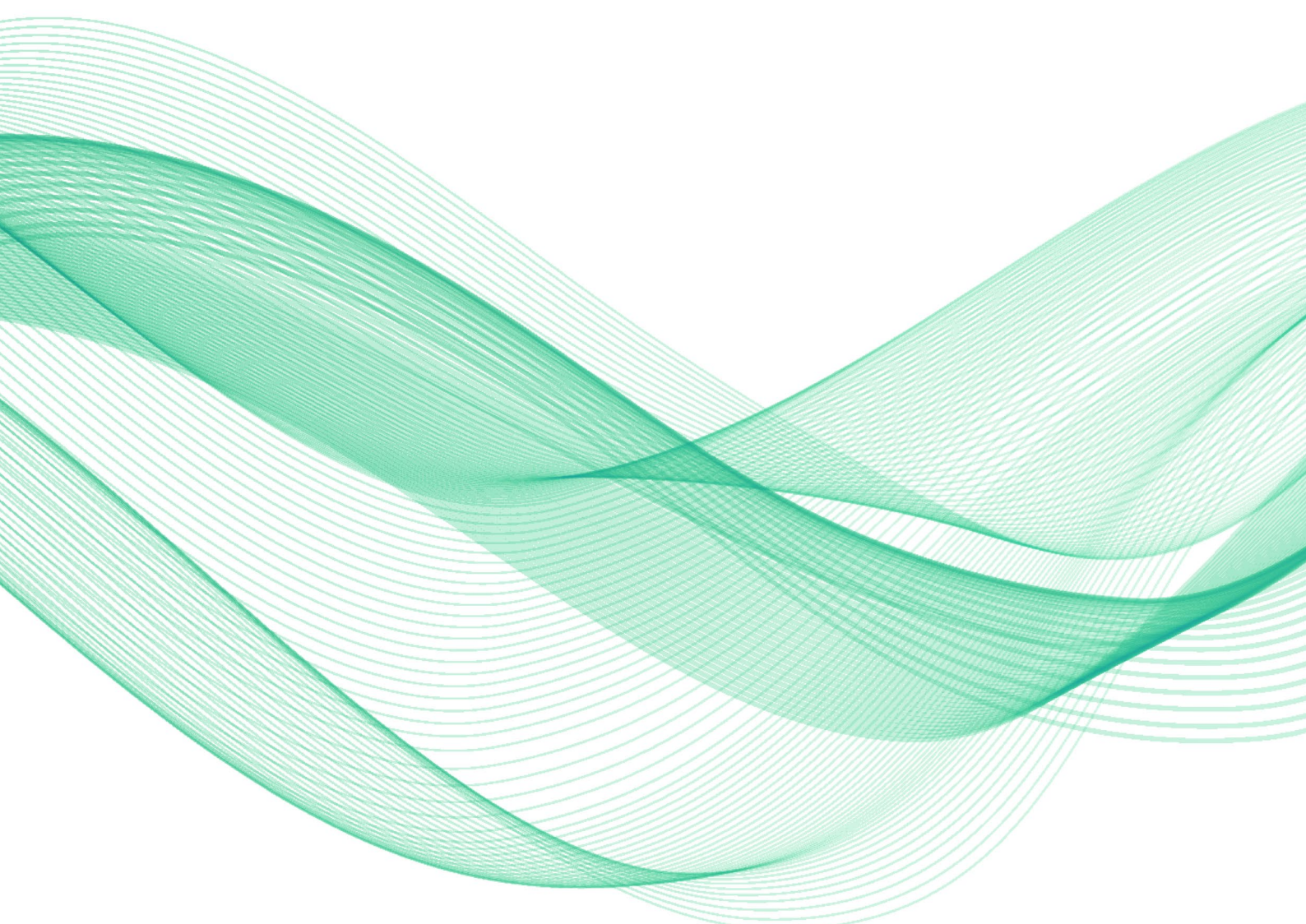


Communications – the digital backbone of the distributed energy system

Considerations of approaches for mission
critical communications solutions



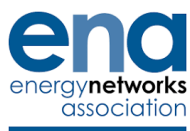
Foreword

“A clean, affordable, secure and resilient energy system supported by digital technology, depends on reliable communications solutions. These solutions provide the effective visibility, control and coordination required for real-time operations and restoration of increasingly dynamic electricity networks.

Today’s report from Energy Connect is an important step in the journey towards these solutions as it highlights the foundational role of communication. It provides practical analysis on the mission-critical use cases, their requirements and the potential approaches to meet those requirements.”

Lawrence Slade

CEO, Energy Network Association and board member for Energy Connect





“The energy system is transforming; networks and in particular electricity distribution networks are undergoing unprecedented change as the UK transitions to a digitalised, affordable and low-carbon distributed energy system. Telecoms are the backbone infrastructure to this future energy system. Without resilient communications real-time visibility and control of the networks are lost, impacting automation and flexibility.

This report considers different potential communication approaches against the mission-critical requirements, and analyses different operating models for dedicated mobile networks implemented internationally.

With this report we are spotlighting areas for further consideration that need to be addressed to ensure energy networks have the mission-critical telecom solutions they need to achieve UK energy security and resilience objectives.”

Cristina Data

CEO, Energy Connect (previously JRC)



The energy system is transforming

UK energy networks are undergoing unprecedented changes, to deliver a low-carbon, affordable, flexible, secure and resilient energy system.

As renewable generation, energy storage, electric vehicles and other distributed energy resources connect across the network, both supply and demand are becoming increasingly variable and decentralised. This is making the electricity system more dynamic, complex and challenging to operate than the largely predictable system of the past.

Managing this complexity requires intelligent and connected networks. Visibility and control are fundamental to secure system operation; visibility to understand, and control to enable timely action. Without resilient communications visibility is lost, automation becomes ineffective, resilience decreases, restoration slows and customer connections take longer. The resilient communication infrastructure underpinning the energy networks is therefore a critical part of the digital backbone of the future energy system.

Electricity distribution networks are at the centre of this transformation. Historically power flowed in one direction from a relatively small number of large, centralised power stations to where it was needed. Today, generation, storage and flexible demand

are increasingly connected directly to distribution networks, creating multidirectional power flows and requiring much greater real-time coordination and control.

At the distribution level, core systems such as Supervisory Control and Data Acquisition (SCADA), Active Network Management (ANM), and mission-critical operational voice communications remain fundamental to both day-to-day network operation and restoration following faults and outages. These systems play a vital role in maintaining network reliability, minimising customer minutes lost and customer interruptions and enabling the efficient and affordable delivery of electricity to UK homes and businesses, further leveraging market flexibility. As distributed energy resources proliferate through medium and low voltage layers, these core capabilities are evolving beyond monitoring and reactive control. Increasingly they are being enhanced by edge computing and AI supporting automated fault detection, predictive asset management, dynamic capacity management, and real-time monitoring of network performance and power quality.

Extended visibility and control are driving mission critical telecoms requirements

Distribution Network Operators (DNOs) operate in a diverse communications environment that combines public and private, wired (copper & fibre) and wireless, terrestrial and non-terrestrial communications services. They employ the service or services which best address each use case for their widespread operational needs, including using redundant routing if a primary service fails.

Meeting the needs of the most critical use cases is increasingly challenging as distributed renewable generation, energy storage and other flexible resources proliferate across dispersed geographical areas, driving a more dynamic and low inertia system. As we continue the electrification of our economy and society, the architecture of the electricity system changes and the communication solutions need to change with it.

A move to modern 4G and 5G based technology presents an opportunity to replace older communications infrastructure with potential limitations in terms of resilience, cyber security and capacity.

In this report we focus on those elements of communication networks that are necessary to support the mission-critical uses underpinning real-time grid monitoring, control and restoration. They are essential to maintaining system security

and reliability and must extend as assets become more geographically dispersed and the operational boundary of the electricity network expands across the UK.

These are:

- Resilient wide area power backup.
- Latency requirements and guaranteed timely delivery.
- Assured, high availability coverage that reaches the assets.
- Security.

These elements enable critical communications to continue after a grid-power outage for the 72 hours necessary to achieve the Energy System Restoration Standard and ensure critical control and visibility communications are guaranteed to be delivered securely to widespread assets.

Different approaches raise different points for consideration

Government are considering a range of options to meet the telecoms requirements of the energy sector; we have considered three approaches for our analysis as outlined in table 1. This report considers these approaches as standalone options, and for each approach, highlights areas requiring further consideration to ensure the mission-critical telecoms needs of the energy networks are met.

Table 1: Approaches to the provision of mission-critical telecoms for the energy networks

APPROACH	KEY CONSIDERATIONS
Reinforced public mobile	• Delivery of end to end 72-hours power resilience across all comms elements (access, backhaul and core) in light of Ofcom's cost analysis. • Prioritisation of guaranteed traffic with low and stable latency. • Coverage of energy assets, often remote, indoor and below ground level and uplink limited. • Isolation to ensure security of utilities traffic.
Emergency Services Network (ESN)	• Current ESN's resilience to be assessed against energy asset requirements. • Prioritisation of guaranteed traffic with low and stable latency. • Coverage to remote, indoor and below ground assets and uplink limited. • Isolation to ensure security of utilities traffic. • Timing of deployment of service for energy against completion of ESN delivery programme for Home Office, scheduled for end of 2029. • Governance and decision making between the different sectors. • Emergency services and energy sector critical communications on one shared infrastructure, creating a single point of failure.
Mission critical private mobile network	• Latency, coverage, traffic isolation and power resilience are built in by design. • Deployment and operating models will need to be established, and governance agreed by the sector. • Requires dedicated spectrum and a pipeline for future growth. • Communications operations requires sufficiently resourced, specialist skilled workforce.

For over 5 years Energy Connect and the Energy Networks Association¹, through its Strategic Telecommunications Group, have supported the case for private mobile networks to address the specific requirements of electricity networks

including smart grid, distributed generation and a whole energy system approach on the basis that they are a cost-effective way of meeting the networks' requirements.

¹ Operational telecommunications – Energy Networks Association (ENA).

Focus on dedicated mobile networks: different working deployment and governance models

Utilities across several European countries, and beyond, are deploying dedicated, mission-critical private networks for their grids, increasingly framed as a matter of energy security and national resilience.

The utilities studied need to be resilient during outages; they need guaranteed delivery of critical communications unaffected by network congestion, secure, affordable and capable of wide area and deep indoor coverage to reach dispersed and often hard to access assets.

Different models have been deployed internationally; from a single DNO owning and operating their own private network, to a utility-owned and operated national network built from regional infrastructure, and a single national network and operator which is owned by the DNOs.

We selected these three examples as they outline a range of different working models for undertaking the functions that would be necessary to deploy and run these communications networks. Additional models are analysed in section 5.

A nationwide dedicated network – Germany

The German policy approach treats communication as an enabler for digital transformation of the grid, in response to the priority placed on the Energiewende – the German energy transition.

Germany has designed, built and now operates a **nationwide dedicated private mobile** 4G network for critical infrastructure. The network is owned and operated by 450connect GmbH, a national operator which itself is owned by the utilities that are the primary users of the network.

The network is largely complete; it covers around 96–98% geographic coverage of Germany using a planned 1600 sites.

The German network is a specialised, limited capacity network, with low band coverage requiring an order of magnitude fewer sites than a public commercial network; it provides a resilient and secure solution for the mission critical needs of the electricity sector, and offers non-discriminatory access to other utilities and other critical-infrastructure operators; this approach leaves the higher capacity, low criticality uses to be delivered by commercial terrestrial and non-terrestrial public network services (mobile and fixed). This network leverages existing commercial sites to optimise coverage. Due to its indoor reach as well as national reach, the hardened network also offers visibility and control of distributed energy resources in front of and behind the meter and provides connectivity for smart metering gateways.

Meeting national and regional needs, a federated approach – Austria

Austria has also built a dedicated 450 MHz network for critical utilities communications, utility owned and with non-discriminatory access for other users. ArgoNET, uses exclusive low-band spectrum to deliver a private and closed network with up to 72-hour hardening against power blackouts, and with a 4G LTE deployment on 5G ready hardware.

Austria has opted for a **federated, regional deployment and operating model** to meet their national objectives. A central body, ArgoNET, a company wholly owned by 10 regional DNOs, holds the spectrum, the standards and a central core network, while 10 regional distribution network operators build, own and operate their own regional networks, which interconnect into a single national platform.

Austria leans heavily on the regional DNO owned sites rather than commercial towers. The Austrian design is best understood as a single national network assembled from many regional sub networks: a federated, multi-core platform joined by interconnection.

An independent DNO driven solution – United States Southern Linc

Southern Linc is the mission-critical wireless network of Southern Company, one of the largest energy holding companies in the United States. **It is built, owned and operated by a single vertically integrated utility**, although its scale is closer to national in UK terms; the territory it covers, at more than 122,000 square miles, is larger than the entire UK landmass.

The network build commenced in 1996 when it launched with narrowband push to talk technology, and from around 2010 the network was upgraded to 4G/LTE, enabling SCADA telemetry and control and other critical use cases. The network has power resilient georedundant cores, and RAN sites have battery backup and carry-on site fuel and generation sufficient for around five days of autonomous operation.

Southern Linc now operates commercially, selling services to other critical user customers, and acts as a capacity donor to other utilities and to US first-responder and public-safety agencies.

Deployment models' considerations

The international examples of private mobile networks above have different tradeoffs and considerations of their own, encompassing, for example, architectural complexity, security considerations, and centralised versus distributed communications network operations, resourcing and competencies.

A DNO independent self-build and ownership model gives complete control and operation of the network to DNOs, requiring each to have access to the resources to deploy and operate separate networks.

At the other extreme, a centralised national network operator model provides uniformity and operational efficiency but requires DNOs overseeing a separate single entity that has to be created with requisite competencies.

A federated model shares the obligations; a central body can hold the spectrum, standards and core, while regionally organised DNOs build, own and operate their own deployments under that umbrella, interconnecting into one national network. The federated model buys DNO ownership, autonomy and a form of regional resilience, at the cost of more distributed operations and a greater interconnection and interoperability burden. Every DNO in this model might need to replicate the competencies and resources to own and run their own network operations.

Conclusions

The resilient communications network underpinning the energy infrastructure is the digital backbone of the future digitalised energy system. It is not an add-on, it is a fundamental enabling component of energy modernisation.

As energy networks, and electricity in particular, are undergoing unprecedented change, the mission-critical telecoms infrastructure supporting this change has to evolve to ensure affordable, low-carbon energy resilience and security.

Different communications networks, private and public, mobile and fixed, terrestrial and non-terrestrial will all have a role to play as different use cases drive different network and architecture requirements. Our analysis has focused on the mission-critical use cases and their requirements in terms of assured coverage, security, power resilience, latency and guaranteed delivery.

Several approaches are available to extend visibility and control across the transforming energy networks to support the delivery of a digitalised, low-carbon energy system; they all raise key areas requiring further considerations to ensure they meet the mission-critical needs of energy networks.

Public mobile networks can meet many of the energy networks' use cases; achieving the requirements of the mission-critical use cases (SCADA, ANM and resilient voice), will require additional considerations in light of the current public telecom networks extent and capabilities.

Our analysis of international deployment of dedicated private 4G/5G mobile networks has highlighted how different deployments and governance models have been implemented internationally to meet the specific objectives of coverage, latency, security and resilience by design. A dedicated network with low frequency spectrum means that a small number of sites are able to reach fixed assets, an order of magnitude lower than the MNOs have deployed in the countries analysed. Additionally, the communications networks under review, in most cases, cover smart metering and smart grid infrastructure and include the critical communication needs of other utilities. Radio spectrum is an essential component for a dedicated private network to address mission-critical communication needs; with short-term availability and a potential pipeline for growth.

The need for action is clear, as the energy system evolves, it needs telecoms solutions that meet a set of evolving requirements; there is now a clear government priority on energy security and focus on assessing the telecom needs of the sector covering both operational and restoration scenarios.

About the author: **Joe Butler** is an independent technology policy consultant. Most recently he served as Chief Technology Officer and Board Member at Digital Catapult. His experience spans technology and telecommunications policy and regulation, having held roles at the National Infrastructure Commission, the Department for Digital, Culture, Media & Sport (DCMS), and Ofcom. He is also an Honorary Professor at the University of Bristol Smart Internet Lab.

1 Scope & Approach

Energy Connect commissioned this report to analyse the critical role of telecommunications as a foundational enabler of the future energy system. A digitalised, sustainable, affordable, secure and resilient energy system depends on reliable communications to provide the visibility, control and coordination required to operate and restore increasingly complex electricity networks, making telecommunications a vital part of the UK's energy infrastructure.

The UK's 2025 Ten Year Infrastructure Strategy² made recommendations to assess the communications needs of energy, water and transport and to determine whether there is a case for policy or regulatory intervention. That assessment is currently being undertaken by NISTA, with DCMS covering telecoms, and relevant government departments considering sectoral communication needs.

This document focuses on the electricity distribution network operators and their mission-critical use cases; those in support of real-time grid monitoring and management, and grid restoration from a partial or national power outage. Distribution networks are expected to see the most significant changes as low-carbon distributed energy resources are integrated directly into the grid, their requirements are taken as a starting point to establish the blueprint for a mission critical telecoms solution.

While the distribution electricity networks are undergoing radical transformation and drive the needs considered here, the communications network approaches we reviewed could benefit the whole energy system, and wider critical utilities.

The broad telecoms approaches considered here are: reinforcing public mobile networks, utilising the Emergency Services Network, and deploying a dedicated mission-critical private network. In the report we highlight key considerations necessary for each of these approaches to meet the requirements of the most critical use cases. The document considers mission-critical private network deployments in other nations to understand what has been achieved, potential timescales and deployment options.

This report outlines key areas that need to be addressed, across all options, to ensure DNOs have the mission-critical telecom solution they need to achieve UK energy security and resilience objectives; it does not set out a costed business case or a financing structure for any of the approaches it discusses.

² NISTA, UK Infrastructure: A 10 year strategy, June 2025.

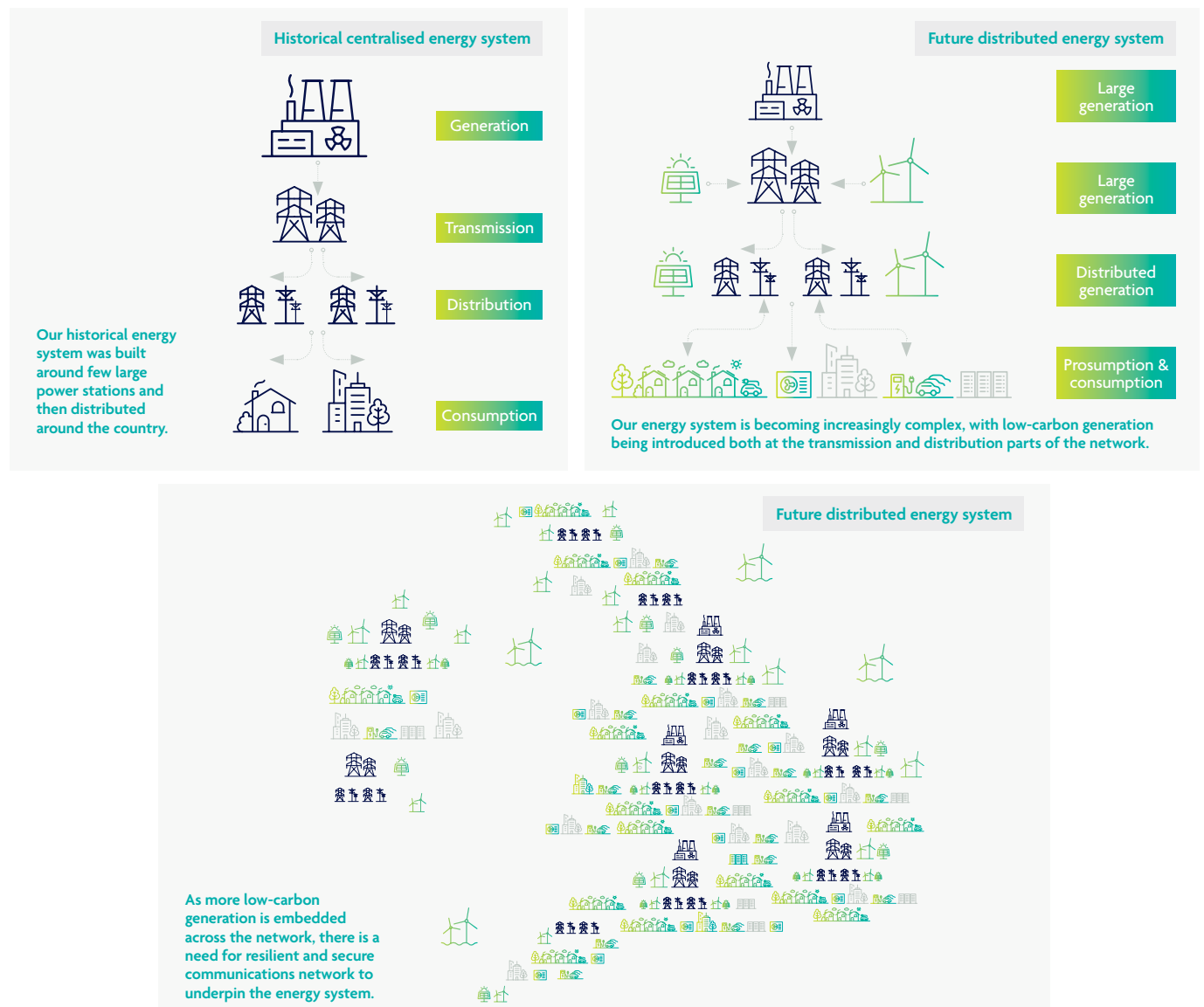
2 Communications underpinning a distributed energy system

UK energy networks are undergoing unprecedented change to deliver a low carbon, affordable, flexible, secure and resilient energy system.

As renewable generation, energy storage, electric vehicles and other distributed energy resources connect across the network, both supply and demand are becoming increasingly variable and decentralised. This is making the electricity system more dynamic, complex and challenging to operate than the largely predictable system of the past.

Managing this complexity requires intelligent and connected networks. Visibility and control are fundamental to secure system operation; visibility to understand, and control to enable timely action. Without resilient communications visibility is lost, automation becomes ineffective, resilience decreases, restoration slows and customer connections take longer. The resilient communication infrastructure underpinning energy networks is therefore a critical part of the digital backbone of the future energy system.

Figure 1: The transforming energy system



Electricity distribution networks are at the centre of this transformation. Historically power flowed in one direction from a relatively small number of large, centralised power stations to where it was needed. Today, generation, storage and flexible demand are increasingly connected directly to distribution networks, creating multidirectional power flows and requiring much greater coordination and control.

At the distribution level, core systems such as Supervisory Control and Data Acquisition (SCADA), Active Network Management (ANM), and mission-critical operational voice communications remain fundamental to both day-to-day network operation and restoration following faults and outages. These systems play a vital role in maintaining network reliability, minimising customer minutes lost and customer interruptions and enabling the efficient and affordable delivery of electricity to UK homes and businesses. As distributed energy resources proliferate through medium and low voltage layers, these core capabilities are evolving beyond monitoring and reactive control. Increasingly they are being enhanced by edge computing and AI supporting automated fault detection, predictive asset management, dynamic capacity management, and real-time monitoring of network performance and power quality.

The pressing need for enhanced visibility across the grid

Distributed generation currently accounts for around 30–35% of GB installed generation capacity. Distributed generation is expected to stay at this proportion looking ahead, but as part of a far larger electricity system.³ NESO state that operating a clean power electricity system in 2030 and a significantly larger electricity system towards 2050 requires greater coordination between transmission and distribution assets and operators. They state that visibility of distribution connected assets is critical; greater visibility will help optimise energy balancing and maintain network resilience and network operations⁴.

In November 2021, Storm Arwen cut power to almost a million homes in Great Britain, with some communities without power for over a week and three lives lost. The Electronic Communications Resilience & Response Group Post Incident Report⁵ noted that thousands of mobile base stations were disrupted by power outages. The Energy Emergencies Executive Committee Final Review⁶ commissioned by the BEIS secretary of state listed specific necessary actions including:

“Action R4: Energy Network Operators should continue to engage with DCMS and Ofcom to secure the utility spectrum so that the energy sector can develop its own resilient data/voice networks in the future.”

In 2025, Spain and Portugal suffered a national power outage affecting tens of millions of people. Once power failed, so did the communications relied on to help restore it. Payment systems went down because they ran over the same broadband network; hospitals, commerce and transport were all affected, at a cost estimated in the billions⁷. These events underscore that electricity is fundamental, being upstream of almost all other services, including national infrastructure networks such as communications and broadband, essential services, economic activities and protection of people's health and safety.

For this reason, a national power outage from a failure of the national electricity system is high on the UK national risk register⁸. While a nationwide electricity failure has never occurred, similar scale events have internationally, so it is regarded as an extremely high impact and credible, although low probability and rare occurrence. The policy approach taken in the UK is that it must adequately prepare for the worst-case scenario. Increased distributed generation with a high volume of renewables, could increase the risk of a cascade failure, as seen elsewhere.

3 NESO, *Future Energy Scenarios 2025: Pathways to Net Zero*, v.5 (November 2025), p.46.

4 NESO, *Future Energy Scenarios 2025: Pathways to Net Zero*, v.5 (November 2025), p.46.

5 EC-RRG, 2021/2022 Severe Storms Post-Incident Report, May 2022. https://assets.publishing.service.gov.uk/media/62828be08fa8f556165a1dec/GOV.UK_ECRRG_Post_Incident_Report_-_2021_2022_Severe_Storms.pdf

6 Energy Emergencies Executive Committee (E3C), Storm Arwen Review: Final Report, BEIS, June 2022. <https://www.gov.uk/government/publications/storm-arwen-electricity-distribution-disruption-review>

7 ENTSO-E Expert Panel, *Final Report on the Grid Incident in Spain and Portugal on 28 April 2025*, 20 March 2026.

8 Cabinet Office, National Risk Register 2025 edition, January 2025. <https://www.gov.uk/government/publications/national-risk-register-2025>

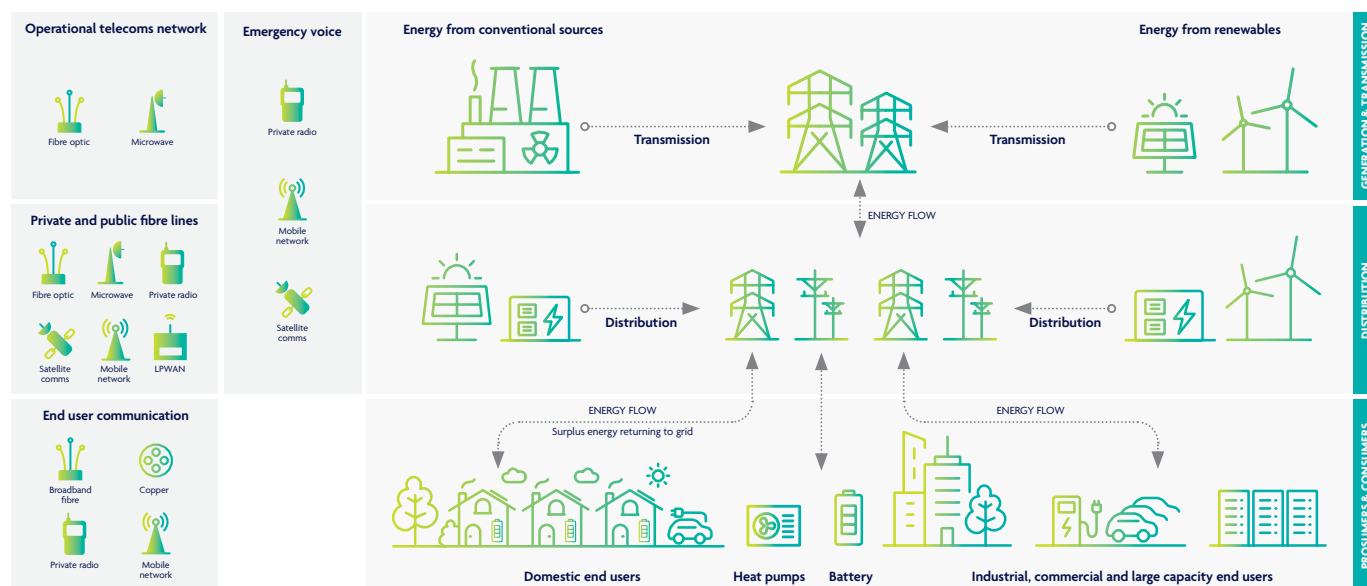
It is essential that these communications are maintained when power fails

Communications networks for monitoring, automation, control, flexibility services and restoration cannot fail when power fails. It is exactly in these circumstances that visibility is needed to enable informed actions to manage demand and supply and restart the energy system, locally, regionally or nationally. Mission-critical operational voice communication between field engineers and control rooms also becomes essential. Repeated major outages have highlighted a primary lesson to learn is the interdependence of communications and power. Grid power goes out, communications go down, and therefore restoration is hampered.

Meeting the GB Electricity System Restoration Standard requires 72-hours power backup for the telecommunications infrastructure supporting restoration⁹, to ensure critical functions can be undertaken without grid power. Looking forward, this increasingly needs to reach further, to maintain visibility and control as distributed energy resources proliferate across the UK more widely.

Historically in the transmission grid sufficient private communications have been deployed and integrated into the system as they are essential to support safe operation. In the distribution layer there are different public and private communication, wireless and wired, technologies deployed and there is an ongoing need for widespread connectivity to reach new distributed and flexible energy resources.

Figure 2: Overview of telecoms solutions across the energy system



9 DESNZ (formerly BEIS), *Electricity System Restoration Standard*, April 2021.

3 Defining mission critical communication needs

Multiple use cases and heterogeneous networks

DNOs and the wider energy system depend on a wide range of communications services and networks for very diverse use cases. Alongside a large, embedded base of private fibre, copper and wireless communications, public terrestrial and satellite services are currently employed, from public mobile to wide area IOT. The requirements of each use case and decisions around cost and practicality dictate the most appropriate choice of communications employed. Lower criticality traffic, which is often also the higher bandwidth traffic, generally has multiple communications options available. Redundant routing across multiple communications services is routinely employed to improve aggregate resilience where, if one service fails, another may be available as a backup.

Mission-critical use cases

There are however a class of use cases, with more stringent requirements, which here are grouped under the term **mission critical**. These use cases are essential to real-time grid monitoring, control and stability, and grid restoration from partial or national power outage. These essential services will become increasingly critical as networks become more complex and dynamic and therefore must continue uninterrupted, with requirements that must be met even when grid power may be out.

This narrower set of use cases and their requirements is the principal focus of this document. They are key differentiators defining the essential needs of the communications solutions. The critical use cases considered in this study as representative are SCADA, Active Network Management and critical voice communications.

Table 2: Critical use cases of the energy network

USE CASE	DESCRIPTION
SCADA	Aggregates telemetry from thousands of field RTUs, providing control rooms with real-time network visibility, alarm monitoring, and remote switching capabilities. These are typically installed at substations, distribution transformers, and embedded generation sites, sampling real-world electrical values (voltage, current, phase) and able to execute actions (tripping circuit breakers, adjusting tap changers, or sending setpoints to inverters).
Active Network Management	ANM is an automated control system deployed by DNOs to continuously monitor network parameters and dynamically alter generators' output or demand in real time to prevent power grid overloads. Rapid growth of renewable and flexible distributed resources such as solar arrays and battery storage brings two-way power flows that frequently strain local thermal and voltage limits, which ANM controls. To maintain thermal and voltage stability with high penetrations of renewables ANM systems continuously ingests RTU telemetry via SCADA, calculate network headroom, and constrain embedded generation site level RTUs where needed.
Critical Voice	Field communications for day-to-day operations and during restoration, MCPTT provides secure, prioritised, and resilient voice channels. Enabling control room dispatchers and field crews to safely coordinate physical line repairs, manual RTU overrides, and complex electricity system restoration.

At the distribution level, Remote Terminal Units (RTUs), SCADA networks and smart distribution grid elements (circuit breakers, switches etc) form the foundational layer for grid visibility and control, supporting DNOs coordinating demand, generation and flexibility on the grids. Higher level functions such as active network management act to constrain demand and supply to prevent overloads, are dependent on SCADA systems and other data sources. Distribution automation can happen autonomously, with fall-back mechanisms available for period when communications may not be available. These local decisions may trigger actions which when observed from a whole grid perspective may not have been as accurate as if they were fully interconnected with central systems.

Not included in the scope of the network approaches being considered in this study, but which fit the mission critical use cases in the distribution layer of the grid are **teleprotection and synchrophasor functions** to protect high voltage equipment and keep the energised grid stable. Teleprotection has latency requirements from 3–20ms, and stringent jitter requirements of around 0.2ms. Synchrophasors have slightly less stringent latency and jitter requirements of 100ms and 5–10ms jitter. Both of these are beyond the limit of what is currently achieved in practical and currently deployed on LTE/5G networks. While pilots are underway of Ultra Reliable Low Latency Communication 5G (URLLC) for teleprotection and inter substation signalling, in practice the requirements for teleprotection and synchrophasors are currently mainly met by fibre, microwave and UHF point to point links, already deployed to the key assets. For the purposes of the network approaches considered in this study, these use cases are considered as out of current scope, although are potentially addressable within the lifetime of the network as technology upgrades and pilot and trials continue to explore the capabilities of private LTE/5G.

SCADA and ANM have latency requirements which are readily achievable by a number of communications approaches including those considered here. Typically, high-priority primary SCADA traffic, runs over core MPLS¹⁰ networks for deterministic latency requirements of 20ms, and round-trip times for secondary SCADA typically between 200–500ms. ENA EREC G100 (Power Export Limitation Schemes) specifies dynamic export control and ANM response times at the DNO level, mandating a maximum 2 second communications delay.

Backup power requirements to meet the Energy System Restoration Standard

This set of distribution network mission critical use cases are broadly covered by grid code GC0156¹¹. GC0156 mandates that critical control systems must have independent backup power (batteries/UPS or local generators) capable of keeping essential monitoring and communication alive for up to 72 hours without grid electricity. It applies to critical entities and assets connected to the GB power system. For the DNOs and distribution, this includes broadly DNOs' key assets such as primary substations, the larger power plants connected to the local distribution networks, and any holders of Energy System Restoration Standard contracts at the distribution level.

The code mandates the 72-hour backup power for specific essential hardware such as communications & dispatch systems, control & telemetry hardware such as RTUs and SCADA nodes, and auxiliary systems required to keep the power plant in a safe condition during an outage while waiting for grid power to return.

¹⁰ Multiprotocol Label Switching (MPLS) is a networking mechanism that can provide guaranteed, fixed latency communication paths essential for sensitive operational technology like substation control and teleprotection.

¹¹ NESO, GC0156: Facilitating the Implementation of the Electricity System Restoration Standard | National Energy System Operator, 2025.

Essential requirements of mission critical use cases

In the table below we outline the essential requirements of communications networks that are necessary to support these mission-critical use cases, underpinning real-time grid monitoring, control and restoration as they evolve and push further to the edge of the grid and across the UK.

In summary, mission-critical use cases require: wide-area, high availability, assured coverage, stable latency, security and guaranteed timely delivery in the face of lower-priority traffic and power outages. The capacity requirements for these mission-critical use cases is notably relatively modest, though will grow over time. Latency requirements for future mission-critical use cases are not defined, but are likely to become more stringent as the grid becomes more dynamic.

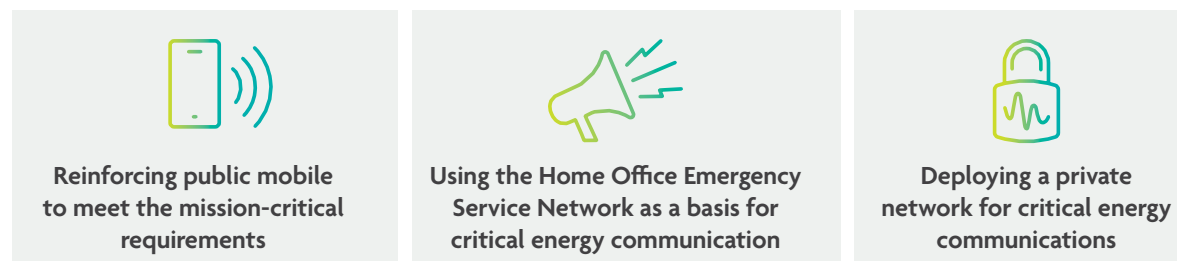
Table 3: Essential requirements of mission-critical use cases

Resilient wide area power backup	Communications networks for monitoring, control and restoration cannot fail when grid power fails. It is exactly in these circumstances that visibility is needed to enable informed and coordinated actions to manage demand and supply and restore the energy system regionally and nationally. The Energy System Restoration Standard ¹² requires 72 hours of battery backup for communication equipment for this reason. As visibility and control extend to a larger number of geographically dispersed assets, this requirement increasingly applies across a wider operational footprint.
Latency requirements and assured delivery	Whilst latency is currently relatively achievable e.g. for SCADA systems, there is a requirement for guaranteed delivery of telemetry and control messaging, requiring deterministic communications. During the conditions that matter most such as a major incident or widespread outage, network congestion must not delay or prevent the transmission of operationally critical traffic. Mission-critical communications therefore require deterministic performance, prioritisation and assured service availability.
Coverage that reaches the assets	Communications need to reach where energy assets and field workforce are, including indoor, below ground and remote locations. Unlike consumer communications networks, many energy sector use cases are uplink-dominated, requiring reliable transmission of telemetry and status information from widely distributed assets back to control centres.
Security and cyber resilience	Security is the first order requirement given the criticality of energy provision and the downstream services dependent on energy. As digitalisation increases and cyber threats become more sophisticated, communications networks remain a key attack surface. Recent developments in advanced AI models demonstrate an unprecedented ability to rapidly discover software vulnerabilities and exploit weaknesses. For critical national infrastructure such as the energy system, the next decade demands an elevated commitment to secure architecture, robust identity and access management, continuous monitoring and resilience against both cyber and physical threats.

¹² DESNZ (formerly BEIS), *Electricity System Restoration Standard*, April 2021.

4 Different approaches and considerations

Three broad approaches are considered to meet these mission-critical requirements looking forward:



The table below summarises key considerations necessary to ensure the solution will meet requirements for each approach. These considerations are discussed in the following sections.

Table 4: Key considerations for the three approaches to mission-critical communications

APPROACH	KEY CONSIDERATIONS
Reinforced public mobile	• Delivery of end to end 72-hour power resilience across all comms elements (access, backhaul and core) in light of Ofcom's cost analysis. • Prioritisation of guaranteed traffic with low and stable latency. • Coverage of energy assets, often remote, indoor and below ground level and uplink limited. • Isolation to ensure security of utilities traffic.
Emergency Services Network (ESN)	• Current ESN's resilience to be assessed against energy assets requirements. • Prioritisation of guaranteed traffic with low and stable latency. • Coverage to remote, indoor and below ground assets and uplink limited. • Isolation to ensure security of utilities traffic. • Timing of deployment of service for energy against completion of ESN delivery programme for Home Office, scheduled for end of 2029. • Governance and decision making between the different sectors. • Emergency services and energy sector critical communications on one shared infrastructure, creating a single point of failure.
Mission-critical private mobile network	• Latency, coverage, traffic isolation and power resilience are built in by design. • Deployment and operating models will need to be established, and governance agreed by the sector. • Requires dedicated spectrum and a pipeline for future growth. • Communications operations requires sufficiently resourced, specialist skilled workforce.

Reinforced public mobile

UK public mobile networks can meet the technical requirements such as latency for SCADA telemetry, critical voice communications and upstream critical functions such as ANM. Key areas for further consideration, to meet the mission-critical requirements, would be around ensuring guaranteed, timely delivery of energy mission-critical traffic with stable latency/low jitter, considerations with regards to prioritisation above commercial traffic, ensuring coverage of energy assets which fall outside population dense areas, and analysis of the capability to meet the wide area power backup requirement as connectivity requirements expand towards the edge of the network.

- **Power resilience** UK public mobile networks today carry no mandated power resilience. Commercially self-installed power back up is typically less than 4 hours. Ofcom has reviewed the subject of mobile network power resilience, informed in part by the lessons of Storm Arwen. In its revised Network and Service Resilience Guidance (updated in June 2026), Ofcom concluded not to mandate a universal, fixed number of hours for battery backup across UK mobile mast sites¹³.

In its Mobile RAN power resilience Technical Report and CFI Update published in 2025 Ofcom estimated the aggregate costs likely to be incurred to improve power resilience across all four MNOs UK radio access network sites. To achieve a 4-hour power backup Ofcom estimated a cost of £2.2–£4.4 billion¹⁴. Because of this significant cost, which Ofcom noted would likely be passed on to consumers, it concluded that mandating universal, fixed battery backup across all mobile sites was financially disproportionate. Further evidence of what might be commercially provided comes from Vodafone's "Enhanced Power" programme¹⁵, announced in November 2025 which addresses over 10,000 sites across Europe, with a tiered layer of "Critical Access Sites" brought to a minimum of four hours, and a smaller core of around 400+ sites taken to a full 72 hours.

Hardening a public mobile macro site to 72 hours is considerably more demanding than hardening a purpose-built low band private network. This can be understood because a macro site which draws anything between 5–10kW to run multiple mobile spectrum bands needs roughly 10 times the battery capacity of a lower power, low frequency system focused on limited uses. This larger battery storage pushes sites into further structural engineering and practicality considerations.

While reinforcing a public mobile network to achieve power resilience is possible, it is unlikely as a standalone network solution to be the most cost-effective route for a stringent 72 hours end to end telecoms network requirement, consistent with Ofcom's analysis.

An alternative approach is to use different communication services in parallel to provide redundancy, such as satellite services and meet the power backup requirements through combined communications service uptime guarantees. How well all elements of a heterogeneous approach would respond in the event of a widescale outage has not yet been tested.

- **Traffic prioritisation** This is essential in order to meet the need for guaranteed delivery of traffic and latency requirements. This is technically feasible at a cost with LTE and 5G Non-Stand Alone (5G NSA) systems which are widely deployed in the UK today. It could also be managed more readily through 5G network slicing once 5G Stand Alone networks (5G SA) are deployed on a national basis and covering the assets targeted by the DNOs. With energy traffic receiving the top level of prioritisation above commercial traffic, ensuring guaranteed transmission of SCADA, uninterrupted ANM and mission-critical voice are feasible. There have been examples of control centre operations impacted by a failure of comms due to congestion in the public mobile network, which this could address.

¹³ Ofcom, *Network and Service Resilience Guidance for Communications Providers*, 2026 revision, June 2026.

¹⁴ Ofcom, *Mobile RAN power resilience: technical report and Call for Input update*, February 2025.

¹⁵ Vodafone Group, "Vodafone to boost resilience and extend power backup time at 10,000 plus mobile sites serving emergency services," press release, 28 November 2025. <https://www.vodafone.com/news/newsroom/technology/vodafone-to-boost-resilience-and-extend-power-backup-time-at-10000-plus-mobile-sites-serving-emergency-services>

- **Coverage** Use of public networks will need to ensure coverage of the specific assets, given these are often in hard-to-reach locations, remote and below ground. Where coverage gaps exist, the network could be augmented with additional sites. High availability, assured coverage is required to assets even when the network is subject to high demand. Modelling coverage against the specific UK asset base and critical use cases requirements will need to be undertaken.
- **Security** Public networks are fundamentally designed to maximise connectivity to the internet, as noted above, the need to segregate critical traffic from the internet will be increasingly important to minimise vectors of attack in an increasingly hostile environment.
- **Technology Refresh** DNO assets deployed on the network have a long lifespan of >15 years against the more frequent mobile industry technology refresh cycles, typically every 10 years. Consideration will need to be given to the impact of technology refresh rounds on energy networks.

The Emergency Services Network

The ESN has a number of features of benefit to communications for the energy sector. A national footprint of more than 19,500 sites, extended coverage, a mission critical application layer, and working traffic prioritisation for emergency services use. It has planned power backup in excess of the 72 hour requirement being deployed across a subset of sites.

Broadly two routes are considered for the energy sector to use ESN. Commercial leasing of capacity from BT/EE, and deployment of a separate mission critical private network utilising the ESN infrastructure.

Commercial Leasing of Capacity from BT/EE

A commercial lease of capacity from BT/EE, including through BT's new Mission Boost¹⁶ service offerings could meet the requirements in broadly similar terms, as set out in the earlier consideration of a reinforced public mobile network.

There are two key differences. Firstly, the potential benefit of being able to meet power resilience requirements through the existing public ESN investment and planned programme of network upgrades underway. Secondly, critical energy traffic in this situation can be prioritised above the public commercial tier of traffic, whilst still requiring prioritisation considerations between energy and emergency services traffic.

This could present challenges to the guaranteed delivery and latency requirements of traffic such as SCADA telemetry and voice. In a national power outage scenario, where emergency services will have heightened activity, this requirement may not be met, as the critical energy traffic is likely to be in a lower tier than the emergency services. Detailed modelling would be necessary to establish if there is sufficient capacity from the power resilient layer of ESN sites for emergency services traffic and energy critical traffic during a multi-day national power outage scenario across the UK energy sites.

Mission-critical private network built using ESN infrastructure and spectrum

A more substantive route is carrying energy traffic on a separate critical private network over ESN's shared core as a Multi Operator Core Network overlay (MOCN).

This approach could provide a number of advantages to the energy operators for their critical communications. In this approach there would be an additional independent core for energy sector users, added to the ESN infrastructure. This enables the existing ESN base station RAN equipment and ESN existing licensed radio spectrum to be shared, but with a separate mobile network operator identity (PLMN) dedicated for the energy sector communications layer. Advantages of the approach include:

- **Infrastructure sharing:** MOCN reuses the infrastructure that is already built including the ESN/EE masts and extended area service sites.

¹⁶ BT Business, "BT launches new service to support mission-critical communications across the UK," 11 June 2026.

- **Logical separation and control:** With its own PLMN and core, the energy sector would run its own subscriber database, SIMs, authentication and security policy. Its traffic would not mix with blue light or consumer traffic in the core. The core could sit in its own geo-redundant data centres under independent management. This could give isolation at the data centre level, and enable energy to design services and data paths around its needs.
- **Prioritisation:** In this approach prioritisation with respect to all traffic tiers is technically viable and becomes a matter of policy. ESN is already engineered for priority and pre-emption for the emergency services. Energy mission-critical traffic could be given defined priority classes, and occupy a level tier to the emergency services, offering the possibility that emergency services critical traffic would not squeeze out energy sector critical traffic in capacity constrained situations.

There are a number of considerations, which would need to be taken into account to adequately specify this approach and understand that it meets energy critical communication requirements.

- **Prioritisation:** While prioritisation becomes a matter of policy there are important implications to consider. To ensure the requirements of latency and guaranteed delivery for telemetry and control are met, some energy sector traffic may need to be prioritised above blue light services. This is particularly likely to be necessary in a national power outage scenario when both emergency services and the energy sector will have heightened critical needs.
- **Power resilient coverage:** High availability, assured coverage to remote, indoor and below ground assets would need to be assessed, with the potential need to augment the resilient coverage layer.

- **Timing:** ESN's own delivery programme runs to the end of 2029. Integrating an additional separate energy private network overlay would essentially add a new project deliverable to the existing timetable. A realistic development and deployment route might be to begin only once ESN's own delivery programme is complete, commencing in 2030 or beyond.
- **Governance:** Governance and decision making would need to be established between the different services, covering key issues including prioritisation policy, resilience investments, coverage to assets and technology upgrade/sunsetting roadmaps.
- **Security:** The need to segregate critical traffic from the internet will be increasingly important to minimise vectors of attack in an increasingly hostile environment.

This approach would benefit from further modelling. During an emergency national power outage situation, the emergency services and energy sector communications needs could be in direct contention for capacity on the network at the same time. It would be essential that both sectors' needs could be serviced in such a challenging situation where the two sectors need to be working in parallel to achieve their goals.

This approach concentrates the emergency services' and the energy sector's critical communications onto one shared infrastructure, creating a single point of failure. A major network failure or cyber-attack could degrade both services at once. This is observed as a cross-cutting consideration that is beyond the scope of this report and is likely to sit with the Cabinet Office.

These considerations are on the basis of a standalone network. It is noted that there is a wider heterogeneous mix of network services available in some parts of the country which may support meeting needs using redundant communication services.

Dedicated mission-critical private network

A dedicated private network differs from the other approaches as it is designed to meet specific requirements from the outset. DNOs establish the detailed requirements, and the network is designed and deployed to meet them; which assets must be covered, what availability each class of traffic must have, how long radio sites and backhaul must run without grid power, and how the network is secured.

Employing low frequency spectrum and a low site count, enables power resilience to be designed into the system from the beginning. Similarly, capacity dimensioned against solely the critical use cases, supports an efficient radio network and the affordability of meeting 72 hours of power backup through the network.

Coverage can be planned against the asset base, potentially making use of a DNOs existing estate of sites with infrastructure such as power, towers and backhaul. A dedicated network gives the sector control over the security architecture and standards, including how far the network connects to the public internet. Network connectivity to the internet can be restricted to defined, controlled exchange points, or removed entirely.

From a security perspective, the option of deploying a private network, allows for a number of ways to separate critical traffic from the internet, including being completely isolated from the internet, reducing the potential numbers of attack vectors into the system.

Energy Connect has developed coverage models for different DNOs to understand the scale of infrastructure required to support the deployment of private networks. These studies focused on leveraging existing DNOs radio sites, to take advantage of existing power resilience and to minimise infrastructure costs.

Analysis commissioned by Energy Connect has estimated the capital cost of deploying a private network. With input from UK DNOs the cost of deployment (access, backhaul, core and data centres) was estimated to be around £215 million.¹⁷

In section 5 we have analysed three international case studies that provide evidence of dedicated, secure, resilient and affordable private networks in operation.

Satellite

We have not considered and analysed satellite as a potential standalone approach; satellite communication services are used to provide a secondary or tertiary failover layer for mission-critical electricity grid telecommunications, or in some cases to reach remote and hard-to-reach assets. They provide route diversity from terrestrial networks, and are used in this way in the UK and in many other nations as a vital part of the telecommunications portfolio. Eutelsat OneWeb and IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite), the major European Union constellation expected to be operational around 2030, will continue to play an important and developing role.

Restoration from a nationwide power outage is highly challenging, and from an engineering perspective it is beneficial to have resiliency, redundancy and security in the communications systems employed to the maximum extent possible.

¹⁷ <https://www.energyconnect.org.uk/publications/economic-rationale-for-enabling-smart-grid-functionality-of-the-uk-energy-system>

5 International Deployments of Private Networks for Critical Communications

We have explored the justification behind and implementation of a number of different international examples to understand the lessons learned

Several European utilities have deployed, mission-critical private networks for their grids, increasingly framed as a matter of energy security and national resilience. We have chosen to highlight three examples.

The drivers for deployment are consistent across these examples. The energy transition is decentralising the grid, multiplying the assets that must be monitored and controlled, making grid management and restoration increasingly challenging with energy security an increasing national concern. The utilities studied are seeking communications solutions that meet requirements similar to those of the UK operators; resilient during outages, guaranteed delivery of critical communications unaffected by network congestion, secure, affordable and capable of wide area and deep indoor coverage to reach dispersed and often hard to access assets and connect field force across the national territory.

But while the goal is shared, the international deployments analysed offer proof points of how different models have been deployed to meet national objectives: a single DNO owning and operating their own private network, to an independently owned and operated regional infrastructure combining into a national network layer, and a single national operator which is owned by the DNOs.

We selected these three examples as they span a range of different working models for undertaking the functions necessary to deploy and run these networks, shown in Figure 3. In section 6, we provide further details with regards to the individual functions and models within the framework, introduced here to better contextualise the three deployment models under review.

The UK could adopt a variant of any of these deployment models, depending on DNOs needs and on UK wider policy objectives and desired outcomes.

Further detail on these national deployment examples is contained in Annex 1.

Figure 3: Framework outlining functions and models for private networks

FUNCTION > MODEL	1. INDEPENDENT SELF-BUILD	2. SPECTRUM VEHICLE	3. STANDARDS & INTEROP	4. COORD SHARED PLATFORM	5. COORD SHARED PLATFORM FLEX BUILD	6. DNO OWNED NATIONAL NETWORK SPV OPERATED
Spectrum & regulatory	DNO	SPV	SPV	SPV	SPV	SPV
Standards & interoperability	DNO	DNO	SPV	SPV	SPV	SPV
Procurement & supply chain	DNO	DNO	DNO	SPV	SPV	SPV
Core, platform & credentials	DNO	DNO	DNO	SPV	SPV	SPV
Build (sites, RAN, backhaul)	DNO	DNO	DNO	DNO	choice	SPV
Operate & maintain	DNO	DNO	DNO	DNO	choice	SPV

Southern Linc (US)

ArgoNET (Austria)

450connect (Germany)
Utility Connect (NL)

A nationwide dedicated network – Germany

The German policy approach treats communication as a precondition for the energy transition, not an adjunct to it; an enabler for digital transformation of the grid, in response to the priority placed on the Energiewende, the German energy transition.

Germany has designed, built and now operates a nationwide dedicated private wireless 4G network for critical infrastructure. The network is owned and operated by 450connect GmbH, a national operator which itself is owned by the utilities that are the primary users of the network. The network runs on 450 MHz spectrum that the regulator reserved for the energy and water sectors and licensed exclusively for this use until 2040. It is deployed mainly on commercial towers, using utilities tower infrastructure to supplement where necessary.

The network is largely complete. It covers around 96–98% geographic coverage of Germany using a planned 1600 sites, with 90% geographic coverage delivered roughly four years from the 2021 spectrum allocation.

Because it is a specialised, limited capacity network with low band coverage requiring an order of magnitude fewer sites than a public commercial network, the whole network is hardened to a 72-hours, redundant standard. The German approach tackles the hard problem of ensuring resilience, robust, secure connectivity for the mission critical needs, it offers capacity for other non-critical uses in situations where it is available, and leaves the higher capacity, low criticality uses to be addressed by heterogeneous use of commercial terrestrial and non-terrestrial public network services. The platform provides the foundation for grid digitalisation at scale. Due to its indoor reach as well as national reach, the hardened network can carry substation control, offer visibility and control of distributed energy resources in front of and behind the meter, as well as providing connectivity for smart metering gateways.

A regional, federated approach – Austria

Austria has also built a dedicated 450 MHz network for critical utilities communications, ArgoNET, which sets out to meet the same objectives as the German model, with the same broad approach: exclusive low-band spectrum, a private and closed network, up to 72-hours hardening against power blackouts, with a 4G LTE deployment on 5G-ready hardware, utility ownership, and non-discriminatory access.

Austria has adapted the same underlying requirements to its own national circumstances and to the preferences of its distribution network operators, by using a federated, regional deployment and operating model. A central body, ArgoNET GmbH, a wholly owned company of 10 regional DNO shareholders, holds the spectrum, the standards and a central core network, while 10 regional distribution network operators build, own and operate their own regional networks, which interconnect into a single national platform.

Austria leans heavily on the regional DNO owned sites, supplementing with commercial towers where necessary.

The Austrian design is best understood as a single national network assembled from many regional sub networks: a federated, multi-core platform joined by interconnection.

The central layer ArgoNET is the licensed national mobile network operator. It holds the 450 MHz spectrum and a single national operator identity, Public Land Mobile Network (PLMN); it defines the uniform technical solution and does the central engineering and planning; it runs the central core and connectivity-management platform and provides common support and maintenance. Critically, it procures all base-station and central-systems hardware and software through a single central framework contract, so every region deploys from the same approved-equipment menu. ArgoNET and the DNOs jointly operate the interconnection between regional subnetworks and the central systems, and handles cross-border coordination.

The regional layer Each owning DNO builds, owns and operates the regional “subnetwork” in its own territory. It owns the infrastructure, the radio sites typically being on its own or existing infrastructure installations, and it runs its regional network with its own dedicated packet core and network management, staffed 24/7 by the utility. Each region is engineered to be fully autonomous in an emergency; with its own core a regional network can continue operating even if cut off from ArgoNET’s central systems. Regional builds include their own geo-redundant central technology, and the whole regional network is engineered for up to 72 hours autonomous availability across all elements.

An independent DNO driven solution – United States Southern Linc

Southern Linc is the mission-critical wireless network of Southern Company, one of the largest energy holding companies in the United States. It is built, owned and operated by a single vertically integrated utility, although its scale is closer to national in UK terms; the territory it covers, at more than 122,000 square miles, is larger than the entire UK landmass.

The network build commenced in 1996 when Southern Company, serving around 9 million customers across one of the most hurricane-exposed regions of the United States, concluded it needed its own wireless communications to both keep operating and to speed up restoration when severe weather struck. It launched with narrowband push to talk technology, and from around 2010 the network was upgraded to 4G/LTE, using 3 MHz of 800 MHz spectrum and reaching operation by 2017 as CriticalLinc, enabling SCADA telemetry and control and other critical use case. The network has power resilient georedundant cores, and RAN sites have battery backup and carry on site fuel and generation sufficient for around five days of autonomous operation.

Across nearly three decades and a long succession of major hurricanes including Hurricane Katrina in 2005 and Zeta in 2020, there is a consistent record of the network enabling the utility to communicate, maintain visibility and speed restoration. Public networks in these extreme situations often suffered widespread outages. Southern Linc now operates commercially, selling services to other critical user customers, and acts as a capacity donor to other utilities and to US first-responder and public-safety agencies.

Southern Linc’s own leadership has been candid that spectrum was only part of the challenge. Sustaining a specialist workforce able to operate and maintain a mission-critical telecoms network was a hard, enduring requirement, and a heavy lift for a utility acting alone even covering an area larger than the UK.

6 Delivery and deployment models for a mission-critical private network

Germany, Austria and US Southern Linc give proof points of three different network architectures, ownership and operating models. The UK could adopt one of these approaches, or a variant. The three deployments are examples within a wider set where functions that needs to be undertaken can either be centralised or distributed to the DNOs.

Figure 4 shows the distinct functions that need to be undertaken to deploy a national scale network or regional network, grouped into six layers. Each of these functions can either be undertaken by each DNO, or could be centralised and undertaken by a Special Purpose Vehicle (SPV) – a central body established to undertake the common functions.

Figure 4: Functions required to deploy private telecoms solution

1 Spectrum & regulatory	1 Hold the spectrum licence(s) 2 Spectrum assignment & cross-boundary interference coordination 3 Regulatory, policy & Ofgem/Ofcom engagement; licence compliance
2 Standards, security & interoperability	4 Technical standards & reference architecture 5 Security architecture & cyber policy 6 Interoperability rules, SIM/credential scheme & identity
3 Procurement & supply chain	7 Vendor selection/equipment approval 8 Central/framework procurement & commercial leverage; device certification
4 Core, platform & credentials	9 Core network & the slicing/sharing platform 10 Credential operation (HSS/UDM), provisioning, OSS/BSS
5 Design, build & physical infrastructure	11 RF planning & detailed network design 12 Site acquisition & infrastructure provision 13 Civil works & RAN installation 14 Backhaul/transport design & build
6 Operate & maintain	15 NOC, monitoring, assurance/SLAs, optimisation, lifecycle upgrades 16 Field maintenance & fault repair
17 Cross-cutting wrapper – the ownership vehicle itself: governance, financing/balance sheet, delivery & technology risk ownership, cost-allocation/charging between DNOs, and onboarding other CNI users (water, gas, transport) or third-party revenue.	

In the models considered here it is assumed the SPV is owned by the DNOs, but this could also include wider energy system stakeholders becoming shareholders, or indeed representation of other utilities such as gas or water. In the case studies analysed, DNOs that hold shares in the SPV, sit on its board and therefore have clear governance mechanisms for ensuring the network/s and the network operator meet the needs of their regulatory and commercial obligations.

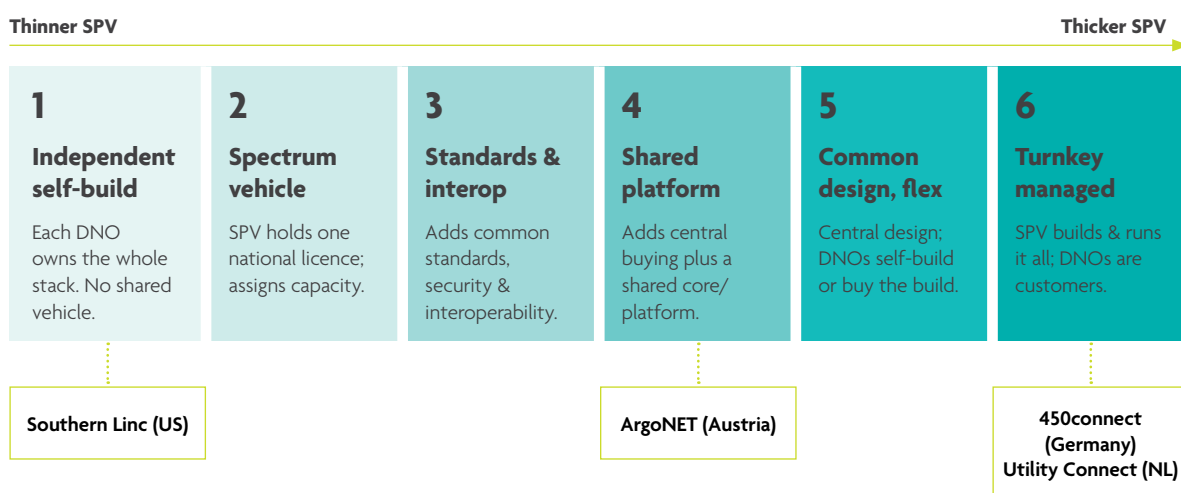
Energy Connect (previously Joint Radio Company) currently coordinates spectrum for the electricity and gas utilities and holds spectrum licences on their behalf. Energy Connect also undertakes radio planning functions for DNOs.

Deployment and operating models

Figure 5 shows six illustrative models for the SPV, from a thin vehicle with only the minimal functions through to a thick vehicle taking on the maximum responsibility, each step moving more of the

functional responsibilities from the regional DNO to the central SPV. Figure 3 earlier in the document shows where the dividing line of responsibility between DNO and SPV falls in these illustrative models.

Figure 5: Illustrative deployment and operating models with position of international examples shown



Model 1, independent self-build. Each DNO builds, owns and operates everything in its own area. There is no shared vehicle. This vehicle can work for a single DNO operating in isolation, but with multiple adjacent DNO regions sharing a spectrum allocation there is interference to manage. **Southern Linc (United States) is an example of model 1**, it built and operates the whole stack for its own service area. That area is larger than Great Britain, and there were no interfering utility neighbours. The example shows that the full capability can be held in one company, but that company noted explicitly the scale of resources needed were “a heavy lift”.

Model 2, spectrum vehicle. The SPV holds one national licence and coordinates and manages spectrum use across regions for a spectrum allocation. Everything else stays with the DNO.

Model 3, standards and interoperability. The SPV also sets technical standards, the security architecture and the interoperability rules, including the SIM and credential scheme.

Model 4, shared platform. The SPV also runs procurement and equipment approval, operates the core network and credentials, and holds RF design authority. Each DNO builds and operates its own sites. **ArgoNET (Austria) sits at Model 4.** Ten Austrian DNOs own the vehicle. The SPV holds the spectrum, sets the standards, runs the approved-equipment framework and operates the central core. Each DNO builds and operates its own regional network, largely on its own sites.

Model 5, common design, flexible build. As Model 4, but each DNO chooses whether to build and operate its own area or for that to be delivered by the SPV.

Model 6, turnkey managed network. The SPV builds and operates everything. The DNOs are shareholders and customers. **450connect (Germany) sits at Model 6.** Four shareholders, representing a broad base of German DNOs and utilities, own the SPV. It holds the spectrum, ran a single national procurement, built the network largely on commercial tower sites and operates it. The DNOs are shareholders in the SPV and customers of it. Utility Connect in the Netherlands follows the same pattern at smaller scale.

Key considerations with regards to private networks operating models

There are considerations across the different models, from a centralised national network to a distributed regional network, in terms of resourcing, as well as delivery risk and achieving the needs of the DNOs and government.

- **Regional networks versus a national network**

- **Whole-system visibility.** Different models are likely to require different solutions to ensure a whole system and national level visibility; for day to day operations or during an event like a regional or national outage.
- **Operation across licence boundaries.** Ability to operate across license and network boundaries, in case of partial or national power outage, will need to be in place, to allow DNOs field force to communicate across multiple networks.
- **One network for other critical infrastructure.** Centralised v distributed networks will require different governance and operating models to allow potential for other utilities such as water and gas to be beneficiaries of the network for some of their critical communication needs. Germany and Austria both provide non-discriminatory access to other critical infrastructure operators. Southern Linc sells capacity to public safety agencies and others.
- **Scale in procurement and devices.** One national specification and one order volume attract suppliers and support certified, sovereign equipment benefiting from economies of scale.

- **Specialist capability and delivery**

Deployment of different models from centralised to federated, will need to consider how to address dedicated workforce and skillsets requirements across multiple areas such as core network operation, security operations, network operations, vendor and contract management, and device certification.

Federated solutions would allow greater DNOs' oversight of relevant functions, centralised models

would benefit from the integration of functions and roles against a planned national build and a uniformity of delivery, standards and deployment strategy across the network.

- **Scale and use of existing assets**

A private network can be built on the utilities' own estate, on commercial towers, or both. Own sites are easier to harden to 72 hours power resilience, because the operator controls the power supply and the compound.

UK DNOs hold towers, substation sites, resilient power and secure compounds across their areas, and in many cases private fibre that can carry backhaul. Austria built predominantly on utility sites. Germany, built substantially on a commercial tower framework and pays for it over the life of the licence, but it is also supplemented by utility owned sites.

A central model may still use DNO sites, but access might be through leases or contribution agreements which need to be agreed. A devolved model can still buy centrally, but only if the vehicle holds the procurement function (Models 4 to 6).

- **Security and complexity**

Security is a matter for specialists in DNOs and other organisations, but we note that the different models are likely to present different security considerations.

Complexity scales with the number of operators, cores and interconnections. Each additional core is another system to secure, patch and assure. Each interconnection between cores is a trust boundary, and interconnection and roaming are recognised across the mobile industry as exposed points. More operators require more security functions, and incident response that has to be coordinated across organisations rather than run within one.

Whichever model is chosen, the credential, identity and security architecture must be common. Without that, devices cannot move between networks, and the national layer cannot function.

7 Radio Spectrum for Private Networks for Critical Communications

Spectrum availability is a significant gating issue for deployment of a private network approach. This is true in the UK where the issue has been discussed and consulted on for more than a decade with no resolution.

International examples of private networks for electricity grid and other utilities communications invariably focus on low-frequency spectrum, principally for good propagation characteristics resulting in cost-effective deployments. In these examples, national scale coverage, including remote areas and indoor penetration is achievable with a small network of sites.

Ofcom’s 2023 Call for Input on spectrum to support utilities sector transformation was the most recent published consideration¹⁸. Three bands were considered for a dedicated mission critical private network for critical communications. A small block at 700 MHz harmonised across Europe for broadband public protection and disaster relief (PPDR); the 450–470 MHz band, on which most comparable European utility networks are built; and, a longer term possibility, spectrum that may be released from the UHF television band as terrestrial broadcasting evolves.

Table 5: Comparison of the three candidate bands

BAND	BANDWIDTH	PRINCIPAL GATING FACTORS	INDICATIVE AVAILABILITY	ECOSYSTEM MATURITY
700 MHz (PPDR) Band 28	2×3 MHz	- No incumbents in the sub band - SDL coexistence with EE - competing interest for allocation - potential need for specialised base station equipment	Potential immediate availability	Excellent device ecosystem excellent (global Band 28).
450 MHz Bands 31/72	2×5 MHz	- Heavily used band with many incumbents - UK reversed band plan – partial or full replan and incumbent migration required	Estimates of 5 years for availability with limited use potentially sooner – TBD	Very good and rapidly maturing device ecosystem focused on utility uses. Emerging European energy/ critical utility band
500/600 MHz (UHF)	TBD – potentially wider bandwidth	- Incumbent DTT primary to 2034/beyond, and PMSE - WRC-31 and national policy decisions pending	Post 2034 – currently uncertain	Unclear

¹⁸ Ofcom, *Call for Input: Potential spectrum bands to support utilities sector transformation*, June 2023, and November 2023 update.

700 MHz is the most immediately available option, potentially addressing the DNOs pressing timescales. On technical fit and on ecosystem depth for the energy sector specifically, the evidence would more likely point to 450 MHz, which is the band in which a utility specific supply chain has formed, and on which European deployments are built including Germany, Austria, Netherlands and Poland. The UHF DTT clearance option is currently only a possibility with many uncertainties in terms of size and location of band, possible support and European/worldwide consensus, and downstream potential for harmonised equipment with economies of scale. At this time there is not sufficient certainty to consider the UHF DTT spectrum that may potentially be available as anything other than a potentially useful source of future additional capacity for the evolving needs of the digital grid and wider energy and utilities.

Devices and terminal equipment are likely to account for the majority of the cost, and the greater benefits in terms of device innovation, over the lifetime of the network. A private network enabling widespread digital assets to be connected for digitisation of the grid will serve hundreds of thousands of assets, so it is essential to know that this is a low-risk path with an evolving device ecosystem.

On the device and terminal side specifically both 700 MHz and 450 MHz have healthy ecosystems. 700 MHz is most mature reflecting Band 28 global scale with excellent device and equipment availability. 450 MHz has an established and growing ecosystem, with particular focus on the utility and energy equipment needed by DNOs and other utilities. Access to this band, would enable the UK to benefit from other national first movers and investments which have developed this ecosystem.

Both 700 MHz and 450 MHz provide good low-band spectrum options from a coverage perspective. Both offer the ability to provide national-scale coverage with a low site count. Energy Connect has undertaken dimensioning studies for DNOs confirming this.

450 MHz has excellent reach to indoor and hard to reach locations. In European nations such as Germany, use of 450 MHz has enabled a low site count private network to cover DNO's own assets as well as be a bearer for the nation's smart meters, and for smart grid visibility and control of assets such as residential EV chargers and heat pumps behind the meter.

700 MHz availability in the UK

700 MHz spectrum could potentially be made available relatively straightforwardly were that decided to be the right course. This appears to be the most appropriate solution to enable a private network to address the pressing mission-critical communication needs of the UK electricity distribution system underpinning real-time grid monitoring, control and restoration, and potentially also benefitting the wider whole energy system and utilities. Allocation in the near future would enable deployment of a private network to commence quickly, providing the potential of a standardised, power resilient national platform in the near term.

There is potential interest in the 2×3 MHz band from others, including the Home Office who noted an interest in 700 MHz spectrum to support ESN device to device communications (through technology such as Sidelink) alongside traditional cellular coverage¹⁹.

The potential capacity limitations of the 2×3 MHz, would need to be considered and detailed capacity modelling would be beneficial to establish exactly what can be serviced with a realistic base station deployment. Because of the low capacity needs of the critical use cases, SCADA telemetry, ANM and critical voice communications, there is evidence that 2×3 MHz is sufficient to meet these mission critical needs, even if it restricts the overall utility of the network. Both Southern Linc in the US, and Utility Connect in the Netherlands offer examples of utilities running private networks for critical electricity communications including SCADA, ANM and critical voice communications on a 2×3 MHz allocation.

¹⁹ Ofcom, *Call for Input: Potential spectrum bands to support utilities sector transformation*, June 2023.

450 MHz availability in the UK

Spectrum for an electricity private mission-critical communications network has been discussed and consulted on for more than a decade, including consideration of the 450 MHz band which other European nations have allocated for this use.

410–470 MHz spectrum in the UK has a number of incumbent licensees including a large number of private mobile radio users, and a band plan that is different to mainland Europe for historical reasons. This means that access to the 450 MHz band is unlikely to become available for some time for critical utility communications, and not in the timescales that meet DNOs immediate needs. There is, however, a strong case for exploring a future spectrum pipeline that includes a 450 MHz allocation alongside earlier access to 700 MHz. This could potentially add capacity and further coverage to a dedicated private network were it to be deployed. This could meet longer-term needs and offer the potential for a network with additional capacity for electricity, whole energy system and other utility critical communications.

Ofcom and its predecessor the Radiocommunications Agency have considered reconfiguring the band to ensure optimal use on a number of occasions over the last two decades, including in 2002–2004, in 2008, in 2014–2015, and in 2023²⁰. Broadly, on each of these occasions the conclusion has been that reconfiguration would bring benefits, but the cost and disruption were not considered proportionate to justify action.

Over the decade since the most recent decision the context of energy security has sharpened considerably. Net Zero is a core government mission, underpinned by grid modernisation and flexibility. The electricity grid itself has grown increasingly central to UK energy, and is increasingly complex to manage. And a nationwide electricity failure is high on our national risk register, classified with the highest possible impact severity rating of 5/5 (“Catastrophic”). This signifies potential economic damages in the tens of billions of pounds and a severe risk to life (defined as potentially causing over 1,000 fatalities or 2,000 casualties).

The 400–470 MHz band is a vitally important section of the radio spectrum, and a long-term perspective on its optimal use is essential. A further development which may make a case for reviewing the position in the 400–470 MHz band is the potential for interference from more recent deployments in neighbouring nations. DNOs currently use narrow band SCADA links in the band to serve their essential telemetry needs communicating with grid assets such as distribution sub stations. These links are increasingly seeing outages which appear to be as a result of cross channel interference from other European nations. This is likely to be because increasingly other European nations (including those discussed here such as Germany and the Netherlands) are deploying high power mobile networks in the band, which has historically not been the case. It means that in certain weather conditions the existing licensees in the UK 400 MHz band are vulnerable to long range interference from ducting conditions and an unaligned UK band plan. DNOs have experienced cases where a large number of links have gone down due to interference for periods of several hours. Such vulnerabilities are a concern for the electricity system as a whole, given they would hamper the ability to undertake restoration following a partial or national power outage during those periods.

The UK operates a “reverse” transmit/receive configuration to mainland Europe, commonly referred to as reverse duplex. This has been possible due to limited interference from abroad, an assumption that may no longer hold given the growing number of high power deployments and forecast increasing occurrences of ducting conditions due to climate change.

Taken together these factors suggest a review of the situation by Ofcom and other stakeholders would be beneficial, to establish what is feasible in the near term and longer term, as well as to address concerns over cross channel interference from European nation deployments of high power 4G/5G systems.

²⁰ Radiocommunications Agency consultation on realigning 450–470 MHz, December 2002, and Ofcom decision not to proceed, July 2004. Mott MacDonald review for Ofcom, 2008. Ofcom, *Strategic Review of UHF Spectrum at 420–470 MHz (UHF Bands 1 and 2) Call for Inputs*, 4 December 2014. Ofcom, *Call for Input: Potential spectrum bands to support utilities sector transformation*, June 2023.

Potential for a multi spectrum band solution

Both the 700 MHz and 450 MHz spectrum options should be pursued as potential allocations for a dedicated private network, including in combination.

The 700 MHz spectrum provides an ability to meet the most essential mission-critical communication near term needs of the DNOs, enabling a network to be deployed and made operational using 2×3 MHz.

Longer-term availability of additional spectrum at 450 MHz (or, in the far longer term, the UHF 500/600 MHz band) would enable a multiband

deployment on the same network infrastructure. This could add significantly to the utility of the private network, adding longer-term capacity for electricity DNOs, and opening up the potential of a 72-hour power resilient national network with additional capacity dedicated for wider critical utilities.

Where such a long-term approach to be considered at the outset, network infrastructure could be deployed cost effectively in anticipation of both 700 MHz and 450 MHz bands from the outset. Many of the assets are not duplicated, including land, masts, power, backhaul and the core network.

8 Conclusions

The UK's dependence on electricity is fundamental because almost everything else, infrastructure such as mobile networks & broadband, water and transport, the internet, hospitals, education, is downstream dependent on it. A national outage of the electricity grid is accordingly high on the UK national risk register, registered as a catastrophic impact event – the highest level that can be recorded.

The resilient communications network underpinning the energy infrastructure is the digital backbone of the future digitalised energy system. It is not an add-on, it is a fundamental enabling component of energy modernisation, playing an increasingly important role in enabling visibility, management and control of an increasingly complex energy grid.

Different communications networks, private and public, mobile and fixed, terrestrial and non-terrestrial will all have a role to play as

different use cases drive different network and architecture requirements. Our analysis has focused on the mission critical use cases and their requirements in terms of coverage, security, power resilience, latency and guaranteed delivery.

Several approaches are available to extend visibility and control across the transforming energy networks to support the delivery of a digitalised, low carbon energy system; they all raise key areas requiring further considerations to ensure they meet the mission critical needs of energy networks.

Table 6: Key considerations for the three approaches to mission-critical communications

APPROACH	KEY CONSIDERATIONS
Reinforced public mobile	• Delivery of end to end 72-hours power resilience across all comms elements (access, backhaul and core) in light of Ofcom's cost analysis. • Prioritisation of guaranteed traffic with low and stable latency. • Coverage of energy assets, often remote, indoor and below ground level and uplink limited. • Isolation to ensure security of utilities traffic.
Emergency Services Network (ESN)	• Current ESN's resilience to be assessed against energy assets requirements. • Prioritisation of guaranteed traffic with low and stable latency. • Coverage to remote, indoor and below ground assets and uplink limited. • Isolation to ensure security of utilities traffic. • Timing of deployment of service for energy against completion of ESN delivery programme for Home Office, scheduled for end of 2029. • Governance and decision making between the different sectors. • Emergency services and energy sector critical communications on one shared infrastructure, creating a single point of failure.
Mission critical private mobile network	• Latency, coverage, traffic isolation and power resilience are built in by design. • Deployment and operating models will need to be established, and governance agreed by the sector. • Requires dedicated spectrum and a pipeline for future growth. • Communications operations requires sufficiently resourced, specialist skilled workforce.

A move to modern 4G and 5G based technology (private and public) presents an opportunity to replace ageing communications infrastructure with known limitations in terms of resilience, cyber security and capacity. This would provide a standardised platform with a clear technology upgrade path, enabling DNOs to draw on the full device ecosystem innovations as the digitalisation of the UK grid proceeds provided that any such network meets the mission critical characteristics that have been identified above.

Public mobile networks, can meet many of the energy networks use cases; achieving the requirements of the mission critical use cases (SCADA, ANM and resilient voice), will require additional considerations in light of the current public telecom networks extent and capabilities.

Our analysis of international deployments of dedicated private 4G/5G mobile networks has highlighted how different deployments and governance models have been implemented internationally to meet the specific objectives of coverage, latency, security and resilience by design.

A dedicated network with low frequency spectrum means that a small number of sites are able to reach fixed assets, an order of magnitude lower than MNOs currently have deployed in the countries analysed. Additionally, the communications networks under review, in most cases, cover smart metering and smart grid infrastructure and include other the communications needs of other utilities. Radio spectrum is an essential component for a dedicated private network to address mission critical communication needs; with short term availability and a potential pipeline for growth.

The need for action is clear, as the energy system evolves, it needs telecoms solutions that meet a set of evolving requirements; there is now a clear government priority on energy security and focus on assessing the telecom needs of the sector covering both operational and restoration scenarios.

ANNEX 1

International Case Study 1: German deployment of a mission-critical private network for energy

A case study of 450connect – a utility-owned dedicated network

Summary

Germany has designed, built and now operates a nationwide dedicated private wireless 4G network for critical infrastructure with power utilities as the primary users. The network is owned and operated by 450connect GmbH, a national operator which itself is owned by the utilities that are the primary users of the network. The network runs on 450 MHz spectrum that the regulator assigned with the obligation to primarily address the requirements of the energy and water sectors and licensed exclusively to 2040.¹⁴

Defining characteristics are power resilience and wide area coverage. Every base station carries 72-hour battery back-up; backhaul is a self-operated, redundant microwave ring, meaning each base station has redundant backhaul with 72-hour power back-up; the core and voice platforms are geographically redundant. Microwave rings and core locations are connected via a redundant self-operated 72-hour power backed-up backbone ring to which utility customers can also directly connect to ensure full resilience of their Smart Grid applications. The network runs independently of the public mobile operators, engineered to keep working during and after a grid failure, supporting operation during outages, restoration, and black start.^{5,8,12,15,16} Low-band spectrum gives it national reach including rural areas and deep-indoor coverage from a comparatively small number of sites, which is what makes hardening every site to this standard affordable.^{1,17}

The network is largely complete. On the operator's reporting it covers around 96–98% of German land area, with 90% coverage delivered with 1000 sites roughly four years from the 2021 spectrum allocation.⁸ The network is able to carry substation control, distributed resource management and smart metering, giving the sector a stable, sovereign foundation for a decade plus modernisation programme.¹⁸ Energy change and digitization

requires communication throughout the network, thus having a resilient communication network in place allows flexibility in applications going forward through simple connectivity via sim cards.

The cost for the network, while not public, is low demonstrating efficiency and effectiveness in roll out model and approach and when benchmarked against alternative approaches.

This case study sets out the context, the spectrum and governance choices, the development pathway, the architecture, the services and the outcomes.

Context and challenge

Germany's dedicated critical infrastructure network approach has happened in response to the priority placed on the Energiewende, the German energy transition. As generation shifts from a few large plants to a large amount of distributed and flexible generation such as solar farms, wind energy and battery storage and millions of distributed, often behind-the-meter resources, the perspective taken was that the grid can only be balanced and controlled if those assets can be observed reliably and controlled in near real time. The German policy approach treats communication as a precondition for the energy transition, not an adjunct to it.¹

The summary rationale for the German approach was for a network which was able to operate during outages, coordinate restoration and support black start restoration. Although more recent events have sharpened the case such as the Iberian blackout leaving millions of people without power⁶, earlier failures in Germany, including Berlin power cuts and the 2021 flooding in the west, had already exposed the cost of losing communications alongside power and the issue of interdependence: power relying on communications, and communications relying on power.^{18,18} The wider threat picture including natural hazards, cyber-attack, geopolitical tension all presented challenges to power, but also all the downstream services dependent on power.^{8,18}

The conclusion reached jointly by the German state and the energy sector was that this capability lay outside what commercial mobile networks are structured to deliver, and should be treated as national resilience infrastructure.¹²

Mapping to the mission-critical requirements

While the digital use cases of DSOs and the wider energy sector are numerous, eg. CCTV, perimeter security, predictive maintenance, Germany's approach is to separate out those use cases which could reasonably be managed through public mobile, satellite and other routes, from the truly mission-critical requirements that must be available to maintain grid stability and for grid restoration.

The mission-critical use cases were noted to be of relatively limited capacity – critical telemetry and control to significant, distributed energy assets and mission-critical voice communications.¹ However the requirements for serving those use cases are challenging, including wide-area national coverage, multi-day power-independent availability, prioritisation, security isolation, in the German case deep indoor reach, and long-horizon technology stability. Germany sees Smart Meter Gateways increasingly as devices to manage distributed loads on the grid such as residential heat pumps and solar.

Spectrum choice

Low-band 450 MHz propagates further and penetrates structures better than the mid and high-bands used for mobile broadband, so equivalent coverage needs far fewer sites.¹⁷ The consequence is not simply the coverage, but what a low site count makes affordable. As most of the cost of a mobile network is driven by site count, building and operating a network with far fewer base stations and moreover hardening every one of them with extended battery back-up and redundant backhaul becomes financially feasible.

After a demand survey and consultation, BNetzA made the 450 MHz band available primarily for usage by energy and water critical infrastructure.¹ The allocation was contested with police, security and military bodies who had sought the same band, and the dispute was settled at government level in favour of the energy sector regarded as being fundamental

and upstream, with limited security co-use permitted where it does not compromise critical energy needs.^{2,3} Usage rights were awarded to 450connect in 2021, running to 2040.^{4,5}

The holding is 2×4.74 MHz, deployed today as a slim ~4.6 MHz LTE carrier or a 1.4+3 MHz combination with LTE-M in-band, with the operator targeting a standard 5 MHz carrier. This limited spectrum works with a focus on purely low capacity mission-critical use cases, as a resilience and coverage-first layer, not a broadband network for all utility use cases.

Governance, ownership and commercial model

The network is owned by the utilities that are the key users of it. 450connect GmbH is a joint venture with four equal shareholders: Alliander, a Dutch energy-network operator; E.ON, which majority owns nine regional distribution system operators; a consortium of ten regional utilities; and Versorger-Allianz 450, an alliance of more than fifty predominantly municipal utilities that includes the EnBW subsidiary Netze BW and Deutsche Bahn's distribution operators.⁴ The shareholders together supply around 90% of Germany's area with critical infrastructure services.

The network is run as an open platform: connectivity is offered via a standard wireless service contract on a non-discriminatory basis not only to the shareholder utilities but to other utilities and other critical-infrastructure operators.¹⁴

A single national "NetCo" makes commissioning efficient and spectrum planning consistent. 450connect controls the design of the network and the menu of approved equipment and coordinates all network deployment centrally, so interoperability across the network is guaranteed by design and vendors can be selected against security and sovereignty criteria. Requirements are fed in through a structured steering process, and in certain regions roll-out is delivered with regional utility partners who contribute sites and local capability.

The commercial model rests on generating revenues from shareholders, other utilities and critical infrastructures from connectivity services. Investment and upfront funding is carried by the shareholders and project finance.¹⁹

Development pathway and coordination

In 2016 Alliander acquired and rebranded the incumbent licence holder as 450connect, and utilities built regional CDMA450 networks that served as proof of concept.²¹ The 450 MHz band allocation was contested between the energy sector and public safety and security, which required resolution at government level.^{2,3}

Considerable effort was needed to address coordination and alignment, resulting in a coherent approach from government policy, down through regulation, and down through industry coordination. The utilities presented a unified position to government and regulator through the sector associations making a clear case to policymakers.^{11,21} A model of joint control offered to all interested utilities and non discriminatory access to all utilities – shareholders and others – addressed potential competition concerns.¹ The spectrum assignment process resulted in binding coverage and 72-hour power resilience obligations.⁸

450connect's build leaned substantially on existing commercial tower infrastructure as well as being supplemented with utility owned sites. Under long-term framework agreements the operator has access to Deutsche Funkturm's (DFMG) large site network and additionally Vantage Towers' and ATC's German portfolio of towers.^{8,12,20} Sites contributed by shareholder and partner utilities supplement this commercial estate rather than forming its backbone. Co-locating on an established tower base avoids greenfield construction, and was seen in combination with the low site count that 450 MHz affords, as a rapid path to widespread deployment. This commercially led site strategy is a notable point of contrast with the utility asset led approach seen in the following Austrian case study.

Technical architecture and design

The network is a standardised LTE system (LTE450), with LTE-M carried in band for low data machine traffic and a defined evolution path toward 5G. This gives access to a global device and vendor ecosystem.^{5,13} Nokia supplies the radio network and holds a maintenance contract running to 2040.⁵

The whole network from base station through backhaul to core is hardened to remain available through a grid blackout. Coverage is provided from roughly 1,600 planned base station locations, each with 72-hour battery backup.⁸ Backhaul is a self-operated microwave ring with redundant links, and the LTE core is geographically redundant.

Security follows from a closed, sovereign design. The backbone is self operated with tightly controlled access.¹⁵ The network is built to the standards applied to KRITIS (critical-infrastructure) operators

in Germany, and is operated as a closed network.⁹ Traffic prioritisation is implemented through technical mechanisms in both the radio access and transport layers, so that the most critical flows are prioritised when capacity is under load, using the LTE quality of service framework. A business and operations support system comparable to that of a commercial operator handles provisioning, administration and billing for the network's user organisations.¹⁰

Voice is provided as an end-to-end mission-critical push to talk (MCPTT) service, to offer utility field forces, control rooms and crisis teams a blackout resilient voice capability.

Routers are certified for the network through 450connect's approved equipment whitelist. They combine 450 MHz connectivity with a standard public LTE modem and dual SIM capability, so a connected asset can also route over, or fall back to commercial public mobile networks.¹³ The dedicated 450 MHz network is the primary bearer for mission-critical traffic and the public path adds capacity and redundancy for non-critical traffic. This enables devices to serve both the hardened mission-critical functions and less critical functions with appropriate connectivity from a single installation.

Nokia supplies the radio network and the certified end devices under a contract that also covers maintenance to 2040.^{5,8} Comarch provides the business and operations support system,¹⁰ and site build and management draw on specialist providers alongside the commercial tower companies.

Services and use cases

Because of the network's wide-area coverage and deep indoor coverage, it is able to reach widespread distribution assets as well as distributed assets "behind the meter". The network is therefore able to be a bearer of substation control, distributed resource management and smart metering. In Germany grid operators are able to control some behind the meter some consumption devices such as EV chargers and heat pumps during potential grid overloads, to balance supply and demand.²²

The service portfolio spans three tiers. The first is critical and operational communication such as switching procedures, reliable field voice and emergency communication during storms or blackout. The second is critical machine to machine communication for the active grid: connection and control of primary and secondary substations, generation and controllable loads and prosumers, and the equivalent critical M2M communications in gas and water. The third is smart meter gateways and remotely read gas, water and heat meters, seen as increasingly relevant for grid control in Germany.

Grid modernisation in Germany is a programme of a decade or more. Utilities can procure against a modern, standardised platform and draw on the full contemporary device ecosystem innovations as digitisation proceeds, rather than being confined to a narrow legacy control-system world. The network solves the resilience critical core needs, while the wider and much larger set of lower criticality needs, routine monitoring, CCTV and similar can be met through other commercial network services. This approach tackles the hard problem of ensuring resilience, robust, secure connectivity for the mission critical needs, offers spillover benefits to other uses when there is capacity, and leaves the large capacity, low criticality uses to be solved by heterogeneous use of commercial terrestrial and non terrestrial public network services.

Deployment status and outcomes

Implementation is largely complete. The network is based on roughly 1,600 planned sites and, on the operator's reporting, around 96–98% of German land area as of 2026, with the remaining gaps confined to a forested rural areas that are being filled.⁸ Measured from the 2021 spectrum allocation, 90% coverage was achieved in approximately four years with 1000 mobile sites.

The outcome is a national, resilient, sovereign communications platform, owned by its beneficiaries and open to all qualifying critical-infrastructure users, delivering grid resilience including black start and providing a foundation for grid digitisation at scale. The cost logic underpinning it that low band coverage needs an order of magnitude fewer sites than a high band equivalent, combined with relatively modest capacity sized around critical use cases, means building and operating the network and hardening the whole network to a 72 hour, redundant standard is affordable.

Key observations from the German case study

Feasibility Germany is one of a number of clear, real world data points showing that such a network can be cost effectively deployed and that the promised benefits have been accrued. Critical utilities are beneficiaries for their critical use cases beyond the DNOs.

Affordability Low band spectrum needs far fewer sites. Combined with limited spectrum bandwidth targeted on only critical use cases makes building and operating a dedicated network with full 72-hour, redundant hardening affordable.

Rapid deployment Germany moved from spectrum award to 90% coverage in about four years, with full coverage expected in 2026.

Clear resilience standards Germany specified a resilience standard which extends across a national footprint. This 72-hour standard follows the recommendation of Germany's Federal Office for Civil Protection and Disaster Assistance (BBK) that critical-infrastructure operators sustain emergency power for at least 72 hours without external refuelling.¹⁴

Whole energy sector utilisation The 450 connect network is a shared, resilient communications bearer, with visibility across German DNO's assets, and also to behind the meter assets. Services are able to be offered to all parts of the sector. This includes a metering tier for smart meter gateway connectivity, operators can control behind the meter devices such as EV chargers and heat pumps to control demand and supply, alongside wider grid control/M2M and critical voice. In Germany smart metering gateway traffic can be carried over a number of options such as public cellular and broadband, and 450connect adds another option addressing indoor and hard to reach meters and critical use cases for load management.

A stable national platform as a foundation for digital transformation The network provides a key pillar of the grid digitisation with a national footprint. A secure and resilient platform using standardized 4G mobile technology giving DSOs and other critical utilities access to the modern device ecosystem and equipment innovations.

Coordination The German timeline shows a lengthy part of the process was aligning government, regulators and industry behind a single position. Once aligned, delivery was relatively quick.

Facts and figures

Table 7: Facts and figures for the German 450connect deployment

ATTRIBUTE	DETAIL
Operator	450connect GmbH, Cologne.
Ownership	Utility joint venture; four equal shareholders – Alliander; E.ON (9 regional DSOs); a regional utilities consortium; Versorger-Allianz 450 (50+ mostly municipal utilities).
Shareholder reach	Shareholders together supply around 90% of Germany's area with critical infrastructure services.
Spectrum	450 MHz band; 2 × 4.74 MHz; exclusive; administratively assigned to critical infrastructure.
Licence term	To 2040 (20 years; awarded 2021).
Technology	LTE (LTE450); LTE-M in-band; 5G evolution path.
Sites	~1,600 planned base station locations.
Coverage	~96–98% of land area (2026); limited rural gaps being filled, target >99%.
Power resilience	72-hour battery back-up at every base station and throughout backhaul and backbone network.
Backhaul & core	Self-operated redundant microwave ring and national backbone; geo-redundant LTE core and MCPTT.
Voice	Mission-critical push-to-talk (MCPTT).
Access	Non-discriminatory: shareholders, other utilities, other critical infrastructure via standard wireless connectivity service contract.
Principal vendors	Nokia (radio, core, maintenance to 2040); Comarch (BSS/OSS).

Development timeline

- **2013** – First tests in the band with the utility industry.
- **2013** – Utilities and associations articulate demand for secure, dedicated communication.
- **2016** – Alliander acquires and rebrands the licence holder as 450connect; regional CDMA450 networks; smart-metering legal framework takes shape.
- **2019** – Alignment of associations BDEW and VKU and interested utilities to jointly advocate for a spectrum allocation procedure.
- **2020** – BNetzA reserves the band for critical infrastructure; utility joint venture 450connect formed.
- **2021** – Licence awarded to 450connect, running to 2040.
- **2022** – Nokia selected for the radio network; Comarch for BSS/OSS.
- **~2025–26** – Roll-out largely complete; ~96–98% land-area coverage.

Annex 1 references

1. Bundesnetzagentur (BNetzA), Decision of the President's Chamber of 16 November 2020 on the award procedure and rules for spectrum in the 450 MHz band (451.00–455.74 MHz/461.00–465.74 MHz) for wireless network access, primarily for critical infrastructure applications, ref. BK1-20/001.
2. Clean Energy Wire, "Grid agency votes to give Germany's energy industry own blackout-proof communication line."
3. Clean Energy Wire, "German energy industry to receive dedicated radio frequency to weather blackouts."
4. 450 MHz Alliance, "450connect Receives the 450 MHz License Rights for the Next 20 years," 9 March 2021.
5. Nokia, "Nokia chosen by 450connect to supply network technology for LTE450 critical infrastructure network in Germany," press release, 14 February 2022.
6. ENTSO-E, "28 April 2025 Iberian blackout" – final report of the Expert Panel; and contemporaneous reporting of the event.
7. Arthur D. Little, "450 MHz – the spectrum phoenix," 2026.
8. teltarif.de, "450connect: an almost unknown mobile network," 25 April 2026 (coverage and resilience status).
9. Horstmann, "Why do energy utilities need a connection to the 450 MHz network?"/"450 MHz radio network: insights and status quo," 2025.
10. Comarch, "Comarch becomes new partner of 450connect, sole operator of the 450 MHz frequencies in Germany," 18 May 2022.
11. BDEW/VKU, open letter of the German energy and water industry on the urgent need to allocate the 450 MHz frequencies, November 2019.
12. Vantage Towers AG, "Vantage Towers and 450connect sign long-term partnership for the roll-out of a nationwide critical-infrastructure network," press release, February 2022.
13. INSYS icom, "LTE450: critical infrastructures always online" – product information and Versorger-Allianz 450 membership, 2026.
14. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), guidance on emergency power supply for operators of critical infrastructure and authorities (recommendation of at least 72 hours without external refuelling).
15. 450connect and GasLINE, "450connect und GasLINE sind Partner für bundesweiten Backbone," press release, 26 April 2022.
16. gwf Gas + Energie, "Zukunftssicheres Kommunikationsnetz für die Gaswirtschaft," issue 01-02/2024 (reproduced on 450connect.de).
17. Energie & Management daily, "Eon-Tochter baut 450-MHz-Netz aus," 22 February 2024 (reproduced on 450connect.de).
18. 450connect, "450connect erreicht 1.000 Funkstandorte: 90 Prozent Flächenabdeckung als Rückgrat der Resilienz in Deutschland," press release, 8 October 2025.
19. LBBW, "LBBW finanziert den Aufbau des bundesweiten LTE450-Funknetzes durch 450connect," press release, 2 March 2022.
20. Deutsche Funkturm, "450connect und Deutsche Funkturm beschleunigen Ausbau kritischer Infrastruktur," 20 November 2025.
21. 450connect, "Organisation" (company background and history), 450connect.de, accessed September 2026.
22. Bundesnetzagentur, Ruling Chamber 6, Determination BK6-22-300 on the integration of controllable consumer devices and grid connections under §14a EnWG, 27 November 2023.

ANNEX 2

International Case Study 2: Austrian deployment of a mission-critical private network for energy

A case study of ArgoNET a utility-owned dedicated network

Summary

Austria has regionally built and is nationally building a dedicated 450 MHz network for critical infrastructure that rests on the same foundations as the German 450connect model examined in the previous case study of Germany: exclusive low-band spectrum, a private and closed network, hardening against blackouts, standardised LTE evolving to 5G, utility ownership, and non-discriminatory access.^{1,2} Austria has adapted the German approach to its own national circumstances and to the preferences of its distribution network operators (DNOs).

The single most important difference is the building and operating model. In Germany a single entity builds and operates the whole national network. In Austria the central body, ArgoNET, holds the spectrum, the standards and designs, the approved equipment framework and a central core, while the 10 regional DNOs that are the shareholders of ArgoNET build, own and operate their own regional networks, which interconnect into one national platform.¹ Also a significant difference is that Austria's network deployment approach is chiefly on utility owned sites rather than commercial towers, with a different ownership model.^{1,2} It also divides use of the spectrum band via slicing, and is of a smaller scale given the landmass. The core objective and requirements are shared with Germany, including the focus on critical infrastructure with full network redundancy, power resilience requirements of up to 72 hours and low band national coverage, but the deployment and operating model to achieve this are different.

Context and challenge

Austria's drivers mirror Germany's. A decentralising, decarbonising grid, with rapid growth in distributed generation, storage and flexible load (photovoltaic capacity alone approached 8,000 MWp in early 2025). A similar view was taken that the grid can only be balanced and controlled if dispersed assets can be monitored and actuated reliably, including through power restoration.²

The rationale for a dedicated low band network is therefore essentially the same as in the German case, with public mobile networks not being able to provide the particular stringent requirements of coverage depth, blackout resilience, security isolation and long horizon stability that were requirements of their grid critical communication.^{2,6}

Like Germany, Austria separates the genuinely mission-critical requirements, resilient telemetry and control of distributed energy assets, and emergency communication, from the wider set of utility connectivity needs that can be met by public mobile, satellite and commercial services.¹ The 450 MHz network is scoped to be the resilient critical use case core. ArgoNET centrally offers connectivity services to all other utilities and critical infrastructures which may include 4G/5G connectivity for less critical, higher capacity needs subject to residual network capacity and demand.²

Spectrum

ArgoNET is the exclusive holder of Austria's 450 MHz spectrum (3GPP band 72)⁷. The low band rationale is the same as Germany's: long range and deep building penetration from few sites (cells reach up to around 20 km)⁸, making nationwide, indoor-capable coverage affordable to build and to harden.^{1,2,5}

ArgoNET holds the spectrum allocation and divides usage of the band into slices to better differentiate the owning utility for its own regional needs and ArgoNET for its central platform services offering connectivity services to all other utilities and critical infrastructures in Austria.¹ This split gives each regional DNO dedicated, guaranteed capacity in its own territory, preserves capacity for ArgoNET's national platform role ensuring services for all critical infrastructures, and also reserves headroom for "roaming" utilities operating outside their home region.

Governance, ownership and commercial model

ArgoNET is a 100% shareholding of 10 regional Austrian DNOs, with headquarters in Gmunden.^{1,2} This guarantees they have control and governance over the mission critical communications infrastructure required for grid stability and smart metering. The venture grew out of earlier regional networks, notably with Energie Steiermark and Energie AG Oberösterreich from around 2016, before consolidating into the 10 DNO structure.³

This is a more direct all operator ownership than in the case of Germany's many operators, where four larger shareholder groups represent a broader base. In both countries access is non discriminatory, so ArgoNET offers secure services to owners and to other qualifying critical infrastructure users alike.¹ The commercial logic is shared at achieving reasonable returns on capital, rather than profit maximisation.

ArgoNET built operational experience through regional CDMA and LTE networks before scaling to a national footprint as the 10 DNO joint venture.^{3,4} The national build grew incrementally from existing regional utility initiatives starting in 2014.

Technical architecture and design

The Austrian design is best understood as a single national network assembled from regional networks; a federated, multi-core platform. Modern LTE permits several radio access networks and several cores to operate together under one operator identity with strict separation and secured, ring-fenced capacity. ArgoNET designs and builds its platform on this basis² dividing a central layer and a regional layer, joined by interconnection.

The central layer, ArgoNET

ArgoNET is the licensed national mobile network operator. It holds the 450 MHz spectrum and a single national operator identity (PLMN); it defines the uniform technical solution and does the central engineering and planning; it runs the central core and connectivity-management platform and provides common support and maintenance; and, critically, it procures all base-station and central-systems hardware and software through a single central framework contract, so every region deploys from the same approved-equipment menu.¹ ArgoNET and the DNOs jointly operate the redundant interconnection between regional subnetworks and the central systems, and handles cross-border

coordination with 450 MHz neighbouring operators and spectrum authorities.¹ In summary ArgoNET holds everything that must be common for the network to be one network: spectrum, radio planning, standards, equipment, the central core and the operator licence. ArgoNET, owned by the regional DNOs, has the mobile technology and network operating expertise that is required to design and coordinate the network build, and train and support the local operations.

The regional layer, the DNOs

Each owning DNO builds, owns and operates the regional "subnetwork" in its own territory. It owns the radio infrastructure, the sites and base stations, typically on its own or existing tower, and backbone infrastructure, and it runs its regional network with its own dedicated packet core and network management, staffed 24/7 by the utility.¹ Each region is engineered to be fully autonomous in an emergency; with its own core, a regional network can continue operating even if cut off from ArgoNET's central systems. Service quality is guaranteed through dedicated radio slices, so critical traffic is protected within each region.² Regional builds include their own geo redundant central technology, and the whole regional network is engineered for up to 72 hour autonomous availability across all elements.¹

National network layer

The regional subnetworks interconnect with one another, giving coverage and handover efficiencies at regional borders without the need to go through ArgoNET's central systems, enabling continuity of service across borders, rather than a patchwork of disconnected regional islands.¹

The uniform technical solution and the single central equipment framework guarantee interoperability across every region.¹ Because ArgoNET holds the PLMN, the spectrum and takes care of network planning and optimisation, the many regionally owned parts of the network present as one licensed national network.

The resilience standard itself is up to 72 hours of autonomous availability, extended explicitly to backhaul and core as well as the radio sites. LTE450 devices also carry a standard public LTE modem and support dual-SIM operation if required, allowing non critical traffic to use the commercial networks while the dedicated network retains its blackout independence. The LTE450 SIMs are individually distributed by ArgoNET for each regional network.^{1,5}

Services, use cases and the digitisation platform

Wide-area coverage and deep indoor coverage enables reach to widespread distribution assets as well as distributed assets “behind the meter”. So resilient telemetry and control of grid assets (substations, distributed generation, switching and monitoring), smart metering and emergency communication are all able to be serviced by the network.^{1,4}

Deployment status and outcomes

Each DNO builds in its own territory, predominantly on its own or existing radio installations, with site infrastructure provided by the utility wherever possible.¹ This is the mirror image of Germany, where the build leaned heavily on commercial tower companies.

The network is smaller in absolute terms compared to Germany given the smaller country geographic area. Coverage is live with about 200 sites across many regions and expanding toward national, although there is no single national coverage figure published.²

Because each DNO owns and controls its own rollout, the incentive to complete its territory sits squarely with the beneficiary of the service. The Vorarlberg project run by illwerke vkw is illustrative, covering demanding alpine terrain consists of a final build of some 15 to 20 sites only, mostly on existing installations, with geo-redundant central technology and up to 72-hour resilience, scheduled to complete end of 2027 at a quoted investment of roughly €2.2 million.¹

Key observations from the case study

A federated ownership and deployment approach

Austria, alongside Germany, gives another real world data point that establishes efficient and cost effective deployment and operation of a private communications network for energy is viable. Albeit on a smaller landmass than the UK, Austria demonstrates a network can be built predominantly on utilities’ own and existing sites, a contrast with the commercial tower led German build.

Germany runs one redundant central core, one operator and one builder in a single NetCo; Austria runs one central spectrum holder and national platform above many regional cores, operators

and builders. The German approach essentially optimises for central uniformity and operational efficiency, where Austria optimises for DNO ownership, direct control and regional autonomy, accepting more distributed operations and a greater interconnection burden.

These trade-offs are clear choices. The federated model buys DNO ownership, autonomy and resilience through regional cores, but at the cost of more distributed operations, a greater interconnection and interoperability burden. The single, central, national operator model buys uniformity, operational efficiency, but requires DNOs to cede direct control and a single entity to be capitalised for carrying most of the investment (albeit of which they are direct or indirect shareholders of). Austria and Germany demonstrate two viable points on a spectrum of deployment, governance and operating models. The UK could adopt either or variants thereof, depending on trade-offs of regional versus national factors, network complexity and the central vs distributed and replicated resources and specialist skills necessary. Security concerns may also impact architectural decisions in a more complex, regional and interconnected approach.

Were the UK to have only 2×3 MHz available this may make an approach of independent regional networks challenging with regard frequency coordination and usable capacity with which further work would need to address.

Development timeline

- **2013** – ArgoNET founded; becomes holder of Austria’s 450 MHz (band 72) licence
- **2014** – First regional CDMA450 network deployment started with Energie AG Oberösterreich
- **2016** – Second regional CDMA450 network built with Energie Steiermark.
- **2019** – Energie Steiermark takes a strategic stake; regional footprint expands
- **2020** – LTE450 technology introduced
- **2024/2025** – ArgoNET sold to DNOs and therewith consolidation into a national platform owned by 10 regional DNOs; nationwide rollout in progress.
- **from 2024** – Further regional LTE450 network deployments such as Vorarlberg (illwerke vkw) started.

Annex 2 references

1. illwerke vkw AG (C. Atzlesberger), “LTE450 Projekt Vorarlberg – Vorstellung VTV,” 12 November 2025.
2. ArgoNET GmbH, company, technology and partnership pages, argonet.at (accessed 2026).
3. 450 MHz Alliance, “Energie Steiermark invests in ArgoNET with 34 percent stake,” 2019.
4. 450 MHz Alliance, “Annual Global Update 2025” (public version), December 2025.
5. INSYS icom, “LTE450 – the network for secure communication,” 2026.
6. ArgoNET GmbH, application to the Telekom-Control-Kommission for approval of a change in ownership structure under §20(4) TKG 2021, 30 July 2024, ref. F 6/24 (redacted version published by RTR).
7. RTR (Rundfunk und Telekom Regulierungs-GmbH), “Spektrum 450 MHz”, and Telekom-Control-Kommission decisions F 4/13 (24 February 2014) and F 3/16 (27 June 2016) approving the transfer of 450 MHz usage rights to ArgoNET.
8. antennen.at, “ArgoNET 450 MHz,” March 2024.

ANNEX 3

International Case Study 3: US Southern Linc

A single utility self-built mission-critical network

Summary

Southern Linc is the mission-critical wireless network of Southern Company, one of the largest energy holding companies in the United States. Unlike the German and Austrian cases, where the network is owned by a consortium of utilities, Southern Linc is built, owned and operated by a single vertically integrated company for its own electric utilities, and then made available to others.^{1,7} The area covered by the Southern Linc network at more than 122,000 square miles is larger than the UK landmass so in some ways it is akin to a national scale in a UK context.^{2,4}

Southern Linc has operated a dedicated network across the hurricane exposed US southeast since 1996, and its LTE network since around 2016, through a long succession of major storms. Its reliability record is widely cited within the US utility sector, designed to ensure continued communications during outages and to speed restoration. It has similar resilience to the German and Austrian case studies, but has been operating for a long enough period to have been tested in severe storms and prolonged outages.^{1,3,7,15}

While it was designed and deployed to support Southern Company through storms and power outages with principally SCADA and critical voice communications, it has become a platform that carries a growing population of grid control, monitoring, metering, sensor and workforce devices.^{2,4,16} Southern Linc operates as a commercial carrier selling to external customers, providing communications for other utilities and to public safety agencies including US first responders.^{7,10,15}

Ownership and build model

In 1996, Southern Company which serves around nine million customers¹⁶ across one of the most hurricane exposed regions of the United States, concluded it needed its own wireless communications to ensure continued communications during power outages and to speed restoration when severe weather struck. It launched Southern Linc that year on narrowband push to talk technology. From around 2015 it upgraded its network to LTE with Ericsson, beginning operation in 2016 and fully operating in 2019 as CriticalLinc, widely described as the first dedicated mission-critical LTE network in the United States.^{1,7,10} The network runs on 3 MHz of licensed 800 MHz spectrum (3GPP Band 26).^{10,17}

Southern Linc is not a joint venture of a number of utilities, but a single company which designed, deployed and operates its own network with its own workforce. Southern Linc's CEO has publicly stressed that while spectrum was one part of the challenge, another enduring requirement is a qualified workforce able to operate and maintain the network, which was noted as "a heavy lift for utilities".⁷

The network covers roughly 122,000–127,000 square miles across Alabama, Georgia, Mississippi and the Florida Panhandle. It has of the order of 1,200 cell sites.^{7,17} Ericsson supplies the core technology.^{1,2}

The cores are geo-redundant, each backed by two generators.^{7,17} At the mobile sites last mile backhaul has redundancy at roughly 80% of sites. There is battery back up of about eight hours at every site, and on site fuel and generation sufficient for around five days of autonomous operation.⁷ Much of the backhaul runs on fibre owned by Southern Company itself, reducing dependence on third parties.⁷

The network operates as a commercial carrier, selling wireless services to aligned 3rd parties.^{7,15} Because it owns spare capacity on a network built to mission-critical standards, Southern Linc's leadership set out a vision in 2018 of acting as a 'utility of utilities', leveraging its core capacity for utilities in a similar position.¹⁷ In 2024 it entered agreements with Ericsson, NRTC and Anterix under which Southern Linc hosts the network core for rural electric cooperatives, while the co-ops build their own radio sites using Anterix's 900 MHz spectrum.¹³ It also serves public safety and first responders, and provides interoperable push to talk over CriticalLinc to state agencies in Georgia and Alabama.⁸

While the upfront CapEx was substantial, the case for a self-built network rests on a long-term Total Cost of Ownership (TCO) argument, set out in industry analysis of utility private LTE and consistent with Southern Linc's own account of why the investment proved worthwhile:^{7,12,19,20}

- No OpEx Data Fees: In a standard public MNO or MOCN model, utilities pay recurring monthly SIM card fees and per-megabyte data charges.

By owning the network, Southern Linc pays no data fees to transfer millions of continuous data packets from their substations, meaning the marginal cost of adding a new smart grid sensor is very low.^{12,18}

- Asset life and upgrade control: network assets are held and refreshed on a utility asset lifecycle rather than a carrier's refresh cycle, and the owner controls its own upgrade timetable and capacity headroom.^{10,12,19}
- Commercial Income: Because the network is reliable, Southern Linc sells capacity to public safety agencies, state agencies, school districts and local governments.^{8,15}

Endurance in major storms

Across nearly three decades its dedicated network has been tested by many of the most severe storms to strike the US Southeast, and has repeatedly supported the utility with continued communications and supported restoration. Significant events are summarised below.

Table 8: Facts and figures for the US Southern Linc deployment

STORM	YEAR	NATURE	RELEVANCE TO SOUTHERN LINC
Hurricane Katrina	2005	Catastrophic Gulf hurricane	iDEN-era test; Southern Linc reports full system availability restored within 72 hours. ⁴
Hurricane Irma	2017	Major hurricane, Georgia	First major test of the new LTE network. Southern Linc's engineering manager reported that the network withstood the hurricane and its aftermath, giving assurance that it met its mission critical design. ¹
Hurricane Michael	2018	Category 5 at landfall, FL Panhandle	Southern Linc lost cell sites due to the hurricane. The day after landfall about 88% of its sites in the affected areas were in service; three days after the storm it was back to 100% in Alabama, more than 99% in Georgia and almost 92% in Florida. Southern Linc attributed this to generators or fuel cells at 99% of its LTE sites, and to redundant microwave paths that kept sites connected where fibre had been severed, often by aerial lines torn down with the poles. ^{15,21}
Hurricane Zeta	2020	Hurricane, GA/AL	Zeta knocked out grid power to over 1.5 million Southern Company utility customers. ¹⁴ Southern Linc remained operational across the majority of its footprint. It restored outages at more than 24 sites and deployed 18 mobile assets to keep communications available. More than 10,600 responders worked the restoration. ¹⁴ With communications maintained throughout, Georgia Power and Mississippi Power had restored all customers who could safely receive power by the Monday after the Thursday landfall, and Alabama Power, the worst affected, by the Wednesday. ¹⁴
Hurricane Helene	2024	Cat 4 landfall; catastrophic, statewide GA impact	Severe impact; relied on redundant communications (incl. satellite) to support critical services and multi-agency restoration. ^{3,5,6}

Facts and figures

ATTRIBUTE	DETAIL
Operator	Southern Linc (Southern Communications Services, Inc.), a wholly-owned subsidiary of Southern Company; HQ Atlanta, Georgia.
Ownership model	Single vertically-integrated utility; built, owned and operated for its own electric utilities (Georgia Power, Alabama Power, Mississippi Power).
Spectrum	Licensed 800 MHz (3GPP Band 26).
Technology	iDEN (from 1996) → LTE (CriticalLinc, from ~2016); vendor Ericsson.
Coverage	~122,000–127,000 sq miles across AL, GA, MS and the FL Panhandle.
Sites	Of the order of 1,200 cell sites.
Cores	Geo-redundant, two generators each.
Power resilience	~8h battery at every site plus ~5 days on-site fuel/generation; ~80% of sites with last mile backhaul redundancy.
Backhaul & core	Much backhaul on Southern Company-owned fibre.

Annex 3 references

1. Ericsson, “Keeping the lights on with dedicated LTE” (Southern Linc case study), 2018.
2. Southern Linc/OneLayer, “Southern Linc Leverages OneLayer to Enhance Management and Security of Its Ericsson Private Cellular Network,” 31 March 2025.
3. Gilat Satellite Networks and Hispasat, “Immediate satellite communication to support disaster recovery after Hurricane Helene,” January 2025 (via StockTitan and IoT Insider).
4. Southern Linc, corporate and resilience information, southernlinc.com (accessed 2026; incl. Hurricane Katrina 72-hour restoration).
5. Southern Company, “A storm of unprecedented magnitude – Southern Company’s response to Hurricane Helene,” 17 October 2024.
6. Georgia Power, Hurricane Helene restoration press releases, 28 September – 7 October 2024.
7. UrgentComm, “Southern Linc CEO says utilities, critical entities at ‘inflection point’ on private LTE,” 2022.
8. PR Newswire/Barchart, “Southern Linc and Georgia State Agencies Celebrate Interoperability Project with Ceremony at the Capitol,” October 2025.
9. Renewable Energy World, “‘Private means control’: Why utilities are ditching carriers for their own communication networks,” May 2024.
10. Black & Veatch, “Building the business case for 800 MHz spectrum: a strategic asset for utility grid modernization.”
11. Ericsson, “Ericsson, NRTC, Southern Linc and Anterix ink landmark agreements to deliver connectivity for rural electric cooperatives across the U.S.,” press release, 6 August 2024.
12. Southern Company, “Restoration complete following Hurricane Zeta,” 6 November 2020.
13. Georgia Power (P. Bell), written testimony to the US House Committee on Energy and Commerce (Southern Linc coverage, customer base and reliability record).
14. Southern Communications Services, Inc. d/b/a Southern Linc, statement in support of experimental licence application, 900 MHz band, FCC (service territory, AMI backhaul, SCADA and push-to-talk applications; Southern Company customer numbers).
15. UrgentComm, “Southern Linc offers ‘Basic MCPTT’ and ‘High Performance MCPTT,’ shuts down legacy iDEN system for LTE,” 30 April 2019 (iDEN shutdown; move from 1.4 MHz to 3 MHz; site count; dual cores).
16. Anterix, “Why are utilities embracing private LTE networks? A Q&A with Mike Brozek,” 2024.
17. Burns & McDonnell, “10 Private LTE Considerations for the Utility C-Suite.”
18. Energy Central/Intelligent Utility, “Understanding Private LTE’s Value and (True) Total Cost of Ownership,” October 2022.
19. Federal Communications Commission, “Communications status reports for areas impacted by Hurricane Michael,” 11–26 October 2018 (Disaster Information Reporting System cell-site outage data by county).