Requirements and Methods for Reducing Fault Clearing Times in Smart Grids

Alexander Apostolov

OMICRON electronics

1 Introduction

One of the main characteristics of Smart Grids are the high level of penetration of distributed energy resources (DERs) and the requirements for improved reliability of the electric power system under different abnormal conditions. The DERs are of different sizes and types and are being connected at all different levels of the electric power system – transmission, distribution and low voltage. This introduces significant challenges for protection systems at the transmission and distribution level of the system which need to be considered in the engineering of the protection devices and systems.

In order to remain in service following a short circuit fault the DERs need to be able to withstand the voltage drop until the fault has been cleared by the protection and the circuit breaker. Considering that the protection operating time depends on the type of protection, location of the fault, type of fault and fault parameters, it is clear that these factors need to be analyzed in order to identify the requirements for improvement in the fault clearing time.

The first part of the paper describes what is known as the ride-through characteristic of the DERs and the impact on the operation of the protection and control system on the ability of a DER to remain in service.

The second part of the paper discusses advanced protection functions in multifunctional IEDs and how they can be used to improve the performance of the protection system.

IEC 61850 is the dominant communications protocol recognized as one of the cornerstone technologies for the Smart Grid that brings significant benefits to the industry and allows the more efficient integration of devices of different types into systems. The paper describes the characteristics of the high-speed peer-to-peer communications defined in the standard and how they can be used in protection schemes to reduce the fault clearing time.

The paper then analyses the use of GOOSE messages in communications based protection schemes at the transmission and distribution level.

The use of accelerated protection schemes based on what is known as a wide-area GOOSE is described at the end of the paper. Comparison with the Zone 2 fault clearing times and addressing concerns related to cyber security are discussed.

2 Requirements for the protection and control of systems with DERs

Distributed generators are being typically connected to sub-transmission or distribution systems. The definition of such systems varies between utilities and in some cases systems with voltages as high as 138 kV may be considered as distribution. The addition of distributed generators has a significant effect on the system. The levels of short circuit currents, the dynamic behavior of the system following such faults, the coordination of protective relays are affected and have to be considered in the selection of the protection system. Line protection settings and criteria should take into account in-feed effect, possible power swings and generator out-of-step conditions.

The increased fault clearing times that are caused by the in-feed effect of a distributed generator may not be acceptable to customers with sensitive loads. The voltage sag is experienced not only by users on the faulted feeder, but also on the adjacent feeders, connected to the same distribution system.

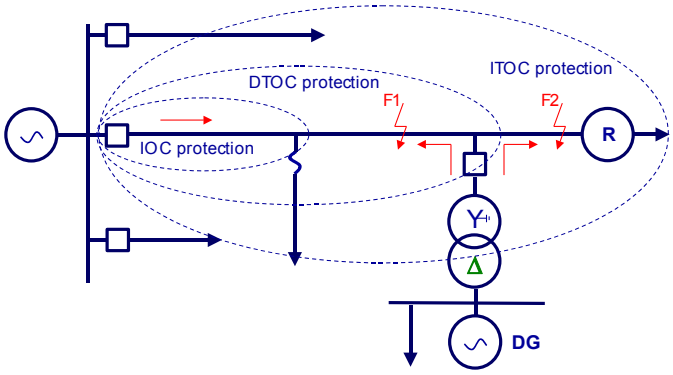


Fig. 1 Distribution feeder with DG

Figure 2 shows the areas of impact of voltage sags or swells on sensitive equipment and demonstrates that the impact depends on two characteristics. The first characteristic of a voltage sag – the depth – is a function of the type of fault, fault location and the system configuration. It will also be affected by the state of the distributed generator – if it is in service or not. Single phase-to-ground faults lead to voltage sag in the faulted phase and to voltage swell in the healthy phases. The level of voltage increase is also affected by the grounding of the interface transformer and should also be taken into consideration.

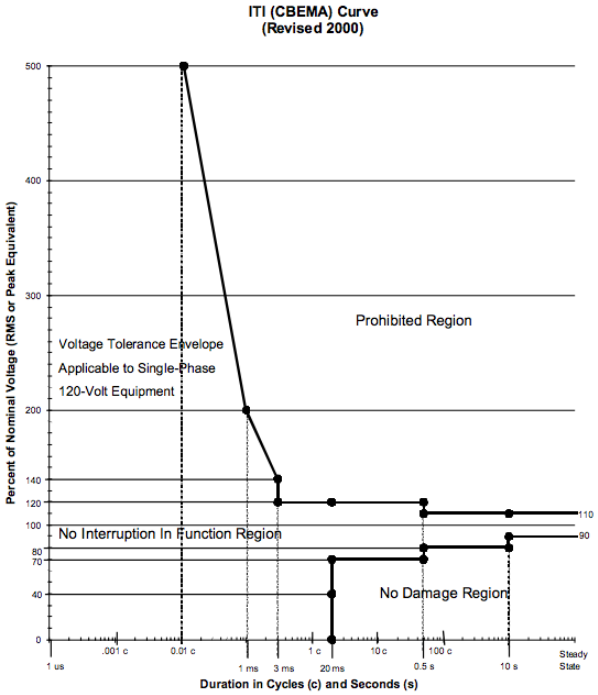


Fig. 2 ITI (CBEMA) curve

The same two characteristics of the fault also have an impact on the ride-through capability of the DER. Figure 3 shows an example of a ride-through characteristic.

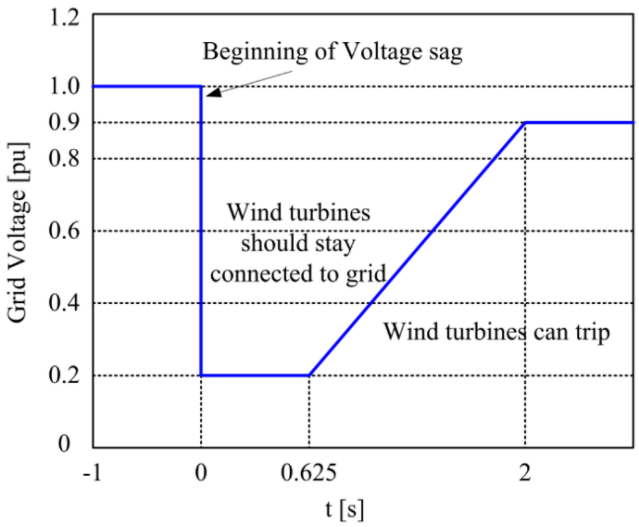


Fig. 3 Ride-through characteristic

This is something that we can't control, but we have to study in order to be able to predict or estimate the effects of different faults on the sensitive equipment. The second characteristic of the voltage sag – duration – is the parameter that we can control by properly applying the advanced features of multifunctional protection relays.

The distributed generator interconnection protection is subject to many papers, as well as standardization work, such as IEEE P-1547. It is clear that the location of the fault and the infeed from the generator will lead to increase of the fault clearing time and coordination problems. This depends more specifically on the type of distributed generator and its interconnection with the electric power system.

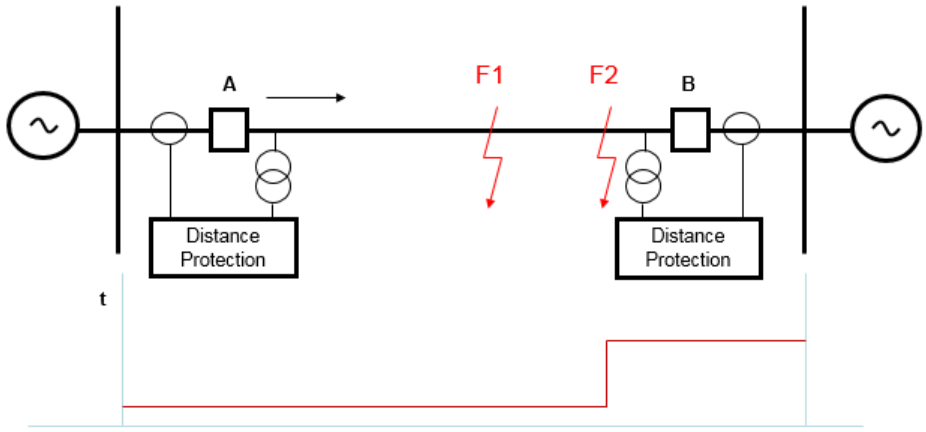


Fig. 4 Distance protection of transmission line

However it is not only the distribution feeder protection that needs to be accelerated. When a short circuit fault occurs on a transmission line connected to a substation with DERs connected at the distribution level, the voltage drop caused by the fault needs also to be considered in the analysis of the performance of the DER and its ability to ride through the fault.

When the fault is in Zone 2 of the protected transmission line (especially on shorter lines) the time delayed trip will depend on the time delay setting which may be in the range of 300 – 400 msec. Such a delayed trip will result in the duration of the voltage sag experienced by a DER in the tripping area of the

ride-through characteristic. An accelerated protection scheme can significantly reduce the fault clearing time and bring it within the stay connected area of the characteristic.

3 Accelerated Line Protection Schemes

Conventional distance protection does not provide instantaneous tripping for all faults on the protected transmission line. Communications based accelerated schemes allow considerable improvement in the overall fault clearing time for any fault within the zone of protection, while at the same time they do not have the high-speed communication requirements that line differential protection has. This is due to the fact that in these schemes a signaling channel is used to transmit simple ON/OFF data (from a local protection device). This provides additional information to the remote end protection device that can be used to accelerate in-zone fault clearance or prevent operation for external faults. These teleprotection schemes can be grouped into three main operation modes. In each mode, the decision to send a command is made by a local protective relay operation:

In **Intertripping**, (direct or transfer tripping) applications, the command is not supervised at the receiving end by any protection function and simply causes a breaker trip operation. Since no checking of the received signal is performed, it is absolutely essential that any noise on the signaling channel isn't seen as being a valid signal. In other words, an intertripping channel must be very secure.

In **Permissive** applications, tripping is only permitted when the command coincides with a protection operation at the receiving end. Since this applies a second, independent check before tripping, the signaling channel for permissive schemes does not have to be as secure as for Intertripping channels.

In **Blocking** applications, tripping is only permitted when no signal is received, but a protection operation has occurred. In other words, when a command is transmitted, the receiving end device is blocked from operating even if a protection operation occurs. Since the signal is used to prevent tripping, it is clear that a signal is received whenever possible and as quickly as possible. In other words, a blocking channel must be fast and dependable.

The protection function that sends the permissive or blocking signal to the remote end determines the type of scheme used. If this is a distance element, we usually talk about Permissive Underreaching or Overreaching schemes, or Blocking schemes. If a directional element is used to initiate the transmission of a signal to the remote end of the protected line - we have Directional Comparison schemes. A directional comparison schemes can be Permissive or Blocking, with directional elements initiating the signal transmission and providing the supervision at the receiving end.

We can consider as an example of an accelerated transmission line protection scheme a Permissive Directional Comparison scheme commonly used to accelerate the clearing of all kinds of faults, including high-resistance faults that are not seen by the distance elements of the transmission line protection relays or line differential relays.

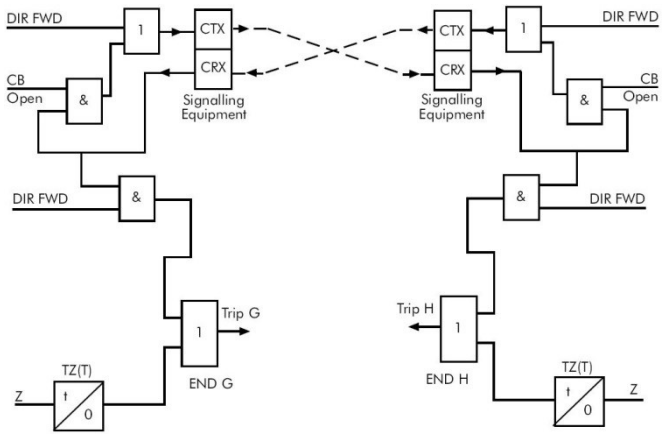


Fig. 5 Permissive Directional Comparison Scheme

The channel for a directional comparison Permissive scheme is keyed by operation of the forward looking elements of the relay. If the remote relay has also detected a forward fault upon receipt of this signal, the relay will operate. Such schemes offer some significant advantages, especially when high-speed directional detection methods based on superimposed current and voltage components are used.

Permissive schemes tend to be more secure than blocking schemes because forward directional decisions must be made at both ends of the line before tripping is allowed. Failure of the signaling channel will not result in unwanted tripping, because no signal is going to be received and the relay does not trip based on a forward directional detection only.

If the source at either end of the line is weak, the directional comparison permissive scheme uses Weak Infeed logic.

Current reversal guard logic is used to prevent healthy line protection maloperation for the high speed current reversals experienced in double circuit lines, caused by sequential opening of circuit breakers.

If the signaling channel fails, Basic distance scheme tripping will be usually available.

The challenge for the implementation of accelerated transmission line protection schemes is that they require a communications channel which, if it is a dedicated one, will require additional costs.

IEC 61850 GOOSE messages are a technology that can help us achieve these goals.

4 Wide Area GOOSE

The GOOSE message was designed for peer-to-peer substation communications and because of that it uses a three layer stack and MAC multicast. This is not suitable for messages that need to be sent over a wide area network. For that reason we need additional features to support GOOSE transmission over wide area networks.

Some network routers designed for the use in the power utility field with IEC 61850 provide features to wrap GOOSE messages into IP packets and transmit them over a WAN.

MPLS networks became the focus of evaluation and deployment in power utilities. They provide connectivity for all kinds of services within a utility, not just protection.

4.1 GOOSE over MPLS

The Multiprotocol Label Switching (MPLS) is a packet-forwarding technology which uses labels in order to make data forwarding decisions.

With MPLS, the Layer 3 header analysis is done just once (when the packet enters the MPLS domain). Label inspection drives subsequent packet forwarding.

In the traditional 7 layer OSI model Layer 2 covers protocols like Ethernet which can carry IP packets, but only over simple LANs or point-to-point WANs.

Layer 3 covers Internet-wide addressing and routing using IP protocols.

MPLS sits between these traditional layers, providing additional features for the transport of data across the network. Because of that MPLS is sometimes called a “Layer 2.5 networking protocol”.

This technology allows the engineering of paths between substations that can transport layer 2 traffic through the WAN, thus effectively extending the LAN into the remote substation. IEDs communicating via GOOSE can exchange information with remote device just as if they were connected to the same local network.

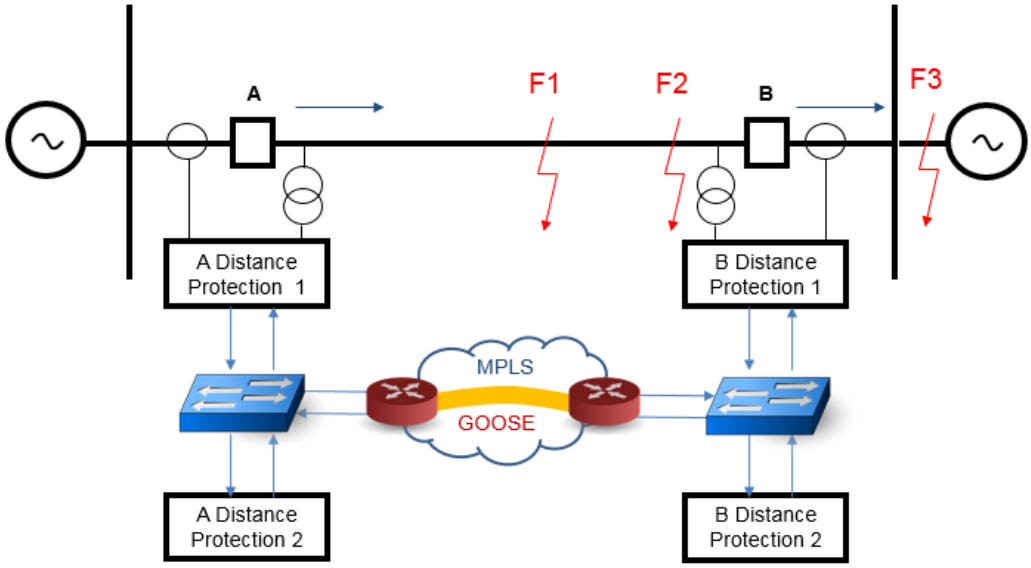


Fig. 6 GOOSE over MPLS

4.2 R-GOOSE

The technical report IEC 61850 90-5 Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118 is the document that also defined the methods for transmitting GOOSE messages over wide area networks based on IP solutions. This report selected UDP/IP as the option to transmit data over large distances. The GOOSE messages based on this technology became known as Routable GOOSE of R-GOOSE.

The Internet Protocol (IP) is a Layer 3 protocol. The Network layer adds the concept of routing above the Data Link layer. When data arrives at the Network layer, the source and destination addresses contained inside each frame are examine to determine if the data has reached its final destination. If that is true, this Layer 3 formats the data into packets delivered up to the Transport layer. The IP allows the routing of data packets (IP packets) between different networks over any distance.

The User Datagram Protocol (UDP) is a Transport Layer 4 network protocol. While TCP (Transmission Control Protocol) is a connection oriented protocol that requires first to establish communications between a client and a server, UDP is connectionless, which makes it more suitable for GOOSE communications.

UDP network traffic is organized in the form of datagrams. A datagram comprises one message unit. The first eight (8) bytes of a datagram contain header information and the remaining bytes contain message data.

A UDP datagram header consists of four (4) fields of two bytes each:

- source port number
- destination port number
- datagram size
- checksum

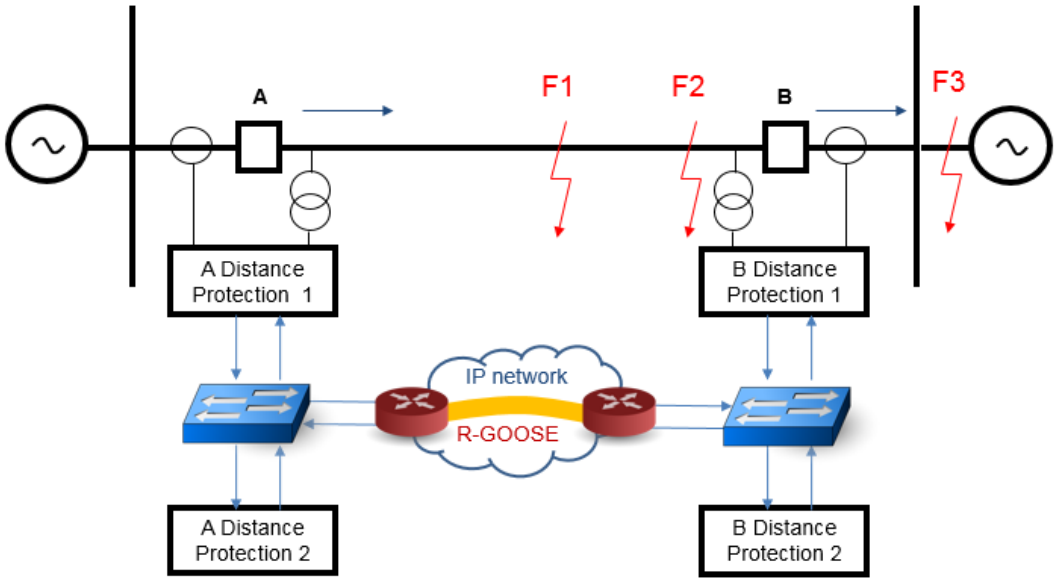


Fig. 7 R-GOOSE over IP network

The UDP checksum protects the message data from tampering. The checksum value represents an encoding of the datagram data calculated first by the sender and later by the receiver. If the checksum does not match indicating a tampered or corrupted data during transmission, the UDP protocol detects it. In UDP the check sum is optional as opposed to TCP where it is mandatory.

The many working applications of the IEEE C37.118 protocol confirm that the use of UDP for the streaming of the synchrophasor data is a proven method that can also be used for the routable GOOSE.

Considering the importance of the check sum as a cyber security tool, IEC 61850 8-1 Edition 2.1 defines

It as mandatory for the IEC 61850 implementations.

The table below shows the UDP field implementation requirements defined in the standard.

UDP	Mandatory/Optional/ eXcluded
Source Port	M
Destination Port	M
Length	M
Checksum	M

5 Propagation Time Measurements in Wide Area Networks

When measuring delay times over WAN [3], the task becomes more complex. Multiple acquisition devices need to be used and they have to be precisely time synchronized to achieve the required timing accuracy. In the following picture, this is indicated by the GPS receivers connected to the acquisition devices.

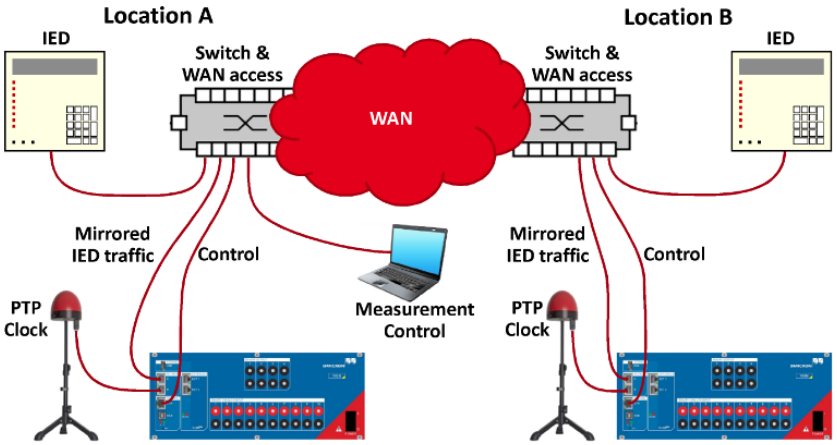


Fig. 8 Propagation time measurement over a WAN

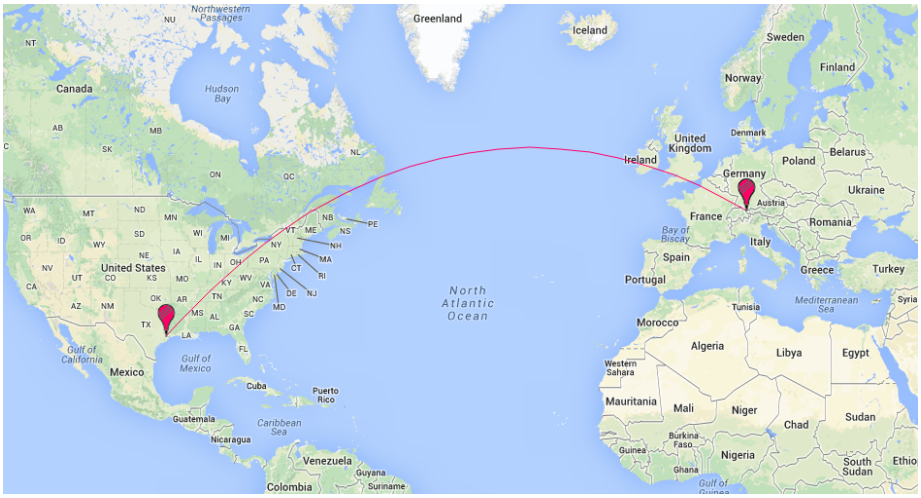
But still the whole measurement system is controlled from one single computer, making the operation as easy as possible. The expected range of the measured propagation delays is of course typically one order of magnitude larger than in LANs, but this depends very much on the bandwidth and WAN technology used.

Again, the measurement is the only way to find about the actual timing of the information exchange between the involved IEDs. A final assessment of the performance of the communication network cannot be made on theoretical evaluations alone.

Of course, such a distributed measurement setup as required with a WAN may be also used in a LAN (e.g. in a large substation) when the capture locations are too far from each other.

5.1 Transatlantic latency

To explore the extremes, a delay time measurement between two locations in two different continents was performed [1]. It is unlikely that time critical data for protection, automation and control will be exchanged over such a distance, but it serves to show the orders of magnitudes that can be expected for the traveling time of information. The following figure illustrates the locations of the two involved sites in Austria and in Texas.



Map data © 2014 Google. Draft Logic distance calculator © 2014 draftlogic.com

Fig. 9 Locations and shortest path (beeline) in between Houston, USA and Klaus, Austria

Of course, such WAN connections involve routing, which means that several convenient features that are available in LANs, as for finding devices, do not work anymore. For setting up the connections properly, the network masks and gateways in the sub-networks and the IP addresses of the involved devices need to be known.

The measured propagation delays are in the range of 80 ms to 100 ms. To show the distribution in more detail, the graphs are biased at 70 ms and the distributions are much narrower than the figure suggests. The standard deviation is less than one percent of the mean value in both directions.

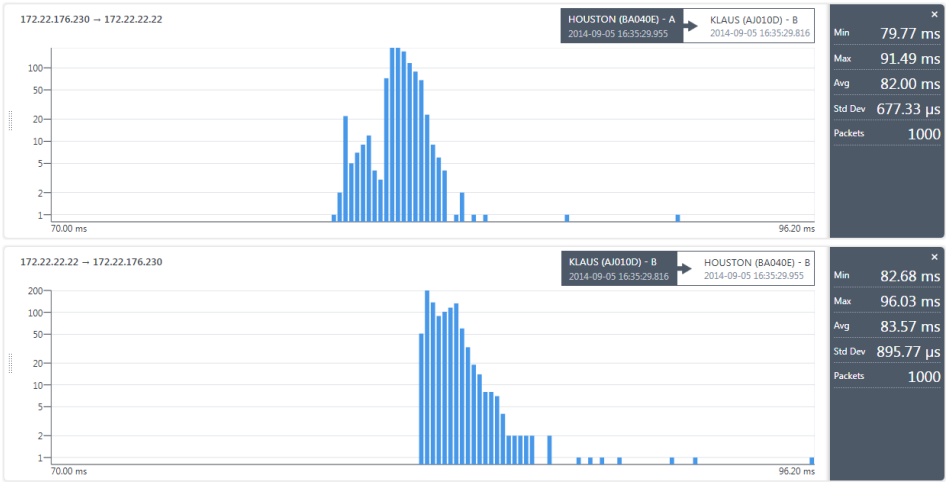


Figure 10: One-way propagation delays between Texas and Austria

The beeline distance between the locations is 8654 km (5377 mi). With the typical figure for the speed of wave propagation on electrical wires or in optical fibers (about 2/3 of the speed of light in the vacuum), the propagation time for this distance equals 43 ms. As the links will not follow the beeline and the actual way for the signals will be longer, at least 50 ms can be attributed to the propagation time in the media alone, leaving about 30 ms to 50 ms for the processing and forwarding the in the involved communication equipment.

It has to be noted that the measured transfer times of less than 100ms are not so much off typical times that occurred in the past on communication channels used for line protection schemes. The evolution of the communication networks now allow the application of proven protection schemes for even larger distances.

6 Conclusions

As can be seen from the results of the measurements of an extreme use case of wide area GOOSE communications, an accelerated transmission line protection scheme will significantly reduce the fault clearing time for faults in Zone 2 of the distance protection.

In a much more realistic implementation within a specific continental area the expected propagation delay of the wide area GOOSE is expected to be in the range of 20 msec which is in the range of the typical communications channels used for accelerated protection schemes, without the additional costs.

Such wide area GOOSE based accelerated protection schemes will help maintain the DERs in operation during and after short circuit faults at both the transmission and distribution levels of the electric power system.

7 References:

1. To GOOSE or Not to GOOSE – that is the question? A. Apostolov, Texas A&M, 31 March – 2 April 2015, College Station, TX, USA
2. Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118, IEC/TR 61850-90-5, Edition 1.0 2012-05
3. Accurately Time Stamped Traffic Acquisition and Evaluations to Assess Communication Networks for IEC 61850 Applications, Fred Steinhauser, Benton Vandiver, Thomas Schossig, OMICRON electronics, PAC World Americas Conference, September 2015, Raleigh, NC, USA

8 Biography

Dr. Alexander Apostolov received MS degree in Electrical Engineering, MS in Applied Mathematics and Ph.D. from the Technical University in Sofia, Bulgaria. He has 42 years' experience in power systems protection, automation, control and communications.

He is presently Principal Engineer for OMICRON electronics in Los Angeles, CA.

He is IEEE Fellow and Member of the Power Systems Relaying Committee and Substations C0 Subcommittee. He is past Chairman of the Relay Communications Subcommittee, serves on many IEEE PES Working Groups and is Chairman of Working Groups C2 "Role of Protective Relaying in Smart Grid".

He is member of IEC TC57 working groups 10, 17, 18 and 19. He is Leader of the Task force "Functional testing of IEC 61850 based devices and systems".

He is Distinguished Member of CIGRE and Convenor of CIGRE WG B5.53 "Test Strategy for Protection, Automation and Control (PAC) functions in a full digital substation based on IEC 61850 applications" and member of several other CIGRE B5 working groups.

He holds four patents and has authored and presented more than 500 technical papers.

He is IEEE Distinguished Lecturer and Adjunct Professor at the Department of Electrical Engineering, Cape Peninsula University of Technology, Cape Town, South Africa.

He is Editor-in-Chief of PAC World.