GEGridSolutions.com

Whitepaper

Wireless Solutions for Reliable Distribution System Protection & Control

Judy LeStrange, Edgard Sammour, Mike Ramlachan, Craig Wester

Introduction

Wireless communications for distribution system protection and control applications offer several operational and cost advantages over traditional hardwired and fiber solutions. Wireless communications applications include implementation of distribution system fault detection, isolation, and restoration (FDIR) schemes, protection, and control of distributed energy resources (DERs) and microgrid control. Fault detection, isolation, and restoration (FDIR) requires the detection of faults on an electric utility distribution system, identifying the type of fault and its location, and controlling feeder reconfiguration to improve distribution network reliability. Distributed energy resources (DERs) connected to an electric utility distribution system typically require the ability for the electric utility operating the grid to remotely control and monitor the DER source(s).

Similarly, the protection and control of microgrids requires coordination with the main grid network protection and operation when switching between non-islanded and islanded modes. Many distribution system communication schemes for protection and control are currently deployed in a point-to-point architecture, but other wireless communications options are available, such as point-to-multi point, which can simplify and centralize the protection logic and the wireless communications architecture. In addition, dual wireless communication links can provide enhanced reliability and flexibility to transform the communications network to support a future point-to-multi point topology.

This paper discusses the advantages of wireless communications solutions and the communication requirements and field performance expectations for distribution system protection and control, such as latency, speed, security, reliability, and scalability. This paper will illustrate wireless communication architectures for FDIR, DER and microgrid control schemes.

Distribution Automation Applications

The application requirements for distribution automation on an electric utility system are the following:

- Speed in the range of seconds is adequate for most applications. However, there are some time critical applications that will require responses in the millisecond range.
- Dependable and secure communications.
- Interoperability between connected distribution devices using non-proprietary protocols, such as IEC 61850.
- Adequate bandwidth for data transfer of distribution device data (device settings, waveforms, sequence of events).
- Multiple protocol support (Modbus RTU, DNP, IEC 61850).
- Communications redundancy using different media.
- Reliable power source for communications, such as battery back-up.

Peer-to-Peer FDIR

To minimize customer outages and operate a reliable power system, distribution utilities normally apply an independent/peer-to-peer fault detection isolation and restoration scheme (FDIR). This application consists of peer-to-peer messaging using IEC 61850 GOOSE. GOOSE messaging allows for interoperability (non-proprietary) between various distribution automation devices. Unlike transmission protection applications, the speed of operation can be within the seconds time range for this type of application. This FDIR architecture also provides support of traditional SCADA distributed network protocol (DNP) for control, monitoring and metering. The application is shown in Figure 1.

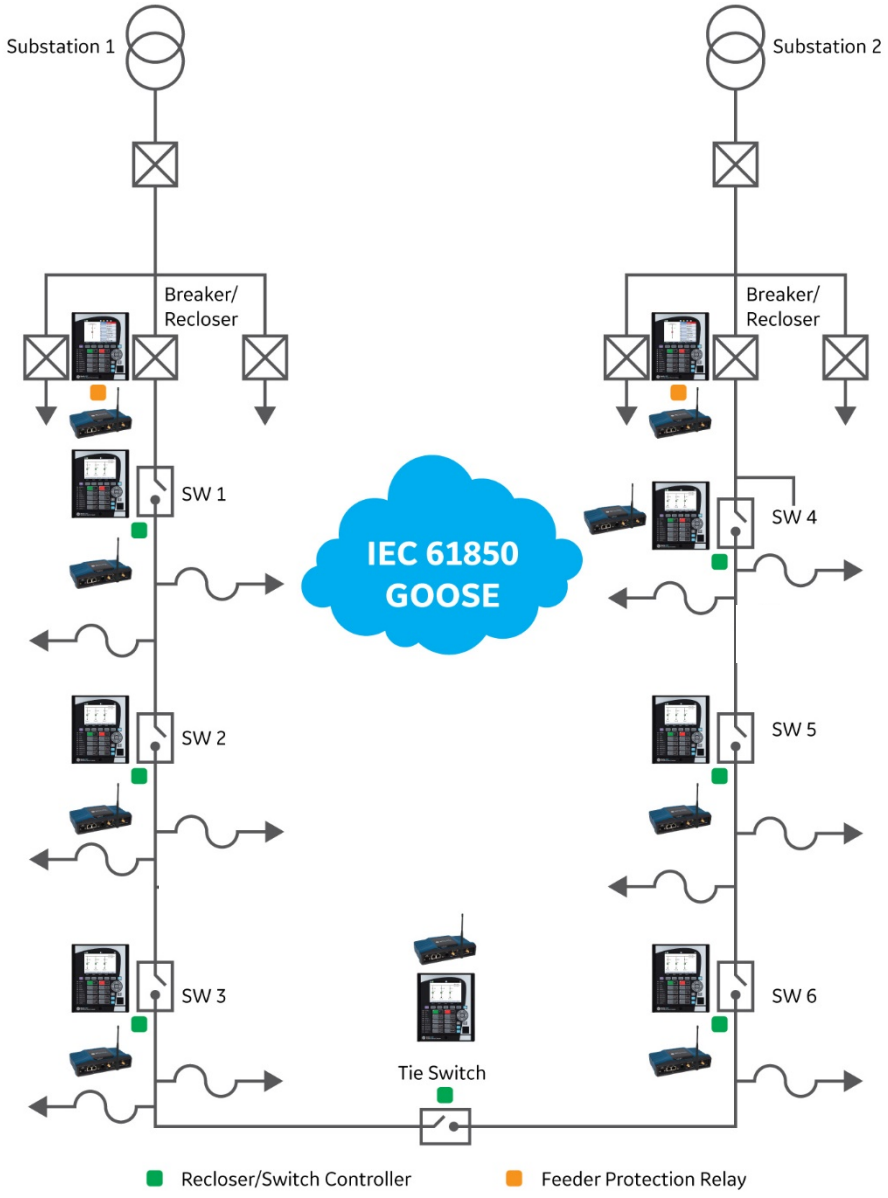

Figure 1 - Independent/Peer-to-Peer FDIR

Centralized / Decentralized FDIR

An alternate to the independent/peer-to-peer FDIR scheme is centralized / decentralized fault detection isolation and restoration (FDIR). This application involves communication to a near-by substation or to central location such as a control center. This application can still use IEC 61850 peer-to-peer messaging for interoperability back to the substation automation device/controller. The application could also use DNP control messages from the control center.

IEC 61850 GOOSE messaging allows for interoperability (non-proprietary) between various distribution automation devices. The speed of operation can be within the seconds time range for this type of application. This FDIR architecture provides support of traditional DNP SCADA protocol for control, monitoring and metering. A decentralized architecture (i.e. nearby substation) has reduced complexity and configuration is easy to setup and

maintain. A centralized architecture allows support of multiple / complex networks, handles multiple fault conditions, and supports the larger amount of data and devices. System load shedding can be accomplished with a centralized architecture. The application is shown in Figure 2.

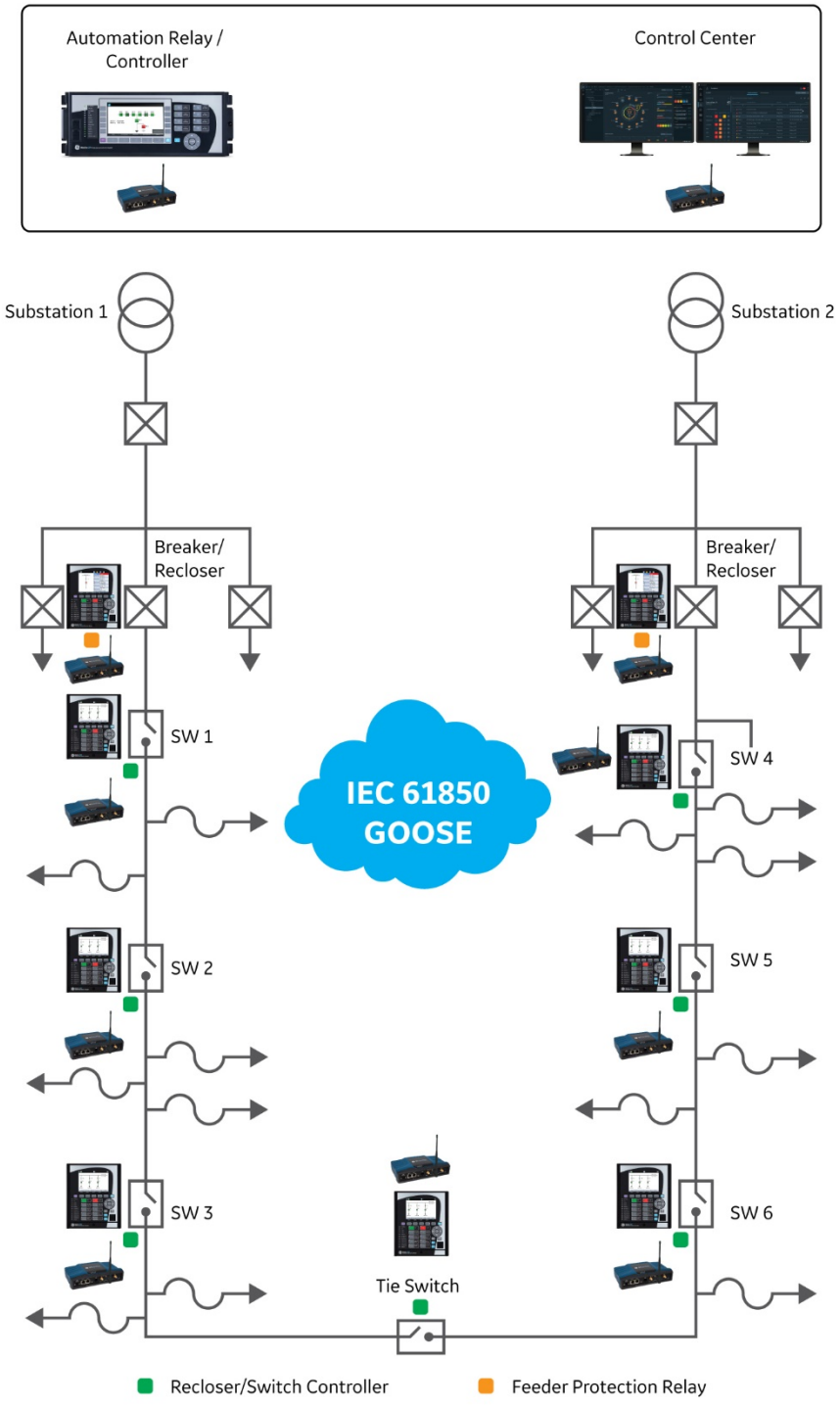

Figure 2 - Centralized / Decentralized FDIR

Distributed Energy Resources (DER)

Combined with today's drive toward green energy and the price competitiveness of renewable energy, utilities are experiencing unprecedented penetration of distributed energy resources. To accommodate these DERs, a solution must be in place to allow the utility to reliably monitor and control these resources. This application involves communication to a near-by substation.

This example illustrates several distribution automation applications. First, the architecture uses IEC 61850 peer-to-peer messaging for interoperability for transfer trip control and blocking after a fault condition at the solar farm or a fault on the utility feeder. Second, the architecture allows for retrieval of device configuration (i.e. settings) and events (waveforms, sequence of events) from each distribution device using IEC 61850. Third, the architecture supports setting group control from the automation controller to the distribution devices. As mentioned previously, IEC 61850 GOOSE messaging allows for interoperability (non-proprietary) between various distribution automation devices. The speed of operation can be within the seconds time range for control in this application. The retrieval of the data may take several minutes, but this is acceptable since it is not time critical to operations. This architecture provides support of traditional DNP SCADA protocol for control, monitoring and metering. The application is shown in Figure 3.

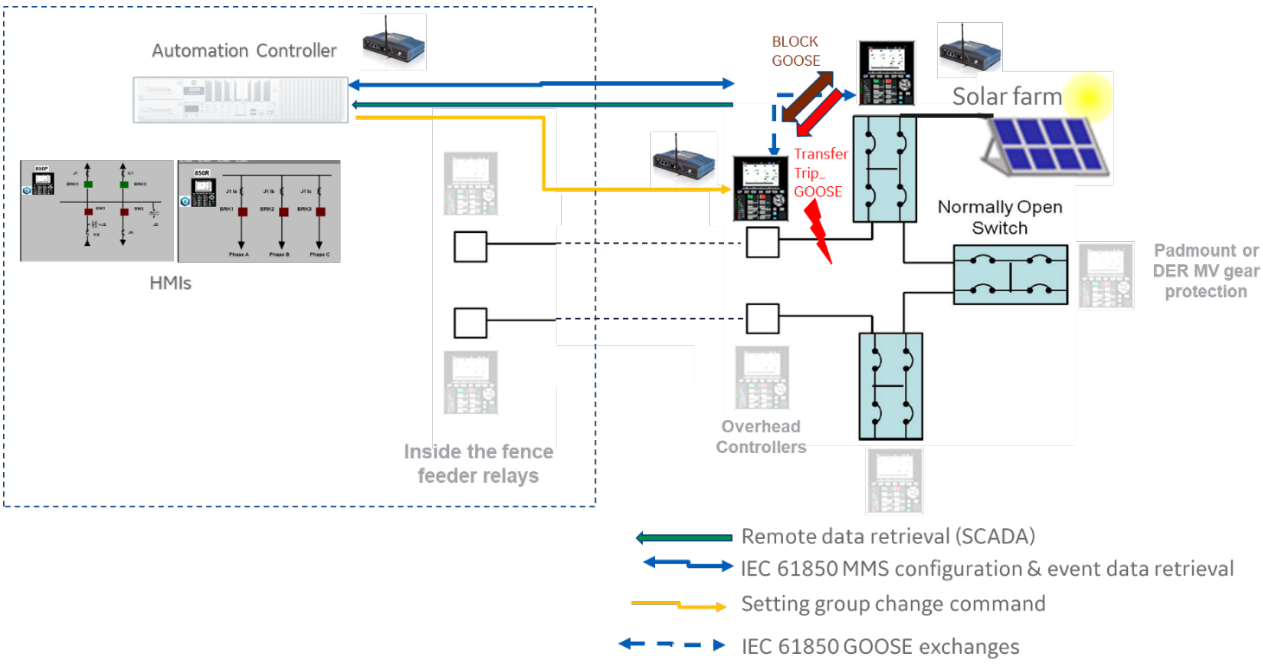

Figure 3 - Distribution Automation with Distributed Energy Resources

Microgrids

Microgrids are a growing segment of the power industry because of the benefits they bring in terms of resiliency. The ability to 'island' from the grid in case of emergencies and be able to continue serving it's loads independent of grid operation is enticing for cities, communities, industrial sites, and campuses. This application involves communications / system integration between the microgrid controller and the various distributed energy resources (DER) assets. The microgrid controller could also communicate to the utilities distribution management system (DMS) for overall system control. A wide mixture of protocols could be used, such as Modbus RTU, DNP, and IEC 61850. The speed of operation can be milliseconds to seconds time range for this application. The application is shown in Figure 4.

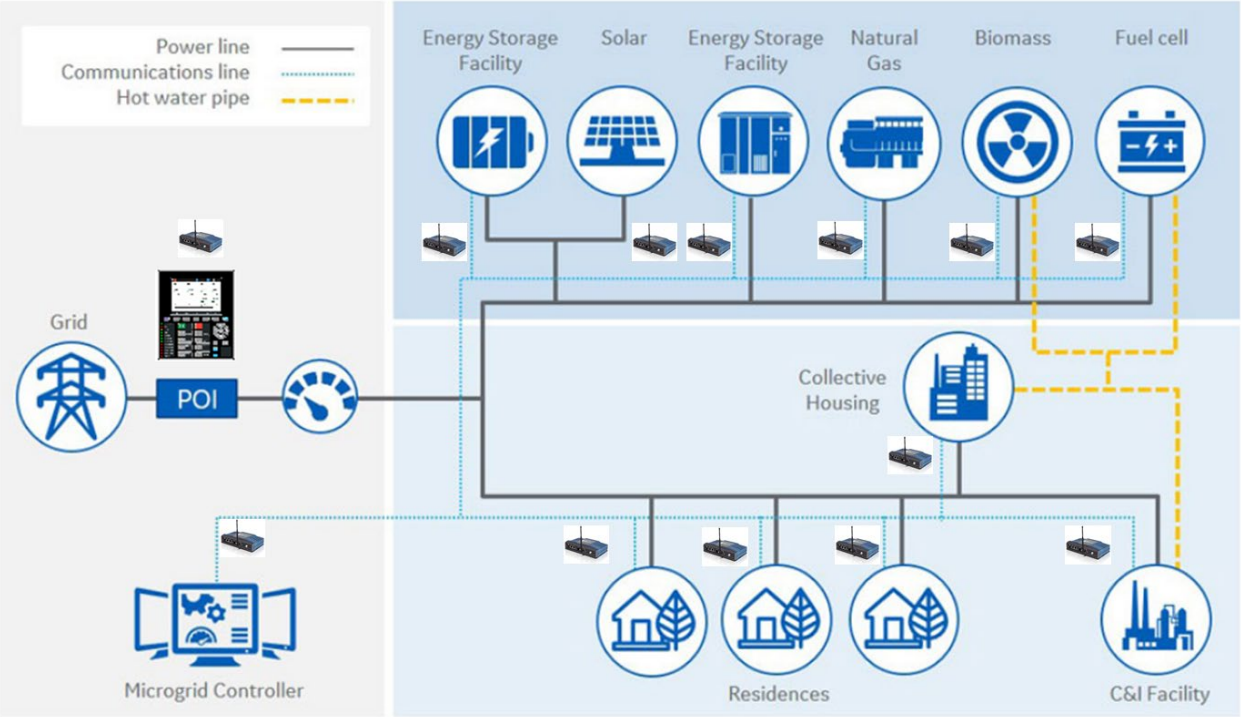

Figure 4 - Microgrid Control System

Wireless Solutions & Architectures

In the following section, we're going to discuss how communication networks address the ever-increasing requirements for automation applications in the distribution grid.

DA Applications: Deciding on Network Performance Requirements

An integral part of the proper and reliable operation of Distribution Automation (DA) applications is the underlying wireless network that interconnects IEDs in the field. This last-mile network, also called Field Area Network (FAN), can vary significantly in the type of radio technology used, capacity (throughput), latency and availability characteristics.

Latency

Network latency generally refers to the time it takes a data message to travel between two IEDs or endpoints over a data network. Various DA applications can have a wide range of latency requirements, from the very aggressive microgrid Fast Load Shedding, which may require < 10 msec of network latency, to more lax monitoring applications, which may be happy with 1-2 seconds of latency. Sometimes aggressive and lax applications may need to co-exist over the same network uplink. In such cases, the network needs to be designed to accommodate the most demanding requirement. The budget allocated for network latency can be relatively subjective and is a factor of the overall automation scheme used. This is usually determined with open technical discussions between automation and telecom groups to try to find a solution that is fast enough, within financial budget means. Latency may also be influenced by business directives (e.g. how quickly a certain distribution segment needs to be restored). For those reasons, data shared in the table below (Figure 5) is to be taken as a general ball-park guidance only.

Throughput

Network throughput is another important requirement to consider when designing control and protection schemes. Throughput in our context refers to the maximum "volume" per second of data that can be transmitted over a wireless network between two IEDs or endpoints. Choices of polling versus report-by exception, frequency of polling, the number of SCADA data points as well as the type of automation protocol (DNP vs serial vs IEC 61850 GOOSE) are important parameters that impact throughput. The more frequent the polling is, and the more data points to transfer, the higher the throughput requirement is. However, from the perspective of SCADA monitoring and control applications, this volume of data is still relatively low. Lower-throughput legacy narrowband networks, which typically offer 1s to 10's of Kbps per IED will still work perfectly fine. However, modern automation applications may add additional load on the network with their need to pull logs or oscillography files from the IEDs over the air after faults and recovery. Such files can be sizeable with multiple megabytes of data whose transfer over lower throughput networks can take a very long time.

Reliability

Network reliability refers to the overall availability of the network whenever it's needed. The higher a network's uptime and availability, the more reliable a network is. Several factors impact availability including the type and quality of networking equipment used, the type of RF spectrum (licensed or unlicensed) and RF technology, network protocols and interference mitigation techniques, as well as design and built-in redundancy of both networking devices and paths. In general, applications related to monitoring are more forgiving when it comes to network reliability. If a network outage occurs, not receiving monitoring data points during that down time may not be as detrimental to grid operations. Applications related to protection such as FDIR or DER and involving transfer trips are more impaired with network outages. As an example, if communications is lost between IEDs in an FDIR segment and a fault occurs at the same time, local protection kicks in to isolate that segment but restoration won't complete until the communications network is back online to allow the coordination of reclosers. Network reliability is an engineering and financial undertaking as well. The question to ask at the end

is how much more is it going to cost to have connectivity to an IED or substation with a 99.99% uptime versus 99.999% uptime. How much downtime can we afford, and during downtime what are some mitigation schemes we can use on the automation side to maintain safety while reducing risk and financial loss.

Cyber Security

Cybersecurity is an increasingly hot topic for utilities. It is as important to maintain in the distribution grid as it is for transmission and generation critical assets. When thinking through possible attack vectors, one should consider the worst-case scenario of what could an intruder possibly do with direct access to a recloser or a microgrid controller. What damage could they possibly cause? The answer should help us visualize how secure the underlying data network must be. While in general, intrusion into devices such as reclosers can result in power outages and imbalance in the grid, intrusion into seemingly benign monitoring data can be similarly impactful. For an intrusion that's tied to the power auction market, having illegal access into monitoring equipment and data may offer them a significant advantage over others.

DA Applications	One-Way Network Latency Between IEDs	Network Reliability Requirement	Network Throughput Per IED	Cyber Security
Peer-to-Peer FDIR	<100 msec	High	1's to 10's of Kbps	High
Centralized FDIR	<200 msec	High	10's of Kbps	High
Decentralized FDIR	<100 msec	High	10's of Kbps	High
DER Disconnect/Trip	<100 msec	High	10's of Kbps	High
Microgrid Control System	<100 msec	High	10's to 100's of Kbps	High
Microgrid Fast Load Shedding	< 10 msec	High	10's to 100's of Kbps	High
Monitoring	1-2 seconds	Low	10's to 100's of Kbps	Low/Medium
Control	1-2 seconds	High	10's of Kbps	High

Figure 5 - Summary of typical FAN Network Requirements for DA Applications

DA Applications: Choosing a FAN Radio Technology

Various RF technologies exist, and selection is driven by the requirements for the network. Popular technologies in the world of utilities have traditionally included unlicensed 900MHz (ISM), licensed narrowband frequencies, and public or private LTE cellular. Part of the decision-making process for choosing the right RF technology involves the utility's investment models, available cash, and desire for owning and operating the network versus outsourcing the ownership to a carrier or supplier.

Because of the vast variety of DA applications today, most medium to large utilities tend to deploy a hybrid of RF network technologies rather than rely on one. As an example, spread-spectrum 900MHz ISM has traditionally been used for transfer trip, while licensed narrowband is used to SCADA polling or report-by-exception. Topology, latency, and bandwidth application requirements play into the decision-making process. While fiber optics technologies may be a consideration for a last-mile network in cities and urban developments, when it comes to suburban deployments fiber becomes too cost-prohibitive and RF technologies become an ideal replacement.

Application-driven RF technologies are offered by device manufacturers to address specific applications on the distribution system. Line sensors, transformer monitors and underground vault gas detection equipment may be manufactured with embedded cellular or Wi-Fi technology to provide a one box solution to the utilities' network. A risk to application-specific RF technology is that it may not integrate with the overall design and requirements of the system easily. It is often better to address the communications network in a holistic manner, identifying applications and solutions for each application, after RF technology is vetted and selected.

The cost of investing in a certain RF technology is tied to utilities' preferred CAPEX or OPEX models too. Some technologies like private cellular require large CAPEX to build the infrastructure and purchase (or lease) the cellular spectrum but reduce the overall and long-term operational costs while providing higher network capacity, reliability, and a relatively future-proof network. On the other side, public cellular networks are pre-built by the carriers and using such technology incurs little CAPEX for the utility. It's basically limited to the cellular device/modem. The OPEX however can be significantly higher on the long term as each site retains a recurring fee for the monthly cellular usage. From a reliability perspective, utilities have historically steered away from public carriers for fear of unavailability during congested times (natural catastrophes) and due to OPEX costs. However recent offerings on public carrier spectrum such as FirstNet™ have provided utilities and critical services with premier bandwidth and priority access into those public cellular networks.

Utilities generally prefer unlicensed spectrum such as TV White Space, 900 MHz ISM or 2.4/5.8 GHz bands to avoid paying licensing costs and reduce OPEX. The ubiquitous nature of those bands in most regions, as well as their relatively good throughput are another attraction. Some disadvantages of unlicensed spectrum include the potential of interference if the band is crowded. This could be mitigated to a certain extent by using vendor-specific radio technologies involving advanced RF media access controls (MACs), beam-forming technology, as well as other mechanisms like frequency hopping, bandwidth sizing, forward error correction (FEC) and other technologies.

Licensed narrowband spectrum is generally more preferred for field area networks (FANs), but it is subject to availability. Licensed spectrum for most sub-1GHz bands is obtained through the FCC and paid for by the utility on an annual basis. In some cases, such as the 700MHz upper A block band, the spectrum is purchased from a private spectrum owner entity and its license renewed through the FCC every 10 years. As is the case of unlicensed networks, the utility would need to build and maintain the radio infrastructure of licensed networks which may be CAPEX heavy if tower construction is involved. Licensed narrowband technology in the 100, 200, 400 and 900MHz spectrum offers a relatively low throughput per remote/IED. However, because of FCC regulations, the radios are allowed to transmit at a much higher power than in unlicensed bands, resulting in a significant increase in coverage/distance. It is not uncommon to find licensed narrowband links exceeding 30 miles in distance between the access point (AP) and remote. This aspect of narrowband tends to optimize infrastructure CAPEX in that the utility doesn't have to build as many access point/base station towers as is the case with the unlicensed band or cellular technology.

The following table (Figure 6) summarizes common RF technologies used in the utility Field Area Network, and their corresponding performance and financial characteristics.

RF Technology	RF Band Ownership	Typical One-Way Latency	Available Throughput Per IED	CAPEX	OPEX	Typical Network Topology
TV White Space	Unlicensed Public	10's of msec	10's of Mbps	High	Medium	P2P, P2MP, Mesh
900 MHz ISM Band	Unlicensed Public	10's of msec	10's of Kbps to Low 1000's of Kbps	High	Medium	P2P, P2MP, Mesh
2.4 to 5.9 GHz ISM Band	Unlicensed Public	10's of msec	1s to 10's of Mbps	High	Medium	P2P, P2MP, Mesh
Narrowband 100, 200, 400, 900	Utility Owned	100's of msec	10's of Kbps	Higher	Medium	P2P, P2MP, Mesh
Upper A Block Wide Band 700 MHz	Utility Owned	10s to 100's of msec	100's of Kbps	Higher	Medium	P2P, P2MP, Mesh
CBRS 3.5-3.7GHz Band	Utility Owned Semi-Public	10's of msec	10's of Mbps	Higher	High	P2MP
Private LTE Bands	Utility Owned or Leased	10's of msec	10's of Mbps	Highest	High	P2MP
Public Cellular	Carrier Owned	10's of msec	10's of Mbps	Lowest	High	P2MP

Figure 6 - Performance Criteria of Various RF Technologies

DA Applications: Choosing a Network Topology

Network topologies define the path of communications between nodes in a network. Network topologies exist at several layers in the Open Source Interconnect (OSI) model which is widely used in commercial networks. In a practical scenario, while a physical/layer 1 topology may look like a direct point-to-point connection to a radio remote or IED, OSI layer 2 over which the payload-carrying protocol (e.g. IEC 61850 GOOSE) operates may look like a multipoint or hub where every sent packet is heard almost simultaneously by all IEDs on that VLAN.

Therefore, it is important while designing a network to have full awareness of the various automation protocols in current use and their method of operations. It is equally important to build networks that are future proof for automation protocols that may be added on IEDs down the road via firmware updates. In this section we will overview three commonly used network topologies and discuss their pros and cons.

Point-to-Point

Point to point topologies are the simplest from a network perspective and constitute a direct link between two end points. The following example shows an IED and a controller residing in a substation.

Figure 7 – A Simple Point to Point Topology

Point to point topologies are usually deployed when the need is simple, which is to connect one remote site to some local resource such as in a DER transfer trip application. But the simplicity of topology doesn't always translate to simplicity of communications. Let's go back to the point to point example and look at a simple transfer trip application case in point between a DER and a substation.

Point-to-Multipoint

These are the most common RF topologies in field area network (FAN) deployments and can be built using legacy narrowband radios, ISM radios, broadband radios, or even cellular LTE technology. The Point-to-multipoint (aka multipoint) FAN network typically consists of an access point (AP aka base station) generally deployed at a substation, and several downstream radios attached to IEDs on feeders. See Figure 8 below for an example.

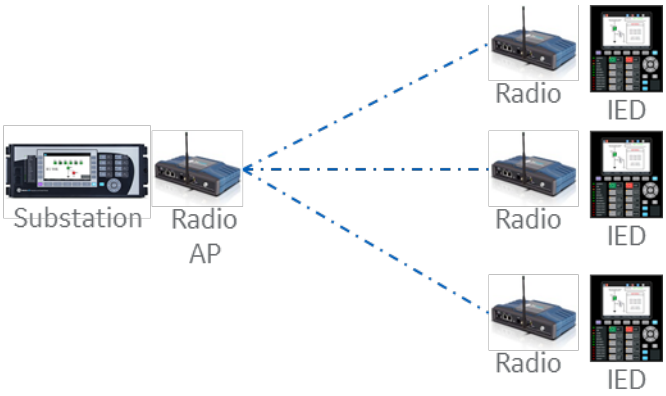

Figure 8 - A Typical Point-to-Multipoint Topology

The scalability or network density of AP Radio depends on the radio technology used, vendor, and latency/throughput requirements. It can range from a 1:10's in traditional narrowband and ISM radio networks, to 1:1000's in LTE-based cellular technology.

Multipoint networks can easily enable communications for centralized as well as decentralized DA applications. They also allow communications between the end points, e.g. in the case of a peer-to-peer FDIR, if needed. In such a case, apparently the data travels from one IED through its radio to the access point and then downstream to the other IED.

A multipoint topology can be used for latency-sensitive applications such as transfer trips if the network and the choice of RF technology/capacity are well thought through to accommodate aggressive latency needs.

On such networks where the AP is "shared" with the remote radios, it becomes crucial to use quality of service (QoS) network technologies to prioritize traffic accordingly. As we saw in the above matrix, a significant number of protocol exchanges and data streams may exist simultaneously on the simplest of networks. We would then need to identify our most critical protocols (applications) and use QoS to give them a higher priority and a dedicated bandwidth. This ensures that even during network congestion, those critical packets have priority access to the network as well as a pre-determined carved-out network capacity.

Mesh

A mesh network topology (Figure 9) enables an any-to-any connectivity scenario between radios in a large network. It allows a radio attached to an IED to "look around" and establish a connection with the nearest radio with the best radio signal, and with the shortest distance to the backhaul. Mesh networks traditionally have much shorter ranges (100's of meters) between the radios than point-to-point or multi-point networks (several miles), and that's mainly due to the omni antennas needed in mesh networks that disperse the RF signal instead of focusing it. On the positive side, the automatic nature of the mesh network generally offers IEDs more than one uplink path to the substation or backhaul. Mesh networks use increasingly complex and highly optimized routing protocols in order to enable a radio to: (1) find the nearest radio with the strongest RF signal, (2) with the highest available throughput capacity, and (3) with the shortest distance (lease number of hops) between the subject radio and the takeout/backhaul AP.

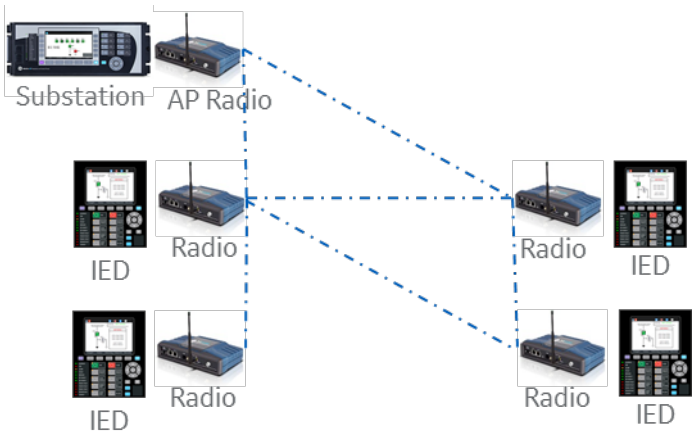

Figure 9 - Mesh Network Topology Example

Mesh networks can be highly resilient to network failure and generally offer backup paths. However, the price one pays for such resiliency is generally network capacity and latency. Since a data packet may need to travel via several mesh hops between source and destination, latency may be impacted, as well as available network throughput. Newer mesh technologies using higher capacity bands such as in TV White Space (TVWS), as well as the sub-6GHz broadband and the newer 60 GHz band. Those bands may offer 10's of Mbps of throughput per mesh node, as well as extreme low latency.

One final consideration to keep in mind for mesh networks is whether the use of protocols, such as IEC 61850 GOOSE or other protection-oriented protocols, is needed. Because such protocols are highly sensitive to latency, the mesh network may need to be planned in such a way that a worst-case scenario multi-hop connectivity may still offer the needed latency for the application.

Improving Field Area Network Reliability Through Design Considerations

Several complex network design factors can have an impact on the availability and reliability of the wireless field area network (FAN), and hence contribute to the overall improvement of grid reliability.

Radio Device Ruggedness

While it is a given that utilities tend to require rugged network equipment in the field, especially in unventilated enclosures, not all ruggedness labels are the same. Some radio manufacturers build and design their radio circuit boards and systems following rugged standards such as IEC 61850, IEEE 1613, and some military standards. Other vendors not only build to, but they test and certify their equipment with 3rd party independent laboratories to gain the improved confidence and reliability with the "certified" label. In addition to the commonly acknowledged utility device hardened standards, the US government has recently required federal agencies to identify and develop responses to the electromagnetic pulse (EMP) threat which may result from nuclear detonation. It is important to factor in compliance or certification to standards that improve device immunity against EMP to future-proof the network.

Radio Device Lifespan

This aspect is closely tied to radio device ruggedness. The lifespan of field area network equipment doesn't only impact reliability, but it also affects OPEX. Radio manufacturers can offer a mean time between failures (MTBF) number which estimates the mean number of years it will take before a device hardware failure is expected. The higher the number the better. MTBF is tied closely to how well the internal circuitry is designed, the quality of its components, and how well and holistically the overall device and solution is designed with reliability in mind.

Number of Radio Uplinks

While most SCADA applications can tolerate some network downtime due to the loss of a radio uplink, some applications related to protection or Fast Load Shedding have a much higher requirement for network availability. In some cases, fiber optic communications make sense to use, such as in an urban area due to the proximity of IEDs. However, since the majority of field area networks are spread out over large distances, fiber becomes cost-prohibitive to extend to all IEDs.

To solve the requirement of needing a network that's more reliable than one whose remotes have a single radio uplink, utilities may consider solutions that involve radios with multiple uplinks (e.g. multiple embedded modems), or ones that involve two radios devices each with one or more uplinks to offer the redundant paths. Mesh radios offer an alternative viable solution due to their ability to automatically route traffic to backup uplink nodes should the primary one fail. However, these mesh solutions come at a financial and latency cost. Therefore, special considerations and device optimizations, including the right choice of RF band and technology need to be factored in while considering mesh topologies.

The example shown in Figure 10 below illustrates an IED attached to a radio device that has two embedded modems. The primary modem in this case may operate on narrowband or unlicensed ISM bands, and the backup radio could use cellular technology.

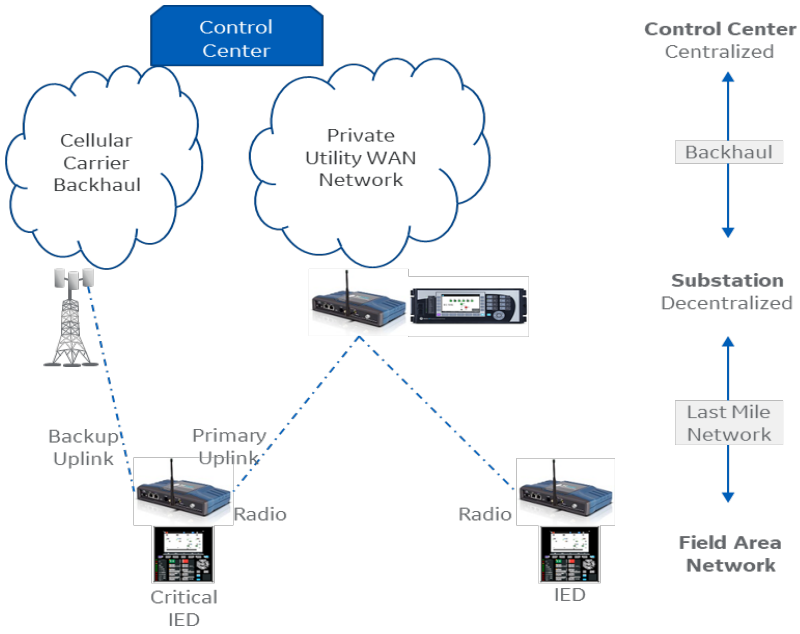

Figure 10 - Example of an IED with a Dual Uplink Radio

The Choice of RF Bands

As noted earlier, unlicensed radio bands save on operation costs due to the lack of licensing needs but are more open to interference since they're free for all to use. Utilities using unlicensed bands need to consider radio technologies and vendors that have built-in robust interference avoidance mechanisms in order to maximize uptime during times of congestion.

Licensed narrowband frequencies in the 100, 200, 400, 700 and 900MHz spectrum are generally much more robust against interference since it is illegal to operate in those frequencies if not licensed. The FCC allocates specific frequencies to specific geographic areas so that a single entity may own and operate them in that area.

Cellular technology is generally very robust against interference because it operates on licensed bands (generally owned by the carriers).

Improving Grid Reliability with Network Security Considerations

While cyber security is a domain that mainly revolves around illegal access and intrusion into network and data assets, it may have an impact on grid stability. If a hacker gets hold of a controller inside of a microgrid, or a protective IED, etc. they may have the power to trip load or generation and cause havoc in a network. This is one of many reasons to give particular attention to cyber security to improve overall grid stability and integrity.

Securing Data Transmission

Data communication between any two automation or communication devices outside of a physical security perimeter must be encrypted to scramble data against open-air eavesdroppers. Such intruding entities may have the ability to listen to radio transmissions using special software-defined radios or spectrum analyzers. The larger the encryption key, the better. Keys that are used to encrypt and decrypt data in a field area network today are generally either 128-bit or 256-bit in size. Key rotation algorithms with certificate management must be used instead of static keys, in order to ensure, should a key be compromised by an intruder, they would soon be locked out from using it after the network generates and exchanges new sets of keys.

Securing Communication Devices

Radio vendors can use several technologies to strengthen their networking device security against physical or remote intrusion. As an example, secure boot technologies ensure that all modular hardware components in a certain radio device are tied together electronically at the factory. This ensures that should an intruder gain physical access to an enclosure and replaces a compromised RF module inside of a radio device, the device will reject it since its factory signature doesn't match. Secure firmware is a similar technology that guards against the manipulation of firmware. If intruders attempt to change parts of a firmware file, the radio device will reject it and refuse to load it. Other technologies such alarm contacts that trigger an alert to network operators should an enclosure door open, or sensor embedded in the radio to detect movement can also be helpful. Finally, secure manufacturing practices are a very important consideration. A few years ago, Bloomberg discussed in length an attempt by a foreign government to intercept computer and communication chip supply chains and implant hidden backdoors on seemingly innocent devices. For this reason, ensuring that radio manufacturers have a tight control and auditing of their supply chain, and use secure manufacturing practices will help mitigate against such risks.

Securing Users and Data Integrity

Several mechanisms can be used to ensure that only authorized users can access the specific network and automation devices they are authorized to use, and at the authorized level. Technologies centered around authentication, authorization, and accounting (AAA) technologies such as RADIUS or TACACS/+ will enable and monitor operators/user's behavior on the network.

To ensure data integrity, basic firewalling mechanisms can be used at specific network entry points to ensure that only allowed data types and protocols can be transferred, while all others are explicitly blocked. More advanced technologies involving intrusion detection (IDS) monitor network traffic and look inside of data packet headers for pre-programmed anomalies. If as an example a DNP3 or IEC 61850 GOOSE packet with unexpected commands is detected, the operators could be alerted of the incidence. Intrusion prevention systems (IPS) go a step further by blocking such malformed or ill-formed packets from traveling the network, and then reporting the incident to the operators. Finally, as it touches everything artificial intelligence (AI) is being integrated in security appliances to protect not only against known threats, but also humanly-unpredictable or unexpected threats. They work by studying "normal" patterns of communication over an extended period of time and then monitor the network, while still "learning" for patterns that aren't supposed to be there. This includes not only malformed packets, but unexpected behaviors such as accessing an IED from a network where it's not supposed to be seen.

Conclusions

The field area network (FAN) plays an important role in distribution grid stability as it enables communication between its various IEDs and automation devices. Specific care needs to be taken while choosing and designing the FAN radio technology to ensure the highest availability possible of the network, so that the automation building blocks achieve their goals and requirements as needed.

The choice of radio technology impacts performance characteristics such as network capacity, latency, and reliability. While licensed narrowband technologies have been the de-factor winner for several years, newer cellular-based technologies are picking up steam due to their wide availability, as well as improved network capacity and latency. Considerations of OPEX and CAPEX and whether to build your own or lease, factor into the choice of radio technology as well.

The ability to properly meet and exceed DA applications performance requirements such as throughput and latency is another important factor that plays into choosing the right radio technology. The radio topology has an impact as well. While point-to-multipoint is much more commonly used, mesh topologies that offer improved resiliency may be an attractive option with newer broadband-based mesh radios that offer significantly higher throughput and lower latency than traditional 900MHz ISM based mesh radios. However, mesh is a compromise because the distance between any two radios must be significantly less than other topologies.

Network security is an ever more important consideration to securing the grid and protecting against harmful intrusions. In addition to the commonly understood technologies of encrypting data packets, and authorizing the right users into the network, newer technologies have been emerging to try to catch up to hackers. Technologies like intrusion detection notify operators if intrusions following a pre-programmed fingerprint occurs. Intrusion prevention technologies not only alert the operator when an intrusion is detected, but they automatically block the data and/or user from network access. Finally, with the advent of artificial intelligence and its adoption in the cyber security community, highly advanced security appliances are now able to detect and protect against not only known intrusions, but also against ones that are yet to be designed and attempted. This is all thanks to neural networks, and the ability of such appliances to continuously learn and share “learned experiences” between various technology layers.

For more information on the 850R and 850P, visit:

https://www.gegridsolutions.com/multilin/catalog/dac.htm

Biographies

Judy LeStrange is a Regional Sales Manager for Industrial Communications, a division of GE Grid Solutions. Judy is responsible for southeast US customer relationships and sales of wireless and optical fiber networking products and services. She was a senior product manager for 4 years and AMI technical program manager for 1 year. Prior to GE, Judy was a product marketing manager at Eka Systems for 1 year. Judy has an MBA from University of Rochester – Simon Business School and a Bachelor of Science in Mechanical Engineering from Rochester Institute of Technology.

Edgard Sammour is a Regional Sales Manager for the Industrial Communications, a division of GE Grid Solutions. He assists utilities and critical infrastructure organizations solve their industrial IoT networking challenges with GE's wireless and optical solutions. Prior to his current position, Edgard held roles in product management and project engineering at GE, as well as roles in product marketing and network engineering at Cisco Systems. Edgard has a master's degree in Electrical Engineering from Oklahoma State University.

Ravindranauth (Mike) Ramlachan is a Lead Sales Application Engineer for Grid Automation, a division of GE Grid Solutions. He is the key customer contact for technical issues, including protection and control application support. Prior to GE, Mike worked at Consolidated Edison of NYC for 10 years, performing protection system design, fault and coordination studies, fault analysis, and developing relay settings. Mike has a master's degree in Electrical Engineering from Stevens Institute of Technology.

Craig Wester is a Regional Sales Manager for Grid Automation, a division of GE Grid Solutions. He provides sales management, application assistance, and solution assistance to electric utilities, electric cooperatives, electric municipals, and consulting firms throughout the states of NC, SC, GA, AL, TN and FL for protection, control, and automation. Craig has a Bachelor of Science in Electrical Engineering from University of Wisconsin-Madison. Craig joined GE in 1989 as a utility transmission and distribution application engineer. He is a member of IEEE.

For questions related this paper or to request a demo or quote please contact:

GE Grid Solutions
Direct Call: 1-844-379-9630
INDC.MDSInsideSales@ge.com

For more information related to Protection & Control devices, contact 1-800-547-9629 or sales.gridsolutionsap@ge.com

GEGridSolutions.com

GEA-33197
English
210604