White Paper

Using wireless communication networks to enable outage management

As viewers of Super Bowl XLVII are well aware, power outages are no fun. And as the organizers of the big game, as well as the responsible utility, the venue and their vendors discovered, they're bad for business.

But the cost and inconvenience of a 30 minute outage during a prime time football game is miniscule compared to that of a major hurricane or blizzard. Such events can disrupt electrical service for days or even weeks.

In addition to catastrophic failures, utilities and their customers are subjected to small scale outages on a much more frequent basis. Trees fall, cars knock down utility poles and animals short out feeders. Utilities are measured by their regulators on both the number and duration of outages. They may face penalties for poor performance on these metrics. While some outages can't be avoided, their length and scope – the number of affected customers – can be minimized.

For decades, utilities have relied on customer phone calls and dispatching crews to the field to identify outage areas. They often received delayed and imprecise outage information, slowing power restoration. Their reactive response and long outage durations are often viewed negatively by customers.

Utilities can improve customer satisfaction by deploying software, intelligent devices and network communications to implement a state-of-the-art outage management system. These technologies can minimize the scope and duration of outages and enable proactive engagement with affected customers.

A key element enabling proactive outage management is real-time, bidirectional communication with utility devices in the field. Communications permit outage management systems (OMS) and other utility software systems to collect up-to-the second information from the distribution system, adjust system operation and provide information to customer service systems and personnel for proactive customer engagement. Even better, the OMS could predict pending failures, enabling scheduled preventative maintenance and reducing unscheduled maintenance under outage conditions.

Enhancing outage management using smart grid infrastructure

Smart grid devices can enhance outage management. Utilities can leverage AMI, FCI and DA installations to improve their outage response.

Leveraging AMI to enhance outage management

AMI can assist outage detection and isolation. Smart meters with last gasp capabilities alert the OMS the moment an outage occurs. Because all affected meters issue a last gasp message when an outage occurs, utilities get timely outage notification and an accurate picture of outage location.

Restoration notifications from smart meters can help avoid "OK on arrival" dispatch of line crews. When timestamped, they also help utilities accurately calculate Customer Average Interruption Duration Index (CAIDI).

Automated FCI monitoring

Traditional faulted circuit indicator (FCI) monitoring entails having a lineman drive along a distribution feeder, visually inspecting each FCI to see if it has tripped. By integrating communication capability with FCIs, the OMS can perform this task from a central location. Automated FCI monitoring can hasten fault detection and location while eliminating the tedious task of driving power lines to look for tripped FCIs.

Dynamic feeder reconfiguration

Advances in communications have enabled smart distribution automation. Intelligent switches, reclosers, sectionalizers, capacitor banks and transformers can be actively monitored and remotely operated from substations and utilities' data centers.

With smart DA devices, utilities can quickly and automatically pinpoint distribution network faults, reducing the scope and duration of outages and protecting critical assets. Smart DA devices automatically isolate faults and reconfigure feeders to restore electricity with no operator intervention, reducing outage duration from hours to minutes, as shown in the following example.

During normal operation, the neighborhood is served by distribution feeders from three substations, as shown in Figure 1.

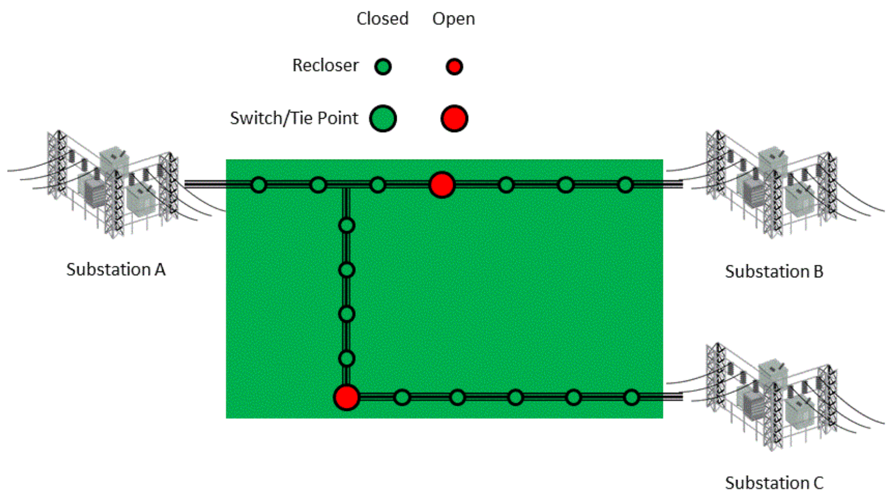

Figure 1

In Figure 2, a fault occurs, perhaps because a car hits a utility pole. The fault causes all customers normally served by Substation A to lose power. Without smart reclosers and switches, this condition would remain until trucks with line crews rolled into the area to restore power.

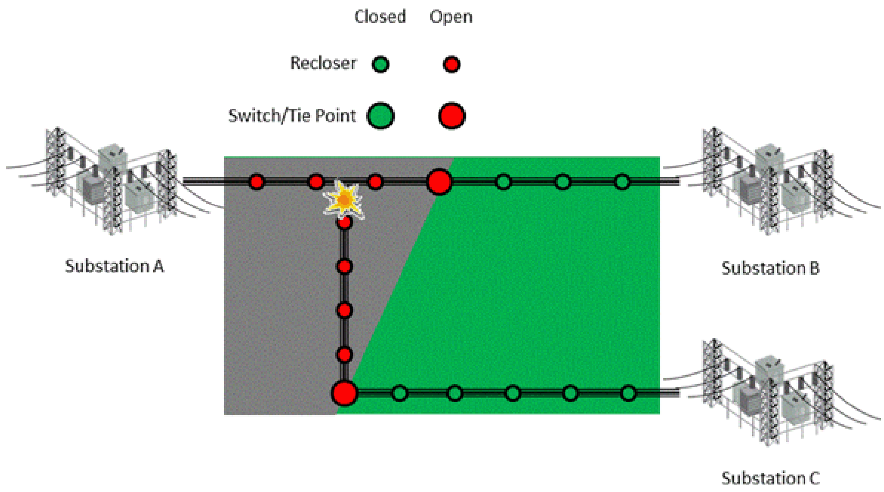

Figure 2

With smart reclosers and switches, service between the fault region and the various substations is restored by automatically closing the switches serving as tie points between the distribution circuits and the reclosers between the tie points and the fault, as shown in Figure 3. Now the outage is contained to the area between the accident site and the nearest recloser in the direction of each substation.

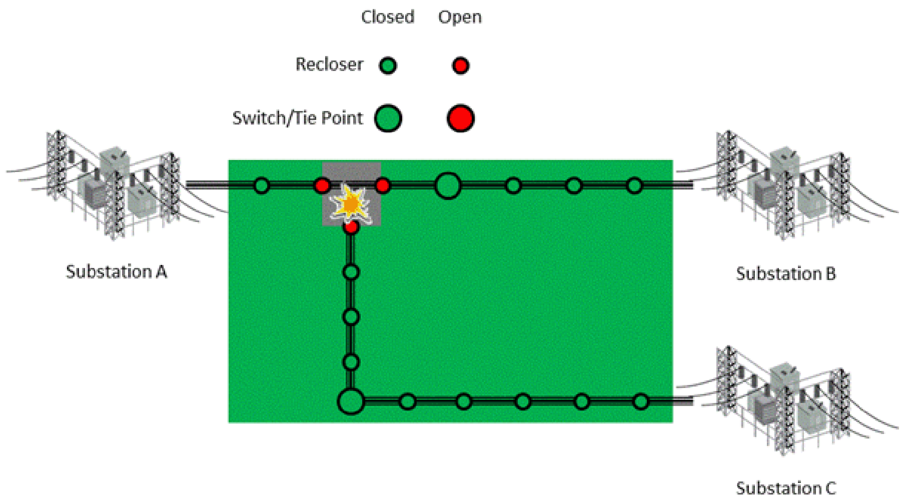

Figure 3

Without dynamic feeder reconfiguration, isolating the fault is a manual process. Manipulating switches requires truck rolls, which can take hours. With smart technology, the process is automated – requiring little or no manual intervention – and accomplished in minutes.

Functionality similar to what is described in the example is being deployed by utilities today, as evidenced by Avista's well-known smart grid projects in Spokane and Pullman, Washington.

Field worker communications

Outage management is further enhanced when the network used for machine-to-machine communications is also used for mobile workforce automation. Providing access for mobile workers enables them to access all information available in the data center without leaving the field.

As Jimmy Bagley, Deputy City Manager of Rock Hill, South Carolina explains, "The practical application of this system will be the ability of the utility workers, during an outage event, to access real-time outage data from their vehicle in the field. Direct access to data ensures the utility crew will know that customers have power before leaving the area."

Proactive customer engagement

With smart grid technology detecting, locating and minimizing faults, utilities can turn the traditional customer engagement model during outages on its head. Instead of waiting for customers inform them of outages, utilities can contact customers by phone, email, text, the web and social media to notify them about outages and their scope, cause and expected duration. Customer service reps can also be better prepared to respond to inbound calls.

Eliminating outages with predictive maintenance

The best outage is one that doesn't happen. Intelligent distribution equipment with high speed communications can help the Distribution Management System (DMS) identify likely failures, allowing the utility to replace components before they cause an outage.

Potential failures can be predicted using a variety of techniques. For example, a transformer's temperature and kVA load are good predictors of pending failure. Transformers with sensors and communication capability can provide temperature and loading data to the DMS which can, in turn, identify a potential failure point before an outage occurs. A more complex method requires intelligent electronic devices (IEDs) throughout the distribution system to collect large amounts of oscillography data and to send it to the data center to detect patterns that indicate pending failures.

Wireless communication networks: A key to enabling advanced outage management

Wireless Field Area Networks (FANs) provide the communications needed by outage management systems and other utility software systems to collect up-to-the second information from the distribution system, adjust system operation, proactively engage affected customers and predict pending failures. The FAN links smart meters and IEDs in the distribution system to the data center. IEDs usually connect directly to the FAN. Smart meters generally use a lower bandwidth Neighborhood Area Network (NAN) to communicate with an AMI collector that aggregates data from a large number of smart meters. The collectors, in turn, connect to the FAN. The FAN transports information between NANs and IEDs and the utility's core IP network. The core IP network connects to the data center, where the OMS and other smart grid software systems are located. Figure 4 shows the overall network architecture.

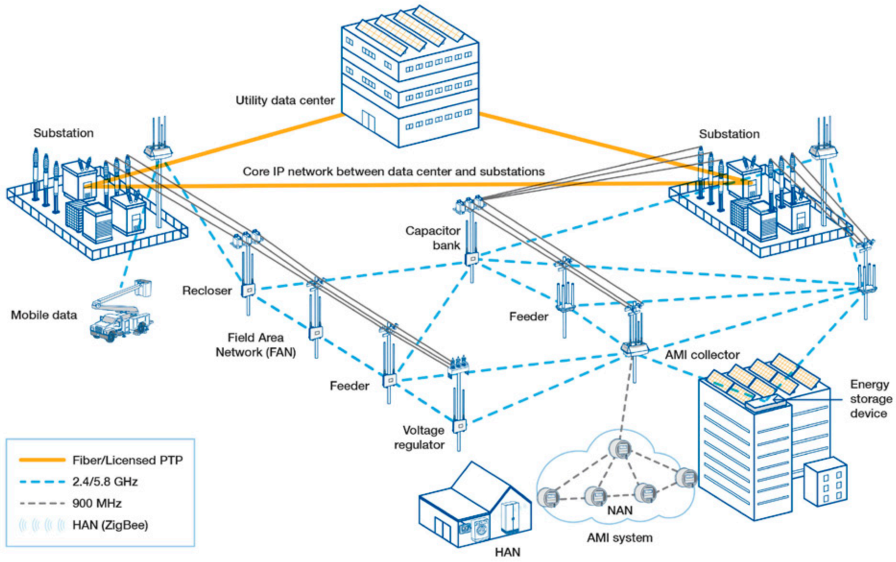

Figure 4

The OMS shares information with systems such as the GIS and IVR via the utility's enterprise network with workers and systems in the field communicated using the FAN, as shown in Figure 5.

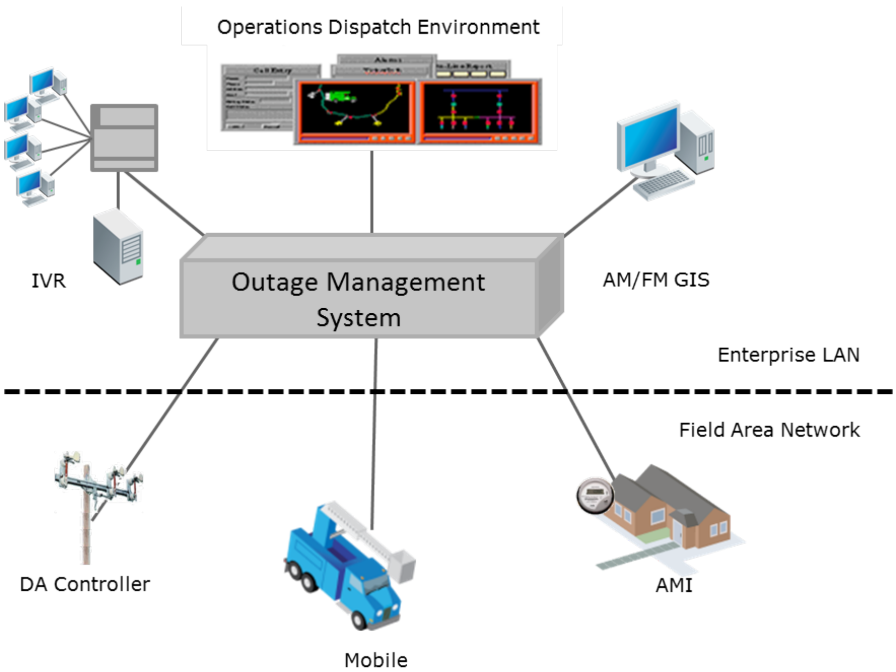

Figure 5

Field Area Network requirements

FANs must meet the superset requirements of all current and future applications.

High capacity

Traditionally, utility applications sent and received little data. Consequently, utilities generally installed low capacity networks.

As IEDs proliferate, become smarter and gather more information, capacity needs are changing. High capacity networks are required because more applications and devices use the FAN and they send and receive more data.

Low latency

Many applications in the distribution system are not latency sensitive. However, the few that are, including protection and safety applications, tend to be critical. Because a unified FAN must support the requirements of all deployed applications, low latency is essential.

Application prioritization

Low latency is essential but doesn't help if traffic for safety and protection applications is stuck in a queue behind less important traffic, e.g., AMI interval reads. Therefore, application prioritization is required to ensure that delay-sensitive traffic gets to its destination in time.

High availability

Communications are most critical during outages. FANs must operate even when events disable the electric grid. High capacity mesh networks that automatically use multiple paths, channels and frequency bands to route around failures and congestion are especially reliable. Individual communication devices must be ruggedized, weatherized and supply battery backup.

Scalable

Field area networks must scale to cover large geographic areas, potentially the utility's entire service territory. They must also scale to support, directly or via NANs, millions of connected devices.

Secure

As utilities adopt IP in field area networks, fear of cyber-attacks increases. However, IP-based architectures bring security advantages. The tools used to thwart cyber-attacks in enterprise networks have been honed for years and are constantly being updated. Enterprise security tools that should be leveraged in FANs include IPsec virtual private networks (VPNs), firewalls, RADIUS authentication and AES encryption.

Flexible

To support the widest variety of applications and devices, the FAN must be built on industry standards such as TCP/UDP/IP, 802.11 (Wi-Fi) and 802.3 (Ethernet). To best integrate IEDs, the FAN must also support secure network connections to devices that use serial RS-232 or RS-485 links and automation protocols such as DNP-3, Modbus, SEL Mirrored Bits and IEC 61850.

Summary

As outage management evolves, the vision of a self-healing distribution grid that predicts failures before they happen comes closer to reality. Intelligence and bidirectional communication are key enablers. Using wireless FANs, outage management systems located in utility data centers can collect up-to-the second information from the distribution system, adjust system operation, proactively engage affected customers and predict pending failures, enabling preventative maintenance.

1KHA - 001 290 - SEN - 1002- 01.2016

For more information please contact:

ABB Wireless
3055 Orchard Dr.
San Jose, CA 95134

Phone: 408-331-6800
E-Mail: tropos.sales@nam.abb.com
www.abb.com

Power and productivity
for a better world™