dena
German Energy Agency

Future Energy Lab

dena ADVISORY OPINION

EnerCrypt

Cyber Innovations for the Secure Energy System of the Future

Legal information

Publisher:
Deutsche Energie-Agentur GmbH (dena)
German Energy Agency
Chausseestrasse 128 a
10115 Berlin, Germany
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

Authors:
Mathias Böswetter, dena

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

Image credits:

shutterstock/TippaPatt

Last updated:

12/2021

Please cite this publication as follows:

Deutsche Energie-Agentur (Publisher) (dena, 2021) “EnerCrypt – Cyber Innovations for the Secure Energy System of the Future”

Federal Ministry
for Economic Affairs
and Climate Action

This publication is issued on behalf of the Federal Ministry for Economic Affairs and Climate Action. The German Energy Agency (dena) assists the Federal Government in various projects to implement the energy and climate targets in the context of the energy transition.

Table of contents

Foreword

Cyber security must be innovative to meet the needs of the energy transition. The EnerCrypt report by the German Energy Agency (dena) investigates which innovative potential the energy transition holds for cyber security – and how much it will depend on cyber innovation to prevent the process of transforming the energy system falling prey to burgeoning threats from the cyber realm. The report is thus intended to stimulate discussion on the issue of cyber security in the energy industry from an innovative perspective and to highlight its significance in structuring the energy transition.

So far, a different appreciation has prevailed in this highly regulated sector: cyber security is, from the perspective of the energy industry, primarily a factor that is determined by compliance and certification and that incurs costs and expenditures. Viewed from the regulator's side, the provisions set out in the relevant laws (IT Security Act 2.0 (IT-SiG 2.0), BSI Act (BSIG) and Energy Industry Act (EnWG)) and ordinances (Ordinance on the Determination of Critical Infrastructures (BSI-KritisV)) adhere to a systemic concept of accumulated individual risks that require certification for grid operation or power generation. According to BSI-KritisV or EnWG, energy installations only become critical factors in supplying the general public if they exceed certain threshold values[1] or, as a separate factor, are deemed (grid operators according to the EnWG) so critical that disruption would endanger the supply of electricity or gas to the population at large. This means, by inverse logic, that systemic risks can only be determined following the failure of such KRITIS facilities.

But the energy transition comes with a fresh set of challenges for the protection of critical infrastructure within the energy system: the overall systemic risk of the energy system cannot simply be grasped as the aggregate sum of its 'KRITIS parts'. Equally, it would be misguided to address this risk just by progressively lowering the threshold values, as doing so would make the expenses incurred for certifying an information security management system (ISMS) neither economical nor purposeful. An ISMS uses a complex process to ensure compliance with protection goals such as confidentiality, integrity and availability in organisations with considerable technical and human resources.

While cyber security has mainly prioritised ensuring the safety of large-scale thermal power plants and grids so far – and primarily medium and high-voltage grids for which certification seems reasonable and purposeful – the focus is now shifting to include the protection of decentralised plants and distribution grids as well. Firstly, power generation is increasingly moving in the direction of renewable energy sources connected to the distribution grids. Secondly, the volatile generation patterns among these kinds of producers and the bidirectional capacity flows caused in the distribution grids by new actors such as prosumers or flexumers, demand greater digitisation to meet the growing demand for information in the increasingly complex process of grid monitoring and control. In connection with the Smart Meter Gateway roll-out, the degree of digitisation will rise significantly over the years ahead due to the ramp-up of electromobility and the provision of flexibility through controllable loads such as heat pumps.

Against this backdrop of digitisation and decentralisation, a paradigm shift will be necessary to address cyber security in a manner that meets the needs of the energy transition: it is no longer possible to guarantee

[1] The BSI KRITIS Ordinance defines threshold values above which its provisions will apply to a market partner. For instance, power generating plants used in the supply of electricity fall under BSI-KritisV if its generating capacity is greater than 104 MW. [47]

protection of the energy system with a relatively manageable number of facilities in the extra-high and high-voltage range and an approach that is based solely on certifications. The significance of cyber attacks for system security will also grow considerably going forward at all grid and power generation levels due to the increasingly connected physical and information technology. What has been lacking in this context is an approach that consistently merges the needs of operating technology and IT (IT/OT convergence) to create end-to-end, integrated operational security.

Finally, the energy transition will connect millions of new, partially decentralised plants to the distribution grids, which in turn will impact grid security, as their level of criticality differs from that of large-scale power plants: while individual producers and loads may initially be perceived as inherently uncritical, they may nonetheless, in an aggregate sense, pose a threat to system security due to the aggravated interactions and cascade effects in a distribution grid characterised by bidirectional load flows. On the other hand, the increasing decentralisation and the associated use of many different systems may also give rise to greater resilience in the overall system.

The central proposal of the EnerCrypt report states that in order to close the gap between the certified ISMS of KRITIS facilities and new systemic risks that may arise from decentralisation, connectivity and smaller structures, cyber security must be based on digital innovations if it wishes to meet the needs of the energy transition. This form of cyber security is hence also dependent on innovative companies and platforms that build networks and connections between the energy and digital industries. Demonstration and pilot projects that promote networking and close exchange between relevant actors are imperative, especially given the wide and heterogeneous range of stakeholders in the energy sector. More determined action should also be taken in the light of current geopolitical developments. A sensible first step would be to establish cross-sectoral dialogue so that a group of experts from both fields could define specifically the relevant questions. This would help to identify the essential tasks and hence determine what needs to be done next. The tasks are wide and varied and must ultimately be pushed and implemented by the actors themselves as a means of protecting and upgrading their own facilities and services. An essential aspect in this regard is to create an interdisciplinary exchange initiative, with the aim of first systematically mapping all areas of activity and of building the basis for an innovative learning environment.

Cyber innovations and a fresh sense of urgency in the energy industry. In the energy industry, however, digital innovations and innovative companies are still focusing on new business models. The provision of data in the energy industry is a priority issue in this regard: data is increasingly perceived as the actual raw material to create value in the energy industry going forward. Hence, the funding of digital innovations and innovative companies has reflected to a certain degree how established energy industry actors have deployed data-driven business models in the hope of overcoming the uncertainty that has marred the last two decades due to market liberalisation and falling energy prices. Ultimately, then, it represents the attempt by these actors to reinvent their roles, for instance as data platform operators. With this in mind, other areas of digital innovation – also cyber security – have remained largely invisible so far and have thus been unable to encourage suitable sectors to become involved in the energy industry in a manner that has stimulated very fruitful exchange between the energy and digital industries in the area of new business models.

Another sense of urgency has emerged for the energy industry over recent weeks and months, shining a far brighter spotlight on the issue of cyber security in the energy industry: firstly, there has been a steady rise in the frequency and severity of cyber attacks on the IT infrastructures of municipal utilities (e.g. Schwerin at the end of 2021), their IT service providers (e.g. KISTERS AG at the end of 2021) or on other companies involved in the energy transition (e.g. VESTAS at the end of 2021). Vulnerabilities such as Log4J also created further

uncertainty across all sectors and industries at the end of last year. Secondly, an increasingly fraught geopolitical situation has led to a rapid increase in energy prices. The energy industry is therefore facing fresh challenges that will, and must necessitate a more urgent approach towards innovation. The war in Ukraine has demonstrated that cyber attacks on state institutions and companies must be taken seriously as a present and serious threat to critical infrastructures and hence to society as a whole.

The deployment of wiper malware, which is used for the irretrievable erasure of data, represents a new quality and politicisation of cyber attacks. Unlike the widely publicised ransomware attacks of recent months and years, wiper malware is not used to solicit ransom in the form of cryptocurrencies and aims instead at the complete and irretrievable deletion of data to render the IT or OT unusable. Even an accidental spillover of this wiper malware to Germany might have serious effects on the energy industry and critical infrastructures.

Bearing this in mind, the EnerCrypt report is coming at precisely the right time: for Future Energy Lab and the German Energy Agency, it marks the start of a series of projects and initiatives on the issue of cyber security for the energy transition and cyber innovations. These projects and initiatives are intended to accompany the envisaged energy independence by ensuring digital sovereignty in the cyber realm and by establishing cyber security structures that meet the needs of the energy transition. Taken together, these elements lay the foundation for successfully implementing the Federal Government's goal of achieving geopolitical independence in the electricity sector by 2035 – including the associated degree of connectivity and digitisation.

With kindest regards,

Andreas Kuhlmann
Chief Executive
at German Energy Agency (dena)

Philipp Richard
Head of Division, Digital technologies and start-up ecosystem at German Energy Agency (dena)

1 Introduction

The energy system is vital to the economic, social and political life of a modern industrial state. However, the increasing and necessary digitisation of the energy system within the energy transition also leads to continuous expansion in potential targets and attack vectors. The 2015 cyber-attack on the Ukrainian distribution grid infrastructure in particular – which affected hundreds of thousands of people – demonstrates that critical energy infrastructure is increasingly becoming an attractive target. The importance of cybersecurity for the energy sector is therefore growing all the time.

Operators in the Federal Republic of Germany must demonstrate a minimum level of IT security in accordance with the IT Security Act and the Energy Industry Act and implement appropriate state-of-the-art organisational and technical measures to protect their IT systems, components and processes in order to ensure the functionality of critical energy infrastructures. Moreover, notification obligations stipulate that critical IT incidents – especially cyber-attacks – must be reported to the Federal Office for Information Security (BSI). It is important to take note nonetheless that the energy transition is precipitating an increasing transformation of the energy system towards smaller, decentralised power generating plants to which the requirements for critical infrastructures do not apply, although they represent, in an aggregate sense, a significant risk to the security of supply in the Federal Republic of Germany as a target for cyber-attacks.

In order to close this gap, for instance, the Smart Meter Gateway (SMGW) for secure metering point operation has created an infrastructural foundation for cyber-secure digitisation beyond the scope of formal critical infrastructures. Faced with the foreseeable rise in digitisation and connectivity, for example through renewable energy, e-mobility, heat pumps and IoT solutions – especially at lower voltage levels – the requirements for the IT security of the SMGW were specified in such a way to enable both cyber innovations and accommodate a constantly shifting threat landscape.

> This report aims to identify and evaluate key trends and developments that could exploit or harness this scope for innovation as a means of creating cyber innovations that are of increased relevance to the energy sector and in doing so contribute to the overarching goal of shaping a secure energy system for the future. Besides the operation of metering points, the report uses future digital technologies to investigate trends and developments to strengthen operating resources and ICT infrastructure within the energy industry from the perspective of their cyber security and with a particular focus on the distribution grid level.

As a basis for the consideration of cyber innovations for the secure energy system of the future, Chapter 2 presents and classifies trends and developments addressing digitisation and future technologies in the energy industry. Current and future trends within the energy industry are discussed in a first step to provide an initial overview of projected requirements, use cases and challenges (Section 2.1). This is used as a basis to identify technologies from the areas of digital communication (Section 2.2) and general future technologies (Section 2.3) that would enable secure digitisation and application implementation. Concluding this section is a discussion and evaluation of the various concepts to strengthen the cyber security of technical operating resources, with due consideration of particular requirements within the energy industry (Section 2.4).

Chapter 3 draws on this to identify and discuss innovative use cases within a mercurial threat landscape. It begins by investigating specific use cases for the energy industry from the perspective of both customers and grid operators (Section 3.1). Historical attacks are then analysed and clear recommendations for action and requirements with regard to cybersecurity derived as a basis for evaluating the cyber-secure implementation of these specific use cases (Section 3.2). This analysis concludes with a discussion of national rules and regulations concerning the cybersecurity of critical energy systems (Section 3.3).

Chapter 4 focuses on the potential of cybersecurity to drive innovation within the energy industry. For this purpose, various areas of application are used initially to determine the status quo of energy industry innovations in the Federal Republic of Germany (Section 4.1). A particular focus is placed on SMWG infrastructure as a case study to consider the necessary communications infrastructure (cf. Section 4.2). This chapter concludes with a discussion of the feasibility and possible technologies for transitioning towards a cyber-secure environment in the energy sector, especially with a view to IT security and data protection requirements (Section 4.3).

Adding practical experience obtained both nationally and internationally, Chapter 5 uses the insights to analyse funding policy options in Germany. The insights were acquired in particular from the contents of two workshops that were held with representatives from industry and politics while preparing this report. The chapter begins by discussing both general and specific funding policy measures (Section 5.1). It then presents international experience with infrastructures that are comparable to the SMGW infrastructure in Germany as well as further experience with cybersecurity in the energy industry (Section 5.2). The chapter rounds off the report with a discussion of specific solution strategies to promote innovation in Germany (Section 5.3).

The report ends in Chapter 6 with a comprehensive summary of acquired insights and analyses. In particular, it draws an overarching conclusion that also provides an outlook on the challenges facing the German energy industry in the near and more distant future. The insights and analyses contained in this report can help in designing meaningful and purposeful measures to overcome these challenges.

> The secure electricity grid of the future will be built on several pillars, and all stakeholders must be involved in and contribute to this process. Innovations in energy technology that address decentralisation of the electricity grid, the digitisation of surrounding IT and Operational Technology networks and end-to-end cybersecurity in all these areas are indispensable factors for the viable design and implementation of the energy transition, as well as for enabling changed consumption patterns and new value-added services and use cases. This report discusses and analyses the status quo, the upcoming challenges and added values as well as tools from the field of IT that are useful for – or even crucial to – this process.

2 Trends and developments in the digital energy industry

After embarking on the energy transition, Germany has worked towards the goal of modernising and digitising the energy industry and minimising negative environmental impacts for several decades. Important core aspects include, on the one hand, the growing significance of (decentralised) systems according to the Renewable Energy Sources Act (EEG) and the accommodation of fluctuating demands on the electricity grid due to new consumption patterns on the other. Among other things, these are caused by the increasing use of electromobility, which places additional demands on (digital) flexibility management, grid monitoring and stabilisation, as well as adjustable, customer-centric tariff models, in addition to the challenges associated with expanding the technical facilities within the energy industry.

This transformation of the digital energy industry is necessarily accompanied by increasing demands for new technologies, both for digital communication and practical applications. Energy grids are classified as critical infrastructure (KRITIS), so a particular focus is inevitably placed on the cyber security of technologies that are designed to protect the energy system of the future from sophisticated cyber threats. These include the installed communications technologies, cryptographic methods and overarching technologies such as grid control, process monitoring and Smart Meter Gateways (SMGWs).

To ensure the cyber security of energy systems going forward, it is important to analyse current and future developments and trends in the energy industry, determine the associated requirements and use cases, and identify and understand technologies that could be useful in their realisation. This chapter begins by outlining current and future developments in the energy industry itself (Section 2.1), thus generating an initial overview of future requirements, use cases and challenges. This is used as a basis to present technologies from the areas of digital communication (Section 2.2) and general technologies (Section 2.3) that could enable secure digitisation and application implementation. The chapter ends with a discussion of the various concepts to strengthen the cyber security of technical operating resources (Section 2.4), whereby the associated concepts and discussed technologies are evaluated with due consideration of particular requirements within the energy industry.

2.1 Trends and developments in the energy industry

Distribution and transmission system operators are facing a paradigm shift that is taking place at a rate of knots within the European energy industry as part of the energy transition. This transformation is characterised mainly by the increasing closure of thermal systems plants and a widespread expansion of renewable energy generating units – with photovoltaics and wind power at the forefront – that come with more volatile generation patterns. In Germany, the burgeoning use of electricity generation from renewable energy generating units is also reflected in the current figures, which reveal that the electrical energy obtained from the energy sources of geothermal energy, photovoltaics, offshore/onshore wind power, biomass, municipal waste and hydroelectric power had, by 2020, risen by a factor of 2.4 compared to 2010 [33]. In 2020, onshore wind farms and photovoltaic systems made a significant contribution to this energy source mix, delivering 105.3 billion kWh and with 50.4 billion kWh of electrical energy, respectively. [33]. Renewable energy generating units accounted for a shared of 44.2 per cent of the total energy source mix in Germany in 2019 [32].

These circumstances and other key framework conditions defined by climate protection targets (e.g. Clean Energy Package [75]) lead to further targets and challenges for the energy sector, which are grouped into the areas of reducing greenhouse gas emissions, increasing energy and resource efficiency, promoting emission-free technologies and furthering the expansion of renewable energy generating units. Improving the flexibility of the (pan-European) energy industry and enabling non-discriminatory access to the electricity markets for new players are key elements in achieving these targets. This may create additional potential to overcome the fresh challenges presented by an increasingly unsteady energy yield. Measures to balance supply with energy demand, consumption and storage might then include the use of flexibilities in energy supply and intelligent grid management concepts as means of ensuring the stability and security of supply throughout the energy system. A crucial aspect in meeting these challenges will be to ensure methodical exploitation of these flexibilities in the energy system, accompanied by maximised use of renewable energy generating units with efficient deployment of current and new infrastructures, which are characterised for example by the more widespread integration of information and communication technology (ICT).

Fresh challenges for grid operation. It follows, therefore, that the growing use of volatile, renewable energy sources has fundamental and far-reaching consequences for grid operation. The required grid observability and the strategies to maintain system stability and security mean that transmission system operators (TSO) increasingly need updated information due to new market participants and actors such as aggregators, who, acting in an organisational capacity, bundle the electricity generated by decentralised providers and market the supply on the balancing energy market as aggregated flexibilities. Distribution system operators (DSO) are tasked with ensuring secure operation of the distribution grid. Bidirectional power flows caused by the growing number of decentralised power generating units and highly volatile prosumers in distribution grids can take the systems to their operating limits in which the permissible line or grid capacities and the technical limits for voltage range and resource utilisation are reached in increasingly short intervals at local level.

Predicting the network condition is becoming more and more important for distribution system operators – especially in regard to their ability to exert direct influence by accessing balancing energy or through congestion management – due to the volatile feed-in levels associated with renewable and weather-dependent generators, but also consumers (in the sense of negative balancing energy) This means that the design and implementation of concepts for flexibility deployment and a reliable, predictive detection and assessment system for bottlenecks within the distribution grid will also need to include measures to determine and forecast grid condition. These procedures for condition assessment are most frequently encountered in grids that possess a highly developed measurement infrastructure for maximum observability, as is the case in high-voltage and ultra-high voltage grids. At lower voltage levels, however, these estimation methods will then face an under-determined system with few validated measurements, which have little or no measurement infrastructure. The focus is therefore placed on generating condition data for lower voltage levels. In the long term, the need to ensure observability and potentially even management of medium and low-voltage grids and their connected generators and loads will be an essential boundary condition for improving efficiency in the system stability and security of ancillary services provided by grid operators. The technology in some distribution grids – from a historical perspective – was not designed to cope with the increasing prevalence of decentralised power generation. In particular, the basic functionalities of technical protection concepts in distribution grids use static parameters and are built on classic distribution grid structures with a unidirectional power flow, which means that intermediate feeds and refeeds into the higher grid level are largely absent. Flexible, event-driven adaptation of configuration

parameters or functional scopes is not included and is currently not possible from the viewpoint of data generation, transmission and processing in the field. Altering the grid topology to ease the load, for instance in response to fluctuating load flows, might produce states that cannot be controlled using the classic protection concepts that are currently in place. Potential technical solutions to meet this challenge will go hand in hand with adaptive and connected grid protection concepts that adapt the protection parameters in the event of power flow shifts and topology changes and in doing so ensure safe operation. The grid expansion measures that accompany the implementation of the smart grid paradigm must include a coherent upgrade of protection systems.

Ancillary service contributions from the distribution grid. In future, distribution grids will take on an increasing share in the provision of ancillary services (voltage and reactive power management, congestion management and supply restoration). Distribution system operators therefore carry more and more responsibility for coordinating the use of decentralised power generating plants in the provision of ancillary services. Associated with this is the need for involved actors – grid operators especially – to sync measures in emergency situations based on mutually recognised power generation and load assumptions, for instance within disruption and congestion management as well as redispatch. At present, redispatch interventions in power generating plants are only available to transmission system operators as a means of alleviating bottlenecks in their grids. But this capability should be made available for use in distribution grids in line with the principles of Redispatch 2.0 [35]. The envisaged liberalisation of the redispatch and balancing energy markets for generating units in magnitudes greater than 100 kW, as well as the use of redispatch or flexibility measures to eliminate bottlenecks in local or regional areas, will transform the load and power generating patterns among these new market participants. In future, the currently known methods and technologies for ensuring security of supply from the area of transmission grids will become increasingly relevant in rules to prevent critical situations in distribution grids. These include, in particular, power generation and load flow forecasts that can be used at short notice in distribution grid operations to determine and release available grid capacities and to initiate redispatch and flexibility measures under the conditions of increasingly market-oriented power generation and load patterns.

The markets for flexibilities that are beneficial to the grid are currently limited and largely restricted to the use of balancing power and redispatch at TSO level, as well as disconnectable loads at distribution system operator level. In future, these instruments will no longer be sufficient to balance load and power generation peaks in the grid and to ensure secure grid operation [31]. The deployment of flexibilities that are beneficial to the grid for the provision of ancillary services will increase going forward within the context of smart energy grid systems that place high demands on IT infrastructures, systems and processes. For this concept to be put into practice, grid operators must have access to ancillary services such as the provision of flexibilities to avoid grid congestion or the beneficial use of decentralised energy units for balancing group management in a manner that enables their contracting and control as needed. In turn, this requires the efficient marketing of all flexibilities from decentralised energy units that are beneficial to the grid through a form of dynamic aggregation that also enables very small systems to participate in markets, thus creating a flexibility portfolio comprising one or more aggregators. This would take participation by decentralised energy units in the energy market to a whole new level: they can offer their surplus energy as flexibility and in doing so, for instance, evolve from being just power generating plants that feed electricity into the grid and are switched off by the grid operator when critical grid conditions occur, into competitive decentralised energy units with active market participation. Flexibility can be used in a variety of ways: by the transmission system operator, for instance, to maintain system stability or by the distribution system operator to deal

with critical grid situations at local level. In this context, flexibility can also be used increasingly as a fast compensation method within a balancing group.

Market communication model. Moreover, both aspects can promote the Federal Government's targets of strengthening balancing group commitments and eliminating barriers to free competition in the marketing of flexibility options. Within this framework, the market communication model describes roles, areas and objects within the energy sector and how they relate to each other. Responsibilities and tasks as well as the functions of areas and objects are defined for each of the roles [34].

In addition, the circumstances and framework conditions arising from the energy transition will lead to increasing interaction between all players, such as transmission and distribution system operators, power plant operators, customers and consumers, prosumers and aggregators as well as exchanges. To establish coordinated processes of network and system management that guarantee stable and secure grid operation in the future, this growing interdependency will necessitate a more lively exchange of information via system-relevant communication channels that are independent of the public communication network. It follows that the electricity grids will have to cope with increasing data volumes and heterogeneous data sources going forward. This will involve remote connection of a considerable proportion of the electrical equipment for real-time access to system-relevant measured variables (e.g. grid frequency). Various segments of the energy sector are yielding big data that may potentially be valuable for utilities, grid operators and end-users. Big data algorithms and edge computing technologies are being applied to harness this information for a variety of purposes such as forecasting electricity supply and demand, condition estimation and grid control and for promoting participation in electricity markets.

New system architectures and technologies. The traditional organisation of energy systems implies a centralised architecture with the levels of power generation, transmission and distribution. In future, the growing prevalence of distributed power generating plants occupying different voltage levels may result in the development of more complex architectures for secure operation of the whole system on a global scale. Entirely decentralised architectures ensure that information is compartmentalised. Intervening actors do not require global information as a result, which offers interesting perspectives in the context of autonomous and isolated micro-grids as insular solutions. An alternative is to install multi-agent systems based on artificial intelligence (AI) methods using agent technology. This approach is usually suitable for complex challenges in which individual agents are tasked with identifying a solution to a global problem, either through cooperation or competition.

The increasing generating capacity from decentralised power generating plants in distribution grids – which is largely connected by means of inverters – leads firstly to less inertia in grid operation and secondly to the more complex task of ensuring stable grid operation, as each decentralised generation plant can actively influence the grid condition. Accordingly, this situation is becoming more acute for micro-grids, which creates fresh challenges that require innovative solution concepts such as the design of grid-connected and grid-forming inverters to match the generating capacity in micro-grids.

The energy transition and its associated new generation options based on renewable energy sources have created innovative opportunities for the sustainable generation of electricity. At the same time, though, fresh challenges are arising for grid operation, which must be dealt with by using sensors and actuators to expand transparency and management in the distribution grids. Not only must they meet the demands of grid operation, but also enable value-added services and sustainable use cases in the energy industry. This could involve the deployment of new technologies that, in the form of infrastructures, hardware or software, will play integral roles in the establishment of future energy information systems. To ensure that control, operational and trading requirements are dealt with efficiently and robustly at distribution level and to meet the challenges ahead, the scale and complexity of such changes to the system necessitate the introduction of more decentralised and flexible architectures, as well as support from advanced communication infrastructures. Advanced active control and operational management structures are needed. This must be built on an end-to-end solution approach for regional control systems in grid operation and the trading of energy and services on local markets. Combining this with new algorithms and cyber innovations would enable the timely detection of local bottlenecks (e.g. voltage bottlenecks or overloads in power feeds) and support the correction of global imbalances such as load balancing and frequency control.

2.2 Innovations in the area of digital communication

The increasing requirements outlined above and the growing volume of digital communication associated with power grids are already precipitating the conversion and expansion of suitable communication infrastructures. Aside from the requirements for transmission rates and costs, the security of communication and the transmitted data possesses particular relevance in this regard. This creates two central challenges for component and system manufacturers as well as grid operators (TSOs and DSOs):

1. selection of suitable communication technology; and
2. its protection from cyber-attacks.

Cyber-attacks in communication networks typically target the integrity of transmitted data as well as the availability of interfaces. This section collates current communication technologies from the field of wireless and wired communication and evaluates them in regard to their areas of application.

Many core components can be connected using proprietary, wired infrastructures, especially in TSOs and larger DSOs. The operation of dedicated fibre optic networks as well as networks based on power line communication is widespread. But this kind of infrastructure is not always available in the context of a smart grid. Smaller DSOs, municipal utilities or other, sometimes new players such as charging point operators do not always possess these infrastructures or the ability to use wired infrastructure from internet service providers (ISPs). The situation is similar in existing installations at TSOs for which a communication network connection was not planned. Furthermore, there are a number of use cases in which wired connection does not make sense for technical or economic reasons. Among them are projects in the field of the Internet of Things (IoT), including those by various municipalities to increase energy efficiency or optimise processes. Wireless communication networks are being used or even built in all of these cases.

There is an immense range of wireless technologies available. Others will soon be added to current technologies such as LTE, NB-IoT, GSM, TETRA, Long Range Wide Area Network (LoRaWAN), Sigfox and WLAN. 5G and LTE-M based on the recently awarded frequencies around 450 MHz are of particular importance to the energy industry.

Here, the heterogeneity of wired and wireless technologies extends over various dimensions that differ according to technical performance characteristics (data rate, latency, scalability), data sovereignty (an IPS's public network or proprietary operation) and other factors. Figure 2.1 shows an overview of technologies and their central properties. Although many technologies come with their own, sometimes proprietary methods of protecting against cyber-attacks, the framework conditions for secure operation are changing rapidly. Current regulations and requirements focus heavily on technical aspects, despite the highly volatile threat situation.

The following provides an initial overview of the key properties of various communication technologies and the challenges associated with protecting against cyber-attacks.

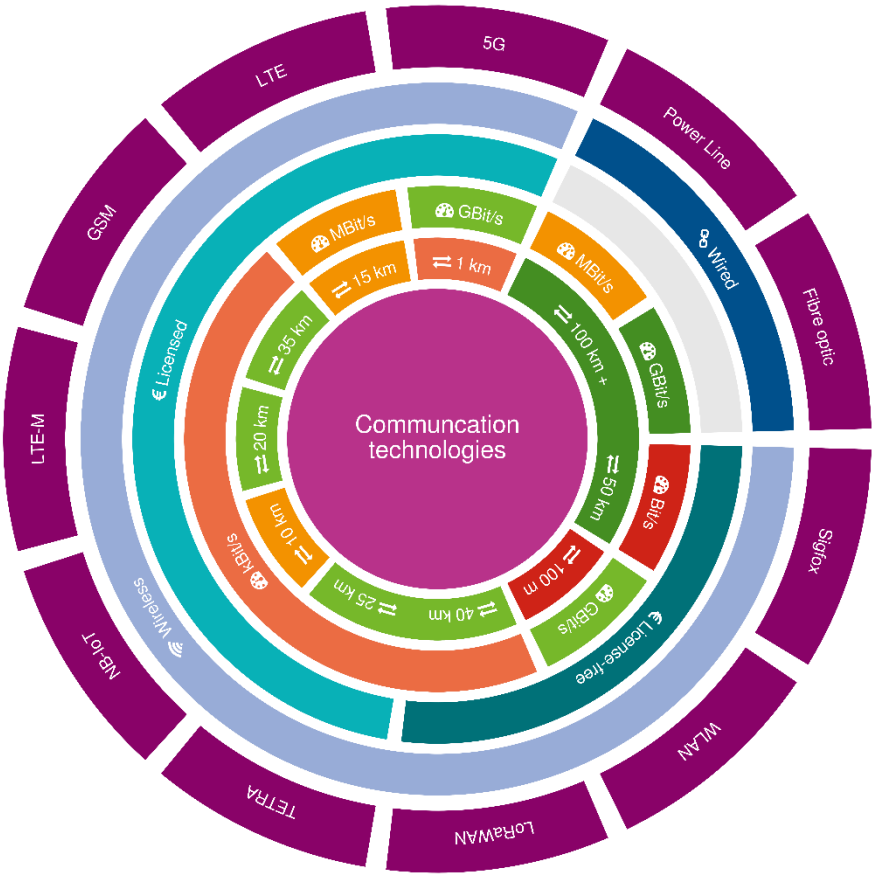

Figure 2.1: The communication technologies that are relevant to the energy industry can basically be divided into wireless and wired technologies. In addition, they come with different properties that relate to the availability of licenses, data rates and range. Other aspects such as security features, latency, construction and maintenance costs or energy requirements must always be considered as well.

2.2.1 Wired communication

Fibre optic networks enable symmetrical transmission rates of up to hundreds of GBit/s even over long distances, making them the only technology to exhibit these future-proof performance characteristics. The costs for the necessary optical fibres are relatively low. Civil engineering work and the specialist knowledge and tools needed to splice the connections are the main cost drivers. Common approaches to minimise dedicated civil engineering works include the use of available above-ground structures such as electricity pylons or the compulsory installation of an empty pipe during road construction. The high capacities of

optical fibres enable the implementation of other services in addition to the transmission of smart grid data, if necessary in cooperation with an internet service provider (ISP).

Power line communication utilises the existing electricity grid as its transmission medium and is available in narrowband and broadband versions, which differ hugely in regard to range and throughput. However logical it may seem to use the existing power grid as a transmission medium, doing so involves major challenges with regard to transmission stability. Electricity cables are not designed for data transmission and initial field tests showed somewhat sobering results [83].

Wired communication usually does not come with built-in security features. Instead it is up to the communication protocols to provide protection. Typical examples of this include virtual private networks (VPNs) or Transport Layer Security (TLS). A simple physical safeguard lies in the fact that installed fibre optic cables are usually difficult for an attacker to access. Suitable measures will generally detect the tapping or infiltration of packets.

2.2.2 Wireless communication

Wireless communication technologies that are currently being discussed for use in the smart grid – such as LTE, NB-IoT, GSM, TETRA, LoRaWAN, Sigfox, WLAN, 450 MHz LTE-M or 5G – are cellular networks. Cellular networks are characterised by point-to-multipoint connection architectures, in which each cell is implemented by a base station. Base stations require an exposed location, stable electricity supply and a connection to the communication network to forward the received data, which is usually realised using fibre optic networks.

The performance characteristics of the various communication technologies are largely determined by how advanced the technology is, the frequency it uses and the available bandwidth. In this regard, significantly higher range (cell size) and structural penetration are achieved at low frequencies under 1 GHz (e.g. 450 MHz LTE-M or LoRaWAN). But only limited bandwidth is available at low frequencies, which severely inhibits throughput and scalability (compared to 5G, for example).

Regulatory aspects of frequency use are another important distinction for wireless communication technologies. Technologies that are primarily used in mobile networks (LTE, NB-IoT, GSM, TETRA, 450 MHz LTE-M) operate on licensed frequency bands that are exclusively assigned to companies (e.g. mobile network providers, 450connect GmbH) at considerable cost. Although these investments have to be recouped, exclusive assignment also ensures that the networks are operated with guaranteed quality standards. Technologies such as LoRaWAN, Sigfox and WLAN use unlicensed frequency bands that are publicly accessible, subject to certain rules (e.g. maximum access time or maximum radiated power). While this free use reduces the cost of operation, it can also lead to frequencies becoming overloaded at certain locations, with serious implications for network stability.

5G, for example, offers high data rates with low latencies and existing network infrastructures of mobile phone companies are generally compatible for use. Disadvantages include the operating costs, the security of supply away from urban areas due to the low ranges and the loss of data sovereignty – even when using a dedicated virtual channel (‘network slice’). By contrast, LoRaWAN provides relatively large ranges at low operating costs, but exhibits a low data rate with high latencies. Overload situations may also occur due to the use of free frequencies. Existing regional networks can be drawn on in some cases, although in many cases it is necessary and sensible for energy grid actors to run a proprietary network.

Given the fact that electromagnetic waves are very difficult to shield against attacks, all wireless communication technologies possess internal security mechanisms, as described below using the examples of LoRaWAN, 5G and 450 MHz LTE-M.

LoRaWAN has security mechanisms on two layers [72]: between the sensors and the base station and between the sensor and the user application. Key exchange is one of the biggest challenges in this regard, and a successful attack has already been carried out [24, 37, 94]. Discussions are ongoing to identify mechanisms based on proprietary development [80] or standards such as TLS or DTLS (datagram Transport Layer Security) to protect LoRaWAN user data [57, 95]. The limited data rate and small activity time window present additional challenges, as current security protocols are often not optimised for narrowband connections [62].

The improved security in 5G mobile technology compared to the previous standards (LTE) is an important aspect. Particularly noteworthy factors in this regard include asymmetrically encrypted transmission of the mobile subscriber's cross-device identity (international mobile subscriber identity, IMSI), cryptographic confirmation of the mobile operator when roaming (authentication confirmation) and secure algorithms for the encryption of data traffic within the 5G infrastructure with mutual authentication of devices and networks. [76, 93].

LTE-M at 450 MHz is an important technology for the energy systems of the future in the Federal Republic of Germany. The decision by the Federal Network Agency to award dedicated 'frequencies for digitisation of the energy transition' [22] to 450connect GmbH[2] [23] opens the door to a completely redesigned wireless communication network for the energy industry. The most important feature of this planned network is the more favourable propagation characteristics at a frequency of 450 MHz compared to conventional mobile communication networks. Achieving nationwide coverage will require a far smaller number of base stations, which impacts favourably on investment and operational costs within project planning, while also enabling rapid implementation. Initial modelling tests have demonstrated that installing ten base stations could be sufficient for area-wide coverage in a large city like Düsseldorf [87]. Participation by regional energy providers would ensure prompt identification of required locations for base stations, if necessary.

The planned network is nevertheless facing a number of stiff challenges. At present, there is a lack of large-scale measurements for a final evaluation of building penetration (down to basement level). The establishment and operation of such a secure, highly available network for critical infrastructure is challenging from an engineering perspective as well. A higher degree of automation through software-defined networking (SDN) and network functions virtualisation (NFV) could help with this process. Nonetheless, it remains imperative to draw on genuine expertise from day one, especially in the area of security. In general, the application of security by design methods from the project's inception would help with the consistent realisation of cyber security.

The need to improve internet coverage in rural areas has placed satellite systems firmly back on the agenda. A distinction must be made here between geosynchronous Earth orbit (GEO), medium Earth orbit (MEO) and low Earth orbit (LEO). GEO satellite systems have been around for decades, but with the significant disadvantage that the runtime of a message is at least 500 ms, an unacceptable length for many use cases. MEO and LEO systems (nano-satellites) circle at a far lower orbit (between 160 km and 2,000 km), which shortens the orbital period considerably.

[2] "450connect GmbH is an association of four shareholders: the previous sole shareholder Alliander AG, a consortium of regional energy providers, E.ON and the utility alliance 450 MHz, which includes several municipal utilities and energy and water providers." [23]

Communication between satellites has also been proposed to reduce the transmission needed between Earth and space. Communication with satellite systems requires complex and expensive modems (satellite dishes) that only work with a clear view of the sky.

2.2.3 Dedicated and public infrastructure

In principle, the use of wired or wireless public infrastructure made available by an ISP or the construction of dedicated, proprietary infrastructure – either managed by the owner or external parties – would be viable options for the operation of suitable systems. Potential cost savings and complete data sovereignty are prompting various actors involved in the energy system of the future to consider the independent construction and operation of their own independent communication network. A dedicated network potentially offers advantages in the areas of IT security and quality of service (QoS) compared to a public infrastructure that is used and occupied by significantly more participants. But any project of this kind would be challenging due to insufficient know how and experience. A comprehensive, modern and robust security concept is indispensable for critical infrastructures in particular – and ISPs can draw on the benefits of considerably greater experience in this field.

In this regard, wired networks come with the advantage of being far less susceptible to sources of interference and attacks originating from parties with network access. But the implementation of security features in these networks is obligatory as well. The cost of creating large-area coverage by means of a wired network tends to be higher than for wireless networks, and the cost benefit associated with wireless networks is also accompanied by greater flexibility in the connection of new devices. Factors such as lower bandwidths, higher latencies, vulnerabilities to interference factors – both in normal operation and within the framework of attacks – and the potential use of unlicensed frequency bands are specific challenges when dealing with wireless networks. Moreover, the limited bandwidth and packet size – depending on the technology – also prevent or at least hamper the use of standard security procedures.

All the same, the special challenges of operating dedicated infrastructure, especially for its secure design and implementation, are offset by a number of advantages as well. Complete control over the network enables far greater flexibility, which makes it easier to respond to events and implement planned changes both purposefully and quickly. QoS guarantees can also be put in place, as the communication pathways and scopes are known and controllable.

Dedicated networks are superior to public networks in terms of software, configuration and physical infrastructure as their specific structures and arrangements are optimised for a particular use case, assuming they are operated with the necessary expertise. By licensing the 450 MHz frequency band to the energy industry, LTE-M provides a potentially rewarding opportunity to build a nationwide wireless network. The comparatively small number of base stations required in this regard reduces the costs of building, maintaining and operating the network, and the specific radio technology is compatible with a large number of use cases.

The process of selecting a suitable communication technology will always hinge on the intended area of application. While wired technologies – fibre optics especially – come with or support the best technical properties and security features, wireless communication technologies possess significant advantages in terms of mobility, flexibility and cost requirements. With a view to future viability, it is generally advisable to define greater requirements than would be strictly necessary at present. In addition to greater requirements placed in the application itself – e.g. the data rate or latency – the security mechanisms going forward may also place higher demands on the communication technology than is currently the case. Secure communication is an absolute prerequisite for the long-term viability of electricity grids and the energy industry as a whole and must be taken into account and implemented at all times with the requisite degree of foresight.

2.3 Cyber innovations through the use of general future technologies

The communication technologies presented above are basic building blocks for implementing a plethora of digital applications within a secure framework. Bearing in mind that digitisation, fresh use cases and the requirements associated with the energy transition are inevitably accompanied by a rise in data volumes, safety-critical applications and new communication patterns, safety and application-oriented technologies also possess relevance within a broader context than just communication. In the area of information technology (IT), both new and established technologies offer potential for enabling innovative use cases within a secure and functionally versatile environment. The following section initially provides an overview of technologies that could be used to implement applications of this kind in the energy industry. It then discusses technologies whose particular properties would contribute decisively to cyber security.

2.3.1 Pioneering technologies for application-oriented innovations

New use cases within the energy industry are built to a significant extent on the decentralisation of energy production and the availability of new technologies such as SMGW infrastructure. Optimisation of personal consumption, local energy markets and flexible load and charge management are just a few of the use cases that require innovative technologies. In this regard, it is imperative to strike a balance between openness and transparency, as well as between aspects such as privacy and maximum security. While Section 3.1 describes specific use cases, the following elaborations present an overview of technologies with properties that may be relevant to their actual implementation.

Intelligent measuring systems. The ongoing smart meter roll-out is aimed at building an efficient infrastructure to implement the energy transition. In this framework, the competent metering point operator is gradually equipping distribution grid consumers with a certified smart metering system (iMSys). The iMSys consists of a modern measuring device (smart meter) and the smart meter gateway (SMGW). Here, the SMGW acts as a central communication unit that processes the consumer's measurement data and forwards it to the relevant market actors. A security module is installed in the SMGW to protect and encrypt communication. It functions as a key and certificate repository and manages the necessary cryptographic operations. Certification is based on a public key infrastructure run by a certification body commissioned by the Federal Office for Information Security (BSI). Section 4.2 provides a more detailed description of the SMGW infrastructure and the relevant actors in the energy sector, with a focus on the associated IT security aspects.

Cloud and edge computing. The shift from a centralised energy industry to decentralised energy production with associated trade also demands that technologies deployed to promote these trends must operate within a decentralised framework. Cloud and edge computing approaches can be used to process the growing volumes of data from multiple sources in an appropriate manner. Central resources could be applied flexibly and purposefully to replace local processing in the field. This would also enable outsourcing of responsibility for operating the infrastructure. Cloud services promise high availability and are generally low-maintenance for end customers. Typical models offered within cloud computing include 'software-as-a-service' (SaaS), 'platform-as-a-service' (PaaS), 'infrastructure-as-a-service' (IaaS) and 'function-as-a-service' (FaaS), which come with varying degrees of abstraction in the underlying hardware and software.

In many areas, cloud migration and the flexibility of related services offer significant advantages in regard to attack resilience and costs. Nevertheless, these advantages go hand in hand with a number of disadvantages that must not be neglected. Cloud migration inevitably means that customers surrender control over their own information to a third party, potentially compromising data privacy and integrity – in regard to both storage and processing [61]. In addition, users have no control over the availability of services. They are unable to rectify disruptions at the cloud provider by themselves, and such problems may also occur at times when an outage is particularly critical for customers. It follows, therefore, that concepts for the use of cloud computing in the energy industry especially must always contain backup solutions, along with encryption, authentication and validation.

Edge computing is another concept that is often mentioned together with the cloud. Unlike cloud computing with its logically centralised structures, the data processing operations in edge computing are performed already on the fringes of the network or within the network itself. This improves the deployment of distributed resources and enables the early reduction of data quantities, for instance by means of aggregation. For the energy industry, direct data processing close to the operational technology devices can also strengthen the ability to take action in the event of disruption in other areas of the network. But aspects of security are particularly relevant and must not be neglected, even when processing data on devices that have fewer available resources than with centralised concepts. Nonetheless, any widespread conversion within energy systems would be particularly challenging, as the concept of edge computing contradicts the conventional flow of information.

Blockchain technology and smart contracts. Blockchain belongs to the family of distributed ledger technologies and is another auspicious candidate for fulfilling the requirements of new use cases and decentralised structures [79]. Known for their use in the creation of cryptocurrencies like Bitcoin [71] or Ethereum [92], blockchains are built around decentralised structures and cryptographic methods that enable the secure and inalterable storage of data without the supervision of a trusted third party (TTP).

The system is put into practice through the use of cryptographic methods to form data blocks into chains, in which each block can only store a limited amount of any information. Attaching new blocks enables the blockchain to store more information, cryptographically protecting the information stored in the previous blocks. In general, it is no longer possible to remove older blocks from the blockchain. But the persistence of information comes with the drawback that the size of a blockchain will inevitably grow and will soon require more storage and computing capacity, especially if interactivity is lively or there are large volumes of data [69]. It is therefore important to consider carefully in all cases whether blockchain is an appropriate method for implementation.

A variety of consensus protocols exist for the decentralised decision on whether new blocks should be attached to the existing blockchain. The proof-of-work (PoW) method, which requires significant processing capacity, is widely used in public blockchains with unknown participants such as Bitcoin or Ethereum. By contrast, blockchains with access restrictions and known participants – within corporate consortia, for instance – rely exclusively on the proof-of-authority (PoA) method.

A blockchain's ability to enable persistent and inalterable storage of information can also be harnessed to realise decentralised applications. Smart contracts (SC) allow data collection, information processing and the digital mapping of contractual terms and conditions, as well as their implementation within a blockchain, which means that a 'digital contract' possesses the same benefits as the blockchain itself [79]. Ethereum-based blockchains offer native support for smart contracts [92]. Here, smart contracts can be created in the Solidity programming language as quasi-Turing-complete programmes, stored on the blockchain and executed in the Ethereum Virtual Machine (EVM) environment, in which all operations and interactions associated with the SC are made transparent by the blockchain link and can be validated by all parties involved. But issues of data protection must always be taken into account when storing data in a blockchain [68]. The unique properties of smart contracts within the framework of secure decentralised applications mean that smart contracts might also represent a valuable technology for the energy industry [79]. But further action must still be taken to overcome challenges of scalability and legal issues before blockchains can be established successfully within the energy sector.

Artificial intelligence and machine learning. While blockchain technology focuses on aspects of transparency and decentralisation within data storage and processing, dynamic algorithms and methods for data processing and the resolution of domain-specific problems are another field that is relevant to the energy industry in which AI is playing an increasingly important role.

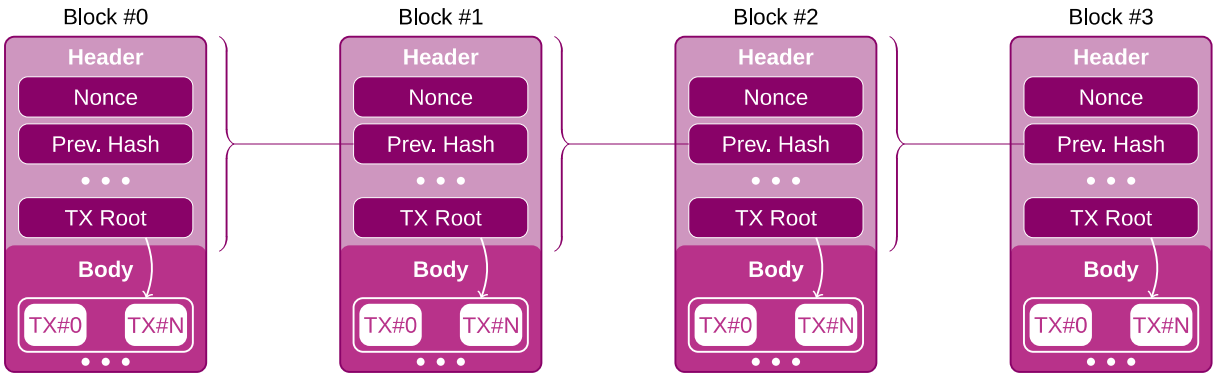

Figure 2.2: The blocks in the blockchain are divided into a header and body section. The body stores information in the form of transactions (TX) that are cryptographically linked to the header. Each block contains the hash value of the previous block, which establishes its connection to the chain. A nonce is required to attach a block to the blockchain, which is a value that affects the hash value of the current block. The block is only accepted if the hash value satisfies certain requirements, for instance that it does not exceed a certain value. Selecting a suitable nonce is laborious, which essentially makes a subsequent change or replacement of blocks impossible.

'Intelligence' can be a nebulous and sketchy concept, so the field of AI is also difficult to define. Broadly speaking, AI is defined as the capability of an algorithm or programme to solve problems dynamically and flexibly, which creates the impression of intelligence. Today's AI instances are designed primarily for specific problems [85] [90] and are described as 'weak AI' due to their specialised nature.

But a combination of several specialised AI systems can also enable the realisation of more complex use cases such as autonomous driving.

Among others, prominent branches of AI include machine learning (ML), artificial neural networks (ANN) and deep learning. In this process, suitable systems for solving problems are fed a series of examples to 'teach' them how to generalise what they have learned. Common areas in which these AI methods are used include algorithms for the automatic recognition of motives or faces in images [97], as well as the detection of anomalies in communication patterns. The pattern and anomaly detection capabilities of ML-based programmes can also be harnessed to develop methods for detecting network-based attacks in the form of intrusion detection systems (IDS). This can also be applied to problems within cyber-physical systems such as electricity grids, in which anomaly detection can be used to address suboptimal or critical states [66]. AI can therefore be installed at the network and physical levels of energy grids for the purposes of (cyber) security and efficiency optimisation.

In principle, the functions of an AI system can be divided into the following categories [90]: i) information detection, ii) identification of relevant information, iii) derivation of additional information and iv) preparation and implementation of recommended courses of action. The complexity of possible applications rises proportionate to the number of these aspects that are combined within an AI-based system.

Unlike conventional algorithms, the behaviour of AI systems, especially in the context of ML, is not always entirely deterministic: the ability to recognise patterns in data that were not included in the learning process means that the AI might categorise information incorrectly. The system's opacity could then prevent a clear determination of what caused this mishandling. It follows, therefore, that the implementation of an automatic AI-assisted system of inferred recommended courses of action must always be examined critically in cyber-physical systems.

But AI nevertheless offers significant potential for applications within the energy industry: Besides IDS, auspicious use cases for AI include process modelling, forecasting systems and planning methods, which are explained in more detail in Chapter 3.

2.3.2 Future technologies for cyber security in electricity grids

While the technologies discussed in Section 2.3.1 predominantly pave the way for new use cases, this section addresses both cryptographic procedures and more advanced concepts with a focus on cyber security. A comprehensive cyber security concept must include mechanisms to prevent, monitor and respond to specific incidents. The following summarises and discusses suitable technologies: general and special cryptography methods are aspects of preventive mechanisms to thwart cyber-attacks, along with active network control. A combination with detection measures in the form of IDS and general process monitoring enables the early detection of cyber-attacks that overcome the preventive measures. Automated response mechanisms come with elevated risks when IT and physical systems interact directly: measures that are erroneously initiated due to false alarms can cause considerable damage – both economically and in regard to health. A combination of automated monitoring, automated recommended courses of action and manual execution of any response measures mitigates the risk of inappropriate responses and leaves system control entirely in human hands.

Cryptographic methods and paradigms. The encryption and authentication of network communication are essential methods of preventing the tapping or manipulation of communication content. As a rule, a line must be drawn between symmetric and asymmetric cryptographic methods.

Symmetric methods always use the same secret key for both encryption and decryption [30]. Within this family, the AES (Advanced Encryption Standard) [63] is a widely used algorithm that symmetrically encrypts individual data blocks and enables variable key lengths. Based on current knowledge, AES is considered quasi-quantum-secure due to this variability: The Grover algorithm [59] is the only known algorithm enabled by quantum computing whose use can quadratically accelerate the process of breaking an AES-encrypted message. But the capability for exponential acceleration does not exist within quantum computing [77]. This means that despite quantum computing, the use of keys with an adequate length is sufficient to guarantee the effectiveness of AES encryption, as this form of encryption, when used and implemented correctly, can only be overwhelmed by a brute force attack, which is therefore also inefficient for quantum computers. Broadly speaking, symmetric encryption processes come with the advantages that they are secure and, in particular, fast and universally applicable. But secure use is predicated upon the secret key being exchanged in an equally secure manner, which is also possible using asymmetric cryptography methods.

Unlike symmetric methods, two separate keys for encryption and decryption are used in asymmetric cryptography. A private key, which is known to only one party, is used to derive a public key, which can be distributed to all potential participants in communication and other parties. This principle can be used for encryption as well as authentication.

A typical method for authenticating messages is that a checksum of the message is encrypted with the sender's private key and then sent to the recipient together with the actual message as a digital signature. The recipient can then use the matching public key to decrypt the encrypted checksum and verify it against the message. If the checksum matches, the recipient can be certain that the checksum was encrypted by the owner of the private key and that the message was not tampered with during transmission [30]. Message encryption works in the same way. When a message is encrypted using the recipient's public key, it can only be decrypted by a party that possesses the matching private key.

Unlike data-based symmetric cryptography that ultimately works at the level of individual bits, asymmetric cryptography methods interpret information as numbers and perform mathematical operations on these numbers. Specific knowledge in the form of the matching key is then the only way to reverse these operations. It follows that these keys must satisfy specific mathematical requirements, so that – unlike in symmetric cryptography – a valid key cannot consist of just any number and longer keys are generally required to achieve a comparable level of security. In addition, performing the mathematical operations on large volumes of data is more complex than using symmetric encryption. This is why hybrid approaches are frequently used. They apply symmetric cryptography to encrypt large quantities of data and then distribute the symmetric keys by means of asymmetric cryptography. The Diffie-Hellman method is a widely used option to provide asymmetric key pairs via communication channels that are not completely secure. Pre-installed certificates can also protect this method against man-in-the-middle attacks.

The security of many asymmetric methods is based on the assumption that the underlying mathematical function for deriving keys cannot be reversed effectively by a computer. Besides the issue of encryption in general, the growing relevance of quantum computers necessitates the use of *post-quantum cryptography* (PQC) in particular, as this assumption of mathematical complexity for conventional methods can be bypassed in some cases by means of Shor's algorithm [84]. PQC aims to provide signature and key-agreement protocols that remain secure, even when a quantum computer is used. In 2020, BSI published recommended courses of action for the migration of pre-quantum methods [52] to promote a timely switch to sustainably secure procedures, especially in the area of key-agreement protocols. The National Institute of Standards and Technology (NIST) is currently leading a standardisation process for PQC, which entered its

third phase in 2020 [2, 52]. The BSI recommendation [52] lists the code-based Classic-McEliece scheme [5] and the lattice-based FrodoKEM method [3]. These recommendations are largely consistent with the remaining NIST candidates. However, BSI rates the potentially greater security of the FrodoKEM method as more important than its poorer performance compared to similar methods.

When combined with symmetric methods that are viewed as post-quantum secure, these key-agreement protocols are essential for protecting communication and data that is stored for longer periods in modern systems, especially in the area of critical infrastructure. Digital signing methods are particularly interesting in addition to asymmetric procedures for encryption and key agreement. Here, CRYSTALS-DILITHIUM, FALCON and Rainbox are included in the third and final round of the NIST standardisation process [2], whereby all three algorithms do not depend on storing states and are hence also suitable for distributed systems, virtual environments and backup-based systems. Alternatives to these algorithms for post-quantum security include stateful hash signatures, of which both LMS (Leighton-Micali Hash-Based Signature) and XMSS (eXtended Merkle Signature Scheme) have already been adopted by BSI as procedures standardised by the Internet Engineering Task Force (IETF) [52]. However, the necessity to store a state and the limitation on the number of possible signatures with one key are frequently rated as disadvantages of these methods, which makes the aforementioned lattice-based and multi-variant signature schemes more promising alternatives.

The use of hybrid methods is advisable due to the paucity of experience with PQC and the lack of opportunities to test their security properties within a practical environment [29]. Two parallel protocols can be used for key exchange instead of relying exclusively on a PQC method – assuming they support protocols such as TLS (Transport Layer Security) or SSH (Secure Shell). The entire key exchange remains secure, provided one of the two protocols is also secure. Additional post-quantum security can be achieved as well by selecting a 'conventional' method and a PQC procedure. Indeed, the level of security will not decline at all compared to the current status. The conventional method continues to protect the data, even if the PQC procedure proves to be insecure.

It is already advisable to use PQC in the long-term protection of data and to prepare systems for the existence of quantum computers at an early stage due to the threat presented by the 'harvest now, decrypt later' approach, in which data is collected today for downstream decryption using quantum computers. A combination of proven symmetric cryptography with an adequate key length and the quantum-safe key-agreement and signature procedures presented here is necessary in this regard. This means that an awareness of potential threats that may cause damage in the absence of timely adaptation must be created at all levels, in addition to the technical implementation.

The primary purpose of conventional encryption concepts is to enable encryption between two parties or a group of parties who share the same symmetric key. But conventional asymmetric encryption of the symmetric key is inefficient in a scenario in which a sender wishes to transmit encrypted information to several recipients who are able to decrypt this information, as the symmetric key must be asymmetrically encrypted and transmitted individually for each of the recipients. The key distribution process provides additional attack vectors, especially in decentralised use cases involving participants with conflicting interests such as local decentralised energy markets. An example would be the deliberately erroneous encryption of a symmetric key for a particular recipient.

Attribute-based Encryption (ABE) offers a cryptographic solution for use cases that are particularly vulnerable to this kind of attack [6]. In this case, the symmetric key is not encrypted individually for each participant, and participants instead receive predefined attributes in the form of cryptographic keys from one or more

key authorities. For encryption, the sender uses a logical formula consisting of conjunctions and disjunctions for these attributes, so that any participant who possesses the assigned attributes to satisfy the formula can decrypt the data.

Concepts and implementations for post-quantum security exist in the area of ABE as well [78]. The ABE encryption concept enables detailed access control to information and optimisation of the key distribution process. It does, however, have negative implications for performance, so that the necessity of using ABE should always be reviewed critically.

Fully Homomorphic Encryption (FHE) is another example of a special encryption method [56]. Generally speaking, the consequence of using encryption to protect confidential information is that the information in question can only be processed by a party with access to it. FHE resolves this issue by encrypting data in such a way that certain operations, such as addition or multiplication, can also be performed on this encrypted data and the result itself is also encrypted. For data x and y and a homomorphic encryption algorithm E, $E(x + y) = E(x) \oplus E(y)$, in which $\oplus$ represents addition with homomorphic encryption. FHE can be particularly helpful within cloud computing, as it enables the decentralised processing of encrypted data, while still preserving its privacy and security. Applying FHE is always complex, which means that – depending on the area of application – less powerful partial homomorphisms can and should be used so as to benefit performance.

> In summary, energy industry information should be encrypted for long-term storage. Cryptographic methods and message authentication must also be applied to protect current and future communication channels and to create a resilient foundation for withstanding cyber-attacks.

Overarching concepts for system-wide cyber security. Encrypted communication and information processing are essential building blocks for protecting current and future energy systems. But additional measures are necessary as well to ensure an adequate level of security at the overall system level. In this case, technical measures and human conduct must be coordinated. While the security-focused awareness training for staff members and concepts such as password policies or two-factor authentication [13] that are also recommended or prescribed by BSI increase security in cases of (unwitting) misconduct or targeted attacks (e.g. phishing) against users and systems, the introduction of additional technical measures and concepts for the prevention and detection of cyber-attacks is still advisable.

Software-defined networking (SDN) for active network configuration, control and monitoring is a possible means of prevention and detection [82]. SDN is based on the principle that local decisions made by routers and switches in regard to data forwarding (control plane) will, under normal circumstances, be logically separate from actual operative implementation of the data forwarding (data plane) and will be handled by a logically centralised controller. The data plane processes data packages based on rules that can be dynamically created and adapted via the controller. The main advantages compared to static and local configuration are, on the one hand, the possibility to consider the overall network topology for configuration and, on the other, the ability to make changes that are necessitated in response to new network situations and that may simultaneously affect several devices that need to be controlled in a coordinated manner.

Knowledge and control of individual data flows also enable security-based applications at network level: communication between specific devices or network segments can be dynamically enabled or suppressed, new communication paths activated or deactivated in the event of a fault, and a central unit can specifically disconnect hosts from the network, for instance in the event of an attack. Well-known concepts in the area of

SDN include the OpenFlow protocol [70] and the network programming language P4 [7], which uses programmes that are executed on compatible switches to enable the handling of network packets and flows. Given that correct network configuration that is planned from a security perspective is an essential factor for ensuring resilience against cyber-attacks, the application of a SDN concept can contribute to elevated cyber security in the energy sector and should be taken into consideration.

SDN, authentication and encrypted communication are essential building blocks in the advance prevention of cyber-attacks. It makes sense nevertheless to put additional detection measures in place, as optimised prevention of successful cyber-attacks cannot be entirely excluded. Active monitoring of potential attacks can help to initiate the appropriate defensive countermeasures at an early stage to prevent or mitigate damage, and not only after an attack has already caused greater damage. Intrusion detection systems (IDS) are suitable methods of timely detection, as they continuously and automatically monitor connected components connected in order to identify and report conspicuous behaviour. IDS can even be added to upgrade current systems.

A general distinction is made between two different types of IDS: signature/rule-based IDS attempt to recognise known attacks based on stored patterns. The benefit of this is that they mostly detect cyber-attacks with a high degree of accuracy. But the stored patterns need to be updated continuously so as to detect additional or new attacks. It follows, therefore, that these IDS only possess the capability to recognise known attacks. In contrast, anomaly-based IDS model normal system behaviour and raise the alert if it deviates too far from normal patterns, which can means that novel cyber-attacks can be detected as well. But anomaly-based IDS become more susceptible if the modelled normal behaviour changes over time, which is a known cause of false alarms. Machine learning has yielded significant progress over recent years, especially in the field of anomaly-based IDS research.

An IDS can be used in different areas, irrespective of these two fundamental operating principles: On the one hand, monitoring a system's underlying network traffic (network-based) is a good way to detect attackers according to how they influence network communication. This enables, for example, the detection of unusual connections or even special attacks on protocols and devices. SNORT [25] and Zeek [88] are among the established solutions in this area that draw on signature- or rule-based methods. On the other hand, host-based IDS can be installed on computer systems to catch attacks whose effects are not visible in the network. Examples include the use of an USB stick to compromise or the propagation of malware within one or across several computers. Wazuh [91] belongs to the known solutions used in distributed computer networks.

Process-based IDS are also installed, especially in cyber-physical systems (CPS). Cyber-physical systems collect and control measured values to establish a connection to the real world – like in distributed electricity grids. Process-based IDS can detect the impact of a cyber-attack in process data and in doing so exert direct influence on physical conditions. These IDS can substantially improve security, especially when used in a context with Operational Technology devices. Implausible values, the absence of measurements or anomalies in the execution of control commands are attacks against the process itself, which can, however, also be detected and reported at IT level. Although IDS can generally be combined with automated countermeasures as an intrusion prevention system (IPS), the risk presented by incorrectly executed countermeasures should be taken into account, especially in cyber-physical systems. Overall, therefore, IDS present an upgradable option for the rapid detection of cyber-attacks and downstream initiation of countermeasures before the attack can inflict any significant damage.

A wide range of technologies exist for the secure implementation of IT-based use cases that can advance digitisation and decentralisation of the energy industry in line with practical needs and security requirements. In particular, technologies that offer significant security enhancements without making profound changes to existing systems – as is the case with IDS – should be examined comprehensively and soon for use within energy systems.

2.4 Cyber-secure upgrading of technical energy infrastructures

The technologies and concepts discussed in the foregoing enable sometimes innovative use cases or can primarily ensure security in electricity grids. In this regard, communication technologies (cf. Section 2.2) and cryptographic methods (cf. Section 2.3.2) in particular are relevant to security at device level. The following section discusses the specific requirements for individual operating resources in IT to ensure cyber security in the electricity grid and then formulates clear recommendations for cyber-secure upgrading of equipment. At present, the available equipment designed for longevity cannot meet all of these requirements, so additional concepts are needed to safeguard current devices over their envisaged operating lifetimes.

Technical requirements for cyber-secure operating resources. The objective of running operating resources for two to three decades places special demands in their technical features. Firstly, all installed components must be conceived for this longevity and function reliably over the envisaged period. Secondly, the devices must be designed with sufficient flexibility and foresight to enable their adaptation when new requirements or problems arise.

As a rule, the following aspects must be taken into account in the development and equipment of cyber-secure operating resources:

1. All hardware must be designed for longevity and reliably fulfil its functions.
2. Resources must be planned with adequate leeway, which means that storage and computing capacities should be selected in such a way that they will satisfy the anticipated requirements up to the end of their intended lifetimes.
3. Elements that are relevant to security or specific functionalities, including cryptography or communication modules, must be modular and interchangeable. This enables their adaptation to new insights and changing requirements, without requiring the replacement of complete devices.
4. General purpose hardware should be selected whenever possible, so hardware that can flexibly fulfil common tasks. Processors in particular should be suitable for general areas of application to ensure they can also be deployed for new tasks.
5. The capability to import functional and security updates on the software side is a key requirement for sustainable cyber security. A mandatory policy to install regular security updates is advisable. Aside from closing security vulnerabilities in the system itself, it should also be possible to replace or update the applied algorithms, especially in the area of cryptography.

The extended asset deployment times conflict with a continuously and rapidly changing IT landscape in which new use cases, threats, security mechanisms, vulnerabilities and technologies lead to the underlying assumptions that applied when the asset was put into operation becoming obsolete several times over the course of its lifetime. Forward-looking design of operating resources therefore becomes all the more important, both in regard to the hardware and in the area of software functionality. As set out in the BSI

technical directive TR-02102-1 [17], for example, the specific encryption used must always be adapted to reflect current recommendations and the latest insight into security. This places direct demands in software updates and general purpose hardware, i.e. exchangeable special modules. New methods – for instance longer keys or more complex algorithms – can also increase the demands on computing capacity, as well as on working and long-term memory. The potential for increasing requirements must be taken into account with adequate leeway in the design of devices, as equipment deficiencies will either be at the expense of its longevity (the devices will then need to be replaced) or at the expense of cyber security.

At present, hardware remains in use despite exhibiting deficiencies in cyber security as replacing equipment is costly and time-consuming. But this procedure must not be maintained in the long term, especially in view of the worsening threat scenarios and increasing digitisation of the energy industry. Standardised certification processes for the use of equipment can also incentivise manufacturers and operators to shoulder the additional costs incurred for installing equipment with sufficient capacities. These processes decide at regular intervals on the permission to use equipment models, especially in the context of KRITIS. However, the specific trade-off between cost or resource efficiency and forward-looking equipment remains a challenge that requires coordinated consideration from an economic, technical, political and regulatory perspective.

Cyber-secure upgrading of current technical operating resources. This section discusses concepts that can elevate the level of security in existing networks, bearing in mind that some of the operational equipment presently in use does not meet current or future cyber security requirements, despite having been designed for the long term.

One obvious option is to replace affected operating equipment with alternatives that are designed and manufactured to fulfil the aforementioned criteria. But less radical measures are advisable as an interim solution, as such an approach would be immensely challenging from both an organisational and financial perspective. Specific modules within units can be exchanged or retrofitted in some cases. Software updates can potentially ensure the security of devices that have sufficient available resources. Attacks on inter-device communication and the exploitation of protocol properties or vulnerabilities place a particular emphasis on the connectivity and cryptographic capabilities of the devices. It is true, however, that all participants in the communication must be aligned, so that the weakest link usually defines the security level.

Regardless of the specific operating equipment, software-defined networking (SDN) and intrusion detection systems (IDS) are good methods of improving the control and monitoring of communication patterns. But these concepts do not bring any added value in regard to confidentiality (encryption) or authenticity (authentication) of the communication. By and large, there are two concepts to improve the security of communications if the options to upgrade the operating resources are largely or entirely absent:

a) protocol-specific peculiarities are exploited – without their replacement – to embed security functions in the communication (retrofitting); or b) individual communication sections are protected by means of middlebox-based encryption.

In the case of retrofitting, for example, message authentication codes (MACs) are integrated into unused protocol fields or protocol fields occupied with default values, possibly in a truncated form. The advantage here is that devices whose features cannot be updated remain able to send and receive valid communication packets. But the level of security achieved in this way will still be quite low, as only a few bits can be used to transmit a MAC in many cases. In addition, an IDS or other security system may interpret field assignments that conflict with the protocol standard as an attack or discrepancy, which must be taken into account when using the system.

Deploying middleboxes to upgrade cyber security is one method of achieving high security on partial sections of the communication path. They can also be used to ensure the compatibility of retrofitting measures for individual units. In these cases, the middlebox adapts and reads the protocol fields without the actual unit noticing. Middleboxes are also suitable for implementing encrypted communication channels between individual network sections. For example, sections between individual sites of an energy grid system can be connected by means of VPN tunnels to route and encrypt all data traffic with suitable authentication. However, implementation requires installing appropriate devices to upgrade the network by establishing VPN tunnels. Moreover, this will only protect against attacks on the relevant communication sections: This method will not create end-to-end encryption, so an attacker with access to communication between the operating resources and the middlebox will still be able to draw on the original attack options.

The concepts presented here are unable to replace conversion to cyber-secure operating resources on a permanent basis, as they are inadequate to fulfil the standard of end-to-end encryption and authentication. However, the use of one or more of these concepts to upgrade cyber security in current operating equipment is advisable in any case as a short-term method to increase security and enable the transition to operating resources with built-in cyber security features.

> The energy sector is facing fresh challenges due to growing demands on the performance and flexibility of energy grids, decentralisation in the context of the energy transition and progressive digitisation. The security of energy systems is an essential aspect both at the physical level and in the area of digital monitoring and control. New – but also long-established – technologies from the areas of digital communication, IT security and IT in general provide opportunities to implement new applications, to ensure security going forward and to protect current systems against new threats as well.

3 Innovative use cases within a shifting threat landscape.

Technological progress in both the energy industry and information technology – combined with the paradigm shift towards greater decentralisation and customer interaction in the energy industry – provides scope for new and innovative use cases that can only be realised through advancements in the area of digitisation. These use cases enable or strengthen developments such as the energy transition, flexible tariff design and electromobility, as well as general grid stability and resilience. But this also creates new potential for cyber-attacks against energy network operators and their customers, so cyber security must be a top priority for the energy industry in the future. The following begins by investigating specific use cases for the energy industry from the perspective of both customers and grid operators (Section 3.1). It then proceeds to analyse historical attacks (Section 3.2) and evaluate the implementation of cyber security in order to derive specific recommended courses of action and requirements to cope with a corresponding attack model. Finally, it concludes by presenting national rules and regulations that have already been established in this context (Section 3.3).

3.1 New use cases caused by technological and structural change

Transformation of the energy industry towards decentralisation and digitisation, in combination with new technologies in the areas of communication, cryptography, data processing and system security, presents huge potential for innovative use cases in the area of facility control and flexibility management. These opportunities also extend to customers in the areas of self-optimised consumption, local energy markets and tariff design, and with regard to their dual role as prosumers who dynamically feed energy into the grid or consume it. This section provides an overview of use cases from the perspective of grid operators (Section 3.1.1) and customers (Section 3.1.2). In particular, challenges and potentially useful technologies are analysed in this context.

3.1.1 Use cases for grid operators

Decentralised power generating plants (DPGP) based on renewable energies account for growing share of current and future electricity production. Their dependence on external conditions such as solar radiation and wind makes it difficult to forecast production capacities, and actual production may be exposed to spontaneous fluctuations. But electricity storage facilities and conventional power plants can be coordinated – also within the framework of Redispatch 2.0 – to adjust the feed-in of electricity to current consumption and in doing so prevent bottlenecks and adapt feed-in localisation. Protecting against line and transformer overload can necessitate these measures as well, in addition to fluctuations in generation capacities and consumption. This means that overarching, end-to-end digital communication between generators and infrastructure operators is indispensable. Reliable and automated execution of suitable actions is intrinsically linked to strict high demands on the communication and control infrastructures. Reliable operation as well as resilience against disruptive factors and attacks are fundamental prerequisites for use in the KRITIS sector, so that encryption and security measures in particular must be factored into the equation at an early stage.

At the same time, the increased demand for electricity and the growing share of large private sector consumers within the framework of electromobility pose new challenges for the electricity grid. Digital communication presents two other new areas of application to guarantee the stability of the electricity grid. Firstly, the expanding charging point infrastructure necessitates the establishment of a charging management system that is coordinated or directly controlled by the grid operator. This enables the grid operator to ease the strain on the electricity grid by dynamically throttling or even deactivating the charging of electric cars, depending on the current production capacities and the charging situation. Secondly, this concept can be developed into another use case by harnessing the storage capacities of electric cars for feed-in. This could be done for congestion management within the framework of vehicle-to-grid concepts (V2G).

But both cases create several critical requirements for a suitable technical solution: on the one hand, control must be reliable and safe. In particular, the additional feed-in of capacity from the private sector must be technically safe and trouble-free for both the individual and the electricity grid in general. Unauthorised access is just as critical here as in the ICT network of an electricity grid operator, but the grid operators' more limited control over a corresponding communication network infrastructure presents an additional challenge. A basic prerequisite for these use cases is that the measured values and control commands in particular must be encrypted and authenticated. Data protection and privacy aspects play an essential role as well on the other hand. Interfering with the charging behaviour of an electric car – combined potentially with additional discharging of the vehicle battery – may significantly restrict the vehicle's usability as such. Instructions issued by the owners, for instance concerning a time at which the vehicle battery needs to be charged, must be taken into account in every case. Potential emergencies cannot be disregarded, either, and must be included in a suitable technical concept. For example, to ensure that a vehicle remains operable for at least short periods of time, a vehicle battery should never be discharged to below a certain level.

The need for dynamic and transparent tariff models is also growing to ensure that customers acquire added value from their decision to place available capacities and control options at the grid operator's disposal. Aside from proprietary solutions, the smart meter gateway (SMGW) offers significant potential for innovation and can play a key role in the combination of technical and tariff aspects for the aforementioned use cases at the interface between end customers and grid operators. For this to happen, though, all stakeholders – from end customers to charging station manufacturers and grid operators – must appreciate the SMGW as a uniform, open and purposeful technology. Comprehensive technical capabilities of the gateway itself, transparency in regard to the technology – especially in communications with private sector customers – and targeted regulatory support can contribute to fulfilling this requirement.

The aforementioned Redispatch 2.0, congestion management and direct marketing are good examples in the context of SMGW-based use cases. Viewed from an aggregate perspective, current and frequently updated information concerning the momentary feed-in or extraction of power by individual households enables a more accurate assessment of the general state of the grid, early detection of bottlenecks and timely initiation of countermeasures. Provided that comprehensive data protection measures are in place, this information can also be used to provide external market participants with the option of obtaining wide-ranging value-added services. Like with the aforementioned charging management and V2G concepts, the SMGW can also be used to run other devices within the framework of the smart grid. End consumers or prosumers can negotiate a favourable tariff model with the grid operator that enables control of end devices or entire consumption facilities for a limited time and amount. This gives the grid operator better control over bottlenecks, which can be reduced or even eliminated as a result.

3.1.2 Use cases for customers

In addition to use cases that are primarily designed with the interests of grid operators in mind, others are also relevant that offer benefits and new opportunities directly to customers or affect the electricity grid on the 'last mile' and ensure widespread acceptance of changes to existing infrastructures and processes. Fundamental concepts such as V2G and variable tariff design have already been discussed from the operator's point of view. The following places a particular focus on the customers' perspective and on the SMGW.

While congestion and flexibility management in particular are incentives for increased customer interaction among grid operators, more affordable tariff models or other financial aspects represent the principal concerns of end customers. In the ideal scenario, these tariff-based use cases offer an advantage for both sides, provided they adhere to suitable proprietary and self-monitoring and ensure that aspects such as data security or privacy are taken into account. A time-variable tariff structure, when communicated transparently to customers via the SMGW, for example, allows customers to optimise their own consumption and save costs by adjusting their consumption to the current tariff. Grid operators are hence offered the opportunity for indirect congestion management, while customers can benefit financially.

Decentralisation of the electricity grid affects not only the electricity grid operators themselves, but also increasingly the customers. The integration of photovoltaic systems or dedicated electricity storage systems and concepts such as V2G gives them a dual role as consumers and electricity producers (prosumers). Aside from the aforementioned interaction with the electricity grid operator, these aspects also create options for direct peer-to-peer markets. In addition to the previously discussed possibilities to optimise personal consumption, this also creates business models for customers to buy electricity capacities for storage or to feed them into the grid at a profit, depending on the momentary market price. Local energy markets (LEMs) can serve as largely neighbourhood trading platforms, depending on the specific capabilities of the prosumers – for instance their available storage and production capacities – and the fluctuating supply and demand relationship [79].

LEMs enable customers to purchase electricity from other consumers and not just directly from the grid operator or dedicated electricity suppliers. This creates incentives for them to invest in photovoltaic and storage systems on the one hand, but also to participate in a LEM merely as consumers on the other. Connecting several LEMs to create a supra-regional market can further increase cost efficiency, but also requires more complex technical solutions that meet the requirements of such a decentralised platform, especially with regard to data security and privacy.

Reliability, trustworthiness and the protection of customer data should be mentioned as the principal requirements for an LEM platform. None of these aspects are possible without a solid security infrastructure. In this regard, reliability and trustworthiness include system availability and fault resilience, as well as low latencies in regard to price developments and the general market situation. Supply transparency must also be maintained to forestall potential manipulation. It follows that operation requires either a fully trusted party or a form of decentralised realisation, for example with blockchain technology. SMGWs should also be mentioned for secure communication between all participants. Assuming the application platform is open, they can be installed as a pivotal element for the secure implementation of LEMs.

Besides these short-term tariff options, the demand for a more flexible tariff design also creates the use case of enabling customers to choose their electricity supplier more dynamically. A secure, standardised interface, for instance in the SMGW, could allow customers to switch their tariff flexibly. Aspects such as the

automatic transmissions of meter readings, remote diagnosis options or the process of entering installations in the core market data register (MaStR) represent additional use cases for an architecture such as the SMGW that can benefit from increasing digitisation, assuming a rigorous security culture is in place.

> Digitisation, the advancement of technology and structural change within the energy industry precipitated by the energy transition provide potential for new use cases that can offer benefits for both customers and grid operators. Innovative solution approaches can be to the benefit of use cases such as flexibility management, grid stability and resilience against grid segmentation as well as flexible tariff models and the dual role of prosumers. Several conditions must be met to exploit this potential, which can largely be summarised as mutual utility and (cyber) security. Any solution approach must always consider the interests of end customers and grid operators alike to ensure added value for all stakeholders. In regard to customers, financial incentives such as more flexible tariff models may help to implement applications that primarily offer benefits to the grid operators. Moreover, all solutions must take into account – and consistently implement – aspects of data security and privacy from day one.

3.2 Historical attack vectors and cyber threats in tomorrow's world

The need and demand to ensure the particular security of energy systems are based on several examples that underline, sometimes dramatically, the vulnerability of these grid systems, as well as the consequences of successful cyber-attacks. The process of safeguarding the cyber security of energy grids, especially in regard to new use cases (cf. Section 3.1), requires detailed reappraisal and in-depth understanding of historical attacks, in order to derive insight into future threat scenarios as well. Implementation of the aforementioned applications cannot proceed with focus until an adequate degree of cyber security has been achieved or becomes attainable. This section initially outlines historical cyber security incidents, which are then analysed in regard to their overarching criteria such as attack phases and general attack vectors. It then proceeds to discuss cyber threats (Section 3.2.2) that will conceivably acquire additional relevance and must hence be taken into account, especially in the context of digitisation and concepts such as the SMGW, in order to create cyber innovations that ensure the security of the energy system going forward.

3.2.1 Analysis of historical cyber-attacks and research findings

The number of cyber-attacks targeting electricity grid actors has increased steadily in the recent past. The consequences of these attacks are, in the best case scenario, cushioned by redundancy systems, but widespread and lengthy power cuts affecting thousands to hundreds of thousands of people have already occurred. [38]. The risks to which electricity grids are exposed within the framework of cyber-attacks are due to various factors: phishing and social engineering are entry methods that rely on (unwitting) human misconduct instead of technical security vulnerabilities. [66]. An absence of security measures then enables undetected action in the network, during which frequently outdated protocols that fall short of the standards of modern IT security facilitate the infliction of immense damage. [66]. The following section describes and analyses three cyber-attacks against electricity grids or their components in order to identify typical vulnerabilities and derive abstract procedures. Specific recommended courses of action and technical solutions to counteract these attacks are then presented on this basis.

The Aurora Generator Test. The particular risk posed by combining legacy communication protocols that are directly connected to physical equipment was highlighted by the Aurora Generator Test in 2007 [96]. The tested attack attempts to desynchronise a generator with the associated electricity grid and specifically

exploits time delays in security mechanisms. In the first phase of the attack, the synchronised generator is disconnected from the grid by opening the circuit breakers. The decline in load causes the generator to speed up, so that the grid frequency it generates runs ahead of the rest of the grid. This results in a shift of almost half a phase within just a few milliseconds. In the second step of the attack, the opened circuit breakers are closed again [96]. The asynchronous phase between the generator and the electricity grid causes an immense torque to be exerted on the generator, which may exceed its tolerance and in doing so cause permanent damage.

This vulnerability is particularly relevant because it also exploits the lack of encryption and authentication in Modbus and other legacy protocols. This highlights the immense importance of protection mechanisms in controller communication, in addition to physical protections such as monitoring switch operations and preventing a switch from closing when the phase deviates. It would be extremely difficult to conduct such a precisely timed attack manually, and it would require physical access to switches or the control system. By contrast, an attack targeting vulnerabilities in communication protocols would not need this level of access. The Aurora Generator Test highlights the potential of cyber-attacks to cause physical damage to equipment or even people.

Cyber-attacks on the Ukrainian electricity grid. Two of the most prominent attacks against electricity grids took place in Ukraine in 2015 and 2016, respectively [38, 67]. Grid system operators (similar to a distribution system operator) were the target of both cyber-attacks, which resulted in power cuts for several hundred thousand customers. A coordinated attack on three electricity distribution companies was detected on 23 December 2015, affecting control and management equipment of SCADA (supervisory control and data acquisition) systems as well as network devices. The attackers had presumably gained access to internal systems nine months beforehand by emailing Office documents with malware to employees as part of spear phishing attacks. This enabled the passive collection of information, especially in the form of credentials, providing access to further systems and network areas, as well allowing the acquisition of information about the functions and interactions of the ICT network and control equipment. It is reasonable to assume that the attackers had immense resources at their disposal, as there is also a suspicion that operational equipment belonging to employees was tampered with. The attack took place on 23 December 2015. The perpetrators used the acquired information and access details to switch over at least 27 substations, which directly caused the power blackout for many customers. To frustrate diagnosis and rectification, simultaneous attacks were carried out on monitoring systems, the uninterruptible power supply (UPS) and control servers, as well as on the firmware of field devices.

Similar to the 2015 attack, a grid system operator was the victim of a cyber-attack on 17 December 2016 that caused the failure of a substation and which resulted in a blackout for around a fifth of Kiev's electricity consumers or several hundred thousand customers [67]. Despite the lack of hard evidence, the attack is widely attributed to Russian hackers. Investigations into the incident point to the use of 'Industroyer/CRASHOVERRIDE' malware, which was specifically designed for use against industrial networks and energy grids in particular. It acts by establishing a connection to an external control server or can operate autonomously without external communication, whereby the malware commands a variety of communication protocols used in energy grids and can therefore read, manipulate or generate switching commands and monitoring messages. Besides the possibility to control devices, this also creates the option for false data injection, which means the deliberate manipulation of measured value messages such as voltage measurements or switch positions. Once transmitted, the false information can provoke switching operations in the control centre or conceal fault conditions.

The two attacks on the Ukrainian electricity grid demonstrate that cyber threats to the energy sector have long been a reality and that highly developed attack tools already exist. Attackers with the necessary expertise are able to inflict considerable damage on electricity grids. The scale of the two attacks on Ukraine's electricity grid underlines furthermore the relevance of IT to complex attacks: This kind of coordinated, parallel approach against several substations and grid operators would be difficult to achieve without extensive deployment of IT infrastructure in the cyber-attack. These Ukrainian case studies additionally reinforce the priority of ensuring the adequate protection of IT infrastructure against attacks of this kind. Moreover, the general attack strategies can be inferred from their complexity. These strategies will be presented in the following.

Abstracted attack vectors, attacker models and attack phases. The attackers' approach in various scenarios enables their abstraction to general procedures and the identification of common universal vulnerabilities. Insights can be obtained in regard to the different phases, especially in regard to the more complex attacks on the Ukrainian electricity grid. Abstracted models of this kind, in particular with a focus on ICT networks, have already been designed on several occasions, for example in the context of the ICS (industrial control system) cyber kill chain [4], which distinguishes between two attack phases: the intrusion phase, which includes preparatory steps, and the ICS attack phase, which constitutes the actual attack [4]. But a breakdown into further phases is more precise in the context of energy grids in particular, as the large-scale network structure and the subdivision into different network segments represent a major difference compared to general ICT networks.

The following attack phases can hence be distinguished for the ICT networks in electricity grids, whereby the severity of the repercussions generally rises with each new phase. The attack phases and their typical actions are summarised additionally in Figure 3.1.

1. During external reconnaissance, attackers analyse their target for potential gateways and attack vectors. This includes active and passive investigation of the (external) network and potentially spying on buildings and employees as well.
2. Initial intrusion is the second step in which the attackers gain access to an internal network segment or a device connected to the internal network.
3. a) This is followed by internal reconnaissance. The phase is used to gather additional information about the system, especially communication patterns and credentials to other network segments. The information is then used to prepare the following attack phases.

   b) Acquired information and credentials are used for access expansion. The attackers gain access to further systems and network segments, which they can exploit for additional reconnaissance.
4. Preparation for the actual ICT attack begins as soon as the perpetrators have compromised a sufficient number of systems.
5. a) The ICT attack is performed. Individual or multiple systems are attacked by manipulating or preventing communication, sending control commands to destabilise the electricity grid or manipulated measured values to the control centre as part of a false data injection (FDI).

   b) Simultaneous or downstream measures for detection and response disruption can be initiated by manipulating log files, interfering with backup systems or blocking control system components.

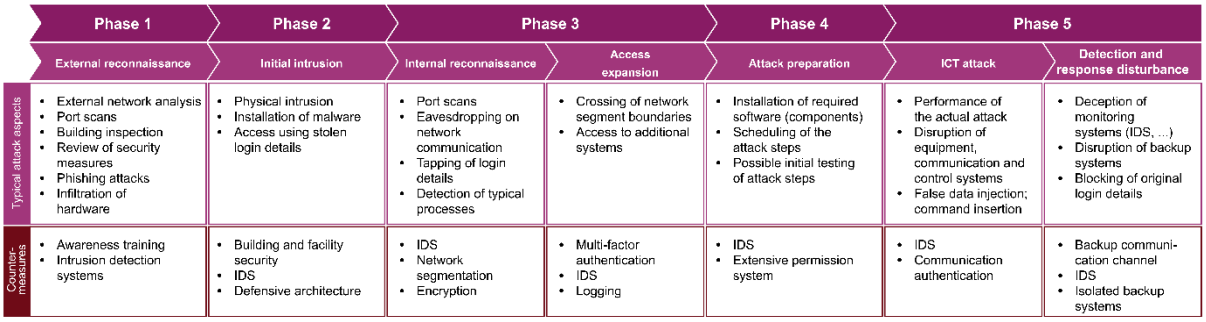

Figure 3.1: Attacks on the ICT infrastructure of a grid system operator can be divided into five main phases. Detailed information about the network, communication patterns and users can be gathered once network intrusion has been planned and prepared. This information is used to plan the technical requirements and strategy and ultimately to carry out the actual attack. In addition to the actual targets, this process may also disrupt the systems to detect or respond to the attack. A variety of countermeasures exist for each phase, either in a preparatory sense or to repel the attack.

Viewing the attack from an abstracted perspective enables the identification of typical vulnerabilities and points of attack and in doing so to derive appropriate countermeasures. A common preparatory method is to conduct the attack using employees of the target infrastructure operator. Attackers can gain access to the network without directly leveraging dedicated cyber security solutions, for instance by phishing or leaving prepared USB sticks in the car park, which are then picked up and used by employees who unwittingly open a gateway. It is therefore indispensable to create adequate security awareness among all employees at an early stage in order to nip in the bud any risks that are based on these methods. The risk of a successful attack can be significantly reduced at an early stage in combination with intrusion detection systems (IDS), which detect port scans at an early stage, for example.

In addition to the physical protection of facilities and buildings, a defensive configuration of the host's network equipment is necessary to prevent or at least detect the initial intrusion during attacks. Disabling unused network ports, monitoring the network topology and IDS increase the likelihood that an attack will be directly detected and prevented. IDS also play a crucial role in the prevention and detection of attacks beyond phase 3. They possess broad areas of application and are relatively easy to retrofit in established systems, so their use is mandatory according to the IT Security Act 2.0 (IT-SiG) as well. Nevertheless, defensive network architectures with segmentation and encryption as well as multi-layer authentication mechanisms are also indispensable to counter attacks effectively. In the event that credentials still fall into the hands of attackers, a fine-grained permission system helps to limit their possibilities. An IDS or log monitoring system that reports the use of credentials to access unusual systems or network areas can further restrict the options.

Despite all these security measures to facilitate the detection of attacks, the encryption of all communication and, in particular, the authentication and integrity assurance of measurement value messages and control commands are absolutely necessary for the effective prevention of multi-phased attacks. Fast, efficient and correct responses in the event of an attack also requires detailed response plans (incident response strategies), for example in the form of catalogues of measures and regular exercises.

3.2.2 Cyber threats to the energy systems of the future

The attack vectors highlighted here underline the importance of comprehensive cyber security concepts in current and future energy grids. Current trends in the energy industry towards decentralisation and digitisation as well as ongoing progress within information technology will create additional opportunities

for cyber-attacks in the near future. Attackers are offered a broad set of targets due to the growing connectivity of the electricity grid and the use of public infrastructure such as mobile communication networks. The reliance on digital communication to control assets will also grow as the traditional staffing in some facilities – including smaller substations and wind turbines – is reduced or cut entirely as a result of this change.

Exacerbating this broader set of targets are potential risks associated with the availability of novel technologies such as quantum computers. The deployment of post-quantum cryptography should therefore take place as promptly as possible to protect communication and especially the stored information from unauthorised access in the long term. Even if the decryption of information encrypted with pre-quantum methods will only become possible in the future, encrypted data can already be tapped and stored for decryption at a later date. It is thus reasonable to state that future quantum computers already pose a risk to information security and must be taken into account accordingly.

In addition, the connection of controllable (large) consumers such as charging stations or SMGW-supported devices presents potential risks for the energy industry as well. On the one hand, attackers can target several of these devices and significantly disrupt the electricity grid by switching consumers on or off in a synchronised fashion, which can impact grid frequency if there are enough consumers. On the other hand, manipulating the capacity values transmitted by the SMGW can have negative effects on the grid if the actual capacity deviates from reported values that are used for scheduling purposes [65].

In addition, the aspect of customer privacy has been assigned a low priority until now as it has not presented a noteworthy target for attacks. But the increasing connectivity along the electricity grid and through to the consumers means that customer information such as general consumption patterns or daily capacity values, transmitted via an SMGW for example, are no longer under the customers' direct control. The adequate and seamless security of this information must be guaranteed during transmission through the network, processing by grid operators and potential downstream storage. Interaction must also be prevented between third parties and an SMGW or any other communication device that can disclose relevant information.

> Overall, it is fair to say that concepts such as PQC for encryption, integrity assurance and authentication, a defensive network architecture and awareness training for prevention and IDS and SDN for detection – combined with sweeping response plans – are indispensable both today and for future attack scenarios on energy grids and must hence form the basis of any security concept. Nonetheless, a high level of safety should not only be viewed merely as an obligation, but also as a foundation and opportunity for extensive innovations that guarantee progress and viability for the energy industry going forward.

3.3 Regulations and standards for the cyber security of critical infrastructures (KRITIS)

The immense relevance of the technologies, concepts and approaches presented here to guarantee cyber security in energy grids means they have already been enshrined in valid regulations, rules and standards related to the energy industry. This section compiles and discusses corresponding regulatory bases for IT security in the supply of energy.

The Energy Industry Act (EnWG) [44] is the legal foundation for energy supply by means of electricity and gas networks and defines the rights and obligations of grid operators in both the transmission and distribution grids. Customer installations must also satisfy the minimum technical requirements as set out in the application rules of the Association of Electrical, Electronic & Information Technologies (VDE), as defined for the individual voltage levels. The Renewable Energy Sources Act (EEG) [42], adds to the EnWG and deals primarily with facilities for the generation of energy from renewable sources. The Act on the Digitisation of the Energy Transition (GDEW), which also comprises the Metering Point Operation Act (MsbG) [43], stipulates the legally binding, nationwide installation of modern metering equipment and a binding plan for the deployment of smart metering systems (iMSys). Smart meter roll-out is becoming increasingly delayed, also due to a temporary court injunction imposed by Münster Higher Administrative Court on 4 March 2021, halting the installation of iMSys. The court reasoned its decision by stating that the requirements for the SMGW set out in the MsbG and the valid technical directive TR 03109-1 [15] of the Federal Office for Information Security (BSI) do not satisfy the minimum statutory requirements, in particular with regard to a minimum level of interoperability [73].

Figure 3.2 outlines the material regulatory foundations for secure grid, facility and metering point operation in the energy supply sector.

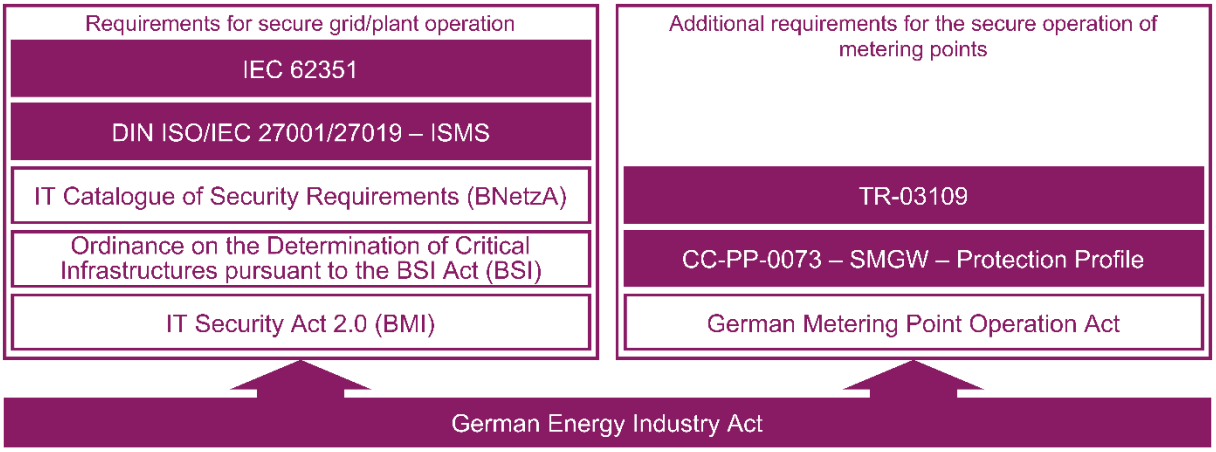

Figure 3.2: The Energy Industry Act defines the legal foundation for information and IT security in energy supply. However, further legal and technical guidelines exist for the safe operation of grids and facilities that are based on or supplement the Energy Industry Act. Similarly, requirements regarding secure metering point operation are enshrined in law by the Metering Point Operation Act and technical directives.

In Germany, the legal basis for cyber security is mainly set out in the IT Security Act 2.0 (IT-SiG)[51], which strengthened the role of BSI in particular in regard to the central organisation of IT security in the energy supply sector. Special requirements apply to critical infrastructures, which are assigned this status by the Ordinance on the Designation of Critical Infrastructures under the BSI Act (BSI-KritisV). BSI KritisV defines thresholds above which technical installations in the energy sector are classified as critical infrastructure [47]. The limits for various technical installations according to BSI-KritisV have been lowered in conjunction with the IT Security Act 2.0, and it is apparent that the energy transition is viewed as a key factor prompting the adaptation of requirements with regard to IT security in the energy sector. The corresponding thresholds are shown in Table 3.1. Also of relevance to grid operators is the catalogue of IT security requirements pursuant to Section 11 (1a) EnWG that was issued by the Federal Network Agency (BNetzA)

[19]. It defines basic protection targets (availability, integrity, confidentiality) for all grid operators and stipulates in particular the implementation of an information security management system (ISMS) according to DIN ISO/IEC 27001 [40], which must additionally include energy-specific requirements pursuant to DIN ISO/IEC TR 27019 [41].

While the introduction of an ISMS optimises or documents internal company processes in particular related to information security, systemic measures must also be put in place to guarantee information security. Grid and station control technology must satisfy the IEC series of standards 62351 [27] in this respect. Risks related to communication links in the telecontrol network are taken into account here, in addition to requirements for the installed components (e.g. telecontrol devices, network devices, control systems). An example of this is the protection of used telecontrol protocols such as IEC 60870 [26] and IEC 61850 [28], which do not include their own measures for secure communication. Energy facilities have their own catalogue of IT security requirements like the one pursuant to Section 11 (1b) EnWG. It applies to all facilities that are designated as critical infrastructure according to the BSI KritisV. The German Association of Energy and Water Industries (BDEW) has also defined basic IT security recommendations for the energy sector in cooperation with its Austrian sister association, which are set out in the best practice white paper on requirements for secure control and telecommunications systems [36].

Electricity production		Threshold
Power generating plants	Net installed capacity	104 MW
	Net installed capacity in those contracted as black start facilities	0 MW
	Net installed capacity in facilities pre-qualified to deliver primary balancing capacity	36 MW
Installations or systems for the control/bundling of electrical capacity	Net installed capacity	104 MW
	Net installed capacity in those contracted as black start facilities	0 MW
	Net installed capacity in facilities pre-qualified to deliver primary balancing capacity	36 MW

Table 3.1: KritisV [47] stipulates new thresholds for critical infrastructures, which come into effect in January 2022. The thresholds for electricity generating facilities and for the control/bundling of electrical capacity are provided here as examples.

There are also specific efforts for the further development of a comprehensive, EU-wide cyber security strategy for various sectors, including the energy sector, within the framework of the EU NIS2 Directive ('Network and Information Systems'). An EU-wide basis for the cyber security standard will be prescribed in this regard by the 'Network Code on Cybersecurity', which was tabled by the European Network of Transmission System Operators for Electricity (ENTSO-E) in a draft version in October 2021. [39]. This offers potential for the harmonisation of cyber security standards across Europe, especially for critical infrastructures, and also creates a level playing field for affected sectors.

With regard to metering point operation, another distinction must be made between the minimum requirements for the IT security of the SMGW itself – which are defined in the associated BSI-CC-PP-0073 protection profile – and the requirements placed in the functional basis and the infrastructure that is relevant to operation. The latter is governed by the aforementioned multi-part TR-03109, which includes

requirements for interoperability (parts 1 and 2), cryptographic specifications (part 3), requirements regarding the public key infrastructure (PKI) used in the system (part 4), the communication interfaces for connecting meters and controllable facilities (part 5) and requirements for gateway administration (part 6).

It follows, therefore, that extensive regulatory specifications are in place to address IT security from both an operative and technical perspective. It is worth noting, however, that the multitude of individual and complementary guidelines can also create problems in the design and implementation of new products, such as the SMGW, so that early coordination in regard to the individual regulations is becoming increasingly important. The need for forward-looking adjustments to guidelines, recommendations and their derivation processes was identified already in the 'Phased model for the further development of standards for digitisation of the energy transition' [53], including specific recommended courses of action. Regular updates of technical requirements and recommendations are necessary as well, and a central compilation of relevant technologies would help to install IT security as a dedicated, changing component within the energy industry. This would enable the categorisation of cryptography procedures according to their security level as a means of ensuring that the frequent modifications and new developments are communicated appropriately. Aside from security regulations in general, there should also be a discussion of incentives that encourage actors to implement security beyond the minimum requirements.

Innovation in the areas of tariff design, grid management and grid-oriented applications is an essential aspect in transforming the energy industry in the face of the energy transition and future challenges. Historical attacks on the electricity grids emphasise the importance that cyber security has already acquired for the energy industry. Cyber security will become even more important in the context of progressive digitisation and must be planned with foresight and implemented consistently. The 'security by design' paradigm offers immense potential for innovation, provided that all parties – regulators, implementing bodies and end customers – are included in the process transparently and their individual requirements are taken into account. The following chapter addresses this issue and explores the role of cyber security in the context of application-oriented innovations within the energy industry as well as the problems and opportunities acquired from experience with the SMGW. Its purpose is hence to identify factors that promote or inhibit relevant innovations.

4 Cyber security as a driver of innovation within the energy industry

Digitisation of the energy industry comes with potential for innovation in various areas of application, of which selected areas are considered below as examples (Section 4.1). With regard to the necessary communication infrastructure, the following considerations focus in particular on the smart meter gateway infrastructure (SMGW), which will form a secure basis for connecting end customers to other actors in the implementation of both market-related and grid-related processes (Section 4.2). But minimum requirements for IT security and data protection must also satisfied to implement innovative use cases, irrespective of the installed infrastructure. The feasibility of this project and potential technologies for its support are examined in Section 4.3.

4.1 Status quo of innovations within the energy industry at national level

The decline in conventional generation capacities is leading to fresh challenges in the area of ancillary services such as operational management, instantaneous and balancing reserve, voltage stability and black start capability (cf. Section 2.1). Renewable feeders and controllable loads at distribution grid level are becoming more important as means of maintaining system security. In addition to balance sheet effects (e.g. due to forecast errors for feed-ins from renewable energy sources), there are also foreseeable challenges that will affect the electricity grids themselves. They concern on the one hand the distribution grid level, where additional expansion of the power grid is already necessary in some cases to fulfil the technical boundary conditions due to high feed-in and bidirectional load flows. New demands are being placed on the transmission grids on the other, as supra-regional transport leads to greater load on the transmission grids due to the widening spatial distance between the power generation and consumption centres. Additional challenges arise, especially in the area of ultra and high-voltage transmission, due to the low societal acceptance of power line construction projects that complicate conventional grid expansion or grid reinforcement according to the NOVA principle (grid optimisation first, then grid strengthening before any further grid expansion) [1]. In addition to conventional expansion of the power grid, technologies that enable more extensive monitoring and control of the technical grid systems in particular offer additional potential for ensuring continued and reliable grid operation.

Asset management and diagnostics. Diagnostic procedures are required during maintenance and replacement in order to predict malfunctions and take suitable action for their prevention. They can also be used to monitor new types of operating equipment as a means of acquiring additional experience in regard to their long-term behaviour. Components are checked at fixed intervals in the time-based maintenance strategy. The condition-based maintenance strategy is potentially a more effective and cost-optimised method. It has the advantage that sensor technology is deployed to determine ageing status, even for concealed parts. This prevents the replacement of devices that are still in good working order and minimises the risk of outages in the event of random defects. Faults are detected and rectified quickly, which helps to improve the security of supply. Condition-based maintenance is used in high and ultra-high voltage grids, but not in medium voltage grids for economic reasons. Condition assessment of local grid stations and other equipment in the medium and low-voltage range is based exclusively on manual and visual inspections. But the use of suitable low-cost sensor technology presents opportunities to implement more efficient and

objective diagnostics for the relevant equipment at lower voltage levels as well.

Protection and assistance systems. The protection technology provides essential functions for safety and reliability, as well as for the rapid disconnection of high short-circuit currents to mitigate damage and prevent its propagation. Safety refers to the avoidance of overfunctioning, while reliability describes the avoidance of underfunctioning. Digital protection devices that make their decisions based on a set of protection criteria are currently considered state of the art. Common protection criteria include overcurrent, impedance and current difference. Besides their actual safeguarding functions, modern digital protection devices have additional automation and monitoring functions, are equipped with modular hardware that is independent of the protective function, and are connected to the grid control centre by means of the communication protocols IEC 60870-5-103/104 [26] or IEC 61850 [28]. There has been no use so far of decentralised communication ('peer-to-peer') between protection devices for binary decision processes with remote metering points or station components (e.g. breaker failure protection, signal comparison procedures) included in the parameter sets of adaptive protection concepts for bidirectional load flows.

In telecontrol tasks, the central control systems commonly deployed by distribution grid operators are primarily used to support maintenance and servicing activities and to monitor the essential operating equipment at medium and high voltage level. But sector coupling and the establishment of connectivity within the increasingly decentralised energy system with volatile generators, new types of consumers and distribution grid storage are leading to a precipitous rise in the need to enable observation and control of the system. As a result, operational management decisions must take a continuously rising quantity of process information and degrees of freedom into account. Assistance systems are already being used in some cases here. They act by processing and visualising electricity grid information for management staff, performing specific grid calculations and providing decision-making support in critical situations. Overall, though, these systems remain at a nascent stage of their development and mainly comprise data processing capabilities at present.

Distribution grid transparency. In general, the distribution system operator (DSO) carries out electricity grid monitoring and grid control for high voltage installations in a similar way as in the transmission grids. This means that the high-voltage grid is completely observable and that condition assessments and grid security calculations are performed cyclically. In most cases, no or only isolated measurements are available for the medium-voltage grid, and a 'distribution grid condition assessment' is carried out instead. Its purpose is to estimate the condition of the grid based on just a few measured values, the topology and, if applicable, historical time series. Some grid operators have fully connected the measurement technology for the medium-voltage grid to the grid control system. The activation process is also extremely laborious for the DSOs as well. Moreover, the control centre monitors grid condition during work on the grid, as is the case at higher voltage levels. Regular grid operation at the interface between the transmission system operator (TSO) and the DSO consists primarily of the exchange of data. For example, information is exchanged by telephone between the control centres when actions are carried out in one grid area that may have relevant effects on the upstream or downstream grid. At present, the TSO receives the power plant schedules for the power plants that are connected to the high-voltage grid from the market participants. The DSO does not usually engage in any market-driven utilisation of flexibilities obtained from power generating plants and consumers. Flexibilities will be utilised in future to the benefit of both the grid and the market along the lines of a multi-use approach. At present, the TSO's influence on the power generating plants is aimed mainly at interventions within the framework of grid security management. TSOs and DSOs also interact within the framework of balancing group management, in which the TSO assumes the role of balancing group

coordinator. The master and transaction data for the time series of balancing group totals are transmitted to the DSO for this purpose. Automation is still largely lacking in the exchange of information between grid operators and market participants in many ancillary service processes.

An intelligent electricity grid is divided into a variety of domains according to the usual model of communication technology. Within this concept, the customer network enables communication between household appliances and the matching smart metering systems or the SMGW. The SMGW acts as the central interface between the connected end customers and all other actors involved (cf. Section 4.2). A modern wide-area network infrastructure should enable real-time monitoring or control of the energy grid. A variety of wired and/or wireless communication technologies can be used to exchange information within the network areas.

Communication networks within the energy sector. In many cases, sensors are only connected via dedicated radio due to the various communication technologies for different applications, as connection via fibre optics, DSL or the mobile network (LTE/4G) is not always possible because of inadequate network coverage or for cost reasons. ISM bands (industrial, scientific and medical) are available as a cost-effective connection via a radio system. The 450 MHz radio frequency assigned to the energy sector releases new capacities compared to the free 433 MHz, 868 MHz and 2.4 GHz frequencies that have been used so far for the connection of different applications. It should be noted that the range of these radio connections may be impaired in complex scenarios, depending on the circumstances on the ground. This leads to disproportionately high expenditure on the construction and operation of the infrastructure, as a high density of access points (feeder networks) needs to be established in order to ensure seamless supply. The development of a nationwide radio network with dedicated usage capacities for the electricity grid remains nascent in Germany, although the first steps have now been completed with licensing of the 450 MHz radio frequency.

In Germany, the Federal Network Agency (BNetzA) and the Federal Office for Information Security (BSI) have been monitoring the issue of system security in supply networks with high penetration and dependence on ICT for several years. Adding to this are the activities of various national and international associations from the electricity sector, among them the European Network of Transmission System Operators for Electricity (ENTSO-E), the German Association of Energy and Water Industries (BDEW) and the Network Technology/Network Operation Forum at VDE (VDE FNN). A variety of detailed security standards therefore exist for the energy sector, some mandatory, in addition to the common security standards such as the ISO 27000 series [40], the BSI IT-Grundschutz [48] and the standards issued by the National Institute of Standards and Technology (NIST) [74].

Within this framework, many of these standard series address the establishment of IT networks in critical infrastructures, including those run by grid operators. The grid operator IT networks can be roughly divided into two categories in this regard: office networks and process networks. Office networks are comparable with other company networks. They are used primarily for ordinary office communication by means of standard applications, email traffic and data processing. The only noteworthy difference between an office network and other company networks is that the office network will occasionally access process-relevant data such as weather forecasts. This means that there are connections to the process network, although they do not allow switching operations. Operator process networks include all IT components that are involved in process operations. Included in this, for instance, are computers in the control centre, programmable logic controllers, switches and routers, as well as the physical communication routes connecting the individual components. There is an imminent danger to grid stability if a cyber attacker gains write access to the

process network. Even read access or the manipulation of data introduced into the process network can disrupt grid operations or disclose sensitive information.

Operators find themselves in the unusual situation of drawing almost exclusively on dedicated lines (mostly fibre optics) for process networks, despite the large geographical area, which means that the networks are spatially separated from the public networks. While this does offer a far greater degree of security, it leads also, for legacy reasons, to the use of insecure or unencrypted protocols. Moreover, the available equipment portfolio with operating life times of 20 to 30 years complicates the introduction of security mechanisms that actively influence communication such as encryption and authentication. This creates a situation in which essential state-of-the-art security mechanisms are not deployed within the process networks.

Market communication and the regulatory framework. Market connection measures are governed by a variety of regulatory requirements such as Commission Regulation (EU) 2017/1485 establishing a System Operation Directive [64], the ENTSO-E Continental European Operations Manual, the Transmission and Distribution Code, the Energy Industry Act (EnWG) and the Renewable Energy Sources Act (EEG) [42]. They therefore establish the interface between the electricity market and grid operation. The communication process within the energy industry is based on the applicable statutory requirements. The EnWG [44], the German Metering Point Operation Act (MsbG) [43], the Grid Expansion Acceleration Act (NABEG 2.0) [45] and the Electricity Grid Access Ordinance (StromNZV) [46] are of central importance for market communication.

In its decisions that are binding for all market participants, BNetzA has drawn on the legal framework outlined above to define standardised market processes. Involved in the establishment of processes are actors and associations within the energy industry who prepare, for example, proposals for changes or joint ideas for solutions. But the inclusion of various market participants and actors within the energy industry in the development of new solution approaches is still in its infancy. Absent any subsequently foreseeable conversion to decentralised measured value distribution, the BNetzA has stipulated that, notwithstanding the requirements of BSI TR-03116-4 [14], the period for the permissible use of certified private signature keys or combined certificates shall be extended both for signature generation and for decryption of the data sent to this email address in accordance with BK6-18-032 [21]. It is nevertheless the intention of BNetzA (from 1 October 2023) that the use of Applicability Statement 4 (AS4) as a web service based on Transport Layer Security (TLS) and a BSI smart metering public key infrastructure [11, 12, 16] shall apply as technology standards for the greatest possible interoperability with electronic market communication in Europe [20].

The national strategy for digitisation of energy industry processes is currently dominated by the adaptation and expansion of the existing regulatory framework, which is potentially limiting or delaying the opportunities for technical implementation. Affected industries are still uncertain about the Act on the Digitisation of the Energy Transition (GDEW). It states that the SMGW shall be the central and sole communication interface for the connection of relevant generators and consumers. In some cases, relevant actors are already far more advanced in the implementation of their own solutions, for example in relation to value-added services. When dealing with proprietary solutions, though, it is reasonable to enquire into the extent to which interoperability, security and data protection can be guaranteed.

Decentralisation of feed-in is leading to a growing need to expand or strengthen the grid. In addition, operating equipment in the lower voltage levels is exposed to greater loads that cannot be subjected to advanced monitoring and diagnostic techniques due to an absence of sensors, leading to inadequate transparency in regard to their condition. There is also a need for greater grid transparency for connecting decentralised power generating plants and end customers to the distribution grid. But this is beset by delays in implementation due to the temporary halt on expansion (cf. Section 3.3) for SMGW infrastructure and the hesitant use of this infrastructure for the roll-out of value-added services in Germany. A reliable infrastructure can potentially be built using a nationwide wide radio network with dedicated usage capacities for the electricity grid such as the 450 MHz radio frequency. Nonetheless, portfolio operating equipment with a lifespan of 20 to 30 years is frustrating the implementation of established and new security concepts, which are essential to the sustainable introduction of new cyber innovations in the energy sector.

4.2 Case study: Measuring point operation and SMGW infrastructure in Germany

The smart metering system (iMSys) as the central component of the SMGW infrastructure in Germany has already been discussed in Section 2.3.1. In addition to the SMGW itself, the valid regulatory framework defines the entirety of necessary infrastructure and the tasks of the actors involved. Within this framework, the requirements address issues relating to the infrastructural roll-out and deployment (Section 4.2.1), as well as specific security requirements defined for the SMGW itself (Section 4.2.2).

4.2.1 SMGW infrastructure and roll-out

The expansion of SMGW infrastructure in Germany is currently in the roll-out phase and has been delayed temporarily by various regulatory processes.

Smart meter roll-out. The smart meter roll-out in Germany will take place incrementally and will be completed for the majority of end customers by 2027. It will be carried out by the competent metering point operator in each case, and roll-out for all power generating plants with a nominal output above 7 kW will take place by 2024. The procedure for consumers depends on annual energy consumption and will be completed by 2024 for an annual energy consumption above 10,000 kWh and by the end of 2027 for consumption of between 6,000 and 10,000 kWh. The latest available figures indicate that the overall roll-out rate for modern metering devices relative to all existing grid connections is around 10.9 per cent, with an upward trend in terms of the number of systems installed per year (as of the end of 2019). [54].

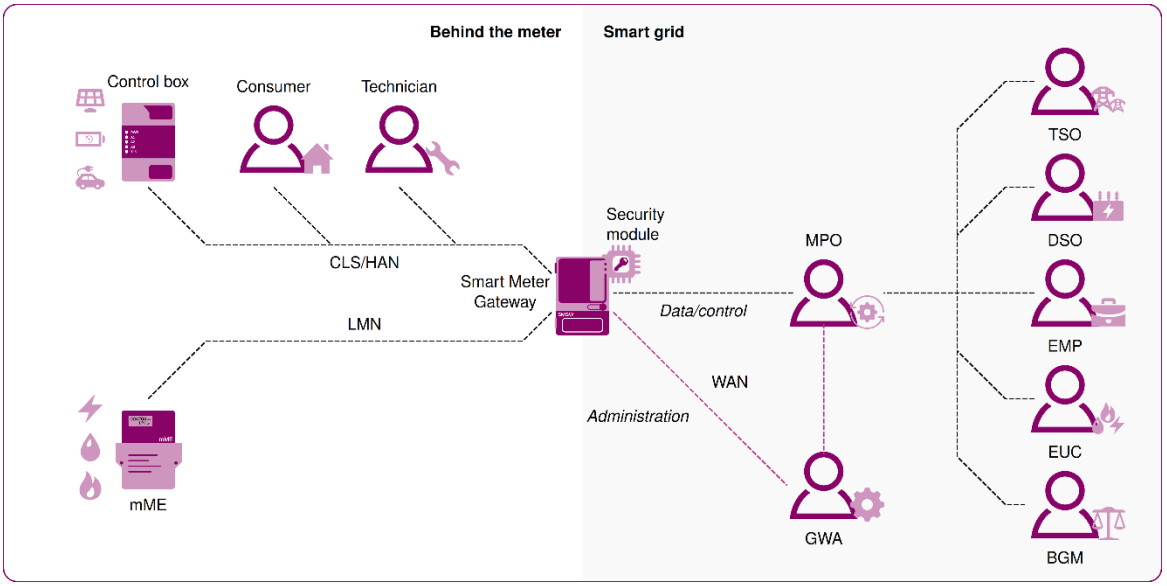

Figure 4.1: SMGW infrastructure and actors participating in communication according to the market communication model 2020 [18].

Market communication and participating actors. An overall infrastructure consisting of various isolated communication network areas and participating actors has been put in place with the market communication model and the specifications for the SMGW infrastructure itself. Figure 4.1 is a schematic diagram showing the relevant actors and grid segments. In this context, the SMGW is used for the secure connection of end consumers to external actors, which potentially enables them to provide additional data and control options.

The metering point operator (MPO) is responsible installing, operating, maintaining and reading the meters. It is at the discretion of both end customers and the energy providers to select their MPO, as long as a modern metering device is used. Unless otherwise specified by the customer, the local distribution system operator is generally responsible for operating the metering point.

The gateway administrator (GWA) is in charge of technical operation of the iMSys and, in this role, is responsible in particular for installing, operating and maintaining the SMGW as well as for connecting the metering systems and other technical equipment to the SMGW. The tasks and obligations are set out in the technical directive TR-03109-6 [10]. The processes associated with operating the SMGW include, among others, processing support and the provision of metering data to other authorised actors. The tasks of the GWA are assigned to the MPO as well, although the MPO can farm them out to a certified contractor. BSI certifies companies in their role as GWAs, subject to their compliance with relevant statutory requirements. Among others, they include the establishment, operation and documentation of an information security management system (ISMS) as well as the implementation of requirements defined in the relevant technical directives for gateway operation. 42 companies hold this certification at present (as per November 2021) [49].

Relevant market actors that may be authorised to access metering data are the local grid operator, the energy utility company (EUC) for billing purposes and other external market participants (EMP) such as the operator of a virtual power plant.

Integration of value-added services. Aside from the provision of measurement values, additional control options for the management of generation and load are required in particular for the delivery of value-added

services. A suitable opportunity to control feed-in from power generating plants and consumption at building and device level is to be realised according to Section 14a Energy Industry Act (EnWG) within the framework of a specification for a control box, which will be prepared by the VDE-FNN (technical regulator). Another step towards standardising communication was taken by extending the control box specification to include a 'digital interface'. The corresponding FNN note makes explicit reference to its implementation by means of EEBUS [89]. 'EEBUS' is the name given to the development of a communication interface to enable generic communication between systems behind the grid connection, among them PV systems, storage systems, heating systems, white goods and electromobility systems.

A key challenge is to simplify the platform's use by external market participants. Overcoming this issue would help to improve the general acceptance of iMSys and SMGW as a central platform for implementation of value-added services. The BSI and the Federal Ministry for Economic Affairs and Climate Action (BMWK) are pursuing an approach to achieve this end by developing a phase model for the standardisation of energy industry use cases that should be implemented by means of the SMGW infrastructure [53]. The objective in this regard is gradual digitisation of the energy sector. A focus is placed on obtaining feedback from the energy sector to ensure highly practicable standardisation of the relevant use cases. As a rule, the phase model distinguishes between energy industry use cases and the system use cases and functional modules that would be required for their implementation. Examples of use cases in the energy industry include:

1. Control of low-voltage consumption devices in accordance with Section 14a EnWG
2. Charging of batteries for electric vehicles at publicly accessible charging infrastructure
3. Participation in the balancing energy market
4. Provision of data for value-added services

System use cases and functional modules include:

1. Power limitation/power monitoring by means of SMGW
2. Processing of measurement values for billing the metered charging current at the charging point for different users of the charging infrastructure

The procedure of engaging in practical consultations with experts from the energy sector to establish the use cases to be implemented using the SMGW infrastructure might be a promising approach to improve industry-wide acceptance of the SMGW platform and accelerate delivery of value-added services to end customers. Such approaches are already being specifically targeted by projects such as DigENet. It is important here to strike a reasonable balance that would improve usability and acceptance of the 'SMGW platform' and to minimise the risk that the industry will develop proprietary solutions for the delivery of value-added services in a manner that bypasses the available infrastructure.

4.2.2 Security-compliant use of SMGW infrastructure

The SMGW itself is designed as a secure gateway to connect communication between end customers and other participating actors. Accordingly, the system must satisfy requirements that are relevant to security, for instance in the provision of network interfaces and the integration of a security module used to encrypt the data transmissions and for other purposes.

Network architecture. As shown in Figure 4.1, the SMGW provides physically dedicated interfaces for the relevant networks and in doing so acts as a gateway between them. The measuring systems are integrated in

the local metrological network (LMN). The home area network (HAN) connects all relevant systems to the end customers. This may include decentralised power generating plants, control boxes or energy management systems. Systems within the HAN are grouped together to form a controllable local system (CLS). The wide area network (WAN) is used for communication with the GWA and all external market participants. Market participants use the SMGW to establish a secure, encrypted connection to the end customers' systems by means of the CLS channel.

A variety of transmission media can be deployed as a rule for the WAN. They include dedicated 450 MHz infrastructure, public mobile communication (LTE) or power line communication (cf. Section 2.2).

Encryption and certification. The certificates for the SMGWs themselves are issued by BSI. At present, four products from different manufacturers are certified in total. The certificates were first issued between December 2018 and December 2019. Five other manufacturers are currently completing the certification process for their products (as of November 2021) [50].

TLS 1.2/1.3 is used to encrypt SMGW communication. This ensures secure communication with external market participants, irrespective of the infrastructure used. Asymmetric cryptography methods like those used in TLS potentially possess two vulnerable points. When establishing a connection, the server and client (in this case, for example, an external market participant and the SMGW) exchange cryptographic messages using asymmetric key exchange algorithms (e.g. RSA/ECDH) to derive a symmetric key. This key is then used to encrypt the rest of the session. In addition, proof of identity during authentication involves providing the public key, which draws on suitable exchange algorithms (RSA/ECDSA) as well. Potentially, these asymmetric algorithms can be replaced going forward by quantum-safe algorithms or used as part of a hybrid exchange procedure.

Security module. The SMGW has a dedicated security module for encryption and storage of the relevant keys whose requirements are defined in the technical directive TR-03109-2 [9]. The security module provides the SMGW with cryptographic functionalities such as key material generation, key exchange, digital signatures and general encryption and decryption operations. Moreover, it generates random numbers for cryptography and acts as a repository for key material, the root certificate for the smart metering public key infrastructure (SM-PKI) and quality label certificates. But other (public) certificates are stored in the gateway (GW). The specifications of TR-03109-3 [8] are implemented to set the length of the keys.

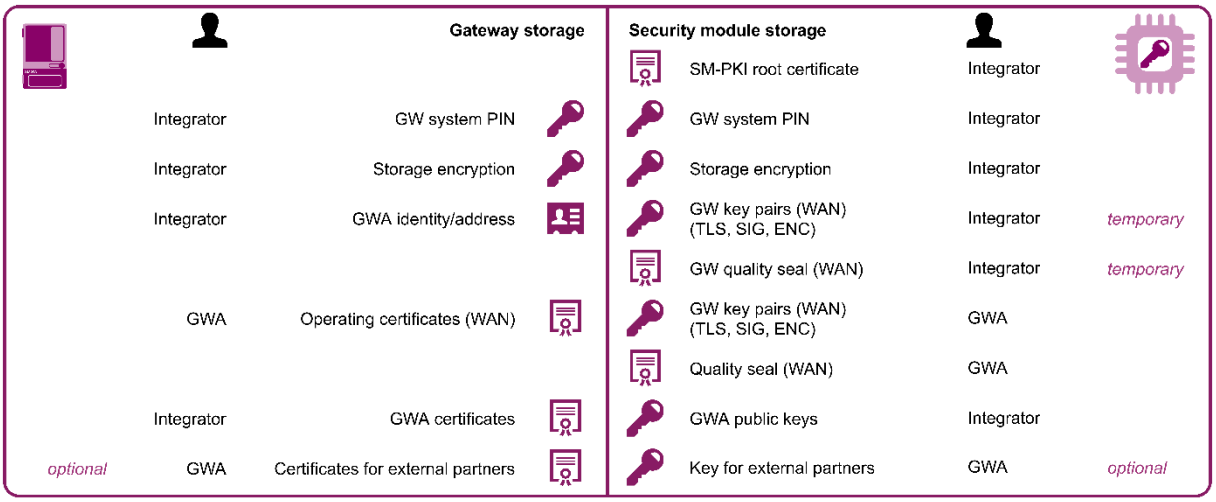

Figure 4.2: The key and certificate material for secure operation of the SMGW is installed, renewed and added to by the integrator and the GWA during the life cycle (based on [9]).

SMGW security is built on adherence to a six-stage life cycle that leads from production processes through integration, installation and personalisation, and on to operation, as well as an additional decommissioning stage [9]. The current stage in this cycle is also stored in the security module, but only with a distinction between ‘not initialised’, ‘initialised’ and ‘terminated’. Initial and permanent key and certificate material is installed in the GW and in the security module during the life cycle of the SMGW. Figure 4.2. provides an overview of these keys and certificates.

The integrator performs the personalisation and integration measures for the security module. It imports the current root certificate of the SM-PKI and then generates preliminary key pairs for TLS communication, signatures and keys as well as certificates for WAN communication by the GW. In this context, the public keys are also exported and matching quality label certificates stored in the SM-PKI for authentication during key exchange. A PIN is created additionally to connect the security module to the GW and keys for memory encryption are generated. The identity of the future GWA must be known for further configuration. The GWA transmits to the integrator a signed configuration file for the security module containing the GWA’s public certificate chains for authentication and encryption. The integrator then loads them into the GWA’s certificate memory, where they are verified by the GW using the SM-PKI.

Once these measures are complete, the initial configurator can install the SMGW at its intended destination and it can then be personalised by the GWA for normal operation. To do this, the GWA uses the previously installed, temporary WAN communication key and the GWA key material. After successful authentication, the GWA then replaces the temporary key material installed by the integrator with newly generated keys and certificates to enable secure operation. The SMGW is prepared for normal operation once this is complete. The GWA must set up suitable profiles with key material for authentication and encryption to enable other entities like service technicians to interact with the SMGW. Key and certification material for communication via channels other than the WAN must be created for this, depending on the connection. TLS-secured interaction with the SMGW is then enabled by means of the matching interface.

The SMGW and associated infrastructure provide a fundamentally secure environment for application innovations and the implementation of value-added services. The integrated security module, which is implemented with cryptographic operations such as encryption, signature generation and verification and key exchange, acts as the central security component within this framework. Specific technical requirements, including key lengths and algorithms, are updated annually to guarantee security in the long term. Certification according to the minimum requirements for both of the involved actors (GWA) and the SMGWs themselves is carried out by BSI. The current approach of implementing feedback from energy sector professionals in the standardisation of use cases based on the SMGW infrastructure is positive and should be intensified to strike a reasonable balance between data protection, security and the feasibility of use cases.

4.3 Transition to a cyber-secure environment for the energy sector

The previous section introduced the SMGW infrastructure and the challenges associated with its specification and use. What sets the SMGW infrastructure apart is that it connects virtually all relevant players in the energy sector (grid operators, suppliers, end customers, providers of value-added services, etc.). The issues of information security and data protection were initially top of the agenda during specification, also because the infrastructure is used to transmit both customer-specific and network-relevant data. However, alternative solutions for the short-term implementation of some use cases may also be conceivable for the industry, especially for the transitional period until complete roll-out and unrestricted usability of the infrastructure have been achieved. The SMGW infrastructure specifications can still be used to derive basic requirements for the permissible or necessary communication patterns and IT security of these alternative solutions.

An example of this would be the communication technology for the connection of charging infrastructure. Two functional requirements deserve special mention in this regard: capacity control (in a manner that is beneficial to the grid) and billing of the charging process, whereby a distinction between private and public charging infrastructure is necessary. In this context, grid load shifting potential – again in a manner that is beneficial to the grid – can be harnessed by means of intelligent charging infrastructure for electric vehicles. The substantial load shifting potential associated with electric vehicles can be exploited as a flexibility option to balance out the demand curve or to adjust feeding-in of electricity from renewable energy sources. This means that the three previously separate areas of electricity, personal mobility and ICT will merge in future e-mobility systems. Aside from the aspects that are beneficial to the grid, innovative business aspects such as machine-to-machine payments and transaction processing on a distributed information system require the vehicles and charging infrastructure to possess computing power and connectivity.

With more than 150,000 publicly accessible charging points in Europe and their greater integration into energy supply systems going forward, the charging infrastructure is particularly deserving of protection and must be secured against potential cyber threats. Security concepts for several use cases must be integrated within electromobility (e.g. charging management, billing, charging point reservation). Doing so will secure essential processes and interfaces between the market participants such as charging in compliance with calibration law (the display of numerical sequences on metering devices and assigned per charging point according to calibration law) and authentication (automatic authentication based on the charging contract stored in the vehicle within the framework of plug & charge).

It is vital in this context to protect the operational and organisational platforms used for electronic exchange in a manner that accounts for basic security elements such as confidentiality, integrity and authentication, for example in regard to the PKI stipulated by ISO 15118. Moreover, challenges for e-mobility arise in connection with the protection of personal data, data ownership and de facto access control by the vehicle manufacturer, as uniform regulations on mandatory data sharing are yet to be introduced. Within e-mobility, these uncertainties largely relate to the use cases of charging management and the associated need for information on battery test capacities, charging speeds, expected departure times and also the vehicle's anticipated charging curves.

Standardised digital interfaces to improve data quality within the reporting processes permit facilitated access to the electromobility ecosystem. Standardisation can also reduce complexity in this context, ensure uniform communication between market participants and in doing so create security of investment for new technologies. For sustainable digitisation, the market participants must guarantee data and cyber security within the framework of minimum standards similar to those for the SMGW infrastructure. The absence of uniform standards for the electromobility ecosystem necessitates a review of existing concepts and international standards for modern security architectures and cryptographic procedures and, where applicable, their transfer to the specific requirements of electromobility.

Ownership and protection of data, as well as the safeguarding of systems and processes against manipulation and exfiltration of data, are therefore important topics in the field of e-mobility that must be taken into account additionally for the sustainable operation of systems. Besides e-mobility, the sustainable realisation of new use cases in the energy sector is characterised by data protection, interoperability and cyber security requirements imposed by the regulatory bodies, standardisation systems and existing directives, respectively. Cyber security is a special component within sustainable implementation of the use cases, whereby both current and new cyber security solutions are applied in the integration of security concepts. Reactive security measures also make a complementary contribution to security, in addition to the preventive 'security by design' concepts that are part of the system architectures (e.g. encryption, network segmentation, access control, authentication, integrity protection). Common systemic solutions for detecting and monitoring communicative events in this context include established methods such as IDS (intrusion detection system) or SIEM (security information and event management) for the passive improvement of the security situation by increasing situational awareness about communication events within the system. In most cases, however, these solutions are introduced downstream of preventative security concepts, whereby reactive measures along the lines of incident response strategies are deployed when preventative measures fail.

The integration of all security technologies seems at odds with reality, in view of security concepts whose goal and modes of operation appear to conflict – such as encryption of communication channels to protect the confidentiality of data and IDS that actively or passively intercept data for attack detection. Possible technical solutions to resolve this conflict might be middlebox solutions similar to the SMGW approach, in which, for example, the head-end for encryption and authentication can be integrated into the IDS and used as a secure proxy in the existing communication channel. In this case, however, deployment of the solutions would include active involvement in the communication networks and processes, whereas passive IDS solutions would offer the advantage of not interfering with operations through active participation in the communication processes. Other approaches go in the direction of federated or distributed monitoring, in which local IDS listen directly to the data producers and send alarms or messages to a central security solution (e.g. SOC or SIEM). Another option would be to use a host-based IDS acting as a set of security

sensors for solutions delivering compliance with protection requirements and encryption capabilities. However, backwards compatibility with regard to the device performance resources must also be taken into account in this regard, as additional overhead may be needed for device computing capacities, which in itself could produce active (negative) interference during operation. These kinds of legacy restrictions may be a key criterion for the integration of other security solutions such as encryption. Transitional solutions in this regard may include passive IDS without encryption due to the absence of backward compatibility, as well as middleware solutions. Harmonisation of these security technologies can be achieved through purposeful security concepts in which the technologies are deployed to complement each other and enhance added value for security.

Some use cases – among them the communication connection for charging infrastructure – require concepts that can be put into practice quickly in order to enable a transitional solution until the SMGW infrastructure is up and running completely. But they must still ensure a minimum level of data protection and IT security, as the systems are used firstly to transmit customer-specific data and secondly because they allow various options for grid control, for instance by managing power during the charging process. Relevant requirements for the SMGW are applicable to these temporary solutions as well.

Likewise, the transition of the process networks for grid operators will probably take place as a multi-step process. Some legacy devices do not possess adequate performance to implement state-of-the-art security mechanisms such as encryption, without expanding the existing infrastructure. In this regard, deployment of an IDS represents a non-invasive option that can be implemented quickly to monitor process network communication and detect anomalies.

In future, SMGW infrastructure will act as the central communication infrastructure for connecting end customers to other market actors. A minimum level of IT security and data protection is guaranteed with the SMGW as the central gateway and integrated security module, especially for the implementation of value-added services. However, in order to be able to implement a maximum of value-added services with the SMGW, upgrades will still be necessary in the future. Moreover, the nationwide smart meter roll-out will probably still take some time. Standardisation of the envisaged use cases to be implemented with the SMGW infrastructure is necessary first of all in this regard, in close coordination with specialists from the energy industry. Secondly, transitional solutions will be required for the initial period, for instance to enable the connection of communication technology to the charging infrastructure. But they too must also comply with the minimum requirements for data protection and IT security. Cyber security technologies that can be deployed at short notice are also needed for portfolio infrastructure such as process networks run by grid operators. Although these infrastructures are separate from the public networks, most do not provide adequate protection against IT attacks due to their sizeable inclusion of legacy components. Here, IDS are solutions that can be implemented quickly to monitor data traffic and detect attacks. In addition, however, communication must be protected by encryption, although doing so will probably require widespread replacement in sections of the current infrastructure.

5 Measures for funding cyber innovations in the energy industry

Creating secure technical foundations – from communication technologies and secure data processing to comprehensive solutions such as the smart meter gateway (SMGW) – is a basic requirement for cyber innovations in the German energy industry. But the development of these technologies, their integration within the complex current topologies and the evaluation of their security levels will necessitate additional funding, also from the state. A broad spectrum of possible funding measures is available to establish Germany as a location for innovation in the digital energy industry, which can also draw inspiration from international best-practice examples. This chapter starts by presenting general measures for the funding of cyber innovations (Section 5.1). It then proceeds to compare and discuss developments in the area of cyber innovations at international level, with a focus on the smart metering infrastructure (Section 5.2). The chapter ends with an analysis and discussion of specific solution strategies for cyber innovations in Germany (Section 5.3).

5.1 Funding measures for cyber innovations

There is a wide range of opportunities to obtain funding in the various sectors and at the different levels of the energy industry. International experience and expertise could also help Germany to make progress in the field of cyber innovations for the energy industry. For this purpose, two workshops were held with national and international representatives from the energy industry and politics during preparation of this report. The results of these workshops are included in the following discussion.

General structure of the funding policy. Funding policy pursues a variety of objectives: from cyber security and digitisation to the energy transition and market diversity or Germany's status at the vanguard of the energy industry, government funding policy may address a broad range of aspects in different ways. Essentially there are two approaches, each with their own advantages and disadvantages.

German funding policy primarily adopts a top-down approach, in which the state, as the funding authority, awards funds to clearly defined projects. Funding is tied to projects that address, develop and/or implement predefined core aspects. This means that funds can be allocated specifically to actors whose projects are consistent with the views of the funding authority. It also enables the promotion of particular issues and technologies. But alternatives may be disregarded or inadequately considered if the wrong targets are set, which could restrict the actors in their freedom to innovate.

This is in contrast to the bottom-up approach, which is used successfully in Israel and elsewhere. Funds are made available across a wider range of areas in this case, and actors are invited to submit funding applications for specific proposals. The less stringent criteria means that funding can be allocated for approaches that would have been discarded at an early stage in exclusively top-down scenarios. While this procedure assigns greater influence to the beneficiaries and generally enables for a broader range of approaches, it also comes with an elevated risk that funding will be awarded to approaches that ultimately fail to achieve their goals.

Specific funding policy measures. Practical experience from other sectors and countries has yielded a number of incentive opportunities to promote cyber security and cyber innovation. Among them are the bug

bounty programmes that offer hackers a reward for identifying security vulnerabilities, depending on how critical they actually are. The software developer agrees to pay the price and the hackers can take legal action if the software developer fails to honour the obligation. This means that in the bug bounty programmes, the software developers not only undertake to pay for the identification of security vulnerabilities but also give hackers the security that their claims can be exercised in a court of law. The introduction of crowdsourcing to detect, assess and report software flaws by the cyber security community appears in particular to augment traditional methods of addressing relevant threats. Nevertheless, rigorous internal security analyses will remain an essential element in the modernisation of applied cyber security. Bug bounty programmes have the potential to raise awareness for cyber security threats in the digital, networked environment if the results, such as newly identified software bugs, are shared transparently.

But staff must receive regular cyber security awareness training to continue strengthening this aspect within human-in-the-loop processes. Courses of this kind draw the attention of employees to issues of cyber security and information security and highlight where they intersect with personal responsibilities and actions. The aim is to achieve a level of control over information security that is adequate to protect the company's data and networks. It follows, therefore, that practical workshops and study programmes with cyber security awareness courses must be introduced in order to teach employees about attacks and cyber security. The courses should be designed in such a way that the acquired knowledge can be put into practice straight away with a view to minimising the 'risk of human error' in a company's IT security. The issue of best practices within company policies can support employees in this area as well. Cyber innovations – for instance virtual training environments for incident response – can support and encourage the process of training and raising awareness here as well.

However, ongoing development of cyber security standards remains the basis for developing solutions that improve IT security in specific sectors. Besides defining specifications, these standards should provide practical instruction that addresses the prevention and detection of security incidents, as well as possible responses once they have occurred. The overall objective of cyber security standards is to improve the security of IT systems, networks and critical infrastructures. As a rule, cyber security standards define requirements for the functionality and reliability of the relevant systems, as well as guidelines for the management of information, criteria for the evaluation of security measures, techniques for remedying security deficiencies and procedures for monitoring security breaches. The state can actively promote and guide the research, development and implementation of these standards by providing suitable content and financial support.

Development of new services. The development of new use cases for the energy industry that can only be put into practice with highly connected and powerful infrastructures might create new service opportunities for the provision of infrastructures, platforms and software as well as the implementation of collaborative tasks. The advantages of scalability play a particularly important role. They ensure that the infrastructure can be dynamically adapted to current requirements, but also according to the existing level of process automation. Cloud-based back-ends are a prominent infrastructural solution for the technical design of scalable and cost-effective use cases. In this scenario, the cloud merely provides a virtual data centre in the form of 'infrastructure-as-a-service'. 'Platform-as-a-Service' provides a platform for the development of applications, while 'function-as-a-service' only delivers the business logic and 'software-as-a-service' accommodates the entire chain, from hosting to implementation of the business logic in software. Part of the responsibility is transferred to the service provider here, depending on the structure. This refers to the implementation of appropriate measures regarding IT security and data protection as well as the

responsibility for configuring and operating the infrastructure, the deployed software and for executing the business logic.

Cloud-based back-end solutions are increasingly suitable for use in the energy industry, for instance in EMP back-end connections or for charging infrastructure in the area of electromobility. Beyond cloud-based back-ends, Redispatch 2.0 enables new service providers such as direct marketing companies to accept the tasks of plant operators and carry them out in line with the specifications. This may also lead to the emergence of innovations prompted by cyber security, especially associated with the provision of secure infrastructures and 'software-as-a-service'. In addition, service provider may take charge of the maintenance of components and software, as well as special services that are geared primarily at identifying and eliminating current security vulnerabilities in the system. Incident response services could then emerge, with responsibility for monitoring, evaluating and responding to IT security incidents ('SOC-as-a-service'). Synergies and interfaces between service providers can be exploited here to deliver mature cyber security solutions as a service to stakeholders, in which infrastructure, software, life cycle management, security operations and incident response are included as interconnected solutions. Another area with broad opportunities for funding programmes is the development and standardisation of suitable cloud systems that consider the specific requirements of the energy sector and implement future-proof security standards. Financial and operative support can foster the development and establishment of suitable technologies and services.

> Regardless of how funding is provided in the specific instance – also as financial grants – the top-down and bottom-up approaches both come with pros and cons in regard to their likelihood of strengthening cyber innovations. While prior state knowledge allows the more targeted and organised allocation of funding services within top-down approach, the bottom-up approach enables greater flexibility and a broader range of innovation potential. Funding policy decisions must always be rooted in an awareness of the advantages and disadvantages of each approach in order to strike a suitable balance between the different methods. A structured top-down funding policy can and should be complemented by more liberally designed bottom-up projects. In addition to promoting the development of new technologies and the implementation of corresponding standards, other company-specific measures – especially bug bounty programmes and security awareness training – can be useful methods that should be applied across the board in regard to cyber security within the industry. There is also a noticeable trend involving the increased outsourcing to external providers of individual services as well as the establishment and operation of necessary infrastructure for the implementation of new use cases 'as-a-service', whereby the deployment of cloud-based infrastructure in particular is a comparatively scalable and cost-efficient approach.

5.2 Roll-out of smart metering systems in an international comparison

The roll-out and active deployment of smart metering systems has progressed to very varying degrees at European level. Italy initiated the large-scale introduction of smart meters for end customers just after the turn of the millennium. [86]. Around 36.7 million meters were installed here between 2001 and 2011. The relevant legal framework allowed the distribution system operators to add the resulting costs to the grid fees. Faced with the impending obsolescence of existing meters and the need to improve their functions, the regulator has established a framework for the introduction of second generation smart meters. The first-generation meters no longer satisfied the minimum technical requirements and were unable to deliver measured values updated in 15-minute increments. In fact, the technical and regulatory life time of a meter

is about 15 years. Compared to other regulators in Europe, the Italian authorities were therefore confronted with two challenges quite early on: firstly, the widespread provision of smart meters to all consumers, and secondly, the practical utility of meters that had already been deployed [81]. When introducing a new incentive system, the regulatory authority must ensure that all stakeholders share in the benefits so that costs and benefits are balanced. Examples for the implementation of these requirements include the obligation for full disclosure of demonstration project findings and the demand to enable improved and more extensive services for consumers in the roll-out of next-generation meters. It follows, therefore, that preserving the competitive element is important for the innovation process, as it ensures not only greater cost efficiency, but also provides a strong incentive for participants to find effective solutions that can be used in the roll-out phase – as was the case with the smart meter roll-out in Italy.

Another case study is the Netherlands, where a smart meter bill was introduced in 2008 proposing a 100 per cent roll-out, which would be mandatory and carry heavy fines or even custodial sentences for anyone refusing [55]. The technical specifications for the meters proposed in this context included in-house display units, an alarm for unexpected consumption peaks, real-time measurements as well as options for remote device programming and communication with other meters. The utility companies launched a test phase in 2012. It involved the installation of 600,000 smart meters to acquire early experience and to detect potential problems so that any necessary adjustments could be identified in time for the second phase – large-scale roll-out. Mass introduction began in 2014 with more than 1 million installations within a year. 78 per cent of the roll out had been completed by 2019. Customers were not asked to pay for installation, but the grid operators transferred the costs to the grid fees in this case as well.

Initial plans for the roll-out of smart meters in the UK envisaged the deployment of 53 million gas and electricity meters by 2020 [55]. The government also decided to place the energy providers in charge of roll-out. Upfront costs were also carried by the providers and are passed on to consumers' bills. Initial experience acquired during the roll-out indicated that smart meters only work to a limited extent, especially in high-rise buildings, basements and rural areas. At the beginning of 2015, 134,000 of the 1.3 million newly installed smart meters only worked like classic meters and required manual reading due to technical limitations. Another problem was that the first-generation meters were not universally compatible with other providers, which made it more difficult for end consumers to switch to a different company. Large-scale introduction began in 2016, but incorrect installation meant that over 10 per cent of households required multiple visits to complete the work.

Different approaches for the roll-out of smart meter systems were applied in each of these countries. The roll-out of new technology can be organised on the one hand by defining short-term targets and making cyclical or early adjustments if technical problems are identified during implementation. This roll-out approach can be observed in Italy and the Netherlands. The objective in these cases was to achieve fast roll-out, although this required considerable technical and regulatory adjustments following the initial phase. The UK, on the other hand, adopted a more technocratic approach. At times, introduction of the metering systems experienced technical difficulties and was beset with problems relating to social acceptance, which occasionally delayed the process.

Introduction in Germany again follows a top-down approach, in which all requirements for the infrastructure are derived primarily from regulatory requirements. Compared to Italy, where the focus of the initial roll-out was mainly to use smart meters as a means of reducing electricity theft [58], the roll-out strategy in Germany focuses on the technical functionalities of the smart meters, on certification and the secure communication interface [60]. In particular, the plan is to ensure that the devices need replacement as rarely as possible and

that they can be designed for a maximum service life, taking into account the calibration cycles and compatibility with new technical functions. Roll-out at national level has been delayed at times due to various regulatory problems and is sometimes facing low levels of acceptance due to a lack of standardisation and issues with the usability of the infrastructure, among other things. Overall, a reasonable balance needs to be struck between rapid implementation – in the form of pilot projects, for instance – detailed planning and government funding, in consultation with all stakeholders involved in the roll-out of new technologies.

> While demonstrators and 'learning by doing' can yield valuable insights regarding the feasibility of a new technology in the early phases of its roll-out, centralised planning and technology support measures are particularly necessary to drive cost-effective roll-out during later phases. While the companies entrusted with implementation and policy makers are important stakeholders, indirect actors must also be involved throughout the implementation process for the propagation of new technology if it is to achieve widespread adoption. In the case of the SMGW, these actors include consumers, the general public and other relevant market players. Embedding the issue of funding for specific technologies into broader transformation programmes might be a more effective strategy than merely funding technologies as stand-alone transformation tools.

5.3 Solution strategies to fund innovation in the German energy industry

In principle, a variety of options exist to fund innovation in the energy industry. The plethora of new use cases relating to the decentralisation of power generation in the electricity grid and digitisation of the sector provides potential for establishing new technologies in many areas. The following section discusses suitable funding and the design of further development processes.

Political funding of innovation Adopting a third way between the targeted funding of specific technology and more liberal funding that is aimed at more general research projects and not earmarked for particular technologies can lead to efficient promotion of innovation in the national energy industry (cf. Section 5.1). In this regard, the funding of specific technology is based on findings from previous research that identified auspicious technologies with market potential. By contrast, funding that is not earmarked for particular technology explores possible alternative solution approaches and hence defines an objective without a specific transitional pathway.

In concrete terms, the funding of pilot projects and demonstration environments can also help to positively influence the acceptance and applicability of new technologies and ensure that technology developments from research are translated into productive systems. Moreover, funding the expansion of demonstrators to use and develop new technologies in operational environments is a meaningful way to validate the technological maturity of cyber innovations, especially in the area of IT security. Doing so can also improve the effectiveness of the developed technologies, as suitable tests cannot usually be performed in full or without risk within productive operation. For example, synthetic attack trials can be conducted in a secure, closed and controlled environment in the development of IT attack detection technologies.

Both research into and the use of new technologies in the energy sector are determined by current developments of the relevant regulatory framework and the minimum requirements for the technical implementation of use cases specified therein. Establishing transparency in regard to viability and acceptance should be a defined objective in the development of regulatory measures. This must be built on continuous exchange between the competent authorities and the relevant actors in the energy sector at the

earliest possible stage in the development of new regulations. Adopting this approach would enable the timely emergence of regulations that are representative, comprehensible and implementable for the industry.

Stringent simplification, abridgement and digitisation of planning, approval and certification processes offer additional potential for the funding and acceleration of innovations. Shortening or accelerating planning and approval processes can create a conducive environment for the faster integration and use of new technologies in productive operations. In this context, the greater powers vested in the Federal Office for Information Security (BSI) by the IT Security Act can help to establish a central contact point for IT security in critical infrastructures. Outsourcing certification to external providers (remaining under the supervision of the BSI) may be a sensible option to speed up the process, ease the strain of the authority and allow it to focus on core tasks.

Funding innovation in the field of IT/OT security for the energy industry. Market-oriented funding strategies must be initiated to ensure economic viability and drive the development of sector-specific IT security technologies. To this end, actors within the industry must be incentivised to use technologies whose functions go beyond the fulfilment of current minimum requirements. Solutions must therefore be developed so that meaningful measures can be implemented in the area of cyber security that exceed the scope of the catalogue of IT security requirements. This must also take into account that an assessment to determine the extent to which installed components correspond to the state of the art will be mandatory going forward within the framework of IT/OT network expansion, and not merely a functional inspection to ascertain fulfilment of minimum requirements. In future, this will likely necessitate shorter audit intervals to reflect the comparatively fast pace of modernisation within the IT sector. The modernisation of network operators' process networks would benefit from suitable measures in this regard, and legacy components could be promptly replaced with state-of-the-art technologies. It would also represent a method of fulfilling fundamental IT security requirements such as encryption of data traffic.

Continued development of the SMGW infrastructure. Sustainable realisation of many use cases that will be implemented in the energy sector going forward will require a 'security by design' SMGW infrastructure to provide a safe foundation in the long term. However, transitional solutions, developed in the short term to compensate for current delays in the roll-out and to address the challenges associated with the infrastructure's usability, accessibility and interoperability, must meet precisely the same IT security and data protection requirements and enable future transition to the SMGW infrastructure (cf. Section 4.3). Standardising of use cases for the implementation of network- and market-specific functions in close cooperation between authorities and experts from the industry can contribute to improved acceptance and usability of the infrastructure. End customers may also show greater acceptance if provided with options for the detailed monitoring of their own user profile and for optimising costs, for example through dynamic tariff models, provided the systems ensure rigorous standards of data protection at the same time. In future, most grid and metering point operators will be able to outsource to external service providers some of the tasks and responsibilities that may be associated with establishing and operating the SMGW infrastructure. Outsourcing operation of the infrastructure 'as-a-service' and the deployment of cloud-based infrastructure provide a considerably more flexible and scalable approach in this regard, especially for smaller companies.

At present, the implementation of cyber innovation in the energy sector is largely defined by the need for companies to meet the current minimum regulatory requirements, which means that the competent authorities retain central control over this process.

As is currently being discussed in other areas, for example in the expansion of renewable energies, a variety of approaches should be applied to streamline this process for stakeholders, among them a simplification of current regulations, the development of future regulations in close consultation with industry, the elimination of red tape and shortened planning, approval and certification procedures. Incentives should also be introduced for the use of technologies whose functional capabilities extend beyond the minimum requirements. Measures should also be put in place to upgrade current networks, especially in the IT/OT sector, to a level that reflects the state of the art for both functionality and security. Secure infrastructure design – based for instance on the SMGW infrastructure – will be of vital importance for the majority of value-added services in the long term. To accommodate future developments, the use cases should be standardised and infrastructure defined within a harmonised framework that ensures a high level of security as well as operational suitability right from the outset.

6 Summary and conclusion

The trend towards more decentralised structures in the context of the energy transition and the digitisation of the energy sector are creating new challenges for the industry. Overcoming these challenges will require the development and use of innovative technologies or the transfer of current concepts and technologies from other sectors to the energy industry. Increased monitoring and greater automation in the grids in particular, but also the emergence of new market roles (e.g. metering point operation and gateway administration), are creating new areas of activity and hence market and development potential for sector-specific solutions in the fields of communication technology and cyber security. At least a minimum level of cyber security is indispensable for all participating actors that influence the 'provision of critical services in the supply of energy'. There are extensive regulatory requirements for both operational and IT security. For innovation-driven progress to succeed, all relevant actors must be able to recognise unequivocally which components of the rules and regulations are binding for them and which actions are necessary to fulfil the associated minimum requirements. The individual regulations must be coordinated in view of the increasing complexity of cyber security, also because the requirements in this area are constantly evolving.

This report examined the smart meter roll-out in Germany as a case study for the establishment of new technologies, which essentially involves technocratic implementation with a top-down approach. Nationwide roll-out is not yet complete due to a variety of delays. As the analysis of the roll-out process for smart metering systems in various European countries shows (cf. Section 5.2), there is no patent recipe or optimum approach for the nationwide and widespread establishment of new technologies like the SMGW infrastructure. Alternative strategies for establishing new technologies are needed in this case which find a balance within the regulatory framework to ensure that clear minimum requirements for the functionality of the devices and infrastructure are fulfilled. Notwithstanding, any 'over-specification' might have negative consequences on a competitive market. Transparent development of a regulatory framework and standards within a process that involves all key stakeholders from the outset is an essential part of ensuring this aspect is accommodated suitably. A comprehensive and flexible funding policy may also help to optimise these processes. Within this process, it is not up to the market participants alone to exert active and representative influence on the ongoing developments. Instead, an almost holistic inclusion of all perspectives is needed for a sustainable realisation of the technologies to ensue. This comprises, for instance, the consideration of a future-proof design of large-scale infrastructures with long-term deployment prospects, which should not only involve forward-looking dimensioning on the hardware side, but also take into account a reasonable life-cycle management process from the software side.

Besides standardising use cases and implementing security requirements, metering point operators face the challenges of ensuring that the new technologies are interoperable with their current technologies and that the SMGWs can connect to their networks. It is not possible to make a universally valid recommendation for the specific communication technology required in this context, as this always depends on the individual application and the circumstances on the ground. Section 2.2 presented the most important technologies that possess greater relevance for the industry. It is vital to weight up the (short-term) feasibility and risk minimisation potential of measures that are intended to elevate cyber security in order to assess which of them should be implemented within which time frame. In general, however, it makes sense to create incentives for the implementation of measures that go beyond mere compliance with the minimum standard ('security by design').

In order to enable the rapid establishment of new technology on the market in the future, the bureaucratic and technical processes for approval and certification need to be simplified, made more transparent and accelerated. Projects that are designed to achieve technological progress can be promoted within the framework of specific funding policy measures according to the top-down or bottom-up approach (cf. Section 5.1), depending on whether they focus on the targeted promotion of specific technologies or are intended to cultivate an innovative spirit. Hybrid funding approaches can prioritise particular aspects according to their current progress and in doing so address current challenges within an adaptable framework. Where there are plans to promote market interest in a technology during the early phases especially, a promising approach can be to focus on the funding of pilot projects and demonstrations in order to investigate the practicality of developed concepts, increase their acceptance among relevant actors and identify necessary modifications at an early stage. Adopting a technocratic approach that includes holistic and forward-looking goals becomes more important in the later phases of funding as a means of stabilising the establishment of new technology on the market.

> Broadly speaking, there are many methods available that would serve the energy transition and the development of innovative applications in Germany's energy industry, along with national and international experience in these fields. The core aspects identified in this report for a sustainably (cyber-)secure and forward-looking energy industry in Germany and Europe are transparency, interoperability, carefully defined funding policy, application-orientation, communication and data security, as well as a comprehensive and highly practical regulatory framework that is coordinated throughout the industry. In this regard, it is necessary to strike a balance between cyber security concepts, cost aspects and areas of application, with participation from all actors from the energy industry and politics.

List of abbreviations

ABE	Attribute-based Encryption
AES	Advanced Encryption Standard
AS4	Applicability Statement 4
BDEW	German Association of Energy and Water Industries
BGM	Balancing group manager
BMWK	Federal Ministry for Economic Affairs and Climate Action
BNetzA	Federal Network Agency
BSI	Federal Office for Information Security
BSI-KritisV	Ordinance on the Designation of Critical Infrastructures under the Act on the Federal Office for Information Security
CLS	Controllable Local System
CPS	Cyber-physical system
DPGP	Decentralised power generation plant
DSL	Digital Subcriber Line
DTLS	Datagram Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman (cryptographic method)
ECDSA	Elliptic Curve Digital Signature Algorithm
EEG	Renewable Energy Sources Act
EMP	External market participant
ENTSO-E	European Network of Transmission System Operators for Electricity
EnWG	Energy Industry Act
EVM	Ethereum Virtual Machine
EUC	Energy utility company
FaaS	Function-as-a-Service
FDI	False Data Injection
FHE	Fully Hormophic Encryption
GBit/s	Gigabits per second
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
ICT	Information and communications technology
IMSI	International Mobile Subscriber Identity
iMSys	Intelligent measuring system
IoT	Internet of Things
IPS	Intrusion Prevention System
ISMS	Information Security Management System

ISP	Internet Service Provider
IT	Information technology
AI	Artificial intelligence
ANN	Artificial neural network
KRITIS	Critical infrastructure
kW	Kilowatt
kWh	Kilowatt-hour
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	Core market data register
MBit/s	Megabit per second
MEO	Medium Earth Orbit
MHz	Megahertz
ML	Machine Learning
mME	Modern measuring equipment
Bn	billion
m/s	Metres per second
MPO	Metering point operator
MsbG	German Metering Point Operation Act
MW	Megawatt
NABEG 2.0	Grid Expansion Acceleration Act
NB-IoT	Narrowband IoT
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
NOVA	Grid optimisation, enhancement and expansion
OT	Operational Technology
PaaS	Platform-as-a-Service
PIN	Personal Identification Number
PKI	Public key infrastructure
PoA	Proof of Authority
PoW	Proof of Work
PQC	Post-quantum cryptography
QoS	Quality of Service
RSA	Rivest-Shamir-Adleman (cryptographic method)
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 infrastructure
SOC	Security Operations Center
SSH	Secure Shell
StromNZV	Electricity Grid Access Ordinance
TLS	Transport Layer Security
TR	Technical directive
TTP	Trusted Third Party
TSO	Transmission system operator
UPS	Uninterruptible power supply
V2G	Vehicle-to-Grid
VDE	Association for Electrical, Electronic & Information Technologies
VDE FNN	Network Technology/Network Operation Forum at VDE
VKU	German Association of Local Public Utilities
DSO	Distribution system operator
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
XMSS	eXtended Merkle Signature Scheme

Bibliography

[1] 50 Hertz Transmission GmbH, Amprion GmbH, TenneT TSO GmbH, TransnetBW GmbH. Netzentwicklungsplan: NOVA-Prinzip. https://www.netzentwicklungsplan.de/de/nova-prinzip (retrieved on 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] Federal Office for Information Security (BSI). Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen. Technical report, 2014.

[9] Federal Office for Information Security (BSI). Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls. Technical report, 2014.

[10] Federal Office for Information Security (BSI). Smart-Meter-Gateway-Administration. Technical report, 2015.

[11] Federal Office for Information Security (BSI). Certificate Policy der Smart Metering PKI. Technical report, 2017.

[12] Federal Office for Information Security (BSI). Smart Metering PKI – Public Key Infrastruktur für Smart Meter Gateways. Technical report, 2017.

[13] Federal Office for Information Security (BSI). Technische Richtlinie TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government. Technical report, 2019.

[14] Federal Office for Information Security (BSI). BSI TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4. Technical report, 2020.

[15] Federal Office for Information Security (BSI). Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. Technical report, 2021.

[16] Federal Office for Information Security (BSI). BSI TR-03116-3 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3. Technical report, 2021.

[17] Federal Office for Information Security (BSI). Technische Richtlinie TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Technical report, 2021.

[18] Federal Network Agency. 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 (retrieved on 26/11/2021).

[19] Federal Network Agency. 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 (retrieved on 23/10/2021).

[20] Federal Network Agency. 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 (retrieved on 26/10/2021).

[21] Federal Network Agency. 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 (retrieved on 26/10/2021).

[22] Federal Network Agency. Presse – Vergabe von Frequenzen im Division 450 MHz. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2020/20201116_450mhz.html, 2020 (retrieved on 30/08/2021).

[23] Federal Network Agency. 450 MHz – Erfolgreiche Bewerbung der 450connect GmbH. https://www. bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2021/20210309_450Mhz.html?nn=267872, 2021 (retrieved on 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 and Helmut Knebl. Introduction to Cryptography: Principles and Applications, 2007.

[31] German Association of Energy and Water Industries (BDEW). Konkretisierung des Ampelkonzepts im Verteilungsnetz, 2017.

[32] German Association of Energy and Water Industries (BDEW). Datenerhebung 2019 – Bundesmix 2019, 2020.

[33] German Association of Energy and Water Industries (BDEW). Die Energieversorgung 2020 – Jahresbericht, 2021.

[34] German Association of Energy and Water Industries (BDEW). Rollenmodell für die Marktkommunikation im deutschen Energiemarkt, 2021.

[35] German Association of Energy and Water Industries (BDEW). BDEW-Branchenlösung Redispatch 2.0, 2020.

[36] German Association of Energy and Water Industries (BDEW). und Oesterreichs E-Wirtschaft. White paper: 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 (retrieved on 29/11/2021).

[40] International Organization for Standardization. ISO 27000 – ISO 27001 and ISO 27002 Standards. https://www.27000.org (retrieved on 23/10/2021).

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

[42] Federal Office of Justice. German Renewable Energy Sources Act (EEG) https://www.gesetze-im-internet. de/eeg_2014/ (retrieved on 23/10/2021).

[43] Federal Office of Justice. Metering Point Operation Act (MsbG). https://www.gesetze-im-internet.de/messbg/ (retrieved on 23/10/2021).

[44] Federal Office of Justice. Energy Industry Act (EnWG). https://www. gesetze-im-internet.de/enwg_2005/ (retrieved on 23/10/2021).

[45] Federal Office of Justice. Grid Expansion Acceleration Act (NABEG). https://www. gesetze-im-internet.de/nabeg/BJNR169010011.html(retrieved on 23/10/2021).

[46] Federal Office of Justice. Electricity Grid Access Ordinance (StromNZV). http://www. gesetze-im-internet.de/stromnzv/index.html (retrieved on 23/10/2021).

[47] Federal Office for Information Security. BSI KRITIS Ordinance of 22 April 2016 (Federal Law Gazette I p. 958), last amended by Article 1 of the Ordinance of 6 September 2021 (Federal Law Gazette I p. 4163), 2021.

[48] Federal Office for Information Security (BSI). https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (retrieved on 23/10/2021).

[49] Federal Office for Information Security (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 (retrieved on 11/10/2021).

[50] Federal Office for Information Security (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 (retrieved on 11/10/2021).

[51] Federal Office for Information Security (BSI). Second Act to Increase the Security of Information Technology Systems (IT Security Act 2.0, IT-SiG 2.0). https://www.bsi.bund.de/DE/Das-BSI/ Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html (retrieved on 23/10/2021).

[52] Federal Office for Information Security (BSI). Migration zu Post-Quanten-Kryptografie – Handlungsempfehlungen des BSI. Technical report, 2020.

[53] Federal Office for Information Security (BSI). Stufenmodell zur Weiterentwicklung der Standards für die Digitalisierung der Energiewende, 2020.

[54] Federal Ministry for Economic Affairs and Energy (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 (retrieved on 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. Federal Environment Agency, 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] European Commission. Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation. https://eur-lex.europa.eu/legal-content/DE/ TXT/PDF/?uri=CELEX:32017R1485&from=LT (retrieved on 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] Higher Administrative Court of North Rhine-Westphalia. Stopp der Einbauverpflichtung für intelligente Messsysteme (Stromzähler) im einstweiligen Rechtsschutzverfahren – case number 21 B 1162/20.

[74] National Institute of Standards and Technology (NIST). NIST Standards. https://www.nist.gov/standards (retrieved on 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 and 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 and 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] Network Technology/Network Operation Forum at VDE. 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
German Energy Agency

www.dena.de