renewGRID Reprinted with permission from the April 2011 issue

Outlining The Communications Behind Distribution Automation

As DA applications evolve and become more prevalent, utilities will need a solid working knowledge of these systems' networking requirements.

By Narasimha Chari

From a utility's perspective, the primary business goal of distribution automation (DA) is to achieve the ability to improve operating efficiencies, service reliability and service quality while simultaneously achieving energy efficiency and conservation goals. Although these goals and objectives are not new, developments in the broader environment are sharpening these motivations and driving utilities to invest further in DA.

The advent of electric vehicles and distributed generation creates a requirement for the ability to actively manage loads, as well as to accommodate variable and intermittent generation sources, within a distribution system that has traditionally only accommodated one-way flows of electricity. These stresses and challenges on the distribution infrastructure also bring into focus a utility infrastructure that is aging and, in many cases, in need of upgrades.

Distribution automation can be considered both a set of applications and a suite of technologies that enable a utility to monitor, control, coordinate and optimize the operation of the distribution system. It comprises devices with embedded intelligence and communications capabilities communicating over a network with application software at substations and in the utility's data centers.

Although there are islands of automation supporting disparate applications today, utilities do not have comprehensive visibility of, and control over, their distribution systems. However, more intelligent devices, along with newer generations of communications technology, are creating new options for utilities and helping speed progress toward the realization of the broader vision.

Narasimha Chari

As a set of applications, DA includes many individual applications with their own specific communications needs. For instance, volt/VAR optimization is enabled by the ability to monitor, control and optimize voltage levels along distribution feeders and to the consumer, resulting in energy-demand reductions and the optimized operation of the distribution infrastructure. Fault detection, isolation and recovery systems allow the grid to be reconfigured - in some cases, in real time - in order to mitigate or prevent outages. Monitoring capabilities that are extended to devices such as transformers allows for more proactive - as well as reactive - strategies to optimize distribution-system assets.

There is a range of devices to which automation and communication are being extended, including switches, reclosers and sectionalizers. In addition, there are many devices, such as transformers, that have never incorporated communications and are only now becoming economical to network on a wide scale.

DA communication requirements

Distribution systems are evolving from being merely a means for distributing electricity to having a growing and important role in delivering information and communications among operators, participants, devices and applications. Accordingly, the communications network that serves to interconnect these building blocks and transport information is a fundamental and foundational building block of this evolution. Therefore, the choice of communications technology is critical to the success of these applications.

The communications capabilities that exist in utility distribution networks today are often limited in extent, tied to proprietary network architectures and lacking in the advanced capabilities needed to enable the DA applications of the future. However, there is a growing recognition by utilities of the value that could be unlocked by having a pervasive, common communications network that is based on open standards and Internet Protocol (IP), is reliable and secure, and has the performance characteristics and functionality to serve as the foundation for multiple utility applications.

The most relevant communications system requirements, specifically for DA, relate to performance (latency and system capacity), reliability, quality of service (QoS) and security. Standards-based interoperability of devices from multiple vendors, network management capabilities, degree of utility control over the network, and system cost are additional considerations that factor in to the choice of a communications technology.

Network performance characteristics. The required level of network performance varies from application to application (see Table 1), but generally speaking, latency (or round-trip response time) and bandwidth (or communications link speed) are the most important metrics of network performance for DA applications.

Some DA applications, such as transformer monitoring, are relatively delay-tolerant and can accommodate latencies of several minutes. Outage detection using faulted circuit indicators require latencies measured in seconds. Other applications that require the control of switches, reclosers and sectionalizers (such as feeder reconfiguration), demand lower latencies, in the tens to hundreds of milliseconds. Extremely fast switching and protection applications can require sub-cycle latencies (less than 17 milliseconds).

Communications link speed is not as important as latency, because most DA devices do not generate large quantities of data to be transported over a network. However, taken in aggregate, a network comprising tens of thousands or hundreds of thousands of devices can require multiple megabytes per second of capacity over an area covered by a single substation. In addition, there are newer applications requiring even higher bandwidths that have not been implemented in the past because of network limitations.

Furthermore, utilities are beginning to understand the value of building out a common communications infrastructure that can support multiple applications, including DA, advanced metering infrastructure (AMI), backhaul, substation security and mobile-workforce management. Accommodating all of these applications - many of which are extremely bandwidth-intensive - requires a network that can scale to meet the higher aggregate-capacity requirements.

Table 1: Network Performance Requirements for DA Applications

	Monitoring and Sensing	Conditioning and Control	Switching and Protection
Applications	• Asset monitoring • Power-quality monitoring • Predictive maintenance	• Volt/VAR optimization	• Fault detection, isolation and recovery • Feeder reconfiguration • Outage management
Grid Devices	• Transformers • Cap-bank neutral current monitors • Voltage and current sensors	• Voltage regulators • Capacitor-bank controllers • FCIs	• Switches • Reclosers • Sectionalizers • Breakers
Bandwidth	• Low	• Low	• Medium
Latency	• High (minutes)	• Medium (seconds)	• Low (tens of milliseconds)

Reliability. Because many DA applications are mission-critical, they require a network that has very high levels of availability and survivability. Availability measures expected network uptime under normal operating conditions, and is usually measured by a "number of nines" (e.g., "four nines" equates to 99.99% availability, or under an hour of downtime per year). Survivability is a measure of the network's ability to withstand exceptional events (e.g., storms or hurricanes) and continue operating.

Survivability is a function of underlying radio technology characteristics, as well as a function of the network and system architecture. For example, mesh architectures have high levels of availability and survivability and are capable of adapting routes, topology and transmission-link parameters in real time in response to changing network conditions. The communications network needs to be highly reliable, with backup power options, in order to continue operating even during power outages and to aid in service restoration.

QoS. DA comprises multiple applications with different delay tolerances and bandwidth needs. Switching and protection applications require lower delays, typically measured in milliseconds, whereas some monitoring applications can tolerate delays of several seconds. Some applications are "bursty" and can generate a lot more data traffic than others.

In addition, there may be other non-DA applications sharing the network, such as AMI. Transporting data traffic from multiple applications over a shared network infrastructure requires built-in, application-level QoS mechanisms so that applications can be recognized and identified. In turn, applications can be assigned the appropriate priority levels within the transport layer, and delay-sensitive applications will be able to achieve predictable and low levels of latency.

Security. The security requirements for the monitoring and control of devices on the distribution grid are evolving, but they are generally more stringent, given the mission-critical nature of the applications and the de-

Table 2: Comparison of Wireless Technologies for DA

	Private Narrowband Radio Systems	Public-Carrier Cellular Networks	Private Mesh Systems
Latency	100s-1000s of ms	100s-1000s of ms	10-100 ms
Capacity	0.01-0.1 Mbps	0.1-10 Mbps	1-100 Mbps
Security	Medium	Medium-High	High
Reliability	Medium	Medium	High
QoS	Limited	Limited	Yes
Standards-Based Interoperability	Proprietary	Yes (GPRS, GSM, EDGE, 1xRTT, EV-DO, HSPA, LTE)	Yes (802.11/802.16 and IP)
Manageability	Limited	Very limited	Enterprise-class
Control	Utility owns and operates	Carrier owns and operates	Utility owns and operates

vices that are being controlled. There is also a growing awareness of cyber threats to critical-infrastructure control systems.

Although security has technical, organizational and operational aspects, the network itself needs to provide a number of security controls, including authentication and authorization of devices and users, network access control, protection of critical data during transmission, traffic segmentation across applications, configuration change logs and audit trails. There are a number of applicable security standards (including North American Electric Reliability Corp. Critical Infrastructure Protection standards, Federal Information Processing Standard 140-2 and the distribution management profile created by the Advanced Security Acceleration Project - Smart Grid) that will apply to DA devices and applications, as well as to the communications links among them.

Proprietary and non-interoperable communications technologies and equipment have hindered the adoption and integration of multi-vendor systems. However, a set of communications standards that meet utility requirements for DA and other applications is now available. Using IEEE open standards such as 802.11, 802.16 and 802.3 Ethernet at the link layer can simplify device and application integration while offering orders-of-magnitude higher levels of performance than older, narrowband technologies.

DA communications have historically been based on industrial protocols such as DNP3 and on utility-developed supervisory control and data acquisition applications. At the network and higher layers, there is growing adoption of communications end points that support Ethernet interfaces and the IP protocol suite, as well as standardized protocols such as IEC 61850. However, legacy, non-IP devices will continue to play a role and must be accommodated within the communications network paradigm through the use of protocol adapters, if needed.

Large-scale utility deployments will include hundreds of thousands of DA and communications end points that will be networked. As these end points migrate to IP, utilities will encounter a number of opportunities. For instance, the end points will become individually addressable and "pingable" over the network, thereby enabling the extension of network-management functions to the devices. These functions include device-status monitoring; remote batch administration of configuration settings and security policies; over-the-air software upgrades and security fixes; and network-performance monitoring.

Wireless technologies

There are a number of communications technologies that utilities have used over the years to communicate with assets on the distribution system, and there are now several newer technologies available that offer more powerful capabilities. Some of the more common communications technologies in use by utilities include power-line carriers, leased lines, fiber-optics, licensed and unlicensed microwave radio systems, point-to-point and point-to-multipoint (PTMP) wireless links, cellular radios and private radio-frequency mesh networks.

Although hard-wired communications links - such as leased lines or fiber-optic links - are desirable, they are sometimes not economical, especially when there is a large and growing number of devices that require connectivity. Wireless communication represents an attractive alternative for cost-effectively extending communications over long distances and to a wide array of devices.

There are a number of competing wireless technologies and architectures for delivering wide-area connectivity out to DA devices, and each has different performance characteristics, economics and applicability to DA applications. In comparing these technology choices, it is helpful (at the risk of oversimplification) to group them into three major categories: private narrowband radio systems, standards-based private mesh systems, and public-carrier cellular networks (see Table 2).

Examples of private narrowband radio systems include point-to-point and PTMP licensed or

unlicensed microwave radio links, neighborhood-area AMI mesh networks and tower-based licensed radio systems. In general, they use vendor-proprietary radio communications technology and do not offer native IP support, although some efforts toward technology standardization (such as IEEE 802.15.4g) are under way. These legacy radio systems generally offer speeds of up to hundreds of kilobytes per second and latencies of hundreds of milliseconds and higher) and a limited degree of QoS and security.

Standards-based private mesh systems have come to market within the last decade, and they are typically based on IEEE 802.11 or 802.16 standards and support the IP suite. The 802.11 networks are commonly based on a self-organizing mesh architecture, with routers deployed on utility poles, buildings or substations. Conversely, 802.16-based systems follow a PTMP architecture, with a base station at a communications tower communicating with multiple subscriber units. Also, 802.11 systems usually operate in an unlicensed spectrum (2.4 GHz and 5 GHz), while 802.16 systems typically operate in unlicensed (e.g., 5.4 GHz), lightly licensed (e.g., 3.65 GHz) or licensed spectrum bands.

Both kinds of private mesh systems offer higher levels of performance (multi-megabytes-per-second link speeds and latencies as low as a few milliseconds). They both also offer native IP support and standards-based QoS and security mechanisms. Many of these systems can provide enterprise-class network-management capabilities and serve as complementary architectures for multiple utility systems.

Cellular networks are owned and operated by wireless carriers, and they offer a different economic model for end-point connectivity that is based on recurring costs for a service offering. Multiple generations of cellular technology have been deployed by the carriers and are encountered in the field, from first-generation analog cellular to 3G networks. The next generation of 4G networks are beginning to be rolled out by major carriers and will offer higher levels of performance.

These networks have throughputs of up to a few megabytes per second and latencies in the range of hundreds of milliseconds. They conform to cellular-industry standards, and multiple vendors provide communications end points. In general, the public carrier model provides a lower degree of visibility, control, security and manageability for DA than a private, utility-owned network can provide. There are also concerns about the levels of availability, survivability and QoS achievable over cellular networks that have been designed primarily to support mobile operator business models.

> The most relevant communications system requirements relate to performance reliability, quality of service and security.

Evolution of DA comm

Although utilities have been extending automation out into the distribution system for decades now, this push has been accelerating and intensifying in the last few years, driven partly by advances in computing and telecommunications.

As Moore's Law continues to drive down the cost of computing, processing has extended steadily further and deeper into the grid, enabling distributed intelligence at the level of devices such as switches and reclosers. Newer generations of DA devices increasingly support standard interfaces and protocols, making it easier to integrate them with communications. At the same time, advances in communications are lowering the delivery cost per bit and making it economical to extend connectivity out to more end points, as well as to new categories of networked devices (such as transformers and capacitor banks) that have traditionally not been connected to a communications network.

The availability of real-time two-way communications technologies, in conjunction with increased computational capabilities, supports new DA functions - including real-time monitoring, coordination and control, and various distributed protection schemes - in addition to local automation. This combination of trends is helping utilities extend automation from the substations out to multiple kinds of devices out on feeders while enabling more sophisticated applications and functionality within the network.

Over time, as communications technologies advance and the costs of processing and communications continue to decline, it is possible to envision a future where each device on the power-distribution system is equipped with distributed software intelligence, as well as advanced communications capabilities, and is part of a unified network for power and information exchange. Although this vision is still far from reality, it represents a logical goal for DA: enabling a grid that is smarter, more reliable and more efficient than it is today.

Narasimha Chari is co-founder and chief technology officer of Tropos Networks, where he focuses on system and product architecture, product planning and advanced corporate development. Chari led the design and development of the company's core intellectual property, including wireless networking and routing protocols. He can be reached at chari@tropos.com or (408) 331-6800.