



Leopoldina
Nationale Akademie
der Wissenschaften

 **acatech**
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

 **UNION**
DER DEUTSCHEN AKADEMIEN
DER WISSENSCHAFTEN

April 2021
Position paper

The resilience of digitalised energy systems

Options for reducing blackout risks



“Energy Systems of the Future” is a project of:

German National Academy of Sciences Leopoldina | www.leopoldina.org

acatech – National Academy of Science and Engineering | www.acatech.de

Union of the German Academies of Sciences and Humanities | www.akademienunion.de

Impressum

Publisher of the series

acatech – National Academy of Science and Engineering (lead institution)
Munich Office: Karolinenplatz 4, 80333 Munich, Germany | www.acatech.de

German National Academy of Sciences Leopoldina
Jägerberg 1, 06108 Halle (Saale) | www.leopoldina.org

Union of the German Academies of Sciences and Humanities
Geschwister-Scholl-Straße 2, 55131 Mainz, Germany | www.akademienunion.de

Edited by

Anja Lapac, acatech

Scientific coordination

Dr. Achim Eberspächer, acatech
Dr. Berit Erlach, acatech
Dr. Marita Blank-Babazadeh, OFFIS
Katharina Bähr, acatech
Sanja Stark, OFFIS

Production coordination and typesetting

Annika Seiler, acatech

Design

aweberdesign.de . Büro für Gestaltung

Cover photo

[shutterstock.com/142043677/Gianluca Muscelli](https://shutterstock.com/142043677/Gianluca_Muscelli)

Printing

Kern GmbH, Bexbach, Germany
Printed on acid-free paper, Printed in EC

ISBN: 978-3-8047-4225-3

Bibliographic information: German National Library

The German National Library has recorded this publication in the German National Bibliography;
detailed bibliographic data can be retrieved from the internet <http://dnb.d-nb.de>.

Preface

Digitalisation can enable a more environmentally-friendly, reliable and economically efficient energy supply. However, it also gives rise to new failure causes and vulnerabilities. On 14 August 2003, for example, a major blackout in the Northeast of the US and parts of Canada left 55 million people without electricity. It was two days before power was restored to all those affected. The blackout was caused by an undetected software bug that triggered an unfortunate chain of events, ultimately with dramatic consequences. In 2015, meanwhile, Ukraine became the first country in the world to suffer a power outage caused by hackers.


Blackouts pose a particular threat due to the electricity system's unique role among critical infrastructures. Problems with the electricity supply can very quickly cause serious disruption to the water supply and sewerage systems, the transport system, the healthcare system, and information and communication technology.

An ESYS working group used a range of future scenarios for 2040 to explore the evolution of blackout risk factors and identify any new ones that could arise. Both the energy transition and digitalisation are dynamic trends, and it is not always possible to control the factors that influence them. As unforeseen and unforeseeable events become more common, established risk management measures will no longer be effective.

According to the experts, the concept of resilience offers a valuable approach for coping with this uncertainty. A resilient energy system is able to absorb incidents without damage, or is at least able to return to normal operation rapidly, affordably and with a minimum of damage. The working group has identified 15 policy options that can form the building blocks of a resilience strategy for preventing major blackouts.

It is clear that, in the future, the responsibility for maintaining a reliable electricity supply will no longer rest exclusively with the large energy supply actors. Smaller energy supply actors, private individuals, and actors from outside of the electricity system – such as platform operators, public communication network operators and device manufacturers – will also have to do their bit to ensure resilience.

We would like to thank the experts and reviewers who contributed to this paper for their valuable input.



Prof. (ETHZ) Dr. Gerald Haug
President
German National Academy of
Sciences Leopoldina



Prof. Dr.-Ing. Jan Wörner
President
acatech – National Academy of
Science and Engineering



Prof. Dr. Dr. Hanns Hatt
President
Union of the German Academies
of Sciences and Humanities

Contents

Preface	3
Contents	5
Abbreviations	6
Glossary	7
Summary	11
1 The energy transition and digitalisation: countering new blackout risks .	17
1.1 The serious damage caused by lengthy blackouts	18
1.2 The transformation of the energy supply	19
1.3 The digital revolution	20
1.4 New blackout risks	21
1.5 A resilience-based approach to preventing outages	25
1.6 Methodological approach used by the working group	26
2 Policy options	27
2.1 Policy area 1: Understanding and managing the interactions between ICT and energy systems...	30
2.2 Policy area 2: Systemic development of cybersecurity	34
2.3 Policy area 3: Strengthening the contribution of grid operators and grid users to technology resi- lience	39
2.4 Policy area 4: Ensuring that ICT integration of small devices supports grid stability	42
2.5 Policy area 5: Increasing incentives for grid operators to strengthen resilience	45
2.6 Policy area 6: Ensuring that private actors are involved in the design and implementation of resi- lience measures	48
2.7 Policy area 7: Institutionalising long-term risk and resilience assessment	53
3 Conclusion	56
References	58
The Academies' Project	61

Abbreviations

ARegV	Incentive Regulation Ordinance for power grids
BSI	Federal Office for Information Security
BSI-KritisV	BSI Regulation on the Determination of Critical Infrastructures
CI	Critical infrastructure
ENTSO-E	European Network of Transmission System Operators for Electricity
ICT	Information and communication technology
PV	Photovoltaic
StromNEV	Verordnung über die Entgelte für den Zugang zu Elektrizitätsversorgungsnetzen

Glossary

Aggregator	Aggregators trade and supply energy, but are not connected to the customer's provider. They group together generating units, flexible consumers and storage units for commercial purposes, scaling up small units to a marketable volume.
Blackout	A blackout is a major power outage in a region, affecting at least 500,000 customers and lasting a minimum of several hours.
Cascade effect	A sequence of events or processes, each of which builds on the previous one.
Cybersecurity	Cybersecurity encompasses all aspects of information and communication technology security. It extends the scope of information security to the whole of cyberspace. This includes all information technology connected with the Internet and similar networks, together with the communication, applications, processes and processed information that this technology enables. When discussing cybersecurity, there is often also a special focus on cyberattacks. ¹
Digitalisation of the electric power system	The digitalisation of the electric power system refers to the ongoing advances in ICT-based connectivity of applications, processes, stakeholders and physical technical equipment or objects. Digitalisation also encompasses the acquisition, processing, exchange and analysis of information and data in every value-added stage and across different value-added stages of the electric power system. This helps to generate knowledge, make decisions, and determine the corresponding actions such as control interventions. The resulting new processes are often automated and supported by artificial intelligence mechanisms.
Distribution grid	Distribution grids are used to distribute electrical energy to the end customer.
Distribution system operator	The operator responsible for a distribution grid (see Grid operator and Distribution grid).
Grid/system operator	Grid operators are responsible for planning, building and operating the electricity grid. In particular, they are responsible for deploying any technical resources and making any interventions necessary to ensure an uninterrupted supply of electricity in their section of the grid. Depending on the voltage level, a distinction is drawn between transmission system operators (TSOs, for grid voltages of 220 kilovolts or more) and distribution system operators (DSOs, for grid voltages of 110 kilovolts or less).
Grid tariffs	Fees charged for access to the transmission and distribution grids.
Grid user	A natural or legal person who feeds electricity into or draws electricity from a power grid. This includes e.g. operators of generating systems or subordinate grid operators.
Information security	The aim of information security is to protect information. This information may be stored as a hard copy, on a computer, or in someone's head. The protection goals or core values of information security are confidentiality, integrity and availability. Many users also include other core values. ²

¹ BSI 2020-1.

² BSI 2020-2.

	Threats can arise through force majeure, human error, technology failure or deliberate attacks.
Internet of Things	The Internet of Things refers to physical objects or virtual, digital objects that are equipped with ICT, sensors and actuators and connected to the Internet.
Load	The total electrical power drawn from a grid at a given point in time.
Operating resources	Umbrella term for electrical equipment such as power lines, transformers and switchgear.
Patch	A patch is an update of existing software versions that adds new functionality or fixes bugs and security vulnerabilities.
Patchability	Patchability refers to a technical system's ability to have its installed software easily and remotely updated during operation, either automatically by the manufacturer, or by the operator if they are qualified to do so.
Path dependency	This is the effect that occurs when the barriers resulting from decisions taken in the past make it difficult or impossible to switch to a different option. These barriers can arise if changing systems would mean that previous investments could be lost (sunk costs). The cost advantages of mass production (economies of scale) or high user numbers (network effects) also give established systems an advantage over any alternatives. In this position paper, however, the focus is not so much on the necessary investment as on the time that it would take to upgrade the relevant systems. This is because systems will remain vulnerable until an upgrade designed to fix any weaknesses has been completed.
Prosumer	This term is an amalgamation of "producer" and "consumer". It reflects the fact that small private actors such as households can now produce as well as consume electricity (e.g. via solar panels on their roofs).
Resilience (of the energy system)	Resilience means that an energy system's function – here, security of supply – is maintained (possibly with some limitations) when it comes under pressure, or can at least be rapidly restored.
Risk	Assessment of the likelihood of specified negative impacts arising from e.g. operational failings or undesired events, taking into account the relevant variables such as the probability of such events occurring.
Sector coupling	Sector coupling involves connecting the electricity, heating and mobility energy sectors to create an integrated energy system that provides the necessary energy services to private, commercial and industrial customers. Examples include combined heat and power, power-to-gas, or heat pumps and heating resistors (power-to-heat).
Smart connection agreements	Smart connection agreements are flexible grid connection agreements for electricity producers that allow the grid operator to curtail the connection (with or without compensation for the producer).
Smart home	This term encompasses all the aspects and services involved in connecting appliances and automating processes in people's homes.
Socio-technical system	A socio-technical system is characterised by the interaction between social and technical factors. The importance of this interaction is explained by the coevolution of technology and society, in which both elements mutually influence and shape each other.
Subordinate grid	Subordinate grids are lower voltage level grids that are connected to a higher voltage level grid. Grid B is subordinate to Grid A if it is connected to Grid A, and if Grid A is either a transmission grid itself or if electricity is transmitted from the transmission grid to Grid B solely via Grid A.
Supervisory control system	Supervisory control systems perform two key functions: they monitor processes or components and control them using telecontrol technology.

Transmission grid	Transmission grids transmit electricity over large distances (hundreds or thousands of kilometres) so that consumption and generation can be balanced across large areas. They also make it possible to connect very large power plants or industrial consumers. Transmission grids operate at voltages of 220 to 380 kilovolts (Extra High Voltage). High-voltage direct current (HVDC) transmission is used to transmit electricity over very large distances and via submarine power cables.
Transmission system operator	The operator responsible for a transmission grid (see Grid operator and Transmission grid).
Voltage levels	There are different voltage levels for the transmission and distribution of electrical energy. Generating and consuming units are connected to different voltage levels, depending on the extraction or feed-in of electric power.

Summary

Over the next two decades, the energy transition and the growth of digitalisation will result in new risks to the electricity supply. A resilience strategy will be required to manage these risks and reliably prevent blackouts and their damaging impacts on society. The “Resilience of digitalised energy systems” working group of the Academies’ Project “Energy Systems of the Future” has identified the following points as the key pillars of any such strategy:

- **Digitalisation** should be **actively shaped** and promoted, since it offers the opportunity to efficiently and securely integrate decentralised electricity generation structures, electric mobility and new market players into the energy system.
- **Small players** in the energy supply market, **actors from outside the energy supply** sector (appliance manufacturers, platform operators, public communication network operators) and **private households** all have a growing influence on the security of the energy supply. They should therefore be more closely involved in efforts to strengthen resilience.
- New targets for cybercriminals and the electricity system’s greater reliance on information and communication technology could result in **unforeseen or even unforeseeable incidents** with the potential to pose a major threat. Grid operators must be able to manage these risks.
- Policymakers must endeavour to anticipate future developments in good time and ensure that the resilience strategy called for in this paper is continuously adapted. This will require **systematic monitoring**.

Digitalisation and growing complexity are resulting in new threats

A reliable electricity supply is indispensable in a modern industrialised society. Major blackouts – i.e. **lengthy and widespread power outages** – would almost instantly cause serious disruption to and potentially even the collapse of other critical infrastructure such as transport systems, the water supply and sewerage systems, the healthcare system, and information and communication systems.

The energy transition is making the energy system more complex. More and more electrical power is being produced by wind and solar systems, the output of which fluctuates depending on the weather, season and time of day. Demand for electricity to power electric vehicles and heat pumps is growing. Private households are now generating electricity with their own solar panels, while new market players with new business models are emerging alongside the traditional energy providers. Meanwhile, the large power plants that used to ensure a stable electricity supply are being decommissioned.

At the same time, the pace of **digitalisation** is accelerating rapidly. Connectivity, automation and the use of digital technology are all increasing – and not just in the electricity sector. Billions of devices – including everything from lights and fridges to industrial equipment – are now connected via the **Internet of Things**. Since these devices are also connected to the power grid, their combined effect can influence the stability of the electricity supply.

The growing role of information and communication technology (ICT) is key to ensuring a reliable and economically efficient energy supply – the energy transition cannot succeed without digitalisation. However, the increasing complexity of the energy supply also gives rise to new blackout risks:

1. The electricity supply can be destabilised if **several small electricity generators and consumers** are all switched on or off at the same time, either intentionally or by chance.
2. The electricity supply is becoming more vulnerable to **ICT failures**. One particularly problematic aspect is that some of the relevant ICT systems cannot be switched off in the event of a failure without seriously jeopardising the electricity supply.
3. The complex interactions between decentralised generation, market activity and changes in consumption make it **harder to predict** the system's behaviour and could mean that **incidents unfold in complex new ways**.
4. **Uncertainty about future developments inhibits optimal system design**. A further challenge is that the speed of innovation in the ICT sector is difficult to reconcile with investment cycles in the electricity sector, which tend to be several decades long.

A resilience strategy for unforeseen and unforeseeable risks

The changes in the energy system and the growing impact of digitalisation are heightening uncertainty about future developments. As a result, it is becoming increasingly difficult to calculate the probability of known or expected events such as hacker attacks. While conventional risk analysis techniques employing this approach have until now formed the basis of a robust system, they are no longer enough. The grid operators responsible for the system's overall security will also have to come to terms with a far more uncertain and unpredictable future. It will be increasingly important for them to be capable of **responding to** and coping with **unforeseen or unforeseeable events** and rapidly restoring the system to normal operation, even in the event of a blackout. **Resilience** is a tried-and-tested **concept** for managing this kind of situation. Resilience means that the system can absorb the impacts of an incident without collapsing, and then rapidly return to normal operation. Depending on the circumstances, it may be necessary to accept a short-term drop in supply quality in the worst-case scenario (see Figure 1).

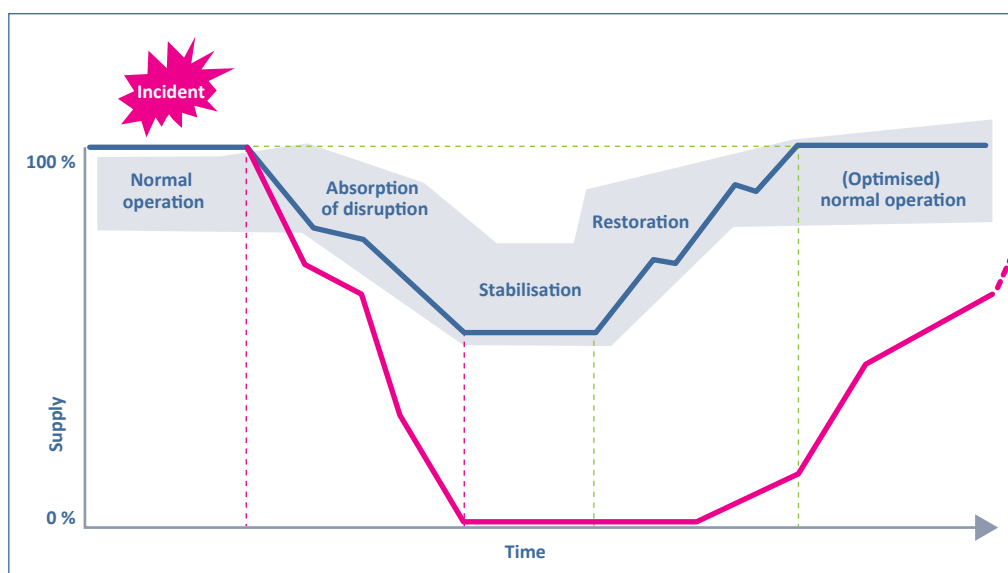


Figure 1: Restoring system functionality: responding appropriately to an incident (absorption of disruption), reverting to critical functions and stabilising the system (stabilisation), followed by a controlled return to normal system operation (restoration).³

A **resilience strategy** calls for a portfolio of measures. These include the exhaustive identification of weaknesses and risks, measures to support the system's robustness, resilience and adaptability, and measures to promote learning and improve the system, including cost-effective emergency response planning.

The working group has identified **15 policy options** (see next page) that can form the building blocks of a resilience strategy for preventing major blackouts. The policy options were chosen to address the **areas where action is required today** in order to tackle the new risks that will emerge over a **longer-term timeframe between now**

³ Babazadeh et al. 2018, p. 32 f.

and 2040. It will be vital for the resilience strategy to keep pace with the rapid progress of digitalisation and the energy transition in order to fully harness the potential for an efficient, secure and sustainable energy supply and successfully manage blackout risks in a digitalised world.

Options for reducing blackout risks

The following measures have been identified as the building blocks of a comprehensive resilience strategy for a digitalised energy system. The measures have been grouped into different policy areas:

Policy options:

Understanding and managing the interactions between ICT and energy systems



In the future, the electricity supply will be increasingly dependent on ICT systems. It is vital to ensure that ICT system failures do not result in blackouts.

- **PO 1. Analyse interdependencies between the electricity supply and communication networks** in order to minimise the risk of cascading failures.
- **PO 2. Establish rules for resilient communication networks** by stipulating higher redundancy and blackout proofing standards.
- **PO 3. Encourage the relevant actors to integrate the operation of ICT systems and electricity grids** with a view to incorporating ICT monitoring into grid operating systems and enabling integrated situational awareness.

Policy options:

Systemic development of cybersecurity



All the relevant actors must bring their cybersecurity measures up to a sufficiently high standard. This will call for new technological and organisational solutions.

- **PO 4. Introduce cybersecurity standards for all actors relevant to blackouts**, including small grid operators, actors from other industries, and behind-the-meter devices.
- **PO 5. Define measures for addressing security vulnerabilities** in order to counter vulnerabilities caused by human error in security management, software bugs or government-mandated backdoors.

Policy options:

Strengthening the contribution of grid operators and grid users to technology resilience



Grid operation is set to become more challenging, especially in distribution grids. Both small grid operators and the operators of small generating systems will need to make a much greater contribution to resilience than is usually the case today.

- **PO 6. Accelerate digitalisation of electricity grids**, ensuring that small grid operators also have the necessary technological resources.
- **PO 7. Formulate guidelines for enabling resilience through decentralised structures.** Individual sections of the grid that are able to operate in island mode can temporarily maintain the local electricity supply during a blackout and help to restore the overall supply.

Policy options:
Ensuring that ICT integration of small devices supports grid stability



In the future, the majority of devices and appliances will be connected to and digitally controlled via the Internet. It will be vital to avoid undesired simultaneous activity that can jeopardise the stability of the electric power system, for instance when high load peaks are caused by large numbers of devices being switched on at the same time. On the other hand, these devices can also be used to actively stabilise the power system.

- **PO 8. Promote standardisation to prevent problematic simultaneous activity**, for instance through the introduction of minimum patchability standards for electricity generators and devices. This would enable device software to be updated during operation in order to address new requirements.
- **PO 9. Increase the use of decentralised units to strengthen system stability**, and promote the enabling communication technology connections.

Policy options:
Increasing incentives for grid operators to strengthen resilience



There is a general lack of effective and efficient incentives for grid operators and market players to behave in a way that strengthens resilience. The relevant market incentives should be created.

- **PO 10. Incorporate a resilience component into the incentive regulation** in order to encourage grid operators to invest in resilience.
- **PO 11. Introduce grid tariffs and smart connection agreements that strengthen resilience** by influencing the locations chosen for renewable energy systems and the way they are operated.

Policy options:
Ensuring that private actors are involved in the design and implementation of resilience measures



Private actors may also need to manage their systems in a way that supports the grid. A stakeholder forum should be created to provide input on this aspect and to develop solutions that are viable for the relevant user groups and address any acceptability issues.

- **PO 12. Establish a stakeholder forum to address the interests of private actors** and include all the relevant actors in the decision-making process for new regulations.
- **PO 13. Raise awareness about the influence of private actors** through information and education campaigns.

Policy options:
Institutionalising long-term risk and resilience assessment



Digitalisation and the energy transition will give rise to unforeseeable trends that could increase the risk of black-outs. An appropriate organisational framework should be created that enables flexible responses for coping with these trends.

- **PO 14. Create an organisational framework for incident reporting and resilience assessment**, and develop appropriate resilience indicators.
- **PO 15. Establish an overarching monitoring process** to facilitate regular evaluation of the resilience strategy.

Table 1: Overview of policy areas and policy options (POs)

1. The energy transition and digitalisation: countering new blackout risks

The electric power system is one of the critical infrastructures (CIs) that modern industrialised societies rely on for their wellbeing. Other CIs include the water supply and sewerage systems, the transport system, the healthcare system, and information and communication systems. **The electricity supply plays a special role among CIs**, since its failure would very quickly cause serious disruption to all the other CIs.

Compared to other parts of the world, Europe's electricity supply is very reliable and robust to disruption. However, the **energy transition** could jeopardise the high security of supply that Europe is accustomed to. A growing percentage of electricity generation is accounted for by renewables, which in some cases are dependent on the weather, season, or time of day. Moreover, electricity demand is rising and consumption patterns are changing due to trends such as electric mobility and a wider switch to electrical power in the context of decarbonisation. Last but not least, **digitalisation** is transforming the electric power system. Over the next two decades, some of the mechanisms that grid operators currently use to maintain system stability will be lost as a result of this transition. It will also give rise to **new forms of disruption** that are still relatively unimportant or even completely unknown today.⁴ Even events that are not directly related to the electricity supply can have an impact on the secure operation of the electric power system. For instance, a pandemic could result in key operational and maintenance personnel being unable to come into work, either because they themselves are unwell or because a family member has fallen ill, although fortunately this did not happen during the Covid-19 pandemic in 2020. Digitalisation can help to significantly mitigate many of the challenges to the electricity supply that can arise in these situations.

This position paper proposes a series of **policy options** which, if implemented, can already start to address the new threats that will arise over the medium term due to the combined effects of the energy transition and the growth of digitalisation. One particular challenge is posed by the continuous changes to the electric power system itself, which make a greenfield approach impossible. The paper focuses on ways of **preventing major blackouts**, or at least mitigating them as effectively as possible. The term "blackout" is used throughout to refer to lengthy, major regional power outages.

Whatever precautions are taken, there is always a residual risk of a nationwide blackout lasting several days. Policymakers must ensure that their general disaster preparedness plan will still be effective if this happens. However, this scenario is beyond the scope of the present position paper.

All the findings, methodological approaches and policy options discussed in this paper are described and elucidated in detail in the accompanying study.⁵

1.1 The serious damage caused by lengthy blackouts

A 2011 study by the Office of Technology Assessment at the German Bundestag graphically depicts the consequences of lengthy blackouts.⁶ The first serious impacts, such as road accidents due to traffic light failures, can start to occur immediately after the outage. The healthcare system is particularly badly affected – the number of fatalities and injuries due to accidents is exacerbated by the disruption to the emergency services and transport system. It is no longer possible to make landline calls, and mobile telephony is also seriously affected after a few hours. This means that people can no longer call out the emergency services or police to attend an emergency. It is also impossible to keep the public properly informed. After a few days, livestock start dying on farms. Hospital patients unable to cope with the deterioration in medical care fall into a critical condition. The food supply is disrupted and there is a danger of rioting and other threats to public order. There is a sharp increase in looting, vandalism and other criminal offences, and there is very little that the police can do. Not only are they unable to cope with the sheer volume of incidents, but in most cases people are not even able to call them out in the first place. Even if the electricity supply is restored after a few days, there are still many long-term or permanent impacts. There is lasting damage to public trust, not only in energy providers but also in the State and in society itself.

A lengthy blackout would also have huge economic costs. Although there are no precise quantitative estimates for this eventuality, an estimate that put the cost of a one-hour power outage at noon on a winter weekday in Germany at EUR 600 million in 2010 provides a useful point of reference.⁷ The hourly cost of a longer outage would probably be significantly higher.

Accordingly, this position paper focuses on **major power outages (black-outs)** that could occur **over the next two decades** in connection with the transformation of the overall energy system. The timeframe up to 2040 was chosen in order to address long-term trends. However, it was considered that anything longer than two decades would be inappropriate, since it would be too difficult to predict developments in digitalisation after that date. A power outage is defined as “major” if it affects a region with at least 500,000 customers and lasts several hours.⁸

⁵ Mayer/Brunekreeft 2021.

⁶ Petermann et al. 2011.

⁷ Piasceck et al. 2013.

⁸ Based on Büchner et al. 2014, BSI-KritisV 2017, p. 7.

1.2 The transformation of the energy supply

The energy transition has led to an increase in renewables' share of the electricity generated in Germany – wind, solar, hydroelectric and biomass already accounted for over 46% of net domestic electricity generation in 2019. In the European Green Deal⁹ published in 2019, the European Union also affirms its goal of transitioning to mainly renewable energy production by 2050, as part of a fully-integrated, digitally connected European energy market. The following energy supply trends mean that it is necessary to reassess future blackout risks:

- **Diversity of generating structure:** In the future, a large proportion of Germany's electricity will come from small renewable energy systems, while the amount of electricity fed into the grid from conventional power plants will decline. As a result, electricity generation will no longer be purely demand-driven, but will also depend on the weather, season and time of day.
- **Geographical diversity:** The resources for generating hydroelectric, biomass, wind and solar power vary across Europe's regions. Increasingly, electricity is no longer generated in the vicinity of major industrial centres with high demand. Instead, it is produced in locations with good wind and solar resources, such as the sparsely populated regions of northern and north-east Germany. This means that the electricity must be transported over longer distances.
- **Rising demand and changing consumption patterns:** In the future, demand for electricity will rise in the heating and transport sectors. As a result, electricity will play an even more important role in the overall energy supply. Consumption patterns are also changing due to the growing numbers of electric vehicles, heat pumps and other flexible, controllable electricity consumers in both private households and industry, and the rising number of stationary storage systems. ICT systems also account for a significant share of total energy demand.
- **Growing strain on electricity grids:** Even today, the increasing quantities of wind and solar power being fed into the grid mean that distribution system operators are already having to intervene more frequently to prevent grid congestion caused by generation peaks – and this trend is expected to grow much stronger in years to come. Transmission grids are also operating close to their limits on a more regular basis.
- **Changing role of small private actors:** Generation, storage and consumption can converge at local level in the shape of small private actors known as **prosumers**, who not only consume electricity but also generate it themselves, feed it into the grid and store it.
- **More volatile energy markets:** Energy markets are moving towards smaller, more easily traded quantities of energy and shorter supply periods, but a wider geographical spread. Different price signals for different areas are becoming increasingly necessary.

- **New business models:** New business models are already emerging today in areas such as renewable energy marketing and smart home platforms for connecting devices within households.

1.3 The digital revolution

Digitalisation is affecting almost every area of our economy and society, and the energy supply is no exception. Applications and processes are being networked and automated, physical objects are being connected to the Internet, social media is changing the way people interact, and artificial intelligence is being used to support or even make decisions. Many digitalisation developments are **unforeseeable** due to the speed of innovation, their rapid market penetration and their disruptive nature.

Information and communication technology (ICT) is being used to **increase connectivity** throughout every part of the energy supply system. The rollout of smart meters has huge potential for digitalising the energy supply system, since it provides a secure infrastructure for controlling decentralised units. Its implementation is currently the subject of intensive discussions between the relevant standardisation bodies and the Federal Office for Information Security (BSI). But there is much more to digitalisation and ICT – they encompass all technologies, applications and processes used for the electronic acquisition, processing and communication of information. This includes hardware such as servers and communication networks, but also software. More and more data is becoming available, and the systems for processing it – often in real time – are constantly improving. Distribution grids in particular will need to be more extensively automated in order to efficiently integrate the growing but fluctuating quantities of electricity generated by renewable energy systems.

IT/OT convergence can add value. Until now, strict physical separation was always maintained between the ICT systems used for business and administrative processes and transactions (IT/information technology) and the ICT systems used to directly control production processes (OT/operational technology). Today, however, there is more and more interaction between these two areas. One example is the use of OT data to determine when maintenance work needs to be carried out. Conversely, OT systems also have interfaces with other systems, for instance so that they can take account of how switching operations affect the service life of operating resources (i.e. electrical equipment such as power lines, transformers and switchgear) in order to improve economic efficiency.

Digitalisation will lead to the emergence of **new** energy supply **actors** offering digitally enabled products or energy supply platforms. Examples include smart home application platforms and market platforms for trading energy. In the future, it is likely that more or less all consumer devices and appliances, from lights to TVs and fridges, will be connected to the Internet in what is known as the Internet of Things. Providers from other industries are already marketing systems such as smart home solutions that can control appliances and devices automatically. Consequently, it is not enough simply to consider technical and operational processes when assessing the impacts of digitalisation – changing social and economic trends must also be taken into account.

In order to manage these new complexities efficiently, ICT will need to play an increasingly important role in the operation of the electric power system. This will in turn give rise to **new vulnerabilities** caused by cybersecurity weaknesses, software bugs, or human error when using the software in question. Restoring the electricity supply in a distributed, digitalised energy system will also be more complex. On the other hand, digitalisation makes it possible to **respond far more quickly to unforeseen events**. This is because software can generally be updated in far less time than it takes to develop and replace physical components. **Digitalisation is here to stay – it offers huge opportunities, but also poses threats to the security of the energy supply.**

The developments associated with the energy transition and digitalisation are thus leading the responsible actors into a world that is **far more uncertain and unpredictable**. It is likely that there will be many more minor incidents, and these will need to be swiftly resolved or absorbed so that they do not escalate into major power outages.

1.4 New blackout risks

The ESYS working group used a range of future scenarios for 2040 to explore the development of blackout risk factors and identify new ones that could arise during the next two decades as a result of changes in the system. **Four basic causes of new risk factors** were identified. There is very little that policymakers can do to mitigate the basic causes themselves.

Basic cause 1: The multitude of **small, actively controllable electricity generators and consumers** are system relevant due to the possibility of simultaneous activity enabled by digitalisation. This includes both the possibility that the output of multiple units will be switched off or reduced at the same time, and simultaneities, i.e. the simultaneous use of the grid infrastructure by large numbers of electricity generators or consumers. The effects of simultaneously switching a large number of small consumers (e.g. heat pumps, charging electric vehicles or home electricity storage systems) on or off via the Internet can result in destabilising frequency fluctuations. The causes of problematic simultaneous activity include the participation of the relevant units in automated markets. Switching commands from other platforms operated e.g. by the device or unit manufacturers or by independent actors from other industries can also result in undesired simultaneous activity. And problems may also be caused by targeted malicious tampering. Moreover, a lack of incentives for grid-stabilising behaviour can cause issues, especially with small, decentralised generators. Lack of acceptance can be a further difficulty – some members of the public are sceptical about technological solutions that impinge on their freedom of choice. This can hinder the deployment of solutions that could help to stabilise the grid. New municipal or cooperative structures can also alter the balance of interests.

Basic cause 2: ICT failures can result in major threats. The measures currently taken to protect against digital incidents such as software bugs or cyberattacks fall a long way short of what will be required in a highly digitalised future. At present, only relatively large systems and infrastructures are classified as critical infrastructure (see infobox on “Critical electric power supply infrastructure”) and are therefore obliged to

protect their ICT systems against digital incidents. In the future, however, ICT systems that have not traditionally been regarded as components of the energy system will also pose a threat. In conjunction with the platform economy, the small, connected devices that are described under “Basic cause 1” constitute a particularly significant and widespread vulnerability. If someone hacks a platform, they can gain control of all the devices connected to it. These risks are compounded by other trends in the ICT sector. Firstly, the short innovation cycles and pressure to bring software products to market as quickly as possible can tempt developers to cut corners with regard to security standards and software quality. Secondly, the tendency for device manufacturers to form oligopolies or monopolies means that the same security vulnerabilities can potentially affect a very large number of devices. When taken together, these devices become system-critical. And thirdly, highly professional products and services for enabling cyberattacks and identifying security vulnerabilities have now become a “growth market”. This trend also includes State actors in Germany and other parts of the world, who are increasingly requiring backdoors to be built into software and developing tools to launch their own cyberattacks (e.g. “State trojans”). A further complication is that defective or maliciously compromised ICT systems cannot simply be switched off – doing so would result in a blackout, since it would no longer be possible to control the electricity grid. In other words, even if it has been compromised, the system must continue to operate without causing further faults or damage. But this is extremely difficult in a highly distributed system where there are multiple responsible actors and where new types of problems can arise. Moreover, many of the actors will not be able to build up the know-how needed to deal with this kind of security issue.

Critical electric power supply infrastructure

Supplying electrical power is a **critical service**. The BSI Regulation on the Determination of Critical Infrastructures (German: **BSI-Kritisverordnung** – BSI-KritisV) defines what may be classified as **critical infrastructure**.¹⁰ This involves calculating the net capacity for which at least 500,000 people would be affected in the event of a power outage. The following specific types of system are classified as critical infrastructure on this basis:

- **Generating systems** with an installed net nominal capacity of more than 420 megawatts. These include generating plants, decentralised generating units, storage systems, and facilities or systems for controlling/aggregating electric power.
- **Transmission and distribution grids** that transmit or distribute over 3,700 gigawatt hours a year.
- Key facilities and systems for trading electricity that are relevant to physical, short-term spot trading in the German market and that trade more than 200 terawatt hours a year on the market.
- **Behind-the-meter** devices that consume or feed in more than 420 megawatts.

¹⁰ See BSI-KritisV 2017.

What exactly does this mean?

The following table provides some examples of what this means for a highly connected future energy system:

System type	Typical installed capacity ¹¹	Number of units equivalent to 420 megawatts	This is roughly equivalent to: ¹²
Decentralised generating units			
Solar (low-voltage level)	14.25 kilowatts	28,000	9.5% of units in Baden-Württemberg
Onshore wind (high- and extra-high voltage levels)	2 megawatts	210	13% of units in Lower Saxony
Behind-the-meter devices			
Fridges	140 watts	3,000,000	All the households in Berlin and Hamburg combined
Heat pumps	2 kilowatts	210,000	9% of residential buildings in Baden-Württemberg (the German state with the highest number of heat pumps)
Peer-to-peer markets as illustrated by the SmartQuart Bedburg¹³			
Per household <ul style="list-style-type: none"> Two people (with annual consumption of 2,400 kilowatt hours) Heat pump 	2.5 kilowatts: <ul style="list-style-type: none"> 0.5 kilowatts 2 kilowatts 	168,000 households	1% of municipalities in Germany

Table 2: How many decentralised units does it take to reach the size of a critical infrastructure?

The examples shown in Table 2 are just **rough estimates** based on the BSI-KritisV criteria. They nevertheless serve to demonstrate that a critical mass of electrical units can be reached relatively quickly. The actual number of units needed to pose a threat to security of supply will depend on multiple factors such as the **units' location** and **spatial distribution**. This is something that should be investigated when developing resilience measures. It may be necessary to review the thresholds for classifying systems as critical infrastructure. It is also important to check whether any other actors should be taken into account (see policy option 4).

¹¹ Authors' own calculation based on Netztransparenz 2019; BDEW 2017.

¹² Authors' own calculation based on Netztransparenz 2019; Statistisches Amt für Hamburg und Schleswig-Holstein 2020; Statistik Berlin Brandenburg 2020, Statistisches Landesamt Baden-Württemberg 2020.

¹³ This district includes 130 homes, with one heat pump per household. It is assumed that electricity is traded via a platform. The calculations are based on these assumptions. See SmartQuart 2020.

Basic cause 3: The system's technical complexity makes it harder to predict operational impacts. Because it is affected by the weather, season and time of day, the generation of electricity using photovoltaic (PV) and wind power systems requires rapid – and often immediate – responses to changes in these factors. However, the growing number of decentralised electricity generation and storage units means that the interdependencies between the different system components are becoming more and more complex and can have unforeseen and mutually reinforcing effects. The use of artificial intelligence to autonomously control decentralised units can also result in emergent behaviours that make it harder to predict the behaviour of the system as a whole. Finally, future energy markets could also give rise to unpredictable system dynamics, for instance due to variable tariffs where the price charged for electricity can go up or down at different times, or due to new types of market such as peer-to-peer markets, which are not centrally controlled and where electricity is bought and sold directly between two parties.

In addition, the growing **mutual interdependence between the electricity and ICT systems** can give rise to more complex incidents. The electricity supply of the future will be much more dependent than it is today on the correct functioning of ICT components both within the energy system (e.g. grid operators' control systems) and outside of it (e.g. platforms or smart home systems). At the same time, ICT is critically dependent on the electricity supply. Accordingly, an ICT system failure can cause parts of the electricity supply system to fail and vice versa. In the worst case scenario, this could result in cascading subsystem failures. In other words, even small subsystem failures could escalate into a major blackout. And if a blackout does occur, these interactions and all their potential feedback effects could also make it more difficult to gain an overview of the situation and restart the system.

Basic cause 4: Uncertainty about future developments inhibits optimal system design. The design of the electric power system – including its technical structure and processes, guidelines and regulation – is based on explicit and implicit assumptions about the future. However, the uncertainties described above mean that some of these assumptions are likely to prove incorrect. This is further complicated by the fact that once a technology has been implemented or an infrastructure built, it creates a path dependency. In other words, it becomes harder to adapt to new, unexpected developments at a later date, due to factors such as the length of time needed to carry out retrofits. The different rates of development of energy infrastructure and ICT constitute a further challenge. Many electricity system components remain in use for several decades, whereas software is often updated several times a year, and ICT innovation cycles are just a few years long.

Regulatory risks can also arise from a failure to adequately define the responsibilities of different actors, or from a lack of coordination between different countries. The unpredictable evolution of public opinion is another factor that adds to the uncertainty.

1.5 A resilience-based approach to preventing outages

Why are current approaches to blackout prevention no longer enough?

Conventional risk management focuses on identifying and eliminating system design flaws. To do this, it relies heavily on empirical knowledge and lessons learnt from the past. Risks are measured and evaluated by estimating the probability of an adverse event occurring and the damage it would be likely to cause. The results are used to eliminate weaknesses, creating a robust, less **vulnerable** system. **Robustness** is the antithesis of vulnerability – a robust system can cope with an adverse event without detriment to its performance quality. Until now, the primary trigger of most blackouts was the failure of a major component – e.g. of a large power plant or of a short-circuited transmission grid line. This would result in a succession of further faults. The probability of a blackout in Germany has been kept extremely low thanks to an appropriate system design, with a particular focus on redundancy¹⁴ of large operating resources.

However, in the light of the basic causes of new blackout risks described in the previous section, it is clear that we lack the knowledge and experience to carry out a risk-based assessment of key future risk factors.¹⁵ The **increased complexity of the electricity supply** (basic causes 2 and 3) makes it impossible to undertake a full analysis of all possible adverse events. Meanwhile, the **uncertainty** (basic cause 4) regarding the future evolution of the electric power supply means that risk prevention measures cannot cover all possible developments. In addition, different actors draw different conclusions from the generally available knowledge about the future electricity supply (**socio-political ambiguity**). Factors such as their own particular values will therefore influence how they evaluate the acceptability of certain risks and the measures needed to prevent them.

Resilience is a tried-and-tested concept for coping with the uncertainties in complex socio-technical systems. The fact that its main focus is on achieving a soft landing¹⁶ after an adverse event has occurred makes resilience a more effective means of coping with unforeseen incidents. A **resilient electricity supply** is able to absorb incidents without damage or, if parts of the system do fail, is at least able to return to normal operation rapidly, affordably and with a minimum of damage.¹⁷ A resilient system is particularly well equipped to cope with new conditions associated with the systemic changes caused by the energy transition and digitalisation. This position paper does not discuss measures to increase the system's physical robustness and resilience, or switching operations that respond automatically to physical parameters such as voltage or frequency in order to absorb any deviations from normal operation.

Figure 2 illustrates the concept of resilience and shows the advantages of a resilient system over a non-resilient system. Incidents can be absorbed, allowing the electricity supply to be partially maintained and the system to be restored significantly faster.

¹⁴ Redundancy means the availability of additional operating resources that perform the same function but are not required under normal operating conditions. If an operating resource fails, these additional resources can take over its function.

¹⁵ Based on Aven/Renn 2009.

¹⁶ See Kröger 2019, p. 291 and Thoma 2014, p. 14.

¹⁷ Based on acatech/Leopoldina/Akademienunion 2017, p. 10.

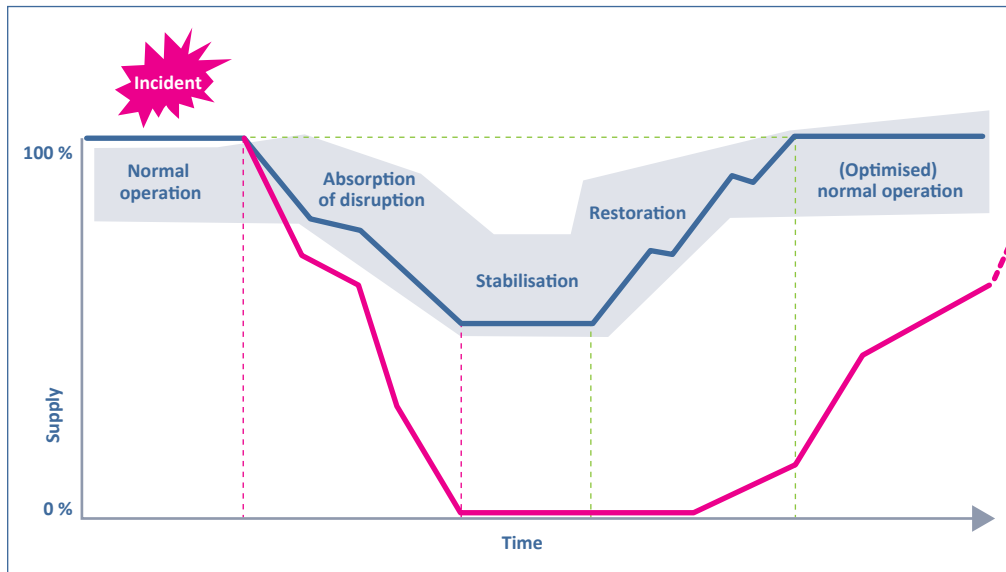


Figure 2: Restoring system functionality: responding appropriately to an incident (absorption of disruption), reverting to critical functions and stabilising the system (stabilisation), followed by a controlled return to normal system operation (restoration).¹⁸

1.6 Methodological approach used by the working group

Drawing on risk governance¹⁹ methodology, a comprehensive environment analysis of the future energy supply system with a particular emphasis on digitalisation was carried out in a series of interdisciplinary workshops, supported by academic research. The focus was on developments that will be relevant to blackouts over the next twenty years. A scenario analysis was then undertaken in order to assess potential future developments. Four different scenarios described what the future energy system might look like in 2040. The emerging new threats that could lead to blackouts were analysed for each scenario. It was found that the origins of these threats could be traced back to four basic causes.

The next step involved identifying ways of countering these new threats. Finally, policy options for implementing these solutions were formulated, assigned to the relevant actors, and evaluated by a cross-disciplinary team. The policy options focus on the areas where action is required today. This is because some measures will take several years to implement (for instance if research and development is necessary), and because the future development of the energy system needs to be planned well in advance due to the long-term investments involved.

¹⁸ Babazadeh et al. 2018, p. 32 f.

¹⁹ IRGC 2018.

2 Policy options

New ways of thinking will be required in order to effectively counter the risks arising from the changes in the electricity supply system and ensure continued security of supply in the future.

Consequently, the ESYS working group identified seven problem-oriented **policy areas** for which it formulated corresponding policy options. If implemented promptly, these policy options can help to solve the medium- to long-term problems that they address by 2040. The authors also set out how policymakers can encourage the responsible actors to implement these measures and support their efforts to do so. The measures are designed to strengthen resilience so that major blackouts can be prevented or so that the electricity supply can be restored as quickly as possible after a blackout, thereby minimising the social, economic and environmental impacts.

The following overview of the policy areas and policy options outlines the problems that arise from the basic causes of blackouts that are described in Chapter 1.4 and are addressed by the different policy areas. It also lists the concrete policy options proposed to tackle them:

Policy options: Understanding and managing the interactions between ICT and energy systems



In the future, the electricity supply will be increasingly dependent on ICT systems. It is vital to ensure that ICT system failures do not result in blackouts.

- Policy option 1 – Analyse interdependencies between the electricity supply and communication networks.
- Policy option 2 – Establish rules for resilient communication networks.
- Policy option 3 – Encourage the relevant actors to integrate the operation of ICT systems and electricity grids.

Policy options: Systemic development of cybersecurity



ICT threats (that may also originate from outside the electricity supply system) can seriously disrupt the electricity supply and call for both technological and organisational solutions.

- Policy option 4 – Introduce cybersecurity standards for all the relevant actors.
- Policy option 5 – Define measures for addressing security vulnerabilities.

Policy options:**Strengthening the contribution of grid operators and grid users to technology resilience**

Grid operation is set to become more challenging, especially in distribution grids. Both small grid operators and the operators of small generating systems will need to make a much greater contribution to resilience than is usually the case today.

- Policy option 6 – Accelerate digitalisation of electricity grids.
- Policy option 7 – Formulate guidelines for enabling resilience through decentralised structures.

Policy options:**Ensuring that ICT integration of small devices supports grid stability**

In the future, the majority of devices and appliances will be connected to and digitally controlled via the Internet. It will be vital to avoid undesired simultaneous activity that can jeopardise the stability of the electric power system, for instance when high load peaks are caused by large numbers of devices being switched on at the same time. On the other hand, these devices can also be used to actively stabilise the power system.

- Policy option 8 – Promote standardisation to prevent problematic simultaneous activity.
- Policy option 9 – Increase the use of decentralised units to strengthen system stability.

Policy options:**Increasing incentives for grid operators to strengthen resilience**

There is a general lack of effective and efficient incentives for grid operators and market players to behave in a way that strengthens resilience. The relevant market incentives should be created.

- Policy option 10 – Incorporate a resilience component into the incentive regulation.
- Policy option 11 – Introduce grid tariffs and smart connection agreements that strengthen resilience.

Policy options:**Ensuring that private actors are involved in the design and implementation of resilience measures**

Private actors may also need to manage their systems in a way that supports the grid. A stakeholder forum should be created to provide input on this aspect and to develop solutions that are viable for the relevant user groups and address any acceptability issues.

- Policy option 12 – Establish a stakeholder forum to address the interests of private actors.
- Policy option 13 – Raise awareness about the influence of private actors.

Policy options:**Institutionalising long-term risk and resilience assessment**

Digitalisation and the energy transition will give rise to unforeseeable trends that could increase the risk of black-outs. An appropriate organisational framework should be created that enables flexible responses for coping with these trends.

- Policy option 14 – Create an organisational framework for incident reporting and resilience assessment.
- Policy option 15 – Establish an overarching monitoring process.

Table 2: Overview of the policy areas and policy options

Key areas for implementation of policy options

Venturing into an unknown future is a constant learning process that requires continuous action and an awareness of path dependencies. Some of the threats outlined in this paper could become reality within the next few years. Consequently, policymakers must act now so that they can respond to these developments. There are **four key areas** where policy options can be implemented:



Processes, products and regulations: Actors are required or encouraged to modify their operational processes or products. Measures in this category can be deemed appropriate if we already know that there is a problem with resilience for which solutions exist and can be evaluated.



Research: Gaps in our currently inadequate knowledge about a digitalised energy system are closed, allowing the development of measures to strengthen resilience. This is achieved primarily through studies and research papers.



Organisations: The relevant authorities and bodies can be restructured or newly established in order to delegate and operationalise responsibility for the policies in question.



Participation: An approach based on dialogue and transparency helps to ensure the acceptability of the relevant measures and build confidence in the appropriateness of the relevant decisions.

The individual policy areas and options are outlined and discussed in the following seven subsections. The subsection on each policy area begins with a description of the key problem and the resulting threats that could cause blackouts during the coming decades. The key policy options requiring urgent action are then discussed and assigned a timescale for their implementation (●●● in the next two years, ●● in two to four years, ● in five to ten years). The effectiveness of each policy option in terms of strengthening resilience is also rated (●●● major contribution, ●● significant contribution, ● modest contribution).

There are various ways in which policymakers can implement the proposed policy options. The next step should therefore be to analyse various concrete solutions for implementing the findings presented in this paper. For instance, it will be necessary to weigh up the pros and cons of regulatory solutions versus financial incentives and of government regulation versus self-regulation for each policy option. It will also be necessary to consider whether a common European approach should be pursued or whether a national solution is (initially) more practicable. The answers to these questions vary on a case-by-case basis and should therefore be analysed separately for each policy option. An exhaustive discussion of the different implementation pathways for each of the 15 policy options is beyond the scope of this position paper and would be at odds with its goal of providing an accessible overview of the most important risks, policy areas and potential solutions. Accordingly, this position paper should also be seen as an attempt to kick-start the public and policy debate on the concrete implementation of the policy options.

2.1 Policy area 1: Understanding and managing the interactions between ICT and energy systems

In the future, the security of the electricity supply will be far more dependent on ICT than it is today. This applies not only to grid operators, but also to other energy actors such as electricity traders and distributors. But actors originating from outside the energy industry – such as the operators of the public communication networks that underpin the Internet – will also have a significant influence on energy supply security. The interdependencies between the electricity supply and ICT systems mean that there is a danger of cascading failures. For instance, a communication system failure could cause a power failure, which could in turn trigger further disruption to communication systems, resulting in further power outages, and so on. ICT issues that cause the simultaneous failure of multiple ICT components are particularly critical.

In the future, electricity and ICT systems will combine to form an overall system characterised by mutual interdependencies – in other words, a complex cyber-physical energy system. Digital technology can help to manage this complexity and improve the system's predictability and stability. However, a lack of situation-specific information about possible disruption to ICT systems can lead to errors in the operation of the power grid at any time. Appropriate cybersecurity measures can go some way towards mitigating the impact of faulty or unstable ICT systems (see policy area 2). However, the ICT applications and communication system used for planning, monitoring and control purposes are still widely viewed as external systems that operate “alongside” the strictly physical electricity supply system. This view no longer accurately reflects reality and should be replaced by an approach that recognises the convergence of the two systems.

ICT systems also play an especially important role in helping to rapidly restore the grid after a blackout. Grid operators must work together to coordinate the technical aspects of restarting the grid, power plants must be controlled and connected in a co-ordinated manner, and information about the status of the grid – which remains fragile while it is being restarted – and about the balance between load (electricity consumption) and feed-in must be continuously analysed. Failure to ensure that the relevant ICT systems are equipped to cope with power outages would seriously compromise efforts to restore the electricity supply.



Policy option 1
Analyse interdependencies between the electricity supply and communication networks

Outcome: Coordination of the energy infrastructure and the relevant communication systems ensures that their mutual interdependencies no longer constitute a risk.

Urgency: ● ● ● **Effectiveness:** ● ● ● ●

What action can be taken today?

- Learn more about the interdependencies between the two infrastructures.
- Formulate European guidelines in cooperation with industry associations and policy bodies.

The mutual interdependencies between the technical side of the electricity supply system and the relevant communication networks must be managed in a way that makes cascading failures impossible or at least extremely unlikely. One way of achieving this is by reducing the dependency of system relevant ICT systems in one section of the grid on the electricity supply in other sections of the grid. The responsible grid operators ensure that any sections of the grid not affected by a potential power outage do not rely either directly or indirectly on ICT systems in the section of the grid affected by the outage in order to maintain the electricity supply. This means that, in the event of an outage, only the ICT systems in the affected area would be compromised (and could be secured), without disruption to the ICT systems in other sections of the grid. However, the extent to which this is actually possible remains unclear. The challenge is made more difficult by the multiple connections between ICT systems and the fact that communication networks and electricity grids often cover different geographical areas.

Before a solution of this kind is developed and implemented, it is essential to know which interdependencies exist between communication networks and the electricity supply system and how they can be mitigated in order to maintain a basic electricity supply if communication is disrupted. Potential cybersecurity vulnerabilities arising from these interdependencies should also be identified. Government should therefore initiate the necessary studies and research programmes. The findings of these studies and projects should be discussed at European level and translated into procedures and regulations. As well as government, it is particularly important to ensure the involvement of the European TSO network (ENTSO-E), the DSO network that has been called for by the European Union but has not yet been established,²⁰ and the relevant standardisation organisations.

²⁰ Regulation (EU) 2019/943, Arts. 52–56.


Policy option 2
Establish rules for resilient communication networks


Outcome: The communication networks have an adequate level of redundancy and, where necessary, are blackout-proof.

Urgency: ● ● **Effectiveness:** ● ● ● ●

What action can be taken today?

- Identify requirements for blackout-proof communication for the electricity grid
- If necessary, specify standards for the technology used.





Greater redundancy must be built into communication networks in order to significantly reduce the risk of a communication network failure jeopardising the electricity supply. It is important to take common cause failures into account, in order to ensure that the same issue does not also cause the redundant systems to fail.

Operators should also make part of the communication network blackout-proof. This would involve equipping it with its own, independent, potentially battery-based power supply that would allow it to keep functioning in the event of a power outage. This is necessary for a variety of reasons, for example to support restoration of the system by the grid operators or island mode operation in the event of a blackout.

The grid operators should come to a technical decision regarding which parts of the communication networks need to be blackout-proof, the length of time that the backup systems should be able to operate during a power outage, and the best mix of technologies from both a technical and an economic standpoint. Their recommendations should form the basis of binding instructions for the grid operators to implement the relevant measures in the field.

In addition to the CDMA 450 mobile communication standard that is currently under discussion, other technology solutions should also be examined. These could include prioritising parts of the public mobile communication network for critical services, and satellite communication, which is becoming more affordable and is not affected by power outages.

Policy option 3



Encourage the relevant actors to integrate the operation of ICT systems and electricity grids

Outcome: Integrated situational awareness of electricity grids and ICT networks makes it possible to identify ICT malfunctions that could cause operational disruption.

Urgency: ● ● **Effectiveness:** ● ●

What action can be taken today?

- Incorporate ICT monitoring into grid operating systems.
- Industry associations to plan and reach binding agreement on the coordination of ICT status transmission between the actors.

In future, the technical electricity system parameters and the system status data of the relevant ICT components and communication networks should be integrated to provide overarching situational awareness. This will allow the operational side to take account of any data that has not been transmitted or has been transmitted incorrectly. In other words, the operational systems of the grid operators and other actors who affect the system's stability must identify and assess potential ICT system malfunctions as early as possible and take the appropriate action to address them.

Information about the TSOs' communication systems is already available today and should be integrated into the grid control systems. This information can usually be extracted from the communication monitoring systems. Training exercises could then be organised to practise how to use the information in the event of an incident (see policy option 6). Grid operators could also carry out pilot projects in which defined use cases are employed to test the effectiveness of the integrated control systems. The responsible national and/or European associations should pursue and prioritise action in the following three directions:

1. From high to lower voltage levels: The big DSOs in the high-voltage level should integrate their ICT information in the same way as the TSOs.
2. From grid operators to other actors: As system security measures become increasingly reliant on ICT systems that are not controlled by the grid operators, as in the case of wind farm control, for example, it will be essential for the grid operators to know the status of these systems and reflect it in their operations.
3. From individual grid operators to the cascade: In order to assess their grid's current status, grid operators need to know whether subordinate grids (i.e. lower voltage level grids connected to their grid) are able to carry out their instructions.

Binding regulations governing the exchange of the relevant ICT data must be formulated for each of these action points. These regulations should stipulate the relevant data formats and how often operational transaction data must be shared, for example. ENTSO-E already regulates data sharing for TSOs.

2.2 Policy area 2: Systemic development of cybersecurity

Cyberattacks are a new threat to the electricity supply that has recently come to the fore, following power outages in Ukraine in 2015 and 2016 that were found to have been intentionally caused by acts of sabotage.²¹ ICT failures have also already contributed to a number of major power outages. The security situation is set to become even more challenging over the coming years and decades. In accordance with the Act on the Federal Office for Information Security, the BSI Regulation on the Determination of Critical Infrastructures²² currently only requires dedicated cybersecurity measures to be implemented by the operators of particularly “large” energy system infrastructures such as large power plants (see infobox on “Critical electric power supply infrastructure”). But future blackouts could also be caused by a cyberattack on a large swarm of “smaller” systems that are present in huge numbers in the energy system. These include standard distribution grid automation components, photovoltaic system control units and electrical appliances in private households, all of which can increasingly be accessed via the Internet. This type of cyberattack is made easier by the fact that many of these devices run the same software. As a result, the same software security vulnerability can be exploited to attack large numbers of devices simultaneously. The combined impact can be greater than the failure of a large power plant, and can certainly result in a blackout. ICT systems that do not form part of the energy infrastructure – such as central service platforms, smart home services and manufacturers’ remote maintenance control centres – can also have a combined system-critical effect. This is because they control huge numbers of devices that are thus vulnerable to malfunctions or sabotage. In view of the sheer number and diversity of systems and ICT components that will affect the future energy supply, it is clear that the current cybersecurity measures for critical energy system infrastructure are no longer adequate. At present, hardly any measures are in place to protect against the threat of a successful attack on these systems.

But it is not just unintended malfunctions and criminal activity that can pose cybersecurity threats. In a bid to combat crime more effectively, governments also sometimes order cybersecurity vulnerabilities known as backdoors to be built into ICT systems so that they can be accessed without the usual access permissions, as well as developing tools to launch their own attacks. All critical infrastructures could be threatened if details of these backdoors got into the wrong hands.

The speed of innovation in the ICT sector poses a further challenge. Protracted security standard certification processes must not be allowed to hold back innovation. The problems that this can cause are illustrated by the rollout of smart meters, where delays in the certification process caused uncertainty in the market and led to issues with the implementation of other services (gateway administration and value-added services). These delays can also lead to the emergence of alternative solutions outside of the secure smart meter infrastructure. There is thus a danger that, as well as being less efficient, cumbersome procedures could also compromise security.

Cybersecurity can never be guaranteed by the introduction of technical solutions alone. On the contrary, relying on technical solutions creates a false sense of security and can actually increase vulnerability. Accordingly, the actors in charge of ICT systems should

²¹ Whitehead et al. 2017.

²² BSI-KritisV 2017.

ensure that their processes combine technical and organisational measures. It is not enough to focus on preventing cyber disruption – it is also vital to keep the system running during an incident, resolve the issue, and analyse what went wrong. Many actors lack the necessary knowledge or personnel to do this.

Policy option 4

Introduce cybersecurity standards for all actors relevant to blackouts

Outcome: Smaller actors and actors from other industries are covered by cybersecurity standards along the lines of the BSI Regulation on the Determination of Critical Infrastructures. These standards have been harmonised as far as possible at European level, and are innovation-friendly.

Urgency: ● ● ● **Effectiveness:** ● ●

What action can be taken today?

- Define risk scenarios as a basis for the standards and identify the relevant actors.
- Protect small grid operators against simultaneous attacks.
- Adapt security standards for the relevant third parties.



The first step in formulating new security standards involves the use of risk scenarios to establish which cybersecurity issues that are at present relatively overlooked could result in blackouts. As well as attacks on transmission and large distribution grids, these risk scenarios should also address other types of attacks and failures, especially those that affect a large number of small units or relevant ICT systems belonging to actors outside of the energy value chain, such as manufacturer platforms or centrally managed smart home systems. The risk scenarios should be regularly updated to keep pace with the rapid and unpredictable development of digitalisation. These scenarios can be especially helpful for implementing security by design, where cybersecurity is built into the design of new solutions and systems.

In the medium term, the binding cybersecurity standards developed on the basis of these scenarios in order to protect the electricity supply should be harmonised and standardised throughout the EU. It will be important to ensure that the regulations and certification procedures are appropriate for the size of the actors.

If binding security standards are also adopted for small, behind-the-meter devices, it could help to prevent the potential threat to the electricity supply posed by huge numbers of consumer products with security vulnerabilities. In addition, the grid connection rules for electricity consumers and generators in the distribution grid should at least be expanded to include cybersecurity measures that make it harder to carry out simultaneous attacks on a large number of such units.

The standardisation process should be accelerated to keep pace with the rate of digital innovation, in order to ensure that the innovations required for the energy transition are not held back or completely prevented. However, it will also still be necessary to meet high data protection requirements. This will call for the establishment of a security standard development process that regularly evaluates the standards' effectiveness and allows for their subsequent modification as and when necessary. The standards could be designed by industry associations on the basis of government requirements, while certification could be carried out by qualified market actors. The latter should be able to carry out certifications faster and more cost-effectively than the State.

Policy option 5

Define measures for addressing security vulnerabilities

Outcome: The number of blackout-relevant cybersecurity vulnerabilities has been minimised, and a rapid response to security incidents is possible.



Urgency: ● ● **Effectiveness:** ● ● ●

What action can be taken today?



- Reduce the risks arising from government-mandated security vulnerabilities.
- Reduce the risk from security vulnerabilities in products that perform system-critical roles.
- Protect OT against IT failures.
- Create European emergency response teams to provide support in the event of a cyberattack.

Even the best security measures cannot provide total protection against ICT-based vulnerabilities due to software bugs, human error in security management or government-mandated backdoors.

Government-mandated backdoors are created when government authorities retain a means of accessing ICT components or develop ICT tools that allow them to access third-party computers so that they can manipulate or delete their data and programs. Examples include State trojans and active cyber defence software.²³ Since measures of this type present a high risk to security of supply, a detailed risk assessment is indispensable (also for other critical infrastructures). While the assessment process should be as transparent as possible, a certain degree of confidentiality will of course be necessary. The appointment of a body independent of the Ministry of the Interior to monitor the assessment process would help to ensure the quality of this measure.

Third-party States can gain access to system-critical ICT components in other countries by ordering their manufacturers to build security vulnerabilities into their software. One way of countering this threat is to require manufacturers to disclose the source code to government inspection bodies. This approach was adopted by the UK government to address Huawei's involvement in upgrading the mobile communication network.²⁴ However, questions remain about how to carry out such inspections. There is also some discussion about whether only certain European manufacturers should be allowed to supply ICT systems for particularly critical core parts of the electricity supply system. Dependency on individual manufacturers could also be reduced by obliging CI operators to use products made by different manufacturers alongside each other, and requiring them to ensure that products are replaced periodically or can be replaced sufficiently quickly.

A common security strategy should be developed for IT/OT systems. Where necessary, it should be possible to clearly separate the two in order to protect the OT side. Everything possible should be done to ensure that IT problems do not lead to critical disruption of OT systems. Appropriate fallback solutions should also be identified.

²³ While the authors recognise that measures such as State trojans are highly controversial, their ethical, technical and legal evaluation lies outside the scope of this position paper.

²⁴ Katwala 2019.

Many relevant infrastructure operators do not have personnel with the knowhow required to thwart and analyse a complex cyberattack aimed at causing a blackout. Support could be provided by emergency response teams made up of experts in this field, ideally assembled at European level.

IT/OT convergence

IT/OT convergence is a phenomenon associated with digitalisation. Operational technology (OT) refers to ICT systems that interact directly with physical equipment or technical processes. In this context, information technology (IT) refers to ICT systems used to carry out business or administrative processes and transactions, such as accounting, contract management and customer management.

In the interests of security, OT systems used to be kept physically separate from IT systems – data could not be directly transmitted between the two system environments. However, IT/OT convergence has led to a move away from this strict separation, in favour of greater integration of IT and OT systems and data sharing between them. This allows costs to be reduced by eliminating parallel infrastructures, and also enables more seamless workflow integration. IT/OT convergence is occurring in many industries, including the energy sector.

One potentially security-critical negative impact of IT/OT convergence was highlighted when participants in a field trial simulating a local blackout attempted to refuel an ambulance. Although the filling station had an independent backup power supply capable of maintaining power during a blackout, the pump (OT) communicated with the point of sale system (IT) before allowing customers to commence refuelling – and on this occasion, the point of sale system rejected the refuelling request, since it was unable to connect to the tax authority responsible for fiscal transactions. While this feedback from the IT system to the OT system is actually desirable in everyday operation, it caused a problem in a blackout situation by preventing the ambulance from refuelling.

This illustrates how a failure outside of the OT system (in this case the failure of the tax authority's IT system) can have undesired effects on the OT side (preventing use of the pump in an emergency). This becomes even more problematic for more system relevant OT systems such as power plant or grid control systems. An extremely cautious approach should therefore be taken to IT/OT convergence in the context of critical infrastructure.

2.3 Policy area 3: Strengthening the contribution of grid operators and grid users to technology resilience

The transformation of the electricity supply caused by its growing decentralisation and digitalisation, coupled with the increasingly volatile generation of electric power, means that the danger of “nasty surprises” for grid operators is increasing as every year goes by. The system’s growing complexity will make it harder and harder for grid operators to predict their grids’ behaviour over the next two decades. Future incidents could also be very different to the incidents that occur today – the interactions between generating systems that are affected by the season, time of day and weather, the huge number of devices that can be controlled via the Internet, and digital business models could result in sudden, unexpected fluctuations in output. Distribution grids will increasingly be pushed to their physical and technical limits, and will be characterised by extensive automation and far more complex, (pro)active and challenging operational requirements. As a result, any failures could have more serious implications. Many DSOs will have to respond to the significant increase in the fragmentation and diversity of new actors by intervening to stabilise their own grids far more frequently than they do today.

Consequently, operators of small generating units will need to provide much more technical support to strengthen resilience, and lower voltage level grid operators will also need to do their bit.





Policy option 6
Accelerate digitalisation of electricity grids

Outcome: Grid operators are much better equipped to support the system, thanks to extensive digitalisation, new processes and regular resilience training.

Urgency: ● ● ● **Effectiveness:** ● ● ●

What action can be taken today?

- Establish criteria for technical equipment – including those of small grid operators – and for sharing information to enable proactive system operation.
- Establish a process for monitoring and evaluating progress with grid digitalisation.
- Provide mandatory training on coping with unforeseen events.

In order to resolve complex future incidents, grid operators will require comprehensive situational awareness of the current system status, including information about subordinate grids, the degree of flexibility currently available, and short-term predictions of system dynamics. Extensive digitalisation of distribution grids and the generation and storage units and controllable consumer devices connected to them will be essential for grid operators to acquire and share this situational awareness and agree on the necessary measures among themselves. The coordinated development of the digital infrastructure and the definition of standards for sharing information among all the actors will be key to making this possible. Grid operators should take the needs of upstream grid operators into account when implementing their own digital infrastructure. Regulators and grid operators must ensure that digitalisation is implemented in a way that also allows small grid operators and coalitions of regional or local actors to cope with new requirements. The BMWi and BSI²⁵ standardisation strategy could be extended in order to assist with this objective. In addition, the relevant ministries could promote the necessary research through individual calls for tenders on the topic of “resilience and digitalisation” under the auspices of the 7th Energy Research Programme.²⁶

A process should be established to agree on the relevant digitalisation goals, monitor their timely implementation, and adjust them as necessary. The digitalisation of the grids should be tracked and evaluated through this parallel monitoring process, with the results being used to formulate recommendations or mandatory measures. The digitalisation of the grids must go much further than simply rolling out smart meters. Given the critical importance of local conditions in the distribution grids, distribution system operators should retain the freedom to implement digitalisation in line with their particular circumstances.

All grid operators should receive mandatory training that gives them the opportunity to practise coping with novel and unforeseen blackout-relevant incidents and test new ICT- and AI-enabled technologies and tools. Other actors who play an important role in dealing with incidents – such as telecom network operators – should be included in this training. It will be essential to agree on a standardised process and clear criteria for developing and carrying out these training exercises.

²⁵ BSI/BMWI 2020.

²⁶ For more on initiatives to improve data sharing among grid operators, see also the Coordinet (www.coordinet-project.eu) and TDX Assist (www.tdx-assist.eu) projects.



Policy option 7
Formulate guidelines for enabling resilience through decentralised structures

Outcome: Individual sections of the grid are able to operate in island mode and thus temporarily maintain the electricity supply during a blackout. The supply of critical consumers is prioritised.

Urgency: ● ● **Effectiveness:** ● ● ● ●

What action can be taken today?

- Carry out R&D projects and field tests to establish how best to implement this goal.

Given the appropriate technical and regulatory conditions, it is possible for part of a distribution grid to temporarily operate in “island mode” during a blackout, maintaining a usually limited local electricity supply. The part of the grid operating in island mode is reconnected to the rest of the grid as soon as the blackout ends. Island mode operation helps to mitigate the impact of blackouts and restore the grid to normal operation.

The supply of electricity to critical consumers such as hospitals and the fire service should be prioritised if the section of the grid operating in island mode does not have enough generating capacity to fully supply the area it covers. All the relevant actors (grid operators, unit operators, businesses and the general public) should be closely involved in a participatory process geared towards establishing the regulatory framework and technical conditions required to enable selective island mode operation.

As well as introducing socially acceptable and non-discriminatory rules for island mode operation, it will be necessary to determine which sections of the grid should be operated in island mode and how to calculate the minimum requirements for generating, consuming and storage structures. Storage units can play an especially important role in ensuring stable island mode operation.²⁷ This potential function of storage units in the energy system should be addressed by future storage technology R&D. The relevant ICT requirements should also be taken into account (see also policy option 2), and fallback solutions should be developed that are capable of coping with ICT component failure. It will furthermore be necessary to find a way of developing common rules for island mode operation and coordinating its implementation. In particular, it will be important to identify the rules that should be established as European standards through the ENTSO-E network. Any potential new roles and duties for grid operators should also be clarified. For example, the grid operator could either completely take over responsibility for load and generation control during island mode operation, or they could support the self-organisation of aggregators or decentralised electricity generators and consumers.

Answers to these questions should be identified through R&D projects, and pilot projects should be carried out to test the relevant solutions in the field under real-life conditions. Calls for tenders for these projects could be issued under the auspices of Germany’s 7th Energy Research Programme, for example. Since implementation of these measures will be a lengthy process, it should be commenced as soon as possible. The

²⁷ For an in-depth discussion of how battery storage systems can be used, see acatech/Leopoldina/Akademienunion 2020-1.

establishment of the necessary regulatory framework will take even longer and should therefore also begin without delay.

2.4 Policy area 4: Ensuring that ICT integration of small devices supports grid stability

Within the next few years, almost all new electricity generating units (roof-mounted solar units, combined heat and power systems, etc.) and devices²⁸ that come onto the market will feature Internet connectivity. The combined capacity of these devices will eventually reach the point where mass synchronous activity (triggered e.g. by software bugs, malicious attacks or simultaneous user activity) can increase the risk of a blackout by causing large and rapid power fluctuations in the electricity grid that cannot be absorbed by the measures currently in place.

Critical simultaneous activity can also occur with units that are not directly controllable via the Internet, but that have the same grid-stabilising behaviour built into their firmware. This has already been witnessed in the case of the 50.2 hertz problem. Based on the assumption that the number of PV units would only grow slightly in the future, in 2005/2006 the Association of German Grid Operators, as it was then known, introduced a rule stipulating that PV units should shut down automatically if there was an oversupply of electricity (i.e. if the frequency exceeded 50.2 hertz). However, due to the energy transition, the number of PV units increased so dramatically that switching them all off at the same time would have massively overcompensated for the oversupply, thereby destabilising the system. As a result, some 300,000 PV units had to be retrofitted in a process that took a full year to complete. This demonstrates how any rules built into a system are always based on assumptions about the future. If these assumptions prove to be incorrect, they can create a vulnerability in the energy system that can take substantial effort to remedy. Rather than the cost of any necessary retrofits, it is the time needed to carry them out that has a critical impact, since there will be a long period during which blackouts could be caused by incidents arising from vulnerabilities in the infrastructure that has not yet been upgraded. This problem can be even more serious for old equipment covered by grandfather clauses, due to the more complex legal provisions covering retrofits of such equipment.

On the other hand, synchronous generating and storage unit activity can also be induced intentionally in order to support grid stability. Doing so can reduce demand for balancing energy from large power plants or support island mode operation in the event of a blackout (see policy option 7). Decentralised generating units already contribute to system stabilisation today, for example by helping to maintain voltage stability and contributing to control reserves.

²⁸ In this context, the term “device” refers to behind-the-meter electrical devices such as heat pumps, electric heaters, household appliances, domestic charging stations or home electricity storage systems.

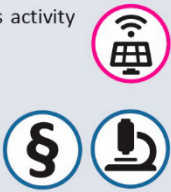
Policy option 8
Promote standardisation to prevent problematic simultaneous activity

Outcome: Device standards reduce the likelihood of simultaneities and simultaneous activity jeopardising grid stability.

Urgency: ● ● ● **Effectiveness:** ● ●

What action can be taken today?

- Develop, adopt and introduce a patchability standard.
- Carry out studies and research into the validation of switching command plausibility using local physical variables.



Unplanned and unforeseeable simultaneities or the simultaneous switching off of devices and generating units must be recognised as a potential risk and included in any resilience strategy. Accordingly, expert committees must develop use-case-specific minimum standards that are future-proof and encompass a wide range of potential units and devices. International standardisation would deliver important benefits, since critical simultaneous activity has the same negative impacts throughout the synchronous grid of Continental Europe.

One important aspect that must be addressed by these standards for generating units and devices is the need to guarantee patchability. Patchability means that the manufacturer or the operator can easily and remotely update a technical device's software during operation by installing patches. It is important to implement patchability today, since some units and devices are used for several decades and it is impossible to predict which technical requirements they may have to meet in the future. This will require cooperation between regulators, manufacturers and other affected actors such as the operators of the units and devices in question. It will be especially important to clarify funding issues, liability questions, rules relating to product discontinuation, and responsibilities for communication links.

Protection against behaviour that could potentially harm the system can also be provided through local plausibility checking, whereby generating units and devices independently validate the plausibility of switching commands – for example using physical variables such as voltage and frequency – and respond accordingly. Artificial intelligence solutions can be particularly useful in this context. It is not currently possible to say which kind of plausibility checking could determine whether the switching commands transmitted by the grid operator are likely to have a negative impact on the grid in a given situation. The grid operators must therefore carry out the necessary studies and research in conjunction with the other relevant actors (such as unit and device manufacturers and operators). It will also be necessary to ensure that the relevant plausibilities are patchable.



Policy option 9
Increase the use of decentralised units to strengthen system stability

Outcome: Decentralised units contribute significantly to the stability of the electric power system.

Urgency: ● ● **Effectiveness:** ● ● ● ●

What action can be taken today?

- Develop measures to create the necessary communication technology connections and ensure that the relevant actors, such as grid operators, operators of units and devices, and telecommunications companies are involved in this process.
- Research the use of artificial intelligence to enable an appropriate response to complex and unfamiliar incidents or attacks.

The systemic importance of small units and devices can also be used to positive effect – in the future, decentralised generating units and controllable devices can and should make a much greater contribution to the resilience of the energy system than they do today. For example, they can provide system services to help ensure secure and reliable system operation, or help to restore the electricity supply after a blackout. In addition to the necessary power electronics equipment, this will call for cost-effective communication technology integration of the units and devices in question with the grid operator's control system. This should go further than merely providing the option of curtailment.

While the rollout of smart meters does provide for the connection of decentralised units, the focus is primarily on billing processes and variable tariffs, rather than on the potential for supporting system stability by controlling connected units or providing value-added services for customers. In order to ensure the desired connectivity, the current regulations should be supplemented by (international) agreements on standards for interoperability and for the incorporation of decentralised units into large-scale platforms. In the summer of 2019, grid operators and operators of the relevant units and devices started working together in the CONNECT+ project, with a view to resolving the technical and regulatory data sharing issues. Pilot projects with grid operators, telecommunications companies and aggregators will seek to demonstrate that there are affordable solutions for meeting the high ICT connection requirements for incorporating small units and devices into a balancing energy pool.

An even more far-reaching approach to integrating small generating units and controllable power-consuming devices involves controlling them via artificial intelligence algorithms that are built directly into the units and devices themselves. This enables an appropriate response even to complex and unfamiliar incidents or attacks. The relevant artificial intelligence techniques are still in their infancy and require extensive further research.

However, the use of small units and devices to support system stability is not only a question of technological and economic feasibility. While these aspects are already being studied in various research and pilot projects, the acceptance of this approach by small private actors should also be addressed through the appropriate measures (see 2.6).

2.5 Policy area 5: Increasing incentives for grid operators to strengthen resilience

As the number of decentralised and digitally connected units and devices increases in the future electricity grid, it will become more and more important for the relevant actors, including grid operators, to take measures to strengthen resilience. However, the energy industry's regulatory framework contains very few elements that explicitly take resilience into account. Grid operators' investment decisions can have a significant influence on the resilience of the electric power system. At present, however, grid operators have no incentive to include externalities – or their avoidance – in their investment decisions. While the grid operators pay for the resilience measures, it is the grid users who benefit from them. The cost of measures to strengthen resilience is not currently recognised in the German Incentive Regulation Ordinance (ARegV) for power grids. Incentive regulation is an instrument designed to prevent grid operators from making a monopoly profit from the natural monopoly of the electricity and gas grids, and to ensure that they operate their grids cost-efficiently. The revenue caps create an incentive to reduce costs for a given, quantifiable operation and thereby increase profits. However, incentive regulation does not resolve all of the relevant challenges. It is therefore necessary to determine whether the desired impact on resilience can be achieved in an economically efficient manner through incentive regulation, or whether effective threat protection can only be accomplished through (additional) regulatory instruments (e.g. in the field of cybersecurity, see policy options 4 and 5).

Two (of the most important) ways of addressing this problem are discussed below. However, it should be stressed that there are many other regulatory issues that are of relevance in this context.

Incentive regulation (see policy option 10): The revenue cap established by the ARegV is key to determining the incentives for grid operators. Whether and how incentive regulation effectively takes resilience into account depends on the type of costs generated by the measures to strengthen resilience and on the measures that are already included in the ARegV (e.g. quality or “Q” components). Because they share a lot of common ground, the distinction between quality and resilience regulations is not always crystal-clear. However, we argue that in its current form, the ARegV does not create adequate incentives to strengthen resilience as defined in this paper, and that an additional instrument is therefore necessary. It is true that grid operators do already have the opportunity to claim back some of the cost of measures to strengthen resilience. However, the focus here is on whether grid operators also have strong enough incentives to actually use these instruments. We propose that a resilience component should be added to the instruments in question.

Grid tariffs (see policy option 11): Grid tariffs are the fees charged for access to the transmission and distribution grids. The corresponding regulations also determine the feed-in tariffs for decentralised units. We argue that resilience should be included in the current debate on smart connection agreements. These flexible grid connection agreements for electricity producers allow the grid operator to curtail the connection (with or without compensation for the producer).

Ultimately, the current interruptible loads approach²⁹, which is based on a voluntary, self-healing process, already attempts to achieve a similar effect for loads to the effect that would be achieved by smart connection agreements. The key difference between these two instruments relates to how voluntary they are. While interruptible loads offer the freedom to choose how much, when, and at which (variable) price the instrument is used, in smart connection agreements these details are all regulated beforehand and are binding once the agreement has been signed. The only free choice is whether or not to sign the smart connection agreement.

29 Regulated by AbLaV 2016.



Policy option 10
Incorporate a resilience component into the incentive regulation

Outcome: The ARegV contains incentives for grid operators to implement effective measures to strengthen resilience.

Urgency: ● ● **Effectiveness:** ● ● ●

What action can be taken today?

- Incorporate an “R” component into the ARegV as an additional regulatory measure to strengthen resilience.

The ARegV³⁰ uses the term “quality” to refer to the electric power system’s security of supply. Quality is determined by “grid reliability” and “grid efficiency”. Articles 18–20 of the ARegV regulate the “Q components”, where “Q” stands for quality. Resilience, as defined in this paper, is not covered by the Q components. There are two reasons for this. Firstly, the indicators for determining quality are unsuitable for evaluating resilience as well. Resilience is preventive and predictive, and thus focuses on a different timepoint to quality. Secondly, the causes of the failures discussed in this paper in the context of resilience are usually beyond the control of the grid operators, who are therefore not liable for them. This means that the monetary consequences are also outside the scope of the ARegV and cannot therefore act as an incentive for the grid operators.

Without additional incentives, grid operators will not include the externalities (i.e. all the costs arising from a lengthy power outage that affect third parties but not the grid operators themselves) of a supply failure in their investment decisions for resilience measures. This is why the ARegV needs an additional regulation aimed at strengthening resilience – in other words, an “R component”, where “R” stands for resilience.

The following key questions must be answered before a resilience component can be implemented in practice:

- What are the appropriate indicators for a resilience component?
- What instruments would help to improve the incentives for grid operators?

The concrete implementation of a resilience component is a complex matter that requires in-depth analysis. Whichever instrument is chosen, its parameters should strike an appropriate balance between the effectiveness of the incentives and the financial risks for the grid operators.

³⁰ ARegV 2019.

Policy option 11

Introduce grid tariffs and smart connection agreements that strengthen resilience

Outcome: An amendment to the Electricity Network Charges Ordinance allows grid operators to modify grid tariffs in order to effectively strengthen resilience.

Urgency: ● ●

Effectiveness: ● ●

What action can be taken today?

- Add a resilience component to smart connection agreements to reward the choice of locations that strengthen resilience and the avoidance of simultaneities.



The grid tariff structure is regulated by the Electricity Network Charges Ordinance (German: Stromnetzentgeltverordnung, StromNEV).³¹ However, the level that grid tariffs are set at is determined by the revenue cap and hence by the ARegV. The tariff structure and cost allocation are the most important factors for determining grid tariffs, although they may also vary on the basis of other factors such as time and location. However, resilience has never been included as a criterion.

There are two factors relating to grid use and access charges that are particularly relevant to the resilience of the electric power system: simultaneity effects and grid topology. In both cases, differentiated grid tariffs can influence behaviour in a way that strengthens the electric power system's resilience. Smart connection agreements are one approach that could prove useful in this context. These flexible grid connection agreements are currently being trialled in countries such as France, Belgium and the UK.³² Smart connection agreements aim to tackle grid shortages through the grid connection fee, especially for renewables, along similar lines to the regulation requiring operators to contribute to the cost of expanding the grid (German: Netzausbauzuschuss). It is proposed that a resilience component should be added to smart connection agreements. Grid users who choose locations that strengthen resilience and/or who reduce simultaneities would be rewarded, and vice versa.

The exact design will be strongly influenced by the details of the relevant grid topology. The agreements should therefore be implemented flexibly and on a case-by-case basis by the grid operator, and the appropriate incentives should be created through the ARegV (see policy option 10).

2.6 Policy area 6: Ensuring that private actors are involved in the design and implementation of resilience measures

The connected, digitalised energy system is a complex socio-technical system in which it is equally important to take technological and social factors into account. This type of system is characterised by the coevolution of technology and society: the technological system influences society by affecting the way people live, while its own development is in turn influenced by social innovations and trends. For example, the market

³¹ StromNEV 2019, §§ 15 ff.

³² See Furusawa et al. 2019.

responds to greater public awareness of the importance of energy efficiency by providing new technological products, which in turn influence public awareness through marketing or energy labels.

In the future, units and devices belonging to small private actors will have great potential for supporting the energy system and strengthening resilience thanks to their advanced technical connectivity. However, this will also mean that private actors' behaviour becomes increasingly important, since the generating units and devices that they use could potentially have a system-critical impact (see 2.4). Moreover, most small private actors do not realise that they can have this impact.

Even today, private actors are already playing an increasingly active role and influencing the shape of the energy system, for example as prosumers. Other developments include the establishment of energy cooperatives to operate wind and PV systems, and the first examples of community initiatives in which private households create their own local system for exchanging energy among themselves. Digitalisation and the growing number of home electricity storage systems and electric vehicles could further strengthen this trend.

In the future, grid operators will be able to harness the potential contribution to resilience enabled by the digitalisation of private households in order to obtain data to improve their consumption forecasts, to directly control the units and devices e.g. by selectively switching PV units on or off, or to organise island mode operation. Ultimately, however, all these measures involve intervening in the actors' private affairs and will therefore require a certain level of acceptance.

As a result, implementation of these measures could cause problems such as a loss of freedom of choice and trust. There is also a danger of measures failing because they do not appeal to the target group, for example. These problems could mean that the potential of private units and devices to strengthen resilience remains unexploited, solutions are not implemented, and new regulations fail to achieve the desired effect, thereby increasing the likelihood of system-critical situations.

The role of industry

Industrial actors must also do their bit to strengthen resilience. They can do this indirectly by ensuring that the devices and equipment used in the electric power system meet various different requirements for strengthening resilience. These include:

- Ensuring that ICT systems (e.g. platforms) comply with the relevant security standards (see policy option 4)
- Ensuring that small behind-the-meter devices comply with the relevant security standards (see policy option 4)
- Disclosing source code to government inspection bodies so that it can be checked for any security vulnerabilities (policy option 5)
- Enabling flexible configuration of technical device software (policy option 8)

The following industrial actors would be affected by these measures:

- **Manufacturers of energy technology** and the associated OT systems (e.g. smart operating resources, generating and storage systems)
- **Developers of ICT systems** for the electricity supply (e.g. ICT components and communication network equipment)
- **Operators of ICT systems** connected with the electricity supply (e.g. data centres, platforms, communication networks)

In addition to the above, industrial actors are already contributing actively to the resilience of the electric power system by making part of their demand flexibility available to grid operators. The flexibility of some industrial processes can be marketed and used to support system stability, for example in the form of control reserves or interruptible loads.³³ In the future energy system, however, it will be necessary to make far greater use of the flexibility of industrial and commercial electricity consumers.³⁴ Significant synergies are generated in this context by **Industrie 4.0** – the increased connectivity of machines and industrial and business processes enabled by the digitalisation of industry. Industrie 4.0 allows businesses to configure their processes to consume electricity more flexibly. Prices on the electricity exchange provide them with an incentive to respond flexibly to fluctuations in the supply of wind and solar power.³⁵ Digitalisation also contributes to more **resource-efficient production**.³⁶

- In the future, manufacturing processes will be climate-friendlier or even climate-neutral. This will involve more than simply replacing gas, oil and coal with renewables. In some instances, it will mean completely transforming the relevant production processes (e.g. direct reduction of iron ore, where hydrogen replaces fossil fuels in blast furnace processes in the steel industry³⁷). However, this could lead to changes in demand patterns that will need to be taken into account by grid operators (see 1.2).

³³ See Umweltbundesamt 2015.

³⁴ See acatech/Leopoldina/Akademienunion 2020-2.

³⁵ For examples, see Agora 2016.

³⁶ See Plattform Industrie 4.0 2020.

³⁷ See Agora 2020.

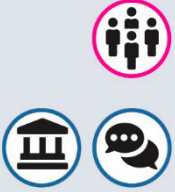
Policy option 12
Establish a stakeholder forum to address the interests of private actors

Outcome: An ongoing, transparent process ensures that all the relevant actors are involved in the decision-making process for new regulations.

Urgency: ● ● ● **Effectiveness:** ● ●

What action can be taken today?

- Establish a stakeholder forum to develop solutions that are acceptable to private actors and ensure that they are implemented transparently.



A stakeholder forum should be established in order to include all the relevant players in the decision-making process for new regulations that affect private actors. As well as the regulator and the private actors themselves, the other main players are the grid operators, aggregators, industry associations and consumer organisations. It is important to ensure an ongoing and transparent process, since new technological developments and new actors will continue to emerge. The ultimate goal should be for the outcomes of the process to be accepted by all the stakeholders.

The acceptance of these regulations by private actors is a particularly sensitive issue. Any questions or concerns regarding matters such as data protection and invasion of privacy should be identified and addressed as soon as possible. The stakeholder forum will also need to decide which measures are critical for resilience and should therefore be mandatory, and which measures can be implemented through appropriate incentive systems (e.g. voluntary self-regulation, financial incentives).

Incentive systems and regulations can of course have both positive and negative impacts on the electric power system. Consequently, it is important to design incentives in a way that achieves the desired effect while at the same time preventing or absorbing any negative impacts. It is also necessary to address the possibility of the incentives being rejected by the relevant actors. The incentive systems and their impacts should be studied in appropriate research projects and tested in experiments or regulatory sandboxes.

Policy option 13



Raise awareness about the influence of private actors

Outcome: Private actors understand their influence on the stability of the electric power system and are digitally literate.

Urgency: ● ● ● **Effectiveness:** ● ●

What action can be taken today?

- Carry out information and education campaigns on the topic of resilience for different target groups, taking into account the different information needs of the groups in question.

It is important that small private actors should understand how their behaviour influences the stability of the electric power system and what they can do to support the system's stability. Accordingly, it is necessary to raise awareness of the problem and promote both digital literacy and a basic understanding of complexity.

Private actors are not directly responsible for the system's resilience. Nevertheless, they should have access to comprehensive information on any matters affecting their rights and interests. In order to ensure transparency and build trust, the information provided should reflect the needs of the relevant groups and ensure the private actors' inclusion and sovereignty.

The first step should be to develop and implement information initiatives such as campaigns. These should include education measures both in schools and as part of continuing professional development programmes. In order to strengthen the private actors' (digital) sovereignty, it is important to ensure that the information is transparently adapted to their respective needs, for example through an information portal for different target groups and with different communication formats. These measures can be even more effective if they are planned using behavioural analytics, so that different aspects of individual behaviour are reflected and addressed more effectively.

It is important to ensure that the providers of the education measures and in particular the information campaigns are not perceived to have vested interests. Consequently, the relevant content should be developed by government ministries, consumer protection organisations or alliances of these actors. Private actor advocacy groups such as consumer protection organisations and data privacy initiatives should also be included in order to build trust in the supervisory authorities and instruments. These groups should be involved in both the design and the communication of the relevant interventions.

2.7 Policy area 7: Institutionalising long-term risk and resilience assessment

The decisions taken by regulatory authorities and operational actors such as grid operators are often based on past experience and on the analysis of foreseeable future developments. While this approach has hitherto proven to be perfectly adequate for making the right decisions, as evidenced by the high reliability and quality of the electricity supply, it will be less effective in the future. This is because the system will become far more complex and unpredictable due to digitalisation's fast-growing influence on the energy supply – for example through the Internet of Things, digital business models, digitalised or automated operational processes, artificial intelligence and the platform economy. Unexpected developments that could pose a threat to the electric power system could potentially come about much faster than is currently the case.

Consequently, future risk assessments and measures will need to place more emphasis on coping with uncertainty and unexpected developments. It will be necessary to include risk factors for which past experience provides very little guidance. In the interests of coping more effectively with unexpected future events, the concept of resilience should be more strongly embedded in risk assessments and in policy measures geared towards maintaining security of supply. This will call for the creation of a more appropriate institutionalised organisational framework.

However, it is difficult to evaluate how much a measure contributes to resilience when basic data about multiple past incidents and their impacts is lacking, and when it is not yet possible to adequately measure and assess the resilience of the electricity supply. This reduces the effectiveness and efficiency of efforts to ensure resilience.

At EU level, the Regulation on risk-preparedness in the electricity sector³⁸ already institutionalises detailed, supranational risk assessments for TSOs. It also provides for the designation of a national crisis coordinator tasked with acting as a contact point in the event of an electricity crisis. However, the Regulation only applies to transmission grids and extreme blackouts, and its focus is confined to the medium term and foreseeable risks. Its scope should therefore be extended so that greater emphasis is placed on unforeseen events and long-term developments. Moreover, it should not focus exclusively on the technical aspects. Normative concepts and judgements can also change over the course of a long-term social transformation process such as the energy transition, as illustrated by attitudes towards nuclear power in Germany. The decisions of the regulator and also of grid operators often create path dependencies, since they result in the construction of particular types of infrastructure. Any resilience strategy should therefore take a range of potential social developments or even instabilities into account.

³⁸ Regulation (EU) 2019/941 on risk-preparedness in the electricity sector, see Regulation (EU) 2019/941.

Policy option 14

Create an organisational framework for incident reporting and resilience assessment

Outcome: Appropriate organisational structures exist for reporting and analysing incidents. Potential risks are systematically evaluated using objective resilience assessment indicators and taken into account by grid operators and other relevant actors.



Urgency: ● ● ● **Effectiveness:** ● ● ●



What action can be taken today?

- Establish an independent, central incident information and reporting office.
- Establish a government or government-supervised institution to carry out regular risk assessments.
- Develop appropriate resilience indicators and establish the corresponding standards.

An independent, central, European incident information and reporting office should be established to pool and process continuously updated information about blackout-relevant risks, incidents, cybersecurity vulnerabilities and potential countermeasures for grid operators. This information should be made available in several different languages. The office could also formulate recommendations based on its analysis of the data. It should ensure that national authorities and emergency response teams are promptly informed about incidents, and should also work closely with the relevant actors, such as grid operators and potentially manufacturers. It is also necessary to clarify how the office would cooperate with the crisis coordinators provided for by the EU Regulation on risk-preparedness in the electricity sector. Initially, the office should be established at national level. The lessons learnt could then be used to help design and build a corresponding institution at European level.

The institutional framework for risk assessment should also be strengthened. A government or government-supervised institution should be created to identify developments that could pose a threat to the energy system at an early stage and make recommendations to policymakers. The EU Regulation on risk-preparedness in the electricity sector could serve as a template, allowing early warning systems and indicators (e.g. for market risks, technical disruption or political upheaval) to be developed and incorporated. Monitoring of long-term trends and the development of adaptation strategies are further valuable measures that could be used as a basis for formulating policy recommendations. As well as blackouts, the risk assessment system should also include smaller power outages and brownouts, together with sectors that can indirectly affect the energy system through their connections to communication networks. It will also be necessary to promote the development of new methodologies that enable better forecasting. As well as experts on the energy supply, this process should also include ICT and risk research experts and social scientists.

It will also be necessary to create a framework for evaluating the effectiveness of different measures. The first step will involve developing appropriate qualitative and quantitative indicators. The specifications and standards for the indicators can be established either nationally or at European level (e.g. under the auspices of an EU mandate). Clear evaluation standards will enable resilience by design, i.e. the incorporation of resilient behaviour into solutions at the design stage. They will also provide a robust evidence base and justification for investments in grid ICT, thereby supporting a clear, transparent process.



Policy option 15
Establish an overarching monitoring process

Outcome: The entire resilience strategy for the electricity supply is independently evaluated on a regular basis.

Urgency: ● ● ● **Effectiveness:** ● ● ● ●

What action can be taken today?

- Establish an overarching monitoring process and an institution responsible for carrying it out.

An independent institution should be created to carry out ongoing monitoring on behalf of government, in order to establish the effectiveness, efficiency and adequacy of the resilience strategy being pursued, both now and in the foreseeable future. Whereas the risk assessment institution proposed in policy option 14 would be tasked with developing concrete risk instruments and new resilience measures, the focus of this institution would be on evaluating the overall resilience strategy and its implementation. In other words, its role would be to scrutinise policy decisions that have implications for the resilience of a digitalised energy system. Among other things, this process would enable early identification of path dependencies and implementation of appropriate responses. The interactions between different measures should also be taken into account so that potential negative impacts can be anticipated.

The institutional framework for risk assessment and the development of risk assessment indicators and standards (see policy option 14) will provide a valuable source of information for this overarching monitoring process. Accordingly, these measures should be implemented before or at the same time as the monitoring process.

A number of different models could be used to implement the monitoring process:

- In order to guarantee its political impartiality, the monitoring could be carried out by a separate, independent expert body along the lines of the German Council of Economic Experts. A dedicated Act would have to be passed to enable the establishment of such a body.
- Expert evaluation of the information collected, aggregated and analysed by the Executive, along the lines of the Federal Government's "Energy of the Future" monitoring process.
- Participation of stakeholders and civil society organisations in order to create acceptance and develop explicit targets. Direct involvement of members of the public would also be possible, but this would involve a significantly higher workload, especially if a representative cross-section of society was required.
- Studies on individual aspects.

The findings of the monitoring process would be used by policymakers to update the resilience strategy by making adjustments to the relevant measures, abandoning measures that are ineffective or inefficient, and introducing new ones.

3 Conclusion

The onward march of digitalisation and the accompanying transformation of the energy system shows no sign of abating. Digitalisation is key to managing the changes in the electric power system caused by fluctuations in the power fed into the grid by wind and solar systems, decentralised generating structures, electric mobility and new market actors. At the same time, however, it increases the system's complexity by enabling the emergence of new actors who can affect the system's security, including actors from outside of the system. It also leads to new vulnerabilities and interdependencies between the electricity and ICT systems. Unforeseen or unforeseeable events and trends can destabilise the electric power system and cause blackouts, with devastating consequences for society. By implementing an appropriate resilience strategy, policymakers can create a framework that will make it possible to maintain the reliable electricity supply that we are accustomed to in tomorrow's digitalised, highly connected and climate-friendly energy system. The resilience by design principle should be employed wherever possible to ensure that the relevant solutions are designed in a way that strengthens resilience. Resilience should thus be a fundamental requirement for technological and societal security solutions.³⁹

The 15 resilience strategy policy options presented in this paper address the risks that are likely to arise over the next twenty years due to the combined effects of the growth of digitalisation and the energy transition. Since implementation of some measures will take a long time (research is still required in some cases to acquire the necessary knowledge), it should be commenced as soon as possible. Moreover, long-term investments in electricity grids and generating systems can create path dependencies and should therefore take future developments into account. It is true that measures to strengthen resilience will initially mean higher costs. However, these costs must be weighed up against the costs associated with major blackouts. We currently lack the methods and data needed to carry out concrete risk assessments that establish whether measures are proportionate to the probability and cost of the damage they prevent. However, these calculations are in fact unnecessary for the electricity supply scenarios considered in this paper, since the cost of the proposed measures is trivial compared to the damage caused by a blackout. The projected seriousness of this damage is so great because it can include not only economic effects but also major social and environmental impacts.

The proposed measures are mainly aimed at energy supply actors. Small actors who are currently considered to play a less important role in major blackouts – such as municipal utilities and the operators of small units – are becoming increasingly important for ensuring the system's future resilience compared to large energy providers and TSOs. A resilient system will also have to incorporate actors who until now were considered to have little if anything to do with the causes, prevention and mitigation of

³⁹ See acatech 2014, pp. 20 and 25.

blackouts. These include device manufacturers, platform operators, public communication network operators, private households, interior ministries and police authorities. Effective implementation of the proposed policy options could be supported by analysing the interests of the affected and involved actors. These actors will be extremely important in the future and will influence the resilience of the electric power system in all manner of different ways – for instance through their growing importance for the system's operation and reliability, by increasing its vulnerability to cyberattacks, or through new forms of simultaneous activity, since switching large numbers of small devices on or off at the same time can destabilise the electricity supply.

A number of fundamental **data protection** issues are raised by the increasing connectivity of devices in private households as a result of digitalisation together with the interventions that, as discussed in this paper, grid operators may need to make in order to stabilise the system. It will be vital to keep discussing these questions from both a legal and a social science perspective. Although these issues are not explored in this position paper because they are not directly connected to resilience, they are nonetheless extremely important.

The digitalisation of our everyday lives and the transformation of our energy supply mean that new measures are needed to prevent the huge damage that blackouts can cause to society. Certain aspects of digitalisation will need to be managed more actively, new actors must be obliged to contribute to resilience, and potential future developments or disruptions must be anticipated in good time by policymakers. This position paper sets out a range of measures and strategies that can help to make this happen. At this point in time, it is not possible to say how frequently and rapidly some of these measures will need to be adapted in the future. That is something that will need to be determined by the outcomes of a systematic monitoring and learning process.

References

AbLaV 2016

Verordnung zu abschaltbaren Lasten (Ordinance on Interruptible Load Agreements) of 16 August 2016 (Federal Law Gazette I p. 1984), most recently amended by Article 9 of the Act of 22 December 2016 (Federal Law Gazette I p. 3106).

acatech 2014

acatech – Deutsche Akademie der Technikwissenschaften (Ed.): *Resilien-Tech. Resilience-by-Design: Strategie für die technologischen Zukunftsthemen* (acatech POSITION), 2014.

acatech/Leopoldina/Akademienunion 2017

acatech – Deutsche Akademie der Technikwissenschaften, Nationale Akademie der Wissenschaften Leopoldina, Union der deutschen Akademien der Wissenschaften (Eds.): *Das Energiesystem resilient gestalten: Maßnahmen für eine gesicherte Versorgung* (Science-Based Policy Advice Series), 2017.

acatech/Leopoldina/Akademienunion 2020-1

acatech – Deutsche Akademie der Technikwissenschaften, Nationale Akademie der Wissenschaften Leopoldina, Union der deutschen Akademien der Wissenschaften (Eds.): *Centralized and decentralized components in the energy system. The right mix for ensuring a stable and sustainable supply* (Science-Based Policy Advice Series), 2020.

acatech/Leopoldina/Akademienunion 2020-2

acatech – Deutsche Akademie der Technikwissenschaften, Nationale Akademie der Wissenschaften Leopoldina, Union der deutschen Akademien der Wissenschaften (Eds.): *Grid Congestion as a Challenge for the Electricity System. Options for a Future Market Design* (Science-Based Policy Advice Series), 2020.

Agora 2016

Agora Energiewende: *Flex-Efficiency - Ein Konzept zur Integration von Effizienz und Flexibilität bei industriellen Verbrauchern*, 2016, URL: <https://www.agora-energiewende.de/veroeffentlichungen/flex-efficiency/> [retrieved: 15.10.2020]

Agora 2020

Agora Energiewende: *Klimaneutrale Industrie - Schlüsseltechnologien und Politikoptionen für Stahl, Chemie und Zement*, 2020. URL: https://www.agora-energiewende.de/fileadmin2/Projekte/2018/Dekarbonisierung_Industrie/164_A-EW_Klimaneutrale-Industrie_Studie_WEB.pdf [retrieved: 15.10.2020]

ARegV 2019

Anreizregulierungsverordnung (Incentive Regulation Ordinance) of 29 October 2007 (Federal Law Gazette I p. 2529), most recently amended by Article 3 of the Ordinance of 23 December 2019 (Federal Law Gazette I p. 2935).

Aven/Renn 2009

Aven, T./Renn, O.: "The role of quantitative risk assessments for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism." In: *Risk Analysis*, 29: 4, 2009, pp. 587–600.

Babazadeh et al. 2018

Babazadeh, D./Mayer, C./Lehnhoff, S.: "Cyber-Resilienz". In: *bulletin.ch*, 5, 2018, pp. 32–34.

Statistisches Landesamt Baden-Württemberg 2020

Statistisches Landesamt Baden-Württemberg: Gebäude und Wohnungen, 2020. URL: https://www.statistik-bw.de/Wohnen/Gebaeude-Wohnungen/BW-BT_einfamilienhaeuser.jsp [retrieved: 25.09.2020].

BDEW 2017

Bundesverband der Energie- und Wasserwirtschaft (BDEW): Standardlastprofil Strom, 2017. URL: <https://www.bdew.de/energie/standardlastprofil-strom/>. [retrieved: 25.09.2020].

Statistik Berlin Brandenburg 2020

Statistik Berlin Brandenburg: Basisdaten, 2020. URL: <https://www.statistik-berlin-brandenburg.de/BasisZeitreiheGrafik/Bas-Mikrozensus.asp?Ptyp=300&Sageb=12011&creg=BBB&anzwer=5>, [retrieved: 25.09.2020].

BSI-KritisV 2017

BSI-Kritisverordnung (BSI Regulation on the Determination of Critical Infrastructures) of 22 April 2016 (Federal Law Gazette I p. 958), amended by Article 1 of the Regulation of 21 June 2017 (Federal Law Gazette I p. 1903).

BSI 2020-1

Bundesamt für Sicherheit in der Informationstechnik (BSI): Glossar der Cyber-Sicherheit, C, 2020. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817276 [retrieved: 12.05.2020].

BSI 2020-2

Bundesamt für Sicherheit in der Informationstechnik (BSI): Glossar der Cyber-Sicherheit, I, 2020. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817288 [retrieved: 12.05.2020].

BSI/BMWI 2020

Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesministerium für Wirtschaft und Energie (BMWi): Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende, Roadmap für die Weiterentwicklung der technischen BSI-Standards in Form von Schutzprofilen und technischen Richtlinien, 2020. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/standardisierungsstrategie.pdf?jsessionid=1CC3BDDCADA723CE15B04AA0D8F4D66.1_cid503?__blob=publicationFile&v=3 [retrieved: 09.07.2020].

Büchner et al. 2014

Büchner, J./Katzfey, J./Flörcken, O./Moser, A./Schuster, H./Dierkes, S./van Leeuwen, T./Verheggen, L./Uslar, M./van Amelsvoort, M.: *Moderne Verteilernetze für Deutschland (Verteilernetzstudie)*, study commissioned by the Federal Ministry for Economic Affairs and Energy (BMWi), 2014.

European Commission 2019

European Commission: Communication on The European Green Deal, 2019. URL: https://ec.europa.eu/info/publications/communication-european-green-deal_de [retrieved: 03.04.2020].

Furusawa et al. 2019

Furusawa, K./Brunekreeft, G./Hattori, T.: *Constrained Connection for Distributed Generation by DSOs in European Countries* (Bremen Energy Working Papers No. 28), Jacobs University Bremen, 2019.

IRGC 2018

International Risk Governance Center (IRGC, Ed.): *Guidelines for the Governance of Systemic Risks*, Lausanne: International Risk Governance Center (IRGC) 2018.

Katwala 2019

Katwala, A.: Here's how GCHQ scours Huawei hardware for malicious code, 2019. URL: <https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk> [retrieved: 26.06.2020].

Kröger 2017

Kröger, W.: "Securing the Operation of Socially Critical Systems from an Engineering Perspective: New Challenges, Enhanced Tools and Novel Concepts". In: *European Journal for Security Research*, 2, 2017, pp. 39–55.

Kröger 2019

Kröger, W.: "Achieving Resilience of Large-Scale Engineered Infrastructure Systems". In: No-roozinejad Farsangi, E./Takewaki I./Yang T./Ashtaneh-Asl A./Gardoni P. (Eds.): *Resilient Structures and Infrastructure*, Singapore: Springer 2019, pp. 289–313.

Mayer/Brunekreeft 2021

Brunekreeft, G./Mayer, C. (Eds.): *Resilienz digitalisierter Energiesysteme. Blackout-Risiken verstehen, Stromversorgung sicher gestalten* (Energy Systems of the Future series), Munich, 2021.

Netztransparenz 2019

Netztransparenz: EEG-Anlagenstammdaten 2017, 2019. URL: <https://www.netztransparenz.de/EEG/Anlagenstammdaten>, [retrieved: 19.02.2019].

Petermann et al. 2011

Petermann, T./Bradke, H./Lüllman, A./Poetzsch M./Riehm, U.: *Was bei einem Blackout geschieht: Folgen eines langandauernden und großräumigen Stromausfalls*, Berlin: edition sigma 2011.

Piasceck et al. 2013

Piasceck S./Wenzel, L./Wolf, A.: *Regional Diversity in the Costs of Electricity Outages: Results for German Counties* (HWWI Research Paper 142), Hamburg Institute of International Economics (HWWI) 2013.

Plattform Industrie 4.0 2020

Plattform Industrie 4.0: Was ist Industrie 4.0?, 2020. URL: <https://www.plattform-i40.de/PI40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html>, [retrieved: 15.10.2020]

Regulation (EU) 2019/943

Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast).

Regulation (EU) 2019/941

Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC.

SmartQuart 2020

SmartQuart: Bredburg – Das elektrische Quartier, 2020. URL: <https://smartquart.energy/about/bedburg/> [retrieved: 25.09.2020].

Statistisches Amt für Hamburg und Schleswig-Holstein 2020

Statistisches Amt für Hamburg und Schleswig-Holstein: *Statistisches Jahrbuch 2019/2020, 2020*, Hamburg 2020. URL: <https://www.hamburg.de/contentblob/1005676/e93bee7f01624bcadfd70efe661d6e28/data/statistisches-jahrbuch-hamburg.pdf> [retrieved: 25.09.2020].

StromNEV 2019

Stromnetzentgeltverordnung (Electricity Network Charges Ordinance) of 25 July 2005 (Federal Law Gazette I p. 2225), most recently amended by Article 1 of the Ordinance of 23 December 2019 (Federal Law Gazette I p. 2935).

Thoma 2014

Thoma, K. (Ed.): *Resilien-Tech – “Resilience by Design”: a strategy for the technology issues of the future*. Acatech STUDY. Series editor: acatech – National Academy of Science and Engineering, Munich 2014.

Umweltbundesamt 2015

Umweltbundesamt (Ed.): *Potentiale regelbaren Lasten in einem Energieversorgungssystem mit wachsendem Anteil erneuerbarer Energien*, 2015.

Whitehead et al. 2017

Whitehead, D./Owens, K./Gammel, D./Smith, J.: “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies”. In: *70th Annual Conference for Protective Relay Engineers (CPRE)*, 2017, pp. 1–8.

The Academies' Project

Mit der Initiative „Energiesysteme der Zukunft“ geben acatech – Deutsche Akademie der Technikwissenschaften, die Nationale Akademie der Wissenschaften Leopoldina und die Union der deutschen Akademien der Wissenschaften Impulse für eine faktenbasierte Debatte über Herausforderungen und Chancen der Energiewende in Deutschland. In interdisziplinären Arbeitsgruppen erarbeiten rund 100 Expertinnen und Experten Handlungsoptionen für den Weg zu einer umweltverträglichen, sicheren und bezahlbaren und Energieversorgung.

The working group on the “Resilience of digitalised energy systems”

Digitalisation has a crucial role in the energy transition due to the high level of automation required to control an energy system with large numbers of small electricity generating and storage units, volatile electricity feed-in and increasing sector coupling. At the same time, digitalisation brings new risks such as cyberattacks or ICT bugs. This interdisciplinary working group investigated how blackouts can be prevented in the digitalised future energy system.

The working group's findings are presented in two publications:

1. The **analysis** “*Resilienz digitalisierter Energiesysteme. Blackout-Risiken verstehen, Stromversorgung sicher gestalten*” (*Resilience of digitalised energy systems. Understanding blackout risks, ensuring a secure electricity supply*) provides a comprehensive overview of current scientific knowledge about the risks of a digitalised energy system and the application of the resilience concept to the electricity supply. It also discusses in detail the working group's policy recommendations for addressing the risks of a digitalised energy system and the application of the resilience concept to the electricity supply.
2. The **position paper** “*The resilience of digitalised energy systems. Options for reducing blackout risks*” provides a concise overview of the findings.

Members of the working group

Dr. Christoph Mayer (Lead)	OFFIS, Oldenburg
Prof. Dr. Gert Brunekreeft (Lead)	Jacobs University Bremen
Dr. Marius Buchmann	Jacobs University Bremen
Mathias Dalheimer	Fraunhofer ITWM
Dr. Volker Distelrath	Siemens AG
Prof. Dr. Bernd Hirschl	IÖW/BTU Cottbus
Prof. Dr. Jochen Kreusel	Hitachi ABB Power Grids
Prof. Dr. Wolfgang Kröger	ETH Zürich
Prof. Dr. Sebastian Lehnhoff	OFFIS, Oldenburg
Dr. Till Luhmann	BTC AG
Prof. Dr. Jannika Mattes	University Oldenburg
Prof. Dr. Ellen Matthies	University Magdeburg
Dr. Philipp Werdelmann	Westnetz GmbH
Prof. Dr.-Ing. Christof Wittwer	Fraunhofer ISE

Scientific coordinators

Dr. Achim Eberspächer	acatech
Dr. Berit Erlach	acatech
Katharina Bähr	acatech
Dr. Marita Blank-Babazadeh	OFFIS, Oldenburg
Sanja Stark	OFFIS, Oldenburg

Reviewers

Prof. Dr. Frank Eggert	TU Braunschweig
Prof. Dr. Michael Fehling	Bucerius Law School
Prof. Dr. Georg Götz	Justus-Liebig-University Gießen
Prof. Dr. Matthias Jarke	RWTH Aachen
Prof. Dr. Johanna Myrzik	University Bremen

Participating institutions

acatech – National Academy of Science and Engineering (lead institution)

German National Academy of Sciences Leopoldina

Union of the German Academies of Sciences and Humanities

Board of Directors

The Board of Directors manages and represents the project

Prof. Dr. Dirk Uwe Sauer (Chair)	RWTH Aachen
Prof. Dr. Christoph M. Schmidt (Deputy)	RWI – Leibniz Institute for Economic Research
Prof. Dr. Hans-Martin Henning	Fraunhofer Institute for Solar Energy Systems ISE
Prof. Dr. Karen Pittel	ifo Institute
Prof. Dr. Jürgen Renn	Max Planck Institute for the History of Science
Prof. Dr. Indra Spiecker genannt Döhmann	Goethe University Frankfurt

Board of Trustees

The Board of Trustees determines the strategic orientation of the project activities.

Prof. Dr. Reinhard F. Hüttl (Chair)	acatech Vice-President (Office currently dormant)
Prof. Dr.-Ing. Dieter Spath	President acatech (former until 19.03.2021)
Prof. (ETHZ) Dr. Gerald Haug	President Leopoldina
Prof. Dr. Dr. Hanns Hatt	President of the Union of the German Academies of Sciences and Humanities
Prof. Dr. Bärbel Friedrich	Former member of Leopoldina Presidium
Prof. Dr.-Ing. Edwin J. Kreuzer	President of the Academy of Sciences and Humanities in Hamburg
Prof. Dr. Andreas Löschel	University of Münster, chair of the committee of experts for the “energy of the future” monitoring process
Prof. Dr. Robert Schlögl	Director of the Fritz Haber Institute of the Max Planck Society and Max Planck Institute for Chemical Energy Conversion
Oda Keppler (Gast)	Head of Directorate, Federal Ministry of Education and Research
Dr. Rodoula Tryfonidou (Gast)	Head of energy research unit, Federal Ministry for Economic Affairs and Energy

Project coordination

Dr. Ulrich Glotzbach	Head of Coordination Office “Energy Systems of the Future”, acatech
----------------------	--

Basic data

Project duration

03/2016 to 02/2022

Funding

The project is funded by the Federal Ministry of Education and Research (funding code 03EDZ2016).

The Board of Trustees of the Academies' Project adopted the position paper on 06.11.2020.

The Academies would like to thank all the authors and reviewers for their contributions. The Academies bear sole responsibility for the content of the position paper.

SPONSORED BY THE



Federal Ministry
of Education
and Research

**German National Academy
of Sciences Leopoldina**

Jägerberg 1
06108 Halle (Saale)
phone: 0345 47239-867
Fax: 0345 47239-839
Email: leopoldina@leopoldina.org

Berlin Office:
Reinhardtstraße 14
10117 Berlin

**acatech – National Academy
of Science and Engineering**

Karolinenplatz 4
80333 München
phone: 089 520309-0
Fax: 089 520309-9
Email: info@acatech.de

Berlin Office:
Pariser Platz 4a
10117 Berlin

**Union of the German Academies
of Sciences and Humanities**

Geschwister-Scholl-Straße 2
55131 Mainz
phone: 06131 218528-10
Fax: 06131 218528-11
Email: info@akademienunion.de

Berlin Office:
Jägerstraße 22/23
10117 Berlin

The German National Academy of Sciences Leopoldina, acatech – National Academy of Science and Engineering, and the Union of the German Academies of Sciences and Humanities provide policymakers and society with independent, science-based advice on issues of crucial importance for our future. The Academies' members and other experts are outstanding researchers from Germany and abroad. Working in interdisciplinary working groups, they draft statements that are published in the series of papers *Schriftenreihe zur wissenschaftsbasierten Politikberatung* (Series on Science-Based Policy Advice) after being externally reviewed and subsequently approved by the Standing Committee of the German National Academy of Sciences Leopoldina.

Series on Science-based Policy Advice

ISBN: 978-3-8047-4225-3