrscheinlichkeit werden Schutzziele formuliert.

Schritt 3 widmet sich der **Analyse von Schutzanforderungen**, um Schutzziele einhalten zu können.

Dies ist wiederum im Schritt 4 die Grundlage, um entsprechende **Schutzmaßnahmen** festzulegen, deren Umsetzung die Einhaltung der Anforderungen gewährleistet.

Schnittstellenliste und grundlegende Sicherheitsmaßnahmen

SchnittstelleNr_ Nachricht-Nr	Absenderkomponente Zielkomponente	Informationen	Sicherheitsmaßnahmen
S01_01	mMe Gebäude Y und Z - SMGW Gebäude Y / Z	Messdaten Energie und Leistung für Markt sowie Anschlussnutzer	
S01_02	SMGW Gebäude Y / Z - mMe Gebäude Y und Z	Konfigurationsdaten	
S02_01	EMG – SMGW HAN	Schnittstelle für lokale Bereitstellung der Messdaten nicht genutzt in Phase 2 des AutonomieLab Leimen	
S03a_01	SMGW CLS der Anschlussnutzer Gebäude Y / Z - CLS-Modul Anschluss-nehmer	Verschlüsselter und signierter Payload mit beliebigen Daten → im betrachteten Use Case Plim-Signal zur Einstellung einer Maximalleistung;	
S03a_02	CLS-Modul Anschlussnehmer - SMGW CLS der Anschlussnutzer Gebäude Y / Z	Statusdaten	
S03b_01	CLS-Modul als Teil Steuerbox – Aktorik an Netztrennschütz	Steuerdaten für Abschalten und Anschalten Netzanschluss	
S03b_02	CLS-Modul als Teil Steuerbox - EMG Gebäude Y	Steuerdaten mit Leistungsvorgabe (Plim-Signal des gemeinsamen Netzanschlusses)	
S03b_03	CLS-Modul als Teil Steuerbox - EMG Gebäude Z	Steuerdaten mit Leistungsvorgabe (Plim-Signal des gemeinsamen Netzanschlusses)	
S04_01	WAN-Router VNB - SMGWs der Anschlussnutzer Gebäude Y / Z	Transport von Informationen zu und von SMGWs mit verschlüsseltem und signiertem Payload mit beliebigen Daten	
S04_02	WAN-Router - GWA und EMT-Plattform	Transport von Informationen zu und von GWA/EMT mit verschlüsseltem und signiertem Payload mit beliebigen Daten	
S05_01	EMG - Aktorik: Schaltgeräte 1 bis N je Gebäude Y	Ein- und Ausschaltsignale im privaten LAN des Gebäudes Y	

S05_02	EMG - Aktorik: Ladepunkt im Gebäude Y	Ein- und Ausschaltsignale für Ladepunkt im privaten LAN des Gebäudes Y	
S05_03	EMG - Aktorik: Schaltgeräte 1 bis N je Gebäude Z	Ein- und Ausschaltsignale im privaten LAN des Gebäudes Z	
S05_04	Sensorik Wechselrichter - EMG	Messdaten vom Wechselrichter zu PV-Anlage und Batterie im privaten LAN des Gebäudes Y	
S05_05	EMGs der Gebäude Y - S5-WAN-Router der Anschlussnutzer	Messdaten PV-Monitoring **EMG als Proxy zwischen CLS-Modul und Gebäude-LAN**	
S05_06	S5-WAN-Router der Anschlussnutzer - EMG des Gebäudes Y	Steuerdaten nach eventueller zusätzlicher Verhandlung der Aufteilung von Plim durch Quartiers-EMS	
S05_07	S5-WAN-Router der Anschlussnutzer - EMG des Gebäudes Z	Steuerdaten nach eventueller zusätzlicher Verhandlung der Aufteilung von Plim durch Quartiers-EMS	
S06b_01	S5-WAN-Router Gebäude Y – EMS Quartier in der Cloud	Messdaten PV-Monitoring den Liegenschaftszellen	
S06b_02	EMS Quartier in der Cloud - S5-WAN-Router Gebäude Y	Steuerdaten nach eventueller zusätzlicher Verhandlung der Aufteilung von Plim durch Quartiers-EMS	
S06b_03	EMS Quartier in der Cloud - S5-WAN-Router Gebäude Z	Steuerdaten nach eventueller zusätzlicher Verhandlung der Aufteilung von Plim durch Quartiers-EMS	
S06a_01	EMT-Plattform - Infosystem Messdaten	Schnittstelle nicht genutzt in Phase 2 des AutonomieLab Leimen	
S06a_02	EMT-Plattform - Basisdienste IoT-Plattform	Schnittstelle nicht genutzt in Phase 2 des AutonomieLab Leimen	
S06a_03	S5-WAN-Router – Betriebs-komp. Markt und Netz	Schnittstelle nicht genutzt in Phase 2 des AutonomieLab Leimen	
S06a_04	S5-WAN-Router – Komponente Messstellenbetrieb	Schnittstelle nicht genutzt in Phase 2 des AutonomieLab Leimen	
S07_01	EMT-Plattform – GWA	Kommunikationsdaten	
S07_02	GWA – EMT-Plattform	Quittungsmeldungen, Statusdaten	
S09_01	Komponente Leitwarte Fernwirkung und Netzmonit. – EMT-Plattform	Leistungsbegrenzungssignal Plim; Wiederzuschaltungs-signal nach Netzwiederaufbau	

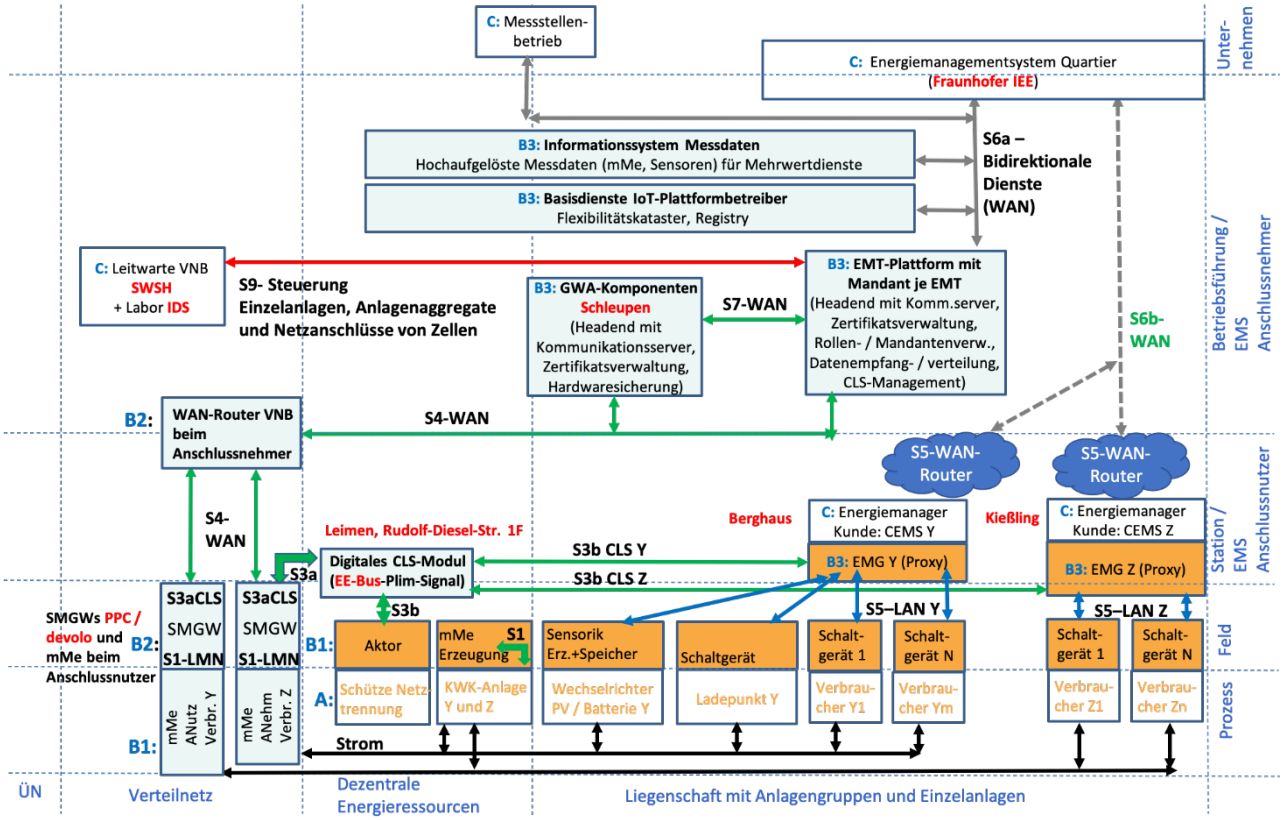

Abb. 11: Schnittstellenarchitektur S1 bis S9

4 Quellen

siehe Quellenverzeichnis in

Kießling, A. et al. (11/2020): Grundlagen der Massenfähigkeit. Methoden, Modelle für Interoperabilität durch Regeln, Standards und Normen sowie Verhältnis von Innovation, Standardisierung und Regulierung. Zusammenfassung, Motivation, Abgrenzung, Werkzeuge, Anwendung. Von https://www.csells.net/de/ergebnisse-c-sells/arbeitspakete/45-arbeitspaket1-2.html abgerufen