Ansätze zur Gewährleistung der IKT-Sicherheit von intelligenten Messsystemen bei Endverbrauchern

Untersuchung im Auftrag des

Bundesamtes für Energie BFE

3003 Bern

Abschlussbericht
31.10.2015

Projektteam
Dr. Volker Zeuner, vZsecurITy
Andreas Grossenbacher, aartesys

Begleitung seitens BFE
Dr. Matthias Galus (Projektleitung)
Bruno Le Roy

vZsecurITy
Vorstadtstrasse 192
CH-4712 Laupersdorf
Tel. +41 79 251 12 00
http://www.vzsecurity.ch/

Management Summary

Smart Metering Systeme werden im Rahmen der Energiestrategie 2050 (ES2050) als intelligente Messsysteme beim Endverbraucher bezeichnet. Unter diesen Systemen werden elektronische Zähler mit mehreren Schnittstellen verstanden, die über eine bidirektionale Kommunikationsinfrastruktur mit einem zentralen Datenverarbeitungssystem verbunden sind[1]. Sie führen vermehrt Informations- und Kommunikationstechnologien (IKT) in den Betrieb der Energieversorgungsunternehmen ein. Es bestehen über eine Vernetzung verschiedener Informationsverarbeitungssysteme beim Energieversorgungsunternehmen Schnittstellen zu Vorgängen im Abrechnungs- und Verwaltungssystem sowie zum Betrieb der elektrischen Netze. Smart Metering Systeme können so verschiedene Risiken für die kritischen Infrastrukturen bilden, unter anderem können sie etwa ein Eingangstor zu nachgelagerten Systemen oder durch direkte Manipulation eine Gefahr für den stabilen Netzbetrieb sein. Sie sind so ein Bestandteil der Stromverteilungsnetze und damit ein Teil einer kritischen Infrastruktur und es liegt daher auf der Hand, dass die Smart Metering Systeme informationstechnisch gesichert sein müssen. Die konkreten Gefährdungen und somit Risiken, welche durch Smart Metering Systeme für das Stromversorgungsystem eingeführt werden, sind in einer Schutzbedarfsanalyse durch eine unabhängige Entität – vornehmlich die Bundesverwaltung – zu identifizieren und zu analysieren. Vorliegende Studie geht grundsätzlich von bestehenden, ernst zu nehmenden Gefährdungen sowie Risiken aus, was im Allgemeinen durch internationale Erfahrungen und Vorgehensweisen gestützt wird.

Die vorliegende Studie analysiert die grundsätzlich möglichen Ansätze, welche für eine Sicherung der Infrastruktur in Frage kommen. Die Ansätze zur Sicherung der Systeme werden durch die Freiheitsgrade „Tiefe von Definition der Sicherheitsanforderungen“ sowie Art und Weise einer „Validierung der Umsetzung von Sicherheitsanforderungen“ bestimmt. Die Analyse der Ansätze zur Sicherstellung eines vertrauenswürdigen Betriebs der Smart Metering Systeme fokussiert sich nach einem Ausschlussverfahren auf 4 sinnvolle und weiter vertiefte Varianten. Die vertiefte Analyse dieser 4 Varianten zeigt, dass Forderungen von Sicherheitsfunktionalitäten sowie die Validierung ihrer Implementierung grundsätzlich sinnvoll sind. Ein Ansatz zur Sicherung der Systeme sollte die folgenden wichtigen Punkte beinhalten:

- IKT-Sicherheitsanforderungen für intelligente Messsysteme in der Schweiz, wie sie werden übergreifend gefordert, feingranular spezifiziert und sind einheitlich.
- Die IKT-Sicherheitsanforderungen werden für einzelne Komponenten – auch Prüfgegenstände genannt – der intelligenten Messsysteme festgelegt. Die Abgrenzung der Komponenten und die Anforderungen an sie müssen die Sicherheit des Gesamtsystems gewährleisten.

[1] Vergleiche hierzu Bundesamt für Energie. (2014). Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz.

- Die Anforderungen gewährleisten einen umfassenden Schutz vor den in der Schutzbedarfsanalyse identifizierten Gefährdungen und härten Komponenten wie auch das Gesamtsystem.
- Eine Prüfung der Implementierung der geforderten IKT-Sicherheitsfunktionalitäten pro Prüfgegenstand wird durchgeführt.
- Die Prüfung der Prüfgegenstände erfolgt gemäss im Vorfeld erarbeiteter Prüfschemata, die auf die IKT-Sicherheitsanforderungen und auf die Prüfgegenstände zugeschnitten sind. Das Prüfschema definiert wonach geprüft werden sollte.
- Die Prüfschemata gewährleisten die Nachweise der Korrektheit und Wirksamkeit der Funktionalitäten. Zudem sichern sie die Reproduzierbarkeit der Prüfergebnisse und eine hohe Qualität der Prüfungen insgesamt.
- Die Prüfung der Anforderungen erfolgt durch akkreditierte Prüfstellen und dort durch fachlich qualifiziertes Personal. Detaillierte Dokumentationen der Prüfungen werden erstellt.
- Eine Kontrollstelle sichert und überwacht die Qualität des Validierungsprozesses und der Prüfstellen. Sie erteilt die Zulassung der Geräte nach bestandener Prüfung und kann ggf. zyklische Nachprüfungen im Betrieb in jedem Fall aber bei Unregelmässigkeiten im Betrieb verlangen.

Diese wichtigen Punkte werden im durch diese Studie vorgeschlagenen Ansatz zur Sicherung der Smart Metering Systeme über eine „Konformitätsprüfung mit einem zugrunde liegenden Schutzprofil“ (Variante 3) umgesetzt. Der gewählte Ansatz sieht zunächst vor, die Gefährdungen über das Smart Metering System und die sich ergebenden Risiken durch den Bund im Rahmen einer Schutzbedarfsanalyse zu untersuchen. Der Ansatz sieht weiter subsidiär organisierte Arbeitsgruppen aus unabhängigen IKT-Experten, Herstellern und Branchenvertreter vor, die gemeinsam die nötigen, technischen Grundlagen für den beschriebenen Prozess erarbeiten. Die Arbeitsgruppen definieren also die Prüfgegenstände des Smart Metering Systems, grenzen diese gegeneinander ab, definieren die Anforderungen und geeignete Prüfschemata für diese. Der Bund ist insofern involviert, als dass er die Sicherung der intelligenten Messsysteme nach Stand der Technik und die Prüfung der subsidiär erarbeiten Anforderungen durch unabhängige, akkreditierte Prüfstellen fordert und über eine Kontrollstelle für eine gleichbleibend hohe Qualität der eingeführten intelligenten Messsysteme sorgt. Die Kontrollstelle prüft die Prüfergebnisse auf Basis der erstellten Prüfberichte, beaufsichtigt die Prüfstellen und erteilt die Zulassungsberechtigung bei zufriedenstellenden Prüfergebnissen. Sie kann Nachbesserungen der Smart Metering Systeme verlangen oder bei Unregelmässigkeiten im Betrieb Nachprüfungen anordnen.

In der von den Autoren favorisierten Variante sind die möglichen Freiheitsgrade für die Ausgestaltung einer schweizerischen Konformitätsprüfung der Prüfgegenstände hoch. Der Ansatz sieht den Bund involviert bei der Schutzbedarfsanalyse, der Benennung einer Kontrollstelle,

deren Ausstattung mit Kompetenzen, die es ihr erlauben, die beschriebenen Aufgaben zu vollziehen und der Forderung von sicheren intelligenten Messsystemen. Der Bund ist also miteinzubeziehen bei der Erarbeitung der technischen Grundlagen, welche allerdings subsidiär durchgeführt werden. Anschliessend entwickeln Hersteller die Systeme und lassen sie von akkreditierten Prüfstellen prüfen. Die Kontrollstelle kontrolliert die Prüfergebnisse u.a. auf Basis der Prüfberichte erteilt eine produktgebundene Zulassungsermächtigung. Bei defizitären Prüfungen oder Unregelmässigkeiten veranlasst sie Nachbesserungen durch den Hersteller. Die Hersteller liefern im Anschluss konforme Systeme inklusive Benutzer- sowie Prüfdokumentation an die Betreiber und nehmen sie gemäss Anforderungen in Betrieb. Während des Betriebs gewährleistet der Hersteller den nötigen Support. Die Kontrollstelle kann zyklische Nachprüfungen verlangen oder aber bei auffälligen Unregelmässigen Nachprüfungen beim Betreiber anordnen.

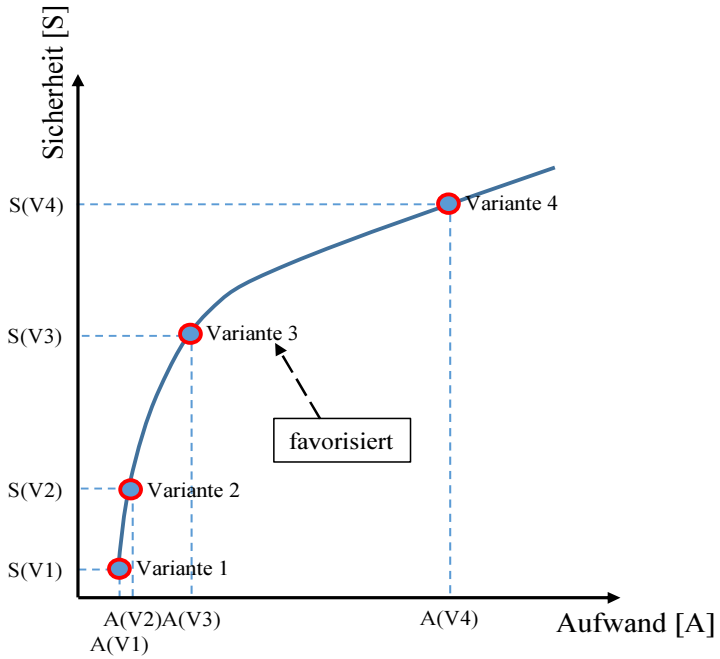

Abbildung A: Mögliche Varianten zur Gewährleistung der IKT-Sicherheit und ihr Verhältnis von Aufwand zu erreichter Sicherheit. Qualitative Abbildung.

Dieser Ansatz erlaubt, Anforderungen, Prüfschemata sowie Prüfgegenstände individuell für die nationalen Belange festzulegen und bietet die nötige Flexibilität hinsichtlich Schweiz spezifischer und pragmatischer Lösungen. Er reduziert den Regulierungsaufwand auf das Wesentliche und ermöglicht eine potentiell hohe Akzeptanz seitens Betreibern und Herstellern. Der Ansatz weist ein sinnvolles bzw. gutes Verhältnis von Aufwand zu erreichtem Sicherheitsniveau auf, wie Abbildung A zeigt. Der Aufwand der Variante 3 resultiert in einem überproportionalen Gewinn an Sicherheit im Vergleich zu den anderen Varianten. Variante 4 bietet zwar das höchste Sicherheitsniveau im Ergebnis erscheint aber vom Aufwand her kaum tragbar.

Zu statuieren ist ferner, dass der favorisierte Ansatz nicht nur für intelligente Messsysteme beim Endverbraucher anwendbar ist, sondern sich auch auf andere IKT-Strukturen bzw. auf andere Branchen übertragen lässt und somit zu hebende Synergien aufweist.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AT	Österreich
BFE	Bundesamt für Energie
BMWi	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CH	Schweiz
D	Deutschland
EnWG	Energiewirtschaftsgesetz
ES2050	Energiestrategie 2050
EU	Europäische Union
EVU	Energieversorgungsunternehmen
FDL	Finanzdienstleistung
IKT	Informations- und Kommunikationstechnik
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organisation for Standardization
METAS	Eidgenössisches Institut für Metrologie
NIST	National Institute for Standards and Technology
OEM	Original Equipment Manufacturer
SAS	Schweizerische Akkreditierungsstelle
SCADA	Supervisory Control and Data Acquisition
SKI	Schutz Kritischer Infrastrukturen
SMGW	Smart Meter Gateway
StromVG	Stromversorgungsgesetz
TR	Technische Richtlinie

1. Hintergrund und Zielsetzung

Das Stromnetz wird intelligenter werden und zunehmend Informations- und Kommunikationstechnologien (IKT) vor allem auf den tieferen Netzebenen enthalten. In internationalen Gremien finden Aktivitäten in der Standardisierungen für diese Entwicklung statt, die auch darauf abzielen, das intelligente Stromnetz der Zukunft sicher zu machen. Die Aktivitäten sind oftmals dadurch gekennzeichnet, dass sie sich auf infrastrukturelle Aspekte, z.B. Schnittstellen in Prozessen beziehen. Es werden existierende Standards harmonisiert bzw. ergänzt [1]. In der Schweiz hat man sich in der Vergangenheit auf die höheren Netzebenen fokussiert, ein Bedarf weitere Arbeiten vor allem im Bereich der Verteilnetze anzustossen war nicht dringend [2].

Auch die Schweiz wird ihre Stromnetze in Richtung intelligenter Netze weiterentwickeln. Anfang des Jahres 2015 publizierte das Bundesamt für Energie (BFE) die Smart Grid Roadmap für die Schweiz [3]. Sie stellt einen konsensbasierten Leitfaden zur Implementierung intelligenter Netze in der Schweiz dar. Auf Basis einer Vision leitet sie übergreifende Funktionalitäten intelligenter Netze ab und analysiert die zur Umsetzung der Funktionalitäten nötigen Technologien, deren Kombination und nötige Standards. Die betrachteten Technologien umfassen auch das Smart Metering als eine wesentliche Lösung. Das BFE hat schon früh eine Kosten-Nutzen Analyse hinsichtlich einer flächendeckenden Einführung dieser Systeme erstellen lassen, die klar positiv ausfiel [4]. Dementsprechend schafft das erste Massnahmenpaket der Energiestrategie 2050 (ES2050) über die vorgesehene Anpassungen zu Art. 15 und Art. 17 Stromversorgungsgesetz (StromVG) geeignete Rahmenbedingungen für eine Einführung von Smart Metering Systemen – oder wie es in der ES2050 heisst „von intelligenten Messsystemen beim Endverbraucher“ [5]. Der Gesetzesentwurf sieht eine Delegationsnorm an den Bundesrat vor, der technische Mindestanforderungen an diese Systeme vorgeben kann. Im November 2014 hat das BFE ein Grundlagendokument zur Einführung der Smart Metering Systeme publiziert [6], in dem erstmals eine klare Begriffsdefinition und Abgrenzung dieser Systeme niedergelegt wurde. Die Smart Metering Systeme bestehen aus mehreren Komponenten. Hierzu zählen das intelligente Messgerät, d.h. der eigentliche Smart Meter, eine bidirektionale Kommunikationsinfrastruktur, ein zentrales Datenverarbeitungssystem sowie eine Visualisierungsplattform. Die intelligenten Messgeräte umfassen elektronische Elektrizitätszähler, eine Kommunikationsschnittstelle (WAN) zur bidirektionalen Kommunikationsinfrastruktur sowie weitere Schnittstellen. Das Grundlagendokument idetifiziert sinnvolle Einführungsmodalitäten und technische Mindestanforderungen an die Messsysteme sowie an die Messgeräte und die Kommunikationsinfrastruktur selbst. Im Rahmen der Arbeiten zum Grundlagendokument wie auch zur Smart Grid Roadmap wurde ein Bedarf festgestellt, Datensicherheit in Smart Grids und vor dem Hintergrund der regulatorischen Einführung von Smart Metering Systemen vertieft zu betrachten, und sinnvolle Lösungen zu suchen, um deren Sicherheit zu gewährleisten [3,7].

Grundsätzlich basieren die Funktionen und das Potenzial intelligenter Messsysteme auf einer Nutzung von IKT. Smart Metering Systeme erfüllen neben wichtigen Aufgaben im Strommarkt

auch gewisse Aufgaben in der Netzplanung und sogar im Netzbetrieb. Sie liefern Daten für Abrechnungssysteme, sie stellen zusammen mit zentralen Datenverarbeitungssystemen Daten für Bilanzgruppen und für den Übertragungsnetzbetreiber zur Verfügung, um eine ausgeglichene Leistungsbilanz zu prüfen und können für Prognosewerkzeuge verwendet werden. Daten in aggregierter Form können im Netzplanungsprozess zur Überwachung der Versorgungsqualität, z. B. von Ausfällen, oder zur Beobachtung der Spannungsqualität im Netzbetrieb genutzt werden. Die intelligenten Zähler sind über eine IKT-Infrastruktur des Netzbetreibers also mit anderen Systemen verbunden, die für Netzbetrieb verwendet werden, so z. B. SCADA-Systemen. So macht die Nutzung der Smart Metering Systeme sie auch zum Teil einer kritischen Infrastruktur – nämlich des Stromnetzes. Deswegen ist unbedingt eine Aufarbeitung und Darlegung zu etablierender Prozesse zur Gewährleistung der Datensicherheit[2] intelligenter Messsysteme vorzunehmen. Es ist offensichtlich, dass Endkunden einen vertrauenswürdigen Betrieb erwarten, welcher u.a. ihre Rechte als Konsumenten bzw. als Kleinanbieter lokal erzeugter elektrischer Energie nicht nachteilig tangiert. Sie erwarten darüber hinaus Systeme, deren Software und Hardware so entwickelt wurden, dass sie nicht durch unautorisierte Zugriffe auf die zugrunde liegende IKT kompromittiert werden können und dadurch unter Umständen die allgemeine Versorgungssicherheit gefährdet wird.

Die Erfüllung der oben angeführten Erwartungen unterschiedlicher Interessengruppen ist durch entsprechende IKT-basierte Angriffe oder externe Störungen bedroht. Den daraus resultierenden Risiken müssen geeignete Massnahmen der Datensicherheit entgegenstehen. So müssen geeignete Produkte und Systeme eingesetzt werden, die als Einheit bezüglich der Effizienz ihrer IKT-Sicherheitsfunktionalitäten geprüft sind. Arbeiten die Einzelkomponenten der Einheit in einer komplexen IKT-Umgebung zusammen, muss für diese Umgebung sinnvollerweise ein übergeordnetes IKT-Sicherheitskonzept greifen. In der Umsetzung dieser Konzepte werden oft Informationssicherheitsmanagementsysteme (ISMS) gemäss der ISO27000-Reihe angewendet. Die ISO27000-Reihe enthält auch spezifische Standards für den Energiebereich. Es bestehen also bereits technisch geeignete Herangehensweisen zur Gewährleistung der IKT-Sicherheit in den übergreifenden Systemen der Energieversorgungsunternehmen (EVU). Deshalb stellt sich vielmehr die Frage, inwiefern weitere technische Anforderungen über die vom BFE festgehaltenen, möglichen Mindestanforderungen [6] hinaus bei einer regulatorisch vorgegebenen Einführung an die Smart Metering Systeme gestellt werden sollten, damit diese in der IKT-Umgebung der EVU sicher betrieben werden können.

Die Erfahrung aus anderen europäischen Staaten zeigt, dass für einen vertrauenswürdigen Betrieb der Smart Metering Systeme Sicherheitsanforderungen definiert werden müssen. Diese variieren von Staat zu Staat in Detailgrad und Tiefe. Es stellt sich für die Schweiz die Frage, wie die Datensicherheit von Smart Metering Systemen gewährleistet werden kann, welche An-

[2] Als Synonym wird im Dokument auch von IKT-Sicherheit generell gesprochen, die systemisch weiter gefasst ist als Datensicherheit.

sätze hierfür sinnvollerweise in Frage kommen und wie die entsprechenden Prozesse auszugestalten sind. Durch die Beantwortung dieser Fragen kann von Beginn an bei einer regulatorisch geforderten Einführung die Sicherheit der Smart Metering Systeme in Design und Einführung berücksichtigt werden. So können Kosten gespart werden, da eine Nachrüstung bereits im Betrieb stehender Systeme sich aus Erfahrung komplex und aufwändig gestaltet. Zudem würde ein nicht vertrauenswürdiger Betrieb der Systeme die Akzeptanz dieser in der Bevölkerung deutlich schmälern.

Die vorliegende Studie untersucht daher grundsätzlich mögliche Ansätze, wie die Datensicherheit von Smart Metering Systemen gewährleistet werden kann und ordnet diese vor dem Hintergrund ihrer Sinnhaftigkeit, Umsetzbarkeit und ihres Aufwands. Dazu wird zunächst in Kapitel 2 eine Rundschau geboten, welche Ansätze zur Gewährleistung der Datensicherheit von Smart Metering Systemen in anderen Ländern verfolgt werden. Weiter wird in Kapitel 2 kurz dargelegt, welche Ansätze in anderen Branchen in der Schweiz Anwendung finden, um die dort betriebene IKT-Infrastruktur zu sichern. Kapitel 3 zeigt allgemein, welche Ansätze für Smart Metering Systeme in der Schweiz existieren und bewertet ausgewählte nach qualitativen Kriterien. Aus der Auswahl an Ansätzen wird in Kapitel 4 eine sinnvolle Lösung konkret ausgestaltet und beschrieben. Es werden einzelne Schritte aufgezeigt, um etwaig notwendigen regulatorischen Anpassungsbedarf zu identifizieren. Kapitel 5 zieht dann entsprechend Schlussfolgerungen.

2. Internationale und nationale Ansätze zur Gewährleistung der Datensicherheit

2.1 Internationale Ansätze im Bereich Smart Metering

2.1.1 Österreich

In Österreich wurde Ende Dezember 2010 die Novelle des Energiewirtschafts- und Organisationsgesetzes [8] beschlossen. Sie enthält erstmals Vorgaben über eine österreichweite Einführung von Smart Metering Systemen. Die E-Control hat als Regulierungsbehörde Verordnungsermächtigungen erhalten. So sollen etwa die Art und der Umfang der Funktionsanforderungen, der Dateninhalt oder die an den Kunden bereitzustellenden Informationen durch die E-Control per Verordnung geregelt werden. Dazu hat die E-Control mehrere Verordnungen erlassen. Die erste dieser Verordnungen der E-Control wurde 2011 beschlossen und enthält die technischen Mindestanforderungen [9]. Hinsichtlich Sicherheit wird in dieser Verordnung festgehalten, dass die Geräte und die zur Kommunikation verwendeten Technologien nach anerkanntem Stand der Technik abzusichern und zu verschlüsseln sind. Die Erläuterungen halten fest, dass der „Stand der Technik“ ein auf einschlägigen, wissenschaftlichen Erkenntnissen beruhender Entwicklungsstand technischer Verfahren, Einrichtungen und Betriebsweisen ist, dessen Funktionstüchtigkeit erprobt ist. Namentlich wird darauf hingewiesen, dass nur die Geräte, nicht aber die gesamte IKT-Infrastruktur, welche sich auch bei den Netzbetreibern befindet, zu sichern ist. Die Sicherung der Geräte wird dem Netzbetreiber überlassen. Weitere Anforderungen, die über die Sicherung der Geräte hinausgehen und auf das gesamte Smart Metering System abzielen, sind nicht weiter spezifiziert. Weiter erliess die E-Control 2012 eine Verordnung zur Einführung intelligenter Messgeräte [10]. Bis Ende 2019 soll ein Abdeckungsgrad von 95% der Messpunkte erreicht werden. Dies wird jedoch insofern relativiert, als dass auf die technische Machbarkeit der Einführung verwiesen wird. Des Weiteren hat die E-Control die Datenformat- und Verbrauchsinformationsdarstellungsverordnung geändert, um Vorgaben zu machen, wie mit den über Smart Metering Systeme aufgenommen Daten umzugehen ist und welche Daten den Verbrauchern in welcher Form zugestellt werden sollen [11].

Im Rahmen der Arbeiten zur Festlegung des Standes der Technik zur Absicherung der Smart Meter führte der Regulator zwischen 2012 und 2014 zusammen mit der österreichischen Elektrizitätswirtschaft, dem Übertragungsnetzbetreiber und Bundesministerien ein auf die gesamte Elektrizitätswirtschaft ausgerichtetes Cyber-Security Projekt durch, das insbesondere auch Fragen bezüglich Smart Metering Systeme beantworten sollte. Ziel der gemeinsamen, auf freiwilliger Kooperation beruhenden Initiative war es, in einem strukturierten, auf internationalen Standards basierenden Analyse- und Bewertungsprozess systemrelevante Risiken für die Versorgungssicherheit im Strombereich durch die Nutzung von IKT zu beleuchten [12]. Basierend auf diesen Erkenntnissen wurde ein Katalog von Sicherheitsanforderungen für Smart Metering Systeme seitens der österreichischen Elektrizitätswirtschaft entwickelt [13]. Er folgt der auf

einer Metaebene durch die Verordnung [9] vorgegebenen Architektur der Systeme, konkretisiert diese und definiert schliesslich Teilsysteme, die unterschiedliche Sicherheitsanforderungen erfüllen müssen. Die spezifizierte Architektur, welche als Grundlage für die Definition der Anforderungen herangezogen wird, basiert auf dem Standard NIST 7628 [14] und ist eine Konkretisierung international vorgeschlagener Standards [15]. Zu den Anforderungen zählen unter anderem bestimmte Verschlüsselungsverfahren. Einzelne Anforderungen unterscheiden sich in ihrer Tiefe und ihrem Detailgrad teilweise stark voneinander. Dieses Dokument definiert den in der österreichischen Regulierung referenzierten „Stand der Technik. Eine Prüfung betreffend der Umsetzung von Sicherheitsanforderungen wird in der durchgeführten Risikoanalyse als ein wichtiges Handlungsfeld identifiziert, jedoch nicht weiter konkretisiert.

2.1.2 Deutschland

Gemäss dem in 2012 angepassten Energiewirtschaftsgesetz (EnWG) dürfen in Deutschland in bestimmten Fällen nur noch bestimmte Messsysteme, nach schweizerischem Verständnis intelligente, eingebaut werden. Dies ist der Fall bei Neubauten, bei grösseren Renovierungen, enverbrauchern mit mehr als 600 kWh Verbrauch pro Jahr und bei Produktionsanlagen erneuerbarer Energie über 7 kW Anschlussleistung. In allen anderen Fällen soll dies nur geschehen soweit dies technisch und wirtschaftlich vertretbar ist (siehe §§21c ff. EnWG). In Deutschland werden grundsätzlich intelligente Zähler und intelligente Messsysteme unterschieden. Der Unterschied liegt in der kommunikationstechnischen Anbindung begründet. Intelligente Zähler sind grundsätzlich digitale Zähler, die zu intelligenten Messsystemen erweiterbar sind. Intelligente Zähler verfügen nach deutschem Verständnis über keine bidirektionale Kommunikationsverbindung mit einem zentralen System zur Auslesung und/oder Steuerung. Intelligente Messsysteme hingegen binden intelligente Zähler ein und müssen gewissen Mindestanforderungen genügen, die in einer Messsystemverordnung noch näher festgehalten werden sollen. Sie müssen jedoch in jedem Fall gemäss §21e EnWG in Verordnungen weiter zu spezifizierenden Schutzprofilen und Anforderungen an Interoperabilität entsprechen. Sie sind aus der Ferne auslesbar und steuerbar. Diese Systeme verfügen in Anlehnung an §21d Energiewirtschaftsgesetz (EnWG) über eine Messeinrichtung zur Erfassung elektrischer Energie, bestehend aus einem Zähler und einer Kommunikationseinheit, welche als Smart Meter Gateway (SMGW) bezeichnet wird [16].

Aufgrund der Verarbeitung und Zusammenführung personenbezogener Verbrauchsdaten in Messsystemen sowie möglicher negativer Rückwirkungen auf die Energieversorgungssicherheit ist die Sensibilisierung in Deutschland vergleichsweise hoch. Bekannt gewordene Hackerangriffe auf intelligente Messsysteme, unter anderem in den USA, resultierten in einem zunehmenden Bedarf an sicheren Lösungen bei der Einführung intelligenter Messsysteme in Deutschland. Die Sicherheit und der Datenschutz waren also von Anfang an ein zentrales Thema in

Deutschland. So wurde auch hier zunächst eine Gefährdungs-, Risiko- und Schutzbedarfsanalyse durchgeführt[3]. Auf Basis dieser Analyse wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) durch das Bundesministerium für Wirtschaft und Technologie (BMWi) im September 2010 mit der Erarbeitung eines Schutzprofils[4] sowie im Anschluss mit der Erarbeitung einer technischen Richtlinie (TR) für die Kommunikationseinheit eines intelligenten Messsystems beauftragt, um einen einheitlichen technischen Sicherheitsstandard für alle Marktakteure zu gewährleisten. Verweise auf das Schutzprofil und technische Richtlinien wurden 2012 im EnWG verankert. Das „7 Eckpunkte Paket intelligente Netze“ nennt insgesamt drei relevante Verordnungen, die die Einführung von Smart Metering Systemen in Deutschland gestalten werden: die Messsystemverordnung, die Datenkommunikationsverordnung und die Einführungsverordnung [17]. Mittlerweile hat das BMWi jedoch ein Digitalisierungsgesetz auf den Weg gebracht. Es bündelt die Anliegen der angestrebten Verordnungen auf gesetzlicher Stufe. Ob weitere Verordnungen zur Konkretisierung dieses Gesetzes erlassen werden ist derzeit noch unklar [18].

Das Schutzprofil [19,20] legt erforderliche Mindestsicherheitsanforderungen fest. Es wurde auf Basis des „Common Criteria (CC)“-Standards entwickelt. Zukünftige SMGW müssen hinsichtlich der Implementierung des Schutzprofils geprüft werden und erhalten nach positivem Prüfergebnis ein Zertifikat als verbindlichen Nachweis über die Erfüllung der Schutzziele. Zur Gewährleistung von Interoperabilität und der technischen Umsetzung der Sicherheitsanforderungen des Schutzprofils hat das BSI Vorgaben in einer technischen Richtlinie (BSI TR-03109) [21] festgehalten. Abbildung 1 zeigt die Bestandteile der technischen Richtlinie. Die Anforderungen sind offensichtlich weitreichend und komplex. Die Hersteller sind derzeit daran, ihre Produkte auf diese Anforderungen hin zu modifizieren.

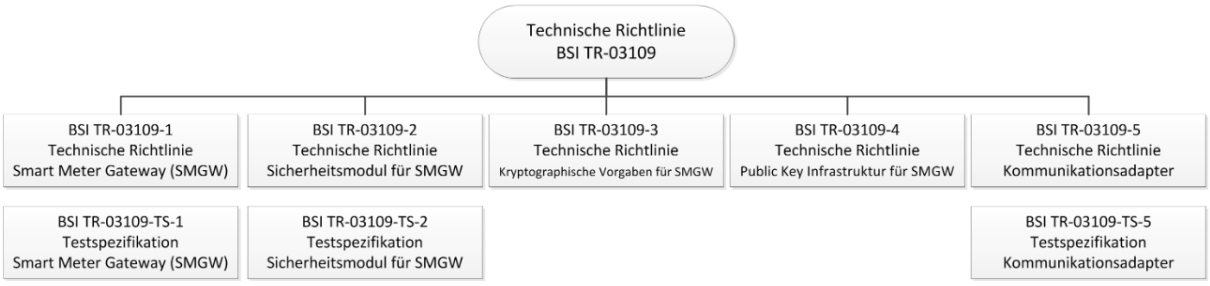

Abbildung 1: Struktur der technischen Richtlinien. Quelle: www.bsi.bund.de

Die Vorgehensweise in Deutschland zeichnet sich durch streng formale Prüfvorgaben und sehr hohe Anforderungen an die intelligenten Messsysteme bzw. an die SMGW aus. Weiter existieren zusätzliche Vorgaben für die Betriebsumgebung. Der Standardisierungsgrad ist sowohl für

[3] Die Studie ist nicht veröffentlicht und daher nicht verfügbar. Das Unternehmen secunet Security Networks AG hat die Studie „Sichere Informations- und Kommunikationstechnologien für das Smart Grid“ zusammen mit einer Anzahl von Konsortialpartnern auch aus der EVU Branche für das BMWi durchgeführt.
[4] Das Schutzprofil wird weitläufig auch als Protection Profile im englischen Sprachgebrauch bezeichnet.

das Anforderungsprofil als auch für den Prüfprozess sehr hoch. Ein Nachweis bezüglich der Einhaltung der technischen Richtlinie erfolgt über vom BSI anerkannte Prüfstellen.

Viele Grundlagen für eine Überprüfung der IKT-Sicherheit von Smart Metering Systemen liegen in Deutschland also seit einiger Zeit vor. Bedauerlicherweise muss festgestellt werden, dass diese Vorreiterrolle noch nicht zu einer erfolgreichen Umsetzung geführt hat. Eine bis dato möglicherweise ungenügende IKT-Sicherheitsaffinität im Bereich des Messwesens in der Stromversorgung sorgt dafür, dass entsprechende Aktivitäten schleppend vorankommen. Dies könnte wiederum der Tatsache geschuldet sein, dass weder Hersteller noch Betreiber frühzeitig in den Entwicklungsprozess eingebunden wurden. Die Situation wurde sicher noch dadurch verschärft, dass ein sehr komplexes Instrumentarium – die CC – seitens IKT-Sicherheitsspezialisten einseitig auf die Situation bei den intelligenten Messsystemen übertragen wurde. Festgehalten kann jedoch werden, dass Deutschland gewisse grundsätzliche Pfeiler eines Sicherheitskonzeptes für Smart Metering Systeme verankert hat. Hierzu zählen eine standardisierte Prüfung (hier: Evaluation gemäss CC) der Implementierung der Anforderungen durch unabhängige Prüfstellen, ein standardisiertes, stringentes Prüfverfahren grosser Prüftiefe sowie ein strenger Anforderungskatalog. Zur Zulassung der Systeme muss nach erfolgreicher Prüfung noch ein vom BSI herausgegebenes nationales IKT-Sicherheitszertifikat erlangt werden.

Derzeit werden in Deutschland zudem bei Netzbetreibern hinsichtlich IKT-Sicherheit Rahmenbedingungen über das Schutzprofil für Smart Metering hinaus gesetzt. Erst kürzlich publizierte die Bundesnetzagentur (BNetzA) weiterführende Anforderungen, die von den Leitsystemen der Netzbetreiber erfüllt werden müssen [22]. Informationssicherheitsmanagementsysteme (ISMS) bei den Netzbetreibern sind zu etablieren, die standardisierten Anforderungen genügen [23, 24] und mindestens Telekommunikations- sowie elektronische Datenverarbeitungssysteme umfassen. Die Netzbetreiber werden angehalten, den ordnungsgemässen Betrieb der betroffenen IKT-Systeme sicherzustellen, indem sie Risiken bewerten und durch geeignete Massnahmen behandeln. Hiervon sind Leitsysteme, Systembetrieb, Übertragungstechnik und Sekundär- sowie Automatisierungstechnik betroffen. Weiter wird gefordert bis Ende 2015 zumindest eine Person pro Netzbetreiber zu benennen, die als Ansprechpartner bezüglich IKT-Sicherheit der BNetzA dienen soll. Des Weiteren sollen bis Anfang 2018 alle ISMS der Netzbetreiber gemäss entsprechender Normen zertifiziert werden. Das Schutzprofil für Smart Metering Systeme und diese weitergehenden Sicherheitsstandards sollen nebeneinander implementiert werden.

2.1.3 USA

Die Einführung von Smart Metering Systemen wird auch seit längerer Zeit in den Vereinigten Staaten von Amerika (USA) diskutiert. Derzeit sind dort ca. 30% der Endverbraucher mit Smart Metering Systemen ausgestattet [25]. Die Einführung von Smart Metering Systemen ist von Bundesstaat zu Bundesstaat anders geregelt. Die Mehrzahl der Bundesstaten, in denen Smart Metering Systeme derzeit Anwendung finden, hat jedoch gewisse regulative Vorgaben hinsichtlich der Einführung getroffen oder evaluiert sie. Gerade hinsichtlich Sicherheit der Smart Metering Systeme lässt sich festhalten, dass in den USA kein obligatorischer Prüfungs- oder

Zertifizierungsprozess etabliert ist oder gefordert wird. Die Auswahl der Systeme, ihre technische Ausgestaltung sowie ihre Einführung werden weitgehend den EVU überlassen. Damit variieren die technischen Funktionalitäten der Systeme und die einzelnen Vorgehensweisen zur Einführung landesweit sehr stark. Um jedoch die Einführung dieser Systeme zu unterstützen, gibt es einen Anzahl Quellen, welche freiwillige Richtlinien und Empfehlungen sowie Best-Practice Leitfänden darstellen an denen sich die EVU, die eine Einführung planen, orientieren können [14, 26, 27, 28]. Es existieren demnach viele Empfehlungen in den USA, um die Cyber-Sicherheit der Systeme zu gewährleisten, keine von ihnen ist jedoch abschliessend massgebend. Vorgaben oder Forderung für eine wie auch immer geartete Prüfung der Sicherheit dieser Systeme sind nicht existent.

2.2 Nationale Ansätze zur Sicherung von IKT Infrastrukturen anderer Branchen in der Schweiz

Die Überprüfung der IKT-Sicherheitseigenschaften eines Produktes oder Systems besitzt immer dann eine gewisse Bedeutung, wenn im Betrieb der IKT ein bestimmtes Risiko zu kontrollieren ist bzw. Haftungsfälle durch fehlerhafte Implementierung, mangelhafte Sicherheitseigenschaften, Hackerangriffe oder Fahrlässigkeit möglich sind. Aus systemischen Gründen ist die Verwendung von IKT in der Stromversorgung und dort in den tieferen Netzebenen (ab Netzebene 3 abwärts) kaum verbreitet. Dies ändert sich jedoch mit der Einführung von Smart Metering Systemen. Andere Branchen sind von dieser Thematik aber schon länger betroffen.

2.2.1 Finanzdienstleister

In der Finanzbranche entstehen Risiken fast ausschliesslich aus möglichen wirtschaftlichen Haftungsfällen und – natürlich bei publik werden – aus Image-Schäden. Die Risiken leiten sich aus gewissen Verwundbarkeiten ab, die sich z. B. durch Zugangspunkte zum jeweils betriebenen IKT-System ergeben, die ausserhalb des Einflussbereiches des Dienstleisters liegen. Ein Beispiel für ein Gerät ausserhalb des Einflussbereichs des Betreibers ist die Herausgabe von e-Banking Geräten (Geräte mit Software) oder Anwendungen (nur Software). Das Schadenspotential in dieser Branche ist ein rein wirtschaftliches. Grundsätzlich lässt sich feststellen, dass auch in dieser Branche zunächst eine Gefährdungs- und Risikoanalyse durchgeführt wird. Basierend auf dieser Analyse wird ein Schutzbedarf definiert und darauf aufbauend gewisse Vorgaben an Systeme gefordert. Nachdem eine funktionale Abnahmeprüfung durch das jeweilige Unternehmen erfolgt ist, wird ein interner oder externer Penetrationstest durchgeführt. Auf Basis der Ergebnisse werden Einfallstore identifiziert und Handlungsbedarf zur Sicherung dieser ausgewiesen, der schrittweise behoben wird. Zusammenfassend lässt sich statuieren, dass hier keine standardisierte Vorgehensweisen oder Sicherheitsanforderungen existieren, das Thema Sicherheit aber je nach Applikation und wirtschaftlichem Schadenspotential eine vergleichsweise hohe Priorität hat, die individuell und im Einzelfall bearbeitet und gelöst wird.

2.2.2 Pharmabereich

In der Pharmabranche sind Fälle denkbar, bei denen aus mangelnder IKT-Sicherheit Schäden an Leib und Leben resultieren können. Beispielsweise könnte eine manipulierte Prozesssteuerung zu Abweichungen von einer erprobten Rezeptur und damit schädlichen Medikamenten führen. Grundsätzlich existiert eine Qualitätssicherung. Zudem muss angemerkt werden, dass fast immer das zu betrachtende System oder Produkt im unmittelbaren Einflussbereich des zuständigen Betriebs lokalisiert ist und daher ISMS greifen können. Es existiert ein entsprechender kommerzieller – aber nicht öffentlicher – Quasi-Standard [29], der Sicherungsmöglichkeiten aufzeigt. Die Vorgehensweisen basieren auf einer Gefährdungs- und Risikoanalyse dieses Bereiches. Hinsichtlich einer Prüfung etwaiger Sicherheitsfunktionalitäten sind spezielle Penetrationstests möglich aber nicht die Regel. Die bei der Analyse gemäss [29] gefundenen Vorgehensweisen zur Sicherung finden Berücksichtigung im entsprechenden ISMS der Hersteller. Es kann also auch hier zusammenfassend statuiert werden, dass auf Basis einer Risikoanalyse zwar eine quasi-standardisierte Vorgehensweise existiert, um die Datensicherheit zu gewährleisten, es jedoch keine standardisierten Sicherheitsanforderungen gibt.

2.3 Zwischenfazit

Es zeigt sich aus den nationalen und internationalen Erfahrungen und Vorgehensweisen, dass die Identifizierung von Gefährdungen und den damit verbundenen Risiken grundlegend sind für weitere, konkretere Überlegungen. Erst wenn die Risiken, die mit der Einführung von Smart Metering Systemen in der Schweiz verbunden sind, bekannt sind, lässt sich ein Schutzbedarf für diese Infrastruktur ableiten. Dies kann gesamthaft in einer ganzheitlichen Schutzbedarfsanalyse geschehen (siehe Kapitel 4.1).

Die Erstellung einer Schutzbedarfsanalyse ist nicht Teil der vorliegenden Untersuchung. Vielmehr wird für die weiteren Überlegungen im Kapitel 3 davon ausgegangen, dass ein wie auch immer gearteter Schutzbedarf für die in der Schweiz angedachten Smart Metering Systeme besteht. Dies ist eine realistische Annahme, insbesondere vor dem Hintergrund, dass Deutschland und Österreich teilweise sehr weitgehende und spezifische Sicherheitsanforderungen für diese Infrastruktur vorgesehen oder umgesetzt haben. Im Weiteren wird die Frage eruiert, mit welchen Vorgehensweisen ein bestehender Schutzbedarf erfüllt werden kann.

3. Diskussion von Möglichkeiten zur Gewährleistung der Datensicherheit

Die Europäische Kommission hat die Herausforderungen bezüglich Datensicherheit bei der Einführung von intelligenten Messsystemen bei Endverbrauchern erkannt und Grundlagen erarbeitet, wie die Sicherheit der Systeme gewährleistet werden kann. In einer Studie der ENISA [30], der europäischen IKT-Sicherheitsbehörde, wird ein Ansatz dazu vorgeschlagen. Das Dokument spricht sich bezüglich einer Gewährleistung der IKT-Sicherheit explizit dafür aus, dass eine unabhängige Entität die Konformität der Smart Metering Systeme gegenüber IKT-Sicherheitsanforderungen prüft. Dies ist bei weitem jedoch nicht die einzige Möglichkeit, die Sicherheit der Systeme zu gewährleisten und muss auch nicht die sinnvollste Art und Weise für die Schweiz sein. Daher gilt es, die Gestaltungsspielräume für die Schweiz aufzuzeigen. Im Folgenden werden zunächst die Freiheitsgrade zur Gestaltung der Lösungsansätze beschrieben.

3.1 Freiheitsgrade von Ansätzen zur Gewährleistung der Datensicherheit

Für die Sicherstellung eines vertrauenswürdigen Betriebs von Smart Metering Systemen sind grundsätzlich zwei Freiheitsgrade vorhanden. Zum einen ist zu wählen, in welcher Tiefe, mit welcher Verbindlichkeit und wie die IKT-Sicherheitsanforderungen spezifiziert – also festgelegt – werden. Unter Spezifikation sind allgemein schriftliche Informationen zu verstehen, die Eigenschaften näher definieren (Standards, Architektur, Funktionen, etc.). Zum anderen ist zu wählen wie sichergestellt wird, dass die spezifizierten Anforderungen auch realisiert bzw. im Produkt umgesetzt wurden. Typischerweise erfolgt die Sicherstellung durch eine geeignete Validierung[5], d. h. Prüfung, der IKT-sicherheitstechnischen Anforderungen.

3.1.1 Spezifikation von IKT-Sicherheitsanforderungen

Ein IKT-System weist in der Regel nur wenige Sicherheitsfunktionalitäten auf, die für eine/n Benutzer/in unmittelbar zu erkennen sind. Trotzdem sind Sicherheitsfunktionalitäten oft inhärent umgesetzt. So gehen die meisten Benutzer/innen grundsätzlich davon aus, dass ein vertrauenswürdiger Betrieb möglich ist. Während z.B. das Einloggen an einem Computer-Terminal als selbstverständlich erfahren wird, ist die damit verbundene interne Zugriffskontrolle nur für die wenigsten transparent.

Bei Systemen und Produkten, die Funktionalitäten bzgl. Datensicherheit aufweisen, sollte davon ausgegangen werden können, dass die Sicherheitsfunktionalitäten aktiv und wirksam sind und nur wenige spezielle, zusätzliche Konfigurationen benötigt werden. In der Entwicklung

[5] Im Folgenden sollen Validierung und Konformitätsprüfung differenziert verstanden werden. Eine Validierung ist eine streng formale Prüfung der Vollständigkeit und Wirksamkeit geforderter Anforderungen an ein Produkt. Eine Konformitätsprüfung testet, inwiefern die geforderten Funktionalitäten im Produkt umgesetzt wurden und das Produkt damit konform bezüglich der Anforderungen ist. Der Unterscheid liegt also in der formalen Überprüfung der Wirksamkeit.

sollten notwendige Sicherheitsanforderungen bereits einer frühen Phase identifiziert werden, sodass die entsprechenden Funktionalitäten, welche die Anforderungen erfüllen, von Anfang an Eingang in die Systemarchitektur sowie die Implementierung finden (Security by Design). So ist ein vergleichbares Produkt, welches ähnliche Sicherheitseigenschaften nur durch mögliche Konfigurationseinstellungen erhält, ohne dass in einer frühen Entwicklungsphase Sicherheitsanforderungen identifiziert und entsprechende Massnahmen implementiert wurden, im Vergleich deutlich weniger vertrauenswürdig. Ein Produkt, in dessen Lebenszyklus Sicherheitsaspekte frühzeitig berücksichtigt wurden, ist per se das vertrauenswürdigere.

Der erste Aspekt in der Diskussion, wie die Sicherheit von Smart Metering Systemen zu gewährleisten ist, betrifft also die Art und Weise der Spezifikation der Sicherheitsanforderungen in Breite, Tiefe und ggf. auf Basis von Standards. Die Spezifikation wird in einem Anforderungskatalog festgelegt. Dort wird spezifiziert wie konkrete Massnahmen beispielsweise in Bezug auf Autorisierung, Authentifizierung, Verschlüsselung für die einzelnen Komponenten des Systems umzusetzen sind. Weitere Vorgaben können hinsichtlich der Architektur, den Funktionalitäten und des Lebenszyklus der Komponenten sowie für den Betrieb derselben gemacht werden. Die Komponenten des Systems müssen derart geeignet gegeneinander abgegrenzt werden, dass ihre Sicherheitsfunktionalitäten die Sicherheit des Gesamtsystems gewährleisten. Die Vorgaben hinsichtlich den Funktionalitäten können in ihrer Tiefe stark variieren.

Die Spezifikationen der Anforderungen kann frei, standard-konform (semi-formal), schutzprofil-konform (formal) oder mit einem strukturiertem Zustandsmodell beschrieben (streng-formal) erfolgen. Eine freie Spezifikation der Anforderungen kann im Vergleich mehr unentdeckte, individuelle Fehler oder Schwachstellen enthalten. Folgt die Spezifikation einem bestimmten, in entsprechenden Gremien ausgearbeiteten und abgestimmten Standard, so ist dieser in der Regel auf dem Niveau eines Lastenheftes (entspricht der Anforderungsebene) für Hersteller. Diese setzen die geforderten Spezifikationen idealerweise auf dem Niveau eines Pflichtenheftes (entspricht der Umsetzungsebene) in den Funktionalitäten des Produktes um. Falls ein Schutzprofil, wie in Deutschland, für einen bestimmten Anwendungsfall existiert, ist dieses in aller Regel schon auf einem sehr feingranularen Niveau eines Pflichtenheftes vorgegeben. Die Spezifikation der Anforderungen in einem Schutzprofil weist einen deutlich höheren Detailierungsgrad als z.B. ein Industriestandard auf.

Grundsätzlich gilt, dass geeignete Sicherheitsfunktionalitäten gefordert werden sollten, deren Vollständigkeit und Wirksamkeit sichergestellt sowie deren Zusammenwirken bei der Abwehr bestimmter Gefährdungen (Korrektheit) gewährleistet ist. Die Sicherheitsfunktionen müssen einem Angriff nennenswert und idealerweise quantifizierbar Widerstand leisten können.

3.1.2 Validierung der Sicherheitsfunktionalitäten

Die Art und Weise wie sichergestellt wird, dass die Anforderungen korrekt umgesetzt und wirksam sind ist der zweite Freiheitsgrad bei der Gestaltung eines Prozesses zur Gewährleistung der

Datensicherheit. Grundsätzlich lässt sich dies über eine wie auch immer geartete Prüfung der Sicherheit erreichen, die feststellt, ob und inwiefern die Anforderungen umgesetzt wurden und die Umsetzung wirksam ist. Zur Validierung zählen also alle Aspekte, die zur Überprüfung einer oder mehrerer der postulierten Eigenschaften angewendet werden müssen. Zu nennen sind hier z. B. die Spezifikation der Sicherheitsfunktionalitäten durch den Hersteller, das Schema in dem geprüft wird (Prüfschema), die Prüfstelle, die Prüferqualifikation, die sinnvolle Abgrenzung von Prüfgegenständen[6] innerhalb des Gesamtsystems, die prüfungsunterstützende Dokumentation sowie das Prüfverfahren (z.B. Black Box-Test, Zero Day Exploits, etc.).

Hinsichtlich der Validierung gibt es eine Vielzahl an Ausprägungen. In bestimmten Branchen werden inhouse Prüfungen durchgeführt, welche die Korrektheit und Wirksamkeit der Sicherheitsfunktionalitäten bewerten. Hier werden von unternehmenseigenen Personen bzw. IKT-Experten Penetrationstests oder andere Verfahren verwendet, um die Qualität der Sicherheit festzustellen. Das Ergebnis einer vorgängig erstellten Risikoanalyse[7] bestimmt dabei die Prüftiefe. Die Prüfungen können auch von externen Spezialisten in Form von Penetrationstests geschehen. Diese können ggf. auch ein Prüfsiegel herausgeben, dessen Belastbarkeit aber gering ist.

Diesen Vorgehensweisen stehen Verfahren der Konformitätsprüfungen gegenüber. Diese sind mehr oder weniger standardisiert und stellen fest, inwiefern die Produkte gegenüber den gestellten Anforderungen (siehe Kapitel 3.1.1.) konform sind. In diesen Verfahren wird mit ganzheitlichen Ansätzen die IKT-Sicherheit validiert. Dies umfasst mindestens die Verifikation der Sicherheitsarchitektur und der Sicherheitsfunktionalitäten wie sie in der Produktspezifikation postuliert sind. Des Weiteren wird die korrekte Implementierung der Sicherheitsfunktionalitäten in einer vertrauenswürdigen Umgebung getestet und die Wirksamkeit der Sicherheitsfunktionalitäten über den gesamten Lebenszyklus eines Produkts, also inklusive Entwicklung, Auslieferung, Inbetriebnahme, Wartung, Updates, etc., begutachtet. Die Begutachtung des Produkts erfolgt grundsätzlich hinsichtlich der Vollständigkeit und Widerstandsfähigkeit der Sicherheitsfunktionalitäten gegen entsprechende Angriffe.

Die Validierung der IKT-Sicherheit erfolgt in einer unabhängigen, anerkannten Prüfstelle. Eine Prüfstelle für IKT-Sicherheit betreibt ein Qualitätsmanagement. Die Prüfstelle kann akkreditiert sein. Hat sie bei einer nationalen Akkreditierungsstelle gemäss ISO17025 [31, 32] das entsprechende Verfahren durchlaufen, werden Standards beim Qualitätsmanagement eingehalten. Die fachliche Qualifikation der Prüfer wird so einheitlich sichergestellt.

Akkreditierte Prüfstellen benötigen ein spezifiziertes Prüfschema pro Komponente – dann auch als Prüfgegenstand bezeichnet –, womit sie die Umsetzung der Sicherheitsanforderungen prüfen. Hier existieren zwei Arten einer möglichen Akkreditierung auf Prüfschemata. Typ A basiert auf internationalen Standards, z.B. CC und der ISO15408 Serie [33, 34, 35]. Typ B lässt

[6] Ein Prüfgegenstand ist eine abgrenzbare Komponenten des zu gesamtheitlich zu überprüfenden Systems, an die gewissen Anforderungen gestellt werden, deren Umsetzung von der Prüfstelle für diese Komponenten überprüft werden.
[7] Siehe Abschnitt zur Finanzbranche in der Schweiz.

nationalen Vorgaben basierend auf festgelegten Prüfverfahren, welche modifiziert werden können [36]. Die Prüfstelle übernimmt die Prüfschemata, welche vorgängig zusammen mit den Sicherheitsanforderungen und den Abgrenzungen der Komponenten erstellt wurden, falls sie sie als geeignet einstuft und meldet das Verfahren bei der Akkreditierungsstelle. Die Prüfstelle kann ihre Prüfschemata auch selber definieren. Daraus ergibt sich zum einen eine grundsätzlich sehr hohe Reproduzierbarkeit der Ergebnisse, so dass erstens dasselbe Produkt bei zwei verschiedenen Prüfstellen das gleiche Prüfergebnis erzielt und zum anderen zwei gleichwertige Produkte in derselben Prüfstelle das gleiche Ergebnis erzielen. Weiter wird durch dieses Vorgehen sichergestellt, dass eine umfassende Dokumentation und Nachvollziehbarkeit aller Schritte dieser Validierung vorliegt. Eine solche Prüfstelle kann ebenfalls ein Prüfsiegel herausgeben, dessen Belastbarkeit aufgrund des Akkreditierungsverfahrens sehr hoch ist.

Eine Zertifizierungsstelle für IKT-Sicherheit, welche ebenfalls nach entsprechenden Standards akkreditiert [37] bzw. national benannt wurde, kann darüber hinaus eine durchgeführte Prüfung der Prüfstelle zertifizieren. Dies umfasst die Überprüfung aller prozeduralen Schritte und Ergebnisse der Prüfstelle im Einzelfall. Ein entsprechendes Zertifikat erhöht die Belastbarkeit der Prüfergebnisse der Prüfstelle nochmals beträchtlich. Alle international akzeptierten Standards für die Validierung der IKT-Sicherheit von Produkten und Systemen sehen bzgl. der Zertifizierung vor, dass zunächst eine als Prüflabor akkreditierte Prüfstelle als dritte Partei eine tief gehende Evaluation des Prüfgegenstands vornimmt, bevor die Zertifizierungsstelle das Prüfergebnis bewertet. Es können Sicherheitszertifikate aus anderen Nationen anerkannt werden. Lizensierte Prüfstellen sind verfügbar [37]. In den meisten Staaten werden gemäss ISO15408 [32, 33, 34] nationale Sicherheitszertifikate herausgegeben. Für den Prüfprozess durch akkreditierte Stellen sind dabei relativ viele Aspekte wie Spezifikation, Prüfung, Inbetriebnahme streng reglementiert. Einem nationalen IKT-Sicherheitszertifikat auf der Stufe der internationalen Anerkennung gemäss CC kann eine sehr hohe Belastbarkeit attestiert werden.

3.2 Lösungsraum zur Gewährleistung der Datensicherheit von Smart Metering Systemen

Zur Gewährleistung der Sicherheit intelligenter Messsysteme in der Schweiz kann eine Anzahl generischer Ansätze verfolgt werden. Es können hierzu freie Spezifikationen bis feingranular-standardisierte Kataloge von IKT-Sicherheitsanforderungen sowie verschiedene Arten der Validierung adaptiert werden. Abbildung 2 stellt die verschiedenen Ausprägungen der oben diskutierten Freiheitsgerade dar. Die Achsen, die das Koordinatensystem bilden, sind daher der „Spezifikationstiefe der Sicherheitsanforderungen“ und den „Validierungsmöglichkeiten“ zugeordnet. Sicherheitsanforderungen können frei, standardisiert oder durch ein Schutzprofil vorgegeben sein. Die Beschreibungstiefe der Anforderungen steigt über diese hinweg an. Eine Validierung kann durch eine Inhouse Prüfung, durch einen externen Penetrationstest, durch eine

Konformitätsprüfung oder durch eine IKT-Sicherheitszertifizierung realisiert werden. Hierbei steigt jeweils die Prüftiefe und die formalen Vorgaben zur Prüfung wachsen stetig an.

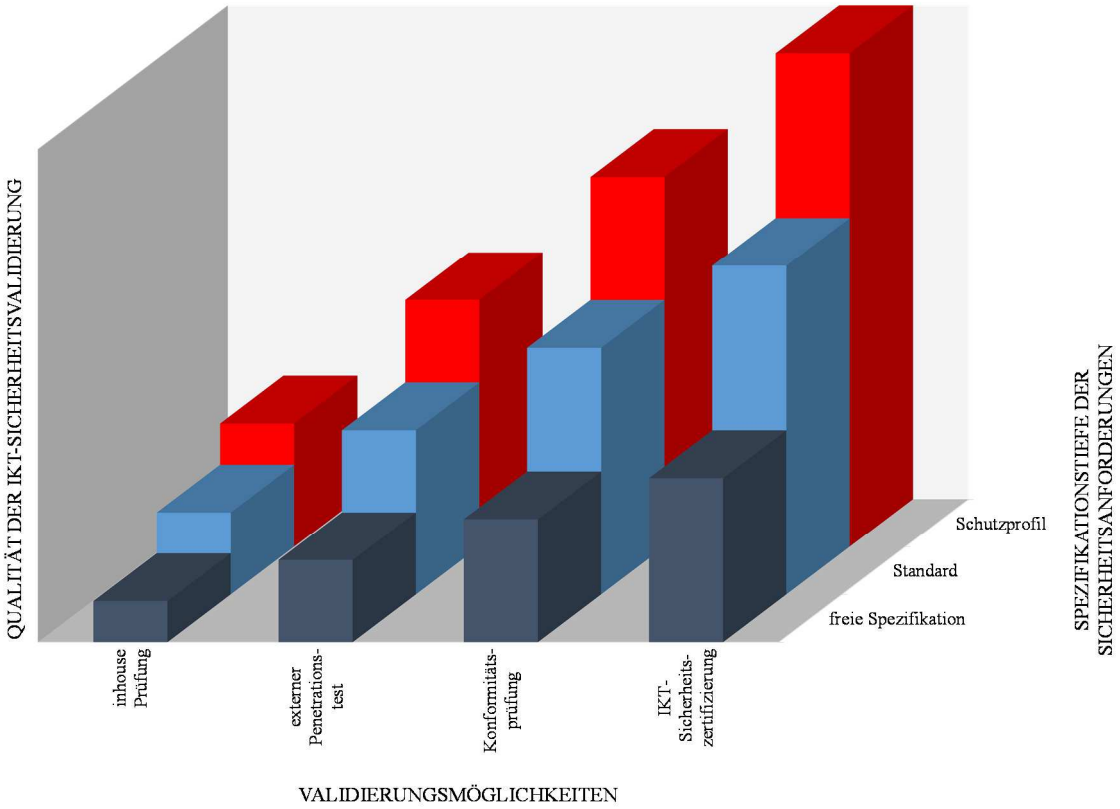

Abbildung 2: Möglichkeiten zur Gewährleistung der Datensicherheit für Smart Metering Systeme

Die Höhe der Balken in Abbildung 2 ist willkürlich gewählt und kann als Belastbarkeit der Prüfergebnisse hinsichtlich Datensicherheit, als Prüftiefe aber auch als Validierungsaufwand verstanden werden. Mit steigenden sicherheitstechnischen Anforderungen sowie Prüfumfängen kann bei erfolgreichem Durchlaufen einer entsprechenden Validierung ein aus Sicht der IKT-Sicherheit deutlich gesenktes Betriebsrisiko angenommen werden. Das verbleibende Restrisiko wird reduziert und erfordert letztlich geringere Aufwände in einem nachgelagerten ISMS. Eine umfassendere und tiefergehende Überprüfung begründet jeweils bessere Systemhärtung und damit ein im Vergleich geringeres Betriebsrisiko.

Von der Vielzahl der möglichen Kombinationen werden diejenigen Varianten mit per se vergleichsweise hohem Betriebsrisiko von der weiteren Untersuchung ausgeschlossen. Ebenso werden mögliche, jedoch unter Umständen unsinnige Varianten, z. B. solche, die vergleichsweise einen hohen Aufwand aber eine ungenügende Validierungstiefe aufweisen, nicht weiter betrachtet. Zu den im weiteren Verlauf betrachteten Varianten zählen: der externe Penetrationstest mit zugrunde liegendem Standard als Minimalvariante, die Konformitätsprüfung gegen einen zugrunde gelegten Standard der Sicherheitsanforderungen, die Konformitätsprüfung

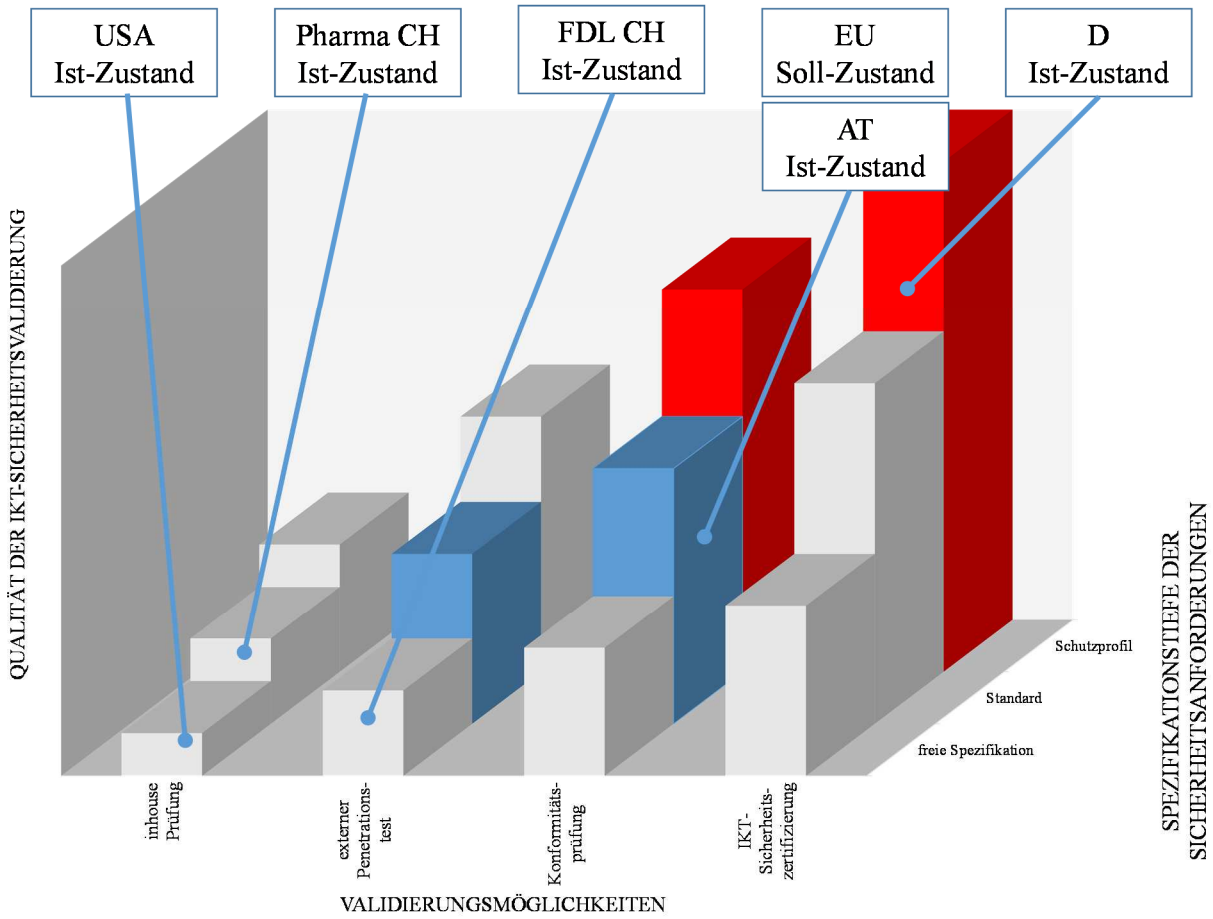

Abbildung 3: Ausgewählte Varianten zur Diskussion von Vor- und Nachteilen bei der Gewährleistung der Datensicherheit von Smart Metering Systemen.

gegen ein zugrunde gelegtes Schutzprofil sowie als Maximalvariante das IKT-Sicherheitszertifikat mit zugrunde liegendem Schutzprofil. Ebenso wie die nicht weiter betrachtete inhouse-Prüfung mit zugrunde liegendem Schutzprofil stellt auch die Etablierung eines IKT-Sicherheitszertifikats mit zugrundeliegendem frei spezifiziertem Anforderungsprofil aufgrund der qualitativen Ungleichgewichte zwischen Prüfverfahren und Spezifikationstiefe eine wenig sinnvolle Vorgehensweise für eine Validierung dar. Sie werden daher nicht weiter betrachtet.

Abbildung 3 zeigt die ausgewählten Varianten und ordnet die in Kapitel 2 vorgestellten internationalen Vorgehensweisen zur Sicherung von Smart Metering Systemen sowie die nationalen Lösungen anderer Branchen zur Sicherung anderer IKT-Infrastrukturen dem Lösungsraum zu. Es ist ersichtlich, dass die Auswahl der näher zu betrachtenden Varianten wesentliche und fortgeschrittene Lösungen abdeckt. Die Lösungen, welche in anderen Sektoren umgesetzt werden, weisen eine eher geringe Qualität der zu erreichenden Sicherheit auf. Dies ist aber vor dem Hintergrund, dass es sich bei den dort zu schützen Infrastrukturen teilweise nicht um kritische Infrastrukturen handelt[8]. Im internationalen Vergleich erscheint die Auswahl der vertieft zu

[8] Gemäss der Strategie SKI zählen Banken zu den kritischen Infrastrukturen.

prüfenden Ansätze im Mittelfeld und daher als pragmatische Lösung. Im Folgenden werden die einzelnen Varianten näher betrachtet und einer Analyse unterzogen.

3.2.1 Variante 1: Externer Penetrationstest mit zugrunde liegendem Standard

Diese Variante charakterisiert sich vor allem durch einen weitgehenden Handlungsspielraum für Hersteller. Sie wählen die nötigen Technologien und – wesentlich wichtiger – deren Spezifikation zur Sicherung des Produktes entsprechend einem selbst gewählten Standard. Sicherheitsfunktionalitäten sind daher nicht einheitlich definiert. Sie sollten mindestens in einem Pflichtenheft an den Hersteller festgehalten sein. Nach der Herstellung der intelligenten Messsysteme erfolgt eine interne Qualitätssicherung der Einhaltung vom Betreiber geforderter Sicherheitsfunktionalitäten oder Standards. Durch eine Erklärung des Herstellers wird die Konformität zu dem selbst gewählten Standard oder den Anforderungen bestätigt. Der Hersteller erstellt zudem eine Benutzerdokumentation, die Handbücher zur Administration und Nutzung des Systems umfasst und Vorgaben für einen vertrauenswürdigen Betrieb macht.

Nachdem die intelligenten Messsysteme vom Betreiber käuflich erworben und installiert wurden, veranlasst dieser externe Penetrationstests durch einen Prüfer; typischerweise einen IKT-Experten. Hierbei werden unter Umständen Schwachstellen identifiziert, die in einem Bericht festgehalten und dem Betreiber zur Verfügung gestellt werden. Dieser Bericht wird dann dazu verwendet, das System weiter zu härten und etwaige Einfallstore, die die Datensicherheit gefährden, in Zusammenarbeit mit dem Hersteller zu schliessen. Die Penetrationstests können in regelmässigen Abständen ggf. durch unterschiedliche Prüfer durchgeführt werden, was wiederrum zu einer wiederholten Härtung führt. Das Betriebsrisiko solcher Systeme ist als vergleichsweise hoch einzuschätzen, da zunächst nicht ohne weiteres festgestellt werden kann, ob die Sicherheitsfunktionalitäten wie sie im Pflichtenheft gefordert wurden, wirksam implementiert sind. Sollte ein externer Penetrationstest zu dem Schluss kommen, dass das System sicher aufgesetzt wurde, heisst das noch nicht, dass alle Sicherheitsfunktionalitäten wirksam implementiert wurden sondern nur, dass dieser spezielle Prüfer nicht in der Lage war, Sicherheitslücken zu entdecken. Dies kann z. B. an äusseren Umständen, wie z. B. einer unzureichenden Dokumentation der Sicherheitsfunktionalitäten, oder an der Kompetenz des Prüfers liegen. Die Aussagekraft der Analyse ist also stark abhängig von der Qualität des Prüfers und dem Informationsmaterial, das zur Verfügung steht. Tabelle 1 gibt einen Überblick wichtiger Aspekte.

Abbildung 4 zeigt die Ergebnisse einer SWOT (Strengths, Weaknesses, Opportunities, Threats) Analyse dieser Variante. Die Stärken (Strengths) liegen im oberen, linken Sektor. Zu nennen ist hier zunächst die hohe Eigenverantwortung und Eigenorganisation seitens Hersteller aber auch der Betreiber, die Sicherheitsaspekte in Pflichtenheften fordern müssten. Dabei haben die Hersteller einen grossen Freiraum in der Entwicklung und Implementierung von Sicherheitsfunktionalitäten, was sich ggf. kostendämpfend auswirkt. Aufgrund der wenig formalen Prüfung einer wirksamen Implementierung der Sicherheitsfunktionalitäten können in dieser Variante der Aufwand und somit die Kosten für die Validierung gering gehalten werden. Grundsätzlich ist es möglich, die Konformität zu einem technischen Standard zu verifizieren, jedoch

kann man nicht eine Härtung gegenüber allen wesentliche Schachstellen nachweisen. Die Variante beinhaltet die Möglichkeit, unabhängige IKT-Sicherheitsexperten zu Rate zu ziehen.

Variante 1: Externer Penetrationstest mit zugrunde liegendem Standard		
Aspekt	Beschreibung	Bemerkungen
Benötigte Dokumentation	- Pflichtenheft zur Entwicklung des Smart Metering Systems - Lastenheft listet Standards auf - Konformitätserklärung / Herstellererklärung bzgl. Standard Benutzerdokumentation	- Einschlägige Standards geben Implementation gewisse Richtung - Im Minimum Pflichtenheft mit Sicherheitsfunktionalitäten seitens Betreiber an Hersteller - Konformitätserklärung des Herstellers bestätigt Entsprechung
Sicherheitsfunktionalitäten	- Nicht einheitlich	- Sicherheitsfunktionalitäten sollten im Pflichtenheft mindestens ausformuliert sein
Prüfkriterien	- Nicht standardisiert - Nicht spezifiziert bzw. dokumentiert; individuell durch Betreiber festzulegen - Externer Prüfer geht u.U. nach eigenem Schema vor; agiert damit in Rolle Sachverständiger oder Gutachter	- nicht formal / standardisiert; damit keine umfassende Prüfvorschrift - Externer Penetrationstest entspricht z.B. Verwundbarkeitsanalyse; es können auch Standards verwendet werden - Externer Penetrationstest ohne Abgleich mit implementierten, zu überprüfenden Funktionalitäten und ohne Testen derselben auf Entwicklerebene detektiert Schwachstellen denen u.U. keine konkrete Vorgabe im Pflichtenheft entspricht - Externer Prüfer könnte ggf. nicht alle Schwachstellen identifizieren
Betriebsrisiko	- hoch; zugesicherte Sicherheits-Eigenschaften sind nur schwach validiert	–

Tabelle 1: Übersicht Aspekte Variante 1: Externer Penetrationstest mit zugrunde liegendem Standard.

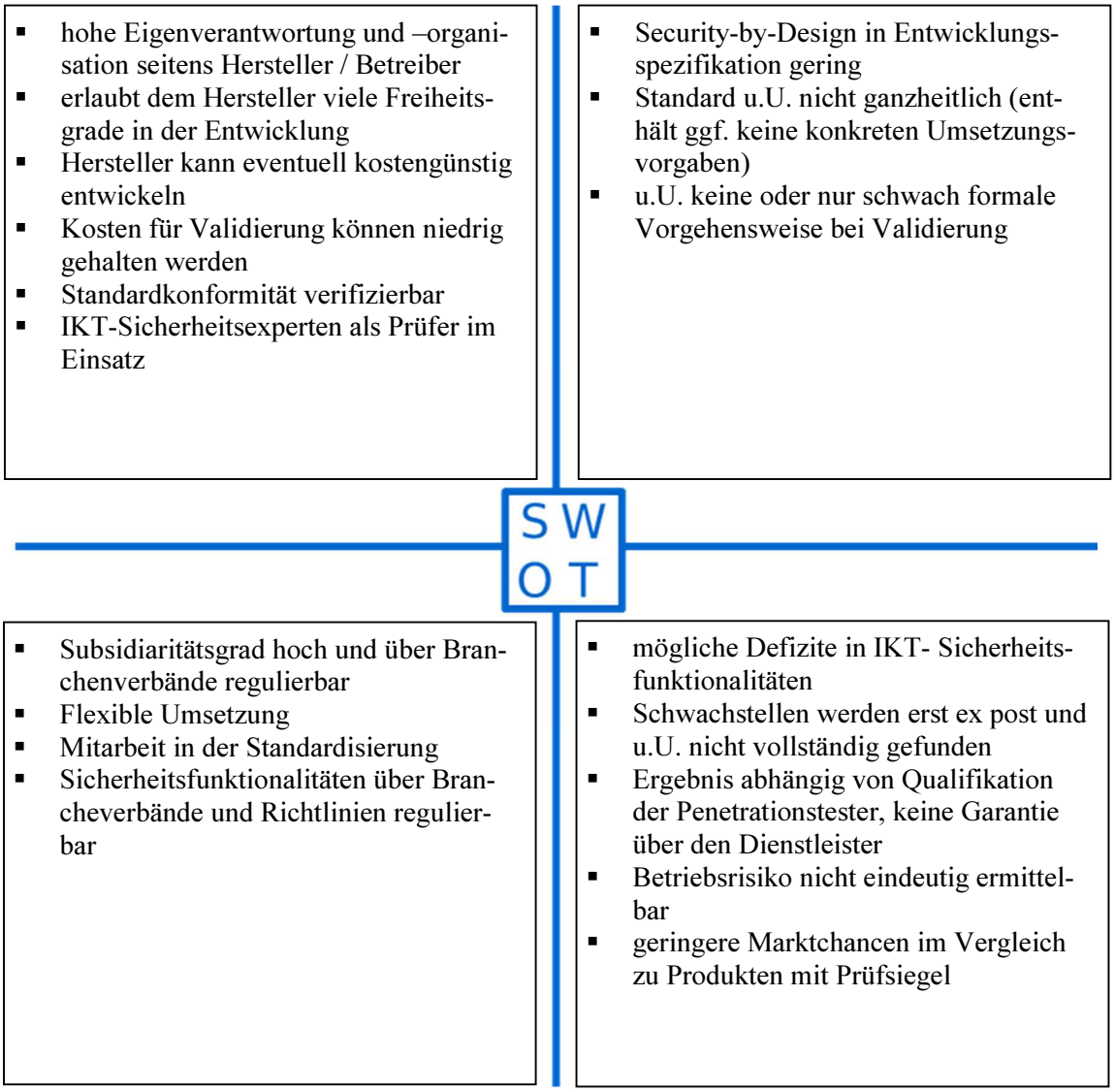

Abbildung 4: SWOT-Analyse Variante 1: externer Penetrationstests mit zugrunde liegendem Standard.

Als Schwachstellen (Weaknesses) kann aufgeführt werden, dass während der Entwicklung der intelligenten Messsysteme seitens der Hersteller das Themengebiet der Datensicherheit als zweitrangig aufgefasst werden kann. Das muss nicht zwangsläufig der Fall sein, wird jedoch durch Forderungen der Betreiber in ihren Ausschreibungen stark beeinflusst. So können z. B. aufgrund von Kostensensitivität oder Komplexität ungenügende Forderungen seitens der Betreiber in den Pflichtenheften festgehalten werden. Damit wären Hersteller, aufgrund eines Kostendruckes, bei der Ausschreibung gezwungen, Sicherheitsfunktionalitäten kaum anzubieten bzw. zu implementieren. Weiter kann ein seitens des Betreibers geforderter Standard zwar technisch anerkannt sein, entspricht aber ggf. nicht den Risiken, die durch den Betrieb des Systems entstehen. Aus einer Standardkonformität ergibt sich per se nicht zwingend eine Vorgabe, welche die Sicherheitsaspekte ganzheitlich widerspiegelt. Ein Industrie- oder Branchenstandard kann sich z.B. auf technische Aspekte der Betriebssicherheit beschränken. Eine weitere

Schwachstelle dieser Variante ist die schwach formale Vorgehensweise zur Validierung der geforderten Sicherheitsfunktionalitäten.

Zu den Chancen (Opportunities) kann gezählt werden, dass grundsätzlich der Subsidiaritätsgedanke in dieser Variante bestimmend ist. Die Handhabung der Sicherheitsthematik wird wesentlich durch die betroffene Branche und die Hersteller geprägt. Ihnen wird es überlassen, die Herausforderungen in der Sicherheit für Smart Metering Systeme anzugehen und zu lösen. Die Umsetzung kann so relativ flexibel und angepasst auf die heterogenen Bedürfnisse der Betreiber erfolgen. Dadurch wird eine hohe Akzeptanz bei den Betreibern erreicht.

Zu den Risiken (Threats) kann gezählt werden, dass gerade durch die individuellen Lösungen der Sicherheitsfragen eine hohe Wahrscheinlichkeit für Defizite in der Umsetzung der Sicherheitsfunktionalitäten besteht. Fehler oder Schwachstellen im gesamten Sicherheitskonzept oder in den einzelnen Sicherheitsfunktionalitäten können erst ex post und ggf. nicht vollständig festgestellt werden. Geforderter Standards können unter Umständen unzweckmässig sein. Dies mag ex post zu nachgelagerten Arbeiten führen, die komplex und kostenintensiv sein können. Das Ergebnis der Überprüfung der Sicherheit durch Penetrationstests ist stark abhängig von der Qualität und Erfahrung des gewählten Prüfers. Dadurch erhöht sich im Allgemeinen das Risiko des Betriebs dieser Systeme. Weiter weisen intelligente Messsysteme, welche über kein Prüfsiegel oder eine andere offizielle Bestätigung der Sicherheitsqualität verfügen, geringere Marktchancen auf bzw. stossen auf geringere Akzeptanz. Zudem birgt diese Variante die Gefahr, dass durch einen Datenverlust bei einem Betreiber, die Akzeptanz der Technologie in der Bevölkerung wesentlich beeinträchtigt wird.

Kurzfazit Variante 1

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. Hier bietet zwar die Verwendung von Standards Vorteile. Es existieren durchaus Standards in denen IKT-Sicherheitsaspekte behandelt werden, die aber in Pflichtenheften auch explizit gefordert werden müssen. Die Standards bewegen sich jedoch eher auf einem abstrakten Anforderungsniveau und beinhalten wenig konkrete Vorgaben für eine Implementierung. Die Vorteile, die die Verwendung von Standards bieten könnte, sind wegen ihrer wenig konkreten Ausprägungen, den grossen Spielräumen und einer ggf. geringen Eignung bezüglich Anwendungsfällen von intelligenten Messsystemen eher marginaler Art. Aus Sicht der Sicherheit erscheint es unbedingt wünschenswert, dass Systeme, die in einer kritischen Infrastruktur zur Anwendung kommen, einem für sie auch geeigneten Standard für IKT-Sicherheit entsprechen. Da andere Staaten individuell zugeschnittene aber grundsätzlich ganzheitliche Ansätze für ihre Situation verfolgen, lässt vermuten, dass die Variante 1 eher als untergeordnet zu betrachten ist.

3.3.2 Variante 2: Konformitätsprüfung mit zugrunde liegendem Standard

Diese Variante charakterisiert sich ebenfalls durch einen noch vergleichsweise hohen Handlungsspielraum für Hersteller, ist jedoch prozessual spezifischer ausgestaltet. Auch hier wählen

Hersteller die nötige Technologie und deren Spezifikation zur Gewährleistung der Datensicherheit, ggf. entsprechend anerkannter Standards und erklären dahingehend eine Konformität. Es sind einzelnen Komponenten des Smart Metering Systems gegeneinander abzugrenzen, damit Standards auf sie angewendet werden. Es existiert eine externe Prüfstelle, die die Konformität hinsichtlich der erklärten Einhaltung der Standards prüft. Somit wird ein Nachweis bzgl. der Erfüllung der durch Betreiber geforderten oder der durch Hersteller gewählten Standards erbracht und die Korrektheit in der Implementierung der Sicherheitsfunktionalitäten festgestellt.

Variante 2: Konformitätsprüfung mit zugrunde liegendem Standard		
Aspekt	Beschreibung	Bemerkungen
Benötigte Dokumentation	- Pflichtenheft entsprechend geforderten Standards zur Entwicklung - Lastenheft listet Standards auf - Konformitätserklärung / Herstellererklärung bzgl. Standard - Benutzerdokumentation	- Im Minimum Pflichtenheft mit geforderten Standard(s) seitens Betreiber an Hersteller - Einschlägige Standards geben Richtung der Implementationen vor - Konformitätserklärung des Herstellers bestätigt Entsprechung
Sicherheitsfunktionalitäten	- Ggf. abstrakt im Standard beschrieben; u.U nicht hinreichend konkret bzgl. Korrektheit und Wirksamkeit der IKT-Sicherheitsfunktionen - Implementierung gemäss Anforderungen des Standards	- Sicherheitsfunktionalitäten sollten im Pflichtenheft mindestens ausformuliert sein - Durch Prüfung der Konformität ist die Korrektheit, jedoch nicht die Wirksamkeit, der Sicherheitsfunktionalitäten validierbar
Prüfkriterien	- Externe Prüfstelle oder Gutachter gemäss ISO17000er Serie akkreditiert - Prüfschemata liegen vor - Prüfsiegel bzgl. Standardkonformität verleihbar - Konformitäts-Prüfer/innen agieren als IKT-Sicherheitsprüfer	- Standard vorhanden, formal aber eine generische Vorgabe; spezifische Ausformulierung nicht garantiert - Konformitätsprüfung weist eher geringe Vorgaben für Sicherheitsvalidierung auf - Einsatz akkreditierter Gutachter bzw. Prüfstellen; fachliche Qualifizierung sichergestellt - Spezialisierung Prüfer auf IKT-Sicherheit nicht obligatorisch - Formuliertes Pflichtenheft für die Umsetzung entsprechender Anforderungen mit grösserer Nähe zum Prüfgegenstand sinnvoll
Betriebsrisiko	- mittel bis hoch; zugesicherte Eigenschaften nur auf Anforderungsebene validiert	–

Tabelle 2: Übersicht Aspekte Variante 2:Konformitätsprüfung mit zugrunde liegendem Standard.

Die Wirksamkeit wird der Implementierung wird in dieser Variante jedoch nicht geprüft. Die Prüfstelle ist akkreditiert und verfügt über ein definiertes Schema mit dem es die Implementierung der Sicherheitsfunktionalitäten gemäss den Anforderungen des Standards prüft. Nach einer erfolgreich absolvierten Prüfung wird ggf. ein Prüfsiegel durch die Prüfstelle vergeben. In jedem Fall wird ein Prüfbericht für den Betreiber erstellt, sodass dieser jederzeit die Konformität seines Systems auf Anfrage gegen extern bestätigen kann. Das Betriebsrisiko des intelligenten Messsystems kann hier noch als mittel bis hoch eingestuft werden, da zwar die zugesicherten, sicherheitsrelevanten Eigenschaften gemäss einem Standard erfüllt werden, jedoch fraglich bleibt, ob die Funktionalitäten wirksam sind bzw. den Gefährdungen entsprechen. Tabelle 2 gibt wichtige Aspekte der Variante wieder.

Abbildung 5 zeigt die Ergebnisse der SWOT-Analyse der Variante 2. Die Stärken (Strengths) sind in den ersten drei Punkten die Gleichen wie die der Variante 1. Zu den weiteren Stärken zählt die Etablierung einer anerkannten und neutralen Prüfstelle als ein, vor allem prozessualer, Vorteil. Durch die akkreditierte Prüfstelle wird sichergestellt, dass die intelligenten Messsysteme von qualifizierten Prüfern eines einheitlichen Kompetenzniveaus geprüft werden. Die Akkreditierung der Prüfstelle ermöglicht die Vergabe eines Prüfsiegels, das die Qualität des Produktes transparent darlegt. Aufgrund der strukturierteren Vorgehensweise auf Basis von Prüfschemata werden die Reproduzierbarkeit und damit die Belastbarkeit der Ergebnisse wesentlich verbessert.

Die Schwachstellen (Weaknesses) stimmen teilweise mit denen der Variante 1 überein. Zudem kann als Schwachstelle dieser Variante der im Vergleich zur Variante 1 grössere Aufwand für die nötige Abgrenzung der einzelnen Prüfgegenstände identifiziert werden. Eine Abgrenzung und sinnvolle Definition ist aufgrund der technischen Komplexität nicht trivial. Zudem steigen die die Kosten einer solchen formaleren Validierung im Gegensatz zu der Variante 1. Die Verwendung von qualifizierten Prüfer, die Prüfstelle, die dort nötige Infrastruktur sowie Dokumentationen erhöhen die Kosten im Vergleich zu Variante 1.

Chancen (Opportunities) dieser Variante sind neben dem im Vergleich zu Variante 1 zwar niedrigerem aber immer noch hohem Subsidiaritätsgrad nun auch ein Einfluss des Staates. Dieser war in Variante 1 kaum vorhanden. Er wird hier über eine grundsätzlich regulierbare Prüfstelle gesichert. Eben diese bietet nun über eine externe Qualitätssicherung einen zusätzlichen Nutzen, indem sie eine geeignete Implementation der sicherheitstechnischen Forderungen sichert. Hierdurch werden auch Interessen des Staates hinsichtlich der Sicherung kritischer Infrastrukturen umgesetzt. Durch die zwingende, externe Konformitätsprüfung ist der Anreiz höher, von Anfang an Datensicherheit als ein wichtiges Element in die Spezifikation des Pflichtenheftes und somit in die Entwicklung des Produktes einfliessen zu lassen. Herstellerseitig bietet Variante 2 den Vorteil, dass sich durch den Erhalt eines Prüfsiegels die Vermarktung des Produktes im Ausland verbessern kann.

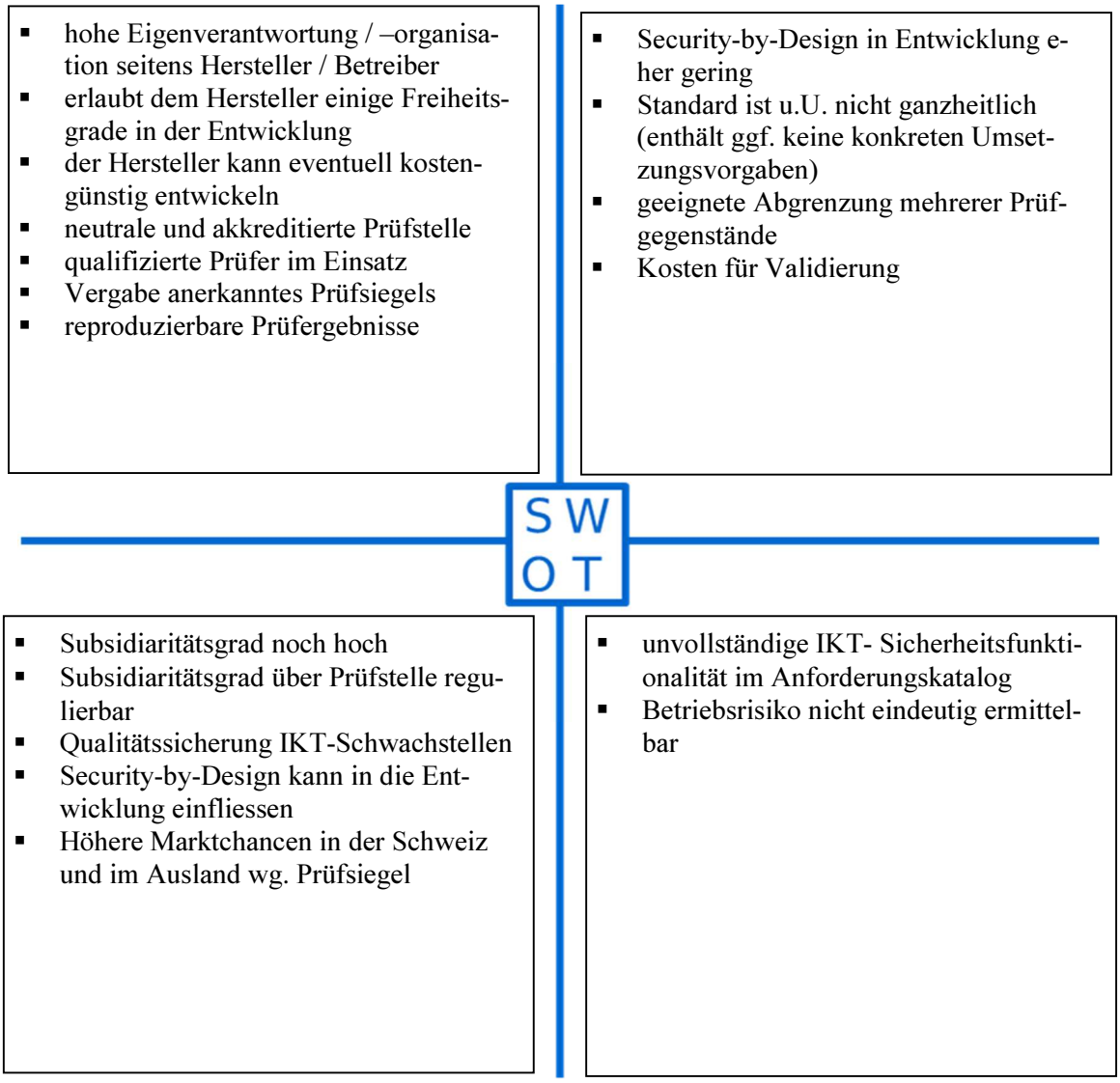

Abbildung 5: SWOT-Analyse Variante 2: Konformitätsprüfung mit zugrunde liegendem Standard.

Die Anzahl Risiken (Threats) dieser Variante sind im Vergleich zu Variante 1 stark reduziert. Zu ihnen zählt unter anderem, dass Sicherheitsanforderungen unvollständig in den von Betreibern für die Komponenten geforderten Standards abgedeckt oder definiert sind. Somit wären die intelligenten Messsysteme nicht gegen alle Gefährdungen geeignet abgesichert. Insbesondere das Zusammenspiel der Anforderungen kann durch eine fehlerhafte Abgrenzung der Komponenten gefährdet sein. Das kann in dieser Variante leicht zu Schwachstellen des gesamten Sicherheitskonzeptes führen. Diese Schwachstellen können in dieser Variante nicht ohne weiteres erkannt werden, da die Konformitätsprüfung sich nur auf die Erfüllung der vorher festgesetzten Anforderungen konzentriert, nicht aber auf deren Vollständigkeit bzw. Wirksamkeit. So ist auch das Betriebsrisiko aus einer konservativen Sicht als mittel bis hoch einzuschätzen bzw. nicht feststellbar. Es hängt stark davon ab, wie und auf Basis von welchen Annahmen die Sicherheitsanforderungen definiert wurden.

Kurzfazit Variante 2

Eine formale Konformitätsprüfung ist klar aufwendiger und damit kostenintensiver als individuell, also pro Betreiber, durchgeführte Penetrationstests. Dafür werden aber auch mehr Prüfaspekte, da sie in den entsprechend dafür entwickelten Prüfschemata vorgegeben werden, bearbeitet. Die Kosten für eine Konformitätsprüfung liegen bei den Herstellern, werden aber den Betreibern über den Produktpreis weitergegeben und belasten dadurch den Endkunden.

Eine Prüfstelle für Konformität sollte gem. der ISO17000er-Standardfamilie [31, 32] akkreditiert sein. Das ist ohne weiteres möglich und kaum kostentreibend. Durch ein von der Prüfstelle angewendetes, mehr oder weniger formales Validierungsverfahren ist es möglich gegenüber einem geeigneten, z. B. durch Betreiber über Richtlinien vorgegebenen Standards, eine gewisse einheitliche Standardkonformität mit vergleichsweise grösserer Prüftiefe zu erreichen. Hierzu sollten aber Komponenten des Messsystems derart abgegrenzt werden, dass geeignete Standards pro Komponenten verwendet werden. Es ist fraglich, ob eine solche Abgrenzung der Komponenten bzw. Prüfgegenstände generisch erfolgen kann, damit im Anforderungskatalog dem Anspruch einer hinreichend hohen Sicherheit des gesamten Systems entsprochen werden kann. Letztlich sind Prüfkriterien und die Prüfschemata aus den verwendeten Standards pro Komponente abzuleiten.

3.2.3 Variante 3: Konformitätsprüfung mit zugrunde liegendem Schutzprofil

Diese Variante orientiert sich in einem stärkeren Masse an einem zentralen und spezifischeren Ansatz und weist somit einen geringeren Grad an Subsidiarität auf als die vorhergehenden. Hier findet die Spezifikation der Sicherheitsanforderungen für intelligenten Messsysteme in einem abgestimmten, feingranularen Schutzprofil statt. Es enthält konkretere, tiefgehende Anforderungen an die Messsysteme bzw. an seine Einzelkomponenten. Auch hier sind die Komponenten des Systems also geeignet gegeneinander abzugrenzen. Das Schutzprofil leitet sich aus anerkannten Standards für IKT-Sicherheit ab, kann aber durch Einbezug der Hersteller, Betreiber sowie Sicherheitsexperten auf die nationalen Bedürfnisse optimal angepasst werden. Über den Einbezug der Hersteller kann eine hinreichende Flexibilität des Schutzprofils gewährleistet werden, obwohl es detailliertere Anforderungen umfasst, die bei der Entwicklung der intelligenten Messsysteme berücksichtigt werden müssen. Das Schutzprofil wirkt auf Implementationsebene und bildet somit eine Art Pflichtenheft für Hersteller. Nachdem das intelligente Messsystem gemäss Schutzprofil hergestellt wurde, erfolgt wieder eine Konformitätserklärung des Herstellers auf Basis einer vorgängig durchgeführten internen Qualitätssicherung. Der Hersteller dokumentiert die Implementierung der geforderten Sicherheitsfunktionalitäten.

Das intelligente Messsystem wird nach Fertigstellung einer externen Prüfstelle zusammen mit der Dokumentation der Sicherheitsfunktionalitäten übergeben. Hierbei wird nicht jedes einzelne System übergeben, sondern es wird nur ein Muster übergeben, das geprüft wird. Es wird unter gewissen Voraussetzungen als repräsentativ angenommen. Die Prüfstelle prüft die Umsetzung der Anforderungen, die Wirksamkeit der Funktionalitäten und die korrekte Implementierung basierend auf dem Schutzprofil. Durch die Akkreditierung der Prüfstelle werden eine

fachliche Qualifizierung der Prüfer und eine hohe Qualität der Prüfung gewährleistet. Eine IKT-sicherheitstechnische Ausbildung der Prüfer ist in dieser Variante weiterhin nicht obligatorisch aber grundsätzlich natürlich von Vorteil. Sollten die intelligenten Messsysteme den Anforderungen entsprechen, kann ein Prüfsiegel gemäss dem verwendeten Prüfverfahren vergeben werden. Zusätzlich wird die Qualität der Prüfergebnisse durch eine staatlich kontrollierte Kontrollstelle geprüft, die die finale Zulassung erteilt. Das Betriebsrisiko kann in dieser Variante als mittel bis niedrig eingestuft werden, weil zusätzlich zur Konformität im Sinne der Korrektheit auch die Wirksamkeit der IKT-Sicherheitsfunktionalitäten geprüft wird und die Forderungen wesentlich feingranularer sind. Tabelle 3 gibt einen Überblick wichtiger Aspekte der Variante.

Variante 3: Konformitätsprüfung mit zugrunde liegendem Schutzprofil		
Aspekt	Beschreibung	Bemerkungen
Benötigte Dokumentation	- Pflichtenheft gemäss Schutzprofil (selber wiederum abgeleitet aus einem Standard) - Lastenheft gemäss einem Standard - Konformitätserklärung / Herstellererklärung bzgl. Standard und Schutzprofil - Entwicklungsdokumentation in Übereinstimmung mit Schutzprofil - Benutzerdokumentation	- Schutzprofil, aus Standards abgeleitet, spezifiziert Anforderungen zur Implementation von Funktionalitäten (Pflichtenheft) - Entwicklungsdokumentation als Leitfaden für Validierung möglich
Sicherheitsfunktionalitäten	- Schutzprofil - Nachweis der Erfüllung der Anforderungen des Standards basierend auf feiner granularen Schutzprofil	- Durch Abgleich Schutzprofil vs. Implementierung können Korrektheit und Wirksamkeit der Sicherheitsfunktionalitäten validiert werden
Prüfkriterien	- Externe Prüfstelle oder Gutachter gemäss ISO17000er Serie akkreditiert - Prüfschema liegt vor - spezifisches Prüfsiegel bzgl. Erfüllung Schutzprofil verleihbar - Prüfer/innen verfügen über Qualifikation als IKT-Sicherheitsprüfer - Kontrollstelle erteilt Zulassung auf Basis der Prüfberichte	- Durch Einsatz akkreditierter Prüfstellen fachliche Qualifizierung sichergestellt - Spezialisierung Prüfer auf IKT-Sicherheit obligatorisch Standard ist u.U. eine zu generische Vorgabe; enthält wenig Konkretes für die Validierung; daher Schutzprofil richtige Spezifikationsform - Pflichtenheft kann Umsetzung Anforderungen mit grösserer Nähe zum Prüfgegenstand widergeben
Betriebsrisiko	- mittel bis niedrig; zugesicherte Eigenschaften sind auf Anforderungsebene sowie auf Implementierungsebene validiert	–

Tabelle 3: Übersicht wichtiger Aspekte Variante 3: Konformitätsprüfung mit zugrunde liegendem Schutzprofil.

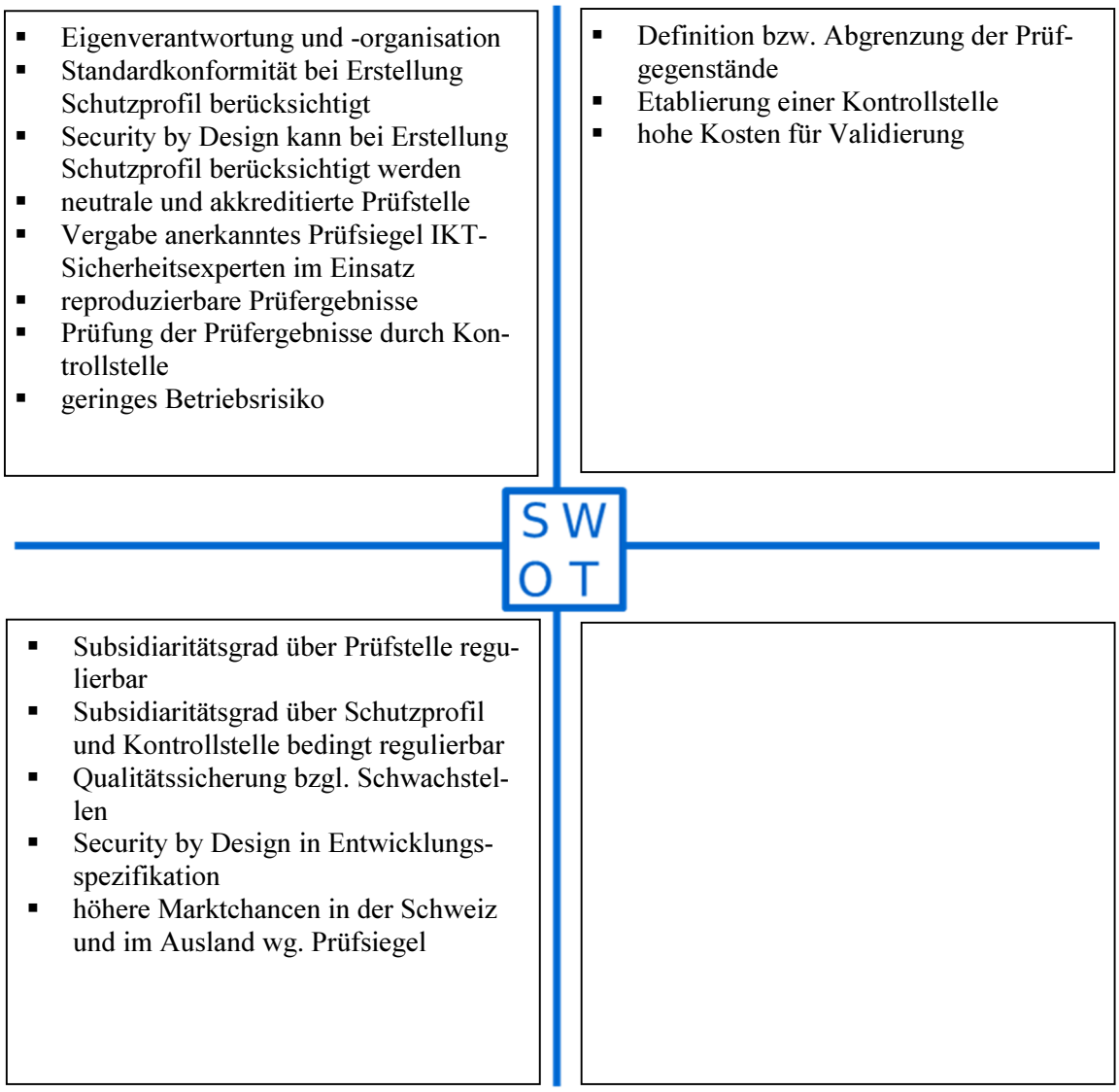

Abbildung 6: SWOT-Analyse Variante 3: Konformitätsprüfung mit zugrunde liegendem Schutzprofil.

Abbildung 6 stellt die Ergebnisse der SWOT Analyse dieser Variante dar. Viele Stärken entsprechen denen der Variante 2. Hinzu kommt, dass eine Standardkonformität durch die Verwendung des Schutzprofils gewährleistet wird, die zugleich sehr spezifisch ist. Durch die Vorgabe eines Schutzprofils kann von Anfang an IKT-Sicherheit in der Produktentwicklung bei Architektur und zu Einzeltechnologien (Security-by-Design) berücksichtigt werden. Das Schutzprofil bietet hierfür einen detaillierten Leitfaden. So können die intelligenten Messsysteme einfacher anforderungskonform hergestellt werden und weniger Freiheitsgrade in der Herstellung reduzieren Fehler. Die Variante ermöglicht zudem eine Kontrolle der Prüfergebnisse durch eine staatlich kontrollierte Stelle. Damit kann langfristig die Sicherheit der Systeme gewährleistet werden, da die Prüfstelle bei der Erarbeitung der Schutzprofils involviert ist und die Interessen des Staates im Bereich kritischer Infrastrukturen einbringt und Stichproben im Betrieb anordnen kann. Diese Variante bietet ein relativ geringes Betriebsrisiko.

Schwachstellen (Weaknesses) können im Wesentlichen dreierlei identifiziert werden. Zunächst kann davon ausgegangen werden, dass auf Herstellerseite oft nicht genügend Qualifikationen bestehen, um die entsprechenden Prozesse effizient und mit einer nötigen Qualität zu etablieren, die Sicherheitsanforderungen gemäss Schutzprofil zu realisieren und die dazugehörige Dokumentation zu erarbeiten. Diese Qualifikation muss oft erst aufgebaut bzw. ausgebaut werden. Weiter sind wie in Variante 2 die Abgrenzung der Prüfgegenstände und die Festlegung der an sie zu stellenden Anforderungen nicht trivial. Auch die Etablierung einer Kontrollstelle kann unter dem Gesichtspunkt eines erhöhten Verwaltungsaufwands als Nachteil ausgelegt werden. Die Kosten dieser Variante sind im Vergleich zu Variante 1 eher hoch, jedoch nur geringfügig höher als die Kosten der Variante 2.

Die Chancen (Opportunities) dieser Variante entsprechen grundsätzlich denen der Variante 2. Ein Einfluss des Staates wird nun aber nicht nur über die regulierbare Prüfstelle sondern auch über die Kontrollstelle und eine Beteiligung an der Erarbeitung des Schutzprofils gesichert. Diese Vorgehensweise bietet einen höheren Qualitätsstandard der Sicherheitsfunktionalitäten als in den bisherigen Varianten. Zudem wird auch die Erfüllung dieser spezifischeren, feingranularen Funktionalitäten auf Korrektheit, Vollständigkeit und Wirksamkeit geprüft. Durch die Vorgabe des Schutzprofils werden von Anfang an Sicherheitsfunktionalitäten in die Entwicklung und Herstellung der intelligenten Messgeräte derart integriert, so dass ein sehr hohes und durch das Schutzprofil genau vorgegebenes Niveau an Sicherheit erreicht wird.

Kurzfazit Variante 3

Variante 3 ist durch die Erarbeitung und Verwendung des Schutzprofils geprägt. Das Schutzprofil bietet gleichzeitig eine Standardkonformität sowie, basierend auf einer Schutzbedarfsanalyse, einen Kanon geeigneter, konkreten Gefährdungen entgegen stehender Schutzfunktionalitäten. So wird sichergestellt, dass die Sicherheitsfunktionalitäten der Prüfgegenstände sachgerecht, umfassend und korrekt definiert wurden und über die reine Konformität auch ihre Wirksamkeit geprüft wird. Eine steigende Anzahl formaler Randbedingungen an die Sicherheit der intelligenten Messsysteme, also der zunehmende Grad der Feingranularität, senkt jedoch zwangsläufig Freiheitsgrade in der Entwicklung. Falls diese formalen Randbedingungen die Prozesse eines Herstellers überfordern, kann seine Produktentwicklung kostenintensiver werden, was letztlich das Risiko von Verlusten auf Herstellerseite erhöht. Zudem steigen die Kosten für intelligente Messsysteme auf dem Markt. Hersteller können und sollen daher ihre Interessen durch Mitarbeit an einem abgestimmten Schutzprofil wahrnehmen. Grundsätzlich bietet diese Variante, vorausgesetzt der Verhältnismässigkeit der Anforderungen wird Rechnung getragen eine äusserst sinnvolle Lösung. Ein geeignetes Schutzprofil kann unter Berücksichtigung der in anderen Ländern gemachten Erfahrungen erstellt und auf die spezifischen Anforderungen des hiesigen Energieversorgungssystems adaptiert werden.

Bei der Erarbeitung der Schutzprofile sollte beachtet werden, dass wichtige Funktionen von Smart Grids weiter unterstützt oder zumindest nicht verunmöglicht werden. Das erscheint nicht trivial, da sich die Diskussion um Smart Grids, sowie deren Funktionalitäten und technischen

Umsetzungen noch im Fluss befindet. Die Rolle intelligenter Messsysteme ist derzeit über die Grundlagenarbeiten in der Schweiz abgegrenzt, trotzdem sind weitere sinnvolle Funktionalitäten von Smart Metering Systemen in Smart Grids denkbar. Sie kristallisieren sich ggf. erst mittelfristig im Betrieb heraus. Die zu setzenden Randbedingungen für eine Gewährleistung der Datensicherheit dürfen solche weiteren allfällig sinnvollen Evolutionsschritte nicht verhindern. Dies wiederum steht in einem Widerspruch zur grundsätzlichen Idee von Schutzprofilen, die feingranular technische Anforderungen festlegen und Vorgaben machen. Vor dem Hintergrund, dass in Smart Grids zunehmend IKT eingesetzt werden wird, die unter Umständen mit intelligenten Messsystemen interagiert oder mit ihnen vernetzt wird, erscheint jedoch eine feingranulare Spezifikation zu implementierender Sicherheitsfunktionalitäten ein als deutlich stärkeres und nötiges Instrument. Gewisse Risiken lassen sich jedoch nicht abschliessend vermeiden.

3.2.4 Variante 4: IKT-Sicherheitszertifikat mit zugrunde liegendem Schutzprofil

Diese Variante weist hinsichtlich IKT-Sicherheit die höchste Qualität auf. Sie orientiert sich an einer zentral organisierten Lösung. Wie in Variante 3 folgt die Entwicklung der intelligenten Messsysteme und in diesem Zusammenhang die Datensicherheit einem vorgegebenen Schutzprofil, welches in dieser Variante nun zusätzlich eine Sicherheitszertifizierung durchläuft. Das Schutzprofil ist gemäss CC standardisiert [33, 34, 35] und verfügt über eine ausserordentlich feingranulare und rigide Spezifikation.

Nachdem das intelligente Messsystem gemäss Schutzprofil hergestellt wurde, durchläuft das dieses, wie auch in den anderen Varianten, eine interne Qualitätssicherung beim Hersteller, die sich aufgrund der Anforderungen der CC als vergleichsweise aufwendig gestaltet. Danach erfolgt wiederum eine Konformitätserklärung durch den Hersteller, der eine entsprechende Entwicklungsdokumentation – soweit für die Prüfung gefordert – und weitere spezielle Prüfdokumente bereitstellt. Die Prüfdokumente werden gemäss den detaillierten Anforderungen der CC für das Schutzprofil erstellt und erfordert etwa 25 Einzeldokumente.

Die Prüfung des Produktes findet durch eine externe, unabhängige Prüfstelle statt. Das Prüfverfahren ist durch die Anwendung der CC in seinen Einzelheiten ebenfalls – wie das Schutzprofil – rigide vorgeben. Die Prüfstelle selbst ist nicht nur akkreditiert, wie in der vorhergehenden Varianten, sondern ist zudem lizensiert durch eine zur Herausgabe von CC-Zertifikaten berechtigte Zertifizierungsstelle. Diese fungiert hier als Kontrollstelle wie in Variante 3. Sie muss hier für sich gesondert gewisse, hohe Anforderungen erfüllen, um die Berechtigung zur Zertifizierung zu erlangen. So kann sie z. B. selbst akkreditiert [37, 38] sein. Diese Stelle vergibt schliesslich ein IKT-Sicherheitszertifikat an das von der Prüfstelle evaluierte Produkt. Das CC-Zertifikat verleiht der Prüfung nochmals ein deutlich höheres Gewicht als ein Prüfsiegel einer Stelle, welche die Prüfung nach national definierten Anforderungen und nach einem eigenen Schema (siehe Variante 3) durchführt. Tabelle 4 fasst die wesentlichen Merkmale dieser Variante zusammen.

IKT-Sicherheitszertifikat mit zugrunde liegendem Schutzprofil		
Aspekt	Beschreibung	Bemerkungen
Benötigte Dokumentation	- Pflichtenheft gemäss Schutzprofil (PP abgeleitet aus Standard) - Lastenheft gemäss Schutzprofil - Dokumentation der 6 Assurance Classes: bei einer vorgeschriebenen CC-Prüfstufe erfordert dies ca. 25 Einzeldokumente (Assurance Components)	- vorhandene Standards der Energiebranche hinsichtlich IKT-Sicherheit nur schwach berücksichtigt
Sicherheitsfunktionalitäten	- feingranulare Anforderungen gemäss Schutzprofil - Schutzprofil gemäss ISO15408 (Common Criteria) zertifiziert	- sehr feingranulare und rigide Spezifikation - Schutzprofil wurde durch theoretischen Zertifizierungsprozess bzgl. Widerspruchsfreiheit validiert - Sicherheitseigenschaften aus Sicht IKT-Sicherheit auf einem sehr hohen Niveau spezifiziert - Fehlen ggf. wünschbarer Freiheitsgrade bei der Umsetzung
Prüfkriterien	- Detailliert spezifiziert gemäss ISO15408, Common Criteria - Prüfstelle gemäss ISO17025 akkreditiert - Zertifizierungsstelle gemäss ISO/IEC 17065 akkreditiert oder national als „zuständige Stelle“ benannt - IKT-Sicherheitszertifikat gemäss Common Criteria	- Validierung gemäss Common Criteria durch standardisierte Anforderungen und standardisierte Vorgehensweise zur Prüfung gekennzeichnet - In Verbindung mit auf breiter Basis erarbeitetem Schutzprofil stringentere Ergebnisse im Vergleich zu einer Prüfstelle, die ein eigenes Verfahren verwendet - Prüfsiegel mit deutlich mehr - Zertifizierung kann Ergebnisse verschiedener Prüfstellen in gleicher Weise aufwerten - CC-Zertifikat deutlich höheres Gewicht im Vergleich zu weniger formalen Konformitätsprüfung
Betriebsrisiko	- niedrig; zugesicherte Eigenschaften sind vorgegeben und tiefgehend validiert	–

Tabelle 4: Übersicht Variante 4: IKT-Sicherheitszertifikat mit zugrunde liegendem Schutzprofil

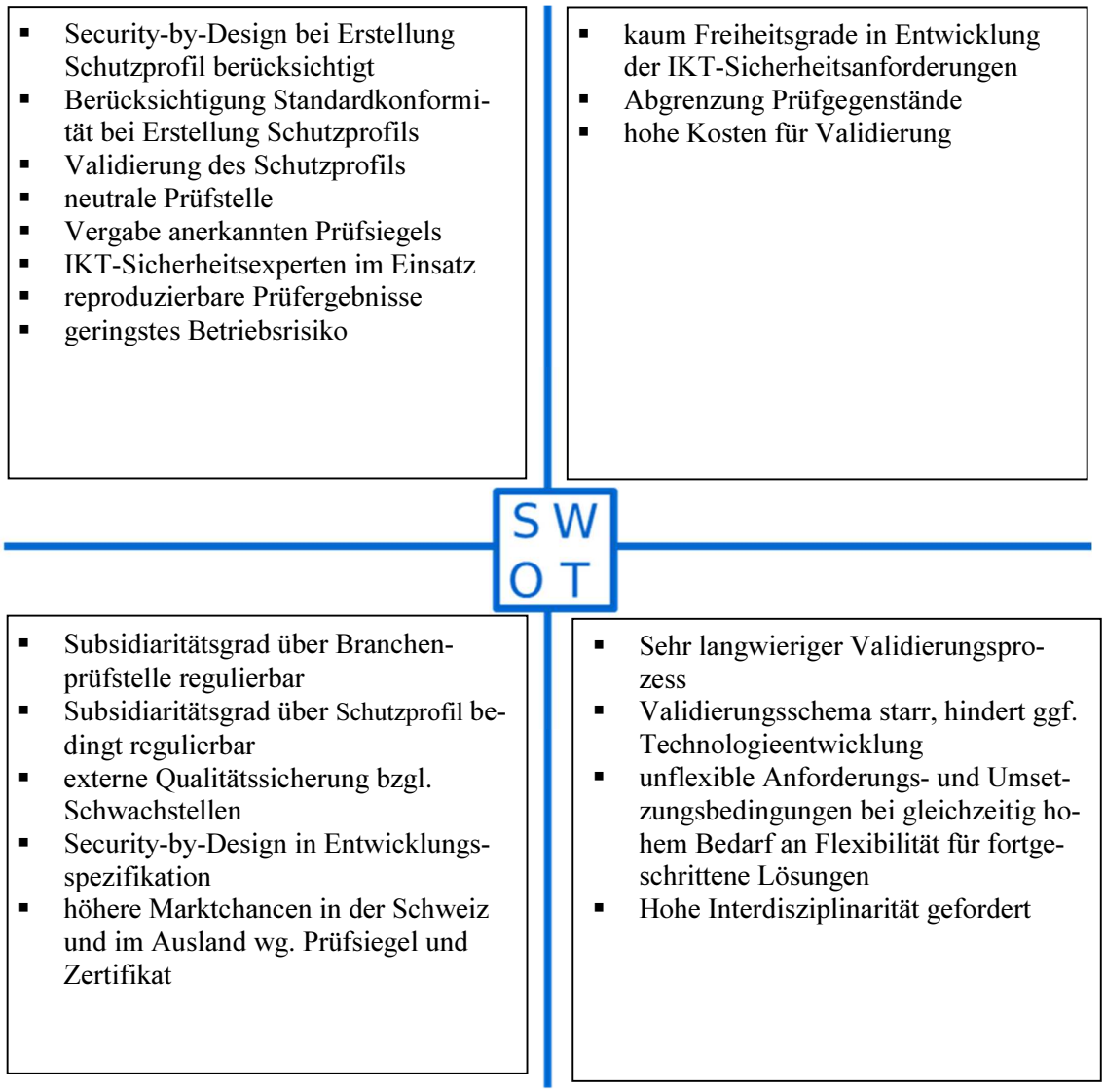

Abbildung 7: SWOT-Analyse Variante 4: IKT-Sicherheitszertifikat mit zugrunde liegendem Schutzprofil

Abbildung 7 stellt die Ergebnisse der SWOT Analyse der Variante 4 in verkürzter Form dar. Die Stärken (Strengths) dieser Variante sind grundsätzlich ähnlich zu denen der Variante 3 allerdings ausgeprägter. Das Schutzprofil hat denselben Prüf- und Zertifizierungsprozess, dem die Smart Meter Systeme als Produkte unterworfen sind, durchlaufen und ist damit objektiv auf einem sehr hohen Niveau der IKT-Sicherheit. Besonders gilt es hier festzuhalten, dass das Betriebsrisiko, aufgrund des feingranularen, und standardkonformen Schutzprofils sowie des feingranularen Prüfschemata gering ist.

Im Wesentlichen können auch ähnliche Schwachstellen (Weaknesses) wie in Variante 3 identifiziert werden, die ebenfalls ausgeprägter sind als zuvor. Insbesondere gilt es festzuhalten, dass kaum Freiheitsgrade in der Entwicklung der IKT-Sicherheitsanforderungen und damit der

Sicherheitsfunktionalitäten existieren, da sehr feingranular festgehalten ist, was zu realisieren ist und wie dies zu geschehen hat. Das Schutzprofil berücksichtigt vorhandene Standards der Energiebranche hinsichtlich IKT-Sicherheit nur schwach. Durch die in den CC formulierten, äusserst feingranularen Festlegungen, die sowohl das Prüfverfahren, die Prüftiefe und den Prüfgegenstand genaue definieren, lässt diese Variante Freiheitsgrade und eine hinreichende Flexibilität vermissen. So wird Innovation in den Produktentwicklungen erschwert, weil für Upgrades unter Umständen eine Re-Zertifizierung erfolgen muss. Hersteller müssen zudem ihre Produkte und Prozesse hinsichtlich des Schutzprofils anpassen, was kostenintensiv ist. Weiter können Hersteller überfordert sein mit der Erstellung der für die Validierung benötigten Dokumente, so z. B. der Entwicklungsspezifikation der intelligenten Messsysteme. Die Kosten der Validierung der Variante 4 sind klar die höchsten im Vergleich zu den vorhergehenden Varianten.

Die Chancen (Opportunities) dieser Variante sind die Gleichen Variante 3, sind jedoch ebenfalls ausgeprägter, da die Anforderungen, etc. spezifischer und daher die Ergebnisse tendenziell qualitativ höherwertiger sind.

Als Risiko (Threats) muss hier vor allem gesehen werden, dass der Validierungsprozess sich langwierig gestaltet. Da die Entwicklungsgeschwindigkeit von Technologien - eben auch der Technologien zu Angriffszwecke - wesentlich höher ist als die Validierungsgeschwindigkeit in dieser Variante, kann die Härtung der Systeme schnell unzweckmässig werden. Hier liegt ein grundsätzliches Problem dieser Variante begründet. Die unflexiblen Anforderungs- und Umsetzungsbedingungen des Validierungsprozesses stehen einem gleichzeitig einem Bedarf an Flexibilität zur Gestaltung fortschrittlicher technischer Lösungen gegenüber, der Anwendungsfälle abbildet, die ggf. bei der Entwicklung der sicherheitstechnischen Anforderungen nicht berücksichtigt wurden. Sind Anforderungen einmal erlassen, können sie ggf. technische Lösungen, welche z. B. im Bereich Smart Grid gebraucht werden, einschränken oder verhindern und könnten so Innovation hemmen. Die Anforderungen und ihre technische Umsetzung können nur sehr schwer kontinuierlich dem sich entwickelnden Stand der Technik angepasst werden. Weiter ist bei der Erarbeitung der Anforderungen eine hohe Interdisziplinarität gefordert, da die Prozesse nicht nur aus Sicht IKT sicher und praktikabel sein müssen sondern eben auch vor dem energiewirtschaftlichen Hintergrund.

Kurzfazit Variante 4

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 jedoch ein IKT-Sicherheitszertifikat gemäss CC klar das stärkste verfügbare Instrument dar. Die Definition der Prüfgegenstände, die umfassende Vorgabe der zu dokumentierenden Prüfaspekte, wie unter anderem Entwicklungs-, Benutzer- und Administratorendokumentation, Produktlebenszyklus, das streng formale Prüfschemata sowie die Akkreditierungen der Prüf- bzw. der Zertifizierungsstelle bilden ein umfassendes System zur Validierung, bei dem idealer Weise alle Aspekte der Prüfgegenstände, die relevant für

dessen IKT-Sicherheitsfunktionalitäten sind, berücksichtigt werden. Dazu kommen Anforderungen an die unmittelbare Betriebsumgebung in Form von technischen Richtlinien für eine Kommunikationseinheit, die kryptographischen Algorithmen und für die Testverfahren, welche von der Prüfstelle geprüft werden. Falls kein entsprechendes Zertifizierungsschema für die Prüfstelle verfügbar ist, können in dieser Variante basierend auf den CC-konforme IKT-Sicherheitszertifikate Prüfstellen aus anderen Nationen anerkannt werden. Lizensierte Prüfstellen sind auf der Homepage der CC-Organisation zu finden [38].

Die Vorteile bringen auch wesentliche Nachteile mit sich. 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. Eine grundsätzlich hilfreiche Strategie für Validierungsverfahren mit einem hinterlegten IKT-Sicherheitszertifikat besteht darin, vorab Prüfgegenstände durch geeignete Abgrenzung zu reduzieren. Hier besteht jedoch die Gefahr unterschiedlicher Auffassungen bei Herstellern und den Herausgebern eines Schutzprofils was als notwendig bzw. hinreichend anzusehen ist.

3.3 Bewertung der Varianten und Fazit

Die Varianten 1 bis 4 weisen jeweils Vor- und Nachteile auf, die es gegeneinander abzuwägen gilt. Um einen Richtungsentscheid hinsichtlich der vertieften Untersuchung von einer der soweit für die Schweiz als grundsätzlich sinnvoll erachteten Varianten zu treffen, sind weitergehende Überlegungen notwendig. Tabelle 5 zeigt dafür eine Gegenüberstellung der vier Varianten im Lichte relevanter Kriterien (erste Spalte). Die Einstufung der Ergebnisse entspricht der Skala: „nicht gegeben“, „mässig gegeben“, „gegeben“. Die Kriterien sind wesentlich für eine sinnvolle Lösung und sollen hier gleich gewichtet werden.

Die Tabelle zeigt, dass Variante 3 wesentliche Vorteile gegenüber den anderen Varianten zeigt. Dies bestätigt das Bild, welches die Kurzfazits bisher vermittelten. 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. Das ist bei den anderen Varianten nicht zwingend gegeben, da entweder kaum oder nur wenige konkrete, spezifische Vorgaben für die Schweiz gemacht werden können oder die Verhältnismässigkeit der Überprüfung nicht gegeben ist. Die Variante 3 ermöglicht weiter die Definition pragmatischer, gut umsetzbarer wie auch wirksamer Vorgaben, die mit einer hohen Akzeptanz rechnen

können, weil die Variante eine noch hohe Subsidiarität im Spezifikationsprozess vorsieht. Beachtet man die Heterogenität der hiesigen Betreiber der intelligenten Messsysteme ist dies wichtig und bei den anderen Varianten kaum gegeben. Letztlich bestehen schon Beispiele in anderen Ländern, wie die Variante 3 umzusetzen wäre, was die Arbeiten vereinfachen kann, da vorteilhafte Vorgehensweisen adaptiert und Fehlentwicklungen vermieden werden.

Relative Bewertungskriterien einer Lösung zur Gewährleistung der Datensicherheit				
Beschreibung	**V1**	**V2**	**V3**	**V4**
Ansatz für die vertrauenswürdige Gewährleistung der Sicherheit intelligenter Messsysteme	nicht gegeben	mässig gegeben	gegeben	gegeben
Ansatz für die Entwicklung Schweiz spezifischer Regelungen	nicht gegeben	mässig gegeben	gegeben	nicht gegeben
Vorgaben für verhältnismässige (Aufwand vs. Sicherheit) Validierungsverfahren möglich	nicht gegeben	mässig gegeben	gegeben	nicht gegeben
Vorgaben für einheitliche, abgestimmte Sicherheitsanforderungen	nicht gegeben	mässig gegeben	gegeben	mässig gegeben
Beispiele vergleichbarer Verfahren (international und national)	nicht gegeben	nicht gegeben	gegeben (z.B. in AT)	gegeben (z. B. in D)

Tabelle 5: Bewertung der ausgewählten Varianten durch Kriterien einer möglichst optimalen Lösung zur Gewährleistung der Datensicherheit.

Der Richtungsentscheid hinsichtlich einer Variante sollte jedoch nicht nur vor dem Hintergrund der oben genannten Kriterien, sondern auch vor dem Schweiz spezifischen Hintergrund und den hiesigen Vorteilen erfolgen. Genannt wurde bereits die Berücksichtigung des stark verankerten Subsidiaritätsprinzips. Die Einbindung vieler Interessen ermöglicht eine breit abgestützte Meinungsbildung, schafft eine hohe Akzeptanz und sorgt für pragmatische Lösungen die umsetzbar sind, könnte jedoch aufgrund einer Verwässerung zu einer zu niedrigen technischen Lösung führen. Dies gilt es zu verhindern. Eine hohe Akzeptanz wird umso wichtiger, als dass die Heterogenität der Betreiber ein Problem darstellen kann. Rigide Vorgaben können sich dahingehend kostensteigernd auswirken, als dass die Komplexität ggf. prohibitiv für kleinere Betreiber sein kann du hier Personal und Kompetenz ggf. unnötig aufgebaut werden muss. Eine einheitliche Lösung, die weitgehend akzeptiert wird, bietet zudem Vorteile für Hersteller und Betreiber der intelligenten Messsysteme, da zu stark individualisierte Lösungen ggf. weder Sicher noch effizient sein können. Wesentlich für die Umsetzung einer der diskutierten Varianten sind daher Ausgewogenheit und Wirkung der Lösung, die durch den Einbezug der wesentlichen Interessengruppen bei der Erarbeitung für die Schweiz ermöglicht wird. Die Ziele

einer Schweiz spezifischen Lösung können für eine nachfolgende Bewertung der Varianten also wie folgt festgehalten werden:

1. Angemessener Anforderungskatalog (Spezifikation) für die IKT-Sicherheit

    a. Tiefe und Durchdringung der abgestimmten, sicherheitstechnischen Anforderungen im Lebenszyklus der Produkte: Spezifikation der Funktionalitäten, Anforderungen an Produktentwicklung, Auslieferung und Betrieb

    b. Tiefgehende Forderungen zur Umsetzung der Sicherheitsanforderungen

2. Verhältnismässigkeit einer Validierung (Prüfschema)

    a. Gutes Verhältnis von Vertrauenswürdigkeit zu Aufwand bei Prüfung von Komponenten

    b. Qualität der Prüfer, der Prüfungen und Reproduzierbarkeit

Ziele	Eigenschaften	Erreichung			
	Beschreibung	V1	V2	V3	V4
1. Angemessener Anforderungskatalog	a) Tiefe, Durchdringung der Anforderungen im Lebenszyklus	nicht gegeben (Begutachtung erfolgt ex post)	mässig gegeben (vom Standard i.d.R. nicht vorgegeben)	gegeben (abhängig vom Schutzprofil)	gegeben (Prüfverfahren so definiert)
	b) Tief gehende Umsetzung Sicherheitsanforderungen	nicht gegeben	mässig gegeben (möglich)	gegeben (relativ gut)	gegeben (sehr gut)
2. Ausgewogenheit Prüfschema	a) Optimales Verhältnis von Vertrauenswürdigkeit zu Aufwand bei der Prüfung von Komponenten	nicht gegeben (zu informelle Vorgehensweise)	mässig gegeben (Wirksamkeit nicht geprüft)	gegeben (sehr gut)	nicht gegeben (Aufwand sehr hoch)
	b) Qualität der ▪ Prüfer ▪ Prüfungen Reproduzierbarkeit	nicht gegeben (uneinheitlich; nicht formal nachgewiesen)	gegeben (gut)	gegeben (gut)	gegeben (sehr gut)

Tabelle 6: Bewertung der Varianten hinsichtlich einer wirksamen und pragmatischen Lösung zur Gewährleistung der Datensicherheit intelligenter Messsysteme.

Tabelle 6 zeigt eine Bewertung der Varianten hinsichtlich der Angemessenheit eines Anforderungskatalogs sowie der Verhältnismässigkeit eines Prüfschemas. Der Anforderungskatalog sollte ganzheitliche Sicherheitsaspekte über den Produktlebenszyklus umfassen sowie konkrete und prüfbare Umsetzungsvorgaben machen, welche die Bewertung von Korrektheit und Wirksamkeit der IKT-Sicherheit erlauben. Das Prüfschema sollte durch ein ausgewogenes Verhältnis von Aufwand für die Prüfung und Belastbarkeit der Ergebnisse gekennzeichnet sein. Gleichzeitig muss eine Vorgabe an die Qualität der Prüfverfahren existieren. Die Bewertungsskala besteht auch hier wiederrum aus „nicht gegeben“, „mässig gegeben“, „gegeben“.

Tabelle 6 zeigt – auch im Zusammenhang mit der Tabelle 5 –, dass hinsichtlich der gesetzten Ziele die Variante 1 kaum einer vertieften Betrachtung bedarf. Zwar weist sie, wie die SWOT-Analyse des Kapitels 3.2 gezeigt hat, aus Sicht Hersteller viele Stärken und wenige Risiken auf, aber aus Sicht Betreiber, Konsumenten und Staat vermag sie aufgrund eines kaum angemessenen Anforderungskataloges, der weder genügend Tiefe noch Breite aufweist, kaum hinsichtlich eines geeigneten Sicherheitsniveaus zu überzeugen. Nicht zu vernachlässigende Betriebsrisiken im Bereich der Sicherheit machen die Variante aus einer Gesamtperspektive unattraktiv.

Variante 4 kann als Maximalvariante verstanden werden. Ihre Stärken liegen bei sehr tiefgehenden und breiten Anforderungen. Sie gewährleistet einen sehr sicheren Betrieb der Infrastruktur. Hinsichtlich Verhältnismässigkeit sind jedoch Schwächen eminent. Gerade die tiefgehenden, technischen anspruchsvollen Anforderungen und die aufwendigen Prüfverfahren wirken sich als stark hemmend für eine zügige Einführung sicherer intelligenter Messsysteme aus. Mehr noch, die Variante ist tendenziell kostentreibend, erhöht Verwaltungsaufwand und Komplexität. Betreiber und Hersteller können überfordert werden. Da ein ausgewogenes Verhältnis von Vertrauenswürdigkeit gegenüber Aufwand bei dieser Lösung tendenziell nicht erreicht werden kann, scheidet auch diese Variante für die folgenden Betrachtungen aus.

Bei den beiden Varianten 2 und 3 zeichnet sich ab, dass ein formal vorgegebener Validierungsprozess und ein Anforderungskatalog wesentliche Vorteile bieten. Variante 2 weist Nachteile bezüglich der Angemessenheit der Anforderungen auf, da diese auf Basis der verfügbaren Standards zu offen oder zu lose formuliert sind, als dass sie wirklich gut geeignet sein können, ein adäquates Sicherheitsniveau zu bieten. Dies gilt über den gesamten Lebenszyklus der Produkte als auch für die einzelnen sicherheitstechnischen Anforderungen. Zudem bestehen kaum internationale Erfahrungen mit dieser Variante, was jedoch nicht heissen muss, dass sie daher per se nicht umsetzbar ist. So schneidet diese Variante auch nur mässig hinsichtlich des Ziels eines angemessenen Anforderungskataloges ab. Eine Konformitätsprüfung der korrekten Implementierung liefert aufgrund der vorgegebenen Validierungsschritte belastbare und reproduzierbare Ergebnisse. Die Wirksamkeit wird jedoch nicht geprüft und ist daher nicht unbedingt gewährleistet. Die Variante kann somit nicht vollends hinsichtlich der zu erreichenden Ziele überzeugen, ist aber aufgrund der Bewertung nicht unbedingt für die Schweiz auszuschliessen.

Die Variante 3 ist hinsichtlich der beiden Ziele – also hinsichtlich eines angemessenen Anforderungskataloges und der Verhältnismässigkeit der Prüfung - als gut geeignet zu bewerten. Die Erarbeitung eines Schutzprofils mit feingranularen Anforderungen an Lebenszyklus und Technik wirkt sich vorteilhaft auf das Sicherheitsniveau aus. Die Anforderungen können in der nötigen Breite und Tiefe definiert werden. Dadurch, dass das Schutzprofil subsidiär auf Basis einer Schutzbedarfsanalyse erarbeitet wird, ist zudem ihre Angemessenheit, auch vor dem Hintergrund der Schweiz spezifischen Situation mit vielen, heterogenen Netzbetreibern, gesichert. Die formale Konformitätsprüfung gegen das individuell für die Schweiz erarbeitete Schutzprofil bietet ein gutes Verhältnis von Vertrauenswürdigkeit zu Aufwand. Zudem bietet ein Schutzprofil eine detaillierte Wegleitung für die Umsetzung der Sicherheitsfunktionalitäten in Design und Herstellung. Die individuell auf das nationale Schutzprofil ausgelegte Prüfung ermöglicht eine geeignete und schlanke Umsetzung der Konformitätsprüfung. Die Prüfschemata und die Prüfgegenstände werden vorgängig angemessen und subsidiär erarbeitet, was das Verhältnis zwischen Prüfungsaufwand und Sicherheitsniveau sinnvoll gestaltet. Die Qualität der Prüfer, der Ergebnisse und die Reproduzierbarkeit lassen sich als gut einschätzen.

Variante 2 und Variante 3 sind also grundsätzlich beide möglich für die Schweiz. Variante 3 ist etwas aufwändiger, bietet aber letztlich deutlich bessere Ergebnisse hinsichtlich der Kriterien in Tabelle 5 und der Ziele in Tabelle 6. Im Folgenden soll daher untersucht werden, wie Variante 3 konkret ausgestaltet werden kann. Kapitel 4 stellt dar, welche Rollen Bund, Betreiber und Hersteller einnehmen, wie der gesamte Prozess zur Gewährleistung der Datensicherheit für Smart Metering Systeme in der Schweiz aussehen kann, welche Aktivitäten jeweils erforderlich sind. Dazu werden zunächst nötige Vorarbeiten beschrieben, auf die der eigentliche Prozess aufsetzt.

4. Konformitätsprüfung intelligenter Messsysteme mit zugrunde liegendem Schutzprofil

Die Konformitätsprüfung mit zugrunde liegendem Schutzprofil bietet - also die Variante 3 - ein effizientes Validierungssystem, das auf dem Subsidiaritätsprinzip aufbaut, ein vergleichsweise hohes Vertrauenswürdigkeitsniveau sichert und einen hohen Grad an Flexibilität bietet. Ein vertrauenswürdiger Betrieb bedeutet die Minimierung der Auswirkungen IKT-basierter Angriffe auf schützenswerte Daten und auf den Betrieb der Smart Metering Systeme im Rahmen der Verhältnismässigkeit. Einem Verlust der Vertraulichkeit bzw. der Integrität sowie dem Verlust der Verfügbarkeit der Daten oder sogar des gesamten Systems wird vorgebeugt. Die auszugestaltende Lösungsstrategie umfasst gemäss Variante 3 des Kapitels 3.2

- die Identifizierung eines Schutzbedarfs und darauf basierend
- die Erarbeitung eine abgestimmten sicherheitstechnischen Anforderungskataloges,
- sowie eine Validierung der umgesetzten Anforderungen durch Prüfstellen, welche ein geeignetes Prüfverfahren geeigneter Prüftiefe verwenden.

Dabei sollte beachtet werden, dass einzelne Interessengruppen (z.B. Hersteller oder Betreiber) keine inakzeptablen Einschränkungen hinnehmen oder ungerechtfertigte Aufwände tragen müssen. Abbildung 8 veranschaulicht die Lösungsstrategie und die wesentlichen Teilschritte, die in Kapitel 4.1, 4.2 und Kapitel 4.3 näher erläutert werden

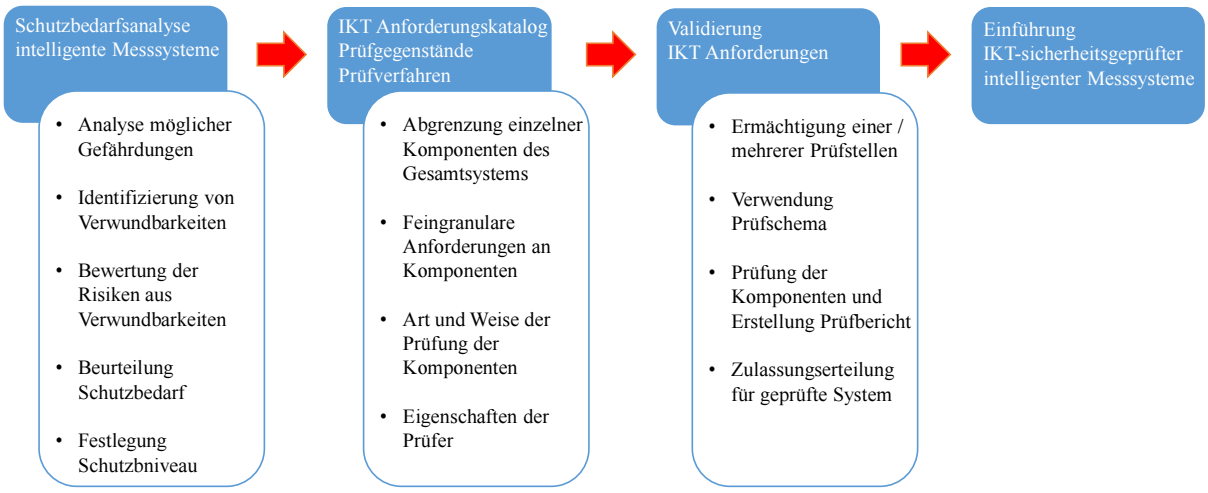

Abbildung 8: Wesentliche Prozessschritte zur Gewährleistung der Datensicherheit intelligenter Messsysteme beim Endverbraucher.

4.1 Schutzbedarfsanalyse

Eine grundsätzliche Randbedingung ist die Anwendung eines ganzheitlichen Ansatzes, so dass sichergestellt ist, dass keine erwartete IKT-Sicherheitsschwachstelle unberücksichtigt bleibt. Dieser ganzheitliche Ansatz wird bei einer umfassenden Schutzbedarfsanalyse berücksichtigt. Neben den Gefährdungen identifiziert und umreisst sie Risiken, deren Eintrittswahrscheinlichkeiten sowie das Schadensausmass[9]. Sie ist die Grundlage zur Erstellung eines IKT-Sicherheitsanforderungskatalogs. So wurden auf internationaler Ebene Schutzbedarfsanalysen durchgeführt, um eine Basis für die Sicherung dieser Infrastruktur zu legen. Diese Analysen werden als vertraulich eingestuft und sind für die in der Schweiz zu leistenden Arbeiten nicht erhältlich. Die Ergebnisse der deutschen Schutzbedarfsanalyse sind implizit im Schutzprofil des Smart Meter Gateway enthalten, welches den deutschen Sicherheitsanforderungskatalog darstellt[10]. Es ist nicht trivial, den Schutzbedarf aus diesen Anforderungen heraus zu destillieren. Die Anforderungen und damit auch der Schutzbedarf sind zudem weder direkt auf die schweizerischen Verhältnisse (vgl. [6]) anwendbar noch stossen der deutsche Prozess zur Validierung oder die konkreten Sicherheitsanforderungen an die Smart Metering Gateways auf eine übergreifende Akzeptanz.

Die Schutzbedarfsanalyse für Smart Metering Systeme muss also für die Schweiz gesondert erstellt werden, um die hiesigen Verhältnisse von Grund auf abzubilden. Die technischen Funktionen von Smart Metering Systemen sind hierzu bereits identifiziert [5]. Anwendungsfälle bei denen Smart Metering Systeme involviert sind, sind in [7] umrissen, müssen aber ggf. noch näher und auf Basis der technischen Funktionen konkretisiert werden. So kann ein für die Schweiz individuell angepasster und sinnvoller Anforderungskatalog erstellt werden. Die Schutzbedarfsanalyse muss aus folgende, aufeinander aufbauende Elemente enthalten:

- Analyse möglicher Gefährdungen, welche die intelligenten Messsysteme bzw. deren Funktionalitäten und die Datensicherheit beeinträchtigen könnten.
- Identifizierung von Verwundbarkeiten der Komponenten intelligenter Messsysteme und Bewertung der Risiken, welche sich aus den jeweiligen Verwundbarkeiten ergeben. Dabei sollten auch Gesamtsystemrisiken für die Stromversorgung betrachtet werden, die von den intelligenten Messsystemen ausgehen könnten.
- Beurteilung des Schutzbedarfs für Komponenten intelligenter Messsysteme und Empfehlung eines geeigneten Schutzniveaus. Bei der Festlegung des erforderlichen Schutzniveaus ist das Prinzip der Verhältnismässigkeit zu berücksichtigen.

[9] Ein Schutz gegen jegliche Gefährdungen ist kaum möglich noch wirtschaftlich sinnvoll. Risiken bleiben immer, wenn auch noch so klein, bestehen.
[10] Die technischen Mindestanforderungen an intelligente Messsysteme bei Endverbrauchern in Deutschland, welche sich nicht auf die Sicherheit beziehen, unterscheiden sich stark von denen, welche in der Schweiz als sinnvoll identifiziert wurden. Insbesondere decken die in Deutschland im Referentenentwurf zur Einführungsverordnung von Smart Metering angestrebten Mindestfunktionalitäten eine Vielzahl von Steuerungsmöglichkeiten und Kommunikationsverbindungen mit verschiedenen Akteuren ab. Insofern unterscheiden sich die Anwendungsfälle für Smart Metering Systeme in Deutschland und der Schweiz grundsätzlich.

Die Schutzbedarfsanalyse schafft somit eine Grundlage zur Erarbeitung geeigneter Massnahmen zum Schutz dieser Infrastruktur. Ein Beispiel sei der Lastunterbrecher. Falls eine sogenannte Breaker-Funktion im Smart Metering System implementiert ist, muss untersucht werden, inwiefern von dieser Gefährdungen ausgehen und welche Risiken diese Funktion nach sich zieht. Ein weiteres Beispiel wäre die Erstellung von Prognosen von Last und Produktion für den Netzbetreib, deren Integrität für die Stabilität des Netzes wichtig ist. Weitere Möglichkeiten sind in der Analyse zu identifizieren.

4.2 Anforderungskatalog, Prüfgegenstände und Prüfschemata

Nachgelagert zur Schutzbedarfsanalyse ist ein Anforderungskatalog in der Schweiz zu erstellen. Er spezifiziert in der Form eines Schutzprofils – d.h. feingranular – technische Anforderungen für die Smart Metering Systeme, die die Systeme gegen die zuvor erkannten Risiken zu wappnen. Die prüfbaren IKT-Sicherheitsfunktionalitäten sind direkte Gegenmassnahmen zu den in der Schweizer Schutzbedarfsanalyse identifizierten Gefährdungen. In dem Anforderungskatalog wird spezifiziert, welche Sicherheitsmassnahmen – beispielsweise in Bezug auf Autorisierung, Authentifizierung und Verschlüsselung – für einzelne Komponenten des Systems die Gefährdungen abwehren bzw. auf ein hinnehmbares Mass (Restrisiko) mindern.

Im schweizerischen Anforderungskatalog müssen also gleichzeitig zu den technischen Sicherheitsanforderungen auch einzelnen Komponenten des Systems gegeneinander abgegrenzt werden. Hierfür kommen alle Elemente des intelligenten Messsystems gemäss der Definition in [6] in Frage. Diese Gegenstände werden als Prüfgegenstände bezeichnet und auf die Erfüllung der Anforderungen geprüft. Sie weisen nach der bestandenen Prüfung eine nachgewiesene Härtung gegen die identifizierten Gefährdungen (z. B. Hacker-Angriff o.ä.) auf. Die Abgrenzung der Prüfgegenstände muss so erfolgen, dass Anforderungen an diese Gegenstände in ihrem Zusammenwirken die für intelligente Messsysteme angenommenen Gefährdungen vollständig und wirksam abwehren. Die Abgrenzung mehrerer logisch, räumlich und funktional unterschiedlicher Komponenten erleichtert auch die technische Umsetzung und Prüfung, ist aber keinesfalls trivial. Die Definition eines Prüfgegenstands und entsprechende Prüfung als eigenständiges Objekt muss erfolgen, weil ein allfällig bereits beim Betreiber der Geräte implementiertes Information Security Management System (ISMS) keine Aussage zum Grad und Stand der „Systemhärtung“ eines Systems gegen unbefugte Zugriffe ausserhalb des unmittelbaren Einflussbereichs des Betreibers (z. B. im Haushalt des Angreifers) erlaubt.

Es genügt nicht einen Katalog sicherheitstechnischer Anforderungen und die zu prüfenden Gegenstände zu definieren. Es ist in der Schweiz weiter festzulegen, wie die Gegenstände geprüft werden. Hierzu müssen Prüfschemata entwickelt werden, die pro abgegrenztem Prüfgegenstand definiert werden. Das Prüfschema ist die spezifische Anleitung zur Untersuchung, ob die Kor-

rektheit und die Wirksamkeit der implementierten Sicherheitsfunktionalitäten im Prüfgegenstand gewährleistet sind. Hierbei ist auf eine sinnvolle Prüftiefe zu achten. Weiter gewährleisten Prüfschemata einheitliche Qualitätsstandards. Hierzu zählen u.a. die Spezifikation und Transparenz der Verfahren an sich, die Vergleichbarkeit der Ergebnisse, eine Dokumentation des Prüfschemas und der Ergebnisse, sowie die Anforderungen an die Prüfer selbst (Ausbildung gemäss gewisser Standards), etc. Die schweizerischen Prüfschemata sollen für pragmatische, auf die Schweizer Situation zugeschnittene Lösungen sorgen. Die Arbeiten zur Definition eines geeigneten Prüfschemas erfolgen parallel zur Festlegung der Sicherheitsanforderungen.

4.3 Validierung der IKT Sicherheitsanforderungen

Nachdem also Anforderungen, Prüfgegenstände und Prüfschemata definiert wurden, gilt es die Implementierung der Sicherheitsanforderungen auf Vollständigkeit und Wirksamkeit zu überprüfen. Dies geschieht durch akkreditierte Prüfstellen, die das dazu das spezifizierte Prüfschema heranziehen. Gemäss der gewählten Variante existieren zwei Typen von Prüfschemata. Typ A basiert auf internationalen Standards, z.B. CC bzw. ISO15408, und Typ B auf einem individuellem, gegebenenfalls auf nationaler Basis festzulegenden Standard [35]. Die Prüfstelle übernimmt ein erstelltes Prüfschema und meldet es bei der Akkreditierungsstelle. Falls kein Dritter ein Prüfschema erstellt, kann die Prüfstelle ihr Prüfschema grundsätzlich auch selbst definieren. Die Prüfstelle wird, sofern sie die Auflagen der Akkreditierungsstelle erfüllt, akkreditiert und kann dann offiziell die Prüfung der intelligenten Messsysteme gemäss der Prüfschemata vornehmen. Bereits bestehende ausländische, akkreditierte Prüfstellen können verwendet werden, wenn die betreffende Prüfstelle ihre Akkreditierung um das entsprechende Prüfschema aus dem national spezifizierten Anforderungskatalog erweitert sich für die Typ B Prüfung dieses Kataloges akkreditieren lässt. Eine nationale Prüfstelle muss also nicht gefordert werden, wäre aber aufgrund der geographischen und kulturellen Nähe vorteilhaft.

Die Stelle prüft Prüfgegenstände eines Produktmusters des intelligenten Messsystems, das in der Schweiz eingeführt werden soll. Dies erfolgt unter der Annahme einer gleichbleibenden Qualität der Produktion. Die Systeme müssen einer speziellen, gleichbleibenden Art der Konfiguration zugeordnet werden, indem nachgewiesen wird, welche Konfiguration der Software und der Hardware verwendet wurde. Die Prüfung sollte im Idealfall möglichst unabhängig vom Stand der Technik sein. Die Prüfung sollte mit der Einführung neuer Technologien im Bereich IKT weiterhin möglich sein, selbst wenn sich technische Umsetzungen der Anforderungen ändern.

Nach einer erfolgten Prüfung erstellt die schweizerische Prüfstelle einen Prüfbericht, in dem sie entweder den Nachweis der Konformität zum Anforderungskatalog dokumentiert oder aber Defizite bei nicht konformen Prüfgegenständen ausweist. Bei erfolgreich durchlaufener Konformitätsprüfung wird dem Prüfgegenstand ggf. ein Prüfsiegel mit Lebensdauer mitgegeben, das bei gewissen Updates oder Upgrades allenfalls zu erneuern ist. Um festzustellen, ob die

Prüfstelle qualitativ gute Arbeit geleistet hat, ob defizitäre Produkte ggf. doch betrieben werden dürfen oder ob Nachbesserungen erfolgen sollen, muss eine Kontrollstelle etabliert werden, die eine finale Zulassungsermächtigung der Geräte verantwortet.

4.4 Rollen im Rahmen der Etablierung einer Konformitätsprüfung

Damit eine Sicherheitsvalidierung gemäss dem Prozess aus Abbildung 8 stattfinden kann, sind Vorarbeiten und Aktivitäten verschiedener Akteure notwendig. Abbildung 9 zeigt die nötigen Vorarbeiten, Aktivitäten und die Interaktion der unterschiedlichen Akteure.

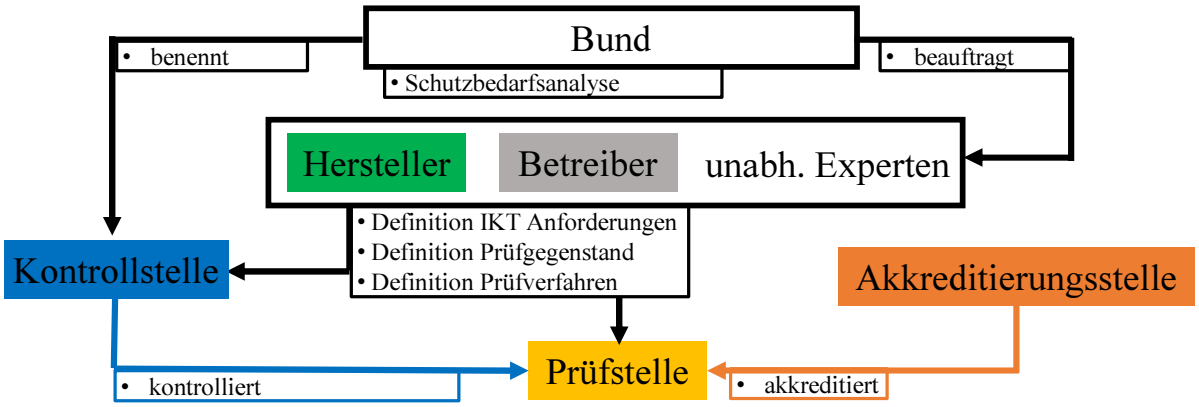

Abbildung 9: Notwendige Vorarbeiten und Aktivitäten unterschiedlicher Akteure, um eine geeignete Ausgangssituation für IKT-Sicherheitsvalidierungen zu schaffen.

4.4.1 Bund

Der Bund erstellt die Schutzbedarfsanalyse und identifiziert zusammen mit unabhängigen Experten die Gefährdungen und Verwundbarkeiten von intelligenten Messsystemen im Kontext des gesamten Stromversorgungssystems. Er analysiert die Risiken, bestimmt den Schutzbedarf. Und legt somit die Grundlage für die weiteren materiellen Arbeiten. Der Bund reguliert weiter den Prozess zur Gewährleistung der Datensicherheit in intelligenten Messsystemen, indem er die Pflicht zur akkreditierten Prüfung der korrekten und wirksamen Umsetzung von IKT-Sicherheitsanforderungen festlegt, den Stand der Technik für die Sicherheitsmassnahmen als ausschlaggebend erklärt und eine Aktualisierungen der Sicherheitsanforderungen vor dem Hintergrund des Standes der Technik fordert. Hierzu benennt der Bund eine Kontrollstelle. Er fordert die Erarbeitung der Sicherheitsanforderungen vor dem Hintergrund des Standes der Technik, die Abgrenzung der Prüfgegenstände und die Erarbeitung der Prüfschemata, welche subsidiär von Herstellern, Betreibern und unabhängigen IKT-Experten durchgeführt werden sollte. Er kann externe IKT-Experten beauftragen, die subsidiär erarbeiteten Grundlagen zu begutachten und kann auf Basis der Einschätzungen des Gutachtens Nachbesserungen fordern.

4.4.2 Betreiber Smart Metering Systeme (Strombranche/Verteilnetzbetreiber)

Die Betreiber beteiligen sich an den Arbeiten zur Definition der sicherheitstechnischen Anforderungen, der Abgrenzung von Prüfgegenständen sowie der Prüfschemata. Sie lassen ihr Wissen hinsichtlich interner Prozesse, Datenaustausch sowie Schnittstellen einfliessen. Die Betreiber setzen für das intelligente Messsystem schliesslich die hinsichtlich IKT-Sicherheit zugelassenen Produkte ein. Der Betreiber ermöglicht die Durchführung von Stichproben aus begründetem Anlass.

4.4.3 Hersteller (OEMs)

Die Hersteller sind ebenfalls an der Erarbeitung der sicherheitstechnischen Anforderungen, der Abgrenzung von Prüfgegenständen sowie der Erarbeitung der Prüfschemata beteiligt. Die Hersteller entwickeln daraufhin Produkte, welche die Anforderungen an die Prüfgegenstände bezüglich IKT-Sicherheit aus dem Anforderungskatalog erfüllen. Die im Anforderungskatalog definierten Prüfgegenstände sind als abgrenzbare funktionale Einheit in den hergestellten Produkten enthalten. Um die Erfüllung der Sicherheitsanforderungen durch den Prüfgegenstand zu validieren, und im Erfolgsfall die Zulassung zum Einsatz des Produkts im Feld zu erhalten, lässt der Hersteller die Geräte durch eine akkreditierte, ermächtigte Prüfstelle prüfen.

4.4.4 Unabhängige IKT Experten

Diese werden bei der Erarbeitung der Schutzbedarfsanalyse, der IKT Sicherheitsanforderungen, der Prüfschemata und der Abgrenzung der einzelnen Prüfgegenstände einbezogen und arbeiten beratend mit. Sie sorgen dafür, dass die durch Hersteller und Betreiber ausgestaltete, pragmatische Lösung technisch weiterhin genügend gut geeignet ist, die Gefährdungen abzuwehren. Sind können auch von Bund beauftragt werden, die subsidiär erarbeiteten, technischen Grundlagen zu begutachten.

4.4.5 Prüfstelle

Die Prüfstelle ist eine eigenständige, unabhängige juristische Person. Sie ist keine Einheit der Bundesverwaltung sondern sozusagen am Markt etabliert. Sie erfüllt die Prüfstellennorm ISO17025 und durchläuft die notwendigen Prozesse zur Akkreditierung durch die Schweizerische Akkreditierungsstelle (SAS)[11]. Sie ist akkreditiert, eine Prüfung basierend auf einem Anforderungskatalog durchzuführen. Die Prüfstelle nimmt Prüfaufträge in der Regel vom Hersteller entgegen. Ein Prüfauftrag kann auch durch Dritte (z.B. Betreiber) in der Rolle eines Sponsors vergeben werden. In letzterem Falle würde der Betreiber die Kosten der Prüfung übernehmen, die ansonsten vom Hersteller übernommen und in den Produktpreis eingepreist werden. Die Prüfstelle führt Prüfungen gemäss dem Anforderungskatalog, der Prüfgegenstände

[11] Derzeit sind von der SAS 35 Prüfstellen für Elektrotechnik, 2 Prüfstellen für Informatik, keine Prüfstellen für die IKT-Sicherheit akkreditiert. In Europa sind ca. 30 Stellen für IKT-Sicherheit akkreditiert.

und der Prüfschemata durch. Gegenstand der Prüfung im Prüflabor ist der Prüfgegenstand selbst in Form eines bereitgestellten Musters und der entsprechenden Spezifikationen. Nach Abschluss der Prüfung teilt die Prüfstelle dem Hersteller und ggf. dem Sponsor das Prüfergebnis in Form eines Prüfberichts mit. Sie kann ein spezifisches Prüfsiegel vergeben.

4.4.6 Kontrollstelle

Die Kontrollstelle wird vom Bund benannt und begleitet die Erarbeitung des Anforderungskatalogs, die Abgrenzung der Prüfgegenstände sowie der Prüfschemata. Sie stellt deren Aktualität fachlich sicher. Die Kontrollstelle führt ein Verzeichnis geeigneter, akkreditierter Prüfstellen, welche nachgewiesen haben, dass sie das Prüfschema im Anforderungskatalog durchführen können und prüft diese in regelmässigen Abständen. Die Kontrollstelle entscheidet letztlich auch, ob die nationale Akkreditierung einer internationalen Prüfstelle nötig ist. Durch die Forderung einer Akkreditierung durch die SAS oder eines Äquivalentes kann der Kontrollstelle ein gewisser Spielraum gelassen werden, welche Prüfstellen ermächtigt werden. Der Prüfprozess zur Gewährleistung der Datensicherheit selbst soll direkt an fachliche Prüfstellen übergeben werden. Lediglich eine kompetente Prüfung der Prüfberichte sowie der Ergebnisse wäre bei einer Bundesstelle als Kontrollstelle zu etablieren. Sie erteilt nach einer Korrektheits-Bewertung der Prüfung eine Zulassung zum Betrieb und vergibt ggf. ein Zeichen, das am Messgerät selbst angebracht wird. Dieses kann Grundlage für die Anrechenbarkeit der intelligenten Messsysteme in den Netzkosten sein. Bei Mängeln, die durch die Prüfstelle festgestellt werden, kann die Kontrollstelle eine Forderung an den Hersteller zur Nachbesserung formulieren. Die Kontrollstelle kann Stichproben an markteingeführten Produkten sowohl beim Hersteller vor Ort als auch bei installierten Produkten bzw. implementierten Anwendungen durchführen.

Ein derartiges Vorgehen ist derzeit in der Schweiz schon etabliert. Eine Kontrollstelle ist bei der METAS für Messgeräte eingerichtet. Sie wacht derzeit über die Einhaltung der Konformität von Stromzählern hinsichtlich messtechnischer Anforderungen und vergibt dabei eine Zulassungszertifikat und ein Zulassungszeichen. Letztere werden an den Messgeräten angebracht, nachdem ihre Konformität bzgl. den messtechnischen Anforderungen erwiesen wurde. Ähnlich soll auch die Kontrollstelle für IKT-Sicherheit funktionieren.

4.4.7 Akkreditierungsstelle

Die Schweizerische Akkreditierungsstelle SAS betreut die Prüfstellen in der Schweiz hinsichtlich der Einhaltung der in ISO17025 spezifizierten Anforderungen hinsichtlich Qualitätsmanagement und fachlicher Qualifikation[12].

[12] Ausländische Prüfstellen, welche wiederrum durch ausländische Akkreditierungsstellen akkreditiert wurden, einzubeziehen erscheint grundsätzlich möglich, bedarf aber noch einer vertieften, vor allem juristischen Abklärung.

4.5 Ablauf der IKT-Sicherheitsvalidierung – Schritt für Schritt

Die folgenden Schritte beschreiben die Abwicklung einer Konformitätsprüfung nach Variante 3, die mit der Abbildung 10 veranschaulicht ist. Die Beschreibung dieses Ablaufs basiert auf der oben ausgeführten Rollenverteilung der jeweiligen Akteure, konkretisiert ihre Aufgaben aber dort wo nötig.

- **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. Die Prüfgegenstände sind Teil eines intelligenten Messsystems; ihre erforderlichen Sicherheitsfunktionalitäten werden detailliert im Anforderungskatalog festgelegt. Der Hersteller stellt sein Produkt, die dazu gehörende und notwendige technische Dokumentation sowie weitere Informationen über sicherheitsrelevante Prozesse (gem. Anforderungskatalog) der Prüfstelle zur Verfügung. Zu diesem Lieferumfang gehören u.a. die Produktidentifikation (z.B. Seriennummer; Versionsstand aus einem Konfigurationskontrollsystem etc.), die Produktdokumentation sowie alle die IKT-Sicherheitsfunktionalitäten umfassenden, technischen Spezifikationen. Darüber hinaus werden die sicherheitsrelevanten Prozesse im Lebenszyklus eines Prüfgegenstandes vom Hersteller für die Prüfstelle dokumentiert (Sicherheit in der Entwicklung, bei der Auslieferung, bei der Inbetriebnahme, Updatefunktionalitäten).

- **Schritt 2: Produkt an Prüfstelle**

Die Prüfung läuft – ggf. interaktiv – zwischen Prüfstelle und Hersteller ab. Die Prüfschritte, die im Prüfschema für die einzelnen Prüfgegenstände aufgeführt sind, werden Schritt für Schritt ausgeführt und die im Anforderungskatalog definierten Sicherheitsfunktionalitäten überprüft. Während der Prüfung unterstützt der Hersteller die Prüfstelle durch zusätzliche Informationen, welche in begründeten Fällen seitens der Prüfstelle angefordert werden können. 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. Dies kann z. B. auf Basis dokumentierter Prozesse erfolgen. Die Prüfung kann bei festgestellten Mängeln auch Revisionszyklen des Prüfgegenstandes durch den Hersteller zur Behebung zulassen. Die Prüfstelle übermittelt nach Abschluss der Prüfung das Prüfergebnis in Form eines Prüfberichtes an den Hersteller. Im Erfolgsfall sollte von dieser Prüfstelle ein Prüfsiegel vergeben werden, dass einen Nachweis der Konformität darstellt und eine Revisionssicherheit ermöglicht. Im Falle einer erfolgreich absolvierten Prüfung unterrichtet der Hersteller die Kontrollstelle und das Produkt erhält von der Kontrollstelle eine Zulassung zum Betrieb.

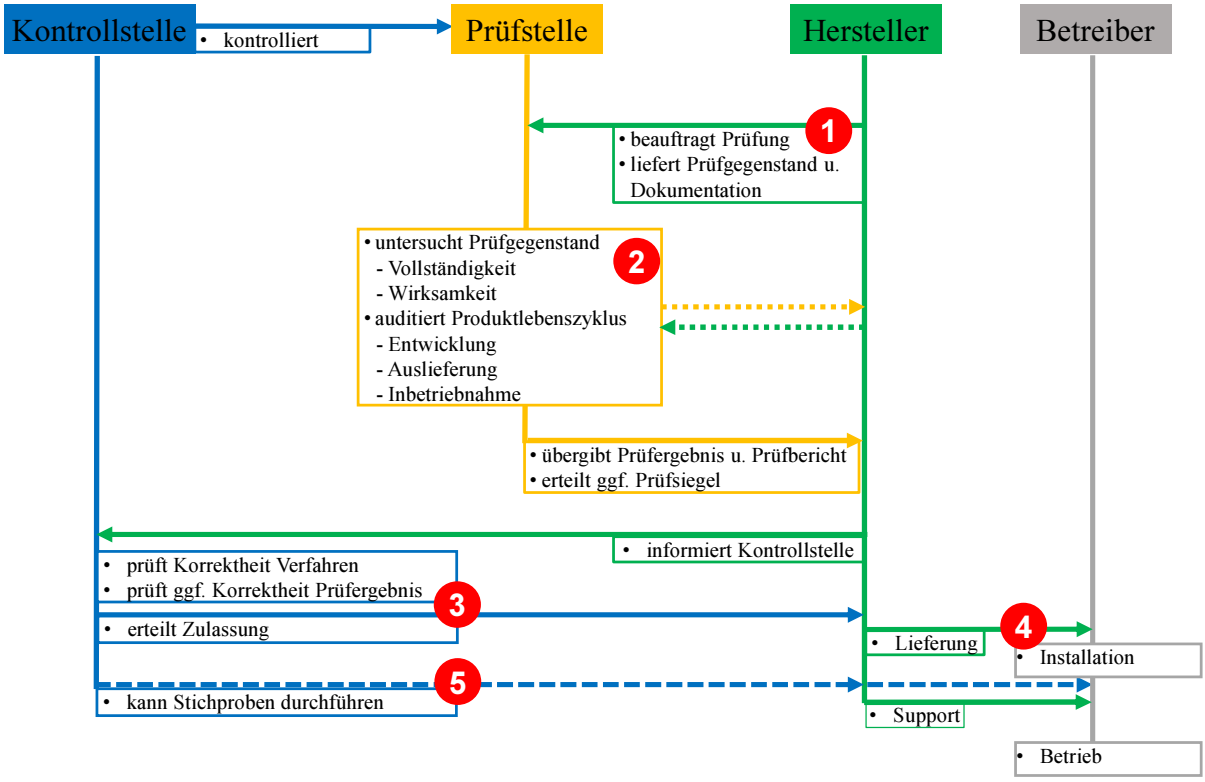

Abbildung 10: Ablauf der IKT Sicherheitsvalidierung - Schritt für Schritt. Die Nummern bezeichnen die im Text beschrieben Schritte.

- **Schritt 3: Prüfung durch Kontrollstelle und Zulassungsermächtigung**

Die Kontrollstelle erhält den Prüfbericht vom Hersteller des intelligenten Messsystems und nimmt das betreffende Produkt in ein Verzeichnis auf. Sie prüft den Bericht hinsichtlich der Korrektheit des Verfahrens und der Ergebnisse. Bei Unregelmässigkeiten oder defizitären Prüfungen veranlasst sie Nachbesserungen oder Prüfungen bei einer anderen Prüfstelle. 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. Das Prüfsiegel und die Zulassung der Kontrollstelle erlauben Transparenz für die vom Regulator durchgeführte Kostenprüfung und sichern so die Anrechenbarkeit.

- **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. Letztere könnten z.B. gehäufte Fehler in Abrechnungsprozessen oder Datenlecks sein.

5. Schlussfolgerungen

Smart Metering Systeme sind ein Bestandteil der Stromverteilungsnetze und damit auch ein Teil einer kritischen Infrastruktur. Es bestehen über eine Vernetzung verschiedener Informationsverarbeitungssysteme beim EVU Schnittstellen zu Vorgängen im Abrechnungs- und Verwaltungssystem sowie zum Betrieb der elektrischen Netze. Eine Sicherung der für Smart Metering Systeme verwendeten Infrastruktur ist sinnvoll, da sie entweder ein Eingangstor zu nachgelagerten Systemen oder durch direkte Manipulation eine Gefahr für den stabilen Netzbetrieb bilden können. Ihre Abgrenzbarkeit von weiteren Systemen des EVU ermöglicht jedoch eine weitgehend isolierte Betrachtung. Inwiefern Gefährdungen und somit Risiken für das Stromversorgungsystem durch den Einsatz von Smart Metering bestehen, muss vorab eine Schutzbedarfsanalyse zeigen. Diese Schutzbedarfsanalyse sollte von einer neutralen Entität – vorzugsweise der Bundesverwaltung – vorgängig zu etwaigen Arbeiten hinsichtlich der Definition von sicherheitstechnischen Anforderungen erstellt werden. Ist sie erstellt, gilt es, die intelligenten Messsysteme derart abzusichern, dass die identifizierten Risiken wesentlich reduziert werden. Dabei sollte jedoch der Aufwand für die technische Sicherung und für die Validierung der wirksamen Sicherung nicht unverhältnismässig werden.

Die Schutzbedarfsanalyse ist nachgängig zu der vorliegenden Studie zu erstellen, welche an dieser Stelle vielmehr davon ausgeht, dass Gefährdungen grundsätzlich bestehen und die Systeme daher zu sichern sind. Die vorliegende Studie betrachtet daher die grundsätzlich möglichen Ansätze für eine Sicherung der Infrastruktur. Diese Ansätze werden durch die Ausgestaltung der Freiheitsgrade „Validierungsschemata“ und „Anforderungstiefe“ bestimmt. Die Ansätze weisen jeweils Stärken und Schwächen auf, die für 4 ausgewählte sinnvolle Ansätze untersucht werden, um einen Lösungsweg für die Schweiz aufzuzeigen.

Die Analyse der 4 ausgewählten Ansätze zur Sicherstellung eines vertrauenswürdigen Betriebs der intelligenten Messsysteme zeigt im Wesentlichen, dass eine Validierung der Implementierung von Sicherheitsfunktionalitäten von intelligente Messsystemen, welche die im Vorfeld definierten Sicherheitsanforderungen erfüllen, sinnvoll und erstrebenswert ist. Die Validierung sollte die folgenden wichtigen Punkte beinhalten:

- IKT-Sicherheitsanforderungen für intelligente Messsysteme in der Schweiz werden übergreifend gefordert, feingranular spezifiziert und sind einheitlich.
- Die IKT-Sicherheitsanforderungen werden für einzelne Komponenten – d. h. auch Prüfgegenständen – der intelligenten Messsysteme festgelegt. Die Abgrenzung der Komponenten und die Anforderungen an sie müssen die Sicherheit des Gesamtsystems gewährleisten.
- Eine Prüfung der Implementierung der geforderten IKT-Sicherheitsfunktionalitäten pro Prüfgegenstand ist sinnvoll.

- Die Prüfung der Prüfgegenstände erfolgt gemäss im Vorfeld erarbeiteter Prüfschemata, die auf die IKT-Sicherheitsanforderungen und auf die Prüfgegenstände zugeschnitten sind.
- Die Prüfschemata gewährleisten die Nachweise der Korrektheit und Wirksamkeit der Funktionalitäten. Zudem sichern sie die Reproduzierbarkeit der Prüfergebnisse und eine hohe Qualität der Prüfungen insgesamt.
- Die Prüfung der Anforderungen erfolgt durch akkreditierte Prüfstellen und dort durch fachlich qualifiziertes Personal. Detaillierte Dokumentationen der Prüfungen werden erstellt.
- Eine Kontrollstelle sichert und überwacht die Qualität des Validierungsprozesses und der Prüfstellen. Sie erteilt die Zulassung der Geräte nach bestandener Prüfung und kann Nachprüfungen im Betrieb verlangen bei Unregelmässigkeiten im Betrieb.

Der in diesem Bericht ausgewählte und ausgestaltete Lösungsansatz für eine Validierung (Variante 3 der insgesamt untersuchten 4 Varianten) setzt diese wichtigen Punkte gut um. Im gewählten Ansatz ist die nötige Flexibilität für die Ausgestaltung einer Schweiz spezifischen Lösung vorhanden wobei ein gleichbleibend hoher Schutz der kritischen Infrastruktur gewährleistet werden kann. Der gewählte Ansatz setzt auf ein Verfahren, das es erlaubt, Anforderungen, Prüfschemata und Prüfgegenständen individuell und für die nationalen Belange zu entwickeln und festzulegen. Er bietet so die Möglichkeit für subsidiär auszugestaltende, technische Lösungen, die den nötigen Pragmatismus aufweisen. Dadurch kann ein gutes bzw. sinnvolles Verhältnis zwischen zu treibenden Aufwand und erreichter Sicherheit erzielt werden. Dies ist in Abbildung 12 dargestellt, in der die 4 untersuchten Varianten (V1-V4) bezüglich des zur Realisierung nötigen Aufwandes (A) geordnet werden. Die Y-Achse stellt qualitativ das erreichte Sicherheitsniveau (S) dar. Sobald eine wie auch immer geartete Sicherung erfolgt ist ein gewisser Aufwand nötig. Der Aufwand für Variante 2 steigt im Vergleich zu Variante 1 marginal, doch auch der Zugewinn an Sicherheit ist marginal. Der zu treibende Aufwand für Variante 3 ist klar höher als der für die ersten beiden Varianten, jedoch bietet Variante 3 einen überproportionalen Gewinn an Sicherheit. Variante 4 bietet zwar insgesamt das höchste Sicherheitsniveau im Ergebnis, erscheint aber vom Aufwand her kaum tragbar.

Zu statuieren ist ferner, dass der favorisierte Ansatz nicht nur für intelligente Messsysteme beim Endverbraucher anwendbar ist, sondern sich auch auf andere IKT-Infrastrukturen bzw. auf andere Branchen übertragen lässt und somit zu hebende Synergien aufweist. Vor dem Hintergrund eines auch in anderen Bereich steigenden Sicherheitsbedarfs, kann aus einer übergeordneten Sicht, die über die Frage der Smart Metering Systeme im Energiebereich hinausgeht, die Variante 3 insgesamt als eine anpassungsfähige und schlanke Lösung bewertet werden. Klar ist, dass die zu prüfenden, technischen Anforderungen branchenspezifisch ausgelegt werden müssen. Vorteilhafterweise, erlaubt die Variante 3 genau dies.

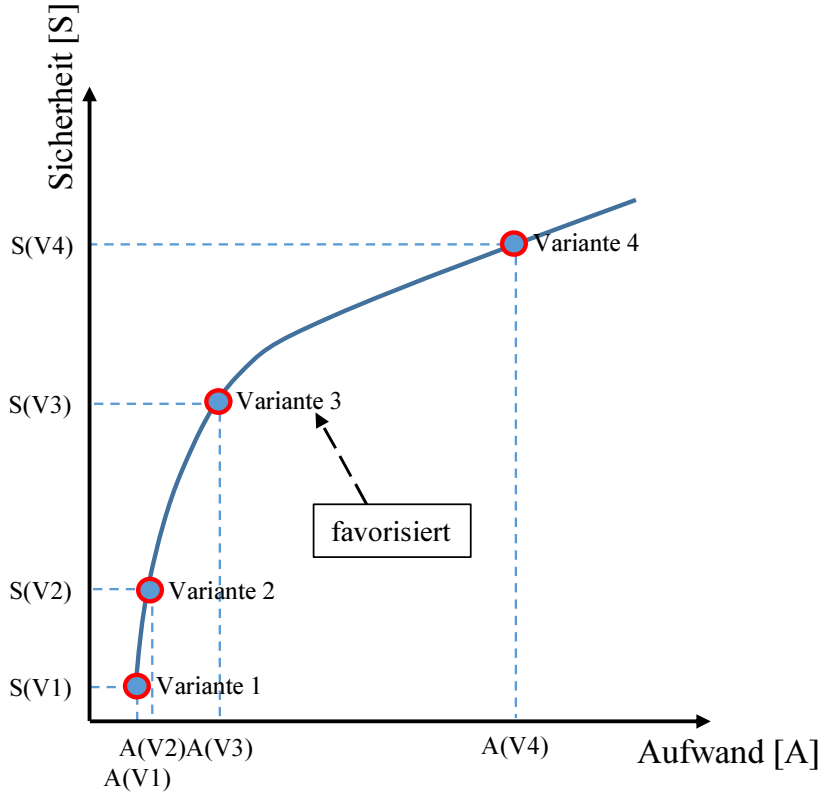

Abbildung 12: Mögliche Varianten zur Gewährleistung der IKT-Sicherheit und ihr Verhältnis von Aufwand zu erreichter Sicherheit. Qualitative Abbildung.

Der durch die Gutachter favorisierte Ansatz sieht Arbeitsgruppen aus unabhängigen IKT-Experten, Herstellern und Branchenvertreter auf subsidiärer Stufe vor, die gemeinsam Grundlagen erarbeiten für den Validierungsprozess erarbeiten. Subsidiär werden die Prüfgegenstände –also die Komponenten für die es Anforderungen zu definieren gilt – gegeneinander abgegrenzt, IKT-Sicherheitsanforderungen an diese Komponenten definiert, die wiederrum das gesamte Messsystem gegen die in der Schutzbedarfsanalyse festgestellten Gefährdungen härten, Letztlich werden auch geeignete Prüfschemata für die Anforderungen erarbeitet. Die Prüfschemata geben das konkrete Vorgehen zur Überprüfung der Konformität, der Vollständigkeit und der Wirksamkeit der IKT-Sicherheitsfunktionalitäten hinsichtlich der Anforderungen vor. Der Bund ist kaum vertieft involviert. Er fordert eine Sicherung der intelligenten Messsysteme nach Stand der Technik und eine Prüfung der Anforderungen durch unabhängige, akkreditierte Prüfstellen. Der Bund sorgt über eine Kontrollstelle für eine gleichbleibend hohe Qualität der eingeführten intelligenten Messsysteme, indem die Kontrollstelle die Prüfstellen beaufsichtigt, die Prüfergebnisse sichtet und bei zufriedenstellenden Ergebnissen eine Zulassungsermächtigung erteilt. Das hält den gesamten Prozess schlank, anwendungsnah und minimiert regulatorische Eingriffe.

6. Literaturverzeichnis

[1] CEN, CENELEC, ETSI. (2012). Smart Grid Coordination Group. First set of standards. Brüssel, Belgien.

[2] Verband Schweizerischer Elektrizitätsunternehmen (VSE). (2011). Branchenempfehlung Strommarkt Schweiz. ICT Continuitiy, Umsetzungsdokument zur Gewährleistung der ständigen Disponibiolität der Informatik- und der Kommunikationstechnologie zwecks Sicherstellung der Versorgung. Aarau, Schweiz.

[3] Bundesamt für Energie. (2015). Smart Grid Roadmap Schweiz. Wege in die Zukunft der elektrischen Netze. Bern, Schweiz. www.bfe.admin.ch/smartgrids.

[4] Bits to Energy Lab, Ecoplan AG, Weisskopf Partner GmbH, ENCO AG. (2012). Folgeabschätzung einer Einführung von Smart Metering“ im Zusammenhang mit „Smart Grids“ in der Schweiz. Studie im Auftrag des Bundesamtes für Energie. Bern, Schweiz. www.bfe.admin.ch/smartgrids.

[5] Bundesamt für Energie. (2013). Botschaft zum 1. Massnahmenpaket der Energiestrategie 2050.

[6] Bundesamt für Energie. (2014). Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz. Bern, Schweiz. www.bfe.admin.ch/smartgrids.

[7] AWK Group AG. (2014). Datensicherheit und Datenschutz für Smart Grids: offene Fragen und mögliche Lösungsansätze. Bern, Schweiz. www.bfe.admin.ch/smartgrids.

[8] Elektrizitätswirtschafts- und -organisationsgesetz (EIWOG). (2010). Wien, Österreich.

[9] E-Control. (2011). Intelligente Messgeräte-Anforderungsverordnung 2011 (IMA-VO 2011). Wien, Österreich.

[10] E-Control. (2012). Intelligente Messgeräte-Einführungsverordnung (IME-VO 2012). Wien, Österreich.

[11] E-Control. (2012). Änderung der Datenformat- und Verbrauchsinformationsdarstellungsverordnung (DAVID-VO 2012). Wien, Österreich.

[12] Österreichs Energie, Infraprotect, APG, TLP-White, E-Control, Bundeskanzleramt Österreich, bmwfw, BMI, Repucco. (2014). Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft unter besonderer Berücksichtigung von Smart-Metern und des Datenschutzes. Wien, Österreich.

[13] European Network for Cyber Security. (2014). Anforderungskatalog Ende-zu-Ende Sicherheit Smart Metering. Studie im Auftrag der Österreich Energie, Wien, Österreich.

[14] National Institute of Standards and Technology (NIST). NIST Interagency Report 7628, Guidelines for Smart Grid Cybersecurity. USA. http://csrc.nist.gov

[15] CEN, CENELEC, ETSI (2011). Technische Richtlinie 50572. Funktionale Referenzarchitektur für die Kommunikation in intelligenten Messsystemen. Brüssel, Belgien.

[16] Energiewirtschaftsgesetz (EnWG). (2007). Berlin, Deutschland.

[17] Bundesministerium für Wirtschaft und Energie (BMWi). (2015). Baustein für die Energiewende: 7 Eckpunkte für das „Verordnungspaket intelligente Netze“. Berlin, Deutschland. http://www.bmwi.de/DE/Themen/energie,did=695704.html

[18] Bundesministerium für Wirtschaft und Energie (BMWi). (2015). Referentenentwurf für ein "Gesetz zur Digitalisierung der Energiewende". Berlin, Deutschland. http://www.bmwi.de/DE/Themen/energie,did=726276.html

[19] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2014). Common Criteria Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP). BSI-CC-PP-0073-2014. Berlin, Deutschland. https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html

[20] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2014). Common Criteria Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP). BSI-CC-PP-0077-2014. Berlin, Deutschland. https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html

[21] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2013). Technische Richtlinie BSI TR-03109. Berlin, Deutschland. https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html

[22] Bundesnetzagentur (BNetzA). (2015). IT-Sicherheitskatalog gemäss §11 Absatz 1a Energiewirtschaftsgesetz. Bonn, Deutschland. http://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit.html

[23] DIN ISO/IEC 27001:2008-09. (2008). Informationstechnik – IT- Sicherheitsverfahren – Informationsmanagementsysteme – Anforderungen (ISO/IEC 27001:2005). Berlin: Beuth Verlag, Deutschland.

[24] DIN ISO/IEC 27000:2011-07. (2011). Informationstechnik – IT- Sicherheitsverfahren – Informationsmanagementsysteme – Überblick und Terminologie (ISO/IEC 27000:2009). Berlin: Beuth Verlag, Deutschland.

[25] US Department of Energy (DOE). (2014). Smart Grid System Report. Report to Congress. Washington, DC, USA. http://energy.gov/sites/prod/files/2014/08/f18/SmartGrid-SystemReport2014.pdf.

[26] National Electrical Manufacturers Association (NEMA). NEMA SG-AMI 1-2009, Requirements for Smart Meter Upgradeability. USA. http://www.nema.org

[27] Department of Energy (DOE), Office of Electricity Delivery & Energy Reliability. Cybersecurity Risk Management Process (RMP). USA. http://energy.gov

[28] International Electrotechnical Commission (IEC). 62351: Power Systems Management and Associated Information Exchange. http://www.iec.ch/smartgrid/standards/

[29] International Society for Pharmaceutical Engineering (ISPE). Good Automated Manufacturing Practice (GAMP). http://www.ispe.org

[30] European Network and Information Security Agency (ENISA). (2014). Smart grid security certification in Europe – Challenges and recommendations. https://www.enisa.europa.eu/

[31] International Organization for Standardization (ISO). ISO/IEC 17000:2004.Conformity assessment – vocabulary and general principles. http://www.iso.org

[32] International Organization for Standardization (ISO). ISO/IEC 17025:2005. General requirements for the competence of testing and calibration laboratories. http://www.iso.org.

[33] International Organization for Standardization (ISO). ISO/IEC 15408-1:2009. Information technology – security techniques – evaluation criteria for IT security – part 1: Introduction and general model. http://www.iso.org.

[34] International Organization for Standardization (ISO). ISO/IEC 15408-2:2008. Information technology – security techniques – evaluation criteria for IT security – part 2: security functional requirements. http://www.iso.org.

[35] International Organization for Standardization (ISO). ISO/IEC 15408-3:2008. Information technology – security techniques – evaluation criterie for IT security – part 3: Security assurance components. http://www.iso.org.

[36] Schweizerisches Staatssekretariat für Wirtschaft (SECO). Schweizerische Akkreditierungsstelle (SAS). Regelungen für die Akkreditierung. Dokument Nr. 741.dw. http://www.seco.admin.ch/sas/00032/02632/index.html?lang=de.

[37] International Organization for Standardization (ISO). ISO/IEC 17065:2012. Conformity assessment – requirements for bodies certifying products, processes and services. http://www.iso.org

[38] The common criteria for information technology security evaluation. https://www.commoncriteriaportal.org/

7. Glossar

Anforderungskatalog Dokument (wie z.B. die *Sicherheitsanforderungen für Smart Meter* von Oesterreichs energie) erstellt unter Mitwirkung der Betreiberbranche und der Kontrollstelle etc. Es spezifiziert die Prüfgegenstände und die ITK-Sicherheitsanforderungen an diese, sowie die von einer Prüfstelle durchzuführenden Untersuchungen. Es wird redaktionell gepflegt von der Kontrollstelle

Assurance Class(es) Dies ist ein Fachterminus der Common Criteria. Er umfasst zu dokumentierende Prüfaspekte bzgl. Sicherheit in Entwicklung, Benutzer- und Administratorendokumentationen, Produktlebenszyklus, Evaluation Sicherheitsvorgaben, Tests sowie einer Analyse etwaiger Schwachstellen.

Benutzerdokumente Dies ist eine Dokumentation des Herstellers bzgl. des Betriebs des Produkts und umfasst Benutzerhandbuch, Administratorenhandbuch u.s.w.

Datensicherheit Datensicherheit hat das technische Ziel, Daten jeglicher Art in ausreichendem Maße gegen Verlust, Manipulationen und andere Bedrohungen zu sichern. Der Begriff bezieht sich auf die technische Umsetzung der IKT-Sicherheit. Hierunter versteht man die Gewährleistung der Vertraulichkeit (nur autorisierte Benutzer haben Zugang zu übertragenen und gespeicherten Daten), der Integrität (Schutz vor beabsichtigten oder unbeabsichtigten Veränderungen), der Verfügbarkeit (Gewährleistung des ständigen Zugriffs auf die Daten) und der Kontrollierbarkeit (Prüfung der Maßnahmen durch Protokollierung). Datensicherheit hat also zum Ziel, beliebige Daten vor Schäden wie Manipulation und Nicht-Verfügbarkeit schützen. Hierzu zählen unter anderem Aspekte wie die physische Sicherheit, der Schutz vor Fremdzugriffen, der Schutz vor internen Zugriffen, die Verschlüsselung der Kommunikation, die Datensicherung wie auch Updates und Patches.

Gefährdung Als Gefährdung wird eine konkrete Gefahr bezeichnet, die für ein konkretes Schutzgut besteht. Die Gefährdung entspricht daher einem potentiellen Ereignis oder einer potentiellen Entwicklung mit möglichen Auswirkungen für ein Schutzgut. In manchen Themen wird verschiedentlich für Gefährdung auch der Begriff Bedrohung gebraucht.

Herstellerdokumente Dies ist eine produktbezogene Dokumentation des Herstellers bezüglich Prüfschema (für Prüfer) sowie des Betriebs des Produkts (für Prüfer sowie Anwender).

Intelligentes Messsystem	Ein intelligentes Messsystem ist eine in ein Kommunikationsnetz eingebundene Messeinrichtung zur Erfassung des Verbrauchs elektrischer Energie beim Endkunden oder der Produktion dieser beim Produzenten, wobei der tatsächliche Energiefluss elektrischer Energie, die tatsächliche Nutzungszeit und weitere Grössen erfasst werden. Zum intelligenten Messsystem gehört ein intelligentes Messgerät, eine bidirektionale Kommunikationsschnittstelle, die innerhalb oder ausserhalb des intelligenten Messgerätes angesiedelt sein kann, ein Kommunikationssystem sowie ein Zählerdatenverarbeitungssystem. Die Werte, die das Messgerät aufnimmt, werden über die bidirektionale Anbindung des Messgerätes an das Zählerdatenverarbeitungssystem gesendet. Letzteres gibt es in unterschiedlichen Ausprägungen, welche abhängig von den Funktionalitäten des Gesamtsystems sowie der Anzahl angebundener, intelligenter Messgeräte sind. Als Synonym soll auch der Ausdruck „Smart Metering Systeme“ gelten.
Intelligentes Messgerät	Intelligente Messgeräte erfassen den tatsächlichen Energiefluss elektrischer Energie und die tatsächliche Nutzungszeit. Sie zeigen diese Werte an, speichern sie, oder verbreiten diese bidirektional über das Kommunikationsnetz, dem sie angeschlossen sind. Sie sind ein Teil des intelligenten Messsystems. Als Synonym soll auch der Ausdruck „intelligente Zähler“ gelten.
IKT-Sicherheit	Bei der IKT stehen die technische Verarbeitung und Übertragung von Informationen im Vordergrund. Die IKT – Sicherheit umfasst somit Eigenschaften eines funktionierenden IKT-Systems, die verhindern sollen, dass nicht-autorisierte Datenmanipulationen möglich sind oder die Preisgabe von Informationen stattfindet. Der Einbezug der Kommunikationstechnologie bedeutet in diesem Zusammenhang, dass der Kommunikationsweg ebenfalls Eigenschaften zur Sicherung aufweist. Hier soll IKT-sicherheit synonym zu IT-Sicherheit verwendet werden.
Konformitätsprüfung	Ist ein Nachweis durch eine unabhängige Stelle, dass vorab festgelegte Anforderungen bezogen auf einen Prozess, ein Produkt oder ein System durch die Implemtierung erfüllt sind.
Lastenheft	Dies ist eine Spezifikation auf Anforderungsebene (engl.: Requirements Specification) für Hersteller, Entwickler etc. Es kann z.B. vom Kunden erstellt werden.
Lebenszyklus Produkt	Gesamtheit der Prozessschritte von der Grobspezifikation des Produktes über Implementierung und Auslieferung, Inbetriebnahme und Betrieb.
Pflichtenheft	Dies ist Spezifikation auf Umsetzungsebene (engl.: Feature Specification) gemäss der die Hersteller, Entwickler etc. die Anforderungen des Lastenheftes umzusetzen gedenken.

Prüfbericht	Der Bericht ist eine umfassende, archivierbare Dokumentation der Prüfschritte die durchgeführt wurden, und der entsprechenden Prüfergebnisse. Er benennt explizit und identifizierbar die Version des Prüfgegenstands, die Version des Prüfschemas und Version des Anforderungskatalogs sowie das Datum der Prüfung des Lebenszyklus.
Prüfergebnis	Dies ist eine Aussage einer Prüfstelle darüber, ob für einen in Prüfgegenstand die spezifizierten IKT-Sicherheitsanforderungen vollständig und wirksam erfüllt sind und ob im Lebenszyklus prozedurale Sicherheitslücken existieren.
Prüfgegenstand	Funktionale Teilmenge eines Produkts, für die geeignete sicherheitstechnische Anforderungen sinnvoll gestellt und geprüft werden können. Ein Prüfgegenstand ist im Anforderungskatalog spezifiziert und wird von der Prüfstelle hinsichtlich der Umsetzung der Anforderungen zu untersuchen sein.
Prüfsiegel	Ein Prüfsiegel wird von der Prüfstelle herausgegeben und ist ein Nachweis, dass das Produkt die Prüfung erfolgreich durchlaufen hat.
Risikomanagement	Dieser Begriff umfasst sämtliche Massnahmen zur systematischen Erkennung, Analyse, Bewertung, Überwachung und Kontrolle von Risiken.
Schutzprofil	Dokument, das basierend auf einer Schutzbedarfsanalyse und Industriestandards angenommenen Gefährdung geeignete Sicherheitsfunktionen gegenüberstellt, so dass deren Korrektheit und Wirksamkeit geprüft werden kann. Die Funktionen basieren auf Standards sind aber detaillierter im Schutzprofil vorgegeben.
Sicherheitsfunktionalitäten	Dies sind definierte, informationstechnische Eigenschaften innerhalb eines Prüfgegenstands, um bestimmte Gefährdungen mit einer gewissen Widerstandsfähigkeit gegen Angriffe abzuwehren.
Validierung	Im Bereich der Produktqualitätssicherung wird darunter die formale Prüfung der Eignung des Produktes oder Systems verstanden, dass es die Anforderungen in der Praxis erfüllt also wirksam ist. Die Eignungsprüfung erfolgt auf Grundlage eines vorher aufgestellten Anforderungsprofils und kann sowohl technisch als auch personell geschehen. Eine Validierung geht weiter als eine Konformitätsprüfung, da hier auch Wirksamkeit geprüft wird.