Modernizing Distribution Grid for DER Integration Using Distributed Edge Intelligence: Wireless Applications & Test Results

PALAK PARIKH, CRAIG WESTER, ROBERT MUZIOL
GE Renewable Energy
Canada, US

SUMMARY

This paper focuses on modernizing the distribution grid with distributed edge intelligent devices communicating over industrial wireless solutions. Distributed intelligence can be part of distribution protection, automation & control (PAC) solutions installed not only in the substation but also dispersed across the geographical area of distribution grid, including pole mount reclosers, pole mount switches, pad/vault mount load switches or Ring Main Units (RMUs), and various controllers. Industrial wireless technology can be applied to various power applications where a wired communications network has proven difficult to deploy or has less feasibility (e.g. low installation cost, mobility/portability, remote location coverage, rapid installation, etc.). Robust industrial wireless technologies or combination of technologies can deliver reliable, dependable, secure and cost-effective solutions for protection, control, automation and monitoring applications. Industrial wireless can be implemented for various distributed intelligence applications such as DER transfer trip/block, auto-reclose and restoration, dynamic change of relay configuration; and remote DER monitoring. Industry standard IEC 61850 communications and cyber security are important to the modernization of the distribution grid.

KEYWORDS

Distribution Grid, Edge Intelligence, DER (Distributed Energy Resources), Wireless Technologies, IEC 61850

1. Wireless Technologies in the Distribution Network

Advanced industrial wireless technology offers inexpensive installation, rapid deployment, widespread access, and mobile/portable communications which often cannot be proved by wired technologies and even older wireless technologies. As communication networks evolve and data demand from the network increases, advancements in industrial wireless technology is demonstrating strong applicability for various power grid applications. There have been recent advancements in industrial wireless communications that can be utilized by new protection, automation and monitoring applications in distribution & industrial facilities to provide robust and reliable performance.

Industrial wireless technology can provide the power utility with industrial grade reliability, security and performance. Industrial wireless devices are built with various substation-hardened standards, such as IEEE 1613 and IEC 61850-3, with the devices able to withstand electrostatic discharge (ESD) and electromagnetic field (EMF) radiation as well as mechanical vibrations and extreme temperatures which are commonly encountered in grid applications. Wireless networks are equipped with encryption technologies like IPSec VPNs and APNs with key rotation used to enable an end-to-end encrypted IP tunnel through which data can flow securely between utility assets. Similar to a private network, a public wireless network allows RADIUS, authorization, authentication and accounting services to allow cyber security to grid edge devices.

As shown in Figure 1 for Industrial and Distribution Protection and Automation, appropriate wireless technology can be selected and deployed to meet data latency and throughput requirements. This article focuses on three basic wireless technologies: 1) Cellular, 2) Licensed, and 3) Unlicensed.

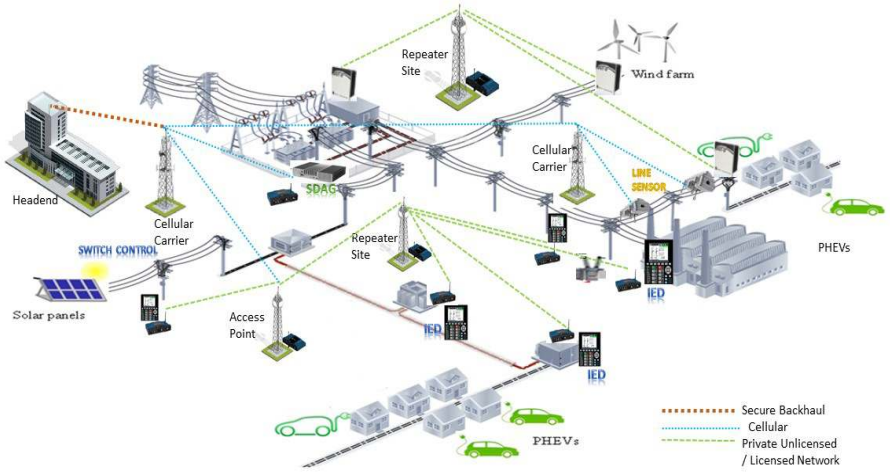

Figure 2 - Example of Wireless communications Network over a Power Network

2. Comparison of Wireless Solutions

The diverse set of spectrum rules (frequency, power, bandwidth) used by governments and power industries across the globe contributes to the variety and contributing to this diversity is the fact that not every wireless use-case is the same. Designers need to trade off bandwidth for range and transmit power for energy savings. The result is a varied combination of key performance metrics that results in many different wireless standards and pseudo-standards. Below we summarize some of the most popular technologies.

Table 1 - Wireless Technologies Comparison

Wireless Technology	Adjacent Nodes Latency	Throughput	Reliability	Range	Topology
Wi-Fi / Proprietary Broadband	<10 msec	100's of Mbps	Medium	< 1 mile	Point to Multipoint, Mesh
WiMAX	< 10 msec	10's of Mbps	Very High	1 – 10 miles	Point to Multipoint
Licensed Narrowband	100's of msec	10's of Kbps	Very High	5 – 50 miles	Point to Multipoint
Unlicensed Frequency Hopping	10's of msec	1 to 10's of Mbps	Hight with Mesh or dual uplinks	< 30 miles	Point to Multipoint
Public Cellular Carriers	50 msec (LTE)	10's of Mbps	High with QoS	1-5 miles	Point to Multipoint

By using standard networking and security methods, wireless equipment can be used in a hybrid manner to provide connectivity to all devices and locations required. As shown below, often the best way to pick the best solution is to not select a single wireless technology and use a combination or hybrid solution.

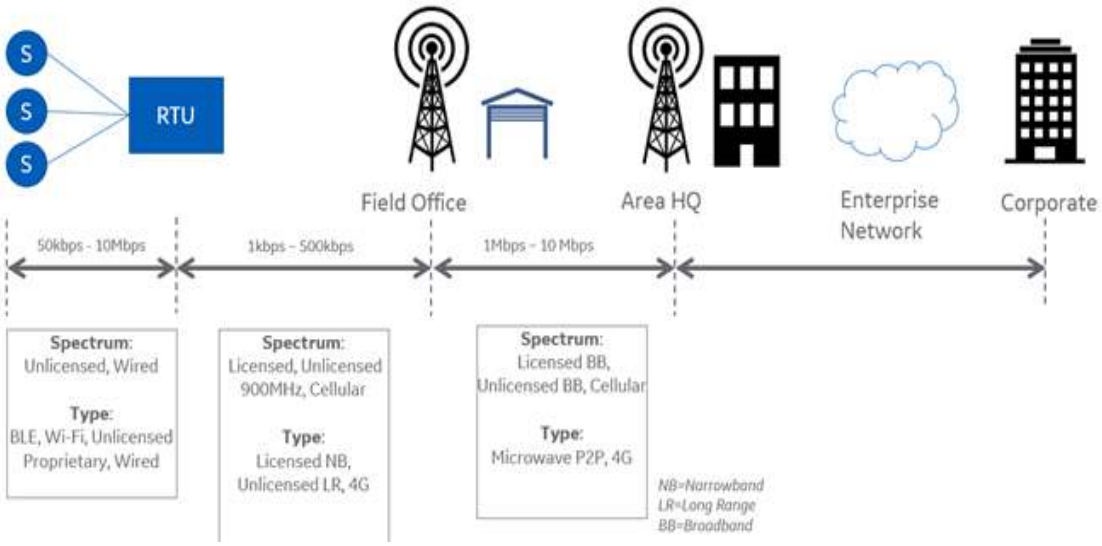

Figure 2 - Hybrid Wireless Communications

3. Distribution Automation Application Requirements & Considerations for Wireless Technologies

In the following section, we're going to discuss how communication networks address the ever increasing requirements for automation applications in the distribution grid. An integral part of the proper and reliable operation of Distribution Automation (DA) applications is the underlying wireless network that interconnects IEDs in the field. This last-mile network, also called Field Area Network (FAN), can vary significantly in the type of radio technology used, capacity (throughput), latency and availability characteristics.

Latency
Network latency generally refers to the time it takes a data message to travel between two IntelligentElectronic Devices (IEDs) or endpoints over a data network. Various DA applications can have a wide range of latency requirements, from the very aggressive microgrid Fast Load Shedding, which may require < 10 msec of network latency, to more lax monitoring applications, which may tolerate with 1-2 seconds of latency. Sometimes aggressive and lax applications may need to co-exist over the same network uplink. Latency may also be influenced by business directives (e.g. how quickly a certain distribution segment needs to be restored). For those reasons, data shared in the table below (Table 2) is to be taken as a general ball-park guidance only.

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

Reliability
Network reliability refers to the overall availability. The higher a network's uptime and availability, the more reliable a network. Several factors impact availability including the type and quality of networking equipment used, the type of Radio Frequency (RF) spectrum (licensed or unlicensed) and RF technology, network protocols and interference mitigation techniques, as well as design and built-in redundancy of both networking devices and paths. In general, applications related to monitoring are more forgiving when it comes to network reliability. If a network outage occurs, not receiving monitoring data points during that down time may not be as detrimental to grid operations. Applications related to protection such as Fault Detection Isolation & Restoration (FDIR) or DER and involving transfer trips are more impaired with network outages. As an example, if communications is lost between IEDs in an FDIR segment and a system fault occurs at the same time, local protection operates to isolate that segment but restoration won't complete until the communications network is back online to allow the coordination of distribution reclosers. Network reliability is an engineering and financial undertaking as well. The question to ask at the end is how much more is it going to cost to have connectivity to an IED or substation with a 99.99% uptime versus 99.999% uptime. How much downtime can be afforded, and during downtime what are some mitigation schemes we can use on the automation side to maintain safety and restore as many grid customers as possible while reducing risk and financial loss.

Cyber Security
Cybersecurity is an increasingly important topic for utilities, and it is as important to maintain in the distribution grid as much as it is for transmission and generation critical assets. When thinking through possible attack vectors, one should consider the worst-case scenario of what could an intruder possibly do with direct access to a recloser or a microgrid controller. What damage could they possibly cause? The answer should help us visualize the security requirement of the underlying data network. While in general, intrusion into devices such as reclosers can result in power outages and imbalance in the grid, intrusion into seemingly benign monitoring data can be similarly impactful. For an intrusion that's tied

to the power auction market, having illegal access into monitoring equipment and data may offer them a significant advantage over others.

Table 2 - Summary of FAN Network Requirements for DA Applications

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

4. Considerations for Wireless Network Reliability & Cybersecurity

Several network design factors can have an impact on the reliability and security of the wireless network, and hence contribute to the overall improvement of grid reliability and resilience/security.

Redundancy in Radio Uplinks

While most SCADA applications can tolerate some network downtime because of the loss of a radio uplink, some applications related to system protection or Load Shedding have a much higher requirement for network availability. Utilities may consider solutions that involve radios with multiple uplinks (e.g. multiple embedded modems), or ones that involve two radios devices each with one or more uplinks to offer the redundant paths. Mesh radios offer an alternative solution due to their ability to automatically route traffic to backup uplink nodes, however they come at a financial and latency cost. Therefore, special considerations and device optimizations, including the right choice of RF band and technology need to be factored in while considering mesh topologies. The example shown in Figure 3 below illustrates an IED attached to a radio device that has two embedded modems. The primary modem in this case may operate on narrowband or unlicensed ISM (Industrial, Scientific and Medical) bands, and the backup radio could use cellular technology.

The Choice of RF Bands

Unlicensed radio bands save on operation costs but are more open to interference since they're free for all to use. Utilities using unlicensed bands need to consider radio technologies and vendors that have built-in robust interference avoidance mechanisms to maximize uptime during times of congestion. Licensed narrowband frequencies in the 100, 200, 400, 700 and 900 MHz spectrum are generally much more robust against interference since it is illegal to operate in those frequencies if not licensed. The FCC allocates specific frequencies to specific geographic areas so that a single entity may own and operate them in that area. Cellular technology is generally very robust against interference because it operates on licensed bands (generally owned by the carriers).

Securing Data Transmission

Data communication between any two automation or communication devices outside of a Physical Security Perimeter must be encrypted to scramble data against open-air eavesdroppers. Such intruding entities may have the ability to listen to radio transmissions using special software-defined radios or spectrum analyzers. The larger the encryption key, the better. Typical keys that are used to encrypt and decrypt data in a Field Area Network today are generally either 128-bit or 256-bit in size. Key rotation

algorithms with certificate management must be used instead of static keys, in order to ensure that should a key be compromised by an intruder, they would soon be locked out from using it after the network generates and exchanges new sets of keys.

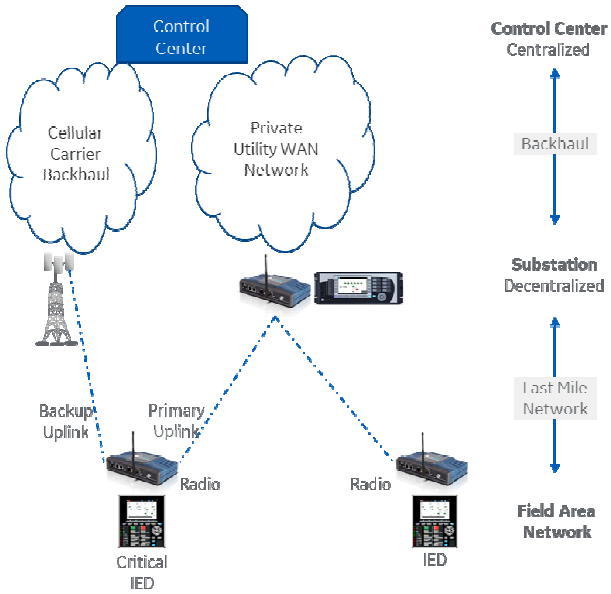

Figure 3 - Example of an IED with a Dual Uplink Radio

Securing Communication Devices

Radio vendors can use several technologies to strengthen their networking device security against physical or remote intrusion. As an example, Secure Boot technologies ensure that all modular hardware components in a certain radio device are tied together electronically at the factory. This ensures that should an intruder gain physical access to an enclosure and replace a compromised RF module inside of a radio device, the device will reject it since its factory signature doesn't match. Secure Firmware is a similar technology that guards against the manipulation of firmware.

Securing Users and Data Integrity

Several mechanisms can be used to ensure that only authorized users can access the specific network and automation devices they are authorized to use, and at the authorized level. Technologies centered around Authentication, Authorization and Accounting (AAA) technologies such as RADIUS or TACACS/+ will enable and monitor operators/user behavior on the network. To ensure data integrity, basic firewalling mechanisms can be used at specific network entry points to ensure that only allowed data types and protocols can be transferred, while all others are explicitly blocked.

Securing Features available in Today's IEDs and Gateways

IEDs (pole mount reclosers, pole mount switches, pad/vault mount load switches) and substation gateways have the capability to offer advanced cyber security features that further help grid operators to comply with NIS and NERC CIP guidelines or other security regulations. Those features are strong passwords, authentication/authorization/accounting server support (AAA - Radius), Role Based Access Control (RBAC) and non-erasable cyber event recorder (Syslog for SEM).

5. Test Setup & Results

Figure 4 below shows the test rack with two IEDs, (1) Padmount controller 850P; (2) Recloser controller 850R with both IEDs exchanging IEC 61850 GOOSE for distribution automation applications with three radios - MDS Orbit (one access point and two remotes). In addition, these IEDs are communicating with substation gateway (G500) HMI software connected to the radio access point to access and retrieve data, logs, Automatic Record Retrieval Manager (ARRM) status and IED analog values and digital input state status from connected IEDs.

The radio link technology used for these tests is 900MHz unlicensed wireless technology. The radio links are setup with RF cables and 30dB attenuators that gives around 4-6 miles between IEDs (850P & 850R) and access point (MDS Orbit).

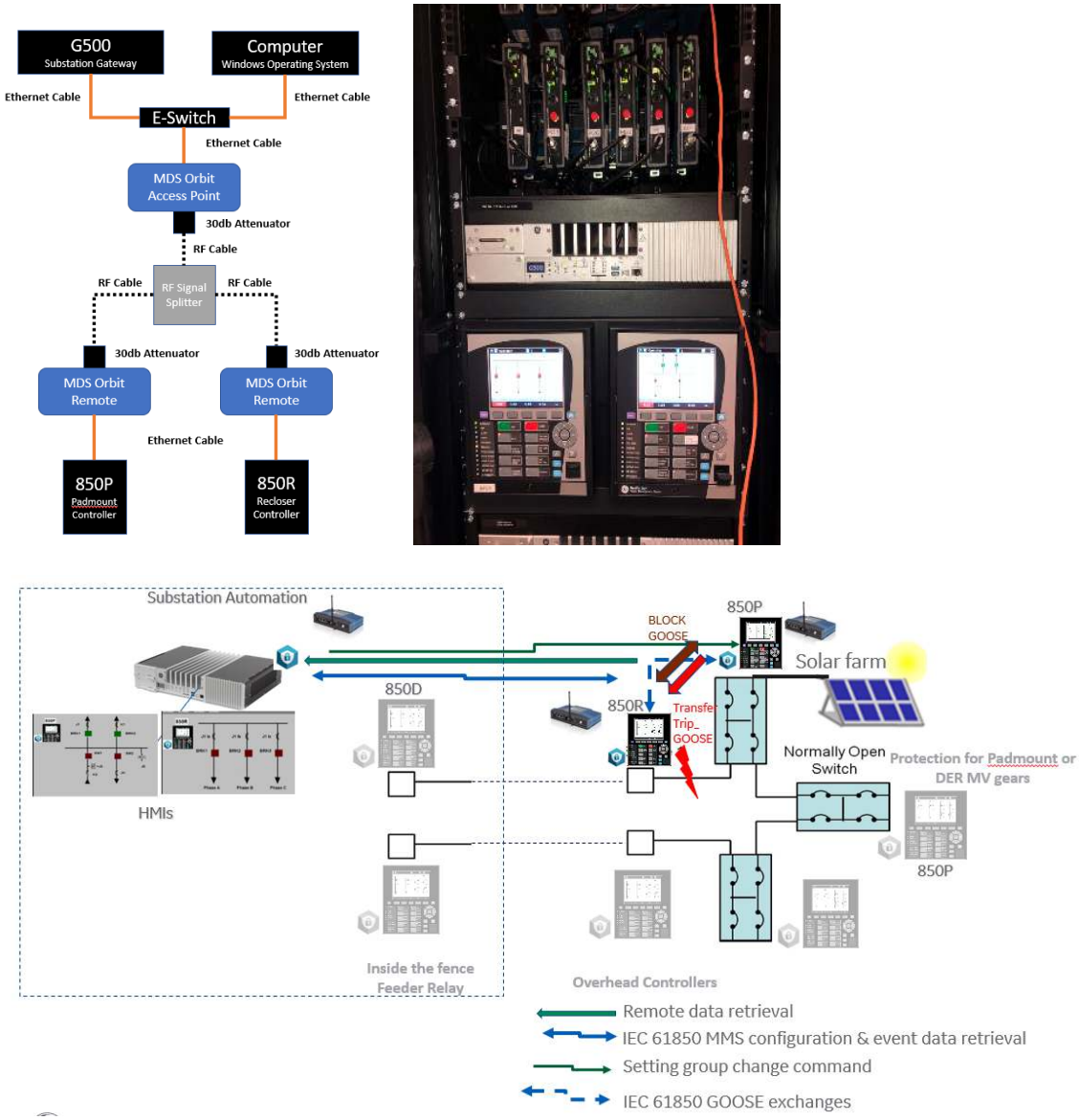

Figure 4 – Test Setup at Lab Environment

The following table (Table 3) highlights the performance of 900MHz unlicensed wireless technology for distribution automation and control applications using IEC 61850 peer-to-peer GOOSE with maximum delay of 51ms and control command using IEC 61850 TCP/IP (client-server) with maximum delay of 202 ms.

Table 3 - Performance of 900MHz Unlicensed Wireless technology for Control and Automation Application

Automation, & control Use Cases	Latency			Packet/File size Bytes (B)	Notes
	Min	Max	Average		
IEC 61850 GOOSE (peer-to-peer)	20.24 ms	51 ms	27.31ms	300	GOOSE between 850P and 850R for Transfer Trip / Block AR on DER fault
Control command (client/server)	154 ms	202 ms	184 ms	500	G500 requested to dynamic Setting Group Change using IEC 61850 MMS from setting group 1 to 2 in the IED

Additional test results are taken to show the remote file transfer mechanism to perform data retrieval. The following table (Table 4) presents file transfer protocol performance for various file types – sequence of event (SOE) retrieval, fault record (COMTRADE format) files, and setting configuration IEC 61850-6 configured IED Description (CID) file.

Table 4 Performance of 900 MHz Unlicensed Wireless technology for File Transfer

Device File Management Use Cases	Latency			Packet/File size Bytes (B)	Notes
	Min	Max	Average		
Remote Event File Retrieval	1s	3s	2 s	2182	Substation gateway requested and received file using File Transfer Protocol (FTP)
Fault Records, IEEE COMTRADE file transfer	1 s	5s	3s	158,004	Data transfer speed observed at 32 KBps using File Transfer Protocol (FTP)
New Setting Configuration Upload of IEC 61850 CID file	50 s	110 s	79 s	2,261,205	Data transfer speed observed at 28 KBps using File Transfer Protocol (FTP)

6. Summary

Recent advancements in industrial wireless technology are applied to various power applications where wired network is difficult to deploy or has less feasibility e.g. low installation cost, mobility/portability, remote location coverage, rapid installation, etc. Robust industrial wireless technologies or combination of technologies can deliver reliable, secure and cost-effective solutions for protection, automation and monitoring applications. Cyber security requirements are achieved over both licensed/private and unlicensed/public wireless technology options and enabling the available cyber security features in today's IEDs. Suitable wireless technology should be selected based on criteria such as bandwidth, range, data latency, and regional frequency spectrum availability. Industrial wireless has already been applied for DER transfer trip, , distribution automation, dynamic IED configuration change, and remote DER or substation monitoring. While licensed narrowband technologies have been the de-facto winner for several years, newer cellular-based technologies (e.g. 5G) is picking up due to their ubiquitous presence, as well as improved network capacity and latency. Considerations of OPEX and CAPEX, and whether to build your own or lease factor in the choice of radio technology as well. Using dual band radio technology provides additional network reliability. The test results present that industrial wireless technology has potential to meet performance requirements for the distribution applications especially with proliferation of DERs.

BIBLIOGRAPHY

[1] Palak Parikh, Justin Smith, Michael Pilon, "Wireless Technologies and their applications for Protection, Automation and Monitoring", PAC World Article, Dec. 2018.

[2] Mike Ramlachan, Edgard Sammour, Craig Wester "Wireless Solutions for Reliable Distribution System. Protection & Control" Teaxas A&M Conf. 2021

[3] EPRI Tech. Rep., "Wireless Connectivity for Electric Substations," Feb. 2008.

[4] P Parikh, TS Sidhu, A Shami, "Investigating Performance of Wireless LAN for IEC 61850 Based Smart Distribution Substations", IEEE Transactions on Industrial Informatics 9 (3), 1466-1476, Oct 2012.

[6] National Electric Sector Cybersecurity Organization Resource (NESCOR), "Cyber Security for DER Systems", July 2013