# GRID RESILIENCE & PHYSICAL PROTECTION OF ENERGY INFRASTRUCTURE

e·on

Infosys®
Navigate your next

# Table of Contents



## Executive Context and the Core Problem

In early January 2026, a targeted attack on the energy supply happened in Berlin, Germany, which is considered one of the most severe power outages the city has experienced in decades. The southwest of the city was particularly affected, where a central part of the power grid was routed via a cable bridge.

On this cable bridge, several power lines were deliberately set on fire. Within a short time, both high-voltage and medium-voltage cables were destroyed. Because these lines were bundled together in one location, a central part of the power supply failed simultaneously. As a result, tens of thousands of households and numerous businesses were left without electricity, and many people were also without heating, communication, and in some cases even functioning emergency services.

The cable bridge functioned as an important node within a supply ring. Through it, electricity was distributed to several districts. Although German power grids are generally designed with redundancy, these are not necessarily spatially separated. Redundancies provide security of supply in the case of a technical failure, not necessarily in the case of sabotage.

Another factor was the physical structure of the cable bridge. As an openly accessible piece of infrastructure with cables running closely side by side, it was especially susceptible to sabotage. A single fire was enough to destroy several critical connections at once.

Restoring the power supply proved difficult. While some areas were reconnected relatively quickly, it took several days before full service was restored. The main reason was that high-voltage cables are complex and time-consuming to replace and must be installed under strict safety requirements.

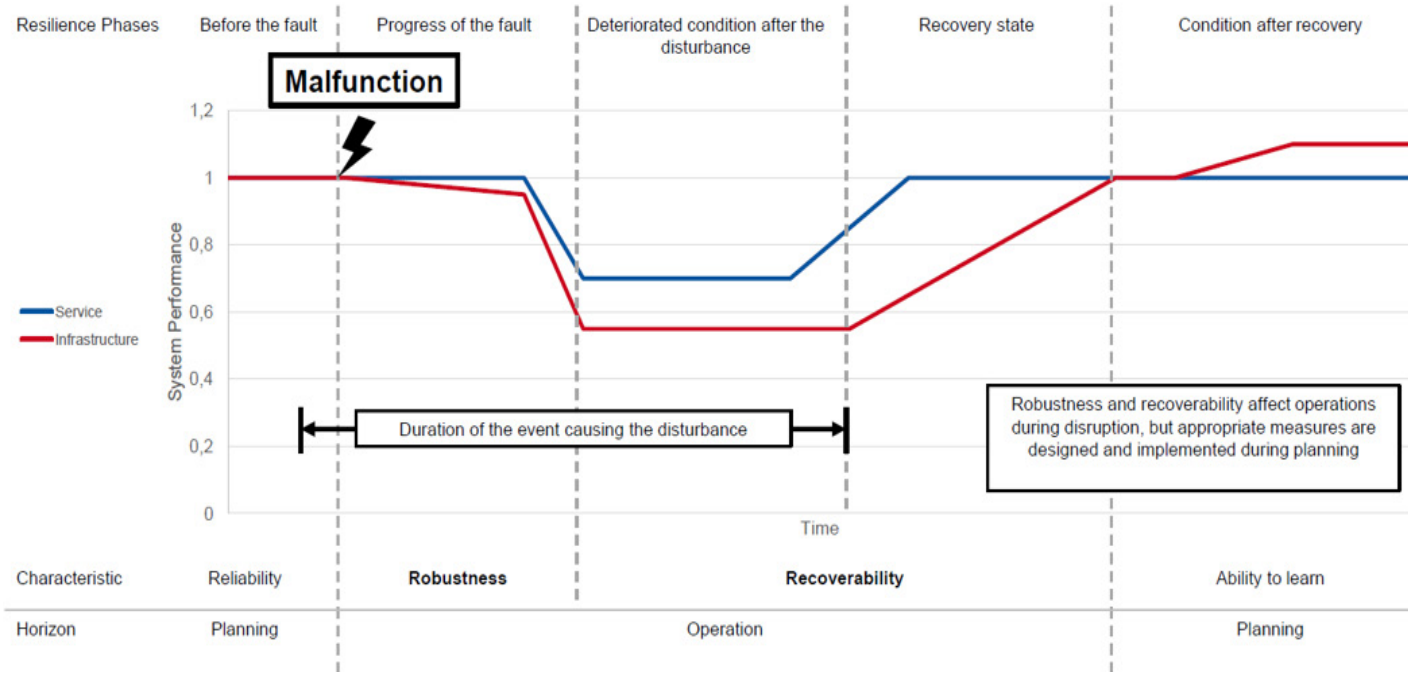
In summary, the attack exploited a physically vulnerable point in the network where several key connections converged and whose failure could not be quickly compensated for.

The sequence of events can be divided into three phases based on the resilience curve (see figure 1): prevention, detection, and mitigation. Each of these phases presents its own challenges that need to be addressed, not only for highly populated urban areas but also for rural grid areas.

This innovation challenge should support the protection of critical grid infrastructure by enabling stronger prevention, faster detection, and more effective mitigation of attacks, sabotage or other external influence to safeguard energy system resilience and security of supply. .

**Resilience curve**

figure 1



# *Problem Statement*

## Cluster 1: Prevention / Physical Protection of Grids

We are seeking innovations that prevent the failure of energy grid assets. Proposals should focus on improving the reliability of these assets, enhancing their protection, making their design more robust and/or impede attackers/saboteurs for as long as possible.

## 1. The Problem Space

Prevention (physical protection) in the resilience curve refers to all measures taken before a disruption occurs within the energy system, specifically in the distribution grids, to prevent outages or minimize their impact. The goal is to reduce the vulnerability of the infrastructure as much as possible so that, ideally, no drop in system performance occurs, or at least that any decline is significantly mitigated.

Within the resilience curve, prevention ensures that either no performance drop occurs or that any decline in the event of a disruption is significantly smaller. This helps maintain system stability for as long as possible, even under stress, and reduces the likelihood of large-scale outages or cascading effects.

## 2. Considerations/ Guardrails for the solution

All solutions should align with the following guiding principles:

- Applicable to Germany and Europe (brownfield environment / existing grids)
- Comply with regulatory and approval processes
- Cost efficient and scalable approaches that can cover critical assets over a wide grid area (e.g. also for rural areas).
- Cost-efficiency also refers to financial trade-offs between cost of physical protection / hardening of infrastructure vs. potential risk reduction ("Where / which assets and which solutions to focus on with limited resources to generate the most risk-mitigation?")
- Consider different types of potential attacks and disturbances, e.g. direct human actions, drone or vehicle attacks etc.
- Optionally, real-time warning capabilities to allow operators to protect the assets before a damage occurs

## 3. Desired Outcomes

- Concept as minimum requirement, describing technical solution and step-by-step application in detail. Ideally, demonstration and/or practical application
- Description how to apply concept for distribution grids (European grid structures must be considered)
- How would your solution prevent or impede attackers from damaging or destroying critical grid infrastructure?
- How would your solution have worked in the Berlin case?
- How would your solution work for rural grid areas?
- Description of scalability (cost / effort, how to scale, which assets to focus on…?)

# Problem Statement

## Cluster 2: Detection / Surveillance

We are seeking solutions that can quickly detect planned, happening, and/or performed acts of sabotage or attacks on grid assets, enable a fast information chain and quick response and limit the impact of such acts on the asset. Even after an act of sabotage, the asset should remain operational to the greatest extent possible.

## 1. The Problem Space

Detection and surveillance in the resilience curve refer to the ability of the energy system and electrical grid to continuously monitor, identify, and interpret disruptions, anomalies, or emerging threats as early as possible. Actions are taken during an upcoming or ongoing disruption in the energy system to limit its impact and prevent further escalation.

In practice, operational measures are taken such as redispatching power plants, rerouting electricity flows, activating reserve capacities, and, if necessary, implementing controlled load shedding to prevent a total system collapse. Automated protection systems also play a key role by quickly disconnecting faulty components to stop disturbances from spreading.

Within the resilience curve, in this phase the depth and duration of the performance drop is reduced by containing the disruption and avoiding cascading failures. It ensures that critical parts of the system remain operational and create the conditions for a faster and more efficient recovery phase.

## 2. Considerations/ Guardrails for the solution

- Applicable to Germany and Europe (brownfield environment / existing grids)
- Comply with regulatory and approval processes, especially General Data Protection Regulation (GDPR) conformity
- Cost efficient and scalable approaches that can cover critical assets over a wide grid area (e.g. also for rural areas).
- Consider different types of potential events, e.g. direct human actions, drone or vehicle attacks etc.
- If IT-related solution is used, consider cybersecurity measures
- Nice to have: Potentially real-time warning capabilities to allow operators to protect the assets before a damage occurs

## 3. Desired Outcomes

- Concept as minimum requirement, describing technical solution and step-by-step application in detail, including used technology / hardware, references to existing solutions from other sectors, information processing / flow and storage / usage, requirements for application in the grid (e.g. power and/or data connection) as well as advantages and disadvantages of chosen technology. Ideally, demonstration and/or practical application.
- Description how to apply concept for distribution grids (European grid structures must be considered)
- How would your solution prevent or impede attackers from damaging or destroying critical grid infrastructure?
- How would your solution have worked in the Berlin case?
- How would your solution work for rural grid areas?
- Description of scalability (cost / effort, how to scale, which assets to focus on…?)
- Ideally, enable simple connection / implementation into existing DSO systems (IT / OT / general processes…)
- Ideally, solution should provide timely and actionable alerts
- Ideally, differentiate between diverse states, e.g. physical attack vs. operational anomalies
- Ideally, reduce false positives / unnecessary alarms to a minimum
- Ideally, provide redundancy, even if single component or system fails

# Problem Statement

## Cluster 3: Mitigation / Operational Emergency Response

We are looking for innovations that minimize downtime caused by sabotage of grid assets. The goal is to quickly mitigate the effects of sabotage through rapid repair measures or asset design and return to normal operation.

## 1. The Problem Space

Even with better prevention and detection, distribution grids need stronger mitigation capabilities to contain incidents, preserve service continuity, and recover rapidly. In the context of the resilience curve, mitigation refers to the ability to limit the depth and duration of performance degradation after a disruptive event by containing the disturbance, sustaining essential functions where possible, and enabling a faster return to stable operation, potentially combined with temporary solutions to re-supply customers until default service and infrastructure have recovered sufficiently.

## 2. Considerations/ Guardrails for the solution

- Applicable to Germany and Europe (brownfield environment / existing grids)
- Comply with regulatory and approval processes
- Account for health, safety and environmental standards. Ensure high level of workforce safety.
- Cost efficient and scalable approaches that can cover critical assets over a wide grid area (e.g. also for rural areas).
- Solutions should support DSO and emergency teams and not substitute them
- Solution should account for continuous safe operation of remaining, intact infrastructure and prevent further disruptions or negative cascading effects.
- Solution should be implementable into existing emergency and resilience planning, not act as stand-alone-tool
- Solution should work under difficult conditions, e.g. bad weather conditions, night, loss of standard communication etc.

## 3. Desired Outcomes

- Concept as minimum requirement, describing technical solution and/or concept as well as step-by-step application in detail. This might include system or process overviews, descriptions on backup resources / hardware on stock, references to existing solutions from other sectors, information flows, instructions on safe application etc. Ideally, demonstration and/or practical application, e.g. by modeling/simulation and/or hardware/lab test.
- Clearly define which focus category your mitigation solution accounts for, e.g. hardware-based repair, software-based grid stabilization and/or human resources/training/awareness.
- Description how to apply concept for distribution grids (European grid structures must be considered)
- How would your solution enable fast recovery of damaged grid infrastructure and/or provide temporary supply / relief and/or support return to normal operation?
- How would your solution have worked in the Berlin case?
- How would your solution work for rural grid areas?
- Description of scalability (cost / effort, how to scale, which assets to focus on…?)
- Optional: Consider synergies with detection solutions, e.g. exact detection of affected (an non-affected) grid areas

## Expected Impact. How big is the problem

By further improving the resilience of Europe's grid infrastructure with more than 10 million kilometers of networks and more than 2 million distribution transformers across the EU, this innovation challenge can make a meaningful contribution to ensuring reliable energy supply, maintaining grid stability, and securing continuity of service for millions of households, businesses, and critical societal functions.

# *Criteria for All Challenges*

## 1. Transferability and Scalability in Europe and Globally

The proposal must be transferable and scaleable to Europe and globally. Scalability within India is nice-to-have but not mandatory.

### a. Explicit transferability to Europe (mandatory)

- Clear explanation of how the solution can be adapted to European regulatory[1], market, and customer contexts
- Identification of required modifications (e.g. standards, cost structure, integration)

### b. Global scalability potential (mandatory)

- Core concept is not India-specific in its fundamentals
- Demonstrates relevance to other markets facing similar constraints

### c. Scalable within India (good to have)

- Clear pathway from pilot to large-scale deployment
- Addressable market size and adoption drivers identified
- Key customer(s)/segments identified

## 2. Leverages Strengths of the Indian Innovation Landscape

Proposals must demonstrate a strong alignment with India's proven innovation strengths:

- **Cost efficient engineering:** The idea leverages engineering approaches that minimize cost without compromising essential functionality.
- **Frugal innovation mindset:** The solution delivers high value with limited resources and avoids unnecessary complexity.
- **Constraint-driven creativity:** The proposal explicitly shows how constraints related to cost, infrastructure, skills, or system complexity have informed the design.

## 3. Practicality and Rapid Deployability

The idea must be suitable for rapid validation and deployment in the coming 12 to 18 months in a large, diverse markets in the EU and globally, and as a good-to-have, India:

- Addresses a clearly identifiable real-world problem.
- Demonstrates usability in environments with varying levels of infrastructure maturity.
- Shows evidence that the solution can be tested, piloted, or scaled without long development cycles.

## 4. Solution Quality Requirements

All submitted solutions must meet the following non-negotiable design principles:

### a. Simple

- Clear core functionality
- Minimal dependencies
- Easy to understand, use, and maintain

### b. Robust

- Reliable under variable operating conditions
- Tolerant to imperfect infrastructure or user behavior
- Low maintenance requirements

### c. Affordable

- Cost structure suitable for price-sensitive markets for EU and global markets and optionally, Indian markets
- Transparent assumptions on production, deployment, and operating costs, presented in the form of estimates for Total Cost of Ownership (TCOs) or techno-economic assessments

## *Overall proposed ideas will be measured on how they fare on three "I's"*

- **Innovation:** novelty, competitive differentiation, translation across markets (EU, global, India)
- **Implementation:** adoption risks, co-innovation risks, regulatory hurdles, time to deploy, time to mature market
- **Impact:**
  - how much you can make - serviceable addressable market size (% of TAM)
  - how much you can save – resilience, robustness, reliability

Participants should ensure ideas are in broad alignment with European regulations. Guidance can be provided by E.ON on request on more specific details of European regulations.

For more information, contact askus@infosys.com

Infosys®
Navigate your next