STROM ± RESILIENZ

Bernd Hirschl, Astrid Aretz, Mark Bost
Mariela Tapia, Stefan Gößling-Reisemann,

Vulnerabilität und Resilienz des digitalen Stromsystems

Endbericht des Projekts „Strom-Resilienz“

Institut für ökologische Wirtschaftsforschung (IÖW)
und
Universität Bremen, Fachgebiet Resiliente Energiesysteme

gefördert durch das Bundesministerium für Bildung und Forschung (BMBF)
im Rahmen des Förderschwerpunkts „Innovations- und Technikanalyse“ (ITA)
FKZ 16 1677

Berlin | Bremen, 14. Juni 2018

i | ö | w INSTITUT FÜR ÖKOLOGISCHE WIRTSCHAFTSFORSCHUNG

Universität Bremen
RESILIENTE ENERGIESYSTEME

Impressum

Autor/innen:
Prof. Dr. Bernd Hirschl (IÖW),
Dr. Astrid Aretz (IÖW),
Mark Bost (IÖW),
Mariela Tapia (Uni Bremen),
Prof. Dr. Stefan Gößling-Reisemann
(Uni Bremen)

Projektleitung:
Institut für ökologische
Wirtschaftsforschung (IÖW)
Potsdamer Straße 105
10785 Berlin
Tel. +49 – 30 – 884 594-0
www.ioew.de
Federführung für die Kap. 3 und 6

In Kooperation mit:
Universität Bremen
Fachgebiet Resiliente Energiesysteme
Enrique-Schmidt-Str. 7
28359 Bremen
www.res.uni-bremen.de
Federführung für die Kap. 4 und 5

Zitiervorschlag
Hirschl B. et al. (2018): Vulnerabilität und Resilienz des digitalen Stromsystems. Schlussbericht. Berlin, Bremen, Download: www.strom-resilienz.de

Der vorliegende Bericht entspricht dem redaktionell überarbeiteten formalen Endbericht des Forschungsprojekts „IKT und Stromversorgung: Potenziale und Risiken der Kopplung in Bezug auf Vulnerabilität und Resilienz“ (kurz „Strom-Resilienz“). Das Projekt wurde durch das Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Förderschwerpunkts „Innovations- und Technikanalyse“ (ITA) über den Projektträger VDI/VDE Innovation + Technik GmbH gefördert. Für nähere Informationen zum Projekt: www.strom-resilienz.de .

Berlin, Bremen, Juni 2018

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Danksagung

Unseren herzlichen Dank richten wir an das Bundesministerium für Bildung und Forschung für die finanzielle Förderung der Forschungsarbeiten im Projekt Strom-Resilienz. Besonders bedanken wir uns auch bei den Interviewpartnern und bei den Teilnehmerinnen und Teilnehmer unserer Workshops und unserer Abschlusstagung in Berlin und Bremen für die wertvollen Kommentare, neuen Ideen und offenen Diskussionen.

Unser Dank gilt auch den Mitarbeiterinnen und Mitarbeiter beim Projektträger VDI/VDE Innovation + Technik GmbH, die mit Rat und Tat zur Seite standen, sowie der Wissenschaftlichen Koordination des Förderschwerpunkts „Innovations- und Technikanalyse“ (ITA).

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BDEW	Bundesverband der Energie- und Wasserwirtschaft e.V.
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team for Federal Agencies
DA	Data Access
DDoS	Distributed Denial of Service
DER	Distributed Energy Resources
DMS	Distribution Management System
DNP3	Distributed Network Protocol
DOS	Denial of Service
DSO	Distribution System Operator
EMS	Energy Management System
ENISA	European Network and Information Security Agency
EV	Electric Vehicle
GOOSE	Generic Object Oriented Substation Event
HAN	Home Area Network
HMI	Human Machine Interface
ICS	Industrial Control System
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IoT	Internet of Things
ISMS	Information Security Management System
IT	Information Technology

LMN	Local Metrological Network
MITM	Man-In-The-Middle
MSPC	Multivariate Statistical Process Control
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIDS	Network-Based Intrusion Detection System
NIST	National Institute of Standards and Technology
oK	Open Konsequenz
OPC	OLE for Process Control
OT	Operation Technology
PKI	Public Key Infrastructure
PP	Protection Profile
PV	Photovoltaik
RBAC	Role-Based Access Control
RTU	Remote Terminal Unit
SAIDI	System Average Interruption Duration Index
SCADA	Supervisory Control and Data Acquisition
SEP	Smart Energy Profile
SGAM	Smart Grid Architecture Model
SMGA	Smart Meter Gateway Administrator
SMGW	Smart Meter Gateway
TNC	Trusted Network Connect
VA	Vulnerability Assessment
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
WAN	Wide Area Network
ZLL	Zigbee Light Link

1 Einleitung und Problemstellung

Das heutige und noch mehr das zukünftige Leben und Wirtschaften beruht maßgeblich auf einer stabilen Stromversorgung. Von der Herstellung, Kühlung und Zubereitung von Lebensmitteln, über die Trinkwasserversorgung, das Gesundheitssystem, dem überwiegenden Teil aller Arbeitsplätze und Kommunikationssysteme bis hin zu sanitären Systemen wie der Toilettenspülung und Abwasserbehandlung sind praktisch alle Lebens- und Arbeitsbereiche von der Funktionsfähigkeit elektrischer und elektronischer Geräte und Systemkomponenten und somit von der Elektrizität abhängig. Damit bekommt die (weitgehend) störungsfreie Stromversorgung einen hohen Stellenwert. Die katastrophalen Folgen eines längeren großflächigen Stromausfalls wurden eindrücklich im TAB-Bericht „Was bei einem Blackout geschieht“ dargestellt (Petermann et al. 2011).

Vor dem Hintergrund solcher weitreichenden, katastrophalen und somit ökonomisch und sozial kaum tragbaren Folgen ist die Frage der Vulnerabilität und Resilienz des Stromversorgungssystems eine aus unserer Sicht zentrale, die in der gegenwärtigen Debatte der Transformation des Energie- und hier insbesondere des Stromsystems noch nicht hinreichende Beachtung findet. Sehr wohl wird der gemäß EnWG eingeforderte Tatbestand der Versorgungssicherheit thematisiert, u. a. bei der Frage der Harmonisierung des Ausbaus von Erneuerbaren Energien (EE) und Netzausbau oder der Forderung nach Kapazitätsmechanismen, um eine stabile Stromversorgung zu gewährleisten. Damit verbunden ist in der Regel die Schaffung von zusätzlicher Flexibilität im Energiesystem, um die Schwankungen der künftig das Energiesystem dominierenden dargebotsabhängigen und somit fluktuierenden EE aus Wind und Sonne ausgleichen zu können. Flexibilitätspotenziale werden dabei unter anderem in der Steuerung bzw. Abregelung von Stromerzeugungsanlagen, der Steuerung von Lasten im Rahmen von Demand-Response bzw. Demand-Side-Management (DSM), Energiespeichern unterschiedlicher Art und damit ggf. verbundenen Optionen zur Kopplung der Versorgungssysteme für Strom, Wärme, Gas sowie der Sektoren Mobilität und Industrie gesehen. All diese Maßnahmen erfordern in unterschiedlichem Maße die Einführung von Informations- und Kommunikationstechnik (IKT) in das Energiesystem, um diese bspw. über das Internet oder andere Kommunikationsinfrastrukturen zu vernetzen, was auch als „Smart Grid“ bezeichnet wird.

Die notwendige Vernetzung auf Kommunikations- und Steuerungsebene führt jedoch zu einer weiteren Dimension, welche in den bisherigen Debatten mit einem Fokus auf die Stabilität des Stromsystems „alter Prägung“ noch weitgehend unbeachtet blieb. Der ständige notwendige Ausgleich von Erzeugung und Verbrauch hat in einem von dezentralen und erneuerbaren Erzeugungseinheiten geprägten System einen per se erhöhten Koordinierungsbedarf zur Folge, der in der Smart Grid Variante über Kommunikations- und Steuerungssysteme auf unterschiedlichen Skalen gedeckt werden soll. Die zunehmende Einführung solcher Kommunikations- und Steuerungssysteme in das Energiesystem hat einerseits das Potenzial, die Stromversorgung resilienter zu machen, vor allem durch eine Erhöhung der Koordinationsfähigkeit und Reaktionsfähigkeit im Stromnetz, es erhöht aber gleichzeitig dessen Verwundbarkeit durch Fehler oder Ausfälle der IKT oder dessen Manipulation von außen. Es gilt also eine Balance zu schaffen zwischen Steuerbarkeit und Flexibilität einerseits und Eindämmung neuer Verwundbarkeiten andererseits.

Der Stromausfall von 2015 in der Ukraine war der erste öffentliche Zwischenfall im Energiesektor, der auf eine Cyber-Attacke zurückzuführen ist. Etwa 225.000 Verbraucherinnen und Verbraucher waren von dem mehrstündigen Ausfall betroffen. Der Vorfall macht zum einen die Verwundbarkeit durch IKT-Angriffe von außen deutlich, zum anderen zeigt er, dass komplexe Attacken dieser Art durchführbar sind (ICS-CERT 2016).

Auch in Deutschland wurde im Rahmen eines Sicherheitstests in einem Stadtwerk gezeigt, wie Hacker die Kontrolle über dieses und somit über die Strom-, Wasser- und Gasversorgung übernehmen können (Lindner 2014). Weitere Angriffsmöglichkeiten werden durch die zunehmende Verwendung „intelligenter" Stromzähler („Smart Meter") geschaffen. „Cyber-Angriffe auf die Infrastruktur sind zu einer Hauptsorge der Energiekonzerne […] geworden", konstatieren daher auch die Deutschen Mittelstands Nachrichten (DMN 2014). Nach Ansicht des Bundesamts für die Sicherheit in der Informationstechnik (BSI) ist die Sicherheit von industriellen Steuersystemen (ICS, engl. Industrial Control Systems) in vielen Bereichen bisher vernachlässigt worden. Zum Messen, Steuern und Regeln von Abläufen, beispielsweise zur Automation von Prozessen und zur Überwachung von großen Systemen, kommen in vielen Bereichen der Industrie ICS zum Einsatz. Diese finden häufig Verwendung in der produzierenden Industrie und in Branchen, die zu den kritischen Infrastrukturen (KRITIS) gezählt werden, z. B. Energie, Wasser, Ernährung oder Transport und Verkehr. Das BSI nennt dabei explizit Energie als eine der Kritischen Infrastrukturen, in denen solche Automatisierungssysteme zunehmend zum Einsatz kommen (BSI 2013a; Scherschel 2013).

Das BSI hat einen Leitfaden zur Absicherung von ICS veröffentlicht. Im Hinblick auf die immer deutlicher werdenden Defizite beim Schutz vieler dieser Systeme hat dieses Thema in jüngster Zeit besondere Brisanz gewonnen. Der Superwurm Stuxnet zeigte eindrucksvoll, wie wichtige Infrastruktur zum Ziel für Cyber-Angriffe wird, trotzdem melden Expertinnen und Experten immer wieder gravierende Sicherheitslücken in ICS-Software. Mit seinem 124-seitigen Papier wendet sich das BSI sowohl an IT-Fachpersonal, das mit den besonderen Problemen von industriellen Kontrollsystemen noch nicht vertraut ist, als auch an die Hersteller dieser Systeme. Es versucht, die möglichen Probleme einzugrenzen und bewährte Methoden zur Risikominderung aufzulisten. Nach Ansicht der Behörde ist die Sicherheit von Steuersystemen in vielen Betrieben in der Vergangenheit vernachlässigt worden, da diese Infrastruktur oft nicht an öffentliche Netze angebunden war. Mit dem Einzug von Computerhardware in alle Bereiche eines Betriebes und der damit einhergehenden Vernetzung ist die schützende "Air Gap"[1] aber nur noch in den wenigsten Fällen vorhanden. Und auch in Fällen, in denen kritische Hardware nicht direkt an das Internet angeschlossen ist, können Angreifer oft durch Spear Phishing andere Rechner in einer Firma übernehmen und als Brückenkopf benutzen. Sind sie erst einmal im internen Netz, kommen sie früher oder später meist auch an ihr Ziel. Eben aus diesem Grund muss die IT-Sicherheit eines Betriebes immer im Ganzen betrachtet werden, erklärt das BSI. Da ist es kein Zufall, dass das Amt ebenfalls in einem anderen Dokument dazu aufruft, alle Computer, die derzeit noch auf Windows XP laufen, schnellstmöglich auf neuere Windows-Versionen umzustellen.

Ausgangsthese des Vorhabens ist, dass die Vulnerabilität eines IKT-basierten „smarten" Energiesystems gegenüber Ausfällen der IKT-Infrastruktur oder Angriffen auf diese von außen bisher nicht ausreichend untersucht worden ist. Der Fokus liegt bisher auf klassischen Sicherheitskriterien der Energieversorgung, welche durch die zunehmende Vernetzung durch teils Internet-basierte Kommunikations- und Steuereinheiten um eine neue Dimension erweitert werden müssen. Daraus ergeben sich folgende Forschungsfragen, die im Rahmen des Projekts maßgeblich untersucht worden sind:

[1] Als Air Gap (englisch für „Luftspalt") wird in der Informatik ein Prozess bezeichnet, der zwei IT-Systeme voneinander physisch und logisch trennt, aber dennoch die Übertragung von Nutzdaten zulässt.

– Welche Eigenschaften, Strukturen und Elemente von Stromversorgungssystemen sind entscheidend für ihre Vulnerabilität und Resilienz?
– Welche Resilienz-Anforderungen (insbes. IKT-seitig) müssen an ein künftiges IKT- und EE-basiertes Stromversorgungssystem gestellt werden?
– Welche Stromversorgungssysteme können diese erfüllen; wie wichtig ist hierfür die Granularität des Systems?
– Welche Rahmenbedingungen sind für ein solches resilientes Energiesystem erforderlich und welche Akteure müssen mit einbezogen werden, so dass künftige Innovationen die notwendigen Anforderungen erfüllen?

2 Stand des Wissens

Für die Analyse der möglichen Optionen für die Ausgestaltung des Stromsystems wurde die vorhandene Literatur ausgewertet. Kurz vor Projektbeginn wurde die Studie *Der Zellulare Ansatz: Grundlage einer erfolgreichen, regionenübergreifenden Energiewende* von der Energietechnischen Gesellschaft im VDE (VDE ETG) veröffentlicht (VDE 2015), die für das Projekt eine wertvolle Grundlage für die Diskussion über die Granularität des Energiesystems war. Bei diesem Ansatz werden sogenannte Energiezellen gebildet, innerhalb derer Verbrauch und Erzeugung von Energie lokal ausbalanciert und damit der Austausch mit benachbarten Zellen und Regionen möglichst gering gehalten werden soll. Daneben liegen eine Reihe weiterer Studien vor, die sich mit unterschiedlichen Ausbaupfaden, insbesondere mit hohem Anteil erneuerbarer Energien beschäftigen (siehe z.B. Lüllmann (2015) oder Peter (2013)) und Ausbauoptionen hinsichtlich unterschiedlicher Granularität behandeln (siehe z.B. Breyer (2014) oder Bauknecht (2015)).

Relevante Studien zu Vulnerabilität und Gestaltungsprinzipien eines resilienten Systems wurden auch für die Entwicklung von AP 2 und AP 3 ausgewertet. Der für die Vulnerabilitätsanalyse verwendete methodische Ansatz basiert auf der von (Gößling-Reisemann et al. 2013; Brand et al. 2017; von Gleich et al. 2010) entwickelten Arbeit. Die Definition der Strategie zur Erhöhung der Resilienz von cyber-physikalischen Energiesystemen wurde auf dem bereits früher entwickelten Design von resilienten Energiesystemen (Acatech et al. 2017) und (Gößling-Reisemann 2016) aufgebaut. Darüber hinaus wurde eine Überprüfung der relevanten Literatur über Smart Grid Architekturmodelle und Cyber-Vulnerabilität in Smart Grids durchgeführt, um ein Verständnis der Systemkomplexität und -herausforderungen herbeizuführen sowie potenzielle Bedrohungen, Angriffsmechanismen und vorgeschlagene Abwehrmaßnahmen zu identifizieren, z.B. (NIST 2014; ENISA 2013; CEN-CENELEC-ETSI 2014; NESCOR 2015). Nähere Angaben zur verwendeten Literatur zur Entwicklung der beiden Arbeitspakete befinden sich in den entsprechenden Kapiteln dieses Berichts.

Daneben konnten in das Projekt Ergebnisse aus anderen Forschungsarbeiten einfließen, die sich mit der Vermeidung sowie den Phasen während eines und nach einem Blackout beschäftigen. Für die Vermeidung eines Blackouts wurde in dem vom Bundesministerium für Bildung und Forschung

(BMBF) geförderten Projekt *SIMKAS 3D* eine Anwendung entwickelt, mit der Krisen in Versorgungsinfrastrukturen frühzeitig erkannt und möglichst zeitnah bewältigt werden.[2]

Mit der Phase während eines Blackouts beschäftigt sich das vom Bundesministerium für Wirtschaft und Energie (BMWi) im Rahmen der Forschungsinitiative „Zukunftsfähige Stromnetze“ geförderte Vorhaben *LINDA*, in dem die Forscherinnen und Forscher ein auf mehrere Spannungsebenen im Verteilnetz skalierbares Konzept entwickeln, welches einen stabilen Inselnetzbetrieb ermöglichen soll. Bei lang anhaltenden Ausfällen sollen dezentrale, schwarzstartfähige Erzeugungsanlagen eine Notversorgung für kritische Infrastruktur in lokalen Inselnetzen sicherstellen.[3]

Für die Phase nach einem Blackout setzen verschiedene Projekte an und entwickeln Konzepte für den Netzwiederaufbau. So fördert das BMWi innerhalb der Forschungsinitiative „Zukunftsfähige Stromnetze“ im Projekt *Netz:Kraft* das Entwickeln neuer Lösungen für den Netzwiederaufbau, die die künftige Struktur mit einem hohen Anteil erneuerbarer Energien berücksichtigen.[4] Die in diesem Projekt entwickelten Lösungen können eingesetzt werden, wenn die Ursachen für den Blackout behoben sind und somit die Voraussetzungen für den Normalbetrieb wieder gegeben sind und der Netzwiederaufbau begonnen werden kann.

Auch im benachbarten Ausland laufen thematisch verwandte Forschungsvorhaben, deren Ergebnisse in die Projektarbeit eingeflossen sind, wie z.B. das im Rahmen des Österreichischen Sicherheitsforschungs-Förderprogramm „KIRAS“ durchgeführte Projekt *Blackoutprävention und -intervention* (Reichl et al. 2015).

[2] https://www.inter3.de/de/projekte/details/article/berliner-infrastruktur-besseres-krisenmanagement-durch-simulation-von-krisenszenarien.html

[3] https://www.lew-verteilnetz.de/media/6156/pilotprojekt-linda-flyer.pdf

[4] http://www.energiesystemtechnik.iwes.fraunhofer.de/content/dam/iwes-neu/energiesystemtechnik/de/Dokumente/Projekte/Netz_Kraft-Projektvorstellung-Forschungsfragen-Ziele-20151127.pdf

3 Energieszenarien, IKT-Optionen und Zusammenhänge

Bearbeitung und Texterstellung: IÖW

Zunächst wurden Studien zur möglichen Entwicklung des deutschen Energiesystems ausgewertet, wobei der Fokus einerseits auf Optionen der Informations- und Kommunikationstechnik (IKT) im Energiesystem und andererseits in Bezug auf die mögliche Granularität des Energiesystems lag. Der Begriff „Granularität“ ist in diesem Zusammenhang neu und nicht klar definiert. Im Rahmen des Projekts werden derzeit folgende Arbeitsdefinitionen des Begriffs im Energiesystem verwendet:

1. Größe des kleinsten Netzelements, das eine stabile Versorgung gewährleisten kann (je kleiner, desto größer die Granularität).
2. Größe des kleinsten zu stabilisierenden Netzelements beim Wiederaufbau (je kleiner, desto größer die Granularität).

Eine endgültige eindeutige Definition des Begriffs steht somit noch aus. Auch andere Definitionen sind nicht ausgeschlossen. Der Kerngedanke ist aber stets der gleiche, nämlich inwieweit das Energiesystem im Notfall in kleinere stabile Einheiten zerfallen und die Versorgung für einen Großteil der Bevölkerung aufrechterhalten kann. Das heutige Energiesystem weist bspw. noch eine recht geringe Granularität auf, da es von Großkraftwerken dominiert wird, welche die Netzstabilität und somit die Versorgungssicherheit gewährleisten, während die vielen dezentralen Erzeugungsanlagen dazu bisher kaum beitragen. Dies wird sich jedoch mit der Umsetzung der Energie- und Klimaschutzziele der Bundesregierung in den nächsten Jahrzehnten deutlich ändern, wobei auch bei einem von erneuerbaren Energien dominierten Energiesystem Szenarien mit hoher oder geringer Granularität denkbar sind. So würde bspw. ein Energiesystem, welches durch große Offshore-Windparks oder Desertec-Ansätze dominiert wird, eher eine geringe Granularität aufweisen.

Da die *Granularität* des Energiesystems bisher unter diesem Begriff nicht diskutiert wird, wurden vor allem Szenarien ausgewertet, welche den Zentralisierungsgrad des Energiesystems zum Gegenstand haben. Dies sind vor allem folgende Studien:

1. Bauknecht et al. (2015): Energiewende - Zentral oder dezentral? Diskussionspapier im Rahmen der Wissenschaftlichen Koordination des BMBF Förderprogramms: „Umwelt- und Gesellschaftsverträgliche Transformation des Energiesystems“.
2. Breyer et al. (2014): Vergleich und Optimierung von zentral und dezentral orientierten Ausbaupfaden zu einer Stromversorgung aus erneuerbaren Energien in Deutschland. Reiner Lemoine Institut (RLI) im Auftrag von Haleakala-Stiftung, 100 prozent erneuerbar stiftung und BVMW Bundesverband mittelständische Wirtschaft, 21. Januar 2014.
3. Grünwald (2014): Moderne Stromnetze als Schlüsselelement einer nachhaltigen Energieversorgung. Berlin: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), Dezember 2014.
4. Lüllmann (2015): Analyse der Vulnerabilität von Elektrizitätsversorgungssystemen mit unterschiedlich ausgeprägter Integration erneuerbarer Energien. Karlsruhe: Fraunhofer-Institut für System- und Innovationsforschung ISI, gefördert durch das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU).

5. Peter (2013): Modellierung einer vollständig auf erneuerbaren Energien basierenden Stromerzeugung im Jahr 2050 in autarken, dezentralen Strukturen. Im Auftrag des Umweltbundesamtes, 31. August 2013.
6. VDE (2015): Der Zellulare Ansatz: Grundlage einer erfolgreichen, regionenübergreifenden Energiewende. VDE-Studie. Frankfurt a. M.: VDE ETG (Energietechnische Gesellschaft im VDE).

Die IKT- bzw. Smart-Grid-Optionen im Energiesystem werden vor allem in folgenden Studien ausführlich diskutiert und dargestellt:

7. VKU (2012): Anpassungs- und Investitionserfordernisse der Informations- und Kommunikations-Technologie zur Entwicklung eines dezentralen Energiesystems (Smart Grid).
8. Appelrath et al. (2012): Future Energy Grid. Migrationspfade ins Internet der Energie. Acatech Studie.
9. VDE ITG (2014): VDE-Positionspapier: Smart Grid Security. Energieinformationsnetze und -systeme.
10. VDE ITG (2010): Energieinformationsnetze und -systeme. Bestandsaufnahme und Entwicklungstendenzen. Informationstechnische Gesellschaft im Verband der Elektrotechnik Elektronik Informationstechnik e.V.

3.1 Szenarien zur Granularität

Darüber hinaus wurden auch einige Meta-Analysen der Agentur für Erneuerbare Energien (AEE) sowie weitere Studien und Journal-Artikel berücksichtigt. Auf Basis dieser Literatur wurden drei **Szenarien zur Granularität** im Energiesystem entwickelt, welche sich bzgl. der Nomenklatur an den verschiedenen Studien im Auftrag des Umweltbundesamts orientieren, aber nicht mit diesen gleichzusetzen sind. Anhand dieser Szenarien sollen Vulnerabilitäts- und Resilienz-Untersuchungen in den folgenden AP durchgeführt werden:

1. **„Lokal-autarke Kleinzellen“ ➔ sehr hohe Granularität**
   - Quartiere, Industriebetriebe und Gewerbeparks können i. d. R. mit Einschränkungen lokal-autark betrieben werden (Normalbetrieb mit Netzanbindung; größtmöglicher Ausgleich innerhalb der Zellen)
2. **„Verbundnetz Plus“ ➔ mittlere Granularität**
   - Gliederung des europäischen Verbundnetzes in Zonen von etwa Bundeslandgröße (mit Stadt-Umland-Kopplung)
3. **„Internationales Verbundnetz“ ➔ geringe Granularität**
   - Bei Bedarf Zerfall in heutige Regelzonen

Diese Szenarien haben zunächst eine Reihe von Gemeinsamkeiten, welche sich aus den Energie- und Klimaschutzzielen der Bundesregierung ergeben:

- **Anteil erneuerbarer Energien (EE) an der Stromerzeugung:** 100 %
- **Erzeugungsmix** basiert überwiegend auf fluktuierenden EE (PV & Wind).

- **Netzausbau:** Erfüllung des (n-1)-Kriteriums angepasst an die jeweilige geografische Verteilung der Stromerzeugung.
- **Intersektorale Netzkopplung („Hybridnetze"):** Es wird generell von einer zunehmenden Kopplung der Netze für Elektrizität, Gas und Wärme ausgegangen, z. B. mittels Power-to-Gas, Power-to-Heat etc. Die räumliche und strukturelle Verteilung wird dabei entsprechend der Flexibilitätsverteilung angenommen.
- **Speicherbedarf:** Sehr unterschiedliche Annahmen möglich
  - In jedem Fall Technologie-Mix notwendig (unterschiedliche Kurz-/Mittel-/Langzeitspeicher).
  - Bedarf stark abhängig von erschließbarer Flexibilität (DSM), Austausch im EU-Stromverbund (alpine und skandinavische Pumpspeicher), Nutzung großer solarthermischer Kraftwerke mit Speicher (CSP), Netzausbau.
  - Tendenziell kann man für dezentralere Szenarien einen höheren Speicherbedarf annehmen, der jedoch sehr vom geforderten Autarkiegrad abhängt.

Tab. 3.1 zeigt die Unterschiede der drei Szenarien.

Tab. 3.1: Charakterisierung von Szenarien zur Granularität des Energiesystems

Szenario / Merkmal	Zellularer Ansatz	Regionenverbund	International Großtechnik
Granularität	Hoch	Mittel	Gering
Räumliche Verteilung	Dezentral entsprechend Nachfrage	Dezentral	Zentral
Anteil Offshore-Wind an gesamter Windenergie	10 %	20–40 %	50–80 %
Flexibilität	überwiegend auf Verteilnetzebene	überwiegend auf Verteilnetzebene	überwiegend auf Übertragungsnetzebene
Steuerung	dezentral (z. B. dezentrale Märkte/ VNB)	Mischung zentraler und dezentraler Steuerung	zentral (z. B. über Spotmarktpreis)

3.2 Optionen zu IKT-Aspekten

Unabhängig von diesen Szenarien bezüglich der Granularität kann das Energiesystem auch durch unterschiedliche Merkmale in Bezug auf die verwendete Informations- und Kommunikationstechnik (IKT) und weitere Aspekte charakterisiert werden. Im Bereich IKT sind das vor allem die folgenden Aspekte:

1. **IKT-Durchdringung:** Die Durchdringung bei Erzeugern und Verbrauchern kann sehr unterschiedlich sein. Insbesondere kleinere Erzeuger und Verbraucher könnten im Rahmen von Bagatellgrenzen von einer flächendeckenden Steuerung ausgenommen sein. Damit hat insbes. die Durchdringung mit Smart Metern mit Steuerungsfunktion maßgeblichen Einfluss darauf, wie

groß die kleinsten steuerbaren Einheiten sind und wie viel Flexibilität durch diese auf Verteilnetzebene erschlossen werden kann.

  – Bei ausreichender EE-Leistung können auch fluktuierende Erneuerbare stärker bedarfsorientiert gefahren werden, indem z. B. Windparks im Normalbetrieb leicht gedrosselt laufen, sodass sie auch zusätzlich entstehenden Strombedarf decken können.

2. **Smart-Meter-Funktionen:** Unterschiedliche Funktionen möglich:

  – Messung und Abrechnung, um insbes. variable Tarifmodelle zu ermöglichen und so Flexibilität zu erschließen.

  – Fernschaltfunktionen zur Steuerung ausgewählter Verbrauchsgeräte wie Wärmepumpen, Nachtspeicherheizungen, Klimageräte, Spül-/Waschmaschinen etc., um in Verbindung mit variablen Tarifmodellen Flexibilität automatisiert zu erschließen.

3. **Datenaustausch:** Verbrauchs- und Erzeugungsdaten (sowie darauf basierende Prognosen) können entweder in zeitlich und räumlich hoch aufgelöster Form von der Stelle der Erhebung (z. B. Smart Meter) bis auf das nationale Niveau hinauf weitergegeben werden oder am Ort der Erhebung verbleiben und nur aggregierte Daten an die nächsthöhere Ebene weitergeben. Für Deutschland ist derzeit letzteres vorgesehen mit der Option, die feingranularen Daten auch an einen Dienstleister zum Zwecke der Auswertung und Visualisierung weiterleiten zu können.

4. **Daten- & Service-Verteilung:** Derzeit gibt es einen Trend, Daten und Services zunehmend in das Internet zu verlagern („Cloud“-Services). Dies hat den Vorteil, dass sie sich energie- und ressourceneffizient betreiben und administrieren lassen. Dienste und Sicherheitskonzepte mit hohem Schutzniveau können zentral einer großen Anzahl von Nutzerinnen und Nutzern zur Verfügung gestellt werden. Gegenüber dezentral beim Anwender betriebenen Konzepten muss sich der Anwender nicht mit der Durchführung von Aktualisierungen, Backups oder Sicherheitskonzepten beschäftigen. Dieser Komfortgewinn wird jedoch mit einer hohen langfristigen Abhängigkeit gegenüber dem Dienstanbieter erkauft. Gleichzeitig stellen solche Clouds mit einer Vielzahl angeschlossener Nutzerinnen und Nutzer ein sehr viel attraktiveres Ziel für Hacker aus unterschiedlichsten Kreisen dar, als eine Vielzahl von Einzelzielen.

5. **Virtuelle Kraftwerke (VK):** Heute dienen VK vor allem zur Bereitstellung von Regelenergie auf den nationalen Märkten und werden meist zentral durch deutschlandweit tätige Dienstleister im Auftrag der jeweiligen Betreiber gesteuert. Es gibt aber auch regionale Steuerungsansätze. Bei starker Durchdringung auf Niederspannungs-Ebene könnten sie perspektivisch zum Abgleich von Verbrauch und Erzeugung in lokalen Microgrids/Energiezellen dienen. Appelrath et al. (2012) sieht eine Entwicklung in fünf Schritten:

  a. VK-Systeme in **Fahrpläne** aufnehmen und diese abfahren, unter heranziehen von Schnittstellen der Fernwirktechnik.

  b. Komponentennutzung zum Einsatz vieler kleiner, heterogener Anlagen als Teil des VK, die den Fahrplan beachten und auf Abweichungen in Echtzeit reagieren.

  c. Netzberechnungen sind in die Fahrpläne integrierbar. **VK dienen zur Netzabschnittoptimierung und agieren als „Autonome Netzagenten“** vornehmlich im **Niederspannungsbereich**. Daten aus Messeinrichtungen und Messumformern können zu Prognosen genutzt werden, um auf die Erzeugungsanlagen einzuwirken. Das VK kann nun für einen Netzabschnitt Steuersignale berechnen, um Anlagen nach einem Fahrplan zum eingrenzenden Netz nutzbar zu machen.

d. VK-Systeme **können horizontal mit anderen VK-System gekoppelt** werden. VK-Systeme sind somit **nicht mehr eine „zentrale Lösung", sondern die Steuerungsintelligenz ist fortan über mehrere Systeme** verteilt.

e. Von nun an können **Geschehnisse im Netz selbst organisiert** betrieben werden und die Konvergenz von IKT und elektrischem System ist vollständig erfolgt. Intelligenz ist vollständig **dezentralisierbar**.

6. **Pluralität der Hersteller und technischen Lösungen:** Im Rahmen des ersten Workshops wurde bemängelt, dass aufgrund mangelnder Pluralität von Herstellern und Lösungen sich am Markt häufig Lösungen durchsetzen, welche die Anforderungen nicht optimal erfüllen. Anspruchsvolle Standards verbunden mit strengen Kontrollen und einer hohen Pluralität an Herstellern und Lösungen könnten diese Situation verbessern, sofern bei Netz- und Anlagenbetreibern sowie Dienstleistern ein entsprechend hohes Kompetenzniveau vorhanden ist.

7. **Sicherheitsniveau technischer Standards:**

   – Technisch (Inselnetzfähigkeit, Schwarzfall- und Schwarzstartfähigkeit von DEA und IKT, Auswahl der Kommunikationsnetze, Verschlüsselung, Sicherung gegen Defekte, Redundanzen, …)

   – Organisatorisch (Prüfung auf Fehler und Einhaltung von Standards, Umgang mit Defekten, Update-Versorgung, Zugangssicherung, Schnittstellendokumentation, Datenschutz, …)

   – **Integration und Sicherheit mobiler Endgeräte:** Es gibt insbes. im Smart-Home-Bereich einen zunehmenden Trend, Verbrauchsgeräte wie Heizung, Klimatisierung, Beleuchtung etc. zentral zu steuern, was meist auch die Möglichkeit eines Fernzugriffs via Internet mit PC oder Smartphone umfasst. Smartphones gelten aber derzeit als am schlechtesten abgesicherte IT-Systeme, u. a. weil das System mit dem größten Marktanteil, Android, bisher über keine Update-Automatik zum Schließen kritischer Sicherheitslücken verfügt. Sie gelten als attraktive und leichte Ziele für Hacker. Hackern könnte so perspektivisch eine sehr einfache Hintertür offenstehen, um durch die Kontrolle vieler Smartphones auch Kontrolle über signifikante Lasten im Energiesystem zu erlangen. Für ein hohes Integrations-Niveau sollte auch das Sicherheitsniveau entsprechend hoch sein.

Tab. 3.2 zeigt eine Übersicht der beschriebenen IKT-Optionen, die weitgehend unabhängig voneinander mit den Szenarien zur Granularität kombinierbar sind.

Tab. 3.2: Optionen zu IKT-Aspekten
(Alle Merkmale weitgehend unabhängig voneinander mit Szenarien zur Granularität kombinierbar.)

Option / Merkmal	A	B	C
IKT-Durchdringung bei Erzeugern	Alle Erzeuger	Alle mit Ausnahme von Kleinanlagen	Große Erzeuger
IKT-Durchdringung bei Verbrauchern	Alle Verbraucher	Alle mit Ausnahme von Kleinverbrauchern	Große Verbraucher
Smart-Meter-Funktionen	Alle mit voller Steuerungsfunktion	50 % Durchdringung mit Steuerungsfunktionen	Nur Messung und Abrechnung
Datenaustausch	Details nur in Zelle; nach außen nur aggregiert	Details nur im Verbund; nach außen aggregiert	Alle Details gehen bis zum ÜNB / (inter-) nationalen Regulator
Daten- & Service-Verteilung	Vollständig Cloud-basiert	Mix aus Cloud- und dezentralen Diensten	Vollständig dezentral
Virtuelle Kraftwerke	Regelung fokussiert auf Zelle; nationaler Austausch möglich	Regelung fokussiert auf Verbund; nationaler Austausch möglich	Regelung auf (inter-) nationaler Ebene
Pluralität der Hersteller und techn. Lösungen	Hoch	Mäßig	Gering
Sicherheitsniveau technischer Standards	Hoch	Mäßig	Gering

3.3 Weitere Aspekte zur Charakterisierung des künftigen Energiesystems

Neben den Aspekten Granularität und IKT können in Bezug auf Vulnerabilität und Resilienz weitere Merkmale zur Charakterisierung des Energiesystems von Bedeutung sein. Im Folgenden wird eine Auswahl dieser Merkmale kurz vorgestellt, ohne Anspruch auf Vollständigkeit zu erheben:

1. **Kompetenzniveau**: Derzeit gibt es in Deutschland über 800 teils sehr kleine Verteilnetzbetreiber (VNB). Vielen von diesen fehlt die für die Digitalisierung des Energiesystems und die damit verbundenen Herausforderungen bzgl. Cybersecurity notwendige Kompetenz. Daher müssen sich entweder kleinere VNB zusammenschließen und so eine Größe erreichen, für die sich der Aufbau der notwendigen Kompetenz in-house lohnt, oder sie müssen diese Kompetenz durch einen

Dienstleister erfüllen lassen. Ähnliches gilt laut den Teilnehmerinnen und Teilnehmern der Workshops auch bereits für die Kompetenz bzgl. der Wechselwirkungen zwischen Anlagen im Netz.

2. **Kontroll-Niveau**: Hohe technische Standards und Anforderung an die Kompetenz von Akteuren bringen wenig, wenn sie in der Praxis unzureichend eingehalten werden. Daher sind Mechanismen erforderlich, welche die Einhaltung dieser Standards sicherstellen. Vieles spricht dafür, dass das übliche Haftungsrecht hierfür unzureichend ist und häufige strenge Kontrollen eher geeignet sind, dieses Ziel sicherzustellen. Zusätzlich wären auch staatliche Organisationen denkbar, in denen Hacker beschäftigt werden, um die Sicherheit der kritischen Infrastrukturen zu testen und zu verbessern.
3. **Elektromobilität:** Fahrzeuge könnten künftig einen Großteil der steuerbaren Lasten im Verteilnetz ausmachen, wenn sie Verbrennungsmotoren tatsächlich weitgehend verdrängen sollten. In diesem Fall müssten die Fahrzeuge beim Laden zwangsläufig Angebot und Nachfrage sowie örtliche Netzparameter beim Laden berücksichtigen, um einen stabilen Netzbetrieb zu gewährleisten. Zusätzlich wäre auch eine Rückspeisung von den Fahrzeugen ins Netz denkbar. Entscheidend für die weitere Entwicklung der E-Mobilität ist vor allem die Entwicklung im Bereich der Batteriespeicher, wo erhebliche Kostenreduktionen notwendig sind.
4. **Anteil EE-Gas (H_2, Methan, …):** Eine Alternative zu Elektrofahrzeugen könnte der Betrieb mit EE-Gas sein, welches durch den Einsatz von erneuerbarem Strom gewonnen wird und sich sowohl in Verbrennungsmotoren als auch über Brennstoffzellen in Elektromotoren einsetzen lässt. Limitierend ist hier das Angebot von EE-Gas sowie einer entsprechenden Infrastruktur. Darüber hinaus lässt sich EE-Gas auch in anderen Verbrennungsprozessen zur Bereitstellung von Raum- und Prozesswärme sowie zur Rückverstromung im Stromsystem nutzen. Allerdings sind die Margen im Mobilitätsbereich potenziell am höchsten.

4 Verwundbarkeiten des Strom-IKT-Nexus

Bearbeitung und Texterstellung: Uni Bremen

Mit der zunehmenden Konvergenz der Informations- und Kommunikationstechnologien (IKT) hat sich das Energiesystem zu einem großen und komplexen cyberphysikalischen Energiesystem entwickelt. Dies bringt neben Chancen zur Steigerung der Leistungsfähigkeit und Effizienz auch Risiken in Bezug auf die Cybersicherheit mit sich.

Die Hauptziele der Arbeitspakete AP 2 und AP 3 sind die Ermittlung von Vulnerabilitäten, die durch die Digitalisierung von Energiesystemen entstehen können, sowie die Erarbeitung von Strategien, die dabei helfen, Energiesystemen so zu gestalten, dass die Systemleistungen auch unter Stress erhalten bleiben.

In einem ersten Schritt wurde eine Vulnerabilitätsanalyse (VA) durchgeführt, um kritische Punkte, Strukturen und Elemente zu identifizieren, die das System anfällig für Cyber-Angriffe machen. Um dies zu erreichen wurde ein interdisziplinärer Ansatz gewählt, bei dem Akteure des Energiesektors und IKT-Lösungsanbieter durch Interviews und Workshops einbezogen wurden.

Die Ergebnisse aus der VA wurden als Ausgangspunkt verwendet, um zu ermitteln, wie zukünftige cyberphysikalische Energiesysteme nicht nur aus bereits erwarteten, sondern auch aus unvorhersehbaren Störungen besser vorbereitet werden können.

4.1 Methodik

4.1.1 Vulnerabilitätsanalyse (VA)

Der ereignisbasierte VA-Ansatz, der bereits bei der Untersuchung der Klimaanfälligkeit der Energiesysteme in Nordwestdeutschland angewandt wurde (siehe dazu (Gößling-Reisemann et al. 2013; Brand et al. 2017; von Gleich et al. 2010)), wird als Grundlage für die Vulnerabilitätsanalyse verwendet. Der Ansatz berücksichtigt die Verwundbarkeit nicht nur als Funktion der Systemexposition, der Empfindlichkeit des Systems gegenüber externen/internen Störungen und der potenziellen Auswirkungen auf die Systemleistungen, sondern auch die Fähigkeit des Systems, diese zu bewältigen. Die sogenannte Anpassungsfähigkeit des Systems basiert auf bestehenden oder geplanten Anpassungsstrategien und der Bereitschaft der betroffenen Akteure, diese Maßnahmen umzusetzen. Eine schematische Darstellung der verwendeten VA-Methodik ist in Abb. 4.1 dargestellt.

Es ist erwähnenswert, dass im Bereich der IT-Sicherheit der Begriff "Schwachstelle" häufig eine Schwachstelle in einem Informationssystem, Systemsicherheitsverfahren, internen Kontrollen oder einer Implementierung bezeichnet, die von einer Gefahrenquelle ausgenutzt oder ausgelöst werden könnte (NIST 2014). Diese Definition unterscheidet sich von der in unserer VA-Methodik und stellt nur die Exposition des Systems gegenüber einer Störung dar, ohne die Anpassungskapazität zu berücksichtigen.

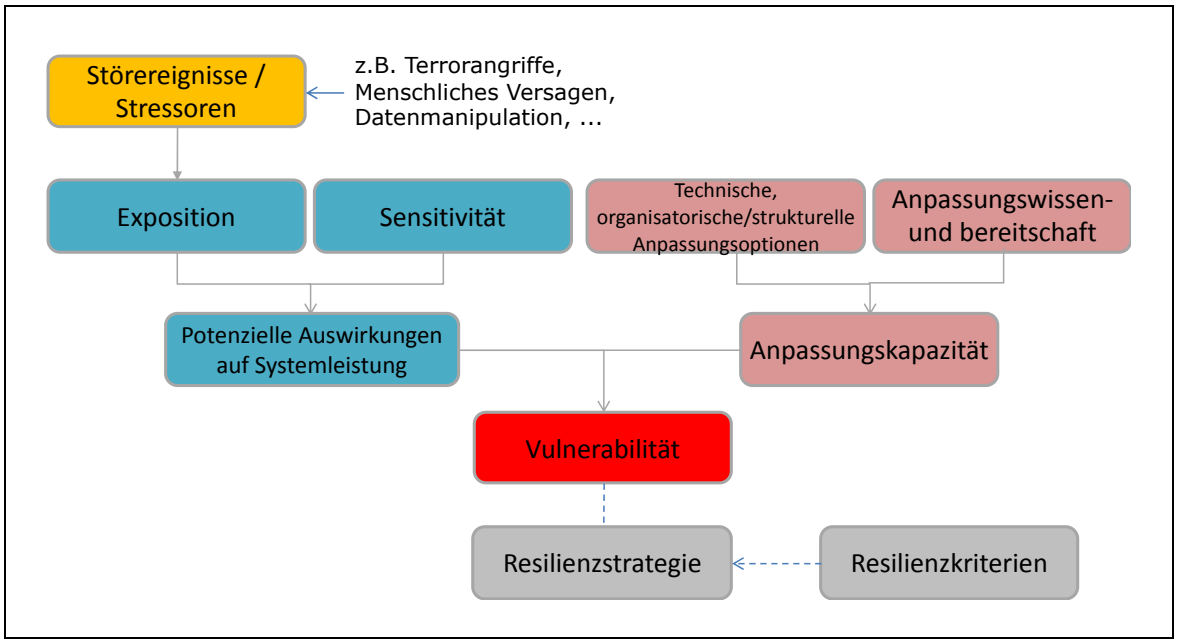

Abb. 4.1: Schematische Darstellung der Methodik der Vulnerabilitätsanalyse
Eigene Darstellung basierend auf (Gößling-Reisemann et al. 2013; Schuchardt et al. 2010; von Gleich et al. 2010)

Damit werden die potenziellen Auswirkungen von Störungen auf die Systemleistungen von Stromnetzen bewertet. Diese wurden nach spezifischen Parametern sowohl für die elektrische als auch für die IT-Infrastruktur definiert sind (siehe Tab. 4.1). Die quantitativen Kriterien der elektrischen Infrastruktur werden durch die Fähigkeit des Systems bestimmt, die Anschlussleistung aufrecht zu erhalten (Gößling-Reisemann et al. 2013). Die qualitativen Kriterien werden durch direkte technische Parameter definiert, bspw. Stromqualitäts- oder Zuverlässigkeitsindizes, und durch indirekte Parameter, bspw. wirtschaftliche Auswirkungen (z.B. Auswirkungen auf den Energiemarkt, Abrechnungsungenauigkeit) und soziale Auswirkungen (z.B. Gefährdung der Technologieakzeptanz oder Beeinträchtigung der Privatsphäre der Kunden).

Für die IT-Infrastruktur berücksichtigt der Ansatz die Auswirkungen auf die Sicherheitsanforderungen, d.h. Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit von Daten bei der Übertragung oder im Ruhezustand (z.B. Steuerbefehle, Konfigurationsdaten, Firmware, Software, Zählerdaten usw.). Im Folgenden werden die Sicherheitsanforderungen kurz beschrieben (Cleveland 2016):

– Vertraulichkeit - Verhinderung des unbefugten Zugriffs auf Informationen
– Integrität - Verhinderung der unbefugten Änderung oder des Diebstahls von Informationen
– Verfügbarkeit - Verhinderung von Denial-of-Service und Sicherstellung des autorisierten Zugriffs auf Informationen
– Nachweisbarkeit/Verantwortlichkeit - Verhinderung der Ablehnung einer Handlung, die stattgefunden hat, oder der Inanspruchnahme einer Handlung, die nicht stattgefunden hat.

Tab. 4.1: Definition von Kriterien für die Ermittlung der Systemleistungen des Stromsystems

<table>
<tr><th colspan="2">Systemleistungen des Stromsystems</th></tr>
<tr><td colspan="2">Quantitative Kriterien</td></tr>
<tr><td colspan="2">gesicherte Anschlussleistung und Energiemenge</td></tr>
<tr><td colspan="2">Qualitative Kriterien</td></tr>
<tr><td><u>Direkte technische Parameter</u>

• Netzqualität:
▪ Einhaltung der Bandbreite der Spannung (z.B. 400 V +/-10%)
▪ Einhaltung der Bandbreite der Frequenz (z.B. 50 +/- 0,2 Hz)

• Zuverlässigkeitsindizes (z.B. SAIDI (System Average Interruption Duration Index))</td><td><u>Indirekte Parameter</u>

• Umwelteinflüsse:
▪ CO_2-Emissionen
▪ Land / Ressourcennutzung
▪ Abfallerzeugung

• Wirtschaftliche Auswirkungen
• Kosten/Marktpreiseffekte
• Wettbewerbsfähigkeit

• Öffentliche Akzeptanz
• Privatsphäre des Kunden
• Technologie-Akzeptanz</td></tr>
<tr><th colspan="2">Informationsbestände</th></tr>
<tr><td>• Daten bei der Übertragung oder im Ruhezustand wie:
• Kunden-ID und Standortdaten
• Zählerdaten
• Steuerbefehle
• Konfigurationsdaten</td><td>• Uhrzeit, Uhrzeiteinstellungen
• Zugriffskontrollrichtlinien
• Firmware, Software und Treiber
• Tarifdaten
• …</td></tr>
<tr><td colspan="2">• Sicherheitsanforderungen</td></tr>
<tr><td>• Vertraulichkeit
• Integrität</td><td>• Verfügbarkeit
• Nachweisbarkeit</td></tr>
</table>

Die potenziellen Auswirkungen wurden auf Grundlage von Expertenbefragungen und einer Literaturrecherche den nachfolgenden Stufen zugeordnet:

– **hoch**, wenn die quantitativen Kriterien der Energieversorgung erheblich beeinträchtigt würden.

– **mittel**, wenn die quantitativen Kriterien nicht wesentlich beeinflusst würden, aber wenn die kompromittierte Sicherheitsanforderung eine direkte Auswirkung auf die quantitativen Kriterien

haben könnte, oder wenn mindestens einer der qualitativen Kriterienparameter wesentlich beeinflusst würde.

– **niedrig**, wenn weder die quantitativen noch die qualitativen Kriterien der Energieversorgung wesentlich beeinträchtigt würden oder wenn die kompromittierte Sicherheitsanforderung nur eine indirekte Auswirkung auf die qualitativen oder quantitativen Kriterien haben könnte.

In einem letzten Schritt wurde der Verwundbarkeitsgrad als Ergebnis der Kombination von potenziellen Auswirkungen und Anpassungsfähigkeit gemäß der in Abb. 4.2 dargestellten Logik ausgewertet.

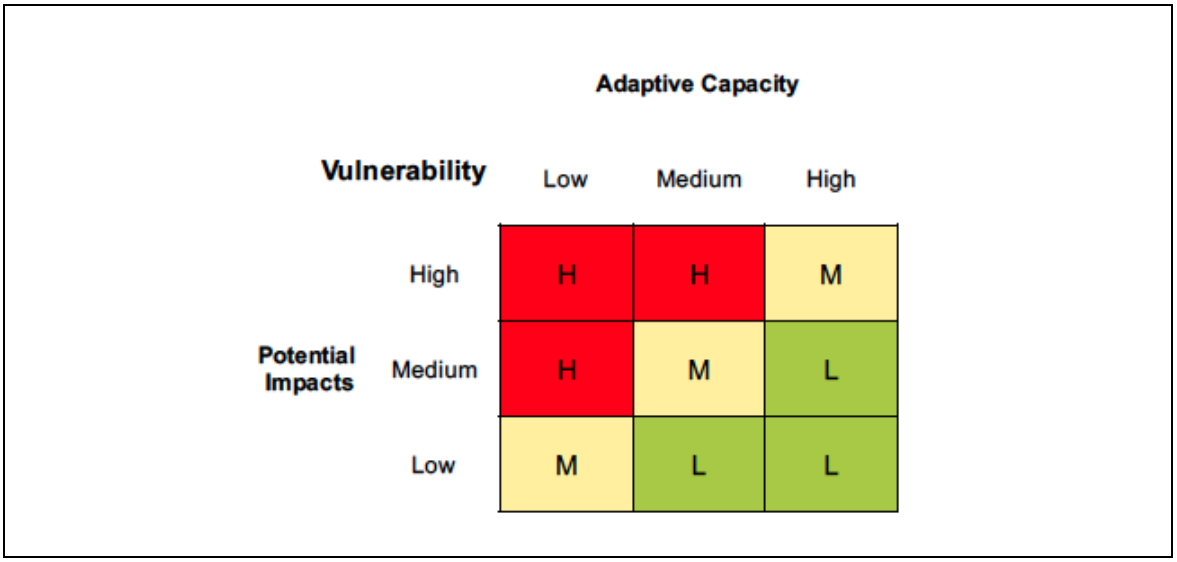

Abb. 4.2: Schema zur Ermittlung der Vulnerabilität (engl.: Vulnerability) aus potenziellen Auswirkungen (engl.: Potential Impacts) und der zugehörigen Anpassungskapazität (engl.: Adaptive Capacity)

Eine hohe Anpassungsfähigkeit neutralisiert bzw. mildert die potenziellen Auswirkungen in der Form ab, dass die Vulnerabilität eine Stufe unter der Einstufung der potenziellen Auswirkung liegt. Dies ist jedoch dann nicht der Fall, wenn die potenziellen Auswirkungen niedrig sind. Eine mittlere Anpassungsfähigkeit des Systems wirkt sich nicht in einer Stufenveränderung gegenüber der Einstufung durch die potenziellen Auswirkungen aus. Eine geringe Anpassungsfähigkeit erhöht die Anfälligkeit um eine Stufe über dem der potenziellen Wirkungsniveaus, basierend auf der Hypothese, dass unter diesen Umständen schwache Störfaktoren lange Zeit unbemerkt (und unbeantwortet) bleiben können, was zu akkumulierenden Auswirkungen auf den Systemdienst führt.

Die Maßnahmen zur Verbesserung der Anpassungsfähigkeit haben ein großes Potenzial nicht nur die Anfälligkeit zu verringern, sondern auch die Resilienz der Systeme zu erhöhen, daher wurden die Ergebnisse der Vulnerabilitätsanalyse als Ausgangspunkt für die Ermittlung der Resilienzstrategie herangezogen.

4.1.2 Referenzarchitekturmodell

Im Mittelpunkt dieser Studie stand das deutsche und europäische Stromnetz, das die gesamte elektrische Energieumwandlungskette abdeckt. Als Referenzarchitekturmodell wurde die Komponentenschicht des Smart Grid Architecture Model (SGAM) (CEN-CENELEC-ETSI 2014) der International Electrotechnical Commission (IEC) im Smart Grid Standards Mapping Tool (IEC 2016a) verwendet. Abb. 4.3 zeigt das für die VA verwendete Referenzarchitekturmodell und Abb. 4.4 zeigt eine vereinfachte Ansicht der SGMA-Ebene.

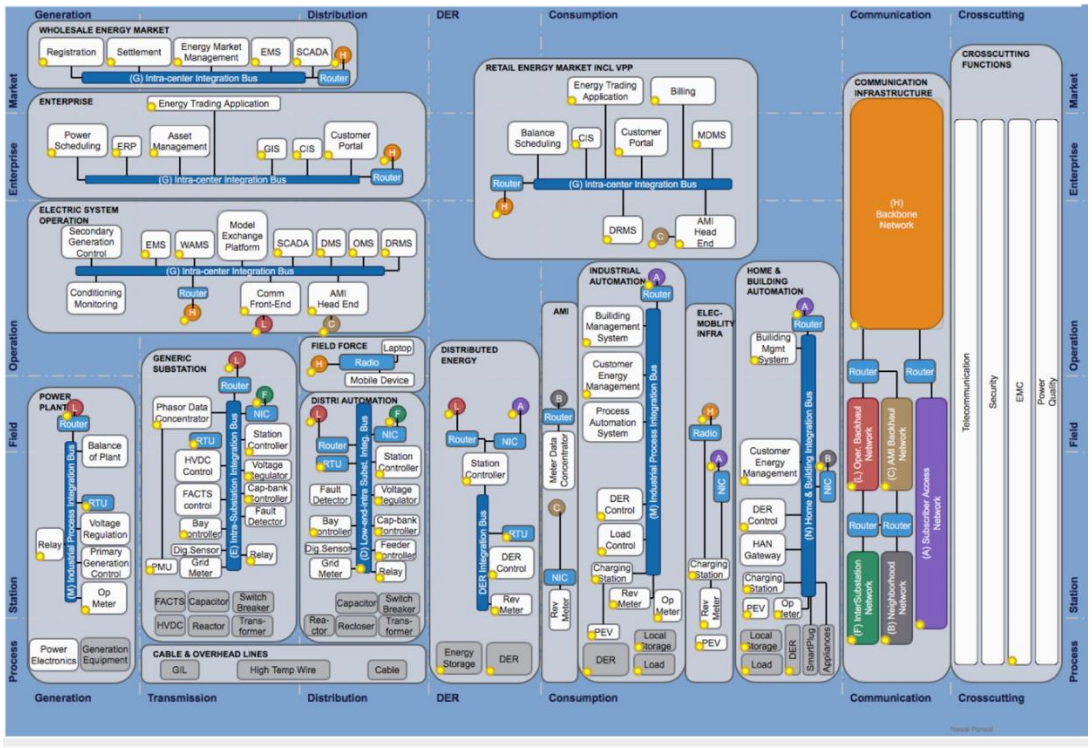

Abb. 4.3: Referenzarchitekturmodell als Grundlage für die Vulnerabilitätsanalyse
Quelle: International Electrotechnical Commission (2016a)

Das SGAM-Modell besteht aus fünf konsistenten Schichten, die Geschäftsziele und -prozesse, Funktionen, Informationsmodelle, Kommunikationsprotokolle und Komponenten darstellen. Jede Schicht deckt die Smart-Grid-Ebene ab, die von Smart-Grid-Domänen und -Zonen überspannt wird. Das SGAM-Modell stellt nicht nur den aktuellen Stand der Implementierungen im Stromnetz dar, sondern bildet auch eine mögliche Entwicklung zukünftiger Smart Grid Szenarien ab, indem es die Prinzipien Universalität, Lokalisierung, Konsistenz, Flexibilität und Interoperabilität unterstützt (CEN-CENELEC-ETSI 2014). Diese Eigenschaften erlaubten es, dieses Referenzarchitekturmodell als Material für die Experteninterviews und Workshops zu nutzen, um über die Cybersicherheit von Energiesystemen zu diskutieren, die eine vollständige Implementierung der Smart Grid-Funktionalitäten voraussetzen.

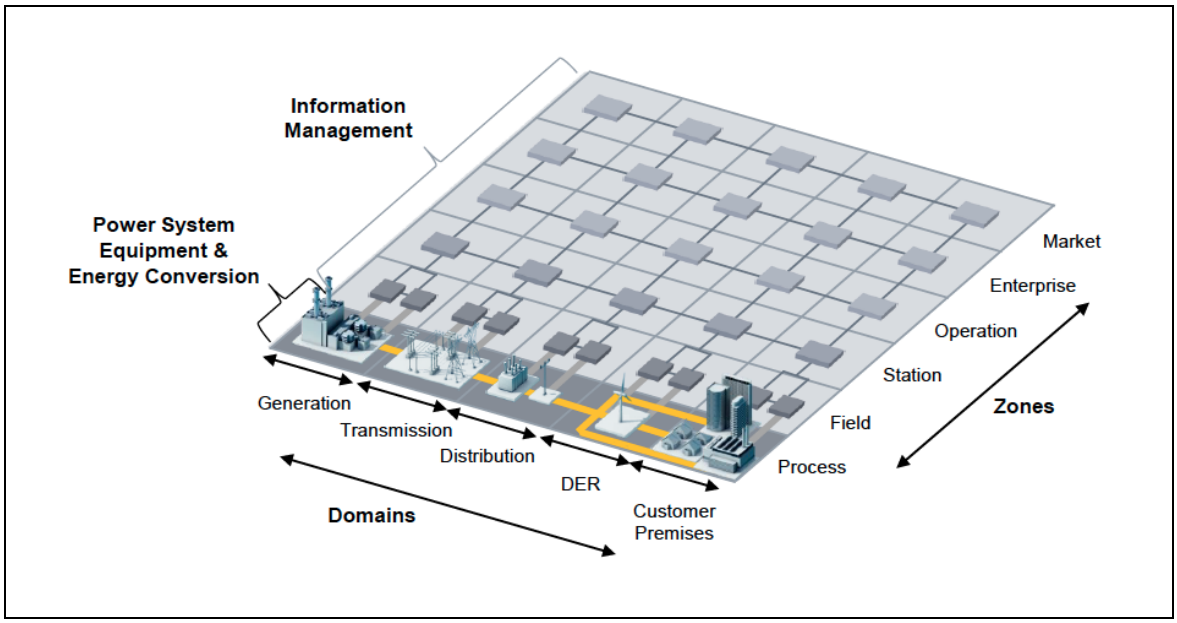

Abb. 4.4: Smart-Grid-Plane
Quelle: CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids CEN (2014)

Diese Studie umfasste die verschiedenen Bereiche des Smart Grids: Erzeugung, Übertragung, Verteilung, verteilte Energieressourcen (Englisch: Distributed Energy Resources DER), Kundenstandort und Smart Grid Zonen: Prozess, Feld, Station, Betrieb, Unternehmen, Markt, entsprechend der SGAM-Architektur. Im Folgenden wird eine Übersicht über die SGAM-Domänen, -Zonen und -Schichten gegeben (CEN-CENELEC-ETSI 2014):

SGAM-Domains:

Bulk Generation: Darstellung der Erzeugung von elektrischer Energie in großen Mengen, z. B. durch fossile, nukleare und Wasserkraftwerke, Offshore-Windparks, Photovoltaik-Großanlagen (PV) - typischerweise an das Übertragungsnetz angeschlossen.

Übertragung (Transmission): Darstellung der Infrastruktur und Organisation, die Strom über weite Strecken transportiert.

Verteilung (Distribution): Darstellung der Infrastruktur und der Organisation, die den Strom an die Kunden verteilt.

DER: Darstellung verteilter elektrischer Ressourcen, die direkt an das öffentliche Stromnetz angeschlossen sind und sich auf kleinteiligere Stromerzeugungstechnologien (typischerweise im Bereich von 3 kW bis 10.000 kW) bezieht. Diese verteilten elektrischen Betriebsmittel können direkt vom Verteilnetzbetreiber (VNB) gesteuert werden.

Kundenstandort (Customer Premises): Der Kunde ist sowohl der Endverbraucher als auch der Stromerzeuger. Die Standorte umfassen Industrie-, Gewerbe- und Wohnanlagen (z.B. Chemieanlagen, Flughäfen, Häfen, Einkaufszentren, Wohnungen). Auch die Energiegewinnung in Form von z.B. Photovoltaikanlagen, Elektrofahrzeugen, Batterien und Mikroturbinen wird darunter verstanden.

SGAM-Zonen:

Prozess (Process): Beinhaltet sowohl die primäre Ausrüstung des Stromnetzes (z.B. Generatoren, Transformatoren, Leistungsschalter, Freileitungen, Kabel, elektrische Verbraucher...) als auch die physikalische Energieumwandlung (Strom, Sonne, Wärme, Wasser, Wind...).

Feld (Field): Einrichtungen zum Schutz, zur Steuerung und Überwachung des Stromversorgungssystems, z. B. Schutzrelais, Feldregler, alle Arten von intelligenten elektronischen Geräten (Englisch: Intelligent Electronic Devices IED), die Prozessdaten aus dem Stromversorgungssystem erfassen und nutzen.

Station: Darstellung der Aggregationsebene für Felder, z.B. für Datenkonzentration, Unterstationsautomatisierung ...

Betrieb (Operation): Der Betrieb von Stromversorgungssystemen im jeweiligen Bereich, z.B. Verteilungsmanagementsysteme (Englisch: Distributed Management System DMS), Energiemanagementsysteme (Englisch: Energy Management System EMS) in Erzeugungs- und Übertragungssystemen, Mikronetzmanagementsysteme, virtuelle Kraftwerksmanagementsysteme (Aggregation mehrerer DER), Fuhrparkmanagementsysteme für Elektrofahrzeuge (Englisch: Electro vehicles EV).

Unternehmen (Enterprise): Umfasst kaufmännische und organisatorische Prozesse, Dienstleistungen und Infrastrukturen für Unternehmen (Energieversorger, Dienstleister, Energiehändler, …), z.B. Vermögensverwaltung, Mitarbeiterschulungen, Kundenbeziehungsmanagement, Abrechnung und Beschaffung.

Markt (Market): Spiegelung der möglichen Marktoperationen entlang der Energieumwandlungskette, z.B. Energiehandel, Massenmarkt, Handelsmarkt....

SGAM-Schichten

Unternehmen (Business): Stellt Geschäftsfälle dar, die einen wahrgenommenen Geschäftsbedarf beschreiben und rechtfertigen.

Funktion (Function): Repräsentiert Anwendungsfälle einschließlich logischer Funktionen oder Dienste unabhängig von physischen Implementierungen.

Information: Repräsentiert Informationsobjekte oder Datenmodelle, die zur Erfüllung von Funktionen und zum Austausch durch Kommunikation benötigt werden.

Kommunikation (Communikation): Stellt Protokolle und Mechanismen für den Informationsaustausch zwischen Komponenten dar.

Komponente (Component): Repräsentiert physikalische Komponenten, die Funktionen, Informationen und Kommunikationsmittel bereitstellen.

4.1.3 Expertenworkshops

Im Juni 2016 und März 2017 wurden zwei Workshops mit Experten aus Industrie und Wissenschaft aus dem IKT- und Energiesektor durchgeführt, um über die Vulnerabilität und Resilienz von cyberphysikalischen Energiesystemen zu diskutieren.

Während des ersten Workshops diente der oben beschriebene Ansatz der Vulnerabilitätsanalyse in einer vereinfachten Version als Grundlage für die Ermittlung von Schwachstellen. Dabei wurden eine Reihe von Cyber-Sicherheitsausfallszenarien, die von der Technischen Arbeitsgruppe 1 der U.S. National Electric Sector Cybersecurity Organization Resource (NESCOR) entwickelt wurden, als Ausgangspunkt für die Diskussion verwendet. Das genannte Dokument beschreibt für jedes der Ausfallszenarien relevante Verwundbarkeiten[5], Auswirkungen und Minderungsstrategien. Mögliche Auswirkungen sind Stromausfall, Geräteschäden, Personenschaden, Einkommensverluste, Verletzungen der Privatsphäre der Kunden und dem Verlust von Vertrauen durch die Öffentlichkeit (NESCOR 2015).

Im Workshop wurden kleine Arbeitsgruppen, die den verschiedenen Bereichen des Energiesektors zugeordnet waren, zusammengestellt. Jede Gruppe analysierte mindestens ein NESCOR-Ausfallszenario, um die Stressoren, die Höhe der Exposition und die Empfindlichkeit des Systems unter vorher beschriebenen Bedingungen zu ermitteln. Auch die Auftrittswahrscheinlichkeit bzw. Möglichkeit des Eintretens dieser Parameter wurden besprochen. Darüber hinaus diskutierten die Gruppen über vorhandene Anpassungsmechanismen, um das Auftreten der Ausfallszenarien zu verhindern und/oder die Systemleistung nach dem Ausfall wiederherzustellen. Es wurden die folgenden Szenarien im Workshop analysiert:

– Bedrohungsagent verursacht Netzinstabilität, indem er die Kontrolle über dedizierte Daten- und Sprachleitungen zwischen Systembetriebszentrum und Anlage erlangt (GEN.10)
– Manipulation von geschaltete Kondensatorbatterien, damit die Netzqualität verschlechtert wird (DGM.10)
– Herunterfahren von DER-Systemen durch gefälschte SCADA-Steuerbefehle (DER.14)
– Fernabschaltung des Massezählers durch autorisierte Person (AMI.1)
– Unerlaubte Preisinformationen wirken sich auf die Einnahmen aus (AMI.10)

Die Ergebnisse des Workshops lieferten uns wertvolle Erkenntnisse über einige der wichtigsten Cybersecurity-Herausforderungen, die aufgrund der zunehmenden Komplexität des IKT-Systems in den verschiedenen Bereichen des Energiesystems zu bewältigen sind.

Im zweiten Expertenworkshop wurden die vorläufigen Ergebnisse der VA vorgestellt und mit den Teilnehmerinnen und Teilnehmern diskutiert. Mit den erhaltenen Rückmeldung wurden die Ergebnisse der VA und der Resilienzstrategie konkretisiert. Ein Schwerpunkt lag auf der Granularität des Energiesystems, aber auch für technische, organisatorische und regulatorische Maßnahmen zur Erhöhung der Resilienz wurden Expertenmeinungen eingeholt.

[5] Der Begriff Verwundbarkeit aus dem NESCOR-Dokument wird in unserer Methodik als Schwäche/Exposition verstanden.

4.1.4 Experteninterviews

Um tiefergehendes Systemwissen für die Vulnerabilitätsanalyse zu gewinnen, wurden fast 100 Experten aus dem IKT- und Energiebereich für diese Studie kontaktiert, von denen 19 von Juni 2016 bis März 2017 an einem persönlichen oder telefonischen semi-strukturierten Interview teilnahmen. Die Befragten wurden nach ihrem Fachgebiet in fünf Kategorien eingeteilt, die in Abb. 4.5 aufgeführt sind.

Während der Interviews wurden die Experten nach möglichen Verwundbarkeiten des aktuellen und zukünftigen Stromsystems, potenziellen Auswirkungen auf die Systemdienstleistungen und möglichen Anpassungsstrategien zur Bewältigung, Anpassung oder Wiederherstellung befragt. Die Liste der in den Interviews verwendeten Fragen befindet sich im Anhang 8.1.2.

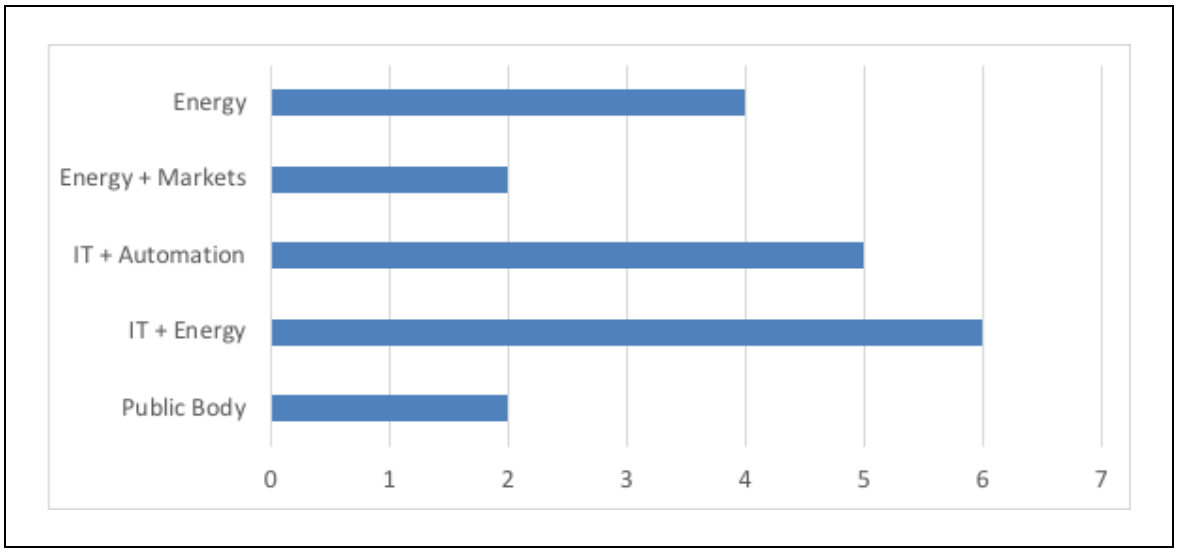

Abb. 4.5: Kategorien und Anzahl der Befragten

4.1.5 Qualitative Inhaltsanalyse

Die Aussagen aus den Expertenworkshops und Interviews wurden mittels qualitativer Inhaltsanalyse nach Mayring ausgewertet und die gefundenen Erkenntnisse als Input für die VA verwendet (Mayring 2014).

Da einige der befragten Experten darum gebeten haben, anonym zu bleiben, wurde für die Interviewanalyse entschieden, als Teilnehmeridentifikation für alle Befragten „Interviewee X“ zu verwenden, wobei X die laufende Nummer entsprechend dem Zeitpunkt des Interviews darstellt. Diese Identifikation wird in den folgenden Abschnitten verwendet, um auf die Aussagen der Befragten Bezug zu nehmen.

Nähere Informationen zur qualitativen Inhaltsanalyse befindet sich im Anhang 8.1.

4.2 Ergebnisse der Vulnerabilitätsanalyse

Die Ergebnisse der Analyse zeigen eine Vielzahl von Schwachstellen auf. Nach Ansicht der Experten könnten die ermittelten Schwachstellen, wenn von einem Angreifer ausgenutzt, potenzielle Schäden anrichten.

Die Ergebnisse wurden in die Kategorien: Technik, organisatorische Sicherheit, menschliche Faktoren und Vorschriften eingeteilt und werden in den folgenden Abschnitten ausführlich dargestellt.

4.2.1 Technologie (Software/Firmware, Hardware und Netzwerk)

4.2.1.1 Unsichere Kommunikation

Die Erhöhung der Anzahl der Systeme, Dienste und Akteure, die am cyber-physikalischen Stromnetz beteiligt sind, erfordert eine höhere Anzahl von Verbindungen. Da nahezu die gleiche TCP/IP-basierte Kommunikationstechnologie wie im Business-IT-Bereich eingesetzt wird, gelten die meisten IT-Sicherheitsprobleme, die aus der Business- oder Standard-IT-Sicherheit kommen, auch für Energiesysteme (Interviewee 1 2016; Interviewee 6 2016). Allerdings sind die Sicherheitsanforderungen für die verschiedenen Verbindungen nicht gleich. Vertraulichkeit ist wegen der Geheimhaltung von Unternehmensinformationen ein wichtiger Aspekt der IT, wird aber in industriellen Kontrollsystemen (ICS) nicht prioritär berücksichtigt, obwohl Integrität und Verfügbarkeit von Daten für den Betrieb der Systeme entscheidend sind (Marin Fernandes 2012).

Wenn die Kommunikation unverschlüsselte oder schwach verschlüsselte Netzwerkprotokolle verwendet, können Authentifizierungsschlüssel und Daten-Nutzlasten abgegriffen werden. Die Verwendung von Klartext-Protokollen kann es Gegnern auch ermöglichen, Session Hijacking und Man-in-the-Middle (MITM)-Angriffe durchzuführen, wodurch der Angreifer die Daten, die zwischen den Geräten übertragen werden, manipulieren kann (NIST 2014). Während einige Verbindungen sicherer sind als andere, kann die am schwächsten geschützte Verbindung, aufgrund des hohen Vernetzungsgrades von cyberphysikalischen Energiesystemen, als Angriffsstartpunkt in andere Domänen genutzt werden (Knapp 2011).

Um die Vulnerabilitäten durch eine unsichere Kommunikationsverbindung zu ermitteln, wurden die Domänen des Energiesystems in drei Cluster eingeteilt: (a) Endverbrauch, (b) dezentrale Energieanlagen und Verteilung, (c) Erzeugung und Übertragung.

Exposition und Sensitivität

a. Endverbrauch

Bei der Smart-Meter-Infrastruktur erwähnte die Mehrheit der Experten, dass Deutschland über ein starkes Verschlüsselungssystem verfügt, das auf der IT-Sicherheitsarchitektur und den Sicherheitsanforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in seinem Smart Meter Gateway Protection Profile basiert (BSI 2014).

In dieser Sicherheitsarchitektur ist die zentrale Kommunikationskomponente ein Smart Meter Gateway (SMGW), siehe Abb. 4.6. Dieses Gateway befindet sich beim Kunden und verbindet die elektronischen Messgeräte im Local Metrological Network (LMN) sowie alle steuerbaren Verbrauchs-,

Speicher- oder Produktionsgeräte im Home Area Network (HAN) mit den verschiedenen Marktteilnehmern (z.B. Smart Meter Gateway Administrator (SMGA) im Auftrag des Messstellenbetreibers, Verteilnetzbetreibers oder Energieversorgers) im Wide Area Network (WAN) (BSI 2015a). Das SMGW sammelt, verarbeitet und speichert die Aufzeichnungen der Zähler und stellt sicher, dass nur berechtigte Personen Zugriff darauf haben. Relevante Informationen werden vor dem Versand durch den kryptographischen Dienst des Sicherheitsmoduls, das als integraler Bestandteil in das SMGW eingebettet ist, signiert und verschlüsselt. Das Schutzprofil definiert die Sicherheitsziele und die entsprechenden Sicherheitsanforderungen des Sicherheitsmoduls, das vom Gateway zur kryptographischen Unterstützung verwendet wird (BSI 2014). Um die Interoperabilität der verschiedenen Komponenten der Smart Metering-Infrastruktur sicherzustellen, hat das BSI technische Umsetzungsrichtlinien definiert, die in der Technischen Richtlinie TR-03109 zu finden sind (BSI 2013b).

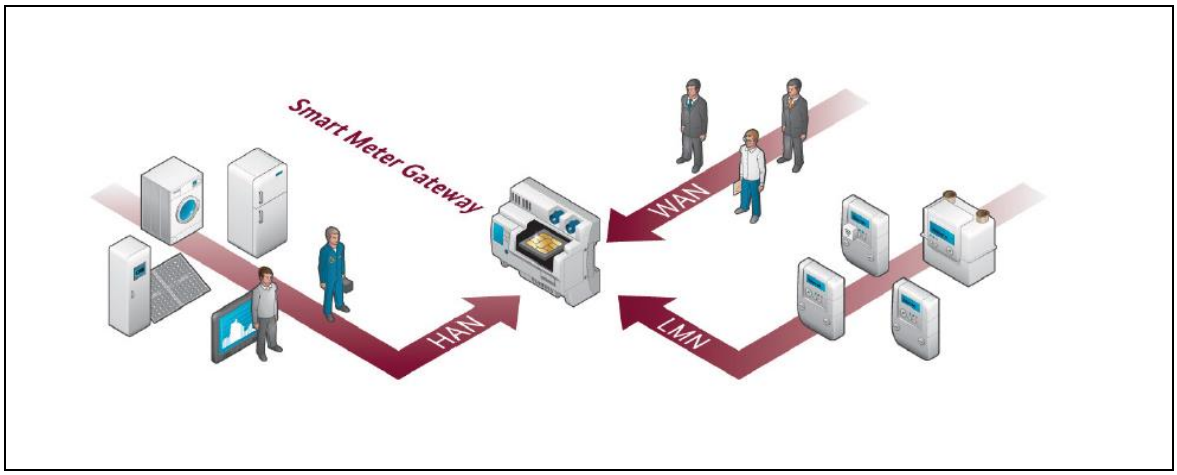

Abb. 4.6: Smart Meter Gateway Architektur
Quelle: Bundesamt für Sicherheit in der Informationstechnik (2015a)

Obwohl dieses Kommunikationssystem darauf abzielt, Datenschutz, Datensicherheit und Interoperabilität zu gewährleisten, haben einige Experten auch erwähnt, dass es einige Nachteile aufweist. Das Schema ist bereits einige Jahre alt und der Hauptzweck besteht darin, nur die Kommunikation zwischen dem SMGW und dem SMGA zu verschlüsseln. Die Sicherheitsanforderungen für die Kommunikation zwischen dem SMGW und anderen Akteuren, d.h. dem externen Markt, sind im SMGA-Zertifizierungsprozess nicht geregelt, was eine potenzielle Sicherheitslücke bedeuten könnte, die die Sicherheitsanforderungen an Smart Metering-Daten beeinträchtigen könnte (Interviewee 8 2017; Interviewee 19 2017).

Eine Bewertung der Schutzprofile und der damit verbundenen technischen Umsetzungsrichtlinien wurde von von Oheimb durchgeführt (von Oheimb 2013). Von Oheimb konnte dabei einige Schwachstellen und Nachteile identifizieren. So erfordert allein der hohe Schutzmechanismus und das Sicherheitskonzept für den SMGW einen hohen technischen Aufwand und bringt hohe Kosten für Implementierung, Zertifizierung und Nutzung mit sich. Im Hinblick auf den Verschlüsselungsansatz wird in der Studie hervorgehoben, dass der Einsatz einer klassischen Public Key Infrastructure (PKI) sehr kritische zentrale Fehlerpunkte einführt, bei denen die Ausnutzung von Schwachstellen zu enormen Schäden am Gesamtsystem führen kann. Diese Einschätzung wurde von einem interviewten IT-Sicherheitsexperten geteilt, der weiter ausführte, dass bei der Verwendung von Public-

Key-Kryptographie im Energiesektor, Energieversorgungssysteme im Wesentlichen Probleme der Public-Key-Kryptographie erben würden, die bereits jetzt die Sicherheit von Onlinesystemen einschränken, wie z.B. von Websites. Im Wesentlichen liegt dabei die Herausforderung im hohen Wartungs- und Pflegeaufwand (Overhead) der Zertifizierungsstellen und der Schlüsselverwaltung von PKI (Interviewee 13 2017).

Bei den Kunden zu Hause können Kommunikationsprotokolle, die in Haus- oder Gebäudeautomationssystemen verwendet werden (z. B. automatisierte Beleuchtungssysteme, Überwachungssysteme, intelligente Geräte und andere IoT-Geräte), einen weiteren Einstiegspunkt für mögliche Datenlecks darstellen. Dies vor allem, weil einige der verwendeten Protokolle bereits unsicher aufgrund ihrer Struktur bzw. ihres Designs sind und von den geltenden Vorschriften nicht adressiert werden. Ein Beispiel einer durch Designfehler verursachten Schwäche kann in den Arbeiten von Morgner et al. gefunden werden (Morgner et al. 2017a; Morgner et al. 2017b). Morgner et al. stellen ausführlich die Ergebnisse einer Sicherheitsanalyse des Netzwerkprotokolls ZigBee Light Link (ZLL) vor. ZLL ist einer der beliebtesten Standards für Beleuchtungssysteme von Wohn-, Geschäfts- und Industriegebäuden. Die Analyse zielte auf das ZLL-Touchlink-Inbetriebnahmeverfahren ab, das für Integration von ZLL-Geräten durch räumliche Nähe statt der Verwendung einer kryptographischen Authentifizierung eingesetzt wird. Die Analyse ergab, dass die Touchlink-Kommunikation auf Kommunikationsframes basiert, die weder gesichert noch authentifiziert sind. Darüber hinaus ist die Übertragung des Netzwerkschlüssels zu einem anzuschließenden Gerät ausschließlich durch einen globalen Masterschlüssel geschützt, der seit März 2015 aufgrund eines Leaks öffentlich verfügbar ist. Dieser Schlüssel kann aufgrund den Rückwärtskompatibilitätsanforderungen an ältere ZigBee Light Link-Produkte nicht verändert werden (Morgner et al. 2017b). ZigBee ist ein beliebter Standard für die drahtlose Low-Power-Kommunikation, der in verschiedenen Internet of Things (IoT)-Geräten für andere Anwendungen implementiert wird, darunter auch Türschlösser und Einbruchmeldeanlagen. Lücken in Sicherheitsanlagen können durch weitere unsichere Zugangspunkte entstehen, die die Sicherheitsanforderungen von Daten innerhalb des HAN beeinträchtigen könnten.

b. Dezentrale Energieanlagen und Verteilung

Die zunehmende Durchdringung dezentraler Energieanlagen (DER) hat die Prozesse im Stromnetz dynamischer und komplexer gemacht (Arghandeh et al. 2016). So haben sich dadurch bspw. die Anzahl der Geräte mit intelligenten Wechselrichtern und Batteriecontrollern, die sich im Besitz von Verbrauchern und Dritten befinden, deutlich erhöht (Qi et al. 2016).

Auf lokaler Ebene verwalten Systeme, die DER zugeordnet werden können, ihre eigenen Erzeugungs- und Speicheraktivitäten autonom, basierend auf den lokalen Gegebenheiten, den vordefinierten Einstellungen und den Präferenzen des Eigentümers. DERs sind jedoch aktive Teilnehmer am Netzbetrieb und müssen mit anderen DERs und Verteilnetzgeräten koordiniert werden (IEC 2016b). Qi et al. schlägt eine DER-Systemarchitektur vor, die die verschiedenen Akteure und Interaktionen in vier Domänen bündelt (siehe Abb. 4.7) (Qi et al. 2016). Diese Domänen bildeten die Grundlage für die Analyse der Cybersicherheit von DER und Smart Invertern.

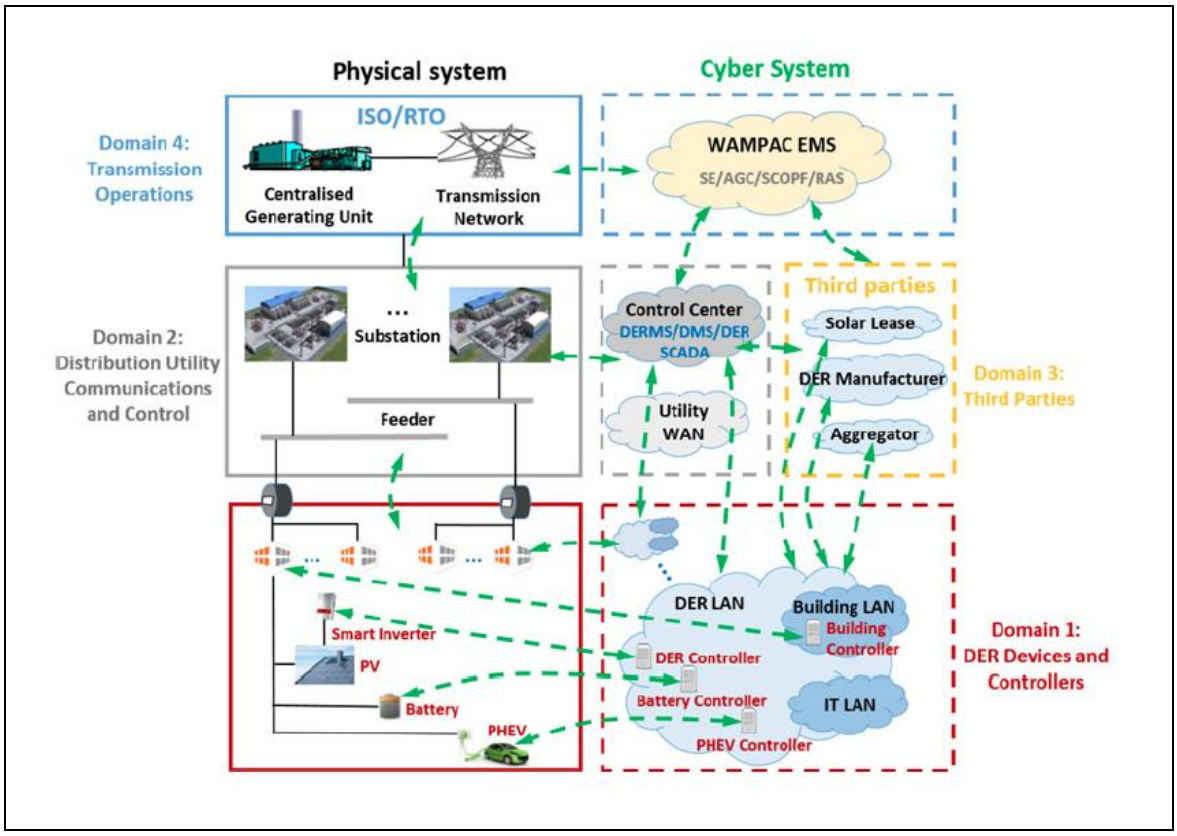

Abb. 4.7: Generische Architektur des Stromsystems mit DER
Quelle: Qi et al. (2016)

Im Folgenden werden einige kritische Punkte im Zusammenhang mit unsicherer Kommunikation hervorgehoben (Qi et al. 2016):

– *Domäne 1: DER-Geräte und Controller:* Die DER-Besitzer erhalten die Informationen über den DER durch die Kommunikation mit intelligenten Wechselrichtern mit unsicheren drahtlosen Kommunikationsprotokollen wie bspw. ZigBee.

– *Domäne 2: Kommunikation und Kontrolle der Verteilnetzbetreiber:* Das Dienstprogramm interagiert mit den intelligenten Wechselrichtern und Controllern über Kommunikationsprotokolle wie bspw. Smart Energy Profile (SEP) 2.0. Diese Protokolle sollten auf Schwachstellen überprüft werden.

– *Domain 3: Drittanbieter:* Die meisten Drittanbieter haben die Möglichkeit, den Status von DER zu überwachen, und einige haben auch die Möglichkeit, ihren Betrieb direkt zu steuern. Außerdem können diese Entitäten eine Verbindung zu einer sehr großen Anzahl von DER haben. Diese Verbindungen kann man sich als zentrale Punkte vorstellen, die von Angreifern genutzt werden könnten, um eine große Anzahl von DER über mehrere Verteilnetze hinweg zu manipulieren und zu beeinflussen.

– *Domäne 4: Übertragung:* DER müssen in die großen Stromnetze integriert werden. Zu den dafür verwendeten Kommunikationsprotokollen gehören das Distributed Network Protocol (DNP3) und die IEC 61850, die aufgrund ihres Designs sicherheitstechnische Mängel aufweisen. Verbesserte Protokollversionen kommen häufig nicht zur Anwendung (siehe Kapitel 4.2.4.1 Fehlende Umsetzung von Sicherheitsstandards und Regulierung).

Wie von einem Interviewpartner aus dem Energie- und Marktbereich erwähnt, ist die Kommunikationsinfrastruktur für DER teilweise reguliert und externe Akteure bspw. Herstellerfirmen (z.B. PV-Wechselrichter oder Windkraftanlagenhersteller) oder Direktvermarkter können auf die Regeleinheit der dezentralen Erzeugungseinheiten zugreifen, um Informationen für Überwachungs- und Steuerungszwecke zu erhalten. Dies erzeugt eine weitere Verwundbarkeit des Systems, wenn der Angriff über die Kommunikationsinfrastruktur dieser Akteure zu den Erzeugungseinheiten erfolgt, falls diese nicht ausreichend gesichert sind und somit eine Hintertür mit Zugang zum System bilden könnten (Interviewee 2 2016).

c. Erzeugung und Übertragung

Kommunikationsprotokolle in ICS und Supervisory Control and Data Acquisition (SCADA) Systemen haben sich im Laufe der Zeit von proprietären Punkt-zu-Punkt-Verbindungen zu offenen Standardprotokollen entwickelt, die in verteilten Systemen verwendet werden (McLaughlin et al. 2015). Am Anfang war die Kommunikationsinfrastruktur von Energieversorgungssystemen generell sicher, da sie von externen Kommunikationsnetzen isoliert war (die so genannte "air-gap" deutsch: Luftbarriere). Zusätzlich basierten sie auf handelsüblicher proprietärer Hard- und Software, was ihnen ein angemessenes Maß an Security-by-obscurity (deutsch: „Sicherheit durch Unklarheit") verlieh (Teixeira et al. 2015). Die erweiterte Konvergenz mit IKT-Netzwerken und die dominante Kommunikation auf Basis von TCP/IP-Protokollen stellen jedoch ein hohes Sicherheitsproblem für das Stromsystem dar (Interviewee 2 2016).

Legacy ICS-Kommunikationsprotokolle wurden ohne Cybersicherheit entwickelt, daher sind keine IT-Sicherheitsmechanismen wie Verschlüsselung oder Authentifizierung implementiert (Interviewee 15 2017). Modbus ist ein einfaches Client-Server-Protokoll, das ursprünglich für die langsame serielle Kommunikation in ICS-Netzwerken entwickelt wurde. Da das Modbus-Protokoll nicht für hochsicherheitskritische Umgebungen konzipiert wurde, werden Modbus-Pakete unverschlüsselt gesendet, so dass es für einen Angreifer leichtes Spiel ist, eine Verbindung zu einem legitimen Netzwerkknoten herzustellen und die Nachricht zu manipulieren. Die Manipulation wird vom Empfänger üblicherweise nicht erkannt, sodass dadurch Messwerte oder Steuerbefehle gefälscht werden können, die zu Systemstörungen führen könnten (Mo et al. 2012; Interviewee 15 2017).

Darüber hinaus sind industrielle Kontrollnetzwerke in einigen Fällen ohne geeignete Sicherheitsmaßnahmen direkt mit dem Internet verbunden und ermöglichen so den Zugang für externe Angreifer, die die industriellen Netzwerke mit Viren oder Malware infizieren könnten (Interviewee 1 2016; Interviewee 15 2017). Suchmaschinen wie SHODAN[6] können dazu verwendet werden, um Internet-konforme ICS-Geräte zu finden. Darüber hinaus sind Open Source- und kommerzielle Tools zur Ausnutzung bekannter ICS-Protokollschwächen im Internet leicht zu finden, was dazu führt, dass eine größere Bandbreite an Systemen potenziellen Angriffen ausgesetzt ist.

In der Stationszone des SGAM-Modells (siehe Kapitel 4.1.2) verwenden einige Sensoren oder intelligente elektronische Geräte (IED) drahtlose Kommunikationswege, die in der Regel aufgrund von Protokollen mit schlechtem Schutz, fehlender Verschlüsselungsmethoden oder falscher Gerätekonfiguration unsicherer sind. Um diese Geräte zu gefährden, muss jedoch ein Angriff in räumli-

[6] https://ics-radar.shodan.io

cher Nähe stattfinden. Dies wird in den seltensten Fälle externe Angreifern bei industriellen Anlagen möglich sein (Interviewee 15 2017). Es wäre jedoch ein Angriffsszenario vorstellbar, bei dem der Eindringpunkt über ein kabelloses Gerät an einer Unterstation stattfindet und sich auf Betriebsmittel des elektrischen Netzes ausbreitet. Sollte solch ein Szenario nicht im Vornherein berücksichtigt werden, könnte dies ein ernsthaftes Risiko darstellen (Interviewee 18 2017).

Die meisten Hersteller verfügen über Fernwartungsschnittstellen für Inspektion und Überwachung größerer Komponenten, z.B. einer Gasturbine zur Stromerzeugung. Über Fernzugriff kann auch in die Steuerungsebene oder Human Machine Interface (HMI)-Ebene gelangt werden, um Updates oder Patches zu installieren. Wenn die Verbindung nicht ordnungsgemäß gesichert ist, kann dieser Fernzugriff den Zugriff auf das Systemgerät oder weitere bösartige Zwecke ermöglichen. Netzbetreiber können auch Fernverbindungen zu verschiedenen Geräten, z.B. Unterstationen, realisieren, um Updates oder Patches zu installieren. Zu diesem Zweck werden spezielle Kommunikationsnetze genutzt werden. Dies ist bereits bei den großen Netzbetreibern üblich. Kleinere Netzbetreiber haben aber auch die Möglichkeit, abgeschottete Netze von Telekommunikationsbetreibern zu mieten und dadurch die Fernwartung sicherer zu gestalten. Vor allem die kleineren Netzbetreiber sollten darauf achten, dass die Sicherheitsrichtlinien für die Kommunikationsinfrastruktur ordnungsgemäß umgesetzt werden, da sonst die Anforderungen an die Datensicherheit nicht erfüllt werden (Interviewee 4 2016; Interviewee 17 2017).

Angriffsmechanismen und Störereignisse

Das Fehlen von Verschlüsselung und Authentifizierungsmechanismen bei Kommunikationsprotokollen ermöglicht es Angreifern, MITM-Angriffe dafür zu nutzen, verschiedene Handlungen durchzuführen, wie a) die Kommunikation zwischen Knoten aufzuzeichnen und veränderte Pakete rückzuspeisen, sodass reales Systemverhalten verborgen bleibt, ohne detaillierte Kenntnisse über das System zu haben, b) Sitzungen kapern, indem die Kommunikationssitzung von dem Angreifer übernommen wird und für nicht autorisierte Kommunikation mit dem Opfer verwendet wird, oder c) Daten zu injizieren oder zu manipulieren, um ausgeführte Befehle und das Gelesene im Kommunikationsstrom in Echtzeit zu verändern (McLaughlin et al. 2015).

Im folgenden Abschnitt werden einige Angriffsmechanismen und Störungen der Kommunikationsinfrastruktur in verschiedenen Bereichen des Energiesystems beschrieben:

a. Endverbrauch

Sniffing- und Abhörung können von entfernten oder lokalen Angreifern eingesetzt werden, um die Vertraulichkeit und Integrität von datenschutzrelevanten oder abrechnungsrelevanten Daten zu gefährden. Entfernte Angreifer im WAN (siehe Abb. 4.6) könnten versuchen, eine Komponente der lokalen Infrastruktur zu kompromittieren, um eine Komponente selbst zu beschädigen oder eine direkte Auswirkung auf das Stromnetz zu erzeugen, z.B. durch Datenmanipulation der intelligenten Wechselrichter. Lokale Angreifer, einschließlich Prosumenten, die Zugriff auf das Gateway und/oder die Zähler haben, könnten versuchen, ohne Berechtigung Anlageninformationen auszulesen oder zu verändern, während sie im LMN gespeichert oder übertragen werden (siehe Abb. 4.6) (von Oheimb 2013).

Denial-of-Service-Angriffe auf die Verfügbarkeit von Netzwerkgeräten innerhalb des HAN könnten durch physische Angriffe auf die Kommunikationsinfrastruktur erfolgen. Die kabelgebundene Kommunikation kann durch „physisches Durchtrennen von Kabeln“ beeinträchtigt werden und die drahtlose Kommunikation abgeklemmt werden (engl. auch „Jamming“ genannt) (McLaughlin et al.

2015). Der Ablauf eines Jamming-Angriffs besteht im ersten Schritt darin, die Kommunikationskanäle abzuhören bis Informationen abgefangen werden können. Anschließend kann der Kanal mit unzulässigem Datenverkehr quasi „überrollt“ werden, um damit möglichst die Datenverfügbarkeit zu beeinträchtigen (Tazi und Abdi 2015). Diese Art von Angriffen kann dazu verwendet werden, um zu verhindern, dass sich fernauslesbare Zähler (Smart Meter) mit dem Router der Netz- bzw. Zählerbetreiber verbinden, indem sie dem Zähler vorgaukeln, die Funkverbindung sei überlastet. Damit wird die Verbindung immer als besetzt angesehen, was den Empfang von Datenpaketen verhindert (Baig und Amoudi 2013) zitiert in (Lopez et al. 2015).

Morgner und Kollegen entwickelten einen realen Angriff auf die drahtlose Kommunikation von ZigBee-Geräten, die häufig im Bereich Smart Home verwendet werden (Morgner et al. 2017b). Die Auswertung ergab, dass die Sicherheitslücken des Protokolls es dem Angreifer ermöglichen, die Verfügbarkeit der Geräte einzuschränken und die Kontrolle über alle Knoten im Netzwerk zu erlangen.

b. Dezentrale Energieanlagen und Verteilung

Versorgungsunternehmen, DER-Hersteller oder Aggregatoren von Drittanbietern müssen möglicherweise mit den DER kommunizieren, um die Betriebspunkte zu kontrollieren und den Status der Geräte zu überwachen. Dies gewährleistet einen zuverlässigen Betrieb des Verteilnetzes und ist daher von entscheidender Bedeutung. Sollte dabei die Kommunikation mit den Endgeräten nicht verschlüsselt sein oder unsichere Netzwerkprotokolle verwendet werden, so bildet das eine Schwachstelle. Angreifer können dann diese Schwachstellen ausnutzen, um MITM-Angriffe durchzuführen, Nachrichten abzugreifen, zu blockieren oder in veränderter weiterzuleiten. Solche Art von Angriffen bergen die Gefahr, dass die Angreifer in die Kontrolle einer großen Zahl an DER kommen könnten, was schwerwiegende Auswirkungen auf den Betrieb des Verteilnetzes haben könnte (Qi et al. 2016).

c. Erzeugung und Übertragung

Der Mangel an Verschlüsselungs- und Authentifizierungmechanismen bei vielen industriellen Steuerungsprotokollen hat zur Folge, dass diese Systeme gegenüber einer Vielzahl von Angriffen ungeschützt sind. Zum Beispiel kann ein Angreifer über MITM Kommunikationsframes abfangen und unverschlüsselte Klartext-Blöcke sammeln, die wertvolle Informationen wie bspw. Quell- und Zieladressen sowie Kontroll- und Einstellungsinformationen liefern könnten (Mo et al. 2012). Der Angreifer kann in Echtzeit Messwerte und Befehle in den Kommunikationsstrom einspeisen oder verändern. Während des Abfangens aller Pakete können einige Pakete gelöscht, geändert oder neue Pakete mit beliebigem Ergebnis injiziert werden. Dieser Angriff ist sehr problematisch, wenn er von einem erfahrenen Benutzer ausgeführt wird, da er schwer zu erkennen ist und ein erhebliches Schadenspotenzial entfalten kann. Ein Angreifer ist in der Lage, Messwerte von entfernten Standorten zu manipulieren sowie zwischen zwei kommunizierenden Knoten wichtige Steuerbefehle zu unterdrücken oder in veränderter Form in den Kommunikationsstrang einzuspeisen (McLaughlin et al. 2015).

Protokollspezifische Angriffe sind in der Literatur zu finden. Mögliche Angriffe wie z. B. Message-Spoofing, Replay-Angriffe, Netzwerk-Scanning und andere, die sich auf Modbus-Sicherheitsprobleme beziehen, sind in (Mo et al. 2012) beschrieben. Open-Source- oder kommerzielle Tools zur

Durchführung von MITM-Angriffen auf Modbus-Netzwerke sind auch im Internet[7] leicht zu finden (Bodungen et al. 2017). In Bezug auf Protokolle, die für die Automatisierung von Umspannwerken verwendet werden, befassen sich Dondossola et al. mit der Verwendung von DoS-Angriffen auf Netzwerke mit dem IEC 60870-5-Protokoll und andere präsentieren einen MITM-Angriff auf ICS, der sich auf die IEC 60870-5-104 stützt (Dondossola et al. 2008; Dondossola et al. 2009; Maynard et al. 2014).

"Crashoverride"-Malware (auch bekannt als "Industroyer") ist ein echtes Beispiel für eine fortschrittliche und hochentwickelte Malware, die mehrere Angriffsmechanismen kombiniert und die Schwächen bestimmter industrieller Protokolle für die Automatisierung von Umspannwerken nutzt. In Box 1 finden Sie detaillierte Informationen zu dieser Malware.

Box 1: "Crashoverride"-Malware

Im Juni 2017 veröffentlichten Sicherheitsforscher von ESET und Dragos eine detaillierte Analyse dieser Malware, die für ICS-Komponenten entwickelt wurde. Nach Ansicht der Autoren ist es sehr wahrscheinlich, dass "Crashoverride" verwendet worden sein könnte, um in einem Umspannwerk in der Ukraine im Dezember 2016 Stromausfälle auszulösen (Siehe: (Cherepanov 2017; Dragos Inc. 2017)). Die Entwickler der "Crashoverride"-Malware zeigten bei dem Angriff, dass sie tiefergehendes Wissen und Kenntnisse industrieller Steuerungssysteme, die in Energiesystemen eingesetzt werden haben, besitzen. Außerdem besitzen sie eine hohe Expertise industrieller Kommunikationsprotokolle, die vor einigen Jahrzehnten ohne Berücksichtigung von Sicherheitsaspekte entwickelt wurden. Daher mussten die Angreifer „nicht nach Protokollschwachstellen suchen; alles, was sie brauchten, war, der Malware beizubringen, diese Protokolle „zu sprechen“ (Cherepanov und Lipovsky 2017).

Die "Crashoverride"-Malware ist ein modulares Framework, das in der Lage ist, Leistungsschalter und Sicherungsautomaten direkt zu steuern.

Abb. 4.8 zeigt die Struktur der Malware, die aus einem Main-Backdoor, einer zusätzlichen Backdoor, einem Loader-Modul und mehreren Support- und Payload-Modulen besteht. Die Backdoors werden von den Angreifern dazu verwendet, um die anderen Komponenten zu installieren und zu steuern. Er verbindet sich mit einem entfernten Server (Command Control Center, C&C), um Befehle zu empfangen und den Angreifern zu melden. Die zusätzlichen Backdoors (eine "trojanisierte" Version der Windows Notepad-Anwendung) bietet einen alternativen Persistenzmechanismus, der es den Angreifern ermöglicht, wieder Zugriff auf ein gezieltes Netzwerk zu erhalten, falls die Main-Backdoor erkannt und/oder deaktiviert wird. Das Launcher-Modul, welches eine bestimmte Uhrzeit und ein bestimmtes Datum enthält, lädt Nutzlastmodule und startet einen Countdown von 1 oder 2 Stunden, um die Datawiper-Modul zu starten. Die Payload-Komponenten zielen auf bestimmte industrielle Kommunikationsprotokolle, die in den folgenden Standards spezifiziert sind: IEC 60870-5-101, IEC 60870-5-104,

[7] Modbus-VCR (siehe https://github.com/reidmefirst/modbus-vcr) ist ein Beispiel für ein frei verfügbares Tool, das in Verbindung mit Ettercap den Modbus-Verkehr aufzeichnet und dann wiedergibt, so dass die Systeme während eines aufgezeichneten Zeitraums wie gewohnt funktionieren.

IEC 61850 und OLE for Process Control Data Access (OPC DA). Das Wiper-Modul wurde entwickelt, um für das System kritische Registrierungsschlüssel zu löschen und das Überschreiben von Dateien zu ermöglichen, sodass das System nicht mehr bootfähig und die Wiederherstellung erschwert wird (Cherepanov 2017; Cherepanov und Lipovsky 2017; Dragos Inc. 2017).

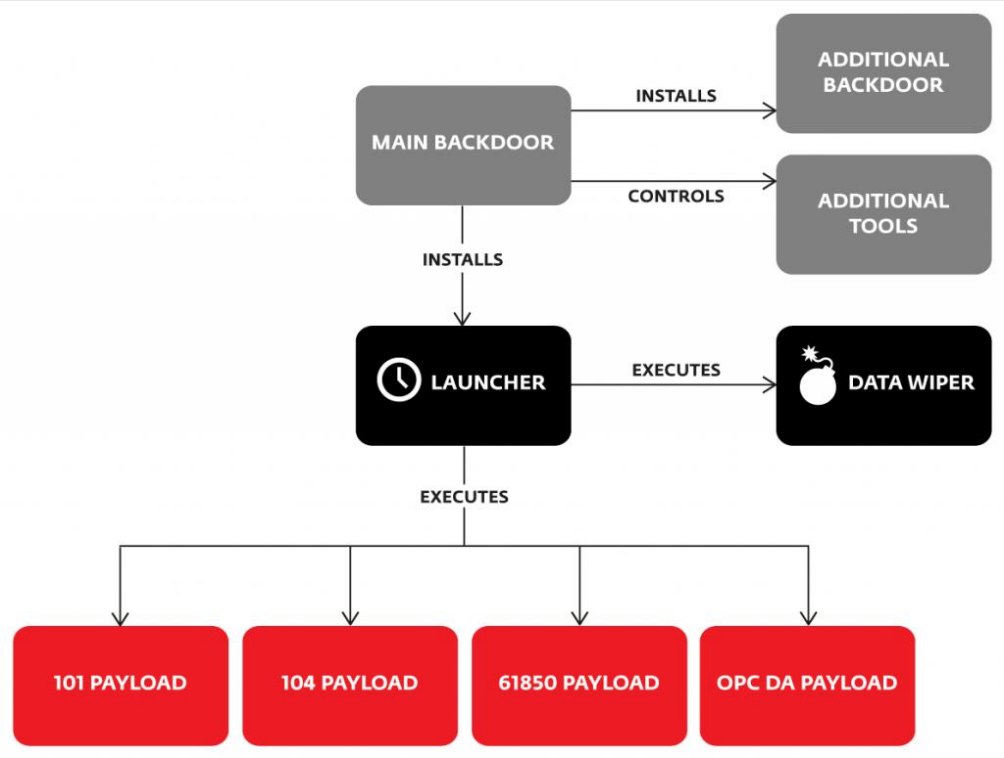

Abb. 4.8: Vereinfachtes Schema der 'Crashoverride/Industroyer'-Komponenten
Quelle: Cherepanov und Lipovsky (2017)

Nachfolgend eine kurze Beschreibung der wichtigsten Merkmale der einzelnen Payload-Module:

- Die Payload 101 ist nach dem internationalen Standard IEC 60870-5-101 (bzw. IEC 101) benannt, der ein serielles Kommunikationsprotokoll zur Überwachung und Steuerung von elektrischen Energiesystemen beschreibt, die für die Kommunikation zwischen ICS und Remote Terminal Units (RTUs) verwendet werden. Die Payload 101 implementiert teilweise das in IEC 101 beschriebene Protokoll und ist in der Lage, eine Konfigurationsdatei zu lesen, um alle angeschlossenen RTUs aufzulisten. Das Hauptziel dieser Payload ist es, den Ein/Aus-Zustand der zugrundeliegenden RTU zu ändern (Cherepanov 2017; Virsec 2017).
- Die 104 Payload ist eine Variante der obigen 101 Payload, die über ein TCP/IP-Netzwerk läuft und RTUs im Netzwerk erkennen kann. Sie wurde nach der internationalen Norm IEC 60870-5-104 (bzw. IEC 104) benannt. Die Malware ‚schließt den ursprünglichen Prozess, der den normalen Überwachungsprozess der Payload durchführt, und ersetzt ihn durch einen Angreifer-Prozess. In Stufe 1 verbindet sich der Angreifer-Prozess mit den Ziel-RTUs und iteriert durch deren Zustände. In Stufe 2 schaltet der Angreifer-Prozess kontinuierlich den Ein/Aus-Zustand der Ziel-RTUs um und protokolliert den Erfolg, so dass die Bediener keinen Alarm erhalten (Virsec 2017).

- Die Payload 61850 ist nach der Norm IEC 61850 benannt, die ein Protokoll für die herstellerübergreifende Kommunikation zwischen Geräten beschreibt, die Schutz, Automatisierung, Messung, Überwachung und Steuerung von elektrischen Schaltanlagen-Automatisierungssystemen durchführen. Einmal ausgeführt, nutzt das Modul eine Konfigurationsdatei, um Ziele zu identifizieren, und ohne eine Konfigurationsdatei listet es das lokale Netzwerk auf, um potenzielle Ziele zu identifizieren. Er kommuniziert mit den Zielen, um festzustellen, ob das Gerät einen Leistungsschalter steuert. Die Payload zählt die Daten auf und erstellt ein Protokoll mit umfangreichen Metadaten über jedes Ziel für den Export in die C&C (Cherepanov 2017; Dragos Inc. 2017; Virsec 2017).
- Die OPC DA Payload Komponente implementiert einen Client für das in der OPC Data Access Spezifikation beschriebene Protokoll. OPC (OLE for Process Control) ist ein Software-Standard und eine Spezifikation, die auf Microsoft-Technologien wie OLE, COM und DCOM basiert. Der Data Access (DA)-Teil der OPC-Spezifikation ermöglicht den Echtzeit-Datenaustausch zwischen verteilten Komponenten, basierend auf einem Client-Server-Modell. Diese Payload fragt die verschiedenen OPC-Server ab und sucht nach Objekten, die von OPC-Servern bereitgestellt werden, die zu Produkten der Firma ABB gehören, wie z.B. deren MicroSCADA-Reihe. Einmal ausgeführt, sendet das Modul einen 0x01-Status aus, der für die Zielsysteme einer "Primary Variable Out of Limits" entspricht, was zu einem Missverständnis des Schutzrelaisstatus führt (Cherepanov 2017; Dragos Inc. 2017; Virsec 2017).
- Zu den zusätzlichen Tools gehört das Denial-Of-Service (DOS)-Tool, das die Schwachstelle CVE-2015-5374 ausnutzt, wodurch das digitale SIPROTEC-Relais von Siemens in einen unempfindlichen Zustand gesetzt wird, bis es manuell neu gestartet wird (Cherepanov 2017).

Potenzielle Auswirkungen auf Systemleistung

Die Nutzung unsicherer Kommunikationskanäle wirkt sich direkt auf Anforderungen an die Datensicherheit aus. Im folgenden Abschnitt werden die potenziellen Auswirkungen auf die Systemleistung für die evaluierten Domänencluster der Datensicherheit (Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit) detailliert beschrieben, siehe dazu auch Tab. 4.1.

a. Endverbrauch

Die Beeinträchtigung der Vertraulichkeit von Daten, insbesondere durch MITM-Angriffe, wird als relevanteres Sicherheitsproblem im Bereich der Smart Metering-Infrastruktur, als auch in anderen Bereichen des Stromsystems gesehen (Interviewee 1 2016). Die Analyse von Energieverbrauchsdaten kann einen wichtigen Einblick in die Privatsphäre der Kunden geben (Greveler 2016). Wenn beispielsweise ein Angreifer in der Lage ist, den Stromverbrauch zu überwachen, der in direktem Zusammenhang mit den Aktivitätsmustern innerhalb des Kundengeländes steht, könnte dies Auswirkungen auf die Sicherheit der Hausbesitzer haben. Angreifer könnten ableiten, wann die Besitzer zu Hause sind und kriminelle Aktivitäten durchzuführen (Interviewee 13 2017).

Die Implementierung von Demand-Response in Privathaushalten könnte Auswirkungen auf die Privatsphäre haben. Benötigt werden Hochfrequenzmessungen des Verbrauchs und der Erzeugung

sowie die Verfügbarkeit von flexiblen Lasten in den Haushalten. Sollten diese datenschutzrelevanten Informationen in falsche Hände geraten, hätte eine Verletzung der Vertraulichkeit dieser Informationen auch Auswirkungen auf die Privatsphäre (Interviewee 18 2017).

Ausführliche Informationen zur Debatte um den Datenschutz für das Smart Meter Sicherheitssystem in Deutschland finden sich in Greveler (2016).

b. Dezentrale Energieanlagen und -verteilung

Kompromittierende Kommunikationsverbindungen zu DER-Systemen könnten einem Angreifer den Zugriff auf eine große Anzahl von DER-Instanzen ermöglichen. Diese Auswirkungen können geringfügig sein, wenn sich der Zugriff Dritter nur auf die Überwachung des Zustands des DER beschränkt. Wenn der Drittanbieter jedoch die Möglichkeit hat, betriebliche Sollwerte oder Softwarekonfigurationen zu ändern, können Angriffe auf diese Systeme schwerwiegende Auswirkungen haben, die über ein einzelnes Verteilnetz hinausgehen können (Qi et al. 2016).

Einige zugehörige Fehlerszenarien finden Sie im NESCOR-Katalog (NESCOR 2015). Das Szenario DER.6 veranschaulicht beispielsweise den Fall, dass ein Angreifer die Befehlsfolge von DER kompromittiert, die durch einen Replay-Angriff möglich ist, was zu einem Ungleichgewicht des Netzes und Stromausfällen führt. Im Szenario DER.14 fälscht ein Angreifer DER SCADA-Steuerbefehle, die zu Instabilität der Stromversorgung führen, einschließlich Ausfällen und Energiequalitätsproblemen.

c. Erzeugung und Übertragung

Dateninjektionsangriffe auf SCADA-Systeme oder intelligente elektronische Geräte können zu Systemstörungen führen. Rogue-Protokoll-Befehle können gesendet werden, um Slave-Geräte in einen inoperablen Zustand zu versetzen, Dienste herunterzufahren oder zurückzusetzen. Bestimmte Befehle können an mehrere Geräte gleichzeitig gesendet werden, Denial of Service (DoS), wodurch der Netzwerkverkehr gestoppt wird. Außerdem können bösartige Codes verwendet werden, um Daten aus der Diagnose zu löschen (Lopez et al. 2015; Mo et al. 2012).

Im Falle der "Crashoverride"-Malware, die Schwachstellen in industriellen Kommunikationsprotokollen ausnutzt, beschrieb das Dragos-Team legitime Angriffs- und Wirkungsszenarien, die Folgendes beinhalten: Unterstationen abschalten und ein Inselereignis erzwingen (Dragos Inc. 2017). Im ersten Szenario werden bösartige Steuerbefehle in einer Endlosschleife wirksam an Leistungsschalter in Unterstationen gesendet. Wenn ein Anlagenbediener versucht, einen Schließbefehl auf seinem HMI (Human Machine Interface) zu geben, wird die Sequenzschleife den Schalter weiter öffnen. Diese Schleife, die offene Schalter aufrechterhält, deaktiviert effektiv die Unterstationsleitung(en) und verhindert, dass Anlagenbetreiber die Schalter verwalten und die Leitung(en) wieder mit Strom versorgen. Die Auswirkungen der Abschaltung einer Leitung oder Unterstation hängen von der Systemdynamik, den Leistungsflüssen und anderen Variablen ab. In manchen Fällen kann es nicht sofort wirken, während es in anderen Fällen zu Stromausfällen kommen kann. Da die Zentrale außerdem die Fernsteuerung der Schalter verliert, ist es notwendig, ein Service-Team zur manuellen Bedienung in die Unterstation zu schicken. Dies wird in wenigen Stunden zu Ausfällen führen.

Im zweiten Szenario zielen Angreifer auf eine oder mehrere RTUs, und ein Steuerbefehl wird gesendet, um eine Schleife zu starten, die den Status des Unterbrechers kontinuierlich zwischen Öffnen und Schließen umschaltet. Die Änderung des Schalterstatus führt zu automatisierten Schutzmaßnahmen, um die Unterstation zu isolieren, die zu Netzinstabilitäten führen könnte. Wenn mehrere Unterstationen koordiniert kompromittiert werden, kommt es zu längeren Stromausfällen.

Bewertung der potenziellen Auswirkungen

Die Verwendung unsicherer Kommunikationskanäle beeinträchtigt die Integrität und Verfügbarkeit der Datensicherheitsanforderungen, die sich direkt auf die Stromversorgung auswirken könnten. Eine Beeinträchtigung des Vertrauens in den Schutz der Daten könnte sich auf indirekte Parameter, d.h. die öffentliche Akzeptanz, auswirken.

Die potenziellen Auswirkungen werden unter Zugrundelegung der VA-Methodik als mittel bis hoch angesehen.

Technische, organisatorische und strukturelle Anpassungsoptionen

Sicherheitsmechanismen sollten aufeinander aufbauen, und es sollten mehrere Sicherheitsstufen verwendet werden, um die Sicherheit des Systems zu gewährleisten. Erstens ist die Implementierung von Verschlüsselung (Kryptographie) bei Daten- und Kommunikationskanälen erforderlich, um die Datenintegrität zu gewährleisten und eine unbeabsichtigte Weitergabe von Informationen während der Übertragung zu verhindern. Darüber hinaus ist die Implementierung von Intrusion Detection Systemen (IDS) erforderlich, um eine effektive Sichtbarkeit der Angreiferaktivitäten zu gewährleisten (Interviewee 1 2016; Interviewee 13 2017). Der Vorteil von IDS ist, dass sie damit bekannte Angriffe identifizieren können. Dafür stehen Datenbanken mit Mustern und Signaturen zur Verfügung, die heruntergeladen werden können. Der Nachteil ist jedoch, dass solche Systeme nicht in der Lage sind, unbekannte Angriffe zu erkennen. Dafür bedarf es anderer Ansätze (Interviewee 1 2016).

Grundsätzlich ist die Verwendung von Verschlüsselung nicht immer die richtige Wahl und ein vollständiges Verständnis der Informationsverwaltungsfunktionen, die bei der Anwendung einer übergreifenden Verschlüsselung verloren gehen, sollte vorher erfolgen (NIST 2014). Wie Experten aus der IT- und Automatisierungsbranche erwähnten, könnte die Datenverschlüsselung in industriellen Steuerungsnetzen die Latenz erhöhen. Einiger Hersteller bieten Verschlüsselungsgeräte an, die vor dem ICS installiert werden können, z.B. SPS, und damit die Kommunikation verschlüsseln bzw. entschlüsseln können. Andere Anbieter entwickeln spezielle Geräte für die sichere Kommunikation zwischen ihren Geräten. Weitere Lösungen sollten in Richtung Verschlüsselung direkt auf industriellen Steuerungen gehen. Quantenverschlüsselung ist eine neuartige Lösung, die insbesondere für die Gewährleistung der Vertraulichkeit entwickelt wurde. Bei industriellen Netzwerke spielt aber die Verfügbarkeit eine sehr wichtigste Rolle, sodass dieser Ansatz erstmal zeigen muss, dass er keine zusätzliche Latenzzeit und Einschränkung der Systemleistung mit sich bringt (Interviewee 15 2017).

Wenn es unpraktisch ist, alle Messungen zu verschlüsseln, ist es wichtig, die angegriffenen Messungen zu erkennen und zu isolieren. Eine effektive Angriffsisolierung ermöglicht es, die Schadenskontrolle (z.B. das Entfernen angegriffener Messungen zur Zustandsabschätzung) rechtzeitig durchzuführen, bevor der Angriff zu einem Ereignis mit erheblichen Folgen führen kann (Teixeira et al. 2015).

Anpassungswissen und -bereitschaft

Bei älteren ICS-Kommunikationsprotokollen gibt es bereits Standards zur Erhöhung der Sicherheit. Zum Beispiel die Norm IEC 62351, die Sicherheitsverbesserungen für Protokolle wie IEC 60870-5-104 und IEC 60870-5-101 vorsieht, aber die Hersteller implementieren diese nicht und stellen in der Regel nur grundlegende Funktionalitäten zur Verfügung, so dass Verteilnetzbetreiber keine sichere Umgebung schaffen können (Interviewee 1 2016) (Siehe Kapitel 4.2.4.1 für weitere Informationen über das Fehlen einer effektiven Implementierung von Sicherheitsstandards als Vulnerabilität).

Experten aus der IT- und Automatisierungsbranche weisen zudem darauf hin, dass nach ihrer Erfahrung Kunden oder Unternehmen der Branche in der Regel keine moderne Technologie, sondern bereits erprobte und robuste Lösungen wünschten (Interviewee 15 2017).

Da ein großer Teil der heutigen Stromnetzeinrichtungen veraltet ist, kann die Datenverschlüsselung aufgrund des entsprechenden notwendigen Aktualisierungsbedarfs der Anlagen kostspielig werden. Daher ist es wichtig zu ermitteln, welche Messungen verschlüsselt werden sollten, um den Nutzen der Schutzmittel zu maximieren (Teixeira et al. 2015).

Bewertung der Anpassungskapazität

Unter Berücksichtigung der Tatsache, dass es bereits Anpassungsmechanismen zur Verbesserung der Kommunikationssicherheit gibt, aber die Bereitschaft zu deren Anwendung begrenzt sein könnte, wird die Anpassungsfähigkeit als mittel eingestuft.

Vulnerabilität

In Anbetracht der hohen potenziellen Auswirkungen und der mittleren Anpassungsfähigkeit wird in diesem Fall die Anfälligkeit durch unsichere Kommunikation als hoch eingestuft.

4.2.1.2 Unsichere Endpunkte

In der Netzwerksicherheit ist ein Endpunkt jedes Gerät, welches sich mit dem Netzwerk verbindet, das reicht von festen Funktionsservern und Desktops bis hin zu jedem beliebigen Gerät, welches netzwerkfähig ist. Endpunkte in verschiedenen Zonen und Domänen des SG-Architekturmodells kennzeichnen ihre eigenen Herausforderungen.

Um die Verwundbarkeit durch unsichere Endpunkte zu bewerten, wurden die Domänen des Energiesystems in drei Cluster eingeteilt: a) Verbrauch, b) verteilte Energieressourcen, c) Erzeugung, Übertragung und Verteilung.

Exposition und Sensitivität

a. Verbrauch

Endgeräte beim Kunden (z.B. Hausautomationssystem, IoT-Geräte, Mobiltelefone, Laptops) sind nicht durch Cyber-Sicherheitsaspekte geregelt und werden mit schlechten Sicherheitsmerkmalen eingesetzt. Wenn daher bekannte Schwachstellen dieser Geräte ausgenutzt werden, könnten sie als bösartige Einstiegspunkte für weitere Angriffe auf die Strominfrastruktur genutzt werden. Diese Geräte verfügen nicht über Sicherheitsfunktionen in Bezug auf die sichere Schlüsselverwaltung

und die sichere Speicherung von Berechtigungsnachweisen. Außerdem gibt es ein Problem bei der Authentifizierung, da die Geräte in vielen Fällen keine ID haben und keine guten Zugangsdaten zur Authentifizierung. Außerdem gibt es nicht genügend Möglichkeiten, um das Patch- und Software-Management der Geräte anzusprechen. Der Zugriff auf das Netzwerk ist ebenfalls eingeschränkt (Interviewee 5 2016; Interviewee 14 2017; Interviewee 18 2017).

Darüber hinaus macht es der Mangel an Software-Integritätsprüfung oder signierter Software in IoT-Geräten einfach, Malware auf diese Geräte hochzuladen, von wo aus ein Angriff gestartet werden könnte, um Denial-of-Service-Angriffe durchzuführen (Interviewee 5 2016).

Wenn die Geräte mehr verteilt sind, gibt es auch ein Problem der Skalierbarkeit der Umsetzung von Sicherheitsmaßnahmen, um sie richtig zu sichern, weil es erforderlich ist, nicht nur wenige Endpunkte zu überwachen, zu warten und zu aktualisieren, sondern Tausende von ihnen (Interviewee 5 2016). In diesem Sinne stellt die Elektromobilität eine zukünftige große Angriffsfläche auf der Kundenseite dar (Experten-Workshop 2 2017).

Nach der deutschen Verordnung müssen Smart Meter sehr strenge Sicherheitsauflagen erfüllen, die darauf abzielen, das Sicherheitsniveau der Zählerinfrastruktur zu erhöhen, es gibt aber auch andere Dienste oder Geräte mit umfangreichen Kontrollmöglichkeiten (z.B. Smartphone-Anwendungen), die derzeit nicht geregelt sind (Experten-Workshop 2 2017).

b. Dezentrale Energieanlagen

Ein komplexeres Problem, das von einem Experten angesprochen wird, besteht dann, wenn Endverbraucher auch Prosumenten sind, d.h. Energieerzeuger, die sowohl selbst erzeugten als auch vom Netz gelieferten Strom verbrauchen. Bisher wurden in einem klassischen Stromnetz Erzeugungs-, Übertragungs- und Verteilnetze von Unternehmen betrieben und als isolierte Systeme behandelt. Der Anschluss von dezentralen Energieressourcen-Systemen an das Netz, die von Endkunden gewartet und betrieben werden, überbrückt jedoch die Luftspalte, die bisher ein gewisses Maß an Cybersicherheit ermöglichte. Das Problem entsteht, wenn diese verteilten Systeme mit unsicheren Netzwerken oder dem Internet verbunden sind. Folglich muss davon ausgegangen werden, dass das System an potenziell unsichere Stellen angeschlossen wird, weshalb herkömmliche Sicherheitsmaßnahmen wie Authentifizierung oder Autorisierung nicht ausreichen werden (Interviewee 14 2017).

Kleine DER-Systeme haben keine verbindlichen Vorschriften zur Absicherung dieser Systeme und stellen daher einen potenziellen Punkt für böswillige Eingriffe dar (Interviewee 2 2016).

c. Erzeugung, Übertragung und Verteilung

Endgeräte an den Stationen und im Feld werden oft an entfernten Standorten installiert, ohne dass Bedienungs- oder Wartungspersonal vorhanden ist. Wenn also Endgeräte an diesen Standorten nicht über angemessene Sicherheitsmaßnahmen verfügen, könnte ein potenzieller Angreifer die Zeit haben, die unsicheren Geräte (Computer oder Netzwerkgeräte) zu gefährden, in das Netzwerk einzudringen und von dort aus einen Angriff zu starten (Interviewee 5 2016).

Auch wenn sich die Endpunkte innerhalb von Industrieanlagen (z. B. Kraftwerke, Umspannwerke) befinden, die normalerweise geschlossene Standorte sind, haben Experten für IT-Sicherheit in der Industrieautomation darauf hingewiesen, dass die Punkte, an denen Benutzer mit dem System in-

teragieren können, ebenfalls Schwachstellen darstellen, da Benutzer oder Bediener Konfigurationsparameter oder Steuerbefehle ändern oder manipulieren können. RTUs und PLCs sind anfällig für diese Art von Störungen (Interviewee 15 2017).

Darüber hinaus können Fernzugriffsmöglichkeiten von Systemen oder Geräten auch potenziell schädliche Eindringlinge darstellen. Der Fernzugriff ist nicht per se unsicher, denn wenn es einen sicheren Kanal mit entsprechenden Maßnahmen gibt, ist es möglich, Angriffe wie das Abhören oder Man-in-the-Middle zu erkennen. Ein Problem könnte jedoch auftreten, wenn einer der Endpunkte potenziell unsicher ist (Interviewee 14 2017). Werden beispielsweise Laptops mit Viren oder Malware infiziert oder gleichzeitig mit unsicheren Netzwerken (z.B. dem Internet) verbunden, können diese Endpunkte das System beeinträchtigen (Experten-Workshop 1 2016).

Angriffsmechanismen und Störereignisse

Wenn das Endgerät kompromittiert ist, muss der Gegner die Kryptographie nicht unterbrechen, um die Daten zu lesen oder zu manipulieren. In den verschiedenen Domänen können unterschiedliche Angriffsmechanismen durchgeführt werden:

a. Endverbrauch

Angreifer könnten bösartigen Codes oder Malware auf schlecht gesicherte Automatisierungsgeräte beim Kunden hochladen, um diese zu kontrollieren und Denial-of-Service-Angriffe gegen das Stromnetz oder andere Infrastrukturen wie Banksysteme zu starten (Interviewee 1 2016; Interviewee 5 2016).

Smart Meter, die sich beim Kunden befinden, können Gegenstand von physischen Manipulationen sein, obwohl diese Geräte derzeit robust sind. Diese Angriffe sind eher spezialisiert auf Informationsbeschaffung, z. B. Seitenkanalangriffe (Interviewee 18 2017). Eine ergänzende Bedrohungsanalyse des Smart Meter Gateways wurde im Rahmen des Forschungsprojekts SPIDER durchgeführt, wo zusätzliche Bedrohungen entdeckt wurden, von denen die meisten in die Manipulation und Denial-of-Service-Aspekte fallen, die die Integrität und Verfügbarkeitssicherheit beeinträchtigen, siehe (Becker 2013) zitiert in (Detken et al. 2014a).

b. Dezentrale Energieanlagen

Ein weiterer möglicher Angriffsmechanismus kann die Datenmanipulation auf DER-Systemkomponenten sein (Interviewee 2 2016). DER benötigt eine Vielzahl von digitalen Geräten, um ihren Betrieb zu steuern und Verbrauchern und Versorgungsunternehmen Informationen über ihren Betrieb zur Verfügung zu stellen. Die meisten DER enthalten intelligente Wechselrichter und DER-Controller; andere können auch Batterie-Controller und sogar Elektrofahrzeug-Controller (EV-Controller) enthalten. Wenn Angreifer direkt auf diese Systeme zugreifen können, sind sie in der Lage, jede ihrer Kontrollfunktionen zu manipulieren oder Statusinformationen an die Versorgungsunternehmen oder Eigentümer zu fälschen (Qi et al. 2016).

c. Erzeugung, Übertragung und Verteilung

Einige Angriffsmechanismen, die gegen ICS-Endpunkte in Stations- und Feldzonen des Stromnetzes auftreten können, sind meist auf menschliches Versagen oder Fehlkonfiguration zurückzuführen. Auch absichtliche Manipulationen von Betriebsparametern können vorkommen. Geräte mit

drahtlosen Schnittstellen könnten ein weiterer Angriffsvektor sein, der sich auf den Betrieb des elektrischen Systems ausbreiten könnte (Interviewee 18 2017).

USB-Sticks, die an das Netzwerk angeschlossen sind, können auch als Einstiegspunkt für die Installation von Malware verwendet werden (Interviewee 1 2016; Interviewee 18 2017). Während des Wartungsdienstes (lokal oder remote) können Techniker über einen privaten Laptop eine Verbindung herstellen, die mit Viren oder anderer Malware infiziert sein kann, die sich in das industrielle Netzwerk verbreiten kann (Experten-Workshop 1 2016).

Der Fernzugriff ist nicht per se unsicher, denn wenn es einen sicheren Kanal mit entsprechenden Maßnahmen gibt, ist es möglich, Angriffe wie Lauschangriffe oder Man-in-the-Middle zu erkennen. Das Problem könnte jedoch auftreten, wenn einer der Endpunkte potenziell unsicher ist (Interviewee 14 2017).

Ähnlich wie bei den Angriffsszenarien beim Kunden können schlecht abgesicherte industrielle Steuerungssysteme, die sich beispielsweise in einer mit dem Internet verbundenen Umspannstation ohne Firewall oder mit einer falsch konfigurierten Firewall befinden, als Teil einer Botnet-Kampagne gefährdet werden, was zu Denial-of-Service-Angriffen führt. Ein weiteres Angriffsszenario könnte sein, dass diese industriellen Kontrollsysteme verwendet werden, um kryptographische Schlüssel zu knacken oder um Bitcoins zu gewinnen, genau wie der Fall von Netzwerkdruckern. Dieses Szenario wird jedoch von einigen IT-Sicherheitsexperten als unwahrscheinlich angesehen (Interviewee 1 2016).

Datenmanipulationen können auch in den oberen Zonen des SGAM, z.B. Betrieb, oder Unternehmen (siehe Abb. 4.3) gegen Datenbankserver (z.B. SCADA Historian Server) durchgeführt werden, wo Daten konsolidiert und freigegeben werden. Qualitätsbits oder die Daten selbst könnten manipuliert werden und somit die im HMI in der Zentrale angezeigten Informationen (z.B. Frequenz) von dem, was im Feld geschieht, abweichen (Interviewee 4 2016).

Potenzielle Auswirkungen auf Systemleistung

a. Endverbrauch

Kompromittierende IoT-Geräte könnten für Lösegeldangriffe gegen Benutzer verwendet werden. In einem zukünftigen Szenario, wenn jemand die Smart Home-Umgebung hackt, könnte der Angreifer einen Geldbetrag verlangen, um die Steuerung von Beleuchtung, Heizung, Autobatterieladung usw. freizugeben (Interviewee 18 2017). Darüber hinaus könnte als indirekte potenzielle Auswirkung die öffentliche Akzeptanz neuer Technologien durch alle Sicherheitsfragen im Zusammenhang mit IoT in der Konsumwelt beeinträchtigt und in den Medien berichtet werden (Interviewee 5 2016).

Smart Meter Gateways, die sich beim Kunden befinden, können manipuliert werden, um den Stromverbrauch zu reduzieren (Interviewee 1 2016; Interviewee 6 2016; Interviewee 18 2017; Interviewee 19 2017). Dies wäre jedoch bedeutungslos, wenn der Angreifer nur ein einziges Gateway treffen könnte. Für einen Angreifer wäre es interessant, mehrere Gateways gleichzeitig durch Trojaner oder andere Malware abzuschalten, um eine größere Wirkung zu erzielen (Interviewee 19 2017). Eine noch größere Wirkung könnte erzielt werden, wenn ein Bedrohungsagent in der Lage ist, die IT-Infrastruktur des Smart Meter Gateway-Administrators zu kompromittieren, um den sicheren Kommunikationskanal zu nutzen und Millionen von Gateways anzugreifen, die mit dem SMGA verbunden werden könnten (Interviewee 19 2017).

Hinsichtlich der Funktion des SMGW, den Haushalt vom Stromnetz zu trennen, erwähnte Greveler, U., in (Greveler 2016), dass das Schutzprofil für das Gateway außer den steuerbaren Verbrauchern keine Funktion bietet, die den Haushalt vom Stromnetz trennt. Eine solche Funktion birgt ein besonderes Risiko, da ein erfolgreicher Angriff auf das Gateway sowohl auf den einzelnen Verbraucher (Funktionsausfall fast aller elektrischen Geräte) als auch auf das Stromnetz (mögliche kaskadierende Abschaltung der Netze bei plötzlicher Abschaltung vieler Haushalte) erhebliche Auswirkungen hätte.

b. Dezentrale Energieanlagen

Angriffe, die eine direkte Kontrolle über die intelligenten Wechselrichter haben, können besonders gefährlich sein, da der Angriff den Betrieb des Geräts abhängig vom Zustand des Netzes intelligent beeinflussen kann. Dies könnte dem Angreifer helfen, unerwünschte Gitterzustände zu verstärken (Qi et al. 2016). Als spekulatives Ausfallszenario nannte ein Experte, dass im Falle, dass ein Bedrohungsagent genügend dezentrale Stromerzeugung wie PV-Anlagen manipulieren und gleichzeitig abschalten könnte, dies zu Netzinstabilität und einigen möglichen Stromausfällen führen könnte, da das Netz selbst nicht in der Lage wäre, den Verlust zu kompensieren. Im Falle des deutschen Netzes gibt es derzeit eine Einspeisung von fast 20 GW auf der niedrigsten Netzspannungsebene und die Netzbetreiber in Europa können nur 3 GW kompensieren. An einem sonnigen Sommertag, wenn PV-Anlagen wahrscheinlich 15 GW auf dieser Schicht speisen und ein Angreifer einen Weg findet, 10 GW zu schalten, könnte dies zu einem großen Blackout führen (Interviewee 17 2017). Wie bereits erwähnt, handelt es sich um ein spekulatives Versagensszenario, das mehr quantitative Analysen erfordert, um die potenziellen Auswirkungen zu bewerten.

c. Erzeugung, Übertragung und Verteilung

An den Endpunkten der Station und der Feld-Zone sind die Endpunkte, wie bereits erwähnt, potenziellen Bedrohungen ausgesetzt, es wird jedoch mehr Aufwand und ein verteilter Angriff erforderlich sein, um einen größeren Einfluss auf das Gesamtsystem zu haben. Je höher die Ebene der Steuerungsarchitektur, desto kritischer wird sie, da die Informationen auf einer bestimmten Ebene aus allen darunterliegenden Schichten gesammelt werden. Auf der untersten Ebene, d.h. in Stations- und Feldzonen (siehe Abb. 4.3), kann eine Manipulation der Betriebsgrenzwerte an Industrieanlagen daher nicht zu großen Auswirkungen auf das Gesamtsystem führen, sondern zu anderen Auswirkungen, wie z.B. auf die körperliche Unversehrtheit der Anlage. Wenn z.B. der Parameter der maximalen Arbeitsbelastung geändert wird, wodurch das Gerät gezwungen wird, über die physikalischen Grenzen hinaus zu arbeiten, könnte dies zu physischen Schäden führen, die Ausfälle verursachen, die sich auf die Leistung des spezifischen Systems auswirken könnten (Interviewee 1 2016; Interviewee 4 2016; Interviewee 15 2017).

In einem größeren Angriffsszenario, wenn eine Trafostation kompromittiert und abgeschaltet wird, führt dies zu einem Stromausfall auf dem von dieser Trafostation abgedeckten Gebiet, z.B. einer Straße oder einem Nachbarschaftsblock. Darüber hinaus könnte sich ein solcher Angriff auf die Gesamtqualität der Energieverteilung in Deutschland auswirken, was sich indirekt auf die Energieversorgungsunternehmen auswirken könnte, da sie nach der Benchmark bezahlt werden und diese Ausfälle für sie eine wirtschaftliche Auswirkung haben könnten. Um einen größeren Ausfall zu erreichen, müssten viele Umspannwerke gleichzeitig kompromittiert werden (Interviewee 1 2016).

Mögliche Auswirkungen: Qualitäts- und Quantitätskriterien betroffen Mittel bis hoch

Bewertung der potenziellen Auswirkungen

Nach den oben genannten potenziellen Auswirkungen können die Quantitäts- und Qualitätskriterien durch verschiedene Angriffsmechanismen beeinflusst werden. Die Wirkung auf die Qualitätskriterien ist höher, wenn gleichzeitig verteilte Angriffe durchgeführt werden. Auch die öffentliche Akzeptanz wäre beeinträchtigt.

Daher wird die potenzielle Wirkung als mittel bis hoch eingestuft.

Technische, organisatorische und strukturelle Anpassungsoptionen

Generell ist die Implementierung von End-to-End-Sicherheit eine Herausforderung. Wie ein IT-Sicherheitsexperte sagte: "Es ist wahrscheinlich nicht realistisch oder naiv zu glauben, dass wir alle Endpunkte sichern können, aber wir müssen sicherstellen, dass wir den Sicherheitsverstoß schnell herausfinden". Darüber hinaus ist es wichtig, Patch-Management-Prozesse einschließlich Tests zu etablieren, um Fehler in der Software und Hardware zu adressieren. Die Netzwerksegmentierung und -überwachung ist ebenfalls erforderlich, um Angriffe zu verhindern und sie zu isolieren (Interviewee 5 2016).

Spezifische Anpassungsmechanismen für jedes Cluster werden wie folgt veranschaulicht:

a. Endverbrauch

Wenn das System stärker verteilt ist, werden mehr Sicherheitsmerkmale benötigt und für die Implementierung auf Geräten beim Kunden, z.B. IoT-Geräte, werden Richtlinien und Implementierungshinweise benötigt, um Hersteller zu unterstützen. Open Source Software würde es ermöglichen, Unterstützung von der Sicherheits-Community zu erhalten (Interviewee 5 2016).

Wie bereits erwähnt, kann jedoch keine hundertprozentige Sicherheit gewährleistet werden, daher wäre es notwendig, diese verteilten Geräte als nicht vertrauenswürdig zu betrachten und ihre Eingaben zu verifizieren, sie sollten mit statistischen Tools analysiert werden, um festzustellen, ob diese Geräte manipulierte oder bösartige Informationen senden. Beispielsweise könnte es erforderlich sein, die Messungen der beim Kunden installierten intelligenten Zähler zu analysieren, um sicherzustellen, dass sie das Netz nicht böswillig beeinträchtigen. Diese Analyse könnte jedoch einige Auswirkungen auf die Privatsphäre haben. Es gibt Möglichkeiten, Messmethoden auf der Ebene der Nachbarschaft statt auf der Ebene der Haushalte zu aggregieren, aber solche Techniken können geheime Sharing-Systeme oder andere kryptographische Protokolle oder Lösungen beinhalten. Daher ist es notwendig, diese Techniken einzusetzen und ein Gleichgewicht zwischen der wahrgenommenen Granularität des Dienstprogramms und der Privatsphäre des Kunden sowie der Gesamtsicherheit des Systems zu finden (Interviewee 13 2017).

Um Angriffe von intelligenten Zählern zu verhindern, sollten ihre Fähigkeiten auf die Auslese- und Kontrollfunktionalitäten beschränkt sein, damit sie weniger Angriffen ausgesetzt sind (Experten-Workshop 2 2017). Außerdem müssten, wie oben erwähnt, viele Smart Meter oder Smart Meter Gateways kompromittiert werden, um eine größere Wirkung zu erzielen. Da ein SMGA an etwa eine Million Gateways angeschlossen werden könnte, ist es dringend erforderlich, dass das SMGA zertifiziert werden muss, was derzeit in Deutschland gesetzlich vorgeschrieben ist (Interviewee 19 2017).

Um die SMGW-Sicherheit zu erhöhen, schlägt die von Detken K. und Kollegen (Detken et al. 2014a; Detken et al. 2014b) entwickelte Arbeit die Verwendung relevanter Aspekte des Trusted Computing-Ansatzes vor, wie zum Beispiel: Messung und Überprüfung der Integrität mit Trusted Network Connect (TNC). Dieses Sicherheitskonzept entspricht den Sicherheitsanforderungen, indem es eine Vertrauenskette generiert. Die Integritätsprüfung wird zunächst beim Booten durchgeführt, wobei der sichere Bootvorgang und der Aufbau der Vertrauenskette einschließlich der TNC-Software genutzt werden. Die Integritätsprüfung erfolgt ebenfalls zur Laufzeit mit Hilfe der (zum Bootzeitpunkt) verifizierten TNC-Software. Die Messwerte von Hard- und Softwarekomponenten werden manipulationssicher im Dateisystem gespeichert. Dies führt zu einer erweiterten Gateway-Sicherheit, die sich auf alle angrenzenden Komponenten auswirkt.

b. Dezentrale Energieanlagen

Im Hinblick auf die Verbesserung der Sicherheit von DER-Systemen haben Experten erwähnt, dass die in Deutschland kurz vor der Implementierung stehende Smart Metering-Infrastruktur auch zur Absicherung dieser Systeme genutzt werden könnte. Dies ist derzeit nicht der Zweck und die Entwicklung weiterer Regelungen wäre notwendig (Interviewee 17 2017).

c. Erzeugung, Übertragung und Verteilung

Präventionsmechanismen wie z.B. schlechte Datenerkennungsschemata oder Datenfilter können verwendet werden. Normalerweise werden Steuerungssysteme unter Berücksichtigung der Tatsache entwickelt, dass einige Daten aus dem Feld fehlerhaft oder falsch sein könnten, daher wird der benötigte Datensatz überschätzt, wodurch die Möglichkeit besteht, falsche Daten zu verwerfen. Die Umsetzung der genannten Nachweisverfahren, die auf physikalischen Modellen (z.B. Strom oder Spannung, durch das Ohm'sche und Kirchhoff'sche Gesetz) beruhen, wird eine weitere Validierung von Daten aus dem Feld ermöglichen (Interviewee 4 2016; Interviewee 12 2017).

Die Implementierung dieses Erkennungsmechanismus wäre auf die verfügbare Datenmenge beschränkt. Experten waren sich einig, dass es auf der Übertragungsebene mehr Daten im Vergleich zur Verteilungsebene gibt, wo es derzeit nicht viele Messgeräte gibt, die eine Herausforderung für die Umsetzung dieser Nachweisverfahren darstellen (Interviewee 12 2017).

Darüber hinaus wird die Implementierung besserer Analyse- und Erkennungsmöglichkeiten auf industriellen Routern und Switches die Sicherheit von industriellen Steuerungssystemen verbessern, um Angriffe von Feldgeräten erkennen und verhindern zu können. Allerdings haben industrielle Netzwerke derzeit nur grundlegende Funktionalitäten, daher sollten Upgrades oder neue Netzwerkgeräte in Betracht gezogen werden (Interviewee 15 2017).

Bewertung der Anpassungsfähigkeit

Einige Anpassungsstrategien für die Prävention sind gegeben, deren Umsetzung wird jedoch begrenzt sein, daher wird die Anpassungsfähigkeit als mittel eingestuft.

Vulnerabilität

Nach der VA-Methodik folgt aus einer Kombination aus hoher potenzieller Wirkung und mittlerer Anpassungskapazität eine hohe Vulnerabilität.

4.2.1.3 Sonstige technologiebezogene Bedingungen

Die folgenden weiteren technologiebezogenen Bedingungen wurden durch die Interviewanalyse identifiziert. Eine umfassende Schwachstellenanalyse war jedoch aus Zeitgründen nicht möglich.

- Unsichere Schnittstelle zwischen Komponenten verschiedener Hersteller oder zwischen verschiedenen Systemen
- Software und Firmware erlauben unbefugte Modifikationen
- Systeme, die in Webservices laufen, wie z.B. virtuelle Kraftwerke

4.2.2 Organisation der Sicherheitsrichtlinien und -verfahren

4.2.2.1 Fehlende interdisziplinäre IT-OT Kenntnisse

Exposition und Sensitivität

Mit der zunehmenden Komplexität und Interdependenzen zwischen IT- und OT (Operation Technology)-Infrastruktur von Energiesystemen hat sich das notwendige Wissen zur Bewältigung der neuen cyberphysikalischen Systeme verändert. Verbindungen zwischen beiden Infrastrukturen müssen auf spezifische Weise untersucht und geschützt werden, was für Experten mit Kenntnissen nur in diesen Bereichen schwierig ist. Interdisziplinäres Wissen fehlt in den meisten Fällen und daher ist es schwierig, die neuen Systeme als Ganzes richtig zu verstehen, zu konzipieren, umzusetzen und zu betreiben (Interviewee 1 2016; Interviewee 2 2016; Interviewee 5 2016).

Beteiligt sind verschiedene Akteure, nämlich traditionelle große Rohstoffanbieter, Verteilnetzbetreiber, typische Verbraucher, aufstrebende Kleinproduzenten, Messdienstleister, Entwickler und Anbieter von IT-Komponenten sowie verschiedene Regulierungs- und Standardisierungsinstitutionen. Die meisten dieser Parteien haben keinen starken Hintergrund in der IT-Sicherheit (von Oheimb 2013). Darüber hinaus kann es bei Ausschreibungen zu Fehlern bei der Beschreibung der Sicherheitsanforderungen kommen, so dass die implementierten Systeme die Mindestanforderungen nicht erfüllen können (Interviewee 18 2017).

Experten einer Domäne können die Auswirkungen und Konsequenzen ihrer Entscheidungen für andere Domänen und Teile des Systems einfach nicht vorhersehen. Betrachtet die IT-Abteilung beispielsweise Server für den OT-Betrieb (z.B. HMI, Historian Server) als Teil der IT-Infrastruktur, können normale IT-Sicherheitsmaßnahmen (z.B. tägliche Antiviren-Updates) Auswirkungen auf den operativen Teil des Systems haben, die sich auf die Verfügbarkeit oder Performance des Systems auswirken (Interviewee 4 2016). Andererseits wird ein erheblicher Teil des OT-Netzwerks über IT-Geräte und -Systeme angeschlossen, gewartet und betrieben. Normalerweise werden diese Anlagen von ICS-Betreibern und -Ingenieuren und nicht von erfahrenen IT-Experten gewartet, was zu häufigen Fehlern bei Wartung, Konfiguration und mangelnder Absicherung führen kann (Bodungen et al. 2017).

Darüber hinaus stellt die laufende Implementierung von IKT in das Strombetriebssystem neue Herausforderungen an den Systembetrieb. Da mehr IKT-Funktionalitäten in elektrische Systeme integriert sind, würde das Betriebspersonal mehr Schulung benötigen, um mit cyber-physikalischen Ereignissen umgehen zu können. Experten sagen, dass diese neuen Systeme qualifiziertes Perso-

nal benötigen, das nicht nur für den Betrieb der bestehenden elektrotechnischen Anlagenteile, sondern auch für die Bedienung der neuen IT-Sicherheitssysteme, z.B. Intrusion/Anomalie-Erkennungssysteme, ausgebildet ist. Das Personal im Betrieb kann nicht innerhalb kurzer Zeit zu IT-Experten umgeschult werden, um auf IT-Fehler richtig reagieren zu können (Interviewee 1 2016).

Einerseits integrieren Betriebszentralen in der Regel keine Störungen oder Alarme aus der IT-Infrastruktur, so dass der Betreiber nicht unterscheiden kann, woher der Fehler kommt (Interviewee 1 2016; Interviewee 18 2017). Andererseits, wenn die IT-Abteilung die Anomalie-Erkennungssysteme und IDS verwaltet, ist unklar, wie eine Störung durch die IT an die Einsatzzentrale übertragen werden könnte, um darauf zu reagieren (Interviewee 18 2017).

Angriffsmechanismen und Störereignisse

Der Mangel an Experten sowohl im IT- als auch im OT-Bereich eröffnet Angreifern viele Möglichkeiten, das System in mehrfacher Hinsicht zu schädigen. Unterschiedliche Ansätze zur Absicherung von ICS aus IT- und OT-Maßnahmen schaffen Sicherheitslücken, wie z.B.: unsachgemäße Netzwerksegmentierung, unsachgemäßes Änderungs- und Konfigurationsmanagement, schlechte lokale/ferne Zugriffskontrolle, schwache Generierung, Verwendung und Schutz von Passwörtern, etc.

Wenn das System aufgrund mangelnder Kenntnisse über anfällige Teile des Systems nicht richtig ausgelegt ist, kann eine unsachgemäße Überarbeitung neu hinzugekommener Software und Firmware zu Problemen mit der Systemstabilität führen. Unsachgemäßes Patch-Management und die Implementierung von IT-Sicherheitsmaßnahmen können dem System schaden, da das gesamte Systemdesign zu komplex wird und Systeme anfällig für Angriffe, Sicherheitslücken oder Fehler bei der Entwicklung und Implementierung von Sicherheitsmaßnahmen werden, die von Angreifern genutzt werden können, um das System zu gefährden.

Ein Angriffsszenario könnte auch den Mangel an IT-OT-Know-how der Betreiber nutzen, wenn Angreifer mit Fehlern und Alarmsignalen die nicht-interdisziplinären Fachkräfte verwirren und zu einem Verlust des Überblicks über das System führen könnten. Kritische Fehler, Steuerungsfehler und falsche Steuerbefehle können dann zu physischen Schäden am System führen (Interviewee 4 2016).

Potenzielle Auswirkungen auf Systemleistung

Die Implementierung unangemessener Sicherheitsmaßnahmen für Cyber-Infrastrukturanlagen könnte unbeabsichtigte Folgen für die physische Infrastruktur haben, die Auswirkungen auf die Systemleistung und -stabilität haben könnten.

Der Mangel an Personal mit Fachkenntnissen sowohl im IT- als auch im OT-Bereich wird den Betrieb des Systems beeinträchtigen. Wenn Vorfälle oder Ereignisse aus der IT im Zusammenhang mit OT auftreten, wäre es nicht möglich, darauf zu reagieren. Bediener ohne entsprechende Schulung können nicht zwischen Fehlermeldungen, die auf technische Störungen oder Naturgefahren zurückzuführen sind, und solchen, die auf einen gezielten Angriff zurückzuführen sind, unterscheiden. Wenn sie das System nicht richtig und dem tatsächlichen Problem entsprechend verwalten können, kann die Leistung des Systems beeinträchtigt werden (Interviewee 4 2016).

Bewertung der potenziellen Auswirkungen

Die Implementierung ungeeigneter Sicherheitsmaßnahmen aufgrund fehlender interdisziplinärer Kenntnisse könnte die Datenverfügbarkeit beeinträchtigen, was sich direkt auf die technischen Parameter auswirken könnte. Die Ausnutzung von Sicherheitslücken kann auch zu Systemausfällen und Stromausfällen führen. Die potenziellen Auswirkungen werden gemäß der VA-Methodik als mittel bis hoch eingestuft.

Technische, organisatorische und strukturelle Anpassungsoptionen

Als Anpassungsstrategien fordern Experten mehr Fachwissen zwischen IT und OT, um diesen Sektoren zu helfen, sich gegenseitig zu verstehen und Konfigurationsfehler oder die Implementierung ungeeigneter Sicherheitsmaßnahmen zu vermeiden (Interviewee 13 2017). Mit mehr Expertise in Querschnitts- und Querschnittsbereichen kann die Industrie zu einem besseren Verständnis ihrer eigenen Komplexität und zur Entwicklung einer ganzheitlichen Sicht auf die Systemarchitektur ausgebildet werden (Interviewee 6 2016; Interviewee 17 2017). Diese Ansicht würde sich auf die Verbindungen und Interaktionen zwischen verschiedenen Komponenten und Domänen konzentrieren.

Mit mehr Querschnittskooperationen können bessere Sicherheitsmessungen und Systemdesigns entwickelt werden, die der Komplexität und Interdependenz zwischen IT und OT Rechnung tragen und, was noch wichtiger ist, den kritischen betrieblichen Anforderungen, nämlich Timing und Verfügbarkeit. Die Definition und Bewertung der Sicherheitsverantwortlichkeiten von der Entwicklung bis zum Betrieb wird dazu beitragen, spezifische Anforderungen zu erfüllen (Interviewee 9 2017).

Eine Konsolidierung der bestehenden Leitlinien und deren Aufteilung auf verschiedene Bereiche könnte hilfreich sein, um Leitlinien für eine breitere Nutzung innerhalb der relevanten Bereiche und für verschiedene am System beteiligte Akteure vorzubereiten (Interviewee 18 2017).

Nur geschulte und erfahrene Bediener sind in der Lage, durch spezifische Fehler zu verstehen und deren Auswirkungen abzuschätzen. Sie reagieren entsprechend und können das System auch im Fehlerfall bedienen, während unsachgemäß geschultes Bedienpersonal Schäden an Komponenten riskieren kann (Interviewee 4 2016). Außerdem sollten sie in Teams von IT- und OT-Experten arbeiten, um besser auf Systemausfälle jeglicher Art reagieren zu können (Interviewee 19 2017).

Aus- und Weiterbildungsprogramme zur Erhöhung des interdisziplinären Wissens der bestehenden Mitarbeiter oder zur Rekrutierung von Fachkräften könnten durch die damit verbundenen Kosten behindert werden (Interviewee 9 2017).

Bewertung der Anpassungskapazität

Unter Berücksichtigung der Tatsache, dass es bereits Anpassungsmechanismen gibt, aber die Bereitschaft zu deren Anwendung begrenzt sein könnte, wird die Anpassungskapazität als mittel eingestuft.

Vulnerabilität

In Anbetracht der hohen potenziellen Auswirkungen und der mittleren Anpassungsfähigkeit wird in diesem Fall die Vulnerabilität durch unsichere Kommunikation als hoch eingestuft.

4.2.2.2 Unsachgemäße Verwaltung von Sicherheitspatches

Exposition und Sensitivität

In einigen Fällen wird die Software nicht regelmäßig auf ihre Aktualität überprüft. Die Folgen eines unsachgemäßen Security-Patch-Managements in den Standard-IT-Netzwerken wurden bei den jüngsten globalen Cyber-Attacken wie 'WannaCry' deutlich. Dieser Angriff würde vermieden oder abgeschwächt, wenn eine angemessene Implementierung der verfügbaren Sicherheitspatches von Unternehmens- und Regierungs-IT-Abteilungen durchgeführt und mehr als 10 Jahre alte Betriebssysteme aktualisiert worden wären.

Experten waren sich einig, dass Systeme, die mit dem Internet verbunden sind, mindestens wöchentlich oder sogar täglich Sicherheits-Patches benötigen, um ihr Sicherheitsniveau aufrechtzuerhalten. Unternehmen und Endanwender sehen jedoch gelegentlich nicht die Notwendigkeit, ihre veralteten Betriebssysteme und Netzwerkkomponenten zu patchen.

Im Falle von industriellen Steuerungssystemen stellte der Experte fest, dass diese Systeme in der Regel nicht gut gepatcht sind, entweder, weil die Hersteller keine Sicherheitspatches für ihre Geräte bereitstellen oder weil das jeweilige System für den Betrieb kritisch ist und es nicht möglich ist, es abzuschalten, um die Sicherheitsmaßnahmen anzuwenden. Dies hat zur Folge, dass die Sicherheitslücken nicht richtig gepatcht werden und die Systeme bösartigen Angriffen ausgesetzt sind.

Angriffsmechanismen und Störereignisse

Der Bedrohungsagent kann auf verschiedene Systemkomponenten zugreifen, indem er eine bekannte Sicherheitslücke ausnutzt, die noch nicht gepatcht wurde. Malware kann installiert und verwendet werden, um ein Gerät oder ein System zu ersetzen oder zu ergänzen, z.B. um sensible Informationen zu senden oder Geräte zu steuern (Mo et al. 2012).

Potenzielle Auswirkungen auf Systemleistung

Abhängig von der Systemdomäne, in der die nicht gepatchte Software oder Firmware kompromittiert wurde, können die potenziellen Auswirkungen unterschiedliche Folgen haben.

Beispielsweise beschreibt das Ausfallszenario AMI.25 aus dem NESCOR-Katalog (NESCOR 2015) die potenziellen Auswirkungen eines Angriffs über eine ungepatchte Firewall in den Messsystemen. Diese Bedingung könnte es dem Angreifer ermöglichen, das AMI-Headend herunterzufahren, was zu Ausfällen führen könnte, da das Versorgungsunternehmen nicht in der Lage ist, in Spitzenzeiten auf die Nachfrage zu reagieren.

Wenn der Angriff auf industrielle Steuerungs-Firmware in Unterstationen gerichtet ist, kann der Bedrohungsagent die Kontrolle über die Unterstation erlangen und Segmente des Verteilungsnetzes abschalten, was zu Stromausfällen führen kann. Das Ausmaß der Ausfälle hängt von der Anzahl der betroffenen Unterstationen ab.

Darüber hinaus kann ein unzureichendes Patch-Management oder ein Fehler im Patch-Prozess auch die Verfügbarkeit der zu patchenden Systemkomponenten beeinträchtigen, was zu Stromausfällen führen kann. (siehe Ausfallszenario AMI.28 in (NESCOR 2015)).

Bewertung der potenziellen Auswirkungen

Basierend auf der obigen detaillierten Analyse werden die potenziellen Auswirkungen auf die Systemleistung als mittel bis hoch bewertet.

Technische, organisatorische und strukturelle Anpassungsoptionen

Experten erwähnten, dass ein korrektes Patch-Management unerlässlich ist, um mit der technologischen Entwicklung Schritt zu halten und Systeme mit Zugang zum Internet zu sichern. Das Management sollte einen Schweregrad und Zeitrahmen für das Patchen von Schwachstellen enthalten (NESCOR 2015).

Regelmäßige Patches für industrielle Steuerungssysteme, insbesondere SCADA-Systeme, stellen jedoch eine Herausforderung dar, da diese Systeme zeitkritisch sind, es keine Testumgebung gibt und Patches neue unbekannte Schwachstellen einführen oder das System letztendlich zerstören können (Cherdantseva et al. 2015). Experten empfehlen den Einsatz redundanter Systeme, um Ausfallzeiten zu vermeiden. Die Anwendung dieser Maßnahme würde jedoch von der Gesamtkonzeption des Systems abhängen und durch zusätzliche Kosten behindert werden.

Selbst wenn wir über alle Patches und Abhilfemaßnahmen auf dem Laufenden bleiben, sind unbekannte Zero-Day-Angriffe und unangekündigte Schwachstellen weit verbreitet (McLaughlin et al. 2015).

Eine weitere Lösung wäre, wie von einigen der Interviewpartner erwähnt, die Einführung verbindlicher Regelungen, um das Bewusstsein und die Bereitschaft zu erhöhen, korrekte Patches und Updates durchzuführen.

Bewertung der Anpassungskapazität

Aus den oben beschriebenen Überlegungen wird nach der VA die Anpassungskapazität als mittel eingestuft.

Vulnerabilität

In Anbetracht der hohen potenziellen Auswirkungen und der mittleren Anpassungskapazität wird die Vulnerabilität in diesem Fall als hoch eingestuft.

4.2.3 Menschlicher Faktor

4.2.3.1 Mangelndes Sicherheitsbewusstsein oder schlechte Reaktion auf Sicherheitsrichtlinien innerhalb der Organisation

Exposition und Sensitivität

Das Fehlen geeigneter Sicherheitstrainings- und Sensibilisierungsprogramme in einer Organisation des Energiesektors, z.B. in Kraftwerken, Verteilungs- und Übertragungsnetzbetreibern usw., kann zu unzureichend geschultem Personal führen, das unbeabsichtigt die Sichtbarkeit, das Wissen und die Möglichkeit für externe oder interne Stressoren bietet, einen erfolgreichen Angriff durchzuführen (NIST 2014).

Einerseits ist Social Engineering nach Ansicht der IT-Experten eines der am schnellsten wachsenden Sicherheitsprobleme. Dieser Angriffsmechanismus ermöglicht es dem Angreifer, eine der Schwächen jeder Organisation auszunutzen: den menschlichen Faktor. In diesem Fall könnte das Personal von externen Angreifern manipuliert werden, um Zugang zum internen System zu erhalten oder einen Angriff durchzuführen. Eine unzureichend geschulte Belegschaft wird sich nicht der Richtlinien und Verfahren bewusst sein, die notwendig sind, um organisatorische Informationen und Geräte zu sichern, was dazu führen kann, dass Schwachstellen ausgenutzt werden können, z.B. das Einfügen von bösartigen USB-Sticks in Maschinen im Unternehmens- oder Betriebsnetzwerk, das Surfen auf verdächtigen Websites, die oft Zero-Day-Angriffe enthalten, oder der Mangel an Sorgfalt mit Ausweisen, die einen teilweisen oder vollständigen Zugriff auf kritische Systeme ermöglichen können (NIST 2014). Darüber hinaus können kritische Informationen über die Systemkonfiguration oder -architektur öffentlich zugänglich sein, z.B. über die Website des Anbieters, des Eigentümers oder der Mitarbeiter. Potenzielle Angreifer können diese Informationen für die Angriffsplanung nutzen.

Weitere potenzielle Bedrohungsfaktoren sind dagegen verärgerte Mitarbeiter mit hohem Potenzial für kriminelles oder bösartiges Verhalten oder ehemalige Mitarbeiter nach ihrem Ausscheiden aus einem Unternehmen (Interviewee 4 2016). Sie verfügen, abhängig von ihrer Position, über hohe Systemkenntnisse und Zugriff auf kritische Funktionen oder sensible Daten, so dass sie in der Lage sein könnten, mögliche schwache interne Strukturen und Methoden zur Durchführung eines Angriffs zu identifizieren und das System schwer zu beschädigen.

Viele Lektionen über Cyber-Bedrohungen wurden von der Organisation in ihrer korporativen ICT-Domäne gelernt, und das Personal wird darauf aufmerksam gemacht und geschult, diese Bedrohungen zu erkennen. ICS-Betreibern, Ingenieuren und andere externe Akteuren, wie beispielsweise ICS-Anbietern, Systemintegratoren, Auftragnehmern und Wartungspersonal, fehlt es an Cybersecurity-Schulungen und -Ausbildungen (Luiijf 2016). Die meisten Angriffe in der Stationszone (siehe Smart Grid-Architektur in Abb. 4.3) kommen nach Aussage der IT-Sicherheitsexperten entweder von menschlichem Versagen, Fehlkonfiguration oder Social Engineering. Während Netzwerke in Betriebs-, Unternehmens- und Marktzonen meist über Firewalls, VPN, IDS und Monitoring-Systeme abgesichert sind, ist die Stationszone extrem anfällig für den Faktor Mensch (Interviewee 1 2016).

Angriffsmechanismen und Störereignisse

Durch Social Engineering entwickeln Bedrohungsagenten neue Mechanismen für ihre Angriffe, die auf unterschiedliche Management-Ebenen in der Organisation abzielen. Zum Beispiel ist „Spear Phishing“ ein Angriffsmechanismus, bei dem externe Angreifer E-Mails mit verstecktem bösartigem Code an Mitarbeiter senden, um das Netzwerk der Einrichtung zu infizieren. Im ukrainischen Fall im Jahr 2015 entwickelten Angreifer eine Malware („Blackenergy 3“) und erstellten bewaffnete Dokumente, um die Malware per E-Mail zuzustellen. E-Mails mit bösartigen Dokumentenanhängen wurden im Rahmen einer Phishing-Kampagne an Personen innerhalb des Unternehmens verschickt. Bedrohungsakteure haben die Malware erfolgreich installiert, nachdem die Mitarbeiter die bewaffneten E-Mail-Anhänge geöffnet haben. Die Malware beinhaltete Plugin-Software, um Systemzugangsdaten zu sammeln und Aufklärungsaktivitäten im internen Netzwerk durchzuführen. Mit den gestohlenen Zugangsdaten griffen Angreifer auf die industrielle Kontrollumgebung zu und führten komplexe Aktionen durch (Booz Allen Hamilton 2017).

Eine weitere Möglichkeit, den Perimeter zu durchbrechen, sind USB-basierte Angriffe. USB-Peripheriegeräte sind zu einem attraktiven Werkzeug für Cyber-Angriffe geworden, bei denen Angreifer

die Benutzer durch Vortäuschen dazu nutzen Zugang zu Systeme zu erlangen. Besonders Betroffen sind Peripheriegeräte, bei denen Anwendungen eher beiläufig benutzt werden. Eine Voraussetzung hierfür ist dass sie eine eingebettete bösartige Payload tragen, die zum Starten von Angriffen verwendet werden kann (Nissim et al. 2017). USB-Geräte können auch zum Angriff auf bestimmte ICS-Ziele verwendet werden, wie z.B. PLCs (Programmable Logic Controllers), wie die berühmte „Stuxnet"-Malware gegen Zentrifugen in der iranischen Urananreicherungsanlage außerhalb von Natanz zeigt. In diesem Fall erfolgte die indirekte Infiltration über infizierte mobile Geräte und USB-Sticks von Auftragnehmern, die legitimen Zugriff auf das kritischste System der Anlage hatten (Langner 2013). Der Stuxnet-Wurm war ein beispiellos komplexer Code, der in drei Phasen attackiert hat. (1) Zuerst zielte es auf Microsoft Windows-Maschinen und -Netzwerke, die sich immer wieder selbst replizieren. Mit Hilfe von kompromittierten digitalen Zertifikaten konnte Stuxnet Firewalls umgehen und verbreitete sich auch über die lokalen Kommunikationsnetze des SCADA-Systems aus. Die Peer-to-Peer-Kommunikationsfähigkeiten von Stuxnet ermöglichten es der Malware, sich selbst zu aktualisieren, selbst wenn das betroffene Gerät keinen direkten Zugang zum Internet hatte. (2) Dann suchte sie nach Siemens Step7-Software, die ebenfalls Windows-basiert ist und zur Programmierung von PLCs verwendet wird. (3) Nachdem die Ziel-SPS infiziert wurde, änderte Stuxnet schließlich ihre Betriebsart. Mit Hilfe des PLC-Rootkits modifizierte die Malware den SPS-Code, um einen Offenlegungsangriff durchzuführen und die empfangenen Daten aufzuzeichnen. Nach einiger Zeit der Datenaufzeichnung beginnt Stuxnet, das physische System durch einen Störungsangriff zu sabotieren. Beim Ändern des Steuersignals, das an die Aktoren gesendet wird, versteckt Stuxnet den Schaden an der Anlage, indem die zuvor aufgezeichneten Daten an die SCADA-Überwachungssysteme weitergeleitet werden (Knapp 2011; Kushner 2013; New Jersey Cybersecurity & Communications Integration Cell 2017). Abb. 4.9 zeigt das Stuxnet-Angriffsszenario.

Ein Beispiel für einen Angriff durch Insider, ist der Fall der Manipulation von intelligenten Zählern in Malta. Mitarbeiter des staatlichen Energieversorgers Enemalta manipulierten rund 1.000 Smart Meter gegen Bestechungsgelder und installierten sie bei Kunden mit hohem Stromverbrauch. Die Smart Meter wurden so konfiguriert, dass sie bis zu 75 Prozent weniger Energie aufzeichneten, als tatsächlich verbraucht wurde. Die Manipulation der Zähler erfolgte ohne Siegel oder Schutzmechanismen zu brechen. Es gibt Hinweise, dass Zähler von anderen Kunden manipuliert wurden, um einen höheren Stromverbrauch zu messen, den Gesamtverbrauch eines Bezirks dadurch konstant zu halten und den Betrug zu verschleiern (BSI 2015b).

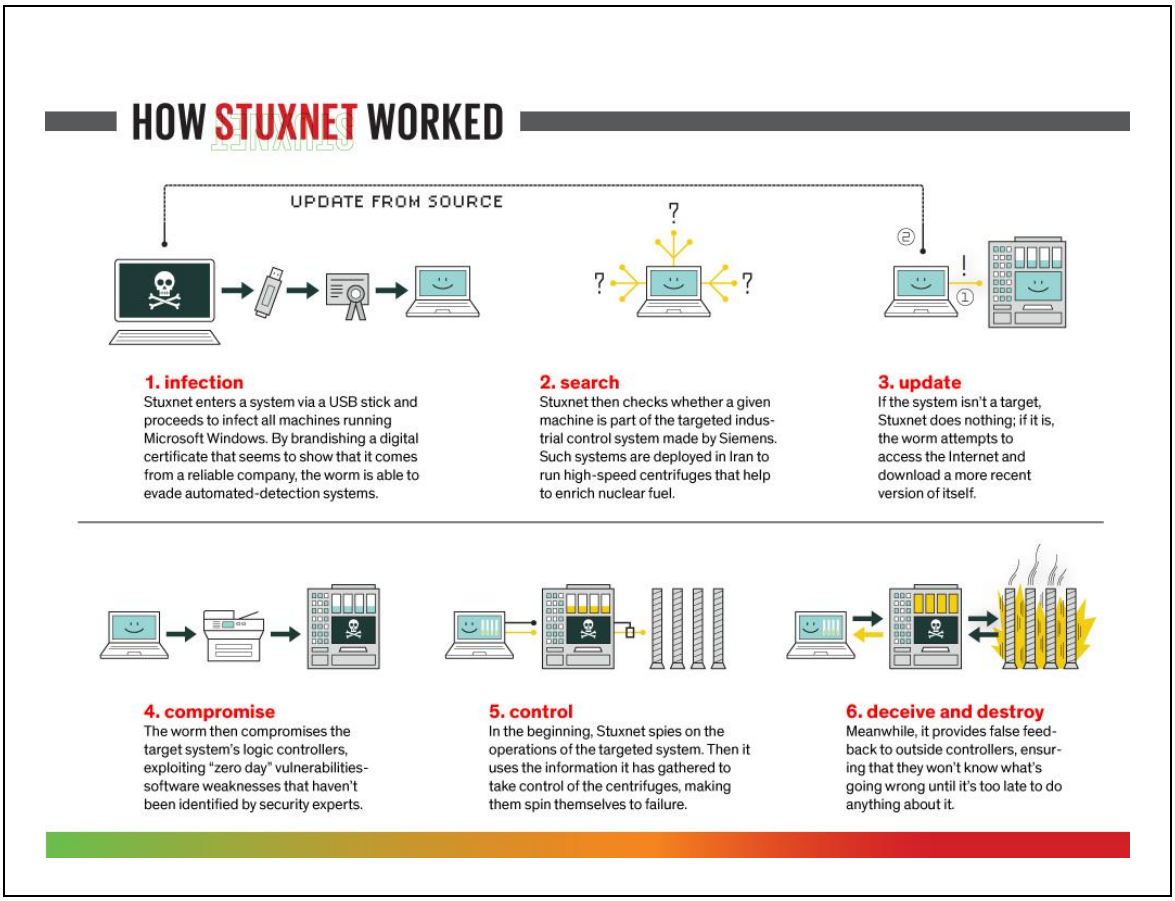

Abb. 4.9: Funktionsweise von Stuxnet
Quelle: Kushner (2013)

Potenzielle Auswirkungen auf Systemleistung

Abhängig von der Relevanz der kompromittierten Daten oder von den Privilegien des Zielbenutzers können die potenziellen Auswirkungen unterschiedlich groß sein. Durch Informationslecks kann ein Bedrohungsagent legitime Berechtigungsnachweise für den Zugriff auf kritische Systeme erhalten. Wenn ein Angreifer ein System passiert, ist es möglich, die SCADA-Systeminfrastruktur (z.B. den Data Historian Server) zu kompromittieren. Wenn die Situation durch eine unsachgemäße Trennung von Unternehmens- und Industrienetzwerk verschärft wurde, könnte der Bedrohungsagent die Kontrolle über Feldgeräte erlangen und falsche oder schädliche Aktionen zur Betriebskontrolle durchführen, die zu Ausfällen von unbekannter Dauer oder direkten physischen Schäden an den Anlagen des ICS führen. Darüber hinaus könnte der Angriff nicht nur die Stromverteilung stören, sondern auch IT-Systeme zerstören, Callcenter überfluten und die Reaktion auf Zwischenfälle verhindern, wie beim Angriff in der Ukraine im Jahr 2015 (Booz Allen Hamilton 2017).

Im Falle der Smart-Metering-Infrastruktur könnte eine Beeinträchtigung der IT-Infrastruktur in den Einrichtungen der Smart Meter Gateway Administration (SMGA) es dem Angreifer ermöglichen, über den sicheren Kommunikationskanal fast eine Million Smart-Meter-Gateways anzugreifen und sie beispielsweise abzuschalten, was zu Netzinstabilität und potenziellen Stromausfällen führen würde (Interviewee 19 2017).

Der NESCOR-Katalog (NESCOR 2015) zeigt weitere mögliche Auswirkungen durch Social Engineering auf: Messinfrastruktur (siehe AMI.3, AMI.9), Übertragung (siehe WAMPAC.4), Verteilung (siehe DGM.10) und Erzeugungsdomänen (siehe GEN.4, GEN.9).

Bewertung der potenziellen Auswirkungen

Unter Berücksichtigung der potenziellen Auswirkungen, die sowohl die qualitativen als auch die quantitativen Kriterien beeinflussen können, werden die potenziellen Auswirkungen auf die Systemleistungen als mittel bis hoch eingestuft.

Technische, organisatorische und strukturelle Anpassungsoptionen

Experten schlagen strengere obligatorische Sicherheitsmaßnahmen auf verschiedenen Organisationsebenen vor, um dem Social Engineering entgegenzuwirken. Bediener und Verwaltungspersonal müssen geschult werden, damit sie sich der Bedingungen bewusst sind, die das System gefährden könnten (z.B. schlechtes Passwortmanagement, unsachgemäße Verwaltung von E-Mail-Anhängen, nicht identifizierte USB-Laufwerke usw.). Mitarbeiter könnten an Social-Engineering-Übungen teilnehmen, bei denen sie firmeneigene Phishing-Mails erhalten oder sie finden platzierte USB-Laufwerke, um zu lernen, wie sie richtig auf die Bedrohung durch Social-Engineering-Angriffe reagieren können (IEC 2016b). Sicherheitsschulungen und Sicherheitsbewusstseinsprogramme sollten an jeden Mitarbeiter entsprechend seiner Position angepasst werden. Es sollte eine kontinuierliche Umschulung über einen bestimmten Zeitraum umfassen, um neue Verfahren, neue Technologien und die Stärkung der Bedeutung des Cybersicherheitsprogramms (ENISA 2012; NIST 2014) zu berücksichtigen. Außerdem sollte es bessere persönliche Hintergrundüberprüfungen für neue Mitarbeiter geben, um sicherzustellen, dass alle Mitarbeiter mit operativem oder administrativem Zugang zu ICS angemessen kontrolliert werden (ENISA 2016).

Es sollte mehr Bewusstsein und Bereitschaft für eine harmonisierte Anstrengung von Personal, Management, IT-Abteilung und Aufsichtsbehörden vorhanden sein, sich auf strenge Sicherheitsrichtlinien für Organisationen zu einigen. Dennoch können die Implementierungskosten von Sicherheitsrichtlinien und Schulungsprogrammen die Genehmigung behindern und das implementierte Sicherheitsniveau einschränken, wie von einem Experten angegeben. Die Anwendung von Sicherheitsmaßnahmen könnte sich auch auf das Engagement der Mitarbeiter beschränken.

Bewertung der Anpassungskapazität

In Anbetracht der Tatsache, dass Anpassungsoptionen gegeben sind, deren mögliche Umsetzung aber von der Bereitschaft der beteiligten Akteure abhängt, wird die Anpassungskapazität als mittel eingestuft.

Vulnerabilität

Gemäß der VA-Methodik führt die Kombination aus einer hohen potenziellen Wirkung und einer mittleren Anpassungskapazität zu einer hohen Vulnerabilität.

4.2.3.2 Mangelndes Sicherheitsbewusstsein bei den Verbraucherinnen und Verbrauchern

Exposition und Sensitivität

Endbenutzer stellen einen weiteren Schwachpunkt für das System dar. Mangelndes Bewusstsein oder mangelndes Verständnis für die Folgen geringer Sicherheit seitens des Kunden könnte das Stromnetz gefährden. Experten bestätigen, dass die Mehrheit der Endanwender kein Expertenwissen über ihre Heimautomationssysteme und Internet of Things (IoT)-Geräte hat und daher nicht weiß, wie sie ihre intelligenten Geräte richtig sichern und warten können.

Experten erwähnten, dass einerseits IoT- und Heimautomationsgeräte, insbesondere Standardprodukte, bekannte Sicherheitslücken aufweisen, die Angreifer ausnutzen können. Andererseits könnten Endgeräte, die nicht ordnungsgemäß gepatcht oder gewartet werden, an das Heimnetzwerk angeschlossen werden, was die Anfälligkeit des Systems durch das Hinzufügen weiterer unsicherer Zugangspunkte erhöht.

Ein komplexeres Problem, das von einem Experten erwähnt wird, besteht darin, dass Endanwender Prosumenten sind, die nicht über das Expertenwissen verfügen, um geeignete Sicherheitsmaßnahmen für DER-Systeme zu implementieren und aufrechtzuerhalten.

Angriffsmechanismen und Störereignisse

Ein Angreifer kann mittels Lauschangriff auf Kundendaten zugreifen und private Informationen, einschließlich des Stromverbrauchs, hinter einer Firewall stehlen, die absichtlich oder unabsichtlich den direkten Zugriff aus anderen Netzwerken ermöglicht. Neben dem Abhören können Angreifer auch Zugriff auf Smart Meter-Geräte erhalten, um Messdaten zu manipulieren oder Daten über Systemparameter von Distributed Energy Resources (DER) zu manipulieren. IoT-Geräte könnten kompromittiert und für einen verteilten Denial-of-Service (DDoS)-Angriff verwendet werden.

Potenzielle Auswirkungen auf Systemleistung

Je nach Angriffsmechanismus kann die Privatsphäre des Kunden gefährdet sein oder es können Kommunikationskanäle als Medium zur Manipulation von Daten und zum Senden falscher Steuerbefehle genutzt werden, die zu Instabilität und Ausfällen des Stromnetzes führen können.

Das Ausfallszenario DER.2 aus dem NESCOR-Katalog (NESCOR 2015) veranschaulicht den Fall, dass ein großes DER-System fälschlicherweise mit einem drahtlosen Unternehmensnetzwerk verbunden ist und somit das DER-System dem Internet ausgesetzt ist. Der Bedrohungsagent könnte die Kontrolle übernehmen und die Funktionsweise der DER-Funktionen verändern. Infolgedessen kann es zu schädlichen Rückleistungsströmen oder Überlastungen von Transformatoren in Umspannwerken kommen.

Unsichere AMI-Netzwerke oder manchmal sogar geschützte Netzwerke könnten Möglichkeiten für einen möglichen Verstoß gegen die Privatsphäre der Kunden bieten, was zu einem Verlust des Kundenvertrauens führen könnte.

Bewertung der potenziellen Auswirkungen

Unter Berücksichtigung der Tatsache, dass die Sicherheitsanforderungen durch mangelnde Integrität und Vertraulichkeit gefährdet sein können und sich auf die qualitativen Kriterien sowie auf die

Energieversorgung auswirken, werden aufgrund des mangelnden Sicherheitsbewusstseins der Verbraucher die potenziellen Auswirkungen auf die Systemleistung als mittel bis hoch eingestuft.

Technische, organisatorische und strukturelle Anpassungsoptionen

Um Verstöße mit potenziell großen Auswirkungen zu vermeiden, empfahlen die Interviewpartner, dass eine Aufklärung über Cybersicherheit für die Endbenutzer erforderlich ist, um ein höheres Sicherheitsniveau zu erreichen. Bessere Kenntnisse des eigenen intelligenten Systems schärfen das Bewusstsein der Endanwender. Darüber hinaus ermöglicht es den Endbenutzern, ihr System ordnungsgemäß zu betreiben und zu warten, so dass sie selbst ein gewisses Maß an Sicherheit gewährleisten können. Obligatorische Sicherheitsmaßnahmen für Hausgeräte und deren Wartung würden helfen, ein Minimum an Sicherheit für Hausautomationssysteme zu erreichen.

Das Erreichen eines höheren Sicherheitsniveaus steht, wie von Experten erwähnt, im Widerspruch zu einer kurzfristigen wirtschaftlichen Logik. Daher wird in den meisten Fällen die Umsetzung höherer Sicherheitsmaßnahmen auf der Kunden- oder Prosumentenseite durch ihre Zahlungsbereitschaft eingeschränkt sein.

Darüber hinaus erklärten Experten, dass die meisten der derzeit geltenden Sicherheitsmaßnahmen versuchen, die bösartigen Angreifer außerhalb des Systems zu halten, weshalb eine der größten Herausforderungen darin besteht, nach einem erfolgreichen Angriff von der Prävention oder Erkennung von Cyber-Angriffen zu einem Wiederherstellungsmechanismus überzugehen. Zusammen mit besseren Überwachungs- und Erkennungssystemen könnte dies bessere Möglichkeiten bieten, um auf Angriffe und manipulierte Daten zu reagieren. Es ist jedoch wichtig, sich der Privatsphäre der Kunden bewusst zu sein, wenn mehr Überwachungssysteme eingesetzt werden. Der Verlust der Privatsphäre könnte die Akzeptanz weiterer Sicherheitsmaßnahmen beeinträchtigen.

Bewertung der Anpassungskapazität

Da die genannten Anpassungsoptionen noch nicht vorhanden sind und die Anpassungsbereitschaft der Kunden begrenzt ist, wird die derzeitige Anpassungskapazität als gering eingestuft.

Vulnerabilität

Nach der VA-Methodik führen mittlere bis hohe potenzielle Auswirkungen auf die Systemleistung in Verbindung mit einer geringen Anpassungskapazität zu einer hohen Gesamtverwundbarkeit hinsichtlich des fehlenden Sicherheitsbewusstseins auf der Seite der Kunden. Die Vulnerabilität wird als hoch eingestuft.

4.2.4 Regulierung

4.2.4.1 Fehlende Umsetzung von Sicherheitsstandards und Regulierung

Exposition und Sensitivität

Verschiedene technische und organisatorische Standards wurden entwickelt, um den Anforderungen der Cybersicherheit in Smart Grids gerecht zu werden. Wie Experten jedoch festgestellt haben, handelt es sich in den meisten Fällen nur um Empfehlungen, deren Umsetzung nicht verpflichtend ist.

So wurde beispielsweise die IEC 62351 entwickelt, um die Sicherheit der Unterstations-Infrastruktur zu gewährleisten und einen Rahmen für die End-to-End-Sicherheit der Kommunikation zwischen Software-Anwendungen zu schaffen. Dieses ist jedoch stark auf den Einsatz von TLS zum Schutz des Stromnetzes gegen verschiedene Angriffsmechanismen angewiesen (International Electrotechnical Commission (IEC) 2007).

Trotz der Tatsache, dass dieser Standard Sicherheitsverbesserungen ermöglicht für Protokolle wie IEC 61850 (GOOSE, SV und MMS), IEC 60870-5-104 und DNP3 sowie IEC 60870-5-101 und serielles DNP3 werden diese in der Praxis nicht immer angewendet (Basagiannis et al. 2015; McLaughlin et al. 2015). Experten erwähnten darüber hinaus, dass die Hersteller die empfohlenen Sicherheitsmaßnahmen in ihren Produkten oft nicht umsetzen. IT-Experten waren der Ansicht, dass das Fehlen verbindlicher Vorschriften zur Durchsetzung von Mindestanforderungen an die Sicherheit von Stromnetzbetreibern oder von Anbietern, die die erforderlichen Sicherheitsanforderungen in ihren Produkten erfüllen, das System möglichen Cyber-Angriffen aussetzt.

Angriffsmechanismen und Störereignisse

Ein Angreifer kann bekannte Schwachstellen aufgrund fehlender Authentifizierung oder Verschlüsselung in bestimmten Standardprotokollen ausnutzen, unbefugten Zugriff auf das System erhalten oder Kommunikationssitzungen manipulieren und beeinträchtigen.

Einige Beispiele für mögliche Störungen sind in der Literatur zu finden, z.B. DoS-Angriffe (Dondossola et al. 2008; Dondossola et al. 2009) oder Man-in-the-Middle (Maynard et al. 2014) auf Netzwerke mit dem IEC 60870-5-Protokoll. Kush et. al. (2014) zeigen ebenfalls einen praktischen Angriff, indem sie Schwächen in der Authentifizierung und Verschlüsselung in GOOSE (engl. Generic Object Oriented Substation Event) ausnutzen, um Nachrichten mit falschen Daten zwischen jeder gültigen Nachricht zu fälschen. In diesem Fall wurde ein Skriptcode in Python verwendet, der es dem Angreifer erlaubt, Netzwerkpakete zu suchen, zu sezieren, zu fälschen und zu senden (McLaughlin et al. 2015).

Potenzielle Auswirkungen auf Systemleistung

Je nach Angriffsmechanismus können die Auswirkungen unterschiedlich sein. Wenn beispielsweise ein Bedrohungsagent unverschlüsselte Klartext-SCADA-Frames (z. B. Distributed Network Protocol 3.0, DNP3) abfängt, die wertvolle Informationen wie Steuer- und Einstellinformationen für intelligente Geräte (IED) enthalten, kann der Bedrohungsagent Gerätedienste herunterfahren, falsche Befehle senden und Störungen verursachen (Kush et al. 2014).

Bewertung der potenziellen Auswirkungen

In Anbetracht der Tatsache, dass die kompromittierten IT-Sicherheitsanforderungen zu Instabilität und Ausfällen des Stromnetzes führen können, werden die potenziellen Auswirkungen auf die Systemleistungen als mittel bis hoch eingestuft.

Technische, organisatorische und strukturelle Anpassungsoptionen

Es gibt gute Praxisrichtlinien, die die Implementierung höherer Sicherheitsstandards empfehlen, um die Gerätekommunikation zum Schutz von Nachrichten und zur Gewährleistung der Integrität innerhalb des Managements von Energiesystemen und der Automatisierung von Umspannwerken

zu gewährleisten. Nach Ansicht von Experten sind sie jedoch nicht obligatorisch und die Einhaltung von Mindestsicherheitsstandards wird nicht durch Vorschriften durchgesetzt.

Darüber hinaus könnte sich die Entscheidung, Altsysteme zu modernisieren, um die Sicherheitsmaßnahmen umzusetzen, aufgrund verschiedener Faktoren bis zum nächsten geplanten Austausch der Lebenszyklusausrüstung verzögern. Das kritische Niveau des Prozesses oder wirtschaftliche Zwänge in der Organisation können die Anwendung behindern. Daher stellen die derzeit installierten Legacy-Geräte mit ihren Protokollen ein Risiko für die Sicherheit dar (Knapp und Samani 2013).

Bewertung der Anpassungskapazität

Berücksichtigt man, dass es bereits Anpassungsoptionen zur Verbesserung der Sicherheit in Smart Grids gibt, deren Einsatzbereitschaft jedoch begrenzt sein könnte, wird die Anpassungskapazität als mittel eingestuft.

Vulnerabilität

In Anbetracht der hohen potenziellen Auswirkungen auf die Systemleistungen und der mittleren Anpassungskapazität wird die Vulnerabilität als hoch eingestuft.

4.2.4.2 Mangelnde koordinierte Anstrengungen zur Verbesserung der Sicherheit

Für diese Kategorie wurde aus Zeitgründen keine umfassende Bewertung nach der VA-Methodik durchgeführt, stattdessen werden im folgenden Abschnitt die wichtigsten Ergebnisse der Interviewanalyse vorgestellt.

In Deutschland konzentrieren sich die Sicherheitsvorschriften vor allem auf Smart Metering und kritische Infrastrukturen, allerdings fehlt nach Ansicht der Experten eine effektive Koordination zur Verbesserung der Sicherheit des Gesamtsystems. Nach der deutschen Gesetzgebung müssen Stromnetzbetreiber ein Information Security Management System (ISMS) auf Basis der IEC/ISO 27001 einrichten und zertifizieren. Derzeit gibt es jedoch keine verbindlichen Vorschriften zur Absicherung kleinerer DER-Systeme (Interviewee 2 2016), die entsprechend der in Kapitel 4.2.1 und 4.2.3.2 durchgeführten VA kritische Punkte aufweisen und von Angreifer ausgenutzt werden können, was wiederum erhebliche Auswirkungen auf das Stromnetz haben könnte.

Auch bei der Smart-Metering-Infrastruktur enthalten die Sicherheitsmaßnahmen auf Basis von Schutzprofilen und technischen Richtlinien (TR-03109) keine Regelungen für andere Dienste oder Geräte, die mit umfangreichen Steuerungsmöglichkeiten ausgestattet sind und an das Hausautomationsnetz angeschlossen werden können.

Darüber hinaus würde eine Verbesserung der Sicherheit von Seiten der Stromerzeugung und der Netzbetreiber zusätzliche wirtschaftliche Investitionen bedeuten, die über die Stromrechnungen an die Kundinnen und Kunden weitergegeben werden könnten. Ein Experte für den Energiesektor erwähnte, dass Kundinnen und Kunden nicht bereit sind, einen höheren Preis für mehr Sicherheit zu zahlen, da sie ihren Stromlieferanten auf der Grundlage des niedrigsten Preises auswählen und daher kein neues Stromnetz akzeptieren würden, das keine wesentlichen direkten Vorteile gegenüber dem alten System bietet (Interviewee 6 2016). Experten für IT-Sicherheit gaben an, dass Kunden weder befragt noch in den Prozess der Energieumwandlung einbezogen wurden, was auch bei

der Digitalisierung der Fall sein könnte. Mangelndes Bewusstsein für die Bedeutung neuer Technologien und deren Sicherheit auf Kundenseite könnte daher die Bereitschaft, in resiliente Energielösungen zu investieren, behindern, da die Kunden die vielen Vorteile eines besonders ausfallsicheren Stromsystems nicht kennen würden (Interviewee 1 2016).

4.2.5 Analyse der Anwendungsfälle

Aus der Interviewanalyse konnten vier Anwendungsfälle identifiziert werden. Jeder Anwendungsfall definiert eine bestimmte Störung. Diese sind (1) GPS-Signal-Spoofing, (2) Insider-Bedrohung von SCADA-Systemen, (3) Manipulation der ICS-Firmware in Unterstationen und (4) Abhören von Daten der Advanced Metering Infrastruktur. Abb. 4.10 zeigt die Lage jedes Anwendungsfalles auf dem Referenzarchitekturmodell.

Die VA-Methodik wurde angewandt, um die Verwundbarkeit aufgrund jeder spezifischen Störung zu bewerten, und die Ergebnisse sind in Abb. 4.11, Abb. 4.12, Abb. 4.13, Abb. 4.14 dargestellt.

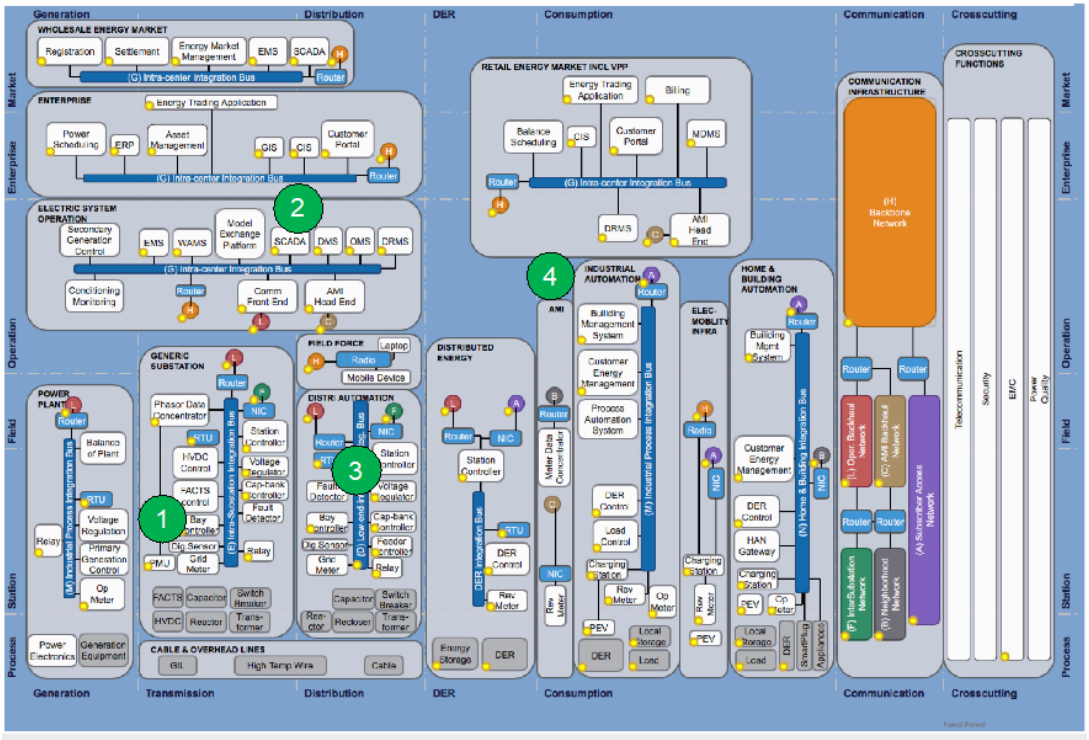

Abb. 4.10: Lage der analysierten Anwendungsfälle auf dem Referenzarchitekturmodell

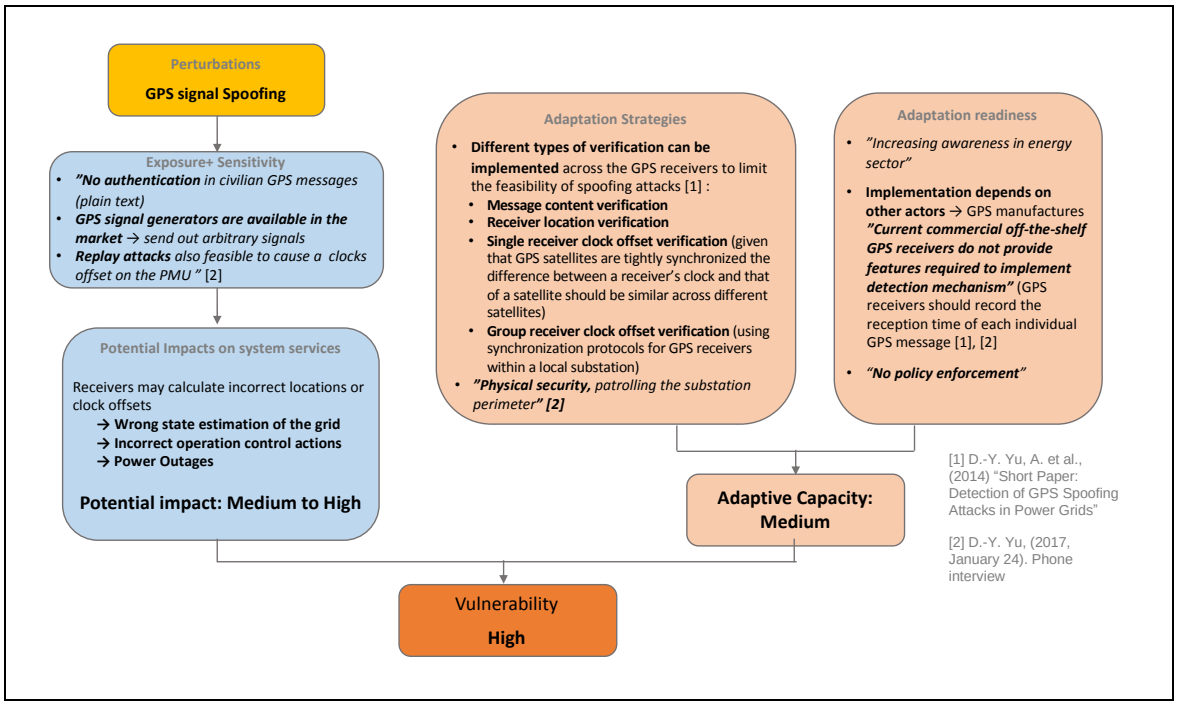

Abb. 4.11: Anwendungsfallanalyse: GPS-Signal-Spoofing

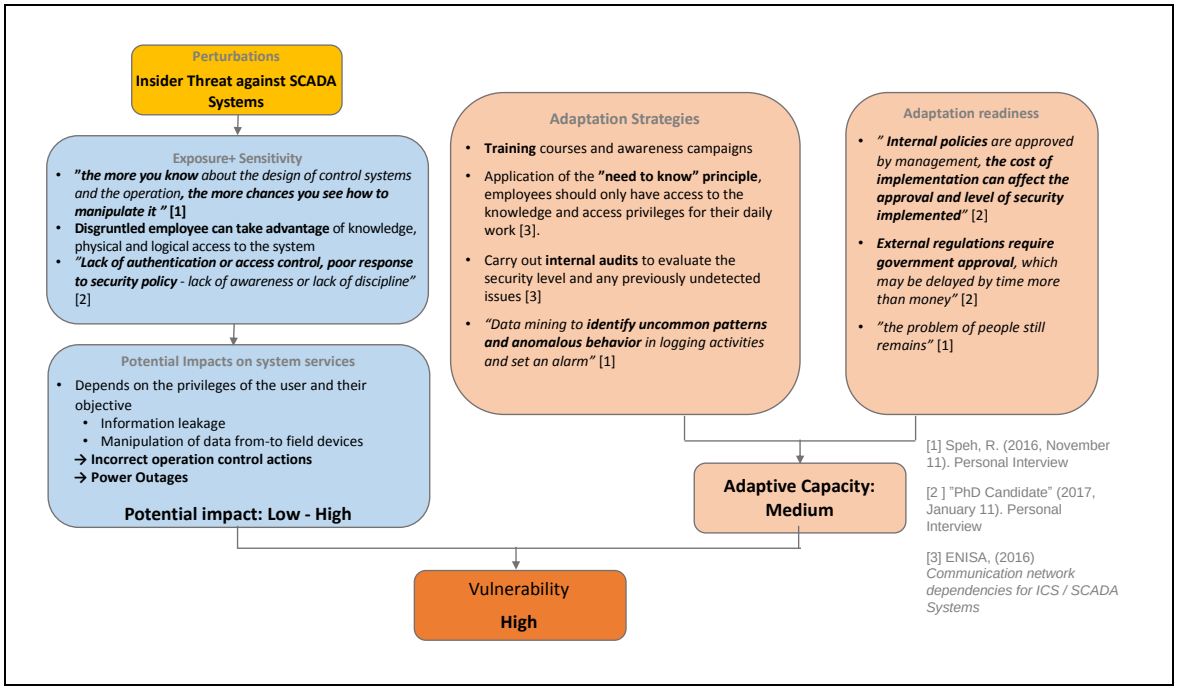

Abb. 4.12: Anwendungsfallanalyse: Insider-Bedrohung innerhalb von SCADA-Systemen

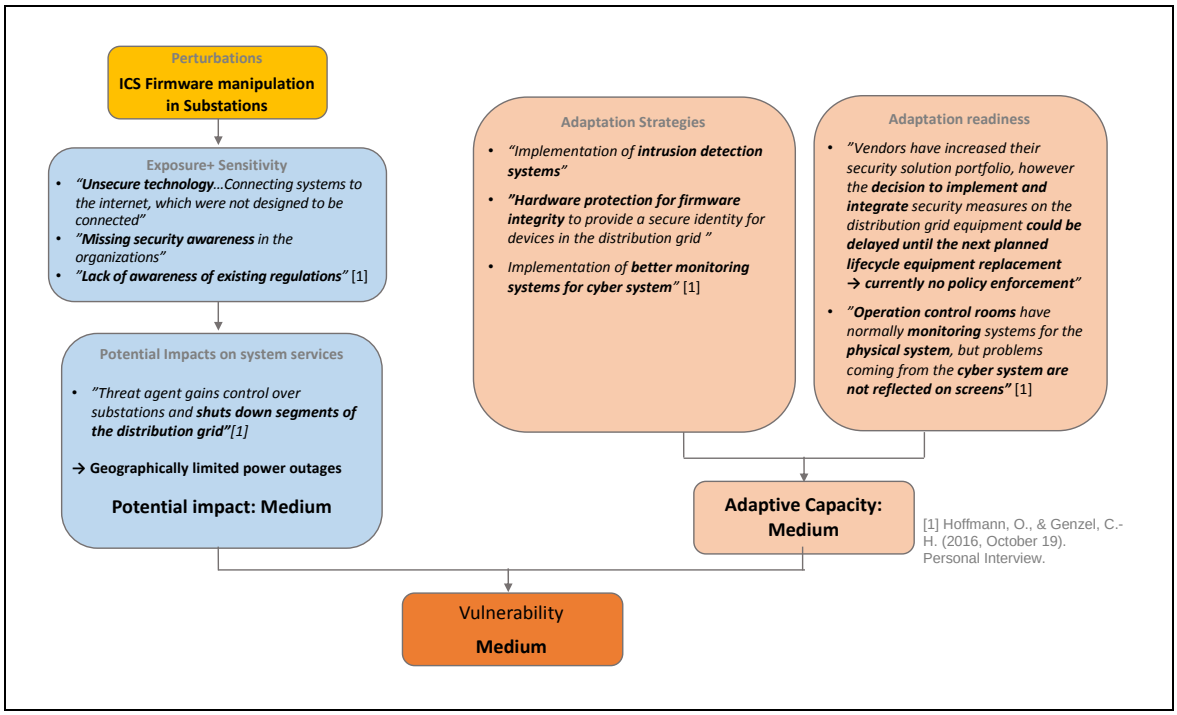

Abb. 4.13: Anwendungsfallanalyse: ICS-Firmware-Manipulation in Umspannwerken

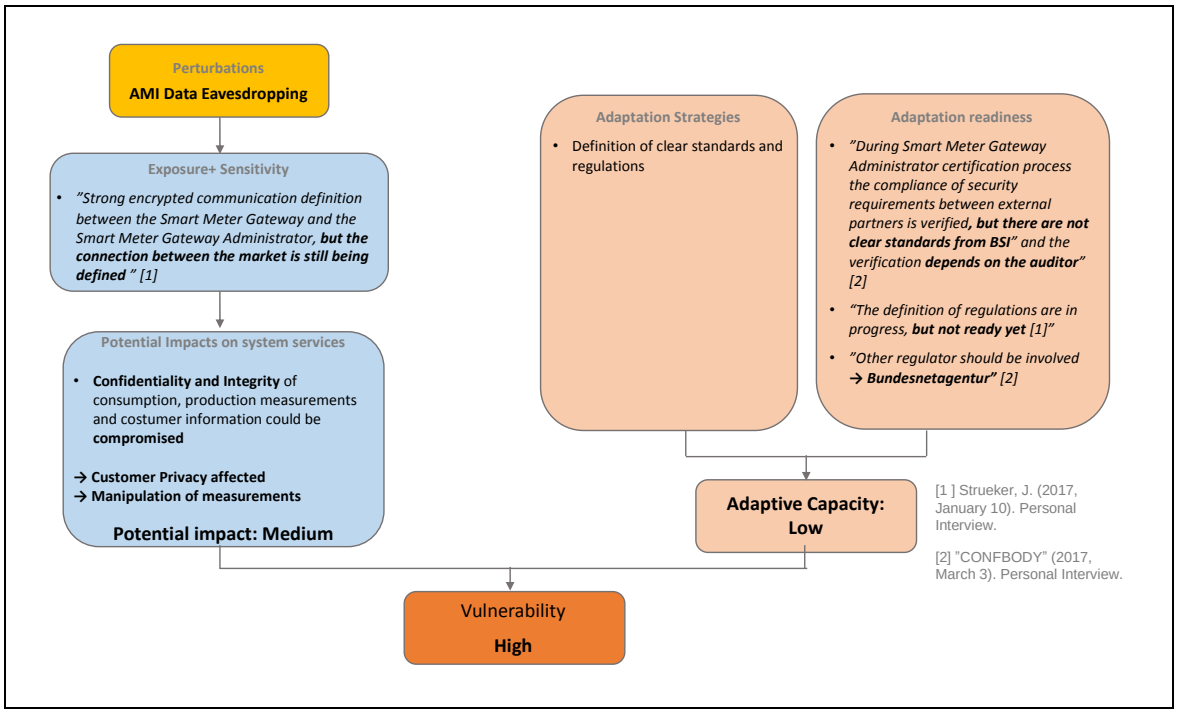

Abb. 4.14: Anwendungsfallanalyse: Advanced Metering Infrastrukturdaten abhören

4.2.6 Zusammenfassung der Ergebnisse der Vulnerabilitätsanalyse

Tab. 4.1 fasst die Ergebnisse der Vulnerabilitätsanalyse für jede der oben beschriebenen Kategorien und Unterkategorien zusammen. Wie man sieht, machen alle identifizierten Zustände in den verschiedenen Kategorien das cyberphysikalische System anfälliger.

Tab. 4.1: Zusammenfassung der Ergebnisse der Vulnerabilitätsanalyse
Quelle: Eigene Darstellung

Kategorie	Unterkategorie	Mögliche Auswirkungen	Adaptive Kapazität	Verwundbarkeit
Technologie	Unsichere Endpunkte	Mittel bis Hoch	Mittel	Hoch
	Unsichere Kommunikation	Mittel bis Hoch	Mittel	Hoch
Richtlinien und Verfahren	Fehlende interdisziplinäre IT-OT Kenntnisse	Mittel bis Hoch	Mittel	Hoch
	Unsachgemäße Verwaltung von Sicherheitspatches	Mittel bis Hoch	Mittel	Hoch
Menschlicher Faktor	Mangelndes Sicherheitsbewusstsein oder schlechte Reaktion auf Sicherheitsrichtlinien in der Organisation	Mittel bis Hoch	Mittel	Hoch
	Mangelndes Sicherheitsbewusstsein bei Verbrauchern	Mittel bis Hoch	Niedrig	Hoch
Regulierung	Fehlende Umsetzung von Sicherheitsstandards und Regulierung	Mittel bis Hoch	Mittel	Hoch
	Mangelnde koordinierte Anstrengung zur Verbesserung der Sicherheit	Mittel bis Hoch	Mittel	Hoch

5 Resilienzstrategien

Bearbeitung und Texterstellung: Uni Bremen

Die Vulnerabilitätsanalyse lieferte wichtige Erkenntnisse über die besonders kritischen Schwachstellen von cyber-physikalischen Stromsystemen. Die dynamische Charakteristik von IKT-Systemen und die komplexen Zusammenhänge und Wechselwirkungen mit dem Stromsystem machen es jedoch unmöglich, alle möglichen Stressoren aus dem Cyberbereich zu analysieren, die das Energiesystem bedrohen könnten. Weitere zum derzeitigen Zeitpunkt völlig unbekannte Stressoren, die aus der Einbindung von IKT herrühren, wollen wir hier allgemein als "Schwarze Schwäne" bezeichnen. Beispiele für Schwarze Schwäne aus der Vergangenheit waren: unvorhergesehene Ausfälle von Informationssystemen (z.B. Bugs, "Zero-Day-Exploits") oder innovative und hoch entwickelte Angriffsmechanismen (z.B. fortgeschrittene persistente Bedrohungen), die erhebliche Herausforderungen an die Entwicklung präventiver Sicherheitsmethoden darstellten. Als weitere Beispiele für diese höchst unsicheren, aber zerstörerischen Ereignisse seien die „WannaCry“ ransomware und die „NotPetya“ Cyber-Angriffe im Jahr 2017 genannt. Der Cyberangriff auf die ukrainische Energieinfrastruktur, der durch die hochgradig angepasste Malware "Crashverride / Industroyer" (siehe weitere Details zu „Crashoverride“-Malware in Box 1 aus Kapitel 4.2.1.1) verursacht wurde, ist ein weiteres Beispiel für einen „Schwarzen Schwan“ der in diesem Fall ein cyberphysikalisches Stromsystem getroffen hat.

Resilienz als Leitbild zu verstehen, hilft bei der Gestaltung von Systemen, um sich auf bekannte und unbekannte Herausforderungen vorzubereiten. Resilienz kann als die Fähigkeit des Systems interpretiert werden, sich auf jede Störung vorzubereiten, diese zu bewältigen und sich von ihnen zu erholen, ohne vorher besondere Kenntnisse über die Ereignisse oder der Stressoren kennen zu müssen (Gößling-Reisemann 2016).

Ein resilientes Energiesystem sollte auf Stressoren aller Art vorbereitet sein. Die Fähigkeiten eines resilienten Energiesystems sollte dies widerspiegeln. Auf einer sehr breiten Ebene können Stressoren durch ihre Dynamik und den Bekanntheitsgrad charakterisiert werden (Gößling-Reisemann 2016), was im Folgenden weiter spezifiziert wird:

– **Bekannt/erwartet:** Stressoren, die die Systeme bereits in der Vergangenheit erlebt haben und bei denen Vorhersagen über zukünftige Ereignisse vorliegen.
– **Unbekannt/unerwartet:** Stressoren, denen das System nie oder nur sehr selten ausgesetzt war und bei denen es keine Vorhersagen für zukünftige Ereignisse gibt.
– **Schleichend/kriechend:** Stressoren, die sich langsam und möglicherweise für einige Zeit unentdeckt entwickeln.
– **Abrupt/plötzlich:** Stressoren, die sich plötzlich oder abrupt ohne Vorwarnung entwickeln.

Ein System, das in der Lage ist, sich auf Stressoren mit einer beliebigen Kombination der oben beschriebenen Charakteristika vorzubereiten, sie zu bewältigen und sich von ihnen zu erholen, benötigt eine Vielzahl von Fähigkeiten, die sich in Robustheit, Anpassungsfähigkeit, Innovationsfähigkeit und Improvisationsfähigkeit zusammenfassen lassen (siehe Tab. 5.1). Wenn sich Stressoren allmählich entwickeln und dem System bereits bekannt sind oder in naher Zukunft erwartet werden können, kann eine Anpassung bestehender Strukturen, Komponenten und Organisationen eingeleitet werden, um besser mit dem Auftreten dieses Stressors fertig zu werden und sich von ihm zu

erholen. Wenn der Stressor allerdings unbekannt ist und sich abrupt entwickelt, werden die Akteure im System keine Zeit haben, innovative Lösungen zu finden oder Widerstand aufzubauen und müssen improvisieren können (Gößling-Reisemann 2016).

Tab. 5.1: Zuordnung der benötigten Fähigkeiten eines Systems, um auf Stressoren vorbereitet zu sein
Die Stressoren werden in der Tabelle nach zeitlichem Auftreten und Bekanntheitsgrad differenziert. Quelle: Gößling-Reisemann (2016)

Dynamik / Art desStressors	bekannt	unbekannt
schleichend	Anpassungsfähigkeit	Innovationsfähigkeit
abrupt	Widerstandsfähigkeit	Improvisationsfähigkeit

Basierend auf den oben beschriebenen allgemeinen resilienzsteigernden Systemfähigkeiten wurde eine Strategie zur Erhöhung der Resilienz von cyber-physikalischen Energiesystemen entwickelt, die auf dem bereits früher entwickelten Design von resilienten Energiesystemen (Acatech et al. 2017) und (Gößling-Reisemann 2016) basiert. Die Strategie gliedert sich in vier Hauptphasen:

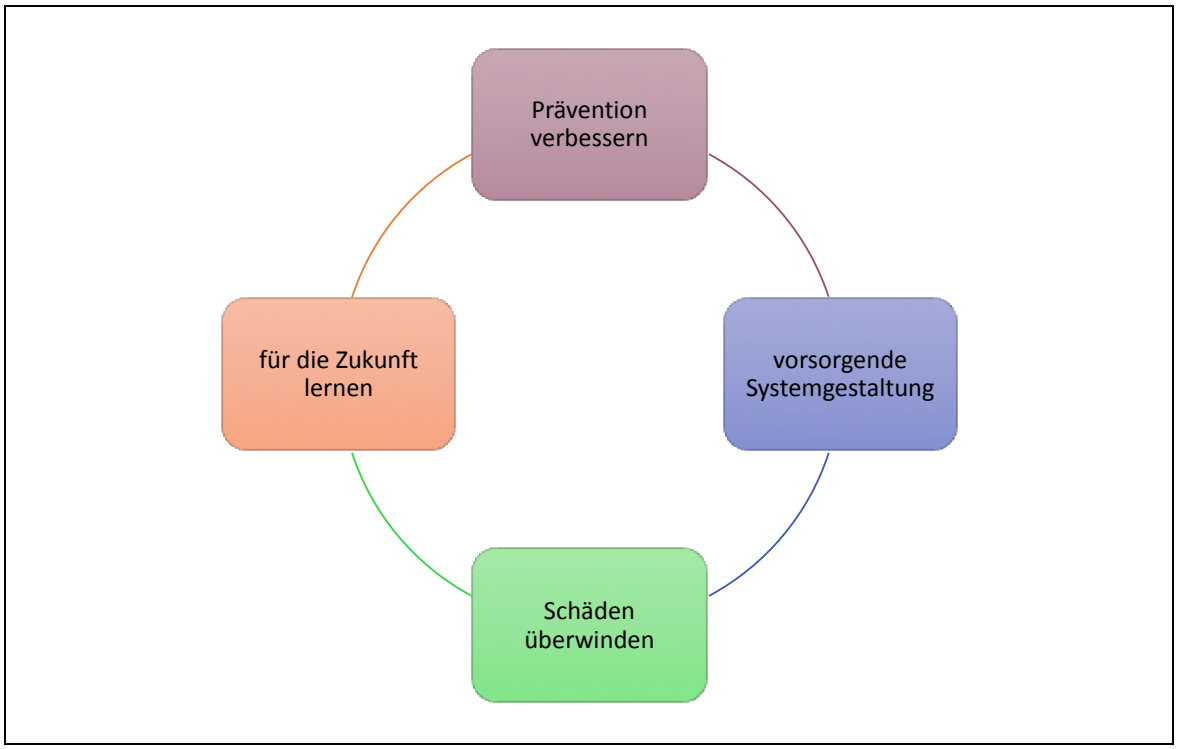

Abb. 5.1: Resilienzstrategiephasen
Strategiephasen basierend auf Acatech et al. (2017)

(1) Vorbereitung und Prävention, (2) Umsetzung eines robusten und vorsorgenden Designs, (3) Krisenmanagement und -bewältigung und (4) Lernen für die Zukunft. Die Expertenaussagen, einschlägige Literatur und eigene Vorschläge wurden zur Ergänzung der Beschreibung der einzelnen

Phasen verwendet. Dies Phasen sind in Abb. 5.1 dargestellt und werden nachfolgend näher beschrieben.

5.1 Vorbereitung und Prävention

Wenn Schwachstellen, Angriffsvektoren und Systemauswirkungen bekannt sind, müssen Gegenmaßnahmen auf der Grundlage traditioneller Risikobewertungs- und Managementverfahren entwickelt werden. Als erster notwendiger Schritt in der Vorbereitungs- und Präventionsphase müssen Schwachstellen im System identifiziert und aus den Ergebnissen wirksame Präventionsmaßnahmen und Leitlinien abgeleitet werden (Acatech et al. 2017). Für diese Aufgaben ist eine gemeinsame Anstrengung und Zusammenarbeit zwischen IT und der Operationstechnik (OT) erforderlich. IT-Cybersicherheit wird in der Regel als Vertraulichkeit, Integrität und Verfügbarkeit von Cyber-Assets angesehen, während die Sicherheit von Energiesystemen auf technischen Entwürfen und Betriebsstrategien basiert. IT- und Energiesystemsicherheit sollten kombiniert werden, um die Resilienz des cyberphysikalischen Energiesystems zu gewährleisten (IEC 2016b).

Verbesserungen bei der Sicherheitsanalyse, der Bedrohungsmodellierung und dem gesamten Systemdesign unterstützen das Ziel, ein resilientes System aufzubauen (Interviewee 13 2017). Risikomanagement und Risikobewertung auf Basis von Modellen und Simulationen helfen, die notwendigen Merkmale von Sicherheitssystemen herauszufinden (Interviewee 18 2017; Interviewee 19 2017). Eine ganzheitliche und umfassende Risikobewertung, die die Überprüfung von Richtlinien und Verfahren sowie die Identifizierung von Assets und Systemen, Kommunikationswegen und Angriffsvektoren, Schwachstellen und Bedrohungsquellen umfasst, wird dazu beitragen, die Höhe des Risikos für Assets und Systeme zu bestimmen. Die Auswertung von Angriffsszenarien und -bäumen wird eine wesentlich genauere Darstellung der Wahrscheinlichkeit liefern, die zu einer Risikominderungsstrategie führt, die besser priorisiert, zielgerichteter und kostengünstiger ist (Bodungen et al. 2017).

Die Rahmen für die Risikobewertung und das Risikomanagement müssen sich auf cyberphysikalische Systeme konzentrieren und die komplexen Zusammenhänge zwischen beiden Infrastrukturen unter Berücksichtigung möglicher Kaskadeneffekte zwischen beiden Infrastrukturen berücksichtigen. Einige Beispiele für Risikomanagement-Tools, die für das IKS oder für Versorgungsnetze entwickelt wurden, finden sich in (Bodungen et al. 2017) und (Schauer et al. 2017). Das Verständnis von Angriffen ist für die Planung und Bewertung von Abwehrmaßnahmen unerlässlich. Die Verwendung eines Ansatzes, der auf Beispielangriffen basiert, ermöglicht eine effektive Kommunikation der Risiken mit den Entscheidungsträgern im Unternehmen. Siehe z.B. den Ansatz mit den Top 20 Cyber-Attacken auf ICS in (Ginter 2017).

Um die Resilienz der ICS weiter zu erhöhen, kommen einige der Standards und gängigen Maßnahmen aus dem Bereich der betrieblichen IT-Sicherheit zur Anwendung, wie z.B. die robuste Programmierung und die Anwendung von Sicherheitsstandards. Im Falle von Stromnetzen wären jedoch spezifischere Sicherheitsstandards erforderlich, die den Aufbau solcher Netze erleichtern (Interviewee 15 2017). Zu diesem Zweck ist eine gemeinsame Anstrengung und Zusammenarbeit zwischen IT- und physischen Systembetreibern erforderlich, um die Möglichkeiten und notwendigen Standards für ein bestimmtes System zu überwachen, da einige Sicherheitsstandards für Computernetzwerke nicht für ICS geeignet sind. Probleme, wie nicht unterstützte Protokolle, müssen in dieser Phase behandelt werden, um spätere Probleme zu vermeiden (Interviewee 1 2016). Wie im Abschnitt zur Vulnerabilitätsanalyse erwähnt, existieren bereits Sicherheitsstandards und -

vorschriften für ICS. Für die Vorbereitung und Prävention ist eine wirksame Umsetzung zur Erhöhung des Sicherheitsniveaus des ICS erforderlich, die jedoch noch fehlt (Bodungen et al. 2017). Wie IT-Experten für ICS erwähnt haben: „[Wir sind der Meinung, dass] die derzeitigen Sicherheitsstandards [für industrielle Kontrollsysteme] nicht schwach sind, aber wahrscheinlich könnte ihre tatsächliche Umsetzung in den Unternehmen einige Schwächen haben“ (Interviewee 15 2017). Die schnelle und effektive Umsetzung bestehender Sicherheitsstandards und -vorschriften ist daher ein wichtiges Thema in dieser Phase.

Die Konsolidierung sowie die Evaluierung bestehender Richtlinien und Best Practices wird Versorgungsunternehmen oder Netzbetreibern helfen, die geeigneten Sicherheitsmaßnahmen für ihr spezifisches System zu finden. So enthält das vom BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW 2015) entwickelte Whitepaper Empfehlungen für alle neu beschafften Leit- und Telekommunikationssysteme für Organisationen der Energiewirtschaft. Der im Rahmen des Projekts SPARKS (Smart Grid Protection Against Cyber Attacks) entwickelte Bericht (siehe (SPARKS Consortium 2016) gibt Empfehlungen zu bestehenden und neuen Standards, die für die Sicherung von Smart Grid-Umgebungen relevant sind, und stützt sich dabei insbesondere auf umfassende Erhebungen zu Smart Grid-Sicherheitsstandards von NIST SP 1180R3 (National Institute of Standards and Technology (NIST) 2014), ENISA Smart Grid Security: Smart Grid-bezogene Normen, Richtlinien und regulatorische (European Network and Information Security Agency (ENISA) 2012) und CEN/CENELEC/ETSI Smart Grid Information Security (CEN-CENELEC-ETSI 2014), um kritische Lücken in bestehenden und in der Entwicklung befindlichen Normen zu identifizieren. Diese identifizierten Lücken betrafen technische Standards im Zusammenhang mit Prozessen wie Risikomanagement, Technologiezertifizierung und Sicherheitssimulation sowie Technologien wie Geräteidentifikation, Protokollspezifikation und Sicherheitsanalyse. Lücken wurden auch in den Leitlinien identifiziert, wie z.B. in den architektonischen Empfehlungen für hybride Architekturen, die sowohl traditionelle zentralisierte Gitter als auch Mikrogitter umfassen.

Darüber hinaus sind effektivere und ansprechendere Sicherheitstrainings- und Sensibilisierungsprogramme für Mitarbeiter von Unternehmen und Mitarbeiter der IT und OT zur Bekämpfung von Angriffen wie Social Engineering von größter Bedeutung für die Vorbereitung und Prävention.

IT-Präventionsmechanismus

Sicherheitsorientiertes Design („Security by Design“) sollte der Standard sein, anstatt nur Sicherheitsfunktionen über Updates und Patches hinzuzufügen, so IT-Experten (Interviewee 13 2017).

Sicherheitsmechanismen sollten aufeinander aufbauen und es sollten mehrere Sicherheitsstufen verwendet werden, um die Gesamtsicherheit des Systems zu gewährleisten. Zum einen ist die Implementierung kryptographischer Methoden für Daten und Kommunikationskanäle erforderlich, um die Datenintegrität zu gewährleisten und eine unbeabsichtigte Weitergabe von Informationen während des Transports zu verhindern. Zum anderen ist die Implementierung von Intrusion Detection Systemen (IDS) erforderlich, um eine effektive Sichtbarkeit der Angreiferaktivitäten zu gewährleisten (Interviewee 13 2017; Interviewee 1 2016).

Doch selbst wenn der Kommunikationskanal sicher ist, können die Endpunkte gefährdet sein. Um die Herausforderungen der End-to-End-Sicherheit zu bewältigen, ist es daher nach Aussage eines IT-Sicherheitsexperten notwendig sicherzustellen, dass es möglich ist, den Sicherheitsverstoß schnell herauszufinden. Sehr wichtige Anforderungen zur Verbesserung der Sicherheit sind die effektive Implementierung von Sicherheitsfunktionen in die Endgeräte im Hinblick auf Authentifizierung und Autorisierung der Nutzung und Kontrolle (Interviewee 5 2016).

Aus Sicht der Sicherheitstechnik ist eine besondere Anforderung die Skalierbarkeit bei der Überwachung, Pflege und Aktualisierung von Endpunkten, da immer mehr Geräte angeschlossen sind, die überwacht, aktualisiert und gewartet werden müssen (Interviewee 5 2016).

Die Implementierung von Trusted Computing-Funktionen ist wichtig für die Integrität von Software/Firmware. Sie besagt, dass es keine sichere Software gibt und dass die Sicherheit hardwarebasiert sein sollte. Eine vertrauenswürdige Plattform, die ein in die Systeme integriertes Hardware-Gerät ist, kann nicht entfernt werden, ohne das System zu zerstören, wodurch die Integrität gewährleistet ist (Interviewee 1 2016).

Weiterhin bezieht sich die Gerätehärtung auf verschiedene Techniken, um die Angriffsfläche der Systemkomponenten zu reduzieren, u.a. durch die Reduzierung der verfügbaren Dienste und Funktionalitäten. Das Schließen unerwünschter Serviceports und das Entfernen nicht benötigter Bibliotheken reduziert die Wahrscheinlichkeit, dass ein Gerät für Sicherheitslücken anfällig ist (Fischer und Lehnhoff 2018). Der zweite Teil des Härtens besteht darin, die Software und Firmware auf dem neuesten Stand zu halten und Patch-Management-Prozesse einzurichten, die Tests zur Behebung von Fehlern an Software und Hardware beinhalten. Die Gerätehärtung erhöht die Fähigkeit eines Systems, laufende Cyber-Angriffe zu absorbieren, indem sie die Komplexität des Auffindens und Ausnutzens von Schwachstellen in den Geräten eines Systems erhöht (Fischer und Lehnhoff 2018).

Bei der Zutrittskontrolle ist die rollenbasierte Zutrittskontrolle (engl. Role-Based Access Control, RBAC) ein gängiger Weg, die Komplexität zu reduzieren, um die Zutrittskontrolle beherrschbar zu machen, wobei die Personen nicht einzelne Personen, sondern funktionale Rollen repräsentieren. Eine Person darf dann in definierten Rollen agieren und jede Rolle hat Rechte als Subjekt in der Zutrittskontrollmatrix (Fischer und Lehnhoff 2018). Die Norm IEC 62351-8 enthält Richtlinien für die Architektur und Implementierung von RBAC in Energiesystemen. Zeitliche Beschränkungen und Rechengrenzen von Geräten machen es unmöglich, vollständige Zugriffskontrollmechanismen bis hinunter zur Feldebene zu haben. Dies kann es erforderlich machen, Bereiche des gegenseitigen Vertrauens zu definieren, in denen keine Authentifizierungs- oder Zugriffsbeschränkungen implementiert sind. Dennoch sollte das Systemdesign explizit den Kontext und die Begründung von Zutrittskontrollentscheidungen angeben, insbesondere unter welchen Umständen kein spezifischer Zutrittskontrollmechanismus auf einem Gerät implementiert ist (Fischer und Lehnhoff 2018).

Um den Datenfluss zwischen den Gruppen besser kontrollieren zu können und einen Angriff zu verhindern, der sich über das gesamte Netzwerk ausbreiten könnte, ist eine Segmentierung in verschiedene Funktionsgruppen unerlässlich. Im ICS sind die grundlegendsten Trennungen zwischen ICS, SCADA und dem Business-Netzwerk möglich, da jedes unterschiedliche Sicherheitsanforderungen hat (Fischer und Lehnhoff 2018).

5.2 Umsetzung eines robusten und vorsorgeorientierten Systemdesigns

Wie bereits erwähnt, erschwert die Unbekanntheit potenzieller zukünftiger Stressoren, die auf das cyberphysikalische System einwirken, die Definition von Maßnahmen zur Prävention oder Vorbereitung. Daher muss sich die zweite Phase der Resilienz des Gebäudes auf die Implementierung eines robusten und vorsorgeorientieren Systemdesigns konzentrieren, um jeder Art von Stressfaktoren zu widerstehen.

Die in Tab. 5.2 zusammengefassten Elemente zur Steigerung der Resilienz stammen aus einer Suche nach Gestaltungsprinzipien und -elementen mit bekannten resilienzsteigernden Eigenschaften, z.B. aus dem Wissen über evolutionäre Prozesse in Ökosystemen oder sozio-technischer Resilienz in Energiesystemen, Organisationen und anderen Anwendungsbereichen. Eine detailliertere Analyse findet sich in (Brand et al. 2017).

Tab. 5.2: Überblick über Prinzipien und Elemente zur Erhöhung der Resilienz von sozio-technischen Systemen
Quelle: Gößling-Reisemann und Thier (2018)

Vielfalt/Diversität	Puffer und Lagerung
Geographische Verteilung	Subsidarität
Redundanz (Anzahl/Funktion)	Modularität/Zellularität
Balance der Rückkopplungsmechanismen (+/-)	(nicht zugeordnet) Ressourcen/Durchhang
Flexible/optionale Kopplung	Flexible Systemanforderungen (Menge/Qualität)

Vielfalt trägt positiv dazu bei, wie ein System auf Stressoren reagieren kann. Um das Konzept der Vielfalt operationeller und potenziell messbar zu machen, schlägt Stirling vor, Vielfalt in Bezug auf Disparität, Vielfalt und Ausgewogenheit zu spezifizieren (Stirling 2007). Unter Disparität versteht man die Unterschiede zwischen den Systemelementen. Vielfalt charakterisiert die Anzahl der verschiedenen Elemente mit der gleichen Funktionalität im System. Das Gleichgewicht wird durch die Verteilung (Mischung) dieser verschiedenen Elemente gegeben (Gößling-Reisemann und Thier 2018). Bei der Anwendung dieser Konzepte auf cyberphysikalische Systeme muss die Vielfalt der Hersteller von IT-Komponenten, Betriebssystemen oder Kommunikationsprotokollen bei der Gestaltung des Systems berücksichtigt werden.

Redundanz beschreibt die Mehrfachverfügbarkeit von Elementen in einem System, entweder in Anzahl oder in funktionaler Äquivalenz. Diese Mehrfach-Elemente werden im Normalbetrieb in der Regel nicht benötigt. Unter numerischer Redundanz versteht man die Bereitstellung mehrerer identischer Elemente mit gleicher Funktion, während sich funktionale Redundanz auf die Situation bezieht, in der dieselbe Funktion durch unterschiedliche Elemente (z.B. durch unterschiedliche Technologien, Betriebssysteme etc.) geliefert wird (Gößling-Reisemann und Thier 2018). Die Redundanz der Kommunikationskanäle oder -geräte muss bei der Auslegung des Systems berücksichtigt werden.

Die **geografische Verteilung** spielt eine wichtige Rolle für die Resilienz. Durch die geografische Verteilung der Systemelemente haben alle lokalisierten Stressoren, von wetterbedingten Ereignissen bis hin zu Terroranschlägen, eine relativ kleine Angriffsfläche (Gößling-Reisemann und Thier 2018). Die Verteilung von systemkritischen Diensten über einen größeren geografischen Bereich erhöht somit die Ausfallsicherheit. Für cyberphysikalische Systeme könnte dies durch geografisch verteilte Steuerungsarchitekturen erreicht werden, eventuell erweitert durch (Mangharam und Pajic 2013), oder basierend auf Multiagentensteuerung (Lehnhoff und Krause 2013).

Die Implementierung von **Puffern und Speichern** in Systemen ermöglicht es dem System, seine Dienste bei internen oder externen Ressourcenbeschränkungen aufrechtzuerhalten. Puffer und

Speicher stellen dem System zusätzliche Kapazitäten zur Verfügung, die kritische Systemzustände nach einer Versorgungsunterbrechung verzögern. Diese Elemente dienen somit mehreren Funktionen, die die Ausfallsicherheit eines Systems erhöhen: Sie entkoppeln Teilsysteme oder Infrastrukturen voneinander und ermöglichen die Funktionsfähigkeit nach Verbindungsabbrüchen; sie verschaffen dem System zusätzliche Zeit für die Wiederherstellung und erleichtern den Wiederherstellungsprozess selbst; wenn sie lokal implementiert werden, können sie dazu beitragen, in Krisenzeiten einen minimalen Service für eine größere Anzahl von Systemnutzern aufrechtzuerhalten (siehe Beispiele in Stromnetzen (Lovins und Lovins 2001). Ein Beispiel ist die Notstromversorgung aus Batterien bei gestörten Übertragungsnetzen (Gößling-Reisemann und Thier 2018). Bei cyberphysikalischen Systemen schlugen die Experten den Einsatz von Backups auf mehreren Ebenen vor. Neben dem trivialen Fall von Energieversorgungs-Backups (USV) sind Backups oder exakte Kopien von digitalen Systemen sowie Daten- und Hardware-Backups erforderlich. Beide sollten auf sichere Weise offline gespeichert werden (Interviewee 2 2016; Interviewee 13 2017). Momentaufnahmen von Systemen vor kritischen Software-Updates sollten verfügbar sein, um die Auswirkungen manipulierter Patches zu minimieren und eine schnelle Wiederherstellung zu ermöglichen.

Ein System, das in Untersegmente unterteilt und aufgeteilt werden kann, wird als **modular/zellulär** bezeichnet, wenn die aggregierten Elemente die volle Systemfunktion in den Untersegmenten bieten. Modularität soll die Reparaturfähigkeit und die Ausfallzeiten in technischen Systemen verbessern, ermöglicht aber auch eine größere Vielfalt, wenn Module mit klar definierten Schnittstellen ausgestattet sind, um den Austausch verschiedener technologischer Implementierungen zu erleichtern (Huang und Kusiak 1998) zitiert in (Gößling-Reisemann und Thier 2018). Bei cyberphysikalischen Systemen kann die Modularität durch die strikte Standardisierung von Schnittstellen und die Verwendung offener Protokolle erreicht werden.

Ein Beispiel für Standardisierungsansätze für Stromverteilungsmanagementsysteme (engl. Distribution Management System DMS) ist die Arbeit des Konsortiums OpenKONSEQUENZ[8] (oK), das deutsche und niederländische Verteilernetzbetreiber, Softwareanbieter, Dienstleister und Forscher zusammenbringt. Die oK treibt die Modularisierung der DMS-Funktionalitäten voran und etabliert eine Referenzarchitektur und Qualitätsstandards, um die bestehende Herstellerbindung und Systemkomplexität zu überwinden. Ziel ist es, die Interoperabilität zu gewährleisten und die Softwareentwicklung unabhängiger und schneller zu machen, während die Softwarequalität erhalten bleibt (Goering et al. 2016).

Die Unterbrechung der Stromversorgung könnte eine der möglichen Folgen eines Cyber-Angriffs sein. Das Ausmaß und die Dauer dieses Ereignisses hängt von der Architektur des Systems ab. Man unterscheidet zwischen einer **zentralen und einer dezentralen Struktur**. Basierend auf den analysierten Interviews werden stark zentralisierte Strukturen mit großen Kraftwerken, zentralen Steuereinheiten und zentraler Datenverarbeitung als weniger resilient angesehen, da sie einen Single Point of Failure darstellen und für Angreifer attraktiver sind. Eine stark dezentrale Struktur gilt jedoch auch nicht als resilient, da sie ein höheres Maß an Koordination und Synchronisation erfordert, um die Leistung und Zuverlässigkeit des Netzes nicht zu beeinträchtigen. Wenn die Koordination in einem dezentralen System stark automatisiert ist, fügt dies eine neue Ebene der Komplexität hinzu und erweitert die Angriffsfläche noch weiter. Ein besserer Weg zu mehr Resilienz könnte mit

[8] https://www.openkonsequenz.de

einer zellulären Struktur erreicht werden, z.B. dem zellulären Ansatz, wie er im (VDE 2015) vorgeschlagen wird, bei dem Erzeugung und Verbrauch in ausreichend großen Zellen ausgeglichen werden. In Deutschland hat der Energieversorger SWW Wunsiedel GmbH eine auf diesem Konzept basierende Lösung entwickelt, die die Segmentierung in kleinere Einheiten aus integrierten Mikrokraftwerken, intelligenten Verbrauchern und Energiespeicherkapazitäten zur Steuerung der Volatilität erneuerbarer Energien und zur Erhöhung der Cybersicherheit vorsieht (Kleineidam et al. 2016a; Kleineidam et al. 2016b).

Für ein stärker strukturorientiertes Element der Resilienzstrategien wurden von den befragten Experten dezentrale physikalische Backup-Systeme diskutiert, die auch bei einem Ausfall zentraler IT- und Kommunikationssysteme eine stabile Stromversorgung innerhalb dezentraler Strukturen gewährleisten können. Sie sollten in der Lage sein, Anpassungen für Systemlasten, Frequenzen und Blindleistungskompensation basierend auf physikalischen Netzparametern durchzuführen, falls die digitale Kommunikation ausfällt.

Im Allgemeinen können Maßnahmen zur Auslegung der Resilienz technische, die die Effizienz betreffen, oder wirtschaftliche Konflikte verursachen. Aus diesem Grund müssen konstruktive Maßnahmen mit einer systematischen Kosten-Nutzen-Analyse bewertet werden, die langfristige Auswirkungen und die Bewertung von Schadenskosten aus seltenen, aber möglichen, extrem schädlichen Ereignissen einschließt (Gößling-Reisemann 2016).

Erkennungsmechanismus

Cyber-Security konzentriert sich darauf, die bösartigen Angreifer außerhalb des Systems zu halten. Cyber-Resilienz sollte jedoch Maßnahmen zur Erkennung und Wiederherstellung umfassen, wenn das System durch einen Angreifer kompromittiert wurde. Sie könnte verschiedene Algorithmen (z.B. maschinelles Lernen, statistische oder Bayesian Netzwerkmethoden u.a.) verwenden, um manipulierte Daten zu identifizieren und als nicht vertrauenswürdig zu kennzeichnen, um als verdächtig behandelt oder ignoriert zu werden (Interviewee 14 2017).

Für die physikalischen Systeme können bestehende Sicherheitsalgorithmen in den Energiemanagementsystemen (engl. Energy Management Systems, EMS), wie z.B. die Zustandsabschätzung des Stromnetzes oder die Erkennung schlechter Daten, genutzt werden, um bei unerwartetem Verhalten Warnungen auszulösen (Friedberg et al. 2015). Die Netzzustandsabschätzung ist eine Technik, mit der Schätzungen von Systemvariablen wie Spannungsgröße und Phasenwinkel (Zustandsgrößen) auf der Grundlage von vermuteten Fehlmessungen von Feldgeräten vorgenommen werden. Der Prozess liefert eine Schätzung der Zustandsgrößen nicht nur, wenn Feldgeräte unvollkommene Messungen liefern, sondern auch, wenn die Leitstelle aufgrund von Geräte- oder Kommunikationskanalstörungen keine Messungen empfängt. Dies gibt dem Betreiber Auskunft über Leistungsflüsse und Spannungsgrößen entlang verschiedener Abschnitte des Übertragungsnetzes und hilft so, betriebliche Entscheidungen zu treffen. Das Kontrollzentrum führt Berechnungen mit Tausenden von Messungen durch, die es über das Wide-Area-Netzwerk erhält (Sridhar et al. 2012). Mehrere Arbeiten wurden für die Entwicklung von Techniken zur Erkennung von schlechten Daten in der Zustandsabschätzung durchgeführt, die gute Schätzungen von Zustandsvariablen trotz Fehlern durch Geräte- und Kanalfehler bieten (Garcia et al. 1979; Handschin et al. 1975; Monticelli und Garcia 1983; Niande et al. 1982; Quintana et al. 1982; Van und Ribbens-Pavella 1985) zitiert in (Sridhar et al. 2012).

Für die Erkennung absichtlicher Angriffe, die darauf abzielen, das Funktionieren der Zustandsabschätzung zu stören (siehe z.B. False Date Injection Attacken in (Liu et al. 2011), müssen zusätzliche Maßnahmen zur Erkennung der bösartigen Daten berücksichtigt werden. Einige Detektionslösungen finden sich in der Literatur. Kosh et al. (2010) untersuchten beispielsweise das Problem der gegnerischen falschen Dateninjektion bei der Schätzung des Zustands des Energiesystems und stellten eine neue Formulierung für das Problem der schlechten Datenerkennung vor. Sie führten eine Heuristik für die Erkennbarkeit eines bestimmten Angriffs durch den Gegner ein, die es erlaubt, besonders schlechte Angriffe für jede Menge von kompromittierten Messungen leicht zu berechnen. In Gaber et al. (2015) wird eine Strategie diskutiert, um das Vorhandensein von schlechten Daten zu erkennen und gleichzeitig abzuschätzen, um die schlechten Daten von den Beobachtungen im Stromnetz trennen zu können.

Für die IKT-Systeme sollten bestehende Sicherheitslösungen, wie z.B. Intrusion Detection Systems (IDS), genutzt werden. Die spezifischen Erkennungsmethoden eines IDS können z.B. ähnliche Regeln wie bei Firewalls sein, die es ermöglichen, Netzwerkverkehr zu erkennen, der gegen Sicherheitsrichtlinien verstößt. Ein IDS kann auch konfiguriert werden, um Aufklärungsaktivitäten wie Host- und Port-Scans zu identifizieren, die auf einen bevorstehenden Angriff hinweisen können (McLaughlin et al. 2015). Wenn Systeme oder Komponenten nicht aktualisiert oder gepatcht werden können, ist es wichtig zu erkennen, ob und wann Systeme kompromittiert wurden (Interviewee 18 2017). Das Open Source Network-based Intrusion Detection System (NIDS) namens Snort[9] ist eines der bekanntesten und meistgenutzten IDS in der Forschungsgemeinschaft. Es kann Protokollanalyse, Inhaltssuche und Inhaltsabgleich in Echtzeit durchführen (McLaughlin et al. 2015).

Anomalie-basierte Detektionssysteme über Kommunikationskanäle ermöglichen die Erkennung und Unterscheidung von Prozessstörungen von verwandten Cyber-Attacken. Sie vergleichen die Definitionen, welche Aktivität als normal angesehen wird, mit den beobachteten Ereignissen, um signifikante Abweichungen zu identifizieren. Die Definition dessen, was normal ist, kann a) schwellenbasiert oder b) profilbasiert sein.

a) Ein schwellenbasierter Prozess kann die Häufigkeit des Auftretens bestimmter Ereignisse überwachen und einen Alarm auslösen, wenn der Schwellenwert überschritten wird. Beispiele in der Kommunikation können die Anzahl der Pakete pro Sekunde, die Größe bestimmter Pakete oder Ströme usw. sein.

b) Die profilbasierte Anomalie-Erkennung konzentriert sich auf die Charakterisierung des bisherigen Verhaltens und die Erkennung von Veränderungen. Dies erfordert in der Regel eine Einarbeitungszeit und eine sorgfältige Auswahl aussagekräftiger Merkmale (McLaughlin et al. 2015).

Eine Studie zu Lösungen für Anomalie-Erkennungs- und Diagnosesysteme auf Basis der Multivariaten Statistischen Prozesskontrolle (engl. Multivariate Statistical Process Control MSPC), die auf die Unterscheidung von Angriffen und Störungen abzielt, findet sich in der Literatur (Iturbe et al. 2016).

Eine weitere Methode zur Erkennung von Angreifern, die versuchen, das System zu übernehmen, könnte sich auf die Untersuchung der Nutzungsmuster der Betreiber und der damit verbundenen

[9] https://www.snort.org/

Datenhistorie stützen, wie ein Experte vorschlug. Die Analyse dieser Nutzungsmuster könnte zeigen, wie die einzelnen Betreiber das System nutzen. Wenn jemand unrechtmäßig erworbene Anmeldedaten aus einer anderen Benutzung verwendet und das System auf eine andere Weise als der rechtmäßige Betreiber betreibt, können diese Abweichungen festgestellt werden. In diesem Zusammenhang ist eine ordnungsgemäße Passwortverwaltung der Schlüssel notwendig, um die unbefugte Verwendung von Anmeldeinformationen zu verhindern (Interviewee 4 2016).

5.3 Krisenmanagement und -bewältigung

Im Falle einer erfolgreichen cyber-physikalischen Störung ist es notwendig, die Krisenbewältigung auf ein möglichst kleines Gebiet oder Subsystem zu verlagern und die Systemdienste so schnell wie möglich wiederherzustellen. Die kritischsten Folgen sind langfristige Stromausfälle. Um den Umfang zu reduzieren, müssen auf regionaler oder lokaler Ebene Notfallplanung und entsprechende Maßnahmen umgesetzt werden (Acatech et al. 2017; Gößling-Reisemann 2016). Das Konzept des Multi-Agenten-basierten dezentralen Regelkonsenses könnte die Stabilität und Sicherheit im Fehlerfall verbessern (Lehnhoff und Krause 2013).

Außerdem muss man wissen, wo der Fehler liegt, um reagieren und das System wiederherstellen zu können. ICT-Monitoring integriert oder gekoppelt mit OT-Monitoring-Systemen ist notwendig, um Fehler in IT-Systemteilen zu erkennen. In den Netzleitstellen werden sowohl IT- als auch OT-Experten benötigt, die in der Lage sein müssen, unterschiedliche IT- und physikalische Infrastrukturen gemeinsam zu handhaben. Die Reaktion auf mögliche Ausfälle sollte im Voraus geplant und umgesetzt werden und nicht nur als Reaktion auf Angriffe und Ausfälle (Interviewee 1 2016; Interviewee 4 2016). Dies erfordert eine aktive Notfallplanung und Übungen mit realistischen Cyber-Attacken. Auch die Überwachung und dynamische Segmentierung ermöglicht die Identifizierung und Isolierung eines gefährdeten Endpunktes (Interviewee 5 2016). Die Segmentierbarkeit hängt mit dem Baukastenprinzip und dem losen (oder optionalen) Kopplungsparadigma zusammen.

Die erforderlichen Wiederherstellungsmechanismen hängen sowohl vom Angriff als auch von den daraus resultierenden Auswirkungen ab. Bei einem Angriff auf das Softwaresystem ist eine Neuinstallation der Programmlogik erforderlich, daher ist eine kompromisslose Sicherung der Steuerungslogik erforderlich. Weiterhin ist eine Aktualisierung der Programmlogik zur Adressierung/Korrektur der Fehler erforderlich (Interviewee 15 2017). Backups auf jeder Softwareebene sind notwendig, um Computer und Terminals nach einem Angriff wiederherzustellen. Auch hier bieten Offline-Backups bessere Sicherheit, da sie nicht von Angreifern kompromittiert werden können (Interviewee 13 2017), obwohl die Installation dieser Backups arbeitsintensiv ist.

Im Falle von Ausfällen in einem zentralen System ist es notwendig, die fehlerhaften Teile zu identifizieren, und es kann hilfreich sein, das System dezentraler zu konfigurieren. Sobald der Wiederherstellungsmechanismus ausgeführt wurde und kompromittierte Komponenten aus Backups eingerichtet wurden, kann die frühere zentralisierte Konfiguration wiederhergestellt werden. So könnte ein System im Fehlerfall allmählich von zentral auf dezentraler und granularer werden und dann wieder zurückgehen. Ein Experte antwortete zu diesem Ansatz, dass „das Arbeiten in kleineren Zellen weniger effizient ist, weil jede Zelle Backup- und Nebenleistungen erbringen muss, aber es ist machbar und praktikabel, solange dies nicht zum allgemeinen Fall wird“. So bald wie möglich sollte das System auf eine zentralere Konfiguration zurückgreifen, die eine effizientere Sicherung und Bereitstellung von Zusatzdiensten ermöglicht (Interviewee 14 2017).

5.4 Für die Zukunft lernen

Vergangene Katastrophen und vermiedene Katastrophen sollten in dieser vierten Phase genutzt werden, um für die Zukunft zu lernen und so die Anpassungsfähigkeit des Systems zu verbessern. Dies kann erreicht werden, indem diese Krisen und Ereignisse dokumentiert und analysiert werden, um die Schwachstellen zu identifizieren, die zu ihrem Auftreten geführt haben (Vulnerability Store). In diesem Sinne würde die digitale Forensik es ermöglichen, Vorfälle und Beinahe-Vorfälle eingehend zu untersuchen und Lehren daraus zu ziehen. Umgekehrt kann die Identifizierung von Stärken, die zur Prävention oder Wiederherstellung beigetragen haben (Solution Store), als Grundlage für Planungsstrategien und Notfallszenarien dienen (Acatech et al. 2017; Gößling-Reisemann 2016).

Das Lernen aus früheren Angriffen könnte die Angriffsfläche, die die verwendeten Bedrohungsagenten verwenden, sowie die Mechanismen des Angriffs aufdecken und dabei helfen, die Oberflächen zu sichern oder Fehler zu beheben. Zum Beispiel ist die Lehre aus Angriffen wie Stuxnet, dass Unternehmen eine bessere Vorbereitung auf Social-Engineering-Angriffe benötigen, was eine bessere Sicherheitsschulung für Mitarbeiter sowie eine angemessene Isolierung von Geschäfts- und Kontrollsystemnetzwerken einschließt (Interviewee 1 2016; Interviewee 13 2017). Der Vorfall mit Stuxnet hat auch gezeigt, dass sich Angreifer mit relativ einfachen Techniken ein vertieftes Wissen über das Zielsystem aneignen können. Sie lehrt ferner, dass zusätzliche Maßnahmen zur Datenspeicherung durchgeführt werden sollten (Interviewee 9 2017; Interviewee 15 2017).

Wenn ein Fehler im System entdeckt und gemeldet wird, warnt dies nicht nur potenzielle Angreifer, sondern auch Hersteller, die dann Gegenmaßnahmen ergreifen können. Werden Mängel nicht gemeldet, sind sie den Herstellern nicht bekannt und können keine Gegenmaßnahmen ergreifen (Interviewee 15 2017). Auch könnten Informationen über erfolgreiche oder erfolglose Angriffe zwischen Unternehmen ausgetauscht werden, um aus Vorfällen zu lernen, vergleichbar mit der Arbeit des CERT-Bundes (Computer Emergency Response Team for Federal Agencies) (Interviewee 19 2017). Besonders abgewehrte Angriffe sollten eine sehr gute Lernquelle sein. Die bisherige Praxis von „don't tell“ müsste durch eine Transparenzregel ersetzt werden, die es erlaubt, aus Fehlern und Erfolgsgeschichten der Vergangenheit zu lernen und gleichzeitig das Recht des Energieanlagenbetreibers auf Schutz seiner kritischen Geschäftsdaten zu wahren.

6 Ermittlung von Optionen zur Ausgestaltung der Rahmenbedingungen für ein resilientes Energiesystem

Bearbeitung und Texterstellung: IÖW

Auf Grundlage der in Kapitel 5 erarbeiteten Ergebnisse wurden Rahmenbedingungen abgeleitet, die zur Verringerung der Vulnerabilität und zur Realisierung einer möglichst hohen und kosteneffizienten Resilienz im Energiesystem notwendig sind.

Dazu muss zunächst vorangestellt werden, dass die Rahmenbedingungen für das Stromsystem in vielen für die Resilienz relevanten Gebieten gerade fundamentalen Veränderungen unterzogen werden, und für einige der laufenden und anstehenden Veränderungen gibt es derzeit auch noch kein klares, abgeschlossenes Bild, wie diese am Ende aussehen werden. Hier sei zum Beispiel das Stichwort der Sektorenkopplung genannt. Dabei sind sowohl Fragen der Technologiewahl und -ausgestaltung, aber auch der generellen Marktordnung und der davon ausgehenden Anreize entscheidend, da diese wiederum neben einem ordnungsrechtlichen Rahmen zur Technologiediffusion und damit letztlich zur grundsätzlichen Systemarchitektur beitragen kann. Schließlich bildet der allgemeine Rahmen für die Digitalisierung, aber auch die Kultur der Nutzung digitaler Strukturen und Devices einen wichtigen Kontext für die hier zu entwickelnden Rahmenbedingungen.

Bei der Festsetzung von neuen Rahmenbedingungen im Kontext der Energiewende bietet sich grundsätzlich die Chance, frühzeitig Resilienzstrategien mit zu berücksichtigen und zu implementieren. Je nach Reichweite der Rahmensetzung handelt es sich dabei auch um für die Resilienz fundamentale Zusammenhänge. Der Fokus in diesem Arbeitspaket lag daher auf der Betrachtung, welche Aspekte oder Elemente in den Rahmenbedingungen für das digitale Energiesystem zu einer Erhöhung der Resilienz führen würden. In Kapitel 6.1 werden zunächst wichtige Rahmenbedingungen, die derzeit für die Stromversorgung gelten, dargestellt und daran anschließend in Kapitel 6.2 Vorschläge formuliert, durch welche geänderten Rahmenbedingungen die Resilienz gesteigert werden könnte. Daran schließt sich ein zusammenfassender Ausblick an, der sich nicht auf punktuelle Handlungsoptionen für die Rahmenbedingungen bezieht, sondern die grundsätzliche Ausrichtung des Stromsystems in den Blick nimmt.

6.1 Wichtige Rahmenbedingungen für die digitale und dezentrale Stromversorgung

Digitalisierungsstrategie der Bundesregierung /Digitalisierungsgesetz

Die Potenziale der Digitalisierung für Infrastrukturen zu nutzen, ist das Ziel der Bundesregierung, für das sie zunächst die Digitale Agenda 2014 – 2017 (BMWi 2014) und daran anschließend die Digitale Strategie 2025 (BMWi 2016) entwickelt hat. Insbesondere der „Intelligenten Vernetzung“ werden große Potenziale zugeschrieben, von der u.a. Leistungssteigerungen, Effizienzgewinne und Wachstum erwartet werden. Um dieses Potenzial zu nutzen, wurde in 2016 das für den Energiebereich relevante Gesetz zur Digitalisierung der Energiewende (Bundestag 2016) beschlossen. Mit dem Gesetz soll die sichere Verbreitung von Smart Grid, Smart Meter und Smart Home in

Deutschland ermöglicht und so die digitale Infrastruktur für eine erfolgreiche Verbindung von Stromerzeugern und großen Verbrauchern vorangetrieben werden. Im Zentrum steht die Einführung intelligenter Messsysteme. Sie dienen als sichere Kommunikationsplattform, um das Stromversorgungssystem energiewendetauglich zu machen.

Während der vergleichsweise hohe Sicherheitsstandard der Smart Meter gegenwärtig dazu führt, dass noch keine Geräte am Markt zugelassen werden konnten, sind bereits eine Vielzahl von anderen Geräten und Tools verfügbar, mit denen Smart Home-Applikationen betrieben werden können. Die Steuerung erfolgt dabei im Regelfall über das Smartphone, das wiederum im Regelfall eine hochgradig unsichere und ungesicherte IKT-Komponente ist. Aber auch der hohe Datenschutz der Smart Meter gemäß Digitalisierungsgesetz und BSI-Standards gilt nicht als absolut sicher, wie durch Experten auf unseren Veranstaltungen und in den Befragungen bestätigt wurde (vgl. hierzu Kapitel 4.2.1).

IT-Sicherheitsgesetz

Für die Betreiber Kritischer Infrastrukturen (KRITIS) gilt das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (Bundestag 2015) und verpflichtet zusammen mit der Verordnung für kritische Infrastrukturen KritisV sowie dem IT-Sicherheitskatalog der Bundesnetzagentur Betreiber Kritischer Infrastrukturen aus den Bereichen Energie, IT und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen zur Umsetzung von Sicherheitsmaßnahmen nach dem Stand der Technik. Eine wesentliche Forderung des genannten Sicherheitskatalogs ist die Einführung eines Informationssicherheits-Managementsystems (ISMS) auf Basis der Normen ISO 27001, ISO 27002 und ISO 27019. Damit werden etwa 2.000 der rund 3,5 Millionen Unternehmen in Deutschland von den gesetzlichen Regelungen adressiert. Im Energiebereich betrifft es Energieerzeuger, Transportnetz- sowie Verteilnetzbetreiber. Das IT-Sicherheitsgesetz adressiert somit insbesondere den Aspekt der Verringerung bzw. Vermeidung der Verwundbarkeit, enthält jedoch keine expliziten Resilienzstrategien.

Die EU-Grid Codes

Mit dem massiven Umbau der Netzinfrastrukturen bestand eine Notwendigkeit, diese Veränderungsprozesse auch in den Rahmenbedingungen für den sicheren Netzbetrieb zu implementieren. Die neuen EU-Grid-Codes beschreiben die Rahmenbedingungen für einen sicheren Netzbetrieb auch mit Energiewandlersystemen im Verteilnetz. Damit wird der Verteilnetzebene viel mehr Verantwortung übertragen, während sie vorher ausschließlich für die Verteilung der elektrischen Energie an die angeschlossenen Kunden zuständig war.

Diese EU-Grid-Codes sind über einen langen Zeitraum erstellt und in den europäischen Rechtsstrukturen verankert worden. Die europäische Union hat sich dabei früh darauf verständigt, dass für diese neuen Aufgaben eines komplett neuen Systemmanagements einfache Vorgaben nicht ausreichen und auch Gesetze nicht sinnvoll sind, da eine Verbindlichkeit in den geforderten Inhalten in allen EU-Mitgliedsstaaten sowie in der zeitlichen Umsetzung gefordert werden muss. Da Vorgaben nicht verbindlich sind und gegen Gesetze juristisch vorgegangen werden kann, wurde der Weg über Verordnungen gegangen, die am dem Tag der Inkraftsetzung rechtsverbindlich, eindeutig und sofort mit der üblichen Frist von drei Jahren umzusetzen sind.

Es sind EU-seitig die folgenden „Network Codes“ als EU-Verordnung veröffentlicht und erlassen worden:

- Verordnung 2016/631 der EU-Kommission zur Festlegung eines Netzkodex mit Netzanschlussbestimmungen für Stromerzeuger („Requirements for Generators – RfG“) (Veröffentlichung am 27.4.2016, Inkrafttreten am 17.5.20116) (Europäischen Union 2016a)
- Verordnung 2016/1388 der EU-Kommission zur Festlegung eines Netzkodex für den Lastanschluss („Demand Connection Code – DCC“) (Veröffentlichung am 18.8.2016, Inkrafttreten am 7.9.2016) (Europäischen Union 2016b)

In Deutschland wurde das Forum Netzbetrieb / Netztechnik im VDE damit beauftragt, die Umsetzung in nationales Regelwerk vorzunehmen, für die folgende Fristen gelten:

- bis zum 17.5.2018 verbindliche Umsetzung aller nationalen Verordnungen, Gesetze etc.
- bis zum 17.5.2019 Ablauf aller Umsetzungsfristen in der Praxis der Netzgesellschaften, Hersteller, Produkte etc.

Ein wichtiges und neues Element des EU-Grid-Codes ist die Forderung von zusätzliche Fähigkeiten an Energiewandlersysteme, mit denen diese ausgestattet sein müssen, um Systemdienstleistungen zu erbringen und zu unterstützen. Die Anforderungen sind abhängig von der Wirkleistung der Anlagen festgelegt und in vier Leistungsklassen unterteilt, die unterschiedliche Eigenschaften nach Tab. 6.1 erfüllen müssen. Grundsätzlich müssen alle Energiewandlersysteme in der Lage sein, Netzfehler als solche zu erkennen und zu überstehen. Die bisherige Strategie, Anlagen bei Netzfehlern vom Netz zu nehmen, wird nicht mehr verfolgt, stattdessen sollen Anlagen so lange wie möglich am Netz betrieben werden. Mit dieser Eigenschaft, aber auch mit der stärkeren Verantwortungszuschreibung auf die Ebene der Verteilnetze werden tendenziell dezentralere Strukturen gestärkt, wie uns die Expertinnen und Experten auf diesem Gebiet bestätigt haben. Dies kann ein Hebel sein, auch weitergehende Resilienzmechanismen auf dieser Ebene zu verankern und die Eigenschaften der Betriebsmittel, die zukünftig von ihnen gefordert werden, als Element zur Stärkung der Resilienz miteinzubeziehen.

Tab. 6.1: Einteilung der Leistungsklassen für Energiewandlersysteme und Anforderungen an Eigenschaften

Typenklasse	**Nationale Leistungsklasse**	**Zu erfüllende Eigenschaften**
Typ A	ab 800 W	großräumiger Systembetrieb und Stabilität inkl. europäischer Regelbetrieb
Typ B	ab 135 kW	Stabile und regelbare automatische Reaktionsfähigkeit in allen Betriebszuständen
Typ C	ab 36 MW	Automatische Reaktion und Unempfindlichkeit gegenüber betrieblichen Ereignissen zzgl. Regelung durch Systemführer
Typ D	ab 45 MW	Basisfähigkeit zum Überstehen großräumiger kritischer Vorgänge, begrenzte automatische Antwort-/Regelfähigkeit

6.2 Vorschläge für Rahmenbedingungen zur Vermeidung eines langanhaltenden Blackouts

6.2.1 IT-Sicherheit

Die Verwundbarkeiten, die die Cybersicherheit betreffen, sind im Rahmen des Projektes ausführlich analysiert und in Kapitel 5 beschrieben worden. Die Angriffsflächen sind sehr vielfältig und in Tab. 4.1 für die Kategorien Technologie, Richtlinien und Verfahren, Menschlicher Faktor und Regulierung zusammenfassend dargestellt. Durch gesetzliche Vorgaben, vor allem durch das IT-Sicherheitsgesetz, gibt der Gesetzgeber Standards für KRITIS-Betreiber verpflichtend vor, um die Cybersicherheit für kritische Infrastrukturen zu erhöhen. Dennoch kann davon ausgegangen werden, dass inhärente Risiken bleiben. Um diese Risiken zu minimieren, wurde im vorhergehenden Kapitel 5 eine Resilienzstrategie vorgestellt, die aus den vier Hauptphasen besteht: (1) Vorbereitung und Prävention, (2) Umsetzung eines robusten und vorsorgenden Designs, (3) Krisenmanagement und -bewältigung und (4) Lernen für die Zukunft. Die einzelnen Phasen beinhalten unterschiedliche Maßnahmen, die zur Umsetzung ergriffen werden können, die ebenfalls dort beschrieben sind.

Während der ersten Phase sollten Schwachpunkte des Systems identifiziert und dementsprechende Sicherheitsmaßnahmen sowie Richtlinien entworfen werden (Acatech et al. 2017). Dabei sollte auch über eine **Ausweitung der Verpflichtung für IT-Sicherheit auf kleinere Betreiber und Hersteller** erfolgen, die aktuell ausgenommen sind. Ggf. ist dies mit entsprechenden Anreizstrukturen bzw. Förderungen zu versehen.

Die zweite Phase der Resilienzstrategie umfasst die Implementierung von robustem und vorsorglichem Design. Anhaltspunkte für ein resilientes Design sind beispielsweise: Diversität der IT-Komponenten in Bezug auf Hersteller, Betriebssysteme und Kommunikationsprotokolle sowie Redundanzen in Kommunikationskanälen und Anlagen. Adaptionsmechanismen, welche Echtzeitüberwachung sowie Angriffserkennungs- und Anomalieerkennungssysteme in Kommunikationskanälen beinhalten, ermöglichen es, Prozessstörungen zu entdecken und sie von Cyber-Angriffen unterscheiden zu können. Hierfür sind Mechanismen / Instrumenten zu entwickeln, die zu den o.g. Resilienzaspekten führen.

In Phase drei des Resilienzmanagements sollte es im Falle eines erfolgreichen cyber-physischen Störfalles in kleinen Bereichen oder Subsystemen möglich sein, die Systemleistung so schnell wie möglich wiederherzustellen. Dies kann mit einer gezielten Abkopplung geschehen, gleichzeitig braucht es dann Strukturen für einen bottom-up-getriebenen Wiederaufbau. Dazu sollten Geschäftskontinuitätspläne, Notfallpläne sowie entsprechende Maßnahmen auf regionaler und lokaler Ebene implementiert werden (siehe dazu auch Kapitel 6.3.1).

Vergangene Katastrophen und vermiedene Ernstfälle sollten in Phase vier genutzt werden, um daraus zu lernen und somit die Anpassungsfähigkeit des Systems zu verbessern. Hierzu zählt, dass Krisen und Ereignisse dokumentiert sowie analysiert werden, um Schwachstellen zu identifizieren. In diesem Sinne würde die digitale Forensik es erlauben, Vorfälle sowie Beinahe-Ausfälle eingehend zu untersuchen und Lektionen daraus zu ziehen. Umgekehrt können die identifizierten Stärken, die zur Vermeidung oder Wiederherstellung beitrugen, als Basis für die Planung weiterer Strategien und Notfallszenarien verwendet werden (Gößling-Reisemann 2016; Acatech et al. 2017).

6.2.2 Betriebsmittel

Die gegenwärtig im Stromnetz genutzten Betriebsmittel haben entweder eine lange historische Entwicklung hinter sich, wie z.B. Transformatoren oder Generatoren, oder aber sind Entwicklungen auf der Basis leistungselektronischer Schaltungen.

Die klassischen Betriebsmittel haben physikalische Eigenschaften, die es ermöglichten, recht einfach gestaltete Infrastrukturen zu bilden, da auf Grund der passiven Eigenschaften das System immer wieder stabile Arbeitspunkte finden kann. Gemeint ist damit, dass im Stromnetz fortwährend Ausgleichsvorgänge stattfinden, die Wechselwirkungen zwischen dem Netz und den Betriebsmitteln verursachen. Die klassischen Betriebsmittel sind in der Lage, auch mit diesen Frequenzen umzugehen, sie wandeln die Energie in Wärme um und dämpfen dynamisch gleichzeitig dadurch das Netz und die Wechselwirkungsprozesse. Im Wesentlichen beruhen die Wechselwirkungen auf einem niederfrequenten Resonanzverhalten.

Leistungselektronisch geführte Betriebsmittel haben ein vollkommen anderes Verhalten. Sie sind historisch abgeleitet aus der Antriebstechnik und verhalten sich wie Anlagen am Netz. Sie sind konzeptionell so aufgebaut, dass ein Betrieb am Netz möglich ist, auf die Netzfrequenz synchronisiert sich ein Betriebsmittel, alle anderen Frequenzen werden „reflektiert“. Das führt zu deutlich verstärktem Resonanzverhalten des Systems, was nicht zielführend ist und Stabilitätsprobleme erzeugt. Üblicherweise betrachtet man bei Stabilitätsuntersuchungen in Stromsystemen immer die unterschiedlichen Effekte um die Nennfrequenz 50 Hz. Das Stromsystem ist aber ein stark nichtlineares System, so dass die Stabilität aller Frequenzkomponenten gesichert sein muss. Die aktuell genutzten Wechselrichter unterstützen diese Sichtweise nicht, sie gehen im Gegenteil davon aus, dass das Netz in der Lage ist, Systemdienstleistungen bereitzustellen, die Wechselrichter benötigen um zu funktionieren, z.B. die Bereitstellung von Kommutierungsblindleistung.

Daher stellt sich die Herausforderung, dass zukünftige Betriebsmittel im Netz folgende Kriterien unterstützen sollen:

- Sicherstellung der Netzverträglichkeit in allen Frequenzbereichen, so dass damit der Anschluss und Betrieb von Anlagen auch bei vermehrt wechselrichtergeführten Systemen möglich ist

- Verursachergerechter Ausgleich der eigenen Einflüsse auf das Netz

- Rückwirkungsarme / -freie Anlagen

- Anlagen müssen „zumutbare“ Dienstleistungen zum sicheren Netz- und Systembetrieb beitragen können

Diese grundsätzlichen Anforderungen sind aktuell in der Diskussion für zukünftige Regelwerke**. Mit den aktuell am Markt befindlichen Anlagen ist ein sicherer Systembetrieb in allen Frequenzen nicht realisierbar und sollte daher in dem Anforderungskatalog für zukünftige Betriebsmittel enthalten sein.**

6.2.3 Zusammenarbeit der Netzbetreiber und Informationsaustausch

Der Aufgaben- und Verantwortungsbereich der Verteilnetzbetreiber hat sich im Zuge der Energiewende deutlich vergrößert. Durch dynamische Verbraucher inklusive Elektro-Fahrzeuge sowie dezentralen Erzeugungsanlagen und Speichern gewinnt der Aufgabenbereich des sicheren Netzbetriebs auf Verteilnetzebene immer mehr an Bedeutung. Gleichsam wird die Betriebsführung aufgrund des immensen Zuwachses an steuerbaren Verbrauchern im Verteilnetz, welche in Abhängigkeit von Marktsignalen das Potenzial haben, mit einer hohen Gleichzeitigkeit ein- und ausgeschaltet werden, deutlich komplexer. Mit der Zunahme marktgetriebener Verbraucher, Speicher, Elektro-Mobilität und volatiler Einspeiser im Verteilnetz müssen die Verteilnetzbetreiber künftig dynamische Netzberechnungen unter der Beachtung der prognostizierten Einspeisung und des Verbrauchs erstellen. Dafür ist es notwendig, Kenntnisse über das erwartete Verbrauchsverhalten zu haben, um so robuste Vorhersagen für alle Erzeugungsanlagen erstellen zu können. Die unterschiedlichen Einspeise- und Verbrauchscharakteristika der angeschlossenen Verbraucherinnen und Verbraucher und Einspeiser sowie deren dynamisches Verhalten haben aber nicht nur Auswirkungen auf das bilanzielle Gleichgewicht zwischen Einspeisung und Verbrauch, sondern auch auf technische Kenngrößen wie Spannung und Blindleistung in den Netzen. Es wird daher nicht genügen, auf aktuelle Netzzustände zu reagieren, sondern eine aktive Steuerung des gesamten Netzes bzw. einzelner Netzknoten bzgl. relevanter Kenngrößen (u.a. Spannung, Blindleistung) durchzuführen (WIBERA 2017). Nur so ist es möglich, drohende Netzengpässe schon frühzeitig zu erkennen und ihnen gezielt entgegenwirken zu können.

Der Einsatz der Flexibilitätsoptionen im Verteilnetz zum sicheren Netzbetrieb und zur Systemstabilität ist daher nur dann möglich, wenn Aufgabe, Verantwortung und Entscheidungshoheit beim jeweiligen Netzbetreiber vereint sind. Eine Kaskade für eine verbindliche Zusammenarbeit der Netzbetreiber soll dies im Notfall gewährleisten, so sieht es der Gesetzgeber im Energiewirtschaftsgesetz vor. Die hierzu erforderlichen Regeln der VDE-ARN 4140 (VDE FNN 2017) wurden von der Branche mit relevanten Stakeholdern entwickelt.

Für die Netzstabilität mit den neuen Betriebsmitteln wird es notwendig, den Frequenzbereich, der beobachtet und unter Kontrolle gehalten werden muss, deutlich zu vergrößern. Die neuen Technischen Anschlussregeln fordern eine Betrachtung der Frequenzbereiche mit dynamischen und statischen Parametern in den Bereichen:

Ca. 0 Hz bis 50 Hz:	Wechselwirkungsprozesse
Um 50 Hz	Betriebs- und Autorisierungskonzepte, Störungsverhalten, RoCoF, Unter- und Überfrequenzcharakteristiken
50 Hz – 2,5 kHz	Power Qualität – mit verursachergerechter Bewertung im Netzanschlusspunkt
2,5 kHz – 9 kHz	Supraharmonische Frequenzen, bewertet in 200 Hz-Bändern
9 kHz – ca. 200 kHz	bisher noch nicht beschrieben, aber z.B. von Industrieelektronik und E-Mobility bereits genutzt – daher sind Rückwirkungen auf Betriebsmittel und System bisher unbekannt

Nach Wibera (2017) erfordert die höhere Systemverantwortung der Verteilnetzbetreiber folgende Anforderungen, die aufgrund der notwendigen statischen und dynamischen Netzstabilität noch erweitert wurden.

- Die Beobachtbarkeit und Steuerbarkeit (BuS) des eigenen Netzes ist zu jedem Zeitpunkt sichergestellt.
- Die dazu notwendige Sensorik und Aktorik ist an den relevanten Netzpunkten im Netz verbaut.
- Dazu ist eine 24/7 besetzte Netzleitwarte (ggf. in Kooperation mit anderen VNB) notwendig.
- Dort wird auch gewährleistet, dass die Kommunikation zu den jeweils vor- bzw. nachgelagerten Netzen über definierte Schnittstellen und Formate zu jedem Zeitpunkt stattfindet und somit die Kommunikationsvorgaben der Kaskade sicher eingehalten werden.
- Die VNB werden zukünftig für ihre Netze Lastfluss- und Netzzustandsprognosen für den Folgetag erstellen. Nur so kann sichergestellt werden, dass tatsächlich die jeweils effizientesten Flexibilitätsoptionen identifiziert werden können.
- In den Bereichen von 0 Hz bis 9 kHz sind entsprechend der Anforderungen der Technischen Anschlussregeln Bewertungen und entsprechende Maßnahmen umzusetzen, um einen stabilen, ungestörten Systembetrieb zu erreichen.
- Dazu gehören weiter Monitoringsysteme, die auf die Lebensdauer sowie Risiken hinweisen, die durch die veränderten Systemeigenschaften entstanden sind. Die neuen Technischen Anschlussregeln verlangen ein Life-Cycle-Management der Netze und der Betriebsmittel und damit eine permanente Anpassung des Systems an die Anforderungen. **Die dazu notwendige Sensorik ist aktuell im Netz nicht vorhanden.**

Hier ist zu beachten, dass durch die zusätzliche Messung von Netzzustandsparametern auch die Kommunikation mit der Netzleitwarte erforderlich wird. Dies birgt gleichzeitig die Möglichkeit der Manipulation der Daten, die ausgetauscht werden sollen. **Daher wird hier eine robuste und sichere Kommunikation erforderlich.**

6.2.4 Sicherung von Rendite für Ausgaben zur Steigerung der Resilienz

Stromnetze gelten als natürliche Monopole, die einer staatlichen Prüfung unterliegen sollen. Damit sollen Anreize für Kostensenkungen bei den Betreibern von Stromnetzen gegeben werden, um diese an Verbraucher weiterzugeben. Es werden den Netzbetreibern Obergrenzen für ihre Entgelte (Price Caps) und Obergrenzen für Erlöse (Revenue Caps) vorgegeben. Um gleichzeitig eine hohe Qualität und Stabilität der Netze zu erreichen, sind zur Sicherstellung von nötigen Netzinvestitionen deshalb bestimmte Regelungen vorgesehen (Investitionspauschalen und Ausnahmegenehmigungen). Eine zusätzliche Qualitätsregelung ermöglicht der Regulierungsbehörde je nach ermittelter Netzqualität Zu- oder Abschläge auf die Netzerlöse einzelner Unternehmen.

Die Vergütung für die Durchleitung von Strom durch Stromnetze wird durch die Stromnetzentgeltverordnung (StromNEV) geregelt, die am 29. Juli 2005 in Kraft trat. Diese Verordnung wurde durch

die Verordnung über die Anreizregulierung der Energieversorgungsnetze (Anreizregulierungsverordnung - ARegV) ergänzt, die seit 1. Januar 2009 die anwendbare Anreizregulierung umsetzt (Bundesregierung 2007). Nach § 19 Qualitätselement in der Regulierungsformel können auf die Erlösobergrenzen Zu- oder Abschläge vorgenommen werden, wenn Netzbetreiber hinsichtlich der Netzzuverlässigkeit oder der Netzleistungsfähigkeit von Kennzahlenvorgaben abweichen (Qualitätselement).

Diese Qualitätselemente sollten durch Resilienzkriterien ergänzt werden, um Anreize für Netzbetreiber zu schaffen, resiliente Strukturen zu implementieren und diese auch durch eine Anerkennung im Rahmen der ARegV vergütet zu bekommen.

6.2.5 Physikalisches Backup

Die Verwundbarkeit der IKT-Infrastruktur ist eine grundsätzliche Gefahr für die Zuverlässigkeit des Stromsystems. Eine Resilienzstrategie könnte sein, das Stromsystem derart aufzubauen, dass vorübergehend ein stabiles System gewährleistet werden, das ohne IKT-Infrastruktur ausschließlich durch netzdienliches Verhalten der Betriebsmittel anhand von Netzparametern aufrechterhalten werden kann.

Es gibt und gab immer wieder Ansätze dazu, Netze auch ohne IKT-Infrastruktur zu führen. Eine Netzführung ist möglich, indem ausschließlich physikalische Signale – nichtlinear der Stabilitätsexponent nach Ljapunov – genutzt wird. Diese Ideen wurden in den früheren Sowjetstaaten ausgearbeitet und auch entsprechend getestet.[10] Forschungen von PD Dr. Fette und weitere Forschungsarbeiten, in denen Netzversuche durchgeführt wurden, haben gezeigt, dass eine Netzführung mit diesen wenigen Größen möglich ist. Allerdings steht dabei keine Grenzwertüberwachung von Betriebsmitteln und Netzen zur Verfügung, um das System stabilisieren und ausbalancieren zu können.

Solange sichergestellt ist, dass die Entropie des Systems geführt werden kann, kann auch die Stabilität des Systems gefunden werden. Dabei müssen bei der Bestimmung der Entropie alle Frequenzkomponenten des Systems eingehen. Entsprechend können Stellgrößen für Betriebsmittel generiert werden.

Zukünftige Regelungskonzepte für Stromsysteme werden solche Komponenten beinhalten, um Entscheidungen für das System aus unterschiedlicher Sichtweise zu gewinnen. Die aktuell genutzten Techniken beruhen im Wesentlichen darauf, dass eine Balancierung der Wirkleistung das System stabilisiert. Für die Frequenz des ganzen Systems stimmt das, für die Sicherstellung der Spannungs- und Blindleistungsstabilität stimmt die Aussage nicht. Hier muss auch das Bifurkationsverhalten der Systeme betrachtet werden.

Auch wenn bereits Praxiserfahrungen zur Führung von Stromsystemen ohne IKT-vorliegen, so besteht für die Etablierung dieses Zustands als eine Resilienzstrategie noch erheblicher Forschungsbedarf.

[10] Dazu wurde in der damaligen Teilrepublik Kasachstan die Netzbetriebsführung auf der Basis der physikalischen Signale des Systems über eine beachtliche Zeit geführt.

6.3 Vorschläge für Rahmenbedingungen für den Fall eines Blackouts

6.3.1 KRITIS-Versorgung im Falle eines Blackouts

Im Falle eines eingetretenen Blackouts ist der Ausfall der kritischen Infrastrukturen die größte Gefährdung für die Bevölkerung. Daher hat die Aufrechterhaltung der kritischen Infrastrukturen zumindest vorübergehend oberste Priorität. Während Teile der kritischen Infrastrukturen mit Notstromaggregaten ausgestattet sind, um unmittelbare Notsituationen zu vermeiden, wie beispielsweise in Krankenhäusern, haben andere Teile der KRITIS eine so große Leistungsaufnahme und benötigen sehr viele dezentrale Komponenten, dass ein vorübergehender Weiterbetrieb nur bedingt durch Notstromaggregate geleistet werden kann, wie beispielsweise bei der Trinkwasserversorgung. Im Falle eines Blackouts könnten daher dezentrale, zumeist erneuerbare Erzeugungsanlagen die Aufgabe übernehmen, in einzelnen Netzabschnitten elektrische Energie bereitzustellen, um gezielt kritische Infrastrukturen zu versorgen. Damit würden einzelne Inselnetze geschaffen.

Dieses Konzept wurde auch in Reichl et al. (2015) unter dem Konzept *NotCluster* vorgestellt und anhand der in Österreich vorhandenen dezentralen Erzeugungsanlagen Berechnungen für die Machbarkeit durchgeführt. Demnach müssen auch im Inselnetzbetrieb die Grundanforderungen an ein Schutzsystem sichergestellt sein, **was nur dann möglich ist, wenn sich das Inselnetz dauerhaft in einem definierten Betriebszustand befindet**. Dabei muss immer eindeutig zwischen Betriebs- und Fehlerfall seitens der Schutzgeräte unterschieden werden können. **Entsprechende Investitionen in die Netzinfrastruktur und in die Schutztechnik sind für einen sicheren und zuverlässigen Inselnetzbetrieb erforderlich.**

Weitere Forschungsprojekte, wie das im Rahmen der Forschungsinitiative der Bundesregierung STROMNETZE geförderte Projekt *LINDA - Netzwiederaufbau mit erneuerbaren Energien* beschäftigen sich mit dem Wiederaufbau bei einer Großstörung durch dezentrale, schwarzstartfähige Anlagen mit einer gesicherten Mindestleistung zunächst für die kritische Infrastruktur.

Die oben zitierten Projekte sind ausschließlich auf das Verhalten von Systemen bei 50 Hz Nennfrequenz ausgelegt. Dabei wird immer davon ausgegangen, dass alle Anlagen ordnungsgemäß funktionieren und stabile Arbeitspunkte gefunden werden können.

Die neuen Betriebsmittel nach den zukünftig geltenden Technischen Anschlussregeln haben deutlich größere Flexibilitäts- und Einstellbereiche, als die bisher bekannten Betriebsmittel. Sie sind daher besser geeignet, eine Wiederherstellung eines Systembetriebs zu unterstützen, müssen allerdings dann auch entsprechend geführt werden. Bisher ist eine entsprechende Infrastruktur im Verteilnetz nicht vorhanden, wird aber zumindest in einzelnen physikalischen Eigenschaften nach den Technischen Anschlussregeln gefordert. Es ist dazu extra die Rolle des Anschlussnetzbetreibers eingeführt worden, die in der Verantwortung ist, die Stabilität seines Netzes in der Spannung und Blindleistung, im Störfall auch in der Frequenz sicher zu stellen.

Allein aus der Aufgabe, Stabilität im Verteilnetz in der Spannung, Blindleistung und Frequenz zu gestalten, Kundenanlagen dazu einzubinden und zu nutzen, kann dazu führen, dass resiliente Eigenschaften der Netze mit geplant und gestaltet werden können. Da der Kunde einen Anspruch darauf hat, eine mit ihm zu vereinbarende Zuverlässigkeit und Verfügbarkeit (Reliability) seines

Netzanschlusses zu gestalten, sind hier Stellschrauben verfügbar, die Resilienzen schaffen können.

6.3.2 Resilienzsteigerung der Bevölkerung

Wenn bei einem langanhaltenden Blackout die Versorgung der Bevölkerung mit dem Notwendigsten nicht mehr mittels der gewohnten Versorgungsketten sichergestellt wird und keine alternativen Versorgungsquellen verfügbar sind, droht die Katastrophe in Form des Rückfalls auf ein vorinfrastrukturelles Versorgungsniveau, ohne dass dafür die entsprechenden Kulturtechniken noch verfügbar sind (siehe auch weitergehende Ausführungen zu diesem Thema in (Bartels und Lorenz 2017)). Bestehende soziale Vulnerabilitäten verweisen daher auf erforderliche Strukturen und Ressourcen zur Vorbereitung auf Versorgungsausfälle sowohl auf Seiten des staatlichen Katastrophenschutzes wie in der Bevölkerung.

Grundsätzlich besteht das Problem, dass staatliche Strukturen ebenfalls von kaskadierenden Infrastrukturausfällen betroffen sein werden. Paradoxerweise wurden parallel zur zunehmenden Vernetzung die Redundanzen und Vorratshaltungen auf staatlicher Seite aus ökonomischen Gründen im Kontext einer nach dem kalten Krieg veränderten Bedrohungswahrnehmung eher zurückgefahren (sog. Friedensdividende). Der Stromausfall im Münsterland 2005 hat jedoch gezeigt, wie schnell der an sich leistungsstarke deutsche Katastrophenschutz in einem einzigen betroffenen Landkreis an seine Grenzen stoßen kann. Grundsätzlich gilt, dass eine lückenlose Ersatzversorgung der Bevölkerung bei größeren Infrastrukturausfällen für den Katastrophenschutz eine unlösbare Aufgabe bleiben wird. In letzter Konsequenz würde dies erfordern, für jedes Infrastruktursystem und seine -leistung entsprechende Redundanzen vorzuhalten, was sowohl logistisch als auch ökonomisch unmöglich sein dürfte.

Angesichts der Grenzen des Katastrophenschutzes und der bestehenden sozialen Vulnerabilitäten stellt sich die Frage nach der Möglichkeit und Grenzen sozialer Resilienz auf Seiten der Bürgerinnen und Bürger. Genauso wenig wie es dem staatlichen Katastrophenschutz gelingen wird, ein Ersatzsystem aufzubauen, können dies die Bürgerinnen und Bürger. Sicherlich ist mit allerhand Kreativität sowie Anpassungsfähigkeit zu rechnen, wie vergangene Infrastrukturausfälle, aber auch andere Katastrophen gezeigt haben (Helsloot und Ruitenberg 2004), aber derartiges Handeln kann allenfalls kürzere Zeiträume überbrücken. Entsprechend wird privaten Haushalten schon seit Jahren empfohlen, Lebensmittel und Wasser für zwei Wochen zu bevorraten (zuletzt in BBK (2017)). Bei einer repräsentativen Umfrage gaben jedoch nur etwa 12 % der Befragten an, über Nahrung für 14 Tage zu verfügen, und nicht einmal 30 % der Haushalte bis zu zwei Tage ohne Wasserversorgung auskommen zu können (Brinkmann et al. 2016). Die Zahlen zeigen, dass zwischen dem behördlich Erwünschten und dem aktuell Umgesetzten große Lücken bestehen. Die Gründe hierfür sind vielfältig. Bevorratung ist aufwendig und gerade in kleinen Wohnungen lassen sich die notwendigen Mengen für eine mehrköpfige Familie schlecht aufbewahren. Bei einer Untersuchung (Menski und Gardemann 2008) sagten knapp 24 % der Personen aus, sich private Lebensmittelbevorratung nicht leisten zu können. Ein weiterer Punkt, und zudem Bedingungsfaktor für den beschrieben Status quo, sind grundsätzliche Defizite in der gesellschaftlichen Kommunikation und Verhandlung von Infrastrukturrisiken sowie entsprechend abgestimmter Gegenmaßnahmen – womit ein zentraler Aspekt zur Steigerung sozialer Resilienz angesprochen ist.

Solange wechselseitig unrealistische Erwartungen hinsichtlich Vorratshaltungen und Notfallplänen bestehen, kann nicht gesellschaftlich verhandelt werden, wie viel Aufwand betrieben werden soll,

um zumindest eine Basisversorgung sicherzustellen, welche Aufgabenteilung zwischen Infrastrukturbetreibern, staatlichem Katastrophenschutz und privaten Haushalten besteht und in wessen Verantwortung das Wohlergehen besonders vulnerabler Gruppen liegt. Kurz, es mangelt gegenwärtig an einer grundlegenden gesamtgesellschaftlichen Risikokommunikation über Infrastrukturrisiken und Bewältigungsstrategien sowie der Angleichung der Erwartungen unterschiedlicher Akteure.

Risikokommunikation wird seitens der zuständigen Behörden und auch der Infrastrukturbetreiber vielfach nur zurückhaltend betrieben, erreicht ihre Adressaten kaum und ist oft in ihrer gegenwärtigen Form nicht geeignet, die intendierten Effekte hervorzurufen. Informationsmaterialien zu Krisensituationen und entsprechende Handlungsempfehlungen sind in der Bevölkerung kaum bekannt (Drews und Raupp 2016). Mit ihnen werden anders als in anderen Ländern die Haushalte nicht proaktiv versorgt, sondern man begegnet ihnen nur, wenn man sie selbst sucht – die Sensibilisierung für das Risiko wird dem Eintritt in die Risikokommunikationsmaßnahme also paradoxerweise bereits vorausgesetzt.

Gelingende Risikokommunikation wird zudem nicht allein durch die Offenlegung von Daten und Fakten oder behördliche Anordnungen erreicht. Stattdessen sollten Bürgerinnen und Bürger in ihren vielfältigen lebensweltlichen Realitäten befähigt werden, ihre jeweilige Situation einzuschätzen und Informationen zu bewerten, die für Entscheidungen im Umgang mit dem Risiko nötig sind (Clausen und Dombrowsky 1990). Sodann sollte Risikokommunikation die spezifischen Vulnerabilitäten in der Gesellschaft berücksichtigen, entsprechende Zielgruppen einbeziehen und Möglichkeiten zur Verringerung der Vulnerabilitäten im gesellschaftlichen Alltag eruieren. Risikokommunikation sollte zudem die Kommunikation der Grenzen staatlicher Katastrophenschutzmaßnahmen und die Notwendigkeit individueller Vorsorge auf Seiten der Bürgerinnen und Bürger umfassen. Dies schließt die Vermittlung von Selbsthilfestrategien unter Berücksichtigung der notwendigen gesellschaftlichen Voraussetzungen, beispielsweise in Form dafür notwendiger Ressourcen, ein.

Eine derartig verstandene breite und aktive Risikokommunikation von Infrastrukturrisiken wäre weit mehr als eine top-down Kommunikation von hinzunehmenden Risiken und individuell vorzuhaltenden Ressourcen, sie wäre vielmehr ein gesellschaftlicher Dialog „wohlinformierter Bürger“ im Sinne des Soziologen Alfred Schütz über Risiken und eine Aushandlung von Verantwortung und Maßnahmen. Gelegenheit für derartigen Dialog gäbe es im Kontext von Infrastrukturveränderungen wie zum Beispiel der Energiewende oder Smart Cities genug, denn diese bergen nicht nur neue Risiken, sondern auch neue Chancen und neue technische Möglichkeiten zur Kommunikation von und über Risiken.

Um ein weiteres Auseinanderdriften von Entscheidern und Betroffenen zu verhindern, müsste eine solche **Risikokommunikation** auch eine gewisse Ergebnisoffenheit hinsichtlich aller zu treffenden Maßnahmen und der zukünftigen gesamtgesellschaftlichen Gestaltung des technischen Unterbaus der Gesellschaft einschließlich der damit verbundenen gesamtgesellschaftlichen Vulnerabilität beinhalten. In einem umfassenden Sinne also soziale Resilienz, die weit mehr ist als materielle Vorräte für Ausfallszenarien, sondern auch zukunftsgewandte Adaptionen und gesellschaftliche Transformation umfasst.

6.4 Zusammenfassender Ausblick

Die Stromversorgung befindet sich in einem Wandel, der alle beteiligten Akteure vor große Herausforderungen stellt. Es gilt neue technische Lösungen für eine zuverlässige Versorgung mit einem

großen Anteil erneuerbarer Energien zu entwickeln, neue Marktteilnehmer zu integrieren und entsprechende Rahmenbedingungen zu gestalten. Dieser Prozess hat begonnen, wird aber noch viele Jahre andauern. Die Transformation des Stromsystems hin zu erneuerbaren Energien erfolgt heute parallel mit seiner Digitalisierung. Diese bietet eine Vielfalt an Vorteilen für die Einbindung dezentraler fluktuierender erneuerbarer Energien durch die Entwicklung von neuen Überwachungs-, Steuerungs- und Betriebsstrategien, sowie viele neue Geschäftsmodelle. Gleichzeitig wird hinsichtlich der Versorgungssicherheit mit elektrischer Energie eine neue kritische Dimension eingeführt, denn durch den zunehmenden IKT-Einsatz im Bereich der Energieversorgung wird diese komplexer und deutlich verwundbarer gegenüber Ausfällen.

In diesem Projekt wurden die durch den vermehrten Einsatz von IKT auftretenden Verwundbarkeiten analysiert und Ansätze für Resilienzstrategien untersucht und daraus Handlungsempfehlungen abgeleitet. Die in den Kapiteln 6.2 und 6.3 beschriebenen Maßnahmen werden als Beiträge zur Steigerung der Resilienz angesehen, mit denen frühzeitig Störungen vermieden werden können, von denen grundsätzlich die Gefahr ausgehen kann, einem Blackout herbeizuführen. Diese Maßnahmen haben sich aus der Projektbearbeitung und aus dem Austausch mit Expertinnen und Experten im Rahmen der Veranstaltungen und Interviews ergeben. Diese Auflistung erhebt damit aber keineswegs den Anspruch auf Vollständigkeit. Des Weiteren wurde während der Projektbearbeitung deutlich, dass mit dem Umgang mit Verwundbarkeiten und der Umsetzung in den Rahmenbedingungen großer Forschungs- und Entwicklungsbedarf besteht. Dieser Bedarf wurde in Ansätzen in den vorangegangenen Kapiteln deutlich gemacht, mit weiteren Forschungsarbeiten ist aber zu erwarten, dass neue Wissenslücken zu Tage treten werden. Die Tab. 6.2 listet die in den vorangegangen Kapiteln aufgeführten Maßnahmen auf. Daran schließt sich eine grundsätzliche Überlegung, die das Design des Stromsystems betrifft und der insgesamt ein höchst relevanter Einfluss auf die Resilienz zugesprochen wird. Für eine abschließende Bewertung und die konkrete Ausgestaltung des Designs sind jedoch noch erhebliche Forschungsarbeiten erforderlich.

Tab. 6.2: Zusammenfassung der Optionen zur Ausgestaltung der Rahmenbedingungen für ein resilientes Energiesystems

Titel	Kurzbeschreibung	Verweis auf Kapitel
Vorschläge für Rahmenbedingungen zur Vermeidung eines langanhaltenden Blackouts		
IT-Sicherheit	Neben der Einhaltung gesetzlicher Rahmenbedingungen für KRITIS-Betreiber die Etablierung einer Strategie zur Erhöhung der Resilienz von cyber-physikalischen Energiesystemen	6.2.1
Betriebsmittel	Erhöhung der Anforderungen an Betriebsmittel für einen sicheren Systembetrieb in allen Frequenzen in Regelwerken	6.2.2
Zusammenarbeit der Netzbetreiber und Informationsaustausch	Verantwortung und Entscheidungshoheit beim jeweiligen Netzbetreiber	6.2.3

	Erweiterung des zu beobachtenden und zu kontrollierenden Frequenzbereichs Monitoringsysteme, die auf die Lebensdauer sowie Risiken hinweisen	
Sicherung der Rendite für Ausgaben zur Steigerung der Resilienz	Ergänzung der Qualitätselemente um Resilienzkriterien im Rahmen der ARegV	6.2.4
Physikalisches Backup	Entwicklung eines Konzepts zur Führung von Netzen ohne IKT-Infrastruktur für den Krisenfall, notwendige Forschungsarbeiten dazu aufnehmen	6.2.5
Vorschläge für Rahmenbedingungen für den Fall eines Blackouts		
KRITIS-Versorgung im Falle eines Blackouts	Etablierung von inselnetzfähigen Notversorgungszentren für die Versorgung von KRITIS durch erneuerbare Energien Entsprechende Investitionen in die Netzinfrastruktur und in die Schutztechnik	6.3.1
Resilienzsteigerung der Bevölkerung	Risikokommunikation von Infrastrukturrisiken als gesellschaftlicher Dialog mit Bürgerinnen und Bürgern über Risiken und eine Aushandlung von Verantwortung und Maßnahmen	6.3.2

Durch die derzeit stattfindende fundamentale Transformation des Stromsystems bietet sich gleichzeitig auch die Möglichkeit, Resilienzstrategien in das Design des Stromsystems zu integrieren. So bieten sich Gestaltungsmöglichkeiten in Bezug auf die Systemarchitektur. Auch wenn das System – im Normalbetrieb - immer ein Zusammenspiel von zentralen und dezentralen sowie digitalen Elementen sein wird, so ist die Grundausrichtung ausgehend von einem zentralen System neu gestaltbar.

Eine Ausprägung der Systemarchitektur, die im Rahmen des Projektes „Strom-Resilienz“ näher untersucht wurde, ist die Granularität des Systems. Damit ist die Größe des kleinsten zu stabilisierenden Netzelements der Stromversorgung gemeint. Extrembeispiele, welche den Begriff der Granularität gut veranschaulichen, sind in diesem Zusammenhang auf der einen Seite ein Stromversorgungssystem, das auf sehr kleinzelligen autarken Einheiten basiert (bis hinunter zu autarken Gebäuden, industriellen Einheiten oder Geräten), und auf der anderen Seite ein stark zentral ausgerichtetes Stromsystem, welches mithilfe von zentralen Steuerungseinheiten und verbleibenden Großkraftwerken eine flächendeckende Versorgung gewährleistet, die auf der Stabilität weniger

großer Zellen basiert. Wie die technische Umsetzung eines feingranularen Systems möglich sein kann, war beispielsweise Gegenstand der Studie „Der zellulare Ansatz“ (VDE 2015).

In diesem Projekt wurde in vielen Diskussionen in den Workshops und der Abschlussveranstaltung der Frage nachgegangen, ob granulare Systeme systemimmanent als resilienter zu bewerten sind. Einigkeit gab es bei den Diskussionen unter den Expertinnen und Experten, dass eher zentral ausgerichtete Systeme andere Verwundbarkeiten aufweisen können als dezentral ausgerichtete Systeme. So sind zentrale Komponenten einzeln betrachtet höchst verwundbar, weil ein Ausfall weitreichende Folgen für die Systemstabilität haben kann, während von kleiner dimensionierten Komponenten in einem dezentralen System nicht so weitreichende Folgewirkungen ausgehen. Andererseits wird eine Verwundbarkeit in der Vielzahl ähnlicher Systemkomponenten (wie Bauteile, Software, Protokolle und Standards) gesehen, die möglicherweise schlechter gesichert oder gewartet werden und daher in der Gesamtheit ein Angriffsziel darstellen können. Insgesamt konnte aus den Diskussionen keine eindeutige Bewertung der verschieden ausgerichteten granularen Systeme hinsichtlich der Resilienz vorgenommen werden. Folglich muss in Bezug auf die Verwundbarkeit de/zentraler IKT-betriebener Energiesysteme trotz aller Lern- und Verbesserungsmöglichkeiten von einer latenten, wenn nicht gar inhärenten Verwundbarkeit ausgegangen werden.

Allerdings können zellulare Konzepte des Energiesystems starke Vorteile bieten, wenn diese so konfiguriert werden, dass auch bei einem flächendeckenden Ausfall der Stromversorgung Teilsysteme mit dem dann verfügbaren erneuerbaren Strom zumindest vorübergehend weiter funktionieren können (siehe dazu Kapitel 6.3.1).

Da die Bedeutung des digitalen Stromsystems für alle anderen (kritischen) Infrastrukturen und damit letztlich für alle Wirtschafts- und Lebensbereiche hochrelevant ist, sollte der Entwicklung einer tragfähigen Resilizenstrategie im Rahmen der Digitalen Agenda der Bundesregierung eine deutlich höhere Aufmerksamkeit zuteilwerden. Darüber hinaus sind derartige Resilienzanforderungen zur Absicherung eines langanhaltenden Blackouts auch im aktuell politisch verhandelten Design des zukünftigen Stromsystems vorzusehen. Zu beiden genannten Themenkomplexen und ihrer Wechselwirkungen bedarf es zudem noch weiterer Forschung sowie Pilotvorhaben, ebenso in Bezug auf konkrete, auf erneuerbaren Energien basierenden Notversorgungskonzepten kritischer Infrastrukturen.

7 Literaturverzeichnis

Acatech, Leopoldina und Akademienunion (2017): Das Energiesystem resilient gestalten: Maßnahmen für eine gesicherte Versorgung. Berlin. http://www.energiesysteme-zukunft.de/publikationen/stellungnahme/das-energiesystem-resilient-gestalten-massnahmen-fuer-eine-gesicherte-versorgung/.

Appelrath, Hans-Jürgen, Henning Kagermann und Christoph Mayer (2012): Future Energy Grid. Migrationspfade ins Internet der Energie. acatech STUDIE. acatech – Deutsche Akademie der Technikwissenschaften, OFFIS e. V., Universität Oldenburg. http://www.acatech.de/feg.

Arghandeh, Reza, Alexandra von Meier, Laura Mehrmanesh und Lamine Mili (2016): On the definition of cyber-physical resilience in power systems. Renewable and Sustainable Energy Reviews 58 (Mai): 1060–1069.

Baig, Zubair A und Abdul Raoof Amoudi (2013): An analysis of smart grid attacks and countermeasures. Journal of Communications 8, Nr. 8: 473–479.

Bartels, Marie und Daniel F. Lorenz (2017): Infrastruktursicherheit als gesellschaftliche Herausforderung. Ökologisches Wirtschaften, Nr. 4/2017: 27–29.

Basagiannis, Stylianos, Rohan Chabukswar, Yi Yang, Kieran McLaughlin und Menouer Boubekeur (2015): Chapter 10 – Implementation Experiences from Smart Grid Security Applications and Outlook on Future Research. In: Smart Grid Security, S. 283–306.

Bauknecht, Dierk, Moritz Vogel und Simon Funcke (2015): Energiewende - Zentral oder dezentral? Diskussionspapier im Rahmen der Wissenschaftlichen Koordination des BMBF Förderprogramms: „Umwelt- und Gesellschaftsverträgliche Transformation des Energiesystems“. Freiburg: Öko-Institut e.V., gefördert vom Bundesministerium für Bildung und Forschung (BMBF). http://www.oeko.de/oekodoc/2368/2015-534-de.pdf.

BBK [Bundesamt für Bevölkerungsschutz und Katastrophenhilfe] (2017): Ratgeber für Notfallvorsorge und richtiges Handeln in Notsituationen. https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Broschueren_Flyer/Buergerinformationen_A4/Ratgeber_Brosch.html;jsessionid=8FCDBB50B9144AF0AC4BF04FA2CD1DE0.1_cid320?nn=4250686.

BDEW [Bundesverband der Energie- und Wasserwirtschaft e.V.] (2015): Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme White Paper Requirements for Secure Control and Telecommunication Systems. https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/OE-BDEW-Whitepaper_Secure_Systems V1.1 2015.pdf.

Becker, C. (2013): Bedrohungsanalyse für Smart Grids und Anpassung des Sicherheitskonzeptes. Bremen: Hochschule Bremen.

BMWi [Bundesministerium für Wirtschaft und Energie] (2014): Digitale Agenda 2014 - 2017. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda-legislaturbericht.html.

BMWi [Bundesministerium für Wirtschaft und Energie] (2016): Digitale Strategie 2025. Bundesministerium für Wirtschaft und Energie. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-strategie-2025.html.

Bodungen, Clint, Bryan Singer, Stephen Hilt, Aaron Shbeeb und Kyle Wilhoit (2017): Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. 1. Aufl. United States: McGraw-Hill Education.

Booz Allen Hamilton (2017): When the lights went out. A comprehensive review of the 2015 attacks on Ukrainian critical infrastructure. McLean, Virginia. https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf.

Brand, Urte, B. Giese, Arnim von Gleich, K. Heinbach und U. Petschow (2017): RESYSTRA. Auf dem Weg zu Resilienten Energiesystemen! Resiliente Gestaltung der Energiesysteme am Beispiel der Transformationsoptionen „EE-Methan-System“ und „Regionale Selbstversorgung“. Schlussbericht.

Breyer, Christian, Berit Müller, Caroline Möller, Elisa Gaudchau, Ludwig Schneider, Kevin Gajkowski, Matthias Resch und Guido Pleßmann (2014): Vergleich und Optimierung von zentral und dezentral orientierten Ausbaupfaden zu einer Stromversorgung aus erneuerbaren Energien in Deutschland. Reiner Lemoine Institut. http://www.bvmw.de/fileadmin/download/Downloads_allg._Dokumente/politik/Studie_zur_dezentralen_Energiewende.pdf.pdf.

Brinkmann, Anna, Joachim Gardemann, Eva Stengel und Karolin Bauer (2016): Ernährungsnotfallvorsorge - Staatliche Strukturen und Tendenzen. In: Neue Stragien der Ernährungsnotfallvorsorge. Ergebnisse aus dem Forschungsverbund NeuENV, hg. v. Ute Menski, S. 43–82. Forschungsforum Öffentliche Sicherheit 18. Berlin.

BSI [Bundesamt für Sicherheit in der Informationstechnik] (2013a): ICS-Security-Kompendium. Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile.

BSI [Bundesamt für Sicherheit in der Informationstechnik] (2013b): TR-03109 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen. Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109-1.pdf?__blob=publicationFile&v=1.

BSI [Bundesamt für Sicherheit in der Informationstechnik] (2014): Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP). Version 1. Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0077V2b_pdf.pdf?__blob=publicationFile&v=1.

BSI [Bundesamt für Sicherheit in der Informationstechnik] (2015a): Das Smart-Meter-Gateway. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf?__blob=publicationFile&v=2.

BSI [Bundesamt für Sicherheit in der Informationstechnik] (2015b): KRITIS-Sektorstudie Energie. Bundesamt für Sicherheit in der Informationstechnik. http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Sektorstudie_Energie.pdf?__blob=publicationFile.

Bundesregierung (2007): Verordnung über die Anreizregulierung der Energieversorgungsnetze (Anreizregulierungsverordnung - ARegV). http://www.gesetze-im-internet.de/aregv/ARegV.pdf.

Bundestag (2015): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf.

Bundestag (2016): Gesetz zur Digitalisierung der Energiewende. https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetz-zur-digitalisierung-der-energiewende.pdf?__blob=publicationFile&v=4.

CEN-CENELEC-ETSI [CEN-CENELEC-ETSI Smart Grid Coordination Group] (2014): SG-CG / M490 / H _ Smart Grid Information Security. ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf.

Cherdantseva, Yulia, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby und Kristan Stoddart (2015): A review of cyber security risk assessment methods for SCADA systems. Computers & Security 56 (Februar): 1–27.

Cherepanov, Anton (2017): WIN32/INDUSTROYER A new threat for industrial control systems. ESET. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.

Cherepanov, Anton und Robert Lipovsky (2017): Industroyer: Biggest threat to industrial control systems since Stuxnet. WeLiveSecurity. 12. Juni. Website: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (Zugriff: 11. April 2018).

Clausen, Lars und Wolf R. Dombrowsky (1990): Zur Akzeptanz staatlicher Informationspolitik bei technischen Großunfällen und Katastrophen. Bonn: Bundesamt für Zivilschutz.

Cleveland, Frances (2016): IEC 62351 Security Standards for the Power System Information Infrastructure.

Detken, Kai-Oliver, Carl-Heinz Genzel, Olav Hoffmann und Richard Sethmann (2014a): Security concept for gateway integrity protection within German smart grids. In: 3rd ASE International Conference on Cyber Security, ASE (Academy of Science and Engineering). Stanford, CA. https://www.spider-smartmetergateway.de/cms/upload/pdf/ECSaR2014_Stanford.pdf.

Detken, Kai-Oliver, Carl-Heinz Genzel, Carsten Rudolph und Marcel Jahnke (2014b): Integrity protection in a smart grid environment for wireless access of smart meters. In: 2014 2nd IEEE International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems, S. 79–86. Offenburg, Germany. https://www.spider-smartmetergateway.de/cms/upload/pdf/IDAACS-Wireless2014_SMGS-Integrity_final.pdf.

DMN [Deutsche Mittelstands Nachrichten] (2014): Hacker stürzen sich auf intelligente Stromzähler. 16. Juli. Website: http://www.deutsche-mittelstands-nachrichten.de/2014/07/64005/ (Zugriff: 14. Oktober 2014).

Dondossola, G., F. Garrone, J. Szanto und F. Gennaro (2008): A laboratory testbed for the evaluation of cyber attacks to interacting ICT infrastructures of power grid operators. In: CIRED Seminar 2008: SmartGrids for Distribution, S. 54–54. http://digital-library.theiet.org/content/conferences/10.1049/ic_20080459.

Dondossola, G., G. Garrone, J. Szanto, G. Deconinck, T. Loix und H. Beitollahi (2009): ICT resilience of power control systems: experimental results from the CRUTIAL testbeds. In: 2009 IEEE/IFIP International Conference on Dependable Systems & Networks, S. 554–559. Juni. http://ieeexplore.ieee.org/document/5270292/.

Dragos Inc. (2017): CRASHOVERRIDE Analyzing the Threat to Electric Grid Operations. https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.

Drews, Julia und Juliana Raupp (2016): Risiko- und Krisenkommunikation im Kontext der Ernährungsnotfallvorsorge. In: Neue Strategien der Ernährungsnotfallvorsorge. Ergebnisse aus dem Forschungsvorhaben NeuENV, hg. v. Ute Menski, S. 119–140. Forschungsforum Öffentliche Sicherheit 18. Berlin. http://www.sicherheit-forschung.de/forschungsforum/schriftenreihe_neu/sr_v_v/sr_18_a.pdf.

ENISA [European Network and Information Security Agency] (2012): Smart Grid Security: Recommendations for Europe and Member States Annex III. Survey and interview analysis. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/survey-and-interview-analysis/view.

ENISA [European Network and Information Security Agency] (2013): Smart Grid Threat Landscape and Good Practice Guide. https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide.

ENISA [European Network and Information Security Agency] (2016): Communication network dependencies for ICS / SCADA Systems. Athens. https://www.enisa.europa.eu/news/enisa-news/attacks-on-ics-scada-how-to-protect-critical-infrastructures.

Europäischen Union (2016a): Verordnung (EU) 2016/631 der Kommission vom 14. April 2016 zur Festlegung eines Netzkodex mit Netzanschlussbestimmungen für Stromerzeuger. http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0631&from=EN.

Europäischen Union (2016b): Verordnung (EU) 2016/1388 der Kommission vom 17. August 2016 zur Festlegung eines Netzkodex für den Lastanschluss. http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R1388&from=EN.

European Network and Information Security Agency (ENISA) (2012): Smart Grid Security: Security Related Standards Guidelines and Regulatory Documents. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/view.

Experten-Workshop 1 (2016): Strom-Resilienz Experten-Workshop 1 Protokoll.

Experten-Workshop 2 (2017): Strom-Resilienz Experten-Workshop 2 Protokoll.

Fischer, Lars und Sebastian Lehnhoff (2018): IT-Security for Functional Resilience in Energy Systems. In: Handbook on Resilience of Socio-technical Systems, hg. v. Matthias Ruth und Stefan Goßling-Reisemann. Edward Elgar.

Friedberg, Ivo, Kieran McLaughlin und Paul Smith (2015): Towards a cyber-physical resilience framework for smart grids. In: 9th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2015, Ghent, Belgium, June 22-25, 2015. Proceedings, hg. v. S. Latré, M. Charalambides, J. François, C. Schmitt, und B Stiller, 9122: S. 140–144. http://link.springer.com/10.1007/978-3-319-20034-7_15.

Gaber, A, K G Seddik und A Y Elezabi (2015): Joint estimation-detection of cyber attacks in smart grids: Bayesian and non-Bayesian formulations. In: 2015 IEEE Wireless Communications and Networking Conference (WCNC):-Track 4 - Services, Applications, and Business Joint, S. 2245–2250. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7127816.

Garcia, A., A. Monticelli und P. Abreu (1979): Fast decoupled state estimation and bad data processing. IEEE Trans. Power Apparat. Syst. PAS-98, Nr. 5: 1645–1652.

Ginter, Andrew (2017): The Top 20 Cyberattacks on Industrial Control Systems. Waterfall Security Solutions. https://static.waterfall-security.com/Top-20-ICS-Attacks.pdf?submissionGuid=1817532c-9229-4b7f-987e-5288b36b017d.

von Gleich, Arnim, Stefan Gößling-Reisemann, Sönke Stührmann, Peer Woizeschke und Birgitt Lutz-Kunisch (2010): Resilienz als Leitkonzept – Vulnerabilität als analytische Kategorie. In: Theoretische Grundlagen für erfolg reiche Klima- anpassungsstrategien, hg. v. K. Fichter und A. von Gleich, S. 13–49. Nordwest20. Aufl. Bremen-Oldenburg.

Goering, Andre, Juergen Meister, Sebastian Lehnhoff, Martin Jung, Matthias Rohr und Peter Herdt (2016): Architecture and Quality Standards for the Joint Development of Modular Open Source Software for Power Grid Distribution Management Systems. In: D-A-CH+ Energy Informatics 2016, S. 36–39. Klagenfurt - Austria. http://www.energieinformatik2016.org/wp-content/uploads/2016/09/Proceedings_DACH-Energy-Informatics_ComForEn-2016-Web.pdf.

Gößling-Reisemann, Stefan (2016): Resilience – Preparing Energy Systems for the Unexpected. In: IRGC Resource Guide on Resilience, hg. v. Igor Link und Valentine Florin. Lausanne: EPFL International Risk Governance Center (IRGC).

Gößling-Reisemann, Stefan und Pablo Thier (2018): On the difference between risk management and resilience management for critical infrastructures. In: Handbook on Resilience of Socio-technical Systems, hg. v. Matthias Ruth und Stefan Goßling-Reisemann. Edward Elgar.

Gößling-Reisemann, Stefan, Jakob Wachsmuth, Sönke Stührmann und Arnim von Gleich (2013): Climate change and structural vulnerability of a metropolitan energy system: The case of Bremen-Oldenburg in Northwest Germany. Journal of Industrial Ecology 17, Nr. 6: 846–858.

Greveler, Ulrich (2016): Die Smart-Metering-Debatte 2010–2016 und ihre Ergebnisse zum Schutz der Privatsphäre. Datenbank-Spektrum 16, Nr. 2 (1. Juli): 137–145.

Grünwald, Reinhard (2014): Moderne Stromnetze als Schlüsselelement einer nachhaltigen Energieversorgung. Berlin: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab162.pdf.

Handschin, E., F. Schweppe, J. Kohlas und A. Fiechter (1975): Bad data analysis for power system state estimation. IEEE Trans. Power Apparat. Syst. PAS-94, Nr. 2: 329–337.

Helsloot, I. und A. Ruitenberg (2004): Citizen response to disasters: A survey of literature and some practical implications. Journal of Contingencies and Crisis Management, Nr. 12/3: 98–111.

Huang, Chun-Che und Andrew Kusiak (1998): Modularity in Design of Products and Systems. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, Nr. 1: 66–77.

ICS-CERT [Industrial Control System Cyber Emergency Response Team] (2016): Cyber-Attack Against Ukrainian Critical Infrastructure. Website: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

IEC [International Electrotechnical Commission] (2016a): Smart Grid Standards Map. Architecture View. Website: http://smartgridstandardsmap.com.

IEC [International Electrotechnical Commission] (2016b): Technical report IEC TR 62351-12 Power systems management and associated information exchange - Data and communications security- Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical sys. 1.0. https://webstore.iec.ch/preview/info_iec62351-12%7Bed1.0%7Den.pdf.

International Electrotechnical Commission (IEC) (2007): Technical IEC Specification TS 62351-1. Power systems management and associated information exchange—data and communications security Part 1: Communication network and system security—Introduction to security issues. Geneva, Switzerland.

Interviewee 1 (2016): .

Interviewee 2 (2016): .

Interviewee 4 (2016): .

Interviewee 5 (2016): .

Interviewee 6 (2016): .

Interviewee 8 (2017): .

Interviewee 9 (2017): .

Interviewee 12 (2017): .

Interviewee 13 (2017): .

Interviewee 14 (2017): .

Interviewee 15 (2017): .

Interviewee 17 (2017): .

Interviewee 18 (2017): .

Interviewee 19 (2017): .

Iturbe, Mikel, Jose Camacho, Iñaki Garitano, Urko Zurutuza und Roberto Uribeetxeberria (2016): On the Feasibility of Distinguishing Between Process Disturbances and Intrusions in Process Control Systems using Multivariate Statistical Process Control. Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W 2016), 2016, Nr. 2: 155–160.

Kleineidam, Gerhard, Georg Jung, Marco Krasser und Bernd Koch (2016a): The Cellular Approach - Security of Micro Smart Grids. In: SPARKS Workshop Nov 2016. https://www.researchgate.net/publication/301231063_The_Cellular_Approach_-_Security_of_Micro_Smart_Grids.

Kleineidam, Gerhard, Marco Krasser und Markus Reischböck (2016b): The cellular approach: smart energy region Wunsiedel. Testbed for smart grid, smart metering and smart home solutions. Electrical Engineering 98, Nr. 4 (Dezember): 335–340.

Knapp, Eric (2011): Chapter 3 – Introduction to Industrial Network Security. In: Industrial Network Security, S. 31–54.

Knapp, Eric und Raj Samani (2013): Chapter 3 – Hacking the Smart Grid. In: Applied Cyber Security and the Smart Grid, S. 57–86.

Kosut, Oliver, Liyan Jia, Robert J. Thomas und Lang Tong (2010): Limiting false data attacks on power system state estimation. In: 44th Annual Conference on Information Sciences and Systems, CISS 2010, S. 1–6. März. http://ieeexplore.ieee.org/document/5464816/.

Kush, Nishchal, Ejaz Ahmed, Mark Branagan und Ernest Foo (2014): Poisoned GOOSE: Exploiting the GOOSE Protocol. In: Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014), Auckland, New Zealand. http://crpit.com/confpapers/CRPITV149Kush.pdf.

Kushner, David (2013): The Real Story of Stuxnet. IEEE Spectrum: Technology, Engineering, and Science News. 26. Februar. Website: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (Zugriff: 10. April 2018).

Langner, Ralph (2013): To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Lehnhoff, Sebastian und Olav Krause (2013): Agentenbasierte Verteilnetzautomatisierung. In: Agentensysteme in der Automatisierungstechnik, hg. v. Peter Göhner, S. 207–223. Berlin Heidelberg: Xpert.press Springer-Verlag. http://link.springer.com/10.1007/978-3-642-31768-2_12.

Lindner, Felix (2014): Licht aus! Sicherheit kritischer Infrastruktur im Test. c't Magazin für Computer Technik, Nr. 9/2014.

Liu, Yao, Peng Ning und Michael K Reiter (2011): False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security 14, Nr. 1: 1–33.

Lopez, Carlos, Arman Sargolzaei, Hugo Santana und Carlos Huerta (2015): Smart Grid Cyber Security: An Overview of Threats and Countermeasures. Journal of Energy and Power Engineering 9, Nr. 7: 632–647.

Lovins, Amory B. und L. Hunter Lovins (2001): Brittle Power -Energy Strategy for National Security. Andover, Massachusetts, USA: Brick House Pub. Co.

Luiijf, Eric (2016): Threats in Industrial Control Systems. In: Cyber-security of SCADA and Other Industrial Control Systems, hg. v. Edward J. M. Colbert und Alexander Kott, S. 69–93. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-32125-7_5.

Lüllmann, Arne (2015): Analyse der Vulnerabilität von Elektrizitätsversorgungssystemen mit unterschiedlich ausgeprägter Integration erneuerbarer Energien. ISI-Schriftenreihe »Innovationspotenziale«. Karlsruhe: Fraunhofer-Institut für System- und Innovationsforschung ISI, gefördert durch das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU). http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-3451039.pdf.

Mangharam, Rahul und Miroslav Pajic (2013): Distributed Control for Cyber-Physical Systems. Journal of the Indian Institute of Science 93, Nr. 3: 353–388.

Marin Fernandes, Pedro (2012): Chapter 11: Introduction to Smart Grid Cyber Security. In: Smart Grid Applications, Communications, and Security, hg. v. Lars Berger und Krzysztof Iniewski, S. 229–320. New Jersey: John Wiley & Sons.

Maynard, Peter, Kieran Mclaughlin und Berthold Haberler (2014): Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks. In: ICS-CSR 2014 Proceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research 2014, S. Pages 30-42. http://dx.doi.org/10.14236/ewic/ics-csr2014.5.

Mayring, Philipp (2014): Qualitative content analysis: theoretical foundation, basic procedures and software solution.

McLaughlin, Kieran, Ivo Friedberg, BooJoong Kang, Peter Maynard, Sakir Sezer und Gavin McWilliams (2015): Chapter 5 – Secure Communications in Smart Grid: Networking and Protocols. In: Smart Grid Security, S. 113–148.

Menski, Ute und Joachim Gardemann (2008): Auswirkungen des Ausfalls Kritischer Infrastrukturen auf den Ernährungssektor am Beispiel des Stromausfalls im Münsterland im Herbst 2005. https://www.fh-muenster.de/humanitaere-hilfe/downloads/Auswirkungen_des_Stromausfalls_05_im_Muensterland.pdf.

Mo, Yilin, Tiffany Hyun-Jin Kim, K. Brancik, D. Dickinson, A. Perrig und B. Sinopoli (2012): Cyber–Physical Security of a Smart Grid Infrastructure. Proceedings of the IEEE 100, Nr. 1 (Januar): 195–209.

Monticelli, A. und A. Garcia (1983): Reliable bad data processing for real-time state estimation. IEEE Trans. Power Apparat. Syst PAS-102, Nr. 5: 1126–1139.

Morgner, Philipp, Stephan Mattejat und Zinaida Benenson (2017a): All Your Bulbs Are Belong to Us: Investigating the Current State of Security in Connected Lighting Systems. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '17, S. 230–240. https://arxiv.org/pdf/1608.03732.pdf http://dl.acm.org/citation.cfm?doid=3098243.3098254.

Morgner, Philipp, Stephan Mattejat, Zinaida Benenson, Christian Müller und Frederik Armknecht (2017b): Insecure to the touch: Attacking ZigBee 3.0 via Touchlink Commissioning. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '17, S. 230–240. Boston, MA, USA. https://www1.cs.fau.de/filepool/publications/wisec2017_touchlink.pdf http://dl.acm.org/citation.cfm?doid=3098243.3098254.

National Institute of Standards and Technology (NIST) (2014): Special Publication 1108R3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. http://dx.doi.org/10.6028/NIST.SP.1108r3.

NESCOR (2015): Electric Sector Failure Scenarios and Impact Analyses – Version 3.0. National Electric Sector Cybersecurity Organization Resource. http://smartgrid.epri.com/doc/NESCOR Failure Scenarios v3 12-11-15.pdf.

New Jersey Cybersecurity & Communications Integration Cell (2017): Stuxnet. NJCCIC. Website: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet (Zugriff: 10. April 2018).

Niande, X., W. Shiying und Y. Erkeng (1982): A new approach for detection and identification of multiple bad data in power system state estimation. IEEE Trans. Power Apparat. Syst PAS-101, Nr. 2: 454–462.

Nissim, Nir, Ran Yahalom und Yuval Elovici (2017): USB-based attacks. Computers and Security 70 (September): 675–688.

NIST (2014): National Institute of Standards and Technology Interagency Report 7628 Rev. 1. National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

von Oheimb, David (2013): IT Security Architecture Approaches for Smart Metering and Smart Grid. In: Smart Grid Security, hg. v. Jorge Cuellar, 7823: S. 1–25. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1. Januar. http://dx.doi.org/10.1007/978-3-642-38030-3_1.

Peter, Stefan (2013): Modellierung einer vollständig auf erneuerbaren Energien basierenden Stromerzeugung im Jahr 2050 in autarken, dezentralen Strukturen. Im Auftrag des Umweltbundesamtes. http://www.umweltbundesamt.de/sites/default/files/medien/376/publikationen/climate_change_14_2013_modellierung_einer_vollstaendig_auf_erneuerbaren_energien.pdf.

Petermann, Thomas, Harald Bradke, Arne Lüllmann, Maik Poetzsch und Ulrich Riehm (2011): Was bei einem Blackout geschieht. Folgen eines langandauernden und großräumigen Stromausfalls. Büro für Technikfolgen- Abschätzung beim Deutschen Bundestag (TAB). http://www.tab-beim-bundestag.de/de/pdf/publikationen/buecher/petermann-etal-2011-141.pdf.

Qi, Junjian, Adam Hahn, Xiaonan Lu, Jianhui Wang und Chen-Ching Liu (2016): Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Physical Systems: Theory & Applications 1, Nr. 1 (Dezember): 28–39.

Quintana, V., A. Simoes-Costa und M. Mier (1982): Bad data detection and identification techniques using estimation orthogonal methods. IEEE Trans. Power Apparat. Syst PAS-101, Nr. 9: 3356–3364.

Reichl, Johannes, Michael Schmidthaler, Kathrin de Bruyn, Gerold Muggenhumer, Lukas Rebhandl, Fabian Frank, Peter Mayr, Hans-Peter Vetö, Gertrud Rossa-Weber, Gerhard Theil, et al. (2015): Blackoutprävention und -intervention. Endbericht. Abschlussbericht. http://www.energieinstitut-linz.at/v2/wp-content/uploads/2016/06/BlackO_2_Endbericht_aa0e3.pdf.

Rubin, Herbert und Irene Rubin (2005): Qualitative Interviewing (2nd ed.): The Art of Hearing Data. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc. http://methods.sagepub.com/book/qualitative-interviewing.

Schauer, Stefan, Sandra König, Martin Latzenhofer und Stefan Rass (2017): Identifying and Managing Risks in Interconnected Utility Networks, S. 79–86. Veranstaltung: SECURWARE 2017, The Eleventh International Conference on Emerging Security Information, Systems and Technologies, 10. September. http://www.thinkmind.org/index.php?view=article&articleid=securware_2017_5_20_30042.

Scherschel, Fabian (2013): Nachholbedarf beim Schutz von industriellen Kontrollsystemen. Heise Security. 12. Januar. Website: http://heise.de/-2057953 (Zugriff: 15. Oktober 2014).

SPARKS Consortium (2016): Deliverable D3.3 Smart Grid Security Standards Recommendations. Hg. v. Paul Murdock. https://project-sparks.eu/wp-content/uploads/2014/04/D-3-3_SmartGridSecurityRecommendations.pdf.

Sridhar, Siddharth, Adam Hahn und Manimaran Govindarasu (2012): Cyber–Physical System Security for the Electric Power Grid.

Stirling, Andy (2007): A general framework for analysing diversity in science, technology and society. Journal of the Royal Society Interface 4, Nr. 15 (22. August): 707–719.

Strauss, Anselm L. und Juliet M. Corbin (2010): Grounded theory: Grundlagen qualitativer Sozialforschung. Unveränd. Nachdr. der letzten Aufl. Weinheim: Beltz.

Tazi, Khadija und Farid Abdi (2015): Review on Cyber-Physical Security of the Smart Grid : Attacks and Defense Mechanisms. 3rd International Renewable and Sustainable Energy Conference (IRSEC): 1–6.

Teixeira, André, Friederich Kupzog, Henrik Sandberg und Karl H. Johansson (2015): Chapter 6 – Cyber-Secure and Resilient Architectures for Industrial Control Systems. In: Smart Grid Security: Innovative Solutions for a Modernized Grid, hg. v. Florian Skopik und Paul Smith, S. 149–183.

Van, Th und Cutsem M Ribbens-Pavella (1985): Bad data identification methods in power system state estimation -a comparative study. IEEE Transactions on Power Apparatus and Systems, Nr. 11. https://www.nvc.vt.edu/lmili/docs/Mili_Bad Data Identification Methods in PS State Estimation_A Comparative Study.pdf.

VDE [Verband der Elektrotechnik, Elektronik, Informationstechnik e. V.] (2015): Der Zellulare Ansatz: Grundlage einer erfolgreichen, regionenübergreifenden Energiewende. VDE-Studie. Frankfurt a. M.: VDE ETG (Energietechnische Gesellschaft im VDE). http://www.vde.com/de/fg/ETG/Arbeitsgebiete/V2/Aktuelles/Oeffenlich/Seiten/VDEETG-StudieDer-ZellulareAnsatz.aspx.

VDE FNN (2017): Kaskadierung von Maßnahmen für die Systemsicherheit von elektrischen Energieversorgungsnetzen (VDE-AR-N 4140). 2. Januar.

VDE ITG [Informationstechnische Gesellschaft im Verband der Elektrotechnik Elektronik Informationstechnik e.V.] (2010): Energieinformationsnetze und -systeme. Bestandsaufnahme und Entwicklungstendenzen. http://www.vde.com/de/fg/ITG/Documents/ITG%20Positionspapier%20Energieinformationsnetze_Webversion.pdf.

VDE ITG [Informationstechnische Gesellschaft im Verband der Elektrotechnik Elektronik Informationstechnik e.V.] (2014): VDE-Positionspapier: Smart Grid Security. Energieinformationsnetze und -systeme.

Virsec (2017): Virsec Hack Analysis: Deep Dive into Industroyer (aka Crash Override). Virsec Systems. 7. Mai. https://virsec.com/virsec-hack-analysis-deep-dive-into-industroyer-aka-crash-override/.

VKU [Verband kommunaler Unternehmen e.V.] (2012): Anpassungs- und Investitionserfordernisse der Informations- und Kommunikations-Technologie zur Entwicklung eines deszentralen Energiesystems (Smart Grid). Endbericht - Kurzfassung. Online nicht verfügbar.

WIBERA [Wirtschaftsberatung AG] (2017): Neue Qualität der Zusammenarbeit von Netzbetreibern im dezentralen Energiesystem. https://www.vku.de/fileadmin/user_upload/Verbandsseite/Sparten/Energiewirtschaft/171109_Gutachten_NQdZ.pdf.

8 Anhang

8.1 Interview-Analyse-Methodik

8.1.1 Experteninterviews

Um adäquate Daten aus relevanten Quellen im Feld zu gewinnen, wurden Experteninterviews als optimale Methode zur Datengenerierung gewählt. Dies erlaubte es uns relevante und aktuelle Informationen direkt von ausgewählten Experten zu beziehen (Rubin und Rubin 2005). Ziel war es, Interviewpartner zu finden, deren langjährige Expertise in der IT- oder Energiebranche einen fundierten Überblick über relevante Themen in diesem Bereich geben kann. Am Ende wurden 19 Interviews mit Experten aus IT, Energie und Märkten geführt. Jedes dieser Interviews wurde auf Englisch geführt, transkribiert und anschließend mittels qualitativer Inhaltsanalyse nach Mayring ausgewertet.

8.1.2 Fragebogen

Berufliche Informationen

1. Welche Ausbildung und welchen beruflichen Hintergrund haben Sie?
2. Welche Position haben Sie zur Zeit? Seit wann?
3. Können Sie Ihre aktuelle Position beschreiben?
   3.1. Was hat das mit Smart Grids zu tun?
   3.2. Wie hängt das mit der Cybersicherheit im Smart Grid zusammen?
4. Sind Sie an einem F&E-Projekt zur Cybersicherheit von Smart Grids in Ihrem Unternehmen beteiligt?
   4.1. Wenn ja, könnten Sie es kurz beschreiben?

Kenntnisse über Studien zur Cybersicherheit in Smart Grids und Risikobewertung

5. Mehrere Standards, Richtlinien und Empfehlungen befassen sich insbesondere mit der Sicherheit und Risikobewertung von Smart Grids im Internet. Ein Beispiel ist der Bericht des U.S. National Institute of Standards and Technology (NIST): "Guidelines for Smart Grid Cyber Security (NIST-IR 7628)".
   5.1. Kennen Sie einige dieser Initiativen?
   5.2. Kennen Sie eine andere Studie zu Fragen der Smart Grid Cyber Security in Deutschland, Europa und/oder weltweit?
      5.2.1. Wenn ja, könnten Sie sie nennen und kurz beschreiben?

Cyber-Sicherheitsschwachstellen in Smart Grids

Unter Berücksichtigung des folgenden Smart Grid-Referenzarchitekturmodells *(siehe (IEC 2016a)) und unter der Annahme einer vollständigen Implementierung der Smart Grid-Funktionalitäten:

6. Welches sind Ihrer Meinung nach die wichtigsten Cybersicherheitsherausforderungen für das Smart Grid, die es zu bewältigen gilt? Warum?
7. Können Sie im Modell der Referenzarchitektur feststellen, welche Komponenten (Energieanlagen oder Informationsbestände) potenziell am anfälligsten sind?
   7.1. Welche davon sind für Ihr Fachgebiet von besonderem Interesse?
   7.2. Aus welchen Gründen?
8. Welche Störungen / Ereignisse können sich auf die Systemleistungen auswirken?
9. Was könnten die potenziellen Auswirkungen dieser Störungen/Ereignisse sein?

10. Welche sind die relevanten Stressoren / Aggressoren für das Auftreten dieser Störungen / Ereignisse?
    a) Menschen
    b) Organisationen
    c) Gefahren
    d) sonstiges: bitte angeben
11. Welche Bedingungen in jedem der folgenden Bereiche erleichtern das Auftreten dieser Störungen / Ereignisse?
    a) Technologie
    b) Organisation/Struktur
    c) Wirtschaft/Regelungen
    d) Kultur/Gesellschaft
12. Im Falle von absichtlichen Störungen, wie ist es möglich, diese Störungen / Ereignisse bei absichtlichen Störungen in die Praxis umzusetzen, sei es in bestehenden oder in zukünftigen Energiesystemen?
    12.1. Was wären die Angriffsmechanismen?
13. Was ist erforderlich oder muss geändert werden, um das Auftreten dieser absichtlichen oder unabsichtlichen Störungen / Ereignisse zu verhindern?

14. Was sind die bestehenden (oder zukünftigen) Anpassungsmöglichkeiten, um die Systemdienste wiederherzustellen?
    14.1. Was könnte auf technischer und organisatorischer Ebene für eine solche Wiederherstellung getan werden?
15. Wie können wir aus vergangenen Ereignissen und den so genannten „Beinaheunfällen“ lernen?
16. Wann und in welchem Umfang können die identifizierten Anpassungsmaßnahmen umgesetzt werden?
17. Wer sind die Akteure und Institutionen, die an der Entwicklung und Regulierung der Umsetzung dieser Anpassungsoptionen beteiligt sind? Von:
    - Energiewirtschaft
    - IT-Bereich
    - Regulierungsbehörden
    - der Markt

System Granularität

In Anbetracht der Entwicklung der Energiesysteme in Bezug auf Produktion, Verbrauch und Kontrolle, die von einem vollständig zentralisierten System zu einem granularen oder dezentralisierten System führt:

18. Wie würde sich die Granularität des Systems auf die Exposition und die Empfindlichkeit gegenüber den zuvor identifizierten Störungen auswirken?
19. Wie würde sich die Granularität des Systems auf die identifizierten Maßnahmen auswirken?

8.1.3 Qualitative Inhaltsanalyse nach Philipp Mayring

Der Schwerpunkt der Methodik der qualitativen Inhaltsanalyse liegt auf dem Aufbau eines Codesystems, das systematisch aus den Befragungsdaten abgeleitet wird und sich dabei an einem methodischen Regelwerk orientiert (Mayring 2014). Bei der qualitativen Inhaltsanalyse liegt der Schwerpunkt auf der Konstruktion und Gründung von Codes auf der Basis von Daten aus zuvor durchgeführten Experteninterviews (Mayring 2014). Codesysteme sind

Ausgangspunkt und Ergebnis der ersten Analyseschritte und tragen zur Zuverlässigkeit dieses methodischen Ansatzes bei. Da diese Methodik auch sehr theoretisch orientiert ist, dienen diese Codes als theoretische Kategorien, die sich an thematischen Aspekten der Daten, Vorkenntnissen und Vorstudien orientieren. Diese Codes wurden mit Textpassagen aus dem Material gefüllt, die relevante Inhalte enthalten, die der thematischen Ausrichtung oder dem Thema des kategorialen Codes entsprechen. Weitere Informationen zum Kodierungsprozess finden Sie in Kapitel 8.1.4 Inhalt der Codierung der die offene Kodierung als Analysewerkzeug behandelt.

Wichtig ist auch, dass der aktuelle Stand der Forschung und die theoretischen Aspekte des Forschungsvorhabens zu jedem Schritt der Inhaltsanalyse beitragen (Mayring 2014). In diesem Projekt haben die Ergebnisse der Literaturrecherche und der Methodik der Vulnerabilitätsanalyse, einschließlich der Ideen, die hinter dieser Methode stehen, einen wesentlichen Anteil an der Durchführung der Inhaltsanalyse.

Ein weiteres Kriterium für die Inhaltsanalyse ist die Objektivität. Dies kann durch die Intercoder-Zuverlässigkeit erreicht werden, die ein Forschungswerkzeug ist, um die Codes verschiedener Forscher zu vergleichen und nach Unterschieden in der Art und Weise zu suchen, wie der Inhalt kodiert wurde. Dieses Tool unterstützt mehrere Forscher und befasst sich mit den Problemen der Standortgrenzen und zu unterschiedlichen Interpretationen des Textmaterial (Mayring 2014). Weiterhin ist eine genaue Bestimmung des verwendeten Basisdatenmaterials sowie dessen Herkunft zu beachten. Das zu analysierende Grundmaterial kann aus allen sprachlichen Daten, Bildern und sogar Videos bestehen. Die häufigste Datenquelle sind transkribierte Interviews (Mayring 2014). Nach der Festlegung einer genauen Fragestellung muss der weitere Analyseprozess abgestimmt werden. Dabei können die Analyseschritte je nach Forschungsthema und der gewählten speziellen Methode der Inhaltsanalyse variieren (Mayring 2014). Diese speziellen Techniken konzentrieren sich auf verschiedene Formen der Verarbeitung von Textdaten: Strukturierung, Erklärung und Verdichtung.

Für dieses Projekt wurde die Technik der Verdichtung gewählt. Ziel war es, das Ausgangsmaterial unter Beibehaltung des Hauptinhalts und der Bedeutung zu reduzieren. Das von (Mayring 2014). vorgeschlagene Standard-Verdichtungsverfahren, das in dieser Studie verwendet wurde, wird kurz beschrieben:

– Nach einer ersten Kodierung wurden die kodierten Textpassagen paraphrasiert, um eine einheitliche Sprachebene zu erreichen. Dabei wurde das ursprüngliche Textmaterial erstmals reduziert, da die Passagen, die beim Sprechen transkribiert wurden, in grammatikalische Abkürzungen umgewandelt wurden. Die wesentlichen Inhalte und Strukturen waren noch in diesen Paraphrasen enthalten, unwichtige Elemente, die keine Bedeutung oder relevanten Inhalte enthalten, wurden gelöscht (Mayring 2014).
– Nach der Paraphrasierung wurde das Material erneut verdichtet. Für diesen Schritt wurde die Abstraktionsebene vereinbart, um diese Paraphrasen zu bearbeiten. Alles unter der gewünschten Ebene wurde zur weiteren Abstraktion und Verallgemeinerung aufbewahrt, alles, was über dieser Ebene lag, wurde beibehalten. Paraphrasen mit gleichem Inhalt wurden integriert und solche ohne relevante Bedeutung weggelassen (Mayring 2014).
– In einer zweiten Reduktionsrunde wurden Paraphrasen ineinander integriert. Auf diese Weise wurden Kategorien auf der gewünschten Abstraktionsebene generiert. In Kombi-

nation damit wurde aus dem Material ein vorläufiges Kategoriensystem mit Zusammenfassungen zu jedem relevanten Thema abgeleitet. Anschließend wurde geprüft, ob das Ausgangsmaterial noch entsprechend dargestellt wurde, indem das ursprüngliche Codesystem, die Kategorien und Paraphrasen überprüft wurden. Wenn die Darstellung der Ausgangsdaten zufriedenstellend war, wurden die Zusammenfassungen weiter reduziert und integriert, bis die gewünschte Konzentration erreicht ist (Mayring 2014).

Beim Aufbau des Codesystems kann dies auf unterschiedliche Weise geschehen: entweder induktiv, deduktiv oder als Mischung aus beidem. Induktiver Aufbau bedeutet, dass bei der Angabe des Codiervorgangs kein Codesystem vorhanden ist. Stattdessen entsteht sie aus den Daten während des Codiervorgangs und der sukzessiven Bündelung des Materials. Codes werden direkt aus dem Material generiert, indem zunächst selektive Kriterien bezüglich des gewünschten Abstraktionsgrades abgeleitet und dann die für das jeweilige Thema relevanten Inhalte ausgewählt werden. Die Forschungsfrage sollte bei diesem Schritt im Auge behalten werden. Während der Codierung wird das Material vollständig betrachtet und die Codes werden konstruiert und mit Codierung gefüllt. Eine erneute Überprüfung und Überprüfung der Codes nach der ersten Codierungsrunde wird notwendig sein, um alle Codes mit dem gesamten Material codieren zu lassen (Mayring 2014).

Die deduktive Konstruktion von Codes beginnt mit einem zuvor generierten Codesystem, das alle theoretischen Hintergründe, Literaturrecherchen und das Forschungsthema berücksichtigt. Dieses vorläufige Codesystem durchläuft dann die oben beschriebenen Prozesse der Kodierung und Zusammenfassung (Mayring 2014).

Die letzte Möglichkeit der Codegenerierung ist deduktiv-induktiv. Es verbindet die Vorteile eines vorläufigen Codesystems, das neben dem theoretischen Hintergrund, der Forschungshypothese und den Vorkenntnissen aufgebaut ist, mit den Fortschritten der Überprüfung, Überprüfung und Überarbeitung des Codesystems während des Kodierungsprozesses (Mayring 2014). Diese Methode wurde in dieser Studie als Ausgangspunkt gewählt, da die Elemente der VA als Codes für das erste Codesystem verwendet werden konnten. Anschließend wurden die Aussagen aus Experteninterviews nach diesen Codes kategorisiert und entsprechend überprüft.

Um den Anforderungen dieses interdisziplinären Methodenmischprojekts gerecht zu werden, musste das Standardverfahren der Inhaltsanalyse geändert werden. Daher wurde der Prozess der Paraphrasierung und Reduktion verkürzt, da die Aussagen der Experten sehr spezifisch und thematisch fokussiert waren. Dies führte dazu, dass größere Textsegmente kodiert wurden. Diese Segmente wurden dann paraphrasiert, um den Fokus auf die gelieferte Bedeutung zu richten und ein konstantes Niveau der Artikulation zu erreichen. Aber anstatt die Segmente der direkten Rede in Abkürzungen zu verwandeln, wurden ganze Sätze konstruiert, um die Struktur der Argumente intakt zu halten und sie für spätere Zusammenfassungen vorzubereiten. Die Paraphrasen wurden dann von jedem Forscher überprüft, um sicherzustellen, dass Inhalt und Bedeutung korrekt extrahiert und verdichtet wurden.

Mit diesen umfassenderen Paraphrasen wurden die ersten Zusammenfassungen für die VA-Methodik erstellt. Der Grund für die Wahl von Paraphrasen, die in ganzen Sätzen und umfassender sind, war, dass sie in der Lage sein sollten, zwischen Aussagen von verschiedenen Experten zu unterscheiden.

Später, als die Phasen für Resilienzstrategien entwickelt und in das Codesystem aufgenommen wurden, wurde das Material erneut mit diesen neuen Kategorien kodiert und paraphrasiert. Diese Paraphrasen wurden auch zusammengefasst, um einen umfassenden Text von jedem wichtigen Code zu erhalten. Diese Zusammenfassungen enthalten verschiedene Aussagen, die wie oben beschrieben gebündelt und reduziert wurden.

Die paraphrasierten Aussagen aus dem Verschlüsselungssystem wurden nach ihrem Thema geordnet, Aussagen zum gleichen Thema, aber von verschiedenen Befragten ineinander integriert. Es wurde Wert daraufgelegt, die spezifische Struktur und Bedeutung von Aussagen intakt zu halten, um zwischen Aussagen verschiedener Experten unterscheiden zu können. Die Zusammenfassungen der verschiedenen Hauptcodes sind im Abschnitt über die Ergebnisse dargestellt.

Im nächsten Abschnitt wird der Prozess der offenen Kodierung näher beschrieben, um zu zeigen, wie Dokumente zunächst analysiert und damit für die Methodik der Inhaltsanalyse vorbereitet wurden.

8.1.4 Inhalt der Codierung

Open Coding, basierend auf der Grounded Theory Methodik von Glaser und Strauss, ist sehr gut geeignet, das Material in einer frühen Analysephase zu öffnen und die ersten Kategorien zu bilden. Dies geschieht durch Klassifizierung, Konzeption und Kategorisierung der Originaldaten (Strauss und Corbin 2010). Durch den ständigen Vergleich während des Prozesses erhalten die Daten Spezifität und Präzision, wobei auch Fragen an das Material gestellt werden - was wird vermittelt, wie wird ausgedrückt, warum wurde genau dieses Wort gewählt, in welchem Kontext wird die Passage, welche Bedeutung wird vermittelt? (Strauss und Corbin 2010). So werden nach und nach immer mehr Konzepte aus den Daten ermittelt, die dann zu Gruppen zusammengefasst werden, aus denen sich Phänomene ableiten lassen (Strauss und Corbin 2010).. Die Konzepte müssen daher entsprechend benannt werden. Dies kann entweder selbst geschehen oder durch in vivo Codes, die direkt aus der Textpassage abgeleitet und übernommen werden (Strauss und Corbin 2010). Nachdem Konzepte und Phänomene abgeleitet wurden, werden die ersten Kategorien erstellt, die Dimensionalitäten enthalten und die Eigenschaften der enthaltenen Konzepte widerspiegeln (Strauss und Corbin 2010).

Es gibt verschiedene Methoden der offenen Codierung. So kann das Material zeilenweise, genauer gesagt Wort für Wort, betrachtet werden. Dies ist der detaillierteste und zugleich effektivste Ansatz, da eine möglichst große Anzahl von Kategorien aus einem Text herausgefiltert werden kann (Strauss und Corbin 2010). Dies ist besonders in frühen Analysephasen wichtig, um eine Fülle von Kategorien zu generieren, die im weiteren Verlauf überprüft und überarbeitet werden können.

Die nächste Kodierungsmethode konzentriert sich auf die Textpassagen pro Satz oder Absatz. Hier werden die Hauptideen der Sektionen herausgefiltert und mit den anderen Konzepten verglichen. Dies ist besonders geeignet, wenn einige Kategorien bereits existieren und in ihrem thematischen Umfeld kodiert werden sollen (Strauss und Corbin 2010).

Ein dritter Ansatz besteht darin, ganze Dokumente zu konsultieren. Hauptziel ist es, Unterschiede zu anderen Dokumenten zu erkennen oder den Gesamtkontext des Dokuments zu

differenzieren (Strauss und Corbin 2010). Offene Codierung führt demnach in besonderer Weise zum Umgang mit dem Ausgangsmaterial, um erste theoretische Bausteine in Form von inhaltlich gefüllten Kategorien abzuleiten. Gerade deshalb ist die Methode geeignet, die Interviewdaten inhaltlich zu analysieren und so zu kategorisieren, dass weitere Analyseschritte folgen können.

Eine weitere Möglichkeit, Dokumente zu kodieren, ist die axiale Kodierung. Die Inhaltsanalyse ermöglicht diesen Schritt nach einer ersten Codierungsrunde, um Daten mit Fokus auf ein bestehendes Codesystem zu prüfen. Es ist aber auch möglich, nur eine axiale Codierung durchzuführen, wenn ein bereits vorhandenes Codesystem validiert werden muss. Dies ist wichtig, um sicherzustellen, dass bestehende Codes als relevante Kategorien ausreichen und genügend Bedeutung enthalten. Das Material wird neben den Codesystemen betrachtet und ständig mit ihnen verglichen. Die strikte Fokussierung auf bestehende Codes, um diese zu erweitern und zu füllen, ist besonders bei Verwendung eines bereits vorhandenen Codesystems erforderlich. In diesem Fall stellt die erste Coding-Runde sicher, dass vorhandene Codes ausreichen oder neu angelegt werden müssen. Eine zweite Codierungsrunde stellt sicher, dass alle Dokumente in den neueren Codes enthalten sind und ob vorhandene Codierungen noch in den richtigen Kategorien sind. Nach Abschluss der zweiten Codierungsrunde sollte das Codesystem präziser und strukturierter sein. Ist dies nicht der Fall, können weitere Codierungs- und Umschlüsselungsrunden durchgeführt werden, bis eine zufriedenstellende Strukturierung und Sättigung erreicht ist (Mayring 2014).

Im Folgenden wird der in dieser Studie durchgeführte Kodierungsprozess beschrieben:

– Textsegmente aus der Interviewtranskription wurden mit Kategorien codiert, die ein bestimmtes Thema enthielten. Diese Themen könnten sein: allgemeine Informationen über Fachinformationen, oder es könnten Inhalte sein, die für Kategorien der VA oder für die Resilienzstrategien relevant sind. Der gesamte Text, der ein bestimmtes Thema enthält, wurde in die entsprechende Kategorie sortiert.
– Die erste Runde der Kodierung kombiniert die Vorteile der offenen Kodierung mit dem Fokus einer axialen Kodierung.
– Wie bei der offenen Codierung wurden aus dem Material neue Codes abgeleitet und das Material zunächst in Codierung zerlegt. Die axiale Codierung mit dem Initialcodesystem (siehe Tab. 8.1) sorgte dafür, dass die Codes in diesem Codesystem entsprechend gefüllt wurden und gewann damit an Sicherheit und Gültigkeit.
– Es war auch wichtig, dass jeder Forscher eine vollständige Codierung, einschließlich aller Dokumente, durchgeführt hat. Danach wurde das Codesystem von jedem Forscher komplett neu codiert. In diesem Schritt wurde jede Kodierung innerhalb eines Codes vollständig betrachtet, wobei der Schwerpunkt auf der Überprüfung der folgenden Punkte lag: (a) wenn die Codierung zum richtigen Code gehört oder ob eine weitere Strukturierung erforderlich war, (b) wenn der Code noch seine ursprüngliche thematische Ausrichtung aufweist, (c) wenn der Code genügend Inhalt enthält, um eine Kategorie zu erhalten, oder (d) wenn der Code ein Untercode eines anderen größeren Codes sein muss.
– Das Forschungsteam überprüfte gemeinsam das resultierende Codesystem, das während dieses Analyseschrittes große Veränderungen erfuhr, da beschlossen wurde, die Struktur zu ändern und die Phasen der Resilienzstrategien und einige Strukturierungen für Teile, die Elemente der VA betreffen, einzubeziehen. Mit diesem neuen Codesystem folgte eine weitere Runde der Codierung und Umschlüsselung.

Das resultierende Codesystem (siehe Tab. 8.2) erwies sich als zuverlässig, um den Inhalt zu erfassen, der von befragten Experten geliefert und später in theoretische Phasen zusammengefasst wurde, die sich aus der VA-Methodik ergeben.

Tab. 8.1 Initialcodesystem

Liste der Codes
Codesystem
Working domain
Challenges
Open category
Professional and educational background
Current job position
Research project
Regulations
Vulnerable assets
Human resources
Administrative staff
Electrical Operators
IT operators
Cyber infrastructure assets
Electrical infrastructure assets
Perturbations
External perturbation
Internal perturbation
Potential impacts
Cyber infrastructure
Confidentiality
Non-repudiation
Availability
Integrity
Electrical infrastructure
Power outages
Large power outage
Small power outage
Qualitative Criteria
Indirect Parameters
Public acceptance
Economic impacts
Impacts on technical parameters
Stressors
Other
Hazards
Degradation
Human errors

Organizations
People
External stressor (P)
Internal stressor (P)
Conditions
Other
Society
Regulations (conditions)
Economy
Organization
Technology
Attack mechanisms
Feasibility
Motivation
Level
Effort
Knowledge
Adaptation strategies
Preparation
Challenges (Prep)
Prevention
Challenges (Prev)
Detection
Challenges (Det)
Response
Challenges (Resp)
Recovery
Challenges (Rec)
Learning
Challenges (Lear)
Implementation of adaptation strategies
Willingness to implement
Readiness to implement
Actors involved
Market
Others
Regulatory authorities
IT sector
Energy sector
Granularity of the system
Low granularity
High granularity

Tab. 8.2 Endgültiges Codesystem

Liste der Codes
Codesystem
New Categories
Insecure communications
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts
Adaptation strategies, implementation
Insecure End-Points
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts
Adaptation strategies, implementation
Insecure interface between components of different vendors
Exposure and Sensitivity
Attack mechanism and Perturbations
Adaptation strategies, implementation
improper change and configuration management
Incorrect setings damage the system or allow to get access
Software and firmware allows unauthorized modification
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts
Adaptation strategies, implementation
Systems running in web services
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts
Adaptation strategies, implementation
Lack of “expert” operators
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts
Adaptation strategies, implementation
Lack of IT-OT experts in the organization
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts
Adaptation strategies, implementation
Improper network segregation
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts

Adaptation strategies, implementation
Improper security patch management
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts
Adaptation strategies, implementation
Lack of effective implementation of security standards
Exposure and Sensitivity
Potential impacts
Adaptation strategies, implementation
Lack of security awareness in the organizations
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts
Adaptation strategies, implementation
Lack of security awareness among consumers
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts
Adaptation strategies, implementation
No economic incentives to invest / lack of coordinated effort
Exposure and Sensitivity
Attack mechanism and Perturbations
Potential impacts
Adaptation strategies, implementation
System malfunctions
Exposure and Sensitivity
Potential impacts
Adaptation strategies, implementation
Failure scenarios
Resilience Strategies
Implementation of adaptation strategies
Willingness to implement
Readiness to implement
Challenges for Resilience
Challenges (Prep)
Challenges (Prev)
Challenges (Det)
Challenges (Resp)
Challenges (Rec)
Challenges (Lear)
Adaptation strategies
Prepare and prevent
Preparation
Prevention

Implementation of robust and precautionary design
Detection
Manage and recover from crisis
Response
Recovery
Learn for the Future
Learning
Granularity of the system
Failures and Malfunctions
Attacks and Impacts
Security Solutions and Response Mechanisms
Cells and Micro Grids
Centralized Architectures
Decentralized Architectures
General Codes
Actors involved
Open category
Challenges
Regulations
Experts Information and Research Projects
Research project
Professional and educational background
Working domain

GESCHÄFTSSTELLE BERLIN
MAIN OFFICE
Potsdamer Straße 105
10785 Berlin
Telefon: + 49 – 30 – 884 594-0
Fax: + 49 – 30 – 882 54 39

BÜRO HEIDELBERG
HEIDELBERG OFFICE
Bergstraße 7
69120 Heidelberg
Telefon: + 49 – 6221 – 649 16-0
Fax: + 49 – 6221 – 270 60

mailbox@ioew.de
www.ioew.de