dena
Deutsche Energie-Agentur

Future Energy Lab

dena-GUTACHTEN

# EnerCrypt

Cyberinnovationen für das sichere Energiesystem der Zukunft

# Impressum

**Herausgeber**
Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin
Tel: +49 (0)30 66 777-0
Fax: +49 (0)30 66 777-699
E-Mail: futureenergylab@dena.de
Internet: www.dena.de
www.future-energy-lab.de

**Autoren**
Mathias Böswetter, dena

Lennart Bader, Fraunhofer FKIE
Martin Henze, Fraunhofer FKIE
Michael Rademacher, Fraunhofer FKIE
Ömer Sen, Fraunhofer FIT
Dennis van der Velde, Fraunhofer FIT
Michael Andres, Fraunhofer FIT

**Bildquelle:**

shutterstock/TippaPatt

**Stand:**

12/2021



**Bitte zitieren als:**

Deutsche Energie-Agentur (Hrsg.) (dena, 2021) „EnerCrypt – Cyberinnovationen für das sichere Energiesystem der Zukunft“

Bundesministerium für Wirtschaft und Klimaschutz

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

# Inhaltsverzeichnis

**Vorwort** ..... **2**

**1 Einleitung** ..... **5**

**2 Entwicklungen und Trends in der digitalen Energiewirtschaft** ..... **7**

2.1 Entwicklungen und Trends in der Energiewirtschaft ..... 7

2.2 Innovationen im Bereich der digitalen Kommunikation ..... 11

2.2.1 Kabelgebundene Kommunikation ..... 13

2.2.2 Drahtlose Kommunikation ..... 13

2.2.3 Dedizierte und öffentliche Infrastruktur ..... 15

2.3 Cyberinnovationen durch den Einsatz allgemeiner Zukunftstechnologien ..... 16

2.3.1 Wegbereitende Technologien für anwendungsorientierte Innovationen ..... 16

2.3.2 Zukunftstechnologien für Cybersicherheit in Energienetzen ..... 20

2.4 Cybersichere Ertüchtigung energietechnischer Infrastruktur ..... 25

**3 Innovative Anwendungsfälle in einer Bedrohungslandschaft im Wandel** ..... **29**

3.1 Neue Anwendungsfälle durch technologischen und strukturellen Wandel ..... 29

3.1.1 Netzbetreiberorientierte Anwendungsfälle ..... 29

3.1.2 Kundenorientierte Anwendungsfälle ..... 31

3.2 Historische Angriffsvektoren und Cyberbedrohungen der Zukunft ..... 32

3.2.1 Analyse historischer Cyberangriffe und Forschungsergebnisse ..... 33

3.2.2 Cyberbedrohungen im Energiesystem der Zukunft ..... 36

3.3 Regulierungen und Standards zur KRITIS-Cybersicherheit ..... 37

**4 Cybersicherheit als energiewirtschaftlicher Innovationstreiber** ..... **41**

4.1 Status quo der energiewirtschaftlichen Innovationen auf nationaler Ebene ..... 41

4.2 Fallstudie: Messstellenbetrieb und SMGW-Infrastruktur in Deutschland ..... 45

4.2.1 SMGW-Infrastruktur und Rollout ..... 45

4.2.2 Sicherheitskonformer Einsatz von SMGW-Infrastruktur ..... 47

4.3 Transition zu einer cybersicheren Umgebung für den Energiesektor ..... 50

**5 Maßnahmen zur Förderung energiewirtschaftlicher Cyberinnovationen** ..... **54**

5.1 Fördermaßnahmen für Cyberinnovationen ..... 54

5.2 Rollout intelligenter Messsysteme im internationalen Vergleich ..... 57

5.3 Lösungsstrategien zur Innovationsförderung in der deutschen Energiewirtschaft ..... 59

**6 Fazit und Zusammenfassung** ..... **62**

**Abkürzungsverzeichnis** ..... **64**

**Literaturverzeichnis** ..... **67**

# Vorwort

**Eine energiewendegerechte Cybersicherheit braucht Innovationen.** Das Gutachten EnerCrypt der Deutschen Energie-Agentur (dena) geht der Frage nach, welche Innovationspotenziale für Cybersicherheit in der Energiewende stecken – und wie sehr diese auf Cyberinnovationen angewiesen ist, damit die Transformation des Energiesystems den steigenden Bedrohungen aus dem Cyberraum gewachsen bleibt. Das Gutachten möchte damit auch einen Diskussionsbeitrag leisten, um das Thema Cybersicherheit in der Energiewirtschaft als Innovationsthema und als einen energiewendegerechten Gestaltungsfaktor zu setzen.

In einem derart stark regulierten Sektor herrscht bisher ein anderes Verständnis: Cybersicherheit ist aus Sicht der Energiewirtschaft zuallererst ein durch Compliance und Zertifizierungen bestimmter Faktor, der Kosten und Aufwände erzeugt. Aus Sicht des Regulators folgen die Anforderungen der einschlägigen Gesetze (IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0), BSI-Gesetz (BSIG) und Energiewirtschaftsgesetz (EnWG)) und Verordnungen (Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV)) einem Risikobegriff, der das systemische Gesamtrisiko aus den bei Netzbetrieb oder Erzeugung zu zertifizierenden Einzelrisiken aufsummiert. Im Sinne von BSI-KritisV oder EnWG werden Energieanlagen immer nur dann für die Versorgung der Allgemeinheit kritisch, wenn diese bestimmte Schwellenwerte[1] überschreiten oder unabhängig davon (Netzbetreiber nach dem EnWG) als so kritisch betrachtet werden, dass im Störungsfall die Versorgung der Allgemeinheit mit Elektrizität oder Gas gefährdet wird. Im Umkehrschluss bedeutet dies, dass systemische Risiken nur aus dem Störungsfall solcher KRITIS-Anlagen abgeleitet werden können.

Die Energiewende stellt den Schutz der Kritischen Infrastruktur Energiesystem allerdings vor neue Herausforderungen: Das systemische Gesamtrisiko des Energiesystems kann nicht einfach als die Summe seiner „KRITIS-Teile“ aufgefasst werden. Auch kann diesem Risiko nicht einfach mit einer zunehmenden Herabsetzung von Schwellenwerten begegnet werden, da hierdurch die anfallenden Aufwände für die Zertifizierung eines Informationssicherheitsmanagementsystems (ISMS) weder wirtschaftlich noch sinnvoll wären. Ein ISMS stellt Schutzziele wie Vertraulichkeit, Integrität und Verfügbarkeit von Organisationen mit erheblichen technischen und personellen Ressourcen durch einen komplexen Prozess sicher.

Lag das Augenmerk bei der Cybersicherheit in der Vergangenheit vor allem auf dem Schutz thermischer Großkraftwerke sowie den Netzen und hier vornehmlich den Mittel- und Hochspannungsnetzen, in denen eine Zertifizierung als verhältnismäßig und als sinnvoll erscheint, so rückt der Schutz dezentraler Anlagen und Verteilnetze gleichermaßen in den Fokus. Erstens verlagert sich die Erzeugung stärker in Richtung erneuerbarer Energieträger, die an den Verteilnetzen angeschlossen sind. Zweitens verlangt das volatile Erzeugungsverhalten dieser Erzeuger und die bidirektionalen Leistungsflüsse durch neue Akteure wie dem Prosumer oder Flexumer in den Verteilnetzen einen höheren Digitalisierungsgrad, um dem steigenden Informationsbedarf bei der zunehmend komplexer werdenden Netzüberwachung und -steuerung genügen zu können. Der Digitalisierungsgrad wird durch das Hochfahren der Elektromobilität und der Bereitstellung von Flexibilität durch steuerbare Lasten wie Wärmepumpen in den nächsten Jahren im Zusammenhang mit dem Smart-Meter-Gateway-Rollout erheblich zunehmen.

[1] In der BSI-KritisV werden Schwellenwerte definiert bei deren Überschreitung ein Marktpartner unter die BSI-KritisV fällt. Beispielsweise fallen bei der Stromversorgung Erzeugungsanlagen mit einer Erzeugungsleistung >104 MW unter die BSI-KritisV [47]

Vor dem Hintergrund von Digitalisierung und Dezentralisierung ist ein Paradigmenwechsel hin zu einer energiewendegerechten Cybersicherheit gefordert: Der Schutz des Energiesystems kann nicht mehr allein durch eine relativ überschaubare Anzahl von Anlagen in der Höchst- und Hochspannung und einem von Zertifizierungen bestimmten Ansatz gewährleistet bleiben. Auch nimmt die Bedeutung von Cyberangriffen für die Systemsicherheit aufgrund der zunehmenden physikalischen und informationstechnischen Verflechtung in Zukunft auf allen Netz- und Erzeugungsebenen erheblich zu. In diesem Zusammenhang fehlt es bisher auch an einer konsequenten Zusammenführung der Sicherheit von Betriebsmitteln und IT (IT-/OT-Konvergenz) hin zu einer umfassenden und integrierten Betriebssicherheit.

Schließlich werden durch die Energiewende Millionen teilweiser neuer dezentraler Anlagen an die Verteilnetze angeschlossen, die ihrerseits mittels einer von Großkraftwerken unterschiedlichen Kritikalität auf die Systemsicherheit der Netze einwirken: Sind einzelne Erzeuger und Lasten für sich betrachtet zunächst unkritisch, können diese innerhalb eines von bidirektionalen Lastflüssen geprägten Verteilnetz in Summe durch sich verstärkende Wechselwirkungs- und Kaskadeneffekte die Systemsicherheit gefährden. Andererseits kann sich durch die steigende Dezentralität und den damit verbundenen Einsatz vieler unterschiedlicher System auch eine erhöhte Resilienz des Gesamtsystems ergeben.

Um die Lücke zwischen den zertifizierten ISMS von KRITIS-Anlagen und neuen systemischen Risiken zu schließen, die sich aus der Dezentralität, Vernetztheit und Kleinteiligkeit ergeben kann, muss – so die Kernthese des Gutachtens EnerCrypt – eine energiewendegerechte Cybersicherheit auf digitalen Innovationen aufsetzen. Die energiewendegerechte Cybersicherheit ist deshalb auch angewiesen auf innovative Unternehmen und Plattformen der Vernetzung und der Verbindung zwischen Energie- und Digitalwirtschaft. Gerade in der vielfältigen Akteurslandschaft des Energiesektors sind Demonstrations- und Pilotierungsprojekte, welche die Vernetzung und den engen Austausch relevanter Akteure fördern, notwendig. Es sollte auch vor dem Hintergrund der aktuellen weltpolitischen Entwicklungen noch entscheidender gehandelt werden. Dabei empfiehlt es sich, in einem ersten Schritt einen branchenübergreifenden Dialog aufzusetzen, um im Kreise von Expertinnen und Experten beider Domänen die relevanten Fragestellungen zu konkretisieren, die wesentlichen Aufgaben zu identifizieren und damit die ersten Schritte festzulegen. Die Aufgaben sind vielfältig und müssen letztendlich durch Eigenantrieb der einzelnen Akteure zum Schutz und zur Verbesserung der eigenen Anlagen und Services vorangetrieben und umgesetzt werden. Mit dem Ziel die Handlungsfelder in der Breite zunächst systematisch zu erfassen und auch die Basis für ein innovatives Lernfeld zu legen, ist eine übergreifende Austauschinitiative wesentlich.

**Cyberinnovationen und eine neue energiewirtschaftliche Dringlichkeit.** In der Energiewirtschaft liegt der Fokus von digitalen Innovationen und innovativen Unternehmen aber nach wie vor auf neuen Geschäftsmodellen. Dabei kommt der Bereitstellung von energiewirtschaftlichen Daten eine übergeordnete Rolle zu: Daten wurden zunehmend als der eigentliche Rohstoff zukünftiger energiewirtschaftlicher Wertschöpfung aufgefasst. In der Förderung von digitalen Innovationen und innovativen Unternehmen spiegelte sich daher nicht zuletzt auch die Hoffnung etablierter energiewirtschaftlicher Akteure wieder, die in den letzten beiden Jahrzehnten erlittene Verunsicherung durch Marktliberalisierung und sinkender Energiepreise durch datengetriebene Geschäftsmodelle zu überwinden und sich schließlich selbst etwa als Datenplattformenbetreiber neu zu erfinden. Andere Bereiche für digitale Innovationen – wie etwa Cybersicherheit – bekamen vor diesem Hintergrund bisher kaum Sichtbarkeit und konnten daher auch nicht jene Sogwirkung aus den entsprechenden Branchen in die Energiewirtschaft hinein entfalten, die im Zusammenhang mit neuen Geschäftsmodellen zu einem sehr fruchtbaren Austausch zwischen Energie- und Digitalwirtschaft geführt haben.

In den letzten Wochen und Monaten hat sich eine andere Dringlichkeit für die Energiewirtschaft abgezeichnet, wodurch das Thema Cybersicherheit in der Energiewirtschaft sehr viel stärker in den Fokus rückt: Erstens nahmen die Häufigkeit und Schwere von Cyberangriffen auf die IT-Infrastrukturen von Stadtwerken (z. B. Schwerin Ende 2021), deren IT-Dienstleistern (z. B. KISTERS AG Ende 2021) oder auf andere Unternehmen der Energiewende (z. B. VESTAS Ende 2021) stetig zu. Schwachstellen wie Log4J führten Ende des vergangenen Jahres darüber hinaus zu einer weiteren Verunsicherung in allen Sektoren und Branchen. Zweitens führte die Verschärfung der geopolitischen Lage zu einem rasanten Anstieg von Energiepreisen. Die Energiewirtschaft steht dadurch vor neuen Herausforderungen und wird daraus eine neue Dringlichkeit für Innovationen ziehen müssen. Der Krieg in der Ukraine hat gezeigt, dass Cyberangriffe auf staatliche Institutionen und Unternehmen als reale und ernste Bedrohung für Kritische Infrastrukturen und damit die Gesellschaft ernst genommen werden müssen.

Mit dem Einsatz von Wiper-Schadsoftware, die das unwiederbringliche Löschen von Daten zum Ziel hat, ist eine neue Qualität und Politisierung von Cyberangriffen erreicht. Im Gegensatz zu den bekannten Ransomware-Angriffen der letzten Monate und Jahre zielen Wiper-Schadprogramme nicht auf Lösegeld in Form von Kryptowährungen, sondern haben die vollständige und unwiederbringliche Löschung von Daten und damit Unbrauchbarmachung von IT oder OT zum Ziel. Auch ein unbeabsichtigter Spillover solcher Wiper-Schadsoftware nach Deutschland könnte schwerwiegende Folgen für die Energiewirtschaft und Kritische Infrastrukturen haben.

Vor diesem Hintergrund kommt das Gutachten EnerCrypt zur rechten Zeit: Es bildet den Auftakt einer Reihe von Projekten und Initiativen zum Thema energiewendegerechte Cybersicherheit sowie Cyberinnovationen des Future Energy Labs und der Deutschen Energie-Agentur. Diese Projekte und Initiativen sollen dazu dienen, die angestrebte Energieunabhängigkeit durch eine digitale Souveränität im Cyberraum und eine energiewendegerechte Cybersicherheit zu flankieren. Beides zusammen bildet die Basis, um die von der Bundesregierung bei Elektrizität angestrebte geopolitische Energieunabhängigkeit bis 2035, mit dem damit verbundenen Vernetzungs- und Digitalisierungsgrad, erfolgreich umzusetzen.

Herzlichst, Ihr

**Andreas Kuhlmann**
Vorsitzender der Geschäftsführung
der Deutschen Energie-Agentur (dena)

**Philipp Richard**
Bereichsleiter Digitale Technologien & Start-up
Ökosystem der Deutschen Energie-Agentur (dena)

# 1 Einleitung

Das Energiesystem ist essenziell für das wirtschaftliche, soziale und politische Leben eines modernen Industriestaates. Die im Zuge der Energiewende zunehmende und notwendige Digitalisierung des Energiesystems führt jedoch auch zu einer stetigen Ausweitung von Angriffsflächen und Angriffsvektoren. Insbesondere der Cyberangriff auf die ukrainische Verteilnetzinfrastruktur 2015, von dem Hunderttausende Menschen betroffen waren, zeigt, dass kritische Energieinfrastrukturen zunehmend zu einem attraktiven Ziel werden. Somit wird Cybersecurity für die Energiewirtschaft ein immer wichtigeres Thema.

Um die Funktionsfähigkeit kritischer Energieinfrastrukturen sicherzustellen, müssen ihre Betreiber in der Bundesrepublik Deutschland nach dem IT-Sicherheitsgesetz und dem Energiewirtschaftsgesetz ein Mindestmaß an IT-Sicherheit nachweisen und zum Schutz ihrer IT-Systeme, -Komponenten und -Prozesse angemessene organisatorische und technische Vorkehrungen nach dem Stand der Technik treffen. Zudem sehen Meldepflichten vor, dass kritische IT-Vorfälle – insbesondere Cyberangriffe – dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet werden müssen. Jedoch ist zu beobachten, dass das Energiesystem im Zuge der Energiewende zunehmend von kleineren, dezentralen Erzeugungsanlagen geprägt wird, die nicht unter die Vorgaben für kritische Infrastrukturen fallen, in Summe als Ziel von Cyberangriffen jedoch trotzdem eine große Gefahr für die Versorgungssicherheit in der Bundesrepublik Deutschland darstellen.

Um diese Lücke zu schließen, wurde beispielsweise mit dem Smart Meter Gateway (SMGW) für den sicheren Messstellenbetrieb eine infrastrukturelle Grundlage für eine cybersichere Digitalisierung abseits formeller kritischer Infrastrukturen gelegt. Aufgrund des absehbar steigenden Grads an Digitalisierung und Vernetzung, beispielsweise durch erneuerbare Energien, E-Mobilität, Wärmepumpen und IoT-Lösungen insbesondere auf den unteren Spannungsebenen, wurden die Anforderungen an die IT-Sicherheit des SMGW so spezifiziert, dass sowohl Cyberinnovationen ermöglicht werden als auch einer sich stetig verändernden Bedrohungslandschaft Rechnung getragen werden kann.

> Das Ziel dieses Gutachtens sind die Identifikation und Bewertung von wesentlichen Trends und Entwicklungen, die diesen Innovationsspielraum nutzen bzw. nutzen könnten, um Cyberinnovationen, die für die Energiebranche eine erhöhte Relevanz aufweisen, zu realisieren und somit zu dem übergeordneten Ziel eines sicheren Energiesystems der Zukunft beizutragen. Dabei werden über den Messstellenbetrieb hinaus Entwicklungen und Trends zur cybersicheren Ertüchtigung von Betriebsmitteln und energiewirtschaftlicher IKT-Infrastruktur unter Zuhilfenahme digitaler Zukunftstechnologien mit einem Fokus insbesondere auf die Verteilnetzebene untersucht.

Als Grundlage für die Betrachtung von Cyberinnovationen für das sichere Energiesystem der Zukunft werden in Kapitel 2 Entwicklungen und Trends hinsichtlich Digitalisierung und Zukunftstechnologien in der Energiewirtschaft dargestellt und eingeordnet. Um eine erste Übersicht über zukünftige Anforderungen, Anwendungsfälle und Herausforderungen zu geben, werden zunächst aktuelle und zukünftige Entwicklungen in der Energiewirtschaft selbst diskutiert (Abschnitt 2.1). Darauf aufbauend werden anschließend Technologien für die sicherere Digitalisierung und Anwendungsrealisierung aus den Bereichen der digitalen Kommunikation (Abschnitt 2.2) sowie der allgemeinen Zukunftstechnologien (Abschnitt 2.3) identifiziert. Abschließend werden verschiedene Konzepte zur cybersicheren Ertüchtigung energietechnischer Betriebsmittel diskutiert und unter Berücksichtigung der besonderen energiewirtschaftlichen Anforderungen bewertet (Abschnitt 2.4).

In Kapitel 3 werden darauf aufbauend innovative Anwendungsfälle in einer Bedrohungslandschaft im Wandel identifiziert und diskutiert. Dazu werden zunächst konkrete Anwendungsfälle für die Energiebranche sowohl aus Kunden- als auch aus Netzbetreibersicht betrachtet (Abschnitt 3.1). Als Grundlage für eine Bewertung der cybersicheren Realisierung dieser konkreten Anwendungsfälle werden anschließend historische Angriffe analysiert sowie konkrete Handlungsempfehlungen und Anforderungen im Hinblick auf die Cybersicherheit abgeleitet (Abschnitt 3.2). Abgeschlossen wird diese Analyse mit einer Diskussion von nationalen Vorschriften und Regulierungen zur Cybersicherheit von kritischen Energiesystemen (Abschnitt 3.3).

Kapitel 4 fokussiert auf das Potenzial von Cybersicherheit als energiewirtschaftlicher Innovationstreiber. Dazu wird zunächst der Status quo der energiewirtschaftlichen Innovationen in der Bundesrepublik Deutschland anhand verschiedener Anwendungsbereiche erhoben (Abschnitt 4.1). Als Fallstudie zur Betrachtung der dafür notwendigen Kommunikationsinfrastruktur wird dann ein besonderer Fokus auf die SMGW-Infrastruktur gelegt (vgl. Abschnitt 4.2). Dieses Kapitel schließt mit einer Diskussion zur Umsetzbarkeit und zu möglichen Technologien für eine Transition hin zu einer cybersicheren Umgebung für den Energiesektor, insbesondere unter Betrachtung von Anforderungen hinsichtlich IT-Sicherheit und Datenschutz (Abschnitt 4.3).

In Kapitel 5 werden die vorherigen Erkenntnisse, ergänzt durch praktische Erfahrungen auf nationaler und internationaler Ebene, für eine Analyse der förderpolitischen Möglichkeiten in Deutschland genutzt. Die vorgestellten Erkenntnisse beruhen insbesondere auf den Inhalten von zwei Workshops, die im Rahmen der Erstellung des Gutachtens mit Teilnehmerinnen und Teilnehmern aus Wirtschaft und Politik durchgeführt wurden. Zunächst werden sowohl allgemeine als auch konkrete förderpolitische Maßnahmen diskutiert (Abschnitt 5.1). Anschließend werden internationale Erfahrungen zu Infrastrukturen, die mit der SMGW-Infrastruktur in Deutschland vergleichbar sind, sowie weiterführende Erfahrungen zu Cybersecurity in der Energiewirtschaft vorgestellt (Abschnitt 5.2). Das Kapitel rundet das Gutachten mit einer Diskussion von konkreten Lösungsstrategien zur Innovationsförderung in Deutschland ab (Abschnitt 5.3).

Das Gutachten schließt in Kapitel 6 mit der Zusammenfassung der Erkenntnisse und Analysen des Gesamtgutachtens. Insbesondere wird ein übergeordnetes Fazit gezogen, das auch einen Ausblick auf die Herausforderungen für die deutsche Energiewirtschaft in naher und weiterer Zukunft gibt. Die Erkenntnisse und Analysen dieses Gutachtens können dabei helfen, diese Herausforderungen fundiert und zielstrebig zu meistern.

> Das sichere Stromnetz der Zukunft wird auf mehreren Grundpfeilern errichtet, wobei alle beteiligten Akteure in diesen Prozess einzubeziehen sind und ihren Beitrag leisten müssen. Energietechnische Innovationen bezüglich der Dezentralisierung des Stromnetzes, der Digitalisierung der umgebenden IT- und Operational-Technology-Netzwerke sowie der ganzheitlichen Cybersecurity in all diesen Bereichen sind unabdingbar, um die Energiewende, die Ermöglichung neuer Verbrauchsmuster sowie neue Mehrwertdienste und Anwendungsfälle zukunftssicher gestalten und umsetzen zu können. Dieses Gutachten diskutiert und analysiert den Status quo, die anstehenden Herausforderungen und Mehrwerte sowie Werkzeuge aus dem Bereich der IT, die für diesen Prozess nützlich oder gar unbedingt notwendig sind.

# 2 Entwicklungen und Trends in der digitalen Energiewirtschaft

Seit mehreren Jahrzehnten arbeitet Deutschland im Rahmen der Energiewende auf das Ziel hin, die Energiewirtschaft zu modernisieren und zu digitalisieren sowie negative Umweltauswirkungen zu minimieren. Wichtige Kernaspekte sind zum einen die wachsende Bedeutung von (dezentralen) Anlagen nach dem Erneuerbare-Energien-Gesetz (EEG), aber auch die Berücksichtigung wechselnder Ansprüche an das Stromnetz durch neue Verbrauchsmuster. Sie werden unter anderem durch die steigende Verbreitung der Elektromobilität verursacht, woraus sich neben der Herausforderung des energietechnischen Ausbaus zusätzliche Anforderungen an (digitales) Flexibilitätsmanagement, Netzmonitoring und -stabilisierung sowie flexible, kundenorientierte Tarifmodelle ergeben.

Diese sich wandelnde digitale Energiewirtschaft geht notwendigerweise auch mit steigenden Ansprüchen an neue Technologien, sowohl zur digitalen Kommunikation als auch im anwendungsorientierten Bereich, einher. Ein besonderer Fokus bei Energienetzen als kritische Infrastruktur (KRITIS) liegt hier zwangsläufig auch auf der Cybersicherheit jener Technologien, die das Energiesystem der Zukunft vor ausgefeilten Cyberbedrohungen schützen sollen. Dies umfasst die eingesetzten Kommunikationstechnologien, kryptografische Verfahren sowie verwendete übergeordnete Technologien wie Netzwerksteuerung, Prozessüberwachung und Smart Meter Gateways (SMGWs).

Um Energiesysteme in der Zukunft cybersicher zu gestalten, ist es wichtig, aktuelle und zukünftige Entwicklungen und Trends der Energiewirtschaft zu analysieren, resultierende Anforderungen und Anwendungsfälle zu identifizieren und Technologien, die der Realisierung dieser Anwendungsfälle dienlich sein könnten, zu identifizieren und zu verstehen. Dieses Kapitel stellt zunächst aktuelle und zukünftige Entwicklungen in der Energiewirtschaft selbst dar (Abschnitt 2.1), um eine erste Übersicht über zukünftige Anforderungen, Anwendungsfälle und Herausforderungen zu geben. Hierauf aufbauend werden anschließend Technologien aus dem Bereich der digitalen Kommunikation (Abschnitt 2.2) sowie aus dem allgemeinen Kontext (Abschnitt 2.3) vorgestellt, die für die sicherere Digitalisierung und Anwendungsrealisierung genutzt werden können. Das Kapitel schließt mit einer Diskussion verschiedener Konzepte zur cybersicheren Ertüchtigung energietechnischer Betriebsmittel (Abschnitt 2.4), wobei entsprechende Konzepte und die diskutierten Technologien unter Berücksichtigung der besonderen energiewirtschaftliche Anforderungen bewertet werden.

## 2.1 Entwicklungen und Trends in der Energiewirtschaft

Der Paradigmenwechsel, der sich in der europäischen Energiewirtschaft im Rahmen der Energiewende rasant vollzieht, stellt die Verteil- und Übertragungsnetzbetreiber vor neue Herausforderungen. Das wesentliche Merkmal dieses Wandels sind die zunehmende Stilllegung von thermischen Anlagen und der zunehmende Ausbau von regenerativen Erzeugungseinheiten, insbesondere Photovoltaik und Windkraft, mit volatilerem Erzeugungsverhalten. Das steigende Wachstum der Stromerzeugung aus erneuerbaren Erzeugungseinheiten in Deutschland zeigt sich auch in den aktuellen Zahlen, nach denen im Jahr 2020 durch den Energieträgermix aus Geothermie, Photovoltaik, Off-/Onshore-Windkraft, Biomasse, Siedlungsabfällen und Wasserkraft im Vergleich zum Jahr 2010 um einen Faktor von 2,4 mehr an elektrischer Energie bereitgestellt wurde [33]. Einen wesentlichen Beitrag zu diesem Energieträgermix leisteten im Jahr 2020 Onshore-Windkraftanlagen mit 105,3 Mrd. kWh und Photovoltaik-Anlagen mit 50,4 Mrd. kWh elektrischer Energie [33].

Im Jahr 2019 betrug der Anteil aller erneuerbaren Erzeugungseinheiten am gesamten Energieträgermix in Deutschland rund 44,2 Prozent [32].

Aus diesen Gegebenheiten sowie weiteren prägenden Rahmenbedingungen durch Klimaschutzziele (z. B. Clean Energy Package [75]) ergeben sich weitere Ziele und Herausforderungen für den Energiesektor, die sich in die Reduktion der Treibhausgasemissionen, die Steigerung der Energie- und Ressourceneffizienz, die Förderung emissionsfreier Technologien und den verstärkten Ausbau erneuerbarer Erzeugungseinheiten gliedern. Ein Schlüsselelement zur Erreichung dieser Ziele ist es, die Flexibilität des (europäischen) Energiewirtschaftsraums zu erhöhen und neuen Akteuren einen diskriminierungsfreien Zugang zu den Strommärkten zu ermöglichen. Daraus können sich zusätzliche Potenziale ergeben, um die neuen Herausforderungen durch ein unstetiger werdendes Energieangebot zu meistern, es mit der Energienachfrage, dem Verbrauch und der Speicherung durch die Nutzung von Flexibilitäten in der Energieversorgung sowie durch intelligente Netzbetriebsführungskonzepte auszugleichen und somit die Stabilität und Versorgungssicherheit des gesamten Energiesystems weiterhin zu gewährleisten. Ein Schlüsselaspekt bei der Bewältigung dieser Herausforderungen ist die effiziente Nutzung dieser Flexibilitäten im Energiesystem, begleitet von der Maximierung des Einsatzes erneuerbarer Erzeugungseinheiten mit effizienter Nutzung bestehender und neuer Infrastrukturen, die beispielsweise durch die zunehmende Durchdringung mit Informations- und Kommunikationstechnik (IKT) gekennzeichnet sind.

**Neue Herausforderungen für den Netzbetrieb.** Der zunehmende Einsatz von volatilen, erneuerbaren Energieträgern hat somit grundlegende und weitreichende Konsequenzen für den Netzbetrieb. Für den Übertragungsnetzbetreiber (ÜNB) ergibt sich aus der geforderten Netzbeobachtbarkeit und den Mitteln zur Aufrechterhaltung der Systemstabilität und -sicherheit ein erhöhter Informationsbedarf bedingt durch neue Marktteilnehmer und Akteure wie Aggregatoren, die den dezentral erzeugten Strom organisatorisch bündeln und als aggregierte Flexibilitäten am Regelenergiemarkt vermarkten. Der Verteilnetzbetreiber (VNB) muss die sichere Aufrechterhaltung des Verteilnetzbetriebs garantieren. Bidirektionale Lastflüsse durch die ansteigende Anzahl von dezentralen Erzeugungsanlagen und hochvolatilen Prosumern auf Verteilnetzebene können zu betrieblichen Grenzsituationen führen, in denen die zulässigen Leitungs- oder Netzkapazitäten und die technischen Grenzen für Spannungsband und Betriebsmittelauslastungen lokal in kürzeren Zeitabständen erreicht werden.

Aufgrund des volatilen Einspeiseverhaltens von erneuerbaren und witterungsabhängigen Erzeugern, aber auch Verbrauchern (im Sinne von negativer Regelenergie) wird die Prognose des Netzzustands für Verteilnetzbetreiber immer wichtiger, insbesondere im Sinne einer direkten Beeinflussung durch Regelenergieabrufe oder Engpassmanagement. Für die Gestaltung und Umsetzung von Konzepten zum Flexibilitätseinsatz und eine zuverlässige, prädiktive Erkennung und Bewertung von Engpässen im Verteilnetz sind daher Verfahren zur Netzzustandsermittlung und -vorhersage notwendig. Solche Verfahren zur Zustandseinschätzung werden in der Regel in Netzen eingesetzt, die aufgrund einer weitreichend ausgebauten Messinfrastruktur ein Maximum an Beobachtbarkeit bieten, wie es in Hoch- und Höchstspannungsnetzen der Fall ist. In niedrigeren Spannungsebenen, die über weniger bis gar keine Messinfrastruktur verfügen, treffen diese Schätzverfahren dementsprechend auf ein unterbestimmtes System mit wenig validierten Messungen. Für die unteren Spannungsebenen liegt folglich der Fokus auf der Generierung von Zustandsdaten. Eine wesentliche Randbedingung ist daher langfristig die Beobachtbarkeit und gegebenenfalls sogar die Steuerbarkeit der Mittel- und Niederspannungsnetze und der daran angeschlossenen Erzeuger und Lasten, um die Bereitstellung von Systemdienstleistungen durch die Netzbetreiber für die Systemstabilität und -sicherheit effizienter zu gestalten. Historisch gesehen sind die Verteilnetze teilweise auch technisch nicht für

die zunehmende Durchdringung mit dezentraler Erzeugung ausgelegt. Insbesondere die Konzepte der Schutztechnik in Verteilnetzen basieren funktional auf klassischen Verteilnetzstrukturen mit unidirektionalem Leistungsfluss, das heißt weitgehend ohne Zwischeneinspeisungen und Rückspeisungen in die übergeordnete Netzebene, und sind statisch parametriert. Eine flexible, ereignisabhängige Anpassung von Einstellparametern oder des Funktionsumfangs ist nicht vorgesehen und im Hinblick auf die Datenerzeugung, -übertragung und -verarbeitung im Feld derzeit nicht möglich. Der Einsatz von Netztopologieänderungen zur Netzentlastung, beispielsweise als Reaktion auf sich ändernde Lastflüsse, könnte zu Zuständen führen, die mit den vorhandenen klassischen Schutzkonzepten nicht beherrschbar sind. Mögliche technische Lösungen zur Bewältigung dieser Herausforderung gehen Hand in Hand mit adaptiven und vernetzten Netzschutzkonzepten, die bei Leistungsflussverschiebungen und Topologieänderungen die Schutzparameter anpassen und einen sicheren Betrieb gewährleisten. Die Netzausbaumaßnahmen, die mit der Umsetzung des Smart-Grid-Paradigmas einhergehen, müssen kohärent die Aufrüstung der Schutzsysteme einschließen.

**Systemdienstleistungsbeiträge aus dem Verteilnetz.** Verteilnetze werden zukünftig einen zunehmenden Anteil an der Bereitstellung von Systemdienstleistungen (Spannungs- und Blindleistungsmanagement, Engpassmanagement und Versorgungswiederherstellung) übernehmen. Verteilnetzbetreiber haben somit eine steigende Verantwortung bezüglich der Koordination des Einsatzes von dezentralen Erzeugungsanlagen zur Erbringung der Systemdienstleistungen. Daraus ergibt sich auch eine weitere Abstimmung von Maßnahmen in Notfallsituationen zwischen den Akteuren, insbesondere zwischen den Netzbetreibern, auf Basis von gegenseitig anerkannten Erzeugungs- und Lastannahmen, wie zum Beispiel im Rahmen von Störungs- und Engpassmanagement sowie Redispatch. Derzeit stehen Redispatch-Eingriffe in Erzeugungsanlagen nur den Übertragungsnetzbetreibern zur Verfügung, um Engpässe in ihren Netzen zu beseitigen. Im Sinne von Redispatch 2.0 [35] soll dies jedoch auch für den Einsatz in Verteilnetzen zur Verfügung gestellt werden. Die angestrebte Öffnung der Redispatch- und Regelenergiemärkte für Erzeugungseinheiten in einer Größenordnung oberhalb von 100 kW sowie der Einsatz von Redispatch- oder Flexibilitätsmaßnahmen zur Beseitigung von Engpässen in lokalen oder regionalen Bereichen werden das Last- und Erzeugungsverhalten dieser neuen Marktteilnehmer entscheidend verändern. Die heute aus dem Bereich der Übertragungsnetze bekannten Methoden und Technologien zur Gewährleistung der Versorgungssicherheit werden in Zukunft zunehmend in Regeln zur Vermeidung von netzkritischen Situationen in Verteilnetzen relevant werden. Dazu gehören insbesondere Erzeugungs- und Lastflussprognosen, die im Verteilnetzbetrieb kurzfristig zur Ermittlung und Freigabe freier Netzkapazitäten, Redispatch und Flexibilitätsmaßnahmen unter den Bedingungen eines zunehmend marktorientierten Erzeugungs- und Lastverhaltens eingesetzt werden können.

Derzeit sind die Märkte für netzdienliche Flexibilitäten begrenzt und beschränken sich weitgehend auf den Einsatz von Regelleistung und Redispatch auf der Ebene der ÜNB sowie abschaltbare Lasten auf der Ebene der Verteilnetzbetreiber. Diese Instrumente werden in Zukunft nicht mehr ausreichen, um Last- und Erzeugungsspitzen im Netz auszugleichen und einen sicheren Netzbetrieb zu gewährleisten [31]. Im Kontext intelligenter Energienetzsysteme, die hohe Anforderungen an IT-Infrastrukturen, Systeme und Prozesse stellen, wird der Einsatz von netzdienlichen Flexibilitäten zur Erbringung von Systemdienstleistungen zunehmen. Die Umsetzung dieses Konzepts erfordert den Zugriff der Netzbetreiber auf Systemdienstleistungen, wie zum Beispiel die Bereitstellung von Flexibilitäten zur Vermeidung von Netzengpässen oder die marktdienliche Nutzung dezentraler Energieanlagen zur Bilanzkreisbewirtschaftung, um diese bei Bedarf kontrahieren und steuern zu können. Dies wiederum erfordert die effiziente Vermarktung aller netzdienlichen Flexibilitäten dezentraler Energieanlagen durch dynamische Aggregation, die auch sehr kleinen Anlagen die Teilnahme an

Märkten ermöglicht, um ein Flexibilitätsportfolio eines oder mehrerer Aggregatoren zu bilden. Damit eröffnet sich für dezentrale Energieanlagen eine völlig neue Dimension der Teilnahme am Energiemarkt: Sie können die nicht selbst benötigte Energie als Flexibilität anbieten und wandeln sich so beispielsweise von reinen Erzeugungsanlagen, die ins Netz einspeisen und bei kritischen Netzzuständen vom Netzbetreiber abgeschaltet werden, zu wettbewerbsfähigen dezentralen Energieanlagen, die aktiv am Marktgeschehen teilnehmen. Flexibilität kann auf unterschiedliche Weise genutzt werden: Sie kann zum Beispiel vom Übertragungsnetzbetreiber zur Aufrechterhaltung der Systemstabilität und vom Verteilnetzbetreiber zur Bewältigung lokal kritischer Netzsituationen genutzt werden. Dabei kann Flexibilität auch verstärkt für den schnellen Bilanzkreisausgleich eingesetzt werden.

**Marktkommunikations-Modell.** Beides kann auch die Ziele der Bundesregierung unterstützen, die Bilanzkreistreue zu stärken und Barrieren für den freien Wettbewerb von Flexibilitätsoptionen abzubauen. In diesem Kontext beschreibt das Marktkommunikations-Modell Rollen, Bereiche und Objekte des Energiesektors und ihre Beziehungen zueinander. Für die jeweiligen Rollen werden Verantwortlichkeiten und Aufgaben sowie Funktionen von Bereichen und Objekten definiert [34].

Die aus der Energiewende resultierenden Umstände und Rahmenbedingungen werden auch zu einer zunehmenden Interaktion zwischen allen Akteuren, wie Übertragungs- und Verteilnetzbetreibern, Kraftwerksbetreibern, Kunden und Verbrauchern, Prosumern und Aggregatoren sowie Börsen, führen. Entsprechend der gestiegenen Interdependenz wird ein intensiverer Informationsaustausch über systemrelevante Kommunikationskanäle unabhängig vom öffentlichen Kommunikationsnetz erforderlich sein, um durch koordinierte Prozesse des Netz- und Systemmanagements auch in Zukunft einen stabilen und sicheren Netzbetrieb gewährleisten zu können. Folglich werden zukünftig steigende Datenmengen und heterogene Datenquellen in den Stromnetzen erwartet, die einen Echtzeitzugriff auf systemrelevante Messgrößen (z. B. Netzfrequenz) durch die Fernanbindung eines erheblichen Teils der elektrischen Betriebsmittel ermöglichen. Es werden in verschiedenen Segmenten des Energiesektors Big Data generiert, die einen potenziellen Wert für Versorgungsunternehmen, Netzbetreiber sowie Endverbraucherinnen und -verbraucher darstellen können und die mithilfe von Big-Data-Algorithmen und Edge-Computing-Technologien für eine Vielzahl von Zwecken genutzt werden, beispielsweise für die Vorhersage von Stromangebot und -nachfrage, für die Zustandsabschätzung und die Netzsteuerung sowie zur Förderung der Teilnahme an Strommärkten.

**Neue Systemarchitekturen und Technologien.** Die traditionelle Organisation von Energiesystemen impliziert eine zentralisierte Architektur mit den Ebenen der Erzeugung, Übertragung und Verteilung. Die zunehmende Durchdringung durch verteilte Erzeugungsanlagen in unterschiedlichen Spannungsebenen kann zukünftig die Entwicklung hin zu komplexeren Architekturen mit sich bringen, um das Gesamtsystem global sicher zu betreiben. Rein dezentrale Architekturen sorgen dafür, dass Informationen abgeschottet werden und keine globalen Informationen von eingreifenden Akteuren benötigt werden, was im Zusammenhang mit autonomen und isolierten Microgrids in Form von Insellösungen interessante Perspektiven bietet. Eine Alternative ist der Einsatz von Multi-Agenten-Systemen auf Basis von Methoden der Künstlichen Intelligenz (KI) unter Verwendung von Agententechnologie. Dieser Ansatz eignet sich in der Regel für komplexe Herausforderungen, bei denen von einzelnen Agenten erwartet wird, dass sie entweder durch Kooperation oder Wettbewerb eine Lösung für ein globales Problem finden.

Die zunehmende Erzeugungsleistung aus dezentralen Erzeugungsanlagen in Verteilnetzen, die überwiegend über Wechselrichter gekoppelt wird, führt einerseits zu einer geringeren Trägheit im Netzbetrieb und andererseits zu der komplexeren Aufgabe, einen stabilen Netzbetrieb zu gewährleisten, da jede dezentrale Erzeugungsanlage den Netzzustand aktiv beeinflussen kann. Dementsprechend verschärft sich diese

Situation für Microgrids und schafft folglich neue Herausforderungen, denen mit innovativen Lösungskonzepten begegnet werden muss, wie zum Beispiel der Auslegung von netzgeführten und netzbildenden Wechselrichtern in Verbindung mit der Erzeugungsleistung in Microgrids.

> Die Energiewende und die damit verbundenen neuen Erzeugungsmöglichkeiten auf Basis erneuerbarer Energien haben neue Optionen für eine nachhaltige Stromerzeugung eröffnet. Gleichzeitig stellen sich aber auch neue Herausforderungen an den Netzbetrieb, denen durch den Ausbau der Netztransparenz und der Steuerbarkeit in den Verteilnetzen mittels Sensorik und Aktorik begegnet werden muss, um nicht nur den Herausforderungen des Netzbetriebs zu begegnen, sondern auch Mehrwertdienste und nachhaltige Anwendungsfälle in der Energiewirtschaft zu realisieren. Hier können neue Technologien zum Einsatz kommen, die in Form von Infrastrukturen, Hardware oder Software Bestandteil zukünftiger Ausgestaltungen von Energieinformationssystemen sein werden. Der Umfang und die Komplexität solcher Veränderungen im System erfordern die Einführung dezentralerer und flexiblerer Architekturen sowie die Unterstützung durch fortschrittliche Kommunikationsinfrastrukturen, um die Anforderungen an Steuerung, Betrieb und Handel auf der Verteilerebene effizient und robust für zukünftige Herausforderungen zu erfüllen. Es werden fortschrittliche aktive Steuerungs- und Betriebsführungsstrukturen benötigt, die einen ganzheitlichen Lösungsansatz für regionale Steuerungssysteme für den Netzbetrieb und den Handel von Energie und Dienstleistungen in lokalen Märkten erfordern. In Kombination mit neuen Algorithmen und Cyberinnovationen können lokale Engpässe rechtzeitig erkannt (z. B. Spannungsengpässe oder Überlastungen in Stromeinspeisungen) und die Behebung globaler Ungleichgewichte wie Lastausgleich und Frequenzregelung unterstützt werden.

## 2.2 Innovationen im Bereich der digitalen Kommunikation

Die zuvor dargelegten steigenden Anforderungen sowie der wachsende Umfang an digitaler Kommunikation im Kontext der Energienetze führen bereits heute zum Um- und Ausbau entsprechender Kommunikationsinfrastrukturen. Neben den Anforderungen hinsichtlich Übertragungsraten und Kosten ist die Sicherheit der Kommunikation und der übertragenen Daten dabei von besonderer Relevanz. Für Komponenten- und Systemhersteller wie auch Netzbetreiber (ÜNB und VNB) ergeben sich zwei zentrale Herausforderungen:

1. die geeignete Auswahl der Kommunikationstechnologie und
2. deren Absicherung gegenüber Cyberangriffen.

Typische Cyberangriffe in Kommunikationsnetzwerken erfolgen auf die Integrität der übertragenen Daten sowie auf die Verfügbarkeit der Schnittstellen. Dieser Abschnitt stellt zur Verfügung stehende Kommunikationstechnologien aus dem Bereich der kabellosen und kabelgebundenen Kommunikation zusammen und bewertet sie hinsichtlich ihrer Anwendungsbereiche.

Viele Kernkomponenten können, insbesondere bei ÜNB und größeren VNB, über bestehende eigene kabelbasierte Infrastrukturen angebunden werden. Weit verbreitet ist der Eigenbetrieb von Glasfasernetzen wie auch von Netzen basierend auf der Power-Line-Kommunikation. Eine solche Infrastruktur ist im Gesamtkontext eines Smart Grids jedoch nicht immer verfügbar. Kleinere VNB, Stadtwerke oder andere, mitunter neue Akteure wie Ladesäulenbetreiber verfügen nicht immer über solche Infrastrukturen oder die Möglichkeit, Kabelinfrastruktur von Internet Service Providern (ISP) zu verwenden. Ähnlich verhält es sich mit Bestandsanlagen bei ÜNB, für die eine Kommunikationsnetzanbindung nicht vorgesehen war. Des Weiteren gibt es eine Reihe von Anwendungsfällen, bei denen eine kabelbasierte Anbindung aus technischen oder

wirtschaftlichen Gründen nicht sinnvoll ist. Dies gilt beispielsweise für Projekte im Bereich des Internet of Things (IoT), wie sie in diversen Gemeinden zur Steigerung der Energieeffizienz oder zur Optimierung von Abläufen durchgeführt werden. In all diesen Fällen werden drahtlose Kommunikationsnetze verwendet oder sogar neu errichtet.

Die Bandbreite an unterschiedlichen Funktechnologien ist immens. Zu bereits verfügbaren Technologien wie LTE, NB-IoT, GSM, Tetra-Funk, Long Range Wide Area Network (LoRaWAN), Sigfox und WLAN kommen in naher Zukunft weitere hinzu. Insbesondere 5G und LTE-M auf Basis der gerade vergebenen Frequenzen um 450 MHz sind für die Energiewirtschaft von besonderer Bedeutung.

Die Heterogenität der kabelbasierten Technologien wie auch der Funktechnologien erstreckt sich dabei über verschiedene Dimensionen von beispielsweise technischen Leistungsmerkmalen (Datenrate, Latenz, Skalierbarkeit) bis zur Datenhoheit (öffentliche Netze eines ISP oder Eigenbetrieb). Abbildung 2.1 zeigt eine Übersicht über die Technologien und ihre zentralen Eigenschaften. Viele Technologien bieten eigene, teils proprietäre Methoden zur Absicherung gegen Cyberangriffe, jedoch ändern sich die Rahmenbedingungen für einen sicheren Betrieb schnell. Die vorhandenen Vorschriften und Anforderungen sind sehr techniklastig bei einer gleichzeitig volatilen Bedrohungslage. Im Folgenden wird eine erste Übersicht über die wichtigsten Eigenschaften von verschiedenen Kommunikationstechnologien sowie die Herausforderungen bei der Absicherung gegen Cyberangriffe gegeben.

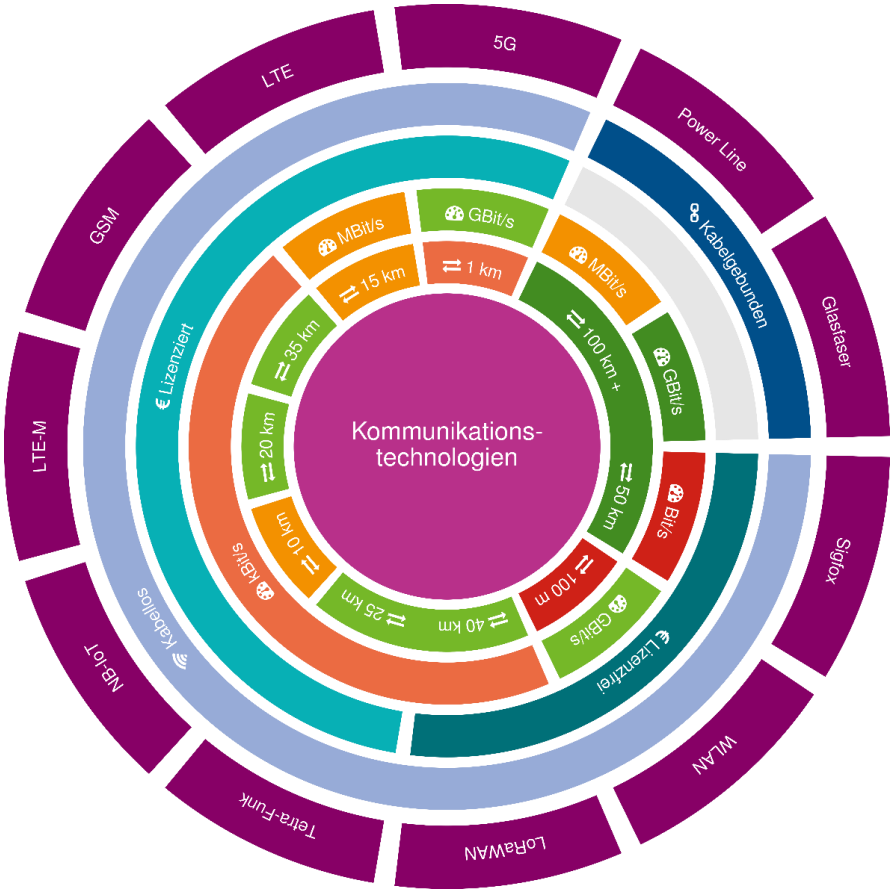


**Abbildung 2.1:** Die für die Energiewirtschaft relevanten Kommunikationstechnologien lassen sich grundsätzlich in kabellose und kabelgebundene Technologien unterteilen. Zudem bieten sie unterschiedliche Eigenschaften hinsichtlich Lizenzierbarkeit, Datenrate und Reichweite. Weitere Aspekte wie Sicherheitsfeatures, Latenz, Bau- und Wartungskosten oder Energiebedarf sind jedoch immer zusätzlich zu berücksichtigen.

### 2.2.1 Kabelgebundene Kommunikation

Glasfasernetze ermöglichen symmetrische Übertragungsraten von bis zu Hunderten von GBit/s auch auf großen Entfernungen und sind damit die einzige Technologie mit diesen zukunftssicheren Leistungswerten. Die Kosten für die benötigten Lichtwellenleiter sind relativ gering. Der Hauptkostentreiber sind die erforderlichen Tiefbauarbeiten und das benötigte Spezialwissen und Werkzeug zum Spleißen der Verbindungen. Um dedizierte Tiefbauarbeiten zu minimieren, sind gängige Ansätze die Nutzung vorhandener oberirdischer Strukturen wie Strommasten oder die zwingende Verlegung eines Leerrohrs beim Straßenbau. Die hohen Kapazitäten von Glasfasern erlauben es, neben der Übertragung der für das Smart Grid relevanten Daten auch weitere Dienste, gegebenenfalls in Kooperation mit einem Internet Service Provider (ISP), zu realisieren.

Power-Line-Kommunikation nutzt als Übertragungsmedium das vorhandene Stromnetz und existiert in den Ausführungen Narrowband und Broadband, die sich in Reichweite und Durchsatz massiv unterscheiden. Obgleich die Nutzung des vorhandenen Stromnetzes als Übertragungsmedium als logisch erscheint, existieren große Herausforderungen hinsichtlich der Stabilität der Übertragung. Stromkabel sind nicht für eine Datenübertragung konzipiert und erste Feldversuche zeigten eher ernüchternde Ergebnisse [83].

Technologieinhärente Sicherheitsfunktionen existieren bei kabelgebundener Kommunikation in der Regel nicht. Vielmehr obliegt es den genutzten Kommunikationsprotokollen, eine Absicherung zu realisieren. Typische Beispiele hierfür sind Virtual Private Networks (VPNs) oder Transport Layer Security (TLS). Eine einfache physische Absicherung besteht dadurch, dass verlegte Glasfaserleitungen in der Regel für einen Angreifer schwer zugänglich sind. Mitschneiden und Einschleusen von Paketen lassen sich mit geeigneten Maßnahmen in der Regel detektieren.

### 2.2.2 Drahtlose Kommunikation

Derzeit für den Einsatz im Smart Grid diskutierte drahtlose Kommunikationstechnologien wie LTE, NB-IoT, GSM, Tetra-Funk, LoRaWAN, Sigfox, WLAN, 450 MHz LTE-M oder 5G sind zellulare Netzwerke. Zellulare Netzwerke sind durch Punkt-zu-Mehrpunkt-Verbindungsarchitekturen gekennzeichnet, wobei jede Zelle durch eine Basisstation realisiert wird. Basisstationen benötigen einen exponierten Standort, eine stabile Stromversorgung sowie die Anbindung an das Kommunikationsnetz zum Weitertransport der empfangenen Daten, was in der Regel durch Glasfasernetze realisiert wird.

Die Leistungsmerkmale der verschiedenen Kommunikationstechnologien sind maßgeblich durch den Entwicklungsgrad der Technologie, die genutzte Frequenz und die zur Verfügung stehende Bandbreite bestimmt. Hierbei gilt, dass bei niedrigen Frequenzen unterhalb von 1 GHz (z. B. 450 MHz LTE-M oder LoRaWAN) eine deutlich höhere Reichweite (Zellgröße) und Durchdringung von Strukturen erreicht wird. Bei niedrigen Frequenzen steht jedoch nur begrenzt Bandbreite zur Verfügung, was den Durchsatz und die Skalierbarkeit (z. B. im Vergleich zu 5G) stark einschränkt.

Eine wichtige Unterscheidung für drahtlose Kommunikationstechnologien besteht ebenfalls in den regulatorischen Aspekten der Frequenznutzung. Technologien, die vorrangig den Mobilfunknetzwerken zuzuordnen sind (LTE, NB-IoT, GSM, Tetra-Funk, 450 MHz LTE-M), nutzen lizenzierte Frequenzbänder, die Unternehmen (z. B. Mobilfunkanbieter, 450connect GmbH) für hohe Investitionskosten exklusiv zugeordnet sind. Auf der einen Seite müssen diese Investitionskosten erwirtschaftet werden, auf der anderen Seite führt die exklusive Zuordnung zu einem Netzbetrieb mit Qualitätsgarantien. Technologien wie LoRaWAN, Sigfox und WLAN nutzen unlizenzierte Frequenzbänder, die unter Beachtung von bestimmten Regeln (z. B. maximale

Zugriffszeit oder maximale Strahlungsleistung) allgemein zugänglich sind. Diese freie Nutzung führt zu Kosteneinsparungen beim Betrieb, kann jedoch ebenfalls dazu führen, dass an bestimmten Orten die Frequenzen überlastet sind, was die Stabilität des Netzes stark beeinträchtigt.

5G besitzt beispielsweise hohe Datenraten und geringe Latenzen und es kann in der Regel auf bestehende Netzinfrastrukturen von Mobilfunkunternehmen zurückgegriffen werden. Nachteilig sind unter anderem die Betriebskosten, die Versorgungssicherheit abseits von urbanen Gebieten durch die geringen Reichweiten und der Verlust der Datenhoheit – selbst beim Einsatz eines eigenen virtuellen Kanals („Network slice“). LoRaWAN hingegen weist relativ große Reichweiten und niedrige Betriebskosten auf, verfügt jedoch nur über eine geringe Datenrate und hohe Latenzen. Durch die Nutzung von freien Frequenzen kann es zudem zu Überlastsituationen kommen. Teilweise kann auf existierende regionale Netzwerke zurückgegriffen werden, vielfach ist jedoch der Betrieb eines eigenen Netzwerks für Energienetzakteure notwendig und sinnvoll.

Aufgrund der Tatsache, dass elektromagnetische Wellen sich nur sehr schwer gegen Angriffe abschirmen lassen, besitzen alle drahtlosen Kommunikationstechnologien interne Sicherheitsmechanismen wie im Folgenden beispielhaft für LoRaWAN, 5G und 450 MHz LTE-M beschrieben.

LoRaWAN bietet Sicherheitsmechanismen auf zwei verschiedenen Ebenen [72]: zwischen Sensoren und Basisstation sowie zwischen Sensor und der Benutzeranwendung. Der Austausch der Schlüssel stellt dabei eine der größten Herausforderungen dar, da er bereits erfolgreich angegriffen wurde [24, 37, 94]. Mechanismen, die die LoRaWAN-Nutzdaten mit eigenen Entwicklungen [80] oder Standards wie TLS oder DTLS (Datagram Transport Layer Security) schützen, werden derzeit diskutiert [57, 95]. Die begrenzte Datenrate und das kleine Aktivitätszeitfenster stellen eine zusätzliche Herausforderung dar, weil derzeitige Sicherheitsprotokolle häufig nicht für schmalbandige Verbindungen optimiert sind [62].

Bei der 5G-Mobilfunktechnologie ist die gegenüber den vorherigen Standards (LTE) höhere Sicherheit ein wichtiger Aspekt. Hervorzuheben sind dabei insbesondere die asymmetrisch verschlüsselte Übertragung der geräteübergreifenden Identität der Mobilfunkteilnehmer (International Mobile Subscriber Identity, IMSI), die kryptografische Bestätigung des Mobilfunkbetreibers beim Roaming (Authentication Confirmation) sowie sichere Algorithmen zur Verschlüsselung des Datenverkehrs innerhalb der 5G-Infrastruktur, bei der sich Geräte und das Netzwerk gegenseitig authentifizieren [76, 93].

Eine für die Energiesysteme der Zukunft in der Bundesrepublik Deutschland wichtige Technologie ist LTE-M bei 450 MHz. Durch die Entscheidung der Bundesnetzagentur, dedizierte „Frequenzen für die Digitalisierung der Energiewende“ [22] an die 450connect GmbH[2] zu vergeben [23], besteht die Chance einer vollständigen Neukonzeption eines drahtlosen Kommunikationsnetzes für die Energiewirtschaft. Das wichtigste Merkmal dieses geplanten Netzes sind die günstigeren Ausbreitungseigenschaften bei einer Frequenz von 450 MHz im Vergleich zu klassischen Mobilfunknetzen. Um eine flächendeckende Abdeckung zu erreichen, wird eine deutlich geringere Anzahl an Basisstationen benötigt, was sich günstig auf die Projektierung im Bereich Investitions- und Operativkosten auswirkt sowie eine rasche Realisierung ermöglicht. Erste Modellierungsversuche zeigen, dass für eine Großstadt wie Düsseldorf die Errichtung von zehn Basisstationen für eine flächendeckende Ausleuchtung ausreichend sein könnte [87]. Durch die Teilnahme regionaler Energieversorger können gegebenenfalls zeitnah die benötigten Standorte für die Basisstationen gefunden werden.

[2] „Die 450connect GmbH ist ein Zusammenschluss aus vier Gesellschaftern: der bisherigen Alleingesellschafterin Alliander AG, einem Konsortium regionaler Energieversorger, E.ON sowie der Versorgerallianz 450 MHz, zu der mehrere Stadtwerke und Energie- und Wasserversorger gehören.“ [23]

Es ergeben sich jedoch weiterhin große Herausforderungen für das geplante Netz. Für eine finale Bewertung der Durchdringung von Gebäuden (bis in Kellerräume) fehlt es aktuell an großflächigen Messungen. Auch sind der sichere, hochverfügbare Aufbau und der Betrieb eines solchen Netzes für kritische Infrastrukturen aus ingenieurwissenschaftlicher Sicht herausfordernd. Ein höherer Grad an Automatisierung durch Software-Defined Networking (SDN) und Network Functions Virtualization (NFV) kann diesen Prozess unterstützen, jedoch muss gerade im Bereich Security unabdingbar von Beginn an auf Expertenwissen zurückgegriffen werden. Allgemein hilft auch der Ansatz Security by Design, Cybersecurity von Beginn an konsequent umzusetzen.

Getrieben durch den Bedarf, mehr Menschen in ruralen Gebieten mit Internet zu versorgen, bekommen aktuell Satellitensysteme erneute Aufmerksamkeit. Dabei muss zwischen Geosynchronous Earth Orbit (GEO), Medium Earth Orbit (MEO) und Low Earth Orbit (LEO) unterschieden werden. GEO-Satellitensysteme sind seit Jahrzehnten im Einsatz, jedoch mit dem signifikanten Nachteil, dass die Laufzeit einer Nachricht mindestens 500 ms beträgt, was für viele Anwendungsfälle nicht tragbar ist. MEO- und LEO-Systeme (Nanosatelliten) arbeiten in einer niedrigeren Umlaufbahn (zwischen 160 km und 2.000 km), was die Umlaufzeit erheblich verkürzt. Darüber hinaus wird eine Kommunikation zwischen den Satelliten vorgeschlagen, um die Anzahl der Übertragungen von der Erde in den Weltraum zu reduzieren. Zur Kommunikation mit Satellitensystemen werden komplexe und kostspielige Modems (Satellitenschüsseln) benötigt, die nur mit einer freien Sicht auf den Himmel funktionieren.

### 2.2.3 Dedizierte und öffentliche Infrastruktur

Für den Betrieb einer entsprechenden Infrastruktur – sowohl kabelgebunden als auch kabellos – sind grundsätzlich sowohl die Nutzung einer öffentlichen Infrastruktur, bereitgestellt durch einen ISP, als auch der Aufbau einer dedizierten eigenen – selbst oder extern administrierten – Infrastruktur möglich. Potenzielle Kosteneinsparungen sowie die vollständige Datenhoheit führen dazu, dass verschiedene Akteure im Energiesystem der Zukunft evaluieren, ein Kommunikationsnetzwerk selbstständig aufzubauen und zu betreiben. Ein dediziertes Netzwerk bietet in den Bereichen IT-Sicherheit und Quality of Service (QoS) mögliche Vorteile gegenüber öffentlicher Infrastruktur, die von wesentlich mehr Teilnehmern genutzt und ausgelastet wird. Aufgrund fehlender Expertise und mangelnder Erfahrung ist ein solches Vorhaben jedoch herausfordernd. Insbesondere im Bereich der kritischen Infrastrukturen ist ein umfassendes, modernes und solides Sicherheitskonzept unabdingbar – in diesem Bereich haben öffentliche ISP einen wesentlichen Erfahrungsvorsprung.

Kabelgebundene Netze haben in dieser Hinsicht den Vorteil, dass sie gegenüber Störquellen und Angriffen, die auf einem Angriffshost mit Netzwerkzugriff beruhen, wesentlich weniger anfällig sind. Die Implementierung von Sicherheitsfeatures ist jedoch auch für solche Netzwerke obligatorisch. Der Kostenaufwand für eine räumlich großflächige Abdeckung über ein kabelgebundenes Netz ist – verglichen mit kabellosen Netzwerken – im Allgemeinen höher.

Der Kostenvorteil kabelloser Netze wird auch von einer höheren Flexibilität hinsichtlich der Anbindung neuer Geräte begleitet. Faktoren wie geringere Bandbreiten, höhere Latenzen, Anfälligkeiten gegenüber Störfaktoren – sowohl im Normalfall als auch bedingt durch Angriffe – und die potenzielle Nutzung unlizenzierter Frequenzbänder stellen besondere Herausforderungen im Umgang mit drahtlosen Netzwerken dar. Die je nach Technologie beschränkte Bandbreite und Paketgröße verhindern zudem den Einsatz von Standardsicherheitsverfahren oder erschweren ihn zumindest.

Den besonderen Herausforderungen einer dedizierten Infrastruktur, insbesondere im Bereich ihrer sicheren Konzeption und Umsetzung, stehen jedoch auch mehrere Vorteile gegenüber. Durch die vollständige Kontrolle über das Netzwerk wird eine wesentlich höhere Flexibilität erreicht, wodurch die Reaktion auf Ereignisse erleichtert wird und auch planmäßige Änderungen gezielt und schneller umgesetzt werden können. Auch Garantien im Rahmen von QoS können implementiert werden, da Kommunikationswege und -umfang bekannt und kontrollierbar sind.

Sowohl seitens der Software und der Konfiguration als auch von der physischen Infrastruktur her sind Netzwerke unter Eigenbetrieb durch ihre spezifische, für den konkreten Anwendungsfall optimierte Konfiguration einem öffentlichen Netzwerk überlegen, sofern sie mit entsprechender Expertise betrieben werden. Durch die Lizenzierung des 450-MHz-Frequenzbandes für die Energiewirtschaft bietet LTE-M eine potenziell lohnende Möglichkeit zum Aufbau eines flächendeckenden drahtlosen Netzwerks. Die recht geringe Anzahl benötigter Basisstationen reduziert die Kosten für Aufbau, Wartung und Betrieb des Netzwerks, wobei die Eigenschaften der spezifischen Funktechnologie für viele Anwendungsfälle angemessen sind.

> Die Wahl der geeigneten Kommunikationstechnologie hängt immer vom beabsichtigten Anwendungsbereich ab. Während kabelgebundene Technologien – insbesondere Glasfaser – die besten technischen Eigenschaften und Sicherheitsfeatures mitbringen bzw. unterstützen, haben drahtlose Kommunikationstechnologien wesentliche Vorteile hinsichtlich Mobilitäts-, Flexibilitäts- und Kostenanforderungen. Allgemein empfiehlt es sich im Sinne der Zukunftsfähigkeit, Anforderungen grundsätzlich höher anzusetzen als unbedingt notwendig. Neben steigenden Anforderungen der Anwendung selbst, beispielsweise hinsichtlich Datenrate oder Latenz, können zukünftige Sicherheitsmechanismen ebenfalls höhere Anforderungen an die genutzte Kommunikationstechnologie stellen als heutzutage. Die Sicherheit der Kommunikation ist ein Grundpfeiler für die langfristige Zukunftsfähigkeit von Energienetzen und der Energiewirtschaft als Ganzes und muss jederzeit vorausschauend berücksichtigt und umgesetzt werden.

## 2.3 Cyberinnovationen durch den Einsatz allgemeiner Zukunftstechnologien

Die zuvor vorgestellten Kommunikationstechnologien sind ein Grundbaustein für die sichere Realisierung digitaler Anwendungen jeder Art. Da Digitalisierung und neue Anwendungsfälle sowie Anforderungen im Rahmen der Energiewende mit wachsenden Datenmengen, sicherheitskritischen Anwendungen und neuen Kommunikationsmustern einhergehen, sind sicherheits- und anwendungsorientierte Technologien auch in einem weiter gefassten Kontext als der reinen Kommunikation relevant. In Bezug auf die Informationstechnik (IT) bieten sowohl neue als auch bereits etablierte Technologien Potenziale, innovative Anwendungsfälle sicher und funktionsorientiert zu ermöglichen. Im Folgenden wird erst ein Überblick über Technologien gegeben, die zur Realisierung solcher Anwendungen in der Energiewirtschaft genutzt werden können. Anschließend werden Technologien diskutiert, die durch ihre Sicherheitsorientierung maßgeblich zur Cybersicherheit beitragen können.

### 2.3.1 Wegbereitende Technologien für anwendungsorientierte Innovationen

Die Dezentralisierung der Energieerzeugung und die Verfügbarkeit neuer Technologien wie der SMGW-Infrastruktur sind eine maßgebliche Ursache für neue Anwendungsfälle im Bereich der Energiewirtschaft. Eigenverbrauchsoptimierung, lokale Energiemärkte sowie flexibles Last- und Lademanagement sind nur einige Anwendungsfälle, für deren Realisierung innovative Technologien benötigt werden.

Hierbei ist eine Balance zwischen Offenheit und Transparenz sowie Aspekten wie Datenprivatsphäre bei maximaler Sicherheit äußerst wichtig. Während konkrete Anwendungsfälle in Abschnitt 3.1 vorgestellt werden, gibt dieser Abschnitt einen Überblick über Technologien, die aufgrund ihrer Eigenschaften für die Realisierung dieser Anwendungsfälle relevant sein können.

**Intelligente Messsysteme.** Ziel des aktuell laufenden Smart-Meter-Rollout ist die Schaffung einer effizienten Infrastruktur zur Umsetzung der Energiewende. Hierbei werden Verbraucher im Verteilnetz durch den zuständigen Messstellenbetreiber schrittweise mit einem zertifizierten, intelligenten Messsystem (iMSys) ausgestattet. Das iMSys besteht aus der modernen Messeinrichtung (Smart Meter) sowie dem Smart Meter Gateway (SMGW). Das SMGW dient dabei als zentrale Kommunikationseinheit, die die erfassten Messdaten des Verbrauchers verarbeitet und an die relevanten Marktakteure weiterleitet. Zur Absicherung und Verschlüsselung der Kommunikation ist das SMGW mit einem Sicherheitsmodul ausgestattet. Es dient als Schlüssel- und Zertifikatsspeicher und stellt die notwendigen kryptografischen Operationen bereit. Die Zertifizierung basiert auf einer Public-Key-Infrastruktur, die von einem durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftragten Zertifizierungsanbieter betrieben wird. Die SMGW-Infrastruktur und die diesbezüglich relevanten Akteure des Energiesektors werden mit einem Fokus auf die damit einhergehenden IT-Sicherheitsaspekte in Abschnitt 4.2 näher beschrieben.

**Cloud- und Edge-Computing.** Die Verlagerung von einer zentralisierten Energiewirtschaft hin zu einer dezentralen Energieerzeugung und dem entsprechenden Handel fordert von Technologien, die diese Trends unterstützen sollen, ebenfalls eine dezentralisierte Funktionsweise. Um die wachsenden Datenmengen aus mehreren Quellen angemessen zu verarbeiten, können Cloud- und Edge-Computing-Ansätze verwendet werden. Statt einer lokalen Verarbeitung vor Ort können zentrale Ressourcen flexibel und gezielt genutzt werden. Gleichzeitig kann auch die Verantwortlichkeit hinsichtlich des Betriebs der Infrastruktur ausgelagert werden: Cloud-Dienste versprechen hohe Verfügbarkeit und sind für die Endkundinnen und -kunden im Allgemeinen wartungsarm. Typische Dienstmodelle, die im Rahmen von Cloud-Computing angeboten werden, sind „Software-as-a-Service“ (SaaS), „Platform-as-a-Service“ (PaaS), „Infrastructure-as-a-Service“ (IaaS) sowie „Function-as-a-Service“ (FaaS), die unterschiedliche Grade der Abstraktion von der zugrunde liegenden Hard- und Software bieten.

Die Auslagerung in die Cloud und die Flexibilität von Cloud-Diensten bieten in vielen Bereichen wesentliche Vorteile im Bereich der Angriffsresilienz und auch der Kosten. Dennoch gehen diese Vorteile auch mit nicht zu vernachlässigenden Nachteilen einher. Durch die Auslagerung in die Cloud geben Kunden die Kontrolle über ihre eigenen Informationen an eine dritte Partei ab, sodass Datenschutz und Datenintegrität potenziell gefährdet sind – sowohl bei der Speicherung der Daten als auch bei ihrer Verarbeitung [61]. Zudem haben die Nutzer keinerlei Kontrolle über die Verfügbarkeit der genutzten Dienste. Störungen beim Cloud-Provider können nicht eigenständig behoben werden und treten gegebenenfalls zu Zeitpunkten ein, zu denen ein Ausfall für die Kunden besonders kritisch ist. Konzepte zur Nutzung von Cloud-Computing müssen somit insbesondere in der Energiewirtschaft immer auch Backup-Lösungen sowie Verschlüsselung, Authentifizierung und Validierung beinhalten.

Ein weiteres, oft gemeinsam mit Cloud-Computing genanntes Konzept ist Edge-Computing. Im Gegensatz zum logisch zentralisierten Cloud-Computing werden Datenverarbeitungsoperationen beim Edge-Computing bereits am Rand des Netzwerks bzw. im Netzwerk selbst durchgeführt. Hierdurch können verteilte Ressourcen besser genutzt und Datenmengen bereits früh beispielsweise durch Aggregation reduziert werden. Für die Energiewirtschaft kann durch direkte Datenverarbeitung nahe an den Operational-Technology-Geräten auch eine Handlungsfähigkeit bei Störungen in anderen Netzbereichen erreicht werden.

Aber auch bei der Verarbeitung von Daten auf Geräten, die im Gegensatz zu zentralisierten Konzepten weniger Ressourcen zur Verfügung haben, sind Aspekte der Sicherheit besonders relevant und dürfen nicht vernachlässigt werden. Da das Konzept des Edge-Computing den traditionellen Informationsflüssen widerspricht, ist eine umfassende Umstellung in Energiesystemen eine besondere Herausforderung.

**Blockchain-Technologie und Smart Contracts.** Die Blockchain-Technologie ist als Vertreter der Familie der Distributed-Ledger-Technologien ein weiterer vielversprechender Kandidat für die Erfüllung der Ansprüche von neuen Anwendungsfällen und Dezentralität [79]. Blockchains, bekannt durch ihre Verwendung bei der Realisierung von Kryptowährungen wie Bitcoin [71] oder Ethereum [92], bieten basierend auf ihrer dezentralisierten Struktur und kryptografischen Methoden die Möglichkeit, Daten ohne die Aufsicht einer vertrauenswürdigen dritten Partei (Trusted Third Party, TTP) sicher und gegen Veränderungen geschützt zu speichern.

Realisiert wird dies durch die kryptografische Verknüpfung von Datenblöcken zu einer Kette aus Blöcken, wobei jeder Block grundsätzlich eine beschränkte Menge beliebiger Informationen speichern kann. Durch das Anhängen neuer Blöcke an die Blockchain werden neue Informationen in ihr gespeichert und zudem die Informationen der vorhergehenden Blöcke kryptografisch gesichert: Ein Entfernen älterer Blöcke aus der Blockchain ist im Allgemeinen nicht mehr möglich. Die Persistenz der Informationen bringt jedoch auch den Nachteil mit, dass eine Blockchain ausschließlich größer wird und, insbesondere bei hoher Interaktivität oder hohen Datenmengen, schnell mehr Speicher- und Rechenkapazitäten benötigt [69], sodass für jede Anwendung immer eine fundierte Abwägung getroffen werden muss, ob eine Blockchain für die Realisierung angemessen ist.

Für die dezentrale Entscheidung, ob neue Blöcke an die existierende Blockchain angehängt werden können, gibt es diverse Verfahren sogenannter Konsensus-Protokolle. In öffentlichen Blockchains mit unbekannten Teilnehmern wie Bitcoin oder Ethereum ist das rechenintensive Proof-of-Work-Verfahren (PoW) weit verbreitet, während Blockchains mit Zugangsbeschränkungen und bekannten Teilnehmern, zum Beispiel im Kontext von Firmenkonsortien, häufig auf das Proof-of-Authority-Verfahren (PoA) setzen.

Die Fähigkeit einer Blockchain zur persistenten und gegen Änderungen geschützten Speicherung von Informationen kann auch genutzt werden, um dezentrale Anwendungen zu realisieren. Smart Contracts (SC) erlauben es, Datenerfassung, Informationsverarbeitung und allgemeine Vertragsbedingungen digital abzubilden und über eine Blockchain umzusetzen, sodass der „digitale Vertrag“ die gleichen Vorteile wie die Blockchain selbst bietet [79]. Auf Ethereum basierende Blockchains bieten Unterstützung für Smart Contracts nativ an [92]. Smart Contracts können hier als quasi-Turing-vollständige Programme in der Programmiersprache Solidity erstellt, auf der Blockchain gespeichert und in der Umgebung der Ethereum Virtual Machine (EVM) ausgeführt werden, wobei alle Operationen und Interaktionen im Kontext des SC durch die Verknüpfung mit der Blockchain transparent sind und von allen beteiligten Parteien validiert werden können. Bei der Speicherung von Daten in einer Blockchain sind jedoch immer auch Fragen des Datenschutzes zu berücksichtigen [68]. Smart Contracts können sich durch ihre einzigartigen Eigenschaften für sichere dezentrale Anwendungen auch für die Energiewirtschaft als wertvolle Technologie erweisen [79]. Herausforderungen hinsichtlich Skalierbarkeit und rechtlicher Fragen bedürfen jedoch noch weiterer Schritte, um Blockchains im Energiesektor etablieren zu können.

**Künstliche Intelligenz und Machine Learning.** Während sich die Blockchain-Technologie den Transparenz- und Dezentralitätsaspekten von Datenspeicherung und -verarbeitung widmet, sind dynamische Algorithmen und Verfahren zur Verarbeitung von Daten und zur Lösung domänenspezifischer Probleme ein auch für die Energiewirtschaft relevantes Gebiet, in dem KI eine wachsende Rolle spielt.

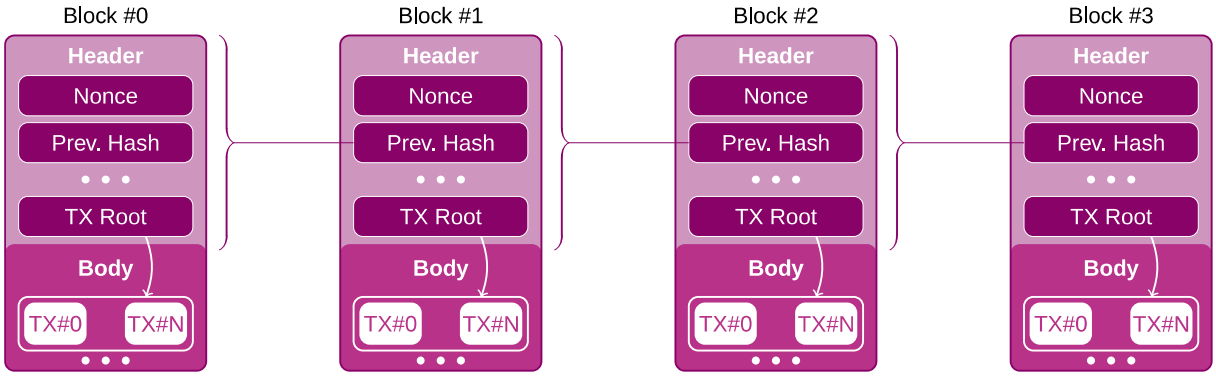


**Abbildung 2.2:** Die Blöcke in der Blockchain sind in einen Header- und einen Body-Abschnitt unterteilt. Im Body werden Informationen in Form von Transaktionen (TX) gespeichert, die kryptografisch mit dem Header verknüpft sind. Jeder Block beinhaltet den Hashwert des vorherigen Blocks, wodurch er mit der Kette verbunden wird. Um einen Block an die Blockchain anzuhängen, wird eine Nonce vorausgesetzt – ein Wert, der den Hashwert des aktuellen Blocks beeinflusst. Nur wenn der Hashwert bestimmte Voraussetzungen erfüllt – er beispielsweise einen gewissen Wert nicht überschreitet –, wird der Block akzeptiert. Die Wahl einer geeigneten Nonce ist aufwendig, wodurch die nachträgliche Änderung oder das Austauschen von Blöcken praktisch unmöglich sind.

Aufgrund der unspezifischen bzw. dehnbaren Definition von „Intelligenz“ lässt sich auch das Feld der KI nur schwer spezifizieren. Grundsätzlich wird unter KI die Fähigkeit eines Algorithmus oder Programms verstanden, Probleme dynamisch und flexibel zu lösen und so den Eindruck der Intelligenz zu vermitteln. Heutige Instanzen von KI widmen sich primär spezifischen Problemen [85, 90] und gelten durch diese Spezialisierung als „schwache KI“. Die Kombination mehrerer spezialisierter KI-Systeme erlaubt jedoch auch die Realisierung von komplexeren Anwendungsfällen wie beispielsweise von autonomem Fahren.

Prominente Teilgebiete der KI sind unter anderem Machine Learning (ML), Künstliche neuronale Netze (KNN) und Deep Learning. Hierbei werden entsprechende Systeme zur Lösung von Problemen zuerst basierend auf Beispielen angelernt, woraufhin das Erlernte anschließend verallgemeinert wird. Algorithmen zur automatischen Erkennung von Motiven oder Gesichtern in Bildern [97], aber auch die Identifizierung von Unregelmäßigkeiten in Kommunikationsmustern sind verbreitete Anwendungsgebiete für diese KI-Methoden. Basierend auf den Muster- und Anomalieerkennungsfähigkeiten von ML-basierten Programmen lassen sich auch Methoden zur Erkennung von netzwerkbasierten Angriffen durch Intrusion Detection Systems (IDS) realisieren. Dies lässt sich auch auf Probleme im Kontext von cyberphysischen Systemen wie Energienetzen übertragen, wo Anomalieerkennung hinsichtlich nicht optimaler oder kritischer Zustände eingesetzt werden kann [66]. So kann KI auch in Energienetzen sowohl auf Netzwerkebene als auch auf physischer Ebene zur (Cyber-)Sicherheit und zur wirtschaftlichen Optimierung beitragen.

Die Funktionen eines KI-basierten Systems lassen sich grundsätzlich in folgende Kategorien unterteilen [90]: i) Informationserkennung, ii) Identifizierung relevanter Informationen, iii) Ableitung weiterer Informationen und iv) Erstellung und Umsetzung von Handlungsempfehlungen. Je mehr dieser Aspekte ein auf KI setzendes System kombiniert, desto komplexere Anwendungen lassen sich realisieren.

Im Gegensatz zu klassischen Algorithmen ist das Verhalten von KI-Systemen, insbesondere im Kontext von ML, nicht immer vollständig deterministisch: Die Fähigkeit, Muster in Daten zu erkennen, die nicht im Lernprozess berücksichtigt wurden, hat zur Folge, dass die KI Informationen potenziell falsch kategorisiert und dass die Ursachen für das Fehlverhalten aufgrund der Intransparenz des Systems nicht zwangsläufig feststellbar sind. Insbesondere die Implementierung einer automatischen KI-gestützten Umsetzung von abgeleiteten Handlungsempfehlungen ist somit in cyberphysischen Systemen immer kritisch zu prüfen.

Dennoch bietet KI ein großes Anwendungspotenzial für die Energiewirtschaft: Neben IDS sind Prozessmodellierung, Prognosesysteme und Planungsmethoden vielversprechende Anwendungsfälle für KI, die in Kapitel 3 näher erläutert werden.

### 2.3.2 Zukunftstechnologien für Cybersicherheit in Energienetzen

Während die in Abschnitt 2.3.1 diskutierten Technologien vorwiegend wegbereitend für neue Anwendungsfälle sind, widmet sich dieser Abschnitt sowohl kryptografischen Verfahren als auch weitergehenden Konzepten mit einem Fokus auf Cybersicherheit. Ein umfassendes Cybersicherheitskonzept muss sowohl Präventiv- als auch Überwachungs- und Reaktionsmaßnahmen für spezifische Vorfälle beinhalten. Im Folgenden werden entsprechende Technologien zusammengefasst und diskutiert: Zur präventiven Cyberangriffsvermeidung sind allgemeine und spezielle Kryptografieverfahren, aber auch aktive Netzwerksteuerung relevant. In Kombination mit Detektionsmaßnahmen in Form von IDS und allgemeiner Prozessüberwachung können Cyberangriffe, die trotz der Präventivmaßnahmen erfolgreich sind, frühzeitig erkannt werden. Bei der direkten Interaktion von IT und physischen Systemen sind automatisierte Reaktionsmaßnahmen mit einem erhöhten Risiko verbunden: Durch Fehlalarme fälschlicherweise eingeleitete Maßnahmen können erheblichen Schaden anrichten – sowohl wirtschaftlich als auch gesundheitlich. Eine Kombination aus automatisierter Überwachung, automatisierten Handlungsempfehlungen und manueller Durchführung etwaiger reaktiver Maßnahmen verringert das Risiko unangemessener Reaktionen und belässt die Systemkontrolle vollständig in menschlicher Hand.

**Kryptografische Verfahren und Paradigmen.** Verschlüsselung und Authentifizierung von Netzwerkkommunikation sind essenzielle Mittel, dem Mitschneiden und der Manipulation von Kommunikationsinhalten vorzubeugen. Bei Verschlüsselungsmethoden wird grundsätzlich zwischen symmetrischen und asymmetrischen Verfahren unterschieden.

*Symmetrische Verfahren* nutzen in der Regel sowohl zur Verschlüsselung als auch zur Entschlüsselung denselben geheimen Schlüssel [30]. In dieser Familie stellt AES (Advanced Encryption Standard) [63] einen weit verbreiteten Algorithmus dar, der einzelne Datenblöcke symmetrisch verschlüsselt und dabei variable Schlüssellängen erlaubt. Durch diese Variabilität gilt AES nach heutigem Wissen auch als quasi post-quantum-sicher: Der Grover-Algorithmus [59] ist der einzige bekannte, durch Quantencomputer ermöglichte Algorithmus, dessen Einsatz das Aufbrechen einer AES-verschlüsselten Nachricht quadratisch beschleunigen kann – die Möglichkeit für eine exponentielle Beschleunigung durch Quantencomputer besteht allerdings nicht [77]. Demnach ist die Verwendung entsprechend längerer Schlüssel hinreichend, um die Wirksamkeit der AES-Verschlüsselung trotz Quantencomputern zu gewährleisten, da die AES-Verschlüsselung bei korrekter Verwendung und Implementierung nur durch einen somit auch für Quantencomputer ineffizienten Brute-Force-Angriff ausgehebelt werden kann. Symmetrische Verschlüsselungsverfahren haben allgemein den Vorteil, dass sie sicher und insbesondere schnell sowie universell anwendbar sind. Eine Voraussetzung für die sichere Anwendung ist allerdings ein ebenso sicherer Austausch des geheimen Schlüssels, der auch mithilfe von asymmetrischen Kryptografieverfahren ermöglicht wird.

Im Gegensatz zu symmetrischen Verfahren kommen in der *asymmetrischen Kryptografie* zwei verschiedene Schlüssel für Verschlüsselung und Entschlüsselung zum Einsatz. Ein privater Schlüssel (Private Key), der ausschließlich einer Partei bekannt ist, wird genutzt, um einen öffentlichen Schlüssel (Public Key) abzuleiten, der an alle potenziellen Kommunikationspartner und sonstige Parteien verteilt werden kann. Basierend auf diesem Prinzip lassen sich sowohl Verschlüsselung als auch Authentifizierung realisieren.

Ein typisches Verfahren zur Authentifizierung von Nachrichten ist, dass eine Prüfsumme der Nachricht mit dem Private Key der sendenden Partei verschlüsselt und zusammen mit der eigentlichen Nachricht als digitale Signatur zur empfangenden Partei gesandt wird. Diese kann die verschlüsselte Prüfsumme mithilfe des entsprechenden Public Key entschlüsseln und gegen die Nachricht verifizieren. Stimmt die Prüfsumme überein, kann die empfangende Partei sicher sein, dass die Prüfsumme durch den Besitzer des Private Key verschlüsselt und dass die Nachricht bei der Übermittlung nicht manipuliert wurde [30]. Analog funktioniert auch die Verschlüsselung von Nachrichten, bei der eine Nachricht mit dem Public Key der empfangenden Partei verschlüsselt wird, sodass nur diese durch den Besitz des zugehörigen Private Key die Nachricht entschlüsseln kann.

Im Gegensatz zur datenbasierten symmetrischen Kryptografie, die im Endeffekt auf einzelnen Bits arbeitet, interpretieren asymmetrische Kryptografieverfahren Informationen als Zahlen und führen mathematische Operationen auf diesen Zahlen durch, die sich nur durch spezifisches Wissen in Form des zugehörigen Schlüssels umkehren lassen. Hierdurch ergeben sich besondere mathematische Anforderungen an die Schlüssel selbst, sodass im Gegensatz zur symmetrischen Kryptografie nicht jede beliebige Zahl ein valider Schlüssel ist und im Allgemeinen längere Schlüssel benötigt werden, um ein vergleichbares Sicherheitsniveau zu erreichen. Zudem ist die Durchführung der mathematischen Operationen auf großen Datenmengen komplexer als die Verwendung symmetrischer Verschlüsselung. Aus diesem Grund kommen oft hybride Verfahren zum Einsatz, die große Datenmengen mit symmetrischer Kryptografie verschlüsseln und den symmetrischen Schlüssel mithilfe asymmetrischer Kryptografie verteilen. Ein weit verbreitetes Verfahren für die Aushandlung der asymmetrischen Schlüsselpaare über einen nicht vollständig sicheren Kommunikationskanal ist das Diffie-Hellman-Verfahren, das durch die Verwendung vorinstallierter Zertifikate auch gegen Man-in-the-Middle-Angriffe geschützt werden kann.

Die Sicherheit vieler asymmetrischer Verfahren beruht auf der Annahme, dass die zugrunde liegende mathematische Funktion zur Schlüsselherleitung nicht effektiv durch einen Computer umgekehrt werden kann. Die steigende Relevanz von Quantencomputern macht neben Verschlüsselung im Allgemeinen insbesondere den Einsatz von *Post-Quantum-Kryptografie (PQK)* notwendig, da die Annahme dieser mathematischen Komplexität der klassischen Verfahren in einigen Fällen mithilfe des Shor-Algorithmus umgangen werden kann [84]. Das Ziel der PQK ist es, insbesondere Signatur- und Schlüsseleinigungsverfahren bereitzustellen, die auch unter Zuhilfenahme eines Quantencomputers sicher sind. Insbesondere im Bereich der Schlüsseleinigungsverfahren hat das BSI im Jahr 2020 Handlungsempfehlungen zur Migration von Prä-Quantum-Verfahren veröffentlicht [52], um den frühzeitigen Umstieg auf langfristig sichere Verfahren zu unterstützen. Das National Institute of Standards and Technology (NIST) führt derzeit einen Standardisierungsprozess für PQK an, der 2020 in die dritte Phase startete [2, 52]. In der Empfehlung des BSI [52] werden das codebasierte Classic-McEliece-Verfahren [5] sowie das gitterbasierte FrodoKEM-Verfahren [3] aufgeführt. Diese Empfehlungen decken sich weitestgehend mit den verbleibenden Kandidaten des NIST, das BSI bewertet im Falle des FrodoKEM-Verfahrens die potenziell höhere Sicherheit jedoch als wichtiger als die schlechtere Performance gegenüber ähnlichen Verfahren.

In Kombination mit den als post-quantum-sicher angesehenen symmetrischen Verfahren sind diese Schlüsseleinigungsverfahren essenziell für die Sicherung der Kommunikation sowie von langfristig gespeicherten Daten in modernen Systemen, insbesondere im Bereich der kritischen Infrastruktur. Neben asymmetrischen Verfahren für Verschlüsselung und Schlüsseleinigung sind auch digitale Signaturverfahren von besonderem Interesse. Im Standardisierungsverfahren des NIST werden hier CRYSTALS-DILITHIUM, FALCON und Rainbox in der dritten Finalrunde berücksichtigt [2], wobei alle drei Algorithmen keinen Zustand speichern müssen

und so auch für verteilte Systeme oder virtualisierte Umgebungen und Backup-basierte Systeme geeignet sind. Als Alternativen für diese Algorithmen im Hinblick auf Post-Quantum-Sicherheit kommen auch zustandsbehaftete Hash-Signaturen in Frage, von denen sowohl LMS (Leighton-Micali Hash-Based Signature) wie auch XMSS (eXtended Merkle Signature Scheme) als von der Internet Engineering Task Force (IETF) standardisierte Verfahren bereits vom BSI aufgegriffen wurden [52]. Die Notwendigkeit der Speicherung eines Zustands sowie die Begrenzung der Anzahl der möglichen Signaturen mit einem Schlüssel werden jedoch oft als Nachteil dieser Verfahren gewertet, sodass zuvor genannte gitterbasierte und multivariate Signaturschemata vielversprechende Alternativen sind.

Aufgrund der mangelnden Erfahrungen mit PQK und der fehlenden Testmöglichkeiten für ihre praktischen Sicherheitseigenschaften ist die Verwendung von hybriden Verfahren empfehlenswert [29]. Statt ausschließlich auf ein PQK-Verfahren zu setzen, können beim Schlüsselaustausch – sofern Protokolle wie TLS (Transport Layer Security) oder SSH (Secure Shell) dies entsprechend unterstützen – auch zwei Protokolle parallel genutzt werden. Solange eines der beiden Protokolle sicher ist, bleibt der gesamte Schlüsselaustausch sicher. Durch die Wahl eines „klassischen“ Verfahrens und eines PQK-Verfahrens lässt sich so erreichen, dass zusätzlich Post-Quantum-Sicherheit erreicht wird und das Sicherheitsniveau im Vergleich zum derzeitigen Stand keinesfalls sinkt. Sollte sich das genutzte PQK-Verfahren als unsicher erweisen, sind die Daten weiterhin über das klassische Verfahren geschützt.

Aufgrund der Gefahr durch das „Harvest now, decrypt later“-Vorgehen, bei dem Daten bereits heute zur späteren Entschlüsselung mit Quantencomputern gesammelt werden, ist der Einsatz von PQK auch heute schon zu empfehlen, um Daten bereits jetzt langfristig zu schützen und Systeme frühzeitig auf die Existenz von Quantencomputern vorzubereiten. Die Kombination aus bewährter symmetrischer Kryptografie mit hinreichend großer Schlüssellänge und den vorgestellten quantensicheren Schlüsseleinigungs- und Signaturverfahren ist hierzu notwendig, sodass zusätzlich zur technischen Umsetzung auch das Bewusstsein für die möglichen Bedrohungen, denen ein Versäumen der rechtzeitigen Adaption Tür und Tor öffnet, auf allen Ebenen geschaffen werden muss.

Klassische Verschlüsselungskonzepte ermöglichen primär die Verschlüsselung zwischen zwei Parteien oder einer Gruppe von Parteien, die alle denselben symmetrischen Schlüssel teilen. Bei einem Szenario, in dem eine sendende Partei verschlüsselte Informationen an mehrere empfangende Parteien übermitteln möchte, die diese Informationen auch entschlüsseln können, ist die klassische asymmetrische Verschlüsselung des symmetrischen Schlüssels ineffizient, da der symmetrische Schlüssel für jede empfangende Partei einzeln asymmetrisch verschlüsselt und übermittelt werden muss. Insbesondere für dezentrale Anwendungsfälle mit Teilnehmern mit gegensätzlichen Interessen, wie beispielsweise lokale dezentrale Energiemärkte, bieten sich im Prozess der Schlüsselverteilung auch zusätzliche Angriffsvektoren, zum Beispiel durch die bewusst fehlerhafte Verschlüsselung des symmetrischen Schlüssels für eine bestimmte empfangende Partei.

Für Anwendungsfälle, die besonders sensibel für eine solche Form von Angriffen sind, bietet die *Attribute-based Encryption (ABE)* eine kryptografische Lösung [6]. Die Verschlüsselung des symmetrischen Schlüssels wird hierbei nicht für jeden Teilnehmenden einzeln vorgenommen, stattdessen erhalten die Teilnehmenden vordefinierte Attribute in Form kryptografischer Schlüssel durch eine oder mehrere Schlüsselautoritäten. Die sendende Partei nutzt eine logische Formel bestehend aus Konjunktionen und Disjunktionen über diese Attribute zur Verschlüsselung, sodass jeder Teilnehmende, der mit den ihm zugewiesenen Attributen die Formel erfüllt, die Daten entschlüsseln kann.

Auch im Bereich der ABE existieren Konzepte und Implementierungen für Post-Quantum-Sicherheit [78]. Das Verschlüsselungskonzept der ABE ermöglicht die detaillierte Kontrolle des Zugriffs auf Informationen und die Optimierung des Schlüsselverteilungsprozesses, bringt jedoch auch negative Implikationen im Bereich der Performance mit sich, sodass die Notwendigkeit des Einsatzes von ABE immer kritisch hinterfragt werden sollte.

Ein weiteres spezielles Verschlüsselungsverfahren ist die *vollständig homomorphe Verschlüsselung (Fully Homomorphic Encryption, FHE)* [56]. Der Schutz vertraulicher Informationen durch Verschlüsselung hat im Allgemeinen zur Folge, dass besagte Informationen nur verarbeitet werden können, wenn die verarbeitende Partei Zugriff auf diese Informationen hat. Mithilfe von FHE wird dieses Problem gelöst, indem Daten so verschlüsselt werden können, dass bestimmte Operationen, wie beispielsweise Addition oder Multiplikation, auch auf diesen verschlüsselten Daten durchgeführt werden können und das Ergebnis selbst auch verschlüsselt ist. Für Daten x und y sowie einen homomorphen Verschlüsselungsalgorithmus E gilt dann $E(x + y) = E(x) \oplus E(y)$, wobei $\oplus$ die Addition unter homomorpher Verschlüsselung repräsentiert. Insbesondere im Kontext von Cloud-Computing kann FHE hilfreich sein, da Daten so dezentral verschlüsselt verarbeitet werden können, Datenprivatsphäre und Sicherheit jedoch gewahrt werden. Die Anwendung von FHE ist grundsätzlich komplex, sodass zugunsten der Performance je nach Anwendungsbereich auch auf weniger mächtige partielle Homomorphismen zurückgegriffen werden kann und sollte.

> Zusammenfassend ist für den Kontext der Energiewirtschaft festzuhalten, dass sowohl langfristig abgelegte Informationen verschlüsselt werden sollten als auch existierende und zukünftige Kommunikationskanäle kryptografisch durch Verschlüsselung und Nachrichten-Authentifizierung gesichert werden müssen, um den Grundstein für Resilienz gegen Cyberangriffe zu legen.

**Übergeordnete Konzepte für systemweite Cybersicherheit.** Verschlüsselte Kommunikation und Informationsverarbeitung ist ein essenzieller Baustein zur Sicherung heutiger und künftiger Energiesysteme. Es sind jedoch weitere Maßnahmen erforderlich, um ein angemessenes Sicherheitsniveau auf Gesamtsystemebene zu erreichen. Hierbei müssen technische Maßnahmen und menschliches Verhalten aufeinander abgestimmt sein. Während sicherheitsfokussierte Awareness-Schulungen für Mitarbeiterinnen und Mitarbeiter sowie Konzepte wie Passwortrichtlinien oder die auch vom BSI empfohlene bzw. vorgeschriebene Zwei-Faktor-Authentifizierung [13] die Sicherheit bei (unwissentlichem) Fehlverhalten oder gezielten Angriffen (z. B. Phishing) gegen Nutzer und Systeme erhöhen, ist der Einsatz weiterer technischer Maßnahmen und Konzepte zur Prävention und Detektion von Cyberangriffen ratsam.

Ein mögliches Präventions- und Detektionsmittel ist Software-Defined Networking (SDN) zur aktiven Netzwerkkonfiguration, -steuerung und -überwachung [82]. SDN basiert auf dem Prinzip, dass die normalerweise lokal von Routern und Switches getroffenen Entscheidungen bezüglich der Datenweiterleitung (Control Plane) von der eigentlichen operativen Umsetzung der Datenweiterleitung (Data Plane) logisch getrennt und von einem logisch zentralisierten Controller übernommen werden. Die Data Plane verarbeitet Datenpakete anhand von Regeln, die über den Controller dynamisch erstellt und angepasst werden können. Wesentliche Vorteile gegenüber der statischen und lokalen Konfiguration sind hierbei zum einen die Möglichkeit, die Gesamtnetztopologie für die Konfiguration zu berücksichtigen, und zum anderen Änderungen vornehmen zu können, die als Reaktion auf neue Netzwerksituationen notwendig werden und potenziell mehrere Geräte gleichzeitig betreffen, die koordiniert gesteuert werden müssen.

Das Wissen und die Kontrolle über individuelle Datenströme (Flows) ermöglichen auch sicherheitsbezogene Anwendungen auf Netzwerkebene: Kommunikation zwischen spezifischen Geräten oder Netzsegmenten kann dynamisch ermöglicht oder unterbunden werden, im Störungsfall können neue Kommunikationswege aktiviert oder deaktiviert und Hosts (z. B. im Falle eines Angriffs) gezielt durch eine zentrale Einheit vom Netzwerk getrennt werden. Bekannte Konzepte im Kontext von SDN sind das OpenFlow-Protokoll [70] sowie die Netzwerk-Programmiersprache P4 [7], die das Handling von Netzwerkpaketen und -flows über Programme ermöglicht, die auf kompatiblen Switches ausgeführt werden. Da eine korrekte und unter Sicherheitsaspekten geplante Netzwerkkonfiguration zur Resilienz gegenüber Cyberangriffen unabdingbar ist, kann der Einsatz des SDN-Konzepts auch im Bereich der Energiewirtschaft zur erhöhten Cybersicherheit beitragen und sollte in Betracht gezogen werden.

SDN, Authentifizierung und verschlüsselte Kommunikation sind essenzielle Bestandteile zur Prävention von Cyberangriffen im Vorhinein. Da trotz optimaler Prävention erfolgreiche Cyberangriffe dennoch nicht gänzlich ausgeschlossen werden können, ist das Etablieren von zusätzlichen Erkennungsmaßnahmen sinnvoll. Durch das aktive Suchen nach Angriffen können die geeigneten Gegenmaßnahmen zur Abwehr eines Angriffs schon frühzeitig zur Schadensverhinderung oder Schadensbegrenzung eingeleitet werden und nicht erst, wenn ein Angriff größeren Schaden angerichtet hat. Intrusion Detection Systems (IDS) eignen sich für eine zeitnahe Detektion, da sie die an ihnen angeschlossenen Komponenten kontinuierlich und automatisiert überwachen, um auffälliges Verhalten zu detektieren und zu melden. Auch in bereits etablierten Systemen können IDS nachgerüstet werden.

Grundsätzlich unterscheidet man zwischen zwei verschiedene Arten von IDS-Ansätzen: Signatur-/regelbasierte IDS versuchen, bereits bekannte Angriffe anhand von gespeicherten Mustern wiederzuerkennen. Der Vorteil dabei ist, dass sie zumeist mit einer hohen Genauigkeit Cyberangriffe detektieren. Um jedoch weitere oder neuartige Angriffe zu erkennen, müssen die gespeicherten Muster kontinuierlich gepflegt werden. Generell können somit nur bereits bekannte Angriffe erkannt werden. Im Gegensatz dazu modellieren anomaliebasierte IDS das normale Verhalten eines Systems und alarmieren bei einer zu großen Abweichung vom Normalverhalten, wodurch auch neuartige Cyberangriffe erkannt werden können. Anomaliebasierte IDS sind jedoch anfälliger, wenn sich das modellierte normale Verhalten über die Zeit ändert, was eine bekannte Ursache für Falschalarme ist. In den letzten Jahren wurden in der IDS-Forschung große Fortschritte mittels Machine Learning gerade im Bereich der anomaliebasierten IDS erzielt.

Unabhängig von diesen beiden fundamentalen Funktionsweisen kann ein IDS in unterschiedlichen Bereichen eingesetzt werden: Einerseits bietet sich die Überwachung des zugrunde liegenden Netzwerkverkehrs (netzwerkbasiert) eines Systems an, um Angreifer anhand ihres Einflusses auf die Netzwerkkommunikation zu detektieren. Dies ermöglicht zum Beispiel die Erkennung ungewöhnlicher Verbindungen oder auch spezieller Angriffe gegen die verwendeten Protokolle und Geräte. Unter anderem sind SNORT [25] und Zeek [88] etablierte Lösungen in diesem Bereich, die sich signatur- oder regelbasierter Methoden bedienen. Andererseits können hostbasierte IDS auf Rechnersystemen eingesetzt werden, um Angriffe, deren Auswirkungen nicht im Netzwerk sichtbar werden, zu erfassen. Beispiele sind das Kompromittieren eines Rechners mittels USB-Stick oder die Ausbreitung von Schadsoftware innerhalb eines Rechners sowie über mehrere Rechner hinweg. Eine bekannte Lösung gerade zur Verwendung in verteilten Rechnernetzen ist beispielsweise Wazuh [91].

Darüber hinaus finden prozessbasierte IDS insbesondere bei cyber-physischen Systemen (CPS) Verwendung. Cyber-physische Systeme stellen die Verbindung zur realen Welt her, indem sie Messwerte erheben und regeln – wie dies auch bei verteilten Stromnetzen der Fall ist. Prozessbasierte IDS können die Auswirkungen

eines Cyberangriffs in Prozessdaten und somit den direkten Einfluss auf physikalische Gegebenheiten feststellen. Insbesondere beim Einsatz im Kontext von Opertational-Technology-Geräten können solche IDS die Sicherheit erheblich steigern. Unplausible Werte, das Ausbleiben von Messungen oder Auffälligkeiten bei der Umsetzung von Steuerbefehlen sind Angriffe gegen den Prozess selbst, die jedoch auch auf IT-Ebene erkannt und gemeldet werden können. Auch wenn IDS grundsätzlich mit automatisierten Gegenreaktionen als Intrusion Prevention System (IPS) kombiniert werden können, sollte insbesondere für Cyber-physische Systeme das Risiko bedacht werden, das durch fälschlicherweise ausgeführte Gegenmaßnahmen entsteht. Insgesamt bieten IDS somit eine nachrüstbare Option, um Cyberangriffe schnell zu erkennen und im Anschluss entsprechende Gegenmaßnahmen einzuleiten, bevor ein Angriff signifikanten Schaden anrichten kann.

> Für die sichere Realisierung von IT-gestützten Anwendungsfällen existiert ein breites Spektrum an Technologien, die anwendungs- und sicherheitsorientiert die Digitalisierung und Dezentralisierung der Energiewirtschaft unterstützen können. Insbesondere solche Technologien, die ohne tiefgreifende Änderungen an vorhandenen Systemen signifikante Verbesserungen der Sicherheit bieten, wie beispielsweise IDS, sollten zeitnah und vollumfänglich für einen Einsatz in Energiesystemen berücksichtigt werden.

## 2.4 Cybersichere Ertüchtigung energietechnischer Infrastruktur

Die zuvor diskutierten Technologien und Konzepte ermöglichen teils innovative Anwendungsfälle oder können vor allem die Sicherheit in Energienetzen gewährleisten. Insbesondere Kommunikationstechnologien (vgl. Abschnitt 2.2) und kryptografische Verfahren (vgl. Abschnitt 2.3.2) sind hierbei für die Sicherheit auf Geräteebene relevant. Die konkreten Anforderungen an individuelle Betriebsmittel im IT-Kontext, die für einen cybersicheren Einsatz im Energienetz notwendig sind, werden im Folgenden diskutiert, um konkrete Empfehlungen für die cybersichere Ertüchtigung der Geräte zu formulieren. Die auf Langlebigkeit konzipierten existierenden Betriebsmittel können derzeit nicht alle diese Anforderungen erfüllen, sodass zusätzliche Konzepte zur Absicherung der vorhandenen Geräte über die angedachte Betriebsspanne notwendig sind.

**Technische Anforderungen an cybersichere Betriebsmittel.** Das Ziel, Betriebsmittel über zwei bis drei Jahrzehnte zu betreiben, bringt besondere Anforderungen an ihre technische Ausstattung mit sich. Einerseits müssen alle verbauten Komponenten auf dieses Langlebigkeitsziel ausgerichtet sein und über den angedachten Zeitraum zuverlässig funktionieren, andererseits müssen die Geräte so flexibel und vorausschauend ausgelegt werden, dass eine Adaption aufgrund neuer Anforderungen ohne Probleme möglich ist.

Grundsätzlich sind für die Entwicklung und Ausstattung cybersicherer Betriebsmittel die folgenden Aspekte zu berücksichtigen:

1. Alle Hardwarekomponenten müssen auf Langlebigkeit ausgelegt sein und zuverlässig ihre Funktionen erfüllen.
2. Bei der Ressourcenplanung muss vorausschauend großzügig vorgegangen werden, das heißt, Speicher- und Rechenkapazitäten sollten so gewählt werden, dass auch die voraussichtlichen Anforderungen zum Ende der angedachten Lebenszeit erfüllt werden.
3. Sicherheitsrelevante und funktionsspezifische Elemente, beispielsweise Kryptografie- oder Kommunikationsmodule, müssen modular und austauschbar sein, um neuen Erkenntnissen und sich ändernden Anforderungen gerecht werden zu können, ohne komplette Geräte austauschen zu müssen.

4. Wenn möglich sollte auf General-Purpose-Hardware, also Hardware, die flexibel allgemeine Aufgaben erfüllen kann, zurückgegriffen werden. Insbesondere bei Prozessoren ist ein allgemeiner Anwendungsbereich hilfreich, um auch neue Aufgaben problemlos erfüllen zu können.
5. Eine Kernvoraussetzung für langfristige Cybersicherheit ist die Möglichkeit, Funktions- und Sicherheits-Updates auf Softwareseite einspielen zu können. Eine Verpflichtung zu regelmäßigen Sicherheits-Updates ist ratsam. Neben dem Schließen von Sicherheitslücken im System selbst sollten auch verwendete Algorithmen, insbesondere im Bereich der Kryptografie, austauschbar bzw. aktualisierbar sein.

Die langen Einsatzzeiten von Betriebsmitteln stehen im Konflikt zu einer sich ständig und schnell verändernden IT-Landschaft, wo neue Anwendungsfälle, Bedrohungen, Sicherheitsmechanismen, Verwundbarkeiten und Technologien mehrfach während der Lebenszeit eines Betriebsmittels zur Überholung der bei der Inbetriebnahme des Betriebsmittels geltenden Annahmen führt. Die vorausschauende Konzeption der Betriebsmittel ist deshalb umso wichtiger, sowohl im Bereich der Hardwareressourcen als auch im Bereich der Softwarefunktionalität. Wie in der Technischen Richtlinie TR-02102-1 des BSI [17] aufgeführt, ist beispielsweise der konkret angewandte Verschlüsselungsalgorithmus immer den derzeitigen Empfehlungen und dem Sicherheitskenntnisstand anzupassen. Hieraus ergeben sich direkt die Anforderungen an Software-Updates sowie Allzweckhardware bzw. austauschbare Spezialmodule. Neue Verfahren können auch erhöhte Anforderungen an die Rechenkapazität sowie die Arbeits- und Langzeitspeicher mit sich bringen, zum Beispiel längere Schlüssel oder komplexere Algorithmen. Diese potenziell steigenden Anforderungen müssen bereits in der Konzeption der Geräte großzügig berücksichtigt werden, da Mängel in der Ausstattung entweder zulasten der Langlebigkeit der dann auszutauschenden Geräte oder zulasten der Cybersicherheit gehen.

Aktuell genutzte Hardware mit unzureichender Ausstattung wird derzeit trotz Mängeln hinsichtlich der Cybersicherheit weiter eingesetzt, da ein Geräteaustausch kostspielig und aufwendig ist – ein Vorgehen, das insbesondere im Hinblick auf wachsende Bedrohungslagen und die zunehmende Digitalisierung der Energiewirtschaft nicht langfristig praktiziert werden darf. Standardisierte Zertifizierungsprozesse für den Einsatz von Betriebsmitteln, die in regelmäßigen Zeitabständen über die Einsatzerlaubnis von Gerätemodellen insbesondere im Kontext von KRITIS entscheiden, können hier auch als Anreiz für Hersteller und Betreiber wirken, die Mehrkosten durch eine großzügige Ausstattung der Geräte zu akzeptieren. Die konkrete Abwägung zwischen Kosten- bzw. Ressourceneffizienz und vorausschauender Ausstattung bleibt jedoch eine Herausforderung, die koordiniert aus wirtschaftlicher, technischer, politischer und regulatorischer Sicht angegangen werden muss.

**Cybersichere Ertüchtigung existierender Betriebsmittel.** Basierend auf der Erkenntnis, dass einige auf Langlebigkeit ausgelegte Betriebsmittel, die derzeit im Einsatz sind, weder aktuelle noch zukünftige Ansprüche an die Cybersicherheit erfüllen, werden in diesem Abschnitt Konzepte erörtert, die das Sicherheitsniveau in existierenden Netzwerken erhöhen können.

Eine offensichtliche Möglichkeit ist der Austausch der betroffenen Betriebsmittel durch solche, die unter Berücksichtigung der zuvor genannten Kriterien entwickelt und hergestellt worden sind. Da dieses Vorgehen jedoch sowohl organisatorisch als auch finanziell eine immense Herausforderung darstellen würde, sind weniger umfangreiche Maßnahmen als Übergangslösung gefragt. In einigen Fällen können gerätespezifisch Module ausgetauscht oder nachgerüstet werden. Geräte, die genug Ressourcen zur Verfügung haben, können potenziell auch durch Software-Updates gesichert werden. Angriffe auf die Kommunikation

zwischen Geräten sowie die Ausnutzung von Protokolleigenschaften oder -schwächen rücken insbesondere die Kommunikations- und Kryptografiefähigkeiten der Geräte in den Vordergrund. Im Allgemeinen ist hierbei jedoch ein Angleichen aller Kommunikationsteilnehmer notwendig, sodass meist das schwächste Glied das Sicherheitsniveau definiert.

Unabhängig von den eigentlichen Betriebsmitteln können mithilfe von Software-Defined Networking (SDN) und Intrusion Detection Systems (IDS) Kommunikationsmuster besser kontrolliert und überwacht werden. Diese Konzepte bieten jedoch keinen Mehrwert hinsichtlich der Vertraulichkeit (Verschlüsselung) oder Authentizität (Authentifizierung) der Kommunikation. Bei fehlender oder nur geringer Möglichkeit, die Betriebsmittel selbst zu aktualisieren, bieten sich im Wesentlichen zwei Konzepte zur Erhöhung der Kommunikationssicherheit an:

a) Ohne den Austausch von Protokollen werden protokollspezifische Eigenarten genutzt, um Sicherheitsfunktionen in die Kommunikation einzubetten (Retrofitting), oder b) einzelne Kommunikationsabschnitte werden durch Middlebox-basierte Verschlüsselung gesichert.

Im Falle des Retrofitting werden beispielsweise Message Authentication Codes (MACs) in potenziell gekürzter Form in ungenutzte oder mit Standardwerten belegte Protokollfelder integriert. Hier bietet sich der Vorteil, dass Geräte, die hinsichtlich dieser Features nicht aktualisiert werden können, weiterhin valide Kommunikationspakete erhalten und senden können. Das hierdurch erreichbare Sicherheitsniveau ist jedoch weiterhin recht gering, da oft nur wenige Bits genutzt werden können, um einen MAC zu übermitteln. Zudem können dem Protokollstandard widersprechende Feldbelegungen auch von einem IDS oder sonstigen Sicherheitssystemen als Angriff oder Unstimmigkeit gewertet werden, was beim Einsatz bedacht werden muss.

Der Einsatz von Middleboxes zur cybersicheren Ertüchtigung ist eine Möglichkeit, hohe Sicherheit auf Teilabschnitten des Kommunikationsweges zu erreichen. Sie können auch genutzt werden, um die Kompatibilität für Retrofitting-Maßnahmen für einzelne Geräte zu gewährleisten, indem die Middlebox die Protokollfelder entsprechend anpasst und ausliest, ohne dass das eigentliche Gerät dies erkennen kann. Mithilfe von Middleboxes können auch verschlüsselte Kommunikationskanäle zwischen einzelnen Netzabschnitten realisiert werden. So können beispielsweise Abschnitte zwischen einzelnen Standorten eines Energienetzsystems über einzelne VPN-Tunnel verbunden werden, über die der gesamte Datenverkehr verschlüsselt und authentifiziert übertragen wird. Die Umsetzung erfordert jedoch die Aufrüstung des Netzwerks mit entsprechenden Geräten, die die VPN-Tunnel etablieren, und schützt nur gegen Angriffe auf den entsprechenden Kommunikationsabschnitten: Eine Ende-zu-Ende-Verschlüsselung kann hierdurch nicht erreicht werden, sodass einem Angreifer, der Zugriff auf die Kommunikation zwischen Betriebsmittel und Middlebox hat, weiterhin die ursprünglichen Angriffsmöglichkeiten zur Verfügung stehen.

Die vorgestellten Konzepte können die Umrüstung auf cybersichere Betriebsmittel nicht dauerhaft ersetzen, da sie das Niveau einer umfassenden Ende-zu-Ende-Verschlüsselung und -Authentifizierung nicht erreichen können. Der Einsatz eines oder mehrerer dieser Konzepte zur Nachrüstung der Cybersicherheit existierender Betriebsmittel ist aber in jedem Fall empfehlenswert, um die Sicherheit kurzfristig zu erhöhen und den Übergang zu Betriebsmitteln mit integrierten Cybersicherheitsfeatures zu ermöglichen.

Wachsende Anforderungen an die Leistungsfähigkeit und Flexibilität von Energienetzen, die Dezentralisierung im Rahmen der Energiewende sowie die fortschreitende Digitalisierung stellen die Energiebranche vor neue Herausforderungen. Die Sicherheit der Energiesysteme ist sowohl auf physischer Ebene als auch im Bereich der digitalen Überwachung und Steuerung ein wesentlicher Aspekt. Neue – aber auch lang bekannte – Technologien aus dem Bereich der digitalen Kommunikation, der IT-Sicherheit und der IT im Allgemeinen bieten Möglichkeiten, neue Anwendungen zu realisieren, Sicherheit zukünftig zu gewährleisten und auch bereits bestehende Systeme gegen neue Bedrohungen abzusichern.

# 3 Innovative Anwendungsfälle in einer Bedrohungslandschaft im Wandel

Der technologische Fortschritt im Bereich sowohl der Energiewirtschaft als auch der Informationstechnik bietet in Kombination mit dem Paradigmenwechsel zu mehr Dezentralität und Kundeninteraktion in der Energiewirtschaft Raum für neue, innovative Anwendungsfälle, die erst durch die fortschreitende Digitalisierung ermöglicht werden. Durch diese Anwendungsfälle werden Entwicklungen wie die Energiewende, eine flexible Tarifgestaltung, die Elektromobilität sowie die allgemeine Netzstabilität und -resilienz ermöglicht oder gestärkt. Hieraus erwachsen jedoch auch neue Potenziale für Cyberangriffe gegen Energienetzbetreiber und ihre Kunden, sodass Cybersicherheit in Zukunft eine Top-Priorität für die Energiebranche sein muss. Im Folgenden werden zunächst konkrete Anwendungsfälle sowohl kunden- als auch netzbetreiberorientiert für die Energiebranche diskutiert (Abschnitt 3.1). Für die Bewertung ihrer cybersicheren Realisierung werden anschließend historische Angriffe analysiert (Abschnitt 3.2), um aus einem daraus resultierenden Angriffsmodell konkrete Handlungsempfehlungen und Anforderungen abzuleiten. Schließlich werden nationale Vorschriften und Regulierungen vorgestellt, die in diesem Kontext bereits etabliert sind (Abschnitt 3.3).

## 3.1 Neue Anwendungsfälle durch technologischen und strukturellen Wandel

Der Wandel der Energiebranche in Richtung Dezentralität und Digitalisierung bietet in Kombination mit neuen Technologien in den Bereichen Kommunikation, Kryptografie, Datenverarbeitung und Systemsicherheit ein enormes Potenzial für innovative Anwendungsfälle im Bereich der Anlagensteuerung und des Flexibilitätsmanagements sowie für die Kunden in Form von Eigenverbrauchsoptimierung, lokalen Energiemärkten und Tarifgestaltung und bezüglich der Doppelrolle als Prosumer, die Kunden einnehmen, die dynamisch Energie ins Netz einspeisen oder diese konsumieren. Dieser Abschnitt bietet einen Überblick über Anwendungsfälle sowohl aus Sicht der Netzbetreiber in Abschnitt 3.1.1 als auch aus Sicht der Kunden in Abschnitt 3.1.2. Hierbei werden insbesondere Herausforderungen sowie potenziell hilfreiche Technologien analysiert.

### 3.1.1 Netzbetreiberorientierte Anwendungsfälle

Dezentrale Erzeugungsanlagen (DEA), die auf erneuerbaren Energien basieren, nehmen einen wachsenden Anteil in der heutigen und zukünftigen Stromproduktion ein. Ihre Abhängigkeit von äußeren Gegebenheiten wie Sonneneinstrahlung und Wind führt dazu, dass die Vorhersage von Produktionskapazitäten erschwert wird und die tatsächliche Produktion spontanen Schwankungen unterliegen kann. Um die Einspeisung von Strom dennoch dem aktuellen Verbrauch anzupassen, können Stromspeicheranlagen sowie konventionelle Kraftwerke – auch im Rahmen des Redispatch 2.0 – koordiniert werden, um Engpässe zu verhindern und die Einspeiselokalisation anzupassen. Neben Schwankungen bei Erzeugungskapazitäten und Verbrauch können auch Leitungs- und Trafoüberlastungsschutz solche Maßnahmen notwendig machen. Eine übergreifende, flächendeckende digitale Kommunikation zwischen Erzeugern und Infrastrukturbetreibern ist somit unabdingbar. Die verlässliche und automatisierte Durchführung entsprechender Handlungen geht mit hohen Anforderungen an die Kommunikations- und Steuerungsinfrastrukturen einher. Ein zuverlässiger Betrieb sowie Resilienz gegen Störfaktoren und Angriffe sind Grundvoraussetzungen für den Einsatz im KRITIS-Bereich, sodass insbesondere Verschlüsselungs- und Sicherheitsmaßnahmen frühzeitig berücksichtigt werden müssen.

Zeitgleich stellen der gestiegene Elektrizitätsbedarf und der wachsende Anteil großer Verbraucher im Privatbereich im Rahmen der Elektromobilität neue Herausforderungen an das Stromnetz dar. Um die Stabilität des Stromnetzes zu garantieren, bietet digitale Koordination zwei weitere neue Anwendungsbereiche. Zum einen macht die wachsende Ladesäuleninfrastruktur ein vom Netzbetreiber koordiniertes oder direkt gesteuertes Lademanagement notwendig. Hierbei kann der Netzbetreiber abhängig von den derzeitigen Produktionskapazitäten und der Ladesituation dynamisch das Laden von Elektroautos drosseln oder gar deaktivieren, um das Stromnetz zu entlasten. Zum anderen lässt sich dieses Konzept als weiterer Anwendungsfall ausdehnen, indem die Speicherkapazitäten von Elektroautos im Rahmen von Vehicle-to-Grid-Konzepten (V2G) auch zur Einspeisung im Zusammenhang mit dem Engpassmanagement genutzt werden können.

In beiden Fällen ergeben sich mehrere kritische Anforderungen an eine entsprechende technische Lösung: Einerseits muss die Steuerung verlässlich und sicher sein. Insbesondere die zusätzliche Einspeisung von Kapazitäten aus dem privaten Bereich muss sowohl für die Privatperson als auch für das Stromnetz im Allgemeinen technisch sicher und störungsfrei erfolgen. Unbefugter Zugriff ist hier ebenso kritisch wie im IKT-Netz eines Stromnetzbetreibers selbst, die geringere Kontrolle der Netzbetreiber über eine entsprechende Kommunikationsnetzinfrastruktur stellt jedoch eine zusätzliche Herausforderung dar. Verschlüsselung und Authentifizierung von Messwerten und insbesondere Steuerbefehlen sind Grundvoraussetzungen für solche Anwendungsfälle. Andererseits spielen auch Datenschutz und Privatsphäreaspekte eine wesentliche Rolle. Durch den Eingriff in das Ladeverhalten eines Elektroautos, potenziell kombiniert mit einer zusätzlichen Entladung des Fahrzeugakkus, kann die Nutzbarkeit des Fahrzeugs als solches im Zweifel wesentlich eingeschränkt werden. Vorgaben der Besitzerinnen und Besitzer, beispielsweise hinsichtlich einer Uhrzeit, zu der der Fahrzeugakku geladen sein muss, sind unbedingt zu berücksichtigen. Auch potenzielle Notfälle sind nicht zu vernachlässigen und müssen in ein entsprechendes Konzept aufgenommen werden: So sollte ein Fahrzeugakku niemals unter einen bestimmten Ladestand entladen werden, um eine kurzfristige Nutzung des Fahrzeugs weiterhin zu ermöglichen.

Damit auch für die Kundinnen und Kunden ein Mehrwert aus der Entscheidung, vorhandene Kapazitäten und Steuermöglichkeiten dem Netzbetreiber zur Verfügung zu stellen, entsteht, wächst auch die Notwendigkeit von dynamischen und transparenten Tarifmodellen. Für die Kombination aus technischen und tariflichen Aspekten für die genannten Anwendungsfälle an der Schnittstelle zwischen Endkundschaft und Netzbetreibern kann neben proprietären Lösungen auch das Smart Meter Gateway (SMGW) eine Schlüsselrolle mit viel Innovationspotenzial spielen. Hierzu müssen jedoch alle involvierten Parteien, von der Endkundschaft über die Ladesäulenhersteller bis hin zu den Netzbetreibern, das SMGW als eine einheitliche, offene und zielführende Technologie ansehen. Zur Erfüllung dieser Voraussetzung können einerseits umfängliche technische Fähigkeiten des Gateways selbst, andererseits aber auch Technologietransparenz – insbesondere in Richtung der Privatkundinnen und -kunden – sowie gezielt eingesetzte regulatorische Unterstützung beitragen.

Im Kontext SMGW-gestützter Anwendungsfälle lassen sich auch der zuvor genannte Redispatch 2.0, Engpassmanagement sowie die Direktvermarktung nennen. Aktuelle und hochfrequente Informationen bezüglich der aktuellen Einspeisung oder Entnahme von Leistung einzelner Haushalte erlauben in der Gesamtheit, den allgemeinen Netzzustand genauer zu erfassen, Engpässe frühzeitig zu erkennen und Gegenmaßnahmen rechtzeitig einzuleiten. Umfangreiche Datenschutzmaßnahmen vorausgesetzt, lassen sich diese Informationen zudem nutzen, um externen Marktteilnehmenden die Möglichkeit für umfangreiche Mehrwertdienste zu bieten. Analog zum bereits benannten Lademanagement und zu V2G-Konzepten können mithilfe des SMGW

auch andere Geräte im Rahmen des Smart Grid genutzt werden: Endverbraucherinnen und -verbraucher oder Prosumer können mit dem Netzbetreiber ein für sie vorteilhaftes Tarifmodell aushandeln, das die zeitlich und betragsmäßig begrenzte Steuerung von Endgeräten oder ganzen Verbrauchseinrichtungen zulässt. Hierdurch erhält der Netzbetreiber bessere Kontrolle über Engpässe, die reduziert oder ganz vermieden werden können.

### 3.1.2 Kundenorientierte Anwendungsfälle

Für eine weitreichende Akzeptanz von Änderungen an bestehenden Infrastrukturen und Abläufen sind neben jenen Anwendungsfällen, die primär auf die Netzbetreiber ausgelegt sind, auch solche relevant, die Vorteile und neue Möglichkeiten direkt für die Kundinnen und Kunden bieten oder das Stromnetz auf der „letzten Meile“ betreffen. Grundlegende Konzepte wie V2G und variable Tarifgestaltung wurden bereits aus Betreibersicht diskutiert. Im Folgenden wird ein besonderer Fokus auf die Kundensicht sowie das SMGW gelegt.

Während für Netzbetreiber insbesondere Engpass- und Flexibilitätsmanagement Anreize für verstärkte Kundeninteraktion sind, stehen für die Endkundschaft primär günstigere Tarifmodelle oder sonstige finanzielle Aspekte im Vordergrund. Diese Tarifanwendungsfälle bieten somit im Optimalfall einen Vorteil für beide Seiten, sofern ein angemessenes Gleichgewicht zwischen Eigen- und Selbstkontrolle eingehalten wird und die Berücksichtigung von Aspekten wie Datensicherheit oder Privatsphäre gewährleistet ist. Durch eine zeitlich variable Tarifgestaltung, die zum Beispiel über das SMGW transparent an die Kundinnen und Kunden kommuniziert wird, haben diese die Möglichkeit, ihren Eigenverbrauch zu optimieren und Kosten einzusparen, indem der Verbrauch dem gegenwärtigen Tarif angepasst wird. So bietet sich dem Netzbetreiber eine indirekte Möglichkeit des Engpassmanagements, während die Kundinnen und Kunden finanziell profitieren können.

Die Dezentralisierung des Stromnetzes betrifft neben den Stromnetzbetreibern selbst auch immer stärker die Kundinnen und Kunden. Sie nehmen durch die Einbindung von Photovoltaik-Anlagen oder dedizierten Stromspeicheranlagen oder durch Konzepte wie V2G eine Doppelrolle als Verbraucher und Stromproduzenten (Prosumer) ein, die neben der zuvor erwähnten Interaktion mit dem Netzbetreiber auch Optionen für direkte Peer-to-Peer-Märkte bietet. Hieraus ergeben sich neben den zuvor diskutierten Möglichkeiten zur Eigenverbrauchsoptimierung auch Geschäftsmodelle für Kundinnen und Kunden, Stromkapazitäten abhängig vom jeweiligen Marktpreis zur Speicherung zu kaufen oder gewinnbringend ins Netz einzuspeisen. Abhängig von den jeweiligen Möglichkeiten der Prosumer, zum Beispiel den vorhandenen Speicher- und Produktionskapazitäten, und dem variierenden Angebots- und Nachfrageverhältnis können lokale Energiemärkte (Local Energy Markets (LEMs)) als nachbarschaftsorientierte Handelsplattformen dienen [79].

Für Kundinnen und Kunden bieten LEMs die Möglichkeit, Strom nicht nur direkt vom Netzbetreiber bzw. von dedizierten Stromanbietern zu kaufen, sondern auch von anderen Prosumern zu beziehen. Hierdurch werden Anreize für sie geschaffen, einerseits in Photovoltaik- und Speicheranlagen zu investieren, andererseits jedoch auch als reine Verbraucherinnen und Verbraucher an einem LEM teilzunehmen. Die Verknüpfung mehrerer LEMs zu einem überregionalen Markt kann die Kosteneffizienz weiter steigern, verlangt jedoch auch komplexere technische Lösungen, die den Anforderungen einer solchen dezentralen Plattform gerecht werden, insbesondere im Hinblick auf Datensicherheit und Privatsphäre.

Als wesentliche Anforderungen an eine Plattform für LEMs sind insbesondere Zuverlässigkeit, Vertrauenswürdigkeit und der Schutz von Kundendaten zu nennen. Alle diese Aspekte setzen zudem eine solide Sicherheitsinfrastruktur voraus. Zuverlässigkeit und Vertrauenswürdigkeit umfassen in diesem Kontext die

Verfügbarkeit und Störungsresilienz des Systems, aber auch geringe Latenzen bezüglich der Preisentwicklung und der allgemeinen Marktsituation. Zudem muss Angebotstransparenz gewahrt werden, um möglichen Manipulationen vorzubeugen. Somit ist entweder eine vollumfänglich vertrauenswürdige Partei für den Betrieb notwendig oder es kann auf eine dezentralisierte Realisierung, beispielsweise mit Blockchain-Technologie, zurückgegriffen werden. Für eine sichere Kommunikation zwischen allen Teilnehmern sind auch SMGWs zu nennen, die, eine offene Anwendungsplattform vorausgesetzt, als zentrales Element zur sicheren Umsetzung von LEMs dienen können.

Neben diesen kurzfristigen Tarifoptionen schafft die Nachfrage nach einer flexibleren Tarifgestaltung auch den Anwendungsfall, den Stromanbieter dynamischer wählen zu können. Über eine sichere, standardisierte Schnittstelle, beispielsweise im Rahmen des SMGW, könnten Kundinnen und Kunden die Möglichkeit erhalten, ihren Tarif flexibler zu wechseln. Aspekte wie automatische Zählerstandsübermittlungen, Ferndiagnoseoptionen oder der Registrierungsprozess von Anlagen im Marktstammdatenregister (MaStR) sind weitere Anwendungsfälle für eine Architektur wie das SMGW, die von der zunehmenden Digitalisierung profitieren können, sofern eine umfassende Sicherheitskultur gegeben ist.

> Digitalisierung, technologischer Fortschritt und der durch die Energiewende bedingte strukturelle Wandel der Energiewirtschaft bieten Potenzial für neue Anwendungsfälle, die sowohl kunden- als auch netzbetreiberorientiert Vorteile bieten können. Anwendungsfälle wie Flexibilitätsmanagement, Netzstabilität und Resilienz gegen Netzsegmentierungen sowie flexible Tarifmodelle und die Prosumer-Doppelrolle können von innovativen Lösungsansätzen profitieren. Um dieses Potenzial auszuschöpfen, müssen mehrere Voraussetzungen erfüllt sein, die sich im Wesentlichen in die gegenseitige Nützlichkeit und die (Cyber-)Sicherheit zusammenfassen lassen. Jeder Lösungsansatz muss immer die Interessen sowohl der Endkundschaft als auch die der Netzbetreiber berücksichtigen, um einen Mehrwert für alle beteiligten Parteien zu gewährleisten. In Kundenrichtung können finanzielle Anreize – etwa flexiblere Tarifmodelle – helfen, auch solche Anwendungen umzusetzen, die primär Vorteile für die Netzbetreiber bieten. Zudem müssen alle Lösungen Aspekte der Datensicherheit und Privatsphäre von Anfang an berücksichtigen und konsequent umsetzen.

## 3.2 Historische Angriffsvektoren und Cyberbedrohungen der Zukunft

Der Notwendigkeit von und der Forderung nach besonderer Sicherheit für Energiesysteme liegen mehrere Beispiele zugrunde, die auf teils dramatische Weise unterstreichen, wie anfällig entsprechende Netze sind und welche Folgen erfolgreiche Cyberangriffe haben können. Der Prozess der cybersicheren Ertüchtigung der Energienetze, insbesondere im Hinblick auf neue Anwendungsfälle (vgl. Abschnitt 3.1), setzt eine detaillierte Aufarbeitung und ein tiefgehendes Verständnis historischer Angriffe voraus, aus denen sich auch zukünftige Bedrohungen herleiten lassen. Erst wenn ein geeignetes Niveau an Cybersicherheit erreicht bzw. verfügbar ist, kann die Realisierung der zuvor genannten Anwendungen konsequent angegangen werden. Dieser Abschnitt stellt zunächst historische Cybersicherheitsvorfälle vor, die anschließend hinsichtlich übergeordneter Kriterien wie Angriffsphasen und allgemeiner Angriffsvektoren analysiert werden. Darauf aufbauend werden Cyberbedrohungen diskutiert (Abschnitt 3.2.2), die insbesondere im Rahmen der Digitalisierung und von Konzepten wie dem SMGW absehbar an Relevanz gewinnen werden und entsprechend berücksichtigt werden müssen, um Cyberinnovationen für das sichere Energiesystem der Zukunft umsetzen zu können.

### 3.2.1 Analyse historischer Cyberangriffe und Forschungsergebnisse

In der näheren Vergangenheit ist die Zahl der Cyberangriffe gegen Energienetzakteure stetig gestiegen. Die Folgen solcher Angriffe werden im günstigsten Fall durch Redundanzsysteme aufgefangen, doch auch weitreichende und lang anhaltende Stromausfälle mit Tausenden bis Hunderttausenden Betroffenen sind bereits Realität geworden [38]. Die Risiken, denen Energienetze im Kontext von Cyberangriffen ausgesetzt sind, bauen auf diversen Faktoren auf: Als Einfallstor sind Phishing und Social Engineering als Methoden zu nennen, die statt technischer Sicherheitslücken auf menschliches (unwissentliches) Fehlverhalten setzen [66]. Fehlende Sicherheitsmaßnahmen ermöglichen dann das unbemerkte Agieren im Netzwerk, wo die oft veralteten und nicht hinsichtlich der IT-Sicherheit entwickelten Protokolle das Anrichten von immensen Schäden begünstigen [66]. Im Folgenden werden drei Cyberangriffe gegen Stromnetze bzw. Stromnetzkomponenten vorgestellt und analysiert, um typische Schwachstellen zu identifizieren und abstrakte Vorgehensweisen abzuleiten. Darauf aufbauend werden konkrete Handlungsempfehlungen und technische Lösungen zusammengestellt, die solchen Angriffen entgegenwirken.

**Der Aurora-Generator-Test.** Das besondere Risiko, das durch die Kombination von älteren Kommunikationsprotokollen und ihrer direkten Kopplung mit physischem Equipment entsteht, wurde bereits 2007 im Aurora-Generator-Test [96] unterstrichen. Der getestete Angriff zielt auf die Desynchronisation eines Generators mit dem zugehörigen Stromnetz und nutzt Zeitverzögerungen in Sicherheitsmechanismen gezielt aus. In der ersten Phase des Angriffs wird der synchronisierte Generator durch das Öffnen der Leistungsschalter vom Netz getrennt. Der Lastabfall hat eine Steigerung der Generatorgeschwindigkeit zur Folge, sodass die vom Generator erzeugte Netzfrequenz der des restlichen Netzes vorauseilt. Innerhalb weniger Millisekunden ist hierdurch eine Verschiebung um nahezu eine halbe Phase erreicht. Im zweiten Schritt des Angriffs werden die zuvor geöffneten Leistungsschalter wieder geschlossen [96]. Durch die asynchrone Phase von Generator und Stromnetz wird ein enormes Drehmoment auf den Generator ausgeübt, das unter Umständen seine Toleranz übersteigt und so dauerhafte Schäden verursacht.

Diese Verwundbarkeit ist insbesondere deshalb relevant, weil sie sich auch die fehlende Verschlüsselung und Authentifizierung von Modbus und anderen älteren Protokollen zunutze macht. Neben physischen Schutzmechanismen, wie der Überwachung von Schalteroperationen und der Verhinderung des Schließens eines Schalters bei abweichender Phase, sind somit Schutzmechanismen in der Kontrollkommunikation von immenser Bedeutung. Ein zeitlich so präzise ausgeführter Angriff ist manuell nur äußerst schwierig realisierbar und setzt den physischen Zugriff auf Schalter oder das Steuersystem voraus, während ein auf den Verwundbarkeiten des Kommunikationsprotokolls aufbauender Angriff ohne diese Voraussetzung auskommt. Der Aurora-Generator-Test unterstreicht, dass Cyberangriffe das Potenzial besitzen, physischen Schaden an Geräten, aber auch an Personen zu verursachen.

**Cyberangriffe gegen das ukrainische Stromnetz.** Zwei der prominentesten Angriffe gegen Stromnetze fanden in den Jahren 2015 und 2016 in der Ukraine statt [38, 67]. In beiden Fällen wurden Stromnetzbetreiber (ähnlich einem Verteilnetzbetreiber) Ziel von Cyberangriffen, was Stromausfälle für mehrere Hunderttausend Kundinnen und Kunden zur Folge hatte. Am 23. Dezember 2015 wurde ein koordinierter Angriff auf drei Stromversorgungsunternehmen festgestellt, wobei sowohl Steuerungs- und Verwaltungsanlagen der SCADA-Systeme (Supervisory Control and Data Acquisition) als auch Netzwerkgeräte betroffen waren. Die Angreifer erhielten vermutlich bereits neun Monate zuvor Zugriff auf interne Systeme, indem Malwarebehaftete Office-Dokumente im Rahmen von Spear-Phishing-Angriffen per E-Mail an Mitarbeiterinnen und Mitarbeiter geschickt wurden. Dies ermöglichte das passive Sammeln von Informationen, insbesondere in Form von Zugangsdaten, die den Zugriff auf weitere Systeme und Netzbereiche ermöglichten, sowie über die

Funktionen und Interaktionen des IKT-Netzes und der Steueranlagen. Zusätzlich wird vermutet, dass auch Einsatzgeräte von Beschäftigten manipuliert wurden, sodass davon ausgegangen werden kann, dass die Angreifer immense Ressourcen zur Verfügung hatten. Basierend auf den gesammelten Informationen und den Zugriffsmöglichkeiten der Angreifer wurden am 23. Dezember 2015 im Rahmen des eigentlichen Angriffs Leistungsschalter in insgesamt mindestens 27 Umspannwerken umgeschaltet, was direkte Ursache für den Stromausfall bei vielen Kundinnen und Kunden war. Um die Diagnose und Behebung dieses Ausfalls zu erschweren, wurden zeitgleich Angriffe gegen Überwachungssysteme, die unterbrechungsfreie Stromversorgung (USV) und Steuerungsserver, aber auch gegen die Firmware von Feldgeräten durchgeführt.

Ähnlich wie beim Angriff im Jahr 2015 wurde ein Stromnetzbetreiber am 17. Dezember 2016 Opfer eines Cyberangriffs, der den Ausfall einer Umspannstation verursachte und für etwa ein Fünftel der Stromverbraucherinnen und -verbraucher von Kiew, mehrere Hunderttausend Kundinnen und Kunden, einen Stromausfall zur Folge hatte [67]. Trotz des Mangels an stichfesten Beweisen wird der Angriff allgemein russischen Hackern zugeschrieben. Die Ermittlungen zu dem Vorfall deuten auf die Nutzung der Malware „Industroyer/CRASHOVERRIDE“ hin, die speziell für den Einsatz gegen Industrienetze, insbesondere Energienetze, konzipiert wurde. Sie kann eine Verbindung zu einem externen Kontrollserver herstellen oder autonom ohne externe Kommunikation operieren, wobei die Malware diverse in Energienetzen eingesetzte Kommunikationsprotokolle beherrscht und so Schaltbefehle und Monitoring-Nachrichten mitlesen, manipulieren oder generieren kann. Dies bietet neben der Möglichkeit zur Steuerung von Geräten auch die Option der False Data Injection, also des gezielten Manipulierens von Messwertmeldungen wie Spannungsmessungen oder Schalterstellungen. Die so übermittelten Fehlinformationen können Schalthandlungen durch die Leitwarte provozieren oder Fehlerzustände vertuschen.

> Die beiden Angriffe auf das ukrainische Stromnetz zeigen, dass Cyberbedrohungen für die Energiebranche längst Realität sind und es bereits weit entwickelte Angriffstools gibt. Angreifer mit entsprechender Expertise sind in der Lage, Stromnetzen erheblichen Schaden zuzufügen. Der Umfang der beiden Angriffe gegen das Stromnetz der Ukraine unterstreicht zudem die Relevanz der IT für komplexe Angriffe: Ein so koordiniertes, paralleles Vorgehen gegen mehrere Umspannwerke und Netzbetreiber wäre ohne die umfassende Nutzung der IT-Infrastruktur im Rahmen des Cyberangriffs nur schwer möglich. Die Priorität eines angemessenen Schutzes der IT-Infrastruktur gegen solche Angriffe wird durch die ukrainischen Fallbeispiele weiter bekräftigt. Zudem erlaubt die Komplexität der Angriffe die Ableitung allgemeiner Angriffskonzepte, die im Folgenden vorgestellt werden.

**Abstrahierte Angriffsvektoren, Angreifermodelle und Angriffsphasen.** Das Vorgehen der Angreifer in verschiedenen Szenarien lässt eine Abstrahierung auf allgemeine Verfahren und die Identifizierung häufiger universeller Verwundbarkeiten zu. Insbesondere aus den komplexeren Angriffen auf das ukrainische Stromnetz lassen sich zunächst Erkenntnisse hinsichtlich verschiedener Angriffsphasen ziehen. Solche abstrahierten Modelle, insbesondere mit Fokus auf IKT-Netze, sind bereits mehrfach konzipiert worden, beispielsweise im Rahmen der ICS (Industrial Control System) Cyber Kill Chain [4], die zwischen zwei Angriffsphasen unterscheidet: der Intrusion-Phase, die vorbereitende Schritte umfasst, und der ICS-Attack-Phase, die den eigentlichen Angriff repräsentiert [4]. Insbesondere im Kontext von Energienetzen ist eine Unterteilung in weitere Phasen jedoch präziser, da hier die großflächige Netzwerkstruktur sowie die Unterteilung in verschiedene Netzwerksegmente einen wesentlichen Unterschied zu allgemeinen IKT-Netzwerken darstellen.

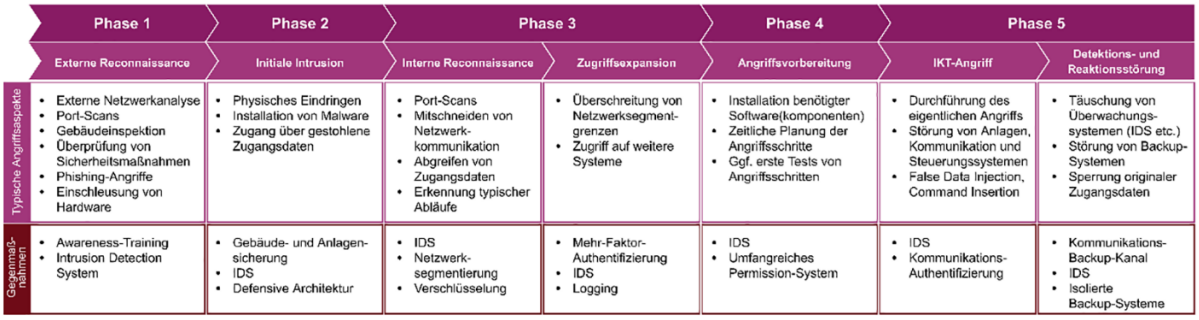


**Abbildung 3.1:** Angriffe gegen die IKT-Infrastruktur eines Stromnetzbetreibers lassen sich in fünf Hauptphasen unterteilen. Nachdem das Eindringen ins Netzwerk geplant und vorbereitet wurde, können detaillierte Informationen über das Netzwerk, die Kommunikationsmuster und die Nutzer gesammelt werden. Diese Informationen werden genutzt, um den eigentlichen Angriff technisch und konzeptuell zu planen und letztendlich durchzuführen. Hierbei können neben den eigentlichen Zielen des Angriffs zusätzlich auch Möglichkeiten gestört werden, den Angriff zu detektieren oder auf ihn zu reagieren. Für alle Angriffsphasen existieren verschiedene Gegenmaßnahmen, um vorbereitend oder akut dem Angriff entgegenzuwirken.

Für die IKT-Netze von Stromnetzen lassen sich daher die folgenden Angriffsphasen unterscheiden, wobei die Schwere potenzieller Folgen im Allgemeinen mit jeder Phase steigt. Die Angriffsphasen und typischen Aktionen während der einzelnen Phasen sind zusätzlich in Abbildung 3.1 zusammengefasst.

1. Während der externen Reconnaissance untersuchen Angreifer ihr Ziel auf mögliche Einfallstore und Angriffsvektoren. Hierzu zählen die aktive und die passive Untersuchung des (externen) Netzwerks, potenziell aber auch das Ausspähen von Gebäuden sowie Mitarbeiterinnen und Mitarbeitern.
2. Der zweite Schritt ist die initiale Intrusion, in der Angreifer Zugriff auf ein internes Netzwerksegment oder ein an das interne Netzwerk angeschlossenes Gerät erhalten.
3. a) Es folgt die interne Reconnaissance. Während dieser Phase werden weitere Informationen über das System gesammelt, insbesondere Kommunikationsmuster und Zugangsdaten zu anderen Netzsegmenten. Mithilfe dieser Informationen werden die folgenden Angriffsphasen vorbereitet.

   b) Zuvor gesammelte Informationen und Zugangsdaten werden zur Zugriffsexpansion genutzt. Die Angreifer erlangen Zugriff auf weitere Systeme und Netzsegmente, die sie zur weiteren Reconnaissance nutzen können.
4. Sobald die Angreifer ausreichend viele Systeme kompromittiert haben, startet die Angriffsvorbereitung für den eigentlichen IKT-Angriff.
5. a) Der IKT-Angriff wird durchgeführt. Es werden einzelne oder mehrere Systeme angegriffen, indem Kommunikation manipuliert oder unterbunden wird, Steuerbefehle zur Destabilisierung des Stromnetzes gesendet werden oder manipulierte Messwerte im Rahmen einer False Data Injection (FDI) an die Leitwarte gesendet werden.

   b) Zeitgleich oder nachbereitend können Maßnahmen zur Detektions- und Reaktionsstörung ergriffen werden, indem Logdateien manipuliert, Backup-Systeme gestört oder Leitsystemkomponenten blockiert werden.

Die abstrahierte Sichtweise auf das Vorgehen bei Angriffen ermöglicht es, typische Schwachstellen und Angriffspunkte zu identifizieren und so entsprechend angemessene Gegenmaßnahmen abzuleiten. Eine häufige vorbereitende Methode ist der Angriff über Beschäftigte des Zielinfrastrukturbetreibers. Über Phishing oder das Platzieren von präparierten USB-Sticks auf dem Parkplatz, die von den Mitarbeiterinnen

und Mitarbeitern mitgenommen werden und so unwissentlich ein Einfallstor öffnen können, bietet sich Angreifern eine Möglichkeit, ohne direktes Aushebeln von dedizierten Cybersicherheitslösungen Zugriff auf das Netzwerk zu erlangen. Es ist daher unabdingbar, frühzeitig ein entsprechendes Sicherheitsbewusstsein bei allen Beschäftigten zu schaffen, um auf diesen Verfahren aufbauende Risiken im Keim zu ersticken. In Kombination mit Intrusion Detection Systems (IDS), die beispielsweise Port-Scans frühzeitig erkennen, lässt sich das Risiko für einen erfolgreichen Angriff so bereits frühzeitig erheblich senken.

Neben dem physischen Absichern von Anlagen und Gebäuden ist eine defensive Konfiguration des Netzwerkequipments von Hosts notwendig, um die initiale Intrusion bei Angriffen zu verhindern oder zumindest zu detektieren. Die Deaktivierung von ungenutzten Netzwerkports, die Überwachung der Netztopologie und IDS steigern die Chance, einen Angriff unmittelbar zu erkennen und zu unterbinden. Auch ab Phase 3 spielen IDS eine wesentliche Rolle für die Prävention und Detektion des Angriffs. Aufgrund ihrer breiten Einsatzgebiete sowie der Möglichkeit, IDS in etablierten Systemen relativ leicht nachzurüsten, ist ihr Einsatz auch nach dem IT-Sicherheitsgesetz 2.0 verpflichtend. Dennoch sind zusätzlich auch defensive Netzwerkarchitekturen mit Segmentierung und Verschlüsselung sowie mehrschichtige Authentifizierungsmechanismen unabdingbar, um Angriffen effektiv entgegenzutreten. Sollten Zugangsdaten dennoch in die Hände von Angreifern geraten, hilft ein feingranulares Permission-System, ihre Möglichkeiten einzuschränken. Ein IDS oder ein Log-Überwachungssystem, das die Nutzung von Zugangsdaten für den Zugriff auf ungewöhnliche Systeme oder Netzbereiche meldet, kann diese Möglichkeiten weiter einschränken.

Trotz all dieser Sicherheitsmaßnahmen, die die Detektion von Angriffen erleichtern, ist die Verschlüsselung jeglicher Kommunikation sowie insbesondere die Authentifizierung und Integritätssicherung von Messwertmeldungen und Steuerbefehlen unbedingt notwendig, um Angriffe über mehrere Phasen hinweg effektiv zu verhindern. Um im Falle eines Angriffs schnell, effizient und korrekt zu reagieren, sind auch umfassende Pläne zur Reaktion (Incident-Response-Strategien), beispielsweise in Form von Maßnahmenkatalogen und durch Übungsdurchführung, notwendig.

### 3.2.2 Cyberbedrohungen im Energiesystem der Zukunft

Die aufgezeigten Angriffsvektoren unterstreichen die Wichtigkeit von umfassenden Cybersicherheitskonzepten in heutigen und zukünftigen Energienetzen. Aktuelle Entwicklungen in der Energiewirtschaft hinsichtlich Dezentralisierung und Digitalisierung sowie der anhaltende Fortschritt im Bereich der Informationstechnologie werden in naher Zukunft weitere Möglichkeiten für Cyberangriffe eröffnen. Durch die zunehmende Vernetzung im Stromnetz und die Nutzung öffentlicher Infrastruktur wie beispielsweise Mobilfunk wird Angreifern eine breitere Angriffsfläche geboten. Da einige traditionell durch Personen besetzte Stationen, beispielsweise kleinere Umspannwerke und Windkraftanlagen, im Zuge dieses Wandels vollständig unbemannt oder mit weniger Personal ausgestattet sind, wird auch hier verstärkt auf digitale Kommunikation zur Steuerung dieser Anlagen gesetzt.

Zusätzlich zur allgemein breiteren Angriffsfläche kommen potenzielle Risiken durch die Verfügbarkeit von neuartigen Technologien, wie beispielsweise Quantencomputern, hinzu. Der Einsatz von Post-Quanten-Kryptografie sollte demnach zeitnah erfolgen, um Kommunikation und insbesondere gespeicherte Informationen langfristig gegen unbefugten Zugriff zu schützen. Selbst wenn die Entschlüsselung von Informationen, die mit Prä-Quantum-Verfahren verschlüsselt wurden, erst zukünftig möglich ist, können verschlüsselte Daten bereits heute abgegriffen, gespeichert und zu einem späteren Zeitpunkt entschlüsselt werden. Die Gefahr für die Informationssicherheit durch zukünftige Quantencomputer ist folglich bereits heute präsent und muss entsprechend berücksichtigt werden.

Auch der Anschluss steuerbarer (Groß-)Verbraucher wie Ladesäulen oder SMGW-gestützter Geräte birgt potenzielle Risiken für die Energiebranche. Einerseits können Angreifer durch die gezielte Ansteuerung mehrerer solcher Geräte versuchen, das Stromnetz signifikant zu stören, indem Verbraucher synchron an- oder abgeschaltet werden, was bei einer ausreichenden Menge an Verbrauchern Einfluss auf die Netzfrequenz haben kann. Andererseits kann das Manipulieren der durch das SMGW übermittelten Leistungswerte negative Auswirkungen auf das Netz mit sich bringen, wenn die tatsächliche Leistung von den gemeldeten und für die Planung genutzten Werten abweicht [65].

Weiterhin ist die Privatsphäre der Kundinnen und Kunden ein Aspekt, der bis heute aufgrund einer geringen Angriffsfläche eine niedrige Priorität hatte. Durch die zunehmende Vernetzung entlang des Stromnetzes bis hin zu den Verbraucherinnen und Verbrauchern verlassen Kundeninformationen wie allgemeine Verbrauchsmuster oder tagesaktuelle Leistungswerte, zum Beispiel über ein SMGW übermittelt, die direkte Kontrolle der Kundinnen und Kunden selbst. Die adäquate Sicherung dieser Informationen, sowohl auf dem Transportweg durch das Netzwerk als auch während der Verarbeitung durch die Netzbetreiber und bei der potenziellen anschließenden Speicherung, muss lückenlos gewährleistet sein. Auch eine Interaktion Dritter mit einem SMGW oder einem anderweitig kommunizierenden Gerät, das entsprechende Informationen bereitstellen kann, muss verhindert werden.

> Insgesamt lässt sich festhalten, dass Konzepte wie Verschlüsselung, Integritätssicherung und Authentifizierung mit PQK-Verfahren in Kombination mit einer defensiven Netzwerkarchitektur und Awareness-Schulungen zur Prävention, IDS und SDN zur Detektion sowie weitreichende Reaktionspläne sowohl heute als auch für zukünftige Angriffsszenarien gegen Energienetze unabdingbar sind und die Grundlage eines jeden Sicherheitskonzepts sein müssen. Ein hohes Sicherheitsniveau sollte jedoch nicht nur als Pflicht, sondern auch als Grundlage und Chance für weitreichende Innovationen gesehen werden, die Fortschritt und Zukunftsfähigkeit der Energiewirtschaft garantieren.

## 3.3 Regulierungen und Standards zur KRITIS-Cybersicherheit

Die vorgestellten Technologien, Konzepte und Vorgehensweisen, Cybersicherheit in Energienetzen zu garantieren, sind aufgrund ihrer enormen Relevanz auch bereits Teil geltender Regulierungen, Vorschriften und Standards mit Bezug zur Energiewirtschaft. In diesem Abschnitt werden entsprechende regulatorische Grundlagen zur IT-Sicherheit in der Energieversorgung zusammengestellt und diskutiert.

Das Energiewirtschaftsgesetz (EnWG) [44] bildet die rechtliche Grundlage für die Energieversorgung über Strom- und Gasnetze und legt Rechte und Pflichten für Netzbetreiber sowohl auf Übertragungs- als auch auf Verteilnetzebene fest. Für Kundenanlagen sind darüber hinaus die technischen Mindestanforderungen entsprechend der für die jeweilige Spannungsebene gültigen Anwendungsregel vom Verband der Elektrotechnik, Elektronik und Informationstechnik e.V. (VDE) maßgeblich. Ergänzt wird das EnWG durch das Erneuerbare-Energien-Gesetz (EEG) [42], das die vorrangige Behandlung von Anlagen zur Erzeugung erneuerbarer Energien regelt. Das Gesetz zur Digitalisierung der Energiewende, das auch das Messstellenbetriebsgesetz (MsbG) [43] umfasst, legt den rechtsverbindlichen, flächendeckenden Einbau moderner Messeinrichtungen und einen verbindlichen Plan zum Einsatz von intelligenten Messsystemen (iMSys) fest. Unter anderem durch einen vorläufigen, gerichtlich angeordneten Stopp des verpflichtenden Einbaus von iMSys durch das Oberverwaltungsgericht Münster vom 4. März 2021 verzögert sich der Smart-Meter-Rollout zunehmend. Der Beschluss wurde damit begründet, dass die durch das MsbG und die gültige Technische Richtlinie (TR) 03109-1 [15] des Bundesamts für Sicherheit in der Informationstechnik (BSI) definierten

Anforderungen an das SMGW nicht die gesetzlichen Mindestanforderungen, insbesondere hinsichtlich eines Mindestmaßes an Interoperabilität, abdecken [73].

In Abbildung 3.2 sind die wesentlichen regulatorischen Grundlagen für den sicheren Netz-, Anlagen- und Messstellenbetrieb in der Energieversorgung dargestellt.

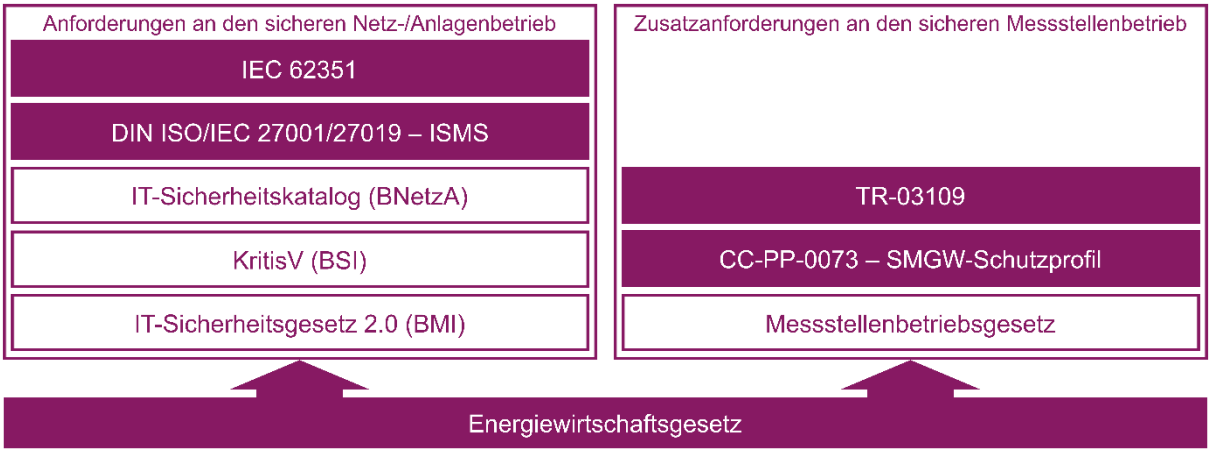


**Abbildung 3.2:** Die rechtliche Grundlage für Informations- und IT-Sicherheit in der Energieversorgung bildet das Energiewirtschaftsgesetz. Für den sicheren Netz- und Anlagenbetrieb existieren jedoch weitere rechtliche und technische Richtlinien, die auf dem Energiewirtschaftsgesetz basieren bzw. es ergänzen. Analog werden auch Anforderungen hinsichtlich des sicheren Messstellenbetriebs rechtlich durch das Messstellenbetriebsgesetz sowie technische Richtlinien konkretisiert.

Die nationale gesetzliche Grundlage für Cybersicherheit ist im Wesentlichen durch das IT-Sicherheitsgesetz 2.0 [51] gegeben, durch das insbesondere auch die Rolle des BSI bezogen auf den Sektor der Energieversorgung hinsichtlich einer zentralen Organisation der IT-Sicherheit gestärkt wurde. Besondere Anforderungen gelten für kritische Infrastrukturen, deren Zugehörigkeit durch die Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) bestimmt wird. Die BSI-KritisV definiert Schwellenwerte, oberhalb derer technische Anlagen des Energiesektors als kritische Infrastruktur gelten [47]. Zusammen mit dem IT-Sicherheitsgesetz 2.0 wurden die Grenzwerte nach BSI-KritisV für verschiedene technische Anlagen heruntergesetzt und es zeigt sich, dass die Energiewende als entscheidender Faktor für die Anpassung der Anforderungen hinsichtlich der IT-Sicherheit im Energiesektor wahrgenommen wird. Die entsprechenden Schwellenwerte können Tabelle 3.1 entnommen werden. Weiterhin maßgeblich für Netzbetreiber ist der IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG der Bundesnetzagentur (BNetzA) [19], der grundlegende Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit) definiert und insbesondere die Implementierung eines Information Security Management System (ISMS) gemäß DIN ISO/IEC 27001 [40], zusätzlich ergänzt um energiespezifische Anforderungen gemäß DIN ISO/IEC TR 27019 [41], für alle Netzbetreiber fordert.

Während die Einführung eines ISMS insbesondere unternehmensinterne Prozesse bezogen auf die Informationssicherheit optimiert bzw. dokumentiert, ist darüber hinaus auch die Gewährleistung der Informationssicherheit aus systemischer Sicht erforderlich. Für Netz- und Stationsleittechnik ist diesbezüglich die IEC-Normenreihe 62351 [27] zu erfüllen. Neben Anforderungen an die eingesetzten Komponenten (z. B. Fernwirkgeräte, Netzwerkgeräte, Leitsysteme) werden hier insbesondere auch Risiken bezogen auf die Kommunikationsstrecken im Fernwirknetz berücksichtigt. Hier ist exemplarisch die Absicherung der eingesetzten Fernwirkprotokolle wie beispielsweise IEC 60870 [26] und IEC 61850 [28] zu nennen, die nativ keine eigenen Maßnahmen zur abgesicherten Kommunikation vorsehen. Für Energieanlagen existiert analog zum

Netzbetrieb gemäß § 11 Absatz 1b EnWG ebenfalls ein IT-Sicherheitskatalog, der für alle Anlagen gilt, die gemäß BSI-KritisV als kritische Infrastruktur anzusehen sind. Der Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) hat zudem zusammen mit seinem österreichischen Schwesterverband im Best-Practice-Whitepaper zu Anforderungen an sichere Steuerungs- und Telekommunikationssysteme grundlegende IT-Sicherheitsempfehlungen für die Energiebranche auf Basis der gesetzlichen Grundlage definiert [36].

| **Stromerzeugung** | | Schwellenwert |
|---|---|---|
| Erzeugungsanlagen | Installierte Nettonennleistung | 104 MW |
| | Installierte Nettonennleistung bei Anlagen, die als Schwarzstartanlage kontrahiert sind | 0 MW |
| | Installierte Nettonennleistung bei Anlagen, die zur Erbringung von Primärregelleistung präqualifiziert sind | 36 MW |
| Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung | Installierte Nettonennleistung | 104 MW |
| | Installierte Nettonennleistung bei Anlagen, die als Schwarzstartanlage kontrahiert sind | 0 MW |
| | Installierte Nettonennleistung bei Anlagen, die zur Erbringung von Primärregelleistung präqualifiziert sind | 36 MW |

**Tabelle 3.1:** Die KritisV [47] sieht ab Januar 2022 neue Schwellenwerte für kritische Infrastrukturen vor. Exemplarisch sind hier die Schwellenwerte für Anlagen zur Stromerzeugung sowie zur Steuerung/Bündelung elektrischer Leistung angegeben.

Im Rahmen der EU-NIS2-Direktive („Netz- und Informationssysteme“) gibt es außerdem konkrete Bestrebungen, eine umfassende Cybersicherheitsstrategie für verschiedene Sektoren, zu denen auch der Energiesektor zählt, übergreifend auf EU-Ebene weiterzuentwickeln. Eine EU-weite Grundlage für den Cybersicherheitsstandard wird hier durch den „Network Code on Cybersecurity“ vorgegeben werden, dessen Entwurf bereits durch die European Network of Transmission System Operators for Electricity (ENTSO-E) im Oktober 2021 vorgelegt wurde [39]. Dies bietet Potenzial, europaweit angeglichene Maßstäbe für die Cybersicherheit insbesondere auch für kritische Infrastrukturen, aber auch gleiche Wettbewerbsbedingungen für betroffene Sektoren zu schaffen.

Bezüglich des Messstellenbetriebs ist darüber hinaus zu differenzieren zwischen den Mindestanforderungen an das SMGW selbst hinsichtlich der IT-Sicherheit, die im zugehörigen Schutzprofil BSI-CC-PP-0073 festgelegt sind, sowie den Anforderungen auf funktionaler Basis und an die für den Betrieb relevante Infrastruktur. Für Zweiteres ist die oben genannte, mehrteilige TR-03109 maßgeblich, die Anforderungen an die Interoperabilität (Teil 1 und 2), kryptografische Vorgaben (Teil 3), Anforderungen bezüglich der verwendeten Public-Key-Infrastruktur (PKI) (Teil 4), die Kommunikationsschnittstellen zur Ankopplung von Zählern und steuerbaren Anlagen (Teil 5) und Anforderungen an die Gateway-Administration (Teil 6) umfasst.

Insgesamt existieren somit umfangreiche regulatorische Vorgaben, die die operative und IT-technische Sicherheit adressieren. Die Vielzahl an individuellen und sich ergänzenden Richtlinien kann jedoch auch zu Problemen bei der Konzeption und Umsetzung neuer Produkte führen, wie beispielsweise dem SMGW, sodass eine frühzeitige Abstimmung der Einzelregularien untereinander immer wichtiger wird. Die Notwendigkeit zukunftsorientierter Anpassungen von Richtlinien, Empfehlungen und deren Herleitungsprozessen wurde bereits im „Stufenmodell zur Weiterentwicklung der Standards für die Digitalisierung der Energiewende“ [53] identifiziert und mit konkreten Handlungsempfehlungen versehen. Weiterhin sind regelmäßige Aktualisierungen der technischen Anforderungen und Empfehlungen notwendig – eine zentrale Zusammenstellung entsprechender Technologien kann helfen, IT-Sicherheit als dedizierte, sich wandelnde Komponente in der Energiewirtschaft zu verankern. So könnten Kryptografieverfahren hinsichtlich ihres Sicherheitsniveaus kategorisiert werden, um die häufigen Anpassungen und Neuentwicklungen angemessen zu kommunizieren. Neben Sicherheitsvorschriften im Allgemeinen sollten auch Anreize diskutiert werden, die Akteure dazu ermutigen, Sicherheit über die Mindestanforderungen hinaus zu implementieren.

Innovationen im Bereich der Tarifgestaltung, der Netzführung und der netzorientierten Anwendungen ist ein wesentlicher Aspekt des Wandels der Energiewirtschaft im Angesicht der Energiewende und der zukünftigen Herausforderungen. Angriffe auf Stromnetze in der Vergangenheit unterstreichen, wie wichtig Cybersicherheit bereits heute für die Energiewirtschaft ist. Im Kontext der zunehmenden Digitalisierung wird Cybersicherheit nunmehr noch wichtiger und muss vorausschauend geplant und konsequent umgesetzt werden. Das Paradigma „Security by Design“ bietet großes Innovationspotenzial, sofern alle Parteien – Regulatorik, Umsetzung und Endkundschaft – transparent in den Prozess eingebunden und ihre jeweiligen Anforderungen berücksichtigt werden. Das folgende Kapitel widmet sich dieser Thematik im Detail und betrachtet die Rolle von Cybersicherheit im Kontext anwendungsorientierter Innovationen in der Energiewirtschaft sowie die Probleme und Chancen aus den Erfahrungen mit dem SMGW, um so Faktoren zu identifizieren, die sich fördernd oder hemmend auf entsprechende Innovationen auswirken.

# 4 Cybersicherheit als energiewirtschaftlicher Innovationstreiber

Die Digitalisierung in der Energiewirtschaft bringt Potenzial für Innovationen in verschiedenen Anwendungsbereichen mit sich, von denen im Folgenden ausgewählte Bereiche exemplarisch betrachtet werden (Abschnitt 4.1). Bei der dafür notwendigen Kommunikationsinfrastruktur wird in den folgenden Betrachtungen ein besonderer Fokus auf die Smart-Meter-Gateway-Infrastruktur (SMGW) gelegt, die zukünftig eine sichere Basis für die Anbindung von Endkundinnen und -kunden an andere Akteure zur Umsetzung sowohl von markt- als auch von netzbezogenen Prozessen bilden soll (Abschnitt 4.2). Aber auch unabhängig von der verwendeten Infrastruktur muss für die Umsetzung innovativer Anwendungsfälle ein Mindestmaß an Anforderungen hinsichtlich der IT-Sicherheit und des Datenschutzes erfüllt werden. Die Umsetzbarkeit dieses Vorhabens und mögliche Technologien zu seiner Unterstützung werden in Abschnitt 4.3 behandelt.

## 4.1 Status quo der energiewirtschaftlichen Innovationen auf nationaler Ebene

Der Rückgang der konventionellen Erzeugungskapazitäten führt zu neuen Herausforderungen im Bereich der Systemdienstleistungen wie Betriebsführung, Momentan- und Regelreserve, Spannungsstabilität und Schwarzstartfähigkeit (vgl. Abschnitt 2.1). Erneuerbare Einspeiser und steuerbare Lasten auf Verteilnetzebene treten stärker in den Vordergrund, um die Systemsicherheit weiterhin zu gewährleisten. Neben bilanziellen Effekten (z. B. aufgrund von Prognosefehlern bei Einspeisungen aus erneuerbaren Energien) sind auch Herausforderungen im Bereich der Stromnetze selbst absehbar. Sie betreffen zum einen die Verteilnetzebene, in der bereits heute in einigen Netzen aufgrund hoher Einspeisung und bidirektionaler Lastflüsse ein zusätzlicher Netzausbau erforderlich ist, um die technischen Randbedingungen zu erfüllen. Zum anderen entstehen neue Anforderungen an die Übertragungsnetze, da der überregionale Transport durch die zunehmende räumliche Entfernung zwischen Erzeugungs- und Verbrauchszentren zu einer erhöhten Belastung der Übertragungsnetze führt. Gerade im Bereich der Höchst- und Hochspannungsübertragung ergeben sich weitere Herausforderungen durch die geringe gesellschaftliche Akzeptanz von Leitungsbauprojekten, die den konventionellen Netzausbau oder die Netzverstärkung nach dem NOVA-Prinzip (Netz-Optimierung vor -Verstärkung vor -Ausbau) [1] erschweren. Neben dem konventionellen Netzausbau bieten insbesondere Technologien, die ein weitergehendes Monitoring und die Steuerung der technischen Anlagen im Netz ermöglichen, weitere Potenziale, um weiterhin einen zuverlässigen Netzbetrieb zu gewährleisten.

**Asset Management und Diagnostik.** Im Rahmen des Wartungs- und Erneuerungsbedarfs von Betriebsmitteln sind Diagnoseverfahren notwendig, um Störungen vorhersagen und durch geeignete Maßnahmen verhindern zu können. Sie können auch zur Überwachung neuartiger Betriebsmittel eingesetzt werden, um weitere Erfahrungen im Hinblick auf das Langzeitbetriebsverhalten zu sammeln. Bei der zeitorientierten Instandhaltungsstrategie werden die Komponenten in festen Intervallen überprüft. Die zustandsorientierte Instandhaltungsstrategie ist potenziell eine effektivere und kostenoptimierte Instandhaltungsmethode. Sie hat den Vorteil, dass der Alterungszustand auch unsichtbarer Teilkomponenten durch den Einsatz von Sensortechnik ermittelt werden kann. Der Austausch von noch funktionstüchtigen Geräten kann so vermieden werden. Außerdem wird das Ausfallrisiko bei zufälligen Defekten minimiert. Fehler werden schnell erkannt und behoben, was zu einer Erhöhung der Versorgungssicherheit beiträgt. Die zustandsorientierte Instandhaltung wird in Hoch- und Höchstspannungsnetzen eingesetzt, in Mittelspannungsnetzen aus

wirtschaftlichen Gründen jedoch nicht. Bei der Zustandsbewertung von Ortsnetzstationen und anderen Betriebsmitteln im Mittel- und Niederspannungsbereich erfolgt die Zustandsbeurteilung auf der Grundlage manueller, rein visueller Inspektionen. Auch auf den niederen Spannungsebenen bietet der Einsatz geeigneter kostengünstiger Sensorik Möglichkeiten, eine effizientere und objektivere Diagnostik für die relevanten Betriebsmittel umzusetzen.

**Schutz- und Assistenzsysteme.** Die Schutztechnik bietet wesentliche Funktionen für die Sicherheit und Zuverlässigkeit sowie für die schnelle Abschaltung hoher Kurzschlussströme zur Schadensbegrenzung und Verhinderung der Schadensausweitung. Sicherheit bezieht sich auf die Vermeidung von Überfunktionen, während Zuverlässigkeit die Vermeidung von Unterfunktionen beschreibt. Aktueller Stand der Technik sind digitale Schutzgeräte, die ihre Schutzentscheidung auf der Grundlage verschiedener Schutzkriterien treffen. Gängige Schutzkriterien sind Überstrom, Impedanz und Stromdifferenz. Moderne digitale Schutzgeräte verfügen neben den eigentlichen Schutzfunktionen über zusätzliche Automatisierungs- und Überwachungsfunktionen, sind mit modularer, von der Schutzfunktion unabhängiger Hardware ausgestattet und werden mittels der Kommunikationsprotokolle IEC 60870-5-103/104 [26] oder IEC 61850 [28] mit der Netzleitstelle verbunden. Eine dezentrale Kommunikation („Peer-to-Peer“) zwischen Schutzgeräten für binäre Entscheidungsprozesse mit entfernten Messstellen oder Stationskomponenten (z. B. Schalterversagerschutz, Signalvergleichsverfahren), die im Rahmen von adaptiven Schutzkonzepten für bidirektionale Lastflüsse in den Parametersätzen berücksichtigt werden, wird bisher nicht eingesetzt.

Für Fernwirkaufgaben werden die heute bei Verteilnetzbetreibern üblichen zentralen Leitsysteme in erster Linie zur Unterstützung von Wartungs- und Instandhaltungstätigkeiten sowie zur Überwachung der wesentlichen Betriebsmittel auf Mittel- und Hochspannungsebene eingesetzt. Im Rahmen der Sektorenkopplung und der informationstechnischen Vernetzung des zunehmend dezentralen Energiesystems mit volatilen Erzeugern, neuartigen Verbrauchern und Speichern in den Verteilnetzen steigt der Bedarf an Beobachtbarkeit und Steuerbarkeit des Systems jedoch enorm. Dies hat zur Folge, dass eine stetig wachsende Menge an Prozessinformationen und Freiheitsgraden im Rahmen von Betriebsführungsentscheidungen berücksichtigt werden müssen. Teilweise werden hier bereits Assistenzsysteme eingesetzt, die Informationen über das Stromnetz für das Netzführungspersonal geeignet aufbereiten und visualisieren, spezifische Netzberechnungen durchführen und in kritischen Situationen Entscheidungsunterstützung bieten können. Insgesamt stehen diese Systeme aber noch am Anfang der Entwicklung und umfassen hauptsächlich eine automatisierte Datenaufbereitung.

**Netztransparenz in Verteilnetzen.** Beim Verteilnetzbetreiber (VNB) erfolgen die Netzüberwachung und die Netzsteuerung für die Hochspannung im Allgemeinen ähnlich wie in den Übertragungsnetzen. So ist das Hochspannungsnetz vollständig beobachtbar und es finden zyklische Zustandsabschätzungen und Netzsicherheitsberechnungen statt. Für das Mittelspannungsnetz sind in der Regel keine oder nur vereinzelte Messungen verfügbar und es wird eine sogenannte Verteilnetz-Zustandsabschätzung durchgeführt. Sie stellt eine Abschätzung des Netzzustands auf Basis weniger Messwerte, der Topologie und gegebenenfalls historischer Zeitreihen dar. Bei einigen wenigen Netzbetreibern ist das Mittelspannungsnetz auch messtechnisch vollständig an das Netzleitsystem angeschlossen. Die Freischaltung ist auch für die VNB mit erheblichem Aufwand verbunden. Auch bei Arbeiten im Netz wird der Netzzustand in der Leitstelle verfolgt, analog zur Vorgehensweise in höheren Spannungsebenen. Der reguläre Netzbetrieb an der Schnittstelle zwischen Übertragungsnetzbetreiber (ÜNB) und VNB besteht in erster Linie in dem Austausch von Daten. So werden beispielsweise telefonisch Informationen zwischen den Leitstellen ausgetauscht, wenn im eigenen Netzgebiet Maßnahmen ergriffen werden, die relevante Auswirkungen auf das vor- oder nachgelagerte Netz

haben können. Heute erhält der ÜNB von den Marktteilnehmern insbesondere die Kraftwerksfahrpläne der in der Hochspannung angeschlossenen Kraftwerke. Eine marktbasierte Nutzung der Flexibilität von Erzeugungsanlagen und Verbrauchern durch den VNB findet in der Regel nicht statt. Zukünftig wird im Sinne eines Multi-use-Ansatzes sowohl der netz- als auch der marktdienliche Einsatz von Flexibilitäten erfolgen. Der Einfluss des ÜNB auf die Erzeugungsanlagen konzentriert sich derzeit hauptsächlich auf Eingriffe im Rahmen des Netzsicherheitsmanagements. Eine Interaktion zwischen ÜNB und VNB findet auch im Zusammenhang mit dem Bilanzkreismanagement statt. Hier übernimmt der ÜNB die Rolle des Bilanzkreiskoordinators. Dafür werden dem VNB Stamm- und Bewegungsdaten für Bilanzkreissummenzeitreihen übermittelt. Der Informationsaustausch zwischen Netzbetreibern und Marktteilnehmern erfolgt in vielen Systemdienstleistungsprozessen noch immer hauptsächlich nicht automatisiert.

Ein intelligentes Energienetz ist nach dem üblichen Modell der Kommunikationstechnik in verschiedene Domänen unterteilt. Innerhalb dieses Konzepts ermöglicht das Kundennetz die Kommunikation zwischen Hausgeräten und den entsprechenden intelligenten Messsystemen bzw. dem SMGW. Das SMGW bildet dabei die zentrale Schnittstelle zwischen den angebundenen Endkundinnen und -kunden und allen weiteren beteiligten Akteuren (vgl. Abschnitt 4.2). Eine moderne Weitbereichsnetzinfrastruktur soll die Möglichkeit der Echtzeitüberwachung bzw. -steuerung des Energienetzes schaffen. Der Informationsaustausch innerhalb der Netzbereiche kann durch den Einsatz verschiedener drahtgebundener und/oder drahtloser Kommunikationstechnologien realisiert werden.

**Kommunikationsnetze im Energiesektor.** Aufgrund der unterschiedlichen Kommunikationstechnologien für verschiedene Anwendungen werden Sensoren oft nur über dedizierten Funk angebunden, da eine Anbindung über Glasfaser, DSL oder das Mobilfunknetz (LTE/4G) aufgrund mangelnder Netzabdeckung oder aus Kostengründen nicht immer möglich ist. Eine kostengünstige Anbindung kann über ein Funksystem in den ISM-Bändern (Industrial, Scientific and Medical) realisiert werden. Wurden bisher die kostenlos freigegebenen Frequenzen bei 433 MHz, 868 MHz und 2,4 GHz genutzt, die eine Anbindung verschiedener Anwendungen über Funk ermöglichen, so werden durch die für den Energiesektor bestimmte Funkfrequenz 450 MHz neue Kapazitäten eröffnet. Dabei kann die Reichweite dieser Funkverbindungen in komplexeren Szenarien und je nach örtlichen Gegebenheiten unter Umständen beeinträchtigt werden. Dies hat jedoch zur Folge, dass ein unverhältnismäßig hoher Aufwand bezüglich des Aufbaus und Betriebs der Infrastruktur entsteht, da für eine lückenlose Versorgung Zugangspunkte (Zubringernetze) in hoher Dichte errichtet werden müssen. Der Aufbau eines flächendeckenden Funknetzes mit dedizierten Nutzungskapazitäten für das Stromnetz befindet sich in Deutschland noch in den Anfängen, obwohl mit der lizenzierten 450-MHz-Funkfrequenz die ersten Bausteine gelegt sind.

Das Thema Systemsicherheit von Versorgungsnetzen mit hoher Durchdringung und Abhängigkeit von IKT wird in Deutschland bereits seit mehreren Jahren von der Bundesnetzagentur (BNetzA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) begleitet. Hinzu kommen Aktivitäten verschiedener nationaler und internationaler Verbände aus der Elektrizitätswirtschaft, wie zum Beispiel des European Network of Transmission System Operators for Electricity (ENTSO-E), des Bundesverbands der Energie- und Wasserwirtschaft e.V. (BDEW) und des Forums Netztechnik/Netzbetrieb im VDE (VDE FNN). Neben den gängigen Sicherheitsstandards wie der ISO-27000er-Reihe [40], dem IT-Grundschutz des BSI [48] und den Standards des National Institute of Standards and Technology (NIST) [74] gibt es daher einige detaillierte Sicherheitsstandards für den Energiesektor, die zum Teil verbindlich sind.

In diesem Zusammenhang befassen sich viele dieser Normenreihen mit der Einrichtung von IT-Netzen in kritischen Infrastrukturen wie denen von Netzbetreibern. Hierbei lassen sich die IT-Netze der Betreiber grob

in zwei Bereiche unterteilen: das Büronetz und das Prozessnetz. Die Büronetze sind mit anderen Unternehmensnetzen vergleichbar. Sie dienen hauptsächlich der Standard-Bürokommunikation mit dem Einsatz von Standardanwendungen, dem E-Mail-Verkehr und der Datenverarbeitung. Der einzige markante Unterschied zwischen dem Büronetz und anderen Unternehmensnetzen besteht darin, dass über das Büronetz gelegentlich auf prozessrelevante Daten, wie zum Beispiel Wettervorhersagen, zugegriffen wird. Es bestehen daher Verbindungen zum Prozessnetz, die jedoch keinen Vermittlungsbetrieb zulassen. Zu den Prozessnetzen der Betreiber gehören alle IT-Komponenten, die am Prozessbetrieb beteiligt sind. Dazu zählen beispielsweise Computer in der Leitstelle, speicherprogrammierbare Steuerungen, Switches und Router sowie die physikalischen Kommunikationsstrecken, die die einzelnen Komponenten verbinden. Gelingt es einem Cyberangreifer, sich schreibenden Zugriff auf das Prozessnetz zu verschaffen, besteht eine akute Gefahr für die Netzstabilität. Auch ein Lesezugriff oder eine Manipulation der in das Prozessnetz eingebrachten Daten können den Netzbetrieb stören oder sensible Informationen preisgeben.

Die Betreiber sind in der besonderen Situation, dass sie für die Prozessnetze trotz der großen geografischen Ausdehnung fast ausschließlich dedizierte Leitungen (meist Glasfaser) einsetzen können und somit die Netze räumlich getrennt von öffentlichen Netzen betrieben werden. Dies bietet ein deutlich höheres Maß an Sicherheit, führt aber auch zur Verwendung unsicherer bzw. unverschlüsselter Protokolle. Darüber hinaus erschweren die vorhandenen Bestandsbetriebsmittel mit Einsatzzeiten von 20 bis 30 Jahren die Einführung von Sicherheitsmechanismen wie Verschlüsselung und Authentifizierung, die die Kommunikation aktiv beeinflussen. Dies führt dazu, dass wesentliche Sicherheitsmechanismen entsprechend dem aktuellen Stand der Technik in den Prozessnetzen nicht zum Einsatz kommen.

**Marktkommunikation und regulatorische Rahmenbedingungen.** Marktanbindungsmaßnahmen unterliegen verschiedenen regulatorischen Anforderungen wie beispielsweise der Verordnung (EU) 2017/1485 der Kommission zur Festlegung einer Systembetriebsrichtlinie [64], dem kontinentaleuropäischen Betriebshandbuch ENTSO-E, dem Transmission and Distribution Code, dem Energiewirtschaftsgesetz (EnWG) und dem Erneuerbare-Energien-Gesetz (EEG) [42]. Sie bilden somit eine Schnittstelle zwischen dem Strommarkt und dem Netzbetrieb. Ausgangspunkt für den Kommunikationsprozess in der Energiewirtschaft sind die geltenden gesetzlichen Vorgaben. Für die Marktkommunikation sind das EnWG [44], das Messstellenbetriebsgesetz (MsbG) [43], das Netzausbaubeschleunigungsgesetz (NABEG 2.0) [45] und die Stromnetzzugangsverordnung (StromNZV) [46] von zentraler Bedeutung.

Auf der Grundlage des oben skizzierten Rechtsrahmens hat die BNetzA in ihren Beschlüssen standardisierte Marktprozesse und Datenaustauschformate festgelegt, die für alle Marktteilnehmer verbindlich sind. An der Entwicklung der Prozesse sind Akteure und Verbände der Energiewirtschaft beteiligt, die zum Beispiel Änderungsvorschläge oder gemeinsame Lösungsideen entwickeln. Die Einbeziehung verschiedener Marktteilnehmer und Akteure aus der Energiewirtschaft in die neuen Lösungsansätze befindet sich allerdings noch im Anfangsstadium. In Ermangelung einer nachträglich absehbaren Umstellung auf eine dezentrale Messwertverteilung hat die BNetzA vorgesehen, dass abweichend von den Vorgaben der BSI TR-03116-4 [14] der Zeitraum für die zulässige Verwendung von zertifizierten privaten Signaturschlüsseln oder Kombizertifikaten sowohl für die Signaturerzeugung als auch für die Entschlüsselung der an diese E-Mail-Adresse gesendeten Daten gemäß BK6-18-032 verlängert wird [21]. Es ist jedoch die Absicht der BNetzA (ab 1. Oktober 2023), dass zukünftig die Nutzung von Applicability Statement 4 (AS4) als Webdienst auf Basis von Transport Layer Security (TLS) und die Nutzung einer Smart-Metering-Public-Key-Infrastruktur [11, 12, 16] des BSI als Technologiestandards für ein höchstmögliches Maß an Interoperabilität mit der europäischen elektronischen Marktkommunikation erfolgen werden [20].

Die nationale Strategie zur Digitalisierung der energiewirtschaftlichen Prozesse ist aktuell durch die Anpassung und Erweiterung der bestehenden Regulatorik geprägt, was potenziell eine Begrenzung bzw. Verzögerung der technischen Umsetzungsmöglichkeiten mit sich bringt. Derzeit herrscht bei den betroffenen Branchen noch Unsicherheit über das Gesetz zur Digitalisierung der Energiewende. Demnach soll das SMGW die zentrale und einzige Kommunikationsschnittstelle für die Anbindung von relevanten Erzeugern und Verbrauchern werden. Die betroffenen Akteure sind mit der Umsetzung eigener Lösungen beispielsweise bezogen auf Mehrwertdienste teilweise deutlich weiter fortgeschritten. Zu hinterfragen ist bei proprietären Lösungen jedoch, inwieweit Interoperabilität, Sicherheit und Datenschutz gewährleistet werden können.

> Die Dezentralisierung der Einspeisung führt zu einem zunehmenden Bedarf an Netzausbau bzw. Netzausbauverstärkung. Darüber hinaus entstehen höhere Belastungen von Betriebsmitteln in den unteren Spannungsebenen, für die jedoch aufgrund fehlender Sensorik und damit nicht ausreichender Transparenz hinsichtlich ihres Zustands keine fortschrittlichen Monitoring- und Diagnosetechniken einsetzbar sind. Bezogen auf die Anbindung von dezentralen Erzeugungsanlagen sowie Endkundinnen und -kunden an das Verteilnetz besteht ebenfalls ein Bedarf an höherer Netztransparenz. Hier entstehen aktuell Verzögerungen in der Umsetzung aufgrund des zeitweise gestoppten Ausbaus (vgl. Abschnitt 3.3) der SMGW-Infrastruktur und der zögerlichen Verwendung dieser Infrastruktur zur Ausbringung von Mehrwertdiensten in Deutschland. Mit einem flächendeckenden Funknetz mit dedizierten Nutzungskapazitäten für das Stromnetz, wie zum Beispiel der 450-MHz-Funkfrequenz, kann jedoch potenziell eine zuverlässige Infrastruktur aufgebaut werden. Allerdings erschweren Bestandsbetriebsmittel mit einer Lebensdauer von 20 bis 30 Jahren die Umsetzung etablierter und neuer Sicherheitskonzepte, die für die nachhaltige Einführung neuer Cyberinnovationen im Energiesektor unerlässlich sind.

## 4.2 Fallstudie: Messstellenbetrieb und SMGW-Infrastruktur in Deutschland

Das intelligente Messsystem (iMSys) als zentrale Komponente der SMGW-Infrastruktur in Deutschland wurde bereits in Abschnitt 2.3.1 eingeführt. Neben dem SMGW selbst sind im Rahmen der gültigen Regulatorik Anforderungen an die gesamte erforderliche Infrastruktur und an die Aufgaben der beteiligten Akteure definiert. Dabei bestehen sowohl Vorgaben an die Ausbringung und den Einsatz der Infrastruktur (Abschnitt 4.2.1) als auch sicherheitsspezifische Anforderungen an das SMGW selbst (Abschnitt 4.2.2).

### 4.2.1 SMGW-Infrastruktur und Rollout

Der Ausbau der SMGW-Infrastruktur in Deutschland befindet sich aktuell noch in der Ausbringungsphase, die zeitweise durch verschiedene Regulierungsprozesse verzögert wird.

**Smart-Meter-Rollout.** Der Smart-Meter-Rollout in Deutschland erfolgt schrittweise für einen Großteil der Endkundinnen und -kunden bis zum Jahr 2027. Er wird vom jeweils zuständigen Messstellenbetreiber umgesetzt, wobei der Rollout bis Ende 2024 für alle Erzeugungsanlagen mit einer Nennleistung oberhalb von 7 kW erfolgen soll. Bei den Verbraucherinnen und Verbrauchern ist dies abhängig vom Jahresenergieverbrauch und erfolgt bis 2024 entsprechend bei einem Jahresenergieverbrauch oberhalb von 10.000 kWh und zwischen 6.000 und 10.000 kWh bis Ende 2027. Insgesamt beträgt die Rollout-Rate für moderne Messeinrichtungen nach den aktuellsten verfügbaren Zahlen etwa 10,9 Prozent bezogen auf alle vorhandenen Netzanschlüsse bei einer steigenden Tendenz hinsichtlich der Anzahl der eingebauten Systeme pro Jahr (Stand: Ende 2019) [54].

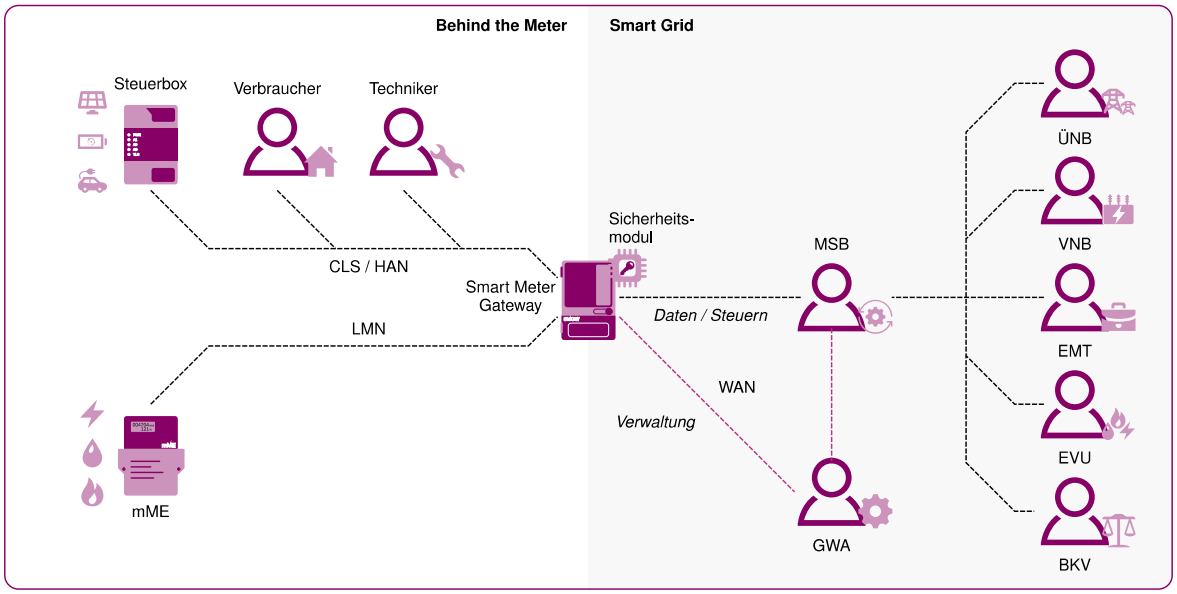


**Abbildung 4.1:** Die SMGW-Infrastruktur und an der Kommunikation beteiligte Akteure auf Basis des Marktkommunikations-Modells 2020 [18].

**Marktkommunikation und beteiligte Akteure.** Mit dem Marktkommunikations-Modell und den Vorgaben an die SMGW-Infrastruktur selbst ist eine Gesamtinfrastruktur bestehend aus verschiedenen isolierten Kommunikationsnetzbereichen und beteiligten Akteuren vorhanden. Die relevanten Akteure und Netzsegmente sind schematisch in Abbildung 4.1 dargestellt. Dabei wird das SMGW zur sicheren Ankopplung der Endverbraucherinnen und -verbraucher an externe Akteure eingesetzt, wodurch für sie potenziell die Bereitstellung zusätzlicher Daten und Steuerungsoptionen ermöglicht wird.

Der Messstellenbetreiber (MSB) ist zuständig für den Einbau, den Betrieb, die Wartung und das Ablesen der Zähler. Der MSB kann durch die Endkundinnen und -kunden wie der Energieversorger auch frei gewählt werden, sofern eine moderne Messeinrichtung betrieben wird. Grundzuständig für den Messstellenbetrieb ist – sofern nicht anders durch die Kundinnen und Kunden bestimmt – der örtliche Verteilnetzbetreiber.

Der Gateway-Administrator (GWA) verantwortet den technischen Betrieb des iMSys und demnach insbesondere die Installation, den Betrieb und die Wartung des SMGW sowie die Anbindung von Messsystemen und anderen technischen Einrichtungen an das SMGW. Die Tätigkeiten und Verpflichtungen sind in der Technischen Richtlinie TR-03109-6 [10] festgelegt. Zu den dem Betrieb des SMGW zugehörigen Prozessen zählen unter anderem die Unterstützung bei der Verarbeitung und das Zurverfügungstellen von Messdaten für weitere berechtigte Akteure. Die Aufgaben des GWA sind ebenfalls dem MSB zugeordnet. Der MSB kann sie jedoch auch als Aufgabe an einen zertifizierten Auftragnehmer abgeben. Für die Tätigkeit als GWA werden Unternehmen vom BSI unter Voraussetzung der Einhaltung entsprechender gesetzlicher Vorgaben zertifiziert. Unter anderem erfordert dies, ein Information Security Management System (ISMS) einzurichten, zu betreiben und zu dokumentieren sowie die sich ergebenden Anforderungen aus den relevanten technischen Richtlinien für den Gateway-Betrieb umzusetzen. Diese Zertifizierung besitzen aktuell insgesamt 42 Unternehmen (Stand: November 2021) [49].

Relevante Marktakteure, die eine Berechtigung zum Zugriff auf Messdaten haben können, sind der örtliche Netzbetreiber, zu Abrechnungszwecken das Energieversorgungsunternehmen (EVU) sowie weitere externe Marktteilnehmer (EMT) wie beispielsweise der Betreiber eines virtuellen Kraftwerks.

**Integration von Mehrwertdiensten.** Zum Angebot von Mehrwertdiensten sind neben der Bereitstellung von Messwerten vor allem zusätzliche Steuerungsmöglichkeiten für das Management von Erzeugung und Last notwendig. Im Rahmen der Spezifikation einer Steuerbox durch das VDE FNN soll eine solche Möglichkeit zur Steuerung der Einspeisung von Erzeugungsanlagen sowie des Verbrauchs auf Gebäude- und Geräteebene nach § 14a EnWG realisiert werden. Mit der Erweiterung der Spezifikation der Steuerbox um die „digitale Schnittstelle“ wurde ein weiterer Schritt hin zu einer standardisierten Kommunikation gemacht. Explizit wird im entsprechenden FNN-Hinweis auf die Umsetzung mittels EEBUS verwiesen [89]. Unter dem Namen „EEBUS“ wird eine Kommunikationsschnittstelle entwickelt, die eine herstellerunabhängige Kommunikation von Systemen hinter dem Netzanschluss, wie beispielsweise von PV-Anlagen, Speichersystemen, Heizung, Weißer Ware und Elektromobilität, ermöglicht.

Eine wesentliche Herausforderung, deren Bewältigung zur allgemeinen Akzeptanz des iMSys bzw. des SMGW als zentrale Plattform für die Umsetzung von Mehrwertdiensten beitragen würde, ist die Vereinfachung der Nutzung der Plattform durch externe Marktteilnehmer. Ein Ansatz, der in diesem Kontext mittels der Entwicklung eines Stufenmodells durch das BSI und das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) verfolgt wird, ist die Standardisierung von energiewirtschaftlichen Use Cases, die mithilfe der SMGW-Infrastruktur umgesetzt werden sollen [53]. Hier wird eine schrittweise Digitalisierung der Energiebranche angestrebt. Im Fokus steht hier insbesondere auch die Einholung von Feedback aus der Energiebranche, um eine praxisnahe Standardisierung der relevanten Use Cases zu gewährleisten. Generell wird im Rahmen des Stufenmodells hierbei zwischen energiewirtschaftlichen Use Cases und den zu ihrer Umsetzung notwendigen Systemanwendungsfällen und Funktionsbausteinen unterschieden. Exemplarische energiewirtschaftliche Use Cases sind:

1. Steuerung von Verbrauchseinrichtungen in der Niederspannung nach § 14a EnWG
2. Laden von Elektrofahrzeug-Batterien an öffentlich zugänglicher Ladeinfrastruktur
3. Teilnahme am Regelenergiemarkt
4. Bereitstellung von Daten für Mehrwertdienste

Zu den Systemanwendungsfällen und Funktionsbausteinen zählen:

1. Leistungsbegrenzung/Leistungsüberwachung mittels SMGW
2. Messwertverarbeitung zur Abrechnung des gemessenen Ladestroms am Ladepunkt für wechselnde Ladeeinrichtungsnutzer

Das Vorgehen, die Anwendungsfälle, die mithilfe der SMGW-Infrastruktur umgesetzt werden sollen, in Absprache mit Fachpersonal aus der Energiebranche praxisnah zu erarbeiten, könnte eine vielversprechende Möglichkeit darstellen, die Akzeptanz für die SMGW-Plattform in der Branche zu erhöhen und die Umsetzung von Mehrwertdiensten für Endkundinnen und -kunden zu beschleunigen. Solche Ansätze werden bereits durch Projekte wie DigENet gezielt gefördert. Hier gilt es, ein angemessenes Verhältnis zu finden, um die Nutzbarkeit und Akzeptanz der „Plattform SMGW“ zu erhöhen und das Risiko, dass Mehrwertdienste durch die Industrie mit proprietären Lösungen an der bereitgestellten Infrastruktur vorbei entwickelt werden zu minimieren.

### 4.2.2 Sicherheitskonformer Einsatz von SMGW-Infrastruktur

Das SMGW selbst soll als sicheres Gateway für die kommunikationstechnische Anbindung von Endkundinnen

und -kunden an andere beteiligte Akteure dienen. Dementsprechend bestehen sicherheitsrelevante Anforderungen an das System zum Beispiel bezogen auf die Bereitstellung von Netzwerkschnittstellen und die Integration eines Sicherheitsmoduls, das unter anderem zur Verschlüsselung der übertragenen Daten eingesetzt wird.

**Netzwerkarchitektur.** Wie in Abbildung 4.1 dargestellt, bietet das SMGW physisch dedizierte Schnittstellen für die relevanten Netzwerke und dient dementsprechend als Gateway zwischen ihnen. Im Local Metrological Network (LMN) werden die Messsysteme eingebunden. Das Home Area Network (HAN) dient der Kopplung von allen relevanten Systemen der Endkundinnen und -kunden. Dazu können dezentrale Erzeugungsanlagen bzw. Steuerboxen oder Energiemanagementsysteme zählen. Die Systeme im HAN werden zu einem Controllable Local System (CLS) zusammengefasst. Das Wide Area Network (WAN) dient hierbei der Kommunikation mit dem GWA und allen externen Marktteilnehmern. Über das SMGW bauen die Marktteilnehmer eine gesicherte, verschlüsselte Verbindung zu den Systemen der Endkundinnen und -kunden über den sogenannten CLS-Kanal auf.

Für das WAN können grundsätzlich verschiedene Übertragungsmedien zum Einsatz kommen. Dazu zählen dedizierte 450-MHz-Infrastruktur, öffentlicher Mobilfunk (LTE) oder der Einsatz von Power Line Communication (vgl. Abschnitt 2.2).

**Verschlüsselung und Zertifizierung.** Die Zertifikate für SMGWs selbst werden vom BSI ausgestellt. Aktuell sind insgesamt vier Produkte unterschiedlicher Hersteller zertifiziert, deren Zertifikate erstmals zwischen Dezember 2018 und Dezember 2019 ausgestellt wurden. Fünf weitere Hersteller befinden sich mit ihren Produkten aktuell noch im Zertifizierungsprozess (Stand: November 2021) [50].

Zur Verschlüsselung der Kommunikation mit dem SMGW wird TLS 1.2/1.3 eingesetzt. Hierdurch wird eine sichere Kommunikation mit externen Marktteilnehmern unabhängig von der eingesetzten Infrastruktur ermöglicht. Asymmetrische Kryptografieverfahren, wie sie bei TLS eingesetzt werden, sind potenziell an zwei Stellen verwundbar. Beim Verbindungsaufbau tauschen Server und Client (in diesem Fall beispielsweise externer Marktteilnehmer und das SMGW) kryptografische Nachrichten unter Verwendung asymmetrischer Schlüsselaustauschalgorithmen (z. B. RSA/ECDH) aus, um einen symmetrischen Schlüssel abzuleiten. Dieser dient dann der Verschlüsselung der verbleibenden Sitzung. Zudem erfolgt bei der Authentifizierung der Identitätsnachweis durch die Bereitstellung des öffentlichen Schlüssels, wobei ebenfalls entsprechende Austauschalgorithmen (RSA/ECDSA) zum Einsatz kommen. Potenziell können diese asymmetrischen Algorithmen zukünftig durch quantensichere Algorithmen ersetzt bzw. in einem hybriden Austauschverfahren eingesetzt werden.

**Sicherheitsmodul.** Zur Verschlüsselung und zur Speicherung der hierfür relevanten Schlüssel besitzt das SMGW ein dediziertes Sicherheitsmodul, dessen Anforderungen in der Technischen Richtlinie TR-03109-2 [9] festgelegt sind. Das Sicherheitsmodul stellt dem SMGW kryptografische Funktionalitäten wie die Generierung von Schlüsselmaterial, den Schlüsselaustausch, digitale Signaturen und allgemeine Verschlüsselungs- und Entschlüsselungsoperationen bereit. Zudem stellt das Sicherheitsmodul kryptografische Zufallszahlen bereit und hält Schlüsselmaterial, das Root-Zertifikat der Smart-Metering-Public-Key-Infrastruktur (SM-PKI) sowie Gütesiegel-Zertifikate vor. Sonstige (öffentliche) Zertifikate werden jedoch im Gateway (GW) gespeichert. Für die Länge der zu verwendenden Schlüssel werden die Vorgaben aus TR-03109-3 [8] herangezogen.

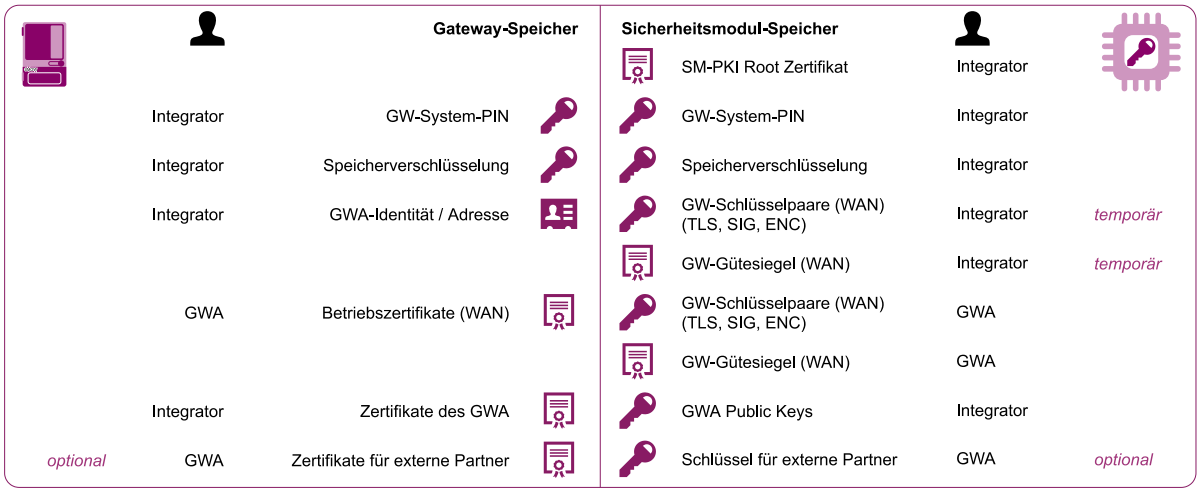


**Abbildung 4.2:** Das Schlüssel- und Zertifikatsmaterial für den sicheren Betrieb des SMGW wird im Laufe des Lebenszyklus durch den Integrator sowie den GWA installiert, erneuert und ergänzt (basiert auf [9]).

Die Sicherheit des SMGW basiert auf der Einhaltung eines sechsstufigen Lebenszyklus, der von Produktionsprozessen über Integration, Installation und Personalisierung bis zum Betrieb führt und zusätzlich eine Außerbetriebnahme vorsieht [9]. Im Sicherheitsmodul selbst wird der aktuelle Abschnitt in diesem Zyklus ebenfalls mitgehalten, wobei jedoch nur zwischen „nicht initialisiert“, „initialisiert“ und „terminiert“ unterschieden wird. Während des Lebenszyklus des SMGW wird initiales und dauerhaftes Schlüssel- und Zertifikatsmaterial im GW sowie im Sicherheitsmodul installiert. Eine Übersicht über diese Schlüssel und Zertifikate bietet Abbildung 4.2.

Die Personalisierungs- und Integrationsmaßnahmen für das Sicherheitsmodul und das GW werden durch den Integrator ausgeführt. Er führt den Import des aktuellen Root-Zertifikats der SM-PKI aus und generiert anschließend vorläufige Schlüsselpaare für TLS-Kommunikation, Signaturen und Schlüssel sowie Zertifikate für die WAN-Kommunikation des GW. In diesem Kontext werden die auch öffentlichen Schlüssel exportiert und entsprechende Gütesiegel-Zertifikate in der SM-PKI gespeichert, um die Authentifizierung beim Schlüsselaustausch sicherstellen zu können. Weiterhin wird eine PIN für die Verbindung des Sicherheitsmoduls mit dem GW gesetzt und es werden Schlüssel für die Speicherverschlüsselung generiert. Für die weiterführende Konfiguration muss die Identität des zukünftigen GWA bekannt sein. Dieser übermittelt eine signierte Konfigurationsdatei für das Sicherheitsmodul an den Integrator, die die öffentlichen Zertifikatsketten des GWA für Authentifizierung und Verschlüsselung enthält, die vom Integrator in den Zertifikatsspeicher des GW geladen werden, woraufhin die Zertifikate vom GW gegen die SM-PKI verifiziert werden.

Nach Abschluss dieser Maßnahmen kann das SMGW durch den Erstkonfigurator an seinem Bestimmungsort installiert werden, um anschließend durch den GWA für den Normalbetrieb personalisiert zu werden. Hierfür nutzt der GWA die zuvor installierten vorläufigen WAN-Kommunikationsschlüssel und das Schlüsselmaterial des GWA. Um den sicheren Betrieb zu ermöglichen, ersetzt der GWA nach der erfolgreichen Authentifizierung das durch den Integrator installierte vorläufige Schlüsselmaterial durch neu generierte Schlüssel und Zertifikate. Anschließend ist das SMGW für den Normalbetrieb vorbereitet. Um auch andere Entitäten, wie beispielsweise Servicetechnikern, die Interaktion mit dem SMGW zu ermöglichen, muss der GWA entsprechende Profile mit Schlüsselmaterial zur Authentifizierung und Verschlüsselung einrichten. Hierzu ist je nach Anbindung auch Schlüssel- und Zertifikatsmaterial für die Kommunikation über von WAN abweichende Kanäle zu erstellen. Anschließend kann TLS-gesichert über die entsprechende Schnittstelle mit dem SMGW interagiert werden.

Mit dem SMGW und der dazugehörigen Infrastruktur besteht grundlegend eine sichere Umgebung für Anwendungsinnovationen und die Umsetzung von Mehrwertdiensten. Das integrierte Sicherheitsmodul, mit dem kryptografische Operationen wie die Verschlüsselung, die Signaturerstellung und -verifizierung sowie der Schlüsselaustausch umgesetzt werden, dient hierbei als zentrale Sicherheitsinstanz. Konkrete technische Anforderungen, wie Schlüssellängen und Algorithmen, werden jährlich aktualisiert, um langfristige Sicherheit zu gewährleisten. Die Zertifizierung entsprechend den Mindestanforderungen sowohl für die beteiligten Akteure (GWA) als auch für die SMGWs selbst erfolgt durch das BSI. Das aktuelle Vorgehen, Feedback von Fachpersonal aus dem Energiesektor bei der Standardisierung von Anwendungsfällen auf Basis der SMGW-Infrastruktur umzusetzen, ist positiv zu bewerten und sollte intensiviert werden, um ein angemessenes Gleichgewicht zwischen Datenschutz und Sicherheit sowie der Umsetzbarkeit von Anwendungsfällen zu erreichen.

## 4.3 Transition zu einer cybersicheren Umgebung für den Energiesektor

Im vorangegangenen Abschnitt wurden die SMGW-Infrastruktur sowie die mit ihrer Spezifikation und Nutzung einhergehenden Herausforderungen vorgestellt. Die SMGW-Infrastruktur stellt insofern eine Besonderheit dar, als dass nahezu alle relevanten Akteure der Energiebranche mit ihr verknüpft sind (Netzbetreiber, Versorger, Endkundinnen und -kunden, Anbieter von Mehrwertdiensten etc.). Bei der Spezifikation standen hier zunächst vor allem die Themen Informationssicherheit und Datenschutz im Vordergrund. Dies ist auch darauf zurückzuführen, dass die Infrastruktur der Übermittlung sowohl von kundenspezifischen als auch von netzrelevanten Daten dient. Insbesondere für den Übergangszeitraum bis zum vollständigen Rollout und zu einer uneingeschränkten Nutzbarkeit der Infrastruktur kommen jedoch für die Industrie auch alternative Lösungen zur kurzfristigen Umsetzung einiger Anwendungsfälle in Betracht. Für diese alternativen Lösungen lassen sich jedoch aus den Spezifikationen der SMGW-Infrastruktur grundlegende Anforderungen an die zulässigen bzw. notwendigen Kommunikationsmuster und die IT-Sicherheit ableiten.

Ein Beispiel hierfür ist die Ausgestaltung der kommunikationstechnischen Anbindung von Ladeinfrastruktur. Hier sind funktional insbesondere zwei Anforderungen zu nennen: die (netzdienliche) Leistungssteuerung sowie die Abrechnung des Ladevorgangs, wobei zwischen privater und öffentlicher Ladeinfrastruktur zu unterscheiden ist. Dabei können netzdienliche Lastverschiebungspotenziale von Elektrofahrzeugen durch intelligente Ladeinfrastrukturen erreicht werden. Hohe Lastverschiebungspotenziale von Elektrofahrzeugen können als Flexibilitätsoption zur Glättung der Nachfragekurve oder zur Anpassung an die Einspeisung von erneuerbarem Strom genutzt werden. Die drei bisher getrennten Bereiche Strom, individuelle Mobilität und IKT werden somit in zukünftigen E-Mobilitätssystemen zusammenwachsen. Neben den netzdienlichen Aspekten erfordern innovative Geschäftsaspekte wie Machine-to-Machine-Payments und Transaktionsabwicklung auf einem verteilten Informationssystem Rechenleistung und Konnektivität in den Fahrzeugen und in der Ladeinfrastruktur.

Mit mehr als 150.000 öffentlich zugänglichen Ladepunkten in Europa und einer zukünftig stärkeren Integration in die Energieversorgungssysteme ist die Ladeinfrastruktur besonders schützenswert und muss gegen mögliche Cyberbedrohungen abgesichert werden. In der Elektromobilität müssen Sicherheitskonzepte für mehrere Anwendungsfälle (z. B. Lademanagement, Abrechnung, Ladepunktreservierung) integriert werden, die wesentliche Prozesse und Schnittstellen zwischen den Marktteilnehmern absichern, wie beispielsweise für das eichrechtskonforme Laden (eichrechtsrelevante Ziffernfolgen auf Messgeräten aufgedruckt und pro Ladepunkt zugeordnet) und für die Authentifizierung (automatische Authentifizierung auf Basis des im Fahrzeug hinterlegten Ladevertrags im Rahmen von Plug & Charge).

In diesem Zusammenhang ist es von grundlegender Bedeutung, die betrieblichen und organisatorischen Plattformen für den elektronischen Austausch unter Berücksichtigung grundlegender Sicherheitselemente wie Vertraulichkeit, Integrität und Authentifizierung gemäß der zum Beispiel nach ISO 15118 geforderten PKI abzusichern. Darüber hinaus stellen der Datenschutz personenbezogener Daten, das Eigentum an den Daten und die faktische Zugriffskontrolle durch den Fahrzeughersteller in der E-Mobilität eine Herausforderung dar, da es noch keine einheitlichen Regelungen zur verpflichtenden Datenfreigabe gibt. Im Bereich der E-Mobilität beziehen sich diese Unklarheiten vor allem auf die Anwendungsfälle des Lademanagements und die entsprechend notwendigen Informationen über Batterietestkapazitäten, Ladegeschwindigkeiten, zu erwartende Abfahrtszeiten und auch zu erwartende Ladekurven des Fahrzeugs.

Standardisierte digitale Schnittstellen zur Verbesserung der Datenqualität im Rahmen der Meldeprozesse ermöglichen einen einfachen Zugang zum Ökosystem Elektromobilität. Standardisierung kann in diesem Zusammenhang auch die Komplexität reduzieren, sorgt für eine einheitliche Kommunikation zwischen den Marktteilnehmern und schafft damit Investitionssicherheit für neue Technologien. Für eine nachhaltige Digitalisierung muss die Daten- und Cybersicherheit von den beteiligten Marktteilnehmern im Rahmen von Mindeststandards, ähnlich wie es bei der SMGW-Infrastruktur der Fall ist, nachvollziehbar gewährleistet werden. Das Fehlen einheitlicher Standards für das Ökosystem Elektromobilität macht es notwendig, bestehende Konzepte und internationale Standards für moderne Sicherheitsarchitekturen und kryptografische Verfahren zu überprüfen und gegebenenfalls auf die spezifischen Anforderungen der Elektromobilität zu übertragen.

Das Eigentum und der Schutz von Daten sowie die Absicherung von Systemen und Prozessen vor Manipulation und Exfiltration von Daten sind somit auch im Bereich der E-Mobilität wichtige Themen, die für den nachhaltigen Betrieb von Systemen berücksichtigt werden müssen. Neben der E-Mobilität ist die nachhaltige Realisierung neuer Anwendungsfälle im Energiesektor durch den Datenschutz seitens der Regulatorik, die Interoperabilität seitens der Normung und die Cybersicherheit seitens der bestehenden Richtlinien geprägt. Ein besonderer Bestandteil der nachhaltigen Umsetzung der Use Cases ist die Cybersicherheit, wobei bestehende, aber auch neue Cybersicherheitslösungen bei der Integration von Sicherheitskonzepten eingesetzt werden. Neben präventiven „Security by Design“-Konzepten, die architektonisch Teil der Systeme sind (z. B. Verschlüsselung, Netzsegmentierung, Zugangskontrolle, Authentifizierung, Integritätsschutz), leisten auch reaktive Sicherheitsmaßnahmen einen ergänzenden Beitrag zur Sicherheit. In diesem Zusammenhang sind systemische Lösungen zur Erkennung und Überwachung kommunikativer Vorgänge, wie IDS- (Intrusion Detection System) oder SIEM-Systeme (Security Information and Event Management), in der Regel bewährte Methoden, um die Sicherheitslage passiv durch ein erhöhtes Situationsbewusstsein über die Kommunikationsereignisse im System zu verbessern. In der Regel werden solche Lösungen jedoch im Anschluss an präventive Sicherheitskonzepte eingesetzt, wobei im Falle des Versagens präventiver Maßnahmen reaktive Maßnahmen im Sinne von Incident-Response-Strategien eingesetzt werden.

Angesichts von Sicherheitskonzepten, die sich in ihren Zielen und Funktionsweisen zu widersprechen scheinen, wie zum Beispiel die Verschlüsselung von Kommunikationskanälen zum Schutz der Vertraulichkeit von Daten und IDS, die aktiv oder passiv Daten zur Angriffserkennung abfangen, scheint die Integration aller Sicherheitstechnologien widersprüchlich zu sein. Mögliche technische Lösungen für diesen Konflikt könnten Middlebox-Lösungen ähnlich dem SMGW-Ansatz sein, bei denen beispielsweise das Headend für Verschlüsselung und Authentifizierung in das IDS integriert und als sicherer Proxy im bestehenden Kommunikationskanal genutzt werden kann. In diesem Fall wäre der Einsatz der Lösungen jedoch auf eine aktive Einbindung in die Kommunikationsnetze und -prozesse festgelegt, während passive IDS-Lösungen den Vorteil hätten,

den Betrieb nicht durch aktive Teilnahme an den Kommunikationsprozessen zu beeinflussen. Andere Ansätze gehen in Richtung föderierte bzw. verteilte Überwachung, bei der lokale IDS direkt bei den Datenproduzenten mithören und einer zentralen Sicherheitsinstanz (z. B. SOC oder SIEM) Alarme oder Meldungen senden. Eine weitere Option wäre die Verwendung Host-basierter IDS, die als lokale Sicherheitssensoren für datenschutzkonforme und verschlüsselungsfähige Lösungen fungieren. Allerdings muss auch hier auf die Abwärtskompatibilität im Hinblick auf die Performance-Ressourcen der Geräte geachtet werden, da zusätzlicher Overhead für die Rechenkapazität der Geräte gefordert werden kann, was wiederum aktive (negative) Interferenzen im Betrieb zur Folge haben könnte. Auch für andere Sicherheitslösungen wie Verschlüsselung können solche Legacy-Beschränkungen ein wesentliches Kriterium für ihre Integration in das System sein. Hier kann passives IDS im Zusammenhang mit fehlender Verschlüsselung aufgrund fehlender Abwärtskompatibilität oder der Verwendung von Middleware-Lösungen eine Übergangslösung darstellen. Eine Harmonisierung dieser Sicherheitstechnologien kann durch gezielte Konzepte erreicht werden, in denen der Einsatz der Technologien komplementär zueinander wirken kann und einen zusätzlichen Mehrwert für die Sicherheit bietet.

> Für verschiedene Anwendungsfälle, wie beispielsweise die kommunikationstechnische Anbindung von Ladeinfrastruktur, werden schnell umsetzbare Konzepte benötigt, um übergangsweise eine Lösung bis zur vollständigen Verwendung der SMGW-Infrastruktur realisieren zu können. Gleichzeitig muss hier jedoch ebenso ein Mindestmaß an Datenschutz und IT-Sicherheit gewährleistet sein, da einerseits kundenspezifische Daten übermittelt werden und andererseits netzrelevante Steuerungsmöglichkeiten, zum Beispiel durch die Leistungssteuerung des Ladevorgangs, entstehen. Entsprechende Anforderungen lassen sich gegebenenfalls vom SMGW auf diese Übergangslösungen übertragen. Ebenfalls erfolgt die Transition der Prozessnetze von Netzbetreibern voraussichtlich in einem mehrschrittigen Prozess. Legacy-Devices weisen teilweise keine ausreichende Performance auf, um State-of-the-Art-Sicherheitsmechanismen wie Verschlüsselung ohne einen Ausbau der vorhandenen Infrastruktur umsetzen zu können. Der Einsatz von IDS bietet diesbezüglich eine schnell umsetzbare und nicht invasive Option, die Kommunikation im Prozessnetz zu überwachen und Anomalien zu erkennen.

Die SMGW-Infrastruktur wird zukünftig die zentrale Kommunikationsinfrastruktur zur Anbindung von Endkundinnen und -kunden an andere Marktakteure darstellen. Insbesondere für die Umsetzung von Mehrwertdiensten ist hier mit dem SMGW als zentralem Gateway und dem integrierten Sicherheitsmodul ein Mindestmaß an IT-Sicherheit und Datenschutz garantiert. Um ein Höchstmaß an Mehrwertdiensten mit dem SMGW umsetzen zu können werden jedoch künftig noch Upgrades notwendig sein. Zudem wird der flächendeckende Smart-Meter-Rollout vermutlich noch einige Zeit in Anspruch nehmen. Hier ist einerseits eine Standardisierung der Anwendungsfälle, die mit der SMGW-Infrastruktur umgesetzt werden sollen, in enger Abstimmung mit Fachkräften aus der Energiewirtschaft erforderlich. Andererseits werden für den Startzeitraum Übergangslösungen benötigt, die beispielsweise die kommunikationstechnische Anbindung von Ladeinfrastruktur ermöglichen. Jedoch müssen diese ebenso Mindestanforderungen hinsichtlich des Datenschutzes und der IT-Sicherheit erfüllen. Für Bestandsinfrastruktur, wie die Prozessnetze von Netzbetreibern, werden ebenfalls kurzfristig einsetzbare Cybersicherheitstechnologien benötigt. Diese Infrastrukturen sind zwar physisch getrennt von öffentlichen Netzen, weisen jedoch aufgrund der hohen Durchdringung von Legacy-Komponenten meist keine ausreichende Absicherung gegen IT-Angriffe auf. Eine schnell einsetzbare Lösung sind hier IDS, die den Datenverkehr überwachen und Angriffe detektieren können. Zusätzlich ist jedoch auch eine Absicherung durch eine Verschlüsselung der Kommunikation notwendig, wofür jedoch voraussichtlich eine grundlegende Erneuerung von Teilen der Bestandsinfrastruktur erforderlich ist.

# 5 Maßnahmen zur Förderung energiewirtschaftlicher Cyberinnovationen

Die Schaffung sicherer technischer Grundlagen – von Kommunikationstechnologien über sichere Datenverarbeitung bis hin zu umfassenden Lösungen wie dem Smart Meter Gateway (SMGW) – ist eine Grundvoraussetzung für Cyberinnovationen in der deutschen Energiewirtschaft. Die Entwicklung solcher Technologien, deren Integration in die vorhandenen komplexen Topologien sowie Sicherheitsevaluationen erfordern jedoch auch weitergehende fördernde Maßnahmen, unter anderem von staatlicher Seite. Um Deutschland als Innovationsstandort im Bereich der digitalen Energiewirtschaft zu etablieren, bietet sich ein breites Spektrum möglicher Fördermaßnahmen an, die auch Inspiration aus internationalen Best-Practice-Beispielen ziehen können. Dieses Kapitel stellt zunächst allgemeine Maßnahmen zur Förderung von Cyberinnovationen vor (Abschnitt 5.1). Anschließend werden Entwicklungen im Bereich der Cyberinnovationen mit einem Fokus auf die Smart-Metering-Infrastruktur auf internationaler Ebene verglichen und diskutiert (Abschnitt 5.2). Das Kapitel schließt mit der darauf aufbauenden Analyse und Diskussion von konkreten Lösungsstrategien für Cyberinnovationen in Deutschland (Abschnitt 5.3).

## 5.1 Fördermaßnahmen für Cyberinnovationen

Es existiert ein breites Spektrum an Möglichkeiten für konkrete Fördermaßnahmen in den verschiedenen Bereichen und auf den unterschiedlichen Ebenen der Energiewirtschaft. Auch internationale Erfahrungen und internationale Expertise können helfen, Deutschland im Bereich der Cyberinnovationen in der Energiewirtschaft voranzubringen. Im Rahmen der Erstellung dieses Gutachtens wurden zu diesem Zweck zwei Workshops mit nationalen und internationalen Vertreterinnen und Vertretern aus Energiewirtschaft und Politik durchgeführt. Die Ergebnisse dieser Workshops fließen in die folgende Diskussion ein.

**Allgemeine Struktur der Förderpolitik.** Die Ziele von Förderpolitik sind vielschichtig: Von Cybersicherheit und Digitalisierung über Energiewende und Marktdiversität bis hin zu einer nationalen energiewirtschaftlichen Vorreiterrolle adressiert staatliche Förderpolitik möglicherweise verschiedenste Aspekte auf unterschiedliche Arten. Grundsätzlich stehen sich hierbei zwei Ansätze mit unterschiedlichen Vor- und Nachteilen gegenüber.

Die deutsche Förderpolitik folgt primär einem Top-Down-Ansatz, bei dem der Staat als fördernde Instanz Förderungen für wohldefinierte Vorhaben vergibt. Förderungen sind an Vorhaben gebunden, die vordefinierte Kernaspekte aufgreifen, weiterentwickeln und/oder umsetzen. Hierdurch können Fördermittel gezielt an solche Akteure vergeben werden, die in ihren Vorhaben mit den Ansichten der vergebenden Partei übereinstimmen, und es können Thematiken und Technologien gezielt forciert werden. Allerdings können falsch gesetzte Vorgaben auch dazu führen, dass Alternativen nicht oder nur unzureichend betrachtet und Akteure in ihrer Innovationsfreiheit eingeschränkt werden.

Dieser Handlungsweise steht der Bottom-Up-Ansatz gegenüber, der beispielsweise in Israel erfolgreich eingesetzt wird. Hierbei werden Fördermittel unter anderem thematisch weiter gefasst bereitgestellt, woraufhin Akteure sich aktiv auf Förderungen mit konkreten Vorschlägen bewerben. Durch die weiter gefassten Kriterien kommen hier auch Förderungen für Ansätze zustande, die bei einem reinen Top-Down-Ansatz früh verworfen worden wären.

Während diese Vorgehensweise stärker durch die Fördernehmer geprägt wird und generell ein breiteres Spektrum an Ansätzen ermöglicht, gibt es jedoch auch ein erhöhtes Risiko, dass Fördermittel für letztendlich nicht zielführende Ansätze vergeben werden.

**Konkrete förderpolitische Maßnahmen.** Im Zusammenhang mit den konkreten Anreizmöglichkeiten zur Förderung der Cybersicherheit, aber auch der Cyberinnovation gibt es einige Möglichkeiten aus der Praxis, die aus anderen Sektoren und Ländern übernommen werden können. Zum Beispiel bieten Bug-Bounty-Programme Hackern eine Prämie für das Auffinden von Sicherheitslücken abhängig von der Kritikalität der jeweiligen Schwachstelle. Der Softwareentwickler verpflichtet sich, den Preis zu zahlen, und die Hacker können rechtliche Schritte einleiten, wenn der Softwareentwickler dies unterlässt. Mit den Bug-Bounty-Programmen verpflichten sich die Softwareentwickler also nicht nur, für die Identifikation einer Sicherheitslücke zu zahlen, sondern sie sichern die Hacker auch rechtlich ab. Insbesondere die Einführung des Crowdsourcing zur Erkennung, Bewertung und Meldung von Softwarefehlern durch die Cybersicherheits-Community scheint in der Lage zu sein, die traditionellen Methoden zur Bewältigung von Cybersicherheitsbedrohungen zu erweitern. Strenge interne Sicherheitsprüfungen werden jedoch weiterhin ein wichtiger Bestandteil der Modernisierung der Cybersicherheitspraxis bleiben. Die Bug-Bounty-Programme haben das Potenzial, das Bewusstsein für Cybersicherheitsbedrohungen in der digitalen, vernetzten Umgebung zu schärfen, wenn die Ergebnisse, wie zum Beispiel neu identifizierte gültige Softwarefehler, transparent weitergegeben werden.

Um die Cybersicherheit innerhalb der menschenzentrierten Prozesse (Human-in-the-Loop) weiter zu stärken, sind regelmäßige Cybersecurity-Awareness-Trainings für das Personal erforderlich. Sie ermöglichen die Schulung der Beschäftigten zur Sensibilisierung für Themen der Cybersicherheit und Informationssicherheit und zeigen die Schnittpunkte dieser Themen mit den eigenen Verantwortlichkeiten und Handlungen auf, um ein ausreichendes Maß an Informationssicherheitskontrolle zum Schutz der Daten und Netzwerke des Unternehmens zu erreichen. Folglich müssen praktische Schulungs-Workshops und Studienprogramme mit Kursen zur Sensibilisierung für Cybersicherheit eingerichtet werden, um das Wissen der Beschäftigten in Bezug auf Angriffe und die Cybersicherheit zu erhöhen. Diese Schulungsinhalte sollten ermöglichen, das erlernte Wissen unmittelbar in die Tat umsetzen zu können, um so den in Bezug auf die IT-Sicherheit eines Unternehmens „wesentlichen Faktor Mensch“ zu minimieren. Auch kann die Bereitstellung von konkreten Handlungsempfehlungen im Rahmen von Leitfäden für die Mitarbeiterinnen und Mitarbeiter in diesem Bereich Unterstützung bieten. Hier können Cyberinnovationen beispielsweise in Form von virtuellen Trainingsumgebungen für Incident Response ebenfalls den Ausbildungs- und Sensibilisierungsprozess unterstützen und fördern.

Die Grundlage für die Entwicklung von sektorspezifischen Lösungen zur Erhöhung der IT-Sicherheit ist jedoch die stetige Weiterentwicklung der gültigen Cybersicherheitsstandards. Sie sollten nicht nur Vorgaben machen, sondern auch Anwendungshinweise geben, die sowohl die Prävention als auch die Detektion und Reaktion bei Sicherheitsvorfällen adressieren. Das übergeordnete Ziel von Cybersicherheitsstandards besteht darin, die Sicherheit von IT-Systemen, Netzwerken und kritischen Infrastrukturen zu erhöhen. In der Regel werden in Cybersicherheitsstandards Anforderungen an die Funktionalität und die Zuverlässigkeit der betreffenden Systeme, Richtlinien für die Verwaltung von Informationen, Kriterien für die Bewertung von Sicherheitsmaßnahmen, Techniken für die Behebung von Sicherheitsmängeln und Verfahren für die Überwachung von Sicherheitsverletzungen definiert. Durch inhaltliche und finanzielle Unterstützung kann der Staat die Erforschung, Entwicklung und Umsetzung solcher Standards aktiv fördern und lenken.

**Entwicklung neuer Dienstleistungsbereiche.** Durch die Entwicklung neuer Anwendungsfälle in der Energiewirtschaft, die hoch vernetzte und leistungsfähige Infrastrukturen zur Realisierung erfordern, können sich neue Dienstleistungsmöglichkeiten in Richtung der Bereitstellung von Infrastrukturen, Plattformen und Software sowie der Umsetzung von gemeinsamen Aufgaben ergeben. Insbesondere die Vorteile der Skalierbarkeit spielen eine wesentliche Rolle. So kann die Infrastruktur dynamisch an die Anforderungen, aber auch entsprechend der vorhandenen Automatisierung von Prozessen angepasst werden. Cloud-basierte Backends sind eine prominente Infrastrukturlösung für die technische Gestaltung skalierbarer und kosteneffizienter Anwendungsfälle. Die Cloud stellt bei dem Dienst „Infrastructure-as-a-Service" lediglich ein virtuelles Rechenzentrum dar. Bei „Platform-as-a-Service" wird eine Plattform für die Entwicklung von Anwendungen oder bei „Function-as-a-Service" ausschließlich die Geschäftslogik und bei „Software-as-a-Service" die komplette Kette vom Hosting bis zur Ausführung der Geschäftslogik in Software bereitgestellt. Je nach Ausprägung wird hier ein Teil der Verantwortung dem Service Provider übertragen. Dies betrifft die Umsetzung geeigneter Maßnahmen bezüglich IT-Sicherheit und Datenschutz wie auch die Verantwortung für die Konfiguration und den Betrieb der Infrastruktur, die eingesetzte Software und die Ausführung der Geschäftslogik.

Cloud-basierte Backend-Lösungen können zunehmend in der Energiewirtschaft Anwendung finden, zum Beispiel für EMT-Backend-Anbindungen oder im Bereich der Ladeinfrastruktur für Elektromobilität. Außerhalb von Cloud-basierten Backends können auch neue Dienstleister im Rahmen von Redispatch 2.0, wie beispielsweise Direktvermarktungsunternehmen, die Aufgaben von Anlagenbetreibern übernehmen und entsprechend den Vorgaben erfüllen. Auch hier können Cybersecurity-motivierte Innovationen entstehen, insbesondere im Bereich des Angebots von sicheren Infrastrukturen und „Software-as-a-Service". Darüber hinaus kann die Wartung von Komponenten und Software von den Dienstleistern oder speziellen Services abgedeckt werden, die primär die Aufgabe verfolgen, bestehende Sicherheitslücken im System zu identifizieren und zu beseitigen. In einem weiteren Schritt können auch Incident Response Services entstehen, die für die Überwachung und Bewertung von IT-Sicherheitsvorfällen sowie für die Reaktion darauf zuständig sind („SOC-as-a-Service"). Hier können die Synergien und Schnittstellen zwischen den Dienstleistern genutzt werden, um den Beteiligten ausgereifte Cybersicherheitslösungen als Dienstleistung anzubieten, bei denen Infrastruktur, Software, Lebenszyklusmanagement, Sicherheitsoperationen und die Reaktion auf Vorfälle Teil von miteinander verbundenen Lösungen sind. Die Entwicklung und die Standardisierung entsprechender Cloud-Systeme, die die speziellen Anforderungen der Energiebranche berücksichtigen und zukunftssichere Sicherheitsstandards implementieren, sind ebenfalls ein Gebiet, das breite Möglichkeiten für Förderprogramme bietet. Finanzielle und operative Unterstützung kann helfen, entsprechende Technologien und Dienstleistungen zu entwickeln und zu etablieren.

Unabhängig von der konkreten Förderleistung wie beispielsweise finanziellen Zuwendungen bieten sowohl der Top-Down- als auch der Bottom-Up-Ansatz Vor- und Nachteile hinsichtlich ihrer Erfolgsaussichten, Cyberinnovationen zu stärken. Während Top-Down-getriebene Förderleistungen auf staatlichem Vorwissen basierend gezielter und organisierter vergeben werden können, bietet der Bottom-Up-Ansatz mehr Flexibilität und ein breiteres Spektrum an Innovationspotenzial. Jede förderpolitische Entscheidung sollte sich der Vor- und Nachteile des jeweiligen Ansatzes bewusst sein, sodass eine angemessene Balance zwischen beiden Ansätzen gefunden werden kann: Eine strukturierte Top-Down-geprägte Förderpolitik kann und sollte gezielt durch freier gefasste Bottom-Up-Projekte ergänzt werden. In Bezug auf die Cybersicherheit der Branche können neben der Förderung der Entwicklung von neuen Technologien und der Umsetzung entsprechender Standards insbesondere auch weitere unternehmensspezifische Maßnahmen wie beispielsweise Bug-Bounty-Programme und Security-Awareness-Trainings sinnvolle Maßnahmen darstellen, die in der Branche flächendeckende Anwendung finden sollten. Zudem ist auch der Trend zu erkennen, dass zunehmend einzelne Services sowie der Aufbau und Betrieb von notwendiger Infrastruktur zur Umsetzung neuer Anwendungsfälle „as-a-Service“ an externe Dienstleister ausgelagert werden, wobei insbesondere der Einsatz Cloud-basierter Infrastruktur ein vergleichsweise skalierbarer und kosteneffizienter Ansatz ist.

## 5.2 Rollout intelligenter Messsysteme im internationalen Vergleich

Auf europäischer Ebene sind die Ausbringung und der aktive Einsatz intelligenter Messsysteme in sehr unterschiedlichen Ausprägungen fortgeschritten.

Italien führte bereits Anfang der 2000er Jahre großflächig intelligente Zähler bei Endkundinnen und -kunden ein [86]. Zwischen 2001 und 2011 wurden hier etwa 36,7 Millionen Zähler installiert. Der einschlägige Rechtsrahmen ermöglichte es den Verteilnetzbetreibern, die hieraus entstandenen Kosten auf die Netzentgelte umzulegen. In Anbetracht der drohenden Veralterung der Bestandszähler und der Notwendigkeit, ihre Funktionen zu verbessern, hat die Regulierungsbehörde einen Rahmen für die Einführung von intelligenten Zählern der zweiten Generation geschaffen. Die Zähler der ersten Generation erfüllten nicht mehr die technischen Mindestanforderungen und waren nicht in der Lage, mindestens alle 15 Minuten aktualisierte Messwerte bereitzustellen. Tatsächlich beträgt die technische und regulatorische Lebensdauer eines Zählers etwa 15 Jahre. Im Vergleich zu anderen Regulierungsbehörden in Europa sahen sich die italienischen Behörden daher recht früh mit zwei Herausforderungen konfrontiert: erstens mit der flächendeckenden Bereitstellung intelligenter Zähler für alle Verbraucherinnen und Verbraucher und zweitens mit der praktischen Nutzung der bereits ausgebrachten Zähler [81]. Im Rahmen der Einführung eines neuen Anreizsystems ist seitens der Regulierungsbehörde sicherzustellen, dass alle Interessengruppen an den Vorteilen teilhaben, sodass Kosten und Nutzen in einem ausgewogenen Verhältnis zueinander stehen. Beispiele für die Umsetzung dieser Vorgaben liegen in der Verpflichtung zur vollständigen Offenlegung der Ergebnisse von Demonstrationsprojekten und der Forderung nach der Ermöglichung verbesserter und umfangreicherer Dienstleistungen für die Verbraucherinnen und Verbraucher im Rahmen der Einführung einer neuen Zählergeneration. Folglich ist es wichtig, das Element des Wettbewerbs im Innovationsprozess zu bewahren, da dies nicht nur eine höhere Kosteneffizienz gewährleistet, sondern auch einen starken Anreiz für die Teilnehmenden darstellt, effektive Lösungen zu finden, die in der Einführungsphase genutzt werden können, wie es bei der Einführung intelligenter Zähler in Italien der Fall war.

Ein weiteres Fallbeispiel sind die Niederlande, in denen im Jahr 2008 ein Gesetzesentwurf für intelligente Zähler vorgelegt wurde, der eine 100-prozentige Einführung vorschlug, die verpflichtend und mit hohen Geld- oder Haftstrafen für Verweigerer verbunden wäre [55]. Die vorgeschlagenen technischen Spezifikationen der Zähler deckten in diesem Kontext Anzeigen im Haus, einen Alarm für unerwartete Verbrauchsspitzen, Echtzeitmessungen sowie Möglichkeiten zur Fernprogrammierung von Geräten und zur Kommunikation mit anderen Zählern ab. Die Versorgungsunternehmen begannen 2012 mit einer Testphase, in der 600.000 intelligente Zähler installiert wurden, um Erfahrungen zu sammeln und mögliche Probleme frühzeitig zu erkennen, damit rechtzeitig für die zweite Phase – die großflächig angelegte Einführung – eventuell erforderliche Anpassungen identifiziert werden konnten. Die Masseneinführung begann 2014 mit mehr als 1 Million Installationen innerhalb eines Jahres. Bis zum Jahr 2019 wurde eine Rollout-Quote von etwa 78 Prozent erreicht. Auch hier war die Installation selbst für die Endkundinnen und -kunden kostenfrei, wurde jedoch durch die Netzbetreiber auf die Netzentgelte umgelegt.

Im Vereinigten Königreich umfasste die ursprünglich geplante Ersteinführung von intelligenten Zählern die Ausbringung von 53 Millionen Gas- und Stromzählern bis 2020 [55]. Die Regierung beschloss außerdem, den Energieversorgern die Verantwortung für die Einführung zu übertragen. Die Vorlaufkosten wurden ebenfalls durch die Versorger getragen und werden auf die Abrechnungen der Verbraucherinnen und Verbraucher umgelegt. Erste Erfahrungen des Rollouts zeigten, dass der Einsatz intelligenter Zähler insbesondere in Hochhäusern, Kellern und ländlichen Gebieten nur eingeschränkt funktioniert. Anfang 2015 funktionierten 134.000 der bis dahin 1,3 Millionen neu installierten intelligenten Zähler nur wie klassische Zähler und mussten aufgrund technischer Beschränkungen manuell abgelesen werden. Ein weiteres Problem war, dass die Zähler der ersten Generation nicht universell mit anderen Anbietern kompatibel waren, sodass der Wechsel des Versorgers für die Endkundinnen und -kunden erschwert wurde. Die groß angelegte Einführung begann 2016, wobei aufgrund von Installationsfehlern mehr als 10 Prozent der Haushalte mehrfach besucht werden mussten, um die Installation abzuschließen.

Der Rollout intelligenter Messsysteme wurde in den genannten Nationen jeweils mit unterschiedlichen Ansätzen umgesetzt. Für die Ausbringung von neuer Technologie besteht einerseits die Möglichkeit, kurzfristige Ziele zu definieren und zyklisch bzw. frühzeitig Anpassungen vorzunehmen, wenn technische Probleme bei der Umsetzung festgestellt werden. Dieses Muster ist beim Rollout in Italien und den Niederlanden zu beobachten. Hier wurde eine rasche Umsetzung des Rollouts angestrebt, die jedoch erhebliche technische und regulatorische Anpassungen im Nachgang an die erste Rollout-Phase erforderte. Im Vereinigten Königreich wurde andererseits an einem eher technokratischen Ansatz festgehalten. Die Einführung der Messsysteme stieß zeitweise sowohl auf technische Schwierigkeiten als auch auf soziale Akzeptanzprobleme, wodurch die Einführung intelligenter Zähler zeitweise verzögert wurde.

In Deutschland erfolgt die Einführung wiederum nach einem Top-Down-Ansatz, bei dem alle Anforderungen an die Infrastruktur vor allem aus regulatorischen Vorgaben abzuleiten sind. Im Vergleich zu Italien, wo in erster Linie die Verringerung des Stromdiebstahls durch Smart Meter beim initialen Rollout im Vordergrund stand [58], liegt der Fokus der Rollout-Strategie in Deutschland auf der technischen Funktion der Smart Meter, der Zertifizierung und der sicheren Kommunikationsschnittstelle [60]. Insbesondere soll sichergestellt werden, dass die Geräte so selten wie möglich ausgetauscht werden müssen und ihre Lebensdauer unter Berücksichtigung der Eichfrist und der Kompatibilität mit neuen technischen Funktionen möglichst langfristig ausgelegt werden kann. Auch national wurde der Rollout zeitweise wegen verschiedener regulatorischer Probleme verzögert und stößt unter anderem aufgrund von fehlender Standardisierung und Problemen bei der Nutzbarkeit der Infrastruktur teils auf Akzeptanzprobleme. Insgesamt muss ein gutes Mittelmaß

zwischen rascher Umsetzung, beispielsweise im Rahmen von Pilotprojekten, und einer detaillierten Planung und Förderung durch die Politik in Absprache mit allen beteiligten Akteuren bei der Ausbringung neuer Technologien erfolgen.

> Während Demonstratoren und „Learning by doing“ in frühen Phasen der Ausbringung einer neuen Technologie wichtige Erkenntnisse hinsichtlich der Umsetzbarkeit liefern können, sind zentralisierte Planung und technologiefördernde Maßnahmen insbesondere in späteren Phasen erforderlich, um die Einführung kosteneffizient voranzutreiben. Die ausführenden Unternehmen und politischen Entscheidungsträger sind zwar wichtige Akteure, jedoch erfordert die Verbreitung einer Technologie auch die Einbeziehung mittelbar beteiligter Akteure – wie im Falle der SMGW-Infrastruktur die der Verbraucherinnen und Verbraucher, der breiten Öffentlichkeit und anderer beteiligter Markteilnehmer – während des gesamten Umsetzungsprozesses, um eine flächendeckende Akzeptanz zu erreichen. Die Einbettung von einzelnen Technologieförderungen in umfassendere Transformationsprogramme kann auch eine effektivere Strategie als die Förderung von Technologien als eigenständigen Transformationsinstrumenten darstellen.

## 5.3 Lösungsstrategien zur Innovationsförderung in der deutschen Energiewirtschaft

Grundlegend existieren verschiedene Optionen, Innovation im Bereich der Energiewirtschaft zu fördern. Die Vielzahl der neuen Anwendungsfälle im Rahmen der Dezentralisierung der Erzeugung im Stromnetz und der Digitalisierung des Sektors bietet an vielen Stellen Potenziale, neue Technologien zu etablieren. Entsprechende Fördermaßnahmen und die Gestaltung von Weiterentwicklungsprozessen hierfür werden im Folgenden diskutiert.

**Innovationsförderung durch die Politik.** Eine Balance zwischen der gezielten technologiespezifischen Förderung und einer freieren, technologieunabhängigen Förderung von allgemeiner gefassten Forschungsprojekten kann zur effizienten Förderung von Innovation in der nationalen Energiewirtschaft führen (vgl. Abschnitt 5.1). Technologiespezifische Förderung basiert demnach auf Erkenntnissen aus vorheriger Forschung, in deren Rahmen Technologien identifiziert wurden, die sich als vielversprechend für den Markt herausgestellt haben. Die technologieunabhängige Förderung ermöglicht dagegen auch die Betrachtung von potenziellen alternativen Lösungsansätzen und gibt somit nur das Ziel, jedoch nicht einen konkreten Transitionspfad vor.

Konkret kann zudem die Förderung von Pilotprojekten und Demonstrationsumgebungen dabei unterstützen, die Akzeptanz und Anwendbarkeit neuer Technologien positiv zu beeinflussen und zu gewährleisten, dass Technologieentwicklungen aus der Forschung auch auf Produktivsysteme übertragbar sind. Insbesondere im Bereich der IT-Sicherheit ist zudem die Förderung des Aufbaus von Demonstratoren, in denen neue Technologien anwendungsnah in betrieblichen Umgebungen eingesetzt und weiterentwickelt werden können, eine sinnvolle Möglichkeit, die Technologiereife von Cyberinnovationen zu demonstrieren. Zudem lässt sich die Effektivität der entwickelten Technologien erhöhen, da entsprechende Tests im Produktivbetrieb im Allgemeinen nicht vollständig bzw. nicht risikofrei durchgeführt werden können. So können beispielsweise für die Entwicklung von Technologien zur Detektion von IT-Angriffen synthetische Angriffsversuche in einer sicheren, abgeschlossenen und kontrollierten Umgebung durchgeführt werden.

Sowohl die Erforschung als auch der Einsatz von neuen Technologien in der Energiebranche sind geprägt vom aktuellen Stand der Ausarbeitung der relevanten Regulatorik und den sich daraus ergebenden Mindestanforderungen an die technische Umsetzung von Anwendungsfällen. Bei der Entwicklung regulatorischer

Maßnahmen ist die Schaffung von Transparenz für die Umsetzbarkeit und Akzeptanz ein anzustrebendes Ziel. Diesbezüglich ist ein stetiger Austausch zwischen den befugten Behörden und den betreffenden Akteuren der Energiebranche zu einem frühestmöglichen Zeitpunkt der Ausarbeitung neuer Regulatorik notwendig, um frühzeitig für die Branche repräsentative, nachvollziehbare und umsetzbare Regularien zu entwickeln.

Weitere Potenziale zur Förderung und Beschleunigung von Innovation ergeben sich durch die weitestmögliche Vereinfachung, Verkürzung und Digitalisierung von Planungs-, Genehmigungs- und Zertifizierungsprozessen. Die Verkürzung bzw. Beschleunigung von Planungs- und Genehmigungsprozessen kann dazu beitragen, die Voraussetzungen dafür zu schaffen, die Integration und den Einsatz von neuen Technologien im Produktivbetrieb schneller umzusetzen. Hierbei kann die Stärkung der Kompetenzen des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Rahmen des IT-Sicherheitsgesetzes dazu führen, dass eine zentrale Anlaufstelle für IT-Sicherheit in kritischen Infrastrukturen aufgebaut wird. Um Zertifizierungsprozesse zu beschleunigen, kann hier ihre Auslagerung an externe Dienstleister (weiterhin unter Aufsicht des BSI) eine sinnvolle Option darstellen, um die Behörde zugunsten ihrer Kernaufgaben zu entlasten.

**Innovationsförderung im Bereich IT/OT-Security für die Energiewirtschaft.** Um die Entwicklung von branchenspezifischen IT-Sicherheitstechnologien voranzutreiben, muss im Rahmen von marktorientierten Förderungsstrategien die Wirtschaftlichkeit dieser Entwicklungen gegeben sein. Dafür müssen für die Akteure der Branche Anreize geschaffen werden, auch Technologien einzusetzen, die funktional über die Erfüllung der aktuellen Mindestanforderungen hinausgehen. Dementsprechend müssen Lösungen entwickelt werden, damit die Umsetzung von sinnvollen Maßnahmen im Bereich der Cybersicherheit über die Anforderungen des IT-Sicherheitskatalogs hinaus erfolgen kann. Hier ist ebenfalls zu berücksichtigen, dass im Rahmen des IT/OT-Netzausbaus zukünftig nicht nur die funktionale Prüfung zur Erfüllung der Mindestanforderungen, sondern auch die Bewertung, inwiefern die eingesetzten Komponenten dem aktuellen Stand der Technik entsprechen, erforderlich sein sollte. Dies erfordert zukünftig voraussichtlich eine Verkürzung der Audit-Zeitabstände, um den vergleichsweise kurzen Modernisierungszyklen in der IT-Branche gerecht zu werden. Entsprechende Maßnahmen wären beispielsweise der Modernisierung von Prozessnetzen der Netzbetreiber zuträglich und es könnten Legacy-Komponenten zeitnah durch State-of-the-Art-Technologien ersetzt werden. Auch können so grundlegende Anforderungen an die IT-Sicherheit wie eine Verschlüsselung des Datenverkehrs erfüllt werden.

**Weiterentwicklung der SMGW-Infrastruktur.** Für die nachhaltige Realisierung von vielen der Anwendungsfälle, die zukünftig in der Energiebranche umgesetzt werden sollen, wird eine mit dem Design einhergehende sichere SMGW-Infrastruktur notwendig sein, die langfristig eine sichere Grundlage bietet. Die kurzfristige zu entwickelnden Übergangslösungen zur Kompensation aktueller Verzögerungen beim Rollout und zur Bewältigung der Herausforderungen hinsichtlich Nutzbarkeit, Zugänglichkeit und Interoperabilität der Infrastruktur sollten jedoch in gleichem Maße Anforderungen an IT-Sicherheit und Datenschutz erfüllen und die zukünftige Transition zur SMGW-Infrastruktur ermöglichen (vgl. Abschnitt 4.3). Zur besseren Akzeptanz und Nutzbarkeit der Infrastruktur kann zukünftig vor allem die Standardisierung der Use Cases zur Umsetzung von netz- und marktspezifischen Funktionen in enger Kooperation zwischen Behörden und Fachkräften aus der Branche beitragen. Bei Endkundinnen und -kunden können des Weiteren insbesondere Möglichkeiten für ein detailliertes Monitoring des eigenen Nutzerprofils und zur Optimierung der Kosten zum Beispiel durch dynamische Tarifmodelle bei einem gleichzeitig hohen Maß an Datenschutz helfen, die Akzeptanz entsprechend zu steigern. In Zukunft werden die meisten Netz- und Messstellenbetreiber in der Lage sein, Teile der Aufgaben und Verantwortlichkeiten, die mit dem Aufbau und dem Betrieb der SMGW-Infrastruktur

verbunden sein können, an externe Dienstleister auszulagern. Die Auslagerung des Betriebs der Infrastruktur „as-a-Service“ und der Einsatz von Cloud-basierter Infrastruktur bilden hier insbesondere für kleinere Unternehmen einen deutlich flexibleren und skalierbaren Ansatz.

Die Umsetzung von Cyberinnovation in der Energiebranche ist momentan maßgeblich davon geprägt, dass die betreffenden Unternehmen die aktuellen regulatorischen Mindestanforderungen erfüllen, wodurch sich eine zentrale Steuerung dieses Prozesses durch die zuständigen Behörden ergibt.

Wie aktuell auch in anderen Bereichen, beispielsweise beim Ausbau der Erneuerbaren Energien diskutiert, sollten diese Prozesse mittels verschiedener Ansätze, wie beispielsweise der Vereinfachung der bestehenden Regulatorik, der Entwicklung der zukünftigen Regulatorik in enger Absprache mit der Industrie und der Entbürokratisierung und Verkürzung von Planungs-, Genehmigungs- und Zertifizierungsprozessen, für die betreffenden Akteure vereinfacht werden. Auch sollten Anreize geschaffen werden, Technologien einzusetzen, die funktional über die Mindestanforderungen hinausgehende Fähigkeiten mitbringen. Insbesondere für Bestandsnetze im IT/OT-Bereich sollte ermöglicht werden, sie auf einen Stand zu bringen, der sowohl funktional als auch sicherheitstechnisch den Stand der Technik widerspiegelt. Für den Großteil der Mehrwertdienste wird langfristig eine sichere Gestaltung der Infrastruktur wie die auf Basis der SMGW-Infrastruktur von zentraler Bedeutung sein. Hierbei sollte für zukünftige Entwicklungen eine Standardisierung der Use Cases und eine Definition der Infrastruktur im Einklang erfolgen, um sowohl ein hohes Maß an Sicherheit als auch die Betriebstauglichkeit von Beginn an zu gewährleisten.

# 6 Fazit und Zusammenfassung

Durch die Entwicklungen in der Energiebranche hinsichtlich einer Dezentralisierung im Rahmen der Energiewende und der Digitalisierung der Energiewirtschaft entstehen neue Herausforderungen für die Branche. Ihre Bewältigung bedarf der Entwicklung und des Einsatzes neuartiger Technologien oder der Überführung bestehender Konzepte und Technologien aus anderen Branchen in die Energiewirtschaft. Insbesondere durch verstärktes Monitoring und zunehmende Automatisierung in den Netzen, aber auch durch die Schaffung neuer Marktrollen (z. B. Messstellenbetrieb und Gateway-Administration) entstehen demnach neue Handlungsfelder und hiermit auch Markt- und Entwicklungspotenziale für sektorspezifische Lösungen in den Bereichen der Kommunikationstechnik und Cybersicherheit. Vor allem ein Mindestmaß an Cybersicherheit ist für alle beteiligten Akteure, die einen Einfluss auf die Erbringung der „kritischen Dienstleistung Energieversorgung“ nehmen, unabdingbar. Sowohl für die operative als auch für die IT-Sicherheit existieren umfangreiche regulatorische Vorgaben. Für betroffene Akteure muss für innovationsgetriebenen Fortschritt transparent erkennbar sein, welche Bestandteile der Regulatorik für sie verbindlich sind und welche konkreten Handlungen zur Erfüllung der sich daraus ergebenden Mindestanforderungen notwendig sind. Bei der zunehmend komplexer werdenden Thematik Cybersicherheit ist hinsichtlich der Einzelregularien eine Abstimmung untereinander erforderlich, auch weil sich die Anforderungen in diesem Bereich stetig weiterentwickeln werden.

Im Rahmen des Gutachtens wurde der Smart-Meter-Rollout in Deutschland als Fallbeispiel für die Etablierung neuer Technologien betrachtet, bei dem im Wesentlichen eine technokratische Umsetzung mit einem Top-Down-Ansatz verfolgt wird. Aufgrund verschiedener Verzögerungen ist der Rollout bisher nicht flächendeckend erfolgt. Wie die Analyse des Rollout-Prozesses intelligenter Messsysteme in verschiedenen europäischen Ländern zeigt (vgl. Abschnitt 5.2), existiert für die flächendeckende und weitläufige Etablierung neuer Technologien wie bei der SMGW-Infrastruktur kein pauschaler, optimaler Ansatz. Hier sind alternative Strategien zur Etablierung neuer Technologien gefragt, wobei im Rahmen der Regulatorik eine Balance gefunden werden muss, um konkrete Mindestanforderungen an die Funktionsfähigkeit der Geräte und die Infrastruktur zu gewährleisten. Eine potenzielle „Überspezifikation“ würde sich gegebenenfalls auch negativ auf einen wettbewerbsfähigen Markt auswirken. Ein wesentlicher Bestandteil zur Sicherstellung dieses Aspekts ist die transparente Entwicklung der Regulatorik und Standards, bei der alle wichtigen Interessengruppen von Beginn an in den Prozess einbezogen werden. Eine umfassende und flexible Förderpolitik kann ebenfalls helfen, diese Prozesse zu optimieren. Innerhalb dieses Prozesses kann nicht nur ein aktiver repräsentativer Einfluss auf den Entwicklungspfad durch die Marktteilnehmer genommen werden, sondern auch eine nahezu ganzheitliche Einbeziehung von Perspektiven für eine nachhaltige Realisierung der Technologien erfolgen. Dazu gehört beispielsweise die Berücksichtigung einer zukunftssicheren Gestaltung großflächiger Infrastrukturen mit langfristigen Einsatzperspektiven, bei der nicht nur eine vorausschauende Dimensionierung auf der Hardwareseite erfolgen sollte, sondern auch ein vertretbarer Life-Cycle-Management-Prozess von der Softwareseite berücksichtigt wird.

Neben der Standardisierung der Use Cases und der Umsetzung von Sicherheitsanforderungen besteht für den Messstellenbetreiber eine Herausforderung in der Sicherstellung der Interoperabilität der neuen Technologien mit seinen bestehenden Technologien und der kommunikationstechnischen Anbindung der SMGWs an sein Netz. Welche Kommunikationstechnologien hierfür konkret eingesetzt werden sollten, ist immer abhängig von der jeweiligen Anwendung und den örtlichen Gegebenheiten, sodass hier keine allgemein gültige Empfehlung möglich ist. Die wichtigsten Technologien, die für die Branche von erhöhter Relevanz sind, wurden in Abschnitt 2.2 vorgestellt. Bei Maßnahmen, die der Erhöhung der Cybersicherheit dienen, ist eine Abwägung von (kurzfristiger) Umsetzbarkeit und Risikominimierungspotenzial entscheidend, um zu beurteilen, welche Maßnahmen in welchem Zeithorizont umgesetzt werden sollten. Generell ist es hier jedoch sinnvoll, auch Anreize dafür zu schaffen, Maßnahmen, die über die Erfüllung des Mindeststandards hinausgehen, umzusetzen („Security by Design“).

Um zukünftig die Etablierung neuer Technologien am Markt zu beschleunigen, müssen die bürokratischen und technischen Prozesse zur Genehmigung und Zertifizierung vereinfacht, transparenter gestaltet und beschleunigt werden. Vorhaben, die dem technologischen Fortschritt dienen, können im Rahmen konkreter förderpolitischer Maßnahmen in Form eines Top-Down- oder Bottom-Up-Ansatzes (vgl. Abschnitt 5.1) gefördert werden, abhängig davon, ob die zielgerichtete Förderung spezifischer Technologien oder die Innovationsfreiheit im Vordergrund stehen soll. Hybride Ansätze der Förderung können gezielte Aspekte dem aktuellen Entwicklungsstand entsprechend priorisieren und somit jeweils aktuelle Herausforderungen adaptiv adressieren. Wenn das Interesse an einer Technologie auf dem Markt insbesondere in frühen Phasen gefördert werden soll, kann der Fokus auf die Förderung der Umsetzung von Pilotprojekten und Demonstratoren ein vielversprechender Ansatz sein, um die Anwendbarkeit von entwickelten Konzepten zu prüfen, die Akzeptanz bei den betroffenen Akteuren zu erhöhen und zu einem frühen Zeitpunkt erforderliche Anpassungen zu identifizieren. In späteren Phasen der Förderung nimmt die Bedeutung eines technokratischen Ansatzes, der ganzheitliche und zukunftsweisende Ziele vorsieht, zu, um die Etablierung einer Technologie am Markt zu stabilisieren.

> Insgesamt stehen der Energiewende und der innovativen Anwendungsentwicklung in der Energiewirtschaft in Deutschland viele geeignete Mittel in Verbindung mit nationalen sowie internationalen Erfahrungen zur Verfügung. Transparenz, Interoperabilität, wohldefinierte Förderpolitik, Anwendungsorientierung, Kommunikations- und Datensicherheit sowie ein umfassendes, praxisorientiertes und branchenweit abgestimmtes regulatorisches Rahmenwerk sind die in diesem Gutachten identifizierten Kernaspekte für eine langfristig (cyber-)sichere und zukunftsorientierte deutsche und europäische Energiewirtschaft. Hierbei ist das Erreichen einer Balance zwischen Cybersicherheitskonzepten, Kostenaspekten und Anwendungsfeldern unter Beteiligung aller Akteure aus der Energiewirtschaft und der Politik erforderlich.

# Abkürzungsverzeichnis

| | |
|---|---|
| **ABE** | Attribute-based Encryption |
| **AES** | Advanced Encryption Standard |
| **AS4** | Applicability Statement 4 |
| **BDEW** | Bundesverband der Energie- und Wasserwirtschaft e.V. |
| **BKV** | Bilanzkreisverantwortlicher |
| **BMWK** | Bundesministerium für Wirtschaft und Klimaschutz |
| **BNetzA** | Bundesnetzagentur |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik |
| **BSI-KritisV** | Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz |
| **CLS** | Controllable Local System |
| **CPS** | Cyber-physisches System |
| **DEA** | Dezentrale Erzeugungsanlage |
| **DSL** | Digital Subcriber Line |
| **DTLS** | Datagram Transport Layer Security |
| **ECDH** | Elliptic Curve Diffie-Hellman (kryptografisches Verfahren) |
| **ECDSA** | Elliptic Curve Digital Signature Algorithm |
| **EEG** | Erneuerbare-Energien-Gesetz |
| **EMT** | Externer Marktteilnehmer |
| **ENTSO-E** | European Network of Transmission System Operators for Electricity |
| **EnWG** | Energiewirtschaftsgesetz |
| **EVM** | Ethereum Virtual Machine |
| **EVU** | Energieversorgungsunternehmen |
| **FaaS** | Function-as-a-Service |
| **FDI** | False Data Injection |
| **FHE** | Fully Hormophic Encryption |
| **GBit/s** | Gigabit pro Sekunde |
| **GEO** | Geosynchronous Earth Orbit |
| **GHz** | Gigahertz |
| **GSM** | Global System for Mobile Communications |
| **GW** | Gateway |
| **GWA** | Gateway-Administrator |
| **HAN** | Home Area Network |
| **IaaS** | Infrastructure-as-a-Service |
| **IDS** | Intrusion Detection System |
| **IETF** | Internet Engineering Task Force |
| **IKT** | Informations- und Kommunikationstechnik |
| **IMSI** | International Mobile Subscriber Identity |
| **iMSys** | intelligentes Messsystem |
| **IoT** | Internet of Things |
| **IPS** | Intrusion Prevention System |
| **ISMS** | Information Security Management System |
| **ISP** | Internet Service Provider |

| | |
|---|---|
| **IT** | Informationstechnik |
| **KI** | Künstliche Intelligenz |
| **KNN** | Künstliches neuronales Netz |
| **KRITIS** | Kritische Infrastruktur |
| **kW** | Kilowatt |
| **kWh** | Kilowattstunde |
| **LEM** | Local Energy Market |
| **LEO** | Low Earth Orbit |
| **LMN** | Local Metrological Network |
| **LMS** | Leighton-Micali Hash-Based Signature |
| **LoRaWAN** | Long Range Wide Area Network |
| **LTE** | Long Term Evolution |
| **LTE-M** | Long Term Evolution for Machines |
| **MAC** | Message Authentication Code |
| **MaStR** | Marktstammdatenregister |
| **MBit/s** | Megabit pro Sekunde |
| **MEO** | Medium Earth Orbit |
| **MHz** | Megahertz |
| **ML** | Machine Learning |
| **mME** | moderne Messeinrichtung |
| **Mrd.** | Milliarde |
| **ms** | Meter pro Sekunde |
| **MSB** | Messstellenbetreiber |
| **MsbG** | Messstellenbetriebsgesetz |
| **MW** | Megawatt |
| **NABEG 2.0** | Netzausbaubeschleunigungsgesetz |
| **NB-IoT** | Narrowband IoT |
| **NFV** | Network Functions Virtualization |
| **NIST** | National Institute of Standards and Technology |
| **NOVA** | Netz-Optimierung vor -Verstärkung vor -Ausbau |
| **PaaS** | Platform-as-a-Service |
| **PIN** | Personal Identification Number |
| **PKI** | Public-Key-Infrastruktur |
| **PoA** | Proof of Authority |
| **PoW** | Proof of Work |
| **PQK** | Post-Quantum-Kryptografie |
| **QoS** | Quality of Service |
| **RSA** | Rivest-Shamir-Adleman (kryptografisches Verfahren) |
| **SaaS** | Software-as-a-Service |
| **SC** | Smart Contract |
| **SCADA** | Supervisory Control and Data Acquisition |
| **SDN** | Software-Defined Networking |
| **SIEM** | Security Information and Event Management |
| **SMGW** | Smart Meter Gateway |
| **SM-PKI** | Smart-Metering-Public-Key-Infrastruktur |

| | |
|---|---|
| **SOC** | Security Operations Center |
| **SSH** | Secure Shell |
| **StromNZV** | Stromnetzzugangsverordnung |
| **TLS** | Transport Layer Security |
| **TR** | Technische Richtlinie |
| **TTP** | Trusted Third Party |
| **ÜNB** | Übertragungsnetzbetreiber |
| **USV** | Unterbrechungsfreie Stromversorgung |
| **V2G** | Vehicle-to-Grid |
| **VDE** | Verband der Elektrotechnik, Elektronik und Informationstechnik e.V. |
| **VDE FNN** | Forum Netztechnik/Netzbetrieb im VDE |
| **VKU** | Verband kommunaler Unternehmen e.V. |
| **VNB** | Verteilnetzbetreiber |
| **VPN** | Virtual Private Network |
| **WAN** | Wide Area Network |
| **WLAN** | Wireless Local Area Network |
| **XMSS** | eXtended Merkle Signature Scheme |

# Literaturverzeichnis


[1] 50 Hertz Transmission GmbH, Amprion GmbH, TenneT TSO GmbH, TransnetBW GmbH. Netzentwicklungsplan: NOVA-Prinzip. https://www.netzentwicklungsplan.de/de/nova-prinzip (abgerufen am 23.10.2021).

[2] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta et al. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology, 2019.

[3] E. Alkim, Joppe W. Bos, L. Ducas, P. Longa, Ilya Mironov, M. Naehrig, V. Nikolaenko, Chris Peikert, A. Raghunathan und D. Stebila. FrodoKEM: Learning With Errors Key Encapsulation Algorithm Specifications and Supporting Documentation, 2020.

[4] Michael J. Assante und Robert M. Lee. The Industrial Control System Cyber Kill Chain. SANS Institute InfoSec Reading Room, 1, 2015.

[5] Daniel J. Bernstein, Tung Chou, Tanja Lange, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Peter Schwabe, Jakub Szefer und Wen Wang. Classic McEliece: Conservative Code-Based Cryptography – 30 March 2019, 2019.

[6] John Bethencourt, Amit Sahai und Brent Waters. Ciphertext-Policy Attribute-Based Encryption. In: 2007 IEEE Symposium on Security and Privacy (SP'07), S. 321–334. IEEE, 2007.

[7] Pat Bosshart, Dan Daly, Glen Gibb, Martin Izzard, Nick McKeown, Jennifer Rexford, Cole Schlesinger, Dan Talayco, Amin Vahdat, George Varghese et al. P4: Programming Protocol-Independent Packet Processors. ACM SIGCOMM Computer Communication Review, 44(3):87–95, 2014.

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI). Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen. Technical report, 2014.

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI). Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls. Technical report, 2014.

[10] Bundesamt für Sicherheit in der Informationstechnik (BSI). Smart-Meter-Gateway-Administration. Technical report, 2015.

[11] Bundesamt für Sicherheit in der Informationstechnik (BSI). Certificate Policy der Smart Metering PKI. Technical report, 2017.

[12] Bundesamt für Sicherheit in der Informationstechnik (BSI). Smart Metering PKI – Public Key Infrastruktur für Smart Meter Gateways. Technical report, 2017.

[13] Bundesamt für Sicherheit in der Informationstechnik (BSI). Technische Richtlinie TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government. Technical report, 2019.

[14] Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4. Technical report, 2020.

[15] Bundesamt für Sicherheit in der Informationstechnik (BSI). Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. Technical report, 2021.

[16] Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI TR-03116-3 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3. Technical report, 2021.

[17] Bundesamt für Sicherheit in der Informationstechnik (BSI). Technische Richtlinie TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Technical report, 2021.

[18] Bundesnetzagentur. Beschluss zur weiteren Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende – Beschlusskammer 6. https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2018/BK6-18-032/BK6-18-032_Beschluss.pdf?blob=publicationFile&v=2 (abgerufen am 26.11.2021).

[19] Bundesnetzagentur. IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz. https://www. bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf? blob=publicationFile&v=1 (abgerufen am 23.10.2021).

[20] Bundesnetzagentur. Konsultation eines Festlegungsentwurfes zur künftigen Absicherung der elektronischen Marktkommunikation Strom. https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2021/BK6-21-282/Konsultationsdokument.pdf? blob=publicationFile&v=4 (abgerufen am 26.10.2021).

[21] Bundesnetzagentur. Mitteilung Nr. 22 zu den Datenformaten zur Abwicklung der Marktkommunikation – Beschlusskammer 6. https://www.bundesnetzagentur.de/DE/Beschlusskammern/BK06/BK6_83_Zug_Mess/835_mitteilungen_datenformate/Mitteilung_22/Mitteilung_22.html?nn=516448 (abgerufen am 26.10.2021).

[22] Bundesnetzagentur. Presse – Vergabe von Frequenzen im Bereich 450 MHz. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2020/20201116_450mhz.html, 2020 (abgerufen am 30.08.2021).

[23] Bundesnetzagentur. 450 MHz – Erfolgreiche Bewerbung der 450connect GmbH. https://www. bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2021/20210309_450Mhz.html?nn=267872, 2021 (abgerufen am 30.08.2021).

[24] Ismail Butun, Nuno Pereira und Mikael Gidlund. Security Risk Analysis of LoRaWAN and Future Directions. Future Internet, 11, 2018.

[25] Cisco. Snort – Network Intrusion Detection & Prevention System. https://snort.org, 1998.

[26] International Electrotechnical Commission. IEC 60870-5-104: Transmission Protocols – Network Access for IEC 60870-5-101 Using Standard Transport Profiles – Edition 2.1, 2016.

[27] International Electrotechnical Commission. IEC 62351-9:2017, 2017.

[28] International Electrotechnical Commission. IEC 61850:2021 – Communication Networks and Systems for Power Utility Automation, 2021.

[29] Eric Crockett, Christian Paquin und Douglas Stebila. Prototyping Post-Quantum and Hybrid Key Exchange and Authentication in TLS and SSH. Cryptology ePrint Archive, Report 2019/858, 2019.

[30] Hans Delfs und Helmut Knebl. Introduction to Cryptography: Principles and Applications, 2007.

[31] BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. Konkretisierung des Ampelkonzepts im Verteilungsnetz, 2017.

[32] BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. Datenerhebung 2019 – Bundesmix 2019, 2020.

[33] BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. Die Energieversorgung 2020 – Jahresbericht, 2021.

[34] BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. Rollenmodell für die Marktkommunikation im deutschen Energiemarkt, 2021.

[35] BDEW Bundesverband der Energie-und Wasserwirtschaft e.V. BDEW-Branchenlösung Redispatch 2.0, 2020.

[36] BDEW Bundesverband der Energie-und Wasserwirtschaft e.V. und Oesterreichs E-Wirtschaft. Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme – Version 2.0, 2018.

[37] Mohamed Eldefrawy, Ismail Butun, Nuno Pereira und Mikael Gidlund. Formal Security Analysis of LoRaWAN. Computer Networks, 148:328–339, 2019.

[38] Electricity Information Sharing and Analysis Center (E-ISAC). Analysis of the Cyber Attack on the Ukrainian Power Grid – Defence Use Case. Technical report, 2016.

[39] European Network of Transmission System Operators for Electricity (ENTSO-E). Network Code for Cybersecurity Aspects of Cross-Border Electricity Flows – Draft: 28.10.2021. https://consultations.entsoe.eu/system-operations/network-code-on-cybersecurity/supporting_documents/211110_NCCS_Legal%20Text_For_Public_Consultation.pdf (abgerufen am 29.11.2021).

[40] International Organization for Standardization. ISO 27000 – ISO 27001 and ISO 27002 Standards. https://www.27000.org (abgerufen am 23.10.2021).

[41] International Organization for Standardization. ISO/IEC TR 27019:2017, 2017.

[42] Bundesamt für Justiz. Gesetz für den Ausbau erneuerbarer Energien. https://www.gesetze-im-internet. de/eeg_2014/ (abgerufen am 23.10.2021).

[43] Bundesamt für Justiz. Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen 1. https://www.gesetze-im-internet.de/messbg/ (abgerufen am 23.10.2021).

[44] Bundesamt für Justiz. Gesetz über die Elektrizitäts- und Gasversorgung. https://www. gesetze-im-internet.de/enwg_2005/ (abgerufen am 23.10.2021).

[45] Bundesamt für Justiz. Netzausbaubeschleunigungsgesetz Übertragungsnetz (NABEG). https://www. gesetze-im-internet.de/nabeg/BJNR169010011.html (abgerufen am 23.10.2021).

[46] Bundesamt für Justiz. Verordnung über den Zugang zu Elektrizitätsversorgungsnetzen. http://www. gesetze-im-internet.de/stromnzv/index.html (abgerufen am 23.10.2021).

[47] Bundesamt für Sicherheit in der Informationstechnik. BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 6. September 2021 (BGBl. I S. 4163) geändert worden ist, 2021.

[48] Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutz. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (abgerufen am 23.10.2021).

[49] Bundesamt für Sicherheit in der Informationstechnik (BSI). Zertifikatsnachweise nach § 25 MsbG. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/ Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/Zertifikatsnachweise-nach-Par-25-MsbG/zertifikatsnachweise-nach-par-25-msbg.html (abgerufen am 11.10.2021).

[50] Bundesamt für Sicherheit in der Informationstechnik (BSI). Zertifizierte Produkte – Intelligente Messsysteme. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/Zertifikate24Msbg/produkte.html (abgerufen am 11.10.2021).

[51] Bundesamt für Sicherheit in der Informationstechnik (BSI). Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). https://www.bsi.bund.de/DE/Das-BSI/ Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html (abgerufen am 23.10.2021).

[52] Bundesamt für Sicherheit in der Informationstechnik (BSI). Migration zu Post-Quanten-Kryptografie – Handlungsempfehlungen des BSI. Technical report, 2020.

[53] Bundesamt für Sicherheit in der Informationstechnik (BSI). Stufenmodell zur Weiterentwicklung der Standards für die Digitalisierung der Energiewende, 2020.

[54] Bundesamt für Wirtschaft und Energie (BMWi). Barometer Digitalisierung der Energiewende: Berichtsjahr 2020. Technical report, 2020.

[55] Frank W Geels, Siddharth Sareen, Andrew Hook und Benjamin K Sovacool. Navigating Implementation Dilemmas in Technology-Forcing Policies: A Comparative Analysis of Accelerated Smart Meter Diffusion in the Netherlands, UK, Norway, and Portugal (2000-2019). Research Policy, 50(7):104272, 2021.

[56] Craig Gentry. A Fully Homomorphic Encryption Scheme. Stanford University, 2009.

[57] PHYSEC GmbH. IoTree – IoT Anwendungen mit höchster Sicherheit, zuverlässiger Konnektivität und einfacher Integration. https://www.physec.de/iotree/, 2021 (abgerufen am 29.11.2021).

[58] GEODE Working Group Smart Grids. GEODE REPORT: Bringing Intelligence to the Grids, 2013.

[59] Lov K Grover. From Schrödinger's Equation to the Quantum Search Algorithm. Pramana, 56(2):333–348, 2001.

[60] Swantje Gährs, Julika Weiß, Hannes Bluhm, Elisa Dunkelberg und Jannes Katner. Erkenntnisse zu Umweltwirkungen von Smart Metern: Erfahrungen aus dem Einsatz von Smart Metern in Europa. Umweltbundesamt, 2021.

[61] Martin Henze, Jens Hiller, Oliver Hohlfeld und Klaus Wehrle. Moving Privacy-Sensitive Services from Public Clouds to Decentralized Private Clouds. In: 2016 IEEE International Conference on Cloud Engineering (IC2E) Workshops, 2016.

[62] Martin Henze, Jens Hiller, René Hummen, Roman Matzutt, Klaus Wehrle und Jan Henrik Ziegeldorf. Network Security and Privacy for Cyber-Physical Systems. In: Houbing Song, Glenn A. Fink und Sabina Jeschke (Hrsg.). Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications. Wiley-IEEE Press, 2017.

[63] Daemen Joan und Rijmen Vincent. Specification for the Advanced Encryption Standard (AES), 2001.

[64] Europäische Kommission. Verordnung (EU) 2017/1485 der Kommission vom 2. August 2017 zur Festlegung einer Leitlinie für den Übertragungsnetzbetrieb. https://eur-lex.europa.eu/legal-content/DE/ TXT/PDF/?uri=CELEX:32017R1485&from=LT (abgerufen am 23.10.2021).

[65] Nikos Komninos, Eleni Philippou und Andreas Pitsillides. Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. IEEE Communications Surveys & Tutorials, 16(4):1933–1954, 2014.

[66] Tim Krause, Raphael Ernst, Benedikt Klaer, Immanuel Hacker und Martin Henze. Cybersecurity in Power Grids: Challenges and Opportunities. Sensors, 21(18), 2021.

[67] Robert M Lee, MJ Assante und T Conway. Crashoverride: Analysis of the Threat to Electric Grid Operations. Dragos Inc., March, 2017.

[68] Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Müllmann, Oliver Hohlfeld und Klaus Wehrle. A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. In: Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC), 2018.

[69] Roman Matzutt, Benedikt Kalde, Jan Pennekamp, Arthur Drichel, Martin Henze und Klaus Wehrle. CoinPrune: Shrinking Bitcoin's Blockchain Retrospectively. IEEE Transactions on Network and Service Management, 18(3), 2021.

[70] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker und Jonathan Turner. OpenFlow: Enabling Innovation in Campus Networks. ACM SIGCOMM Computer Communication Review, 38(2):69–74, 2008.

[71] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Decentralized Business Review, S. 21260, 2008.

[72] Sarra Naoui, Mohamed Elhoucine Elhdhili und Leila Azouz Saidane. Enhancing the Security of the IoT LoraWAN Architecture. In: International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), S. 1–7. IEEE, 2016.

[73] Oberverwaltungsgericht Nordrhein-Westfalen. Stopp der Einbauverpflichtung für intelligente Messsysteme (Stromzähler) im einstweiligen Rechtsschutzverfahren – Aktenzeichen 21 B 1162/20.

[74] National Institute of Standards and Technology (NIST). NIST Standards. https://www.nist.gov/standards (abgerufen am 23.10.2021).

[75] Publications Office of the EU. Clean Energy for All Europeans. 2019.

[76] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca und J. Folgueira. Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges. IEEE Communications Magazine, 55(5):80–87, 2017.

[77] Ray A Perlner und David A Cooper. Quantum Resistant Public Key Cryptography: A Survey. In Proceedings of the 8th Symposium on Identity and Trust on the Internet, S. 85–93, 2009.

[78] Mohammad Shahriar Rahman, A. Basu und S. Kiyomoto. Decentralized Ciphertext-Policy Attribute-Based Encryption: A Post-Quantum Construction. Journal of Internet Services and Information Security (JISIS), 7:1–16, 2017.

[79] Philipp Richard, Sara Mamel uand Lukas Vogel. Blockchain in der integrierten Energiewende, 2019.

[80] Ramon Sanchez-Iborra, Jesús Sánchez-Gómez, Salvador Pérez, Pedro Fernández, José Santa, José Hernández-Ramos und Antonio Skarmeta. Enhancing LoRaWAN Security through a Lightweight and Authenticated Key Management Approach. Sensors, 18(6):1833, 2018.

[81] Luca Lo Schiavo, Maurizio Delfanti, Elena Fumagalli und Valeria Olivieri. Changing the Regulation for Regulating the Change: Innovation-Driven Regulatory Developments for Smart Grids, Smart Metering and E-Mobility in Italy. Energy policy, 57:506–517, 2013.

[82] Martin Serror, Sacha Hack, Martin Henze, Marko Schuba und Klaus Wehrle. Challenges and Opportunities in Securing the Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 17(5), 2021.

[83] Konark Sharma und Lalit Mohan Saini. Power-Line Communications for Smart Grid: Progress, Challenges, Opportunities and Status. Renewable and Sustainable Energy Reviews, 67:704–751, 2017.

[84] Peter W Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM review, 41(2):303–332, 1999.

[85] David Silver, Aja Huang, Chris J Maddison, Arthur Guez, Laurent Sifre, George Van Den Driessche, Julian Schrittwieser, Ioannis Antonoglou, Veda Panneershelvam, Marc Lanctot et al. Mastering the Game of Go with Deep Neural Networks and Tree Search. Nature, 529(7587):484–489, 2016.

[86] Carlo Stagnaro und IB Leoni. Second-Generation Smart Meter Roll-Out in Italy: A Cost-Benefit Analysis. Eurelectric Power Summit, 2019.

[87] Bernd Sörries, Stefano Lucidi, Lorenz Nett und Matthias Wissner. Gutachten Digitalisierung der Energiewende Topthema 3: TK-Netzinfrastruktur und TK-Regulierung, 2018.

[88] The Zeek Project. The Zeek Network Security Monitor. https://zeek.org, 1994.

[89] VDE: Forum Netztechnik/Netzbetrieb. Lastenheft Steuerbox: Funktionale und konstruktive Merkmale – Version 1.3. Technical report, 2021.

[90] Lukas Vogel, Philipp Richard, Michael Brey, Sara Mamel und Konstantin Schätz. Künstliche Intelligenz für die integrierte Energiewende, 2019.

[91] Wazuh Inc. Wazuh The Open Source Security Platform. https://wazuh.com, 2015.

[92] Gavin et al. Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, 151(2014):1–32, 2014.

[93] Wei Xiang, Kan Zheng und Xuemin Sherman Shen. 5G Mobile Communications. Springer, 2016.

[94] Xueying Yang, Evgenios Karampatzakis, Christian Doerr und Fernando Kuipers. Security Vulnerabilities in LoRaWAN. In: IEEE/ACM Third International Conference on IoT Design and Implementation (IoTDI), S. 129–140. IEEE, 2018.

[95] Ilsun You, Soonhyun Kwon, Gaurav Choudhary, Vishal Sharma und Jung Seo. An Enhanced LoRaWAN Security Protocol for Privacy Preservation in IoT with a Case Study on a Smart Factory-Enabled Parking System. Sensors, 18(6):1888, 2018.

[96] Mark Zeller. Myth or Reality – Does the Aurora Vulnerability Pose a Risk to my Generator? In: 2011 64th Annual Conference for Protective Relay Engineers, S. 130–136. IEEE, 2011.

[97] Barret Zoph, Vijay Vasudevan, Jonathon Shlens und Quoc V Le. Learning Transferable Architectures for Scalable Image Recognition. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, S. 8697–8710, 2018.

dena
Deutsche Energie-Agentur

www.dena.de