# Power Systems in Transition

International Energy Agency

Electricity Security 2021

# INTERNATIONAL ENERGY AGENCY

The IEA examines the full spectrum of energy issues including oil, gas and coal supply and demand, renewable energy technologies, electricity markets, energy efficiency, access to energy, demand side management and much more. Through its work, the IEA advocates policies that will enhance the reliability, affordability and sustainability of energy in its 30 member countries, 8 association countries and beyond.

**IEA member countries:**

Australia
Austria
Belgium
Canada
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Japan
Korea
Luxembourg
Mexico
Netherlands
New Zealand
Norway
Poland
Portugal
Slovak Republic
Spain
Sweden
Switzerland
Turkey
United Kingdom
United States

The European Commission also participates in the work of the IEA

**IEA association countries:**

Brazil
China
India
Indonesia
Morocco
Singapore
South Africa
Thailand

Please note that this publication is subject to specific restrictions that limit its use and distribution. The terms and conditions are available online at www.iea.org/t&c/

Source: IEA. All rights reserved.
International Energy Agency
Website: www.iea.org

# Foreword

The International Energy Agency (IEA) was founded in 1974 to help co-ordinate responses to disruptions in the supply of oil. While oil is not quite the force that it once was in the global economy, risks to oil security have not gone away. As such, the IEA continues to play a pivotal role in safeguarding global oil security. But our work has also evolved and expanded significantly over the past four and a half decades. We are now working hard to ensure security of natural gas, particularly the large and growing markets for LNG. And we are increasing our focus on the ever-growing importance of electricity – both for today's economies and societies as well as for the future of energy.

The Covid-19 crisis has underscored electricity's vital role in modern societies. Reliable electricity ensures the smooth functioning of hospitals and enables many people living under lockdown to continue to work, study, shop and socialise from home. At the same time, electricity is critical for successfully achieving transitions to clean energy. The electricity sector is the biggest single source of $CO_2$ emissions today. Thanks to the spectacular rise of wind and solar, electricity is a driving force for reducing its own emissions and those of other sectors.

For rapid clean energy transitions to succeed, electricity security is more important than ever. Today we are witnessing the biggest transformation of the electricity sector since it started to emerge over a century ago. These changes come from new sources of power generation, new digital technologies, new business models, new forms of storage and more. They are exciting and hugely promising, but they also bring new challenges as they disrupt the ways in which complex electricity systems operate.

For years, the IEA's analysis and recommendations have been helping policy makers and other electricity sector leaders tackle these evolving challenges. In this special report, Power Systems in Transition, the IEA lays out in one place what secure power systems of tomorrow will require. A vital step is to increase investments in electricity networks and sources of flexibility such as demand-side technologies and storage resources. This should be complemented by better-designed markets that reward resources that deliver flexibility and capacity.

The growing digitalisation of electricity systems, the rise of smart grids and the diversification towards a wider distribution of generation sources calls for strengthening cyber security measures and making them a central part of the planning and operation of systems. And the effects of climate change mean that systems need to become more resilient to the impacts of rising temperatures and extreme weather events. This can be accomplished through better standards that guide the necessary investments.

Many countries around the world are facing similar challenges. Policy makers, regulators and operators can learn from the experiences of others. As the world's energy authority and the leading global hub for clean energy transitions, the IEA will be at the heart of such co-operation. This is demonstrated by the launch of this report at the IEA's 2nd Global Ministerial Conference on System Integration of Renewables on 27 October, where Ministers and electricity industry CEOs will share best practices and innovative solutions for enabling growing shares of wind and solar power.

The Ministerial Conference is being co-hosted by the government of Singapore, which I would like to thank for their excellent collaboration. I would also like to thank the IEA team who worked hard producing this report under the outstanding leadership of Mr Keisuke Sadamori, the IEA Director of Energy Markets and Security.

The IEA will continue to expand its energy security work to cover emerging global challenges. A notable example is the supply of critical minerals that are used in a wide range of key clean energy technologies – from wind turbines and solar panels to electric vehicles. We will produce a special report next year to provide a forward-looking global picture on this on this important issue.

Dr. Fatih Birol
Executive Director
International Energy Agency



IEA. All rights reserved.

# Abstract

Electricity is an integral part of all modern economies, supporting a range of critical services from healthcare to banking to transportation. The secure supply of electricity is thus of paramount importance. The power sector is going through fundamental changes: decarbonisation with fast growth in variable renewable sources, digitalisation expanding the surface for cyberattacks, and climate change leading to more extreme weather events. In response, governments, industries and other stakeholders will need to improve their frameworks for ensuring electricity security through updated policies, regulations and market designs.

This report surveys the ongoing multiple transformations in the electricity sector, which are leading to a new system in the future. For the first time, three key aspects of electricity security are addressed in one report: energy transitions with more variable renewables, cyber risks, and climate impacts. In addition, the roles of new technologies and demand-side response, and electrification of other sectors are explored. Examples and case studies of all these changes are taken from power systems around the world. Existing frameworks that value and provide electricity security are described, and best practices offered along with recommendations to guide policy makers as they adjust to the various trends underway..



IEA. All rights reserved.

# Acknowledgements, contributors and credits

This report was prepared by a cross-agency group of experts from the Directorate of Energy Markets and Security, the Directorate of Sustainability, Technology and Outlooks and the Strategic Initiatives Office of the IEA. The study was led and co-ordinated by Edwin Haesen, former Head of the System Integration of Renewables (SIR) Unit; and César Alejandro Hernández Alva, Acting Head of the Renewable Integration and Secure Electricity (RISE) Unit. Keisuke Sadamori, Director of Energy Markets and Security, provided expert guidance and advice.

The lead authors of this report were Keith Everhart, Zoe Hungerford, Divya Reddy, Peerapat Vithayasrichareon (Energy transition); Jason Elliott, Enrique Gutierrez, George Kamiya, Grecia Rodriguez (Cyber resilience); Craig Hart, Jihyun Lee, Jinsun Lim (Climate resilience). Other IEA colleagues also contributed to the analysis, including Stefan Lorenczik, Gergely Molnar and Kartik Veerakumar.

Valuable input, comments and feedback were provided by IEA colleagues, including Dave Turk, Laszlo Varro, Paolo Frankl, Laura Cozzi, Peter Fraser, Tom Howes, Brian Motherway, Aad van Bohemen, Brent Wanner, Nicole Thomas, Randi Kristiansen, Sylvia Beyer, Edith Bayer, Michael Waldron, Kathleen Gaffney, Sara Moarif, Vanessa Koh and Clémence Lizé.

Justin French-Brooks was the editor of this report. Thanks go to the Communications and Digital Office for their help in producing the report and website materials, particularly to Astrid Dumond, Tanya Dyhin, Christopher Gully, Jad Mouawad, Jethro Mullen, Isabelle Nonain-Semelin, Julie Puech, and Therese Walsh. Anna Kalista provided essential support.

A high-level workshop on Electricity Security was held in Paris on 28 January 2020. The participants offered valuable insights and feedback for this analysis. Further details are available at https://www.iea.org/events/iea-electricity-security-workshop.

The authors would like to thank the many external experts that provided valuable input, commented on the analysis and reviewed preliminary drafts of the report. They include: Enrique De Las Morenas Moneo, Francesca Gostinelli and Viviana Vitto (Enel); Hans Martin Fussel, Mihai Tomescu and Stephane Quefelec (European Environmental Agency); Stuart Madnick (MIT); Hannele Holttinen (IEA



IEA. All rights reserved.

Wind TCP Task 25); Jochen Kreusel and Alexandre Oudalov (ABB); Manuel Baritaud (EIB); Patrik Buijs (Elia Group); Stephen Woodhouse (AFRY); Laurent Bernat (OECD); Louise Anderson (WEF); Michael Hogan (RAP); Lwandle Mqadi (Eskom); Scott Pinkerton (Argonne National Laboratory); Rosa Kariger and Francisco Laverón (Iberdrola); Laurens de Vries (Delft University); Christophe Blassiau (Schneider Electric); Stefano Bracco (ACER); Doug Arent and Martha Symko-Davies (NREL); Guido Gluschke (ISS); Takashi Hongo (GSSI); Rina Bohle Zeller (Vestas); Ivan Dragnev (EPRI); Roberta Boscolo (WMO); Sushil Kumar Soonee (POSOCO); Tim Watson (University of Warwick); Martin Knudsen (Orsted); Sylvie Parey (EDF); Jean-Michel Glachant (FSR); Masato Yamada and Tusitha Abeyasekera (MHI Vestas); Amro Farid (Dartmouth University); Charlie Smith (ESIG); Kerry Schott (ESB, Australia); Carlos Batlle (U. Comillas); James Falzon (EBRD), Juliet Mian (ARUP); Anjos Nijk (ENCS); Manabu Nabeshima (MOFA, Japan); Russ Conklin, Fowad Muneer and Carolyn Gay (US DOE).

Comments and questions on this report are welcome and should be addressed to EMS-RISE@iea.org.



IEA. All rights reserved.

# Executive summary

**A secure supply of electricity is essential for the prosperity of our societies** and indispensable for the 24/7 digital economy. Recent difficulties caused by the Covid-19 pandemic remind us of the critical importance of electricity in all aspects of our lives, from keeping medical equipment working and IT systems available to accommodating teleworking and videoconferencing. Ensuring safe and reliable electricity supply is of paramount importance for all countries.

**While electricity only accounts for a fifth of total final energy consumption today, its share is rising**. In pathways consistent with the Paris Agreement such as the IEA Sustainable Development Scenario (SDS), the trend will accelerate, and electricity could surpass oil as the main energy source by 2040. Electricity demand increases by roughly 50% in just 20 years in all scenarios of the IEA World Energy Outlook, with growth predominantly concentrated in emerging and developing economies.

Looking ahead, electricity is expected to play a bigger role in heating, cooling, and transport as well as many digitally integrated sectors such as communication, finance and healthcare. The need for robust electricity security measures will become a prerequisite for the proper functioning of modern economies. All this puts electricity security higher than ever on the energy policy agenda.

**The power sector landscape has been undergoing dramatic changes**, shifting from one characterised by centralised, vertically integrated systems using a relatively small number of large dispatchable thermal power plants to one made up of markets with large numbers of power producers of all sizes, many of which are using variable renewable resources. At the same time, the role of digital technologies is increasing exponentially. New digital technologies provide new opportunities for the economy as well as assisting in the management of these more complex systems, but they also expose the electricity system to cyber threats. While governments and industry are employing measures to mitigate climate change, adapting electricity system infrastructure to the impacts of climate change to preserve its robustness and resilience must become a priority.

**These trends call for a broader, widely encompassing approach to electricity security**: one that brings together actions taken at the technical, economic and political levels, with the goal of maximising the degree of short- and long-term



IEA. All rights reserved.

security in a context that simultaneously comprises energy transitions, cyberthreats and climate impacts. This is the first time that a report considers all three of these aspects together.

## Electricity security during energy transitions

**Clean energy transitions will bring a major structural change to electricity systems around the world**. Variable renewable generation has already surged over the past decade. The trend is set to continue and even accelerate as solar PV and wind become among the cheapest electricity resources and contribute to achieving climate change objectives. In the IEA Sustainable Development Scenario, the average annual share of variable renewables in total generation would reach 45% by 2040.

Such rapid growth in variable renewable resources will help alleviate traditional fuel security concerns, but it will **call for a fast increase of flexibility in power systems**. On the other hand, conventional power plants, which provide the vast majority of flexibility today, are stagnating or declining, notably those using coal and nuclear. On the demand side, electrification will increase demand for electricity, and technology and digitalisation are enabling a more active role for consumers as part of more decentralised systems.

**Traditional frameworks for ensuring electricity security will not be sufficient in the face of these changes**. The challenge for policy makers and system planners is to update policies, regulation and market design features to ensure that power systems remain secure throughout their clean energy transitions.

**Experience in a number of countries has shown that variable renewables can be reliably integrated in power systems**. Many countries and regions in many parts of the world have succeeded in this task using different approaches and taking advantage of their flexibility resources. They leave to the world a large set of tools and lessons to be integrated into the policy maker toolkit.

**Making the best use of existing flexibility assets and ensuring these are kept when needed should be a policy priority.** This will require market and regulatory reforms to better reward all forms of flexibility as well as careful adequacy assessments of the impact of decommissioning plans of dispatchable supplies.

**However, going forward, new additional flexibility resources need to develop in parallel with expanding solar and wind**, especially in emerging and developing economies that are facing strong electricity demand growth. Maintaining reliability in the face of greater supply and demand variability will



IEA. All rights reserved.

require greater and more timely investments in networks and flexible resources – including demand side, distributed, and storage resources – to ensure that power systems are sufficiently flexible and diverse at all times.

**Notably, current investment trends do not support such requirements** and will need to be upgraded accordingly, sooner rather than later. Grids are a particular concern, as investment has been decreasing by 16.3% since 2015. Grids also require long-term planning, have long construction lead times and often face social acceptance issues.

**Building new assets to provide needed adequacy and flexibility will require an update to market design**. Increased reliance on renewables will augment the need for technologies that provide flexibility and adequacy to the system. This will include storage, interconnections, natural gas-fired plants in many regions, and demand-side response enabled by digitalisation. Updated approaches to planning will also be necessary, with more advanced probabilistic analyses that account for and enable contributions from all available technologies to adequacy.

## Enhancing cyber resilience

**Digitalisation offers many benefits for electricity systems and clean energy transitions.** At the same time, the rapid growth of connected energy resources and devices is expanding the potential cyberattack surface, while increased connectivity and automation throughout the system is raising risks to cybersecurity.

**The threat of cyberattacks on electricity systems is substantial and growing**. Threat actors are becoming increasingly sophisticated at carrying out attacks. A successful cyberattack could trigger the loss of control over devices and processes, in turn causing physical damage and widespread service disruption.

**While the full prevention of cyberattacks is not possible, electricity systems can become more cyber resilient** – to withstand, adapt to and rapidly recover from incidents and attacks while preserving the continuity of critical infrastructure operations. Policy makers, regulators, utilities and equipment providers must play key roles to ensure cyber resilience of the entire electricity value chain.

**Governments around the world can enhance cyber resilience through a range of policy and regulatory approaches,** ranging from highly prescriptive approaches to framework-oriented, performance-based approaches. Approaches that are more prescriptive have the advantage of allowing for more streamlined compliance monitoring, but they could face challenges in keeping pace with



IEA. All rights reserved.

evolving cyber risks. Less prescriptive, framework-based approaches allow for different approaches and implementation speeds across jurisdictions, but they raise questions around how to establish a coherent and robust cross-country approach to cybersecurity with tangible and effective impact. Implementation strategies should be tailored to national contexts while considering the global nature of risks.

## Enhancing climate resilience

**The electricity system is witnessing increasing pressure from climate change.** Rising global temperatures, more extreme and variable precipitation patterns, rising sea levels and more extreme weather events already pose a significant challenge to electricity security, increasing the likelihood of climate-driven disruption.

While there is a general recognition of these trends and associated risks, **only 17 "IEA family" countries have incorporated concrete actions for climate resilience** of electricity systems into their national adaptation strategies to date. Of those, only six cover the entire electricity value chain.

**Enhancing the resilience of electricity systems to climate change brings multiple benefits.** More resilient electricity systems reduce damage and loss from climate impacts and bring greater benefits than costs. Moreover, deployment of climate-resilient electricity systems helps developing countries address immediate threats from climate hazards and ensure reliable electricity access. Climate resilience also facilitates clean energy transitions, enabling more electrification solutions and accelerating the transition to renewable energy technologies, which are often sensitive to a changing climate.

**Effective policy measures play a significant role in building climate resilience**. The benefits of climate resilience and the costs of climate impacts tend to be distributed unevenly across the electricity value chain. This inevitably raises the question of who should be responsible for delivering resilience measures and paying for them. Policy measures for climate resilience can encourage businesses to adopt resilience measures, thus preventing a potential "market failure".

**A higher priority should be given to climate resilience in electricity security policies**. In many countries, the level of commitment and progress towards climate resilience in the electricity sector still lags behind. Mainstreaming climate resilience in energy and climate policies can send a strong signal to the private sector, inspiring businesses to consider climate resilience in their planning and operation.



IEA. All rights reserved.

## Framework for action

The three areas above require different security responses. The following overarching principles should be applicable: 1) **Institutionalise**: establish clear responsibilities, incentives and rules; 2) **Identify risks**: undertake regular system-wide risk analyses; 3) **Manage and mitigate risk**: improve preparedness across the electricity supply chain; 4) **Monitor progress**: keep track, record and share experiences ; and 5) **Respond and recover**: cope with outages or attacks and capture the lessons learned.

## Co-operation for secure energy transitions

Electricity security matters more than ever if we are to have successful clean energy transitions. In addition to identifying best practices and innovations already underway around the world, new and updated responses from governments and other stakeholders to ensure security, build off existing frameworks and develop methodologies will enable much needed changes to electricity systems.

Many of us are facing similar challenges. Policy makers, regulators and operators can learn from the experience of other countries and regions. **The IEA will be at the heart of such co-operation.**



IEA. All rights reserved.

# Electricity security matters more than ever

## Introduction

### Electricity is essential for the prosperity of our societies

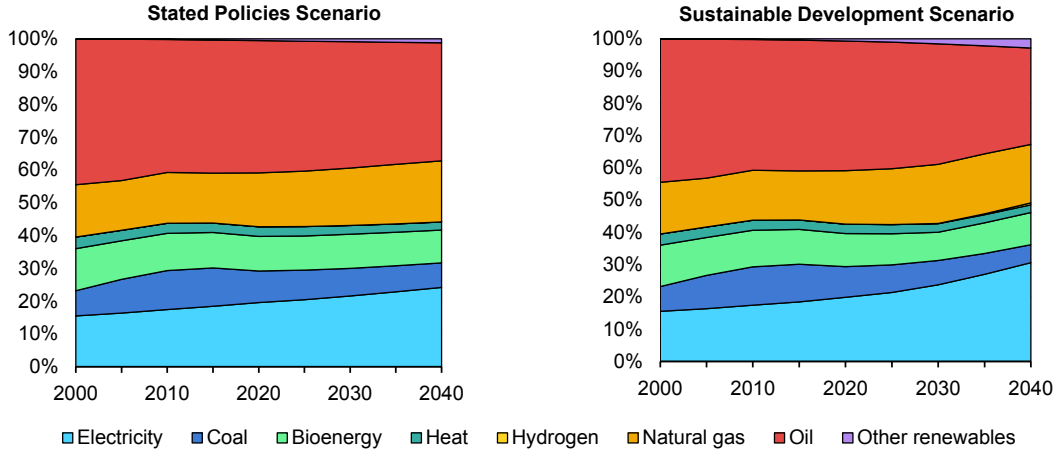
It would be very hard to imagine our modern societies without a secure supply of electricity. While it only accounts for a fifth of primary energy use today, it is indispensable for the 24/7 and increasingly digital economy. Recent difficulties caused by the Covid-19 pandemic remind us of the critical importance of electricity in all aspects of our lives, such as keeping medical equipment working in hospitals and IT systems available for teleworking and video conferencing. The impacts of an extended outage go far beyond the power system or the value of the lost energy purchase itself.

Electricity's share of final energy consumption is set to grow. Having increased from 15% in 2000 to 20% today, it is set to grow to 24% by 2040 if countries stay on their present course as in the Stated Policies Scenario of the IEA World Energy Outlook. Efficient electrification of a range of energy uses could make electricity our most significant energy source. If countries turn towards a diverse, cost-effective mix in line with the Paris Agreement, as in the IEA Sustainable Development Scenario, the role of electricity becomes even stronger, reaching 31% of final energy consumption by 2040. While the share of electricity in final consumption is less than half that of oil today, it overtakes oil by 2040 in the Sustainable Development Scenario.



IEA. All rights reserved.

**Figure 1 Share of global final energy consumption by fuel**




IEA. All rights reserved.

Notes: STEPS = Stated Policies Scenario. SDS = Sustainable Development Scenario.

The growing share of electricity in final energy demand itself does not fully capture its importance. Electricity has critical linkages with other parts of the energy sector, particularly the oil and gas industry, and underpins the basic activities of the residential, commercial and industrial sectors. As electricity drives increased shares of heating, cooling, transport and many digital sectors of communication, finance, healthcare and others, so the need for adequate electricity security measures escalates.

## The electricity system has to cope with a wide range of threats, old and new

Electricity security is often referred to using the term “security of supply” or the more literal phrase of “keeping the lights on”. The ultimate goal is to provide electricity to consumers reliably and at reasonable cost. Many threats exist to meeting this objective, ranging from equipment failure and fuel supply shortages, to operational planning failure, human error and deliberate attack. The IEA applies the following definition:

Electricity security is the electricity system’s capability to ensure uninterrupted availability of electricity by withstanding and recovering from disturbances and contingencies.

Electricity security brings together all actions taken – technical, economic and political – to maximise the degree of security in the context of the energy transition, cyber events and climate impacts, both short and long term.



IEA. All rights reserved.

**Table 1 Key electricity security terms and definitions**

| Term | Definition |
|---|---|
| Adequacy | The ability of the electricity system to supply the aggregate electrical demand within an area at all times under normal operating conditions. The precise definition of what qualifies as normal conditions and understanding how the system copes with other situations is key in policy decisions. |
| Operational security | The ability of the electricity system to retain a normal state or to return to a normal state after any type of event as soon as possible. |
| Resilience | The ability of the system and its component parts to absorb, accommodate and recover from both short-term shocks and long-term changes. These shocks can go beyond conditions covered in standard adequacy assessments. |

Sources: Based on European Commission JRC and IEA Electricity Security.

The themes covered in this report are rarely addressed through the same lens. From a detailed technical perspective, issues such as market design, system stability, cybersecurity or physical resilience may be addressed as separate disciplines. For policy makers they cover similar questions, including how reliability is defined as a measurable objective, which organisations carry which responsibility, and how appropriate incentives are given to the sector to ensure adequacy with a diverse generation mix and adequate transmission and distribution networks.

These themes also become ever more relevant because of related underlying trends. Electricity is expected to take an increasing share of total final energy consumption in the coming decades as we couple electricity with heating, transport and other sectors as part of our drive to decarbonisation. Especially in emerging economies, an enormous rise in demand is foreseen due to population and economic growth. All this puts electricity security higher than ever on the energy policy agenda.

## Types of interruption to electricity supply

As electricity is a regulated good and most often designated as critical infrastructure, governments are generally held accountable for the reliability of power supply. Although the electricity system has always been designed and regulated with reliability and cost-effectiveness in mind, the first step to properly addressing risk is to understand the type, size and depth of different power interruptions. While all of them can have potentially deep economic and safety consequences, proper risk management requires a clear view of the stakes. For this purpose, it is essential to understand the type, causes and magnitude of damage caused by different types of power sector events:



IEA. All rights reserved.

**Cascading blackouts/black system events** occur when an initial outage causes the system to collapse from an increasing series of line overloads. These events affect all customers on the network, except those with back-up generation, during a period from hours to days before full restoration. Social damage is significant as a black system event affects many essential services, such as payment systems, telecommunications and traffic lights. These events are mostly due to equipment failure and simultaneous contingencies, and are very rarely related to lack of installed generation capacity. The Hokkaido blackout in 2018, due to an earthquake, and the South Australian blackout in 2016, a mix of severe storms and flawed interconnection standards, are recent examples.

The potential indirect impacts of blackouts are also enormous and include: transport disruption (the unavailability of trains and charging stations for electric vehicles), food safety issues (risk to the cold chain), problems related to public order (crime and riots), and loss of economic activity. This can lead to health and safety problems as well as substantial financial losses. In extreme cases where power outages relate to extreme natural events, loss of electricity supply exacerbates other recovery challenges, making restoration of the power system one of the earliest priorities.

**Load shedding** is the deliberate disconnection of electrical power in one part or parts of a power system. It is a preventive measure taken by system operators to maintain system balance when supply is currently or expected to be short of the amount needed to serve load plus reserves, after exhausting other options like calling on demand response, emergency supplies and imports. These are short-duration events lasting from minutes to a few hours where small amounts of energy are rationed to segments of consumers (1% to 2% of the unserved energy during a cascading blackout), while allowing loads that provide essential services to continue to be served. They are, from a consumer point of view, indistinguishable from other interruptions on the distribution grid. The anticipated, controlled and limited use of this extreme measure should be seen as an instrument to maintain security of supply.

Most current reliability standards target a level of supply that would expect a small amount of acceptable load shedding as a way to balance security of supply and economic considerations. For example, the Alberta system operator in Canada has needed to apply this type of interruption in three events between 2006 and 2013, with a total duration of 5.9 hours and an amount of energy well below the regulatory (reliability) standard. Even if load shedding results only in small amounts of energy not being served, it completely cuts power supply to certain groups of customers, creating an array of inconveniences. To share the damage



IEA. All rights reserved.

and minimise the inconvenience, the power cuts are often "rolled", switching from one customer block to the next. In the near future, digitalisation should allow power systems to phase out this small but drastic and inefficient way of rationing energy. This would cut energy only to non-essential appliances or storage-enabled devices, and maintain it for other uses where interruption would create more inconvenience, such as lifts.

**Long rationing periods of electricity** occur when system operators and governments have to limit power supplies on a planned basis because of large deficits of electricity supply to meet demand. This is possibly the most harmful type of power sector event that a society can face. Some long-duration rationing events have meant rationing as much of 4% to 10% of annual electricity consumption, creating large social and macroeconomic impacts. They include the one in Brazil in 2001 due to drought and an unsuitable investment framework. The large supply shock in Japan following the Great East Japan Earthquake also belongs to this category, when the government responded with a nationwide electricity conservation campaign that forced industry to make massive electricity demand shifts.

Many emerging economies such as Iraq and South Africa see their economic and social welfare severely impacted by recurrent periods of electricity rationing that can last many months. Although developed economies have solved this type of event due to sound investment frameworks, it remains a challenge for many developing economies. Nonetheless, developed economies should not take for this dimension for granted; investment frameworks need to be updated and resilient to new trends.

**Table 2 Recent examples of major disruption to power supplies**

| Type of event, location, year | Key factors | Extent of blackout |
|---|---|---|
| Load shedding, California 2020 | Heatwave | Rolling blackouts affecting up to 3 million people for up to 2.5 hours across several days |
| Load shedding, United Kingdom 2019 | Lightning strike, operational security | 1 million people for around 40 minutes, aggravated by transport delays |
| Load shedding, California 2019 | Wildfires | Transmission lines shut down affecting 11% of PG&E customers for 3 days |
| Black system event, Hokkaido 2018 | Earthquake | 5.3 million people for 12-48 hours |
| Blackouts, Ukraine 2015-16 | Cyberattacks | 1-6 hours, 200 000+ people |
| Long energy rationing period, Brazil 2001 | Drought, inadequate investment framework | 20% of total energy consumption for 6 months |



IEA. All rights reserved.

# New trends demand an update to electricity security frameworks

## The power sector landscape is changing dramatically

After more than a century of rising electrification, most middle- and high-income countries have managed to reach high levels of electricity reliability. This achievement is the result of complex institutional frameworks often involving multiple institutions and stakeholders. These frameworks govern crucial aspects, from the planning of the physical infrastructure, setting the market and investment frameworks, to the secure operation of the system and preparedness for natural catastrophes.

Electricity security frameworks are the result of more than a century of experience, with a relatively stable set of technological choices and well-understood risks. But past experience, as characterised below, is not always enough to prepare for the future.

- Electricity was mostly provided by vertically integrated utilities with regional monopoly using dispatchable thermal and hydro power plants and centrally controlled transmission and distribution networks.
- Large rotating mass for power generation also provided system inertia. Power generators were controlled manually and not connected to digital networks.
- Regulation made a single entity responsible for the stable supply of electricity in the region and set the electricity tariff at a level sufficient to cover the normal rate of return from the invested asset. Under this system, utilities were able to invest in generation and network facilities with a high level of confidence about their return.

In an increasing number of countries and regions, these assumptions no longer apply.

Electricity market systems with regulated regional monopolies have been replaced by unbundled competitive systems.

Variable renewable sources like wind and solar PV have become cheaper than thermal power generation and are increasing their share of supply. This development is welcome as countries seek to decarbonise the electricity sector. Solar PV is one of the rare technology areas that is on track to achieve its sustainability goals. Wind and solar are indigenous energy sources, and their growth can reduce fossil fuel import bills for many countries.



IEA. All rights reserved.

At the same time, these new variable sources require flexibility in the system to cover their variability and more elaborate forecasting of their outputs. They are non-synchronous generators and do not bring in system inertia.

Variable renewables, solar PV in particular, are more distributed than conventional generators. Systems with distributed resources can be more resilient than centralised systems, but require operators to have greater situation awareness. Some resources are even behind the meter at consumers' properties. Network operators increasingly rely on demand-side response as a key source of flexibility.

To manage such complex systems, the role of digital information technologies is increasing exponentially, exposing the electricity system to cyberthreats.

Governments and industry are promoting decarbonisation of energy systems to achieve sustainability goals such as climate change mitigation, but ongoing climate change is already leading to extreme weather events and is challenging the robustness and resilience of electricity supply infrastructure.

Businesses across the entire electricity supply chain need to invest in secure stable electricity supply in response to these drastic changes, but are challenged by increased uncertainty and complexity surrounding electricity systems.

For this reason, our report focuses on three aspects that will increasingly attract the attention of policy makers:

- a **changing electricity mix** driving new measures to ensure operational security and longer-term system adequacy
- emerging risks to **cybersecurity**
- the need for greater resilience against **adverse impacts of climate change**, including extreme weather events.

This report provides policy makers with a structural review of the types of threats the system will be facing in the coming decades and how they can be managed with proper institutional measures, market design and technology.

The new power sector landscape will be shaped by a combination of factors: a growing role for variable renewables, stagnation or reduced contributions from traditional low-carbon sources such as nuclear and hydro, decreasing thermal fleets, further digitalisation of the economy, climate change, and others. The combination of these factors will alter the potential impact and likelihood of electricity supply interruptions. They may well put more pressure on certain areas of the electricity security framework, such as rules designed to bring investment into the sector, while changing the nature of traditional energy security concerns,

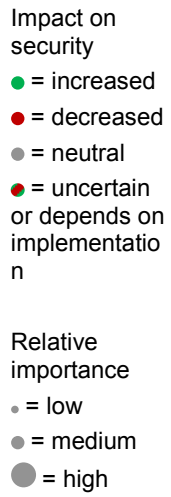


IEA. All rights reserved.

such as fuel security. How the threat map changes will depend on the specific power mix, the policies in place and the external threats to each power system.

**Table 3 Electricity system trends and their potential impacts on various aspects of electricity security**

| Trend | Flexibility | Fuel security | Adequacy | Climate resilience | Cyber resilience | Simultaneous contingencies |
|---|---|---|---|---|---|---|
| Higher shares of variable renewables | | | | | | |
| Smaller fossil-fired fleets | | | | | | |
| Declining shares of dispatchable low-carbon (nuclear/hydro) | | | | | | |
| **Decentralisation** (e.g. distributed generation, battery storage) | | | | | | |
| **Digitalisation** (e.g. connectivity, automation) | | | | | | |




Notes: Circle colour indicates the potential impacts on various security aspects, e.g. flexibility. Circle size indicates the relative level of importance for a specific security aspect. The intent of the table is to illustrate the potential impacts in a generalised way. Actual impacts in specific countries and states/provinces will depend on their context and circumstances, e.g. generation mix, existing infrastructure, geography, climate. Simultaneous contingencies are outages of generation and transmission assets which are unexpectedly affected at the same time by the same event, such as earthquakes.

Secure supply of electricity requires many risk dimensions to be properly managed. From fuel availability and sufficient resources to cover peak demand and periods of stress, such as an unexpected plant outage, to the resources needed to ensure stable behaviour of the power system in real time, all these dimensions need to be considered and assessed. The table indicates how these dimensions can be affected by electricity system trends. Each dimension will be affected, sometimes in a positive manner, reducing the risks and increasing the set of tools available to maintain secure operation, but also potentially in a negative way. For example, in a country where the electricity mix is dominated by hydropower, growing reliance on solar PV could increase climate resilience and act as a good hedge against changing hydrology, but it may also require existing assets to be operated in a new, more flexible way.

A sound electricity security framework needs to map how these trends will alleviate certain security concerns while increasing others.



IEA. All rights reserved.

## Ensuring security of supply requires proper governance

Most large interruptions have multiple causes, and therefore policy makers need to account for many different dimensions in the institutional framework that governs the power sector. This emphasises the need for rigorous analysis to underpin the decision-making behind ensuring reliability and more general security of supply.

As the electricity system continues to evolve due to the energy transition and emerging trends such as cyberthreats and climate change, governments and regulators will need to continue to update the legal and regulatory requirements on all stakeholders to ensure that electricity security is maintained in the face of these changes.

There are already cases of legislative changes to redefine frameworks, roles and responsibilities for various institutional actors in the electricity system to adapt to ongoing transformations in the power sector. The passage of the so-called EU Clean Energy Package is an attempt to restructure the institutional framework for EU electricity markets, including electricity security, in the face of ongoing changes to the fuel mix and increasing interconnectivity across electricity systems. It is a gradual evolution from earlier European legislative initiatives, or packages, for the electricity system published in 1996, 2003 and 2009. These started from an unbundling and market perspective, but increasingly cover security-related provisions.

Regulators, in particular, will have an important role to play in ensuring electricity security amid the energy transition. Either with changes to law or stemming from existing statutory authority, they will need to adjust market designs and standards to reflect greater variability of supply and demand. They will also need to account for new threats such as cybersecurity and climate change.

For example, to support the secure integration of renewables into the grid and manage risks stemming from the retirement of baseload generation and lower utilisation of other plants, the US Federal Energy Regulatory Commission issued Order 842 in February 2018. It requires all new generators (regardless of size or technology) to be capable of providing primary frequency response – a specific ancillary service used to cope with sudden changes in supply and demand – as a precondition for grid interconnection. Similarly, the European Union established a legally binding grid code in 2016 across all its member states that requires all new connections to have essential ancillary service capabilities. This paves the way for future operational rules and balancing markets with ever higher shares of VRE and distributed resources.



IEA. All rights reserved.

# Integrated planning beyond jurisdictional borders is needed, involving a complex set of players

New and emerging threats to the reliability of power systems present challenges to electricity planning frameworks. This is true across market structures, ranging from competitive markets with extensive private-sector participation to more vertically integrated utility models. The implications of such developments for the electricity sector should be taken into consideration together with the fundamentals of generation, transmission and distribution.

In many jurisdictions, increasingly integrated and co-ordinated planning frameworks have played a vital role in the cost-effective and secure transition to a new electricity mix. They increase transparency and provide information to market participants and to all stakeholders in general, informing project developers, grid operators and authorities. These frameworks are increasingly co-ordinating investment in generation and grids. They are also useful for foreseeing the potential outcome of low-probability but high-impact events. New approaches are emerging for co-ordinated and integrated planning practices that expand the traditional scope:

- inter-regional planning across different jurisdictions and balancing areas
- integrated planning across a diversity of supply and demand resources (and other non-wire alternatives)
- integrated planning between the electricity sector and other sectors.

These new approaches are expanding and reaching into distribution networks, which have historically depended on power supplied by the transmission network. The situation is changing as more generation resources are added locally to the distribution network at low- and medium-voltage level. Where deployment of many smaller distributed plants is concentrated geographically, reverse flows from the distribution network up to the transmission level become increasingly common and must be managed securely. Most distribution networks are physically capable of managing two-way flows of power, although a number of upgrades and operational changes in voltage management and protection schemes can be necessary.

Closer co-ordination between transmission system operators and distribution system operators is important for dealing with this change. Policy makers can help ensure that transmission and distribution planning processes are better integrated with generation planning, particularly as the latter begins to take system flexibility into consideration. Appropriate planning rules will play a crucial role in the



IEA. All rights reserved.

expansion of the electricity sector and to foresee the impacts of low-probability but high-impact events, covering the grid, new generation, storage and other flexibility options.

## Electricity security during the energy transition

The clean energy transition will bring a major structural change in the generation profile of electricity systems around the world. Variable renewable generation has already surged over the past decade, driven by cost reductions and favourable policy environments. The trend is set to continue and even accelerate in line with climate change objectives. At the same time, conventional power plants, notably those using coal, nuclear and hydro, are stagnating or declining. On the demand side, electrification will increase demand for electricity, even in a context of growing energy efficiency, requiring far greater levels of investment in power systems than we are witnessing today.

Moreover, technology and digitalisation are enabling a more active role for consumers in power systems, which are poised to become more decentralised in the coming years. The challenge this presents to policy makers and system planners is to ensure system security by putting in place appropriate policies, regulation and market design features to support resource adequacy. This includes the advancement of a diversity of low-carbon generation technologies and new flexibility resources such as demand response, storage, digitalisation and greater market interconnection to help meet the new challenges.

# Low-carbon sources on the rise

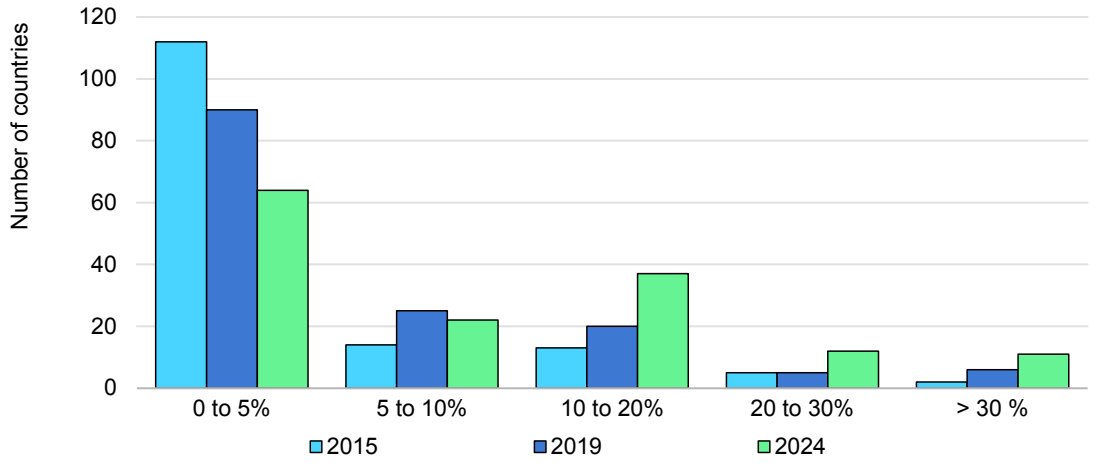
## The energy transition will bring sizeable growth in variable renewables

The energy transition being seen in many systems in the world will bring major changes in the way the system is operated. The most significant is the large-scale deployment of low-cost variable renewables.



IEA. All rights reserved.

**Figure 2 Share of variable renewables in the global electricity mix**

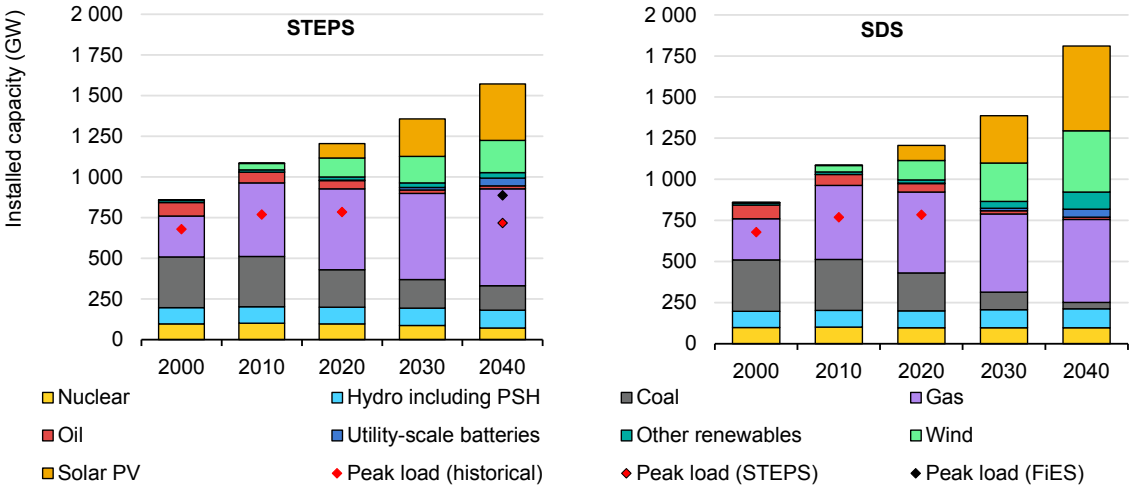



IEA. All rights reserved.

Source: IEA Renewable Energy Market Report 2020.

Along with this large deployment of VRE, conventional power plants that provided the dominant proportion of power system flexibility in past decades are now retiring. The remaining conventional plants are mostly powered by natural gas, particularly in Europe and the United States. In Europe this is developing in parallel with decreasing domestic production of natural gas, leading to a closer link between natural gas supply security and electricity security.

**Figure 3 Installed capacity in the United States, 2000-20, and projections to 2040**




Notes: FiES = Future is Electric Scenario from IEA World Energy Outlook 2018. PSH = pumped storage hydro. STEPS = Stated Policies Scenario. SDS = Sustainable Development Scenario. Most recent historical peak load is from 2017.
Sources: IEA World Energy Outlook 2018; IEA World Energy Outlook 2019; IEA Market Report Series: Renewables 2019.

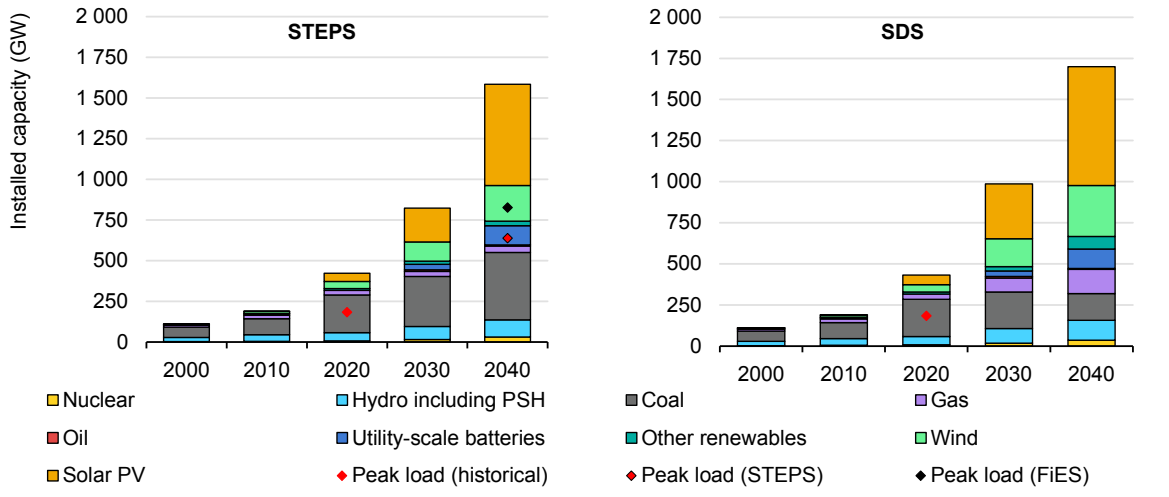
To achieve emission reduction objectives, deployment of wind and solar PV will have to accelerate substantially and will become dominant sources in various



IEA. All rights reserved.

parts of any interconnected system. Nonetheless, the IEA Sustainable Development Scenario points to a diverse supply mix where solar PV and wind are dominant in capacity, but are supported by other low-carbon generation technologies, demand response and storage, as well as digitalisation and market interconnection. Natural gas and coal will still play a role as well, particularly in developing economies like India. Not achieving the scenario's levels of generation from other low-carbon technologies, such as nuclear and biomass, would result in additional costs and challenges. It would be extremely challenging for wind and solar technologies to further accelerate growth to such levels that they can compensate for a lack of other low-carbon generation. Moreover, the scenarios provide a purely techno-economic perspective, without considering social acceptance or political factors related to additional wind turbines, nuclear facilities, fossil fuel plants and new overhead transmission lines, all of which can further complicate achieving an optimal, low-carbon generation mix.

**Figure 4 Installed capacity in India, 2000-20, and projections to 2040**




IEA. All rights reserved.

Notes: FiES = Future is Electric Scenario from IEA World Energy Outlook 2018. PSH = pumped storage hydro. STEPS = Stated Policies Scenario. SDS = Sustainable Development Scenario. Historical peak is based on 2019.

Sources: IEA World Energy Outlook 2018; IEA World Energy Outlook 2019; IEA Market Report Series: Renewables 2019; India Ministry of Power 2020

## Low-carbon dispatchable sources, such as nuclear, see their role reduced in the energy landscape

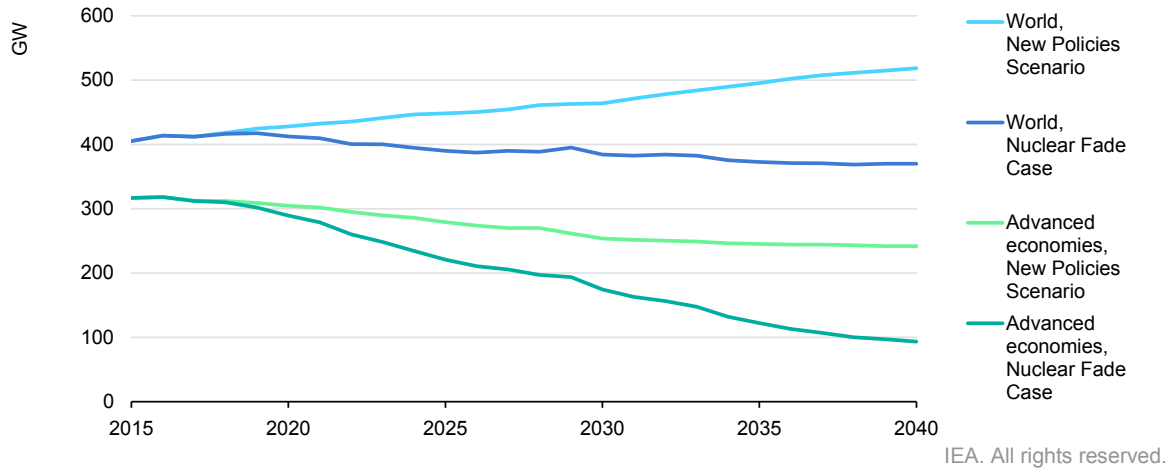
Nuclear power plants are in decline at a global level despite being low-carbon, dispatchable, and, to some extent, flexible generation sources. The IEA Nuclear Power in a Clean Energy System analysis projected a Nuclear Fade Case, which explores what could happen over the coming decades in the absence of any



IEA. All rights reserved.

additional investment in lifetime extensions or new projects. This case is increasingly aligning with what may very well happen in the coming decades in advanced economies. In the scenario, nuclear capacity in advanced economies would decline by two-thirds by 2040, from about 280 GW in 2018 down to just over 90 GW in 2040. The European Union would see the largest decline, with the share of nuclear in generation falling from 25% in 2018 to below 5% in 2040.

**Figure 5 Global nuclear capacity in the New Policies Scenario vs a Nuclear Fade Case**




IEA. All rights reserved.

Source: IEA Nuclear Power in a Clean Energy System.

Other sources such as biomass and biogas are expected to grow, but the pace of growth (from 2.0% of capacity to 2.2% globally in the period 2018-30 in the Stated Policies Scenario) would be much slower than the declines in coal and nuclear. New technologies, such as power plants equipped with carbon capture, use and storage, are progressing far less quickly than required to achieve a sustainable path. As a result, there is a risk that growth in other low-carbon technologies aside from wind and solar PV will be insufficient to compensate for coal and nuclear closures. Clean hydrogen is gaining momentum and has strong potential as a long-term energy storage source if it can be scaled up in the coming decade, as being promoted in various policy initiatives already.

## The energy transition will change the diversity of every power system – changing their vulnerability to shocks

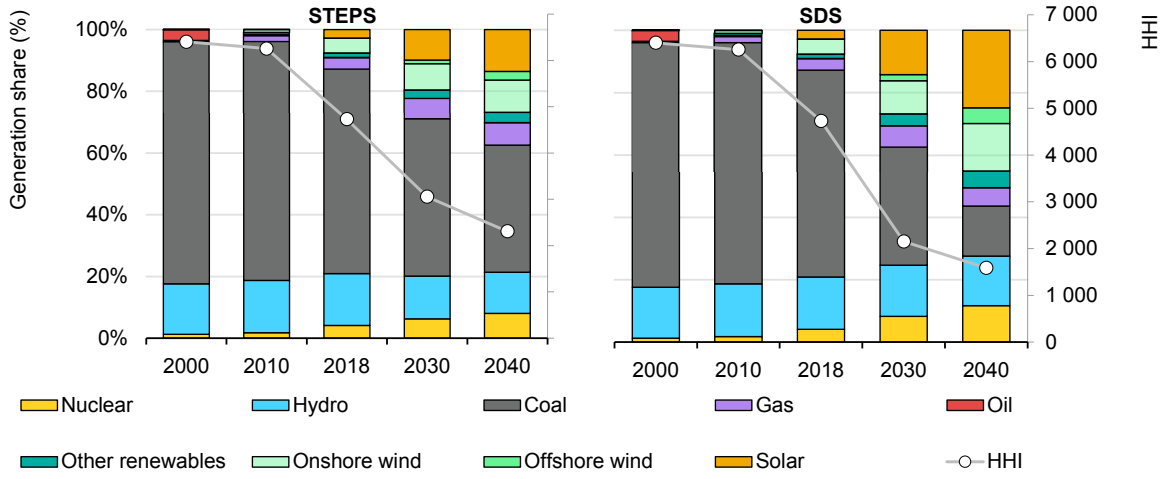
Until now, wind and solar PV have contributed positively to diversity in the generation mix. They are indigenous resources, which have therefore helped fuel-importing countries reduce their import bills and increase their self-sufficiency. A well-diversified generation mix, with contributions from wind and solar PV, can



IEA. All rights reserved.

improve electricity security by mitigating risks arising from physical supply disruptions and fuel price fluctuations. Small-scale generators, such as distributed wind and solar PV, also have the potential to facilitate recovery from large-scale blackouts during the restoration process, while large thermal power plants take longer to resume normal operations since they need a large part of the system to be restored. These are clear examples of electricity security benefits from increasing the share of wind and solar PV. For example, in the People's Republic of China, a shift from a strong reliance on coal to increased wind and solar will increase the diversity of the generation mix out to 2040.

**Figure 6 Distribution of generation in China, 2000-20, and projections up to 2040**




IEA. All rights reserved.

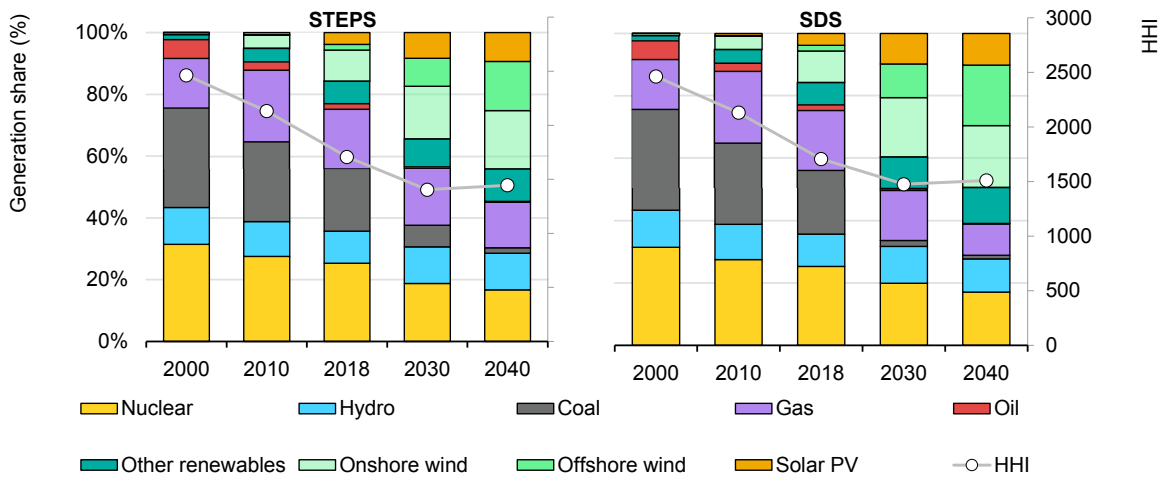
Notes: The Herfindahl-Hirschman Index (HHI) is often used as an indicator of diversity, with a lower total HHI indicating a more diverse mix (the possible range is from near zero to 10 000). Note that this aggregated metric does not account for diversity within a fuel source, for example between local and imported resources or for VRE sources geographically spread out, nor for sources of flexibility such as interconnection and demand response. STEPS = Stated Policies Scenario. SDS = Sustainable Development Scenario.
Source: IEA World Energy Outlook 2019.

Looking ahead, electricity supply systems in some regions could see less diversity in power generation sources. European electricity markets have achieved a high level of interconnection between power systems across many countries. They are endowed with diverse power generation sources, including natural gas, coal, nuclear, hydro, wind, solar PV and other sources. Such generation fuel diversity has been a source of confidence in electricity supply security spanning a wide region. As some generation sources are likely to decline in capacity, the diversity of the future system will need to be found in a low-carbon generation mix, flexibility in supply and demand response, and the ever-increasing importance of grid interconnections.



IEA. All rights reserved.

**Figure 7 Distribution of generation in the European Union, 2000-20, and projections up to 2040**




IEA. All rights reserved.

Note: The Herfindahl-Hirschman Index (HHI) is often used as an indicator of diversity, with a lower total HHI indicating a more diverse mix (the possible range is from near zero to 10 000). Note that this aggregated metric does not account for diversity within a fuel source, for example between local and imported resources or for VRE sources geographically spread out, nor for sources of flexibility such as interconnection and demand response. STEPS = Stated Policies Scenario. SDS = Sustainable Development Scenario.

Source: IEA World Energy Outlook 2019.

Coal-fired power plants, in particular, are being decommissioned to align with ambitions to reduce $CO_2$ emissions and pollution levels. The trend will need to continue in order to achieve climate change mitigation objectives, increasingly supported by policy measures and finance strategies to phase out the use of coal-fired generation.

Many other electricity systems today also have quite a diverse generation mix, with natural gas, coal, nuclear, hydro, biomass, wind and solar PV. A further increase in VRE combined with a decline in conventional generation will require a review of electricity security frameworks by policy makers, supported by input from the wider industry. VRE and other flexibility sources such as demand response and energy efficiency provide an important contribution to adequacy. Fully incorporating these resources into a reliability framework and optimising them in system operations calls for strengthened analysis and appropriate regulatory and market reforms. Early steps in the clean energy transition of particular regions provide critical lessons for those still in an initial phase of their own transition. For the advanced regions, implementation of the next steps is likely to be more challenging than those already achieved.

The significant concentration of low-carbon generation in a few VRE sources, such as onshore wind and PV, will create increasing challenges for policy makers, regulators and system operators. For example:



IEA. All rights reserved.

- The close correlation of VRE generation in certain periods erodes the economic value of energy at these times, potentially creating investment challenges for continued deployment. Additionally, the marginal carbon emission savings will tend to reduce, as higher-emitting energy sources are displaced and competition between low-carbon technologies becomes more common.
- Systems will need to be able to handle increased variability and uncertainty, increasing the need for flexibility.

Tapping into a larger set of variable resources with different generation patterns will reduce these underlying challenges by smoothing the combined VRE output over time, which can both decrease the economic cost of decarbonising the system and soften the integration challenges associated with few generation sources. For instance, solar and wind generation often exhibit both diurnal and seasonal complementarity, reducing the overall variability of VRE output across the day as well as through the year.

For Europe, the growing prospects of offshore wind are a promising opportunity to further diversify the low-carbon mix, as larger capacity factors and complementary generation patterns will soften the integration challenges of VRE. Still, in highly decarbonised systems with diminished nuclear and fossil fleets, other low-carbon sources such as biomass, biogas, hydrogen and carbon capture, use and storage will eventually be needed to cover periods of low VRE generation, together with new flexibility sources such as power storage and the increasing scope of demand-side response.

# Maintaining reliability

## Lower than needed levels of investment in power systems today present risks for tomorrow

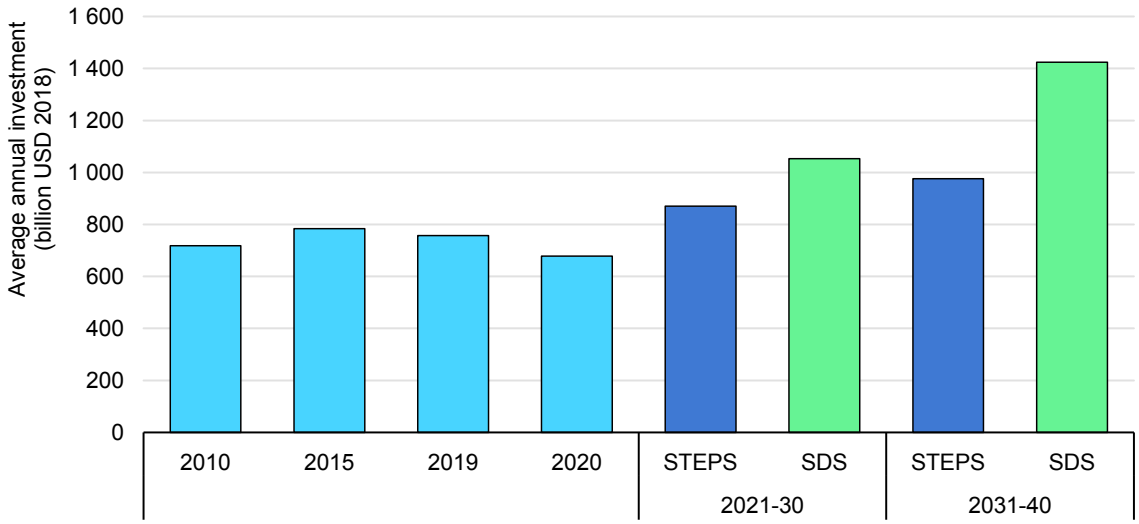
Although wind and solar PV have seen impressive growth in recent years, overall spending in the power sector appears to be less than what will be needed to meet forthcoming security challenges. To this end, the IEA World Energy Investment Report 2020 portrays a rather grim picture. Global investment in the energy sector declines by 20% or USD 400 billion in 2020 in the aftermath of the Covid-19 crisis. The oil and gas upstream sectors see the largest negative impact compared to the electricity sector. Nevertheless, the overall level of investment in power in 2020 declines by 10%. The crisis is prompting a further 9% decline in estimated global spending on electricity networks, which had already fallen by 7% in 2019. Alongside a slump in approvals for new large-scale dispatchable low-carbon



IEA. All rights reserved.

power plants (the lowest level for hydropower and nuclear this decade), stagnant spending on natural gas plants and a levelling off in battery storage investment in 2019, these trends are clearly misaligned with the future needs of sustainable and resilient power systems.

**Figure 8 Average annual global power sector investment, 2010-20, and needs to 2040**




EA. All rights reserved.

Notes: STEPS = Stated Policies Scenario. SDS = Sustainable Development Scenario.
Sources: IEA World Energy Outlook 2019; IEA World Energy Investment 2020.

Low investment levels are projected not only with respect to the requirements of the Sustainable Development Scenario, but also in Stated Policy Scenario pathways. While this has not led immediately to serious power supply incidents, longer-term risks need to be addressed now. Further acceleration can be expected in the deployment of VRE sources like wind and solar PV, due to continuing cost declines and government support schemes. Incentives for flexibility from other parts of the electricity system, including grids, demand response and batteries, receive less focus or only indirect attention in policies and regulatory frameworks worldwide, but are, nevertheless, essential.

The case of European and US electricity markets is very illustrative in this sense. In the past decade following the financial crisis, advanced market economies have seen weaker-than-expected growth in electricity demand in general. Due to a combination of a weak economic recovery, stronger policies on energy efficiency and a rapid spread of efficient technologies like LED lights, electricity demand has stagnated or even declined across all advanced economy systems. By 2015 electricity demand in Europe and the United States was 435 TWh (6.2%) lower



IEA. All rights reserved.

than initial expectations for recovery after the financial crisis. This had important and positive implications for electricity security: there was a major wave of investment into combined-cycle gas turbine capacity just before the acceleration of wind and solar PV capacity additions. These gas turbine plants were envisaged as running at a reasonably high load factor to supply robust demand growth. Despite this not materialising, they still have the technical capacity for low and flexible utilisation, primarily providing grid services, which they have done as the share of variable renewables increased. Many jurisdictions have implemented changes to their market design, such as Capacity Remuneration Mechanisms or scarcity pricing, as means to recognise the contribution of these resources to security of supply and attract investments to them.

This example is relevant to the electricity security discussion. System operators and markets succeeded in maintaining robust electricity security while the share of variable renewables grew faster than expected. However, this task was greatly facilitated by the large excess capacity of predominantly flexible units. It should be emphasised, however, that this capacity balance was not the result of a conscious design; rather, it was the result of an unexpected structural break. It also led to massive-scale value destruction as utilities wrote down assets and their equity capitalisation depreciated. The combination of weak demand and value destruction of flexible assets shaped investor expectations, creating a reluctance to invest in these assets.

Future policy and technology changes can also trigger structural breaks. However, there is no guarantee that these will similarly lead to lower-than-expected demand. On the contrary, the coming decades of the electricity transition might well lead to a re-acceleration of electricity demand growth and a substantially higher generation capacity need, in particular due to a trend of increased electrification.

Technological progress has been highly asymmetrical: low-carbon generating technologies like wind and solar PV, and the technologies enabling electrification such as electric car batteries, have progressed more swiftly and witnessed larger-scale deployment than non-electrical low-carbon options like biofuels. In the previous decade, energy efficiency progress compounded the effect of weaker-than-expected economic growth, leading to surprisingly low power demand.

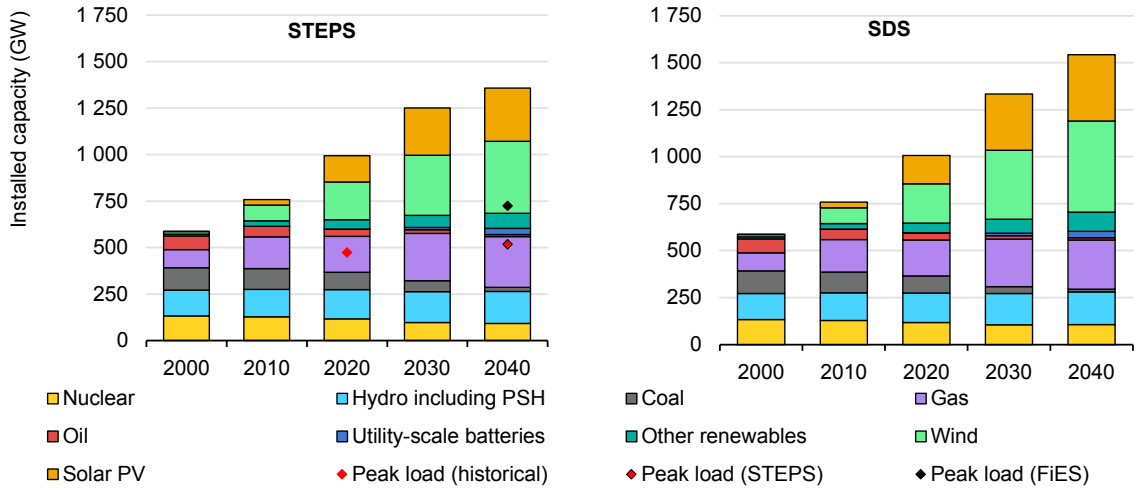
In the next decade, while the macroeconomic downside risk is unfortunately real, electrification might well outweigh efficiency gains; a household buying an electric car on average adds as much electricity demand as dozens of families replacing refrigerators with ultra-efficient models. The impact of direct electrification would be reinforced by an increasing strategic interest in electrolytic hydrogen, which



IEA. All rights reserved.

could replace fossil-fuelled end uses such as heavy trucks or industrial heat. The recently announced EU hydrogen strategy targeting 10 million tonnes of green hydrogen by 2030 would require over 10% of the region's present electricity generation, which equals the total growth in electrical output during 2000-2010 in a context of stagnation in electricity demand in the recent decade.

**Figure 9 Installed capacity in the European Union, 2000-10, and projections up to 2040**




IEA. All rights reserved.

Notes: FiES = Future is Electric Scenario from IEA, 2018. PSH = pumped storage hydro. STEPS = Stated Policies Scenario. SDS = Sustainable Development Scenario. Historical peak load is from 2019.

Sources: IEA World Energy Outlook 2018; IEA World Energy Outlook 2019; IEA Market Report Series: Renewables 2019; ENTSO-E Transparency Platform.

In addition to electrification and reaccelerating demand growth, renewables deployment will also have to cover accelerating and nearly unavoidable coal and nuclear capacity decommissioning in many advanced economies. After the value destruction of the past decade, there is little investment appetite for new conventional flexible assets in most mature energy systems. In any case, these may not always be aligned with a credible low-carbon strategy, as is the case for coal. New flexibility enablers from batteries, wider demand response, deeper interconnection of regional systems, new business models and market designs need to fill the gap.

## The reliability services required to keep the lights on will need to evolve in response

In addition to controlling total system costs and ensuring necessary investment happens at sufficient pace, policy makers need to take into account that a future low-carbon mix requires dedicated action to ensure a secure system. Regardless

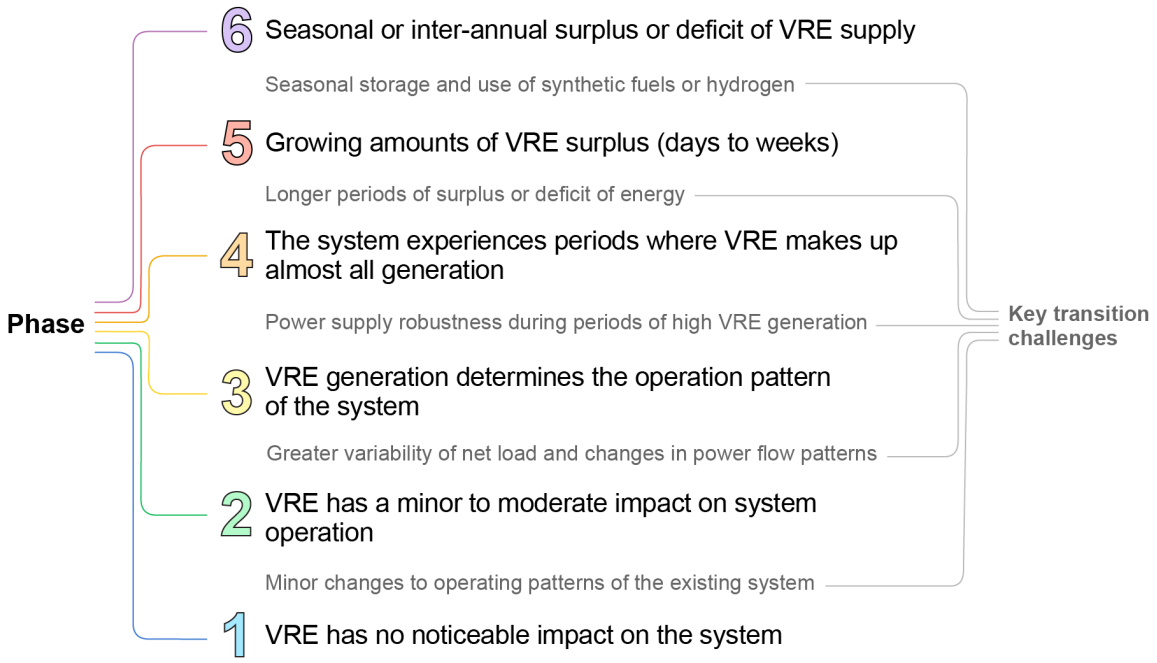


IEA. All rights reserved.

of whether countries follow the STEPS or SDS, the share of VRE will be high at a global level and very high in many regions. This implies technical and economic challenges fundamentally different from the ones power systems have faced traditionally.

The integration of VRE can be classified into six phases that capture the evolving impacts, relevant challenges and priority of system integration tasks to support the growth of VRE. While a system will not transition sharply from one phase to the next, the phased categorisation framework can help to prioritise institutional, market and technical measures. For example, issues related to flexibility will emerge gradually in Phase 2 before becoming the hallmark of Phase 3.

**Figure 10 VRE integration phase assessment**




IEA. All rights reserved.

Source: IEA Status of Power System Transformation 2019.

Most systems are still in Phases 1 to 3 and have up to 10-20% share of VRE in annual electricity production. The general trend is clear that higher phases of system integration are forthcoming for most countries. Many countries are expected to enter Phase 4 in the coming years.

Some steps are operational in nature, particularly from Phase 4 as the system faces multiple periods with high levels of VRE generation. While any system has

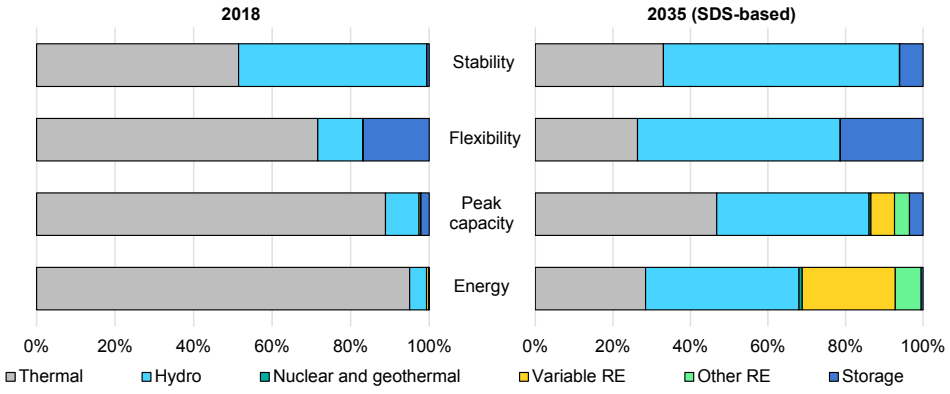


IEA. All rights reserved.

its unique characteristics and legacy, exchange of best practices can support progress in many regions. Inertia provides an illustration of this.

A move to solar PV and wind implies a shift from conventional rotating generation to inverter-based generation. Thermal and hydro generation are based on synchronous machines with heavy rotational mass, which provides inertia to the system. In Phase 4, with a high share of VRE, the system faces challenges in maintaining stability. Inertia is a key parameter in system stability. Solar PV and wind generation, but also electric vehicle chargers, batteries and high-voltage direct-current connections, are all inverter based and do not inherently provide inertia. Technology does allow for a variety of very rapid responses to the needs of the system, known as synthetic inertia. Smaller systems (industrial sites and islands) are already capable of operating at very high levels of VRE infeed. But if large-scale systems such as the extent of continental Europe were to be operated with very high instantaneous solar PV or wind penetration (levels above 70-80%, reached in Phase 4), either new technical inverter capabilities would need to prove their effectiveness or additional investment in synchronous condensers would be needed.

**Figure 11 ASEAN – Shares of different generation technologies in energy and services needed to maintain electricity security**




IEA. All rights reserved.

Source: IEA ASEAN Renewable Energy Integration Analysis.
Note: Flexiblity calculation is based on hourly ramp capabilities of the fleet.

## Ensuring the availability of sufficient dispatchable resources has become the major test for ensuring power system reliability

While coal and oil are increasingly pushed out of the system because of carbon emissions and related financing constraints, the role of the other main fossil fuel

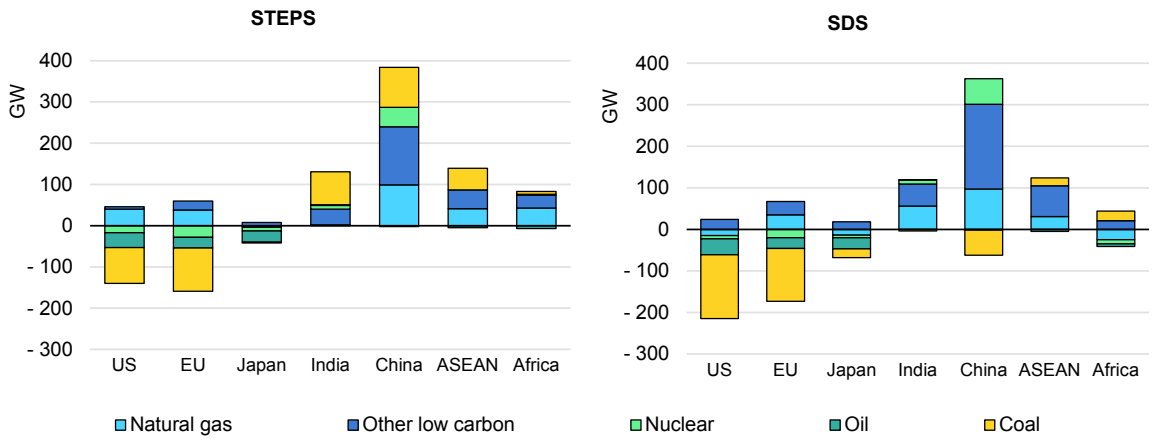


IEA. All rights reserved.

generation technology – gas – remains strongly debated. New gas plants often take a prominent place in electricity mix scenarios as a flexible resource that can be commissioned in relatively short time frames and that has a lower carbon footprint compared to coal and oil alternatives. Power-to-gas technologies also have the potential to further reduce or eliminate net $CO_2$ emissions from gas generation by using green gas as a fuel. This is without prejudice to the role of biomass (upscaling limitations), nuclear energy (not cost-effective at lower utilisation) or hydro (geographical constraints and resource limitations) in general. Public debate often centres around diverging opinions on whether gas is needed in a low-carbon mix, and whether it is a transition fuel or an impediment to ever reaching a fully decarbonised electricity system.

Policy makers should keep several considerations in mind. Bringing the net emissions of the entire economy to acceptable levels in time may not necessarily preclude a very limited share of emissions in the electricity system. Flexible gas peaker plants can provide security to a low-carbon system in a viable manner if the very low number of full load hours are remunerated accordingly. But low-carbon scenarios that rely on gas peaker plants should not expect such plants to materialise spontaneously under present market conditions. Acknowledging the role of gas (or other) fossil fuel plants in a secure low-carbon mix should be focused on ensuring adequacy and complement and facilitate the deployment of low-carbon technologies. Policy debate rightfully needs to scrutinise whether capacity remuneration mechanisms that are open to carbon-intensive sources are designed and implemented in such way.

**Figure 12 Dispatchable generation capacity, net additions by technology, 2030**




IEA. All rights reserved.

Notes: STEPS = Stated Policies Scenario. SDS = Sustainable Development Scenario. Other low carbon includes geothermal, concentrated solar power, biomass and marine.
Source: IEA World Energy Outlook 2019.



IEA. All rights reserved.

Evidently allowing for some level of carbon emissions in the electricity system increases the burden on other already hard-to-abate sectors such as industry and transport. This makes it a fundamental policy question as it balances efforts in other sectors and considers an element of risk hedging. Future breakthroughs in battery storage, the viability of renewable synthetic fuels and the scaling up of demand flexibility may eventually reduce or replace the need for gas plants as known today, or they may not.

# Technology shifts

## Reliance on gas for generation adequacy creates an intimate link between electricity supply security and gas deliverability

In many electricity systems the energy transition goes hand in hand with a rising share of variable renewables (wind and solar) and reduced fuel diversity of flexible electricity generation (due to coal, lignite and nuclear phase-outs). This increases the reliance of the power system on gas-fired power plants during peak demand with simultaneously low wind and solar generation.

Consequently, the role of gas-fired power plants for providing supply flexibility will become increasingly important, creating a more intimate link between security of electricity supply and natural gas deliverability. This makes it necessary to assess the deliverability of the gas system, especially when considering declining domestic production and potential closures of gas storage sites.

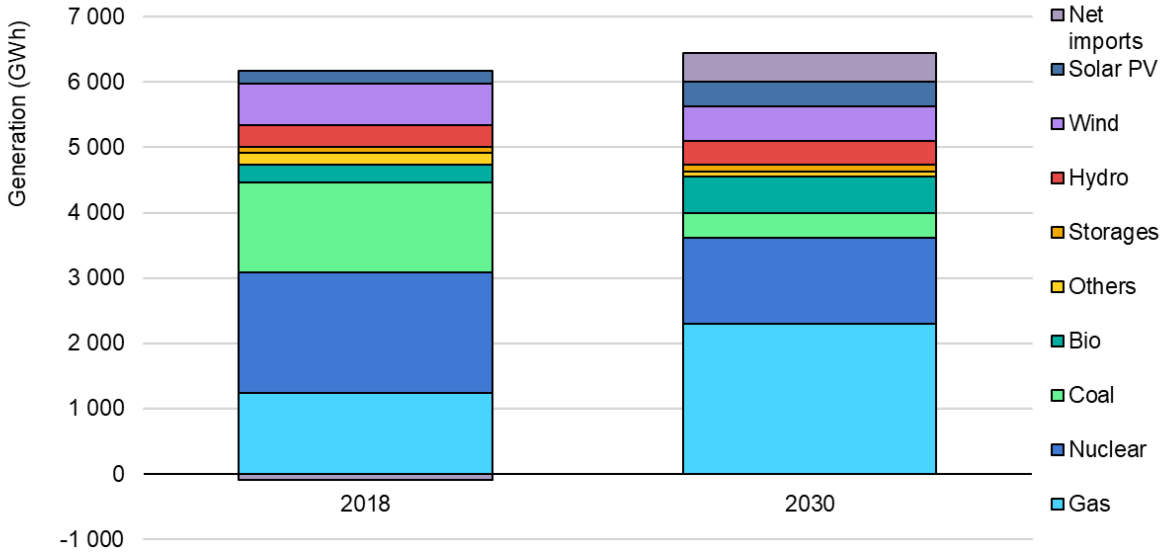
The European Union's energy system will see an acceleration of the transition described above over the next decade, with solar PV and wind doubling their current annual supply, whilst coal and nuclear generation will practically halve during the same period.

Gas-fired generation will become crucial to meet peak demand in extreme weather events – about 85% higher than during the peak in 2018, with a corresponding increase in demand for natural gas.



IEA. All rights reserved.

**Figure 13 North West Europe's peak supply days in 2018 and 2030**




IEA. All rights reserved.

## Digitalisation will come to the fore

Policy makers will need to update their catalogue of technologies that contribute to security of supply and properly address their contribution. They will also need to take advantage of the increased capabilities brought by digitalisation to keep the cost of security of supply down while we electrify other final uses of energy, such as transport and heating.

From an operational point of view, digitalisation and new capabilities brought by technologies such as batteries will expand the toolbox that policy makers and system operators can use to maintain security of supply. Increasing digitalisation has the power to mobilise an array of end-use devices to respond to the power sector's needs, increasing or reducing loads at times of distress. Some power systems, such as in Great Britain, already use batteries storage devices to minimise the damage of sudden outages, injecting almost instantaneously the power needed to avoid cascade events. This was one of the resources that prevented a full-black system event in August 2019. Distributed resources can also be used to support recovery in a black system event and provide a basic level of supply to essential services in cases where towns are electrically "islanded". Technology is already capable of providing many services, and regulation, interconnection standards and grid codes will require updating to take advantage of all the capabilities of existing assets.



IEA. All rights reserved.

In the coming years, deep electrification will require us to take advantage of digitalisation to control an array of electrical devices could reduce their consumption following price signals or technical orders linked to stress on the system.

With the exception of load shedding and calls to voluntarily reduce their consumption, customers have been isolated from almost any interaction related to relieving stress on the system. Following the same approach with high levels of transport and heating electrification would be onerous and wasteful, as technology is already capable of controlling an array of non-critical devices via external telecommunications protocols.

## New technologies like storage, VRE and electric vehicles will change our concept of security of supply

This new stocktaking will also be essential to ensure the long-term availability of resources and adequacy. Larger interconnected electricity systems can smooth out part of the variability of demand and solar PV and wind generation by using geographical diversification. New methodologies are needed to assess the adequacy of a large-scale system with variable sources and more active demand fluctuations. Policy makers need to take into account the extent of the smoothing effect in an interconnected system.

Wind and solar PV outputs have some complementary patterns in particular regions. Offshore wind specifically has relatively high capacity factors, suggesting the extent to which it can be dispatched to follow demand patterns. Large areas see more stable wind generation compared to individual sites. There is, however, a limit to such smoothing effects. Dispatchable generation, storage and more intelligent use of grids and flexible demand will become essential at some point. Extreme and rare situations also need to be planned for, as illustrated in Japan where a large-scale typhoon would cause a major proportion of wind turbines in the country to become unavailable at the same time.

Battery technologies and demand response are growing in capacity and capability, and can play a substantial role in integrating variable renewable generators. These options are effective in providing short-term flexibility and absorbing fluctuations on a minute or hourly basis, although they are not suitable for medium- to long-term energy storage (weeks to months). Many countries experience several consecutive days of low wind speed or rain and heavy cloud. Such weather conditions have not become major obstacles for power supplies thanks to contributions from other flexible power generation sources and electricity trade



IEA. All rights reserved.

with neighbouring regions. Reservoir and pumped storage hydropower are an important source of short- and medium-term energy storage in regions with resource availability. Adding new pumped storage capacity to existing facilities can be an avenue for development where existing resource potential is largely exploited.

Emerging technologies, such as power to hydrogen or biomethanation, have the potential to serve as sources of long-term flexibility, including seasonal. There is, however, still the need for technological development to de-risk their application on a commercial scale if they are to provide the seasonal storage buffer that high-VRE systems need when they enter Phases 5 and 6. These challenges are subject to today's technological availability. Breakthroughs in various key technologies could foster secure electricity supply with very high shares of wind and solar PV in the coming years at a reasonable cost. As long as innovation uncertainty exists in the power system transformation, however, realistic solutions need to be pursued as a technological hedge against such uncertainty. Expanding variable renewable deployment and ramping up innovation efforts are no-regret actions that are essential to steer our energy trajectory onto a sustainable and secure future path. In parallel, governments should make maximum effort to securing diversity in their low-carbon power generation mix by considering measures such as:

- developing hydropower sources, including the refurbishment and upgrade of existing plants to include pumped storage options where possible
- maintaining existing nuclear capacity by lifetime extensions and continuing research into new technologies such as small modular reactors
- expanding the use of sustainable biofuels and biogas in power generation
- pursuing a true transition to synthetic and low-carbon fuels and gases.

A technology-neutral approach should be adopted in policy measures to establish a low-carbon electricity system. And power market designs need to reward not only energy, but also flexibility and adequacy contributions to the entire system. During the period when technological progress or capital resources do not allow for the full decarbonisation of the electricity system, using coal- or gas-fired power plants solely for flexibility purposes or emergency reserves could be options to take advantage of their capacity, if this fits into a wider energy and economy decarbonisation strategy.

From a purely technical and cost perspective, all fuels and all technologies should be considered for achieving a sustainable energy path in all sectors. But the



IEA. All rights reserved.

electricity generation mix should lead the way since it will still be the major source of flexibility.

# New planning tools and incentives

## New technologies need new planning tools. Probabilistic analysis provides better security-of-supply assessment

Policy makers, regulators and system operators can improve the accuracy of their adequacy assessments by moving away from deterministic methods, such as planning reserve margin, and developing probabilistic simulations of the variability and interdependence of outcomes in their systems. Through simulations, decision makers gain a deeper understanding of system elements by valuing their contribution to adequacy, including:

- VRE variability
- outages for generators and transmission lines
- regional interconnection availability
- system reserve margins and main system contingencies
- load variability
- demand response.

In a simulation approach, generation and transmission outage statistics can be combined with a detailed representation of the physical topology of the system. Possible outcomes can be simulated for many different random patterns of outages of all technologies. This provides a more accurate answer compared to considering each piece of infrastructure separately, and it gives a picture of the statistical spread of possible outcomes.

Simulations also allow for deepening the analysis further, for example to account for time-based variation of the likelihood of generator or transmission outage based on the local weather conditions. Larger regions can also be represented, allowing the reliability contribution of interconnected areas to be understood. Different areas may be stressed under similar conditions, in which case a limited contribution to reliability is a given. However, as areas typically have a different energy mix and load profile, and see a smoothing effect in aggregated VRE, interconnections will often provide increased adequacy. Operating reserve margins are another area that deserves close consideration, including dynamic reserve sizing that takes into account load, variable generation and the largest contingencies in the system.



IEA. All rights reserved.

## Market design should translate stress periods in the power system into higher wholesale prices

In an evolving system, the services needed to retain security of supply will also evolve. It is more important than ever to verify that the participants in the power sector are given the right incentives to supply not only clean energy, but also services such as net peak load capacity, flexibility and reserves.

To ensure secure operation, governments and regulators should define an acceptable level of supply interruption. While doing this, policy makers must consider the value that customers place on electricity, and the economic and social impact of limited outages. This is the role of reliability standards. Then regulators need to create market and investment frameworks that can bring the desired level of security. Markets have to deliver not only peak capacity as in traditional power systems, but also all the services needed to ensure secure operation of the system.

Energy-only, energy plus capacity and centrally planned systems approach the incentives for achieving the desired level of security by either setting them administratively or leaving them to market forces. A major point of attention for policy makers in any of the three approaches is to ensure that all forms of flexibility in the system are recognised and can provide system services in an economically sensible manner to minimise overall system costs.

This is particularly relevant when dispatchable capacity expects to be used infrequently – the asset's fixed costs must be compensated either through the margin gained on energy sales during the relatively small number hours in which the unit operates or provides reserves, or through a capacity payment. The energy-only option needs to allow strong energy price signals to avoid the "missing money" problem that occurs when price caps discourage worthwhile investments. Alternatively, whenever a decision is taken to add capacity mechanisms in a liberalised market, careful consideration needs to be given to all possible cost-related impacts, the true verifiable reliability improvements and possible lock-in situations.



IEA. All rights reserved.

# Cyber resilience

## Introduction

### Digitalisation brings many benefits to the electricity system, but raises risks to cybersecurity

Digital technologies offer an array of opportunities to benefit electricity consumers, utilities and the system as a whole, including improved efficiency, cost savings and shorter outage times. They could also help to accelerate clean energy transitions. Connected devices and the Internet of Things, together with other smart grid technologies, can unlock larger demand response resources, improve energy efficiency, and facilitate the integration of higher shares of variable renewables in a cost-effective and secure manner.

The number of connected devices (e.g. smart thermostats and appliances) is growing rapidly, with the global stock projected to double over the next five years to reach 30-40 billion devices by 2025.

However, the growth in connected devices and distributed energy resources – such as distributed generation, electric vehicles and behind-the-meter storage – is expanding the potential cyberattack[1] surface of electricity systems. Increased connectivity and automation throughout the electricity system could also make them more vulnerable to cyberattacks.

A successful cyberattack could trigger the loss of control over devices and processes, in turn causing physical damage and widespread service disruption. In addition to the impacts on critical services, households and businesses that rely on electricity, an attack could result in millions or even billions of dollars in damages for electric utilities, including the costs of dealing with the cyberattack (i.e. detection, investigation, containment and recovery) and its consequences (e.g. from business disruption, information loss, revenue loss and equipment damage).

[1] This report uses the "cyber" prefix to discuss digital security and resilience issues related to intentional and malicious attacks and incidents on the electricity system (e.g. cybersecurity, cyber resilience, cyberattack, cyber risk). The report does not cover unintentional incidents or broader digital security issues such as data privacy. The intent of this report is to provide broad guidance to energy policymakers and companies to enhance resilience in the electricity sector, and does not go into technical details or cover national security issues.



IEA. All rights reserved.

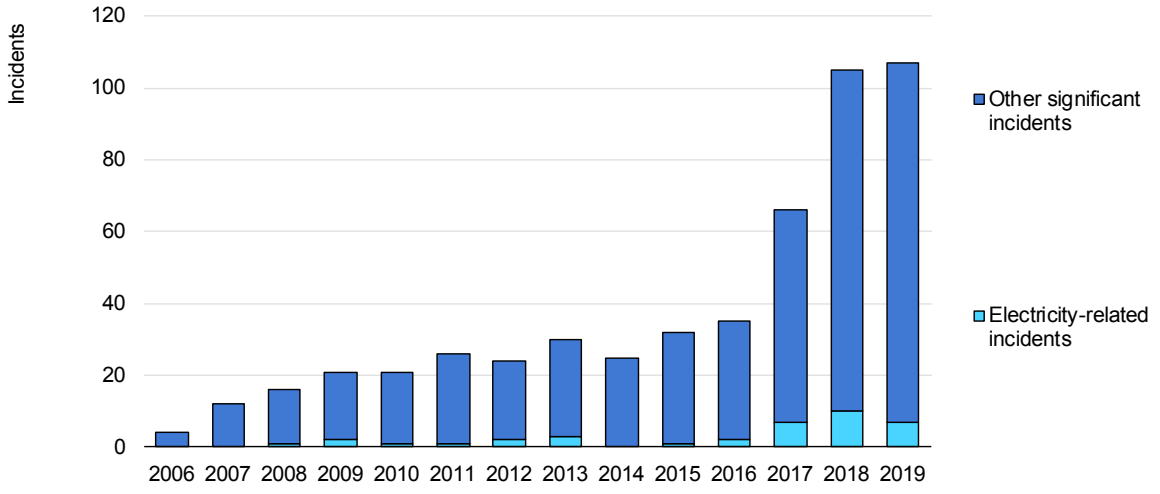
# Enhancing resilience

## The substantial and growing threat of cyberattack warrants strong action to enhance resilience

Cyberattacks are among the top ten global risks in terms of likelihood and impact according to the World Economic Forum's Global Risk Report 2020. For electricity systems, the threat of cyberattack is substantial and growing, and threat actors are becoming increasingly sophisticated at carrying out attacks – both in their destructive capabilities and their ability to identify vulnerabilities.

However, measuring and tracking the risks and impacts are difficult. The first hurdle is the lack of comprehensive publicly available data on cybersecurity incidents. The second is that many incidents may not be reported at all – even to regulators or other authorities – and some attacks may even go undetected. And third is the difficulty of overcoming major differences in scope and definitions, such as what constitutes an "incident" or "attack". For example, a global database tracking "significant" cyber incidents shows the number of incidents has increased dramatically in recent years, including in the electricity sector.

**Figure 14 Significant cyber incidents worldwide, 2006-19**




IEA. All rights reserved.

Note: "Significant" cyber incidents are defined here as cyberattacks on government agencies, defence and high-tech companies, or economic crimes with losses of more than a USD 1 million.
Source: IEA analysis based on CSIS (2020).

Disruptions to electricity systems because of cyberattacks have so far been small compared to other causes, such as power outages from storms, equipment failure or operational errors. The 2015 attack on the western Ukraine power grid was the



IEA. All rights reserved.

first confirmed cyberattack specifically against an electricity network with impacts on system availability. Attackers accessed and manually switched off substations, resulting in 30 substations going offline and 225 000 people losing power. Despite the limited extent of disruption to date, there are plausible scenarios where cyberattacks could cause substantial harm to electricity systems.

While full prevention of cyberattacks is not possible, electricity systems can be designed to be more cyber resilient – to withstand, adapt to and rapidly recover from incidents and attacks, while preserving the continuity of critical infrastructure operations. The capacity to adapt to new technologies – as well as to new risks and threats – is key. Policy makers, regulators, system operators and industry across the electricity value chain all have important roles to play in enhancing the cyber resilience of the system.

## Enhancing cyber resilience is a continuous process, and the collective responsibility of all stakeholders across the electricity value chain

The fundamental principles of cyber resilience, such as embedding a culture of cyber resilience within the organisation and implementing risk management strategies, are generally applicable across a variety of sectors and industries. However, they need to be tailored to account for sector-specific characteristics and needs. In the electricity sector, these include:

- real-time requirements for and expectations of very high availability
- interdependencies and cascading effects within and across systems
- a mix of new technologies and legacy assets with long lifetimes.

Enhancing resilience in the electricity sector should also be considered within the broader context of enhancing resilience across all other critical infrastructure and services, including water, transport, ICT, health and finance.

Enhancing the cyber resilience of electricity systems is a continuous process generally involving several stages: 1) identifying and assessing risks and preparedness; 2) implementing a risk management strategy to prioritise risks and actions; 3) in the event of an attack, following robust response and recovery procedures; 4) documenting and incorporating lessons learned from past incidents; and 5) sharing knowledge with other stakeholders. Because cyberthreats are constantly evolving, all organisations need to continuously monitor and evaluate their vulnerabilities and risk profiles and take appropriate action. For example, some organisations may need to exercise effective threat



IEA. All rights reserved.

hunting and cyberthreat intelligence activities to prepare for high-end threats from highly capable and motivated attackers.

## Cyber resilience needs to be integrated into organisational culture

Cyber resilience activity needs to be integrated into the culture of the organisation and rather than being considered as a separate, technical issue. Without this integration, organisations could fail to address the challenges that come with digital transformation in a holistic, appropriate and consistent way.

In the event of an attack, it is crucial that organisations follow robust response and recovery procedures while documenting and incorporating lessons learned from past incidents. Cyber resilience is a combination of preventive and corrective measures, building on lessons learned after a cyberattack. Reflecting on past attacks can inform the implementation of new measures, as well as reinforce or redesign existing ones as needed. Equally important is communication with external stakeholders in order to improve the threat awareness of the community and to help detect blind spots and vulnerabilities.

Actions by policy makers, regulatory authorities, regulated entities and other stakeholders can enhance cyber resilience across the electricity system and ensure appropriate measures are implemented. Many tools and frameworks are available to provide guidance on and support resilience-building efforts.

**Table 4 Overview of potential actions to enhance cyber resilience**

| Stakeholder | Potential actions to enhance resilience |
|---|---|
| Utilities | • Incorporate cyber resilience into the organisational culture and integrate cybersecurity considerations into enterprise risk management frameworks.<br>• Identify and assess risks and implement a risk management strategy to prioritise areas of action.<br>• Implement robust response and recovery procedures to help maintain operations in the event of a cyberattack, with clearly allocated responsibilities.<br>• Improve existing measures and implement new ones based on lessons learned internally from past incidents, and from external organisations via information sharing and analysis centres (ISACs) or knowledge-sharing platforms.<br>• Exercise threat hunting and cyberthreat intelligence activities to prepare for high-end threats from highly capable and motivated attackers. |
| Equipment suppliers | • Participate in certification programmes to increase trust and security in products, processes and services.<br>• Focus cybersecurity standards on risk management approaches and the processes by which security is maintained once equipment is commissioned.<br>• Promote co-operation to avoid potential fragmentation that might be expected from having different regulators and supervisory bodies. |



IEA. All rights reserved.

| Stakeholder | Potential actions to enhance resilience |
|---|---|
| Policy makers and regulators | • Understand cybersecurity risks and communicate effectively to raise awareness.<br>• Apply or adapt existing tools and guidance for key stakeholders.<br>• Exercise caution when using assessments to compare different organisations.<br>• Develop policies that foster sector-wide collaboration and response procedures.<br>• Set up research partnerships with industry and academia to foster R&D on cyber resilience in electricity.<br>• Facilitate and incentivise the sharing of best practices and vulnerabilities through workshops, bulletins, training, on-line communities, etc.<br>• Provide direction and assistance in setting up ISACs, and participate in international ISACs. |

# Policy and regulatory approaches

## Setting effective cyber resilience regulation is a delicate balancing act between enforcement and innovation

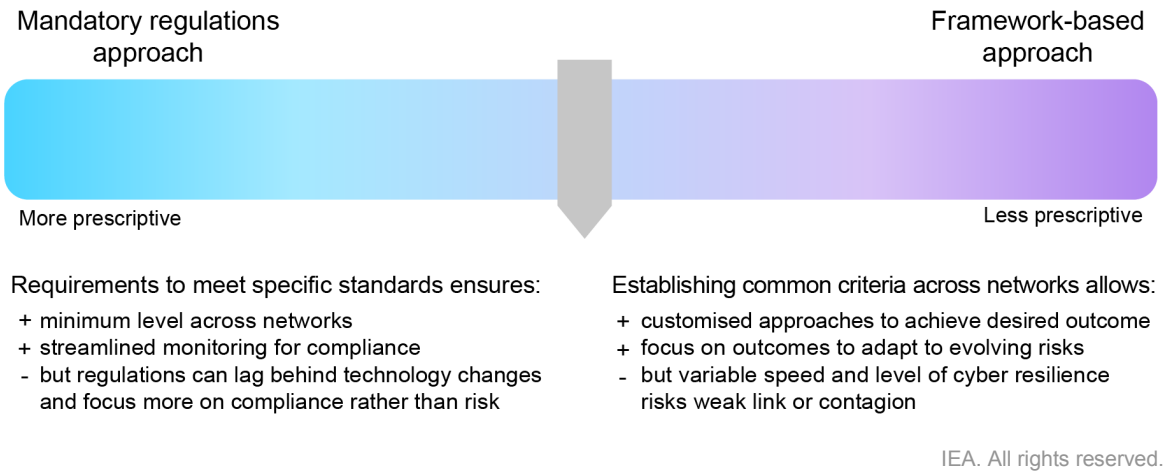
Around the world a number of evolving policy approaches to cyber resilience have already been adopted. These can be categorised on a scale ranging from highly prescriptive approaches with specific mandatory requirements, to less prescriptive performance-oriented framework-based approaches.

A more prescriptive approach entails a detailed set of implementation requirements, monitoring and reporting based on predefined standards, fixed into regulatory, licensing or prequalification requirements. A prime example of this approach are the cybersecurity regulations implemented in the United States through the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. The advantage of such approaches is that they allow for more streamlined compliance monitoring. But, they can face pushback as industry see itself as too burdened by reporting requirements. Furthermore, there may be mismatches between the cycles of hardware, cybersecurity software and regulations. Regulatory updates that recognise technology changes and keep pace with evolving cyber risks are necessary.



IEA. All rights reserved.

**Figure 15 The spectrum of cyber resilience approaches**




IEA. All rights reserved.

Less prescriptive, principle-based, performance-based or framework-based approaches are those that broadly indicate the structure of actors and safeguards that are to be put in place to secure the electricity network. Principle-based approaches aim to fulfil security principles while giving the operator some freedom when implementing the measures. Performance-based approaches, by contrast, are based on a number of metrics to assess the progress or the quality of implementation. Regulators can define specific target metrics, such as achievement of specific standards or time required to address a service disruption, leaving it to the operator to decide on the specific measures that will cost-effectively satisfy these metrics (NARUC, 2020).

An example of a framework-based approach is one adopted recently by the European Commission through the NIS Directive and follow-up legislation on the security of network and information systems. This particularly allows for different approaches and implementation speeds across jurisdictions, which has raised questions around how to establish a coherent and robust transnational approach to cybersecurity with tangible and effective impact. Moreover, as the NIS Directive is a cross-sector framework, it requires further measures to be implemented effectively in each sector. In the coming years, updates to grid codes are expected to bring more clarity as to concrete actions that can be implemented at the transmission and distribution level.

When the approach remains too conceptual and policy strategies have limited actual impact in mitigating risk exposure, the system is de facto depending on the voluntary initiatives of all electricity organisations active in the sector. A lot can already be achieved this way, and many countries and individual organisations have made enormous progress over the past decade. Policy intervention will be



IEA. All rights reserved.

essential to ensure appropriate minimum security requirement levels are set for all actors, to overcome conflicts between operators and manufacturers, to nurture information sharing and to achieve international collaboration. Policies should not necessarily aim to bring every organisation to the same security level, nor to bring every organisation to the level of the most advanced one. However, weak spots need to be avoided in a system that is digitally, electrically and supply chain interconnected.

Prescriptive requirements evidently give the benefit of being very clear on who needs to do what. However, the scope of application set by an authority may simply follow from its own powers and may not necessarily be optimal. The case of NERC CIP in the United States provides an interesting example. While being clear on what applies to all bulk electricity system utilities, it does not cover smaller entities simply because they do not fall under NERC's jurisdiction rather than being a rational choice. When devising policies to ensure cyber resilience in the power system, policy makers should ensure they instigate ecosystem-wide resilience, covering all actors interacting with the power system and their interlinkages rather than only network or system operators.

## Implementation strategies should be tailored to national contexts while considering the global nature of risks

In addition to the choice of regulatory instrument for cyber resilience, there is the question of implementation. For more prescriptive approaches, a compliance-based strategy or checklist can be helpful in linking specific measures with known security risks. However, such approaches run the risk of becoming too focused on ticking boxes to meet the requirements, as well as facing the issue of a lag between technological change and the pace of regulatory change. Alternatively, prioritisation criteria can be applied as a sort of iterative risk assessment, identifying the logical next steps to make the system more secure. Such implementation may lend itself to more dynamic cyber resilience policies, but, as with performance-based regulations, may lack a clear direction or baseline for threat prevention, complicating evaluations of effectiveness or cost recognition by regulators.

There are inherent differences in the implementation of these general approaches, stemming partly from institutional contexts, for example differences in regulatory jurisdictions. This makes direct comparison difficult. While being the examples most often referred to, the United States and the European Union are certainly not the only jurisdictions developing policy frameworks for cybersecurity. Countries around the world, such as Australia, Brazil and Japan, show that it is possible to



IEA. All rights reserved.

enact mixed approaches, borrowing on the strengths of both general approaches, but tailoring implementation closer to the realities of very diverse power systems.

Despite these differences in implementation, however, there is a degree of scope for establishing common approaches to cyber resilience. This is particularly important both because of the global nature of vulnerability to cyberattacks, and because many original equipment manufacturers supply globally, so once a vulnerability is identified in standard equipment it could be exploited in other power systems. For policy makers, this implies co-ordinating with and establishing guidelines for equipment manufacturers.

While policies can enforce a compliance check for the implementation of measures, a true outcome-based approach does not exist specifically for cybersecurity, in contrast to conventional electricity quality of service regulations (for grid development, regulated tariff setting and general SAIDI or SAIFI[2] targets). It remains questionable whether an outcome-based approach can be fully relied upon as a reasonable strategy for the resilience of critical infrastructure. The situation differs from that in grid development, where an investment can be motivated by system modelling analysis showing reduced operational costs or higher reliability, and where the actual impact on grid losses or interruption durations can be measured. A cyber resilience investment can hardly ever be weighed against a monetisable benefit or proven to be effective in retrospect by demonstrating prevented attacks. It is exactly because simply setting targets is not a realistic option that cybersecurity policies for the electricity sector are a complex issue for policy makers.

## It is essential to ensure resilience at the grid edge and across the entire electricity system value chain

As electric vehicles, other behind-the-meter distributed energy resources, and connected devices become more prevalent, the potential for cyberattacks to cause significant disruption to electricity systems could grow. A recent study demonstrated that a targeted attack on personal electric vehicles and fast-charging stations using publicly available data could cause significant disruptions to local power supply. Another study demonstrated how high-wattage devices connected to the Internet of Things, such as air conditioners and heaters, could be used to launch large-scale co-ordinated attacks on the power grid, resulting in local power outages and, in the worst cases, large-scale blackouts.

[2] System average interruption duration index and system average interruption frequency index.



IEA. All rights reserved.

Research is underway in the United States to better understand the potential vulnerabilities of distributed energy resources, and to develop early warning systems and response algorithms to protect power supply. These efforts are particularly important following the enactment of the latest Rule 21 guidelines in California, which require all new solar and storage installations to use smart inverters with remote connectivity, a regulatory trend that is taking place in many power systems around the world.

Protection systems in end-consumer devices are often beyond the typical scope of energy ministries or energy regulators. Their regulation may lie with other government bodies such as consumer protection authorities, public safety and civil protection bodies, energy efficiency departments and even special agencies for IT security as is the case in Germany and France. In this sense, it is important for energy policy makers to engage across various government levels as well as with manufacturer associations and standards bodies to understand the potential risks to the system and how best to address them efficiently and effectively.

In addition, it is important to foster supply chain robustness to ensure that manufacturers have access to reliable, secure components, and that utilities, system operators and grid users have the means to track the security-readiness of the assets and systems they deploy. This applies equally to electricity grids, consumer-facing technologies, and industrial and commercial processes. As companies become increasingly interdependent for industrial and service processes, it is important to build supply chain resilience. Policy makers should ensure that there are platforms for industries and businesses to validate, communicate and improve on any potential cyber-related vulnerabilities in the supply chain. A further important consideration for policy makers is whether this is steered via transparency and trust, or if this is enforced by certification, incentives and penalties.

## Policy makers can play a key role in enhancing cyber resilience across the electricity system

The electricity system has a unique set of operational conditions and requirements, vulnerabilities and solutions compared to other sectors. Enhancing the cyber resilience of electricity systems warrants tailored policies and strategies.

Energy policy makers have a critical role to play in enhancing cyber resilience across the electricity system, beginning with raising awareness and working with stakeholders to continuously identify, manage and communicate emerging vulnerabilities and risks. Policy makers are also well placed to play a central role



IEA. All rights reserved.

in facilitating partnerships and sector-wide collaboration, information exchange programmes and research initiatives across the electricity sector and beyond.



IEA. All rights reserved.

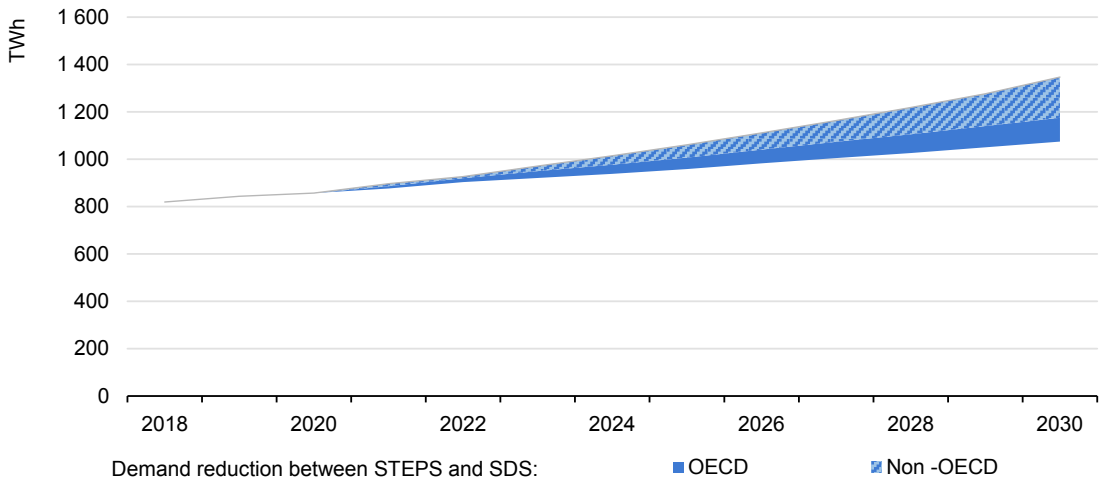
# Climate resilience

## Introduction

### The electricity system is witnessing increasing pressure from climate change

Climate change is resulting in rising global temperatures, erratic patterns of precipitation, sea level rise and more frequent or intense extreme weather events. This has significant implications for electricity security. For generation, the impacts of climate change can reduce the efficiency and alter the availability and generation potential of power plants, including both thermal and renewable facilities. Climate change impacts on transmission and distribution networks can result in higher losses, changes in transfer capacity and particular physical damage. It is also expected to increase electricity demand for cooling in many countries, which will become a driving factor for generation capacity additions.

**Figure 16 The projected growth in residential space cooling demand from 2018 to 2030 under IEA scenarios**




IEA. All rights reserved.

Notes: STEPS = Stated Policies Scenario. SDS = Sustainable Development Scenario.
Source: IEA (2020), Energy Technology Perspectives 2020.

Increasing anomalies in climate patterns already pose a significant challenge to electricity systems and increase the likelihood of climate-driven disruption. In many countries the increasing frequency or intensity of extreme weather events such as heatwaves, wildfires, cyclones and floods are the dominant cause of



IEA. All rights reserved.

large-scale outages. The recent outages due to wildfires and heatwaves in California and Australia demonstrate that electricity systems are already exposed to and largely affected by climate hazards. In the United States the share of extreme weather events attributable to large-scale outages (affecting at least 50 000 customers) over the past two decades has been on average 90%, with at least 75% across the period and all (if not almost all) of the events in certain years.

**Table 5 Overview of main potential impacts on the electricity system due to long-term climate trends and extreme weather events**

| Climate impact | Generation | Transmission and distribution networks | Demand |
|---|---|---|---|
| Rising global temperatures | • Efficiency<br>• Cooling efficiency<br>• Generation potential<br>• Need for addition | • Efficiency | • Cooling & heating |
| Changing precipitation patterns | • Output & potential<br>• Peak & variability<br>• Technology application | • Physical risks | • Cooling<br>• Water supply |
| Sea-level rise | • Output<br>• Physical risks<br>• New asset development | • Physical risks<br>• New asset development | • Water supply |
| Extreme weather events | • Physical risks<br>• Effiiciency | • Physical risks<br>• Efficiency | • Cooling |

The increasing adverse impacts of a changing climate on electricity systems highlight an urgent need for action by policy makers, utilities and relevant stakeholders around the world to enhance their systems' resilience to climate change. Adoption of climate resilience not only reduces damage and loss from climate impacts, but also supports clean energy transitions, which themselves can limit future adverse climate change by deploying low-carbon energy technologies.



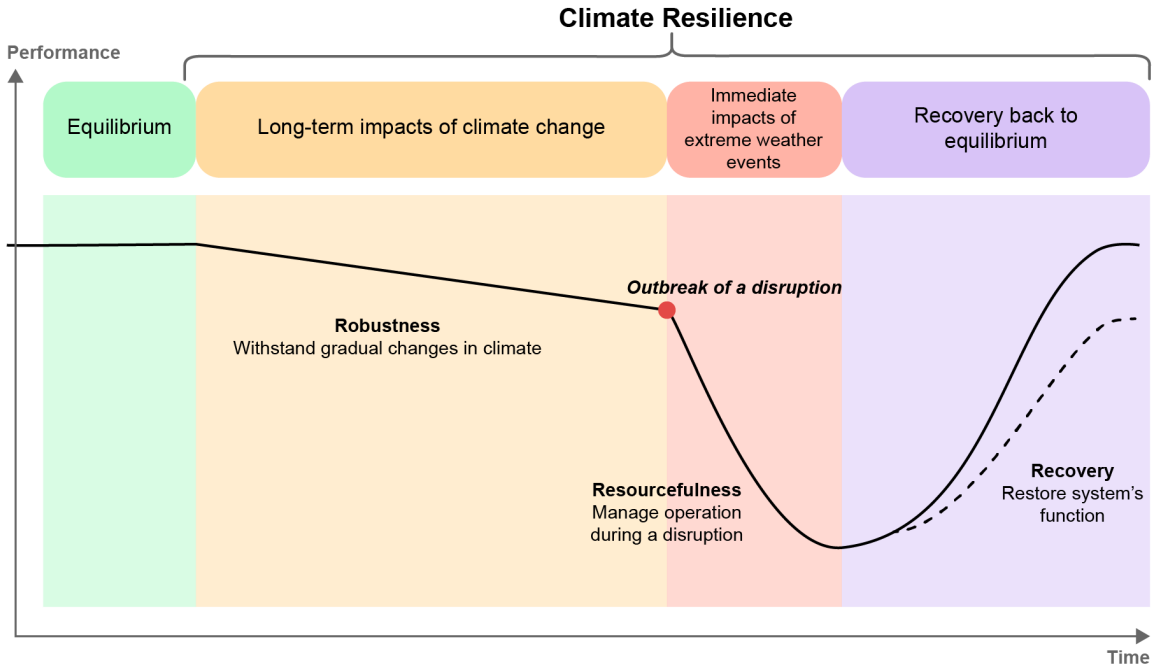
IEA. All rights reserved.

# Benefits of climate resilience

## Climate resilience of electricity systems addresses adverse impacts of climate change.

**Climate resilience** in general is the ability to anticipate, absorb, accommodate and recover from the effects of a potentially hazardous event related to climate change. A more specific conceptual framework for the climate resilience of the electricity system can help policy makers better identify climate resilience as an element of electricity security. It delineates the key dimensions of an electricity system's climate resilience – robustness, resourcefulness and recovery.

**Figure 17 Conceptual framework for climate resilience of the electricity system**




IEA. All rights reserved.

Sources: Argonne National Laboratory (2012), Resilience: Theory and Applications (ANL/DIS-12-1), as modified by International Energy Agency.

Robustness is the ability of an energy system to withstand the gradual long-term changes in climate patterns and continue operation. For example, thermal power plants that use recirculating water for cooling could be more resilient to increasing temperatures than those that use external sources such as rivers or lakes.



IEA. All rights reserved.

Resourcefulness is the ability to continue operation during immediate shocks such as extreme weather events. For example, a hydropower plant with a flood control reservoir is more likely than others are to sustain a minimum acceptable level of operation in the face of floods.

Recovery is the ability to restore the system's function after an interruption resulting from climate hazards. A more resilient electricity system with a well-coordinated contingency plan for communications, temporary assets and workforce will recover faster from the interruptions caused by climate impacts.

## More resilient electricity systems reduce damage and loss from climate impacts

Recent studies suggest that the benefits of resilient electricity systems are much greater than the costs in most of the scenarios considering the growing impacts of climate change. It is estimated that for every dollar invested in climate-resilient infrastructure, six dollars can be saved. According to the World Bank, if the actions needed for resilience are delayed by ten years, the cost will almost double.

For instance, underground transmission and distribution cables, which require a higher upfront outlay than above-ground systems, can significantly reduce potential damage from climate impacts and save recovery costs. Transmission and distribution lines above ground tend to be more vulnerable to climate hazards such as high-speed winds, wildfires, floods and landslides, than underground systems. When storm Gudrun hit Sweden in January 2005, outages in rural areas lasted up to 20 days due to the damaged distribution lines, while those in urban areas with underground cabling lasted only a few hours. Due to the lengthy outages, Swedish network operators lost around EUR 250 million. Moreover, the socio-economic losses due to the interruptions were estimated at EUR 3 billion.

Governments can support efforts to reduce the damage and cost of climate impacts by introducing tailored measures aimed at the specific types of climate hazards they are facing. In California, where wildfires are a major threat, good forest maintenance can minimise the impacts of wildfires on transmission and distribution lines. In Bangladesh, a country highly prone to floods, USD 560 million for additional flood protection could save up to USD 1.6 billion in avoided damage.

## Adopting climate resilience measures contributes to sustainable development and clean energy transitions

The projected increase in climate hazards poses a major threat to meeting universal electricity access, which is one of the objectives of Sustainable



IEA. All rights reserved.

Development Goal (SDG) 7. According to the IEA World Energy Outlook 2019, about 840 million people around the world are still deprived of electricity access. Future changes in climate may significantly limit progress towards universal electricity access, which is one of the objectives of Sustainable Development Goals (SDG), by restricting resource availability, reducing generation and transmission efficiency, and increasing possibilities of outages.

In Zambia, for instance, where only 30-40% of the population have access to electricity (World Bank, 2020), the electricity system is already adversely affected by climate change. A shorter rainy season and more frequent droughts are posing a challenge to hydropower generation which currently accounts for more than 80% of electricity generation in Zambia. In February 2016 the water levels of the Kariba Dam, the biggest electricity source of Zambia, dropped by 88%, prompting blackouts, power rationing and a slowdown in economic development in some places. The disruption occurred again in August 2019, when the Kariba station needed to reduce output and impose daily blackouts. The adoption of climate resilience measures, such as an improved system for monitoring climate hazards and a strategy for diversifying the electricity generating mix, would help Zambia to ensure reliable access to power networks.

Electricity plays a critical role in the transition to a low-carbon energy system. A lack of resilience in electricity systems can also obstruct clean energy transitions, as some renewable energy technologies could be sensitive to a changing climate. This is especially the case in countries whose electricity infrastructure is vulnerable to changes in climate and extreme weather events.

# Policy measures

## Effective policy measures prevent potential market failure in building climate resilience

The benefits of climate resilience and the costs of climate impacts tend to be distributed unevenly across the electricity value chain. It inevitably raises the question of who should be responsible for delivering resilience measures and pay for them.

In principle, power sector businesses have responsibility and direct interest in protecting their own assets and providing reliable services to their customers. While some utilities have taken efforts to align their business interests with climate adaptation efforts, there are several factors that may deter some from adopting resilience measures in practice.



IEA. All rights reserved.

First, the benefits of investment in enhancing climate resilience are likely to become tangible only after a few years or even decades, while the capital cost of implementation is incurred immediately. Second, when climate impacts interrupt electricity supply and lead to large costs to society, generators and operators are expected to bear only a fraction of the entire social costs. Third, a lack of competition and the presence of monopolistic market conditions in some countries could discourage service providers from investing in climate resilience measures for enhanced quality of electricity services.

Therefore, policy makers need to fulfil a critical role in building resilient electricity systems by adopting effective policy measures that can prevent a potential "market failure", while collaborating with business.

## A higher priority should be given to climate resilience in electricity security policies

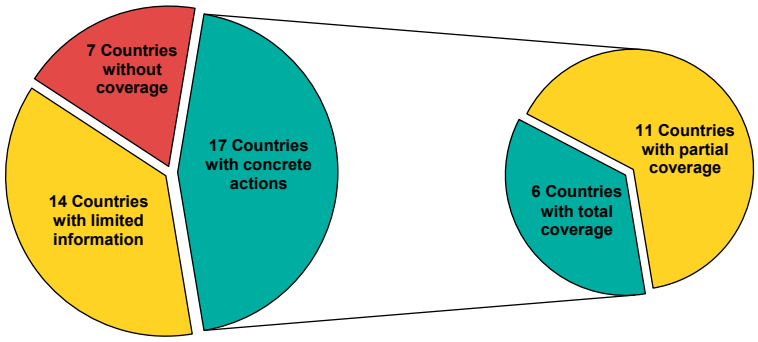
In many countries, the level of commitment and progress towards climate resilience in the electricity sector still lags behind. Even in countries where national strategies or plans for climate change adaptation are in place, the urgent needs of climate resilience in the electricity sector have been often overlooked.

Among 38 IEA family countries, 17 countries have included concrete actions for energy sector resilience to climate change in their National Adaptation Strategies or Plans. More than a half of IEA family countries have very limited or no information dedicated to climate resilience of electricity systems. Even among the 17 countries with concrete actions for climate resilience in the energy sector, some domains of the electricity systems are missing. Only 16% of IEA family countries have incorporated concrete actions for climate resilience of electricity systems into their national adaptation strategies, covering the entire electricity value chain.



IEA. All rights reserved.

**Figure 18 Coverage of the climate resilience of electricity systems in National Adaptation Strategies and Plans, IEA family countries**




IEA 2020. All rights reserved.

Countries that have not yet incorporated climate resilience as a core element of their national strategies and plans to adapt to climate change, need to act immediately. Mainstreaming climate resilience in energy and climate policies can send a strong signal, encouraging the private sector to consider climate resilience of electricity systems and address potential market failures.

Building a clear assessment framework for climate impacts and resilience is the first step to ensure all stakeholders properly understand projected changes in climate. After establishing a common assessment framework, policymakers need to send appropriate signals to essential service providers. They can encourage utilities to include climate resilience in their construction plans and operational regimes by mainstreaming climate resilience as a core element in their own long-term energy and climate policies. Identification of cost-effective resilience measures and creation of an incentivisation mechanism would also encourage utilities to adopt resilience measures. With supportive policy measures, businesses can implement resilience measures, such as physical system hardening, improvement in system operation, recovery planning, and capacity building.



IEA. All rights reserved.

# Recommendations

## These recommendations lay out the path towards a sound electricity security framework

Emerging trends in the electricity sector – namely the energy transition, cyber threats and climate change – will require a rethinking of traditional frameworks for ensuring electricity security. The good news is that policy makers, regulators, system operators and industry have a solid basis from which to build. The basic tenets of electricity security, embodied in existing practices for achieving operational security, adequacy and system resilience, can evolve to adapt to the trends of the future. Moreover, new technologies expand the set of tools that they can use to maintain security of supply.

Many countries have already started to put in place policies, rules and practices that address these major trends affecting their power sectors, offering important lessons. While each trend or threat to the system might require a specific, tailored security response, several overarching action areas can serve as the basis for achieving more appropriate electricity security frameworks for the future. These are as follows: institutionalising responsibilities and incentives; identifying risks; managing and mitigating risks; monitoring progress; and responding to and recovering from disruptions.

# Institutionalise

Establishing clear responsibilities, incentives and rules across the electricity system is imperative for ensuring security in the face of shifting trends and threats. In the case of power supply disruptions, regardless of their cause, a clear framework for assessing threats, communicating risks, allocating accountability and responding to incidents is an essential first step for ensuring the security of the electricity system. To this end, an important element in institutionalising responsibilities entails co-ordination and communication among all participants in the system, in particular to avoid overlapping responsibilities or actions. Relevant incentives need to be created for various actors throughout the electricity system to ensure compliance.



IEA. All rights reserved.

## Energy transition

- Regulators in restructured markets: assess constantly the market to ensure the market design is bringing the adequacy, flexibility and stability services needed for the secure operation of the system.
- System operators: update constantly the interconnection standards of new technologies.
- Policy makers: provide enough forward visibility of the policies affecting the power sector – considering inputs from other authorities and stakeholders into the process.
- System operators in jurisdictions relying increasingly on gas-fired plants as a flexibility resource: include gas-related contingencies in their adequacy assessments.
- Regulators: provide a clear framework to provide every power sector stakeholder with a clear set of obligations to prevent threats and to react in exceptional circumstances.
- Regulators: assign responsibilities for co-ordinated action between the operators of the transmission and distribution systems, including where systems are interconnected.

## Cyber resilience

- Policy makers: designate responsible authorities to set objectives, give direction on measures and assess their implementation.
- Policy makers and regulators: implement co-ordination mechanisms between responsible authorities (both within and outside the electricity sector) to avoid conflicts between various regulatory levels.
- Policy makers and regulators: incentivise or oblige regulated and non-regulated entities to implement cybersecurity safeguards. Measures should aim to improve outcomes, rather than relying only on compliance-based processes that risk becoming a box ticking exercise.The level of enforcement needs to relate to how critical the organisation is to wider system reliability. Positive incentives need to be considered to foster transparency, co-operation and co-ordination.
- Policy makers, regulators and industry: increase the level of awareness of the need for cyber resilience across the sector, including in electricity-related agencies and authorities.

## Climate resilience

- Policy makers: bring climate resilience into the mainstream as a core element of energy and climate plans and regulations.
- Policy makers and regulators, in collaboration with system operators: create long-term scenarios highlighting possible implications of changing weather patterns and extreme weather events for the security of electricity supply.



IEA. All rights reserved.

- Policy makers and regulators: create appropriate incentives for utilities to facilitate timely investment in resilient electricity systems.

# Identify risks

Identifying risks to the electricity system will be a central element of minimising and responding to them. Ensuring that critical risks are known, assessed regularly, prioritised and communicated to relevant actors is essential. To this end, system-level risk analyses should be conducted regularly by designated organisations to identify key threat scenarios and system vulnerabilities. These organisations should communicate the risks they identify to system actors and those actors should implement security protocols based on the level of risk assessed.

## Energy transition

- System operators: conduct regular adequacy-of-supply assessments, including appropriate methodologies adapted to new technologies, considering VRE variability and all system uncertainties.
- Regulators should ensure assessments cover the risks associated with dependence on specific fuel sources.

## Cyber resilience

- Policy makers and regulators: ensure designated organisations regularly conduct system-level risk analyses to identify key threat scenarios and system vulnerabilities.
- Utilities and operators: identify and classify assets, systems and interfaces according to their risk level (likelihood and impact) and assign security measures according to level of system risk.
- Policy makers and industry: facilitate public–private cyber risk information sharing.

## Climate resilience

- Policy makers and system operators: assess climate risks and impacts based on strong scientific evidence.

# Manage and mitigate risk

Power systems need to improve preparedness against risks across the electricity supply chain. In this regard, system assessments in areas such as adequacy and cyber resilience, long-term planning exercises and the setting of standards and sharing of best practices all play important roles. To mitigate risk, policy makers also need to consider establishing market frameworks that provide appropriate



IEA. All rights reserved.

investment signals to holders of assets that provide system security and flexibility. They also need to build capacity in new areas like cybersecurity.

## Energy transition

- Policy makers: assess where increased diversity of the power mix could ensure resilience against social, geopolitical, market, technical and environmental risks.
- Regulators and system operators: consider all flexibility sources as options to satisfy adequacy in long-term planning.
- Regulators and system operators: set rules that reward energy sources for their actual contribution to secure operation, instead of an expected or average contribution.
- System operators: develop grid codes to future-proof connection requirements.
- Regulators: create investment frameworks to take advantage of smart grid infrastructure, enabling a higher degree of visibility and controllability of demand response, storage and VRE.
- System operators: review and adapt historic load-shedding plans in the context of embedded generation, digitalisation of the entire value chain and greater economically viable demand response.

## Cyber resilience

- Policy makers and industry: provide accessible tools and guidance on cyber resilience best practices.
- Utilities: implement proper risk management strategies to identify capabilities and risks of their systems from both IT and OT perspectives. Establishing a clear risk management strategy can help prioritise areas of work and investment decisions to maximise benefits.
- Policy makers, standards bodies, industry and researchers: develop facilities to test and validate effective implementation of cybersecurity measures and controls.
- Policy makers and standards bodies: consider certification of products and services by carefully analysing criticality, enforcement options and market impact.
- Policy makers and industry: develop capacity building for cybersecurity to ensure skills and resources evolve appropriately. This involves achieving buy-in and a basic understanding across the entire organisation. Mandatory training and certification of critical staff should be considered.

## Climate resilience

- System operators and utilities: identify cost-effective resilience measures and check if they could have synergies with other business objectives or involve trade-offs.



IEA. All rights reserved.

- Policy makers and regulators: provide plans and guidelines to ensure decision makers have considered all potential risks and available measures over the entire life cycle of an asset.
- System operators: support physical system hardening of electricity systems, such as technical and structural improvements to power plants, or transmission and distribution networks.
- Regulators and system operators: enhance visibility and controllability in system operation with advanced weather forecasting, smart grid technologies, or application of islanding schemes.

# Monitor progress

Regulators need to ensure that mechanisms and tools to evaluate, monitor and track progress over time are made available. This is important at the operational level for individual utilities, as well as at the level of policy makers and regulatory authorities to understand if strategic objectives are being met. Monitoring mechanisms should include those that assess preparedness, build knowledge on emerging threats and share incident reporting.

## Energy transition

- Regulators: keep track of power system reliability and perform resilience tests.
- Regulators: mandate common planning procedures and information-sharing tools in interconnected systems.

## Cyber resilience

- Policy makers and regulators: develop or provide mechanisms and tools to continuously monitor preparedness.
- Policy makers and regulators: develop mechanisms to monitor and build knowledge around emerging threats. This is an area where partnerships and communication with the intelligence community is essential.
- Policy makers, the intelligence community and industry: develop and support active threat hunting and cyberthreat intelligence mechanisms to prevent or limit the damage from high-end attacks.
- Equipment providers and utilities: conduct active monitoring of the supply chain to detect vulnerabilities.
- Policy makers and industry: develop mechanisms to share incident reports and other information.



IEA. All rights reserved.

### Climate resilience

- Policy makers: adjust resilience measures based on an evaluation system and consultations with stakeholders to enable the constant improvement of adopted resilience measures.

## Respond and recover

Resilience of the electricity system needs to go beyond preventing incidents to also include mechanisms that effectively cope with outages or attacks. This includes comprehensive emergency response frameworks and clear delineation of responsibilities. Emergency response exercises have proven to be effective at boosting preparedness and response capability. Gathering data and lessons learned is also an important element in response and recovery to help prevent mitigate the impact of future events.

### Energy transition

- Policy makers: review substantial events like outages to learn lessons and adapt policies.
- Regulators and system operators: assess and reform adequacy mechanisms when temporary or structural out-of-the-market measures are applied, to guarantee secure operation.
- Regulators and system operators: implement procedures to take advantage of new resources to support recovery, such as distributed generation.

### Cyber resilience

- Utilities: implement robust response and recovery procedures that help maintain operations in the event of a cyberattack, with clearly allocated responsibilities to all main actors.
- Policy makers and utilities: execute regular response exercises and capture lessons learned and adapt practices.
- Policy makers, regulators and industry: stimulate information logging and sharing to facilitate analysis of actual incidents.

### Climate resilience

- Policy makers, regulators, and system operators: co-ordinate recovery efforts among diverse actors.
- Policy makers, regulators, and system operators: support capacity building for a better response to and faster recovery from climate impacts.



IEA. All rights reserved.

# References

Acharya, S., Y. Dvorkin and R. Karri (2020). Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable? IEEE Transactions on Smart Grid, 1–1. https://doi.org/10.1109/tsg.2020.2994177

Argonne National Laboratory (2012). Resilience: Theory and Applications (ANL/DIS-12-1).

Bloomberg. (2019, August). Power-Starved Zimbabwe, Zambia Face Further Drought-Induced Blackouts.

CSIS. (2020). Significant Cyber Incidents. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

EEA (European Energy Agency) (2019), Adaptation challenges and opportunities for the European energy system, https://www.eea.europa.eu/publications/adaptation-in-energy-system

E-ISAC. (2016). Analysis of the cyber attack on the Ukrainian power grid. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Feblowitz, J. (2019, September 27). Is Your Utility Ready for Smart Inverters? Utility Analytics Institute. https://utilityanalytics.com/2019/09/is-your-utility-ready-for-smart-inverters/

Gartner. (2017). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31% from 2016. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Gündüz, N. et al. (2017) Impacts of natural disasters on Swedish electric power policy: A case study, Sustainability 9(2), p. 230 (DOI: 10.3390/su9020230)

GSMA. (2020). The Mobile Economy 2020. https://www.gsma.com/mobileeconomy/

Idaho National Laboratory. (2016). Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector Mission Support Center Analysis Report. https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector.pdf

IDC. (2019). The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. https://www.idc.com/getdoc.jsp?containerId=prUS45213219

IEA. (2016), Energy, Climate Change & Environment – 2016 Insights, OECD/IEA, Paris, https://webstore.iea.org/download/direct/320/

IEA. (2017a). Getting Wind and Sun onto the Grid, https://www.iea.org/reports/getting-wind-and-solar-onto-the-grid

IEA. (2017b). Status of Power System Transformation 2017: System integration and local grids, https://www.iea.org/reports/status-of-power-system-transformation-2017

IEA. (2018). World Energy Outlook 2018, https://www.iea.org/reports/world-energy-outlook-2018

IEA. (2019a). Electricity Information 2019, https://www.iea.org/reports/electricity-information-overview



IEA. All rights reserved.

IEA. (2019b). World Energy Outlook 2019. https://webstore.iea.org/world-energy-outlook-2019

IEA (2019c). Market Report Series: Renewables 2019, https://www.iea.org/reports/renewables-2019

IEA. (2019d). Status of Power System Transformation 2019: Power System Flexibility, https://www.iea.org/reports/status-of-power-system-transformation-2019

IEA. (2020). World Energy Investment 2020. https://www.iea.org/reports/world-energy-investment-2020

IEA 4E EDNA. (2019), Total Energy Model of Connected Devices, https://www.iea-4e.org/document/429/total-energy-model-for-connected-devices

IHA. (2017). Hydropower Status Report 2016.

Lloyd's and University of Cambridge Centre for Risk Studies. (2015). Business Blackout: The insurance implications of a cyber attack on the US power grid. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf

Ministry of Power, Government of India (2020). MERIT – Merit Order Despatch of Electricity for Rejuvenation of Income and Transparency. http://meritindia.in/

OECD (Organisation for Economic Co-operation and Development) (2018), Climate-Resilient Infrastructure, http://www.oecd.org/environment/cc/policy-perspectives-climateresilient-infrastructure.pdf

Oguah, S. and S. Khosla (2017). Disaster Preparedness Offers Big Payoffs for Utilities, World Bank, Washington, DC.

Onishi, N. (2016, April). Climate Change Hits Hard in Zambia, an African Success Story. The New York Times.

Oughton, E. J. et al. (2019). Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks. Risk Analysis, 39(9), 2012–2031. https://doi.org/10.1111/risa.13291

Ponemon Institute and Accenture. (2019). The Cost of Cybercrime. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Ponemon Institute and Siemens. (2019). Caught in the Crosshairs: Are utilities keeping up with the industrial cyber threat? https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf

Robb, J. B. (2019). Testimony of James B. Robb, President and Chief Executive Officer North American Electric Reliability Corporation Before the House Committee on Energy and Commerce Subcommittee on Energy "Keeping the Lights On: Addressing Cyber Threats to the Grid." https://www.nerc.com/news/testimony/Testimony and Speeches/House Energy and Commerce Cyber Hearing Testimony 7-12-19.pdf

Soltan, S., P. Mittal and H. V. Poor (2018). BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. Proceedings of the 27th USENIX Security Symposium, 15–32. https://www.usenix.org/conference/usenixsecurity18/presentation/soltan



IEA. All rights reserved.

UN Secretary General (2019). For Every Dollar Invested in Climate-Resilient Infrastructure Six Dollars Are Saved, Secretary-General Says in Message for Disaster Risk Reduction Day (SG/SM/19807-IHA/1472-OBV/1927, 10 October 2019). https://www.un.org/press/en/2019/sgsm19807.doc.htm

US Department of Energy. (2018). Multiyear Plan for Energy Sector Cybersecurity. https://www.energy.gov/sites/prod/files/2018/05/f51/DOE Multiyear Plan for Energy Sector Cybersecurity_0.pdf

World Bank (2019), Lifelines: The Resilient Infrastructure Opportunity, http://hdl.handle.net/10986/31805

World Bank (2019), Stronger Power□: Improving Power Sector Resilience to Natural Hazards, International Bank for Reconstruction and Development and the World Bank, Washington D.C., http://documents1.worldbank.org/curated/en/200771560790885170/pdf/Stronger-Power-Improving-Power-Sector-Resilience-to-Natural-Hazards.pdf

World Economic Forum. (2020). The Global Risks Report 2020 Insight Report 15th Edition. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf



IEA. All rights reserved.

*"This publication has been produced with the financial assistance of the European Union as part of the Clean Energy Transitions in Emerging Economies programme. This publication reflects the views of the International Energy Agency (IEA) Secretariat but does not necessarily reflect those of individual IEA member countries or the European Union (EU). Neither the IEA nor the EU make any representation or warranty, express or implied, in respect to the publication's contents (including its completeness or accuracy) and shall not be responsible for any use of, or reliance on, the publication."*

The Clean Energy Transitions in Emerging Economies programme has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952363

This publication and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

IEA 2020, Analytical frameworks for electricity security. All rights reserved.

IEA Publications

International Energy Agency

Website: www.iea.org

Contact information: www.iea.org/about/contact

Typeset in France by IEA

Cover design: IEA

Photo credits: © shutterstock



IEA. All rights reserved.