Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Energie BFE
Sektion Risikomanagement und Aufsicht Rohrleitungen

Bericht vom 17. Juni 2016

Studie «Schutzbedarfsanalyse Smart Metering in der Schweiz»

Abschlussbericht

AWK GROUP

Consulting
Engineering
Project Management

Datum: 17. Juni 2016
Ort: Zürich

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

Auftragnehmerin:
AWK Group AG
Leutschenbachstrasse 45, Postfach, CH-8050 Zürich
www.awk.ch

Autor:
Tarkan Bas (AWK Group AG)

Korreferent / Projektbegleiter:
Oliver Schenker / Adrian Marti, Schmuel Holles (AWK Group AG)

BFE-Begleitgruppe: Hans-Peter Binder, Matthias Galus, Christian Holzner, Bruno Le Roy
BFE-Projektleitung: Christian Holzner, christian.holzner@bfe.admin.ch
BFE-Vertragsnummer: SI/300198-01

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

AWK GROUP

Consulting
Engineering
Project Management

Abschlussbericht

Studie «Schutzbedarfsanalyse Smart Metering in der Schweiz»

Im Auftrag von:
Bundesamt für Energie BFE
CH-3003 Bern
www.bfe.admin.ch

17. Juni 2016

Dokumentinformationen

Titel:	Schutzbedarfsanalyse Smart Metering in der Schweiz
Erstellungsdatum:	17. Juni 2016
Anzahl Seiten:	129
Autor:	Tarkan Bas, AWK Group AG
Korreferent / Projektbegleiter AWK Group AG:	Oliver Schenker / Adrian Marti, Schmuel Holles
Begleitgruppe BFE	Hans-Peter Binder, Matthias Galus, Christian Holzner, Bruno Le Roy

Abkürzungen und Begriffe

Abkürzung	Beschreibung
BFE	Bundesamt für Energie
BSI	Deutsches Bundesamt für Sicherheit in der Informationstechnik
Datenkonzentrator	Datenkonzentratoren sammeln von allen angeschlossenen Geräten die Daten und senden diese gebündelt an das zentrale Zähldatenverarbeitungssystem. Durch die Bündelung der Daten lässt sich eine Reduktion des Datentransfers erreichen.
Datenmanager	In der vorliegenden SBA werden unter dem Begriff «Datenmanager» die Rollen «Messstellenbetreiber» und «Messdienstleister» zusammengefasst. Der Messstellenbetreiber ist in der Regel für die Supportprozesse wie z. B. den Einbau und Betrieb sowie die Eichung und Wartung der Messeinrichtung (intelligentes Messgerät) verantwortlich. Der Messdienstleister übernimmt üblicherweise das Ab- und Auslesen der Messeinrichtung, sowie andere Leistungen für den Endverbraucher wie z.B. Weiterbearbeitung der Daten, Abrechnung, Kundenbetreuung oder -beratung. Der Verteilnetzbetreiber ist heute für die Erbringung des Messwesens (Messstellenbetrieb und Messdienstleistung) verantwortlich. Er kann das Messwesen selber erbringen oder die entsprechenden Aufgaben an Dritte auslagern.
Datensicherheit	Siehe IKT-Sicherheit
DM	Datenmanager
DSG	Das schweizerische Bundesgesetz über den Datenschutz
ED	Externe Dienstleister
Endverbraucher	Siehe Prosumer
HAN	Home Area Network
IKT	Informations- und Kommunikationstechnologie
IKT-Sicherheit	Synonym zur Datensicherheit. IKT-Sicherheit umfasst die Sicherheitskonzepte und -Massnahmen zum Schutz der sensitiven Daten und Informationen in jeglicher Form sowie der IKT-Systeme in Bezug auf intelligente Messsysteme.
Integrität	Schutz vor unerlaubter Manipulation

Abkürzung	Beschreibung
Intelligentes Messgerät	Der Begriff „intelligentes Messgerät“ bezieht sich auf einen elektronischen Elektrizitätszähler - auch „Smart Meter“ genannt.
Intelligentes Messsystem beim Endverbraucher	Gemäss Art. 17a Abs. 1 des Gesetzesentwurfs zum Energiegesetz (EnG)[1] vom 4. September 2013 ist ein intelligentes Messsystem beim Endverbraucher eine Messeinrichtung zur Erfassung elektrischer Energie, die eine bidirektionale Datenübertragung unterstützt und beim Endverbraucher den tatsächlichen Energiefluss und dessen zeitlichen Verlauf erfasst. In dieser SBA bezeichnet der Begriff „Intelligentes Messsystem beim Endverbraucher“ stets eine Messeinrichtung im Elektrizitätsbereich.
ISDS-Konzept	Informationssicherheit- und Datenschutzkonzept
LAN	Local Area Network
LMN	Local Metrological Network / Lokales Metrologisches Netzwerk
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
OVP	Online-Visualisierungsplattform
Prosumer	Der Prosumer ist sowohl Einspeiser (Producer) als auch Endverbraucher (Consumer) im Stromnetz und befindet sich normalerweise in der Netzebene 5 oder 7 und in seltenen Fällen in der Netzebene 3.
SBA	Schutzbedarfsanalyse Smart Metering in der Schweiz
Smart Meter	Siehe „Intelligentes Messgerät“
Smart Metering	Mit Smart Metering bezeichnet man das Verfahren Bezügeranschlüsse mit Smart Metern auszurüsten, zu verwalten und Messdaten auszulesen (Quelle: Ref. [3])
Smart Metering System	Siehe „Intelligentes Messsystem beim Endverbraucher“
Tarifierung	Unter Tarifierung ist die direkte Zuordnung von Preisen zu den Verbrauchs- und Erzeugungswerten zu verstehen. Dies ist technisch direkt im intelligenten Messgerät, oder aber erst im Zähldatenverarbeitungssystem möglich.
UC	Use Case
Verfügbarkeit	Systeme, Dienste, Daten und Informationen sind in gefordertem Mass zugänglich und nutzbar. Die Verfügbarkeit impliziert den Schutz gegen Zerstörung und Verlust.
Vertraulichkeit	Schutz vor Einsicht bzw. Zugriff durch Unbefugte
V.v.	Verlust von
WAN	Wide Area Network
Zähldatenverarbeitungssystem	Zähldatenverarbeitungssysteme bieten vor allem Funktionen zur Verwaltung der Messgeräte selbst oder der Bearbeitung der von den Messgeräten aufgenommen Rohdaten wie z. B. Geräteparametrierung, Geräteverwaltung oder Zeitreihenverwaltung.
ZDVS	Zähldatenverarbeitungssystem

[1] https://www.admin.ch/opc/de/federal-gazette/2013/7757.pdf

Relevante Dokumente

Titel	Autor / Herausgeber	Datum	Link / Datei
[1] Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz - Technische Mindestanforderungen und Einführungsmodalitäten	BFE	17.11.2014	_[2]
[2] Datensicherheit und Datenschutz für Smart Grids: Offene Fragen und mögliche Lösungsansätze	AWK Group AG, VISCHER AG, FIR-HSG	30.06.2014	_[3]
[3] VSE Handbuch Smart Metering CH	VSE	2010	_[4]
[4] Anforderungskatalog Ende-zu-Ende Sicherheit Smart Metering	Oesterreichs Energie	03.12.2014	_[5]
[5] TECHNISCHER BERICHT TR 50572: Funktionale Referenzarchitektur für die Kommunikation in intelligenten Messsystemen	CEN/CLC/ETSI	Dez. 2011	_[6]
[6] IT-Sicherheit bei Smart Metering (EWZ), Schlussbericht	EWZ	07.09.2011	_[7]
[7] Projekt «SAK Smart» der St.Gallisch-Appenzellische Kraftwerke AG	-	-	_[8]
[8] Smart Meter Rollout EKZ	-	-	_[9]
[9] DSG - Bundesgesetz über den Datenschutz	Bund	01.01.2014	_[10]
[10] Ansätze zur Gewährleistung der IKT-Sicherheit von intelligenten Messsystemen bei Endverbrauchern	vZsecurITy, aartesys	31.10.2015	_[11]
[11] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken	Bund	19.06.2012	_[12]
[12] ISDS-Konzept Vorlage Risikoanalyse (Excel)	Bund	-	_[13]
[13] Appropriate security measures for smart grids	Enisa	06.12.2012	_[14]
[14] Smart Grid Roadmap Schweiz	BFE	27.03.2015	_[15]

[2] http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06242

[3] http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06012

[4] http://www.strom.ch/fileadmin/user_upload/Dokumente_Bilder_neu/010_Downloads/Branchenempfehlung/HBSM-CH_1018d_2010.pdf

[5] http://oesterreichsenergie.at/branche/stromnetze/sicherheitsanforderungen-fuer-smart-meter.html?file=files/oesterreichsenergie.at/Downloads%20Netze/Smart%20Meter/E2E-Sicherheit-SmartMeter_Dez2014.pdf

[6] https://courses.edx.org/c4x/DelftX/NGI102x/asset/Functional_reference_architecture_for_communications_in_smart_metering_systems.pdf

[7] http://www.bfe.admin.ch/php/modules/enet/streamfile.php?file=000000010700.pdf&name=000000290482

[8] www.saksmart.ch

[9] http://www.powertage.ch/~/media/powertage/Documents/PdfTemplates/Referat_1-1_Smart-Meter_Smart-Rollout_Gmuer-Roman.ashx

[10] https://www.admin.ch/opc/de/classified-compilation/19920153/201401010000/235.1.pdf

[11] http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06437

[12] https://www.isb.admin.ch/dam/isb/de/dokumente/ikt-vorgaben/strategien/ncs/Strategie%20zum%20Schutz%20der%20Schweiz%20vor%20Cyber-Risiken.pdf.download.pdf/Strategie_zum_Schutz_der_Schweiz_vor_Cyber-Risiken_k-DE.pdf

[13] https://www.isb.admin.ch/dam/isb/de/dokumente/ikt-vorgaben/prozesse-methoden/p042/P042-ISDS-Konzept_V3-0-d%20Vorlage_Risikoanalyse.xls.download.xls/P042-ISDS-Konzept_V3-0-d%20Vorlage_Risikoanalyse.xls

[14] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids/at_download/fullReport

[15] http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06308

Zusammenfassung

Intelligente Messsysteme beim Endverbraucher – Smart Metering Systeme – sind ein elementarer Baustein intelligenter Netze, der sogenannten „Smart Grids“. Smart Grids sind eine der wichtigen Infrastrukturen, um mittelfristig eine ökonomisch günstigere und systemtechnisch sichere Integration von erneuerbaren Energien zu ermöglichen. Smart Grids bilden aber auch eine technische Plattform für zukünftige Energiedienstleistungsmärkte und unterstützen insbesondere über Smart Metering Systeme eine weitere, allfällig vollständige Liberalisierung des Strommarktes.

Intelligente Messsysteme beim Endverbraucher sind ein integraler Bestandteil der Energiestrategie 2050 und damit des zukünftigen öffentlichen Stromversorgungssystems. Sie gehören dadurch indirekt zu den kritischen Infrastrukturen der Schweiz.

Intelligente Messsysteme unterstützen neben Energieabrechnungsprozessen und Dienstleistungen des Strommarktes durch ihre informationstechnische Vernetzung mit anderen Technologien aus dem Smart Grid Bereich auch neuartige Funktionalitäten der Stromnetze. Letztere wurden in der Smart Grid Roadmap der Schweiz (siehe Ref. [14]) identifiziert. Das Zusammenspiel von intelligenten Messsystemen und anderen Technologien ist dort beschrieben.

Die bereits abgeschlossene Studie «Ansätze zur Gewährleistung der IKT-Sicherheit von intelligenten Messsystemen bei Endverbrauchern» (siehe Ref. [10]) hat verschiedene Varianten zur Sicherheitsprüfung intelligenter Messsysteme aufgezeigt. Die dort angestellten Untersuchungen kamen u. a. zum Schluss, dass eine spezifische Schutzbedarfsanalyse (SBA) für die Untersuchung von substanziellen Risiken in Zusammenhang mit intelligenten Messsystemen beim Endverbraucher notwendig ist.

Die vorliegende SBA dient als fundamentale Basis zur Erkennung von möglichen Schwachstellen und Bedrohungen in Bezug auf intelligente Messsysteme sowie zur wirksamen Reduktion von identifizierten Risiken mittels Umsetzung der empfohlenen Sicherheitsmassnahmen. Dies erhöht die Widerstandsfähigkeit von intelligenten Messsystemen beträchtlich und damit indirekt auch die Widerstandsfähigkeit der kritischen Infrastruktur Stromversorgung. Die SBA soll der Branche als Grundlage bei der Entwicklung konkreter IKT-Sicherheitsanforderungen bezüglich Smart Metering dienen und allenfalls auch weiteren interessierten Akteuren eine Einschätzung der Risiken in diesem Bereich erlauben. Mit ihren Massnahmenvorschlägen adressiert sie in erster Linie Datenmanager als Betreiber von intelligenten Messsystemen.

Für die Durchführung der SBA wurde zunächst eine konsistente und umfassende Methodik gemäss Kapitel 2 eingeführt, die auf den in der Praxis bewährten Verfahren und Standards aus dem Bereich *Risiko- und Sicherheitsmanagement* basiert.

Im Rahmen der Systemanalyse für das intelligente Messsystem wurden die Architekturvarianten in Kapitel 3.1 eruiert und beurteilt. Die für die vorliegende SBA relevanten Anwendungsfälle, die sogenannten Use Cases (UC), wurden aus Ref. [2] «Datensicherheit und Datenschutz für Smart Grids: Offene Fragen und mögliche Lösungsansätze» übernommen. Sie werden in Kapitel 3.2 bezüglich ihrer Relevanz zur Erfüllung möglicher Mindestanforderungen aus Ref. [1] «Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz - Technische Mindestanforderungen und Einführungsmodalitäten» beurteilt. Anschliessend wurde in Kapitel 3.3 ein *konzeptionelles*, intelligentes Messsystem beim Endverbraucher als architektonische Ausgangsbasis für die Systemanalyse angenommen und dargestellt. Dieses konzeptionelle Konstrukt des intelligenten Messsystems besteht aus einem «Intelligenten Messgerät», einem «Kommunikationssystem», einem «Zähldatenverarbeitungssystem» und einer «Online-Visualisierungsplattform». Es orientiert sich an der Definition eines intelligenten Messsystems aus Ref. [1], Kapitel 2, die schon für die Erarbeitung von möglichen technischen Mindestanforderungen zugrunde gelegt wurde. In Kapitel 3.4 wurde das Untersuchungsfeld geeignet abgegrenzt und die notwendigen, grundlegenden Annahmen getroffen.

In weiteren, iterativen Schritten wurden auf Basis des konzeptionellen, intelligenten Messsystems die Schutzobjekte, Schwachstellen und Bedrohungen identifiziert (vgl. Kapitel 4). Die aus Ref. [1]

hergeleiteten Schwachstellen dienten zusammen mit dem Bedrohungskatalog aus Kapitel 4.3 als Basis für die Identifikation und Bildung von sogenannten «Kern Risiko-Szenarien».

In Kapitel 5 sind vierzehn «Kern Risiko-Szenarien» identifiziert, die in vier Szenariogruppen zusammengefasst sind: «Abrechnungsbetrug», «Verlust von Verfügbarkeit und Integrität», «Netzinstabilitäten» und «Verletzung von Vertraulichkeit und Datenschutz». Die Anzahl der «Kern Risiko-Szenarien» wurde bewusst gering gehalten, damit die Übersicht erhalten bleibt und die Wiederverwendbarkeit der Szenarien zukünftig in allfällig weiteren Schutzbedarfsanalysen und Risikomanagementprojekten für intelligente Messsysteme gewährleistet werden kann.

Bei der Bewertung der aus den Szenarien resultierenden Risiken wurden zwei unterschiedliche Sichten eingenommen, die des Prosumers (sowohl Einspeiser als auch Endverbraucher, siehe Seite 3) und die des Datenmanagers.

Die Abbildung A auf Seite 8 stellt zusammenfassend die Ergebnisse der Risikobewertung dar. Die unterschiedlichen Farben der Risikowerte veranschaulichen die vier Szenariogruppen gemäss Legende. Die Risikowerte lassen sich anhand der Risikomatrix in drei Risikokategorien gliedern: geringes Risiko (grün hinterlegter Bereich), mittleres Risiko (gelb hinterlegter Bereich), hohes Risiko (rot hinterlegter Bereich).

Für die Kern Risiko-Szenarien und deren Beurteilung in Bezug auf Eintrittswahrscheinlichkeit und Schadensausmass dienen Worst Case Überlegungen als Basis. Weil solche Extremereignisse selten zu erwarten sind, wurden die Eintrittswahrscheinlichkeiten generell tief eingestuft.

Die hohen Risikowerte R.05, R.06, R.08, R.09, R.10 und R.11 für Prosumer und Datenmanager resultieren aus den entsprechenden Kern Risiko-Szenarien (RS.05, RS.06, RS.08, RS.09, RS.10 und RS.11), welche u. a. auch mit der Gefährdung der überregionalen Versorgungssicherheit zusammenhängen (vgl. Abbildung A). Die in der SBA verwendete Definition einer solchen Gefährdung ist in Kapitel 2, Arbeitsschritt 7 beschrieben.

Die Kern Risiko-Szenarien RS.08, RS.09, RS.10 und RS.11 (d.h. die Szenariogruppe «Netzinstabilitäten») bilden Spezialfälle von RS.05 «Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten» und RS.06 «Schwerwiegende Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems»:

- RS.08 behandelt den Fall „Lastunterbrecher (Breaker)“, durch welchen eine böswillige oder fehlerhafte Beschränkung oder An- und Abschaltung des Anschlusses bei Prosumern möglich sein kann.
- RS.09 deckt eine mögliche böswillige oder fehlerhafte Steuerung von Verbrauch und Einspeisung der elektrischen Energie bei Prosumern inkl. Haushaltsgeräte wie z. B. Ofen, Klimaanlage etc. ab.
- RS.10 umfasst eine eventuelle böswillige oder fehlerhafte Steuerung von Haus- und Gebäudeautomation bei Prosumern z. B. mittels Aktivierung oder Deaktivierung von Lüftung, Lift etc.
- RS.11 behandelt die mögliche Gefährdung des Netzzustandes durch grossflächige Manipulation oder Einschränkung der Netzüberwachung unter der Annahme dass eine solche Manipulation via intelligentes Messsystem möglich ist.

Auch beim Kern Risiko-Szenario RS.07 «Schwerwiegende Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform» könnte die überregionale Versorgungssicherheit durch negatives Beeinflussen des Prosumerverhaltens im Extremfall – beispielsweise infolge plötzlicher Netzüberlastung – gefährdet werden. Dies ist jedoch eher unwahrscheinlich, daher wurde der entsprechende Risikowert R.07 aus Sicht Datenmanager als „Mittel“ eingestuft.

Ein Abrechnungsbetrug kann in Einzelfällen (R.01a, R.03a) für Prosumer und Datenmanager zu merklichen Schäden führen. Hohe Schäden wären dagegen die Folge grossflächiger Betrugsfälle wie R.01b und R.03b für Prosumer und R.01b, R.02, R.03b und R.04 für Datenmanager. Letztere resultieren aufgrund der relativ tiefen Eintrittswahrscheinlichkeiten jeweils in einem mittleren Risikowert. Es ist jedoch davon auszugehen, dass sich die Bedrohungslage zukünftig weiter verschärft und der grossflächige Abrechnungsbetrug zu einem hohen Risikowert tendiert.

Die Risiken für RS.12 «Offenlegung / Entwendung der auf intelligenten Messgeräten verwalteten Daten inkl. Datenübertragung», RS.13 «Schwerwiegende Daten-Offenlegung / -Entwendung via Zähldatenverarbeitungssystem» und RS.14 «Schwerwiegende Daten-Offenlegung / -Entwendung via Online-Visualisierungsplattform» sind nur aus Sicht des Datenmanagers zu bewerten, da diese Szenarien aufgrund ihrer Art zu einem rein indirekten Schaden für den Prosumer führen würden. Aus Sicht des Datenmanagers stellen die Risikowerte R.12, R.13 und R.14 ein mittleres Risiko dar.

Die qualitative Beurteilung des Schutzbedarfs erfolgte auf Basis von sechs Fragen gemäss Kapitel 2, Arbeitsschritt 10) und durch eine kombinierte Sicht vom Prosumer und Datenmanager, damit umfassende Schlussfolgerungen über alle Risiko-Szenarien hinweg erreicht werden konnten.

Auf Basis der gewonnenen Erkenntnisse wird für intelligente Messsysteme insgesamt ein angemessen hohes Schutzniveau empfohlen.

In Kapitel 6 werden Massnahmenempfehlungen zur Risiko-Reduktion für intelligente Messsysteme abgegeben, die mehrheitlich den Datenmanager adressieren. Ziel ist die branchenweit harmonisierte Erstellung und Umsetzung eines Massnahmenkataloges zur Gewährleistung eines adäquaten Basisschutzniveaus – auch als Grundschutz bezeichnet. Eine kleinere Zahl weiterer Empfehlungen wendet sich an den Prosumer oder externen Dienstleister. Eine Konkretisierung der einzelnen Massnahmen muss durch den Datenmanager für seinen Einzelfall erfolgen. In diesem Kontext kann auch eine Priorisierung der Umsetzung von Massnahmen anhand der in Abbildung A ausgewiesen Risikowerte ins Auge gefasst werden. Diese muss jedoch kritisch geprüft werden, weil sich dadurch das Niveau des Grundschutzes stark reduzieren könnte.

In Kapitel 7.2 wird ein ganzheitliches Vorgehen zur Entwicklung konkreter IKT-Sicherheitsanforderungen durch die Branche empfohlen, das nicht nur die Produktsicherheit sondern auch die integrale Systemsicherheit inkl. betrieblicher Prozesse und Abläufe berücksichtigt. Hinsichtlich etwaig notwendiger regulatorischer Grundlagen verbleibt zu prüfen, inwiefern neue Rahmenbedingungen auf Bundes- oder Branchenebene geschaffen oder bestehende geändert oder ausgeweitet werden müssen, um einen umfassenden und angemessenen Grundschutz zu gewährleisten.

Die Ergebnisse der vorliegenden Schutzbedarfsanalyse zeigen klar, dass durch den Einsatz von intelligenten Messsystemen die Anfälligkeit der öffentlichen Stromversorgung, die zu den kritischen Infrastrukturen gehört, erhöht wird. Dies wird vor allem durch die erhöhte Nutzung von Informations- und Kommunikationstechnologien sowie durch die fortschreitende Vernetzung intelligenter Messsysteme u. a. mit Haus-, Gebäude- und Anlagesteuerungen sowie mit den zentralen Überwachungs- und Steuersystemen der Netzbetreiber verstärkt. Insbesondere bieten die intelligenten Messgeräte, die künftig praktisch bei jedem Prosumer und dadurch in vielen Haushalten installiert werden sollen, vielfältige und örtlich verteilte Angriffsmöglichkeiten, was einen grossen Schutzbedarf dieser Geräte nach sich zieht.

Die vorliegende SBA hat einen branchenweiten, universellen Charakter und erlaubt dadurch eine Adaption auf konkrete Umsetzungsvorhaben für intelligente Messsysteme. Der spezifische Risikokontext dedizierter Umsetzungsprojekte ist hingegen in der SBA nicht abgebildet. Die vorhabens- und umsetzungsspezifischen Schwachstellen und Bedrohungen sind dementsprechend in den Einzelfällen aus den allgemeinen Grundlagen abzuleiten, die im vorliegenden Bericht zur SBA aufgeführt sind. Die Betreiber und Verantwortlichen der intelligenten Messsysteme müssen also eine Transferleistung zwischen den Ergebnissen der vorliegenden Untersuchung und ihren konkreten Umsetzungsvorhaben erbringen.

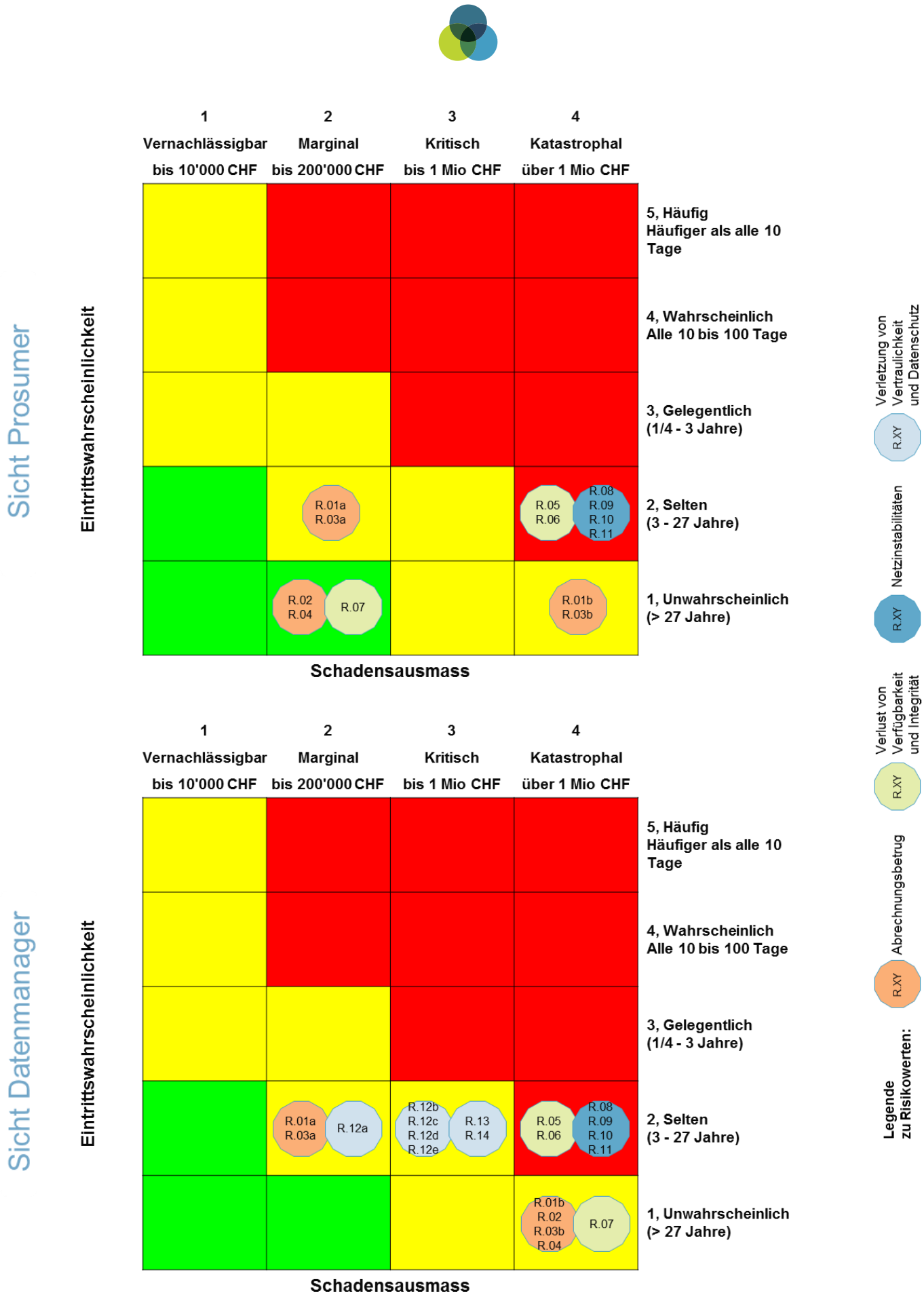


Abbildung A: Gesamtübersicht Risikobewertung für Prosumer (oben) und Datenmanager (unten) Risikokategorien: Gering (grün), Mittel (gelb), Hoch (rot)

Résumé

Les systèmes de mesure intelligents chez le consommateur final – *smart metering* – sont un composant élémentaire des réseaux intelligents - *smart grids*. Ces derniers constituent une des infrastructures importantes qui permettront, à moyen terme, d'intégrer les énergies renouvelables de manière économiquement avantageuse et techniquement sûre. En outre, les réseaux intelligents sont également une plateforme technique pour les futurs marchés de services énergétiques et contribuent, en particulier grâce aux systèmes de mesure intelligents, à la libéralisation – éventuellement complète – du marché de l'électricité.

Les systèmes de mesure intelligents installés chez le consommateur final font partie intégrante de la Stratégie énergétique 2050 et donc du futur système d'approvisionnement public en électricité. De manière indirecte, ils font donc partie des infrastructures critiques de la Suisse.

Grâce à leur interconnexion avec d'autres technologies du domaine des réseaux intelligents par le biais des technologies de l'information, les systèmes de mesure intelligents soutiennent non seulement les processus de décompte d'énergie et les prestations du marché de l'électricité, mais également de nouvelles fonctionnalités des réseaux électriques. La «Feuille de route suisse pour un réseau intelligent» (cf. réf. [14]) identifie de telles fonctionnalités et décrit l'interaction des systèmes de mesure intelligents avec d'autres technologies.

L'étude «Ansätze zur Gewährleistung der IKT-Sicherheit von intelligenten Messsystemen bei Endverbrauchern» (cf. réf. [10], disponible en allemand) indique différentes variantes permettant de contrôler la sécurité des systèmes de mesure intelligents. Elle conclut entre autres qu'une analyse spécifique du besoin de protection est nécessaire pour évaluer les risques substantiels en lien avec les systèmes de mesure intelligents chez le consommateur final.

La présente analyse du besoin de protection sert de base à l'identification d'éventuels points faibles des systèmes de mesure intelligents et des éléments représentant une menace pour l'exploitation sûre de ces systèmes. Cette analyse sert également à réduire efficacement les risques identifiés en mettant en œuvre les mesures de sécurité recommandées. Cela permet d'augmenter considérablement la capacité de résistance des systèmes de mesure intelligents et donc indirectement celle de l'infrastructure critique qu'est celle de l'approvisionnement en électricité. L'analyse du besoin de protection doit servir de base à la branche électrique dans l'élaboration d'exigences concrètes en matière de technologies de l'information et de la télécommunication (TIC) pour les systèmes de mesure intelligents. Elle permet aussi éventuellement à d'autres acteurs intéressés d'estimer les risques dans ce domaine. Les recommandations proposées par l'analyse s'adressent en premier lieu aux gestionnaires de données, en tant que gestionnaire de systèmes de mesure intelligents.

Le document présente en premier lieu (chap. 2) la méthodologie globale et cohérente utilisée pour mener cette analyse. La méthodologie repose sur des procédures et des normes ayant fait leurs preuves dans la pratique dans le domaine de la gestion des risques et de la sécurité.

L'analyse systémique auquel le système de mesure intelligent a été soumis a permis d'identifier et d'évaluer des variantes d'architecture (chap. 3.1). Les cas d'application pertinents pour l'analyse du besoin de protection, ou *Use Cases* (UC), proviennent du document «Datensicherheit und Datenschutz für Smart Grids: Offene Fragen und mögliche Lösungsansätze» (réf. [2], disponible en allemand). Ils font l'objet d'une évaluation au chap. 3.2, dans la perspective de leur pertinence pour remplir les exigences minimales possibles décrites dans le document «Bases pour l'introduction de systèmes de mesure intelligents auprès du consommateur final en Suisse – Exigences techniques minimales et modalités d'introduction» (réf. [1]). Le chap. 3.3 adopte et présente ensuite un système de mesure intelligent *théorique* installé chez le consommateur final en tant que point de départ architectural de l'analyse systémique. Cette structure théorique de système de mesure intelligent est composée d'un appareil de mesure intelligent, d'un système de communication, d'un système de traitement des données mesurées et d'une plateforme de visualisation en ligne. Cette structure s'aligne sur la définition du système de mesure intelligent donnée au chap. 2 du document en réf. [1], définition qui a déjà servi de base à l'élaboration des exigences

techniques minimales possibles. Le chap. 3.4 délimite le champ d'analyse de manière appropriée et définit les hypothèses fondamentales nécessaires.

Les objets à protéger ainsi que leurs points faibles et les menaces possibles sont ensuite identifiés en procédant par étapes itératives et en s'appuyant sur le système de mesure intelligent théorique (cf. chap. 4). Les points faibles déduits du document en réf. [1], accompagnés du catalogue de menaces défini au chap. 4.3, servent de base à l'identification et à l'élaboration de «scénarios de risque élémentaires».

Le chap. 5 présente quatorze scénarios de risque élémentaires répartis dans quatre groupes de scénarios: «décompte frauduleux», «perte de disponibilité et d'intégrité», «instabilité du réseau» et «violation de la confidentialité et de la protection des données». Le nombre de scénarios de risque élémentaires a été maintenu volontairement à un niveau bas, afin de conserver une vue d'ensemble et de garantir la possibilité de réutiliser les scénarios à l'avenir dans le cadre d'éventuelles autres analyses des besoins de protection et de projets de gestion des risques en rapport avec les systèmes de mesure intelligents.

L'évaluation des risques découlant des scénarios adopte deux points de vue différents: celui du prosommateur (tant consommateur que producteur, voir page 3) et celui du gestionnaire de données.

La figure A à la page 13 résume les conclusions de l'évaluation des risques. Selon la légende, les différentes couleurs des valeurs de risque mettent en évidence les quatre groupes de scénarios. La matrice des risques permet de répartir les valeurs de risque en trois catégories: risque faible (fond vert), risque moyen (fond jaune), risque élevé (fond rouge).

Les scénarios de risque élémentaires et leur évaluation par rapport à la probabilité d'occurrence et à l'ampleur des dommages reposent sur des réflexions qui envisagent le cas le plus défavorable (*worst case*). Etant donné que ces types d'événements extrêmes sont rares, les probabilités d'occurrence attribuées sont en général faibles.

Les valeurs de risque élevées pour le prosommateur et le gestionnaire de données (R.05, R.06, R.08, R.09, R.10 et R.11) résultent les scénarios de risque élémentaires correspondants (RS.05, RS.06, RS.08, RS.09, RS.10 et RS.11). Ces scénarios de risque concernent entre autres également la mise en danger de la sécurité de l'approvisionnement suprarégionale (cf. figure A). La définition d'une telle menace dans le cadre de la présente étude figure dans le rapport à l'étape 7 du chapitre 2.

Les scénarios de risque élémentaires RS.08, RS.09, RS.10 et RS.11 (autrement dit le groupe de scénarios «instabilité du réseau») constituent des cas spéciaux de RS.05 «restriction de la disponibilité et de l'intégrité des appareils de mesure intelligents» et de RS.06 «restriction grave de la disponibilité et de l'intégrité du système de traitement des données mesurées»:

- RS.08 concerne le cas de «l'interrupteur de charge (*breaker*)», qui peut entraîner une restriction, une activation ou une coupure malveillante ou erronée du raccordement du prosommateur;
- RS.09 couvre l'éventuelle commande malveillante ou erronée de la consommation et de l'injection d'énergie électrique chez le prosommateur, y compris les appareils ménagers comme le four, la climatisation, etc.;
- RS.10 traite l'éventuelle gestion malveillante ou erronée de la domotique et de l'immotique chez le prosommateur (p. ex. activation ou désactivation de l'aération, des ascenseurs, etc.);
- RS.11 concerne l'éventuelle mise en danger de l'état du réseau en raison d'une manipulation à grand échelle ou d'une réduction de la surveillance du réseau, en admettant qu'un système de mesure intelligent permette une telle manipulation.

Dans le scénario de risque élémentaire RS.07 «restriction grave de la disponibilité et de l'intégrité de la plateforme de visualisation en ligne», la sécurité de l'approvisionnement suprarégionale pourrait également être menacée par l'influence négative du comportement du prosommateur dans les cas extrêmes, par exemple suite à une surcharge soudaine du réseau. Cela est toutefois très im-

probable, ce qui en résulte la valeur de risque R.07 classée «moyenne» du point de vue du gestionnaire de données.

Un décompte frauduleux peut, dans des cas particuliers (R.01a, R.03a), causer des dommages notables pour le prosommateur et le gestionnaire de données. Les dommages seraient en revanche considérables en cas de fraude à large échelle (R.01b et R.03B pour le prosommateur et R.01b, R.02, R.03b et R.04 pour le gestionnaire de données). Ce type de risque est finalement classée «moyen» en raison de sa probabilité d'occurrence relativement faible. Il faut toutefois s'attendre à ce que la menace continue à s'intensifier à l'avenir et que le décompte frauduleux à large échelle tende à se rapprocher d'une valeur de risque élevée.

Les risques relatifs à RS.12 «divulgation / soustraction de données gérées par des appareils de mesure intelligents, transfert de données inclus», à RS.13 «divulgation / soustraction de données d'extrême gravité via le système de traitement des données mesurées» et à RS.14 «divulgation / soustraction de données d'extrême gravité via la plateforme de visualisation en ligne» doivent être évalués uniquement du point de vue du gestionnaire de données car, de par leur nature, les scénarios en question occasionneraient des dommages indirects pour le prosommateur. Du point de vue du gestionnaire de données, les valeurs de risque R.12, R.13 et R.14 représentent un risque moyen.

L'évaluation qualitative du besoin de protection repose sur six questions (cf. chap. 2, étape de travail 10) et part d'une vue combinée du prosommateur et du gestionnaire de données, afin d'obtenir des conclusions globales qui tiennent compte de l'ensemble des scénarios de risque.

Sur la base de ces conclusions, le rapport recommande un niveau de protection raisonnablement élevé pour les systèmes de mesure intelligents.

Le chap. 6 recommande des mesures visant à réduire les risques liés aux systèmes de mesure intelligents. Ces recommandations s'adressent pour la plupart au gestionnaire de données, l'objectif étant d'élaborer et de mettre en œuvre un catalogue de mesures harmonisé pour l'ensemble de l'industrie électrique permettant de garantir un niveau de protection de base adéquat. D'autres recommandations, en moins grand nombre, s'adressent au prosommateur ou au prestataire de service externe. Une concrétisation des mesures individuelles doit être menée par le gestionnaire de données, dans son cas particulier. Dans ce contexte, on peut envisager une priorisation de la mise en œuvre des mesures selon les valeurs de risque présentées à la figure A. Une telle priorisation doit être cependant examinée de manière critique, car elle pourrait induire une forte réduction du niveau de protection de base.

Le chap. 7.2 recommande une démarche globale pour le développement d'exigences concrètes en matière de sécurité des TIC par la branche, démarche qui tient compte non seulement de la sécurité du produit, mais aussi de la sécurité intégrale du système, processus et déroulements opérationnels compris. Quant à l'éventuelle nécessité de définir des conditions-cadres réglementaires, il reste à évaluer dans quelle mesure la garantie d'une protection de base globale et appropriée requiert la création de nouvelles conditions-cadres (au niveau de la Confédération ou de la branche), ou la modification ou l'extension de conditions-cadres existantes.

Les résultats de la présente analyse du besoin de protection montrent clairement que le recours à des systèmes de mesure intelligents augmente la vulnérabilité de l'approvisionnement public en électricité, dont l'infrastructure correspondante fait partie des infrastructures critiques. L'utilisation accrue des TIC et l'interconnexion progressive des systèmes de mesure intelligents avec notamment des systèmes de commande d'habitations, de bâtiments et d'installations ainsi qu'avec les systèmes centraux de commande et de surveillance des gestionnaires de réseau viendront renforcer cette tendance. Les appareils de mesure intelligents, qui seront à l'avenir installés chez quasiment tous les prosommateurs et donc dans de nombreux ménages, offrent en particulier des possibles points d'attaques étendus et géographiquement éparpillés, ce qui engendre un fort besoin de protection pour ces appareils.

La présente analyse du besoin de protection a un caractère universel au sein de la branche, ce qui permet une adaptation aux projets concrets de mise en œuvre de systèmes de mesure intelligents. En revanche, l'analyse ne rend pas compte du contexte de risque spécifique relatif aux projets de

mise en œuvre dédiés. Les points faibles et les menaces spécifiques aux projets et leur mise en œuvre doivent par conséquent être identifiés à partir des fondements généraux définis dans le présent rapport. Les gestionnaires et les responsables des systèmes de mesure intelligents doivent donc procéder à un travail de transfert entre les résultats de la présente analyse et leurs projets concrets de mise en œuvre.

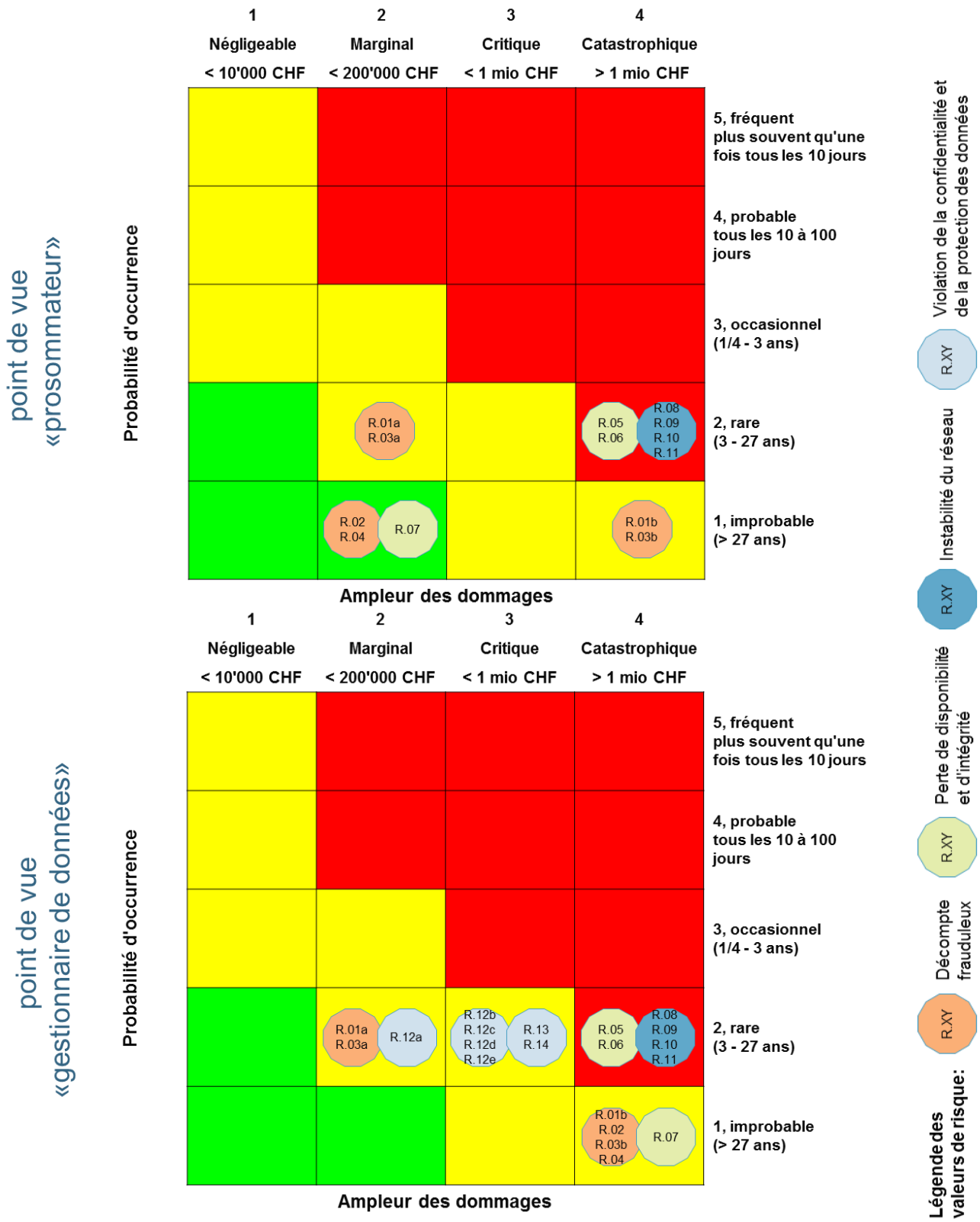


Figure A: vue d'ensemble de l'évaluation des risques pour le prosommateur (en haut) et le gestionnaire de données (en bas). Catégories de risques: faible (vert), moyen (jaune), élevé (rouge).

Inhaltsverzeichnis

1. Ausgangslage und Zielsetzungen

Intelligente Messsysteme beim Endverbraucher – sogenannte Smart Metering Systeme – sind ein wichtiger und erster Baustein intelligenter Netze. Sie tragen zur Erhöhung der Energieeffizienz bei, indem sie helfen, Strom zu sparen. Sie unterstützen neuartige Funktionalitäten der elektrischen Netze (siehe Ref. [14]) und bilden eine Infrastruktur, die eine allfällige vollständige Liberalisierung des Strommarktes unterstützt, in dem Transaktionskosten, wie z. B. Aufwendungen für einen Lieferantenwechsel, reduziert werden. Intelligente Messsysteme sind ein integraler Bestandteil der Energiestrategie 2050[16].

Eine Definition eines intelligenten Messsystems sowie mögliche, technische Mindestanforderungen, welche diese Systeme bei einer landesweiten Einführung aufweisen könnten, finden sich im entsprechenden Grundlagendokument des Bundesamtes für Energie (siehe Ref. [1]). Diese Grundlagen werden als Orientierungshilfe und als Basis für nötige Annahmen im Rahmen dieser Studie verwendet. Damit wird der notwendigen Konsistenz mit den bisherigen Untersuchungen des Bundes in angemessener Weise Rechnung getragen.

Die Resultate einer bereits abgeschlossenen Untersuchung (vgl. Ref. [10]) zeigten, dass eine spezifische Schutzbedarfsanalyse (SBA) zur Identifikation, Analyse und Beurteilung von konkreten, durch den Einsatz von intelligenten Messsystemen beim Endverbraucher entstehenden Risiken notwendig ist. Die SBA ist eine wichtige Voraussetzung und Grundlage für die Definition eines Anforderungskatalogs zur Gewährleistung der IKT-Sicherheit der intelligenten Messsysteme und für eine darauf aufbauende Prüfung der Einhaltung dieser Anforderungen. Ausserdem ist sie zentral, um eine Akzeptanz der Sicherheitsmassnahmen zur Gewährleistung der IKT-Sicherheit bei intelligenten Messsystemen zu schaffen.

Die vorliegende Studie setzt die Durchführung der in Ref. [10] geforderten SBA für intelligente Messsysteme in der Schweiz um und hat folgende Zielsetzungen in Bezug auf intelligente Messsysteme beim Endverbraucher:

- Identifikation von Schutzobjekten sowie Erkennung und Analyse möglicher Schwachstellen und Bedrohungen
- Risikoidentifikation und -bewertung
- Beurteilung Schutzbedarf und Empfehlung eines geeigneten Schutzniveaus
- Vorschlag geeigneter Sicherheitsmassnahmen zur wirksamen Reduktion der identifizierten Risiken
- Aufzeigen eines Vorgehens zur Entwicklung konkreter IKT-Sicherheitsanforderungen

Die intelligenten Messsysteme sind Bestandteil der öffentlichen Stromversorgung und gehören dadurch indirekt zu den kritischen Infrastrukturen der Schweiz. Während der Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS (siehe Ref. [11]) wurde 2015 eine Risiko- und Verwundbarkeitsanalyse des Teilsektors Stromversorgung durch das Bundesamt für wirtschaftliche Landesversorgung BWL erstellt. Smart Metering und -Grid werden in dieser NCS-Analyse nur im Rahmen eines Zukunftsausblickes erwähnt. Weiter liefert die NCS keine direkt vergleichbaren, quantitativen Risikogrundlagen, mit denen die Resultate dieser Schutzbedarfsanalyse abgestimmt werden könnten. Die vorliegende Schutzbedarfsanalyse vertieft vielmehr die NCS-Analyse im Teilbereich Smart Metering und bildet somit eine geeignete Grundlage für

[16] Die Verordnungsarbeiten zur Energiestrategie 2050 haben begonnen. Sie sollen bis im Sommer 2016 abgeschlossen werden und anschliessend in den Konsultationsprozess gehen. Dabei werden auch die in Energiestrategie 2050 vorliegenden Gesetzesartikel Art. 17a StromVG (neu) zum Smart Metering konkretisiert.

nachfolgende Arbeiten. Auf eine weitere Abstimmung mit der NCS-Analyse wurde im Rahmen dieser SBA verzichtet.

2. Methodik zur Durchführung der Schutzbedarfsanalyse

Die zur Durchführung der vorliegenden SBA eingesetzte Methodik ist in der folgenden Abbildung dargestellt und basiert auf den in der Praxis bewährten Verfahren und Normen aus dem Bereich *Risiko- und Sicherheitsmanagement* wie z. B. ISO 31000 und ISO 27005. Bei der Behandlung von Detailschritten wie z.B. der Identifikation von Schutzobjekten, Schwachstellen und Bedrohungen oder der Bildung von Kern Risiko-Szenarien, sind Best-Practices der AWK eingeflossen.

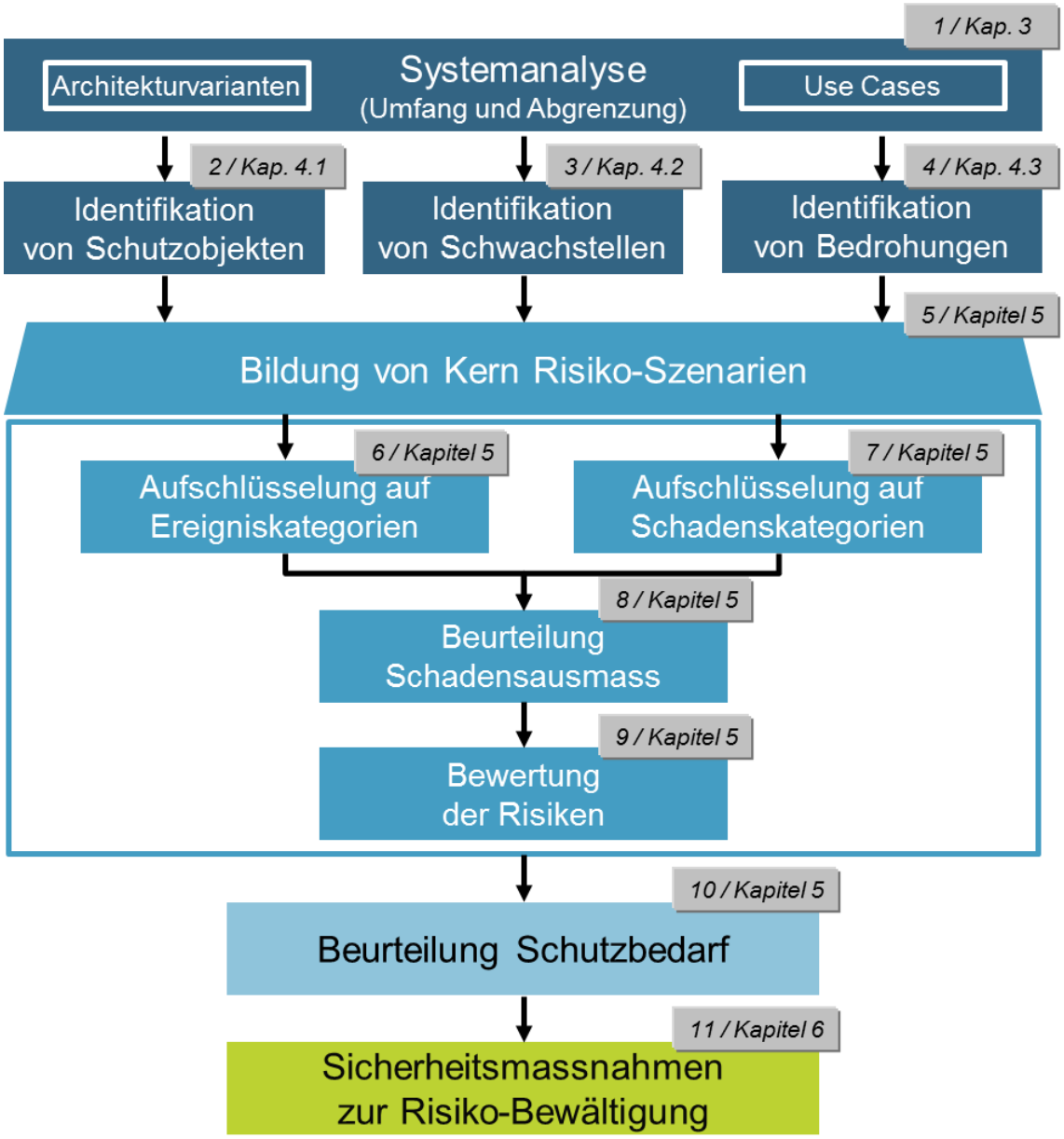


Abbildung 1: Methodik Schutzbedarfsanalyse

Das in Abbildung 1 dargestellte Vorgehen umfasst folgende Arbeitsschritte:

1) **Systemanalyse**: Bei der Systemanalyse wurde das intelligente Messsystem beim Endverbraucher detailliert untersucht, um eine fundierte Basis für die nachfolgende Sicherheitsanalyse zur Identifikation von Schutzobjekten, Schwachstellen und Bedrohungen zu bilden. Vorerst wurden die möglichen, aktuellen Architekturvarianten für intelligente Messsysteme evaluiert und studiert, damit wesentliche Architekturen bezüglich intelligenter Messsysteme beim Endverbraucher in der SBA berücksichtigt werden. Die für den Bereich «intelligente Messsysteme beim Endverbraucher» relevanten Anwendungsfälle (Use Cases) wurden in einem weiteren Arbeitsschritt aus Ref. [2] identifiziert und bezüglich möglicher Daten und Datenströme analysiert. Um die möglichen Mindestanforderungen aus Ref. [1] in Bezug auf deren Relevanz für die vorliegende SBA zu beurteilen, wurden die Mindestanforderungen aus Ref. [1] den für die SBA relevanten Use Cases zugeordnet. Anschliessend wurden der Umfang und die Abgrenzung der vorliegenden SBA mit Hilfe der erarbeiteten Resultate festgelegt und präzisiert. Für den Rest der SBA wurde von der Annahme ausgegangen, dass das betrachtete, konzeptionelle intelligente Messsystem alle Mindestanforderungen aus Ref. [1] mit Ausnahme von 4.1.3C (Recht auf Ausnahmen), 4.1.4A (Lebensdauer) und 4.1.4B (Eigenstromverbrauch) umsetzt und so die daraus resultierenden technischen Merkmale und Eigenschaften wie z. B. die Funktionalität für Softwareaktualisierung aus der Ferne innehat.

2) **Identifikation von Schutzobjekten**: Auf Basis der Resultate der vorangehenden Systemanalyse wurden die Schutzobjekte (Assets) betreffend das intelligente Messsystem identifiziert und in über- bzw. untergeordnete Schutzobjekte aufgeteilt. Die übergeordneten Schutzobjekte bestehen aus dem intelligente Messsystem bzw. dessen vier Komponenten «Intelligentes Messgerät», «Kommunikationssystem», «Zähldatenverarbeitungssystem» und «Online-Visualisierungsplattform».

3) **Identifikation von Schwachstellen**: Schwachstellen (Vulnerabilities) sind Verwundbarkeiten oder mögliche Angriffspunkte bei Schutzobjekten, die eine Einwirkung von potentiellen Gefahren (Bedrohungen) ermöglichen. Für die Identifikation von möglichen Schwachstellen dienten die technischen Merkmale und Eigenschaften, die aus einer eventuellen Umsetzung der technischen Mindestanforderungen aus Ref. [1] resultieren, als primäre Quelle (siehe auch unter Punkt 1) **Systemanalyse**). Beispielsweise kann die Funktionalität für Softwareaktualisierung aus der Ferne aufgrund einer fehlerhaften Sicherheitskonzeption zum mutwilligen oder unabsichtlichen Einspielen von fehlerhaften Software-Updates führen, was die betroffenen intelligenten Messgeräte u. U. betriebsunfähig machen könnte.

4) **Identifikation von Bedrohungen**: Die Bedrohungen sind potentielle Gefahren (z. B. Sabotage, Feuer, Explosion etc.), deren Einwirkung Schäden an den Schutzobjekten verursachen kann. Im Rahmen dieser SBA wurde auf den in der Praxis bewährten Bedrohungskatalog aus Ref. [12] zurückgegriffen, der auf den Bedrohungskatalogen des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) beruht. Die fünf Bedrohungskategorien «Höhere Gewalt», «Organisatorische Mängel», «Menschliche Fehlhandlungen», «Technisches Versagen» und «Vorsätzliche Handlungen» wurden aus diesem Katalog unverändert übernommen. Die einzelnen Bedrohungen wurden zum Teil angepasst, um den Bezug auf intelligente Messsysteme beim Endverbraucher zu verstärken.

5) **Bildung von Kern Risiko-Szenarien**: Basierend auf ISO 31000 und ISO 27005, die aktuell führenden Normen im Gebiet des Risikomanagements, wurde für die Analyse von Risiken in Bezug auf intelligente Messsysteme beim Endverbraucher die *Szenario-basierte Analyse* eingesetzt. Die Stärke dieser Methode liegt darin, dass durch die gebildeten Risiko-Szenarien ein umfangreiches und übersichtliches Bedrohungsbild erstellt werden kann.
   In der vorliegenden SBA dienen die Informationen aus der Systemanalyse sowie die

identifizierten Schutzobjekte, Schwachstellen und Bedrohungen als Basis und Gedankenstütze zur Bildung der Risiko-Szenarien. Beim Erarbeiten von Risiko-Szenarien wurden intensive Gedankenexperimente mittels Analyse der potentiellen Gefahren und deren mögliche Wirkungen auf entdeckte Schwachstellen und Schutzobjekten durchgeführt. Dabei wurde festgestellt, dass etliche Detail-Risiko-Szenarien denkbar sind, was den Rahmen dieser Studie hinsichtlich Übersichtlichkeit und Detailtiefe sprengen würde. Aus diesem Grund wurden die sogenannten «Kern Risiko-Szenarien» definiert. Die Kern Risiko-Szenarien sind übergeordnete Szenarien, die mögliche Detail-Szenarien beinhalten und so ein umfassendes Bild über die Risikolandschaft ermöglichen. Diese SBA umfasst vierzehn Kern Risiko-Szenarien mit dem Zusatzziel, dass diese künftig bei weiteren, möglichen Schutzbedarfsanalysen und Risikomanagementprojekten in Bezug auf intelligente Messsysteme wiederverwendet werden können.

Aufgrund des relativ hohen Abstraktionsgrades der Kern Risiko-Szenarien bzw. deren Varianten sind die zugrundeliegenden Use Cases und Schwachstellen nicht direkt ersichtlich. Eine Zuordnung der Use Cases und Schwachstellen auf die «Kern Risiko-Szenarien» wurde daher im Anhang A.3 erstellt, um die Rückverfolgung auf die Risiko-Szenarien zu vereinfachen.

Für jedes einzelne Kern Risiko-Szenario wurde ein eigener Steckbrief erstellt. Das folgende Beispiel (vgl. Abbildung 2) zeigt den Steckbrief für das Kern Risiko-Szenario «RS.08: Böswillige oder fehlerhafte Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern». Die detaillierte Behandlung von RS.08 findet sich im Kapitel 5.

Jeder Steckbrief enthält die relevanten Bemerkungen und Annahmen sowie die für das jeweilige Kern Risiko-Szenario relevanten Szenariovarianten und übergeordneten Schutzobjekte des intelligenten Messsystems.

Den Kern Risiko-Szenarien bzw. deren Varianten liegen jeweilige *Worst Case* Überlegungen zugrunde. Auch bei der Beurteilung der Risiko-Szenarien in Bezug auf deren Eintrittswahrscheinlichkeit und Schadensausmass im Schritt 9) wird der Worst Case betrachtet.

Die Variantenbildung bei den Kern Risiko-Szenarien erfolgte unter Berücksichtigung von Bedrohungskategorien und abhängig davon, ob es sich um vereinzelte, punktuelle, grossflächige oder schwerwiegende Geschehnisse handelt. Die Attribute «vereinzelt» und «punktuell» deuten darauf hin, dass es sich um einige wenige, jedoch schwere Vorfälle handelt. Während das Attribut «grossflächig» auf eine Vielzahl von örtlich verteilten, folgenschweren Ereignissen hindeutet, signalisiert das Attribut «schwerwiegend» Vorfälle, die generell folgenschwer sind und nicht unbedingt örtlich verteilt sein müssen. Die Szenariovarianten bzw. -ausprägungen ermöglichen eine gründlichere Beurteilung der jeweiligen Kern Risiko-Szenarien in Bezug auf die zu erwartenden Schadensausmasse und Eintrittswahrscheinlichkeiten. Der Schwerpunkt der Variantenbildung liegt jedoch aufgrund der höheren möglichen Auswirkungen auf den Attributen «grossflächig» und «schwerwiegend».

In Abbildung 2 stellen die Szenarien RS.08a und RS.08b Beispiele für die Bedrohungskategorie «Vorsätzliche Handlungen» dar, die u. a. das Ausspähen der Datenkommunikation, das Einschleusen von bösartiger Software (Malware) wie z. B. Trojanern und Viren, Datenmanipulationen, Sabotage (Zerstörung der Daten/Zerstörung der Infrastruktur), Missbrauch von Konten, Zutritts- und Zugriffsberechtigungen und (Distributed) Denial of Service[17] Angriffe umfassen können. Vorsätzliche Handlungen werden durch organisatorische Mängel, menschliche Fehlhandlungen und techni-

[17] Denial of Service (DoS) bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte. Wird die Überlastung von einer grösseren Anzahl anderer Systeme verursacht, so wird von Distributed Denial of Service (DDoS) gesprochen (Quelle: Wikipedia)

sches Versagen begünstigt und können sowohl «Angriffe vor Ort[18]» als auch «Angriffe aus der Ferne[19]» beinhalten.

Soweit sinnvoll umfassen die Varianten auch Szenarien, welche die Bedrohungskategorien «Höhere Gewalt», «Organisatorische Mängel», «Menschliche Fehlhandlungen» und «Technisches Versagen» beinhalten. Da «Organisatorische Mängel» und «Menschliche Fehlhandlungen» in der Realität erfahrungsgemäss sehr eng miteinander verknüpft sind (z. B. Fehlverhalten eines Administrators wegen unzureichender Schulung), wurden diese beiden Bedrohungskategorien jeweils in einer Variante zusammengefasst ausgewiesen (vgl. RS.08e).

Steckbrief «RS.08: Böswillige oder fehlerhafte Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern»	
Bemerkungen	• Der Fall «**Lastunterbrecher**» wird durch RS.08 behandelt
Annahmen	• Eine missbräuchliche oder fehlerhafte Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet nicht statt. • Die Stabilität des elektrischen Versorgungsnetzes kann durch eine grossflächige, böswillige oder fehlerhafte Deaktivierung/Beschränkung des Anschlusses von Prosumern gefährdet werden.
Szenario-varianten	• RS.08a: **Vereinzelte** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf **einzelne** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.08b: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf eine **Vielzahl** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.08c: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch höhere Gewalt**
	• RS.08d: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch technisches Versagen**
	• RS.08e: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem • Zähldatenverarbeitungssystem

Abbildung 2: Beispiel Steckbrief für RS.08

[18] Der sogenannte «Angriff **vor Ort**» setzt physischen Zugang zu den Systemkomponenten oder deren Schnittstellen voraus.

[19] Der sogenannte «Angriff **aus der Ferne**» erfolgt via Fernzugang zu den Systemkomponenten oder deren Schnittstellen

6) **Aufschlüsselung auf Ereigniskategorien**: Die Ermittlung vom Schutzbedarf erfolgt im Endeffekt durch die Abschätzung der schlimmsten möglichen Folgen des Verlustes von Vertraulichkeit, Integrität und Verfügbarkeit. Deshalb ist die Aufschlüsselung von Kern Risiko-Szenarien bzw. deren Varianten auf mögliche Verletzungen von Vertraulichkeit, Integrität und Verfügbarkeit gemäss der nachstehenden fünf Ereigniskategorien die Voraussetzung für eine transparente Beurteilung des Schutzbedarfs:
   - **Verlust von Vertraulichkeit von sensitiven Daten und Informationen**: Dies könnte z. B. durch die Entwendung der auf intelligenten Messgeräten verwalteten Messdaten zustande kommen.
   - **Verlust von Integrität von sensitiven Daten und Informationen**: Ein mögliches Ereignis dieser Kategorie wäre die Manipulation der Daten zur Tarifierung.
   - **Verlust von Verfügbarkeit von sensitiven Daten und Informationen**: Der Verlust von den auf intelligenten Messgeräten gespeicherten Daten würde in diese Kategorie fallen.
   - **Verlust von Integrität von IKT-Systemen und -Services**: Diese Ereigniskategorie umfasst mögliche Störungen an der Funktionsweise der IKT-Komponenten und -Services betreffend intelligente Messsysteme beim Endverbraucher.
   - **Verlust von Verfügbarkeit von IKT-Systemen und -Services**: Die möglichen Einbussen an der Funktionsfähigkeit und Nutzbarkeit von IKT-Komponenten und -Services für intelligente Messsysteme beim Endverbraucher werden in dieser Kategorie zusammengefasst.

7) **Aufschlüsselung auf Schadenskategorien**: Die Zuordnung zu den Schadenskategorien erlaubt eine übersichtliche und vor allem untereinander vergleichbare Beurteilung von Kern Risiko-Szenarien bzw. deren Varianten in Bezug auf die Bestimmung von schlimmsten denkbaren Konsequenzen eines möglichen Verlustes von Vertraulichkeit, Integrität und Verfügbarkeit. In dieser SBA kommen folgende sechs Schadenskategorien zum Einsatz:
   - **Reputationsverlust**: Diese Schadenskategorie umfasst die Schädigung des Rufs von Unternehmen, Organisationen oder Personen infolge negativer Auswirkungen der Vorfälle.
   - **Compliance-Verletzungen**: Die möglichen Verstösse gegen einschlägige Gesetze, Vorschriften und Verträge fallen unter diese Kategorie. Die Compliance-Verletzungen können über Gerichtsverfahren o. ä. zum finanziellen Verlust (z.B. aufgrund möglicher Nachbesserungen und Bussen) und Reputationsverlust führen. Die Compliance-Verletzungen umfassen u. a. auch Verletzungen der eichrechtlich gültigen Gesetze und Vorschriften sowie des Datenschutzgesetzes, die über eine Verletzung von Persönlichkeitsrechten nach Art. 12 DSG hinausgehen.
   - **Finanzieller Verlust**: Finanzielle Einbussen können als Resultat von Schäden an Objekten (z. B. Betriebsmitteln) und Personen entstehen. Die Folgen aus den übrigen Schadenskategorien wie z. B. aus Compliance-Verletzungen könnten grundsätzlich auch zu finanziellen Verlusten führen und daher monetär beziffert werden.
   - **Gefährdung von Leib und Leben**: Diese Kategorie betrifft die Personensicherheit und umfasst jegliche Schäden an Menschen, die durch direkte oder indirekte Einwirkung der elektrischen Energie verursacht werden könnten.
   - **Verletzung von Persönlichkeitsrechten**: Diese Kategorie betrifft die Verletzungen von Persönlichkeitsrechten nach *Art.12 DSG Persönlichkeitsverletzun-*

gen[20]*.* Dabei handelt es sich um einen Spezialfall von Compliance-Verletzungen.

- **Gefährdung überregionaler Versorgungssicherheit**: Diese Schadenskategorie erfasst die Beeinträchtigung oder den Ausfall der Versorgung mit elektrischer Energie für einen bedeutenden Teil der schweizerischen Bevölkerung und Wirtschaft. Ein überregionales Ereignis hat grossflächige Auswirkungen auf das lokale Verteilnetz (Netzebene 7), das regionale Verteilnetz (Netzebene 5), das überregionale Verteilnetz (Netzebene 3) und unter Umständen bis auf Stufe Übertragungsnetz (Netzebene 1) und erfasst somit Tausende von Endverbrauchern.

8) **Beurteilung Schadensausmass**: In diesem Arbeitsschritt wird für jedes Kern Risiko-Szenario bzw. dessen Varianten eruiert, was die Folgen im schlimmsten Fall für die im vorangehenden Schritt als relevant beurteilten Schadenskategorien sein könnten. Die Abschätzung der möglichen Schäden nach Schadenskategorien ermöglicht eine qualitative Bewertung der schlimmsten möglichen Auswirkungen aus den Risiko-Szenarien. Die Aufschlüsselung auf verschiedene Schadenskategorien im Schritt 7) sowie die Beurteilung von verschiedenen Auswirkungen erfolgen jeweils nach zwei unterschiedlichen Sichten („Sicht Prosumer“ und „Sicht Datenmanager“), da diese von den möglichen negativen Folgen eines aufgetretenen Risiko-Szenarios unmittelbar betroffen wären (direkte Risikoträger).

9) **Bewertung der Risiken**[21]: Anschliessend zur Beurteilung des Schadensausmasses werden die Risiken zu den Kern Risiko-Szenarien bzw. deren Varianten bewertet und in der Risikomatrix veranschaulicht (siehe Abbildung 3). Die Risikobewertung erfolgt wie im Arbeitsschritt 8) jeweils nach zwei unterschiedlichen Sichten: die des Prosumers und die des Datenmanagers.

   Der Wert eines Risikos (Risikowert) zu einem Szenario gibt an, in welcher Höhe ein Schaden im schlimmsten Fall (Worst Case) zu erwarten ist und mit welcher Eintrittswahrscheinlichkeit der vermutete Schaden auftreten könnte. Bei der Risikobewertung wird davon ausgegangen, dass die Mindest-Anforderungen mit direkter Sicherheitsrelevanz 4.1.3A, 4.1.3B und 4.1.3D (vgl. Ref. [1], Kap. 4) grundsätzlich umgesetzt sind und das intelligente Messsystem dadurch bereits minimal geschützt ist, jedoch dieser Schutz durch mögliche Lücken in der Sicherheitskonzeption des intelligenten Messsystems verwundbar sein könnte (vgl. Schwachstelle SS.12 aus Kapitel 4.2).

   Für die Bewertung des Risikos für ein bestimmtes Szenario wird zuerst das im Schritt 8) ermittelte Schadensausmass in eine passende Stufe der entsprechenden Bewertungsskala (Tabelle 1) eingeordnet. Zu diesem Zweck wird die monetäre Summe möglicher finanzieller Auswirkungen aus allen Schadenskategorien abgeschätzt. Nach der Quantifizierung des Schadensausmasses wird die Häufigkeit, mit der ein Schaden mit der zu erwartenden Höhe auftreten kann, mit Hilfe der entsprechenden Bewertungsskala (Tabelle 2) beurteilt. Da keine Erfahrungswerte für die Abschätzung der Eintrittswahrscheinlichkeiten in Bezug auf intelligente Messsysteme vorliegen, wurde auf Erfahrungen und Best-Practices aus anderen Bereichen der IKT zurückgegriffen.

   Der Risikowert für ein Szenario resultiert aus der Multiplikation der quantifizierten Werte bzw. der abgeleiteten Stufen betreffend Schadensausmass und Eintrittswahrscheinlichkeit:

   Risikowert = Stufe Schadensausmass * Stufe Eintrittswahrscheinlichkeit

[20] Gemäss Art.12 DSG, Punkt 3 liegt in der Regel keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat

[21] In dieser SBA erfolgte die Risikobewertung durch das Expertenteam AWK.

Die Risikomatrix und Bewertungsskalen, die in dieser SBA zum Einsatz kommen, wurden aus der Vorlage des Informatiksteuerungsorgans des Bundes für ISDS-Konzepte (siehe Ref. [12]) übernommen. Die Beurteilungskriterien für mögliche Auswirkungen wurden in der Skala des Schadensausmasses mit den sechs Schadenskategorien dieser SBA abgeglichen, damit sie auf die Bedürfnisse der vorliegenden SBA zugeschnitten sind.

Da die Risiken in dieser SBA aus Sicht des Prosumers und Datenmanagers bewertet werden, stellen die Risikomatrix und Bewertungsskalen aus Ref. [12] einen guten Kompromiss dar, um die Risikobewertung für ein breites Spektrum von Prosumern bzw. Datenmanagern mit unterschiedlicher organisatorischer und technischer Komplexität durchzuführen.

Für die Abschätzung des Schadensausmasses wurde eine vierstufige Skala mit Stufen von „Vernachlässigbar“ bis „Katastrophal“ verwendet. Die Beschreibung der möglichen Auswirkungen für die jeweiligen Stufen findet sich in der folgenden Tabelle.

Stufe	Bezeichnung	Beurteilungskriterien für mögliche Auswirkungen
1	**Vernachlässigbar**	**Reputationsverlust**: Kein Reputationsverlust **Compliance-Verletzungen**: Einhaltung gesetzlicher und vertraglicher Pflichten nicht gefährdet **Finanzieller Verlust**: Finanzieller Schaden kleiner als 10'000 CHF **Gefährdung von Leib und Leben**: Unfälle oder Krankheiten ohne Arbeitsabwesenheiten **Verletzung von Persönlichkeitsrechten**: Persönlichkeitsrechte nicht gefährdet **Gefährdung überregionaler Versorgungssicherheit**: Überregionale Versorgungssicherheit nicht gefährdet
2	**Marginal**	**Reputationsverlust**: Reputationsverlust klein und von kurzer Dauer (kein Fernsehen und höchstens Kurzmeldung in der Presse) **Compliance-Verletzungen**: Einhaltung gesetzlicher und vertraglicher Pflichten gefährdet oder Erfüllung wesentlicher Verpflichtungen beeinträchtigt **Finanzieller Verlust**: Finanzieller Schaden zwischen 10'000 und 200'000 CHF **Gefährdung von Leib und Leben**: Unfälle oder Krankheiten mit mehreren verlorenen Arbeitstagen aber ohne bleibende Schäden **Verletzung von Persönlichkeitsrechten**: Persönlichkeitsrechte marginal gefährdet **Gefährdung überregionaler Versorgungssicherheit**: Überregionale Versorgungssicherheit nicht gefährdet
3	**Kritisch**	**Reputationsverlust**: Merklicher Reputationsverlust (Artikel in Presse, aber nicht auf der Frontseite - kein Fernsehen) **Compliance-Verletzungen**: Einhaltung gesetzlicher und vertraglicher Pflichten bzw. Erfüllung wesentlicher Verpflichtungen stark eingeschränkt **Finanzieller Verlust**: Finanzieller Schaden zwischen 200'000 und 1‘000'000 CHF **Gefährdung von Leib und Leben**: Unfälle oder Krankheiten mit Hospitalisierung und bleibenden Schäden (Teil-Invalidität) **Verletzung von Persönlichkeitsrechten**: Persönlichkeitsrechte gefährdet **Gefährdung überregionaler Versorgungssicherheit**: Überregionale Versorgungssicherheit kaum gefährdet

Stufe	Bezeichnung	Beurteilungskriterien für mögliche Auswirkungen
4	**Katastrophal**	**Reputationsverlust**: Sehr hoher Reputationsverlust (Frontseite Meldung in Presse und Fernsehen) **Compliance-Verletzungen**: Einhaltung gesetzlicher und vertraglicher Pflichten bzw. Erfüllung wesentlicher Verpflichtungen verunmöglicht **Finanzieller Verlust**: Finanzieller Schaden grösser als 1'000'000 CHF **Gefährdung von Leib und Leben**: Leib und Leben sind gefährdet **Verletzung von Persönlichkeitsrechten**: Persönlichkeitsrechte in hohem Masse gefährdet **Gefährdung überregionaler Versorgungssicherheit**: Überregionale Versorgungssicherheit gefährdet

Tabelle 1: Bewertungsskala für Schadensausmass (Quelle: angepasst aus Ref. [12])

Die Skala für die Abschätzung der Eintrittswahrscheinlichkeiten umfasst fünf Stufen, von „Unwahrscheinlich“ bis „Häufig“. Dabei werden den Stufen die in der folgenden Tabelle aufgeführten Bedeutungen unterlegt.

Stufe	Bezeichnung	Beurteilungskriterien für Eintrittswahrscheinlichkeit
1	**Unwahrscheinlich**	Möglich aber eher unwahrscheinlich. Tritt sehr unwahrscheinlich im Lebenslauf eines Objektes ein. Mehr als alle 10 000 Tage (> 27 Jahre)
2	**Selten**	Tritt selten ein, aber man muss mit Eintritt rechnen. Unwahrscheinlich aber gut möglich im Lebenslauf eines Objektes. Alle 1000 bis 10 000 Tage (3 - 27 Jahre)
3	**Gelegentlich**	Tritt gelegentlich ein. Geschieht mehrmals im Lebenslauf eines Objektes. Alle 100 bis 1000 Tage (1/4 - 3 Jahre)
4	**Wahrscheinlich**	Kommt oft vor. Geschieht manchmal im Lebenslauf eines Objektes. Alle 10 bis 100 Tage
5	**Häufig**	Kommt laufend vor. Geschieht oft im Lebenslauf eines Objekts. Häufiger als alle 10 Tage

Tabelle 2: Bewertungsskala für Eintrittswahrscheinlichkeit (Quelle: Ref. [12])

Die eingesetzte Risikomatrix beinhaltet drei Risikokategorien:

- **Gering**: Diese Kategorie umfasst die Risikowerte zwischen 1 und 2 und wird in der Risikomatrix durch einen grünen Hintergrund dargestellt.
- **Mittel**: Die Risikowerte zwischen 3 und 6 gehören zur dieser Kategorie. Die entsprechenden Zellen werden in der Risikomatrix gelb hinterlegt.
- **Hoch**: Die Risikowerte zwischen 8 und 20 fallen in diese Kategorie. Die entsprechenden Zellen werden in der Risikomatrix rot hinterlegt.

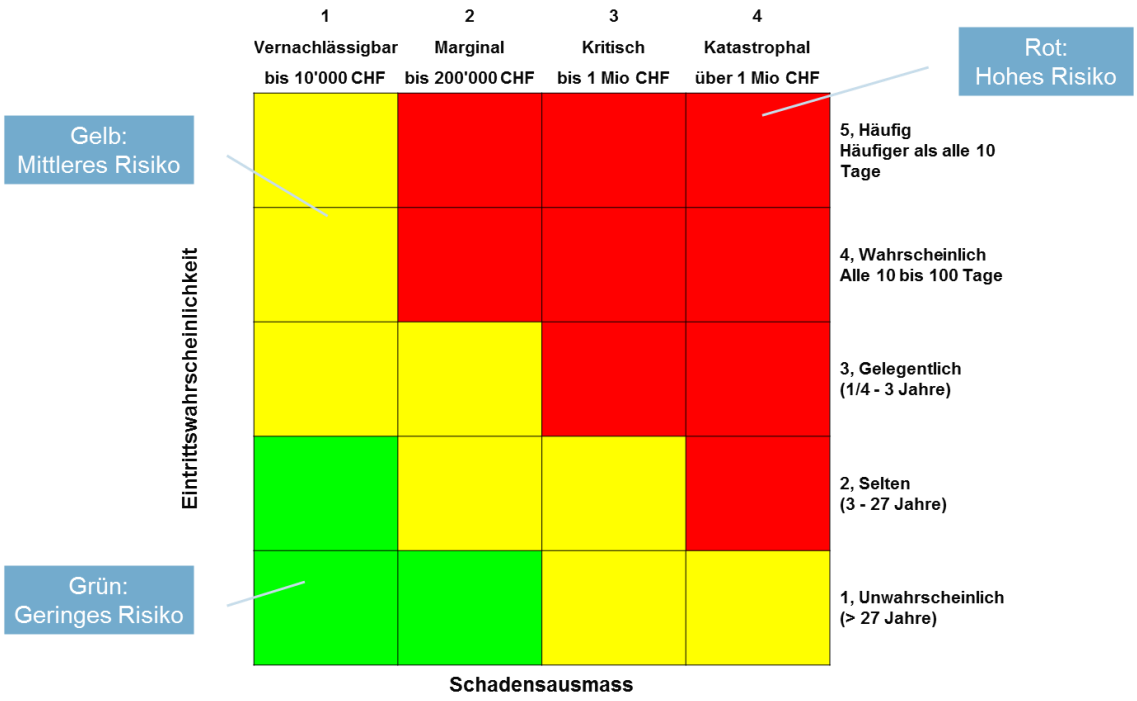


Abbildung 3: Risikomatrix (Quelle: Ref. [12])

10) **Beurteilung Schutzbedarf**: Für die Beurteilung des Schutzbedarfs werden die Resultate aus den Arbeitsschritten 8) und 9) beigezogen. Die Anlehnung an diese beiden Schritte ermöglicht eine qualitative Bewertung der schlimmsten möglichen Auswirkungen aus den Risiko-Szenarien. Die Beurteilung des Schutzbedarfs erfolgt auf Basis der folgenden sechs Fragen, die unter Berücksichtigung von verwendeten Schadens- und Risikokategorien ausgewählt wurden:

- Könnte die Einhaltung der eichrechtlich gültigen Vorschriften erheblich gefährdet werden?
- Könnte die Einhaltung der datenschutzrechtlichen Vorgaben erheblich gefährdet werden?
- Könnte Leib und Leben (Personensicherheit) gefährdet werden?
- Könnte die überregionale Versorgungssicherheit gefährdet werden?
- Wären schwerwiegende finanzielle Verluste durch die zu erwartenden Auswirkungen möglich?
- Wurden hohe Risiken identifiziert?

Im Gegensatz zur Schadensausmassbeurteilung und Risikobewertung (vgl. Arbeitsschritte 8) und 9)) erfolgt die Beurteilung vom Schutzbedarf durch eine kombinierte Sicht vom Prosumer und Datenmanager, damit eine ganzheitliche Bilanz über alle Risiko-Szenarien erzielt werden kann.

Die Schutzbedarfsbeurteilung erfolgt auf Basis der vier Komponenten des intelligenten Messsystems: Intelligentes Messgerät, Kommunikationssystem, Zähldatenverarbeitungssystem und Online-Visualisierungsplattform (vgl. Kapitel 3.3). Bei der Beurteilung wird zwischen den folgenden Schutzbedarfskategorien unterschieden:

- **Gering**: Eine Komponente oder Komponentengruppe hat geringen Schutzbedarf, falls keine der Fragen im Zusammenhang mit dieser Komponente oder Komponentengruppe eindeutig mit „Ja“ beantwortet werden kann.

- **Mittel**: Eine Komponente oder Komponentengruppe hat mittleren Schutzbedarf, falls mindestens eine der folgenden Kriterien im Zusammenhang mit dieser Komponente oder Komponentengruppe erfüllt wird:
  - die Einhaltung der eichrechtlich gültigen Vorschriften oder der datenschutzrechtlichen Vorgaben könnte erheblich gefährdet werden
  - schwerwiegende finanzielle Verluste durch die zu erwartenden Auswirkungen wären möglich
  - hohe Risiken wurden identifiziert
- **Hoch**: Eine Komponente oder Komponentengruppe hat hohen Schutzbedarf, falls mindestens Leib und Leben oder die überregionale Versorgungssicherheit gefährdet werden könnte und hohe Risiken im Zusammenhang mit dieser Komponente oder Komponentengruppe identifiziert wurden. Alleine die Existenz von hohen Risiken führt nicht direkt zu einem hohen Schutzbedarf, womit die Abhängigkeit zu den verwendeten Risikobewertungsgrundlagen reduziert werden kann.

11) **Sicherheitsmassnahmen zur Risikobewältigung**: Die Identifikation und Kategorisierung geeigneter Massnahmen zur Minderung der entdeckten Risiken erfolgte in diesem Arbeitsschritt. Damit eine umfangreiche Massnahmendefinition erreicht werden konnte, wurden unterschiedliche, bestehende Anforderungs- und Massnahmenkataloge konsultiert.

3. Systemanalyse des intelligenten Messsystems

3.1. Mögliche Architekturvarianten intelligenter Messsysteme

Zwecks Grundlagenbildung für die Systemanalyse und Konkretisierung der zu analysierenden Architektur wurden in einem ersten Schritt die möglichen Architekturvarianten für intelligente Messsysteme analysiert. Die Resultate haben gezeigt, dass alle in den Referenzen [3], [4], [5], [6], [7] und [8] untersuchten Systemkonzepte grundsätzlich auf folgende zwei Architekturvarianten abgebildet werden können:

Smart Meter als Master: In dieser Variante dient das intelligente Messgerät beim Endverbraucher gleichzeitig als zentrale Kommunikationseinheit und besitzt die entsprechenden Kommunikationseinheiten und -schnittstellen für einen direkten Anschluss an verschiedene Kommunikationsnetze:

- LMN (Local Metrological Network): Über das LMN (KS1 in Abbildung 4) können die Messgeräte gleicher und anderer Energiesparten (Strom, Gas, Wasser, Wärme) mit dem intelligenten Messgerät verbunden werden.
- HAN (Home Area Network): Das HAN (KS2 in Abbildung 4) dient zur Nahverkehrskommunikation des intelligenten Messgeräts mit Anlagen und Geräten beim Endverbraucher wie z.B. Kundeninformations- und Gebäudeautomationssystemen.
- WAN (Wide Area Network): Die Weitverkehrskommunikation mit einem sogenannten Zähldatenverarbeitungssystem u. a. zur Verwaltung intelligenter Messgeräte erfolgt über das WAN (KS3 in Abbildung 4).

Das intelligente Messgerät verfügt ausserdem über eine lokale Schnittstelle zu Administrations-, Wartungs- und Supportzwecken (KS0 in Abbildung 4).

Smart Meter Gateway: Das sogenannte Smart Meter Gateway ist in diesem Fall eine zentrale, vom intelligenten Messgerät getrennte Kommunikationseinheit und regelt mit seinen Kommunikationseinheiten und -schnittstellen die Kommunikation betreffend Messgeräte unterschiedlicher Energiearten (Strom, Gas, Wärme, Wasser) über LMN, HAN und WAN (vgl. KS1, KS2, KS3 in Abbildung 5).

Das Smart Meter Gateway besitzt eine zusätzliche lokale Schnittstelle für Administration, Wartung und Support (KS0 in Abbildung 5).

In der vorliegenden Studie wird von einer bidirektionalen Datenübertragung zwischen dem intelligenten Messgerät und Gateway ausgegangen und die Abbildung 5 wurde daher mit einem bidirektionalen, roten Pfeil entsprechend ergänzt.

Es kann nicht ausgeschlossen werden, dass ein Smart Meter Gateway zusammen mit einem intelligenten Messgerät unter der Variante «Smart Meter als Master» vereinigt werden kann. Massgebend ist jeweils die konkrete Realisierung. Deshalb ist keine scharfe Abgrenzung zwischen den beiden Architekturvarianten möglich.

Zur Gewährleistung einer möglichst breiten Anwendbarkeit der Ergebnisse werden beide Varianten in dieser Studie berücksichtigt.

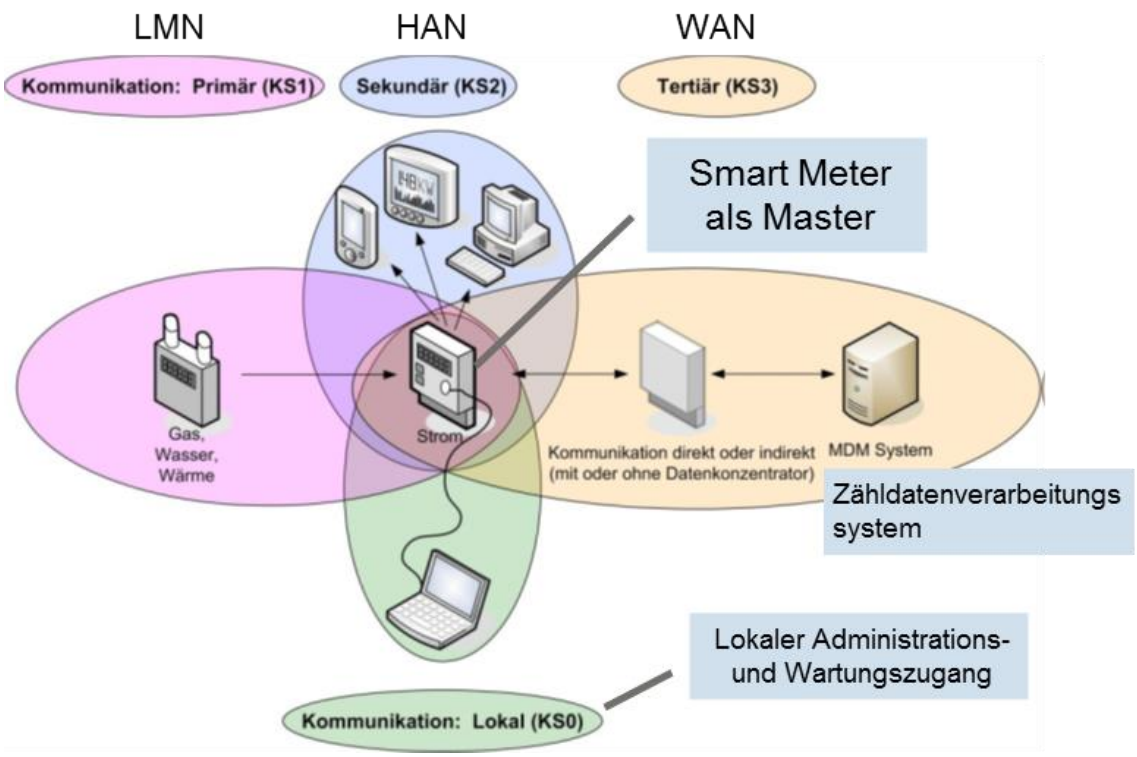


Abbildung 4: Smart Meter als Master (Quelle: Ref. [3])

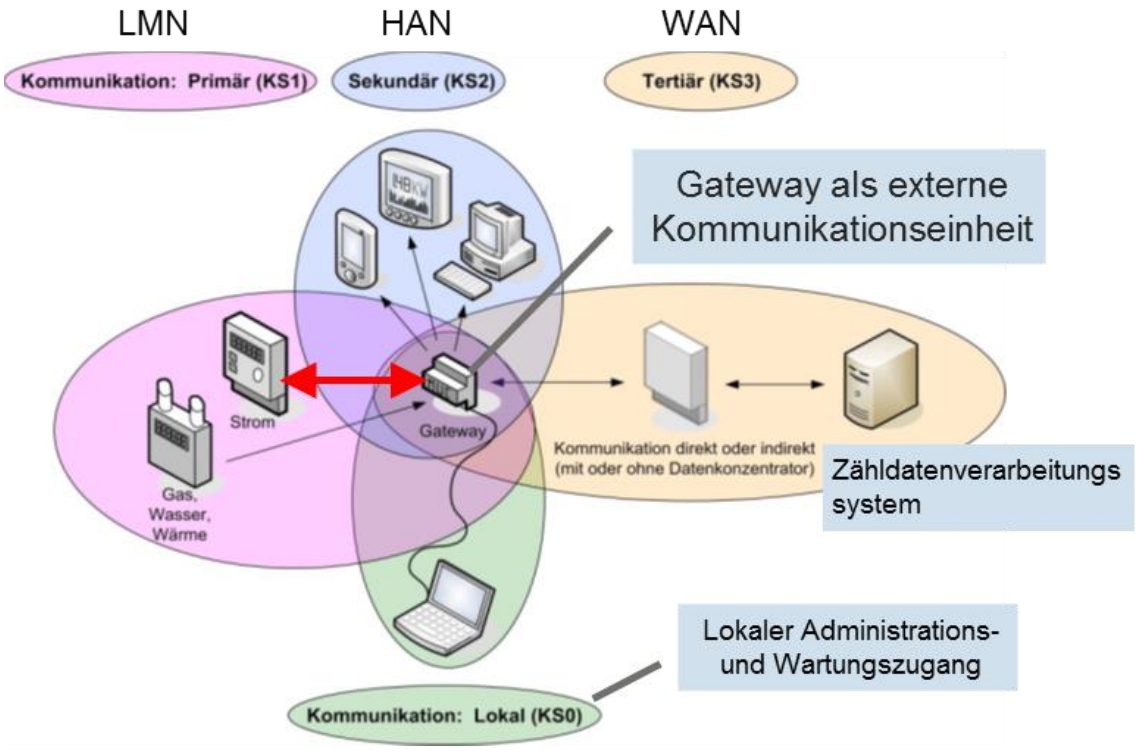


Abbildung 5: Smart Meter Gateway (Quelle: angepasst aus Ref. [3])

3.2. Use Cases für intelligente Messsysteme

3.2.1. Identifikation von relevanten Use Cases für intelligente Messsysteme

In Bezug auf intelligente Messsysteme wurden folgende Anwendungsfälle – sogenannte Use Cases – aus Ref. [2] identifiziert:

- UC1 - Datenmanagement
- UC2 - Demand Side Response
- UC3 - Gebäudeautomatisierung
- UC4 - Systemdienstleistungen
- UC5 - Regionale Flexibilitäten
- UC7 - Fehlererkennung und Netzrekonfiguration
- UC8 - Steuerung Wirk- und Blindleistung
- UC9 - Instandhaltung
- UC12 - Zeitliche Flexibilisierung Ein-/Ausspeisung

Die oben genannten neun Use Cases sind relevant für die vorliegende SBA, da sie die Umsetzung der Funktionalitäten bei intelligenten Messsystemen betreffen. Durch die Detailbetrachtung dieser Use Cases lässt sich eine Gesamtübersicht zu den wesentlichen Daten und Datenflüssen betreffend intelligente Messsysteme zusammenstellen.

Die relevanten Use Cases sind unabhängig von Architekturvarianten und können theoretisch beide Varianten aus Kapitel 3.1 bzw. «Smart Meter als Master» und «Smart Meter Gateway» umfassen.

Supportprozesse, wie z. B. die Installation der intelligenten Messgeräte, sind durch den UC1 – Datenmanagement und den UC 9 – Instandhaltung abgedeckt und auch in den Schutzobjekten enthalten (siehe Kapitel 4.1, SO.02 «Organisatorische Prozesse und Abläufe»).

Die als relevant identifizierten Use Cases wurden in Bezug auf das intelligente Messsystem abgegrenzt und, sofern nötig, angepasst (vgl. Anhang A.4). Bei der Anpassung und Abgrenzung der Use Cases wurde von der Annahme ausgegangen, dass die Daten vom/zum Prosumer im Zusammenhang mit dem intelligenten Messsystem generell durch den Datenmanager verwaltet, aufbereitet und gespeichert sowie den jeweiligen Empfängern weitergeleitet werden. Die an Use Cases vorgenommenen Anpassungen und Abgrenzungen sind lediglich schematischer Art, um die Datenflüsse zum/vom Prosumer in Bezug auf das intelligente Messsystem besser im Überblick zu behalten und haben keinen Einfluss auf die Anzahl technischer Schnittstellen und den Schutzbedarf des intelligenten Messsystems.

3.2.2. Zuordnung von Mindestanforderungen auf Use Cases

Um die Relevanz von möglichen Mindestanforderungen aus Ref. [1] für die vorliegenden SBA zu verifizieren, wurde eine Zuordnung von Mindestanforderungen aus Ref. [1] auf die für diese SBA relevanten Use Cases erstellt (vgl. Abbildung 6).

Diese Zuordnung zeigt, dass die Mehrheit der Mindestanforderungen aus Ref. [1] für die Gewährleistung der Funktionalitäten aus den relevanten Use Cases zwingend erforderlich ist.

Die als optional erachteten Mindestanforderungen mit direkter Sicherheitsrelevanz bzw. 4.1.3A «Sichere Verbindungen», 4.1.3B «Datenschutzgerechte Speicherung» und 4.1.3D «Detektion und Verhinderung Missbrauch» wurden in der Tabelle gesondert in orange ausgewiesen, da sie einen unmittelbaren Einfluss auf den Schutz des intelligenten Messsystems haben.

In Folge dieser Zuordnung wurden alle Mindestanforderungen aus Ref. [1] mit Ausnahme von 4.1.3C «Recht auf Ausnahmen», 4.1.4A «Lebensdauer» und 4.1.4B «Eigenstromverbrauch» in dieser SBA berücksichtigt. Bei den ausgeschlossenen drei Mindestanforderungen handelt es sich um mögliche, nicht-technische Mindestanforderungen.

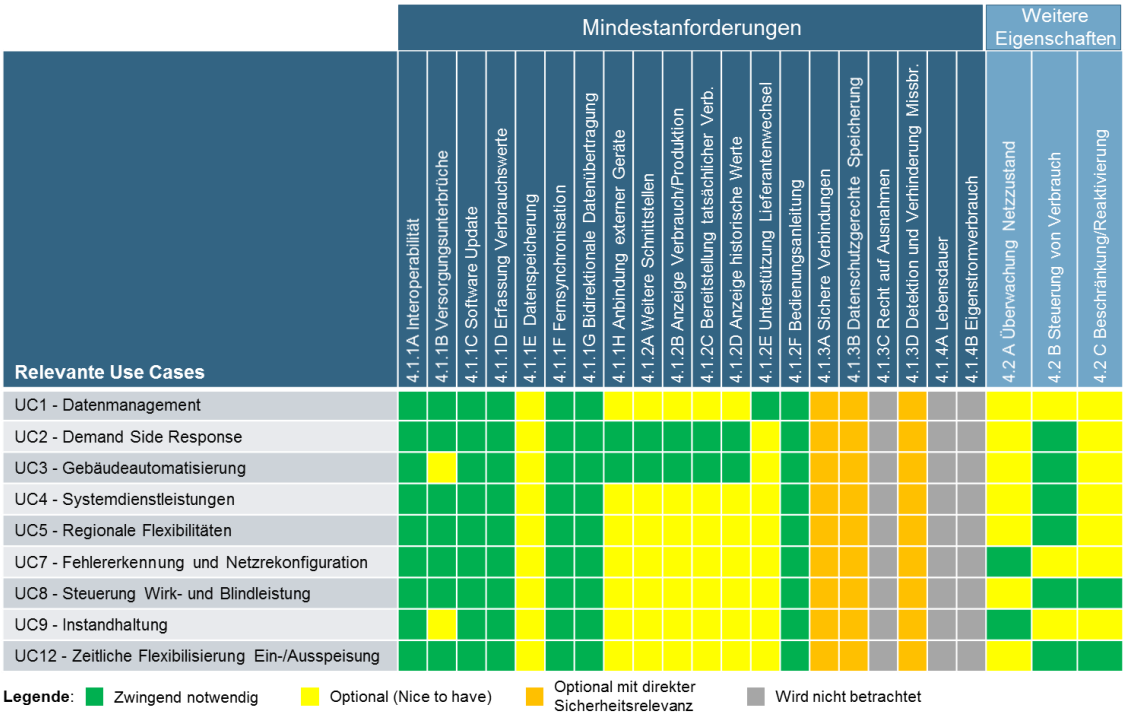


Abbildung 6: Verifikation möglicher Mindestanforderungen im Kontext von relevanten Use Cases

3.3. Das konzeptionelle Modell des intelligenten Messsystems

Aufgrund der zahlreichen technischen Realisierungsmöglichkeiten für intelligente Messsysteme beim Endverbraucher wird in der vorliegenden SBA von einer technologieneutralen Systembetrachtung ausgegangen. Für Systemkomponenten stehen daher die Funktionalitäten im Vordergrund. Die entsprechenden technischen Details werden nicht beachtet.

Der hier verfolgte Ansatz umfasst ein *konzeptionelles*, intelligentes Messsystem beim Endverbraucher, gemäss Ref. [1], Kapitel 2. So kann ein angemessen hoher Abstraktionsgrad erreicht werden, der eine Adaption auf reale Umsetzungsvorhaben erlaubt.

Das konzeptionelle, intelligente Messsystem besteht aus folgenden Komponenten (vgl. Abbildung 7):

- Intelligentes Messgerät (Smart Meter):
  - dient primär zum Gewinnen von Messwerten des Elektrizitätsverbrauchs und der Elektrizitätsproduktion
  - verfügt über eine Wide Area Network (WAN)-Schnittstelle, die es ihm ermöglicht, eine bidirektionale Kommunikation mit einem zentralen Verwaltungssystem (Zähldatenverarbeitungssystem) aufzubauen. Diese Schnittstelle kann physisch im Gehäuse des intelligenten Messgeräts selbst integriert sein. Lösungen, in denen diese Schnittstelle ausserhalb des Gehäuses des eigentlichen Messgerätes angebracht ist, werden als sogenannte Gateway-Lösungen bezeichnet (vgl. Kapitel 3.1, Smart Meter Gateway).
  - umfasst auch das lokale metrologische Netzwerk (LMN). Über das LMN werden Messgeräte anderer Medien des Endverbrauchers wie z. B. Gas, Wasser, Wärme mit dem intelligenten Messgerät (Smart Meter als Master) oder Smart Meter Gateway verbunden (vgl. Abbildung 4 und Abbildung 5). Das LMN wird über das intelligente Messgerät (Smart Meter als Master) bzw. Smart Meter Gateway gegenüber anderen Systemen wie z.B. dem Kommunikationssystem abgetrennt.
  - kann über eine Home Area Network (HAN)-Schnittstelle verfügen, die für allfällige Kundenapplikationen verwendet werden kann.
- Kommunikationssystem:
  - stellt die kommunikationstechnische Verbindung von intelligenten Messgeräten zu einem zentralen Zähldatenverarbeitungssystem her
  - kann dabei unterschiedliche Informationsübertragungstechnologien und weitere Einrichtungen zur Datenübertragung und -verarbeitung verwenden, z. B. Datenkonzentratoren
  - kann über eine zusätzliche, entsprechend geartete Schnittstelle unabhängig vom LMN noch mit weiteren Geräten verbunden werden. Dazu zählen insbesondere weitere intelligente Messgeräte und Mengenmessgeräte anderer Energieträger
- Zähldatenverarbeitungssystem:
  - bezeichnet ein zentrales System beim Betreiber des intelligenten Messsystems
    - zur Verwaltung der intelligenten Messgeräte
    - zur Auslesung von Messdaten aus den intelligenten Messgeräten
    - zur Bearbeitung der von den Messgeräten aufgenommen Daten wie z. B. Geräteparametrierung, Geräteverwaltung oder Zeitreihenverwaltung
    - zum Messsystembetrieb

- ist mit dem Kommunikationssystem und über dieses mit den intelligenten Messgeräten verbunden
- kann zur Validierung und Verarbeitung der aufgenommenen Daten eingesetzt werden
- beinhaltet Schnittstellen zu weiteren Applikationen des Energiedatenmanagements sowie zu anderen Applikationen wie z. B. dem Abrechnungs- und Prognosesystem
- entspricht der „Applikation DM“ in den Use Cases (vgl. Anhang A.4)

- Visualisierungsplattform:
  - kann z. B. Internetportale, Bildschirme im Haushalt oder Visualisierungen auf Geräten wie Mobiltelefonen oder Fernsehern umfassen
  - kann, aber muss sich nicht zwingend, auf dem Messgerät selbst befinden, ist jedoch von einer einfachen Statusanzeige zur Verbrauchsdarstellung auf dem Messgerät zu unterscheiden
  - gilt in der vorliegenden Studie als Online-Dienst (z.B. Internet Portal) ausserhalb der Endverbraucherumgebung, da dies aufgrund der zusätzlichen Schnittstelle zwischen der Visualisierungsplattform und dem Zähldatenverarbeitungssystem als anspruchsvollere Variante beurteilt wurde. Es wird angenommen, dass der Datenmanager die Verantwortung für den Betrieb und Sicherheit der Visualisierungsplattform trägt und die darauf bewirtschafteten Daten über das Zähldatenverarbeitungssystem geliefert werden. Nachfolgend wird von einer „Online-Visualisierungsplattform (OVP)“ gesprochen.

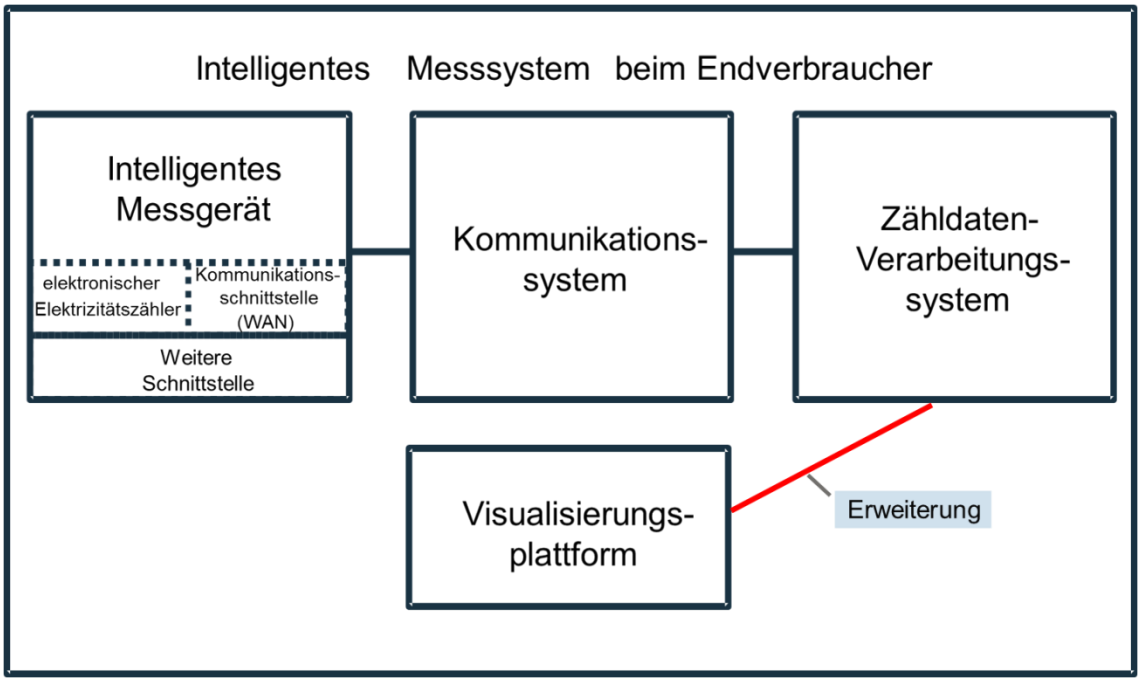


Abbildung 7: Komponenten des intelligentes Messsystems beim Endverbraucher (Quelle: angepasst aus Ref. [1])

3.4. Systemabgrenzung betreffend intelligentes Messsystem

Zwecks besserer Konkretisierung des Umfangs der vorliegenden SBA werden nachfolgend die Aspekte präzisiert, die durch das abstrakte, intelligente Messsystem gemäss Kapitel 3.3 abgedeckt resp. ausgegrenzt werden.

Der Fokus der vorliegenden Studie liegt auf Datensicherheit[22]. Die Schwachstellen, Bedrohungen und Risiken, die durch den Einsatz von Informations- und Kommunikationstechnologien (IKT) bei intelligenten Messsystemen entstehen können, befinden sich im Umfang dieser SBA.

Die technische Kommunikation des intelligenten Messsystems zu Mengenmessgeräten anderer Energieträger (z.B. Gas- und Warmwasserzählern) findet über das LMN statt. Das LMN wird als Bestandteil des intelligenten Messsystems angesehen und gehört explizit zum intelligenten Messgerät. Damit entspricht der Schutzbedarf des LMN dem Schutzbedarf des intelligenten Messgerätes.

Alle technischen Schnittstellen des intelligenten Messsystems befinden sich im Umfang der vorliegenden SBA.

Da das LMN und das HAN sich in der Nahumgebung des Prosumers befinden, werden sie einfachheitshalber unter LAN (Local Area Network) zusammengefasst.

In der vorliegenden SBA werden unter dem Begriff «Datenmanager» die Rollen «Messstellenbetreiber» und «Messdienstleister» subsumiert. Der Messstellenbetreiber ist in der Regel für die Supportprozesse wie z. B. den Einbau und Betrieb sowie die Eichung und Wartung der Messeinrichtung (intelligentes Messgerät) verantwortlich. Der Messdienstleister übernimmt üblicherweise das Ab- und Auslesen der Messeinrichtung, sowie andere Leistungen für den Endverbraucher wie z. B. Weiterbearbeitung der Daten, Abrechnung, Kundenbetreuung oder -beratung[23]. Der Verteilnetzbetreiber ist heute für die Erbringung des Messwesens (Messstellenbetrieb und Messdienstleistung) verantwortlich. Er kann das Messwesen selber erbringen oder die entsprechenden Aufgaben an Dritte auslagern[24].

Der Datenmanager kann die betrieblichen und sicherheitsbezogenen Dienstleistungen für das intelligente Messsystem bzw. dessen vier Komponenten «Intelligentes Messgerät», «Kommunikationssystem», «Zähldatenverarbeitungssystem» und «Online-Visualisierungsplattform» selbst übernehmen oder teilweise oder vollständig an Dritte auslagern. Ausserdem würde eine allfällige zukünftige Liberalisierung des Messwesens[25] den Prosumern ggf. die Möglichkeit bieten, Drittanbieter für die Erbringung von Messdienstleistungen bzw. Messstellenbetrieb auszuwählen und zu beauftragen. Unabhängig davon, welcher Marktakteur diese Rolle in Wirklichkeit übernimmt – Verteilnetzbetreiber oder Dritte – ist der Datenmanager in dieser SBA der Risikoträger für das intelligente Messsystem und hat die Risikoverantwortung in diesem Zusammenhang in letzter Instanz.

---

[22] In dieser SBA wird „Datensicherheit“ synonym zu „IKT-Sicherheit“ verwendet. IKT-Sicherheit umfasst die Sicherheitskonzepte und -Massnahmen zum Schutz der sensitiven Daten und Informationen in jeglicher Form sowie der IKT-Systeme in Bezug auf intelligente Messsysteme.

[23] Siehe „Metering Code Schweiz“ des VSE vom Mai 2016. Metering Code Schweiz erwähnt explizit den «Netzbetreiber», jedoch die Begriffe «Datenmanager», «Messstellenbetreiber» und «Messdienstleister» kommen darin nicht vor.

[24] Siehe Art. 8 Abs. 1 und 2 Strom VV (SR 734.71)

[25] Durch die Liberalisierung wäre der Prosumer in der Lage, den Messdienstleister bzw. den Messstellenbetreiber selber auszuwählen. Aus heutiger Sicht ist es noch offen, ob es zu einer vollständigen Liberalisierung kommt. Siehe auch „Kosten-Wirksamkeits-Analyse von Organisationsmodellen des Messwesens in Stromverteilnetzen in der Schweiz“ (http://www.bfe.admin.ch/php/modules/publikationen/stream.php?extlang=de&name=de_243970106.pdf)

Nicht in der SBA behandelt werden

- Messgeräte für andere Energieträger als Strom (Gas, Wasser, Wärme)
- Netze und Systeme, die nicht zum in Kapitel 3.3 definierten Umfang gehören. Zu diesen Netzen und Systemen gehören z.B. HAN und WAN. Die technischen Schnittstellen des intelligenten Messsystems zu/aus diesen Netzen und -systemen sind jedoch im Umfang der SBA enthalten.
- Abrechnungssysteme und weitere nachgelagerte Systeme
- Erarbeitung von Sicherheitsanforderungen und -massnahmen an nachgelagerte Systeme
- Entwicklung von Architekturmodellen oder -Varianten zu intelligenten Messsystemen
- Analyse von konkreten Realisierungen bezüglich intelligenter Messsysteme
- Evaluation von Produkten und Diensten in Bezug auf intelligente Messsysteme

4. Schutzobjekte, Schwachstellen und Bedrohungen des intelligenten Messsystems

4.1. Identifikation von Schutzobjekten betreffend intelligentes Messsystem

Das intelligente Messsystem bzw. dessen vier Komponenten «Intelligentes Messgerät», «Kommunikationssystem», «Zähldatenverarbeitungssystem» und «Online-Visualisierungsplattform» stellen übergeordnete Schutzobjekte dar und setzen sich aus sogenannten untergeordneten Schutzobjekten zusammen (vgl. Tabelle 1). Die untergeordneten Schutzobjekte ermöglichen eine bessere Konkretisierung von übergeordneten Schutzobjekten und umfassen beispielsweise die entsprechenden Daten und Informationen sowie die Hard- und Softwarekomponenten.

Ref.	Untergeordnete Schutzobjekte	Beschreibung
SO.01	Daten und Informationen	System-, netz-, produktions-, oder verbrauchsrelevante Daten, die u.U. personenbezogene Daten nach DSG umfassen
SO.02	Organisatorische Prozesse und Abläufe	Geschäftsprozesse sowie Betriebs-, Administrations-, Wartungs- und Support-Prozesse betreffend intelligentes Messsystem
SO.03	Technische Prozesse und Abläufe	Prozesse und Abläufe technischer Natur wie z. B. Authentifizierung, Autorisierung, Verschlüsselung etc.
SO.04	Kommunikationsnetze[26], - Schnittstellen - Verbindungen	Kabellose und kabelgebundene Kommunikationsnetze und -Schnittstellen inkl. Admin- und Wartungszugänge sowie alle technischen Kommunikationsverbindungen und -sessionen
SO.05	IKT-Komponenten (Hard- und Software)	Alle Hard- und Softwarekomponenten, die zum intelligenten Messsystem gehören oder durch dieses bereitgestellt werden
SO.06	IKT-Services	IKT-Services betreffend intelligentes Messsystem wie z.B. Funktionalitäten/Dienste Zähldatenverarbeitungssystem, Funktionalitäten/Dienste Online-Visualisierungsplattform etc. inkl. der entsprechenden Benutzer und Administratoren
SO.07	Nicht IKT-Infrastruktur	Strom, Kühlung, Räume, Gebäude etc.
SO.08	Personen	Betrifft das Personal für Betrieb, Administration, Wartung und Support des intelligenten Messsystems sowie den Prosumer

Tabelle 3: Schutzobjektgruppen für das intelligente Messsystem

Das im Rahmen dieser SBA verfolgte Abstraktionsniveau erlaubt nur eine beschränkte, nicht abschliessende Beschreibung der untergeordneten Schutzobjekte. Gestützt auf Ref. [2], Kapitel 7 war jedoch eine weitere Detaillierung des Schutzobjekts SO.01 «Daten und Informationen» möglich. Die daraus identifizierten Daten und Informationen betreffend intelligentes Messsystem wurden zu Wiederverwendungszwecken im Anhang A.2 in zusammengefasster Form ausgewiesen und in Bezug auf Ihrer Relevanz bezüglich Datenschutz und Versorgungssicherheit beurteilt.

4.2. Identifikation von Schwachstellen betreffend intelligentes Messsystem

Dieses Kapitel weist die möglichen Schwachstellen für das intelligente Messsystem gemäss Kapitel 3.3 aus. Die Schwachstellen wurden im Rahmen dieser SBA primär aus Ref. [1] hergeleitet, unter der Voraussetzung, dass das betrachtete, konzeptionelle intelli-

[26] Die Fremdnetze wie HAN und WAN sind nicht im Umfang enthalten, jedoch die Schnittstellen des intelligenten Messsystems zu diesen Netzen. Das LMN wird als Bestandteil des intelligenten Systems angesehen und gehört ebenfalls zum Umfang. Alle technischen Schnittstellen des intelligenten Messgeräts befinden sich auch im Umfang der vorliegenden SBA.

gente Messsystem technische Merkmale und Eigenschaften beinhaltet, die aus einer möglichen Umsetzung der Mindestanforderungen aus Ref. [1] mit Ausnahme von 4.1.3C (Recht auf Ausnahmen), 4.1.4A (Lebensdauer) und 4.1.4B (Eigenstromverbrauch) resultieren würden. Eine lückenhafte Implementierung dieser technischen Merkmale und Eigenschaften oder fehlerhafter Umgang mit den gleichen können zu Verwundbarkeiten oder möglichen Angriffspunkten führen und so eine Einwirkung von Bedrohungen zulassen. Die Schwachstellen dienen zusammen mit dem Bedrohungskatalog aus Kapitel 4.3 als Basis für die Bildung von «Kern Risiko-Szenarien» gemäss Kapitel 5. Eine Zuordnung von Schwachstellen auf «Kern Risiko-Szenarien» befindet sich im Anhang A.3.

Ref.	Schwachstelle	Zugrundeliegende Mindestanforderung aus Ref. [1]
SS.01	Verwaltung von intelligenten Messgeräten aus der Ferne: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption könnte ein Angreifer dadurch die Kontrolle von intelligenten Messgeräten übernehmen und so diese Geräte beliebig manipulieren.	4.1.1A «Interoperabilität»
SS.02	Automatische Anmeldung/Inbetriebnahme von intelligenten Messgeräten innerhalb des intelligenten Messsystems: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption könnte dies einem Angreifer ermöglichen, manipulierte intelligente Messgeräte unbemerkt in das intelligente Messsystem zu integrieren.	4.1.1A «Interoperabilität»
SS.03	Aktualisierung der Software von intelligenten Messgeräten aus der Ferne: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption wäre das mutwillige oder unabsichtliche Einspielen von fehlerhaften Software-Updates möglich, was die betroffenen intelligenten Messgeräte u. U. betriebsunfähig machen könnte.	4.1.1C «Software Update»
SS.04	Synchronisation des internen Kalenders und der Uhr des intelligenten Messgerätes aus der Ferne: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption wäre ein Angreifer dadurch in der Lage, die Systemzeit und die damit verbundenen Funktionalitäten und Prozesse wie z.B. Tarifierung zu manipulieren.	4.1.1F «Fernsynchronisation»
SS.05	Bidirektionaler Datenaustausch zwischen dem Zähldatenverarbeitungssystem und intelligenten Messgerät: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption kann dies u.U. die Sicherheit des intelligenten Messsystems z. B. durch das Einspielen von fehlerhaften oder manipulierten Software-Updates auf das intelligente Messgerät (vgl. SS.03) gefährden	4.1.1G «Bidirektionale Datenübertragung»
SS.06	Auslesen von gespeicherten oder in Pseudo-Echtzeit aufgenommenen Informationen von einzelnen intelligenten Messgeräten aus der Ferne: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption könnte beim Missbrauch z. B. im Sinne eines DDoS-Angriffs die Verfügbarkeit des intelligenten Messsystems gefährdet werden. Zusätzlich erlaubt das Auslesen von gespeicherten Informationen oder augenblicklich aufgenommenen Informationen die Erstellung von detaillierten Last- und Erzeugungsprofilen von Prosumern.	4.1.1G «Bidirektionale Datenübertragung»
SS.07	Anbindung externer Geräte (z.B. Mengenmessgeräte anderer Energieträger) in das intelligente Messsystem und weitere offene, standardisierte Schnittstellen: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption könnten die weiteren technischen Schnittstellen Möglichkeiten bieten, das intelligente Messsystem anzugreifen.	4.1.1H «Anbindung externer Geräte» 4.1.2A «Weitere Schnittstellen»

Ref.	Schwachstelle	Zugrundeliegende Mindestanforderung aus Ref. [1]
SS.08	Erfassung von netztechnischen Parametern zur Überwachung und zur Steuerung des Netzes durch das intelligente Messsystem: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption könnte z. B. durch die Manipulation von erfassten netztechnischen Parametern oder des intelligenten Messsystems u. U. die Stabilität des Netzes bzw. die Versorgungssicherheit gefährdet werden.	4.2A «Überwachung Netzzustand»
SS.09	Identifikation, Gruppierung und Steuerung von dezentralen Verbrauchs- und Erzeugungseinheiten aus der Ferne: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption könnte bei einer grossflächigen, missbräuchlichen Ein- und Ausschaltung von Verbrauchs- und Erzeugungseinheiten die Netzstabilität sowie die Personensicherheit (z.B. Verkehr wird aufgrund eines Stromausfalls nicht mehr geregelt) gefährdet werden.	4.2B «Steuerung von Verbrauch und Einspeisung»
SS.10	Aktivierung / Deaktivierung eines Anschlusses oder Begrenzung des maximalen Leistungsbezuges bzw. Abtransportes eines Prosumers aus der Ferne über das intelligente Messsystem: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption könnte bei einer grossflächigen, missbräuchlichen Aktivierung / Deaktivierung von Prosumer-Anschlüssen die Netzstabilität sowie die Personensicherheit (z.B. Verkehr wird aufgrund eines Stromausfalls nicht mehr geregelt) gefährdet werden.	4.2C «Beschränkung eines Anschlusses»
SS.11	Erzeugung, Aufbereitung, Speicherung, Verwaltung und Bereitstellung von system-, netz-, produktions- oder verbrauchsrelevanten Daten durch das intelligente Messsystem, die u.U. personenbezogene Daten nach DSG umfassen: Im Zusammenhang mit einer mangelhaften Sicherheitskonzeption könnte ein Angreifer dadurch in der Lage sein, z. B. detaillierte Persönlichkeitsprofile abzuleiten oder Vorbereitungen für Angriffe auf die Versorgungssicherheit vorzunehmen.	4.1.2B «Anzeige Verbrauch/Produktion» 4.1.2C «Bereitstellung tatsächlicher Verb.» 4.1.2D «Anzeige historische Werte» .
SS.12	Inadäquate Umsetzung von Sicherheitsanforderungen: Bei den Mindestanforderungen mit direkter Sicherheitsrelevanz (4.1.3A, 4.1.3B und 4.1.3D) geht man davon aus, dass diese nicht einheitlich und konsequent umgesetzt werden und daraus Sicherheitslücken entstehen.	4.1.3A «Sichere Verbindungen» 4.1.3B «Datenschutzgerechte Speicherung» 4.1.3D «Detektion und Verhinderung Missbr.»
SS.13	Manipulation Messtechnik: Der geeichte, messtechnische Teil des intelligenten Messgerätes ist durch den Einsatz von IKT beim intelligenten Messsystem z. B. durch Reprogrammierung manipulierbar.	Nicht anwendbar

Tabelle 4: Mögliche Schwachstellen für das intelligente Messsystem gemäss Kapitel 3.3

4.3. Identifikation von Bedrohungen betreffend intelligentes Messsystem

Aus den vorangehenden Analyseschritten stellt sich heraus, dass im Zusammenhang mit intelligenten Messsystemen zahlreiche Bedrohungen denkbar sind. Im Rahmen dieser SBA wird der in der Praxis erprobte Bedrohungskatalog aus Ref. [12] verwendet. Dieser Bedrohungskatalog kommt in ISDS-Konzepten der Bundesverwaltung zum Einsatz und beruht auf den Gefährdungskatalogen des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI)[27]. Die BSI Gefährdungskataloge bieten Best Practice und dadurch eine gute Basis für die Bildung spezifischer Bedrohungskataloge wie im vorliegenden Fall.

Der Bedrohungskatalog dient zusammen mit den Schwachstellen als Basis für die Identifikation und Bildung von Risiko-Szenarien.

Die fünf Bedrohungskategorien «Höhere Gewalt», «Organisatorische Mängel», «Menschliche Fehlhandlungen», «Technisches Versagen» und «Vorsätzliche Handlungen» wurden aus diesem Katalog unverändert übernommen und können mit Ausnahme der Kategorie «Vorsätzliche Handlungen» unter «Unabsichtliche Bedrohungen» zusammengefasst werden (vgl. Abbildung 8).

Um den Bezug auf die intelligenten Messsysteme beim Endverbraucher zu schärfen, wurden die einzelnen Bedrohungen aus dem Bedrohungskatalog teilweise angepasst.

Die Bedrohungskategorien sind abschliessend formuliert, jedoch nicht die einzelnen Bedrohungen innerhalb dieser Kategorien. Die einzelnen Bedrohungen können bei Bedarf erweitert werden.

Ref.	Bedrohungs-kategorie	Mögliche Bedrohungen
B.01	**Höhere Gewalt**	Verlust des Betriebs-/Wartungs-/Service Personals
B.02		Netzausfall (WAN, LAN)
B.03		Ausfall Kommunikationssystem durch Feuer, Wasser oder andere Naturgewalten
B.04		Ausfall dezentraler Komponenten in der Kundenumgebung durch Feuer, Wasser oder andere Naturgewalten
B.05		Ausfall zentraler Komponenten durch Feuer, Wasser oder andere Naturgewalten
B.06		Datenverlust durch Magnetfelder, Licht etc.
B.07	**Organisatorische Mängel**	Fehlende, ungeeignete, inkompatible Betriebsmittel/Sicherheitsmechanismen
B.08		Fehlende Kontrollen, Tests, Auswertungen
B.09		Fehlende oder unzureichende Schulung
B.10		Fehlende/mangelhafte Leitlinien, Weisungen und Reglemente
B.11		Nicht existierende, mangelhafte oder ineffiziente Prozesse und Prozessabläufe
B.12		Komplexität von Systemen und Komponenten
B.13		Bestehende Abhängigkeiten zu anderen Projekten, Produkten, Tools etc.
B.14	**Menschliche Fehlhandlungen**	Fahrlässigkeit, Unbeabsichtigte Beschädigung
B.15		Fehlverhalten Benutzer (z.B. Kompromittierung/Verlust der Anmeldedaten)
B.16		Fehlerhafte Administration, Wartung und Überwachung (z. B. Konfigurationsfehler)
B.17		Unabsichtliche Gefährdung durch Fremdpersonal
B.18		Verstoss gegen gültige Regelungen durch Nichtbeachtung der Vorschriften

[27] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Ref.	Bedrohungs-kategorie	Mögliche Bedrohungen
B.19	**Technisches Versagen**	Ausfall oder Fehlfunktion von Sicherheitskomponenten
B.20		Hardwaredefekt
B.21		Softwareschwachstellen
B.22		Beeinträchtigung durch Stromausfall etc.
B.23	**Vorsätzliche Handlungen**	Ausspähung der Datenkommunikation
B.24		Einschleusen von bösartiger Software (Malware) wie z. B. Trojanern und Viren
B.25		Datenmanipulation
B.26		Sabotage: Zerstörung der Daten/Zerstörung der Infrastruktur
B.27		Missbrauch von Konten, Zutritts- und Zugriffsberechtigungen
B.28		Erpressung von Mitarbeitern
B.29		Diebstahl, Betrug, Social Engineering[28]
B.30		(Distributed) Denial of Service Angriffe (DDoS)

Tabelle 5: Bedrohungskatalog für das intelligente Messsystem (Quelle: angepasst aus Ref. [12])

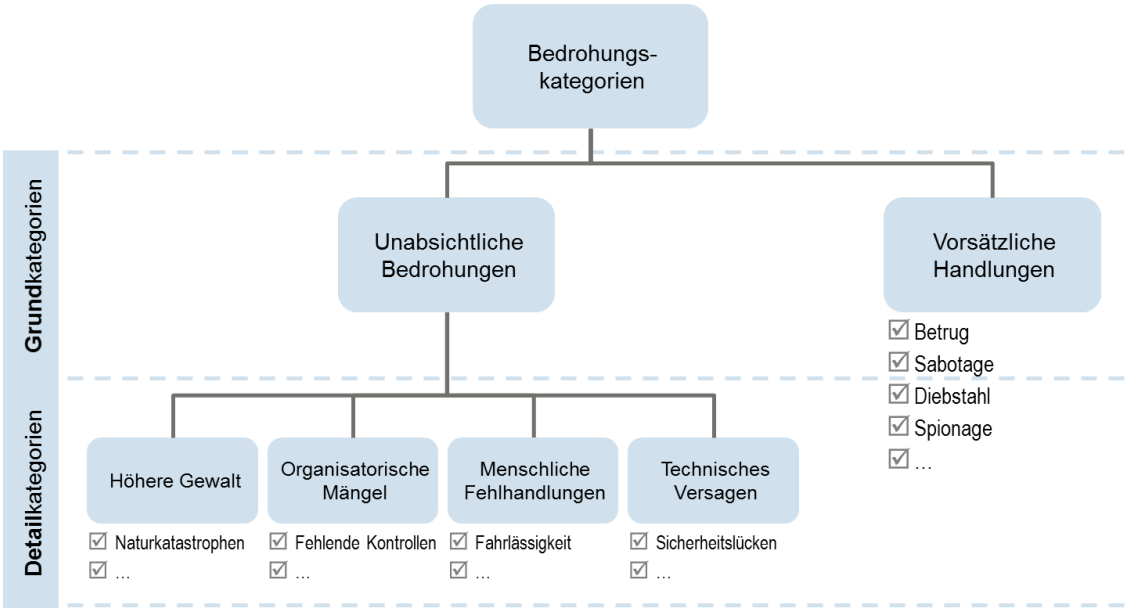


Abbildung 8: Übersicht Bedrohungskategorien

[28] Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen (Quelle: Wikipedia)

5. Risiko-Szenarien

Für die Analyse von Risiken in Bezug auf das intelligente Messsystem beim Endverbraucher kommt in dieser SBA wie in Kapitel 2 eingeführt die Szenario-basierte Analyse zum Einsatz.

Die Risiko-Szenarien sind aus möglichen Zusammenwirkungen zwischen Schutzobjekten, Schwachstellen und potentiellen Gefahren entstanden. Als Resultat daraus wurden die sogenannten «Kern Risiko-Szenarien» gebildet, die weitere, mögliche Detail-Risiko-Szenarien übergeordnet abdecken bzw. beinhalten.

Die Kern Risiko-Szenarien ermöglichen durch ihren Charakter ein umfangreiches Bild über die Risikolandschaft. Diese SBA umfasst vierzehn Kern Risiko-Szenarien, die unter vier Szenariogruppen zusammengefasst sind: «Abrechnungsbetrug», «Verlust von Verfügbarkeit und Integrität», «Netzinstabilitäten» und «Verletzung von Vertraulichkeit und Datenschutz».

Die Kern Risiko-Szenarien sind hinsichtlich Architekturvarianten aus Kapitel 3.1 als unabhängig zu betrachten bzw. beinhalten beide Varianten «Smart Meter als Master» und «Smart Meter Gateway».

Dieses Kapitel behandelt die Arbeitsschritte 5) bis 10) gemäss Kapitel 2, geht zudem auf die Schritte 8) Beurteilung Schadensausmass, 9) Bewertung der Risiken und 10) Beurteilung Schutzbedarf detailliert ein. Die Resultate aus den Schritten 6) Aufschlüsselung auf Ereigniskategorien und 7) Aufschlüsselung auf Schadenskategorien sind aufgrund ihrer textlich wiederholenden Art nur beschränkt als kontinuierliche Lektüre geeignet und werden daher in Anhang A.1 als Nachschlagewerk aufgeführt. Anhang A.1 beinhaltet auch die Steckbriefe für jedes einzelne Kern Risiko-Szenario mit den relevanten Bemerkungen und Annahmen sowie den Szenariovarianten und übergeordneten Schutzobjekten des intelligenten Messsystems. Die folgende Tabelle gibt eine Gesamtübersicht über alle Kern Risiko-Szenarien und deren Zuteilung in Szenariogruppen.

Ref.	Kern Risiko-Szenario	Szenariogruppe
RS.01	Abrechnungsbetrug mittels Manipulation der Tarifierung	**Abrechnungsbetrug**
RS.02	Grossflächiger Abrechnungsbetrug durch Datenmanager	
RS.03	Abrechnungsbetrug mittels Manipulation des geeichten, messtechnischen Teils des intelligenten Messgerätes	
RS.04	Grossflächiger Abrechnungsbetrug durch Datenmanager mittels Manipulation des geeichten, messtechnischen Teils der intelligenten Messgeräte	
RS.05	Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten	**Verlust von Verfügbarkeit und Integrität**
RS.06	Schwerwiegende Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems	
RS.07	Schwerwiegende Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform	
RS.08	Böswillige oder fehlerhafte Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern	**Netzinstabilitäten** (Spezialfälle der Gruppe Verlust von Verfügbarkeit und Integrität)
RS.09	Böswillige oder fehlerhafte Steuerung von Verbrauch und Einspeisung der elektrischen Energie bei Prosumern	
RS.10	Böswillige oder fehlerhafte Steuerung der Gebäudeautomation bei Prosumern	
RS.11	Gefährdung des Netzzustandes durch grossflächige Manipulation oder Einschränkung der Netzüberwachung	
RS.12	Offenlegung / Entwendung der auf intelligenten Messgeräten verwalteten Daten inkl. Datenübertragung	**Verletzung von Vertraulichkeit und Datenschutz**
RS.13	Schwerwiegende Daten-Offenlegung / -Entwendung via Zähldatenverarbeitungssystem	
RS.14	Schwerwiegende Daten-Offenlegung / -Entwendung via Online-Visualisierungsplattform	

Tabelle 6: Übersicht Kern Risiko-Szenarien und der Szenariogruppen

Durch den in dieser SBA gewählten Abstraktionsgrad stützen sich die Kern Risiko-Szenarien und deren Varianten primär auf die übergeordneten Schutzobjekte. Folgende Tabelle zeigt eine Übersicht, welche übergeordneten Schutzobjekte von welchen Szenarien betroffen sind. Daraus ist ersichtlich, dass die Online-Visualisierungsplattform nur in Bezug auf RS.07 und RS.14 eine Relevanz hat und die Szenarien sich mehrheitlich aufgrund der engeren Verknüpfung und grösseren Angriffsfläche auf das intelligente Messgerät, das Kommunikationssystem und das Zähldatenverarbeitungssystem konzentrieren.

Übergeordnete Schutzobjekte intelligentes Messsystem Kern Risiko-Szenarien	Intelligentes Messgerät	Kommunikationssystem	Zähldatenverarbeitungs-system	Online-Visualisierungsplattform
RS.01: Abrechnungsbetrug mittels Manipulation der Tarifierung	x	x	x	
RS.02: Grossflächiger Abrechnungsbetrug durch Datenmanager	x	x	x	
RS.03: Abrechnungsbetrug mittels Manipulation des geeichten, messtechnischen Teils des intelligenten Messgerätes	x	x	x	
RS.04: Grossflächiger Abrechnungsbetrug durch Datenmanager mittels Manipulation des geeichten, messtechnischen Teils der intelligenten Messgeräte	x	x	x	
RS.05: Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten	x	x		
RS.06: Schwerwiegende Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems			x	
RS.07: Schwerwiegende Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform				x
RS.08: Böswillige oder fehlerhafte Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern	x	x	x	
RS.09: Böswillige oder fehlerhafte Steuerung von Verbrauch und Einspeisung der elektrischen Energie bei Prosumern	x	x	x	
RS.10: Böswillige oder fehlerhafte Steuerung der Gebäudeautomation bei Prosumern	x	x	x	
RS.11: Gefährdung des Netzzustandes durch grossflächige Manipulation oder Einschränkung der Netzüberwachung	x	x	x	
RS.12: Offenlegung / Entwendung der auf intelligenten Messgeräten verwalteten Daten inkl. Datenübertragung	x	x		
RS.13: Schwerwiegende Daten-Offenlegung / -Entwendung via Zähldatenverarbeitungssystem			x	
RS.14: Schwerwiegende Daten-Offenlegung / -Entwendung via Online-Visualisierungsplattform				x

Tabelle 7: Zuordnung von Kern Risiko-Szenarien zu den übergeordneten Schutzobjekten

5.1. Risikobewertung und -übersicht

Die untenstehende Abbildung 9 stellt die Gesamtübersicht der Risikobewertung dar, die wie bereits erwähnt nach Sichten der beiden direkten Risikoträger «Prosumer» und «Datenmanager» stattgefunden hat. Diese Grob-Bewertung ist als Orientierungshilfe für mögliche Risiken in Bezug auf das intelligente Messsystem anzusehen.

Die unterschiedlichen Farben der Risikowerte versinnbildlichen die vier Szenariogruppen gemäss Legende. Die Risikowerte lassen sich anhand der Risikomatrix in drei Risikokategorien gliedern: geringes Risiko (grün hinterlegter Bereich), mittleres Risiko (gelb hinterlegter Bereich), hohes Risiko (rot hinterlegter Bereich).

Ein Direktvergleich der abgeschätzten Risikowerte mit anderen Bereichen der IKT resp. mit den anderen Risiken aus der Stromversorgung ist nicht möglich, da die Risikobewertung sehr eng mit den jeweiligen Annahmen, den Schutzobjekten und Schwachstellen sowie dem Bedrohungsumfeld verbunden ist.

Für die Kern Risiko-Szenarien und deren Beurteilung in Bezug auf Eintrittswahrscheinlichkeit und Schadensausmass dienen Worst Case Überlegungen als Basis. Daher sind die Eintrittswahrscheinlichkeiten generell tief eingestuft.

Die hohen Risikowerte R.05, R.06, R.08, R.09, R.10 und R.11 für Prosumer und Datenmanager resultieren aus den entsprechenden Kern Risiko-Szenarien (RS.05, RS.06, RS.08, RS.09, RS.10 und RS.11), welche u. a. auch mit der Gefährdung der überregionalen Versorgungssicherheit zusammenhängen (vgl. Abbildung 9).

Die Kern Risiko-Szenarien RS.08, RS.09, RS.10 und RS.11 (d.h. die Szenariogruppe «Netzinstabilitäten») bilden die Spezialfälle von RS.05 und RS.06:

- RS.08 behandelt den Fall „Lastunterbrecher (Breaker)“, durch welchen eine böswillige oder fehlerhafte Beschränkung oder An- und Abschaltung des Anschlusses bei Prosumern möglich sein kann.
- RS.09 deckt eine mögliche böswillige oder fehlerhafte Steuerung von Verbrauch und Einspeisung der elektrischen Energie bei Prosumern inkl. Haushaltsgeräte wie z. B. Ofen, Klimaanlage etc. ab.
- RS.10 umfasst eine eventuelle böswillige oder fehlerhafte Steuerung von Haus- und Gebäudeautomation bei Prosumern z. B. mittels Aktivierung oder Deaktivierung von Lüftung, Lift etc.
- RS.11 behandelt die mögliche Gefährdung des Netzzustandes durch grossflächige Manipulation oder Einschränkung der Netzüberwachung unter der Annahme dass eine solche Manipulation via intelligentes Messsystem möglich ist.

Auch beim Kern Risiko-Szenario RS.07 könnte die überregionale Versorgungssicherheit durch negatives Beeinflussen des Prosumerverhaltens im Extremfall infolge plötzlicher Netzüberlastung gefährdet werden, was jedoch sehr unwahrscheinlich ist und daher der entsprechende Risikowert R.07 aus Sicht Datenmanager als „Mittel“ eingestuft wurde.

Abrechnungsbetrug kann in Einzelfällen (R.01a, R.03a) für Prosumer und Datenmanager zu merklichen Schäden führen. Hohe Schäden hätten dagegen die grossflächigen Fälle R.01b und R.03b für Prosumer und R.01b, R.02, R.03b und R.04 für Datenmanager zur Folge, wobei diese aufgrund der relativ tiefen Eintrittswahrscheinlichkeiten jeweils zu einem mittleren Risikowert führen. Aufgrund der sich stetig verschärfenden Bedrohungslage tendiert jedoch der grossflächige Abrechnungsbetrug zu einem hohen Risikowert.

Die Risiken für RS.12, RS.13 und RS.14 werden nur aus Sicht des Datenmanagers bewertet, da diese Szenarien aufgrund ihrer Art zu einem rein indirekten Schaden für den

Prosumer führen würden. Aus Sicht des Datenmanagers stellen die Risikowerte R.12, R.13 und R.14 ein mittleres Risiko dar.

In den nachfolgenden Unterkapiteln werden die Beurteilung vom Schadensausmass und die Bewertung der Risiken für die unterschiedlichen Szenariogruppen diskutiert.

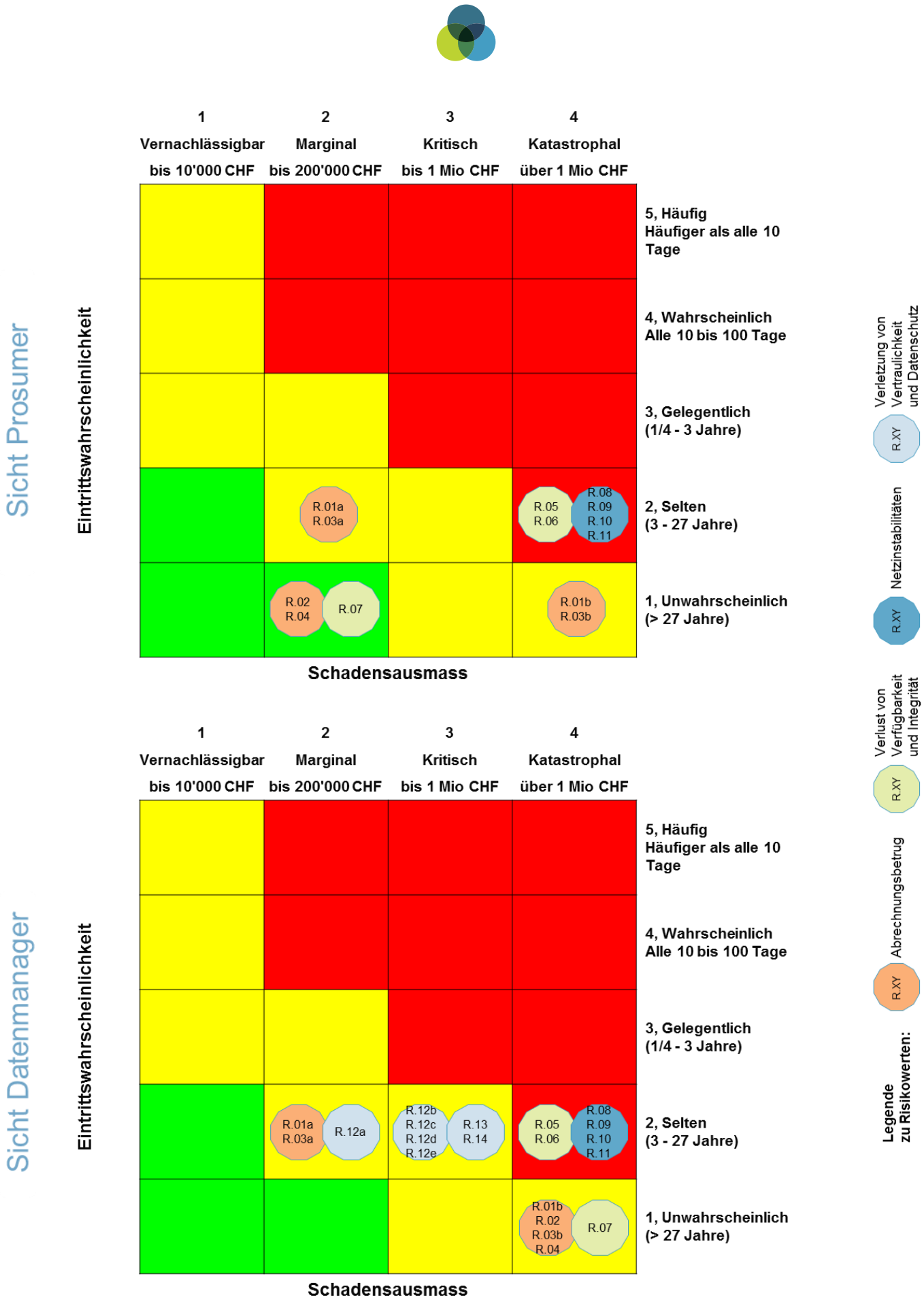


Abbildung 9: Gesamtübersicht Risikobewertung für Prosumer (oben) und Datenmanager (unten) Risikokategorien: Gering (grün), Mittel (gelb), Hoch (rot)

5.1.1. Abrechnungsbetrug

Diese Szenariogruppe behandelt den Betrug betreffend Bezug und/oder Einspeisung der elektrischen Energie in Zusammenhang mit dem intelligenten Messsystem und umfasst folgende Kern Risiko-Szenarien und deren Varianten:

- RS.01: Abrechnungsbetrug mittels Manipulation der Tarifierung
  - RS.01a: **Vereinzelter** Abrechnungsbetrug
  - RS.01b: **Grossflächiger** Abrechnungsbetrug
- RS.02: **Grossflächiger** Abrechnungsbetrug durch Datenmanager (Spezialfall von RS.01)
- RS.03: Abrechnungsbetrug mittels Manipulation des geeichten, messtechnischen Teils des intelligenten Messgerätes
  - RS.03a: **Vereinzelter** Abrechnungsbetrug
  - RS.03b: **Grossflächiger** Abrechnungsbetrug
- RS.04: **Grossflächiger** Abrechnungsbetrug durch Datenmanager mittels Manipulation des geeichten, messtechnischen Teils der intelligenten Messgeräte (Spezialfall von RS.03)

Unter Tarifierung ist die direkte Zuordnung von Preisen zu den Verbrauchs- und Erzeugungswerten zu verstehen. Dies ist technisch direkt im intelligenten Messgerät, oder aber erst im Zähldatenverarbeitungssystem möglich.

Eine Manipulation der Tarifierung umfasst die Manipulation der entsprechenden Daten (Meteringdaten, Tarifdaten betreffend Netz und Energie, Systemzeit etc.) und Prozesse.

Bei RS.01 und RS.03 erfolgt der Abrechnungsbetrug zugunsten des Prosumers und bei RS.02 und RS.04 zugunsten des Datenmanagers. Für die Szenarien RS.01 und RS.02 wird davon ausgegangen, dass der geeichte, messtechnische Teil des intelligenten Messgerätes integer bzw. nicht manipuliert ist. RS.03 und RS.04 konzentrieren sich dagegen ausschliesslich auf mögliche Manipulationen des geeichten, messtechnischen Teils von intelligenten Messgeräten durch den Einsatz von IKT zwecks Abrechnungsbetrug.

Für alle Szenarien der Gruppe «Abrechnungsbetrug» wird angenommen, dass die Online-Visualisierungsplattform keinen Einfluss bzw. Zusammenhang auf/zur Tarifierung hat.

5.1.1.1. Risikobewertung betreffend RS.01 und RS.03

Beurteilung Schadensausmass

Sicht einzelner Prosumer:

- RS.01a und RS.03a: Ein Prosumer begeht den Abrechnungsbetrug über mehrere Jahre. Ein Schaden für den Prosumer könnte wegen der Gesetzesverletzung sowie der Zahlung von Genugtuung (Schmerzensgeld) und Bussen entstehen, falls der Betrug entdeckt wird. Unter der Annahme, dass es sich dabei um einen Gross-Prosumer mit einem Jahresverbrauch von 1.5 Mio. kWh handelt, wäre der monetäre Vorteil bei einem Durchschnittsstrompreis von 15 Rappen pro kWh und bei einer jährlichen Energiedifferenz von 100’000 kWh zugunsten des Prosumers für drei Jahre 45’000 CHF [= 0.15 CHF/kWh x 100’000 kWh/Jahr x 3 Jahre]. Der finanzielle Vorteil für den Prosumer bzw. der finanzielle Nachteil für den Datenmanager hängt sehr stark mit der Grösse des Prosumers bzw. dessen Jahresverbrauch bzw. -Erzeugung der elektrischen Energie sowie mit den Annahmen bzgl. Manipulation der Tarifierung zusammen und kann in der Skala betreffend Schadensausmass stark variieren. Je höher der monetäre Schaden aus einem möglichen Abrechnungsbetrug für den Da-

tenmanager wird, desto höher wäre die Wahrscheinlichkeit für die Entdeckung des Betruges. Die Abschätzung des Schadensausmasses für den Prosumer und Datenmanager orientiert sich im vorliegenden Fall am obigen Beispiel mit Gross-Prosumer als Kompromiss zwischen kleinen und sehr grossen Prosumern und entspricht der Stufe „2, Marginal“ auf der Skala betreffend Schadensausmass.

- RS.01b und RS.03b: Mehrere Gross-Prosumer begehen den Abrechnungsbetrug, im Worst Case in Zusammenschluss/Absprache mit anderen Gross-Prosumern (Stichwort: Organisierte Kriminalität). Daher könnte der Schaden wegen der Gesetzesverletzung sowie der Zahlung von Genugtuung (Schmerzensgeld) und Bussen im schlimmsten Fall erheblich höher (über 1’000’000 CHF) ausfallen als bei RS.01a, falls der Betrug entdeckt wird. Das zu erwartende Schadensausmass wird daher als „4, Katastrophal“ eingestuft.

Sicht einzelner Datenmanager:

- RS.01a und RS.03a: Ein Abrechnungsbetrug durch einen Gross-Prosumer mit einem Jahresverbrauch von 1.5 Mio. kWh könnte beim Datenmanager zu einem Schaden (siehe Beispiel auf Seite 45) führen, unter der Annahme, dass es keine Genugtuung (Schmerzensgeld) gibt. Das vermutete Schadensausmass wird daher als „2, Marginal“ abgeschätzt.
- RS.01b und RS.03b: Ein grossflächiger Abrechnungsbetrug durch mehrere Gross-Prosumer könnte beim Datenmanager zusammen mit dem relativ hoch zu erwartenden Reputationsverlust und mit den Folgen von möglichen Compliance-Verletzungen (Nachbesserungen und Bussen) im schlimmsten Fall zu einem Schaden über 1’000’000 CHF führen, unter der Annahme, dass es keine Genugtuung (Schmerzensgeld) gibt. Grosse finanzielle Schäden in dieser Höhe könnten auch entstehen wenn sehr viele Kleinprosumer über längere Zeit einen Abrechnungsbetrug begehen würden. Das zu erwartende Schadensausmass wird daher als „4, Katastrophal“ eingestuft.

Bewertung der Risiken

- RS.01a und RS.03a: Der Eintritt eines Falls dieser Art wäre selten, jedoch gut möglich im Lebenszyklus eines intelligenten Messsystems. Daher wird die Eintrittswahrscheinlichkeit als „2, Selten“ abgeschätzt.
- RS.01b und RS.03b: Der Eintritt eines Falls dieser Art wäre eher unwahrscheinlich jedoch möglich im Lebenszyklus eines intelligenten Messsystems. Daher wird die Eintrittswahrscheinlichkeit als „1, Unwahrscheinlich“ eingestuft.

Daraus ergeben sich folgende Risikowerte für einzelne Prosumer und Datenmanager:

- Prosumer
  - R.01a = R.03a = 2 (Marginal) x 2 (Selten) = 4 (Mittel)
  - R.01b = R.03b = 4 (Katastrophal) x 1 (Unwahrscheinlich) = 4 (Mittel)
- Datenmanager
  - R.01a = R.03a = 2 (Marginal) x 2 (Selten) = 4 (Mittel)
  - R.01b = R.03b = 4 (Katastrophal) x 1 (Unwahrscheinlich) = 4 (Mittel)

5.1.1.2. Risikobewertung betreffend RS.02 und RS.04

Beurteilung Schadensausmass

Sicht einzelner Prosumer:

- RS.02 und RS.04: Ein finanzieller Schaden für einzelne Prosumer würde bei einem grossflächigen Abrechnungsbetrug durch den Datenmanager entstehen, unter der

Annahme, dass es keine Genugtuung (Schmerzensgeld) gibt (siehe Beispiel auf Seite 45). Der finanzielle Vorteil für den Datenmanager bzw. der finanzielle Nachteil für den Prosumer hängt sehr stark mit der Grösse des Prosumers bzw. dessen Jahresverbrauch bzw. -Erzeugung der elektrischen Energie sowie mit den Annahmen bzgl. Manipulation der Tarifierung zusammen und kann in der Skala betreffend Schadensausmass stark variieren. Je höher der monetäre Schaden aus einem möglichen Abrechnungsbetrug für den Prosumer wird, desto höher wäre die Wahrscheinlichkeit für die Entdeckung des Betruges. Die Abschätzung des Schadensausmasses für den Prosumer und Datenmanager orientiert sich im vorliegenden Fall am obigen Beispiel mit Gross-Prosumer als Kompromiss zwischen kleinen und sehr grossen Prosumern und entspricht der Stufe „2, Marginal“ auf der Skala betreffend Schadensausmass
Der Schaden aufgrund einer Persönlichkeitsverletzung gemäss Art.12 DSG durch eine eventuelle missbräuchliche Bearbeitung von Personendaten durch den Datenmanager, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen, kann nicht getrennt beziffert werden und ist in dem geschätzten Schadensausmass enthalten.

Sicht einzelner Datenmanager:

- RS.02 und RS.04: Der Datenmanager begeht den grossflächigen Abrechnungsbetrug über mehrere Jahre. Der Schaden für den Datenmanager könnte zusammen mit dem relativ hoch zu erwartenden Reputationsverlust und mit den Folgen von Compliance-Verletzungen (Nachbesserungen sowie Zahlung von Genugtuung und Bussen) im schlimmsten Fall über 1’000’000 CHF betragen, falls der Betrug entdeckt wird. Die Höhe der zu zahlenden Genugtuung und Bussen sind aufgrund der Grösse des Vorfalls relativ hoch zu erwarten. Das Schadensausmass wird daher als „4, Katastrophal“ eingestuft.

Bewertung der Risiken

Der Eintritt derartiger Szenarien wäre eher unwahrscheinlich, jedoch möglich im Lebenszyklus eines intelligenten Messsystems. Daher wird die Eintrittswahrscheinlichkeit als „1, Unwahrscheinlich“ eingestuft.

Daraus ergeben sich folgende Risikowerte für einzelne Prosumer und Datenmanager:

- Prosumer
  - R.02 = R.04 = 2 (Marginal) x 1 (Unwahrscheinlich) = 2 (Gering)
- Datenmanager
  - R.02 = R.04 = 4 (Katastrophal) x 1 (Unwahrscheinlich) = 4 (Mittel)

5.1.2. *Verlust von Verfügbarkeit und Integrität / Netzinstabilitäten*

Die Szenariogruppe «Verlust von Verfügbarkeit und Integrität» konzentriert sich auf die Einschränkung der Verfügbarkeit und Integrität des intelligenten Messsystems durch die Gefährdung der korrekten Funktionsweise des intelligenten Messsystems. Betroffen sind Daten und Datenübertragung zwecks Stromabrechnung, Netzüberwachung, Laststeuerung etc. Die Szenariogruppe besteht aus folgenden Kern Risiko-Szenarien und deren Varianten:

- RS.05: Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten
  - RS.05a: **Punktuelle** Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten **durch vorsätzliche Angriffe**
  - RS.05b: **Grossflächige** Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten **durch vorsätzliche Angriffe**
  - RS.05c: **Grossflächige** Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten **durch höhere Gewalt**
  - RS.05d: **Grossflächige** Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten **durch technisches Versagen**
  - RS.05e: **Grossflächige** Einschränkung der Verfügbarkeit von intelligenten Messgeräten und Integrität **durch menschliche Fehlhandlungen oder organisatorische Mängel**
- RS.06: Schwerwiegende Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems
  - RS.06a: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems (ZDVS) und der zusammenhängenden Daten und Funktionalitäten **durch vorsätzliche Angriffe**
  - RS.06b: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems und der zusammenhängenden Daten und Funktionalitäten **durch höhere Gewalt**
  - RS.06c: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems und der zusammenhängenden Daten und Funktionalitäten **durch technisches Versagen**
  - RS.06d: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems und der zusammenhängenden Daten und Funktionalitäten **durch menschliche Fehlhandlungen oder organisatorische Mängel**
- RS.07: Schwerwiegende Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform
  - RS.07a: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform (OVP) und der zusammenhängenden Daten und Funktionalitäten **durch vorsätzliche Angriffe**
  - RS.07b: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform und der zusammenhängenden Daten und Funktionalitäten **durch höhere Gewalt**
  - RS.07c: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform und der zusammenhängenden Daten und Funktionalitäten **durch technisches Versagen**
  - RS.07d: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform und der zusammenhängenden Daten und Funktionalitäten **durch menschliche Fehlhandlungen oder organisatorische Mängel**

Die Szenariogruppe «Netzinstabilitäten» umfasst die nachfolgend aufgeführten Spezialfälle der Gruppe «Verlust von Verfügbarkeit und Integrität» und wird daher im gleichen Kapitel beurteilt:

- RS.08: Böswillige oder fehlerhafte Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern
  - RS.08a: **Vereinzelte** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch vorsätzliche Angriffe**
  - RS.08b: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch vorsätzliche Angriffe**
  - RS.08c: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch höhere Gewalt**
  - RS.08d: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch technisches Versagen**
  - RS.08e: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch menschliche Fehlhandlungen oder organisatorische Mängel**
- RS.09: Böswillige oder fehlerhafte Steuerung von Verbrauch und Einspeisung der elektrischen Energie bei Prosumern
  - RS.09a: **Vereinzelte** Übernahme der Steuerung von Verbrauchs- und Erzeugungseinheiten bei Prosumern via intelligentes Messsystem **durch vorsätzliche Angriffe**
  - RS.09b: **Grossflächige** Übernahme der Steuerung von Verbrauchs- und Erzeugungseinheiten bei Prosumern via intelligentes Messsystem **durch vorsätzliche Angriffe**
  - RS.09c: **Grossflächige**, fehlerhafte Steuerung von Verbrauchs- und Erzeugungseinheiten bei Prosumern via intelligentes Messsystem **durch höhere Gewalt**
  - RS.09d: **Grossflächige**, fehlerhafte Steuerung von Verbrauchs- und Erzeugungseinheiten bei Prosumern via intelligentes Messsystem **durch technisches Versagen**
  - RS.09e: **Grossflächige**, fehlerhafte Steuerung von Verbrauchs- und Erzeugungseinheiten bei Prosumern via intelligentes Messsystem **durch menschliche Fehlhandlungen oder organisatorische Mängel**
- RS.10: Böswillige oder fehlerhafte Steuerung der Gebäudeautomation[29] bei Prosumern
  - RS.10a: **Vereinzelte** Übernahme der Steuerung der Gebäudeautomation (Lüftung etc.) via intelligentes Messsystem **durch vorsätzliche Angriffe**
  - RS.10b: **Grossflächige** Übernahme der Steuerung der Gebäudeautomation (Lüftung etc.) via intelligentes Messsystem **durch vorsätzliche Angriffe**
  - RS.10c: **Grossflächige**, fehlerhafte Steuerung der Gebäudeautomation (Lüftung etc.) via intelligentes Messsystem **durch höhere Gewalt**
  - RS.10d: **Grossflächige**, fehlerhafte Steuerung der Gebäudeautomation (Lüftung etc.) via intelligentes Messsystem **durch technisches Versagen**
  - RS.10e: **Grossflächige**, fehlerhafte Steuerung der Gebäudeautomation (Lüftung etc.) via intelligentes Messsystem **durch menschliche Fehlhandlungen oder organisatorische Mängel**

[29] Hausautomation wird unter Gebäudeautomation zusammengefasst.

- RS.11: Gefährdung des Netzzustandes durch grossflächige Manipulation oder Einschränkung der Netzüberwachung
  - RS.11a: Gefährdung des Netzzustandes durch **grossflächige** Manipulation **oder** Einschränkung der Netzüberwachung via intelligentes Messsystem **durch vorsätzliche Angriffe**
  - RS.11b: Gefährdung des Netzzustandes durch **grossflächige** Einschränkung der Netzüberwachung via intelligentes Messsystem **durch höhere Gewalt**
  - RS.11c: Gefährdung des Netzzustandes durch **grossflächige** Einschränkung der Netzüberwachung via intelligentes Messsystem **durch technisches Versagen**
  - RS.11d: Gefährdung des Netzzustandes durch **grossflächige** Einschränkung der Netzüberwachung via intelligentes Messsystem **durch menschliche Fehlhandlungen oder organisatorische Mängel**

5.1.2.1. Risikobewertung betreffend RS.05, RS.06, RS.08, RS.09, RS.10, RS.11

Beurteilung Schadensausmass

Sicht einzelner Prosumer:

- RS.05a, RS.08a, RS.09a, RS.10a: Es kann nicht ausgeschlossen werden, dass Endverbrauchsgeräte z.B. durch gleichzeitiges Ein- oder Ausschalten von Verbrauchs- und Erzeugungseinheiten (vgl. RS.09) beschädigt werden oder Leib und Leben auf Seite Prosumer gefährdet wird und es sogar zu Todesfällen kommen kann. Finanzieller Verlust könnte für einzelne Prosumer entstehen, falls es zu Sach- oder Personenschaden kommt oder der Bezug und/oder die Einspeisung der elektrischen Energie durch falsche oder fehlende Informationen zu Ungunsten des Prosumers beeinflusst werden. Aus diesem Grund wird das vermutete Schadensausmass für Einzelfälle im schlimmsten Fall als „4, Katastrophal“ eingestuft.
- RS.05b, RS.06a, RS.08b, RS.09b, RS.10b, RS.11a: Bei einem grossflächigen oder schwerwiegenden Vorfall wären die zu erwartenden, negativen Auswirkungen entsprechend höher (weit über 1’000’000 CHF). Das zu erwartende Schadensausmass wird daher als „4, Katastrophal“ eingestuft.
- RS.05c, RS.05d, RS.05e, RS.06b, RS.06c, RS.06d, RS.08c, RS.08d, RS.08e, RS.09c, RS.09d, RS.09e, RS.10c, RS.10d, RS.10e, RS.11b, RS.11c, RS.11d: Höhere Gewalt, technisches Versagen oder menschliches Fehlverhalten in Kombination mit organisatorischen Mängeln könnten zu grossflächigen Fehlfunktionen z. B. gleichzeitigem Ein- oder Ausschalten von Verbrauchs- und Erzeugungseinheiten (vgl. RS.09) bei einer Vielzahl intelligenter Messgeräte führen. Das vermutete Schadensausmass wird auch hier als „4, Katastrophal“ eingestuft.

Sicht einzelner Datenmanager:

- RS.05a, RS.08a, RS.09a, RS.10a: Die Compliance-Verletzungen kämen zustande, falls bestimmte Auflagen aus Gesetzen etc. durch den Datenmanager nicht erfüllt werden könnten. Finanzielle Verluste für Datenmanager könnten durch Schäden an Betriebsmitteln und/oder -Personal sowie an Prosumern oder Dritten aber auch als Folge von Compliance-Verletzungen (Nachbesserungen sowie Zahlung von Genugtuung und Bussen) entstehen. Es kann nicht ausgeschlossen werden, dass Leib und Leben von Prosumern, von Betriebs-, Wartungs- und Support-Personal oder von Dritten gefährdet werden könnte. Selbst Todesfälle könnten eine Folge sein. Die Gefährdung von Leib und Leben hängt u. a. auch von der Grösse des Vorfalls ab (Beispiel: der Verkehr ist aufgrund eines Stromausfalls nicht mehr geregelt). Es wird hier vom Worst Case ausgegangen. Ein merklicher Reputationsverlust wäre auch nicht ausgeschlossen, insbesondere wenn der Fall in den Medien erscheint. Das eventu-

elle Schadensausmass wird für den schlimmsten Fall als „4, Katastrophal“ abgeschätzt.

- RS.05b, RS.05c, RS.05d, RS.05e, RS.06a, RS.06b, RS.06c, RS.06d, RS.08b, RS.08c, RS.08d, RS.08e, RS.09b, RS.09c, RS.09d, RS.09e, RS.10b, RS.10c, RS.10d, RS.10e, RS.11a, RS.11b, RS.11c, RS.11d: Bei einem grossflächigen oder schwerwiegenden Vorfall, der durch vorsätzliche Angriffe oder unabsichtliche Bedrohungen (höhere Gewalt, technisches Versagen oder menschliches Fehlverhalten in Kombination mit organisatorischen Mängeln) zustande kommt, wären die zu erwartenden Auswirkungen entsprechend höher (**weit über** 1’000’000 CHF) und die überregionale Versorgungssicherheit könnte im schlimmsten Fall gefährdet werden.

Bewertung der Risiken

Der Eintritt derartiger Szenarien könnte selten jedoch gut möglich im Lebenszyklus eines intelligenten Messsystems vorkommen. Die Eintrittswahrscheinlichkeit wird bei Risiko-Szenarien, wo es sich um einige wenige schwerwiegende Vorfälle handelt (RS.05a, RS08a, RS.09a, RS.10a) zwar eher höher gegenüber den grossflächigen bzw. schwerwiegenden Szenariovarianten (RS.05b, RS.05c, RS.05d, RS.05e, RS.06a, RS.06b, RS.06c, RS.06d, RS.08b, RS.08c, RS.08d, RS.08e, RS.09b, RS.09c, RS.09d, RS.09e, RS.10b, RS.10c, RS.10d, RS.10e, RS.11a, RS.11b, RS.11c, RS.11d) geschätzt, lässt sich jedoch auf Basis der verwendeten Risikomatrix nicht gesondert ausweisen. Daher wird die Eintrittswahrscheinlichkeit über all diese Kern-Szenarien und deren Varianten hinweg als „2, Selten“ abgeschätzt.

Daraus ergeben sich folgende Risikowerte für einzelne Prosumer und Datenmanager:

- Prosumer
  - R.05 = R.06 = R.08 = R.09 = R.10 = R.11 = 4 (Katastrophal) x 2 (Selten) = 8 (Hoch)
- Datenmanager
  - R.05 = R.06 = R.08 = R.09 = R.10 = R.11 = 4 (Katastrophal) x 2 (Selten) = 8 (Hoch)

5.1.2.2. Risikobewertung betreffend RS.07

Beurteilung Schadensausmass

Sicht Prosumer:

- RS.07a, RS.07b, RS.07c, RS.07d: Finanzieller Verlust könnte für Prosumer entstehen, falls der Bezug und/oder die Einspeisung der elektrischen Energie durch falsche oder fehlende Informationen auf der Online-Visualisierungsplattform zu Ungunsten des Prosumers beeinflusst werden (siehe Beispiel auf Seite 45). Das zu erwartende Schadensausmass wird auf Basis dieser Annahmen als „2, Marginal“ abgeschätzt.

Sicht Datenmanager:

- RS.07a, RS.07b, RS.07c, RS.07d: Die Compliance-Verletzungen kämen zustande, falls bestimmte Auflagen aus Gesetzen etc. aufgrund der eventuell falschen oder fehlenden Informationen auf der Online-Visualisierungsplattform durch den Datenmanager nicht erfüllt werden könnten. Die Folgen von eventuellen Compliance-Verletzungen (Nachbesserungen sowie Zahlung von Genugtuung und Bussen) könnten zu finanziellen Verlusten beim Datenmanager führen, welche im schlimmsten Fall über 1’000’000 CHF betragen könnte. Weitere finanzielle Verluste für Datenmanager könnten entstehen, falls der Bezug und/oder die Einspeisung der elektrischen Energie durch falsche oder fehlende Informationen zu Ungunsten des

Datenmanagers beeinflusst werden. Ein moderater Reputationsverlust wäre auch nicht ausgeschlossen, insbesondere wenn der Vorfall in den Medien erscheint. Durch die eventuell falschen oder fehlenden Informationen auf der Online-Visualisierungsplattform könnten falsche Anreize für Prosumer entstehen, z. B. all ihre Verbraucher einzuschalten, wodurch es im schlimmsten Fall zu einer Gefährdung der überregionalen Versorgungssicherheit wegen plötzlicher Netzüberlastung kommen könnte[30]. Das mögliche Schadensausmass wird als „4, Katastrophal“ eingestuft.

Bewertung der Risiken

Der Eintritt erwähnter Szenarien wäre eher unwahrscheinlich jedoch möglich im Lebenszyklus eines intelligenten Messsystems. Daher wird die Eintrittswahrscheinlichkeit als „1, Unwahrscheinlich“ eingestuft.

Daraus ergeben sich folgende Risikowerte für einzelne Prosumer und Datenmanager:

- Prosumer
  - R.07a = R.07b = R.07c = R.07d = 2 (Marginal) x 1 (Unwahrscheinlich) = 2 (Gering)
- Datenmanager
  - R.07a = R.07b = R.07c = R.07d = 4 (Katastrophal) x 1 (Unwahrscheinlich) = 4 (Mittel)

5.1.3. Verletzung von Vertraulichkeit und Datenschutz

Die via intelligentes Messsystem offengelegten oder entwendeten Daten[31] können z. B. zur Erzeugung von detaillierten Last- und Erzeugungsprofilen von Prosumern oder generell zur Angriffsvorbereitung (Stichwort «information gathering») eingesetzt werden. Diese Szenariogruppe besteht aus folgenden drei Kern Risiko-Szenarien und deren Varianten:

- RS.12: Offenlegung/Entwendung der auf intelligenten Messgeräten verwalteten Daten inkl. Datenübertragung
  - RS.12a: **Punktuelle** Offenlegung, Entwendung oder missbräuchliche Bearbeitung der auf intelligenten Messgeräten verwalteten Daten **durch vorsätzliche Angriffe**
  - RS.12b: **Grossflächige** Offenlegung, Entwendung oder missbräuchliche Bearbeitung der auf intelligenten Messgeräten verwalteten Daten **durch vorsätzliche Angriffe**
  - RS.12c: **Grossflächige** Offenlegung der auf intelligenten Messgeräten verwalteten Daten **durch höhere Gewalt**
  - RS.12d: **Grossflächige** Offenlegung der auf intelligenten Messgeräten verwalteten Daten **durch technisches Versagen**
  - RS.12e: **Grossflächige** Offenlegung der auf intelligenten Messgeräten verwalteten Daten **durch menschliche Fehlhandlungen oder organisatorische Mängel**
- RS.13: Schwerwiegende Daten-Offenlegung / -Entwendung via Zähldatenverarbeitungssystem
  - RS.13a: **Schwerwiegende** Offenlegung, Entwendung oder missbräuchliche Bearbeitung der auf Zähldatenverarbeitungssystem (ZDVS) verwalteten Daten **durch vorsätzliche Angriffe**

[30] Siehe z. B. http://www.energiezukunft.eu/netze/smart-grids/black-out-durch-intelligente-stromzaehler-gn103411/

[31] Als „öffentlich“ eingestufte Daten sind ausser Betrachtung.

  - RS.13b: **Schwerwiegende** Offenlegung der auf Zähldatenverarbeitungssystem verwalteten Daten **durch höhere Gewalt**
  - RS.13c: **Schwerwiegende** Offenlegung der auf Zähldatenverarbeitungssystem verwalteten Daten **durch technisches Versagen**
  - RS.13d: **Schwerwiegende** Offenlegung der auf Zähldatenverarbeitungssystem verwalteten Daten **durch menschliche Fehlhandlungen oder organisatorische Mängel**
- RS.14: Schwerwiegende Daten-Offenlegung / -Entwendung via Online-Visualisierungsplattform
  - RS.14a: **Schwerwiegende** Offenlegung, Entwendung oder missbräuchliche Bearbeitung der auf Online-Visualisierungsplattform (OVP) verwalteten Daten **durch vorsätzliche Angriffe**
  - RS.14b: **Schwerwiegende** Offenlegung der auf Online-Visualisierungsplattform verwalteten Daten **durch höhere Gewalt**
  - RS.14c: **Schwerwiegende** Offenlegung der auf Online-Visualisierungsplattform verwalteten Daten **durch technisches Versagen**
  - RS.14d: **Schwerwiegende** Offenlegung der auf Online-Visualisierungsplattform verwalteten Daten **durch menschliche Fehlhandlungen oder organisatorische Mängel**

5.1.3.1. Risikobewertung betreffend RS.12, RS.13, RS.14

Beurteilung Schadensausmass

Sicht einzelner Prosumer:

- RS.12a: Die Offenlegung, Entwendung oder eine missbräuchliche Bearbeitung von Daten bzw. Personendaten durch den Datenmanager oder Dritte könnte Persönlichkeitsverletzungen gemäss Art.12 DSG (z. B. durch widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern) zur Folge haben, resultieren jedoch nicht direkt in einem finanziellen Verlust für den Prosumer sondern indirekt über weitere Angriffe wie z. B. solcher aus RS.02. Es wird weiter davon ausgegangen, dass durch eine mögliche Offenlegung, Entwendung oder missbräuchliche Bearbeitung der Daten kein nennenswerter Reputationsschaden für den Prosumer entstehen würde. Daher wird auf eine Quantifizierung des Schadensausmasses verzichtet.
- RS.12b, RS.12c, RS.12d, RS.12e, RS.13a, RS.13b, RS.13c, RS.13d, RS.14a, RS.14b, RS.14c, RS.14d: Gegenüber RS.12a könnten die Auswirkungen bei einem grossflächigen oder schwerwiegenden Vorfall zwar höher sein, es wird aber auf eine Quantifizierung des Schadensausmasses auch hier verzichtet, da diese Szenarien nicht direkt zu einem finanziellen Verlust für den Prosumer führen würden, sondern indirekt über weitere Angriffe und Missbräuche.

Sicht einzelner Datenmanager:

- RS.12a: Durch die Offenlegung, Entwendung oder missbräuchliche Bearbeitung von Daten bzw. Personendaten durch den Datenmanager oder Dritte kämen u. U. Compliance-Verletzungen zustande, die im Endeffekt durch Gerichtsverfahren o.ä. mit finanziellen Verlust und Reputationsverlust verbunden sind. Das mögliche Schadensausmass wird im Einzelfall eher als „2, Marginal“ abgeschätzt.
- RS.12b, RS.12c, RS.12d, RS.12e, RS.13a, RS.13b, RS.13c, RS.13d, RS.14a, RS.14b, RS.14c, RS.14d: Bei einem grossflächigen oder schwerwiegenden Vorfall wären die bei R.12a erwähnten Auswirkungen entsprechend höher, jedoch sehr

wahrscheinlich unter 1‘000‘000 CHF. Daher wird die Stufe für das zu erwartende Schadensausmass als „3, Kritisch“ eingestuft.

Bewertung der Risiken

Der Eintritt derartiger Szenarien könnte selten, jedoch gut möglich im Lebenszyklus eines intelligenten Messsystems vorkommen. Die Eintrittswahrscheinlichkeit wird über all diese Kern-Szenarien und deren Varianten hinweg (RS.12a, RS.12b, RS.12c, RS.12d, RS.12e, RS.13a, RS.13b, RS.13c, RS.13d, RS.14a, RS.14b, RS.14c, RS.14d) als „2, Selten“ abgeschätzt.

Daraus ergeben sich folgende Risikowerte für einzelne Prosumer und Datenmanager:

- Prosumer
  - Wird nicht ausgewiesen (siehe Beurteilung Schadensausmass für Prosumer)
- Datenmanager
  - R.12a = 2 (Marginal) x 2 (Selten) = 4 (Mittel)
  - R.12b = R.12c = R.12d = R.13 = R.14 = 3 (Kritisch) x 2 (Selten) = 6 (Mittel)

5.2. Beurteilung Schutzbedarf für das intelligente Messsystem

Die qualitative Beurteilung des Schutzbedarfs erfolgt auf Basis von sechs Fragen gemäss Kapitel 2, Arbeitsschritt 10) **Beurteilung Schutzbedarf** und durch eine kombinierte Sicht vom Prosumer und Datenmanager, um umfassende Schlussfolgerungen über alle Risiko-Szenarien hinweg ermöglichen zu können.

5.2.1. Schutzbedarf für «Intelligentes Messsystem» ohne Online-Visualisierungsplattform

Das intelligente Messgerät, das Kommunikationssystem und das Zähldatenverarbeitungssystem sind gemäss Systemarchitektur nach Kapitel 3.3 eng miteinander verknüpft. Deshalb zielen die Risiko-Szenarien mehrheitlich auf diese Komponenten des intelligenten Messsystems. Aus diesem Grund erfolgt die Schutzbedarfsbeurteilung für diese drei übergeordneten Schutzobjekte zusammen.

Ref.	Frage	Beurteilung
1	Wird die Einhaltung der eichrechtlich gültigen Vorschriften erheblich gefährdet?	Eine erhebliche Gefährdung der Einhaltung der eichrechtlich gültigen Vorschriften wäre gemäss Kern Risiko Szenarien RS.03 und RS.04 bzw. deren Beurteilung/Bewertung möglich.
2	Wird die Einhaltung der datenschutzrechtlichen Vorgaben erheblich gefährdet?	Eine Verletzung von Persönlichkeitsrechten gemäss Art. 12 DSG ist gemäss den Kern Risiko Szenarien RS.02, RS.04, RS.12 und RS.13 bzw. deren Beurteilung/Bewertung möglich
3	Wird Leib und Leben (Personensicherheit) gefährdet?	Eine **Gefährdung vom Leib und Leben** ist gemäss Kern Risiko-Szenarien RS.05, RS.06, RS.08, RS.09, RS.10, RS.11 bzw. deren Beurteilung/Bewertung möglich
4	Wird die überregionale Versorgungssicherheit gefährdet?	Eine **Gefährdung der überregionalen Versorgungssicherheit** ist gemäss Kern Risiko-Szenarien RS.05, RS.06, RS.08, RS.09, RS.10, RS.11 bzw. deren Beurteilung/Bewertung möglich
5	Sind schwerwiegende finanzielle Verluste durch die zu erwartenden Auswirkungen möglich?	Schwerwiegende finanzielle Verluste sind gemäss Kern Risiko-Szenarien RS.01, RS.02, RS.03, RS.04, RS.05, RS.06, RS.08, RS.09, RS.10, RS.11 bzw. deren Beurteilung/Bewertung möglich
6	Wurden hohe Risiken identifiziert?	In Bezug auf Kern Risiko-Szenarien RS.05, RS.06, RS.08, RS.09, RS.10, RS.11 wurden **hohe Risiken** identifiziert

Tabelle 8: Hoher Schutzbedarf für das intelligente Messsystem ohne Visualisierungsplattform

Aus Tabelle 8 ist ersichtlich, dass in Zusammenhang mit diesen drei übergeordneten Schutzobjekten sowohl Leib und Leben als auch die überregionale Versorgungssicherheit gefährdet werden könnten und hohe Risiken identifiziert worden sind, was auf einen **hohen Schutzbedarf** für das intelligente Messsystem mit Ausnahme der Online-Visualisierungsplattform hinweist.

5.2.2. *Schutzbedarf für «Online-Visualisierungsplattform»*

Ref.	Frage	Beurteilung
1	Wird die Einhaltung der eichrechtlich gültigen Vorschriften erheblich gefährdet?	Unter der Annahme, dass die Online-Visualisierungsplattform keinen Einfluss auf den messtechnischen Teil des intelligenten Messgeräts hat, wäre eine Gefährdung der Einhaltung der eichrechtlich gültigen Vorschriften nicht möglich.
2	Wird die Einhaltung der datenschutzrechtlichen Vorgaben erheblich gefährdet?	Eine Verletzung von Persönlichkeitsrechten gemäss Art. 12 DSG ist gemäss Kern Risiko Szenario RS.14 bzw. dessen Beurteilung/Bewertung möglich
3	Wird Leib und Leben (Personensicherheit) gefährdet?	Eine Gefährdung vom Leib und Leben ist gemäss Kern Risiko-Szenario RS.07 bzw. dessen Beurteilung/Bewertung im Extremfall nicht ausgeschlossen
4	Wird die überregionale Versorgungssicherheit gefährdet?	Eine Gefährdung der überregionalen Versorgungssicherheit ist gemäss Kern Risiko-Szenario RS.07 bzw. dessen Beurteilung/Bewertung im Extremfall möglich
5	Sind schwerwiegende finanzielle Verluste durch die zu erwartenden Auswirkungen möglich?	Schwerwiegende finanzielle Verluste sind gemäss Kern gemäss Kern Risiko-Szenario RS.07 bzw. dessen Beurteilung/Bewertung möglich
6	Wurden hohe Risiken identifiziert?	In Bezug auf Kern Risiko-Szenarien RS.07 und RS.14 wurden **mittlere** Risiken identifiziert

Tabelle 9: Mittlerer Schutzbedarf für Online-Visualisierungsplattform

Eine mögliche Verletzung von Persönlichkeitsrechten gemäss Art. 12 DSG über Kern Risiko Szenario RS.14 und eventuelle schwerwiegende finanzielle Verluste gemäss Kern Risiko-Szenario RS.07 führen zu einem **mittleren Schutzbedarf**. Weiter kann eine Gefährdung der überregionalen Versorgungssicherheit sowie von Leib und Leben gemäss Kern Risiko-Szenario RS.07 im Extremfall nicht ausgeschlossen werden.

5.2.3. *Empfehlung Schutzniveau*

Eine Standarddefinition, welches Schutzniveau bei hohem, mittlerem oder geringem Schutzbedarf angezeigt ist, existiert nicht und muss sich an die jeweiligen Schutzbedürfnisse und im vorliegenden Fall an den Bedürfnissen in Zusammenhang mit dem intelligenten Messsystem orientieren. Das Schutzniveau sollte prinzipiell direkt proportional zum Schutzbedarf sein: Je höher der Schutzbedarf ist desto höher sollte das anzustrebende Schutzniveau gesetzt werden.

Auf Basis der Resultate aus den vorangehenden Kapiteln wird für das intelligente Messsystem gesamthaft ein angemessen hohes Schutzniveau empfohlen. Eine Differenzierung des Schutzniveaus zwischen den verschiedenen Komponenten ist in dieser SBA jedoch wenig sinnvoll, da die Zusammenhänge zwischen den verschiedenen Komponenten in einem realen Umsetzungsfall anders bzw. komplexer sein könnten.

Ein angemessen hohes Schutzniveau muss sich an den vorhandenen Risiken und an der Akzeptanz dieser Risiken orientieren. Daher muss das Schutzniveau für das intelligente Messsystem so hoch sein, dass ein einwandfreier Betrieb im Hinblick auf IKT-Sicherheit möglich ist, indem die identifizierten Risiken auf ein *akzeptables* Niveau reduziert werden. Der Entscheid über ein akzeptables Risikoniveau liegt beim Datenmanager, da dieser in Bezug auf das intelligente Messsystem der direkte Risikoträger ist.

Für die Online-Visualisierungsplattform könnte aufgrund der Resultate aus der SBA theoretisch ein niedrigeres Schutzniveau angestrebt werden. Es wird empfohlen, diesen Entscheid im Rahmen einer realen Implementierung durch den Datenmanager auf Basis der Risiken zu fällen.

Kapitel 6.1 umfasst Massnahmenempfehlungen für das intelligente Messsystem im Hinblick auf die Erstellung eines Massnahmenkatalogs zur Umsetzung eines angemessenen Basisschutzniveaus bzw. Grundschutzes durch den Datenmanager.

6. Sicherheitsmassnahmen für intelligente Messsysteme

Für die Bewältigung der Risiken in Zusammenhang mit intelligenten Messsystemen können verschiedene Strategien verfolgt werden. Als primäre Strategie sollte versucht werden, die jeweiligen Risikoursachen bzw. Schwachstellen und Bedrohungen zu eliminieren. In einem weiteren Schritt sollten die Risiken durch geeignete Sicherheitsmassnahmen vermindert werden. Dieses Kapitel konzentriert sich auf die Risikominderung als Risiko-Bewältigungsstrategie und umfasst Massnahmenempfehlungen zur Risiko-Reduktion.

Die Basis für die Massnahmendefinition bilden folgende Anforderungs- und Massnahmenkataloge zur Erreichung von möglichst umfangreichen sowie zielgerichteten und konsistenten Massnahmenempfehlungen:

- Publikation Enisa: Ref. [13]
- Mindestanforderungen 4.1.3A, 4.1.3B und 4.1.3D aus Ref. [1]
- Publikation Oesterreichs Energie: Ref. [4]

Die Massnahmenempfehlungen richten sich in erster Linie an direkte Risikoträger bzw. Prosumer und Datenmanager (Messstellenbetreiber und Messdienstleister gemäss Kapitel 3.4). Vollständigkeitshalber wurden auch Massnahmenvorschläge zu Händen externer Dienstleister (Hersteller intelligenter Messgeräte, IKT-Dienstleistungsanbieter etc.) erarbeitet, da diese indirekt über ihre Produkte und Dienstleistungen die Sicherheit des intelligenten Messsystems beeinflussen. Ausserdem haben sie eine soziale Verantwortung, da mögliche Mängel an den angebotenen Produkten und erbrachten Dienstleistungen grossen Einfluss auf volkswirtschaftlicher und gesellschaftlicher Ebene haben könnten.

Es kann festgestellt werden, dass auch der Bund zu den Risikoträgern gehört. Dies ist jedoch nur indirekt der Fall. Rahmenbedingungen zur Einführung intelligenter Messsysteme werden durch das erste Massnahmenpaket zur Energiestrategie 2050 geschaffen. Über die Norm zur Einführung der intelligenten Messsysteme und die Vorgabe gewisser Funktionalitäten bzw. technischer Mindestanforderungen zeichnet der Bund für die Sicherheit von intelligenten Messsystemen mitverantwortlich. Diese Verantwortung kann hinreichend wahrgenommen werden durch die Vorgabe eines geeigneten Rahmens zur sicheren Ausgestaltung der intelligenten Messsysteme seitens der Unternehmen der Energieversorgung. Rechtlich besteht im ersten Massnahmenpaket der Energiestrategie 2050 gemäss Botschaft bereits eine entsprechende Delegationsnorm. Auf spezifisch an den Bund adressierten Massnahmen wird daher in dieser SBA verzichtet.

Die Konkretisierung und Adaption von Massnahmen hängen stark vom jeweiligen Unternehmen bzw. dessen Bedürfnissen ab. Die Datenmanager, Prosumer und externen Dienstleister müssen die Risiken für sich selbst abwägen und entscheiden, welche Massnahmen sie schlussendlich umsetzen. Sie können bei Bedarf entsprechend der angebrachten Verhältnismässigkeit zusätzliche oder alternative Massnahmen definieren.

Die vorgeschlagenen Massnahmen wurden in Bezug auf ihren Einfluss auf den sicheren Betrieb kategorisiert. Die Kategorisierung erfolgte gemäss folgendem Schema:

- Kategorie 1: Sicherheitsmassnahmen mit direktem Einfluss auf den sicheren Betrieb des intelligenten Messsystems
- Kategorie 2: Sicherheitsmassnahmen mit indirektem Einfluss auf den sicheren Betrieb des intelligenten Messsystems

Alle Massnahmen werden unabhängig von deren Kategorisierung zur Umsetzung empfohlen. Die Massnahmen sind bewusst so ausformuliert, dass diese bei Bedarf für die Formulierung möglicher Sicherheitsanforderungen im Hinblick auf die Gewährleistung des sicheren Einsatzes intelligenter Messsysteme übernommen werden können. Es gilt

sie noch auszugestalten. Für einen wirksamen Schutz müssen die Massnahmen nach deren Umsetzung kontinuierlich gepflegt werden. Die Massnahmenpflege sollte auf der Überprüfung der Wirksamkeit und der Effizienz der Massnahmen basieren. Ein entsprechender Nachweis der Umsetzung ist sinnvoll.

6.1. Massnahmen für Datenmanager

Der primäre Adressat für die empfohlenen Sicherheitsmassnahmen ist der Datenmanager, da er für den Betrieb und die Sicherheit des intelligenten Messsystems die Risikoverantwortung hat.

Aufgrund des hohen Schutzniveaus, das in Kapitel 5.2.3 für das intelligente Messsystem gesamthaft empfohlen wurde, erscheint die Umsetzung von umfassenden Massnahmen über alle Risiko-Szenarien und übergeordneten Schutzobjekte («Intelligentes Messgerät», «Kommunikationssystem», «Zähldatenverarbeitungssystem» und «Online-Visualisierungsplattform») hinweg als angezeigt und verhältnismässig. Die Massnahmenempfehlungen gemäss Tabelle 10 zielen auf einen umfangreichen Massnahmenkatalog zur Umsetzung eines Grundschutzes für das intelligente Messsystem durch den Datenmanager. Es ist zu erwähnen, dass diese Massnahmen in ihrer Gesamtheit unter dem Stichwort «Informationssicherheitsmanagementsystem (ISMS)» subsumiert werden können. Für die Datenmanager, die bereits ein ISMS im Betrieb haben, ginge es dann um die Smart Metering-spezifische Ausweitung der Massnahmen.

Da der Begriff «Datenmanager» die Rollen «Messstellenbetreiber» und «Messdienstleister» gemäss Kapitel 3.4 umfasst und die Massnahmen für alle übergeordneten Schutzobjekte des intelligenten Messsystems gelten, werden die Massnahmen aus Tabelle 10 an diese beiden Rollen gleichzeitig adressiert, wobei die an Messstellenbetreiber adressierten Massnahmen primär für das Schutzobjekt «Intelligentes Messgerät» gelten.

Zweck besserer Übersichtlichkeit wurden die Massnahmen in folgende Gruppen aufgeteilt, wobei die Gruppenbezeichnungen stichwortartig auf die darunterliegenden Massnahmen hinweisen:

- Gruppe «Übergeordnet» umfasst die übergreifenden Sicherheitsmassnahmen
- Gruppe «Betriebliche Sicherheit» definiert die betriebsorientierten Massnahmen
- Gruppe «Sicherheitsaudits» umfassen die Sicherheitsüberprüfungen in Bezug auf die Komponenten und IKT-Systeme des intelligenten Messsystems
- Gruppe «Sicherheit des Personals» beinhaltet die Personensicherheitsprüfungen sowie die Schulung und Sensibilisierung des Personals in Bezug auf IKT-Sicherheit
- Gruppe «Incident Management, Logging, Monitoring und Auditierung» umfasst u .a. die Behandlung von Sicherheitsvorfällen sowie Verhinderung, Erkennung und Protokollierung von Manipulationen
- Gruppe «Schutz der Daten» definiert Massnahmen für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der durch das intelligente Messsystem verarbeiteten oder verwalteten Daten
- Gruppe «Betriebskontinuität» umfasst die Massnahmen zur Notfall- und Katastrophenvorsorge
- Gruppe «Physische und logische Zugangskontrolle» beinhaltet u. a. die Sicherheitsmassnahmen zur Gewährleistung der physischen Sicherheit des intelligenten Messsystems sowie dessen sichere Administration
- Gruppe «Kommunikations- und Netzwerksicherheit» umfasst u. a. Massnahmen zur Sicherung der Datenübermittlung und -Kommunikation zwischen den Komponenten

und IKT-Systemen des intelligenten Messsystems sowie zu den Komponenten und IKT-Systemen ausserhalb des intelligenten Messsystems

- Gruppe «Externe Dienstleister» betrifft die Massnahmen in Bezug auf externe Dienstleister auf Seite des Datenmanagers
- Gruppe «Kryptografie» beinhaltet den Einsatz von sicheren kryptografischen Algorithmen und Verfahren sowie deren Schutz

Ref.	Sicherheitsmassnahme	Kategorisierung [32]	Verweis[33]
Übergeordnet			
DM.01	Erarbeitung, Etablierung und Pflege einer organisations- bzw. unternehmensweiten IKT-Sicherheitspolitik, die an der Geschäftsstrategie ausgerichtet ist	2	SM 1.1
DM.02	Definition, Aufbau, Operationalisierung und Pflege einer IKT-Sicherheitsorganisation mit entsprechenden personellen Ressourcen, Rollen, Aufgaben, Kompetenzen und Verantwortlichkeiten	1	SM 1.2
DM.03	Management von IKT-Sicherheitsrisiken unter Berücksichtigung des komplexen betrieblichen Umfeldes inkl. Definition, Aufbau, Operationalisierung und Pflege eines geeigneten Risikomanagement-Frameworks	1	SM 1.4
DM.04	Regelmässige Identifikation, Analyse und Bewertung von IKT-Sicherheits-Risiken, -Schwachstellen und -Bedrohungen	1	SM 1.5 SM 5.2
DM.05	Systematische und kontinuierliche Behandlung von identifizierten Risiken und Schwachstellen inkl. Definition, Umsetzung und Pflege von detaillierten Behandlungsplänen	1	SM 1.6 SM 5.3
DM.06	Identifikation und Auswahl von technischen Sicherheitslösungen auf Basis von Risikoanalysen und nachgelagerten Kosten-Nutzen-Analysen	2	4.1.3A «Sichere Verbindungen»
DM.07	Erhebung, Dokumentation und Pflege eines Anforderungskatalogs mit detaillierten Sicherheitsanforderungen für das intelligente Messsystem	2	SM 3.1
Betriebliche Sicherheit			
DM.08	Definition, Etablierung und Pflege von Mitteln, Prozessen und Verfahren wie z. B. Konfigurationsmanagement, Release- und Change Management etc. für den sicheren Betrieb, Administration, Wartung und Support des intelligenten Messsystems	1	SM 1.3
DM.09	Aufbau und Pflege eines Inventars für die Komponenten und IKT-Systeme des intelligenten Messsystems	1	SM 3.2

[32] 1: Sicherheitsmassnahmen mit direktem Einfluss auf den sicheren Betrieb des intelligenten Messsystems
2: Sicherheitsmassnahmen mit indirektem Einfluss auf den sicheren Betrieb des intelligenten Messsystems

[33] Verweis auf Publikation Enisa, Ref. [13], durch ***SM X.Y***; Verweis auf Mindestanforderungen 4.1.3A, 4.1.3B und 4.1.3D durch ***4.1.3A, 4.1.3B, 4.1.3D***; Verweis auf Publikation Oesterreichs Energie, Ref. [4], durch ***E2E***

Ref.	Sicherheitsmassnahme	Kategorisierung [32]	Verweis [33]
DM.10	Definition, Verteilung und Pflege von sicheren Basis-Konfigurationen (Security Baselines) für die Komponenten und IKT-Systeme des intelligenten Messsystems	1	SM 3.3
DM.11	Sicherstellung einer manipulationssicheren Konfiguration wie z. B. nur autorisierte Änderung der Systemzeit	1	Keine
DM.12	Verifikation und Durchführung von regelmässigen Software- und Firmware-Updates auf Komponenten und IKT-Systemen des intelligenten Messsystems inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	1	SM 3.5
DM.13	Durchführung der routine- und ausserplanmässigen Wartung von Komponenten und IKT-Systemen des intelligenten Messsystems inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	1	SM 3.4
DM.14	Etablierung und Pflege eines Malwareschutzes auf IKT-Systemen des intelligenten Messsystems inkl. Definition, Etablierung und Pflege von entsprechenden Prozessen und Verfahren	1	SM 9.5
DM.15	Sicherer Umgang mit Speichermedien und Komponenten mit Speichermedien des intelligenten Messsystems inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	1	SM 9.6
DM.16	Bereitstellung und Schutz von notwendigen Ressourcen und Kapazitäten für den sicheren Betrieb des intelligenten Messsystems	1	Keine
DM.17	Sichere In- und Ausserbetriebnahme sowie Entsorgung von Komponenten und IKT-Systemen des intelligenten Messsystems inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	1	SM 3.6
DM.18	Härtung sowie stabiler und resistenter Aufbau von Komponenten und IKT-Systemen des intelligenten Messsystems gegen Angriffe	1	Keine
DM.19	Bereitstellung und Pflege der notwendigen Dokumentation für den sicheren Einsatz und Betrieb des intelligenten Messsystems	1	Keine
DM.20	Implementierung und Pflege von technischen Schutzmechanismen zur Gewährleistung der Vertraulichkeit und Integrität von Daten und Funktionen des Intelligenten Messsystems bei Ausfällen, Fehlern und Fehlhandlungen sowie bei nicht vorhergesehenen Betriebszuständen	1	E2E (Fail-secure)
Sicherheitsaudits			
DM.21	Durchführung von regelmässigen Sicherheitsaudits (z. B. Penetration Testing) zur Überprüfung der Sicherheit von Komponenten und IKT-Systemen des intelligenten Messsystems inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	2	SM 3.7

Ref.	Sicherheitsmassnahme	Kategorisierung [32]	Verweis [33]
Sicherheit des Personals			
DM.22	Durchführung von Sicherheitsüberprüfungen für das interne und externe Personal abhängig vom Aufgaben- und Verantwortungsgebiet	1	SM 4.1
DM.23	Definition, Etablierung und Pflege von geeigneten Prozessen und Verfahren zur Regelung von Ein-, Über- und Austritten von internem und externem Personal	1	SM 4.2
DM.24	Definition, Etablierung und Pflege eines organisationsweiten Sensibilisierungsprogramms zur Förderung des Sicherheitsbewusstseins bei internem und externem Personal sowie bei Prosumern	1	SM 4.3
DM.25	Definition, Etablierung und Pflege eines organisationsweiten Programms zwecks Sicherheitstraining und -Zertifizierung vom Personal abhängig vom Aufgaben- und Verantwortungsgebiet	1	SM 4.4
Incident Management, Logging, Monitoring und Auditierung			
DM.26	Definition, Etablierung und Pflege eines organisationsweiten Incident-Management Prozesses für die Behandlung von Sicherheitsvorfällen in Bezug auf das intelligente Messsystem	1	SM 5.1
DM.27	Etablierung und Pflege von Kontakten zu relevanten Behörden oder Interessengruppen wie z. B. MELANI zum Informationsaustausch in Bezug auf mögliche oder vorhandene Risiken, Schwachstellen und Bedrohungen bzgl. intelligenter Messsysteme	2	SM 5.4
DM.28	Aufzeichnung (Logging), Überwachung (Monitoring) und Auditierung (Auditing) von IKT-Sicherheitsrelevanten Ereignissen und -Vorfällen inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	1	SM 6.1 SM 6.2 SM 8.2
DM.29	Verhinderung, Erkennung und Protokollierung von - unautorisierten Aktionen (Setzen der Systemzeit, Einspielen von Software-/Firmware-Updates, Änderung von Messparametern etc.) - Funktionsstörungen und Fehlern - unautorisierten Zugriffen und Zugriffsversuchen - Manipulationen und Manipulationsversuchen wie z. B. eine physische Öffnung des Messgerätedeckels am intelligenten Messgerät	1	4.1.3D «Detektion und Verhinderung Missbr.»
Schutz der Daten			
DM.30	Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der System-, netz-, produktions-, oder verbrauchsrelevanten Daten innerhalb des intelligenten Messsystems inkl. Authentifizierungsdaten	1	4.1.3A «Sichere Verbindungen»
DM.31	Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der datenschutzrelevanten Daten innerhalb des intelligenten Messsystems gemäss den einschlägigen Bestimmungen des Datenschutzes	2	4.1.3B «Datenschutzgerechte Speicherung»

Ref.	Sicherheitsmassnahme	Kategorisierung [32]	Verweis [33]
DM.32	Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von erzeugten Protokollierungsinformationen innerhalb des intelligenten Messsystems	1	SM 6.3
Betriebskontinuität			
DM.33	Sicherstellung der Kontinuität des Betriebes in Bezug auf das intelligente Messsystem bei oder nach einem schwerwiegenden Vorfall inkl. Etablierung und Pflege von entsprechenden Mitteln, Prozessen, Verfahren und Organisationsstrukturen	1	SM 7.1
DM.34	Etablierung, Pflege und Test von Notfall-/Krisen-Kommunikationsservices, die bei einem schwerwiegenden Vorfall zum Einsatz kommen, um die notwendigen Kommunikationslinks und -Verbindungen mit eigenem Notfallpersonal, mit den Einsatzkräften von Partner-Unternehmen, mit externen Notfallorganisationen sowie mit wesentlichen Steuerungssystemen aufrechtzuerhalten.	1	SM 7.2
Physische und logische Zugangskontrolle			
DM.35	Etablierung und Pflege von Sicherheitsmassnahmen zur Gewährleistung der physischen Sicherheit von Komponenten und IKT-Systemen des intelligenten Messsystems	1	SM 8.1 SM 8.3
DM.36	Implementierung und Pflege von sicheren Authentifizierungs- und Autorisierungsmechanismen wie z. B. Passwortschutz zum Schutz der Informationen, Daten und Schnittstellen des intelligenten Messsystems	1	SM 9.1
DM.37	Sicherung aller Schnittstellen des intelligenten Messsystems inkl. Admin-Schnittstellen für Wartung und Support, Kundenschnittstellen und weiteren Schnittstellen zur Datenübertragung und -Kommunikation	1	Keine
DM.38	Sichere Administration des intelligenten Messsystems unter Beachtung von geltenden Gesetzen, Vorschriften und Verträgen wie z.B. eichrechtlicher und datenschutzrechtlicher Vorgaben	1	4.1.3A «Sichere Verbindungen»
DM.39	Implementierung einer rollenbasierten Zugangskontrolle zum Schutz vor unbefugten Zugriffen auf logische und physische Ressourcen des intelligenten Messsystems inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	1	SM 9.3
DM.40	Sicheres Management von Benutzer-, Gruppen-, Administratoren- und Systemkonten in Bezug auf das intelligente Messsystem inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	1	SM 9.2
DM.41	Etablierung und Pflege sicherer Fernzugriffslösungen auf Komponenten und IKT-Systeme des intelligenten Messsystems inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	1	SM 9.4

Ref.	Sicherheitsmassnahme	Kategorisierung [32]	Verweis [33]
Kommunikations- und Netzwerksicherheit			
DM.42	Sicherung der Datenübermittlung und -Kommunikation zwischen den Komponenten und IKT-Systemen des intelligenten Messsystems (z. B. zwischen dem intelligenten Messgerät und einem zentralen Zähldatenverarbeitungssystem)	1	SM 10.2 4.1.3A «Sichere Verbindungen»
DM.43	Sicherung der Datenübermittlung und -Kommunikation des intelligenten Messsystems zu den Komponenten und IKT-Systemen ausserhalb des intelligenten Messsystems, so z. B. Mengenmessgeräte für andere Energieträger als Strom (Gas-, Warmwasserzähler) oder Zähler für erneuerbare Energieanlagen	1	4.1.3A «Sichere Verbindungen»
DM.44	Etablierung und Pflege netzwerktechnischer Trennung/Isolierung für die Komponenten und IKT-Systeme des intelligenten Messsystems	1	SM 10.1
DM.45	Schutz und Verifikation der Authentizität und Integrität von übermittelten Daten inkl. Software-/Firmware-Updates an internen und externen Datenschnittstellen des intelligenten Messsystems	1	E2E (Datenintegrität)
DM.46	Implementierung und Pflege von technischen Schutzmechanismen zur Erkennung von Replay-Angriffen an jeglichen Datenschnittstellen des intelligenten Messsystems	1	E2E (Datenintegrität)
Externe Dienstleister			
DM.47	Etablierung und Pflege von Sicherheitsvereinbarungen mit externen Zulieferern, Auftragnehmern und Dienstleistungsanbietern, so dass die sichere Handhabung von sensiblen Daten und Informationen durch diese verbindlich geregelt ist und sie bezüglich IKT-Sicherheit sensibilisiert werden.	2	SM 2.1
DM.48	Überwachung der Einhaltung von Vereinbarungen durch externe Zulieferer, Auftragnehmer und Dienstleistungsanbieter inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	2	SM 2.2
Kryptografie			
DM.49	Einsatz von sicheren kryptografischen Algorithmen und Verfahren zur Gewährleistung von Vertraulichkeit, Integrität und Authentizität nach aktuellem Stand der Technik.	1	E2E
DM.50	Schutz von eingesetzten kryptografischen Algorithmen und Verfahren gegen Manipulation und Verlust	1	E2E
DM.51	Schutz vom eingesetzten, kryptografischen Schlüsselmaterial gegen Offenlegung, Entwendung, Manipulation und Verlust	1	E2E

Tabelle 10: Sicherheitsmassnahmen für Datenmanager

6.2. Massnahmen für Prosumer

Tabelle 11 stellt die an Prosumer adressierten Massnahmenvorschläge dar. Es wird angenommen, dass ein Prosumer nur Zugriff auf die Online-Visualisierungsplattform und physischen Zugang zum intelligenten Messgerät besitzt.

Ref.	Sicherheitsmassnahme	Kategorisierung [34]	Verweis[35]
P.01	Wahl starker Passwörter für den Kundenzugang auf die Online-Visualisierungsplattform	2	Keine
P.02	Absicherung von eigenen Netzwerken und -Systemen	2	Keine
P.03	Malwareschutz auf eigenen Systemen	2	Keine
P.04	Verschluss der Zählerschranke gegen unautorisierten Zugang durch Dritte	1	Keine
P.05	Einsatz einer lokalen Ersatzstromversorgung gegen Stromausfälle	2	Keine

Tabelle 11: Sicherheitsmassnahmen für Prosumer

Die Massnahmen P.01, P02 und P.03 betreffen die Kern Risiko-Szenarien RS.07 und RS.14 bezüglich Online-Visualisierungsplattform. Die Massnahme P.04 ist mit Ausnahme von RS.02 und RS.04 (Grossflächiger Abrechnungsbetrug durch Datenmanager) sowie RS.07 und RS.14 für alle Kern Risiko-Szenarien relevant, unter der Voraussetzung, dass auch der Datenmanager physischen Zugang zum intelligenten Messgerät beim Prosumer hat. Die Massnahme P.05 dient zur Absicherung des Prosumers gegen Stromausfälle infolge von Risiko-Szenarien, die im Worst Case die Gefährdung der überregionalen Versorgungssicherheit zur Folge haben könnten, nämlich RS.05, RS.06, RS.07, RS.08, RS.09, RS.10 und RS.11.

[34] 1: Sicherheitsmassnahmen mit direktem Einfluss auf den sicheren Betrieb des intelligenten Messsystems
2: Sicherheitsmassnahmen mit indirektem Einfluss auf den sicheren Betrieb des intelligenten Messsystems

[35] Verweis auf Publikation Enisa, Ref. [13], durch ***SM X.Y***; Verweis auf Mindestanforderungen 4.1.3A, 4.1.3B und 4.1.3D durch ***4.1.3A, 4.1.3B, 4.1.3D***; Verweis auf Publikation Oesterreichs Energie, Ref. [4], durch ***E2E***

6.3. Massnahmen für externe Dienstleister

Externe Dienstleister betreffend intelligente Messsysteme sollten auch Sicherheitsmassnahmen implementieren, da die Sicherheit des intelligenten Messsystems indirekt von ihren Produkten und Dienstleistungen abhängt. Die Sicherheit sollte in den Produkten und Dienstleistungen als Qualitätsmerkmal einfliessen und kann für externe Dienstleister ein Wettbewerbsvorteil werden.

Ref.	Sicherheitsmassnahme	Kategorisierung [36]	Verweis [37]
ED.01	Etablierung, Pflege, Prüfung und ggf. Zertifizierung von sicherheitsrelevanten Prozessen zur Entwicklung und Produktion sowie zur Auslieferung, Installation, Inbetriebnahme, Wartung und Support in Bezug auf das intelligente Messsystem nach anerkannten Standards und/oder Sicherheitsprofilen	2	E2E
ED.02	Etablierung und Pflege eines geschützten Konfigurationsmanagements u. a. zur Verwaltung und Versionierung von Hard- und Softwarekonfigurationen sowie vom Software-/Firmware-Quellcode	2	E2E
ED.03	Etablierung und Pflege eines Fehlermelde- und Fehlerbehebungsprozesses u. a. zur Überwachung, Analyse, Meldung und Behandlung von Sicherheitsschwachstellen	2	E2E
ED.04	Durchführung von regelmässigen technischen Sicherheitsprüfungen (Security Testing) zur Überprüfung der Sicherheit von eigenen Produkten und Dienstleistungen inkl. Definition, Etablierung und Pflege von entsprechenden Mitteln, Prozessen und Verfahren	2	E2E
ED.05	Definition, Etablierung und Pflege eines organisationsweiten Sensibilisierungsprogramms zur Förderung des Sicherheitsbewusstseins bei internem und externem Personal	2	SM 4.3 E2E
ED.06	Definition, Etablierung und Pflege eines organisationsweiten Programms zwecks Sicherheitstraining und -Zertifizierung vom Personal abhängig vom Aufgaben- und Verantwortungsgebiet	2	SM 4.4 E2E

Tabelle 12: Sicherheitsmassnahmen für externe Dienstleister

Tabelle 12 umfasst eine minimale Menge von Sicherheitsmassnahmen für externe Dienstleister über alle Risiko-Szenarien und übergeordneten Schutzobjekte («Intelligentes Messgerät», «Kommunikationssystem», «Zählldatenverarbeitungssystem» und «Online-Visualisierungsplattform») des intelligenten Messsystems hinweg.

[36] 1: Sicherheitsmassnahmen mit direktem Einfluss auf den sicheren Betrieb des intelligenten Messsystems
2: Sicherheitsmassnahmen mit indirektem Einfluss auf den sicheren Betrieb des intelligenten Messsystems

[37] Verweis auf Publikation Enisa, Ref. [13], durch ***SM X.Y***; Verweis auf Mindestanforderungen 4.1.3A, 4.1.3B und 4.1.3D durch ***4.1.3A, 4.1.3B, 4.1.3D***; Verweis auf Publikation Oesterreichs Energie, Ref. [4], durch ***E2E***

7. Entwicklung konkreter IKT-Sicherheitsanforderungen basierend auf der Schutzbedarfsanalyse

7.1. Einführung

Die Studie «Ansätze zur Gewährleistung der IKT-Sicherheit von intelligenten Messsystemen bei Endverbrauchern» (siehe Ref. [10]) hat verschiedene Varianten zur Sicherheitsprüfung intelligenter Messsysteme aufgezeigt. Das Anliegen der in Ref. [10] dargelegten vier Varianten zur Sicherung von intelligenten Messsystemen gegen mögliche Bedrohungen ist, prüfbare Sicherheitsanforderungen zu entwickeln, die eine geeignete Detailtiefe aufweisen und bei einer Überprüfung reproduzierbare Ergebnisse ermöglichen.

In Abbildung 10 sind die wichtigen Prozessschritte zur Gewährleistung der Datensicherheit intelligenter Messsysteme aufgezeigt:

- Schutzbedarfsanalyse (durch den Bund, d.h. die hier vorliegende SBA)
- Definition Anforderungskatalog (durch die Branche)
- Validierung Sicherheitsanforderungen (durch Prüfstellen)
- Einführung intelligentes Messsystem (durch Datenmanager)

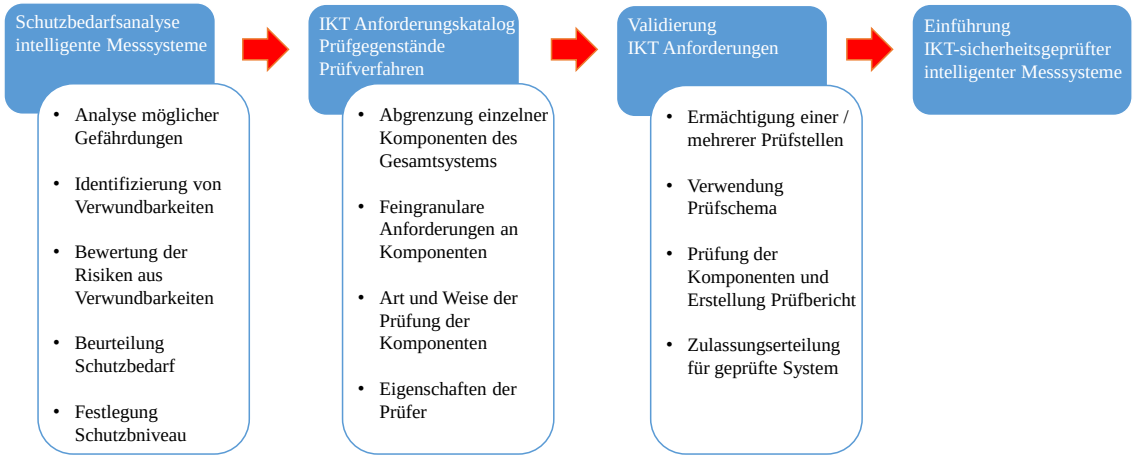


Abbildung 10: Wesentliche Prozessschritte zur Gewährleistung der Datensicherheit intelligenter Messsysteme beim Endverbraucher (Quelle: Ref. [10], Abbildung 8)

7.2. Vorgehen zur Entwicklung konkreter IKT-Sicherheitsanforderungen

Wie der Ablauf einer IKT-Sicherheitsvalidierung nach der in Ref. [10] favorisierte Variante 3 «Konformitätsprüfung mit zugrunde liegendem Schutzprofil» aussehen kann, stellt die Abbildung 11 anschaulich dar.

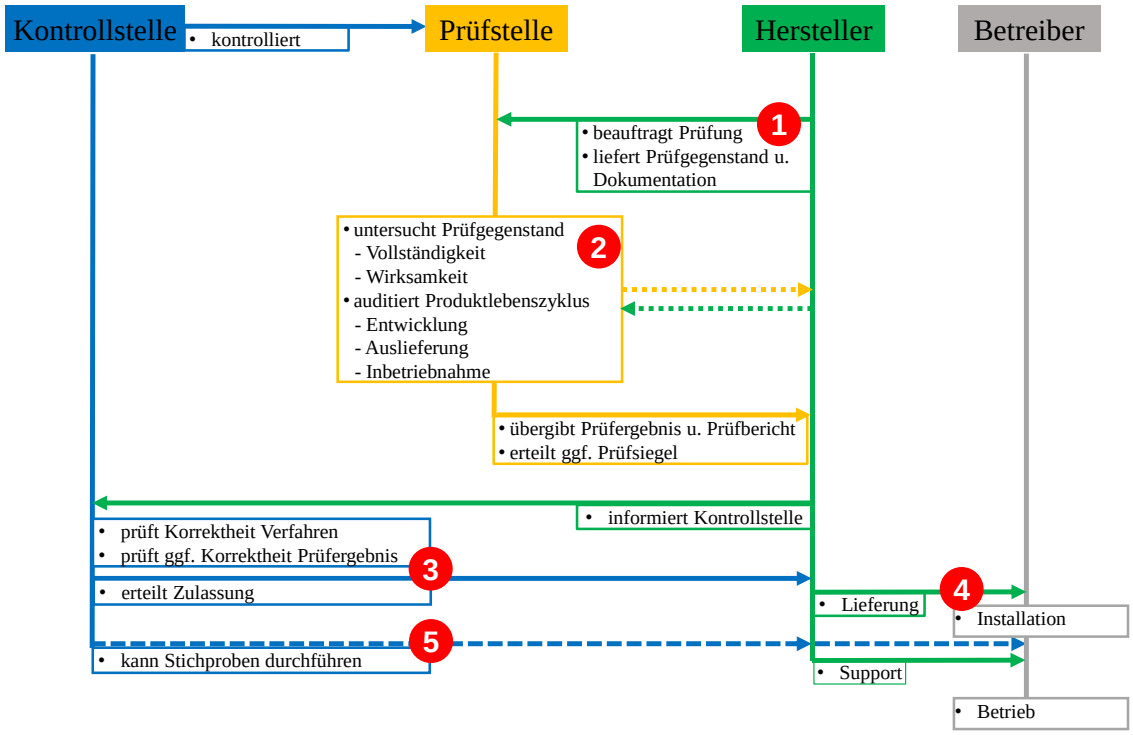


Abbildung 11: Ablauf der IKT Sicherheitsvalidierung (Quelle: Ref. [10], Abbildung 10)

Dieser Ablauf umfasst folgende Schritte (siehe folgenden Auszug aus Ref. [10]):

Schritt 1: Prüfauftrag durch Hersteller und Produkt an Prüfstelle
Eine akkreditierte Prüfstelle wird vom Hersteller (oder z.B. vom Betreiber, der als „Sponsor" für die Kostenübername der Prüfung auftritt) beauftragt, ein intelligentes Messsystem hinsichtlich IKT-Sicherheit und auf Basis des bekannten Anforderungskataloges zu untersuchen.

Schritt 2: Produkt an Prüfstelle
Die Prüfschritte, die im Prüfschema für die einzelnen Prüfgegenstände aufgeführt sind, werden Schritt für Schritt ausgeführt und die im Anforderungskatalog definierten Sicherheitsfunktionalitäten überprüft. Die Prüfstelle ermittelt so die Vollständigkeit und Wirksamkeit der Sicherheitsfunktionalitäten. Zudem auditiert die Prüfstelle den Produktlebenszyklus dahingehend, dass sie die Entwicklung, Auslieferung und Inbetriebnahme soweit möglich überprüft. Die Prüfstelle übermittelt nach Abschluss der Prüfung das Prüfergebnis in Form eines Prüfberichtes an den Hersteller.

Schritt 3: Prüfung durch Kontrollstelle und Zulassungsermächtigung
Die Kontrollstelle vergibt nach Bewertung des Verfahrens resp. des Prüfberichts eine produktgebundene Zulassung zum Betrieb – eine sogenannte Zulassungsermächtigung – inklusive Zulassungszeichen.

Schritt 4: Produktlieferung und Inbetriebnahme
Der Hersteller liefert ein von der Kontrollstelle zugelassenes Produkt an den Betreiber, der eine Installation in seine Betriebsumgebung gemäss der vom Hersteller dokumentierten und von der Prüfstelle geprüften sicherheitsrelevanten Vorgaben hierzu vornimmt.

Schritt 5: Monitoring des Betriebs und Stichproben
Im weiteren Verlauf des Lebenszyklus der zugelassenen Produkte, aber nicht als Bestandteil der Prüfschemata, kann die Kontrollstelle Stichproben an markteingeführten Produkten sowohl beim Hersteller vor Ort als auch bei installierten Produkten bzw. implementierten Anwendungen (beim Betreiber, bzw. bei den installierten Geräten vor Ort beim Endverbraucher) aus begründetem Anlass durchführen.

In der Detailbetrachtung der Studie (Ref. [10]) stellen sich folgende Erkenntnisse als wesentlich dar:

- Es handelt sich um einen stark Hersteller- und Produktorientierten Ansatz. Daher ist dieser Ansatz zwar aus Produktsicht wesentlich und unbedingt sinnvoll. Aus der Sicht der vorliegenden Analyse greift eine alleinige Produktsicherheit jedoch zu kurz vor dem Hintergrund der identifizierten Bedrohungen und Risiko-Szenarien.
- Der Produkt-Lebenszyklus beim Datenmanager von der Entwicklung/Projektierung über den Betrieb bis zur Ausserbetriebnahme und Entsorgung wird nicht berücksichtigt. Die Gewährleistung der integralen Systemsicherheit kann nur erfolgen, wenn neben der Herstellung und Auswahl von sicheren Produkten auch der Einsatz abgesichert ist.
- Ein intelligentes Messsystem gemäss Kapitel 3.3 umfasst neben Hard- und Software-Komponenten u. a. auch Daten, betriebliche Prozesse und -Abläufe, physische Zugangskontrollen sowie Personen (vgl. Kapitel 4.1). Die Gewährleistung der Sicherheit ist ein Prozess beim Datenmanager, der auch die Sicherheit des Produktes an sich umfasst.
- Die eingesetzten Hard- und Software-Produkte können Teil einer viel grösseren Infrastruktur inklusive z. B. Abrechnungssystemen und weiteren nachgelagerten Systemen sein, die nicht nur Komponenten eines intelligenten Messsystems umfassen, und u. U. bei externen Dienstleistern ausgelagert sind.

Basierend auf diesen Erkenntnissen wird das folgende, ganzheitliche Vorgehen zur Entwicklung konkreter IKT-Sicherheitsanforderungen durch die Branche empfohlen, das nicht nur die Produktsicherheit sondern die integrale Systemsicherheit inkl. betrieblicher Prozesse und -Abläufe berücksichtigt (vgl. Abbildung 12):

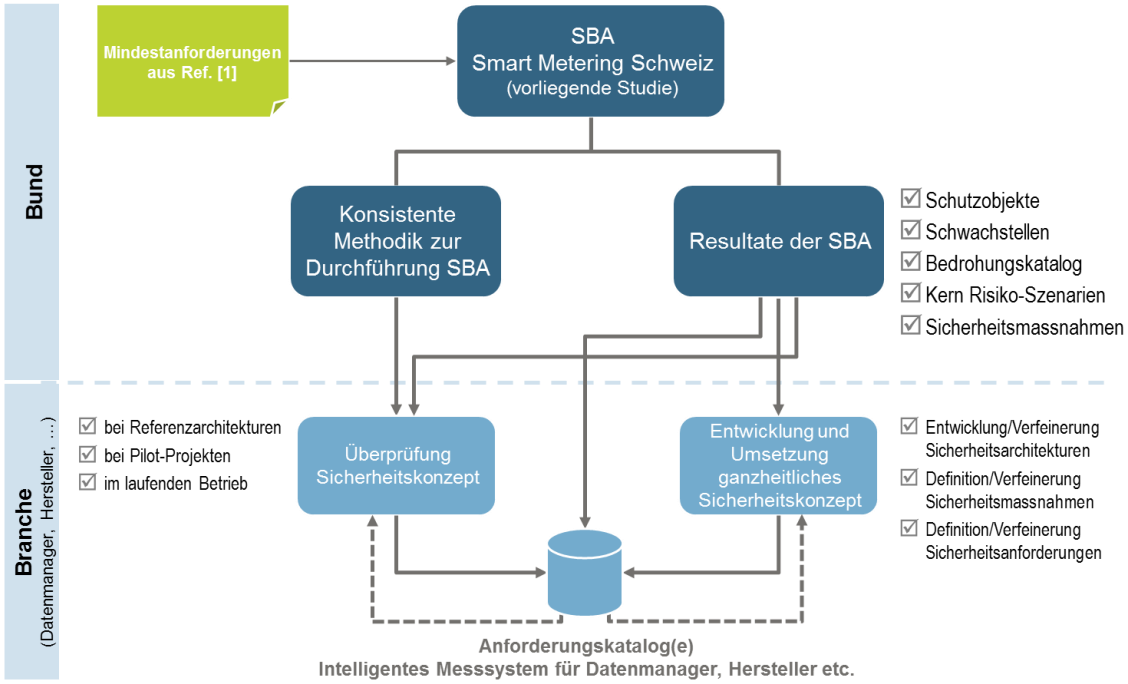


Abbildung 12: Vorgehen zur Entwicklung konkreter IKT-Sicherheitsanforderungen für intelligente Messsysteme

Die vorliegende SBA bildet zusammen mit der eingeführten konsistenten und ganzheitlichen Methodik gemäss Kapitel 2 und den enthaltenen Resultaten die entscheidende

Grundlage für die Entwicklung konkreter, detaillierter und vor allem umfassender sowie angemessener IKT-Sicherheitsanforderungen.

Die Entwicklung konkreter IKT-Sicherheitsanforderungen erfolgt durch die Branche (Messdienstleister/Messstellenbetreiber, Hersteller intelligenter Messgeräte, Branchenverbände sowie weitere betroffene und interessierte Parteien) mittels der beiden unerlässlichen und massgebenden Eckpfeiler «Entwicklung und Umsetzung ganzheitliches Sicherheitskonzept» und «Überprüfung Sicherheitskonzept».

Der Eckpfeiler «Entwicklung und Umsetzung ganzheitliches Sicherheitskonzept» definiert, wie das intelligente Messsystem umfassend abgesichert werden kann und beinhaltet die Definition, Entwicklung, Verfeinerung, Umsetzung und Pflege der entsprechenden Sicherheitsanforderungen, -architekturen und -massnahmen.

Der Eckpfeiler «Überprüfung Sicherheitskonzept» fordert eine regelmässige Überprüfung des umgesetzten Sicherheitskonzepts inkl. der Sicherheitsanforderungen für das intelligente Messsystem sowohl in der Entwicklung/Projektierung als auch im laufenden Betrieb. Es ist von grosser Bedeutung, dass die Ergebnisse aus diesen Überprüfungen in das Sicherheitskonzept und Risikomanagement des intelligenten Messsystems einfliessen und eine wiederkehrende Interaktion zwischen den beiden Eckpfeilen «Entwicklung und Umsetzung ganzheitliches Sicherheitskonzept» und «Überprüfung Sicherheitskonzept» stattfindet.

Die Erstellung von Anforderungskatalogen ist ein kontinuierlicher, iterativer Prozess auf Basis der Resultate aus diesen beiden Eckpfeilern. Es ist erstrebenswert, für Datenmanager und externe Dienstleister (Hersteller intelligenter Messsysteme etc.) jeweils einen separaten, auf die jeweiligen Bedürfnisse abgeschnittenen Anforderungskatalog zu erstellen.

Auf der anderen Seite bilden die erzeugten Anforderungskataloge im Endeffekt eine fundamentale Basis für die Aufrechterhaltung und kontinuierliche Verbesserung der Eckpfeiler «Entwicklung und Umsetzung ganzheitliches Sicherheitskonzept» und «Überprüfung Sicherheitskonzept».

Die Detaillierungstiefe der Anforderungen bzw. Anforderungskataloge hängt sehr eng mit dem Detaillierungsgrad des Sicherheitskonzeptes zusammen. Die Erstellung des Sicherheitskonzeptes für das intelligente Messsystem sollte in Zusammenarbeit mit der Branche erfolgen. Daher müssen die erforderlichen IKT-Sicherheitsanforderungen sowie deren Tiefe mit der Branche und eventuellen Prüfstellen abgestimmt werden.

7.3. Weitere Erkenntnisse und Empfehlungen

Die in Ref. [10] diskutierten Varianten zur Validierung der IKT-Sicherheitsanforderungen bzw. zur Überprüfung des Sicherheitskonzeptes unterscheiden sich nach den Freiheitsgraden „Definitionstiefe der Sicherheitsanforderungen“ und „Validierung der Umsetzung von Sicherheitsanforderungen“ (siehe folgenden Auszug aus Ref. [10]):

Variante 1: Externer Penetrationstest mit zugrunde liegendem Standard
Die IKT-Sicherheitsfunktionalitäten von Smart Metering Systemen werden durch externe Penetrationstests nicht ganzheitlich, d. h. nicht hinsichtlich Korrektheit und nicht hinsichtlich Reproduzierbarkeit der Ergebnisse untersucht. Sie werden lediglich auf ihre Wirksamkeit geprüft.

Variante 2: Konformitätsprüfung mit zugrunde liegendem Standard
Eine formale Konformitätsprüfung ist klar aufwendiger und damit kostenintensiver als individuell, also pro Betreiber, durchgeführte Penetrationstests. Dafür werden aber auch mehr Prüfaspekte bearbeitet, da sie in den entsprechend dafür entwickelten Prüfschemata vorgegeben werden. Letztlich sind Prüfkriterien und die Prüfschemata aus den verwendeten Standards pro Komponente abzuleiten.

Variante 3: Konformitätsprüfung mit zugrunde liegendem Schutzprofil
Variante 3 ist durch die Erarbeitung und Verwendung eines Schutzprofils geprägt. Ein solches Schutzprofil bietet gleichzeitig eine Standardkonformität sowie, basierend auf einer Schutzbedarfsanalyse, einen Kanon geeigneter, konkreten Gefährdungen entgegen stehender Schutzfunktionalitäten[38]. So wird sichergestellt, dass die Sicherheitsfunktionalitäten der Prüfgegenstände sachgerecht, umfassend und korrekt definiert wurden und über die reine Konformität auch ihre Wirksamkeit geprüft wird. Die Variante 3 ermöglicht – im Gegensatz zur Variante 4 – die Entwicklung spezifischer, speziell für die Schweiz geeigneter Lösungen und umfasst zudem Möglichkeiten für eine verhältnismässige Validierung einer korrekten und wirksamen Umsetzung der geforderten Sicherheitsfunktionalitäten.

Variante 4: IKT-Sicherheitszertifikat mit zugrunde liegendem Schutzprofil
Die Vorteile der Variante 3, vor allem die flexible Gestaltung und Anpassung des Schutzprofils sowie die Möglichkeit, ein angemessenes Prüfschema zu definieren, existieren in der Variante 4 nicht mehr. Für die Validierung stellt ein IKT-Sicherheitszertifikat gemäss CC[39] klar das stärkste verfügbare Instrument dar. Zwar gewährleistet die Variante eine hohe Sicherheit, ist aber statischer bzw. rigider als eine einfache Validierung der Sicherheitsfunktionalitäten alleine. Die Aufwände dieses umfassenden Systems zur Gewährleistung der Sicherheit erreichen schnell unverhältnismässige Dimensionen. Dies kann der Fall sein wenn z.B. Prüfschritte wiederholt werden müssen, ein Produkt erstmals geprüft werden soll oder ein Schutzprofil einseitig verabschiedet wird und sich danach herausstellt, dass die Anforderungen in der Praxis durch Betreiber wie Hersteller schwer realisierbar sind. Zudem werden Innovationen gebremst und der Stand der Technik kann nur schlecht in diesem Prozess aktualisiert werden.

Die in Ref. [10] favorisierte Variante 3 «Konformitätsprüfung mit zugrunde liegendem Schutzprofil» sowie die Variante 4 «IKT-Sicherheitszertifikat mit zugrunde liegendem Schutzprofil» sind für einen produktorientierten Ansatz sinnvoll und geeignet.

Dass gewisse IKT-Sicherheitsanforderungen produktspezifisch definiert und geprüft werden, ist durchaus sinn- und zweckvoll. Vor allem, wenn der jeweilige Prüfgegenstand vom Rest des Systems relativ klar abgegrenzt werden kann, wie dies z. B. beim intelligenten Messgerät der Fall ist. In Deutschland erfolgt beispielsweise die Überprüfung des Sicher-

[38] Anmerkung: Dabei muss nicht zwingend oder vollständig auf das Schutzprofil des deutschen Bundesamtes für Sicherheit in der Informationstechnik abgestellt werden.

[39] Common Criteria

heitskonzepts für die Kommunikationseinheit eines Messsystems[40] (dem sogenannten „Smart Meter Gateway“) gemäss Variante 4.

Ein produktorientierter Ansatz kann die Sicherheitsbedürfnisse, welche sich aus vorliegender SBA ableiten lassen, jedoch nur beschränkt abdecken, da ein intelligentes Messsystem gemäss Kapitel 3.3 neben Hard- und Software-Komponenten u. a. betriebliche Prozesse und Abläufe umfasst (vgl. Kapitel 4.1) und eine durchgängig klare Abgrenzung der Prüfgegenstände nur teilweise – wenn überhaupt – möglich sein wird. Aus diesem Grund muss nicht nur die Produktsicherheit sondern die integrale Systemsicherheit abdeckt werden. Dass die Überprüfung des Sicherheitskonzepts beim intelligenten Messsystem ausschliesslich nach der favorisierten Variante 3 stattfinden soll, ist daher nicht zielführend. Es muss eher von einer Kombination der Varianten ausgegangen werden (vgl. Tabelle 13).

Komponenten Intelligentes Messsystem Varianten aus Ref. [10]	Intelligentes Messgerät	Kommunikationssystem	Zähldatenverarbeitungssystem	Online-Visualisierungsplattform
Variante 1: Externer Penetrationstest mit zugrunde liegendem Standard	**Ergänzend**			
Variante 2: Konformitätsprüfung mit zugrunde liegendem Standard	Möglich	**Primär**	**Primär**	**Primär**
Variante 3: Konformitätsprüfung mit zugrunde liegendem Schutzprofil	**Primär**	Theoretisch möglich jedoch nicht verhältnismässig, da eine klare Abgrenzung der Prüfgegenstände nur beschränkt möglich und der Aufwand für die Umsetzung relativ hoch ist		
Variante 4: IKT-Sicherheitszertifikat mit zugrunde liegendem Schutzprofil	Möglich			

Tabelle 13: Zuordnung von Varianten aus Ref. [10] auf die Komponenten des intelligenten Messsystems zur Überprüfung des Sicherheitskonzeptes

Die Abgrenzung einzelner Komponenten des intelligenten Messsystems ist bereits durch den aktuellen Abstraktionsgrad gemäss Kapitel 3.3 gegeben. Für das intelligente Messgerät scheint die Variante 3 aufgrund ihrer Verhältnismässigkeit im Vergleich zur Variante 4 die passendere Variante zu sein, da das Messgerät relativ deutlich von den restlichen Komponenten abgegrenzt werden kann (vgl. Tabelle 13). Es ist durchaus möglich, dass die Schweiz Ihr eigenes Sicherheitsprofil zur Prüfung gemäss Variante 3 entwickeln wird. Es kann jedoch nicht ausgeschlossen werden, dass die Variante 4 durch deren Etablierung in Deutschland und eventuell in weiteren Ländern künftig auch in der Schweiz für die Überprüfung des Sicherheitskonzepts des intelligenten Messgeräts eingesetzt werden könnte. Der Einsatz der Variante 2 in Bezug auf das intelligente Messgerät wäre auch denkbar, da diese voraussichtlich verhältnismässig geringere Kosten gegenüber Varianten 3 und 4 verursachen wird.

Für die restlichen Komponenten bzw. das Kommunikationssystem, das Zähldatenverarbeitungssystem und die Online-Visualisierungsplattform ist eine klare Abgrenzung der

[40] Ein Messsystem im Sinne von § 21c des deutschen Energiewirtschaftsgesetztes EnWG ist eine in ein Kommunikationsnetz eingebundene Messeinrichtung zur Erfassung elektrischer Energie, das den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt.

Prüfgegenstände dagegen nur beschränkt möglich, u. a. aufgrund unterschiedlicher Realisierungen. Daher wird die Variante 2 «Konformitätsprüfung mit zugrunde liegendem Standard» z. B. zur Konformitätsprüfung für diese Komponenten gegen ISO 27001 als Variante mit der geforderten Flexibilität angesehen. Dieses Vorgehen wird auch in anderen Ländern wie z.B. Deutschland, Österreich, England und Holland entsprechend vorangetrieben und erscheint für intelligente Messsysteme in der Schweiz praktikabel sowie verhältnismässig. Der Aufwand für die Umsetzung der Variante 3 scheint dagegen für diese Komponenten nicht verhältnismässig zu sein.

Eine mögliche, vollständige Liberalisierung des Messwesens in der Schweiz würde eine höhere Komplexität, bedingt durch die höhere Anzahl Marktteilnehmer, mit sich bringen. Dadurch könnte eine Sicherheitszertifizierung der Marktteilnehmer und deren Infrastrukturen gemäss Variante 2 bedeutender werden. Dies könnte wiederum dazu führen, dass die Sicherheitszertifizierungen teuer und durch eventuelle Erhöhung der Prüfkriterien komplizierter werden und somit u. U. den Markt behindern könnten.

Die Variante 1 «Externer Penetrationstest mit zugrunde liegendem Standard» wird eher als ergänzend und optional zu den restlichen Varianten angesehen, da sie mit verhältnismässig geringerem Aufwand eine gezielte Überprüfung der Sicherheitsfunktionalitäten bzw. Eruierung der Verwundbarkeiten im Rahmen eines definierten Umfangs (jedoch ohne Garantie auf Vollständigkeit) unter Berücksichtigung der unternehmens- sowie applikationsspezifischen Voraussetzungen erlaubt.

Eine Validierung der Produkte in Zusammenhang mit intelligenten Messsystemen ist gesamthaft sinnvoll. Eine regulative Gestaltung mit Kontrollstellen gemäss Abbildung 11 bietet Vorteile ist aber regulativ intensiv. Die weiteren in Ref. [10] vorgeschlagenen Schritte gemäss Abbildung 10 sollten unter Einbezug der Resultate der vorliegenden SBA durch die Branche geprüft und angegangen werden.

Hinsichtlich etwaig notwendiger regulatorischer Grundlagen verbleibt zu prüfen, inwiefern neue Rahmenbedingungen geschaffen oder bestehende geändert oder ausgeweitet werden müssen, um einen umfassenden und angemessenen Grundschutz für intelligente Messsysteme zu gewährleisten. Angesichts der bedeutenden und tendenziell zunehmenden Risiken und Bedrohungen erscheinen regulatorische Anpassungen auf Bundes- oder Branchenebene sinnvoll, die den ganzheitlichen Grundschutz der intelligenten Messsysteme ins Auge fassen. Wichtig ist, dass etwaige regulatorische Rahmenbedingungen die Produkt- sowie die integrale Systemsicherheit der intelligenten Messsystem adressieren. Vor diesem Hintergrund gibt die frühere Studie zur IKT-Sicherheit intelligenter Messsysteme (Ref. [10]) eine austarierte, gute Möglichkeit vor, wie die Produktsicherheit zu gewährleisten ist, greift aber bei der integralen Systemsicherheit zu kurz, um einen angemessenen Grundschutz sicher zu stellen. Die Ergebnisse der vorliegenden Untersuchung unterstützen somit die aufgezeigte Lösung der früheren Studie, erweitern diese zudem mit erforderlichen Massnahmen, deren Umsetzung letztlich eine angemessene Systemsicherheit und damit einen notwendigen und vorhabenspezifischen Grundschutz intelligenter Messsysteme erlauben.

A. Anhang

A.1. Nachschlagewerk zu den Risiko-Szenarien

Dieses Kapitel enthält Informationen, die aufgrund ihres repetitiven Charakters nur bedingt für eine kontinuierliche Lektüre geeignet sind, jedoch für das Verständnis und die Nachvollziehbarkeit der Resultate dieser SBA eine wichtige Bedeutung haben.

Steckbriefe: Für jedes einzelne Kern Risiko-Szenario wurde ein eigener Steckbrief erstellt, mit dem Ziel, eine übersichtliche Darstellung zu erreichen. Die Steckbriefe umfassen die relevanten Bemerkungen und Annahmen sowie die Szenariovarianten und übergeordneten Schutzobjekte des intelligenten Messsystems, die für das jeweilige Kern Risiko-Szenario relevant sind.

Tabellen zur Aufschlüsselung auf relevante Ereignis- und Schadenskategorien: Eine weitere Tabelle zeigt die Aufschlüsselung des jeweiligen Kern Risiko-Szenarios bzw. dessen Varianten (nachfolgend «Risiko-Szenario») auf die relevanten Ereignis- und Schadenskategorien gemäss Kapitel 2, Arbeitsschritte 6) Aufschlüsselung auf Ereigniskategorien und 7) Aufschlüsselung auf Schadenskategorien.

Der Prosumer und Datenmanager wären von den möglichen negativen Folgen eines aufgetretenen Risiko-Szenarios unmittelbar betroffen und stellen daher die direkten Risikoträger in Bezug auf das intelligente Messsystem dar. Deshalb erfolgen die Aufschlüsselung auf verschiedene Schadenskategorien sowie die nachfolgende Beurteilung von verschiedenen Auswirkungen jeweils aus Sicht des Prosumers und Datenmanagers.

Falls eine Ereignis- oder Schadenskategorie eine Relevanz für das jeweilige Risiko-Szenario und die jeweilige Sicht (Prosumer/Datenmanager) aufweist, wird dies in der jeweiligen Zelle der Tabelle zur Aufschlüsselung auf relevante Ereignis- und Schadenskategorien mit einem „Ja“ vermerkt. Die leeren Zellen weisen auf eine Irrelevanz in diesem Zusammenhang hin und entsprechen einem „Nein“. Die letzte Kolonne der Tabelle «Vorsätzliche Handlungen» zeigt an, ob es sich beim jeweiligen Risiko-Szenario um mutmassliche Angriffe handelt.

Bei der Detailbetrachtung der Tabellen zur Aufschlüsselung auf relevante Ereignis- und Schadenskategorien kommt man zum Schluss, dass die Szenariovarianten keinen Einfluss auf die Aufschlüsselung auf Schadens- und Ereigniskategorien haben bzw. unabhängig von Schadens- und Ereigniskategorien sind.

A.1.1. Kern Risiko-Szenario RS.01

RS.01: Abrechnungsbetrug[41] mittels Manipulation der Tarifierung	
Bemerkungen	• Manipulation der Tarifierung umfasst die Manipulation der entsprechenden Daten (Meteringdaten, Tarifdaten betreffend Netz und Energie, Systemzeit etc.) und Prozesse • Unter Tarifierung ist die direkte Zuordnung von Preisen zu den Verbrauchs- und Erzeugungswerten zu verstehen. Dies ist technisch direkt im intelligenten Messgerät, oder aber erst im Zählldatenverarbeitungssystem möglich.
Annahmen	• Der geeichte, messtechnische Teil des intelligenten Messgerätes ist integer. • Tarifierung kann aber muss nicht im intelligenten Messgerät erfolgen. • Der Abrechnungsbetrug erfolgt zugunsten des Prosumers und der Datenmanager ist nicht am Abrechnungsbetrug beteiligt. • Eine missbräuchliche oder fehlerhafte Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet nicht statt. • Die Online-Visualisierungsplattform hat keinen Einfluss bzw. Zusammenhang auf/zur Tarifierung.
Szenario-varianten	• RS.01a: **Vereinzelter** Abrechnungsbetrug mittels Manipulation der Tarifierung durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf **einzelne** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zählldatenverarbeitungssystem • RS.01b: **Grossflächiger** Abrechnungsbetrug mittels Manipulation der Tarifierung durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf eine **Vielzahl** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zählldatenverarbeitungssystem
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem • Zählldatenverarbeitungssystem

Tabelle 14: Steckbrief für Kern Risiko-Szenario RS.01

[41] Betrug betreffend Bezug und/oder Einspeisung der elektrischen Energie

		Ereigniskategorien					Schadenskategorien						
		Sensitive Daten			IKT-Systeme & -Services								
Risiko-Szenario	Sicht betreffend Schadenskategorien	V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.01a	P		Ja		Ja			Ja[42]	Ja[43]				Ja
	DM						Ja	Ja	Ja[44]				
RS.01b	P		Ja		Ja			Ja[42]	Ja[43]				Ja
	DM						Ja	Ja	Ja[44]				

Tabelle 15:Aufschlüsselung RS.01 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität von Daten sowie IKT-Systemen und -Services in Bezug auf das intelligente Messsystem liegt im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse setzen meistens das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios.

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Finanzieller Verlust könnte für Prosumer zustande kommen, falls der Abrechnungsbetrug nicht zugunsten des Prosumers erfolgt.
- Compliance-Verletzungen könnten entstehen, falls der Prosumer am Abrechnungsbetrug beteiligt ist und dadurch Gesetze verletzt. Dies könnte auch einen finanziellen Verlust für den Prosumer zur Folge haben.
- Falls der Prosumer am Abrechnungsbetrug beteiligt ist, wäre der Reputationsverlust für ihn theoretisch nicht ausgeschlossen, aber man kann davon ausgehen, dass dies eher unwahrscheinlich ist und auch nicht in dem Ausmass sein wird, wie es beim Datenmanager der Fall wäre.

[42] Falls der Prosumer am Abrechnungsbetrug beteiligt ist.

[43] Unter der Annahme, dass der Abrechnungsbetrug nicht zugunsten des Prosumers erfolgt

[44] Unter der Annahme, dass der Abrechnungsbetrug nicht zugunsten des Datenmanagers erfolgt

Sicht einzelner Datenmanager (DM):

- Unter der Annahme, dass der Abrechnungsbetrug nicht zugunsten des Datenmanagers erfolgt, würden für Datenmanager finanzielle Verluste entstehen.
- Die Compliance-Verletzungen kämen dann auch zustande, falls durch den Abrechnungsbetrug bestimmte Auflagen aus Gesetzen etc. durch den Datenmanager nicht erfüllt werden könnten.
- Merklicher Reputationsverlust ist auch nicht ausgeschlossen, insbesondere wenn der Fall in den Medien erscheint.
- Bei einem grossflächigen Abrechnungsbetrug wären die erwähnten Auswirkungen entsprechend höher

A.1.2. Kern Risiko-Szenario RS.02

RS.02: Grossflächiger Abrechnungsbetrag durch Datenmanager mittels Manipulation der Tarifierung	
Bemerkungen	• Es handelt sich um einen Spezial-Fall vom RS.01. • Manipulation der Tarifierung umfasst die Manipulation der entsprechenden Daten (Meteringdaten, Tarifdaten betreffend Netz und Energie, Systemzeit etc.) und Prozesse. • Unter Tarifierung ist die direkte Zuordnung von Preisen zu den Verbrauchs- und Erzeugungswerten zu verstehen. Dies ist technisch direkt im intelligenten Messgerät, oder aber erst im Zähldatenverarbeitungssystem möglich.
Annahmen	• Der geeichte, messtechnische Teil des intelligenten Messgerätes ist integer. • Tarifierung kann, aber muss nicht im intelligenten Messgerät erfolgen. • Der Abrechnungsbetrag erfolgt zugunsten des Datenmanagers und der Prosumer ist nicht am Abrechnungsbetrag beteiligt. • Eine missbräuchliche Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet durch den Datenmanager statt. • Die Online-Visualisierungsplattform hat keinen Einfluss bzw. Zusammenhang auf/zur Tarifierung.
Szenario-varianten	• RS.02: **Grossflächiger** Abrechnungsbetrag durch den Datenmanager mittels Manipulation der Tarifierung zu seinen Gunsten abhängig vom individuellen Lastprofil von Prosumern, welche immer dann – höhere Preise zahlen, wenn sie Strom verbrauchen und/oder – tiefere Preise bekommen, wenn sie Strom einspeisen
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem • Zähldatenverarbeitungssystem

Tabelle 16: Steckbrief für Kern Risiko-Szenario RS.02

		Ereigniskategorien					Schadenskategorien						
		Sensitive Daten			IKT-Systeme & -Services								
Risiko-Szenario	Sicht betreffend Auswirkungen	V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.02	P		Ja		Ja				Ja		Ja		Ja
	DM						Ja	Ja	Ja				

Tabelle 17: Aufschlüsselung RS.02 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität von Daten sowie IKT-Systemen und -Services in Bezug auf das intelligente Messsystem liegt im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse setzen meistens das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios.

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Durch den Abrechnungsbetrug würde für Prosumer ein finanzieller Verlust entstehen.
- Eine missbräuchliche Bearbeitung von Personendaten, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, könnte Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge haben.

Sicht einzelner Datenmanager (DM):

- Durch den Betrug kämen Compliance-Verletzungen zustande, die im Endeffekt durch Gerichtsverfahren o.ä. mit finanziellem Verlust und Reputationsverlust verbunden sind.
- Bei grossflächigem Abrechnungsbetrug wären die erwähnten Auswirkungen entsprechend höher.

A.1.3. Kern Risiko-Szenario RS.03

RS.03: Abrechnungsbetrug mittels Manipulation des geeichten, messtechnischen Teils des intelligenten Messgerätes inkl. entsprechender Messparameter	
Bemerkungen	• Manipulation der Tarifierung umfasst die Manipulation der entsprechenden Daten (Meteringdaten, Tarifdaten betreffend Netz und Energie, Systemzeit etc.) und Prozesse. • Unter Tarifierung ist die direkte Zuordnung von Preisen zu den Verbrauchs- und Erzeugungswerten zu verstehen. Dies ist technisch direkt im intelligenten Messgerät, oder aber erst im Zähldatenverarbeitungssystem möglich.
Annahmen	• Der geeichte, messtechnische Teil des intelligenten Messgerätes ist durch den Einsatz von IKT z. B. durch Reprogrammierung manipulierbar. • Tarifierung kann, aber muss nicht im intelligenten Messgerät erfolgen. • Der Abrechnungsbetrug erfolgt zugunsten des Prosumers und der Datenmanager ist nicht am Abrechnungsbetrug beteiligt. • Eine missbräuchliche oder fehlerhafte Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet nicht statt. • Die Online-Visualisierungsplattform hat keinen Einfluss bzw. Zusammenhang auf/zur Tarifierung.
Szenario-varianten	• RS.03a: **Vereinzelter** Abrechnungsbetrug mittels Manipulation des geeichten, messtechnischen Teils des intelligenten Messgerätes durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf **einzelne** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.03b: **Grossflächiger** Abrechnungsbetrug mittels Manipulation des geeichten, messtechnischen Teils des intelligenten Messgerätes durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf eine **Vielzahl** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem • Zähldatenverarbeitungssystem

Tabelle 18: Steckbrief für Kern Risiko-Szenario RS.03

		Ereigniskategorien					Schadenskategorien						
		Sensitive Daten			IKT-Systeme & -Services								
Risiko-Szenario	Sicht betreffend Auswirkungen	V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.03a	P		Ja		Ja			Ja[45]	Ja[46]				Ja
	DM						Ja	Ja	Ja[47]				
RS.03b	P		Ja		Ja			Ja[45]	Ja[46]				Ja
	DM						Ja	Ja	Ja[47]				

Tabelle 19: Aufschlüsselung RS.03 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität von Daten sowie IKT-Systemen und -Services in Bezug auf das intelligente Messsystem liegt im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse setzen meistens das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios

Kommentar zu den relevanten Schadenskategorien:

Sicht einzelner Prosumer (P):

- Finanzieller Verlust könnte für Prosumer zustande kommen, falls der Abrechnungsbetrug nicht zugunsten des Prosumers erfolgt.
- Compliance-Verletzungen könnten entstehen, falls der Prosumer am Abrechnungsbetrug beteiligt ist und dadurch Gesetze verletzt. Dies könnte auch einen finanziellen Verlust für den Prosumer zur Folge haben.
- Falls der Prosumer am Abrechnungsbetrug beteiligt ist, wäre der Reputationsverlust für ihn theoretisch nicht ausgeschlossen, aber man kann davon ausgehen, dass dies eher unwahrscheinlich ist und auch nicht in dem Ausmass sein wird, wie es beim Datenmanager der Fall wäre.

[45] Falls der Prosumer am Abrechnungsbetrug beteiligt ist.

[46] Unter der Annahme, dass der Abrechnungsbetrug nicht zugunsten des Prosumers erfolgt

[47] Unter der Annahme, dass der Abrechnungsbetrug nicht zugunsten des Datenmanagers erfolgt

Sicht einzelner Datenmanager (DM):

- Unter der Annahme, dass der Abrechnungsbetrug nicht zugunsten des Datenmanagers erfolgt, würden für Datenmanager finanzielle Verluste entstehen.
- Die Compliance-Verletzungen kämen dann auch zustande, falls durch den Abrechnungsbetrug bestimmte Auflagen aus Gesetzen etc. durch den Datenmanager nicht erfüllt werden könnten.
- Merklicher Reputationsverlust ist auch nicht ausgeschlossen, insbesondere wenn der Fall in den Medien erscheint.
- Bei einem grossflächigen Abrechnungsbetrug wären die erwähnten Auswirkungen entsprechend höher.

A.1.4. Kern Risiko-Szenario RS.04

RS.04: Grossflächiger Abrechnungsbetrag durch Datenmanager mittels Manipulation des geeichten, messtechnischen Teils der intelligenten Messgeräte	
Bemerkungen	• Es handelt sich um einen Spezial-Fall vom RS.03. • Manipulation der Tarifierung umfasst die Manipulation der entsprechenden Daten (Meteringdaten, Tarifdaten betreffend Netz und Energie, Systemzeit etc.) und Prozesse. • Unter Tarifierung ist die direkte Zuordnung von Preisen zu den Verbrauchs- und Erzeugungswerten zu verstehen. Dies ist technisch direkt im intelligenten Messgerät, oder aber erst im Zähldatenverarbeitungssystem möglich.
Annahmen	• Der geeichte, messtechnische Teil des intelligenten Messgerätes ist durch den Einsatz von IKT z. B. durch Reprogrammierung manipulierbar. • Tarifierung kann, aber muss nicht im intelligenten Messgerät erfolgen. • Der Abrechnungsbetrag erfolgt zugunsten des Datenmanagers und der Prosumer ist nicht am Abrechnungsbetrag beteiligt. • Eine missbräuchliche Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet durch den Datenmanager statt. • Die Online-Visualisierungsplattform hat keinen Einfluss bzw. Zusammenhang auf/zur Tarifierung.
Szenario-varianten	• RS.04: **Grossflächiger** Abrechnungsbetrag durch den Datenmanager mittels Manipulation des geeichten, messtechnischen Teils des intelligenten Messgerätes bei einer Vielzahl von intelligenten Messgeräten.
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem • Zähldatenverarbeitungssystem

Tabelle 20: Steckbrief für Kern Risiko-Szenario RS.04

		Ereigniskategorien					Schadenskategorien						
Risiko-Szenario	Sicht betreffend Auswirkungen	Sensitive Daten			IKT-Systeme & -Services		Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
		V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit							
RS.04	P		Ja		Ja				Ja		Ja		Ja
	DM						Ja	Ja	Ja				

Tabelle 21: Aufschlüsselung RS.04 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität von Daten sowie IKT-Systemen und -Services in Bezug auf das intelligente Messsystem liegt im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse setzen meistens das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios.

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Durch den Abrechnungsbetrug würde für Prosumer ein finanzieller Verlust entstehen.
- Eine missbräuchliche Bearbeitung von Personendaten, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, könnte Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge haben.

Sicht einzelner Datenmanager (DM):

- Durch den Betrug kämen Compliance-Verletzungen zustande, die im Endeffekt durch Gerichtsverfahren o.ä. mit finanziellem Verlust und Reputationsverlust verbunden sind.
- Bei grossflächigem Abrechnungsbetrug wären die erwähnten Auswirkungen entsprechend höher.

A.1.5. Kern Risiko-Szenario RS.05

RS.05: Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten und entsprechender Daten und Datenübertragung	
Bemerkungen	• Das Risiko-Szenario umfasst auch – den Missbrauch von Systemressourcen wie z. B. Rechenleistung oder Übertragungsleitungen und -Verbindungen zur Kommunikation – Daten und Datenübertragung zwecks Stromabrechnung, Netzüberwachung, Laststeuerung etc. • Durch dieses Szenario werden u. a. auch die Vollständigkeit der Daten und die korrekte Funktionsweise des intelligenten Messsystems gefährdet.
Annahmen	• Eine missbräuchliche oder fehlerhafte Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet nicht statt.
Szenario-varianten	• RS.05a: **Punktuelle** Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf **einzelne** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.05b: **Grossflächige** Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf eine **Vielzahl** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.05c: **Grossflächige** Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten **durch höhere Gewalt**
	• RS.05d: **Grossflächige** Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten **durch technisches Versagen**
	• RS.05e: **Grossflächige** Einschränkung der Verfügbarkeit von intelligenten Messgeräten und Integrität **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem

Tabelle 22: Steckbrief für Kern Risiko-Szenario RS.05

		Ereigniskategorien					Schadenskategorien						
		Sensitive Daten			IKT-Systeme & -Services								
Risiko-Szenario	Sicht betreffend Auswirkungen	V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlich-keitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.05a	P		Ja	Ja	Ja	Ja			Ja	Ja			Ja
	DM						Ja	Ja	Ja	Ja			
RS.05b	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	Ja
	DM						Ja	Ja	Ja	Ja		Ja	
RS.05c	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.05d	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.05e	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	

Tabelle 23: Aufschlüsselung RS.05 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität und Verfügbarkeit von Daten sowie IKT-Systemen und -Services in Bezug auf intelligente Messgeräte liegen im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse (solange sie vorsätzlich erfolgen) setzen meistens das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios.

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Finanzieller Verlust könnte für Prosumer entstehen, falls es zu Sach- oder Personenschaden kommt oder der Bezug und/oder die Einspeisung der elektrischen Energie durch falsche oder fehlende Informationen zuungunsten des Prosumers beeinflusst werden.
- Es kann nicht ausgeschlossen werden, dass Leib und Leben auf Seite Prosumer gefährdet wird und es sogar zu Todesfällen kommen kann.

Sicht einzelner Datenmanager (DM):

- Finanzielle Verluste für Datenmanager könnten durch Schäden an Betriebsmitteln und/oder -Personal sowie an Prosumern oder Dritten aber auch als Folge von Compliance-Verletzungen entstehen.
- Compliance-Verletzungen kämen auch zustande, falls bestimmte Auflagen aus Gesetzen etc. durch den Datenmanager nicht erfüllt werden könnten.
- Es kann nicht ausgeschlossen werden, dass Leib und Leben von Prosumern, von Betriebs-, Wartungs- und Support-Personal oder von Dritten gefährdet werden könnte. Selbst Todesfälle könnten eine Folge sein. Die Gefährdung von Leib und Leben hängt u. a. auch von der Grösse des Vorfalls ab (Beispiel: der Verkehr ist aufgrund eines Stromausfalls nicht mehr geregelt). Es wird hier vom Worst Case ausgegangen.
- Ein merklicher Reputationsverlust wäre auch nicht ausgeschlossen, insbesondere wenn der Fall in den Medien erscheint. Bei höherer Gewalt kann jedoch davon ausgegangen werden, dass die Folgen von Vorfällen mit Sach- und Personenschäden bei der Bevölkerung eher leichter akzeptiert werden und daher der Reputationsverlust voraussichtlich tiefer wird.
- Bei einem grossflächigen (überregionalen) Vorfall wären die erwähnten Auswirkungen entsprechend höher und die überregionale Versorgungssicherheit könnte im schlimmsten Fall gefährdet werden.

A.1.6. Kern Risiko-Szenario RS.06

RS.06: Schwerwiegende Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems	
Bemerkungen	• Das Risiko-Szenario umfasst auch – den Missbrauch von Systemressourcen wie z. B. Rechenleistung oder Übertragungsleitungen und -Verbindungen zur Kommunikation – Daten und Datenübertragung zwecks Stromabrechnung, Netzüberwachung, Laststeuerung etc. • Durch dieses Szenario werden u. a. auch die Vollständigkeit der Daten und die korrekte Funktionsweise des Zähldatenverarbeitungssystems gefährdet.
Annahmen	• Eine missbräuchliche oder fehlerhafte Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet nicht statt.
Szenario-varianten	• RS.06a: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems (ZDVS) und der zusammenhängenden Daten und Funktionalitäten zwecks Zählermanagement etc. durch Angriffe (Eindringen) **vor Ort** und/oder **aus der Ferne** auf ZDVS bzw. auf dessen Systemkomponenten und Schnittstellen
	• RS.06b: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems und der zusammenhängenden Daten und Funktionalitäten **durch höhere Gewalt**
	• RS.06c: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems und der zusammenhängenden Daten und Funktionalitäten **durch technisches Versagen**
	• RS.06d: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems und der zusammenhängenden Daten und Funktionalitäten **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Zähldatenverarbeitungssystem

Tabelle 24: Steckbrief für Kern Risiko-Szenario RS.06

		Ereigniskategorien					Schadenskategorien						
Risiko-Szenario	Sicht betreffend Auswirkungen	Sensitive Daten			IKT-Systeme & -Services								
		V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.06a	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	Ja
	DM						Ja	Ja	Ja	Ja		Ja	
RS.06b	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.06c	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.06d	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	

Tabelle 25: Aufschlüsselung RS.06 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität und Verfügbarkeit von Daten sowie IKT-Systemen und -Services in Bezug auf das Zähldatenverarbeitungssystem liegen im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse (solange sie vorsätzlich erfolgen) setzen zumeist das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios.

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Finanzieller Verlust könnte für Prosumer entstehen, falls es zu Sach- oder Personenschaden kommt oder der Bezug und/oder die Einspeisung der elektrischen Energie durch falsche oder fehlende Informationen zuungunsten des Prosumers beeinflusst werden.
- Es kann nicht ausgeschlossen werden, dass Leib und Leben auf Seite Prosumer gefährdet wird und es sogar zu Todesfällen kommen kann.

Sicht einzelner Datenmanager (DM):

- Finanzielle Verluste für Datenmanager könnten durch Schäden an Betriebsmitteln und/oder -Personal sowie an Prosumern oder Dritten aber auch als Folge von Compliance-Verletzungen entstehen.
- Compliance-Verletzungen kämen auch zustande, falls bestimmte Auflagen aus Gesetzen etc. durch den Datenmanager nicht erfüllt werden könnten.
- Es kann nicht ausgeschlossen werden, dass Leib und Leben von Prosumern, von Betriebs-, Wartungs- und Support-Personal oder von Dritten gefährdet werden könnte. Selbst Todesfälle könnten eine Folge sein. Die Gefährdung von Leib und Leben hängt u. a. auch von der Grösse des Vorfalls ab (Beispiel: der Verkehr ist aufgrund eines Stromausfalls nicht mehr geregelt). Es wird hier vom Worst Case ausgegangen.
- Ein merklicher Reputationsverlust wäre auch nicht ausgeschlossen, insbesondere wenn der Fall in den Medien erscheint. Bei höherer Gewalt kann jedoch davon ausgegangen werden, dass die Folgen von Vorfällen mit Sach- und Personenschäden bei der Bevölkerung eher leichter akzeptiert werden und daher der Reputationsverlust voraussichtlich tiefer wird.
- Bei einem schwerwiegenden Vorfall wären die erwähnten Auswirkungen entsprechend höher und die überregionale Versorgungssicherheit könnte im schlimmsten Fall gefährdet werden.

A.1.7. Kern Risiko-Szenario RS.07

RS.07: Schwerwiegende Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform	
Bemerkungen	• Das Risiko-Szenario umfasst auch – den Missbrauch von Systemressourcen wie z. B. Rechenleistung oder Übertragungsleitungen und -Verbindungen zur Kommunikation • Durch dieses Szenario werden u. a. auch die Vollständigkeit der Daten auf Online-Visualisierungsplattform (OVP) und korrekte Funktionsweise der OVP gefährdet. • Die Online-Visualisierungsplattform soll den Prosumern helfen, ihren Verbrauch und/oder ihre Einspeisung von elektrischen Energie zu optimieren. Sie kann Daten in roher oder aggregierter Form wie z. B. Daten zum Verbrauch/Einspeisung oder Trendanalysen beinhalten.
Annahmen	• Eine missbräuchliche oder fehlerhafte Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet nicht statt. • Bei den durch die Online-Visualisierungsplattform verwalteten Daten handelt es sich um die Kopien von den im Rest des intelligenten Messsystems bewirtschafteten Daten, die über das Zähldatenverarbeitungssystem geliefert werden. • Der Datenmanager trägt die Verantwortung für den Betrieb und Sicherheit der OVP.
Szenario-varianten	• RS.07a: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform (OVP) und der zusammenhängenden Daten und Funktionalitäten durch Angriffe (Eindringen) **vor Ort** und/oder **aus der Ferne** auf OVP bzw. auf dessen Systemkomponenten und Schnittstellen
	• RS.07b: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform und der zusammenhängenden Daten und Funktionalitäten **durch höhere Gewalt**
	• RS.07c: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform und der zusammenhängenden Daten und Funktionalitäten **durch technisches Versagen**
	• RS.07d: **Schwerwiegende** Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform und der zusammenhängenden Daten und Funktionalitäten **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Online-Visualisierungsplattform

Tabelle 26: Steckbrief für Kern Risiko-Szenario RS.07

		Ereigniskategorien					Schadenskategorien						
		Sensitive Daten			IKT-Systeme & -Services								
Risiko-Szenario	Sicht betreffend Auswirkungen	V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.07a	P		Ja	Ja	Ja	Ja			Ja			Ja	Ja
	DM						Ja	Ja	Ja			Ja	
RS.07b	P		Ja	Ja	Ja	Ja			Ja			Ja	
	DM						Ja	Ja	Ja			Ja	
RS.07c	P		Ja	Ja	Ja	Ja			Ja			Ja	
	DM						Ja	Ja	Ja			Ja	
RS.07d	P		Ja	Ja	Ja	Ja			Ja			Ja	
	DM						Ja	Ja	Ja			Ja	

Tabelle 27: Aufschlüsselung RS.07 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität und Verfügbarkeit von Daten sowie IKT-Systemen und -Services in Bezug auf die Online-Visualisierungsplattform liegen im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse (solange sie vorsätzlich erfolgen) setzen zumeist das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios.

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Finanzieller Verlust könnte für Prosumer entstehen, falls der Bezug und/oder die Einspeisung der elektrischen Energie durch falsche oder fehlende Informationen zu Ungunsten des Prosumers beeinflusst werden.

Sicht einzelner Datenmanager (DM):

- Finanzielle Verluste für Datenmanager könnten entstehen, falls der Bezug und/oder die Einspeisung der elektrischen Energie durch falsche oder fehlende Informationen zu Ungunsten des Datenmanagers beeinfluss werden. Auch die eventuellen Compliance-Verletzungen könnten zu finanziellen Verlusten beim Datenmanager führen.

- Compliance-Verletzungen kämen auch zustande, falls bestimmte Auflagen aus Gesetzen etc. durch den Datenmanager nicht erfüllt werden könnten.
- Ein moderater Reputationsverlust wäre auch nicht ausgeschlossen, insbesondere wenn der Vorfall in den Medien erscheint. Bei höherer Gewalt kann jedoch davon ausgegangen werden, dass die Folgen bei der Bevölkerung eher leichter akzeptiert werden und daher der Reputationsverlust voraussichtlich tiefer wird.
- Bei einem schwerwiegenden Vorfall wären die erwähnten Auswirkungen entsprechend höher.

A.1.8. Kern Risiko-Szenario RS.08

RS.08: Böswillige oder fehlerhafte Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern	
Bemerkungen	• Der Fall «**Lastunterbrecher**» wird durch RS.08 behandelt
Annahmen	• Eine missbräuchliche oder fehlerhafte Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet nicht statt. • Die Stabilität des elektrischen Versorgungsnetzes kann durch eine grossflächige, böswillige oder fehlerhafte Deaktivierung/Beschränkung des Anschlusses von Prosumern gefährdet werden.
Szenario-varianten	• RS.08a: **Vereinzelte** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf **einzelne** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.08b: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf eine **Vielzahl** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.08c: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch höhere Gewalt**
	• RS.08d: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch technisches Versagen**
	• RS.08e: **Grossflächige** Deaktivierung / Beschränkung / Reaktivierung des Anschlusses von Prosumern **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem • Zähldatenverarbeitungssystem

Tabelle 28: Steckbrief für Kern Risiko-Szenario RS.08

		Ereigniskategorien					Schadenskategorien						
		Sensitive Daten			IKT-Systeme & -Services								
Risiko-Szenario	Sicht betreffend Auswirkungen	V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlich-keitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.08a	P		Ja	Ja	Ja	Ja			Ja	Ja			Ja
	DM						Ja	Ja	Ja	Ja			
RS.08b	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	Ja
	DM						Ja	Ja	Ja	Ja		Ja	
RS.08c	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.08d	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.08e	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	

Tabelle 29: Aufschlüsselung RS.08 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität und Verfügbarkeit von Daten sowie IKT-Systemen und -Services in Bezug auf das intelligente Messsystem liegen im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse (solange sie vorsätzlich erfolgen) setzen meistens das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios.

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Eine böswillige Beschränkung oder An- und Abschaltung des Anschlusses könnte an Ort und Stelle die Personensicherheit (Leib und Leben) gefährden oder Endverbrauchsgeräte beschädigen, was auch finanzielle Verluste zur Folge hätte.

Sicht einzelner Datenmanager (DM):

- Finanzielle Verluste für Datenmanager könnten durch Schäden an Betriebsmitteln und/oder -Personal sowie an Prosumern oder Dritten aber auch als Folge von Compliance-Verletzungen entstehen.
- Compliance-Verletzungen kämen auch zustande, falls bestimmte Auflagen aus Gesetzen etc. durch den Datenmanager nicht erfüllt werden könnten.
- Es kann nicht ausgeschlossen werden, dass Leib und Leben von Prosumern, von Betriebs-, Wartungs- und Support-Personal oder von Dritten gefährdet werden könnte. Selbst Todesfälle könnten eine Folge sein. Die Gefährdung von Leib und Leben hängt u. a. auch von der Grösse des Vorfalls ab (Beispiel: der Verkehr ist aufgrund eines Stromausfalls nicht mehr geregelt). Es wird hier vom Worst Case ausgegangen.
- Ein merklicher Reputationsverlust wäre auch nicht ausgeschlossen, insbesondere wenn der Fall in den Medien erscheint.
- Eine grossflächige (überregionale) Beschränkung oder Abschaltung des Anschlusses bei Prosumern (z. B. durch gleichzeitiges Abschalten einer grösseren Zahl von intelligenten Messgeräten) könnte zur Instabilität des elektrischen Versorgungsnetzes führen und im schlimmsten Fall die überregionale Versorgungssicherheit gefährden.

A.1.9. Kern Risiko-Szenario RS.09

RS.09: Böswillige oder fehlerhafte Steuerung von Verbrauch und Einspeisung der elektrischen Energie bei Prosumern	
Bemerkungen	• Die Steuerung umfasst z. B. die Aktivierung oder Deaktivierung von Verbrauchs- und Erzeugungseinheiten bei Prosumern inkl. Haushaltsgeräte wie z. B. Ofen, Klimaanlage etc.
Annahmen	• Die Steuerung von Verbrauchs- und Erzeugungseinheiten über ein intelligentes Messsystem ist möglich. • Die Stabilität des elektrischen Versorgungsnetzes kann durch eine grossflächige, böswillige oder fehlerhafte Steuerung von Verbrauch und Einspeisung der elektrischen Energie bei Prosumern gefährdet werden. • Eine missbräuchliche oder fehlerhafte Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet nicht statt.
Szenario-varianten	• RS.09a: **Vereinzelte** Übernahme der Steuerung von Verbrauchs- und Erzeugungseinheiten bei Prosumern via intelligentes Messsystem durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf **einzelne** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.09b: **Grossflächige** Übernahme der Steuerung von Verbrauchs- und Erzeugungseinheiten bei Prosumern via intelligentes Messsystem durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf eine **Vielzahl** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.09c: **Grossflächige**, fehlerhafte Steuerung von Verbrauchs- und Erzeugungseinheiten bei Prosumern via intelligentes Messsystem **durch höhere Gewalt**
	• RS.09d: **Grossflächige**, fehlerhafte Steuerung von Verbrauchs- und Erzeugungseinheiten bei Prosumern via intelligentes Messsystem **durch technisches Versagen**
	• RS.09e: **Grossflächige**, fehlerhafte Steuerung von Verbrauchs- und Erzeugungseinheiten bei Prosumern via intelligentes Messsystem **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem • Zähldatenverarbeitungssystem

Tabelle 30: Steckbrief für Kern Risiko-Szenario RS.09

		Ereigniskategorien					Schadenskategorien						
Risiko-Szenario	Sicht betreffend Auswirkungen	Sensitive Daten			IKT-Systeme & -Services								
		V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlich-keitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.09a	P		Ja	Ja	Ja	Ja			Ja	Ja			Ja
	DM						Ja	Ja	Ja	Ja			
RS.09b	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	Ja
	DM						Ja	Ja	Ja	Ja		Ja	
RS.09c	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.09d	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.09e	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	

Tabelle 31: Aufschlüsselung RS.09 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität und Verfügbarkeit von Daten sowie IKT-Systemen und -Services in Bezug auf das intelligente Messsystem liegen im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse (solange sie vorsätzlich erfolgen) setzen meistens das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios

Kommentar zu den relevanten Schadenskategorien:

Sicht einzelner Prosumer (P):

- Gleichzeitiges Ein- oder Ausschalten von Verbrauchs- und Erzeugungseinheiten könnte an Ort und Stelle die Personensicherheit (Leib und Leben) gefährden oder Endverbrauchsgeräte beschädigen, was auch finanzielle Verluste zur Folge hätte.

Sicht einzelner Datenmanager (DM):

- Finanzielle Verluste für Datenmanager könnten durch Schäden an Betriebsmitteln und/oder -Personal sowie an Prosumern oder Dritten aber auch als Folge von Compliance-Verletzungen entstehen.
- Compliance-Verletzungen kämen auch zustande, falls bestimmte Auflagen aus Gesetzen etc. durch den Datenmanager nicht erfüllt werden könnten.
- Es kann nicht ausgeschlossen werden, dass Leib und Leben von Prosumern, von Betriebs-, Wartungs- und Support-Personal oder von Dritten gefährdet werden könnte. Selbst Todesfälle könnten eine Folge sein. Die Gefährdung von Leib und Leben hängt u. a. auch von der Grösse des Vorfalls ab (Beispiel: Feuer durch Einschalten von Heizöfen). Es wird hier vom Worst Case ausgegangen.
- Ein merklicher Reputationsverlust wäre auch nicht ausgeschlossen, insbesondere wenn der Fall in den Medien erscheint.
- Ein grossflächiges (überregionales) Ein- oder Ausschalten von Verbrauchs- und Erzeugungseinheiten bei Prosumern (z. B. durch gleichzeitiges Ein- und Abschalten einer grösseren Zahl von Haushaltsgeräten) könnte zur Instabilität des elektrischen Versorgungsnetzes führen und im schlimmsten Fall die überregionale Versorgungssicherheit gefährden.

A.1.10. Kern Risiko-Szenario RS.10

RS.10: Böswillige oder fehlerhafte Steuerung der Gebäudeautomation[48] bei Prosumern	
Bemerkungen	• Die Steuerung umfasst z. B. die Aktivierung oder Deaktivierung von Einheiten bei Prosumern in Zusammenhang mit Gebäudeautomation wie z. B. Lüftung, Lift etc.
Annahmen	• Die Steuerung der Gebäudeautomation über ein intelligentes Messsystem ist möglich. • Die Stabilität des elektrischen Versorgungsnetzes kann durch eine grossflächige, böswillige oder fehlerhafte Steuerung der Gebäudeautomation gefährdet werden. • Eine missbräuchliche oder fehlerhafte Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet nicht statt.
Szenario-varianten	• RS.10a: **Vereinzelte** Übernahme der Steuerung der Gebäudeautomation (Lüftung etc.) via intelligentes Messsystem durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf **einzelne** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.10b: **Grossflächige** Übernahme der Steuerung der Gebäudeautomation (Lüftung etc.) via intelligentes Messsystem durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf eine **Vielzahl** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.10c: **Grossflächige**, fehlerhafte Steuerung der Gebäudeautomation (Lüftung etc.) via intelligentes Messsystem **durch höhere Gewalt**
	• RS.10d: **Grossflächige**, fehlerhafte Steuerung der Gebäudeautomation (Lüftung etc.) via intelligentes Messsystem **durch technisches Versagen**
	• RS.10e: **Grossflächige**, fehlerhafte Steuerung der Gebäudeautomation (Lüftung etc.) via intelligentes Messsystem **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem • Zähldatenverarbeitungssystem

Tabelle 32: Steckbrief für Kern Risiko-Szenario RS.10

[48] Hausautomation wird unter Gebäudeautomation zusammengefasst.

		Ereigniskategorien					Schadenskategorien						
Risiko-Szenario	Sicht betreffend Auswirkungen	Sensitive Daten			IKT-Systeme & -Services		Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
		V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit							
RS.10a	P		Ja	Ja	Ja	Ja			Ja	Ja			Ja
	DM						Ja	Ja	Ja	Ja			
RS.10b	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	Ja
	DM						Ja	Ja	Ja	Ja		Ja	
RS.10c	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.10d	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.10e	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	

Tabelle 33: Aufschlüsselung RS.10 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität und Verfügbarkeit von Daten sowie IKT-Systemen und -Services in Bezug auf das intelligente Messsystem liegen im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse (solange sie vorsätzlich erfolgen) setzen meistens das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Böswillige oder fehlerhafte Steuerung der Gebäudeautomation bei Prosumern könnte an Ort und Stelle die Personensicherheit (Leib und Leben) gefährden oder die Gebäudeautomation beschädigen, was auch finanzielle Verluste zur Folge hätte.

Sicht einzelner Datenmanager (DM):

- Finanzielle Verluste für Datenmanager könnten durch Schäden an Betriebsmitteln und/oder -Personal sowie an Prosumern oder Dritten aber auch als Folge von Compliance-Verletzungen entstehen.
- Compliance-Verletzungen kämen auch zustande, falls bestimmte Auflagen aus Gesetzen etc. durch den Datenmanager nicht erfüllt werden könnten.
- Es kann nicht ausgeschlossen werden, dass Leib und Leben von Prosumern, von Betriebs-, Wartungs- und Support-Personal oder von Dritten gefährdet werden könnte. Selbst Todesfälle könnten eine Folge sein. Die Gefährdung von Leib und Leben hängt u. a. auch von der Grösse des Vorfalls ab (Beispiel: der Lift oder die Heizung gerät ausser Kontrolle). Es wird hier vom Worst Case ausgegangen.
- Ein merklicher Reputationsverlust wäre auch nicht ausgeschlossen, insbesondere wenn der Fall in den Medien erscheint.
- Eine grossflächige (überregionale), böswillige oder fehlerhafte Steuerung der Gebäudeautomation bei Prosumern (z. B. durch gleichzeitiges Ein- und Abschalten einer grösseren Zahl von durch die Gebäudeautomation gesteuerten Gerätschaften) könnte zur Instabilität des elektrischen Versorgungsnetzes führen und im schlimmsten Fall die überregionale Versorgungssicherheit gefährden.

A.1.11. Kern Risiko-Szenario RS.11

RS.11: Gefährdung des Netzzustandes durch grossflächige Manipulation oder Einschränkung der Netzüberwachung	
Bemerkungen	• Es geht um das elektrische Versorgungsnetz und dessen Überwachung • Netzüberwachung erfolgt zwecks Störungs-/Fehlererkennung, Netzrekonfiguration und Instandhaltung.
Annahmen	• Eine missbräuchliche oder fehlerhafte Bearbeitung von Personendaten, die Persönlichkeitsverletzungen gemäss Art.12 DSG zur Folge hätte, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, findet nicht statt. • Eine Gefährdung des Netzzustandes ist durch eine grossflächige Manipulation oder Einschränkung der Netzüberwachung via intelligentes Messsystem möglich.
Szenario-varianten	• RS.11a: Gefährdung des Netzzustandes durch **grossflächige** Manipulation **oder** Einschränkung der Netzüberwachung via intelligentes Messsystem durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf eine **Vielzahl** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.11b: Gefährdung des Netzzustandes durch **grossflächige** Einschränkung der Netzüberwachung via intelligentes Messsystem **durch höhere Gewalt**
	• RS.11c: Gefährdung des Netzzustandes durch **grossflächige** Einschränkung der Netzüberwachung via intelligentes Messsystem **durch technisches Versagen**
	• RS.11d: Gefährdung des Netzzustandes durch **grossflächige** Einschränkung der Netzüberwachung via intelligentes Messsystem **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem • Zähldatenverarbeitungssystem

Tabelle 34: Steckbrief für Kern Risiko-Szenario RS.11

		Ereigniskategorien					Schadenskategorien						
		Sensitive Daten			IKT-Systeme & -Services								
Risiko-Szenario	Sicht betreffend Auswirkungen	V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.11a	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	Ja
	DM						Ja	Ja	Ja	Ja		Ja	
RS.11b	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.11c	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	
RS.11d	P		Ja	Ja	Ja	Ja			Ja	Ja		Ja	
	DM						Ja	Ja	Ja	Ja		Ja	

Tabelle 35: Aufschlüsselung RS.11 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Integrität und Verfügbarkeit von Daten sowie IKT-Systemen und -Services in Bezug auf das intelligente Messsystem liegen im Fokus dieses Szenarios.

Hinweis zur Vertraulichkeit: Solche Ereignisse (solange sie vorsätzlich erfolgen) setzen meistens das Sammeln von spezifischen Informationen zur Angriffsvorbereitung voraus. Der Verlust von Vertraulichkeit steht jedoch nicht im Mittelpunkt dieses Risiko-Szenarios

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Gefährdung des Netzzustandes durch grossflächige Manipulation oder Einschränkung der Netzüberwachung via intelligentes Messsystem könnte an Ort und Stelle die Personensicherheit gefährden sowie die Endverbrauchsgeräte und/oder Gebäudeautomation beschädigen, was auch finanzielle Verluste zur Folge hätte.

Sicht einzelner Datenmanager (DM):

- Finanzielle Verluste für Datenmanager könnten durch Schäden an Betriebsmitteln und/oder -Personal sowie an Prosumern oder Dritten aber auch als Folge von Compliance-Verletzungen entstehen.

- Compliance-Verletzungen kämen auch zustande, falls bestimmte Auflagen aus Gesetzen etc. durch den Datenmanager nicht erfüllt werden könnten.
- Es kann nicht ausgeschlossen werden, dass Leib und Leben von Prosumern, von Betriebs-, Wartungs- und Support-Personal oder von Dritten gefährdet werden könnte. Selbst Todesfälle könnten eine Folge sein. Die Gefährdung von Leib und Leben hängt u. a. auch von der Grösse des Vorfalls ab (Beispiel: der Verkehr ist aufgrund eines Stromausfalls nicht mehr geregelt). Es wird hier vom Worst Case ausgegangen.
- Ein merklicher Reputationsverlust wäre auch nicht ausgeschlossen, insbesondere wenn der Fall in den Medien erscheint.
- Eine grossflächige (überregionale) Instabilität des elektrischen Versorgungsnetzes könnte im schlimmsten Fall die überregionale Versorgungssicherheit gefährden.

A.1.12. Kern Risiko-Szenario RS.12

RS.12: Offenlegung/Entwendung der auf intelligenten Messgeräten verwalteten Daten inkl. Datenübertragung	
Bemerkungen	• Datenentwendung kann u. a. zur Erzeugung von detaillierten Last- und Erzeugungsprofilen von Prosumern oder generell zur Angriffsvorbereitung (Stichwort «information gathering») stattfinden. • Als „öffentlich“ eingestufte Daten sind ausser Betrachtung. • Bei den Daten handelt sich nicht nur um Personendaten.
Annahmen	• Personen- sowie Versorgungssicherheit sind nicht betroffen.
Szenario-varianten	• RS.12a: **Punktuelle** Offenlegung, Entwendung oder missbräuchliche Bearbeitung der auf intelligenten Messgeräten verwalteten Daten durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf **einzelne** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.12b: **Grossflächige** Offenlegung, Entwendung oder missbräuchliche Bearbeitung der auf intelligenten Messgeräten verwalteten Daten durch Angriffe (Eindringen) **vor Ort** und**/**oder **aus der Ferne** – auf eine **Vielzahl** Messgeräte oder – auf Kommunikationsnetzwerke (LAN, WAN) / Datenkonzentratoren oder – auf das Zähldatenverarbeitungssystem
	• RS.12c: **Grossflächige** Offenlegung der auf intelligenten Messgeräten verwalteten Daten **durch höhere Gewalt**
	• RS.12d: **Grossflächige** Offenlegung der auf intelligenten Messgeräten verwalteten Daten **durch technisches Versagen**
	• RS.12e: **Grossflächige** Offenlegung der auf intelligenten Messgeräten verwalteten Daten **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Intelligentes Messgerät • Kommunikationssystem

Tabelle 36: Steckbrief für Kern Risiko-Szenario RS.12

		Ereigniskategorien					Schadenskategorien						
		Sensitive Daten			IKT-Systeme & -Services								
Risiko-Szenario	Sicht betreffend Auswirkungen	V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.12a	P	Ja			Ja				Ja		Ja		Ja
	DM						Ja	Ja	Ja				
RS.12b	P	Ja			Ja				Ja		Ja		Ja
	DM						Ja	Ja	Ja				
RS.12c	P	Ja			Ja				Ja		Ja		
	DM						Ja	Ja	Ja				
RS.12d	P	Ja			Ja				Ja		Ja		
	DM						Ja	Ja	Ja				
RS.12e	P	Ja			Ja				Ja		Ja		
	DM						Ja	Ja	Ja				

Tabelle 37: Aufschlüsselung RS.12 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Vertraulichkeit von Daten sowie Verlust von Integrität von IKT-Systemen und -Services sind im Fokus dieses Szenarios.

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Durch die Offenlegung/Entwendung oder durch eine missbräuchliche Bearbeitung von Personendaten, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, könnten Persönlichkeits-verletzungen gemäss Art.12 DSG zustande kommen.
- Die Offenlegung/Entwendung oder eine missbräuchliche Bearbeitung von Daten bzw. Personendaten resultieren nicht direkt zu einem finanziellen Verlust für den Prosumer sondern indirekt über weitere Angriffe wie z. B. solcher aus RS.02.

Sicht einzelner Datenmanager (DM):

- Durch die Offenlegung/Entwendung oder eine missbräuchliche Bearbeitung von Daten bzw. Personendaten kämen Compliance-Verletzungen zustande, die im Endeffekt durch Gerichtsverfahren o. ä. mit finanziellen Verlust und Reputationsverlust verbunden sind.
- Bei einem grossflächigen Vorfall wären die erwähnten Auswirkungen entsprechend höher.

A.1.13. Kern Risiko-Szenario RS.13

RS.13: Schwerwiegende Daten-Offenlegung / -Entwendung via Zähldatenverarbeitungssystem	
Bemerkungen	• Datenentwendung kann u. a. zur Erzeugung von detaillierten Last- und Erzeugungsprofilen von Prosumern oder generell zur Angriffsvorbereitung (Stichwort «information gathering») stattfinden. • Als „öffentlich“ eingestufte Daten sind ausser Betrachtung. • Bei den Daten handelt sich nicht nur um Personendaten.
Annahmen	• Personen- sowie Versorgungssicherheit sind nicht betroffen.
Szenario-varianten	• RS.13a: **Schwerwiegende** Offenlegung, Entwendung oder missbräuchliche Bearbeitung der auf Zähldatenverarbeitungssystem (ZDVS) verwalteten Daten durch Angriffe (Eindringen) **vor Ort** und/oder **aus der Ferne** auf ZDVS bzw. auf dessen Systemkomponenten und Schnittstellen
	• RS.13b: **Schwerwiegende** Offenlegung der auf Zähldatenverarbeitungssystem verwalteten Daten **durch höhere Gewalt**
	• RS.13c: **Schwerwiegende** Offenlegung der auf Zähldatenverarbeitungssystem verwalteten Daten **durch technisches Versagen**
	• RS.13d: **Schwerwiegende** Offenlegung der auf Zähldatenverarbeitungssystem verwalteten Daten **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Zähldatenverarbeitungssystem

Tabelle 38: Steckbrief für Kern Risiko-Szenario RS.13

		Ereigniskategorien					Schadenskategorien						
		Sensitive Daten			IKT-Systeme & -Services								
Risiko-Szenario	Sicht betreffend Auswirkungen	V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.13a	P	Ja			Ja				Ja		Ja		Ja
	DM						Ja	Ja	Ja				
RS.13b	P	Ja			Ja				Ja		Ja		
	DM						Ja	Ja	Ja				
RS.13c	P	Ja			Ja				Ja		Ja		
	DM						Ja	Ja	Ja				
RS.13d	P	Ja			Ja				Ja		Ja		
	DM						Ja	Ja	Ja				

Tabelle 39: Aufschlüsselung RS.13 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Vertraulichkeit von Daten sowie Verlust von Integrität von IKT-Systemen und -Services sind im Fokus dieses Szenarios.

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Durch die Offenlegung/Entwendung oder durch eine missbräuchliche Bearbeitung von Personendaten, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, könnten Persönlichkeitsverletzungen gemäss Art.12 DSG zustande kommen.
- Die Offenlegung/Entwendung oder eine missbräuchliche Bearbeitung von Daten bzw. Personendaten resultieren nicht direkt zu einem finanziellen Verlust für den Prosumer sondern indirekt über weitere Angriffe wie z. B. solcher aus RS.02.

Sicht einzelner Datenmanager (DM):

- Durch eine schwerwiegende Offenlegung/Entwendung oder missbräuchliche Bearbeitung von Daten bzw. Personendaten kämen Compliance-Verletzungen zustande, die im Endeffekt durch Gerichtsverfahren o. ä. mit finanziellen Verlust und Reputationsverlust verbunden sind.

A.1.14. Kern Risiko-Szenario RS.14

RS.14: Schwerwiegende Daten-Offenlegung / -Entwendung via Online-Visualisierungsplattform	
Bemerkungen	• Eine Online-Visualisierungsplattform soll den Prosumern helfen, ihren Verbrauch und/oder ihre Einspeisung von elektrischer Energie zu optimieren. Sie kann Daten in roher oder aggregierter Form wie z. B. Daten zum Verbrauch/Einspeisung oder Trendanalysen beinhalten. • Datenentwendung kann u. a. zur Erzeugung von detaillierten Last- und Erzeugungsprofilen von Prosumern oder generell zur Angriffsvorbereitung (Stichwort «information gathering») stattfinden. • Als „öffentlich“ eingestufte Daten sind ausser Betrachtung. • Bei den Daten handelt sich nicht nur um Personendaten.
Annahmen	• Bei den durch die Online-Visualisierungsplattform verwalteten Daten handelt es sich um die Kopien von den im Rest des intelligenten Messsystems bewirtschafteten Daten, die über das Zähldatenverarbeitungssystem geliefert werden. • Der Datenmanager trägt die Verantwortung für den Betrieb und Sicherheit der OVP.
Szenario-varianten	• RS.14a: **Schwerwiegende** Offenlegung, Entwendung oder missbräuchliche Bearbeitung der auf Online-Visualisierungsplattform (OVP) verwalteten Daten durch Angriffe (Eindringen) **vor Ort** und/oder **aus der Ferne** auf OVP bzw. auf dessen Systemkomponenten und Schnittstellen
	• RS.14b: **Schwerwiegende** Offenlegung der auf Online-Visualisierungsplattform verwalteten Daten **durch höhere Gewalt**
	• RS.14c: **Schwerwiegende** Offenlegung der auf Online-Visualisierungsplattform verwalteten Daten **durch technisches Versagen**
	• RS.14d: **Schwerwiegende** Offenlegung der auf Online-Visualisierungsplattform verwalteten Daten **durch menschliche Fehlhandlungen oder organisatorische Mängel**
Übergeordnete Schutzobjekte	• Online-Visualisierungsplattform

Tabelle 40: Steckbrief für Kern Risiko-Szenario RS.14

		Ereigniskategorien					Schadenskategorien						
		Sensitive Daten			IKT-Systeme & -Services								
Risiko-Szenario	Sicht betreffend Auswirkungen	V.v. Vertraulichkeit	V.v. Integrität	V.v. Verfügbarkeit	V.v. Integrität	V.v. Verfügbarkeit	Reputationsverlust	Compliance-Verletzungen	Finanzieller Verlust	Gefährdung von Leib und Leben	Verletzung von Persönlichkeitsrechten	Gefährdung überregionaler Versorgungssicherheit	Vorsätzliche Handlungen
RS.14a	P	Ja			Ja				Ja		Ja		Ja
	DM						Ja	Ja	Ja				
RS.14b	P	Ja			Ja				Ja		Ja		
	DM						Ja	Ja	Ja				
RS.14c	P	Ja			Ja				Ja		Ja		
	DM						Ja	Ja	Ja				
RS.14d	P	Ja			Ja				Ja		Ja		
	DM						Ja	Ja	Ja				

Tabelle 41: Aufschlüsselung RS.14 auf relevante Ereignis- und Schadenskategorien

Legende zur Tabelle: V.v: Verlust von; P: Prosumer; DM: Datenmanager

Kommentar zu den relevanten Ereigniskategorien

Der Verlust von Vertraulichkeit von Daten sowie Verlust von Integrität von IKT-Systemen und -Services sind im Fokus dieses Szenarios.

Kommentar zu den relevanten Schadenskategorien

Sicht einzelner Prosumer (P):

- Durch die Offenlegung/Entwendung oder durch eine missbräuchliche Bearbeitung von Personendaten, wie z. B. die widerrechtliche Kreierung und Verwendung von detaillierten Last- und Erzeugungsprofilen von Prosumern, könnten Persönlichkeitsverletzungen gemäss Art.12 DSG zustande kommen.
- Die Offenlegung/Entwendung oder eine missbräuchliche Bearbeitung von Daten bzw. Personendaten resultieren nicht direkt in einem finanziellen Verlust für den Prosumer sondern indirekt über weitere Angriffe wie z. B. solcher aus RS.02.

Sicht einzelner Datenmanager (DM):

- Durch eine schwerwiegende Offenlegung/Entwendung oder missbräuchliche Bearbeitung von Daten bzw. Personendaten kämen Compliance-Verletzungen zustande, die im Endeffekt durch Gerichtsverfahren o. ä. mit finanziellen Verlust und Reputationsverlust verbunden sind.

A.2. Detaillierung des Schutzobjektes „Daten und Informationen“

Die relevanten Use Cases erlauben eine Detaillierung des Schutzobjektes SO.01 «Daten und Informationen». Daher wird dieses Schutzobjekt nachfolgend, gestützt auf Ref. [2], ausführlich ausgewiesen.

Daten und Informationen	Datenschutz-relevanz	Verwendung in den Use Cases	Relevanz betreffend Versorgungs-sicherheit	Bemerkungen aus Ref. [2]
Meteringdaten und -Historie	Ja	1, 2, 3, 5, 8	Möglicherweise	Für die Versorgungssicherheit sind die Meteringdaten unkritisch, **sofern** es sich um reine Messwerte zu Abrechnungszwecken und statistische Zwecke handelt und sie nicht zur direkten Berechnung von Netzzuständen und Schaltungen/Steuerungen führen.
Konfigurationsdaten	Möglicherweise	1	Ja	Aus Datenschutzgründen sind die Vertraulichkeit und Integrität der Konfigurationsdaten **möglicherweise** kritisch, weil sie Rückschlüsse auf personenbezogene Daten zulassen könnten.
Kundendaten	Ja	1	Nein	Hierbei handelt es sich insbesondere um Angaben zu einer Person, Vertragsdaten, Messpunkte etc.
Marktinformationen	Nein	2	Ja	Die Integrität der Marktinformationen ist tendenziell als kritisch einzustufen, da in der Masse (grossflächig) mit falschen Werten ein kritischer Netzzustand hervorgerufen werden könnte. Die Verfügbarkeit und Vertraulichkeit der Marktdaten im hier beschriebenen Sinn ist bezüglich der Versorgungssicherheit unkritisch.
Anreizsignale	Möglicherweise	2	Möglicherweise	Die Integrität (jedoch nicht die Verfügbarkeit) der Anreizsignale kann tendenziell als kritisch eingestuft werden, da in der Masse mit falschen Werten ein kritischer Zustand hervorgerufen werden könnte. Inhalt und Form der Daten ist noch nicht bestimmt. Fallweise könnte es sich um Verbrauchsstatistiken, Vergleichsdaten mit dem Verbrauchsdurchschnitt der Nachbarn etc. handeln. Solche Daten wären wahrscheinlich als personenbezogene Daten zu qualifizieren

Daten und Informationen	Datenschutz-relevanz	Verwendung in den Use Cases	Relevanz betreffend Versorgungs-sicherheit	Bemerkungen aus Ref. [2]
System-zustands-daten	Ja	2	Ja	Für die Versorgungssicherheit sind die Verfügbarkeit und Integrität der Systemzustandsdaten als kritisch einzustufen. Mit falschen oder fehlenden Systemzustandsdaten könnten Schaltungen ausgelöst werden, die die Netzstabilität beeinträchtigen und so die Versorgungssicherheit gefährden. Die Systemzustandsdaten lassen Rückschlüsse auf personenbezogene Daten und Unternehmensdaten zu.
Messwerte Endgeräte	Ja	3	Ja	Aus Sicht genereller Versorgungssicherheit kann die Integrität der Messwerte der Endgeräte kritisch sein, insbesondere wenn aufgrund deren an eine grössere Anzahl von Gebäudeautomationen gleichzeitig falsche Steuersignale gesendet werden.
Steuersignale Endgeräte	Möglicherweise	3	Ja	Aus Sicht genereller Versorgungssicherheit kann die Integrität der Steuersignale der Endgeräte kritisch sein, insbesondere wenn an eine grössere Anzahl von Gebäudeautomationen gleichzeitig falsche Steuersignale gesendet werden.
Aufbereitete Verbrauchs-daten	Möglicherweise	3	Nein	Visualisierte bzw. einfach verständlich aufbereitete Verbrauchsdaten des intelligenten Messgerätes bzw. von einzelnen Verbrauchsgeräten stellen potentielle personenbezogene Daten dar. Insbesondere die Daten von einzelnen Verbrauchsgeräten können, falls sie bspw. nur von einer bestimmten Person verwendet werden (etwa ein Dialysegerät für Zuhause), personenbezogene (besonders schützenswerte) Daten darstellen.

Daten und Informationen	Datenschutz-relevanz	Verwendung in den Use Cases	Relevanz betreffend Versorgungs-sicherheit	Bemerkungen aus Ref. [2]
Monitoring-daten	Ja	4	Ja	Falsche Monitoringdaten könnten in kritischen Situationen zu falschen Abrufsignalen führen. Die Vorhaltung der SDL bei den teilnehmenden Anlagen soll laufend überwacht werden. Die hierfür benötigten Daten enthalten die aktuell abrufbare Leistung und je nach Regelleistung (primär, sekundär, tertiär) Angaben zum Arbeitspunkt und zur momentanen Leistung der teilnehmenden Erzeugungseinheit (bspw. einer Turbine). Die Überwachung solcher u.U. geschäftssensibler Unternehmensdaten stellt eine Bearbeitung von personenbezogenen Daten gemäss DSG dar.
Abrufsignale SDL	Möglicherweise	4	Ja	Die Abrufsignale sind bezüglich Integrität und Verfügbarkeit für die Versorgungssicherheit kritisch, da diese genau für diesen Zweck verwendet werden und falsche oder nicht vorhandene Daten im kritischen Zeitpunkt das Netz instabil machen können.
Steuersignale Ein- und Ausspeisung	Möglicherweise	5, 8, 12	Ja	Die Integrität der Steuersignale der Ein- und Ausspeisungen kann für die Versorgungssicherheit als kritisch eingestuft werden, da bei einer breiten Verteilung falscher Werte die Netzstabilität gefährdet werden kann. Im Wesentlichen handelt es sich um An- und Ausschaltungen bzw. Erhöhung oder Senkung der Kapazitäten. Diese Schaltsignale scheinen auf den ersten Blick aus datenschutzrechtlicher Perspektive unbedenklich. Indes ist es denkbar, dass aus der Summe dieser Signale der Bedarf des Netzbetreibers hergeleitet werden könnte und somit diese Datenströme ebenfalls vom Datenschutzgesetz erfasst wären.
Fehler-informationen	Möglicherweise	7, 9	Ja	Bei grossflächigen Fehlern/Ausfällen sollten die Fehlerinformationen (z. B. zu Versorgungsunterbrüchen gemäss Mindestanforderung 4.1.1B) korrekt und verfügbar sein.

Daten und Informationen	Datenschutz-relevanz	Verwendung in den Use Cases	Relevanz betreffend Versorgungs-sicherheit	Bemerkungen aus Ref. [2]
Flexibilisierungs-Opt. Ein-/ Ausspeisung	Möglicherweise	12	Möglicherweise	Die Flexibilisierungsoptionen sind für die Versorgungssicherheit tendenziell bezüglich deren Integrität kritisch, da falsche Daten (wenn z.B. grossflächig manipuliert) falsche Regelungen auslösen könnten und das Netz in einen Instabilen Zustand bringen könnten. Die Flexibilisierungsoptionen sind aus Datenschutzsicht tendenziell kritisch, falls sie Rückschlüsse auf Personen zulassen. Insbesondere beim Prosumer ist es denkbar, dass die Flexibilisierungsoptionen Rückschlüsse auf An- und Abwesenheiten sowie Grössenordnungen des Stromverbrauchs zulassen (z. B. mehr Flexibilität bei Abwesenheit).
Sonstige Daten	Möglicherweise	Nicht anwendbar	Möglicherweise	Zu den sonstigen Daten gehören u.a. - Geschäftsprozesse und Dokumentation zwecks Betrieb, Wartung und Support des intelligenten Messsystems - Authentisierung- und Autorisierungsdaten - Quell-Code und Testdaten - Backups, die für die Kontinuität und Stabilität des Gesamt-Systems unabdingbar sind

Tabelle 42: Detaillierung von Daten und Informationen

A.3. Zuordnung von Use Cases und Schwachstellen auf Kern Risiko-Szenarien

Das hohe Abstraktionsniveau der Kern Risiko-Szenarien birgt den Nachteil, dass eine Aufschlüsselung auf die zugrundeliegenden Use Cases und Schwachstellen nur beschränkt möglich ist. Zwecks Rückverfolgung von Use Cases und Schwachstellen auf Risiko-Szenarien, wurde eine Zuordnung von Use Cases und Schwachstellen auf Kern Risiko-Szenarien in den folgenden Unterkapiteln erstellt.

A.3.1. Zuordnung von relevanten Use Cases auf Kern Risiko-Szenarien

Die relevanten Use Cases gemäss 3.2.1 ermöglichen es, eine Gesamtübersicht zu den wesentlichen Daten und Datenflüssen betreffend intelligentes Messsystem zu erhalten und die Relevanz von möglichen Mindestanforderungen aus Ref. [1] für die vorliegenden SBA zu überprüfen.

Die nachfolgende Tabelle zeigt die Zuordnung von relevanten Use Cases auf Kern Risiko-Szenarien.

Use Cases / Kern Risiko-Szenario	UC1 - Datenmanagement	UC2 - Demand Side Response	UC3 - Gebäudeautomatisierung	UC4 - Systemdienstleistungen	UC5 – Regionale Flexibilitäten	UC7 - Fehlererkennung und Netzrekonfiguration	UC8 - Steuerung Wirk- und Blindleistung	UC9 - Instandhaltung	UC12 - Zeitliche Flexibilisierung Ein-/Ausspeisung
RS.01: Abrechnungsbetrug mittels Manipulation der Tarifierung	x	x							
RS.02: Grossflächiger Abrechnungsbetrug durch Datenmanager	x	x							
RS.03: Abrechnungsbetrug mittels Manipulation des geeichten, messtechnischen Teils des intelligenten Messgerätes	x	x							
RS.04: Grossflächiger Abrechnungsbetrug durch Datenmanager mittels Manipulation des geeichten, messtechnischen Teils der intelligenten Messgeräte	x	x							
RS.05: Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten	x	x	x	x	x	x	x	x	x
RS.06: Schwerwiegende Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems	x	x	x	x	x	x	x	x	x
RS.07: Schwerwiegende Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform		x							
RS.08: Böswillige oder fehlerhafte Deaktivierung / Beschränkung des Anschlusses von Prosumern	x	x	x	x	x	x	x	x	x
RS.09: Böswillige oder fehlerhafte Steuerung von Verbrauch und Einspeisung der elektrischen Energie bei Prosumern		x	x	x	x		x	x	x
RS.10: Böswillige oder fehlerhafte Steuerung der Gebäudeautomation bei Prosumern			x						
RS.11: Gefährdung des Netzzustandes durch grossflächige Manipulation oder Einschränkung der Netzüberwachung				x	x	x	x	x	
RS.12: Offenlegung / Entwendung der auf intelligenten Messgeräten verwalteten Daten inkl. Datenübertragung	x	x	x	x	x	x	x	x	x
RS.13: Schwerwiegende Daten-Offenlegung / -Entwendung via Zähldatenverarbeitungssystem	x	x	x	x	x	x	x	x	x
RS.14: Schwerwiegende Daten-Offenlegung / -Entwendung via Online-Visualisierungsplattform		x							

Tabelle 43: Zuordnung von relevanten «Use Cases» auf «Kern Risiko-Szenarien»

A.3.2. Zuordnung von Schwachstellen auf Kern Risiko-Szenarien

Die Schwachstellen dienen zusammen mit dem Bedrohungskatalog aus Kapitel 4.3 als Basis für die Identifikation und Bildung von «Kern Risiko-Szenarien» gemäss Kapitel 5.

Eine Zuordnung von Schwachstellen auf «Kern Risiko-Szenarien» stellt die folgende Tabelle dar.

Kern Risiko-Szenario	Verursachende Schwachstellen
RS.01: Abrechnungsbetrug mittels Manipulation der Tarifierung	SS.01, SS.02, SS.03, SS.04, SS.05, SS.06, SS.07, SS.11, SS.12
RS.02: Grossflächiger Abrechnungsbetrug durch Datenmanager	SS.01, SS.03, SS.04, SS.05, SS.06, SS.07, SS.11, SS.12
RS.03: Abrechnungsbetrug mittels Manipulation des geeichten, messtechnischen Teils des intelligenten Messgerätes	SS.01, SS.02, SS.03, SS.04, SS.05, SS.06, SS.07, SS.11, SS.12, SS.13
RS.04: Grossflächiger Abrechnungsbetrug durch Datenmanager mittels Manipulation des geeichten, messtechnischen Teils der intelligenten Messgeräte	SS.01, SS.03, SS.04, SS.05, SS.06, SS.07, SS.11, SS.12, SS.13
RS.05: Einschränkung der Verfügbarkeit und Integrität von intelligenten Messgeräten	Alle
RS.06: Schwerwiegende Einschränkung der Verfügbarkeit und Integrität des Zähldatenverarbeitungssystems	SS.05, SS.06, SS.07, SS.11, SS.12
RS.07: Schwerwiegende Einschränkung der Verfügbarkeit und Integrität der Online-Visualisierungsplattform	SS.05, SS.07, SS.11, SS.12
RS.08: Böswillige oder fehlerhafte Deaktivierung / Beschränkung des Anschlusses von Prosumern	SS.01, SS.02, SS.03, SS.04, SS.05, SS.06, SS.07, SS.10, SS.11, SS.12
RS.09: Böswillige oder fehlerhafte Steuerung von Verbrauch und Einspeisung der elektrischen Energie bei Prosumern	SS.01, SS.02, SS.03, SS.04, SS.05, SS.06, SS.07, SS.09, SS.11, SS.12
RS.10: Böswillige oder fehlerhafte Steuerung der Gebäudeautomation bei Prosumern	SS.01, SS.02, SS.03, SS.04, SS.05, SS.06, SS.07, SS.09, SS.11, SS.12
RS.11: Gefährdung des Netzzustandes durch grossflächige Manipulation oder Einschränkung der Netzüberwachung	SS.01, SS.02, SS.03, SS.04, SS.05, SS.06, SS.07, SS.08, SS.11, SS.12
RS.12: Offenlegung / Entwendung der auf intelligenten Messgeräten verwalteten Daten inkl. Datenübertragung	SS.01, SS.02, SS.03, SS.05, SS.06, SS.07, SS.11, SS.12
RS.13: Schwerwiegende Daten-Offenlegung / -Entwendung via Zähldatenverarbeitungssystem	SS.05, SS.06, SS.07, SS.11, SS.12
RS.14: Schwerwiegende Daten-Offenlegung / -Entwendung via Online-Visualisierungsplattform	SS.05, SS.07, SS.11, SS.12

Tabelle 44: Zuordnung von «Schwachstellen» auf «Kern Risiko-Szenarien»

A.4. Use Cases betreffend intelligentes Messsystem

Um die Datenflüsse zum/vom Prosumer in Bezug auf das intelligente Messsystem besser im Überblick zu haben, wurden die Use Cases teilweise angepasst bzw. schematisch vereinfacht, indem angenommen wurde, dass die Datenflüsse zum/vom Prosumer im Rahmen des intelligenten Messsystems über den Datenmanager stattfinden. Die auf dieser Basis abgegrenzten Bereiche stellen die irrelevante Kommunikation und Rollen in Use Cases dar und sind grau markiert.

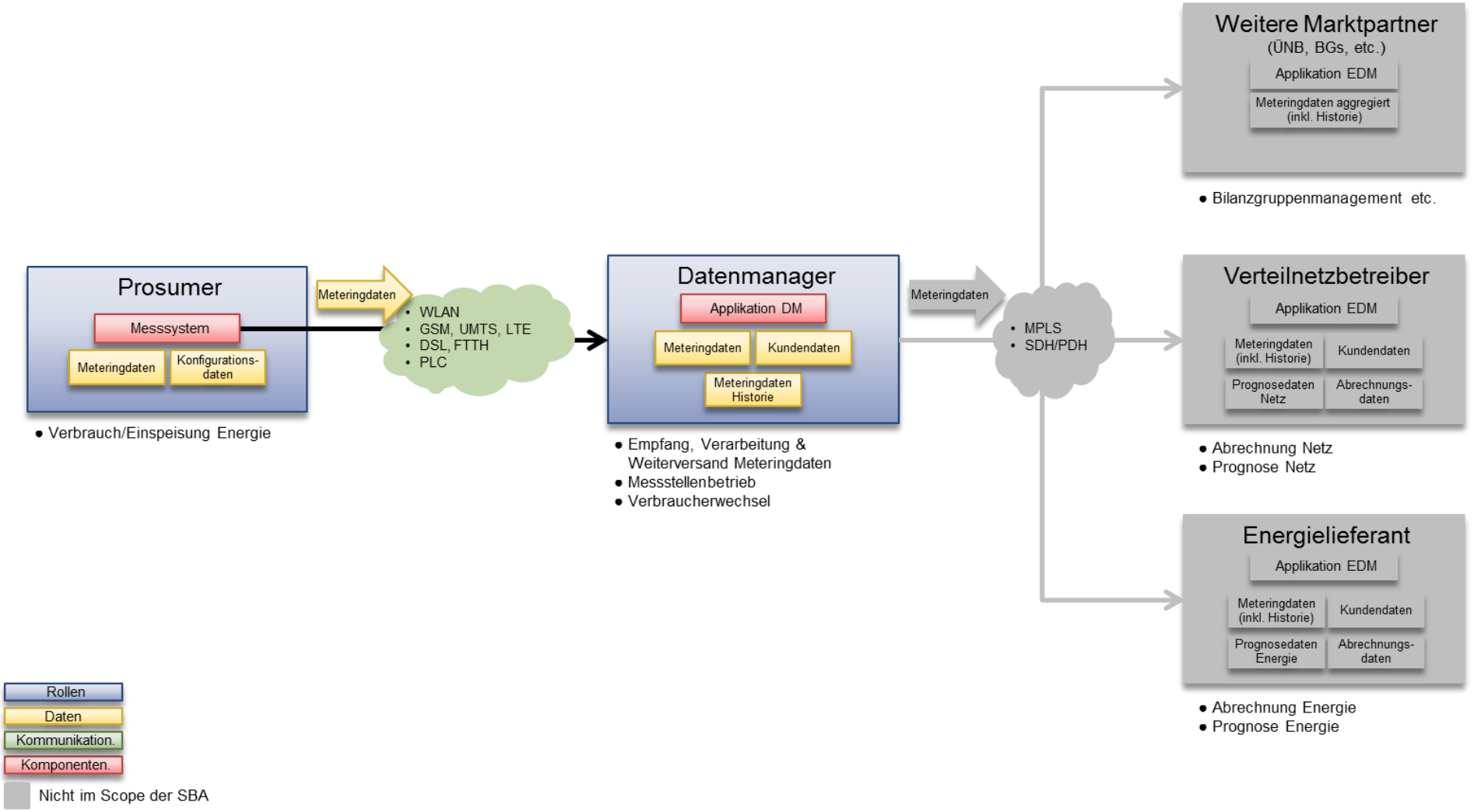
Die pro Use Case vorgenommenen Anpassungen sehen folgendermassen aus:

- UC1 – Datenmanagement
  - Keine Anpassungen
- UC2 - Demand Side Response
  - Keine Anpassungen
- UC3 – Gebäudeautomatisierung
  - Aus Konsistenzgründen mit anderen Use Cases werden die „Steuersignale Endgeräte“ und „Aufbereitete Verbrauchsdaten“ neu auch vom Datenmanager zum Prosumer übertragen.
- UC4 – Systemdienstleistungen
  - Der Verteilnetzbetreiber ist aus Konsistenzgründen mit anderen Use Cases neu mit dem Datenmanager verbunden und nicht mehr mit dem Prosumer.
  - Monitoringdaten vom Prosumer zum Datenmanager wurden in der Abbildung ergänzt. Somit ist die Schnittstelle „Prosumer - Datenmanager“ neu bidirektional.
- UC5 - Regionale Flexibilitäten
  - Keine Anpassungen. DSM-Komponente sollte jedoch nicht separat sondern als integrierter Bestandteil des Messsystems betrachtet werden.
- UC7 - Fehlererkennung und Netzrekonfiguration
  - Der Pfeil vom Prosumer zum Verteilnetzbetreiber wurde aus Konsistenzgründen mit Use Cases 8, 9 und 12 gestrichen.
- UC8 - Steuerung Wirk- und Blindleistung
  - Keine Anpassungen
- UC9 – Instandhaltung
  - Keine Anpassungen
- UC12 - Zeitliche Flexibilisierung Ein-/Ausspeisung
  - Keine Anpassungen

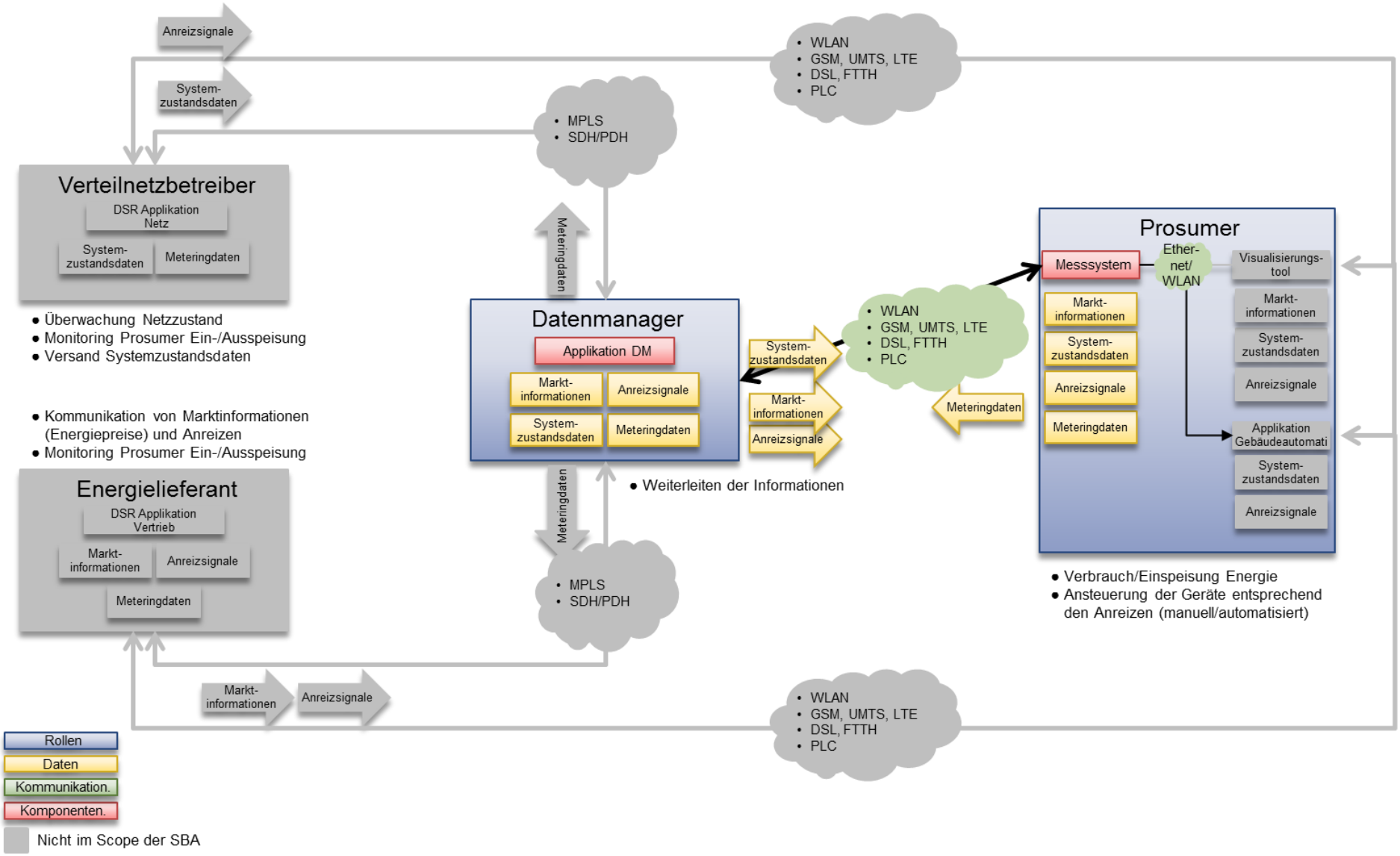
Die in den folgenden Unterkapiteln ausgewiesenen neun Use Cases setzen sich zusammen aus

- Rollen, die im Use Case beteiligt sind
- Komponenten, welche die Ausführung des Use Case unterstützen
- Daten, die für den Use Case benötigt werden
- Kommunikationswege mit Datenflüssen, welche die Daten zwischen den Rollen und Komponenten übermitteln. Die Pfeile der Datenflüsse geben dabei jeweils die Datenflussrichtung an.

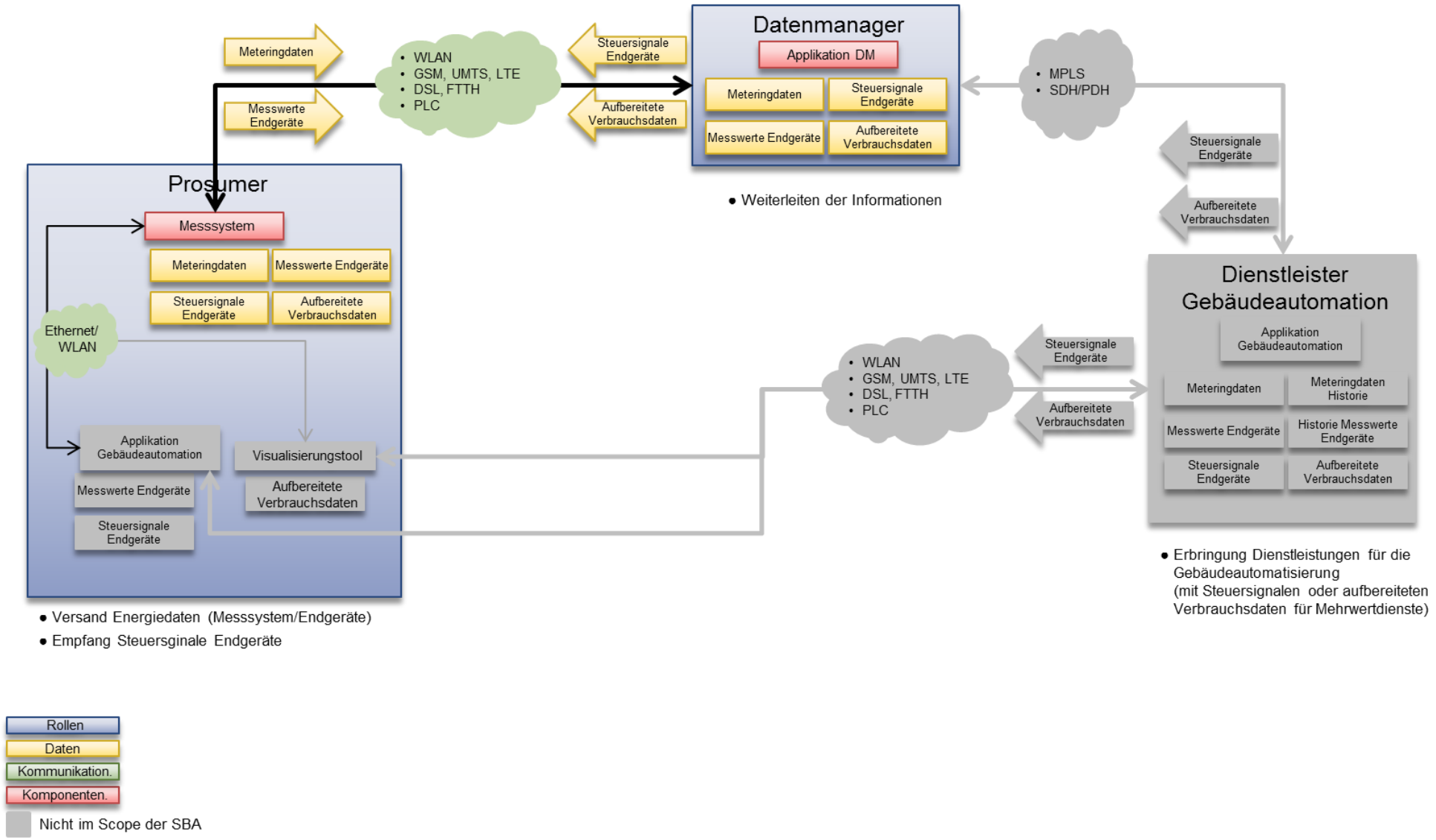
A.4.1. UC1 - Datenmanagement



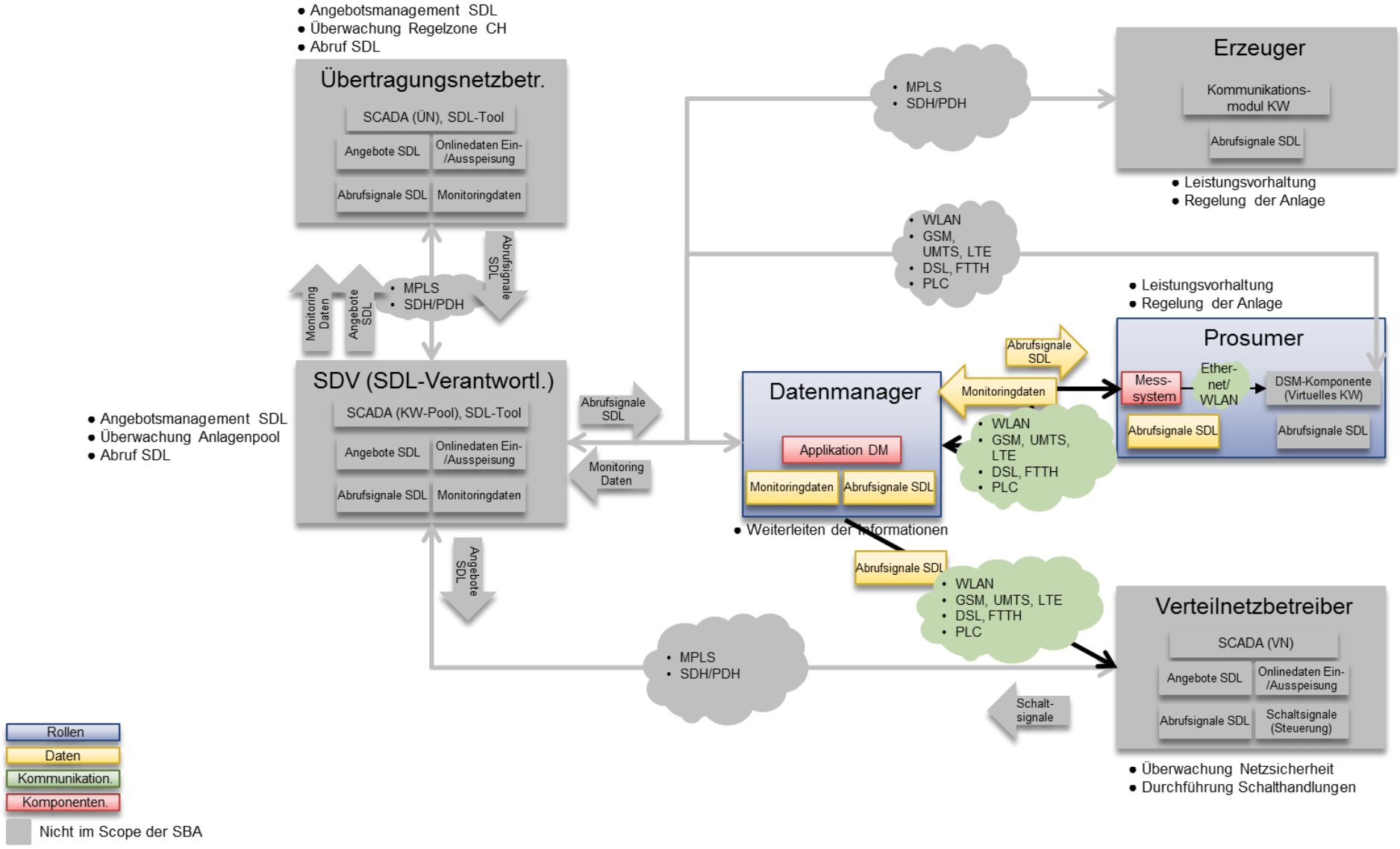
A.4.2. UC2 - Demand Side Response



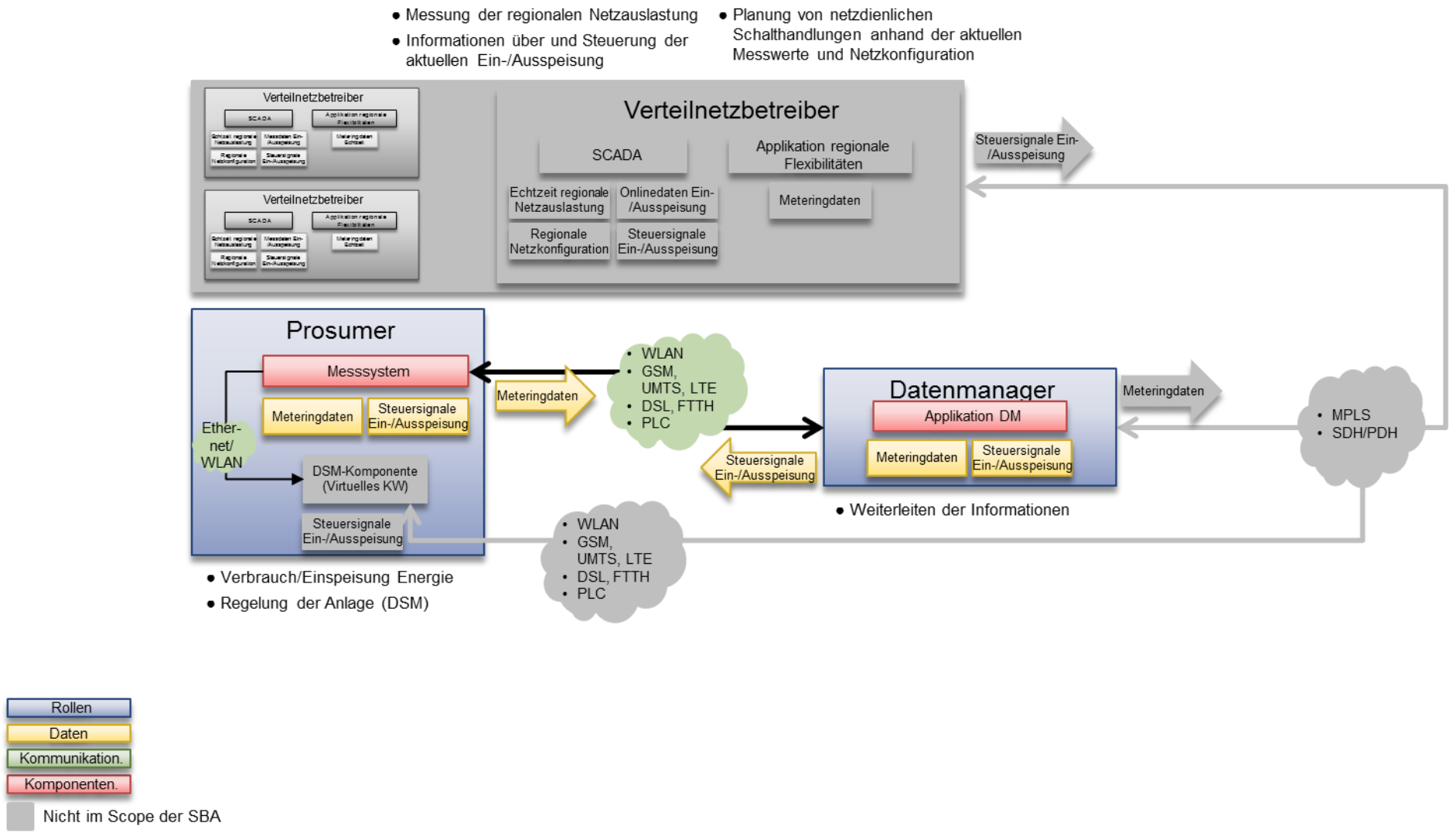
A.4.3. UC3 - Gebäudeautomatisierung



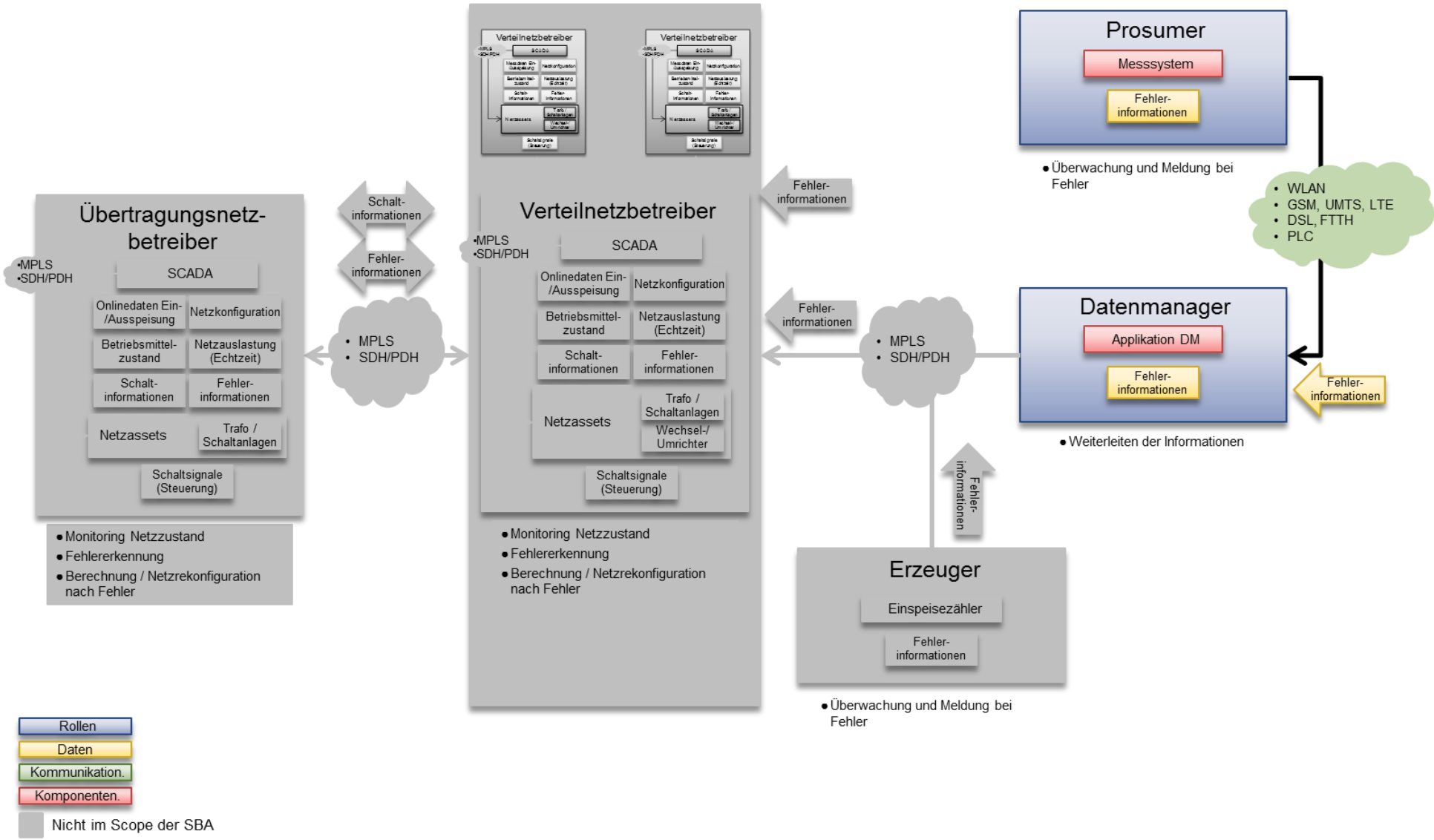
A.4.4. UC4 - Systemdienstleistungen



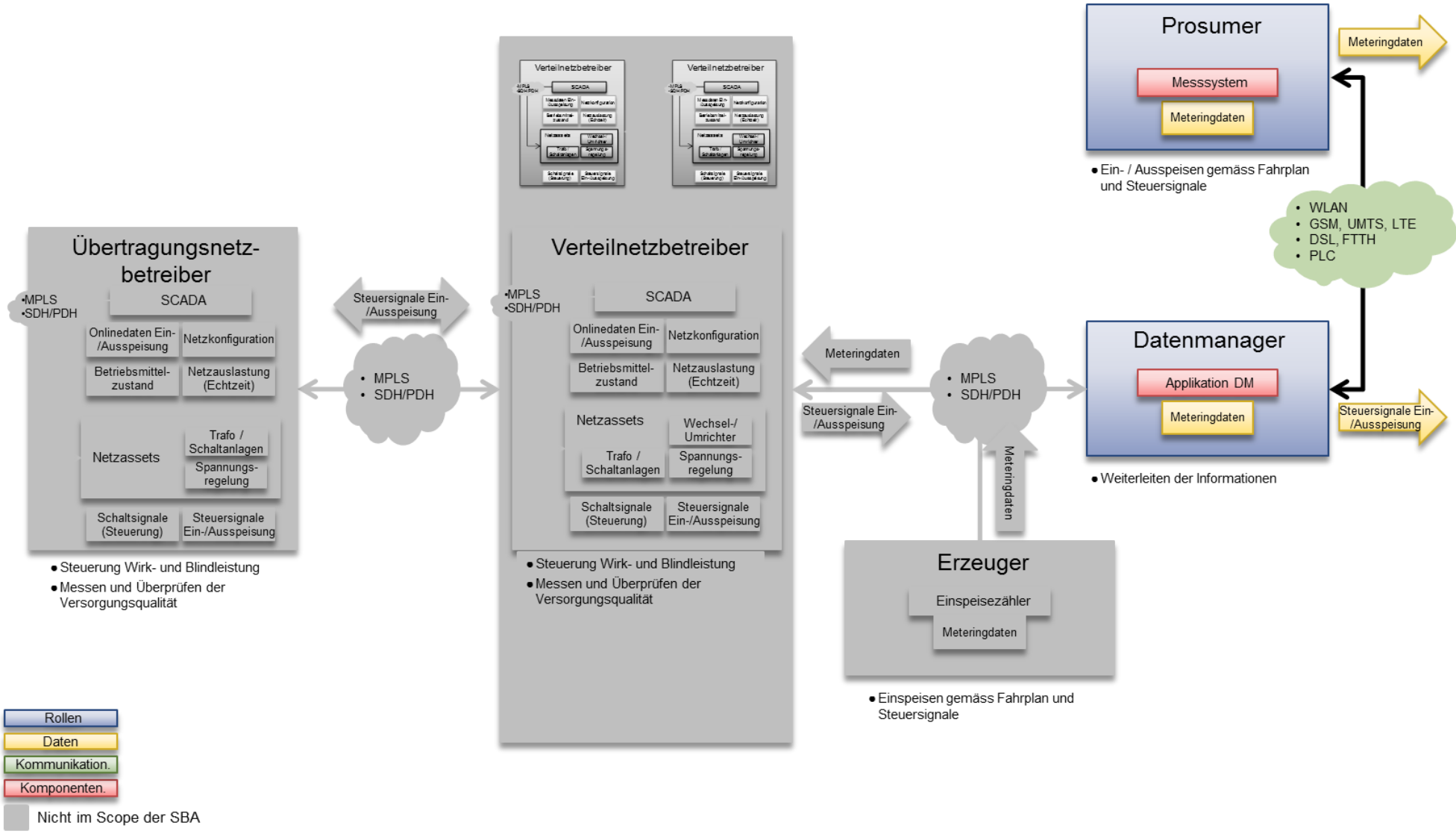
A.4.5. UC5 - Regionale Flexibilitäten



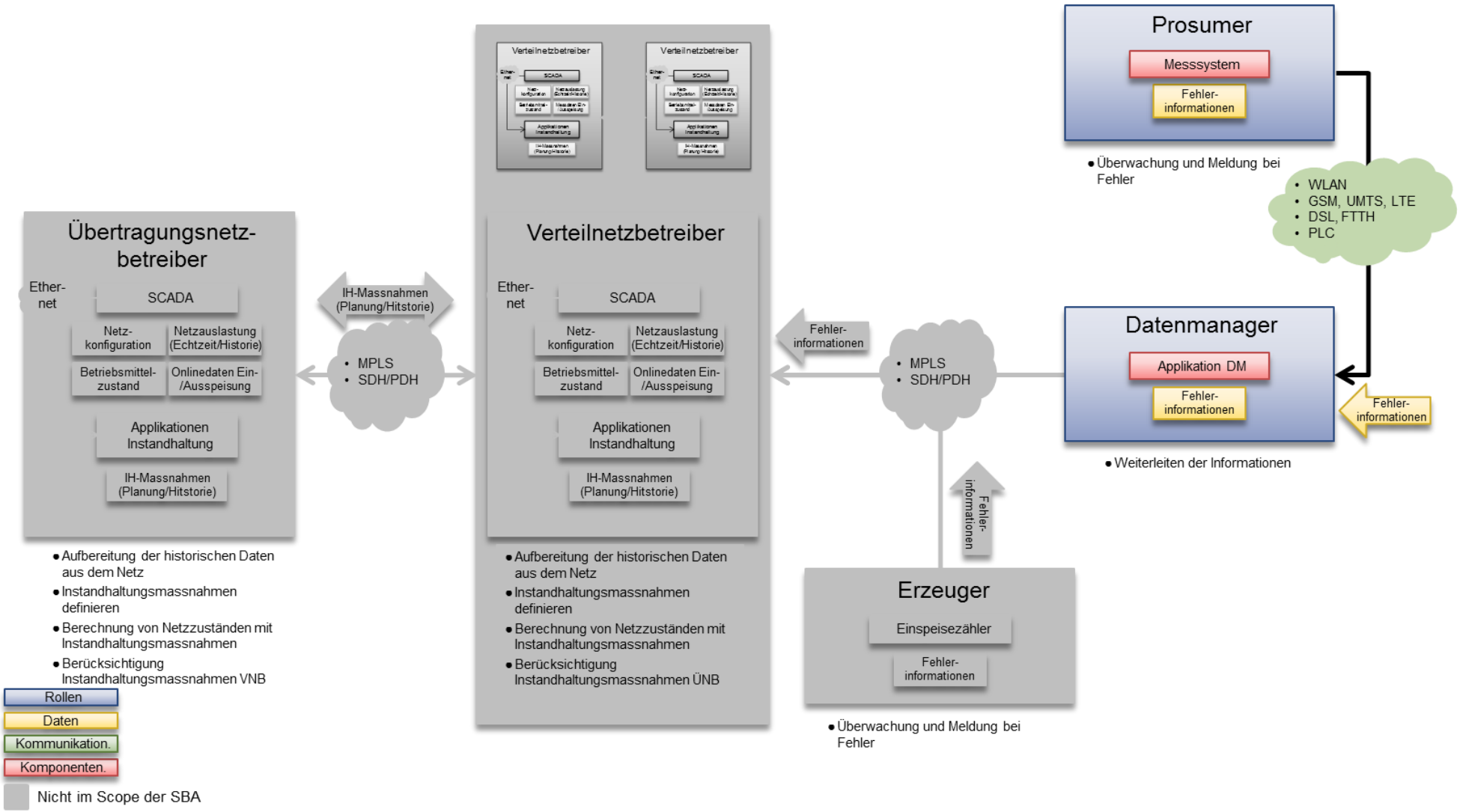
A.4.6. UC7 - Fehlererkennung und Netzrekonfiguration



A.4.7. UC8 - Steuerung Wirk- und Blindleistung



A.4.8. UC9 - Instandhaltung



A.4.9. UC12 - Zeitliche Flexibilisierung Ein-/Ausspeisung