Leopoldina
Nationale Akademie
der Wissenschaften

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

UNION
DER DEUTSCHEN AKADEMIEN
DER WISSENSCHAFTEN

August 2023
Discussion Paper

Are Blackouts in Germany Likely?

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

Discussion Paper

Germany currently has one of the securest energy supplies worldwide. Larger power cuts or blackouts are unlikely. If the changing energy system is to remain as secure in the future as it is today, forward-looking measures must be taken now. In this respect, experts place emphasis on the following points:

- Very few power outages are blackouts. It is important to make this distinction in order to make realistic assessments of events and their consequences.
- There is currently no need to fear a blackout due to energy deficits, since there are strong and sophisticated safeguards.
- These mechanisms may mean temporary interruptions to energy supplies, but usually only affect large-scale industrial consumers and hence do not entail the catastrophic consequences for society that are occasionally feared.
- With the advancement of the energy transition, the energy supply is becoming decentralized and increasingly digitalized. This offers opportunities for energy supply security.
- New risks can also arise, however. It is necessary to address them now for future supply security.

Inhalt

1 Blackouts – a Real Danger?

Germany has one of the securest electricity systems worldwide. Even minor power failures are unusual in daily life. In 2021, the average downtime was a mere 12 minutes and 45 seconds. The quality of energy supply is also high in the European grid as a whole. There are nevertheless presently fears of a blackout, in part fed by the media and politicians. These worries are particularly due to the gas shortage caused by Russia's war of aggression against Ukraine and the currently high downtime rates of France's nuclear power stations. The great interest in the subject of blackouts has manifested itself in, for instance, a debate in the Bundestag, media reports and talk shows.

Firstly, it is important to define the dramatic term "blackout". It evokes the sort of catastrophic scenario the writer Marc Elsberg describes in his novel of the same title in 2013: due to a European-wide blackout lasting several weeks, public order largely collapses. Against the background of the general uncertainty triggered by the war in Europe and the energy crisis, for some people the chances of such a scenario seem much less remote than was previously the case.

Yet an assessment by experts shows:

- Not every power outage is a blackout. Establishing this – and using precise language – is essential, since not every disruption to the energy supply involves the harsh consequences attributed to blackouts. And even if it did come to a blackout, all of Europe would not automatically be "crippled". For a blackout to escalate into the catastrophic scenario described by Marc Elsberg, a number of unfortunate circumstances and mistakes would have to coincide. Experts consider the risk of such a catastrophic blackout to be very low, even with respect to shorter blackouts limited to the regional level – even given the more acute conditions of the current energy crisis. A catastrophic blackout, we can say today, is extremely unlikely.

- Germany is not unprepared for potential blackout events either. There are concrete contingency plans for maintaining basic supplies to the population in the event of a blackout. Critical infrastructure such as hospitals have emergency power supplies. The recommendations of the disaster management agency to have drinking water, a torch, batteries and battery-powered radio at home in case of a longer power cut existed before the current crisis – they just received less discussion and attention.

- The restructuring of the energy system is not only important for climate protection but also opens up an opportunity to enhance supply security: the development of renewable energy sources reduces dependence on fossil fuel imports and with them vulnerable supply chains. The decentralization of the energy supply spreads external risks of outages over a large number of facilities, thereby rendering supply less physically vulnerable and reducing the potential consequences of attacks or acts of sabotage targeting at large power stations or pipelines, for example. Selective use of digitalization also enables the collection of precise information on the state of the energy system and quicker and better responses in critical situations.

On the basis of this initial appraisal, this paper first provides a science-based assessment of the risk of a blackout in the current situation. It explains how a blackout differs from a more minor power cut and a brownout, what causes it and what the consequences are. The paper then illustrates which blackout risk factors will become more influential in the future and shows policy options aimed at maintaining and potentially even increasing supply security through decentralization and digitalization

2 What is a Blackout and What Are Its Consequences?

A blackout is a large power outage. There is no uniform definition stating the spatial scale and duration required before one can speak of a blackout, but the following three characteristics must all be fulfilled at the same time:

- The power outage is of such a scale that the area affected can no longer be adequately supplied by unaffected neighbouring areas.
- The power outage lasts long enough to have severe societal and economic consequences.
- The power outage is unplanned. The grid operators responsible for the secure power supply lose control of events in the power grid for some time at least.

To date, there has never been such a blackout in post-war Germany. However, should one occur, depending on its duration and scale it would entail severe consequences for society: after only a few hours, death and injury rates can rise because rescue services or the police cannot be contacted due to run-down mobile phones. There is a limit to the food that can be prepared for infants. Considerable economic losses (e.g. due to production downtime) can also arise after just a few hours. Hospitals have emergency power supplies with batteries and/or diesel generators that can bridge a power cut for a limited period. After more than 24 hours, however, most hospitals would only be partially operational and patients would have to be transferred to hospitals that can maintain their power supply for longer.

Food supplies would also be appreciably limited after more than 24 hours. An outage lasting several days would result in an increase in deaths in care homes – partly because care workers can no longer get to work if public transport infrastructure and petrol stations are no longer operational, medications are in short supply and residents have hypothermia. In agricultural enterprises, the mass death of livestock would set in. The economic damage would also be enormous: it is estimated that a nationwide power outage in Germany would result in the loss of 0.6–1.3 billion euros per hour. Even if the power supply were up and running again after a few days, the severe consequences for society could also remain long after the outage itself, since it would not be possible to immediately undo the damage caused by the blackout.

However: the consequences outlined here do not occur in the case of **short and small-scale power cuts**, and hence care should be taken to make this distinction. Power cuts lasting several hours limited to a small area, such as a few streets, take place in Germany almost every day. Yet they rarely affect the individual and usually go unnoticed by those parts of the population that are not affected. Often, the cause is damage to an electricity cable during construction work. While even such smaller power cuts are a source of inconvenience and, to an extent, economic losses, their consequences are manageable and not comparable to those of a blackout. Neighbouring areas can supply goods and services such as healthcare without great difficulties.

Another phenomenon to be distinguished from a blackout is the controlled disconnection of some consumers from the supply. Known as a **controlled brownout**, this can be necessary if demand cannot be met at a given point in time, for instance because a large number of power stations cannot be supplied with fuel or are undergoing maintenance work, as is currently the situation with the nuclear power stations in France. In such a case, which has yet to arise in Germany, the grid operator has to disconnect consumers from the grid in order to ensure the stability of the power supply. Ideally, the operator first removes individual large-scale users from the grid on a regional basis and for a limited time only. A large number of industrial enterprises have such potential disconnections written into their electricity supply contracts. If this is not sufficient, several areas are disconnected from the grid by a **rolling shutdown** – that is, an alternating switch-off of predetermined limited duration. Depending on the cause, the consumers affected can receive advance warning and thus prepare. In such cases, the grid operator retains control of what happens with the grid throughout and can also restart supply without any problems. In such cases, there is no risk of shortages of important goods or services.

3 What Are the Causes of Blackouts and Other Power Outages?

The simultaneous technical failure of a large number of power supply facilities (wires, transformers, substations, power stations), natural events in the form of extreme weather, high numbers of staff ill due to a pandemic, human error and malevolent activities such as sabotage, terrorism or war can lead to larger power outages or, in the worst-case scenario, a blackout. For instance, the European grid suffered severe power cuts in 2003 and 2006. In 2003, as many as 95 per cent of Italians were without electricity for several hours. In both cases, human error played a significant role. In Germany in 2005, electricity pylons in Münster were unable to bear the weight of snow on the wires – some people in the region spent several days without electricity. In Ukraine, a cyber attack in 2015 caused a power outage lasting several hours affecting several hundred thousand people. But in all these cases, the brief duration (e.g. a few hours in Europe in 2006 and Ukraine in 2015) or the limited region (Münster in 2005) meant that the extreme consequences described above did not arise.

In the case of a power cut, the grid operators attempt to prevent the destabilization of further parts of the grid and to restore supply in the affected area as quickly as possible. The necessary measures are set out in the **grid restoration maps** and are trained in regular **exercises** simulating different disruption scenarios. In the case of the aforementioned causes (with the exception of war), an outage would only escalate into a superregional blackout lasting several days if other unfortunate circumstances or errors were to occur and prevent stabilization of the rest of the grid and grid restoration.

A potential cause of a power outage lasting days or even weeks throughout large parts of Europe would be a strong solar storm. Simulations show that solar storms could cause damage to large components such as transformers and thereby cause a blackout. The potential effects of such extreme but very unlikely events occupy, among other bodies, the European transmission system operators and the disaster management agencies.

4 Is a Blackout to Be Feared Due to the Energy Crisis?

What is the current situation? Presently, there is little risk of a blackout in Germany due to an **energy shortage**. Fears expressed in the public discussion are unfounded. Even in the worst-case scenario – that is, if the electricity demand were indeed to exceed the capacity of domestic power stations and the deficit couldn't be covered by imports from neighbouring countries – this would not result in a blackout. The grid operators, who would usually be aware of such a shortage at least 24 hours in advance due to predictions and the European coordination processes, would then switch off a few **large-scale industrial consumers** as part of a pre-conceived plan. If this were not sufficient, they would avoid blackouts via rolling shutdowns of grid regions. But even such planned shutdowns are highly undesirable and should only be used as a stopgap. The aim of energy policy must rather be that households, trades and industry can be supplied with electricity in the future at least as well and as securely as they are today.

5 What Are the Risks of Blackouts in the Future?

In the course of the energy transition, the electricity supply will and must change quickly – in order to decarbonize energy supplies, but also in order to reduce dependence on energy imports such as natural gas: a large number of wind energy and photovoltaic plants will then provide the majority of our energy and replace large fossil fuel and nuclear power stations. That this will not necessarily lead to a reduction in supply quality is demonstrated by the last 30 years: in the course of the expansion of renewable energy sources to 45 per cent of net electricity production, supply quality has not declined.

While today the balance between electricity feed-in, transmission losses in the grid and electricity consumption in the European grid is achieved by flexibly adapting electricity production to the desired levels of consumption (**load sequence**), in future electric energy extraction must be adapted to a much greater extent to the fluctuating feed-in of renewable energies (**production sequence**). To this end, it is necessary to create financial incentives for technology that renders consumption more flexible (in particular load shifting in the case of industrial consumers but also e.g. managed electric vehicle charging). In addition to greater use of battery storage systems, green hydrogen or synthetic methane (SNG) produced from it must be hold available for energy production in gas power stations in order to enable climate-neutral bridging of a *dunkelflaute* – that is, several weeks without feed-in from wind and photovoltaic plants – when natural gas may not longer be burnt.

In contrast to today, in the future a large number of small, decentralized plants will combine to ensure a reliable energy supply. They will be joined by a **plethora of actors**: today, it is mainly the producers of large service quantities (operators of large power stations or a large number of renewable energy plants), grid operators and operators of large energy exchanges that affect an energy system's stability. In future, other actors will play a role too, for instance operators of charging infrastructure, prosumers, enterprises focusing on bundling and marketing flexibilities as services (known as aggregators), or software platform operators (vehicle manufacturers, smart home service providers). Coordinating the many plants and operators is only possible using automation and digitalization. Additionally, a larger number of small electricity producers and storage facilities will be available to support the electric energy system as a "swarm" (see 6.1 Utilizing Decentrality).

It is quite clear: this **decentralization and increasing digitalization** of the energy system also influence the risk of a blackout. Some risks are reduced by the restructuring of the energy system. For instance, the development of renewable energies reduces dependence on fossil fuel imports and makes an essential contribution to increasing supply security. And the decentralized structure of the future energy system

reduces dependence on large plants, which can be targets for a physical attack or acts of sabotage. Digitalization helps optimize the interplay of different plants and operators. It allows data on the state of the energy system to be collected, assessed and shared with other relevant actors, thereby facilitating coordinated, fast and effective action in the case of disruption.

However, there are also risks that take on greater relevance in the future system. Today's laws and regulations pertaining to electricity supply security do not address these changes adequately. Potential new blackout risk factors, or risk factors that are increased under these conditions, are in particular the following:

1. In the future, small, actively controllable generation and storage facilities and electrical equipment will become systemically relevant for electricity supply: if they are simultaneously managed using ICT (information and communications technologies) and turned on or off, for instance, this can have significant influence on voltage or frequency, the two most important values for the stability of the electricity grid. This can help stabilize the grid, but in the case of hostile actions or errors, it can also lead to destabilization. The same holds for devices that consume electricity, from vehicles to heat pumps to refrigerators, which are increasingly controllable via the internet.

2. Malfunctions in ICT systems can lead to massive threats. This applies not only to events such as a cyber attack on the control centres in Ukraine in 2015. In the future, much more complex attacks could be planned. Potential targets might be manufacturers of inverters for renewable energy (RE) plants in order to gain access to the RE plants via the inverters connected to the internet. Attacks on operators of IT platforms on which a sufficiently large electric capacity can be controlled via communications technology or direct attacks on a very large number of decentralized plants are also conceivable. In this way, it would be possible to coordinate attacks on power supplies very different to familiar disruptions. A worldwide "market" for software and information that can serve such attacks further increases this risk. States also use this market ("state Trojans"). An attack on ICT systems causing a blackout would require considerable financial resources and personnel on a level probably only available to state-sponsored actors.

3. The increased complexity of the future energy system will make it more difficult to analyse what is going on in the grid. This also has an impact on grid operation. In future, plants and equipment will be increasingly connected digitally and controlled by algorithms, often via use of artificial intelligence (AI). This could create behavioural patterns that are hard to predict, such as synchronized switching on and off of equipment (known as "emergent behaviour").

4. New uncertainties make it difficult to optimally plan and implement a future-proof electric energy supply system: technological development, processes, guidelines, standards and regulations are always created or adapted on the basis of explicit and implicit assumptions about the future – and the future of European energy systems also contains uncertainties. It is also conceivable that there will be (geo)political and societal developments that increase the danger of criminal or terrorist attacks. Hybrid wars with cyber attacks on the energy supply system are a possibility. Some of the uncertainties could prove problematic, in particular if the further development of the energy system creates path dependence – that is, if decisions, once made, create constraints that make it difficult or impossible to switch to another option. This could render later adaptation to surprising developments difficult, for instance if complicated retrofitting processes are necessary.

In order to make the future climate-friendly, decentralized and digitalized energy system as resilient and supply-secure as possible, it is necessary to **actively address the risk factors** outlined above rather than waiting until such a case presents itself. Nevertheless, there will still be the residual risk of a large-scale blackout lasting several days, even in a resilient energy system. Extensive security measures must thus be put in place beyond the energy system too, including in the field of disaster management and disaster prevention. This is the task of the Federal Office of Civil Protection and Disaster Assistance, for instance.

6 What Is to Be Done?

Today's electricity system is so secure and reliable because extensive risk analyses, **practical knowledge** and lessons from the past have been used to eliminate weak spots. The most important component here is **redundancy**: power stations operate with considerable overcapacities, and the transmission systems are devised according to the "N+1" principle – that is, there is always one more connection than is required by a fully functioning system. Further, equipment is scaled in such a way that normal service operates significantly under the permitted maximum. Another important component is **reserve capacities**, some of which are organized on the European and some on the national level. In this way, if two of the larger operating blocks of power stations have outages at the same time, it is possible to compensate without consumers noticing. Some of this reserve capacity is deliberately supplied without digital communication too. Additionally, the national distribution networks are largely located underground, which is expensive but leads to much higher levels of **robustness** to extreme weather than can be seen in the USA, for example.

The approaches used hitherto must now be supplemented, however, in order to deal with future risks of blackouts. The concept of **resilience** has proved itself in such situations: the aim of this concept is to suffer the least possible damage while getting through disruptions which cannot be defended against without incurring losses and which the system's design cannot take into consideration. A resilient power supply is able to intercept disruption unharmed or at least return to normal operations in little time and at acceptable cost – even if the event is surprising or novel. Further, a resilient energy system should be able to respond to expected developments sufficiently effectively and with a favourable cost–benefit ratio. Digitalization in particular can be of assistance here, since the short innovation cycles in the digital economy allow great flexibility.

Besides digital communication, the power system possesses the physical reference variables of voltage and frequency. Production and consumption facilities react in part automatically to deviations in setpoints, thereby contributing to the stability of the power supply. Economically or technologically optimal operation cannot be achieved by these mechanism alone, however; rather, this requires the interplay of these physical regulatory mechanisms and digitally controlled processes.

7 Fields of Action

The aforementioned risk factors play a minor role today, but in the future they will increase significantly. Hence it is of the essence to address potential risks and make provision for them by taking effective measures now. Activities in the following **four fields of action** can contribute to this:

7.1 Utilizing Decentrality

A decentralized digitalized energy supply offers new opportunities to make the energy system resilient. This is a chance that must be taken. Decentralized plants (wind energy, photovoltaics, battery storage systems, etc.) can help prevent or minimize the potential for disruptions to have severe consequences. In the case of a larger power outage, they can switch to emergency operation and secure regional supply within a grid area in what is known as **"isolated operation"** – irrespective of the state of the European grid and usually without large industrial consumers. For instance, large sections of critical infrastructure such as hospitals or emergency services could be supplied as a priority until the general power supply is restored.

This **system-serving deployment of decentralized plants** requires research and development as well as new legal regulations, technical processes and standards. It will be essential that there are no limits to the plethora of technical operations for decentralized plants if we are to be able to respond flexibly to unknown challenges. One way to enable this is if the decentralized plants' software can be adapted using **automatic updates**. In this way, learnings gained from external events or via the software itself can also be fed into the plants retrospectively. If, on the other hand, control is partly implemented in hardware or electrotechnical components, this can mean that later, a large number of decentral plants require retrofitting at their respective sites. This is not only much more expensive than software updates but can also take several years.

Artificial intelligence (AI) can tap further potential for **system stabilization**. Indeed, defence against some novel attacks on power supplies is probably only possible if AI is integrated into the decentralized plants. All this particularly requires the **digitalization of the distribution networks**, since for the most part renewable energy generation is connected to them. Additionally, in the future distribution networks will require large-scale **Demand Side Management** in order to compensate for fluctuations in power generation due to the weather, the time of the day or the season. On the local level, the supply system should be able to cope without uniform central management and should remain operational via self-organization and communication from network node to network node, similar to the internet. Such organization would make sense for instance if the control centre of the responsible grid operator were no longer functional due to a cyber attack.

In the future too, grid operators must take responsibility for the security of the electricity system. To this end, they must have the opportunity to use the potential of the decentralized plants connected via communication technology. This requires supplementary training for operating personnel, who in some circumstances will have to learn how to **deal with completely new and surprising disruptions**, among other things. Not least, regulations must be adapted to secure the financing of these measures.

7.2 Enhancing supply security with secure digital technologies

While political will – not least to retain a secure electricity supply system – and market forces are driving the necessary digitalization of the power supply, it is now necessary to respond to the risks associated with it. On both the European and the national level, there are already extensive measures to increase IT security – some of them also referred to as **"cyber resilience"**. They should be tested for their efficiency and effectiveness with respect to the resilience of the energy system and supplemented by further measures if they do not cover certain risks. A good technical basis would be the planned smart meter infrastructure.

Laws should also apply to actors that are not involved in energy supply per se but could have a large influence on electricity supply security – for instance manufacturers of products with digital components, for which EU regulations are already in preparation. For platform operators, manufacturers of e-bikes or inverters (for instance) and smart home system providers there have yet to be any comprehensive plans for lawmaking, however. On the other hand, there are already corresponding technical standards for intelligent (bi)directional charging.

Above all, we are nowhere near knowing all the dependencies between power supply and developments beyond power supply. These gaps in our knowledge require filling to ultimately limit the risks of blackouts via laws and regulations.

But there are also threats emanating from the state itself: states and their security services have a vested interest in gaps remaining in IT security, assuming that criminal activities can thus be monitored or proven more effectively. Cyber attack tools are also developed ("state Trojans"). If a state decides to use these highly controversial measures to reduce the IT security of many systems and thereby increase the risk of a blackout, an independent authority (especially independent of institutions involved in police or intelligence agency work) should transparently evaluate the benefits of crime fighting versus the risks to European energy supply.

It probably won't be possible to close every security gap in the digitalized energy system. Hence the overriding need is for mechanisms and guidelines in order to maintain the power supply even with corrupted ("hacked") ICT systems.

7.3 Involving the Public

The current energy crisis is triggering fears. For this very reason, the **public discussion** on existing or non-existent risks has to be based on facts. For instance, the term "blackout" is sometimes used imprecisely in the media and in politics and can frighten people – or is even intended to. In order to combat this, **information** is required, including regarding the distinction between planned rolling shutdowns, smaller local power cuts and a large blackout. This information should be tailored to the needs of the target groups, and citizens should receive clarity regarding the respective potential causes.

It should also be made clear that measures taken by private consumers worried about insufficient energy supply for heating could prove problematic: if a very large number of households in a small area use electric fan heaters at the same time, this can trip safety fuses in the lower voltage range and thus lead to a local power cut. Hence it is necessary to check, for instance via surveys, whether the appeals by unions, consumer protection agencies and politics to use such heaters as little as possible have been heeded by consumers.

Yet it is also important to involve the public irrespective of the current situation. In the future energy system, private actors will play a much more active role. As “prosumers”, they can actively manage their own consumption and in some cases their own renewable energy feed-in to the grid, thereby contributing to greater resilience. Here it is necessary to negotiate on the societal level the extent to which grid operators may for instance draw on prosumer facilities to stabilize the grid and which data should be collected in households in order to better predict consumption. Rules and incentives should be developed in transparent procedures and citizens should have the opportunity for involvement.

7.4 Institutionalizing Resilience Strategy with Monitoring

If these and other measures are integrated into a national resilience strategy for energy supply, **institutionalized, independent monitoring** should be established in order to regularly evaluate whether the strategy pursued proves effective and efficient and remains appropriate, and whether undesired path dependencies or side effects have arisen during implementation. On the basis of the results of the evaluation, the political decision-making bodies can then discuss and decide to what extent measures should be extended, added or abolished. A necessary prerequisite here is a regulatory framework – with as much coordination on the European level as possible – that enables resilience to be quantified: in the future, it will not suffice to examine past experiences such as the frequency of power cuts and their causes in order to be able to assess the risk of future blackouts – particularly in the case of new and unprecedented disruptions such as severe cyber incidents.

8 Conclusion

Although it is extremely unlikely that the current energy crisis will lead to large-scale power cuts, the risk of blackouts does exist. However, this risk was there to a similar degree before the crisis; it just received less public attention and less communication by politics and the media. If the power supply is to remain at the high levels we have become used to in the future, we must nevertheless keep a watchful eye on the development of different risk factors. For some of the risk factors are even increasing year by year and new potential causes are also emerging. In particular, attention must be paid to the entanglement of decentralization via the energy transition and digitalization as a further development in the energy system. Done properly, an actively devised digitalization and decentralized renewable energies will even increase the system’s resilience – for instance via the opportunity to create isolated networks – thereby reducing the danger of blackouts. It is to be hoped that the current awareness of the topic will move politics to rapidly implement effective measures.

Sources

More on the Subject

This discussion paper is essentially based on the results of the position paper:

acatech/Leopoldina/Akademienunion (Eds.): The resilience of digitalised energy systems. Options for reducing blackout risks (Series on Science-based Policy Advice), 2021. URL: https://energiesysteme-zukunft.de/en/publikationen/stellungnahme/the-resilience-of-digitalised-energy-systems.

1 Blackouts – a Real Danger?

"There are nevertheless presently fears of a blackout, in part fed by the media and politicians. The great interest in the subject of blackouts has manifested itself in, for instance, a debate in the Bundestag, media reports and talk shows."

Bundestag debate on blackouts, 28 September 2022:

URL: https://www.bundestag.de/dokumente/textarchiv/2022/kw39-de-aktuelle-stunde-blackout-912734

The subject of blackouts in talk shows, e.g. 23 September on Markus Lanz:

https://www.rnd.de/politik/markus-lanz-im-zdf-bauingenieurin-warnt-vor-blackouts-3QLJLVWY5BCWJCFHYCFVVMB4EU.html

... *and 29 November on Sandra Maischberger:*

*https://www.*ardmediathek*.de/video/maischberger/der-chef-der-bundesnetzagentur-klaus-mueller-ueber-die-wahrscheinlichkeit-von-blackouts/das-erste/Y3JpZDovL2Rhc2Vyc3RlLmRlL21lbnNjaGVuIGJlaSBtYWlzY2hiZXJnZXIvNWJiYmUxOTAtYjVhZi00MDkxLTgzMmItZDliNjgzZjBlOTU1*

"Germany has one of the securest electricity systems worldwide. Even minor power failures are unusual in daily life."

Bundesnetzagentur: Kennzahlen der Versorgungsunterbrechungen Strom, 2022.
URL: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Versorgungsunterbrechungen/Auswertung_Strom/start.html// [retrieved 08.12.2022].

CEER Benchmarking Report 6.1 on the Continuity of Electricity and Gas Supply Data update 2015/2016
URL: https://www.ceer.eu/documents/104400/-/-/963153e6-2f42-78eb-22a4-06f1552dd34c

By way of comparison: in the USA, the average supply interruptions amount to several hours each year:
Eia U.S. Energy Information Administration: U.S. customers experienced an average of nearly six hours of power interruptions in 2018, 2020. URL: https://www.eia.gov/todayinenergy/detail.php?id=43915 [retrieved 15.12.2022].

"In 2021, the average downtime was a mere 12 minutes and 45 seconds."

Annual average power interruption is measured using $SAIDI_{EnWG}$ (System Average Interruption Duration Index), which indicates annual power interruption per connected end consumer in a calendar year.
URL: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Versorgungsunterbrechungen/Auswertung_Strom/start.html// [retrieved 08.12.2022].

2 What is a Blackout and What Are Its Consequences?

Examples of definitions of blackouts:

One of the largest regional energy suppliers, EWE, describes a blackout as "a sudden and very extensive power cut affecting a very large number of people for a long period of time."
EWE*: Versorgungslage in schweren Zeiten. Wir ordnen die Geschehnisse aus der Energiewelt ein*, 2022. ULR: https://www.ewe.com/de/media-center/neuigkeiten/stuermische-zeiten-in-der-energiewelt [retrieved 08.12.2022].

The Federal Office for Information Security assumes that outages affecting over 500,000 people "cannot be adequately compensated for with current emergency capacities". This figure should be seen as the minimum threshold and thus also forms the basis of the ESYS statement.

Federal Office for Information Security (BSI): *FAQ on the BSI Kritis Regulation.* ULR: https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-BSI-KritisV/faq_kritisv_node.html [retrieved 08.12.2022].

The Bundesnetzagentur proposes a stricter definition: "A blackout is an uncontrolled and unpredicted outage in which at least larger parts of the European power grid are down."

Bundesnetzagentur: *Stromnetz, 2022*. ULR: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Stromnetz/start.html [retrieved 08.12.2022].

The European Network of Transmission System Operators for Electricity uses the following definition: "Blackout State means the System State where the operation of part or all of the Transmission System is terminated.

European Network of Transmission System Operators for Electricity (entsoe): *Policy 5: Emergency Operations*, 2015. ULR: https://eepublicdownloads.entsoe.eu/clean-documents/Publications/SOC/Continental_Europe/oh/20150916_Policy_5_Approved_by_ENTSO-E_RG_CE_Plenary.pdf [retrieved 08.12.2022].

Consequences of a blackout

Petermann, T./Bradke, H./Lüllman, A./Poetzsch, M./ Riehm, U.: Was bei einem Blackout geschieht: Folgen eines langandauernden und großräumigen Stromausfalls (Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag – 33), Berlin: edition sigma 2011.

"A nationwide power outage in Germany would result in the loss of 0.6–1.3 billion euros per hour."

Petermann, T./Bradke, H./Lüllman, A./Poetzsch, M./ Riehm, U.: Was bei einem Blackout geschieht: Folgen eines langandauernden und großräumigen Stromausfalls (Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag – 33), Berlin: edition sigma 2011, p. 67.

"In agricultural enterprises, the mass death of livestock would set in."

Reichenbach, G./Göbel, R./Wolff, H./von Neuforn, S.: Risiken und Herausforderungen für die Öffentliche Sicherheit in Deutschland. Szenarien und Leitfragen. Grünbuch des Zukunftsforums Öffentliche Sicherheit, Berlin, 2008.

"There is a limit to the food that can be prepared for infants."

Menski, U./Gardemann,J.: Auswirkungen des Ausfalls Kritischer Infrastrukturen auf den Ernährungssektor am Beispiel des Stromausfalls im Münsterland im Herbst 2005, 2008.

Hospital power supply in a power cut

According to a survey by the Deutsches Krankenhaus Institut, some 14% of hospitals are able to maintain complete care of their patients in the case of a power cut lasting several days.

DKI Deutsches Krankenhaus Institut: DKI Krankenhaus-Pool, 2022.
URL: https://www.bdpk.de/fileadmin/user_upload/BDPK/Service/Studien/2022/2022_10_13_Krankenhaus-Pool_Moegliche_Ausfaelle_der_Energieversorgung_und_Notfallplaene.pdf [retrieved 08.12.2022].

Höhne, C./Lenz, K.: Was tun bei einem Stromausfall im Krankenhaus. In: *Deutsches Ärzteblatt*, 116: 44, 1 November 2019.

"Power cuts lasting several hours limited to a small area, such as a few streets, take place in Germany almost every day."

Bundesnetzagentur: Kennzahlen der Versorgungsunterbrechungen Strom, 2022.
ULR: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Versorgungsunterbrechungen/Auswertung_Strom/start.html, 2021 [accessed 8 December 2022].ULR: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Versorgungsunterbrechungen/Auswertung_Strom/start.html , 2021 [retrieved 08.12.2022].

Information on rolling shutdowns / controlled brownouts

Controlled shutdowns are regulated by the Verordnung zur Sicherung der Elektrizitätsversorgung in einer Versorgungskrise (Elektrizitätssicherungsverordnung - EltSV).

3 What Are the Causes of Blackouts and Other Power Outages?

Risks due to natural events such as extreme weather

Panteli/Mancarella point out that extreme weather events have a significant influence on power supply critical infrastructure and that increasing the resilience of the power grid will become more important as the frequency, severity and duration of such events increase due to climate change:

Panteli, M./Mancarella, P.: *Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies*. Electric Power Systems Research, Volume 127, 2015, 259–270.

In the case of a power cut, the grid operators attempt to prevent the destabilization of further parts of the grid and to restore supply (…)

50Hertz Transmission GmbH, Amprion GmbH, Tennet TSO GmbH, TransnetBW GmbH (eds.): *Netzwiederaufbaukonzepte vor dem Hintergrund der Energiewende, 2020.*

In 2003, as many as 95 per cent of Italians were without electricity for several hours.

Union for the Co-ordination of the Transmission of Electricity (UCTE, ed.): *Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy*, 2004.
ULR: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/ce/otherreports/20040427_UCTE_IC_Final_report.pdf [retrieved 08.12.2022].

UCTE 2006 Union for the Co-ordination of the Transmission of Electricity (UCTE, ed.): *Final Report – System Disturbance on 4 November 2006*, 2006.

Bundesnetzagentur: *Bericht über die Systemstörung im deutschen und europäischen Verbundsystem am 4. November 2006*, 2007.
ULR: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/Netzreserve/Bericht_9.pdf [retrieved 08.12.2022].

"In Germany in 2005, electricity pylons in Münster were unable to bear the weight of snow on the wires – some people in the region spent several days without electricity."

Menski, U./Gardemann, J.: *Schneechaos und Stromausfall im Münsterland vom November und Dezember 2005: Auswirkungen auf den Ernährungs- und Gesundheitssektor sowie die private Katastrophenvorsorge und Bevorratung*. In: Das Gesundheitswesen 2009, 71(06), 349–350.

"In Ukraine, a cyber attack in 2015 caused a power outage lasting several hours affecting several hundred thousand people."

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.

Consequences of a solar storm

Eastwood, J.P., Biffis, E., Hapgood, M.A., Green, L., Bisi, M.M., Bentley, R.D., Wicks, R., McKinnell, L.-A., Gibbs, M. and Burnett, C.: *The Economic Impact of Space Weather: Where Do We Stand? Risk Analysis*, 2017, 37: 206-218. ULR: https://doi.org/10.1111/risa.12765.

"Presently, there is little risk of a blackout in Germany due to an energy shortage."

Bundesnetzagentur: *Stromnetz*, 2022.
ULR: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Stromnetz/start.html [retrieved 08.12.2022].

"In the case of a power cut, the grid operators attempt to prevent the destabilization of further parts of the grid and to restore supply in the affected area as quickly as possible. The necessary measures are set out in the grid restoration maps and are trained in regular exercises simulating different disruption scenarios."

Consentec: *Bericht für die deutschen Übertragungsnetzbetreiber*, 2020.
URL: https://www.netztransparenz.de/portals/1/Content/Weitere%20Ver%C3%B6ffentlichungen/Consentec_%C3%9CNB_NWA_Abschlussb_20200707.pdf [retrieved 08.12.2022].

Background information on the European-wide day-ahead electricity market:

European Network of Transmission System Operators for Electricity (entsoe): *Single Day-ahead Coupling (SDAC)*, 2022. ULR: https://www.entsoe.eu/network_codes/cacm/implementation/sdac/ [retrieved 08.12.2022].

4 Is a Blackout to Be Feared Due to the Energy Crisis?

"Presently, there is little risk of a blackout in Germany due to an energy shortage".

Assessment of the Bundesnetzagentur:

"A large-scale blackout is extremely unlikely. The electric energy supply system is designed around redundancy and possesses several security mechanisms intended to prevent the total collapse of the transmission system even in the event of larger disruptive events. The security mechanisms are constantly monitored for their suitability and adapted if necessary."

Bundesnetzagentur: *Stromnetz*, 2022. ULR:
https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Stromnetz/start.html [retrieved 08.12.2022].

5 What Are the Risks of Blackouts in the Future?

The potential design of the future climate-neutral energy supply is examined in various energy scenarios. For example:

Ausfelder et al.: *Sektorkopplung – Untersuchungen und Überlegungen zur Entwicklung eines integrierten Energiesystems,* Schriftenreihe Energiesysteme der Zukunft, Munich 2017.

"In the course of the expansion of renewable energy sources to 45 per cent of net electricity production, supply quality has not declined."

Bundesnetzagentur, Bundeskartellamt: *Monitoringbericht 2022*, 2022, p. 160.
ULR: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Monitoringberichte/Monitoringbericht Energie2022.pdf?__blob=publicationFile&v=3 [retrieved 08.12.2022].

The following definition for the "digitalization of electricity supply" is based on the studies below:

"Digitalization describes the sustained advancement of the information and communications technology (ICT)-based interlinking of applications, processes, actors and machines or objects in the physical world equipped with sensors and actuators. Furthermore, digitalization comprises the collection, processing, exchange and analysis of information and data in all stages of the value chain and beyond different stages of the value chain in the field of electricity supply."

Mayer, C./Brunekreeft, G. (eds.): *Resilienz digitalisierter Energiesysteme. Blackout-Risiken verstehen, Stromversorgung sicher gestalten* (Schriftenreihe Energiesysteme der Zukunft), 2020, p. 22.

The different developments and trends in digitalization (for instance artificial intelligence, digital platforms, cloud computing, big data, the internet of things, distributed ledger technology) and their significance for the energy system are described in detail in Mayer/Brunekreeft 2020, pp. 52–72.

"This decentralization and increasing digitalization of the energy system also influence the risk of a blackout."

Blackout risk factors in the digitalized energy system are described in detail in the position paper and analysis by the ESYS working group "The Resilience of Digitalized Energy Systems":

acatech – Deutsche Akademie der Technikwissenschaften, Nationale Akademie der Wissenschaften Leopoldina, Union der deutschen Akademien der Wissenschaften (eds.): *Resilienz digitalisierter Energiesysteme. Wie können Blackout-Risiken begrenzt werden?* (Schriftenreihe zur wissenschaftsbasierten Politikberatung), 2021. pp. 21–24.

Mayer, C./Brunekreeft, G. (eds.): *Resilienz digitalisierter Energiesysteme. Blackout-Risiken verstehen, Stromversorgung sicher gestalten* (Schriftenreihe Energiesysteme der Zukunft), 2021, pp. 84–91.

"Devices that consume electricity, from vehicles to heat pumps to refrigerators, which are increasingly controllable via the internet."

This is called the internet of things

Vermesan, O./Bacquet, J. (eds.): *Next Generation Internet of Things, Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation*, River Publishers 2018.

State Trojans

The Economist: *Offering software for snooping to governments is a booming business*, 2019. URL: https://www.economist.com/business/2019/12/12/offering-software-for-snooping-to-governments-is-a-booming-business [retrieved 26.06.2020].

"An attack on ICT systems causing a blackout would require considerable financial resources and personnel."

World Energy Council: *Perspectives – The road to resilience,* 2016. ULR: https://www.worldenergy.org/assets/downloads/20160926_Resilience_Cyber_Full_Report_WEB-1.pdf [retrieved 15.12.2022].

Hybride Kriege mit Cyber-Angriffen auf die Energieversorgung:

McGraw, G.: *Cyber War is Inevitable (Unless We Build Security In)*. In: *Journal of Strategic Studies*, 36: 1; 2013, 109–119.

6 What Is to Be Done?

"Power stations operate with considerable overcapacities"

While for some years now Germany has been dependent on imports for a number of hours per annum, this is largely to ensure loads are sustained based on the market. Reserve power stations are also available. Germany's annual maximum load of 81.4 GW in 2021 should be seen in comparison to a power station capacity of 238.4 GW, with over 100 GW of secured output.

Bundesnetzagentur/Bundeskartellamt 2022: *Monitoringbericht 2022*.
URL: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Monitoringberichte/MonitoringberichtEnergie2022.pdf [retrieved 15.12.2022].

"Some of this reserve capacity is deliberately supplied without digital communication too."

Reserve capacity, including without communications connections, primarily applies to frequency containment reserves (FCRs): FCR providers can rapidly respond to larger deviations in power frequency without receiving a request from the transmission system operator.

Information on the minimum requirement for communications connections for reserve capacity providers:

European Network of Transmission System Operators for Electricity: *IT-Mindestandforderungen des Reserveanbieters zur Erbringung von Regelreserve*, 2022.
URL: https://www.regelleistung.net/ext/download/minAnforderungInformationstechnikSrl [retrieved 16.12.2022].

Information on grid operators' measures securing high levels of supply quality:

European Network of Transmission Systems Operators for Electricity(entsoe): *System Operations Reports*.
ULR: https://www.entsoe.eu/publications/system-operations-reports [retrieved 08.12.2022].

Concept of resilience

Kröger, W.: *Achieving Resilience of Large-Scale Engineered Infrastructure Systems*. In: Noroozinejad Farsangi, E./Takewaki I./Yang T./Astaneh-Asl A./Gardoni P. (eds.): Resilient Structures and Infrastructure, Singapore: Springer 2019, pp. 289–313.

7 Fields of Action

"In the case of a larger power outage, they can switch to emergency operation and secure regional supply within a grid area in what is known as 'isolated operation'."

M. Braun, C. Hachmann and J. Haack: *Blackouts, Restoration, and Islanding: A System Resilience Perspective*. In *IEEE Power and Energy Magazine*, vol. 18, no. 4, 54–63, July–Aug. 2020, doi: 10.1109/MPE.2020.2986659.

"On the local level, the supply system should be able to cope without uniform central management and should remain operational via self-organization and communication from network node to network node, similar to the internet."

An overview of such concepts is provided in:

T. Strasser et al., "A Review of Architectures and Concepts for Intelligence in Future Electric Energy Systems," in IEEE Transactions on Industrial Electronics, vol. 62, no. 4, 2424–2438, April 2015, doi: 10.1109/TIE.2014.2361486.

"If, on the other hand, control is partly implemented in hardware or electrotechnical components, this can mean that later, a large number of decentral plants require retrofitting at their respective sites."

An example is what is known as the 50.2 Hertz problem: working on the assumption that not many photovoltaic facilities would be built in the future, in 2005/2006 the responsible association of grid operators (VDN) passed a rule stating that photovoltaic plants have to spontaneously switch off if there is a surplus of electricity (measured by a rise in frequency over 50.2 Hertz). All photovoltaic plants permanently implemented this procedure. However, if many plants switch off, this leads to a reduction in capacity which massively overcompensates the excessive feed-in. In response to this, in 2012 the System Stability Ordinance prescribed that photovoltaic plants had to be refitted. This involved a process taking many years. Additionally, during this period there was a risk that the photovoltaic plants could destabilize the system in special circumstances.

See

Bdew: *50,2-Hertz-Problem: Allgemeine Informationen*, 2012.
URL: https://www.bdew.de/energie/systemstabilitaetsverordnung/502-hertz-problem/ [retrieved 16.12.2022].

"for instance manufacturers of products with digital components, for which EU regulations are already being prepared."

EU Directive EG No. 0359/2020 of the European Parliament and of the Council of 16 December 2020 on measures for a high level of common cyber security across the Union, repealing Directive (EU) 2016/1148.

EU Regulation EG No. 0272/2022 of the European Parliament and of the Council of 15 September 2022 on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

"Indeed, defence against some novel attacks on power supplies is probably only possible if AI is integrated into the decentralized plants."

Eric MSP Veith, Lars Fischer, Martin Tröschel, and Astrid Nieße: Analyzing Cyber-Physical Systems from the Perspective of Artificial Intelligence, 2020, pp. 91f. In Proceedings of the 2019 International Conference on Artificial Intelligence, Robotics and Control (AIRC '19). Association for Computing Machinery, New York, NY, USA, pp. 85–95. https://doi.org/10.1145/3388218.3388222.

Some direct use of AI in energy supply will be regulated by the EU:

EU Regulation EG no. 0106/2021 of the European Parliament and of the Council of 21 April laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

"On both the European and the national level, there are already extensive measures to increase IT security"

Bundesgesetz Nr. 2034 des Bundestages vom 26. August 2016 zur Digitalisierung der Energiewende, Bundesgesetzblatt Jahrgang 2016 Part I No. 43 of 1 September 2016.

EU Verordnung EG Nr. 943/2019 des Europäischen Parlaments und des Rates vom 05. Juni 2019 über den Elektrizitätsbinnenmarkt, Amtsblatt der Europäischen Union (ABl.) No. L 158/54 of 14 June 2019.

As from 1 May 2023, public interest entities (PIEs) are obliged to provide a self-declaration on IT security and update it at least every two years. Which companies are considered PIEs is regulated by the Act on the Federal Office for Information Security (BSIG). URL: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere_regulierte_Unternehmen/UBI/ubi_node.html

EU directives in preparation

The directive on measures for a high common level of cybersecurity across the Union, also known as the Network and Information Security (NIS 2) Directive, was published in the *Official Journal of the EU* on 27 December 2022 and enters into force on 16 January 2023. From this point on, the member states have 21 months to incorporate the directive into national law. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&from=EN#d1e40-80-1.

The directive on the resilience of critical entities was also published in the *Official Journal of the EU* on 27 December. This directive too must be implemented by member states within 21 months.
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&from=DE

Another piece of legislation relevant to ICT products is currently underway: the directive on horizontal cybersecurity requirements for products with digital elements (also known as the Cyber Resilience Act).
URL: https://eur-lex.europa.eu/procedure/EN/2022_272

"States and their security services have a vested interest in gaps remaining in IT security, based on the assumption that criminal activities can thus be monitored or proven more effectively."

See for instance

Bundeskriminalamt (BKA): *Quellen-TKÜ und Online-Durchsuchung,* 2022. URL: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html [retrieved 08.12.2022].

"If a very large number of households in a small area use electric fan heaters at the same time, this can trip safety fuses in the lower voltage range and thus lead to a local power cut."

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.: *Fakten und Argumente Heizlüfter, Strom-Radiatoren und Co.*, 2022. URL: https://www.swa-netze.de/fileadmin/Downloadfiles/Sonstig/bdew/BDEW_Fakten_Argumente_Heizluefter-Heizungsalternativen_2-8-2022.pdf [retrieved 15.12.2022].

Der Tagesspiegel: *Blackout-Gefahr: Netzagentur warnt vor Einsatz von Heizlüftern*, 2022. URL: https://www.tagesspiegel.de/politik/blackout-gefahr-netzagentur-warnt-vor-einsatz-von-heizluftern-8630299.html [retrieved 08.12.2022].

Recommended citation

acatech/Leopoldina/Akademienunion (Eds.): "Are Blackouts in Germany Likely? (Discussion Paper)", Academies' Project "Energy Systems of the Future" (ESYS), 2023. https://doi.org/10.48669/esys_2023-6

This discussion paper is essentially based on the results of the position paper: "The resilience of digitalised energy systems. Options for reducing blackout risks" (https://energiesysteme-zukunft.de/en/publikationen/stellungnahme/the-resilience-of-digitalised-energy-systems)

Core team

Dr. Christoph Mayer (OFFIS, Oldenburg), Dr. Berit Erlach (ESYS Project Office | acatech), Prof. Dr.-Ing. Manfred Fischedick (Wuppertal Institut), Prof. Dr. Hans-Martin Henning (Fraunhofer Institute for Solar Energy Systems ISE), Prof. Dr. Ellen Matthies (Otto von Guericke University Magdeburg), Prof. Dr. Karen Pittel (ifo Institute), Prof. Dr. Jürgen Renn (Max Planck Institute for the History of Science), Prof. Dr. Dirk Uwe Sauer (RWTH Aachen), Prof. Dr. Indra Spiecker genannt Döhmann (Goethe University Frankfurt), Dr. Cyril Stephanos (ESYS Project Office | acatech)

Additional contributors

Christiane Abele (ESYS Project Office | acatech), Benedikte Eiden (ESYS Project Office | acatech), Anja Lapac (ESYS Project Office | acatech), Annika Seiler (ESYS Project Office | acatech)

Series editor

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

DOI

https://doi.org/10.48669/esys_2023-6

Project duration

03/2016 to 12/2023

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

The Academies would like to thank all those involved for their contributions. The Academies bear sole responsibility for the content of this discussion paper.

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

The Academies' Project "Energy Systems of the Future"

In the initiative "Energy Systems of the Future" (ESYS), acatech – National Academy of Science and Engineering, the German National Academy of Sciences Leopoldina and the Union of the German Academies of Sciences and Humanities provide input for the debate on the challenges and opportunities of the German energy transition. Within the Academies' Project, over 160 experts from the science and research communities come together in interdisciplinary working groups to develop policy options for the implementation of a secure, affordable and sustainable energy supply.

Contact:

Dr. Cyril Stephanos
Head of Project Office "Energy Systems of the Future"
Pariser Platz 4a, 10117 Berlin
phone: +49 30 206 30 96 - 0
e-mail: stephanos@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: +49 (0) 345 47239-600
fax: +49 (0)345 47239-919
e-mail: leopoldina@leopoldina.org

Berlin Office:
Reinhardtstraße 14
10117 Berlin

acatech – National Academy of Science and Engineering
Karolinenplatz 4
80333 München
phone: +49 (0) 89 520309-0
fax: +49 (0) 89 520309-9
e-mail: 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: +49 (0) 6131 218528-10
fax: +49 (0) 6131 218528-11
e-mail: info@akademienunion.de

Berlin Office:
Jägerstraße 22/23
10117 Berlin