Leveraging Cellular Networks for Communications Assisted Anti-Islanding Protection

Brian. M. Dob (Hubbell Power Systems) and Thomas. J. Schwartz (GE Renewable Energy MDS)

bdob@hubbell.com

USA

Abstract-- A power system island is a part of the power system grid that becomes separated from the larger power system and depending on the actual load and local generation, may continue to function in this “islanded” state. Islands occur as substation breakers and isolating devices are opened, clearing power system faults, separating local demand and generation resources from the utility’s power system.

Islanding detection and prevention is an important part of distributed generation (DG). 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. Islanding prevention has several benefits, some of which are safety, generator and consumer equipment protection and power system stability.

The most common type of communications assisted detection is Direct Transfer Trip (DTT). This method requires a communications channel between the potential isolating sources and the generator. When an isolating source is opened, creating an island, a DTT signal is sent to the generator. As with all communications assisted methods, the communications channel is critical to the functioning of the system. Different types of communications channels may be used. Often leased telco services are purchased for this purpose. As communications technology shifts from analog and digital Time Division Multiplexed (TDM) circuits to packet networks there are new communications opportunities available. LTE cellular networks stands-out as an attractive option as a result of availability and low cost.

This paper will explore the various aspects of utilizing LTE cellular networks for DTT anti-islanding applications. The aspects considered are network types and infrastructure, cyber security, performance requirements and redundancy options. In addition, results of a real-world test case and cost comparison will be discussed.

Index Terms—Distributed Energy Resources, DER, Distributed Generation, DG, Direct Transfer Trip, DTT, Anti-Islanding, Islanding Detection, Teleprotection, Cellular, LTE

I. Introduction

A power system island occurs when generation becomes electrically separated from the utility’s power system. When this separation occurs, it is possible for the generator to continue to supply power to the island, independent of the utility. Unless appropriate measures are taken, this island condition can otherwise remain indefinitely, so long as the generator has enough capacity to meet the demands of the load (otherwise the generator would be isolated due to voltage, frequency, or other protection devices). [3]

Islanding occurs as a result of system operations, such as the operation of isolating devices like breakers, disconnect switches, and reclosers. Other events such as system switching operations, environmental issues, and equipment failure may also cause power system islanding. [3]

Islands may be formed intentionally or unintentionally. A micro-grid, for example, is designed to intentionally separate from the utility, running autonomously, and reconnecting again when desired. In this case of intentional islanding, the micro-grid is designed to not export power when islanded. As a result, the micro-grid will not be able to supply power outside of its own domain. Still, while not intentionally

islanded, it is possible for a micro-grid to become unintentionally islanded, similar to other traditional grid tied generation sources.

The following discussion around islanding will focus on the unintentional type, where unmitigated risks present a concern. Commonly, communications channels are used to mitigate against the risks of unintentional islanding. Often, establishing these communications channels presents a challenge as the appropriate channels may be cost prohibitive, not easily obtained, or suffer from performance issues. As a result, these challenges may reduce the return on investment (ROI) for the generator, or worse, make the investment not worthwhile. Today, with the wide use of cellular LTE networks and technologies, the opportunity for alternative, lower cost communications channels are possible. Cellular LTE can offer good performance at a significantly lower cost when compared with traditional leased lines or fiber deployments. This will improve ROI and may also help reach renewable energy targets.

II. Islanding Risks

When an unintentional island occurs, there are risks to which the utility as well as the public may be exposed. These typically are risks to personal safety, power quality and equipment damage.

Personal safety is a concern as the generator may back feed power onto disconnected lines. This poses a risk to utility personnel working on these lines, which may be presumed unenergized, but also can be a risk to the public in the case of downed wires within public accessible areas and roadways.

Power quality is also likely to be affected during unintentional islanding. While islanded, regulation from the grid is lost. As a result, power regulation will be reduced, possibly exposing customers to fluctuations in voltage and frequency. As a result of these fluctuations damage can occur with customer and utility equipment within the island.

Also, for synchronous generation, it is necessary to be resynchronized to the grid before reconnecting. Without resynchronization damage can occur to the generator equipment. Consequently, it is necessary to trip the generation so it can be synchronized again.

For the reasons stated above, IEEE 1547 – Standard for Interconnecting Distributed Resources with Electric Power Systems, recommends that an unintentional island be detected and removed within two seconds of an occurrence.[1][3]

III. Anti-Islanding/Islanding Detection

Methods used to mitigate against the associated risks of unintentional islanding are often referred to as anti-islanding protection. This does not refer necessarily to preventing the creation of intentional islands (i.e. micro-grids), but rather applies to the prevention of the existence of unintentional islands. To mitigate against unintentional islands, it is first necessary to be able to detect the presence of an island once it is formed. This can be referred to as islanding detection.

A. Islanding Detection Methods

There are different types of islanding detection methods that are commonly used. Of these there are two major types, local and communications-assisted methods. However, detecting unintentional islands for all various system conditions can be difficult to achieve. This is particularly the case where the island load and generation are closely matched.

1) Local Method

The purpose of local methods is to detect an island condition solely from the generator station without any external communications. The benefit of this is that a minimal amount of equipment is required, reducing cost, and simplifying installation and maintenance. Local detection methods can be broken down into two types, “passive” and “active”.

Both passive and active local methods use voltage and current measurements from the generator station to determine an island condition. Passive methods commonly include under/over voltage and

frequency relays. Active methods will commonly attempt to actively alter or disturb the voltage and/or frequency. This can help determine an island condition more accurately than passive methods.

With either method, when generation and load are closely matched the voltage and frequency will be more stable and may cause the local methods not to operate when desired. This area, between load and generation, is known as the “non-detection zone” (NDZ). To reduce the NDZ, local methods must be set with a high level of sensitivity to detect an island condition. This results in a trade-off between the size of the NDZ and undesired tripping of the generation during normal system disturbances not related to any islanding conditions [2]. This will cause loss of generation at a time when the generation may be critically needed [3]. Therefore, it may not be possible to detect an island under all system conditions. Due to the associated risks of the NDZ, if local methods are to be used, utilities will commonly require minimum loads to be significantly greater than available distributed generation (DG) levels. In other words, the utility may require alternative methods where desired DG levels are a significant portion of the minimum load.

2) Communications-Assisted Method

Communications-assisted islanding detection methods do not solely use local measurements to determine the presence of an island. Using communications channels, they coordinate with other devices to determine the islanded state. This coordination requires the transfer of information between devices for successful operation.

Communications-assisted islanding detection has advantages over local passive and active methods. Although local methods may offer lower equipment and operating costs, communications-assisted methods effectively eliminate the NDZ found in local methods. Since communications-assisted methods rely on external coordination rather than local measurements, the NDZ of local methods is eliminated. Primary islanding detection can then be implemented with the communications method and the local methods can be reserved for backup. One of the main benefits of this scheme is that voltage and frequency elements can be set less sensitively, reducing the number of false positives associated with unrelated system disturbances. [3]

There are different types of communications-assisted islanding detection available. By far the most common is Direct Transfer Trip (DTT) initiated by an isolation device, e.g. breaker, switch or recloser. Other communications-assisted methods are outside the scope of this paper.

B. Direct Transfer Trip

DTT islanding detection functions through the communications of transfer trip signals. This is typically bi-directional communications with both ends transmitting and receiving information. This may include ancillary status information. For the DTT function, only unidirectional communications are necessary, with the utility end transmitting and the generator end receiving the transfer trip signal.

The sending of the DTT signal is initiated, or keyed, by the isolating device capable of creating an island condition. Typically, a ‘B’ contact from the device. This can be a single device such as a substation breaker on a radial distribution line (Fig. 1) or it can be multiple devices where several reclosers (Fig .2) or complex looped systems are used. Typically, each DTT signal will require its own point-to-point communications circuit since the devices are installed in geographically separate locations. Once the transfer trip signal is received at the generator location, the local breaker, or Point of Common Coupling (PCC) will be opened, isolating the generator, and preventing power export. For cases where multiple isolation devices must operate to form an island (Fig. 3), special logic schemes must be used to determine the presence of the island rather than tripping on a single device, not necessarily resulting in an island.

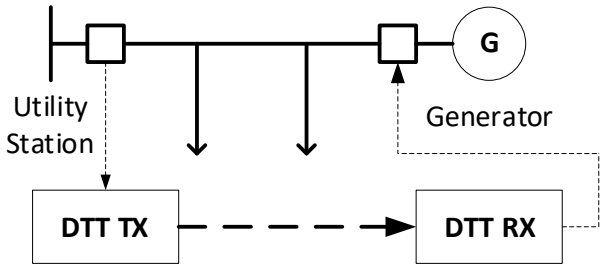

Fig. 1. DTT Radial Line Example

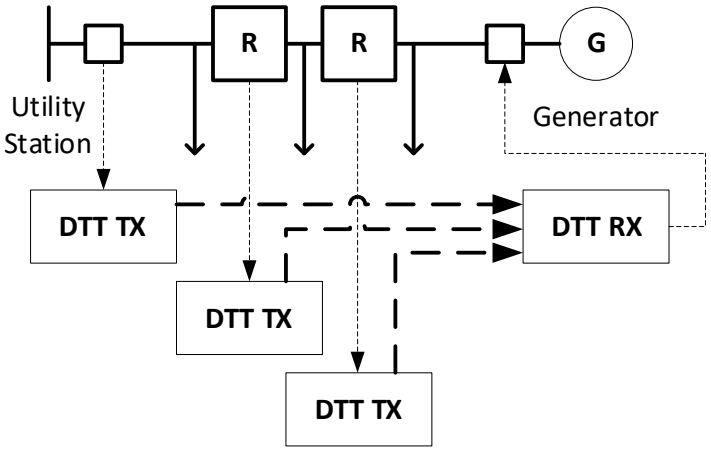

Fig. 2. DTT Example with Multiple Recloser

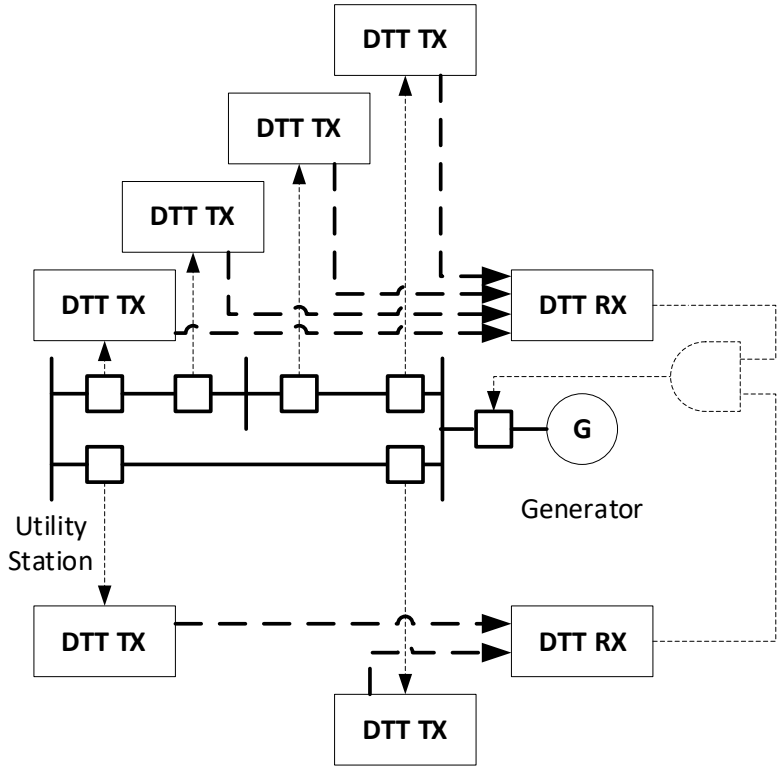

Fig. 3. DTT Looped Systems Example

As described previously, a major benefit of utilizing a communications channel for islanding detection is that it eliminates the NDZ experienced in local methods. As a result, voltage and frequency elements can be set less sensitive, and greatly reduce false operations during unrelated system disturbances. Finally, for many applications DTT is a simple solution for islanding detection. Simple radial lines with generation at one end, like that shown in Fig. 1, are the simplest type and make it easy to design, implement and maintain DTT anti-islanding solutions.

The disadvantages of DTT for anti-islanding start with the initial and/or recurring communications costs as with all communications methods. For a single DTT channel this cost may be manageable, but when the number of isolating devices multiplies, and the interconnection becomes more complex, the number of DTT channels and resulting complexity increases greatly, as in Fig. 2 and Fig. 3.

1) DTT Performance

As with other protection applications, like line protection, that use communications, we must consider the core performance parameters of the communications channel. These parameters are security, dependability, and latency. Security is defined as “the resistance to false operation during adverse conditions such as a poor signal-to-noise ratio or poor bit error rate”. Dependability is defined as “the ability to operate when desired during adverse conditions”. Latency can be defined as “the total time between the initiation of the DTT signal at the transmitting equipment and the physical or actual operation at the receiving equipment”. Typically, security and dependability have an inverse relationship with each other. Measures taken to improve security will often negatively impact dependability. Conversely, measures taken to improve dependability will often negatively impact security. As a result, optimizing security and dependability becomes a balancing act which must be considered when selecting communications channels and parameters. Security is particularly important with any DTT-type signal, including islanding detection. Since a DTT signal can directly cause a trip to occur (it is unsupervised by other elements), a high level of security is needed to prevent false operation and loss of generation. Dependability, although not as critical as security, is still important. When a communication circuit is used as the primary source of islanding detection, dependability becomes somewhat like the NDZ as with local detection. If the DTT receiver does not receive the intended transfer trip signal during the unintentional islanding event, the island is effectively not detected [2] and backup methods will be required to intervene. For the reasons stated above, when selecting DTT communication channels and methods, thorough consideration should be given to these communications channel parameters. [3]

IV. Communications Channels

The type of communications channels selected for DTT is important. Some communications methods can help alleviate the complexity and duplication of devices. Multi-point communications can help reduce the number of independent communications channels required. For example, using a shared wide-area network (WAN) with multicast IEC 61850 GOOSE communications the number of individual point-to-point communications circuits can be greatly reduced. The common legacy type communications are limited to point-to-point and can be cost intensive. Alternatively, current generation communications technologies feature multi-point functionality and much lower costs.

Factors to be considered in selecting channels include availability, equipment cost, operating cost, and reliability. Whichever method is selected, it must conform to the application’s security, dependability, and latency requirements. For leased channels, service level agreements (SLA) may specify pertinent metrics in order to meet the desired performance.

A. Legacy

There are several legacy type communications channels that have traditionally been used for DTT islanding detection. These include fiber optic, Time Division Multiplexed (TDM) digital networks, analog phone line, digital phone line and power line carrier.

Although direct fiber optic is an excellent communications medium, it quickly becomes cost prohibitive as the distance between the utility substation and the generator increases and the number of

communications channels multiplies. The cost to run fiber optic cables is estimated to cost well over $20,000 per mile or more in certain environments.

This often limits the selection to leased services from telecommunications providers. Traditionally these have been copper phone lines utilizing audio tone frequencies or digital TDM circuits like T1. These were readily available and due to the extensive telecom footprint were available in many hard to reach places. In some geographical areas these are still commonly used but have become more costly or are suffering from reduced reliability. This is a result of the telecommunications migrating away from these legacy technologies to packet based and wireless cellular communications. The market demand for legacy communications and the provider's willingness to sufficiently support them has been significantly reduced.

As a result, wireless communications options are being explored as an alternative. Particularly cellular technologies are attractive due to their availability and low cost of entry.

B. Cellular LTE

Long-term evolution (LTE), sometimes referred to as "4G LTE", is a 3rd Generation Partnership Project (3GPP) standard developed for both mobile and fixed devices. 4G LTE provides higher broadband speeds at lower latency than its predecessors. Due to the nature of being standards based, it makes different vendor's products interoperable. It has been traditionally used in the consumer marketplace; however, as time has gone on and the technology reliability and coverage has progressed, the use in industrial spaces is becoming more and more prevalent.

1) Network Types and Infrastructure

There are two different methods of providing service to the Customer Premise(s) Equipment (CPE). One method is to connect into an existing public carrier network such as Verizon or AT&T for example. Another method is to connect into a private LTE network. Both options have benefits and drawbacks. By using a public carrier, the turn up time is very low since most of the deployment and leg work have already been completed, this drastically reduces the up-front costs, but requires a higher recurring cost. A private LTE network is essentially a smaller/scaled-down version of a public carrier network which is owned or leased by the utility for private use. This gives greater security and reliability while also eliminating the risk factor of depending on an outside organization for maintenance and system repairs. The up-front costs of a private network are higher due to installation and obtaining spectrum, however, the recurring costs are minimal since there is no monthly bill.

News of security breaches in all sectors of the economy are increasing, which is putting an extremely heavy focus on cybersecurity. While running on a private LTE network does provide greater isolation benefits that a public carrier would not be able to provide, there are options on the public carrier to increase the security of the network. One method is to use a publicly IP addressable CPE and then secure the device using access control policies and virtual private network (VPN) connections. Another method is to obtain a private Access Point Name (APN) from the carrier. This provides a private network in a sense that it cannot be accessed from the public internet very easily. The cellular network is given a private IP subnet and the only way to access it from the outside world is to open a VPN connection to the carrier. This VPN connection is optional since you could instead use one of the CPE's that is already on the private network as an access-point into the network. One drawback to this method is that even though it is a "private" network, the user data is still traversing the public carrier's network, so the use of a VPN is still recommended.

Another important factor for DTT when comparing public carriers to private LTE is latency. On a public carrier most times the latency will be within tolerance for a DG DTT system, however, this cannot be guaranteed since there will be other users coming and going on the network and have periods of network congestion. Where a private LTE system can excel is the fact that the bandwidth usage is determinate and the administrator can configure quality of service (QoS) policies to maintain a specific service level agreement (SLA), thus guaranteeing a maximum latency and guaranteeing a minimum bandwidth.

2) Redundancy Options

Maintaining availability of the network is one of the highest priorities. This can be achieved by the use of multiple towers available to connect to, but this may not always be an option due to using a public carrier's existing towers or being cost prohibitive on a private network to deploy a high quantity of towers. Other techniques can be used to maintain high availability. One example of this is to use Dual-APN CPE's. This allows the device to failover to a secondary network in the case of a failure on the primary network. The dual APN functionality could be used on two public carriers: a public carrier with a private network, or two private networks. The technology of using Dual SIM has progressed to the point that devices can monitor the ability to pass traffic over the network or even the quality of the wireless signal and switch to the backup SIM/network before the failure even occurs. Another method that can be used along with the dual SIM function is to have a second interface available on the CPE. This could be Ethernet, Fiber, or another Private Radio Technology. This second interface could be primary or secondary to LTE. Many users choose to use both interfaces simultaneously, similar to an out-of-band management channel or even for parallel system design such as using PRP for seamless path failover.

3) Use with IEC 61850 GOOSE

DTT is implemented using IEC 61850 GOOSE, which is typically considered a Layer-2/ethernet based protocol. Except for routable GOOSE (R-GOOSE), this is not natively compatible with cellular networks since they operate at Layer-3/IP. In order to bypass this incompatibility, there are some common standards that can be used such as a Layer 2 Tunneling Protocol (L2TP) or Generic Routing Encapsulation (GRE) tunnel.

V. Real-World Testing

To verify the validity of utilizing Cellular LTE communications for DTT islanding detection, it is necessary to perform real-world testing to demonstrate the system's performance prior to implementing on a live system. This testing must include verifying the critical performance parameters that are key to the operation of the protection system, as discussed previously.

A. Test Case

The goal of the test case is to simulate a DTT system for a simple two- terminal application using LTE cellular communications as closely as possible to a real-world application. Figure 4 depicts the real-world application being simulated while figure 5 is the actual test setup with location A representing the utility station and location B the generator.

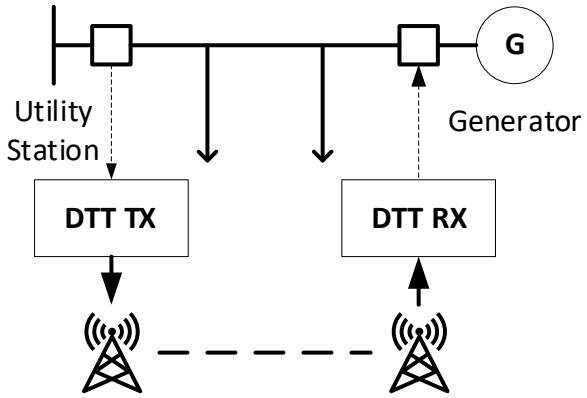

Fig. 4. DTT Cellular Application Example

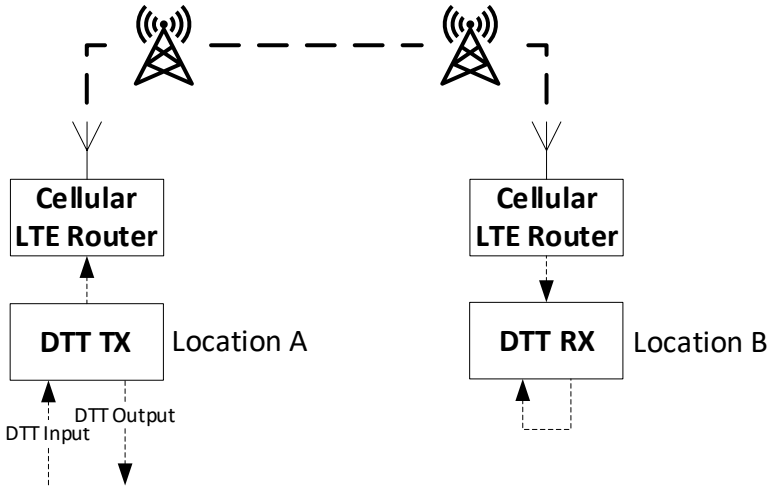

Fig. 5. DTT Cellular Test Setup

1) DTT Transmitter and Receiver

For the test case a common multifunction programmable teleprotection device was used as the DTT transmitter and receiver. This device was equipped with an Ethernet teleprotection communications interface. The Ethernet interface was chosen due to the ease of transporting native Ethernet over LTE cellular as opposed to using serial or digital TDM protocols which would require a conversion process to Ethernet. Aside from the simplicity, there will be a latency savings without the need for serial or TDM to Ethernet conversion. The Ethernet teleprotection interface utilizes standard layer 2 multicast GOOSE protocol. This provides the possibility of interoperability with multiple vendor devices as it is not a proprietary protocol. In addition, since GOOSE is multicast by nature it allows for multipoint communications which will be beneficial when scaling up to more complex systems requiring multiple terminals.

At location A (see Fig. 5), the DTT function is keyed from an external contact. This initiates the device to send a change of state GOOSE message, signaling the DTT function. On successful receipt, the receiver at location B closes a DTT output contact. This contact would normally energize a trip coil to isolate the generation from the line. In this test case, it was decided to instead key another DTT function back to the transmitter, creating a round-trip test. The purpose of this was to be able to evaluate the critical performance parameters from a single end with a common time reference. As a result, all latency measurements would be approximately double the one-way time delay. In this way it was also possible to evaluate bi-directional communications for other applications that would require communications from generator to the utility.

2) Cellular Router

To transport the GOOSE traffic between the DTT transmitter and receiver, an industrial wireless communications router was used. Like the DTT equipment, this device is environmentally hardened for utility substation environments and is capable of being powered from common station battery voltages without the need for external power converters.

The cellular router, to transport the layer 2 DTT GOOSE, must be configured appropriately to do so. For transport over the LTE cellular network, it is necessary to encapsulate the layer 2 GOOSE packet. Generic Routing Encapsulation (GRE) was used to bridge the MAC frames across the tunnel.

Due to the critical nature of the communications and necessary security it was desired to encrypt the traffic. An IPsec Virtual Private Network (VPN) was used to provide end-to-end AES256 encryption. This is a typical level of encryption for critical cyber secure applications. It was known that this may add some additional delay or latency to the DTT but was necessary for the evaluation of the real-world application. In realty the additional delay is relatively insignificant to the baseline delay.

Another cyber security feature that was implemented in the router was a firewall Access Control List (ACL). Since this is a public cellular service the routers are configured with a public IP address. This exposes the connections to the internet. To limit the connections to the routers from the internet the ACL was used to restrict certain unnecessary traffic. In addition to providing an additional level of security this also reduces the amount of data usage and resulting data charges.

3) LTE Cellular Service

In the real-world the cellular service used will be largely dependent on availability in the area. Location A in the test case was geographically located in a valley with relatively poor cellular service and limited options. As a result, the best suitable option was utilizing Verizon LTE service.

The LTE service selected was a standard machine-to-machine (M2M) plan on a public cellular network. Service plans of this type are typically inexpensive and include a monthly access and data usage charge. Charges less than $5 per month and $0.05 per megabyte are common. These charges are significantly less than other typical audio tone or T1 services.

B. Test Results

The test system as described was commissioned and communications were established between the two locations. After which it was possible to perform testing to evaluate performance. As discussed previously, testing would consist of the critical DTT performance parameters: latency, dependability, and security.

Latency, or the measured delay from initiation of the DTT signal to the received output, was measured 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 delay. Although this one-way delay may be about 20-30ms more than would be typical for wired type communications it is appropriate for this type of application and is not significant enough to adversely affect the ability to achieve the IEEE 1547 two second islanding prevention recommendation. To characterize the change in latency over time and under different conditions, dependability testing was used.

With dependability testing the DTT signal is routinely sent and checked for receipt within a defined timeframe. If a DTT output was not received or was received too late it is considered a “missed command”. An additional requirement was that the DTT signal must be received for at least 1ms to be considered valid. With rapid successive testing it is possible to calculate the probability of a missed command (Pmc). As with the latency testing, dependability was performed as a round-trip test, using the average delay time plus a buffer to evaluate the received signal. Three separate evaluation timers, 100ms, 120ms, and 150ms were used to calculate three different Pmc and help characterize the varying latency. For approximately eight hours this test was run with the DTT signal being initiated two times per second. The results of this test are listed in Table 1. During this test there was no interruption in communications identified. Consequently, the missed commands are a result of exceeding the evaluation timer rather than being completely missed altogether. Based on the three different evaluation timers, the variability of latency, at a high confidence level, does not exceed 150ms round-trip or 75ms one-way. In fact, the vast majority are received within 120ms/60ms. It should be noted that a single change-of-state GOOSE retransmission was used in this testing. The retransmission occurred 4ms after the initial change-of-state was sent. This provides the additional opportunity for the DTT to be received in the event the first packet was lost.

Evaluation Timer	DTT Sent	DTT Received	Pmc
100ms	58,748	55,642	5.3%
120ms	58,748	58,588	0.3%
150ms	58,748	58,695	0.1%

Table 1. Dependability Results

Security testing often takes extensive testing which can last for months. With digital communications and error checking it is very unlikely for noise resulting in bit errors to generate a false operation. In lab environments this is accelerated by increasing the Bit Error Rate (BER). Since the test case was to be as close as possible to a real-world application, with no forced bit errors being injected, and very low BER, security was evaluated during the period of availability testing.

The purpose of availability testing was to evaluate the cellular communications over a longer period of time and monitor communications alarms to determine the amount of time the communications circuit was available. In many cases utilities may require isolating generation when communications are lost for set time. Usually this is anywhere from hundreds of milliseconds to one second. Loss of communications tripping is a nuisance to generators and can be problematic, especially in cases where legacy type communications are not maintained well by the provider. Unfortunately, this is a growing issue as providers have moved away from these legacy technologies and infrastructure. By measuring availability, a sense of how frequently this can occur with cellular communications can be gained. Availability testing was done by using receiver communication alarms and the duration of the alarms to determine when the channel was unavailable or not able to communicate. During this time the communications channel was left in an “idle” state, meaning no change of state messages being sent. Only the routine “heartbeat” messages were being transferred between the DTT equipment. On loss of the “heartbeat” message a communications alarm is declared and subsequently cleared when received again. After a period of 28 days and 1 hour, there was a total of nine communications failure events. The total cumulative unavailable time was 535 seconds with the largest event being 395 seconds and a mean duration of 60 seconds and median of 10 seconds. Chart 1 details the nine alarm events. Calculating the percentage of total available time, without alarms, results in 99.98% availability.

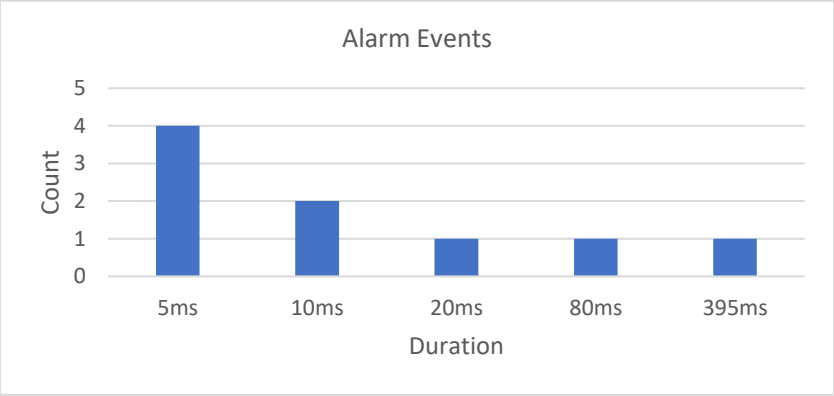

Chart 1. Availability Alarm Events

C. Cost Comparison

As mentioned previously, the routine costs of a M2M cellular service plan can be significantly less than traditional wired services like T1. Table 2 details the cost comparison of a typical T1 service with a M2M cellular service. T1 service costs can vary significantly from place to place. An estimated average of $250 per month is based on industry experience and is likely conservative in many areas.

The majority of the M2M cellular service cost will be from the resulting data usage charges. A single DTT terminal is estimated to use 500MB of data per month. This estimate is based on sending a typical GOOSE packet, sized less than 150 bytes, every two seconds plus additional overhead. The estimated overhead largely consists of additional data used for VPN and IPsec encryption. Not considered is non-essential overhead associated with device management, failure detection, and time synchronization.

Service	T1	M2M LTE Cellular	Difference (Savings)
Monthly Access Charge	$250	$5	$245
Data Charge @ 500MB/mo	$0	$25	($25)
Total (Single End)	$250	$30	$220
Total (Two Ends)	$500	$60	$440
Yearly Total	$6,000	$720	$5,280

Table 2. Cellular Cost Comparison

VI. Conclusion

In conclusion, power system islanding includes several risks related to safety, equipment damage and power quality issues. Because of this, unintentional islands are not desired and need to be prevented. In some cases, detecting island conditions is difficult, especially when using local detection methods. These methods are not as robust at detecting islands where generation and load are closely matched. Communications-assisted methods such as DTT have been used effectively for many years but can bring with them considerable costs and design complexities, especially for applications involving multiple islanding sources and complex interconnections. With the proliferation of DG comes the need for more robust, higher accessibility, and lower cost islanding solutions. [3]

LTE cellular communications is an attractive option due to its wide availability and low cost. With the increasing presence of packet technologies in the power utility space, cellular service can be easily utilized for DTT applications for distributed generation. Also based on the results of the testing the performance is quite good and suitable for the application, even utilizing public networks. Additional benefits include significant cost savings versus other traditional methods. In areas where traditional services have reliability/availability concerns, LTE cellular can also offer an improvement.

Finding the appropriate type of cellular network is important and may vary depending on the needs of the business. For example, choosing public or private infrastructure and APNs, comes down to a cost/benefit analysis. Either way there are many options for managing the pros and cons of each to find a suitable solution. This makes LTE cellular a viable option for DTT islanding detection that can provide a great alternative to traditional methods.

VII. References

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

[2] M. Ropp and A. Ellis, "Suggested guidlines for anti-islanding screening," Sandia Report SAND2012-1365, 2012.

[3] B. Dob and C. Palmer, “Communications assisted islanding detection: Contrasting direct transfer trip and phase comparison methods”, 2018 71st Annual Conference for Protective Relay Engineers (CPRE), College Sation, TX, USA.

VIII. Biographies

Brian M. 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 IEEE with over seventeen

years of experience in the power utility industry, 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.

Thomas J. Schwartz received his BS in Electrical Engineering from the Rochester Institute of Technology in 2017. He is a Cisco Certified Network Professional (CCNP) with over 14 years of experience in the industrial communications industry, focusing on power utility, oil and gas, water and wastewater communications. He is currently the senior technical application engineer for North America in the GE Industrial Communications business.