IT SECURITY

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 p articularly 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 in 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.

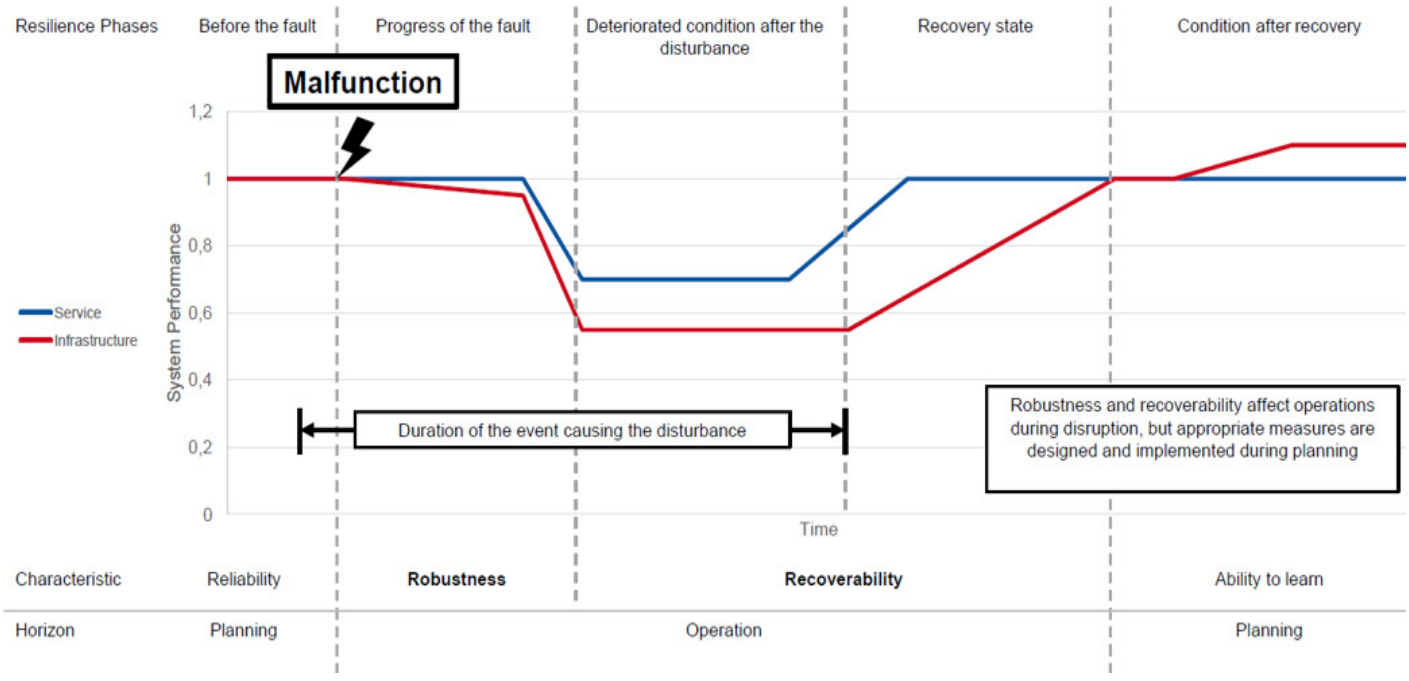
In summary, the attack exploited a physically vulnerable point in the network where several key connections converged and whose failure could not be quickly compensated for.

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.

figure 1

Resilience curve



Problem Statement

Cluster 4: IT security - Improvement of protection systems

We are looking for innovations that automate and systematically execute the testing of IT security systems. The goal is to identify and close vulnerabilities within these systems.

1. The Problem Space

Red and Blue teams are specialized units in cybersecurity that work together to improve the IT security of organizations through simulated attacks and defensive measures. These two teams collaborate closely to realistically test and strengthen an organization's security posture. The Red Team takes on the role of an attacker, using methods such as social engineering or penetration testing to uncover vulnerabilities. The Blue Team, on the other hand, focuses on detecting, defending against, and analyzing these attacks, as well as continuously improving defensive measures. The challenge lies in realistically simulating attacks while simultaneously developing effective protection mechanisms to identify vulnerabilities early and minimize their impact.

2. Considerations/ Guardrails for the solution

- Applicable to Germany and Europe
- Comply with regulatory and approval processes
- Solutions should support IT security teams not substitute them
- Solution should be implementable into existing IT security processes

3. Desired Outcomes

Your task is to develop an intelligent AI agent that integrates and automates the functions of Red and Blue teams by designing a unified, AI-driven 'Purple Team' architecture that autonomously orchestrates the cycle of attack simulation and defensive hardening to provide a self-evolving security loop for critical infrastructure. The agent should independently simulate realistic cyberattacks (Red team perspective), identify vulnerabilities in the IT systems of a grid operator, and at the same time detect, analyze, and defend against these attacks (Blue team perspective). Furthermore, the AI agent should continuously learn from the executed attacks and defense measures in order to proactively close security gaps, optimize defense strategies, and sustainably improve the overall security posture of a grid operator.

Problem Statement

Cluster 5: IT security - Protection schemes for customer-based assets

We are looking for protection measures against coordinated attacks executed by hacked or compromised customer-based assets against grid infrastructure.

The Problem Space

Millions of customer-based energy assets such as EV chargers, heat pumps, rooftop PV, home batteries, smart inverters, and home energy management systems are becoming connected and increasingly relevant for grid operation. Yet many are deployed with limited cybersecurity, inconsistent patching, and fragmented responsibilities across vendors, installers, service providers, and end users. Because these assets are typically outside direct DSO control, visibility and coordinated defense remain limited. This creates a systemic cyber-physical risk: if large numbers of devices are compromised and remotely orchestrated, they could simultaneously alter load, disconnect generation, or distort telemetry. Similar to a DDoS attack, the synchronized behavior of many hacked assets could destabilize grid conditions, trigger protection events, and cause cascading effects across parts of the network. Consider how to either protect critical energy infrastructure against such coordinated attacks or how a higher level of cybersecurity could be brought to existing or planned customer-based, smart energy assets, including potential benefits for the customer.

Considerations/ Guardrails for the solution

- Applicable to Germany and Europe (brownfield environment / existing assets)
- Comply with relevant regulatory, cybersecurity, data protection, and product approval requirements
- Support open standards, interoperability, and vendor-agnostic integration rather than proprietary lock-in
- Compatible with existing heterogeneous customer assets, legacy devices, and vendor ecosystems
- Retrofit-friendly where possible and realistic for mixed fleets of new and already deployed devices
- Minimize operational burden for customers, installers, aggregators, and DSOs
- Solution should account for continuous safe operation of remaining, intact infrastructure and prevent further disruptions or negative cascading effects.
- Customer acceptance and incentives should be considered, including clear end-user value beyond security alone

Desired Outcomes

Your task is to develop a solution that either protects critical grid infrastructure from coordinated attacks or enhances the cybersecurity of customer-based assets through a scalable framework that includes clear incentives and value for the end user. Your solution should include:

- A clear solution concept with architecture, key components, and step-by-step implementation approach
- A description of how the solution detects, limits, or prevents coordinated misuse of compromised customer-based assets
- Analysis, which customer assets might be critical regarding their grid-impact (e.g. rated power) and/or lack of cybersecurity measures
- Explanation of how the solution integrates with DSO, aggregator, vendor, or central monitoring and response structures
- How would your solution prevent or impede attackers from damaging or destroying critical grid infrastructure?
- If you focus on enhancing cybersecurity for customer assets: How to convince customers to invest into cybersecurity (e.g. new software or hardware) and/or connect their assets to central cybersecurity entities?
- Ideally, a pilot, prototype, simulation, or practical demonstration with measurable security and grid-resilience benefits

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

Navigate your next