This is the author accepted manuscript of: Wright, J., & Irvine, J. (in press). What can the Heathrow Airport power outage teach us about resilience? IEEE Reliability Magazine, 3(3). https://doi.org/10.1109/MRL.2026.3717886

What Can the Heathrow Airport Power Outage Teach Us About Resilience?

J. R. Wright
University of Strathclyde

J. M. Irvine
University of Strathclyde

***Abstract*—Events with substantial operational consequences can no longer be regarded as rare occurrences, with multiple such disruptions being observed over the past year. The power outage at Heathrow Airport in March 2025 provides a salient example of how interdependent infrastructure systems can experience cascading operational failures. Although electrical power was restored within hours, the delayed recovery of airport operations exposed vulnerabilities in the airport's capacity to manage cascading failures across interconnected systems. Therefore, highlighting the need for a holistic, systems-based approach to resilience planning. This article is a sociotechnical case study of Heathrow Airport's response to the power outage and considers the lessons that must be learned to enhance infrastructure resilience.**

■ **GLOBAL DEPENDENCE** on and expectations for a continuous power supply are increasing. This introduces significant issues for resilience planning. The power system in Great Britain has not experienced a total system shutdown. However, the North Hyde Substation fire in March 2025 disrupted tens of thousands of consumers and exposed the far-reaching interdependence between critical infrastructure systems. These high impact incidents highlight that, despite provisions in Grid Codes designed to enhance energy system resilience, cascading effects can overwhelm existing protection schemes. As such, responsibility for resilient planning can no longer rest solely with the energy system. It requires those who depend on it to actively prepare for and respond to disruptive events, recognising their role within the broader, interconnected system. The Heathrow incident illustrates the importance of this, as the airport did not have a true understanding of the implications of its electricity network connection agreement. Arguably the power network met its resilience requirements of restoration within 3 hours, but the airport did not resume normal operations for 24 hours. Given the difficulties of bringing Heathrow back online and the effect on the UK economy, what lessons can be learnt for planning for resilient interdependent, interconnected systems?

TECHNICAL BACKGROUND

North Hyde forms part of the UK's electricity transmission and distribution infrastructure, comprising two compounds – a 275kV substation compound, managed by National Grid Electricity Transmission, and a compound containing 66kV, 22kV

and 11kV assets, operated by Scottish and Southern Electricity Networks (SSEN). Within the 275kV substation compound there are three supergrid transformers (SGT): SGT1, SGT2 and SGT3. These transformers step down the voltage, from 275kV to 66kV, for distribution.

In accordance with the National Electricity Transmission System Security and Quality of Supply Standard (NETS SQSS) Industry Governance Framework, the 275kV compound at North Hyde is configured such that two transformers, SGT1 and SGT3, operate under load while a third, SGT2, remains on "hot standby", fully energized and ready for immediate activation when required. If a fault occurs within SGT1 or SGT3, SGT2 can be automatically activated without manual intervention. This redundancy allows the substation to maintain operations should an event cause a single fault outage or if a planned outage is followed by a fault outage. These operational standards are commonly referred to as the N-1 and N-1-1 criteria, respectively.

Heathrow Airport operates a separate private internal electrical distribution network. Ownership of this network is shared between Heathrow Airport Limited and UK Power Network Services. North Hyde, also referred to as Heathrow Substation A, is one of three substations capable of supplying power to Heathrow Airport. Under normal operations, the three independent supply points remain separate within Heathrow Airport's internal electrical distribution network (**Figure 1**). Connecting these supply points would expose Heathrow Airport's internal electrical network to immoderate power flows should a fault occur. Therefore, in the event of a fault, the network must be reconfigured.

THE INCIDENT

On 20 March, SGT3 caught fire. Following the incident, reports were produced by National Energy System Operator (NESO Report) and Heathrow Airport (the Kelly Report) to examine the incident [1, 2]. The NESO report attributed the incident to electrical arcing caused by moisture within the bushing. The substation configuration ensured that the loss of SGT3 automatically triggered the activation of SGT2, thereby reinstating a two-transformer supply and ensuring no interruption to customers. However, the close proximity of SGT1 to the fire activated its protection system, resulting in its disconnection from service. Since SGT2 was operating on the same circuit as SGT1, its direct connection to the wider transmission system was also lost. Consequently, 66,919 domestic and commercial customers on the SSEN Distribution Network, along with an additional 4,736 customers served by Independent Distribution Network Operators, including Heathrow Airport, experienced a loss of power. This power loss rendered several airport terminals and IT systems non-operational. Power to Substations B and C was maintained throughout the event.

According to Heathrow Airport's licence with the Civil Aviation Authority (CAA), if the licensee deems

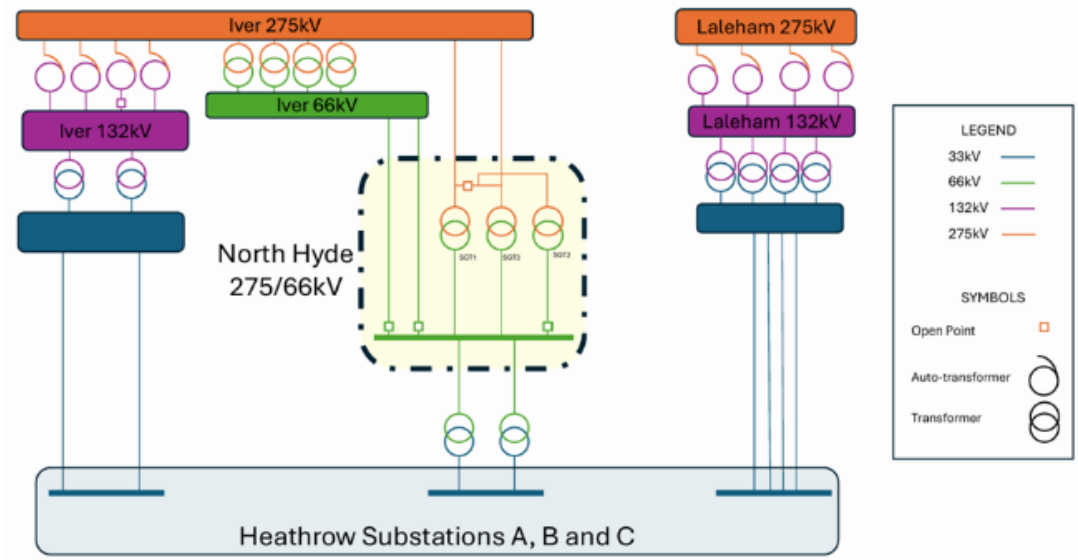

Figure 1. Network Configuration and Supply to Heathrow Airport [1]

that the airport cannot be operated safely, it should be closed. A decision was made to stop operations and close the airport until the situation was better understood. The airport's backup power systems automatically engaged to maintain escape lighting, operate the Air Traffic Control Tower and support other safety-critical systems. Simultaneously, engineers commenced reconfiguration of Heathrow's electrical network. Once power had been restored, safety-checks were carried out to ensure safety-critical systems were fully operational prior to passengers arriving at the airport.

The power outage and decision to close Heathrow Airport had a cascading impact on other services. The Heathrow Express rail service was restricted exclusively to airport staff, road closures were implemented to prevent public access to the airport, and many flights were diverted or cancelled. These measures, deemed essential for response efforts and safety, triggered cascading operational challenges: staff experienced delays in reaching critical work areas, the availability of ground support and logistics services was reduced, locals faced severe traffic delays, and pressure mounted on local hospitality services and other airports. This scenario illustrates how a single point of failure can cascade into a system-wide operational crisis.

North Hyde restored power to more than half of the affected customers within one hour and reinstated supply to the remainder in under 12 hours. By contrast, Heathrow Airport remained closed for approximately 18 hours beyond their normal night flight restrictions. This disparity in performance raises critical questions regarding the airport's understanding of its own systems and the extent to which those systems were effectively and fully tested.

PILLARS OF RESILIENCE

A critical review of resilience literature reveals recurring themes and challenges, leading to key conclusions about the practical assessment of resilience in complex systems such as Heathrow Airport. Five foundational pillars appear to underpin the concept of resilience: definition and context, time, bias, risk and uncertainty, and cost (**Figure 2**).

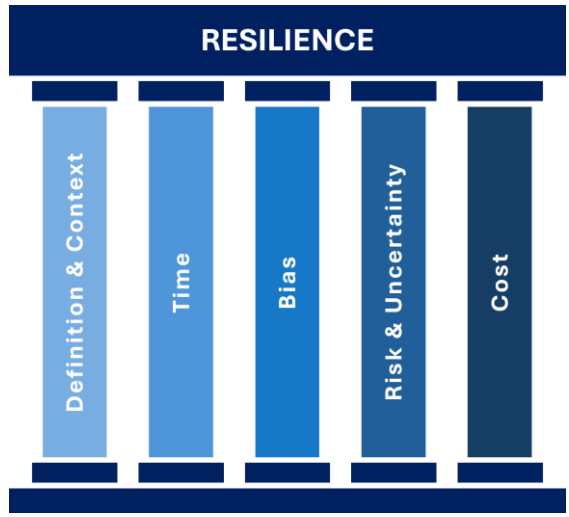

Figure 2. Five Pillars of Resilience

Definition and Context

The diverse interpretations of resilience make achieving a shared, consistent understanding difficult. Individual approaches to resilience produce different interpretations resulting in a collection of incomparable measurements, disparate crisis responses and, potentially, limited system insight. This is reflected in responses to the North Hyde Substation fire.

Consideration of various definitions of resilience can shed light on factors that contributed to this incident. The UK Government defines resilience as "the ability to anticipate, assess, prevent, mitigate, respond to, and recover from natural hazards, deliberate attacks, geopolitical instability, disease outbreaks, and other disruptive events, civil emergencies or threats to our way of life" [3]. Since Heathrow Airport is classified as critical UK infrastructure, it is reasonable to assume that the airport is bound by the UK's official definition of resilience. However, there is no evidence to suggest that this is the case.

The CAA is responsible for regulating all UK airports to ensure they comply with relevant international and UK safety standards. Therefore, it could be argued that responsibility lies with the regulator to articulate and enforce such a definition. Heathrow Airport was granted a license to act as an airport operator under the Civil Aviation Act 2012 [4]. This license puts a requirement on Heathrow to "provide operational resilience", which is defined as the ability to "secure the availability and continuity of airport operation services at Heathrow Airport, particularly in times of disruption." [4] These multiple overlapping definitions create a lack of clarity, making

it challenging to establish a unified understanding of resilience and to operationalize it consistently across different contexts. If the concept of resilience is not clearly and consistently defined by all statutory bodies, compliance by regulated entities is unlikely, if not impossible.

Heathrow claims to operate a “resilient airport” [2]. Although neither the NESO nor Heathrow Airport explicitly define resilience in their post-incident reports, potential definitions may be inferred from the reports’ content.

The Kelly review refers to re-establishing “full operations” and that a “firm connection” should be maintained [2]. “Full operations” is defined as the requirement for all safety systems to operate across the whole passenger journey. This was interpreted to mean that Heathrow operates in an ‘all-or-nothing’ manner. There is no allowance for a degraded or partial service, thus placing considerable, if not impossible, demands on both infrastructure and personnel.

The power outage necessitated the operation of contingency plans. However, these plans were resource intensive. This is evidenced by the observation that “there were not sufficient people available throughout the night to put so many contingencies in place at the same time.” [2] A plan that cannot be implemented effectively for the scenario it has been designed to address can be considered a futile contingency plan. Thus, illustrating a fundamental vulnerability in Heathrow’s operations and lack of resilience.

According to the Energy Networks Association and the European Network of Transmission System Operators for Electricity, a “firm connection” is a connection that remains available in a first fault scenario (N-1 criterion). Likewise, the UK electricity Grid Code states that if a partial or total shutdown occurs without prior planning, it is considered an emergency. In this context, the term 'firm' is, again, used to describe a connection that remains available in a first-fault scenario. As described in the technical background, North Hyde was configured to comply with these specifications. The Kelly review states that in the event of a disruption to a “firm” connection, the “obligations remain with the electricity supplier to provide resilient power to Heathrow.” [2] However, according to the CAA license, Heathrow Airport is obliged to “secure the availability and continuity” of its services and “set out reasonable expectations of what it requires from its partners.” [4]

Given the emergency context, it is unreasonable for Heathrow to expect an “uninterruptible” supply to each of its supply points. Again, reinforcing the all-or-nothing operational expectation, whereby reinstating the three electricity supply points served as the prerequisite for restoring business-as-usual operations. A comparison of these assumed resilient states highlights that Heathrow Airport has yet to establish a clear and consistent definition of resilience.

The NESO report does not provide an explicit definition of resilience. It refers to robustness and redundancy and recognizes that there is a need to establish a common definition going forwards. SSEN successfully contained the outage, limiting it to the local system and preventing any impact on the wider grid. This is consistent with the requirements of the NETS SQSS. Furthermore, monitoring mechanisms exist through the Priority Services Register, enabling proactive engagement with individuals identified as particularly vulnerable to power outages. Individuals who were not enrolled in the Priority Services Register but nonetheless affected by the outage had the option to contact the helpdesk for assistance. On average, calls were answered within 69 seconds, demonstrating the responsiveness of the support system in addressing the needs of those impacted.

Despite the lack of definition, none of the operators (NESO, National Grid Electricity Transmission and SSEN Distribution) appear to have challenged Heathrow Airport's underlying assumption that a continuous, uninterrupted electricity supply would always be available. They were also “not previously aware of the detail of Heathrow Airport’s internal electrical distribution network configuration, or the potential impact of losing a supply point.” Whilst Heathrow’s operations and response are not their responsibility, these organizations do have an obligation to understand consumer expectations and cannot assume that critical dependents will be able to cope. Where entities presume continuous electricity availability, targeted intervention is required to ensure that such expectations are realistic and that appropriate contingency measures are in place. Therefore, NESO, National Grid Electricity Transmission and SSEN Distribution should develop a more thorough understanding of customer assumptions and expectations.

Overall, Heathrow fundamentally lacked a definition of resilience. Without a clearly defined

baseline, it is impossible to measure or manage operational performance effectively. This deficiency was compounded by the absence of a shared understanding between Heathrow Airport and NESO regarding what constitutes a resilient supply. This highlights a critical gap in coordination and shared criteria necessary for ensuring system resilience.

Time

Time is a fundamental factor in the evaluation of system resilience as it is an inherently dynamic concept. Measurement approaches that incorporate a time dimension are often retrospective, rather than prospective, thus delaying possible preventative actions achieved by live observations. Mathematical models, such as the resilience curve, assess metrics like failure duration and recovery time [5]. Metrics do not answer the underlying question of whether a system is resilient. Instead, they provide evidence against which progress towards clearly defined performance goals can be assessed. It is therefore incumbent upon each organization to define what resilience means for its particular circumstances and objectives. Only then should the quantitative goals, indicators, and measurements that are most relevant to assessing that capability be determined. At the same time, any such metrics should be interpreted with appropriate recognition of their underlying assumptions and inherent limitations.

As a result of the power outage, Heathrow Airport was closed for a day (**Figure 3**). This extended closure was partly attributable to Heathrow's limited monitoring capacity, which left the organization unaware of the operational state of its systems. A significant portion of the recovery period was devoted to sequentially restarting systems, one at a time, to identify any system damage. Limited real-time monitoring capabilities most likely resulted in greater reliance on judgment-based assessments rather than on objective data.

Heathrow has a voluntary ban in place that prevents flights scheduled between 04:30 - 06:00 from landing before 04:30. Departures are also not scheduled between 23:00 - 06:00. This offers a six-hour time frame for testing or crisis simulations to take place. However, it appears that the procedures for electrical switchover had not been adequately tested, and the airport failed to recognize that it had introduced single points of failure within its electrical infrastructure. Consequently, there was a complete loss of operational availability, breaching the CAA's requirement to preserve operational continuity under disruptive conditions. Ultimately, Heathrow was unprepared.

On the other hand, SSEN restored supply to customers very quickly, achieving restoration for over 50 percent of affected customers within approximately one hour, even though the equipment at North Hyde had not "recovered". NETS SQSS specifies that restoration following a secured event must be completed within three hours, a requirement that was met successfully. Additionally, the event was contained within secure limits, with all protective measures functioning as intended, and the restoration of systems was carried out swiftly. This flexibility, or adaptability, was possible due to the additional redundancy that had been implemented within the network design.

The power sector maintains a clear commitment to three-hour service restoration, and they make a

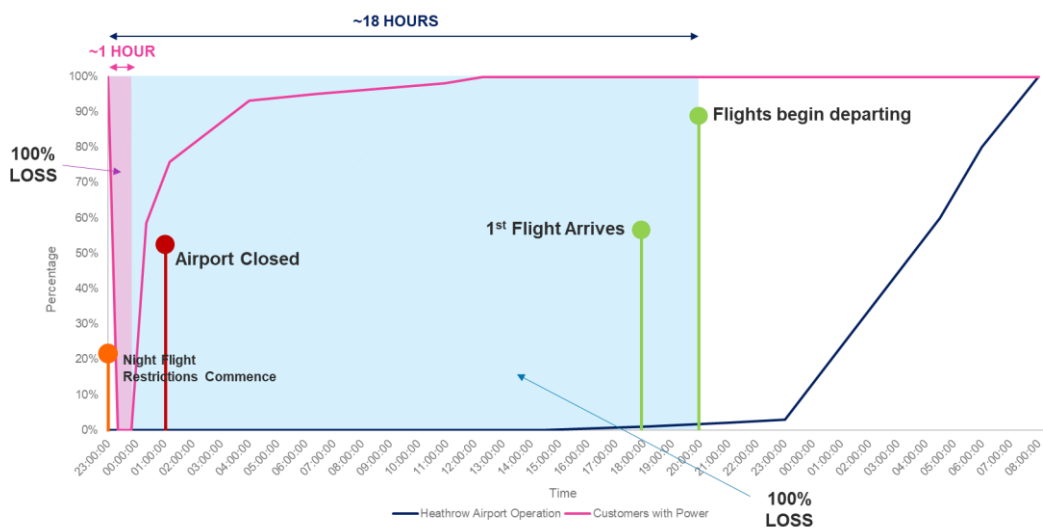

Figure 3. Power Outage Rebound Curve

consistent effort to honor that standard. Heathrow, by contrast, neither recognized this level of expectation nor delivered anything comparable.

Time is also an important consideration for the lifecycle of equipment. The NESO report noted that previous moisture readings from the failed SGT indicated an urgent need for replacement to mitigate the risk of future failure. Although the reading was recorded, the necessary repairs were not implemented. As more CNI equipment nears the end of its lifecycle, timing becomes increasingly critical. It is essential to assess how testing and upgrades should be prioritized during this period to ensure that potential points of failure are not overlooked, as occurred at North Hyde.

Bias

The perceptions of what occurred throughout outage varied across the organizations involved. Heathrow described the power outage caused by fire as an "unprecedented event" [2]. NESO recognizes fire as a major risk, noting that transformer fires occurred in 2015 and 2013, albeit for different reasons. These differing perspectives shaped how they perceived, assessed and responded to the situation, thereby demonstrating bias. This bias affected both expectations and decision-making that led to outcomes that reflected their assumptions rather than an objective assessment of the system's vulnerabilities.

In 2023, Heathrow Airport ran an in-house resilience training exercise on the risk of a National Power Outage, along with Airport community stakeholders and emergency services. However, this exercise obviously did not identify the issues which occurred in March 2025.

When a scenario is designed by those familiar with the environment, it is likely to contain underlying biases and assumptions. Consequently, relying solely on internally generated scenarios must inevitably result in blind posts and other limitations. With so much at stake, external perspectives and diversity of thought are paramount for assessing system resilience to ensure assumptions are challenged and overlooked vulnerabilities are discovered.

Another unnecessary cause of failure is the decision-making framework adopted by Heathrow – the Emergency Services Joint Decision Model (JDM; **Figure 4**). The JDM originates from the Joint Emergency Services Interoperability Principles (JESIP) Joint Doctrine, developed in response to the Civil Contingencies Act (2004) [6]. It was designed to enhance coordination and interoperability among UK emergency responders during multi-agency incident response scenarios. As stated at the outset of the Joint Doctrine, the publication "is not intended as a response document; it is not suitable for referring to during an incident." [6] Rather, its purpose is to support the development of local training, policies and procedures, and aims to enhance interoperability through the consistent application of shared models and principles.

Figure 4. The Joint Decision Model [5]

Heathrow Airport employed the JDM as a mechanism for crisis decision-making, despite its prescribed function as a training and planning framework. The model was printed and displayed around the Airport Operations Control Centre for employees to use during the incident. This raises several critical questions: How were employees taught to use the model? Who holds responsibility for its application? What mechanisms exist to translate decisions into actionable steps? It appears that the principles were never effectively integrated or tailored to Heathrow Airport's own crisis response framework.

Reliance on the abstract guidance left interpretation to individual employees, leaving significant scope for cognitive bias. Rather than fostering coordinated action towards a shared objective, the approach is likely to have promoted existing assumptions and facilitated isolated decision-making during the crisis.

No approach is likely to be entirely consistent,

completely free from bias or misinterpretation, or guaranteed to produce the same course of action every time. However, until a common understanding of resilience is established and sufficient analysis of the system has been conducted, Heathrow Airport's crises responses will remain constrained by organizational biases.

Risk and Uncertainty

Risk is often conflated with resilience; defined as the likelihood and consequences of some future anticipated system perturbation. Whilst risk does not capture the full extent of system behavior, it should form part of an organization's resilience study. It allows for a structured exploration of possible future scenarios, assessment of their potential impacts and identification of uncertainties and gaps in our current understanding. Risk appetite varies across organizations, industries and economies. It is shaped by differing cultural perspectives and the balance between 'protecting' systems from the consequences of loss and potential success of innovation. As such, there needs to be consideration for our own acceptance of risk and well as consideration for the risk introduced into a system that may have a cascading rather than immediate effect.

Heathrow Airport acknowledged the potential for power loss, categorizing it on the risk register as a high-impact, low-likelihood event. Such events are characterized by their severe consequences, which could result in extensive power disruptions and significant financial losses. The associated uncertainties are considerable, owing to limited knowledge about both the probability of occurrence and the potential societal impacts should such an event take place. Therefore, it is common for organizations to prioritize risks perceived as unlikely to occur, particularly when operational capacity and resources are constrained. The resulting risk measurement bias can distort risk perception and lead to decisions that undermine long-term resilience.

Low probability events also challenge decision-making, as it can be difficult to justify investing in precautions for something that appears remote. The maintenance of North Hyde fell victim to this mindset as it was pushed aside in favor of risks that seemed more pressing at the time, despite fire being recognized as a major risk. High-impact, low-likelihood risks warrant attention as failing to manage them effectively could jeopardize the survival of an organization. This highlights the need for strategies that monitor remote risks to ensure maintained continued operation of assets in the event such incidents occur.

The broader, cascading consequences of the outage also appear to have been insufficiently evaluated by Heathrow Airport within its risk assessment. The planned business continuity measures, such as road closures and resource-intensive protocols, appear misaligned with practical considerations. Whilst the overall risk of power loss had been recognized, the specifics of outage duration and its precise impact on operational systems were less well understood by staff outside the technical team. This raises critical questions about who truly understands the risk and how this information is communicated across the organization to ensure informed decision-making and effective response. Major events have the potential to severely disrupt interconnected critical systems, potentially leading to widespread societal breakdown. Therefore, incorporating systemic impacts into risk assessments is essential.

Cost

Cost considerations play a critical role in shaping an organization's decisions and policy directions. Without an understanding of cost, it becomes impossible for organizations or governments to effectively assess which goods and services can be delivered, to what extent, and over what duration. The costs involved in ensuring system resilience across a range of possible futures can be substantial. In a world where there is growing pressure to move faster, improve quality and lower costs, organizations often face a trade-off: invest proactively in resilience measures or avoid upfront costs and risk potential supply disruptions and higher costs in the face of unforeseen events.

Costs can be manipulated. Overstating costs can serve as a protective measure for an organization, preventing the erosion of profit margins in the pursuit of securing business. In 2024, Heathrow announced a £2.3bn accelerated investment plan to upgrade the airport. Energy was identified as a key focus of this investment as the airport seeks to meet Net Zero objectives and future-proof operations against the anticipated substantial increases in electricity demand. However, as a result of the power outage, Heathrow claims that it needs at least an additional £1bn to build a high voltage ring around the airport's internal distribution network for "full resilience". This claim is highly questionable, as resilience cannot be

adequately captured in purely financial terms, and there is little evidence that the proposal has undergone rigorous evaluation or consideration for alternatives solutions.

Similarly, target costs can be used to "inject downward bias" on costings. To compete, and win, in the market, downwardly biased standards encourage innovation and improvement towards greater efficiency and cheaper overheads. Following a funding request in 2018, Ofgem permitted the National Grid Electricity Transmission's request for £18.65 million, plus indirect costs, to invest in advanced monitoring technologies. The criteria for prioritising this technology on certain sites over others was based on factors such as asset population, asset age and historical performance data. North Hyde did not meet the defined criteria. Prior to the incident, National Grid Electricity Transmission assigned SGT3 an end-of-life score of 12.7 out of 100, with higher scores indicating greater proximity to the end of operational life. Based on this assessment, there was no impetus to replace or retire the transformer. Notably, replaceable components are excluded from end-of-life calculations, therefore the state of the transformer bushings had no impact on the score of STG3. The transformer's reported end-of-life score seems incongruous with its documented condition. At 57 years old, with deferred maintenance and faults necessitating urgent removal from service, the low score implies either an unreported major refurbishment or a systemic underestimation of risk within the scoring framework.

This assessment may have resulted from the energy regulator's, Ofgem, desire to deliver networks at the "lowest **possible** cost to consumers" rather than the "lowest **reasonable** cost". Thus, a tension arises between companies setting prices that allows for the recovery of investments made to improve resilience or secure supply in uncertain future conditions and ensuring that prices stay fair and reasonable. Too often, the approval and review of spending decisions don't fully consider the need to balance a wider set of policy objectives, such as financial stability and customers affordability, in addition to system resilience.

Decisions are often based on agreed assumptions regarding current or future conditions (derived from historical data), followed by a comprehensive analysis of potential options before selecting a course of action that best satisfies a set of objectives. Imperfect data sets and limited access to experts make this process challenging to complete (at pace), often leading to a focus on gathering more information to enhance the accuracy of predictions and future actions. As such, decisions are seldom made. There is a need for a more flexible, iterative approach to financial decision making.

LESSONS LEARNED

The Heathrow case demonstrates that resilience in interdependent infrastructure systems is shaped not only by technical capacity but by governance structures, coordination mechanisms and decision-making processes under uncertainty. Misaligned expectations and limited situational awareness affected the system's ability to respond and recover. This predicament is not unique to Heathrow Airport and provides actionable lessons for resilience planning across other critical infrastructure systems.

1. Different Definitions of Resilience

The Heathrow Airport case study demonstrates that organizations hold fundamentally different interpretations of resilience. There is no single correct definition of resilience; rather, organizations must identify the definition that best fits their context and ensure it is consistently understood across teams. This interpretation should be communicated to the organizations with which they interact so that differing perspectives are visible and can be accounted for in resilience planning.

2. Lack of System Awareness

The time required for system restoration is strongly influenced by operational visibility. Increasing observability reduces cognitive load during crises. It allows engineers and operators to focus on corrective actions rather than reconstructing or retesting the whole system under pressure. When downtime has a direct financial impact, delays caused by uncertainty about system structure amplifies losses. Documenting known system dependencies and creating comprehensive network diagrams provide an operational picture, enabling faster, more informed interventions, which supports resilience and efficiency during disruption.

3. Inflexible Operations

A reliance on procedures designed exclusively for business-as-usual conditions constrains operational flexibility during disruption. The decision to shut down the entire airport can be interpreted as a knee-jerk

response, reflecting action bias and limited preparation for degraded modes of operation. Explicitly identifying minimum viable operations provides a basis for maintaining continuity under disruption and avoiding unnecessary system-wide shutdowns. Instead of focusing on specific disaster scenarios and risk calculations, organizations should focus on identifying the most critical system components and sub-systems required to sustain essential functions and the measures required to protect these systems.

4. Shortage of Exercising

Testing your system is important to understand where gaps and weaknesses exist. To test a system effectively, the sociotechnical system must be exercised as a whole. This includes testing decision making and behaviors of people within the organization. Crisis management playbooks, which often detail organizational instructions for defined scenarios, can create a sense of comfort and confidence in ability. Responding to defined scenarios is not resilience as incidents rarely play out as imagined. Guidance is constrained by its temporal context and may fail to address the conditions of evolving systems. Organizations should therefore populate their playbooks with clear architecture and systems diagrams that capture dependencies, interfaces and operational boundaries. These artefacts support faster and more effective decision-making by providing a shared structural reference during time-critical situations.

5. Poor Cooperation Across Boundaries

Critical infrastructure organizations no longer operate as isolated, self-contained entities but as components of wider enterprise networks characterized by dense technical, organizational and regulatory interdependencies. In such systems, groupthink is an organizational hazard, particularly where overlapping responsibilities and shared mental models remain untested. Joint initiatives, such as shared costing frameworks, coordinated response planning and cross-organizational stress testing, help expose divergent expectations and latent conditions that can undermine system performance. Learning from disruption also requires moving beyond counterfactual narratives focused on what should have occurred, which can reinforce blame and inhibit inquiry. In multi-authority environments, a blame-oriented culture complicates learning and obscures systemic contributors to failure. Resilience planning is therefore strengthened by governance arrangements that prioritise collective learning, transparency and the exploration of event dynamics over fault attribution.

CONCLUSION

In conclusion, the Heathrow Airport power outage serves as a powerful reminder of the lessons that need to be learned to create resilient systems.

The primary issue highlighted by the Heathrow case was the absence of a shared understanding among the organizations involved. Each entity operated with its own implicit definition of resilience and a distinct system perspective, resulting in a fragmented approach in which the parties were, in effect, addressing different problems rather than working toward a common objective. This was evident in Heathrow's response which revealed a limited capacity for adaptability, characterized by an overriding focus on restoring normal operations rather than embracing flexibility and learning in the face of disruption. Since the concept of resilience entered engineering and political discourse, both quantitative and qualitative methodologies have been employed in efforts to measure system resilience. Each method introduces its own challenges: quantitative methods tend to translate complex, multidimensional systems into numerical metrics, often at the cost of oversimplification; whereas qualitative approaches contend with inherently ambiguous, context-dependent and often non-comparable definitions and opinions. Ultimately, it is the underlying logic of a resilience perspective that holds the greatest value, not the fine detail.

Modern systems are complex, dependent on each other to function. This entanglement necessitates systems thinking and cooperation across boundaries. Systems should be examined at various levels – from individual components to entire systems and networks of systems – and across different scales. It is essential to rigorously test systems to identify vulnerabilities and weaknesses. In the case of Heathrow, the absence of effective testing meant that critical system gaps remained unknown, limiting the organization's ability to anticipate and respond effectively. The processes of assessment must also be iterative and conducted regularly to continuously monitor system behavior (**Figure 5**). In that way, the impact of causing global events based on local decisions can be considered. Ideally, ongoing assessment should not be rooted in the same methodologies.

A refreshed approach to resilience is necessary – one that integrates both quantitative and qualitative

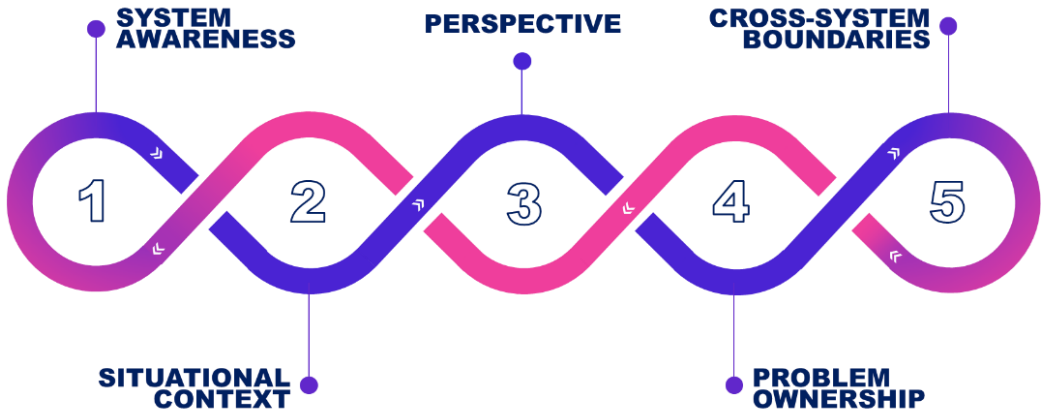

Figure 5: Considerations for Resilience

methods without losing sight of the broader system context. Measurement is important to achieve this, but the goal of resilience assessment extends beyond producing risk scores, rankings or exact values. It should enhance the assessor's understanding of the underlying problem, associated dynamics, inherent uncertainties and areas that require further exploration or research. In this way, assessment becomes a tool for learning and reflection.

We must relinquish the desire for complete control and acknowledge the inherent complexity of systems. What matters is recognizing that our decisions have significant impact on systems beyond our boundaries. No approach is likely to be entirely consistent, completely free from bias or misinterpretation, or guaranteed to produce the same conclusions every time. Until a common understanding of resilience is established, it is unwise to put too much faith in rigorous quantification, or we risk drifting into failure. There is an element of art to determining resilience.

■ REFERENCES

1. "North Hyde Review Final Report", National Energy System Operator (NESO), London, UK, 2025. Accessed: Aug. 4, 2025. [Online]. Available: https://www.neso.energy/publications/north-hyde-review
2. "Kelly Review Report", Heathrow Airport Holdings Limited, London, UK, 2025. Accessed: Aug. 4, 2025. [Online]. Available: https://www.heathrow.com/content/dam/heathrow/web/common/documents/news/Kelly-Review-Report-May-2025.pdf
3. "The UK Government Resilience Action Plan", HM Government, London, UK, 2025. Accessed: Aug. 5, 2025. [Online]. Available: https://www.gov.uk/government/publications/uk-government-resilience-action-plan
4. Civil Aviation Authority, Licence granted to Heathrow Airport Limited by the Civil Aviation Authority under section 15 of the Civil Aviation Act 2012 on 13 February 2014 [Online]. Available: https://www.caa.co.uk/media/tmzmc45t/heathrow-licence-01sep2024-final.pdf
5. M. Bruneau et al., "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," Earthquake Spectra, vol. 19, no. 4, pp. 733–752, November 2003. doi: 10.1193/1.1623497
6. "Joint Doctrine: The Interoperability Framework", Joint Emergency Services Interoperability Principles (JESIP), London, UK, 2024. Accessed: Aug. 5, 2025. [Online]. Available: https://www.jesip.org.uk/downloads/joint-doctrine-guide/

Jane Wright is with the University of Strathclyde, Glasgow, UK, where she is currently pursuing a PhD in Electrical and Electronic Engineering. Her research focuses on enhancing resilience of critical infrastructure with practical application to the power sector. She has worked across government and industry as a security consultant and has previously published a paper evaluating critical infrastructure security policy. Her expertise has led to representation at international conferences and presentations at the Houses of Parliament. She is a member of the IEEE. Contact her at jane.wright@strath.ac.uk.

Dr James Irvine is Academic Lead for the Communications Theme at the Power Networks Demonstration Centre at the University of Strathclyde in Glasgow, where he obtained his BEng (Hons) and PhD in 1989 and 1994 respectively. He is research focuses on wireless radio resource management and cryptography, with applications to transport and power networks, and he works on the Centre for Doctoral Training on the Resilience of Digital Infrastructure with the University of Surrey. A co-author of two books, seven patents and over 200 technical papers, Dr Irvine has given evidence in the UK High Court in cases involving 2G, 3G and 4G technology disputes, and has acted as a non-testifying expert in the US, The Netherlands and Germany. He was General Co-chair of IEEE WCNC2023, and has delivered courses on standards development on five continents. He is a senior volunteer in IEEE, being president of IEEE VTS 2008-9, and chairing the TAB/PSPB Products and Service Committee 2021-4. He currently chairs the PSPB Strategic Planning Committee. Contact him at j.m.irvine@strath.ac.uk.