Leveraging Private LTE Networks for Direct Transfer Trip (DTT) Systems

Jason T. Mills
Engineering
Anterix, Inc.
Woodland Park NJ, USA
jmills@anterix.com

Brian M. Dob
Product Manager
Hubbell Power Systems
Boonton NJ, USA
bdob@hubbell.com

***Abstract*— Interconnection of Distributed Energy Resources (DER), islanding detection and prevention is an important part of the electric utility industry's clean energy goals. IEEE 1547 – Standard for Interconnecting Distributed Resources with Electric Power Systems recommends that an island be detected and removed within two seconds of an occurrence. Utilizing a Private LTE (PLTE) network for islanding prevention delivers several improvements over public carrier options, including enhanced latency, reliability, security for mission-critical grid protection applications and simplified communication interconnection for DERs.**

The most common type of communication-assisted islanding detection and prevention is Direct Transfer Trip (DTT). This method requires communication technology between the potential isolating sources and the DER. When an isolating source is opened, creating an island, a DTT signal is sent to the DER. As with all communications assisted methods, communication technology is critical to the functioning of the system.

Private LTE is a foundational technology that provides connectivity to many types of utility applications. Private LTE networks for DTT applications are a compelling choice due to their high availability, low latency, and high performance while optimizing the total cost of ownership. Private LTE-enabled DTT applications significantly improve latency and reliability compared to public networks. This paper explores utilizing Private LTE cellular networks for DTT anti-islanding applications. The aspects which are considered include the reliability of the network, cyber security, performance requirements and redundancy options.

This paper provides data and results from the lab test conducted using RFL GARD 8000 devices on a QoS-enabled private LTE network. The test results show that a private LTE wireless network provides a communications network with a high level of reliability and deterministic latency for wireless protection applications.

Keywords—Distributed Energy Resources, DER, Distributed Generation, Private Cellular, Direct Transfer Trip, DTT, Anti-Islanding, Islanding Detection, Teleprotection, PLTE, Quality of Service

I. INTRODUCTION

A. Islanding

A power system island occurs when a generator becomes electrically isolated from the power utility source station and continues generating and exporting power. In such instances, the generator will continue powering the local network, or "island," independently from the utility. Without specific controls, this islanded state may persist indefinitely as long as the generator can sustain the load demands or unless it is disconnected due to voltage and frequency protection elements, or other protective measures.

Islanding can result from operational events such as activating isolation devices like breakers, disconnect switches, and reclosers. It may also be triggered by factors, including system switching, environmental conditions, or equipment malfunctions.

Islands can be created deliberately or accidentally. For instance, a micro-grid is designed to intentionally disconnect and operate autonomously from the power utility and reconnect when suitable. In such scenarios, the micro-grid is configured to avoid exporting power while islanded.

This paper focuses on unintentional islanding, where unaddressed risks are a significant concern. Often, communication systems are employed to mitigate these risks. Establishing these systems can be challenging and may include high initial or recurring costs, accessibility issues, or performance issues. These will diminish the return on investment (ROI) for the generator or render the investment unfeasible.

B. Islanding Risks

An unintentional island presents several hazards for both the utility and the public. These hazards generally include threats to personal safety, degradation of power quality, and potential damage to equipment.

Concerning personal safety, there is a danger that generators might inadvertently energize disconnected lines, posing a serious risk to utility workers accessing these lines. The public could also be at risk when energized lines fall within areas accessible to the public, such as streets or walkways.

Power quality tends to deteriorate when an unintentional island forms because the normal grid regulation is absent. This lack of regulation can lead to voltage and frequency fluctuations, which may harm both consumer and utility equipment within the island.

In cases involving synchronous generators, it is crucial that they are resynchronized with the grid prior to reconnection. Failure to resynchronize can lead to damage to the generator equipment. Therefore, it is essential to first disconnect the generation to allow for proper resynchronization.

To mitigate these islanding risks, the IEEE 1547 – Standard for Interconnecting Distributed Resources with Electric Power Systems advises that any unintentional islands be detected and disconnected within two seconds of their formation[1,2]

II. Anti-Islanding

Anti-islanding protection refers to methods used to mitigate the risks associated with unintentional islanding. This protection is crucial for preventing unintentional islands. Detecting the presence of an island once it forms is the first step in mitigating unintentional islands, a process known as islanding detection.

A. Islanding Detection Methods

Islanding detection methods can be categorized into local and communications-assisted methods. Using passive or active detection techniques, local detection methods detect island conditions solely from the generator station without external communications. Passive methods include under/over voltage and frequency relays, while active methods attempt to alter voltage or frequency to detect island conditions more accurately. Local methods may encounter issues when generation and load are closely matched, leading to a "non-detection zone" (NDZ). On the other hand, communications-assisted methods use communications technologies to coordinate with other devices, eliminating the NDZ and reducing false positives during unrelated system disturbances. [2]

1) Direct Transfer Trip (DTT)

Direct Transfer Trip (DTT) is a common communications-assisted method for islanding detection and prevention. DTT transmits transfer trip signals between devices, typically involving bi-directional communications. An isolating device, such as a breaker or recloser, initiates the DTT signal and sends it to the generator location to open the local breaker or Point of Common Coupling (PCC), thus isolating the generator and preventing power export. This method eliminates the non-detection zone and allows for less sensitive voltage and frequency protection elements, reducing false operations during system disturbances. [2]

2) DTT Performance

DTT performance relies on two key parameters: reliability and latency. Reliability ensures the system operates as intended during changing environmental conditions. Latency measures the time between the initiation of the DTT signal and the actual operation at the receiving end. Balancing these parameters is crucial for optimizing DTT performance. Thorough consideration of these parameters is necessary when selecting DTT communication channels and methods. [2]

III. Communications Technologies

Choosing the right communication technologies can reduce complexity and enable a robust, reliable utility application such as DTT. For instance, employing a shared wide-area network (WAN) that supports multicast IEC 61850 GOOSE communications can significantly decrease the necessity for numerous point-to-point communication circuits. Modern communication technologies offer wireless multi-point capabilities that provide utilities a more convenient path to onboard and support additional devices.

When selecting communication technologies, you must consider factors such as availability, equipment costs, operational costs, and reliability. The selected communication technology should meet the mission critical application's requirements for reliability and latency.

A. Legacy Communications Technologies

Historically, utilities have used several legacy communication technologies for DTT anti-islanding, including fiber optic, Time Division Multiplexed (TDM) digital networks, analog and digital phone lines, and power line carrier communications.

Direct fiber optic communication, while highly effective, becomes exceedingly expensive as the distance between the utility substation and the generator expands and the number of required communication channels increases. The installation cost of fiber optic cables can easily exceed $20,000 per mile in most scenarios. This high cost often necessitates leasing services from telecommunications providers. Traditionally, these services have included copper phone lines using audio tone frequencies or digital TDM circuits like T1. These options were widely accessible and reached many remote locations due to the extensive telecom network buildout in the US. Although they are still used in some regions, they have become considerably more expensive and less reliable, as the telecom industry shifts away from these legacy technologies to packet-based and wireless cellular communications. As a result, the demand for legacy communications has dwindled, and providers are less inclined to support them adequately. [2]

There are many wireless communication options for mission critical applications. Specifically, numerous utilities have evaluated and pursued building and managing Private LTE communications networks to address their current and future grid communications requirements, including critical applications such as DTT for distributed generation.

B. Role of Private LTE for Utility Mission Critical Applications

LTE, or Long-Term Evolution, is a standard for wireless broadband communication in mobile networks. It is designed to provide high-speed data and voice services over cellular networks, offering significant improvements in speed, capacity, and latency compared to previous technologies. LTE is built using global 3GPP (Third Generation Partnership Program) standards, thus an investment in LTE infrastructure safeguards

against technology changes and will remain relevant and compatible with future advancements.

A Private LTE communications network is a dedicated wireless network designed to serve a specific organization, such as an electric utility, generation facility or renewable energy source. Unlike public LTE networks operated by mobile network operators (MNOs) to serve the general public, Private LTE networks are owned and controlled by the utility. A Private LTE network allows the utility to tailor the network to its specific needs and use cases, ensuring better control over coverage, performance, and security.

A unique aspect of a Private LTE network is the ability to prioritize data traffic through Quality of Service (QoS). This function is crucial for mission-critical applications using a Private LTE communications network because it ensures reliable and prioritized data transmission. QoS allows network administrators to allocate bandwidth and prioritize traffic for essential services, such as mission-critical use cases, real-time monitoring, and control systems. This prioritization helps maintain consistent performance and reduces latency, which is vital for applications where delays or interruptions can have significant consequences.

Additionally, QoS enhances the overall reliability and security of the network. By managing and optimizing network resources, QoS helps prevent congestion and ensures critical applications receive the necessary bandwidth even during peak usage times. This is particularly important for utilities applications that rely on uninterrupted and secure communications to operate effectively. [3,4]

Without QoS for mission-critical applications in a communication network, several issues can arise such as increased latency and jitter, network congestion and packet loss. Without QoS, these critical applications may experience delays and variability in data transmission, leading to slower response times and potential operational interruptions.

The primary benefits of a Private LTE network include control and customization, coverage, capacity, scalability, reliability, security and privacy. Private LTE networks offer greater control over network parameters, allowing utilities to customize the network to meet their specific requirements around data speed and latency. Coverage and reliability are critical aspects as private LTE networks can be designed to provide coverage in specific areas, including remote or rural locations where typical communications coverage might be limited. The ability to customize the network to the organization's needs promotes reliable connectivity for mission-critical applications regardless of the location of the end device. Utilities can build a communication system with greater resiliency and redundancy, i.e., constructing radio towers to utility-grade standards by implementing backup generation or deploying geographically separated redundant cores.

Private LTE also delivers the capacity and scalability to meet current and future connectivity needs including more connected devices, as well as the requirements of emerging clean energy solutions and smart grid applications.

Private LTE networks offer enhanced security and privacy since the organization fully controls the network infrastructure and data. Private LTE is a suitable solution to enable distributed generation interconnections requiring DTT communications. Overall, Private LTE networks provide organizations with a tailored, reliable, and secure communication solution, making them ideal for mission-critical applications.

C. Components of the Private LTE Network:

- Building a Private LTE communications network requires several key components to ensure reliable and secure connectivity for mission-critical applications. The primary infrastructure elements include (see Figure 1).
- Devices for Mission-critical Applications: End devices, gateways, sensors, and meters having internal radio modules that connect to the chosen spectrum network.
- Spectrum: Private LTE networks require access to licensed or unlicensed spectrum.
- Radio Access Network (RAN): Consist of base stations (eNodeBs) at radio towers that provide wireless connectivity to user devices. The RAN handles radio communication between the devices and the core network.
- Backhaul Network: Connects the RAN to the core network and can be implemented using various technologies such as fiber optics or microwave links.
- Core Network: Manages the overall network operations, including user authentication, data routing, and mobility management. It typically includes components like the Mobility Management Entity (MME), Serving Gateway (SGW), and Packet Data Network Gateway (PGW).
- Network Management System (NMS): This system provides tools for monitoring, managing, and optimizing the network's performance and security[5,6]

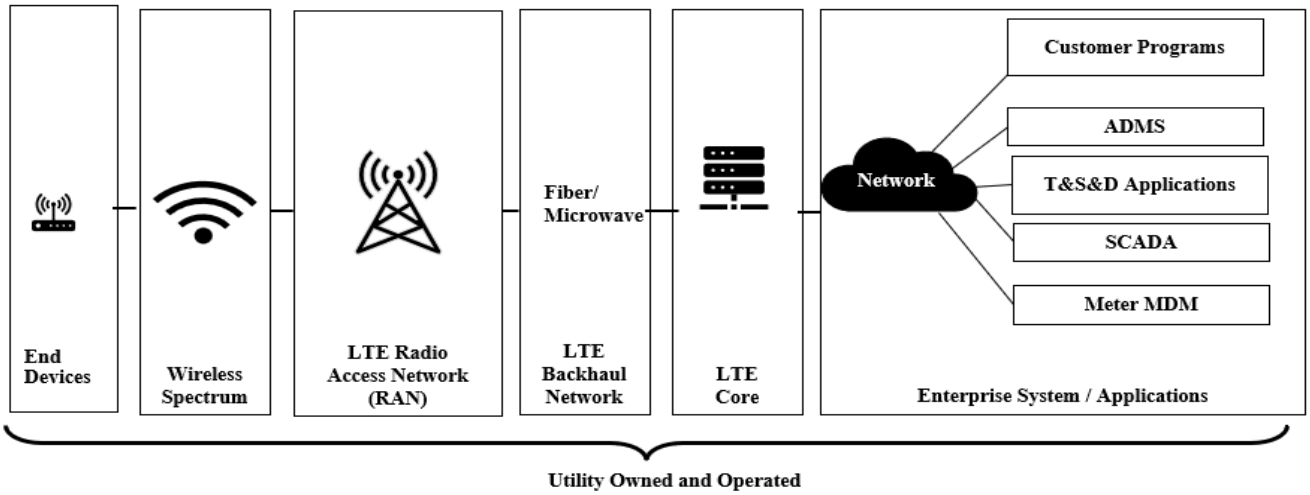

Figure 1 – Private LTE Network Diagram

IV. Lab Testing and Results

To confirm the suitability of using Private LTE communications for DTT anti-islanding, it is essential to conduct lab testing to verify the system's performance. This testing should include verifying the critical performance parameters crucial to the operation of the anti-islanding protection system, as previously discussed.

A. DTT Application and Testing

The objective of this test case is to emulate a DTT system for a straightforward two-terminal application using LTE cellular communications, closely mirroring a real-world scenario. Figure 2 illustrates the simulated real-world application, while Figure 3 shows the actual test setup, with Location A representing the power utility station and Location B the generator.

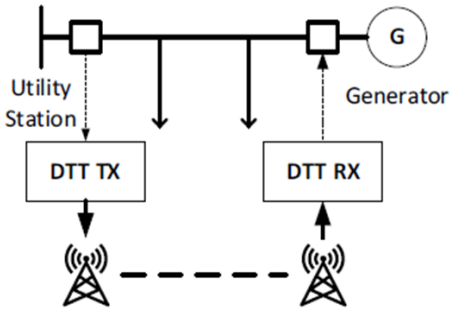

Figure 2 – Distribution DTT Anti-Islanding Cellular Application Example

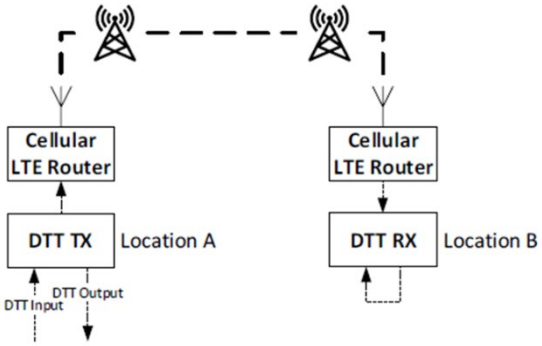

Figure 3 – DTT Anti-Islanding Cellular Test Setup

B. DTT Transmitter and Receiver

For the test case, we used a common multifunction programmable teleprotection device as both the DTT transmitter and receiver. This device featured an Ethernet teleprotection communications interface, chosen for its ease of transporting native Ethernet over LTE cellular networks, unlike serial or digital TDM protocols that require conversion to Ethernet. This setup not only simplifies the process but also reduces latency by eliminating the need for conversion. The Ethernet teleprotection interface uses the standard layer 2 multicast GOOSE protocol, which allows for interoperability with multiple vendor devices and supports multipoint communications, beneficial for scaling up to more complex systems with multiple terminals.

At location A, the DTT transmit function is triggered by an external contact, simulating a substation breaker contact, prompting the device to send a change of state GOOSE message to signal the DTT function. Upon successful receipt, the receiver at location B closes a DTT output contact, which would typically energize a trip coil to isolate the generation from the line. In this test case, however, the decision was made to key another DTT function back to the transmitter, creating a round-trip test. This approach allows for the evaluation of critical performance parameters from a single end with a common time reference,

resulting in latency measurements that are approximately double the one-way time delay. This method also enables the assessment of bi-directional communications for applications requiring communication from the generator to the utility.

C. LTE Network Setup and Diagram

The network setup was designed to emulate a private LTE system where two separate RANs (Radio Access Networks), isolated by separate RF enclosures, backhaul to a single EPC (Evolved Packet Core). It is intended to represent a deployment where devices that require wireless access are geographically separated, requiring separate wireless towers to access the Private LTE network.

V. Test Case 1 – Private/Public LTE

A. Test Case 1A – Private LTE Network

Non-commercial SDRs (Software Defined Radios) were configured to provide a 3MHz US Band 8 (licensed spectrum) carrier in each RF enclosure connected to an on-premises EPC operating on an off-the-shelf x86 computer platform. The end devices communicated layer 2 multicast traffic and required that GRE (Generic Routing Encapsulation) over IPSEC tunnels be established between the gateways to allow traffic to pass between the gateway's subnets. The DTT gateway devices were configured to connect the end devices in the Private LTE system to have a QCI (QoS Class Identifier) set to 5. To simulate real-world data traffic, we added a second gateway (congestion gateway) to the initiator and loopback device sides of the solution. We configured the congestion gateways used in the Private LTE system to have a QCI of 9 (lower priority than QCI5). Due to QCI capabilities of the Private LTE network, the system prioritizes data with QCI value of 5 ahead of data with QCI value of 9. This ability to prioritize data is a key difference-maker for a PLTE system. In this test case, the data generators simulate background data of a partially loaded system in addition to traffic being sent by the DTT application. Open-source software iPerf3 was used to generate TCP traffic and utilize available bandwidth in the system.

The initiator device was configured to send a DTT (Direct Transfer Trip) signal at 250 ms intervals and measure the time for the loopback device to respond/acknowledge the signal. The initiating device would capture the measured time of the DTT signal responses into time buckets set to 90ms, 110ms, and 125ms. Each timer bucket count is the number of DTT signal response(s) (round trip time of the DTT signal) captured in that time interval or less. For field applications, the signal must be one way, or approximately half of the round-trip results in Table 1. The architecture is shown in Figure 4.

B. Test Case 1A – Private LTE Network Results

We commissioned the test system as described and established communication between the two locations. After which it was possible to perform testing to evaluate performance. Testing consisted of the critical DTT performance parameters: latency and reliability.

Table 1

	Total			*Roundtrip Latency*		
	Transmitted	***Received***	***Dropped***	***90ms***	***110ms***	***125ms***
Packet	32,760	32,760	0	31,176	32,760	32,760
% of Total	100%	100%	0%	95.16%	100%	100%

Table 1 – PLTE system with partially loaded background data: DTT Application Data QCI 5 – Background Data QCI 9

System Reliability- The data in Table 1 demonstrates high reliability in packet transmission and reception. Out of 32,760 packets transmitted, all 32,760 were successfully received,

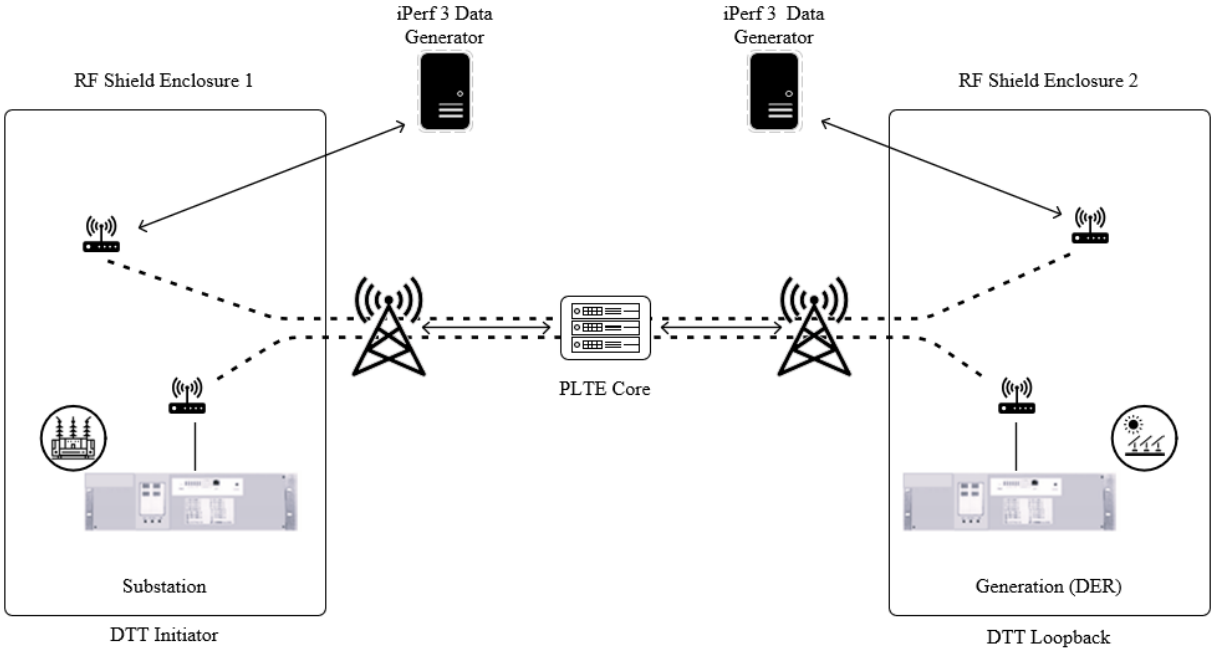

Figure 4 Network Testing Architecture

resulting in a 100% reception rate and 0% packet loss. These results indicate that no packets were dropped during transmission, highlighting the robustness and reliability of the communication network.

System Latency - The data in the table highlights the latency performance of the network. At 90 ms, 95.16% of the packets were received, while at 110 ms and 125 ms, the reception rates were 100.00%. These figures illustrate that the vast majority of packets are delivered in under 90 ms, with all packets being received within 110 ms Keep in mind these times are round-trip measurements, and the one-way latency is assumed to be half this value. These high percentages further emphasize the network's efficiency in delivering packets within acceptable time frames, ensuring timely and reliable data transmission for mission-critical applications.

C. Test Case 1B – Public LTE Network

The objective of this test case is to emulate a DTT system for a basic two-terminal application using public LTE cellular communications, closely mirroring a real-world scenario. Figure 2 illustrates the simulated real-world application, while Figure 3 shows the actual test setup, with location A representing the utility station and location B the generator [2]

D. Test Case 1B – Public LTE Network Summary and Results

We commissioned the test of Figure 2 & 3 system and established communication between the two locations. As discussed previously, testing focused on the critical DTT performance parameters reliability and latency.

We measured latency by taking half of the round-trip time delay. It became evident that the measured delay could vary depending on the current conditions. The typically observed round-trip delay was roughly 80ms, or 40ms for the estimated one-way latency. We repeated the test several times to further characterize the change in latency over time and under different conditions.

With repeated testing the DTT signal was routinely sent and received within a defined timeframe. As with the latency testing, we measured dependability as a round-trip test. We used three separate latency evaluation timers, 100ms, 120ms, and 150ms to help characterize the varying latency. This test ran for approximately eight hours with the DTT signal being initiated two times per second. The test results are shown in Table 2. It should be noted that a single change-of-state GOOSE retransmission was used in this testing[2]

	Table 2					
	Total			***Roundtrip Latency***		
	Transmitted	***Received***	***Dropped***	***100ms***	***120 ms***	***150ms***
Packets	58,748	58,748	0	55,642	58,588	58,695
% of Total	100%	100%	0	94.7%	99.7%	99.9%

Table 2 – Public LTE Network Results[2]

E. Comparison of the performance of the Data from Test Case 1A and 1B

System Reliability - Table 1 shows no packet loss. With PLTE testing, Table 2 also shows no packet loss across all measurements. This indicates that during time of lower congestion a private network and a public network will be similar in overall reliability. This assumes the end device is situated in an area with adequate public network coverage and capacity.

System Latency - The testing confirmed the similar latency performance of the private and public networks. For PLTE testing (Table 1), at 90 ms, 95.16% of the packets were received, while at 110 ms and 125 ms, the reception rates were 100.00%. With public LTE (Table 2), at 100 ms, 94.7% of the packets were received, while at 120 ms and 150 ms, the reception rates were 99.7 % and 99.9%, respectively. These figures illustrate that most packets are delivered in under 100 ms round-trip in both solutions, with nearly all packets received within 150 ms. These high percentages further emphasize both network's efficiency in delivering packets within acceptable time frames, ensuring timely and reliable data transmission for mission-critical applications. This indicates that during times of low congestion a private network and a public network can be similar in overall latency.

F. Conclusion of Test Case 1:

During normal conditions, a private network and a public network can have similar reliability and latency at a given location. The advantages in a Private LTE network is the ability to have deterministic latency, unlike in a public LTE network that prioritizes data as best effort and differs based on device location. Deterministic latency is a key factor when choosing a communication medium for mission-critical applications such as DTT which require precise and reliable communications. Deterministic latency delivers data packets within a set time frame without regard to device location, reducing variability and delays. This predictability is crucial for the timely operation of the grid and for applications such as DTT, Scada, utility automation, real-time monitoring, and control systems. Utilities can benefit from this enhanced performance by minimizing latency and ensuring timely data delivery.

VI. Test Case 2 – Partially Loaded PLTE Network vs Heavily Loaded PLTE Network for DTT Application

In the second test case, the goal was to overload the system with communication traffic indicative of a hurricane, blackout, or other unexpected system event. We added overload traffic to the system to consume bandwidth of the Private LTE network and stress the system. We configured the DTT gateway devices used for connectivity of the end devices in the Private LTE system to have a QCI (QoS class identifier) set to 5. We also configured the congested traffic gateway devices used for connectivity of the end devices in the Private LTE system to have a QCI to 9 (lower priority than QCI5). In this test case, the data generators simulate background data of a partially loaded and heavily loaded system in addition to traffic being sent by the DTT application. Open-source software iPerf3 was used to generate TCP traffic and utilize available bandwidth in the system. See Figure 4

A. Test Case 2 – Partially Loaded vs Heavily Loaded LTE Network Results

We commissioned the test system as described and established communication between the DTT application.

	Table 1					
	Total			*Roundtrip Latency*		
	Transmitted	***Received***	***Dropped***	***90 ms***	***110 ms***	***125 ms***
Packets	32,760	32,760	0	31,176	32,760	32,760
% of Total	100%	100%	0%	95.16%	100%	100%

Table 1 – PLTE system with partially loaded background data : DTT Application Data QCI 5 – Background Data QCI 9

	Table 3					
	Total			*Roundtrip Latency*		
	Transmitted	***Received***	***Dropped***	***90 ms***	***110 ms***	***125 ms***
Packets	30,034	30,034	0	27,782	30,024	30,034
% of Total	100%	100%	0%	92.50%	99.97%	100%

Table 3 – QOS – PLTE system with heavily loaded background data: DTT Application Data QCI 5 – Background Data QCI 9

System Reliability – Both tables show no packet loss across all measurements. These results indicate that during a disaster and/or a peak capacity event a private network should have high performance regardless of the network load.

System Latency – The test result confirms the network performance for DTT data is not degraded even when traffic exceeds the networks capacity. Table 3 and 4 illustrate that most packets are delivered in under 90 ms, with all packets received within 125 ms. These high percentages further emphasize a private network's efficiency in delivering packets within acceptable time frames, ensuring timely and reliable data transmission for mission-critical applications. The test results highlight that even in the most extreme events the private LTE network will have high performance and background data will not have a significant impact on performance.

B. Conclusion of Test Case 2:

Whether during high or low data traffic, the private network will have similar reliability and latency at a given location. A Private LTE system can be designed to meet the reliability and latency requirements for mission-critical data points and devices. This reliability and dependability are crucial for applications to manage an ever-changing utility grid. A Private LTE network enables utilities to focus on crucial operations and not be impacted by the inability to communicate with its field devices. Connectivity to field devices will allow utilities to manipulate equipment and improve the ability of a utility to reroute and provide power to its customers. QOS facilitates the integration of advanced applications like SCADA, AMI, and demand response, improving grid management and efficiency.

VII. DTT Application with PLTE Study Conclusion

In summary, reliable communication for DTT applications is vital for ensuring the efficiency and stability of the power grid. Private LTE networks outperform public networks in DTT applications by creating deterministic reliability to each endpoint and having minimal impact on latency during high data traffic events. A Private LTE network allows utilities to control, manage and ensure reliability of mission-critical applications, such as direct transfer trip for DER applications.

Private networks are designed to serve a specific organization, allowing for dedicated resources and better control over network performance. The ability to design and control a mission-specific Private LTE network means that during high-traffic periods or emergencies, the organization can prioritize critical communications without competing with the public for bandwidth. In contrast, public networks can become congested, leading to slower speeds and unreliable connections. Public networks, while improved over the years, are more vulnerable to outages and performance issues during such events due to the high volume of users. Private networks provide a reliable and controlled communications solution, allowing mission-critical applications remain operational even in challenging conditions.

VIII. Biographies

Brian Dob received his BS in information technology from the New Jersey Institute of Technology in 2004 and MS in engineering management in 2013. He is a member of the IEEE with over twenty years of experience in the power utility industry, which is largely concentrated on power utility communications for protection applications. He is currently responsible for the Hubbell Power Systems/RFL protection product line including Powerline Carrier, Audio Tone and Digital Teleprotection, as well as Line Protection Relays.

Jason Mills, P.E., graduated with M.S. in Power Engineering from Drexel University and a BS of Electrical Engineering from Lafayette College. He has worked in the power industry for 13+ years in the distribution, transmission, and nuclear generation sides of the industry. He has experience working in many areas such as Smart Grid automation, OSI implementation, DER Capacity Planning and Nuclear Risk Management. Currently working at Anterix which is a USA leader in communications technology advancement, providing leadership to utilities to understand their needs for Advanced Connectivity, Data Collection and Smart Infrastructure.

IX. References

[1] Standard for Interconnecting Distributed Resources with Electric Power Systems, IEEE Standard 1547-2003, June 2003.

[2] B. Dob and T. Schwartz, "Leveraging Cellular Networks for Communications Assisted AntiIslanding Protection", PACWorld North Americas Conference, Sept 2021.

[3] Cox Private Networks. (n.d.). Manufacturing & Distribution. Retrieved March10,2025,from:https://www.coxprivatenetworks.com/industries/manufacturing-distribution

[4] CommScope. (n.d.). Skyus 500 Solution Brief. Retrieved March 10, 2025, from https://www.commscope.com/globalassets/digizuite/581284-skyus-500-solution-brief-co-114858-en.pdf

[5] Dusun IoT. (2022). Private LTE Network: Complete Guide in 2022. Retrieved from:https://www.dusuniot.com/blog/private-lte-network-complete-guide-in-2022/

[6] Qualcomm. (n.d.). Private LTE Networks. Retrieved March 10, 2025, from:https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/private-lte-networks.pdf