Resilient Communications Using Various Innovative Wireless Network Topologies

David Dolezilek and Amandeep Kalra
Schweitzer Engineering Laboratories, Inc.

Original edition released March 2018

Resilient Communications Using Various Innovative Wireless Network Topologies

David Dolezilek and Amandeep Kalra, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—As information and control systems continue to grow in size, complexity, and capability, utilities rely more heavily on coordinated processes supported by digital communications. Often, each overlapping control scheme requires dependable, reliable, and fast signal exchange with low latency. Mission-critical applications designed for zero data loss require fast detection and isolation of faults within the communications network and the rapid reconfiguration and reestablishment of message delivery. Dual primary paths provide simple and cost-effective parallel signal delivery. As applications grow more numerous, wireless technology is growing in popularity as a physical layer for the communications backbone due to the high cost of using optical fibers. Unfortunately, and unknowingly, existing wireless Ethernet technologies, designed to support SCADA, introduce far too much latency to support high-speed signal exchange for protection and automation applications.**

The ability to blend multiple protocols, including high-speed data exchange via GOOSE and MIRRORED BITS® communications messages, over a single link creates a wide range of solutions for high-speed automatic control. When engineered correctly to meet signal exchange specifications, wireless serial and Ethernet communications networks increase the performance and capability of automation systems for electric power, water/wastewater, and other critical infrastructures.

This paper discusses the performance comparison of wireless serial and Ethernet communications and innovative wireless network topologies that maximize overall network performance during realistic field conditions. Techniques for simple and inexpensive dual primary data paths are described that provide zero data loss, even during the failure of a radio or communications path. The paper discusses the following:

- **Challenges involved in implementing wireless communications in terms of reliability, dependability, and availability.**
- **Performance comparison between wireless signal exchange methods.**
- **Multiple redundant wireless network topologies for dependable communications.**
- **Best engineering practices for serial and Ethernet wireless networks.**

I. INTRODUCTION

With the advancements in wireless technology and its cost-effectiveness, wireless communications solutions are gaining popularity in rural areas and emerging economies. This paper discusses the various challenges, constraints, and benefits of wireless communication solutions. Additionally, this paper discusses possible topologies to set up resilient communications for various automation applications.

Many automation applications, including industrial applications, use radio communications networks and protocols such as DNP3 or Modbus® to communicate between remote devices and a centralized SCADA system. The client-server protocols support data acquisition and communicate control messages from the centralized SCADA client to the remote devices [1]. In power system applications, radios are used in distribution automation, distributed generation, and as a backup for other primary schemes because of the obvious advantages of easier deployment, simpler planning, and greater cost-effectiveness over hardwired connections.

II. SERVICE LEVEL SPECIFICATION

Users must identify important metrics—key performance indicators—to measure before the system installation to quantify the acceptable level of performance and determine when the installation has met the application requirements. These key performance indicators include latency and reliability and availability.

A. Latency

Minimizing latency is critical for applications requiring high-speed operation. Most radios available today are not suited for low-latency and large data exchange applications. Moreover, these radios buffer data to overcome channel unavailability issues. These buffering mechanisms can lead to out-of-sequence message reception when dealing with applications such as transfer trip schemes that require high-speed IEC 61850 GOOSE message exchange. The out-of-sequence message reception can eventually lead to expiration of time to live (TTL) on the subscriber side, resulting in undesired operations. Modern wireless technology has a feature to disallow buffering to support high-speed protocols.

Due diligence must be done in terms of assessing radio latency, supported protocols, and operating modes during the selection of radios. Spread-spectrum radios have variable latency depending on the radio design. It is good to understand the maximum and minimum latency of a selected radio along with the radio's latency standard deviation to understand the performance of the radio network.

B. Availability

The availability of a network is defined by the ratio of the duration of time the network allows packet exchange to the total amount of time the radio is transmitting data. The availability of a wireless network is much more susceptible to extraneous factors such as magnetic interference, weather, or noise signal interference on the radio frequency. Whereas in wired networks, latencies are consistent for a specific data exchange path and less susceptible to variance because of extraneous factors. The calculation of availability must be made for each protocol because one protocol serving one application might

have different requirements and will depend on the speed of the message exchange. For example, MIRRORED BITS® communications can publish messages every 4 ms, which is the equivalent of 250 messages per second. Now, if the channel is unavailable for less than 4 ms so the receiver receives only 249 messages, that means the protocol availability is 249/250 • 100 = 99.6%. But if the devices exchange messages every 50 ms, the same test with different a protocol will provide a different availability percentage. Also, availability must be evaluated for long-term operation, and typically, longer periods of successful operation yield higher availability. Just like latency, availability calculations are determined by the application itself. For distribution network automation applications, the widely accepted requirements of wireless availability are from 95 to 99.95 percent [2][3].

C. *Cybersecurity*

With increasing threats of cyberattacks on mission-critical infrastructure, it is very important to consider the built-in security features of wireless networks. Wireless networks are prone to various attacks, such as denial of service and spoofing, and have a wider attack surface than wired networks due to the dependence of wireless networks on extrinsic factors. Cybersecurity is not only a requirement for compliance to regulations but is also directly related to the dependability of the network. Radio link security is not only dependent on the error detection capabilities but also on the type of protocol used. Simply stated, the cybersecurity of a wireless system can be defined as the ability of a link to properly operate when called upon and not operate when not called upon.

III. WIRELESS SIGNAL EXCHANGE METHODS

Various industrial and nonindustrial communications protocols are available to exchange information between geographically distributed devices over wired and wireless networks. However, the application requirements eventually determine the type of protocol that should be used. The communications protocols can be defined in two categories.

First are client-server protocols, also called master-slave protocols. With these protocols, multiple sites exchange information based on command-response philosophy with one centralized station acting as the client. These protocols do not have the ability to support high-speed information exchange between sites. The protocols that work with client-server connections include DNP3, Modbus, IEC 61850 MMS.

The second type of protocols is peer-to-peer protocols. These protocols allow the high-speed bidirectional exchange of information. The protocols that fall under this category include MIRRORED BITS and GOOSE communications. MIRRORED BITS communications is a serial-based, purpose-built protocol technology.

Another peer-to-peer message exchange protocol that works in a similar fashion to MIRRORED BITS communications, but for Ethernet-based networks, is GOOSE protocol (described in the IEC 61850 suite of protocols) and also referred to as Generic Substation Event (GSE). In comparison with MIRRORED BITS communications, the GOOSE message exchange has a very large protocol overhead even though it was created to support applications that require high-speed peer-to-peer communications. Because GOOSE is an Ethernet-based protocol, even messages with small payloads require the full Ethernet frame components, including source address, destination address, network logistics, and error checks. The components add up to a total of 133 bytes, regardless of the payload. This overhead varies depending on the size of various parameters of the GOOSE message, such as GOOSE ID, IED name, data set name, and control block name. Hence, GOOSE message configuration requires proper engineering to ensure payloads are as small as possible for fast message exchange. The IEC 61850 GOOSE communications protocol allows the exchange of both binary and analog values and is categorized in various categories, such as P1 and P2/3, depending on the performance and message exchange speed.

Both types of protocols (client-server and Ethernet-based) have their advantages and should be selected depending on the application. All the mentioned protocols work on both wireless and wired networks because only the physical layer (Layer 1) is changed per the Open Systems Interconnection (OSI) model. For example, if an application requires high-speed decision making, then peer-to-peer protocols over a wired network might be a good choice. However, if an application requires fast message exchange over mountainous terrain, then a wireless peer-to-peer protocol could be the solution. If a large amount of data must be exchanged, then client-server protocols would be a good choice over either a wired or a wireless network.

IV. WIRELESS COMMUNICATIONS NETWORK CHALLENGES

Integrating geographically distributed IEDs over a wired network is very challenging, and integrating IEDs over a wireless network becomes harder if proper engineering and best practices are not followed. The application requirements should be kept in mind when determining the type of infrastructure to use. System designers must consider feasibility, the importance of data, and the cost [3].

A. *Line of Sight*

For reliable radio communications, there must be a direct line-of-sight path between the transmitting and receiving radios. Sometimes it can be challenging to get a clear line of sight, depending on the geographical location of the transmitting and receiving stations. Line of sight affects the channel availability and may result in nondeterministic signal exchange with variable performance in terms of speed and latency.

B. *Variable Latency*

Unlike wired communications, wireless communications are more prone to interference from external sources. Moreover, while using repeaters to extend the distance of signal exchange, additional per-hop latency can affect the performance of the system.

V. Wireless Network Topologies

Traditionally, a client-server polling scheme requires that the SCADA radio at the client communicate directly with each remote SCADA radio, one at a time [4]. All the following described topologies are possible with both serial and Ethernet radios for serial and Ethernet communications protocols, respectively.

A. Point-to-Point Topology

A point-to-point system, as shown in Fig. 1, consists of two radios facilitating a message exchange between end devices using a communications protocol. This is the simplest wireless topology and it uses directional antennas at each end. In this scheme, each radio pair is exchanging information independently. However, to increase the distance between the two radios connected to end devices, a repeater radio can be used as shown in Fig. 2. The repeater radio can have either two directional Yagi antennas, one pointing toward the transmitting radio and the other toward the receiving radio, or an omnidirectional antenna. Using radios in a point-to-point link is a cost-effective way to provide secure remote communications without the need to trench fiber, rely on unreliable phone networks, or deal with network availability issues on cellular networks.

Fig. 1. Point to Point

Fig. 2. Point to Point With Repeater

B. Point-to-Multipoint Topology

A point-to-multipoint system consists of one radio acting as a client and communicating to several server radios. Fig. 3 shows a typical recloser restoration scheme using recloser controls over a wireless communications link. In this scheme, all the recloser controls are exchanging information to a real-time distribution automation controller located in the control house. The wireless link provides SCADA, engineering access, and control to restore unfaulted feeder sections.

Similar to point-to-point topology, a repeater station can be used to increase the distance between one or more client-server connections in a point-to-multipoint topology, as shown in Fig. 4.

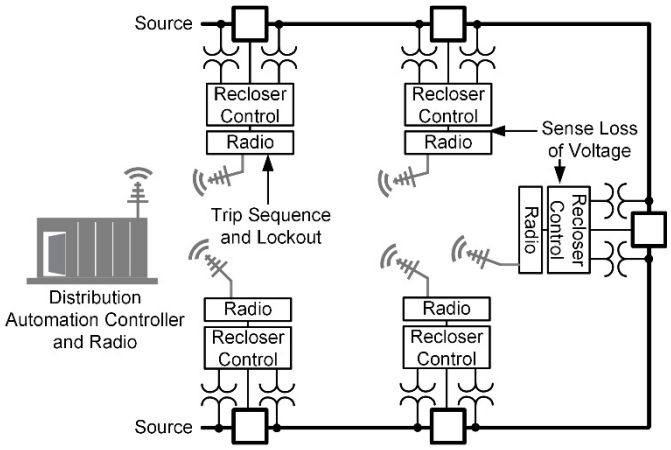

Fig. 3. Point to Multipoint

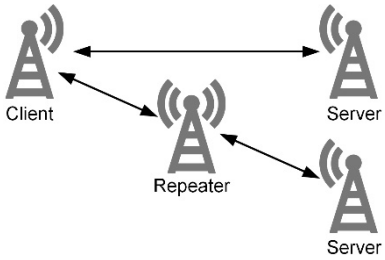

Fig. 4. Point to Multipoint With Repeater

C. Ring Topology

A ring topology enables bidirectional data flow between sites. Messages are repeated at each site and travel around the ring in both directions [1]. As shown in Fig. 5, IED 1, IED 2, and a data concentrator exchange information among each other using wireless ring topology. Ring topology also supports peer-to-peer messages between sites in both directions. This topology is possible with both serial and Ethernet radios. When using serial radios in this topology, they must support multiple ports. For Ethernet radios, a managed Ethernet switch is required to prevent logical looping [5]. The multiple ports on advanced serial radios support simultaneous Mirrored Bits communications and SCADA protocols, such as DNP3, to multiple sites located far away from the central site. This simplifies site-to-site path studies, installation, and communication with sites that do not have a direct line of sight to the central site.

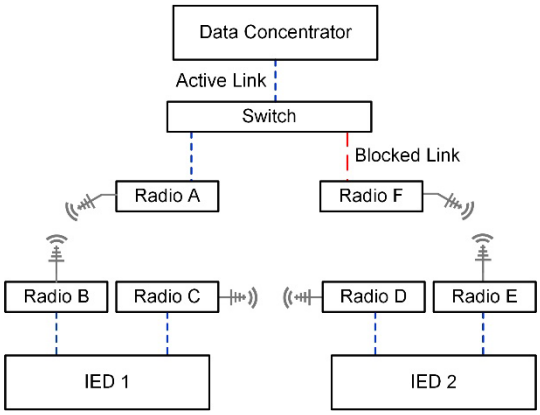

Fig. 5. Ring Topology

With MIRRORED BITS communications and serial radios, protection signals are sent in two directions to two different subscribers. The second subscriber uses logic to forward this protection signal to the first subscriber as contents in a MIRRORED BITS message created by the second subscriber. In this way, if the link from the publisher to the first subscriber fails, the protection signal is still delivered via the path through the second subscriber. This communications method is also used for protection signals going to the first subscriber where local logic forwards them to the second subscriber as contents of a MIRRORED BITS message. This solution requires receipt, logic processing, and republishing of protection signals at each device.

When using GOOSE and Ethernet radios, protection signals are sent in two directions to two different subscribers. The second subscriber then processes and forwards the original data from the GOOSE message to the first subscriber. In this way, if the link from the publisher to the first subscriber fails, the original GOOSE message, containing the protection signals, is delivered via the path through the second subscriber. This solution does not require the logic processing and republishing of protection signals at each device. The data from the original GOOSE message, or more than one, is published in each direction and is repeated to each device.

The advantages of the ring topology include the following [1]:

- A redundant and resilient communications link between a client and the server with fast failover from the primary path to the backup path in case of path failure. This provides data flow redundancy for SCADA protocols and provides more reliable communications than simultaneous bidirectional MIRRORED BITS communications over two channels.
- Accessibility for technicians to diagnose and troubleshoot communications from multiple locations because every radio station can monitor SCADA and engineering access messages to and from every other site.
- Sharing of data load between multiple channels to provide enhanced performance of the communications channels.

The ring topology is a great fit for various control and monitoring applications. The resilient communications enable the reliable support of rapid communications-assisted decision making. A ring topology for control and monitoring applications improves automation system operation, performance, and reliability [1].

D. Multipoint-to-Point Topology

The one other topology that is possible but not very common is a multipoint-to-point link, as shown in Fig. 6. In this topology, the centralized station has one client device connected to multiple radios that are exchanging information between a client device and a field device using multiple point-to-point links. The advantage of using this topology is that each link between the centralized client and the field device is independent of the other links. Advanced serial radios can communicate over multiple radio frequency (RF) channels. To minimize the block error rate of collocated radios, the link between each point-to-point link can have the channel manually set. Also, for Ethernet wireless links, a managed switch can be used at the centralized station to segregate the traffic using VLANs. However, this topology will use $2n$ radios in comparison to $n + 1$ radios for a point-to-multipoint link (where n is the number of remote sites). The user must perform due diligence to select the best topology by comparing the performance and cost of each of the options.

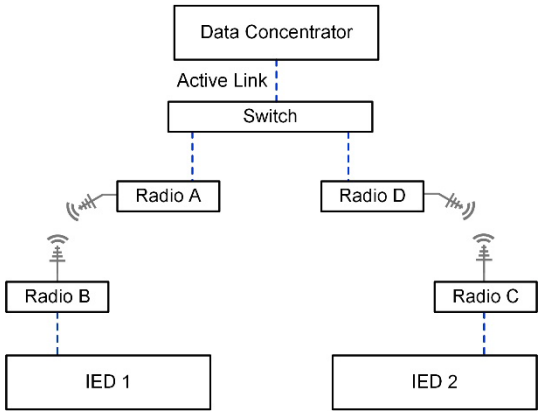

Fig. 6. Multipoint-to-Point Topology

VI. BEST ENGINEERING PRACTICES

As discussed earlier, the peer-to-peer protocols (such as IEC 61850 GOOSE and MIRRORED BITS communications) behave differently and have different requirements from client-server protocols. Using the Ethernet-based IEC 61850 GOOSE communications protocol requires a detailed feasibility study to verify that the application performance requirements can be met with GOOSE over wireless links. System designers must be aware of the various time classes described by the IEC 61850 standard.

As described in the initial paper on this topic [6], digital signal transmission time is essentially the amount of time it takes to get data from one device to another. It begins at the time the publisher detects a change of state and ends when the receiver detects a change of state. The process includes the publisher sending a GOOSE message containing the data change information and the subscriber receiving and decoding the change in the GOOSE message contents [6]. The transfer

time specified for an application is the time allowed for a signal, or two data exchanges, to travel through a communications system. IEC 61850-5 "Communication Requirements for Functions and Device Models" describes transfer time, shown in Fig. 7, as the time between the action of communicating a value from the logic processing of one device to the logic processing within a second device as part of an application [7]. Transfer time includes the transit time and the time it takes to execute the communications-processing algorithm, which encodes the message in the source physical device (PD) and decodes the message in the destination PD. The transit time is the time it takes for the message to travel through the communications network.

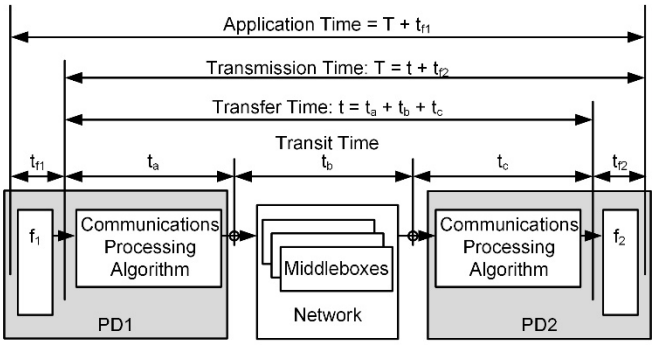

Fig. 7. Transmission Time and Transfer Time Based on IEC 61850-5

The IEC/TR 61850-90-4 network engineering guidelines clarify performance and test requirements and are considered by some to be the most important enhancement among those collectively known as IEC 61850 Edition 2. Of note, they simplify the discussion of transfer time requirements by documenting time classes for different types of messages and their associated transfer times, as shown in Table I. These guidelines allow network engineers to accurately specify and design LANs to satisfy a transfer time class without needing to understand the underlying protection and automation applications [8].

TABLE I
IEC 61850 TRANSFER TIME CLASSES [8]

Transfer Time Class	Transfer Time	Application Example
TT0	>1,000 ms	Files, events, and log contents
TT1	1,000 ms	Events and alarms
TT2	500 ms	Operator commands
TT3	100 ms	Slow automatic interactions
TT4	20 ms	Fast automatic interactions
TT5	10 ms	Releases and status changes
TT6	3 ms	Trips and blockings

To achieve the times in Table I, best engineering practices must be followed. They include:

- Performing due diligence to select the best topology as per the application requirements.
- Completing a simulated radio path study to estimate the availability, reliability, and approximate line of sight for the selected topology.
- Lab testing with clear line of sight to set up the reference for field installation for each radio link.
- For collocated radios, manually selecting radio channels with the largest spacing possible between channels.
- Completing a field path study to verify the field performance with the real-world setup. Some corner cases could be missed in the simulated radio path study.
- Select appropriate antennas for each site to achieve the required level of performance.
- Installing the antennas at appropriate heights to get the best signal reliability and with minimum interference.

Like wired Ethernet networks, it is recommended to validate correct reception of Ethernet packets. As described in [5], because protection and automation message packets are often multicast to numerous subscribers, it is necessary to monitor the receipt of each packet at each receiving subscriber. Ethernet packet messages for protection and high-speed automation signal transfer include GOOSE, Sampled Values (SV), and line current differential (87L).

To validate GOOSE subscriptions, each subscribing device maintains and produces information about the message configuration and the real-time performance of the incoming GOOSE subscriptions. The publisher calculates and stores information for each of the GOOSE messages being published. This information is available in a human-readable format report via an engineering access connection and via a poll-and-response interaction with a data concentrator. The subscriber uses the following GOOSE message configuration information to validate that the GOOSE message is from the intended publisher and matches the engineered subscription design. GOOSE messages that do not match a pre-engineered configuration are discarded. The GOOSE receipt message report contains the following information:

- Message configuration information, including:
  - GOOSE control reference.
  - Multicast address (media access control [MAC]).
  - AppID data set reference.
- Message status, which includes:
  - Priority tag. This is the priority tag value received in the last message. If the priority tag is not received as part of the GOOSE message and is unknown, then the report will indicate that it was not received as part of the packet header. The report must avoid confusion between a received value of zero and a nonexistent tag.

- VLAN. This is the VLAN value received in the last message. If the VLAN value is not received as part of the GOOSE message and is unknown, then the report will indicate that it was not received as part of the packet header. This is done to avoid confusion between a value of zero and a nonexistent VLAN.
- State number. This is the state number value received in the last message.
- Sequence number. This is the sequence number value received in the last message.
- TTL. This value is updated with the expected remaining TTL in milliseconds, which represents the expected time duration before receipt of the next GOOSE message in this specific subscription.
- Error code. The report calculates and displays warnings and error conditions defined by IEC 61850, which include the following:
    - GOOSE configuration revision mismatch, meaning the configuration revision number of the incoming GOOSE message does not match the value as configured in the Configured IED Description (CID) file.
    - GOOSE commissioning is necessary, meaning the "needs commissioning" flag is set to true in the incoming GOOSE message.
    - GOOSE message received out of sequence, meaning that the consecutively received message state numbers and/or message sequence numbers are not in sequence.
    - GOOSE message received corrupted, meaning that the format of the incoming GOOSE message is not as configured, is incorrectly encoded, or is otherwise corrupted.
    - TTL has expired, meaning that a GOOSE message for this subscription was not received within the expected time interval.
- Out-of-sequence count. This is the count of messages lost because of both sequence number and state number out-of-sequence errors. It is not recorded for the first message after the device is turned on or reconfigured.
- Time to live count. This is the count of the number of times a message is not received within the expected time interval, referred to as the TTL.
- Decode error count. This is the count of the number of messages where enough information is decoded to associate them with a subscription, but it fails further decoding because of corruption or errors, such as a mismatched data set.
- Buffer overflow count. This is the count of the number of messages that are discarded because the message receive queue was full. This may occur as a result of time compression in the network that causes two packets from the same subscription to be received within one publication period. The receiving IED should discard the older packets for this subscription and process only the newest one.
- Message lost count. This is the aggregate count of the estimated number of messages lost because of out-of-sequence errors. For each out-of-sequence error, the number of messages lost is estimated by subtracting the expected state number from the received state number and the expected sequence number from the received sequence number and summing them. This estimate is only made if the state number or sequence number in the received message is greater than expected.
- Maximum message lost count. This is the maximum estimated number of messages lost for an out-of-sequence error.
- Total downtime. This is the total time (in seconds) the subscription was in an error state.
- Maximum downtime. This is the maximum time (in seconds) the subscription was continuously in an error state.
- Message status history. The GOOSE report maintains statistics for several of the most recent error events, including date of event, time of event, duration of event, and event error code [4].

VII. Application Examples

In this section, we discuss the advantages of using innovative radios in a ring topology for power system distribution automation and for a water flow management system.

A. Distribution Network Automation

The complexity of the power system is increasing day by day, including increasing integration of distributed generation, including renewable sources. Unlike in the past, multiple distributed generation sites and distributed electrical loads complicate the power system. It is very important for multiple sites to be aware of the health of each other via high-speed, resilient communications.

Wireless technology is very effective at integrating remotely located recloser controls with a centralized distribution automation controller, as shown in Fig. 8. In this scenario, the distribution automation controller in the control house shares information between multiple recloser control sites in a wireless ring topology. Each site has a radio pair installed next to control

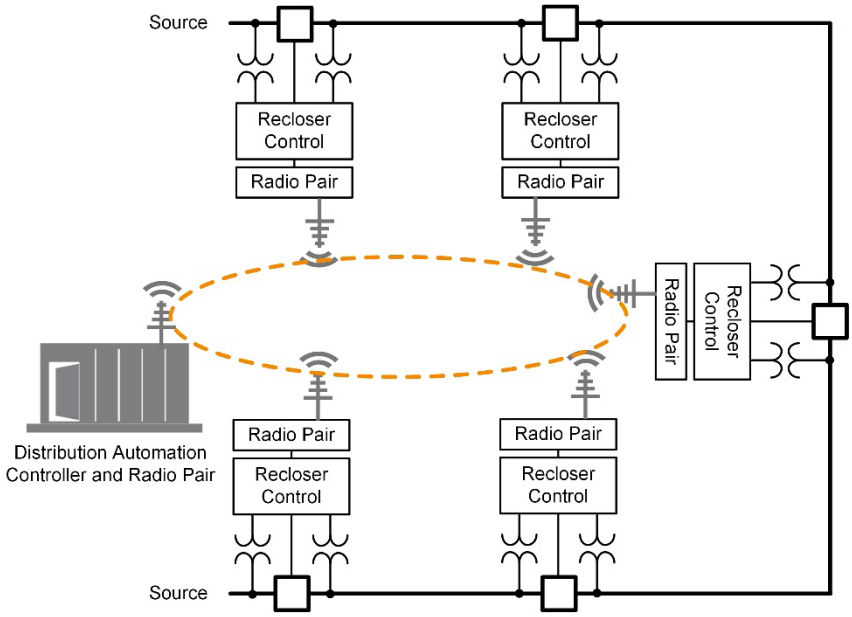

Fig. 8. Using Radios in a Ring for a Smart Recloser Control Application

or monitoring devices to allow message exchange in the wireless ring topology. This topology provides a resilient communications link between sites.

Using high-speed radios in a ring provides the following benefits [1]:

- Early detection of communications and process failures at each site and adjacent sites.
- Ability to create and store typical process data to permit future comparisons to detect abnormalities.
- Timely detection of abnormalities in the process to alert end users of channel failure and trigger condition-based maintenance.
- Automatic reaction to data from any site to trigger fail-safe or preventative actions.
- Improvement of troubleshooting and diagnostic calculations and reduction of calculation time because data are shared between sites over multiple channels.
- Improvement of operational efficiency by decreasing the application downtime and improving processes with system-wide situational awareness.

B. Water Flow Management System

Wireless communications links are very popular in water management applications. In the following example, radio pairs are configured to work in a ring topology for water flow monitoring and water flow control stations, as shown in Fig. 9. In this setup, radio pairs connected and collocated with centralized server stations act as masters. The rest of the radio pairs act as pass-through repeaters to complete the ring. Using this topology for a water flow management system has the following advantages:

- Early detection of water canal flow blockage and leakage.
- Detection of abnormal water loss to alert end users to canal failure and trigger condition-based maintenance of the water canals.
- Improved troubleshooting and diagnostic calculations and reduced calculation time because data are shared between sites over multiple radio channels.
- Prevention of water canal over-flooding by generating alarms for mismatched water flow among interconnected open canals. This prevents damage to gate structures, motors, and crops.
- Improved gate position selection by using both local gate head differential and the changes in flow rate at the upstream intake point and turnouts. Knowledge of the changing upstream water flow rates permits prediction and preparation of changes to flow rate at the local gate [9].

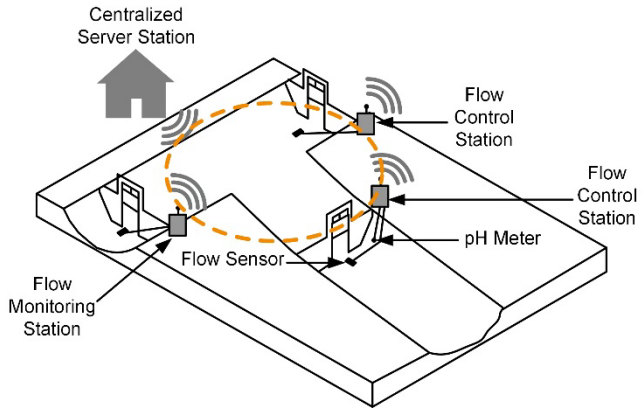

Fig. 9. Water Flow Management System [9]

VIII. CONCLUSION

Wireless communications are a very cost-effective solution to facilitate the exchange of information between geographically distributed locations. Using innovative topologies and best engineering practices, wireless technology performance can be drastically improved. Moreover, using

various tools, the performance of the wireless radios can be quantified to improve the user's confidence in these solutions.

IX. References

[1] D. Dolezilek, E. Sagen, and A. Kalra, "Using the SEL-3031 in a Dual High-Speed Hop-Sync Ring," SEL Application Note (AN2013-22), 2013. Available: https://www.selinc.com.

[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.

[3] F. Stewart, R. Pylant, and R. Baldevia, Jr., "Case Study: Utilizing Ethernet Radios and Communications Processors to Integrate Remote IEDs," proceedings of the 9th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2007.

[4] D. Dolezilek, J. Dearien, and M. van Rensburg, "Lessons Learned and Successful Root Cause Analysis of Elusive Ethernet Network Failures in Installed Systems," proceedings of the International Conference and Exhibition – Relay Protection and Automation for Electric Power Systems, St. Petersburg, Russia, April 2017.

[5] D. Dolezilek, J. Dearien, A. Kalra, and J. Needs, "Appropriate Testing Reveals New Best-in-Class Topology for Ethernet Networks," proceedings of the 13th International Conference on Developments in Power System Protection, Edinburgh, UK, March 2016.

[6] D. Dolezilek and J. Dearien, "Lessons Learned Commissioning and Analyzing Data from Ethernet Network Installations," proceedings of the 5th International Scientific and Technical Conference, Sochi, Russia, June 2015.

[7] IEC/TR 61850-90-4, Communication Networks and Systems for Power Utility Automation – Part 90-4: Network Engineering Guidelines.

[8] IEC 61850-5, Communication Networks and Systems for Power Utility Automation – Part 5: Communication Requirements for Functions and Device Models.

[9] D. Dolezilek and A. Kalra, "Power Management and Automation Scheme for Water Canal Networks," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2013.

X. Biographies

David Dolezilek is the international technical director at Schweitzer Engineering Laboratories, Inc. and has three decades of experience in electric power protection, automation, communication, and control. He leads a team that develops and implements innovative solutions to intricate power system challenges and teaches numerous topics as adjunct faculty. David is a patented inventor, has authored dozens of technical papers, and continues to research first principles of mission-critical technologies. Through his work, he has created methods to specify, design, and measure service level specifications for digital communication of signals, including class, source, destination, bandwidth, speed, latency, jitter, and acceptable loss. As a result, he helped coin the term operational technology (OT) to explain the difference in performance and security requirements of Ethernet for mission-critical applications versus IT applications. David is a founding member of the DNP3 Technical Committee (IEEE 1815), a founding member of UCA2, and a founding member of both IEC 61850 Technical Committee 57 and IEC 62351 for security. He is a member of the IEEE, the IEEE Reliability Society, and several CIGRE working groups.

Amandeep Kalra is an application engineer II with Schweitzer Engineering Laboratories, Inc. (SEL) in Lynnwood, Washington, with several years of experience in designing automation systems and secure communications networks. He has authored numerous technical papers focusing on IEC 61131-based automation controllers, secure Ethernet networks, cybersecurity, and Ethernet-based communications protocols as well as IEC 61850 communications standards. He is a patented inventor and has represented SEL at various international conferences and IEC 61850 interoperability demonstrations organized by UCA and frequently teaches engineering design and application of IEC 61850 solutions. He has a bachelor of technology degree in instrumentation and control engineering from the National Institute of Technology, India, and a master's degree in electrical engineering from California State University, Northridge.