Cybersecurity of wireless communications for protection and control applications

Shashi Sastry, Galina S. Antonova, Steven A. Kunsman, Hitachi ABB Power Grids
Email: shashi.sastry@hitachi-powergrids.com

1. Introduction

Wired and wireless communication methods are two ways of transporting data between two or more locations.

There is a perception in the power systems industry that wireless technologies are less secure compared to wired communication since there are no physical barriers that can be secured as in the case of wired systems. Wired systems can be secured within a perimeter with physical security measures (such as secured rooms with limited access) in addition to hardware, software, and system security solutions.

Wireless communication uses air as the medium of communication and hence there are no physical boundaries to secure.

This paper dispels the myths pertaining to lack of security in wireless communication systems and is focused on IEEE 802.11 Wi-Fi and cellular technologies in particular. First, the paper discusses the cybersecurity requirements as they pertain to power system applications. Second, it discusses the general security controls that categorize cybersecurity requirements and third, the general mechanisms available to implement these security controls**[1]**. There is a general tendency to focus on device security instead of adopting a system-level approach to security. While device security is important, this paper shows that a Defense-in-Depth is a recommended approach to system security that covers the entire end-to-end solution, thereby strengthening even the weakest points in the infrastructure.

The topics presented in this paper are inter-related. However, the sections are organized to make it easier to read each section independently. This allows readers to use this paper as a reference and also to skip section with topics that the reader is already familiar with. Note that security in this paper is used in the context of cybersecurity and not in the context of security and dependability generally used in protection concepts. Application examples with the use of wireless communication technologies for power system applications are also provided in the paper.

2. Wireless Communication

Wireless communication refers to the transfer of data over air as the communication medium using *radios waves*.

Radio waves are a type of electromagnetic signals with wavelengths in the electromagnetic spectrum longer than infrared light, with frequency range 30 hertz (Hz) to 300 gigahertz (GHz). The wireless devices have radio transmitters and receivers that generate radio waves to carry data. These radio waves are generated by transmitters to be received by radio receivers, using antennas. Radio waves

are used for fixed and mobile radio communication, broadcasting, radar and radio navigation systems, satellite communications, wireless computer networks and many other applications.

Wireless communication technology is categorized into different types depending on the frequency, range, distance of communication, data bandwidth, and the type of devices used. The following are the different types of wireless communication technologies.

1. Radio and Television Broadcasting
2. Radar communication
3. Satellite communication and Global Navigation Satellite Systems (GNSS), e.g., Global Positioning System (GPS)
4. Cellular communication
5. 802.11 WiFi
6. Bluetooth

The focus of this paper is Wi-Fi which is IEEE 802.11**[2]** and cellular technologies, as these are more commonly applicable to power system applications.

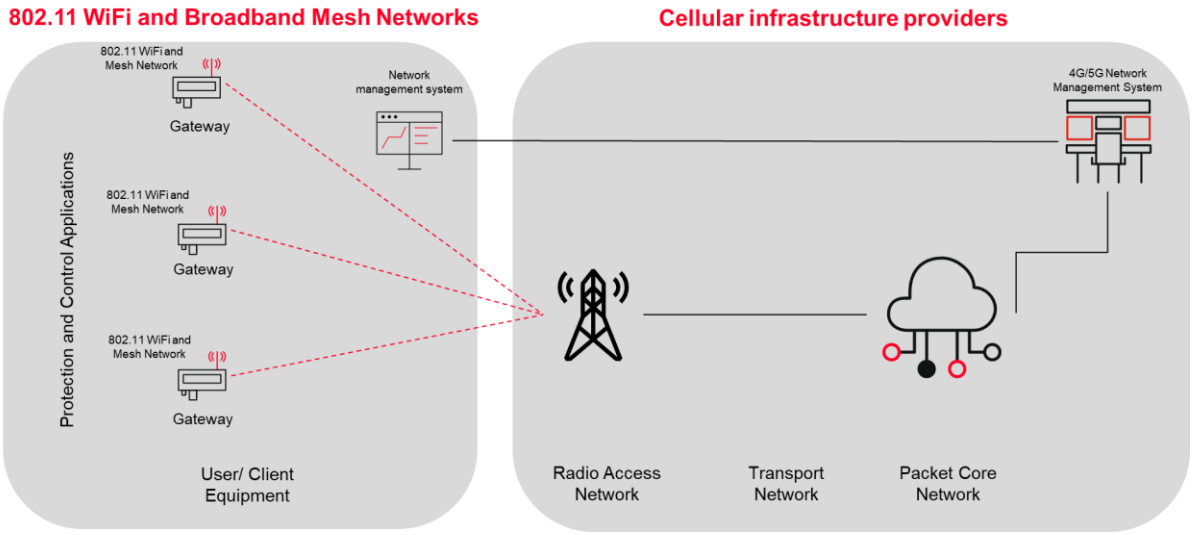

Figure 1: A Typical 802.11 WiFi, Broadband Mesh and Cellular Network

2.1. Wi-Fi

"Wi-Fi" is the common name for the technology specified by the IEEE 802.11 series of standards commonly used for creating wireless Local Area Networks (LANs). A Wi-Fi device creates a local network by broadcasting over pre-defined channels in unlicensed frequency range (2.4GHz or 5.8GHz). It is primarily a short-range local (few hundred feet of coverage area) local area wireless networking technology and it is possible to setup a network without a connection to the Internet. The Internet connection may be over an Ethernet cable, Digital Subscriber Line (DSL) modem, satellite, cellular or even another Wi-Fi network. To create multiple channels in an allocated 2.4 GHz or 5.8 GHz frequency band, Orthogonal Frequency Division Multiplexing (OFDM) is used. The variants of IEEE 802.11 standard specify different number of channels, channel width, interference distances, and so on. The different Wi-Fi standards are IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE

802.11ac and IEEE 802.11ax. The IEEE 802.11 standard itself was the first standard developed to operate in the 2.4 GHz Industrial, Scientific, and Medical (ISM) radio band. The IEEE 802.11a standard followed with support for the 5.8 GHz frequency band with faster speeds but a shorter range. Subsequent standards IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n increased data rates, coverage, and reliability with a reduction in interference as the radio technology hardware improved substantially. The popular newer standards are IEEE 802.11ac and IEEE 802.11ax (also known as Wi-Fi 6 or High-Efficiency WLAN). Wi-Fi 6 also includes a sub-category called Wi-Fi 6E (E for Extended) that uses less congested frequency bands.

2.2. Cellular

Cellular is a long-range Wide Area Network (WAN) wireless technology compared to Wi-Fi. When using cellular data, Internet access can be provided via a connection to a cell tower that might be within line-of-sight or perhaps as far as 20 miles away. That cellular tower usually has a high-speed connection to the Internet.

Cellular technology is becoming increasingly popular. The most common use for cellular technology is to provide cellular telephone services, but the cellular network is also being used more and more often by data communication devices such as pagers, personal digital assistants (PDAs), and handheld computers.

Cellular technology is a form of high frequency wireless communication in which antennas are placed strategically throughout a service area. The service area is divided into many cells, each with its own antenna. This arrangement generally provides subscribers with reliable mobile telephone service of a quality almost that of a hardwired telephone system. Users of voice or data services dial or login to the system, and their voices or data are transmitted directly from their telephone to one of these antennas. In this way, the cellular system replaces the hardwired local loop. Each phone service provider uses a different part of the radio frequency spectrum, which is why cell phones designed for one provider's network often won't work on another provider's network. Additionally, different countries use different frequency ranges.

The network of cell antennas is an intelligent system. For example, as a car is driven through the service area, the user equipment, a cell phone in this case, moves away from one antenna and closer to another. As the signal weakens at the first antenna, the system automatically begins picking up the phone's signal at the second antenna. Transmission is switched automatically to the closest antenna without loss in communication.

3. Defense-in-Depth Approach

With the modernization of the utility industry, the addition of sensors, cameras, and newer data collection mechanisms opens up previously closed systems. As more and more data becomes available for predictive and preventive maintenance, implementing the appropriate security measures is key to keeping the machines and data secure. Wireless technologies provide a cheaper, flexible alternative to adding fiber which is expensive to install and maintain. When used in conjunction with a Defense-in-Depth security process, wireless networks provide secure end-to-end connectivity to transport critical application data.

Defense-in-Depth is a cyber security approach that uses layered defense mechanisms to protect systems and data. With layering, if one defense fails, another is there to block an attack. This intentional redundancy creates greater security and can protect against a wider variety of attacks.

Cybersecurity implementation is an ongoing process that needs to cover older infrastructure in addition to the newer devices and continuously evolving methods. New vulnerabilities are discovered every day and existing threats constantly evolve. Humans are prone to making mistakes. No single security mechanism or policy is adequate to meet all cyber security needs of any critical infrastructure. Also, not all security mechanisms are necessary or are available at every layer. Hence, building in layers of security reduces the chance of a single point of failure. A Defense-in-Depth approach to security requires the adoption of a variety of security measures at all layers. Each defensive layer contains multiple controls to mitigate risks.

As new threats become imminent or new devices are made operational, a layered approach makes it simpler and faster to introduce newer tools or measures to prevent these new incursions or additions respectively. As with other communication technologies, there are many widely available mechanisms to implement security controls in wireless communications.

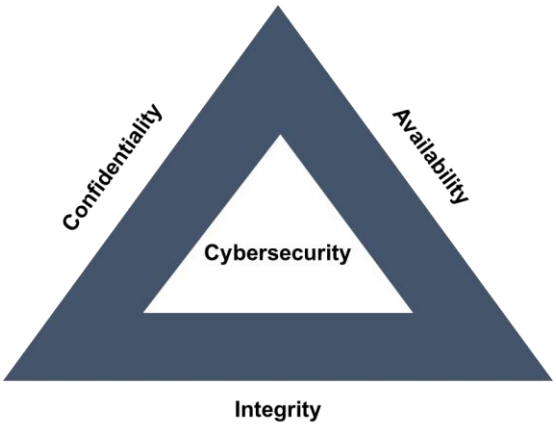

Figure 2: The CIA Triad

Encryption is used to provide confidentiality and maintain privacy both for data in transit as well as data at rest. Any data stored with the wireless device (for example configuration files, system data, and logs) is encrypted and is difficult to access for unauthorized users. All data that is transported using the wireless network is also encrypted. The encryption process should use strong crypto suites as mandated by the respective standards. Encryption is most often used with wireless communication since air is the medium of communication that is not constrained by a physical boundary or perimeter.

Access control to resources is another important aspect of applying security controls to critical resources – network, data, and machines. Humans-to-machine and machine-to-machine access can be limited by authentication and authorization controls such as Remote Authentication Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP). Role-based Access Control (RBAC) is an access-control mechanism defined around roles and privileges. RBAC can be used to enforce the policy of ‘Least Privilege’ as it allows authorized users access to a limited set of resources

that they need to complete their job or tasks and nothing more. RBAC along with RADIUS or LDAP can be used to restrict access to wireless devices (management of the wireless access point or router) as well as other devices that are connected to the wireless communication network.

Authentication is a security control that is used to control who (humans) and what (devices, such as smartphones, laptops, tablets) can connect to the wireless network. There are several ways that authentication can be implemented including and not limited to passwords, security tokens, X.509 or Public Key Infrastructure (PKI) certificates, USB secure keys, and so on. Multifactor authentication is gaining more traction as multiple authentication mechanisms can be combined (passwords, security tokens, RADIUS authentication, etc.) to further restrict only authorized users to have access to the network as well as to the resources connected to that network. Machine-to-machine authentication can be implemented with PKI certificates where supported and this can be used to setup the network elements of the wireless communication network itself.

Almost all wireless network devices provide firewall capabilities and Access Control Lists (ACLs) that are programmed to create segmented areas called zones within the network. Firewall rules are applied to isolate these areas thereby restricting the flow of traffic between the different zones. Access to resources can also be controlled in this manner. Ports or interfaces that are not in use can be disabled physically using configuration commands. The ports can also be programmed to allow only selected application traffic to pass through. This selective access when combined with the user RBAC can restrict access to critical machines and the resources. Furthermore, only authorized users can use secure remote access applications such as Secure Shell (SSH) to remotely access the machines within the network.

Logging provides additional insight and monitoring capabilities for user access and traffic flows. The logs can be sent to an external logging server in a secure manner. Events and alarms are captured using Simple Network Management Protocol (SNMP) Traps and Syslogs. These logs provide historical evidence and can be used as audit trails to observe and further refine access control and traffic flows.

In addition to these mechanisms provided by the wireless communication devices, purpose-built security appliances such as firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are deployed within and between network segments. These security appliances are deployed in other layers of the infrastructure and they strengthen the overall cybersecurity profile of the network.

The security controls provided in a wireless communication network match closely with those in wired networking. The requirements laid out in the cybersecurity standards and the security controls are applicable to wired and wireless networks. In each of the use cases described in this paper, all or some of the security controls can be implemented for the wireless network depending on the application requirements. Based on a risk assessment, the threat levels can also indicate which of the security controls shall be implemented and in which layer.

4. Power Industry Cybersecurity Standards

Cybersecurity standards specify the requirements (the “what”) for protecting the power system infrastructure and applications. At a high level, the standards also list technologies and solutions (the “how”) that enable utilities to meet these requirements following an industry standards approach. As with the enterprise Information Technology (IT) cybersecurity frameworks, there are many standards and models that define the compliance levels for components and communication systems (wired and wireless) specifically for power systems. In fact, power system cybersecurity requirements are starting to merge with the enterprise IT frameworks with the expansion of the digitalization process and the broader use of Cloud-based services. Navigating through the maze of standards, requirements, and solutions can be challenging.

The compliance is greatly assisted by each individual in the organization having at least a basic understanding of the available standards. Educated personnel make better decisions regarding cybersecurity policies for the organization. Humans are considered to be the weakest link in the cybersecurity chain – knowledge will make them the vital link. This is one of the key components of the holistic approach to cybersecurity compliance.

Listed below are a few of the standards that specify requirements that can be used while deploying a wireless communications network. Together they provide a cybersecurity framework for the design and development of secure communication systems:

1. NERC CIP - North American Electric Reliability Corporation Critical Infrastructure Protection**[7][8]**
2. NIST - National Institute of Standards and Technology
3. ISA/IEC 62443 - Standard series for Industrial Network and System Security**[9]**
4. IEEE 1686 - Standard for Intelligent Electronic Devices Cyber Security Capabilities**[10]**
5. IEC 62351 - Standard for Securing Power System Communications**[11]**

It is important to highlight the role of manufacturers of software and systems in the complete lifecycle cybersecurity model. This model encompasses all phases and aspects of product development, starting with the design and development of the hardware, embedded systems, operating system, and drivers right up to the higher layers of applications, networking, user, and management interfaces (command line or graphical). This results in the manufacturing of a secure product – both hardware and software. It also includes the secure software updates to the network device during the operational lifetime of the device.

5. Cybersecurity Compliance - Requirements, Security Controls, and Solutions

The security controls and solutions apply to any communication network including wireless communication systems. These solutions are based on proven techniques in maintaining cybersecurity. As discussed earlier, cybersecurity is a dynamic field with rapidly changing threat models – understanding the basics will prepare individuals for additional learnings if either the requirements or solutions (or both) change. Readers should also note that the standards are generally revised

periodically (IEEE standards are revised every 10 years) and may be amended at any time. Hence, the recommendation is to refer to the latest version of the normative documents.

Wireless communication devices are part of composite protection system and the requirements listed in the standards for the overall protection and control system are also applicable to the wireless communication channels that, in this discussion, use IEEE 802.11 and cellular network devices.

The key security controls that are applicable across different security domains are as follows:

1. Authentication: User-to-device, device-to-device, and user-to-application authentication
2. Access Control: Enforcement of logical security perimeters to prevent unauthorized access
3. Data Integrity: Ensuring the trustworthiness of data in transport and data at rest
4. Confidentiality: Protecting sensitivity and maintaining the privacy of communication as well as data at rest
5. Monitoring and logging: Recording all activities to monitor events and alarms including audit trails
6. Security management: Creating a robust set of cybersecurity policies and procedures to maintain and track equipment, for secure software updates, and key management
7. Availability and robustness: Building a redundant infrastructure to assure high availability of services and systems
8. Data Privacy : Governing how the data is collected, shared, and used

The requirements pertaining to the above security controls are echoed across many different standards. The mechanisms to achieve these security controls can also be applied to any wireless deployment and these controls are listed in Table 1 below.

Table 1: Cybersecurity Requirements

Requirement	**Security Control**	**Solutions**	**Standards**
IED identification and authentication control	Authentication: Human users accessing the wireless device must provide valid credentials to gain access to the device for management purposes. Authorization: Once the user is successfully authenticated, the user is authorized to perform only certain functions on the device. This authorization is based on the job responsibility of the user and is referred to as “role-based“ access control.	All human interfaces must be protected by secure credentials - passwords, tokens, multifactor authentication techniques, and so on. RBAC, RADIUS authentication, Active Directory (AD) or LDAP integration can be used	IEEE 1686 Section 5.1 NERC CIP IEC 62443-4-2 IEC 62351-8

Enforce identification and authentication to support segregation of duties and least privilege	Least Privilege is a policy that assigns certain users, systems, and processes access to resources (networks, systems, and files) that are absolutely necessary to perform their assigned function.	RBAC and RADIUS authentication or LDAP integration.	IEEE 1686 Section 5.1 NERC CIP IEC 62443-4-2 IEC 62351-8
Account management	Management of all accounts locally or centrally is the recommended approach. Users are managed centrally so accounts can be added or terminated using a single application.	Kerberos, RADIUS, LDAP, Active Directory (AD)	IEEE 1686 Section 5.1 NERC CIP IEC 62443-4-2 IEC 62351-8
Enforce password strength checking and password management	Strong passwords must be enforced to prevent brute-force attack. Password policy is enforced by the centralized system in the case of centralized user management.	The wireless device's software can provide this functionality as an inbuilt application. If the authentication is managed by a centralized system, then password policy is enforced by that system.	NIST Special Publication 800-63B NERC CIP IEC 62351-8
Audit Trail	All user actions must be logged for monitoring as well as audit purposes. For example, login and logout actions, configuration and firmware changes, access to the audit logs itself, and so on.	Logs can be transported to an external logging server via: Syslogs SNMP traps	IEEE 1686 Section 5.2 IEC 62443-4-2 IEC 62351-8
Events and Alarms	Events indicate activity that may be occur under normal operations. Alarms are defined as activities which may indicate unauthorized activity or indicate disruptions in normal operations (reboots, unsuccessful logins, etc.)	SNMP Traps	IEEE 1686 Section 5.3 IEC 62443-4-2
Cryptographic Features	Use of secure protocols for data transport and access of the IED itself Strong encryption for remote access and for data transport	Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), SSH,Network Time Protocol (NTP) Simple Network Time Protocol(SNTP), Virtual Private network (VPN) Advanced Encryption Standard (AES) encryption suite	IEEE 1686 Section 5.4 NERC CIP IEC 62443-4-2 IEC 62351-3 (specific for TCP/IP transport layer) IEC 62351-9 (Key Management)

IED Software and Settings	Use of digital signatures and encrypted software ID/Password control for access control of software and configuration updates on the IED device Provide READ-ONLY, READ-WRITE – different levels of access to the IED configuration.	Secure product development lifecycle And supply chain management of hardware and firmware RBAC for configuration management of the IED	IEEE 1686 Section 5.5 IEEE Std C37.231 IEC 62443-4-1
Communication Ports	Enable of disable option on ports such that ports can be shut down or made inactive when not in use especially ports that use TCP or UDP.	Enable/disable unused ports Firewalls to ensure restricted flow of traffic	IEEE 1686 Section 5.6 IEC 62443-4-2
X.509 certificates	Certificate authentication Validity of certificates and revoking of expired certificates	PKI Certificate management with a valid Certificate Authority	IEC 62351-3 Section 5.5 (specific for TCP/IP transport layer) IEC 62351-9 (Key Management)

6. Use of Wireless Communication in Power System Applications

A few application examples are provided in this section. From a cyber security perspective, securing communication from substation to substation (inter-substation communication) is of particular interest. In addition, access to the substation resources is critical to ensure that only authorized personnel can access the resources for maintenance, data collection, or observation purposes.

6.1. R-GOOSE applications with inter-substation communication

To communicate binary and analog data, IEC 61850 technology defined the use of Generic Object - Oriented Substation Event (GOOSE) messages **[3]**. These Layer 2 Ethernet multicast messages are commonly used within an electrical substation for peer-to-peer communications between Intelligent Electronic Devices (IEDs), such as protective relays. Reach of these messages was extended to inter-substation communication with a definition of Routable GOOSE (R-GOOSE) capable of carrying binary and analog data securely between substations. IEC Technical Report (TR) 61850-90-5 first defined the R-GOOSE concept **[4]**.

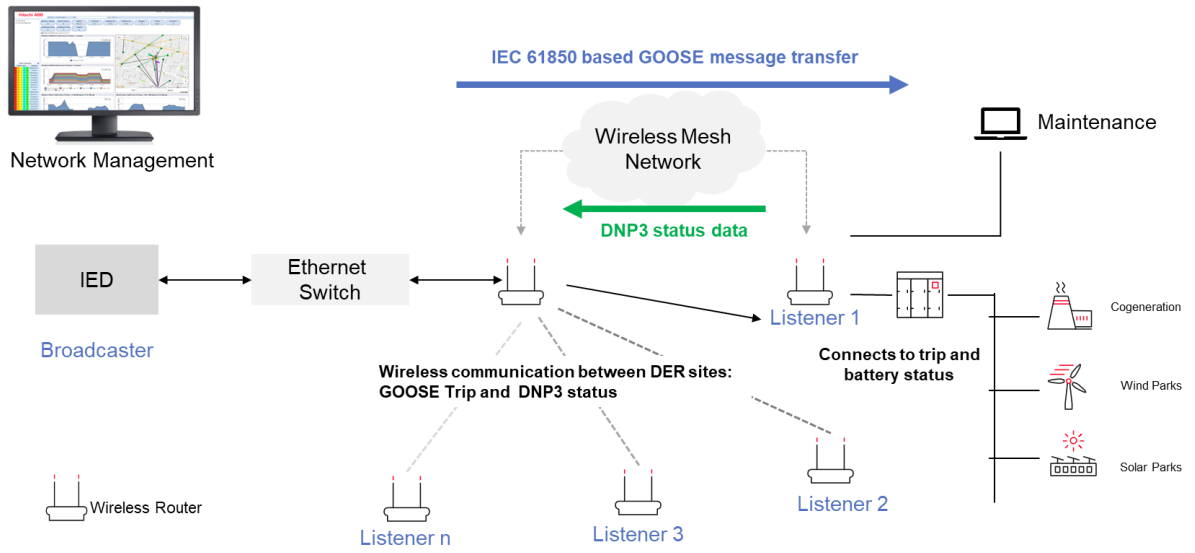

Figure 3: Use of wireless inter-substation GOOSE messages for DER interconnection protection

R-GOOSE communication can be secured over wired and wireless communication media by applying methods specified in IEC 62351-6 **[5]**.

Figure above depicts the use of wireless inter-substation GOOSE communication for Distributed Energy Resource (DER) interconnection protection. In this scheme the head station at the utility end tracks the overall power sourced and consumed by multiple customer DER sites and protects the interconnection transformer from overload in both power flow directions. Commands to reduce and trip generation are issued via GOOSE messages when the set limits are exceeded. Depending on voltage level and criticality of the scheme appropriate cyber security measures can be implemented.

In this illustration, the wireless mesh network is comprised of multiple wireless routers and involves a protocol that authenticates all the members of the mesh network using secure keys. This prevents a rogue device from joining the mesh. The transported data is encrypted using Advanced Encryption Services (AES) encryption within the Wireless Mesh Network. This maintains the confidentiality and the privacy of the GOOSE messages and the data is not exposed to a hacker that may be snooping or eavesdropping the radio waves as it travels through air.

6.2. Synchrophasor-based applications

Synchrophasor measurements are defined as current and voltage phasors with phase angles synchronized to the Universal Coordinated Time (UTC). This allows for correlation of measurements collected from different parts of the system or from different systems[**6**]. Synchrophasor communication protocols vary from legacy serial transmissions to typical TCP/IP, UDP/IP, and multicast transmissions over UDP secured by the IEC 62351-6 methods that were specified in IEC TR 61850-90-5**[4]**. Data transmission rates vary from 10 to 240 frames per second, or up to 4 frames per power cycle (16.66ms for a 60Hz power system).

An example of using wireless communication for synchrophasor data to detect a fallen conductor at a distribution level is shown in the figure below.

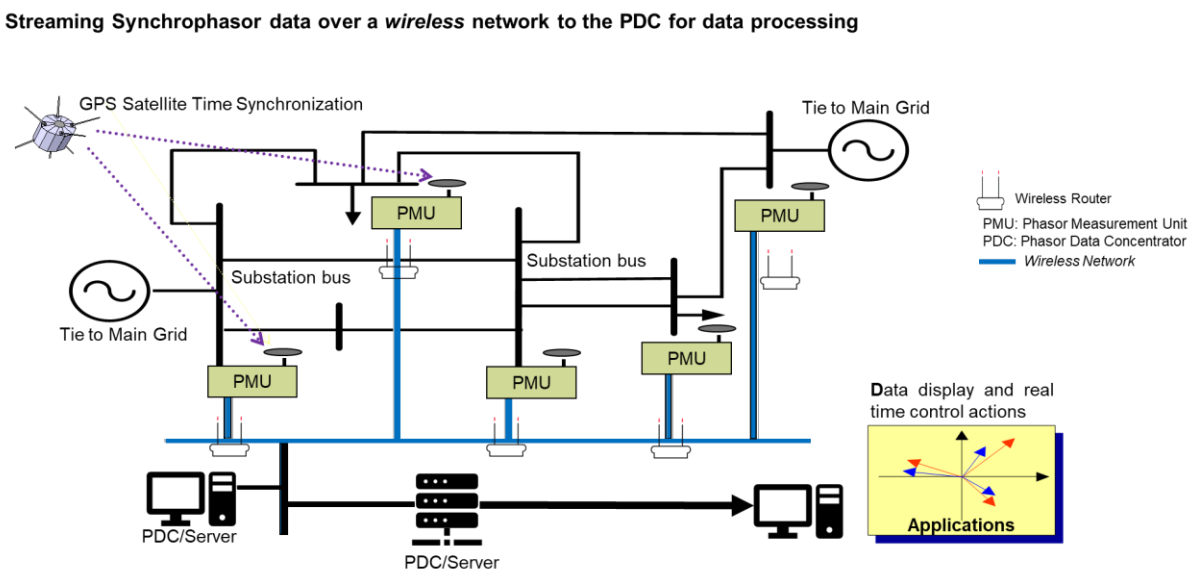

Figure 4: Use of wireless communication for synchrophasor data for fallen conductor check

6.3. Monitoring the Status of Disconnector Switches

Wireless communication can also be used in a substation yard, at transmission, sub transmission and distribution levels, to obtain the current status of disconnector (pallet) switches. Traditionally, copper wires have been used to provide the status of pallet switches from the yard to substation's control building. This, however, requires copper wiring and trenching, a very expensive and time-consuming construction work. Use of wireless communication significantly simplifies the design and reduces the overall project time and cost.

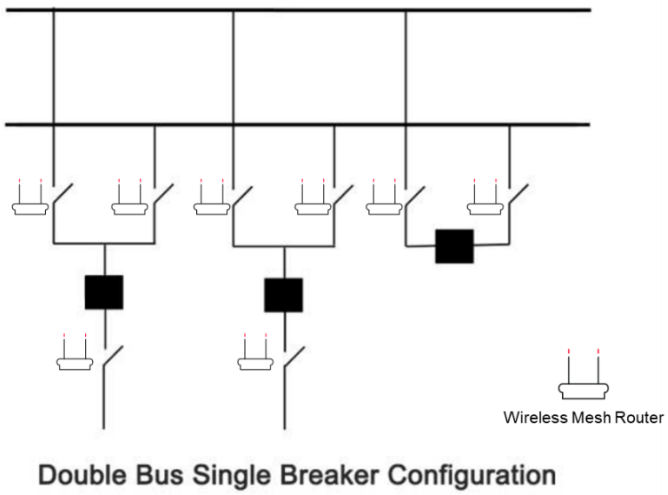

Figure 5: Use of wireless networks to monitor the status of the disconnector switches

Disconnector switch status communication does not impose strict latency (delay) and data rate requirements on the communication technology. Even though the communication network is used mainly for monitoring purposes, there is still a critical need for reliability. As this communication appears inside a cyber secure perimeter, it may not require additional cybersecurity mechanisms. The operation

of a wireless communication network in substation yard for this specific use case was tested and validated in various projects.

6.4. Remote relay access

Remote access is routinely used by protection engineers to interrogate relays by retrieving disturbance records for power system events. Even though the data obtained is not part of protection and control scheme operation, the relay is a mission critical asset that is attractive to a hacker. Therefore, any communication to a relay needs to be secured.

The example in the figure below shows a remote access connection to a relay at a rural location over many different wireless networks.

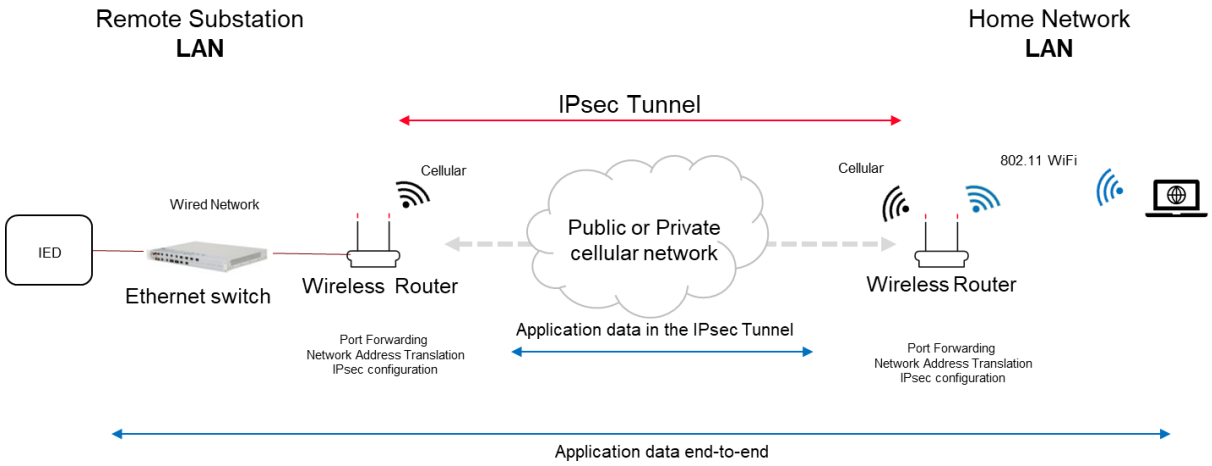

Figure 6: Remote access connection to a relay over wireless networks.

Various security controls can be used to secure data communication - encrypting the wireless traffic over the air using the AES encryption suite, configuring firewall rules on the wireless routers, configuring an IPsec tunnel for encrypting the data communication over a cellular network, and so on.

All of the above application examples illustrate that IEEE 802.11 Wi-Fi and cellular wireless communication technologies provide an inexpensive, flexible, and hybrid communication channel especially in remote areas where deploying a wired communication infrastructure is cost prohibitive or technically not feasible. In each case, the wireless communication network is secured using well-known, proven industry methodologies and techniques.

7. Conclusion

This paper discussed how security measures can be implemented for wireless communications, specifically IEEE 802.11 Wi-Fi and cellular communication technologies. The Defense-in-Depth approach covered in the paper discusses the implementation of security controls at multiple layers and this approach is applicable to both wired and wireless communications. Adopting a Defense-in-Depth approach simplifies the on-going cybersecurity assessment and improvements.

Wireless technologies provide a cheaper, flexible alternative to adding expensive fiber bypassing the need to dig trenches. When used in conjunction with Defense-in-Depth security process, wireless networks provide end-to-end secure connectivity to transport critical communication data.

References

[1] NIST Definition of Security Controls available at https://csrc.nist.gov/glossary/term/security_control

[2] IEEE 802.11™ WIRELESS LOCAL AREA Group of standards

[3] IEC 61850 Group of standards

[4] IEC TR 61850-90-5:2012: Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit Synchrophasor information according to IEEE C37.118

[5] IEC 62351-6:2020: Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850

[6] IEC/IEEE 60255-118-1:2018: Measuring relays and protection equipment - Part 118-1: Synchrophasor for power systems – Measurements

[7] Hitachi ABB Power Grids NERC CIP whitepaper available at https://search.abb.com/library/Download.aspx?DocumentID=4CAE000898&LanguageCode=en&DocumentPartId=A4-web&Action=Launch

[8] NERC CIP - North American Electric Reliability Corporation Critical Infrastructure Protection available at https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[9] ISA/IEC 62443 - Standard series for Industrial Network and System Security

[10] IEEE 1686-2013 - Standard for Intelligent Electronic Devices Cyber Security Capabilities

[11] IEC 62351:2021 - Standard for Securing Power System Communications