Digitalization Trends for Ensuring Power System Resilience

Tohru Watanabe | **Shinji Matsuda** | **Hirotaka Moribe**
**Darren Jones** | **Marek Florkowski, Ph.D.**

Energy utilities provide the foundation for all the activities of society. Strengthening their resilience to ensure they can continuously provide services is a critical challenge for these companies. Power companies use an enormous amount of equipment for a very long time, leading to the risk of degradation. Also, because most equipment is installed outdoors, devices are exposed to risks from the natural environment. Furthermore, now that distributed and networked control systems have become widely used, they also face external threats, such as cyberattacks. Power companies must understand these various risks and take appropriate countermeasures. It is important to have resilience so that if one of these risks actually results in an incident, the issue is quickly detected, and its impact is mitigated. This article describes digitalization trends for strengthening resilience by understanding risks and mitigating their impact, and the development of field service management solutions.

Introduction

The movement toward a carbon-neutral society has gained momentum in recent years, triggering further electrification throughout the economy, and placing greater responsibility on electric power systems, which are core systems of social infrastructure. However, electric power and other infrastructure systems face growing threats and uncertainties, leading to demand for strengthened resilience. Pandemics, natural disasters, geopolitical risks, and cyberattacks have already turned these threats and uncertainties into reality. Infrastructure systems such as electric power, gas, and telecommunications affect each other, and it is difficult to eliminate uncertainties if each operator works independently. Even though

Figure 1 | **Increased Frequency of Natural Disasters**

This graph shows the trend for the number of natural disaster events reported globally from 1900 to 2022. These events include droughts, floods, abnormal weather, extreme temperatures, landslides, wildfires, volcanic activity, and earthquakes.
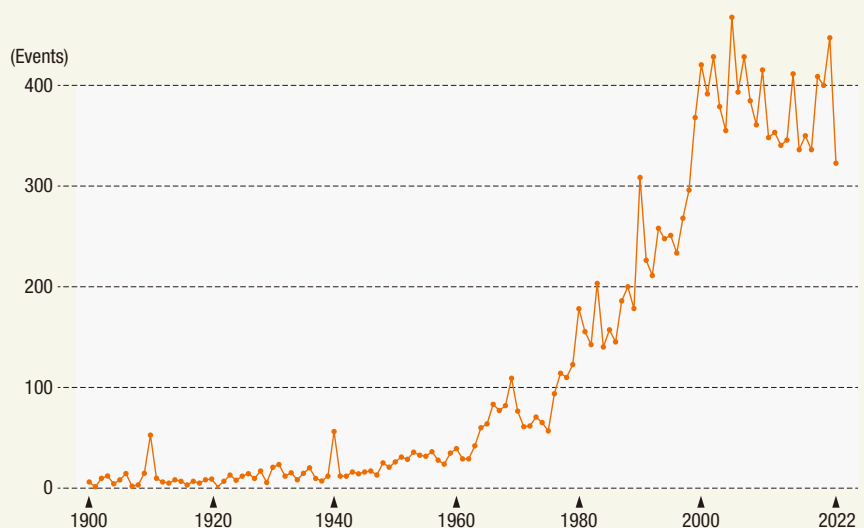
Source: Our World in Data

uncertainties cannot be completely eliminated, it is important to have a system that can respond if sudden, unexpected, and uncertain events occur.

The reality is that incidents involving cyberattacks on infrastructure systems are increasing. Natural disasters are also becoming more frequent (see Figure 1)[1]. In response, power companies and governments in North America are conducting evaluations and countermeasures to ensure the safety and resilience of power transmission networks, including consideration of the surrounding environment[2], [3]. The UK government and power companies are seeking to introduce stress tests for resilience, and holistic (comprehensive) metrics for evaluating overall resilience countermeasures[4].

In this context, there is demand for power companies to reveal their specific policies for strengthening the resilience of their power systems. This article describes trends in strengthening power system resilience and the actions taken by Hitachi.

Trends in Strengthening Resilience

Currently, efforts to strengthen resilience are continuing. The focus is on strengthening resilience not only to counter threats such as cyberattacks and abnormal weather, but also as a key concept for power systems that aim to become net zero and carbon neutral.

Strengthening resilience requires improved threat resistance and recovery capabilities. Resistance capabilities have been improved previously by enhancing equipment robustness and redundancy. To improve recovery capabilities, a holistic approach is required for countermeasures that span entire organizations, networks, and equipment (see Figure 2).

This has posed a new challenge: the need to establish a method for evaluating and proving resilience in a demonstrable way. A concept is required that goes beyond the normal boundaries of risk management. Normal risk management is based on the concept of accepting risks by evaluating the probability of occurrence and scale of impact. However, high-impact, low-probability (HILP) events may occur that result in sudden, unexpected, uncertain, and serious incidents. There is a limit to resistance capabilities against the impact of such incidents through equipment robustness and redundancy, placing pressure on recovery capabilities for returning systems to their original status. One policy idea is to impose stress tests based on a series of key performance

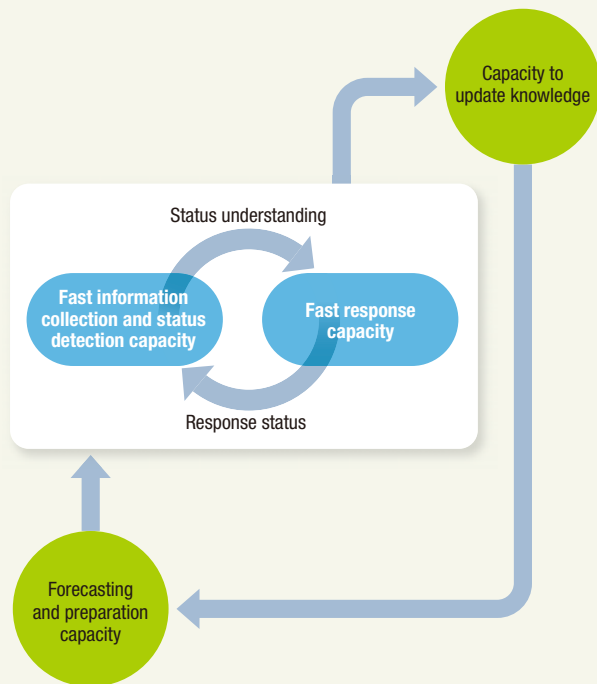## Figure 2 | Resistance Capabilities and Recovery Capabilities

Resistance capabilities are the capacity to minimize the scale of damage caused by threats such as natural disasters and cyberattacks. Recovery capabilities are the capacity to quickly restore damaged systems and equipment to their normal levels.
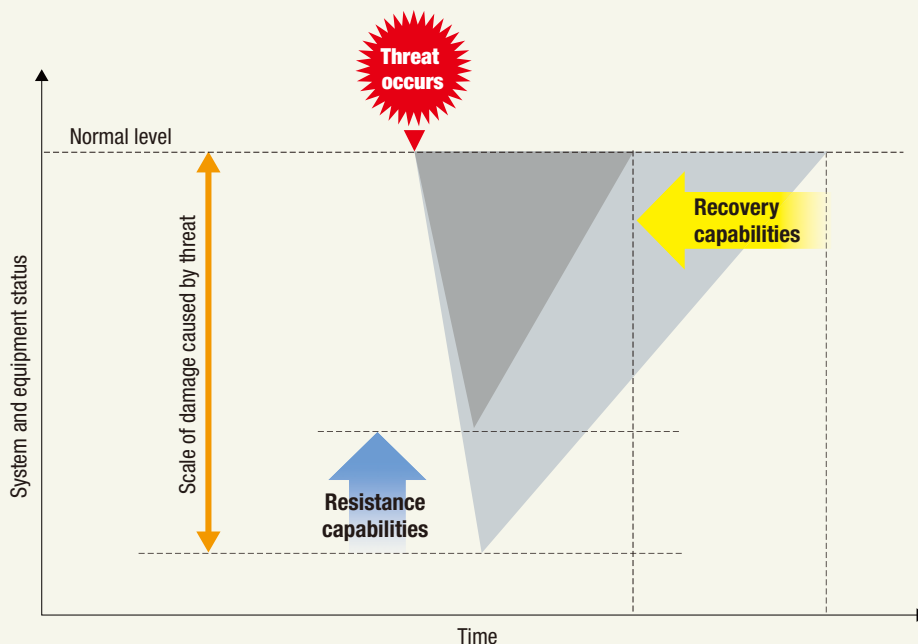
Figure 3 | **Concept of Recovery Capabilities and Capacity for Improving Recovery Capabilities**

Recovery capabilities are composed of reserve capacity to prepare for sudden and uncertain threats, stockpile forecasting and preparation capacity, and the capacity to quickly detect the details and take action should a threat occur. These capacities are strengthened via a capacity improvement cycle based on updating knowledge after the fact.

indicators (KPIs) that integrate resistance capabilities and recovery capabilities[5]. Wider discussion is required for defining the technologies and solutions that can provide recovery capabilities, and then these need to be refined further.

In particular, the following capacities are required to strengthen recovery capabilities:

(1) Forecasting and preparation capacity

(2) Capacity for incident detection based on fast information collection

(3) Fast response capacity

(4) Capacity to improve the first three capacities by updating knowledge through after-the-fact reviews of incidents[6] (see Figure 3).

As described above, evaluations of resilience policies should be designed from the perspective of resistance capabilities and recovery capabilities, taking an approach that covers entire organizations, networks, and equipment.

Policies for Solving Resilience Issues

Hitachi is working to improve the resilience of power systems. As previously described, to strengthen resilience, it is important not only to improve resistance capabilities, but also recovery capabilities. It is making efforts not only to increase the robustness and redundancy of equipment and systems to improve resistance capabilities, but also to strengthen organizational capacity to improve recovery capabilities when recovering from a sudden, unexpected, and uncertain event. This organizational capacity related to recovery capabilities can be strengthened through the digital transformation (DX) of work processes.

The ability to respond to sudden, unexpected, and uncertain incidents can be improved through step-by-step leveling up of capacities; starting with forecasting and preparation, progressing to fast information collection, then the organizational capacity for a fast response, and finally the ability to improve all these capacities by updating knowledge. Hitachi views this model as an opportunity to improve resilience capacities from the perspective of the resilience proficiency model shown in Figure 4.
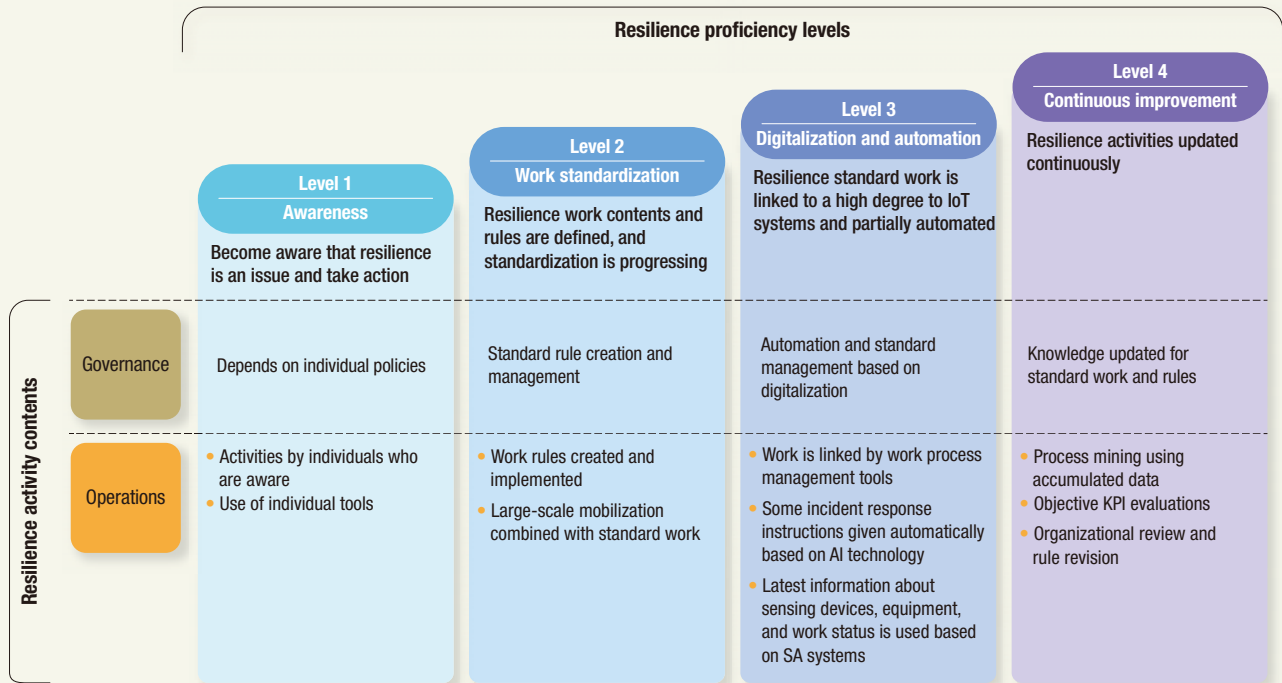
The important concepts in this resilience proficiency model are awareness, work standardization, digitalization and automation, and updating and accumulating knowledge through continuous improvement.

Level 1 is the phase where an individual becomes aware that resilience is an issue, and takes action to respond to sudden, unexpected, and uncertain incidents. In this phase, resilience activities are not standardized across the organization and depend on the initiative of individuals. Individual actions and the use of individual tools correspond to this level.

Level 2 is the phase where the organization defines the work details and rules of resilience and promotes standardization. Organizational knowledge is defined and stored for use by succeeding personnel in the form of rules. Work standardization enables standard tasks to be combined and more manpower to be dedicated to network and equipment resilience. The management of work processes using digital systems corresponds to this level.

Figure 4 | Hitachi's Concept of a Resilience Proficiency Model

Resilience is strengthened through the phases of "Level 1: Awareness," "Level 2: Work standardization," and "Level 3: Proficiency in digitalization and automation." Furthermore, "Level 4: Continuous improvement" strengthens resilience by continuously performing improvements based on updating knowledge via updates to the standard work and rules of resilience activities.

Resilience activity contents		Resilience proficiency levels			
		Level 1 Awareness Become aware that resilience is an issue and take action	**Level 2 Work standardization** Resilience work contents and rules are defined, and standardization is progressing	**Level 3 Digitalization and automation** Resilience standard work is linked to a high degree to IoT systems and partially automated	**Level 4 Continuous improvement** Resilience activities updated continuously
	Governance	Depends on individual policies	Standard rule creation and management	Automation and standard management based on digitalization	Knowledge updated for standard work and rules
	Operations	• Activities by individuals who are aware • Use of individual tools	• Work rules created and implemented • Large-scale mobilization combined with standard work	• Work is linked by work process management tools • Some incident response instructions given automatically based on AI technology • Latest information about sensing devices, equipment, and work status is used based on SA systems	• Process mining using accumulated data • Objective KPI evaluations • Organizational review and rule revision

IoT: Internet of Things   AI: artificial intelligence   SA: situation awareness   KPI: key performance indicator

Level 3 is the phase where standard resilience work is linked to a high degree to Internet of Things (IoT) systems and some activities are automated. The automation of incident responses based on artificial intelligence (AI) technology and the visualization of worksites by integrating sensing devices, equipment, and work processes correspond to this level.

Level 4 is the phase where resilience activities are updated continuously. This is performed as necessary according to changes in the operational environment, such as weather fluctuations or changes in cyberspace. This level encompasses process mining using accumulated data, and rule management that includes revising rules based on objective KPI evaluations, and adapting inherited knowledge to changes, leading to further refinement of rules.

Hitachi has proposed a digitalization framework with the objective of improving recovery capabilities, which will support rule management for resilience activities and automation (see Figure 5). The key points of this framework are shown below.

## (1) Digitalization of information collection

The digitalization of information collection enables faster and more efficient patrol inspections. Also, in the USA, tests have been conducted of patrol by aircraft using digital technology to detect incidents as soon as possible by identifying radio wave and infrared radiation from phenomena (arc discharge, temperatures rises) that cause wildfires. In the future, this is expected to raise the quality of work to a level higher than is possible with visual patrols by humans.

(2) Documentation of rules in a digital playbook that describes how to respond to incidents

Digitally recording the response to incidents and documenting the rules of resilience activities that have been standardized as organization activities are key steps to increase resilience abilities from Level 1 to Level 2 in the resilience proficiency model. Hitachi has also proposed a playbook, which is a definition file that digitally describes the series of processes for

Figure 5 | Digitalization Framework for Resilience Activities

Hitachi has proposed a framework to support the digitalization of information collection, the digitalization of incident response rules, and the optimization of responses using AI. The playbook digitally records the responses to incidents and digitalizes resilience activity rules that have been standardized as organization activities. These are accumulated as organizational knowledge.
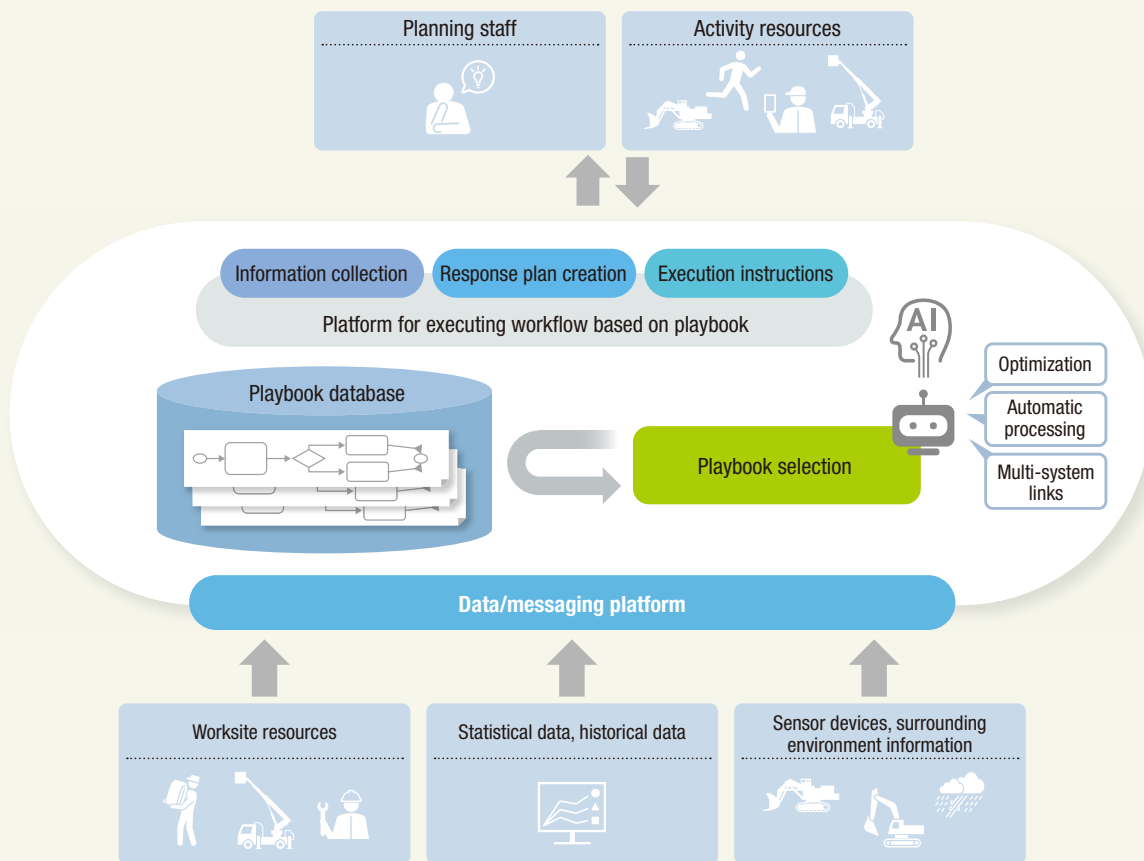
collecting information, creating a response plan, and executing instructions. This playbook is a key step in raising resilience capabilities to Level 3, where activities start to be automated. When considering a response to sudden, unexpected, and uncertain incidents, a playbook that is not dependent on existing systems should allow all elements to be different, such as the simulators, data storage locations, and external systems storing the data related to each incident. This playbook stores organizational knowledge.

(3) Optimization of responses and automatic creation of schedules using AI

To improve the effectiveness of recovery capabilities, the creation and execution of an efficient and flexible recovery schedule for organizations, networks, and equipment is essential. The process is not completed after creating a schedule just one time. Rather, continuous rescheduling is required according to

on-going incidents and changes in the response status, which is a key reason for using digital technology.

Figure 6 shows the concept of digitalization in field service management (FSM) that applies a digitalization framework to the objective of improving recovery capabilities for resilience. The aim is to enable a response to sudden, unexpected, and uncertain incidents, as well as faster and more efficient daily work. Hitachi has actually started to provide a service that collects remote sensing information via satellites to detect overgrown trees that may come in contact with power lines[7].

Based on this framework, Hitachi in the future will also use AI in systems for updating rules according to the accumulated field data and evaluations, and will also continue to expand solutions for total resilience countermeasures for power systems, including networks and equipment.

Figure 6 | Concept of Digitalization in Field Service Management for Resilience

The aim is to establish FSM that flexibly integrates functions to enable a response to sudden, unexpected, and uncertain incidents, as well as faster and more efficient daily work. Functions such as remote sensing via satellites and AI schedulers are combined according to the details of the threat.
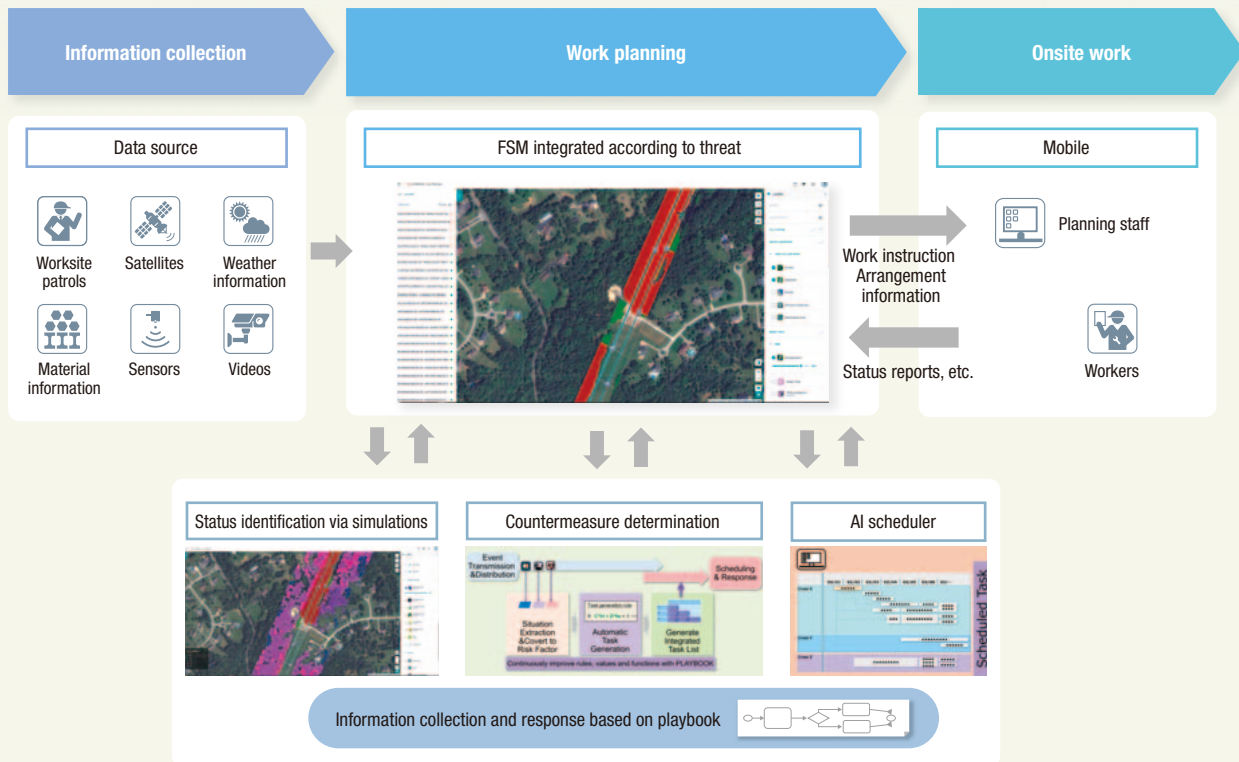
FSM: field service management

Conclusions

This article has described the resilience proficiency model and framework proposed by Hitachi in response to the trend of using digital technology in power systems, which are in a historic era of transition to carbon neutrality. The key points of this framework are the digitalization of information collection, the digitalization of incident response rules, optimization of responses, and automatic generation of schedules using AI.

In the future, based on this framework, Hitachi will expand Lumada solutions for flexible resilience countermeasures that use digital technologies to comprehensively integrate organizations, networks, and equipment. This will help resolve the various issues faced by customers and create new businesses that contribute to strengthening resilience.

References

1) Our World in Data, "Number of recorded natural disaster events, 1900 to 2022" (2023), https://ourworldindata.org/grapher/number-of-natural-disaster-events

2) Southern California Edison, "SCE Proposes Grid Safety and Resiliency Program to Address the Growing Risk of Wildfires" (Sept. 2018), https://newsroom.edison.com/releases/sce-proposes-grid-safety-and-resiliency-program-to-address-the-growing-risk-of-wildfires

3) Southern California Edison, "2023–2025 Wildfire Mitigation Plan" (Mar. 2023), https://www.sce.com/sites/default/files/AEM/Wildfire%20Mitigation%20Plan/2023-2025/2023-03-27_SCE_2023_WMP_R0.pdf

4) Cabinet Office UK, "National Flood Resilience Review" (Sept. 2016), https://www.gov.uk/government/publications/national-flood-resilience-review

5) Pacific Northwest National Laboratory, "Framework for Modeling High-Impact, Low-Frequency Power Grid Events to Support Risk-Informed Decisions" (Dec. 2015).

6) US Federal Energy Regulatory Commission, "Cyber Planning for Response and Recovery Study (CYPRES)" (Sept. 2020).

7) Hitachi News Release, "Hitachi launches Lumada Inspection Insights and strengthens digital and green portfolio" (May 2022), https://www.hitachi.com/New/cnews/month/2022/05/220524a.html

Tohru Watanabe
Digital Transformation Promotion Department, Digital Business Strategy Division, Energy Business Administration Division, Hitachi, Ltd. (at the time of writing). *Current work and research:* Development of service businesses for power system resilience (at the time of writing). *Society memberships:* The Institute of Electrical Engineers of Japan (IEEJ) and the Society of Instrument and Control Engineers (SICE).

Shinji Matsuda
Digital Transformation Promotion Department, Digital Business Strategy Division, Energy Solutions Division, Energy Business Division, Hitachi, Ltd. *Current work and research:* Strategic management of digital transformation in the electric power field.

Hirotaka Moribe
Digital Transformation Promotion Department, Digital Business Strategy Division, Energy Solutions Division, Energy Business Division, Hitachi, Ltd. *Current work and research:* Development of solutions for improving power system resilience. *Society memberships:* IEEJ.

Darren Jones
Hitachi Energy Ltd. *Current work and research:* Technical management related to future energy systems. *Society memberships:* A Chartered Electrical Engineer with the Institution of Engineering and Technology (IET) and a member of CIGRE UK Executive Committee.
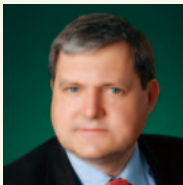
Marek Florkowski, Ph.D.
Hitachi Europe Ltd. *Current work and research:* A senior technical advisor for the development of technologies related to energy systems, future intelligent grids, and digital solutions. He has obtained Full Professor with the AGH University of Science and Technology in Poland and a Ph.D. in Electronics. *Society memberships:* A Senior Member of IEEE, member of CIGRE, as well as the Chair of the Technical Committee Diagnostics of the IEEE Dielectrics and Electrical Insulation Society.