E.DSO Technology Report on Incident Management

Brussels, 3 September 2026

Executive Summary

The increasing digitalisation, decentralisation, and electrification of Europe's power systems are fundamentally changing the nature of incident response and resilience management. Traditionally, incident investigations were focused on electrical failures within clearly defined organisational boundaries. Today, however, incidents increasingly span operational technology (OT), information technology (IT), communications networks, market systems, distributed energy resources, and cybersecurity domains.

E.DSO held a Knowledge Sharing session on Incident Response on 15 June 2026, explored how Distribution System Operators (DSOs) are adapting their incident management practices and what future developments are likely to require. The discussion was informed by a survey among E.DSO members and complemented by case studies from Fluvius (Belgium), Enedis (France), and Stedin (the Netherlands).

The session identified three major shifts affecting incident management:

- Incident investigations are becoming multidisciplinary, requiring collaboration across asset management, operations, IT, cybersecurity, and external stakeholders.
- Grid congestion is emerging as a major operational risk, creating new challenges at the intersection of normal operations and emergency response.
- Digitalisation is increasing both system capabilities and system dependencies, introducing cybersecurity, communications resilience, and data management as integral elements of incident response.

Although weather-related events and traditional asset failures remain significant causes of outages, participants emphasised that future resilience strategies must address the growing interdependence between physical infrastructure and digital systems. This requires stronger cooperation between DSOs and TSOs, more systematic knowledge sharing, and a broader approach to resilience that integrates operational, technical and cybersecurity considerations.

This paper summarises the key findings from that knowledge-sharing session and examines how incident analysis and resilience management may need to evolve in response to changing system conditions. More specifically, the paper seeks to inform future discussions within E.DSO and between E.DSO and other associations regarding:

- The evolution of incident investigation practices in distribution networks;
- The growing interaction between electrotechnical and cyber incidents;
- Opportunities for stronger collaboration between DSOs and TSOs during incident investigations;
- Potential governance models for future incident analysis activities.

Main conclusion of this report, supported by experiences shared by E.DSO members, is that future incident response will require multidisciplinary expertise, stronger TSO-DSO cooperation and greater attention to digital resilience. While physical asset reliability remains essential, the ability to anticipate, manage, investigate and learn from increasingly complex incidents will become a defining capability for future network operators.

Building resilient electricity systems will therefore depend not only on infrastructure investment, but also on integrated governance, collaborative incident management and continuous knowledge sharing across the European energy sector. The best practices and recommendations presented in this paper are intended to support E.DSO members to determine the most effective approach for future incident analysis and resilience cooperation.

Introduction

The European electricity system is undergoing an unprecedented transformation. Rapid deployment of renewable energy sources, electrification of transport and heating, digitalisation of grid operations, and increasing customer participation are creating new operational complexities.

These developments are changing both the causes and consequences of incidents. Whereas traditional outage investigations focused primarily on equipment failures or weather-related damage, modern incidents increasingly involve interactions between:

- Physical grid assets;
- Operational control systems;
- Communications infrastructure;
- Flexibility platforms;
- Distributed energy resources;
- Cybersecurity events.

As a result, incident response is evolving from a primarily engineering-focused activity into a multidisciplinary resilience function.

Policy Context

The discussion was triggered by the increasing recognition at both European and national levels that power system incidents can no longer be analysed solely within traditional organisational and technical boundaries. In E.DSO's Technology and Knowledge Sharing Committee, discussions following the presentation on the Iberian Peninsula incident of April 2025 highlighted ongoing efforts by E.DSO members and the EU DSO Entity to secure and formalize DSO participation in large-scale incident investigations.

This reflects a broader policy evolution in Europe, where the growing integration of distributed energy resources, digital technologies, flexibility markets, and interconnected operational processes is blurring the distinction between transmission and distribution system responsibilities. At the same time, emerging European regulatory initiatives on power system resilience, cybersecurity, and critical infrastructure protection increasingly emphasize coordinated incident management, information sharing, and cross-sector cooperation.

Against this background, participants noted that electrotechnical incident analysis and cyber/resilience incident analysis are currently governed through largely separate processes and expert communities, despite the fact that future incidents are likely to involve both domains simultaneously. The knowledge-sharing session was therefore organised to explore whether existing governance arrangements remain fit for purpose and to provide a basis for recommendations to the E.DSO Board on the possible way forward The knowledge-sharing session was therefore organised to explore whether existing governance arrangements remain fit for purpose and to provide a basis for

recommendations to the E.DSO Board on the possible way forward in incident analysis including considerations of whether future incident investigations should be organised through separate electrotechnical and cyber groups or through a single integrated resilience-oriented framework, including consideration of whether future incident investigations should be organised through separate electrotechnical and cyber groups or through a single integrated resilience-oriented framework.

E.DSO perspective

The session clearly highlighted a common reality across DSO organisations: the increasing complexity of our operating environment driven by digitalisation, climate events, and the growing interdependencies between physical and cyber systems. DSOs perceive that:

- Anticipation is becoming as critical as the response.
- Incident management is no longer only a technical topic. It is equally about organisation, coordination, governance, and decision-making under pressure.
- Learning from incidents is fundamental. Beyond restoring service, the real value lies in DSOs' capacity to analyse events.
- DSOs also see the importance of innovation and new tools, whether in data analysis, automation, or field operation, to enhance both responsiveness and efficiency.

The session confirmed that collaboration across DSOs is essential. The challenges DSOs face are shared, and so must be the solutions. Associations like E.DSO are key to accelerating this. Collective learning helps to build a more resilient European power system.

Key Findings

Incident analysis is expanding beyond traditional outages

The survey among E.DSO members demonstrated that incident investigations are no longer limited to physical power interruptions. The scopes of current investigation increasingly include:

- Power quality disturbances;
- Physical security incidents;
- Cybersecurity incidents;
- Communication failures;
- Disruptions of critical digital services; and
- Smart meter and data platform failures.

This expansion reflects the growing dependence of electricity networks on digital technologies and data-driven processes. Furthermore, responsibility for incident analysis is increasingly shared among:

- Asset management departments;
- Grid operations teams;
- IT organisations; and
- Cybersecurity functions.

The traditional model of isolated engineering investigations is gradually being replaced by cross-functional approaches.

Grid congestion is becoming a major incident driver

One of the strongest messages emerging from the session was the growing significance of grid congestion. Across Europe, increasing deployment of renewable generation, electric vehicles, heat pumps, and flexible demand resources is creating unprecedented loading conditions on distribution networks.

While congestion management has traditionally been treated as an operational planning activity, participants in the Knowledge Sharing session highlighted that persistent congestion can increasingly create conditions resembling incident scenarios. Ambiguity is emerging between planned congestion management measures and emergency protection and restoration procedures.

This overlap introduces uncertainties regarding operational decision making, regulatory compliance and emergency response activation. As congestion becomes more widespread, clearer governance frameworks will be required.

Digitalisation improves flexibility but increases system complexity

All participating DSOs highlighted the importance of digitalisation for future network operation. Digital technologies enable:

- Enhanced visibility of network conditions;
- Faster restoration of outages;
- Remote control of assets;
- Flexibility management; and
- More efficient utilization of network capacity.

However, these benefits come at the cost of increasing operational complexity. Utilities are becoming increasingly dependent on: SCADA systems, GIS systems, Distribution Management Systems (DMS), communication networks, cloud-based services, third-party platforms and assets' data quality.

The result is an expanding attack surface and growing operational dependence on digital infrastructure. Participants agreed that digitalization should not be viewed solely as a technology challenge but as a fundamental resilience challenge.

Cybersecurity risks require a system-wide perspective

Cybersecurity has emerged as a distinct category of risk. Unlike congestion or weather-related events, cybersecurity incidents may occur less frequently but can have significantly broader consequences. Participants noted that cyber incidents may affect simultaneously:

- Control systems
- Monitoring systems
- Communications networks
- Market platforms
- External service providers

Particular concern was expressed regarding the expanding ecosystem of interconnected actors, including:

- Aggregators
- EV charging platforms
- Inverter manufacturers
- Battery operators
- Renewable energy operators

The discussion highlighted that cybersecurity can no longer be considered solely an internal utility responsibility. Instead, resilience increasingly depends on the security posture of the wider energy ecosystem.

TSO–DSO Collaboration will become increasingly important

Current incident investigations generally follow established responsibility boundaries, with TSOs and DSOs investigating incidents within their respective domains.

However, future incidents are expected to involve increasingly interconnected systems. Examples include:

- Congestion-related events;
- Voltage stability problems;
- Flexibility activation failures;
- Digital platform disruptions;
- Cyber incidents affecting multiple network operators.

Participants acknowledged that future investigations may require more integrated approaches that extend across the transmission-distribution boundary.

Emerging Best Practices

Best Practice 1: Dedicated incident analysis capabilities

Fluvius demonstrated the value of maintaining a specialised incident analysis function. Key characteristics include:

- Daily review of incidents;
- Structured incident registers;
- Utilization of operational data sources; and
- Continuous collaboration with control centre personnel.

A dedicated organisational unit work on this within the DSO enables systematic capture of lessons learned and supports continuous improvement across operational processes and asset management.

Best Practice 2: Data-driven crisis preparedness

Enedis presented a mature approach to crisis management based on forecasting and data-driven resource planning. Best practices include:

- Weather-based incident prediction;
- Staffing requirement forecasting;
- Structured crisis escalation procedures;
- Regular training and exercises; and
- Integrated operational command structures.

Forecasting allows organisations to prepare proactively rather than reacting after incidents occur.

Best Practice 3: Multidisciplinary incident reviews

Multiple speakers emphasised the importance of involving diverse expertise in incident investigations. Effective reviews increasingly require contributions from:

- Asset specialists
- Operations teams
- Protection engineers
- IT experts
- Cybersecurity analysts
- Crisis management personnel

This multidisciplinary model reflects the convergence of physical and digital system risks.

Best practice 4: Continuous resilience investment evaluation

Enedis highlighted the importance of measuring the effectiveness of resilience investments. By comparing incident performance under comparable weather conditions over time, organisations can evaluate whether investments in:

- Undergrounding;
- Asset replacement;
- Hardening measures;
- Substation upgrades; and
- Increasing observability of the grid closer to the consumption points

are delivering measurable resilience improvements. Evidence-based investment assessment improves long-term planning and supports regulatory justification.

Best practice 5: Cyber preparedness and contingency planning

Although no significant operational cyber incidents were reported by participating DSOs, several organizations are proactively strengthening resilience through:

- OT monitoring capabilities
- Cyber incident response plans
- Backup communication systems
- Recovery procedures
- Crisis exercises

Preparing for cyber incidents before they occur was widely recognised as a critical resilience practice.

Recommendations

Recommendation 1: Develop integrated incident investigation frameworks

Utilities should evolve from separate electrical, operational, and cyber investigations toward integrated incident-analysis frameworks. Future investigations should routinely assess:

- Physical causes
- Digital system performance
- Communications dependencies
- Human factors
- Cybersecurity implications

Recommendation 2: Strengthen TSO–DSO cooperation on incident management

DSOs and TSOs should establish common approaches for:

- Incident initiation
- Information sharing
- Joint investigations
- Cross-sector lessons learned

Future system incidents are increasingly likely to cross organisational boundaries and require coordinated analysis.

Recommendation 3: Establish clear governance for congestion-related emergencies

Regulators and system operators should clarify when congestion management transitions into emergency system operation. This includes defining:

- Escalation criteria;
- Operator authorities;
- Use of emergency procedures; and
- Interaction with market-based congestion mechanisms.

Clear governance will reduce uncertainty during high-impact events.

Recommendation 4: Adopt a system-wide cyber resilience approach

Cybersecurity governance should extend beyond utility boundaries and include:

- Supply chain participants
- Distributed energy resource operators
- Flexibility service providers
- Technology vendors
- Market platforms

Resilience of the electricity system increasingly depends on the security of the broader digital ecosystem.

Recommendation 5: Enhance knowledge sharing across DSOs

The electricity sector would benefit from more systematic exchange of:

- Incident lessons learned
- Investigation methodologies
- Resilience metrics
- Crisis management practices

An E.DSO knowledge-sharing framework could provide a practical starting point for harmonising approaches and accelerating organisational learning.

Conclusion

European distribution networks are entering a period where resilience challenges are increasingly driven by the interaction between physical infrastructure, digital technologies, operational complexity, and evolving threat landscapes. The traditional distinction between outage management, congestion management, crisis response, and cybersecurity is becoming less clear.

The experiences shared by E.DSO members demonstrate that future incident response will require multidisciplinary expertise, stronger TSO‑DSO cooperation and greater attention to digital resilience. While physical asset reliability remains essential, the ability

to anticipate, manage, investigate and learn from increasingly complex incidents will become a defining capability for future network operators.

Building resilient electricity systems will therefore depend not only on infrastructure investment, but also on integrated governance, collaborative incident management, and continuous knowledge sharing across the European energy sector.