Telecommunications Considerations for Distribution Automation Applications

2012

Executive Summary

Over the last decade, increased worldwide investment in the "Smart Grid" has aimed to enhance the capabilities of the transmission and distribution networks that deliver electric power to energy consumers. By adding monitoring, analysis, control, and communications capabilities to a utility's electrical delivery system, Smart Grid investment broadly seeks to increase the power grid's efficiency and cost-effectiveness by increasing power throughput and reducing or shaping the profile of energy consumption.

In particular, distribution automation (DA) applications represent a subset of Smart Grid applications that hold the potential to quickly realize positive returns on investment (ROI). A prerequisite of such high-value DA applications, however, is the existence of a suitable communications network. This White Paper outlines the general communications requirements for DA applications, discusses the fundamental communications alternatives that are available, and specifically highlights considerations associated with wireless networks for DA applications.

Introduction

As an element of the Smart Grid, DA brings enhancements to the distribution network itself. While the transmission network defines a high-voltage network of transmission lines that connect power-generating plants to substations located near population centers, the distribution network supports the delivery of electricity from the transmission network to its end users. Typically, the distribution network encompasses electrical substations, medium-voltage primary circuits, distributed power transformers, low-voltage secondary lines, and electric meters at the end user's site.

Distribution equipment in the field historically have functioned autonomously, responding to local signals and conditions without operations center involvement: capacitor banks are switched on or off based on voltage or time; fuses blow in the presence of excessive current; reclosers independently determine whether a local fault is momentary or sustained; and so on. DA then represents the application of new technologies in the distribution network in order to realize improvements and enhancements of:

- ***network reliability***, especially in terms of detecting and recovering from equipment failure through real-time and near-real-time monitoring, intelligent control, and dynamic network reconfiguration
- ***network efficiency***, including management of peak loads (load control, demand response), reduction of system losses, and optimization of power generation
- ***asset management***, including characterizing, monitoring, and predicting equipment performance and operational lifetimes, especially for infrastructure such as underground cables where a failure can result in a sustained outage
- ***customer service***, especially as customers benefit from enhancements to network reliability and efficiency and improvements in power quality
- ***network operations***, typically through automated remote monitoring and control systems that can simplify day-to-day network management and reduce truck rolls and demands on field personnel

High-Value DA Applications

DA applications can encompass the remote monitoring and control of components in the substation (substation automation), of components on feeders (feeder automation), and of components at customer sites (meter automation). In particular, a few specific applications have recently emerged as the highest-value DA applications where today's technology can significantly improve current processes and can deliver immediate returns on investment (ROI):

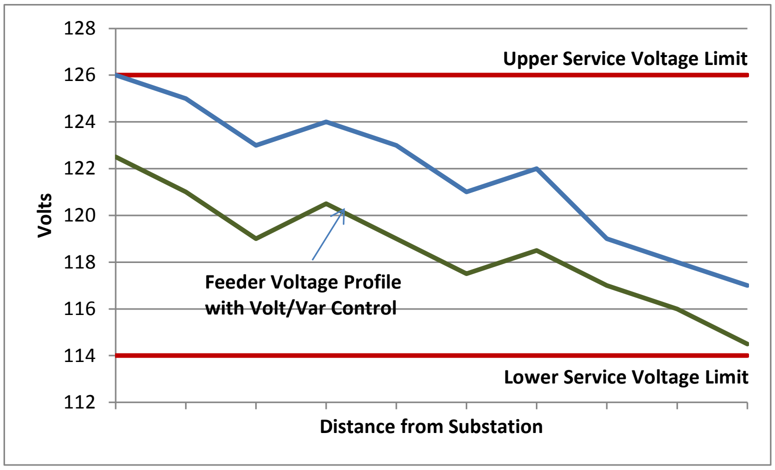
- outage management
- Volt/VAR monitoring & control
- asset management

Outage Management. Traditionally, outage management systems have comprised the response systems put in place to react to telephone calls from customers reporting outages. When enhanced by DA, outage management can incorporate automated fault location, isolation, and service recovery mechanisms to identify, diagnose, locate, and resolve electrical outages. Monitored circuit breakers, faulted circuit indicators, smart meters with outage detection, and solid state breakers and switches for fast fault clearing, system reconfiguration, and transient-free switching can all be part of advanced outage management systems.

The benefits of enhanced outage management performance as enabled by DA applications can readily lead to a positive ROI and justify the investment, including:

- improved customer satisfaction by providing up-to-date and accurate outage and restoration information
- prioritized restoration of emergency facilities and other critical customers.
- reduced outage durations due to faster restoration
- reduced outage frequency through use of outage statistics to make targeted reliability improvements

Voltage/VAR Monitoring & Control. Real-time voltage/VAR management has traditionally been used by a utility to maintain voltage within regulatory limits for consumers, to reduce power losses by improving power factors, and to reduce power generation requirements or the amount of wholesale power that must be purchased.



Automatic voltage regulators, load tap changers (LTCs), and automatically or manually switched shunt capacitors have all been historically used. But the degree of control has been restricted due to:

- limited voltage monitoring and control points (usually only at the point of voltage regulators or capacitors);
- relatively imprecise control systems with coarse control increments for the voltage regulators and capacitors; and
- conservative upper and lower limits on the amount of voltage control are needed in order to prevent voltage excursions elsewhere in the distribution network.

As DA devices become more extensively distributed, improved voltage/VAR capabilities become possible so that voltage/VAR monitoring and control can be used to reduce power demand by consumers and, through conversation voltage control, reduce the total energy supplied to consumers. Realization of these enhanced voltage/VAR monitoring and control objectives can alone justify the required additional investment in DA field equipment and smart meters, improved system monitoring and control software, and advanced voltage regulators and shunt capacitors.

Asset Management. Asset management involves optimizing use of a utility's plant and equipment across the dimensions of cost, performance, and risk/reliability. In this context, DA applications include the introduction of new sensor technologies to collect performance and operational data for cables, transformers, breakers, reclosers, sectionalizers, capacitors, regulators, arresters, and other utility equipment. DA-enhanced asset management then allows a utility to make intelligent choices regarding such issues as budgeting for capital spending versus operations & maintenance (O&M) spending and proactive equipment replacement versus "run-to-failure" decisions.

Communications Requirements for DA

The technologies needed to implement DA applications include:

- advanced sensors and fault indicators
- monitoring technologies integrated with relays, regulators, capacitor, and recloser controllers
- data integration with SCADA (Supervisory Control And Data Acquisition), DMS and other operations systems
- improved power switching devices
- advanced metering capabilities (Smart Meters)
- advanced protection systems, including reclosers integrated with automatic reconfiguration systems
- next-generation transformers, capacitors, regulators, and arresters with integrated monitoring and communications capabilities
- integration of distribution network control with distributed generation sources (fuel cells, microturbines, plug-in hybrid electric vehicles) and new energy storage technologies
- advanced distribution network control systems that can make use of real-time and near-real-time network data to optimize energy efficiency and network reliability

Fundamental to virtually all DA applications, however, is the requirement for telecommunications throughout the distribution network to support connectivity between SCADA, DMS and other operations systems and devices in the field.

SCADA communications systems were created to address the needs of DA-related real-time monitoring and control by supporting telemetry from devices in the field and allowing their configuration from the head end. As SCADA systems have evolved to adopt standard networking technologies such as Ethernet and TCP/IP, the difference between purpose-built SCADA networks and standard networks supporting DA applications (and new or legacy SCADA communications) has blurred.

Similarly, today's Advanced Meter Infrastructure (AMI) deployments involve communications coverage requirements to bring data from smart meters deployed throughout a utility's service area back to a utility's head end. The needs of DA applications, however, typically impose higher and more stringent requirements on the communications network capabilities. Exceptions exist, of course – for example, there are approaches to voltage/VAR monitoring and control applications that can "piggyback" on top of an AMI deployment without imposing more stringent requirements.

A telecommunications network intended to support DA applications must meet requirements in the dimensions of capacity & latency, support of standards, security, coverage, and reliability, but the precise requirements depend on the specific DA application or applications and the utility's overall objectives: What devices will be fielded? What protocol support do they require? What traffic will they generate? With that context in mind, a utility can answer the following types of questions for any candidate network technology:

- **Capacity & latency**
  - — ***Traffic Demand:*** Will the network be able to support anticipated levels of traffic from the various types of DA devices that are to be deployed? Report-by-exception DA devices will only generate network traffic when certain pre-determined thresholds are exceeded, but DA devices used for control and status operations can require continual communications.
  - — ***Bandwidth:*** Given the desired DA applications to be supported and the expected number and types of DA devices, can the network provide adequate bandwidth (capacity) to support the estimated levels of peak and continuous traffic?
  - — ***Latency required by specific DA applications:*** Will the network meet latency requirements for the various DA applications that are expected to be supported? Latency on the order of 10s of milliseconds (or even lower) can be required to meet certain DA applications involving real-time control and status, while other applications may be "latency-tolerant" and not impose stringent latency requirements.
  - — ***Traffic management:*** Can capacity and/or latency be controlled by traffic prioritization and Quality of Service (QoS) mechanisms? Can different DA applications with different capacity and latency requirements be readily supported by the same network?
  - — ***Headroom:*** Can the network support increases in the level of peak or continuous traffic?
  - — ***Future needs:*** Will the network have the capacity and latency needed to support the capacity and latency requirements of future applications?
- **Support of standards**
  - — ***Traffic types***: What types of traffic and protocols can the network support? In particular, does the network provide flexible support for a wide range of DA devices employing such protocols as SCADA-over-IP, DNP3, or IEC 61850 with GOOSE messaging?
  - — ***Networking standards:*** Is the network a layer-3 (IP-based, with routing to support communications across disparate network types) or layer-2 (Ethernet-based, supporting node-to-node packet forwarding) network? Neither type of network is intrinsically "right" or "wrong", but each type introduces different challenges with respect to such issues as node mobility, transport of different DA-related protocols, network management, and integration with existing head-end and network communications capabilities.
- **Security**
  - — ***Network security:*** What security mechanisms are intrinsically provided by the network and its nodes? In general, security mechanisms must address the CIA and AAA triads:
    - ❖ Confidentiality, ensuring that information cannot be read or altered by an unauthorized party
    - ❖ Integrity, ensuring the accuracy and completeness of the information, including the detection of any alteration
    - ❖ Availability, ensuring that communications resources are accessible and usable by an authorized individual, entity, or process
    - ❖ Authentication, controlling which individuals, entities, or processes (*who*) can access the network
    - ❖ Authorization, controlling *what* can be done given access to the network
    - ❖ Accounting, identifying what individuals, entities, or process *did* with access to the network
  - — ***End-to-end security:*** What security mechanisms can be supported over the network? Can network traffic be partitioned, using 802.1Q VLANs, VPNs, or other techniques? Are there limitations?
  - — ***Standards:*** To what degree does the network support the NIST Smart Grid security guidelines (NISTIR 7628) or other national and regional Smart Grid cybersecurity requirements?

- **Coverage**
  - ***Current coverage needs:*** Can the network be deployed to meet the coverage requirements of the currently anticipated DA applications? Can it reach remote substations? Can it reach DA devices deployed in the field as required by the specific DA application? For example, introduction of voltage/VAR monitoring and control as a DA application may require a high number of network nodes to be deployed, with 10 or more monitoring points per distribution feeder line from a substation typically desired

  - ***Future growth:*** Is the network topology flexible enough to support increases of DA device density? Is it flexible enough to support expansions of the overall area of coverage?

- **Reliability**
  - ***Network reliability:*** Does the network provide fault-tolerant communications? Are redundant communications pathways provided? Are single points of failure avoided? Is the network self-healing?

  - ***Product reliability:*** What is the expected operational lifetime of the network equipment? Is the network equipment designed for outdoor deployment? How is it powered? Is backup power available (or necessary, given the application)? How readily can it be deployed in the field environments associated with the specific DA applications to be supported? Etc.

Fundamental Communications Alternatives for DA

While the overall communications network requirements described above can be met by a wide range of technology alternatives, a utility's ultimate procurement decision involves trade-offs and considerations in terms of the network's lifetime costs, especially in terms of capital costs, deployment costs, and operations & maintenance costs; its deployment schedule; and the associated program risk with respect to schedule, cost, and performance.

Two fundamental communications alternatives and choices intrinsically bring these programmatic considerations into focus:

- *whether the DA network should be a <u>wireline</u> or <u>wireless</u> network*, and
- *whether it should employ <u>public</u> or <u>private</u> network facilities*

A wireline network such as a fiber-optic network offers high bandwidth and low latency, making it a common choice to support substation automation applications. But if service is not already available, deployment costs can be high, especially for remote substations, and a wireline network may not readily offer the topology and flexibility needed to support a large number of DA devices deployed in the field. A wireless network, by contrast, can offer bandwidth and latency according to the specific technology and frequency spectrum that is employed and is generally more flexible and cost-efficient to deploy to devices scattered across a wide coverage area. The need to provide coverage for a large number of widely distributed DA devices may alone point to use of a wireless network.

Independently, consideration of whether the network should involve public carrier facilities or be strictly a private network involves issues of costs and control. In general, use of public network facilities implies ongoing operational costs for the utility while the capital expense of the network is borne by the carrier; by contrast, use of private network facilities implies that both capital and operating expenses must be borne by the utility. Perhaps more importantly, however, a private network will be fully under the control of the utility: service availability/coverage and how the network is utilized are expressly determined by the utility.

In practice, a mix of wireline & wireless and public & private networks may be necessary. For example, some DA communications network design options can require public facilities to support backhaul between the utility head-end and the utility's private communications network in the field, or a transitional approach may be desired, initially using public wireless facilities before a private wireless or wireline network is deployed.

Wireless Communications Alternatives for DA

If use of a wireless private network can address a utility's DA objectives and represents an attractive option, then the decision process shifts to other considerations that, eventually, relate back to the ultimate decision criteria of cost, schedule, and risk.

Licensed versus unlicensed spectrum. Comparable wireless technology alternatives that can address the requirements of a utility's DA application may offer the choice of either using frequency spectrum requiring explicit license from the national regulatory body or using spectrum that does not require such licenses (with the use of type-certified equipment). Especially in the United States, licensed spectrum can be very expensive, with only the most well-funded carriers able to participate in spectrum auctions. Other frequency bands, however, may be licensed for special uses, with only a nominal fee required – for example, the 4.9 GHz public safety band is available in Canada, Mexico, and the United States for use by local government entities.

By contrast, spectrum without licensing requirements has been made available to foster the development of new radio technologies. In the United States, the FCC's designation of the ITU-R Industrial, Scientific, and Medical (ISM) bands at 900-928 MHz, 2400-2483.5 MHz, and 5.725-5.850 GHz for use by unlicensed direct sequence or frequency-hopping spread spectrum devices helped accelerate the development of the IEEE 802.11a/b/g/n family of standards and the Wi-Fi Alliance trade association as well as other standards and products. The 2400-2483.5 MHz band has emerged as a band that is almost globally allowed for unlicensed use, albeit subject to specific national transmit power, spectral power density, and technology restrictions.

Thanks to the response of global manufacturers to the availability of unlicensed spectrum, a wide array of vendors and technologies are available to support products operating in the unlicensed bands. From the point of view of a utility and its need to choose wireless communications network equipment supporting its DA applications, this situation implies a variety of product and technology options, the possibility of multiple sources for any given technology, and the cost benefits arising from economies of scale.

Because the spectrum is unlicensed, however, it must be shared with other devices operating in the same band that are not under the control of the utility. As a result, there is a possibility that radio interference from non-utility sources can adversely affect the utility's network. Even so, specific wireless technologies and product implementations can provide mechanisms to avoid interference and mitigate their effects, thus reducing potential impact.

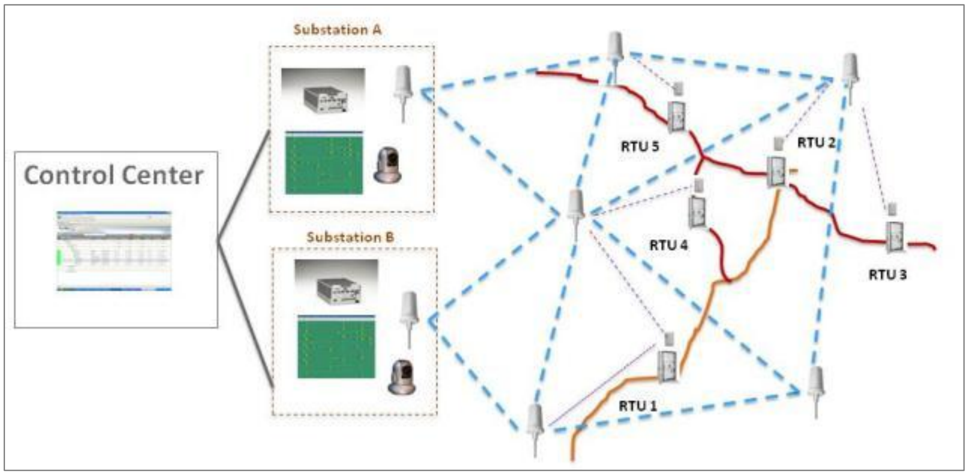
Range. Connectivity and coverage of a wireless network are directly supported by the node-to-node range between two communicating devices. Radio range is determined by various factors, including:

- aspects of the devices themselves – including the *transmit power* as provided by the devices and as allowed by regulation; the *transmit and receive antenna gains* as provided by the devices and as allowed by regulation; and the *receive sensitivities* of the devices, as determined by the specific modulation type, data rate, use of forward error correction coding, and receiver implementations.
- the frequency band employed – range is proportional to the inverse of the frequency, implying that, if all other factors are held equal, operation at higher frequency bands will experience shorter ranges than at lower frequency bands
- local propagation characteristics – in practice, radio range between any two communicating points will be limited by the existence of obstructions along the line-of-sight path between them, the characteristics of such obstructions (in terms of their size and materials), and the presence of diffraction and multipath effects because of the local environment at the transmitter, at the receiver, and in between

If, for whatever reason, the node-to-node ranges achievable with a particular wireless networking technology choice are constrained, then higher costs may be incurred because of the need to deploy more equipment than would otherwise be necessary. Any such consideration of range, however, must be in the context of the coverage required to address the desired DA application(s) – there is no benefit if a specific communications technology choice provides significantly more point-to-point range than is actually needed to meet the coverage requirements.

Wireless Network Topology. Wireless technologies can support three distinct topologies, with each potentially having a place in supporting communications for DA applications:

- *point-to-point systems*, where links are established between pairs of devices. Some point-to-point systems can offer very high-bandwidth and low-latency connectivity, effectively replacing fiber-optic links. By nature, however, point-to-point systems provide limited coverage and are perhaps best suited for use as a backbone connecting the utility head-end with remote substations or field devices that concentrate other traffic.
- *point-to-multipoint systems*, where a hub-and-spoke architecture supports multiple communicating nodes from a single base station. The ability to support multiple nodes from a single base station can reduce hardware and deployment costs while providing the desired network coverage.
- *mesh* or *multi-hop point-to-multipoint systems*, where traffic can be passed from node-to-node. Such systems allow obstacles to be bypassed, permit coverage to be extended beyond the range provided by a single node-to-node pair, and allow connectivity to be deployed as needed. Compared to point-to-multipoint systems, mesh systems can also enhance network reliability, offering multiple alternative paths in the event a node fails or a link deteriorates.



Mesh Networking Architecture provides built-in reliability and ease of deployment

Conclusion

The term "distribution automation" encompasses a wide range of possible applications, each with its own specific communications requirements. A specific utility's DA objectives and planned implementation will ultimately determine its overall communications needs. Ideally, the adoption of any DA technologies will be executed with conscious consideration of the supporting communications network. This White Paper has attempted to provide a broad framework for the general communications requirements imposed by DA applications in terms of capacity & latency, support of standards, security, coverage, and reliability. Fundamental decisions as to whether all or part of the supporting communications network will be wireless or wireline and public or private must be made. The advantages of using a private wireless network for DA applications then lead to further considerations of licensed versus unlicensed spectrum, node-to-node range, and network topology. In conclusion, in determining the most suitable solutions for their distribution automation needs, utilities will need to consider the provisions outlined and described in this paper. Trilliant's Smart Grid communications solutions provide the most cost-effective, highest capacity, and lowest latency solutions for advanced distribution automation that satisfy not only the needs of today, but also those of tomorrow.