Leopoldina
Nationale Akademie
der Wissenschaften

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

UNION
DER DEUTSCHEN AKADEMIEN
DER WISSENSCHAFTEN

April 2021
Summary of the Position Paper

The resilience of digitalised energy systems

Options for reducing blackout risks

German National Academy of Sciences Leopoldina
acatech – National Academy of Science and Engineering
Union of the German Academies of Sciences and Humanities

Over the next two decades, the energy transition and the growth of digitali-sation 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).

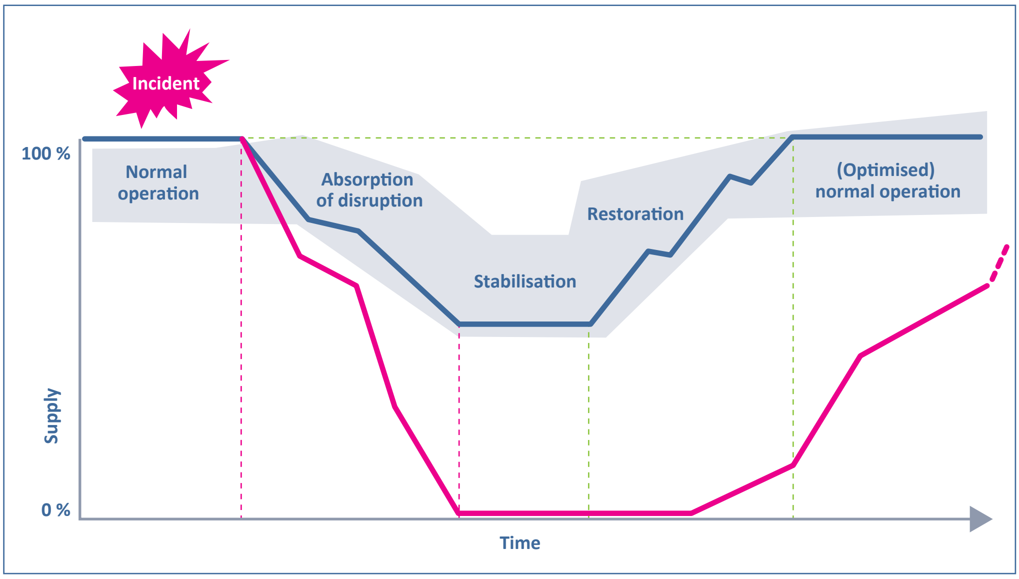

Figure 1: Restoring system functionality: responding appropriately to an incident (absorption of disruption), reverting to critical functions and stabilising the system (stabilisation), followed by a controlled return to normal system operation (restoration).[3]

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 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 blackouts. 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)

All the relevant actors will need to do their bit to strengthen resilience if we are to maintain the highly reliable electricity supply that we are accustomed to. Policymakers can create the necessary framework by establishing an appropriate resilience strategy.

The Academies' Project "Energy Systems of the Future"

The Position Paper *The resilience of digitalised energy systems. Options for reducing blackout risks* evolved within the framework of the Academies' Project "Energy Systems of the Future". In interdisciplinary working groups, about 100 experts are working on different courses of action for the pathway to an environmentally sustainable, safe and affordable energy supply.

Participants in the working group "Resilience of digitalised energy systems"

Members: Dr. Christoph Mayer (Lead, OFFIS), Prof. Dr. Gert Brunekreeft (Lead, Jacobs University Bremen), Dr. Marius Buchmann (Jacobs University), Mathias Dalheimer Fraunhofer ITWM, Dr. Volker Distelrath (Siemens AG), Prof. Dr. Bernd Hirschl (IÖW/ BTU), Prof. Dr. Jochen Kreusel (Hitachi ABB Power Grids), Prof. Dr. Wolfgang Kröger (ETH Zürich), Prof. Dr. Sebastian Lehnhoff (OFFIS), 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), Sanja Stark (OFFIS)

Contact:

Dr. Ulrich Glotzbach
Head of Project Office "Energy Systems of the Future"
Pariser Platz 4a, 10117 Berlin, Germany
phone: +49 30 2 06 79 57 - 0 I e-mail: glotzbach@acatech.de
web: energiesysteme-zukunft.de/en

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.

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