Expanding Protection and Control Communications Networks With Wireless Radio Links

Tom Bartman and Ben Rowland
Schweitzer Engineering Laboratories, Inc.

Laura Rogers
Hawaii Electric Light Company, Inc.

This paper was presented at the 2019 IEEE Rural Electric Power Conference and can be accessed at: https://doi.org/10.1109/REPC.2019.00016.

This paper was previously presented at the 71st Annual Conference for Protective Relay Engineers and can be accessed at: https://doi.org/10.1109/CPRE.2018.8349794.

For the complete history of this paper, refer to the next page.

Presented at the
IEEE Rural Electric Power Conference
Bloomington, Minnesota
April 28–30, 2019

Previously presented at the
Clemson University Power Systems Conference, September 2018,
71st Annual Conference for Protective Relay Engineers, March 2018,
and 44th Annual Western Protective Relay Conference, October 2017

Previous revised edition released September 2018

Originally presented at the
4th Annual PAC World Americas Conference, August 2017

Expanding Protection and Control Communications Networks With Wireless Radio Links

Tom Bartman
Schweitzer Engineering Laboratories, Inc.
671 Moore Road, Suite 200
King of Prussia, PA 19406, USA
tom_bartman@selinc.com

Ben Rowland
Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163, USA
ben_rowland@selinc.com

Laura Rogers
Hawaii Electric Light Company, Inc.
P.O. Box 1027
Hilo, HI 96720, USA
laura.rogers@hawaiielectriclight.com

***Abstract*—Extending reliable and dependable communications for protection and control applications beyond the substation fence to additional sites and field devices can sometimes be a challenging task. Uneven terrain, distance, or other factors can make running cable difficult or impossible. In some cases, wireless communication is a cost-effective and practical alternative to pulling cable.**

Radios have proven to be an effective means of extending communications for supervisory control and data acquisition (SCADA) and engineering access, as well as for critical protection and control applications using serial communications. Low-latency Ethernet protocols like Generic Object-Oriented Substation Event (GOOSE) are becoming popular for high-speed, point-to-multipoint signaling protection and control applications. Radios used in protection and control should be evaluated for the specific application for which they are intended.

This paper examines the application of GOOSE over Ethernet radios and the associated challenges. The paper shares results from a real-world implementation, including results from GOOSE latency tests for protection and control applications.

***Index Terms*—Communications, DNP3, GOOSE, radio, SCADA, secure, wireless.**

I. Introduction

Communications allow for faster electrical protection schemes. However, providing reliable and dependable communication for a protection scheme between two sites can be challenging. Uneven terrain, long distances, and other factors make running cable difficult or impossible. In some cases, wireless communication is a cost-effective and practical alternative. Radio communications using Mirrored Bits® communications and Generic Object-Oriented Substation Event (GOOSE) protocols are practical for applications with an increased number of distributed generation sites, such as solar and wind generation. Some communications links are not owned by the utility, or there are no existing communications links between the sites. Radios offer a cost-effective and quick way to add communications links.

Several types of radios are available for expanding protection and control networks. These include both licensed and unlicensed radio systems. This paper examines the use of industrial, scientific, and medical (ISM) band unlicensed radios. This paper also examines the challenges, technical considerations, security, and cost benefits of applying radios for protection and control applications. Furthermore, the paper shares the results of a distributed generation application implemented at Hawaii Electric Light Company.

II. Technical Considerations When Using Unlicensed Radios

There are several considerations when using ISM-band unlicensed radios. These include topologies, radio line of sight, multipath errors, antenna types, radio path studies, and receiver sensitivity. This section discusses each consideration.

A. Topologies

A radio network topology is the arrangement of radios on the network. Three common topologies are as follows.

1) Point-to-Point

The simplest radio architecture involves only two radios in direct communication. In this case, a master (M) radio is communicating with a remote (R1) radio, as shown in Fig. 1.

Fig. 1. Point-to-Point Topology

A point-to-point link has the highest performance, but has the disadvantage of only providing communication to one remote device.

2) Point-to-Multipoint

Point-to-multipoint networks consist of an access point with multiple connected nodes, as shown in Fig. 2. These networks can provide excellent latency and, depending on the bandwidth, can support fast data rates. Connectivity in remote areas is difficult because each radio needs to have adequate line of sight to the same access point. If line of sight is limited, repeaters are often required.

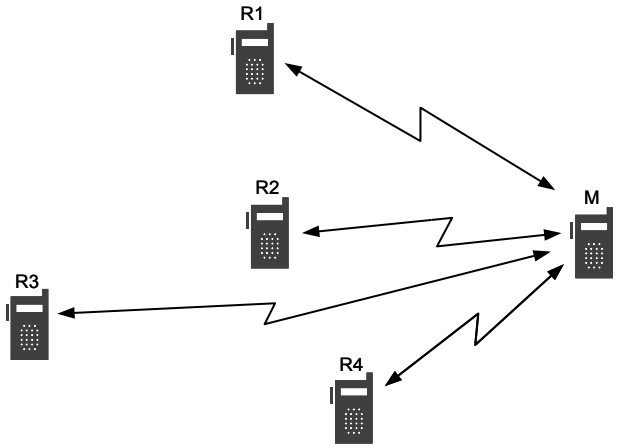

Fig. 2. Point-to-Multipoint Topology

3) Mesh

Mesh networks are optimized for connectivity. In a mesh network, there is no one access point as each radio communicates with multiple adjacent radios, as shown in Fig. 3.

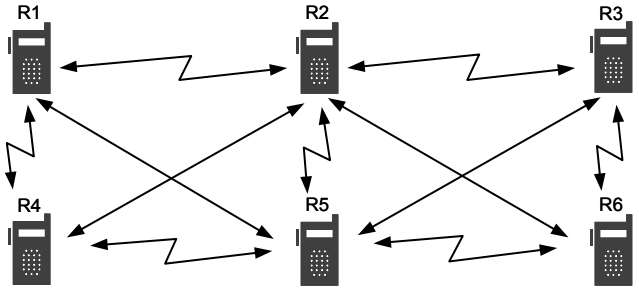

Fig. 3. Mesh Topology

Because mesh networks are optimized for connectivity, they provide limited throughput and relatively poor latency but superior coverage. These systems are popular for advanced metering infrastructure (AMI) networks because residential meters prioritize connectivity over performance. Using AMI networks for distribution automation has its own challenges, but with careful planning, dedicated mesh networks can be designed to work reasonably well for communication with distribution automation devices. Using mesh networks for high-speed protection is not recommended due to poor latency through multiple network hops.

Table I lists the topology and its respective latency, throughput, and connectivity.

Protection applications typically require wireless communication with very low latency. Throughput is of minimal concern because these applications only require that a small amount of data be communicated. Connectivity is important, but in protection applications, getting connectivity to an individual relay is relatively easy, making it of limited concern.

TABLE I
LATENCY, THROUGHPUT, AND CONNECTIVITY OF VARIOUS TOPOLOGIES

	Latency	**Throughput**	**Connectivity**
Point-to-Point	Very low; can be less than 10 ms	High; all the bandwidth is dedicated to one link	Limited by line of sight to the access point; repeaters may be required
Point-to-Multipoint	Low; can be between 10 and 100 ms based on the number of nodes and device design	Medium; bandwidth is split between multiple nodes	Limited by line of sight to the access point; repeaters may be required
Mesh	High; multiple hops make latency slower and unpredictable	Low; multiple network hops limit bandwidth	Not dependent on direct line of sight to the end node

B. Radio Line of Sight

Radios that operate in the 900 MHz ISM band are popular because they do not require a license and they are cost-effective. However, radios in the ISM band are limited by line of sight. This line of sight is typically 30 percent longer than the visual line of sight due to the bending of the earth's surface. As the communications path gets longer, taller antennas are required to maintain the line of sight. When discussing radios and referencing line of sight, it is typically the radio line of sight, not the visual line of sight, that is being referenced. As shown in Fig. 4, the radio line of sight is the concentric ellipsoid-shaped zone between the antennas. This zone is known as the Fresnel zone.

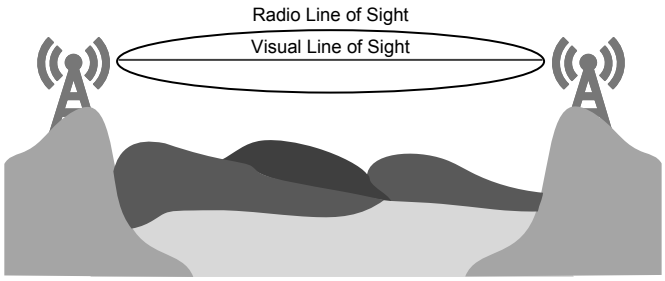

Fig. 4. Radio and Visual Line of Sight

The Fresnel zone is an important consideration for radio communication. Obstructions within the Fresnel zone can reflect radio signals and cause unwanted interference. Reflected or refracted signals can cause the signal to arrive at the receiver out of phase with the desired signal. Interference caused by reflected or refracted radio signals is known as a multipath error. Fig. 5 depicts the maximum Fresnel zone diameter between two antennas.

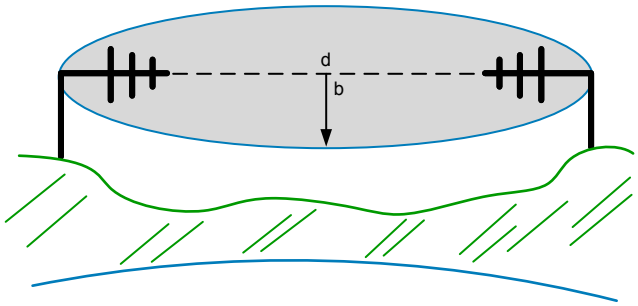

Fig. 5. Fresnel Zone Between Antennas

The formula used to calculate the widest distance of the Fresnel zone is as follows:

$$b = 17.32\sqrt{d/(4f)} \quad (1)$$

where:

b = radius of the Fresnel zone in meters.

d = distance between the transmitter and receiver in kilometers.

f = frequency transmitted in GHz.

C. *Multipath Errors*

Reflection due to atmospheric or geographical conditions causes the signal to reach the receiver via multiple pathways, as shown in Fig. 6. This creates distortion that can cause interference and unintended phase shifting.

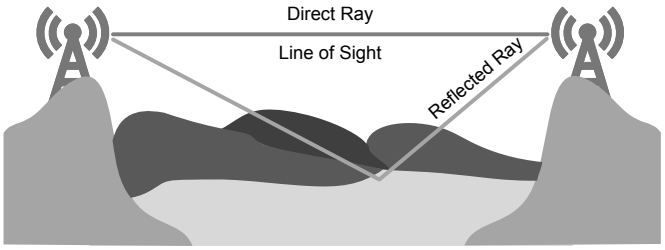

Fig. 6. Multipath Errors Due to a Reflected Radio Signal

Multipath errors that cause poor signal quality can result from anything from a protruding building to a reflection off of a lake. In an example case of a lake application, antennas were installed on opposite ends of a lake, and although the visual line of sight was clear, a portion of the Fresnel zone reflected off the water. Once the antennas were slightly raised, the errors were eliminated. The Fresnel zone should be 60 percent clear of obstructions for reliable radio communications.

D. *Antenna Types*

The two types of antennas that are most commonly used in radio applications for protection and control are an omnidirectional antenna and a directional Yagi antenna.

An omnidirectional antenna, shown in Fig. 7, typically has one vertical element and transmits its energy uniformly around one horizontal plane. The radiation pattern is shown in Fig. 8. An omnidirectional antenna is usually mounted vertically.

Fig. 7. Omnidirectional Antenna

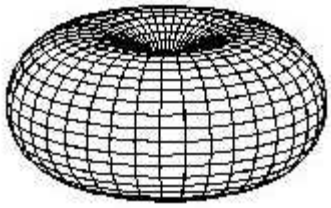

Fig. 8. Omnidirectional Antenna Radiation Pattern

An omnidirectional antenna is commonly used in point-to-multipoint applications where the master site radio must communicate with multiple radios in remote locations.

When communications require a point-to-point link, directional antennas are used. Unlike the omnidirectional antenna, this type of antenna transmits a beam in one direction. Fig. 9 shows a directional Yagi antenna consisting of multiple elements. These elements focus the energy into a beam rather than disperse it over a 360-degree plane. Because the energy is focused in one direction, the antenna has higher gain than the omnidirectional antenna.

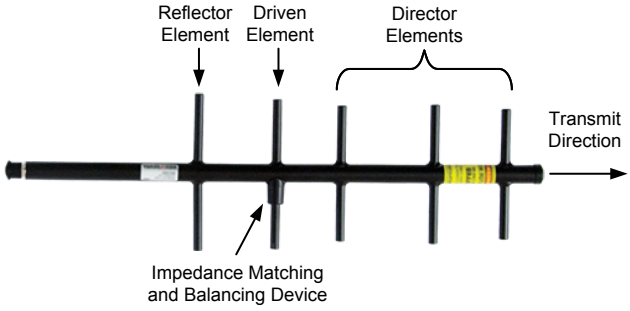

Fig. 9. Directional Yagi Antenna

Directional Yagi antennas transmit wireless information long distances over a narrow beam, as shown in Fig. 10.

Typical ISM-band Yagi antennas have gains that range from 3 dB to 12 dB. Typically, the higher the number of director elements, the narrower the beam, therefore achieving longer distances or higher gains. For example, while a

3-element Yagi antenna might have a gain of 8.5 dBi, a 5-element Yagi antenna might have an increased gain of 11.1 dBi. It is best practice to use a Yagi antenna when an omnidirectional antenna is not needed. Not only does a directional Yagi antenna have more gain, but the directional beam limits unwanted interference.

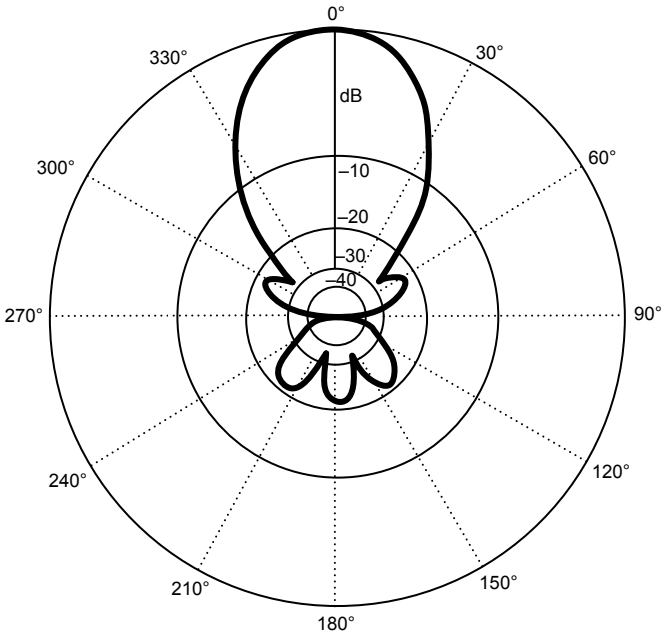

Fig. 10. Directional Yagi Antenna Radiation Pattern

E. *Radio Path Study*

The first step when considering radio communication is a radio path study. Some radio manufacturers offer a free radio path study to determine if the link is viable. A path study is performed using software that accounts for the radio type, antenna type and height, transmission cable type and length, terrain, and clutter. Global Positioning System (GPS) coordinates and antenna heights are required for each site. While path study software typically accounts for terrain, some types of clutter, such as buildings and man-made objects, must be manually entered. Also, it is important to consider the future growth of forests when calculating antenna heights to avoid future interference.

F. *Receiver Sensitivity*

Receiver sensitivity, or the measure of the reliability of the link, is an important radio receiver specification. Receiver sensitivity is the lowest signal level received that the radio can properly decode for reliable operation. If the received signal level drops under the receiver sensitivity, radio performance is degraded due to data errors. Best practice is to design the radio system so that the received signal is well over the receiver sensitivity. The higher the signal level is above the receiver sensitivity, the more reliable the communications link. The difference between the received signal and the receiver sensitivity is called the fade margin. A fade margin of 15 dB is required for a reliable link, but 20 dB is preferred.

III. Link Budget

A link budget determines all of the gains and losses within a communications channel. When a transmitter puts out a signal at a certain power level, the signal experiences gains and losses on its path from the transmitter to the receiver. Antennas have effective gain, but power is lost in cables and in the transmission medium where the link operates. As mentioned earlier, the receiver has a receiver sensitivity, or the minimum threshold at which it can reliably pick up the received signal.

The most significant term in the link budget calculation is the free space path loss (FSPL). FSPL is the amount of loss or attenuation that the signal experiences as it travels through free space, as shown in Fig. 11. FSPL is calculated using the following equation:

$$\mathrm{FSPL} = 20\log(\text{distance in km}) + 20\log(\text{frequency in GHz}) + 92.45 \quad (2)$$

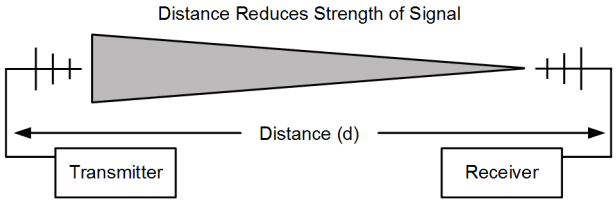

Fig. 11. Free Space Path Loss

A longer link means more FSPL, as does a higher radio frequency. Therefore, a 2.4 GHz radio experiences more FSPL than a 900 MHz radio over the same distance.

Fig. 12 shows an example of a 20-mile radio link budget. The transmitter and antenna provide signal gain, but the transmission cables and signal propagation through free space result in losses. The total gains and losses are calculated as the net result of the received power, or 19.2 dB, above the receiver sensitivity.

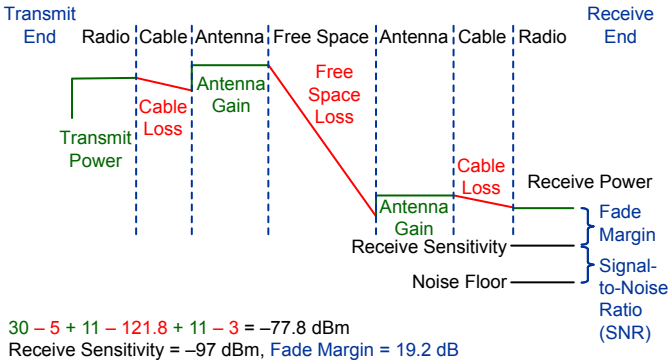

Fig. 12. Example of an End-to-End Link Budget

It is difficult to determine a maximum length for a specific type of transmission cable due to varying applications and link budgets. Table II shows the losses of two common cable types used in radio applications.

TABLE II
TRANSMISSION CABLE LOSSES IN DB

Length (ft)	LMR-400 900 MHz	LMR-400 2.4 GHz	7/8" Helix 900 MHz	7/8" Helix 2.4 GHz
25	1.0	1.7	0.3	0.5
50	2.0	3.4	0.5	1.0
75	2.9	5.1	0.8	1.4
100	3.9	6.8	1.1	1.9
125	4.9	8.5	1.3	2.4
150	5.9	10.2	1.6	2.9
175	6.8	11.9	1.9	3.4
200	7.8	13.6	2.1	3.8
Loss Per Foot	0.039	0.068	0.011	0.019

Refer to the example in Fig. 12. It may be viable to use 100 feet of LMR-400 cable if the FSPL allows for it. In other applications, 100 feet of LMR-400 may have unacceptable loss. In the event of unacceptable loss, a lower-loss cable, or higher-gain antennas, would be required to achieve an acceptable fade margin.

IV. SECURING RADIO COMMUNICATIONS

Although a radio communications link seems like a simple and secure solution, there is a risk that the communication can be intercepted. Encryption adds confidentiality to communications so that only the intended recipient can decipher the information. One popular method of encryption is the Advanced Encryption Standard (AES). AES is a United States government-approved cryptographic algorithm. Using a secret key, AES operates on plain text by breaking data into blocks. These blocks are then scrambled using different transformations. The transformations include substituting bytes, shifting rows, and mixing columns. The algorithm uses several rounds of these transformations before resulting in the final ciphertext. Radio manufacturers employ AES encryption to thwart attackers who attempt to compromise over-the-air data. The AES algorithm is extremely strong. One analysis concluded that it would take a billion years to crack the 128-bit AES key using a brute force attack [1]. Fig. 13 shows an example of two remote sites communicating over a secure wireless link.

The 256-bit AES meets Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Federal Information Processing Standard (FIPS) 140-2 requirements. It can also assist with North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) considerations. AES provides security against man-in-the-middle and replay attacks. When choosing a radio, consider a strong encryption standard such as AES.

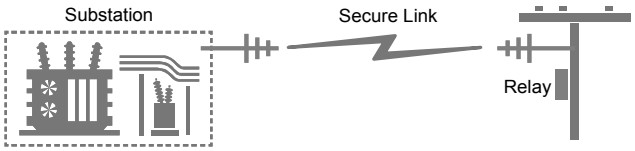

Fig. 13. Wireless Secure Communications

V. MIRRORED BITS COMMUNICATIONS OVER A RADIO LINK

Radios can provide low-cost backup or secondary protection using a transfer trip scheme and MIRRORED BITS communications over point-to-point links. Low latency enables fast teleprotection and control. Teleprotection and control commands are communicated with a typical 5.5-millisecond latency. Common applications for MIRRORED BITS communications protocol over a radio link include recloser, capacitor bank, and voltage regulator controls, substation communications, and distributed generation.

VI. IEC 61850 GOOSE OVER A RADIO LINK

GOOSE is better suited for point-to-multipoint applications, but has a higher latency than MIRRORED BITS communications. Radio communications solutions have been successful in time-critical IEC 61850 GOOSE applications in distribution circuits. One such application is at Hawaii Electric Light Company. In the application, five 250 kW distributed photovoltaic (PV) systems are located in remote areas on multiple Kapua 12 kV distribution circuits. The project overcame various hurdles including the remote locations, the lack of a direct line of sight for radio communications, and power production exceeding power usage on the circuit. Several technologies were integrated to achieve supervisory control and data acquisition (SCADA) capability and the new protection scheme for this project. These technologies include IEC 61850 GOOSE message and DNP3 protocols, Ethernet point-to-multipoint radios, and protective relays.

A. Substation and Remote Site Architecture

The Kapua substation is an older switchgear substation with electromechanical relays that were upgraded to digital microprocessor-based relays. The substation has a SCADA remote terminal unit (RTU) communicating with the energy management system (EMS) via a T1 communications link. The RTU has been upgraded for future communications over an Internet Protocol/Multiprotocol Label Switching (IP/MPLS) network, but is presently using the T1 link for communication back to the EMS. Within the substation, Ethernet networking was installed to enable relay communications to the remote independent power producer

(IPP) sites using IEC 61850 GOOSE messages, mainly due to the large number of sites involved.

The substation relay sends GOOSE trip messages to the relays at each remote site. These GOOSE messages are sent so that the distributed energy resource (DER) breakers at the solar sites are tripped before the substation circuit breaker (CB) opens. Breaker statuses are returned via GOOSE messages. Fig. 14 shows the topology of the substation and remote PV sites.

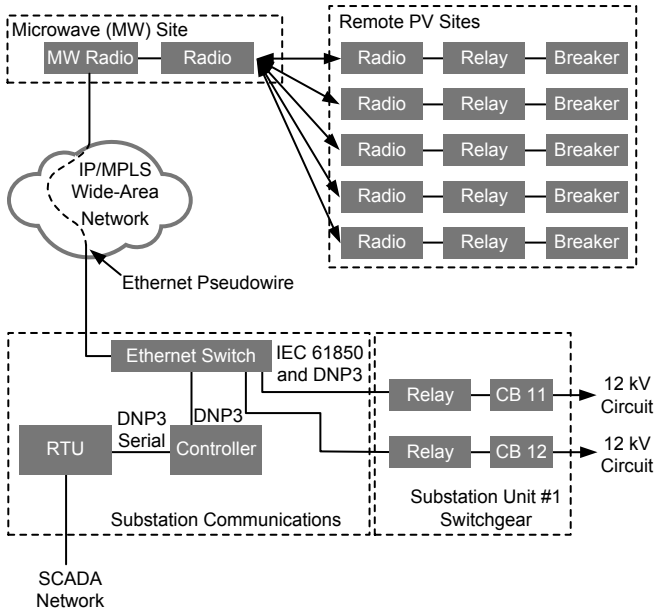

Fig. 14. Substation Topology

Previous projects with similar communication via DERs used MIRRORED BITS communications serial protocol to send transfer trips to the PV system breakers and used DNP3 protocol to bring back statuses, watts, and VARs. MIRRORED BITS communications is a fast serial protocol that is limited to two interfaces per relay. Because of this limitation, IEC 61850 GOOSE was selected for its ability to scale up the number of interfaces for the remote sites. DNP3 was maintained for SCADA.

B. Application of GOOSE and DNP3 Protocols

The project objectives were to provide SCADA monitoring of the PV system watt and VAR outputs, breaker statuses, production curtailment, and fast trip of breakers in the event of a fault on the distribution line. These data are transported over Ethernet using an IP/MPLS fiber network and microwave channels and then over unlicensed ISM-band radios to the five PV sites. The initial settings selected, including an 8-millisecond rate for GOOSE messages, resulted in dropped packets and communications alarms. A bench test was developed to study the cause of the dropped packets and alarms more closely, and the results are shared in Fig. 15 through Fig. 17. The three cases had the following protocol and message rate combinations:

- GOOSE messages every 8 milliseconds and DNP3 messages (original settings).
- GOOSE messages every 20 milliseconds and DNP3 messages.
- GOOSE only and no DNP3 messages.

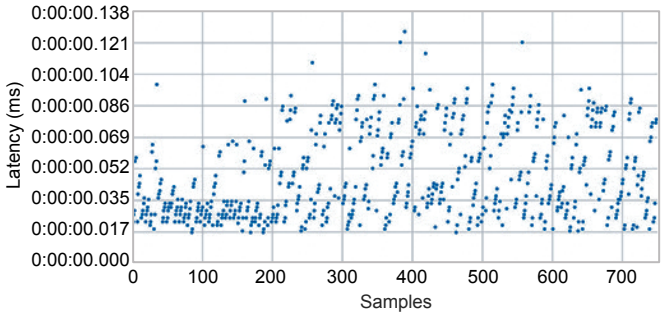

Fig. 15. Round-Trip Latency With GOOSE Messages Every 8 ms and DNP3

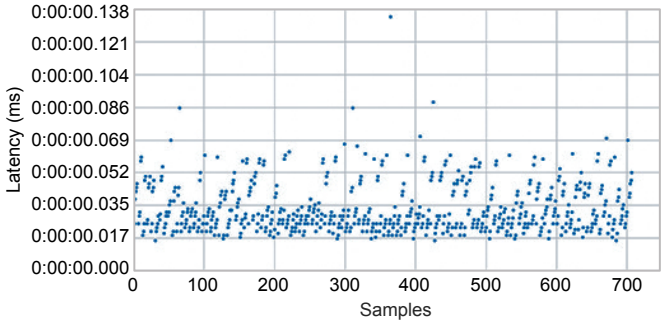

Fig. 16. Round-Trip Latency With GOOSE Messages Every 20 ms and DNP3

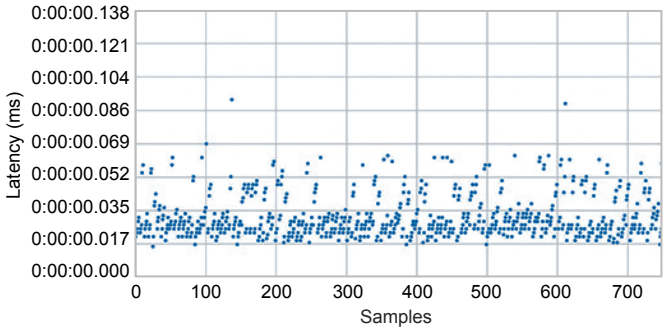

Fig. 17. Round-Trip Latency With GOOSE Messages Every 20 ms and No DNP3

The cases showed that the longest latencies were recorded when the GOOSE message rate was 8 milliseconds. When the time between GOOSE messages was increased to 20 milliseconds, the latencies were more closely grouped—similar to those latencies seen when no DNP3 messages were sent. By adjusting the message rate setting, it was possible to send all the necessary information for all five sites using the radios.

VII. Cost Summary

Fiber-optic communication is the preferred method for protection and control among utilities; however, fiber can be very expensive. Installing fiber on poles is less expensive than burying fiber underground. In most cases, the installation of fiber can be challenging depending on terrain.

A 20-mile fiber installation can cost approximately $65,000 [2]. For the same 20-mile link, a pair of unlicensed ISM radios, antennas, and transmission cables costs approximately $4,500. The benefit of using radios is not only the equipment costs; radios can also save time with fast deployment.

VIII. Conclusion

Radio communication is a cost-effective and reliable solution for extending protection and control networks. When properly studied and designed, radios provide security and dependable communications in both point-to-point and point-to-multipoint topologies using both serial and Ethernet protocols. Radio communications have been studied and successfully deployed in distributed generation applications. Considering the information and guidelines in this paper can assist in determining whether a cost-effective radio solution can be used in the place of fiber-optic communications.

IX. References

[1] M. Arora, "How Secure Is AES Against Brute Force Attacks?" *EETimes*, May 2012. Available: http://www.eetimes.com/document.asp?doc_id=1279619.

[2] S. V. Achanta, B. MacLeod, E. Sagen, and H. Loehner, "Apply Radios to Improve the Operation of Electrical Protection," proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

X. Biographies

Tom Bartman joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2006 as an engineering technician for industrial system products. He is now an application specialist in communications. Prior to joining SEL, he served in the U.S. Navy as an electronics technician with an emphasis on avionics and secure communications. After leaving the Navy, he worked for Harris Inc. as an electronics engineer in the broadcast communications division. He has a degree in applied computer science, is a member of ISSA and $(ISC)^2$, and obtained his Certified Information Systems Security Professional (CISSP) certification in 2013. Tom holds a patent for validation of arc-flash protection.

Ben Rowland received his B.S. in engineering management with an emphasis in electrical engineering from Gonzaga University in May 2014. Upon graduation, he began working for Schweitzer Engineering Laboratories, Inc. (SEL) as an associate application engineer. Ben currently holds the position of product manager for SEL precise time and wireless communications products.

Laura Rogers received her B.S. in Electrical Engineering from Cal Poly San Luis Obispo and Masters in Electrical Engineering from UC Santa Barbara. She worked in aerospace and defense for Hughes and in remote monitoring systems at the University of Hawaii before joining Hawaii Electric Light where she designs substations, communications systems, relay protection and SCADA systems, and interconnections for renewable energy projects. She is a licensed PE in Hawaii.

Previously presented at the 2018 Texas A&M Conference for Protective Relay Engineers and the 2019 IEEE Rural Electric Power Conference.

20190215 • TP6817-01