BURNS McDONNELL

WHITE PAPER / **PRIVATE NETWORKS FOR UTILITIES**

CHOOSING PRIVATE OVER PUBLIC NETWORKS FOR CRITICAL COMMUNICATIONS

BY Dan Bayouth, PE, AND **Matt Olson,** PE

When disaster strikes, communities need power restored quickly. To make that possible, communications are paramount. With limits and conflicting priorities on public communication networks, investment in pursuing and upgrading private networks is becoming more attractive.

A utility's priorities are different from those of public communication network providers like Verizon or AT&T. Each approaches technology investments and measures success differently. They have differing customer service expectations and reliability needs. When natural disaster strikes, they respond differently.

These are some reasons why utilities operate private voice and data networks, rather than outsource communication to public carrier networks. In addition, private networks can be designed to cover areas that commercial providers do not. They also can be hardened to operate in severe conditions, remaining in service during and after hurricanes, fires and other natural disasters.

As the owner and operator of a private network, a utility is aware of the network's status 24/7 and makes all decisions about utilization, maintenance and upgrades. Just as important, a utility has discretion over how private network resources are allocated. If it allows third parties on the network, the utility manages the priority they receive. It can prioritize its traffic over other wireless network users, including public safety agencies and the general public.

GENESIS OF A PRIVATE NETWORK

In the 1950s, when utilities started deploying communications, it was land-mobile and fixed voice circuit networks. The mobile networks were utility-constructed because there were no commercial operators yet. The SCADA (supervisory control and data acquisition) and protection analog voice circuits were often copper circuits leased from the local telephone company. The phone company would provide class A circuits, which were designed to operate during electrical fault conditions, and it would provide a service-level agreement for their repair, often four hours.

Private networks have expanded steadily over time, with the construction of analog microwave networks between the land-mobile radio tower sites. As protection over telephone circuits became more widely deployed, what were once leased phone circuits moved to private analog microwave networks. As mobile voice and data communication grew, and common carriers migrated from copper phone networks to fiber data networks, utilities have elected to maintain and expand their private networks instead of moving critical services to common carriers. That choice is due, at least in part, to the reliability of the public networks. When common carriers were regulated utilities, network reliability was considered a key metric for measuring success. With deregulation, that is no longer the case.

Public carriers also continue to move to Ethernet-based services and retire four-wire analog phone circuits and other legacy services essential for power grid control. No public system replacement technology offers service level guarantees, including latency and service restoration for protective relaying applications comparable to the former class A circuits. In the last 10 years, as the installed base of fiber has increased, and with their expanding need for more real-time information, many utilities now consider private networks a necessity. They are increasing their investment to move all of the communication needs to private networks.

BENEFITS OF A PRIVATE NETWORK

Beyond these logistical concerns, the benefits of "going private" are wide-ranging.

Safety of utility staff. A private network provides staff with situational awareness during operations and system outages. Switching commands and status can be broadcast to make crews aware of system conditions in real time. Because these networks are designed to provide coverage in all areas where staff may be present, radio-carrying staff can quickly signal for help and receive messages when other communication methods are unavailable.

Data networks also can be designed to allow staff to operate equipment remotely. With improved monitoring and control capabilities, staff can diagnose and isolate repair needs more quickly and operate equipment remotely, reducing exposure to hazardous field conditions.

Availability. Utility staff are expected to rush in following a natural disaster or other crisis to restore electric service. Their mission: to help community life return to normal as quickly as possible. Their networks must be designed to support this mission-critical work. This requires hardening communications facilities with backup power and multiple methods of inter-site communication. Structures must be designed to withstand high wind and ice loads, and dual transportation links must be constructed to reach them. Utilities must maintain days' or weeks' worth of backup generator fuel, along with batteries capable of backing up the backup.

Consider Hurricane Michael, which struck the Florida panhandle in October 2018. When utility recovery began the day after the storm, more than 60 percent of wireless sites in 10 affected counties were out of service, according to the Federal Communications Commission. See Figure 1. It took 18 days to restore service to the point where no more than 15 percent of a county's sites remained out of service. A private network in the same area lost communications to about 10 tower sites, and three towers either had all equipment blown off or fell. Using temporary towers, service was restored to all areas within three days.

Relatively economical for utilities to install or modernize. Because fiber cable is immune to noise and requires less maintenance than traditional copper cable, it is a reliable choice for both public and private communications networks. By leveraging existing rights-of-way, utilities can build or modernize networks by installing fiber in optical ground or distribution lines at a marginal cost during line construction or renovation.

Better control of investment life cycle costs. Technology life cycles for utilities and public carriers do not generally align. Public carriers face constant pressure to lure customers from competitors by deploying new features and the fastest speeds. Utilities, on the other hand, are regulated and driven to manage the cost of delivering reliable electric power services. For example, they expect a 10-year service life for the cellular modems they often use for noncritical applications, compared to three years among common carriers.

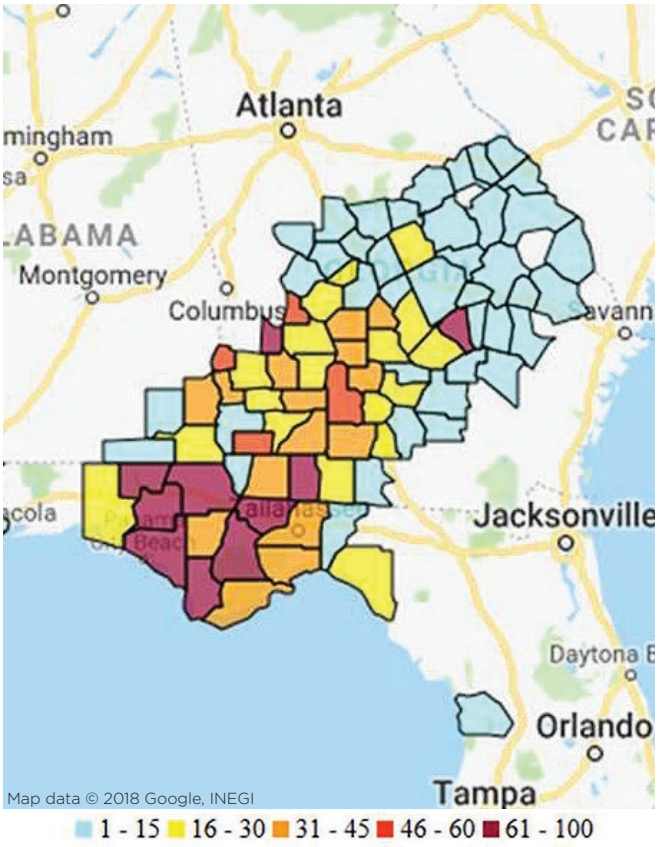

FIGURE 1: *Percentage of cell sites out of service following Hurricane Michael by county on Oct. 11, 2018; Source: Federal Communications Commission*

Over the past 10 years, utilities on public networks have replaced all first- and second-generation modems with third-generation devices, which are in turn being replaced with fourth-generation devices as carriers deploy fifth-generation networks. These upgrades provide little benefit to utilities and are only conducted to maintain compatibility with the public networks that provide them service. The continual redeployment of devices to maintain compatibility is a challenge for most utilities that will only grow more acute. Public carriers typically give utilities six months to three years of notice of planned retirements. This creates planning challenges for utilities, which generally require one to three years to design and build a replacement network or implement upgrades.

Improved incident response management. Utilities that own their communication assets have greater visibility into all aspects of network operation, including remote terminal cabinet battery health and cable maintenance. This visibility makes it possible to identify network issues and their impacts quickly, enabling utilities to allocate appropriate resources in response to incidents or outages.

Consider how detailed infrastructure management helps utilities improve customer service during a storm. If distribution line power to key communications nodes goes out during a storm, operations staff can identify the generator — a key communications hub in the system — that failed, triggering the site to operate on batteries. The operations staff can prevent further degradation by sending staff to the site with a portable power source to restore service. Compare that experience to working with a carrier, which typically provides little information about the system status and does not have the equivalent of an outage management website to communicate the status of repairs with its customers.

Prioritization matching a utility's critical needs. Following an outage, public carriers must focus on restoring network service to all of their customers. Electric utilities' focus, however, is on returning power to *their* customers. The utility's critical needs may not align with those of the public carrier responding to the same incident. For example, communication cables to a large, rural, extra-high-voltage switching station are vitally important to power grid operations, and restoration of such a line is critical to restoring power to customers after an outage. A public carrier may deem these communication lines a much lower priority for restoration, especially if the long radial distribution line serves only a few customers.

To utilities with wired facilities, common carriers also offer minimal committed information rates and the ability to classify information within that rate. On wireless networks, however, utilities do not have the ability to classify important business traffic over any other cellphone user. This has resulted in instances where wireless transmissions cannot get through. In November 2011, for example, an East Coast earthquake caused minimal physical damage, but congested the network all day as users shared their experiences with one another.

As an alternative, some utilities have met their wireless requirements with FirstNet, which prioritizes traffic on AT&T's public network. Utilities, however, are classified as secondary behind public safety agencies, and promoted to top level on FirstNet on a case-by-case basis.

When a utility owns its communications infrastructure, it avoids these issues. As the network's sole administrator, it manages traffic classifications end to end.

CAN THIRD PARTIES PROVIDE THESE MISSION-CRITICAL SERVICES?

While technically possible, service providers don't typically wish to share the level of detail requested, nor commit to redundancy and reliability requirements. Utilities have approached common carriers and proposed infrastructure-sharing arrangements that call for the utility to harden power systems, allow access to their more robust towers, and provide redundant backhaul in exchange for access to spectrum and prioritization of commercial network data. Few of these efforts have resulted in infrastructure-sharing agreements between utilities and public safety agencies, or utilities and common carriers, and in those cases it was often as a response to a government-mandated sharing of public carrier and utility investment.

A few new market entrants have proposed building dedicated networks, but none offers a service at this time. In one case, Southern Company has built networks and offered service to others as part of SouthernLink. Because common carriers are not investing or providing the necessary service levels, utilities are increasing their own investments to meet their needs. It will likely require regulatory actions to realign these interests.

SECURITY AND RELIABILITY CONSIDERATIONS

Are private networks more secure and reliable than public alternatives? It depends on three factors: access and operations control, infrastructure hardening, and cybersecurity impacts.

Access and operations control: Communication outages most commonly occur when workers are making changes on a network. There is no evidence to suggest that private network ownership reduces this risk. Private networks, however, allow utilities to control the timing of maintenance and network improvements, making it possible to schedule work at times that minimize the operational impact of a potential outage.

Avoiding high load days and adverse weather are primary concerns. Utilities generally prefer to make changes during standard working hours, when they have their full workforce in place, rather than at night, when they must call people in. Common carriers, on the other hand, prefer to make changes at night, when the majority of customers are not using the network.

Infrastructure hardening: To help maintain reliability, network electronics on utility-owned private networks meet mission-critical standards for design and construction. That means they include more backup time, greater isolation and more redundant system components. Links between electronics nodes are built of fiber and microwave systems. The fiber is installed on transmission lines whose rights-of-way are clear of trees and often set back from roads, reducing outages from fallen trees, vehicle strikes and ice damage. Radio towers similarly are built to withstand severe weather events. The result is a network that is more reliable than one built to the commercial standards normally followed by public carrier networks.

Cybersecurity impacts: Private networks are often thought to be more secure than public ones, benefiting from fewer access points and more restricted network access. As more devices are added, however, the benefits of these attributes diminish. Rather than presume the network is secure, utility owners should focus on methods for authenticating access to the network, authorizing activity and protecting the integrity of transmitted information.

BUSINESS MODEL CONSIDERATIONS

A utility's operating license allows it to spend capital on items that are used for and useful in power delivery. The utility can then recover these funds from ratepayers at a fixed rate of return. This model gives utilities a significant incentive to invest in network infrastructure. In contrast, costs associated with leasing facilities and services from a public carrier are considered a business expense, which is recovered at cost.

In some cases, a utility can get recovery from leasing, which could incentivize it to lease rather than build capital assets. It is important for a utility to clarify leasing requirements when making these decisions. For example, consider the accounting rules regarding 10- and 20-year irrefutable right-of-use agreements for fiber and licensing agreements for wireless spectrum.

This same concept could also apply to a wireless service. A service provider could build a private network, and access could be included with the cost of purchasing the field device. This approach would align with utility accounting practices for capitalization.

CONCLUSION

The need for real-time information when operating the power grid makes reliable communications a necessity. When the service required is not offered by a common carrier, or if the carrier is not willing to offer service guarantees for the particular application, investing in private infrastructure is the right choice for utilities. Doing so provides maximum control, enabling staff to have the data needed during an event, as well as the ability to communicate with each other while restoring service. All of this supports the safety of the restoration work. Making investments can be the most cost-effective means to achieve the communication necessary while aligning the capital nature of these investments with the business model of a utility.

BIOGRAPHIES

DAN BAYOUTH, PE, is the networks director and an electrical engineer in the Networks, Integration, & Automation Group at Burns & McDonnell, specializing in telecommunications and network engineering. His experience includes multiprotocol label switching (MPLS) WAN; substation IEC 61850; and DWDM network design, construction and integration. He has served as project manager and lead architect for the design and construction of multiple utilitywide network installations that encompass NERC CIP physical and cybersecurity, protective relay transport, DC power evaluation and design, volt/VAR control, recloser automation, and automated metering infrastructure. He is a WAN design specialist with experience in network topology, quality of service (QoS) design, and network testing and acceptance.

MATT OLSON, PE, is vice president and managing director of the Networks, Integration & Automation Group at Burns & McDonnell. He helps utility clients develop networks that support their entire organization. This includes helping them understand how to manage information; designing systems in 3D models; and designing multimillion-dollar, utilitywide fiber networks. Olson is an electrical engineer specializing in telecommunications systems and carrier network design, converged network architecture, and network management systems. In his 20 years of experience, he has supervised the design of more than 1,000 substations of packet network deployment, planned network construction with hundreds of nodes being installed per year, and delivered the applications cutover onto them in as little as a few months. He has also developed industry-leading documentation systems that allow for fast, cost-effective and holistic document management.

ABOUT BURNS & McDONNELL

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction professionals, architects, planners, technologists and scientists to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities with more than 60 offices globally. Founded in 1898, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.

08510-PNU-1021