

Enabling Teleprotection via packet switch wide area networks with guaranteed performance

R. BAECHLI¹, A. FREI, M. KRANICH

**ABB Switzerland Ltd.
Switzerland**

Presented at the annual Western Protective Relay Conference 2018
Spokane, WA
October 15-18

SUMMARY

For reliable operation of electrical grids a variety of applications need to work together seamlessly and with an extraordinary high level of availability. In today's digital world reliable real time communication is the base enabling those applications to perform its task. For this reason operational multiservice communication networks are used. The individual applications have completely different requirements on the communication channel performance, such as latency, bandwidth, availability and symmetry. Failing on this results in critical electrical grid conditions, lack of visibility and the ability for remote control potentially leading to large-scale blackout situations resulting in substantial financial losses and reputation damage.

Applications, which have an immediate impact on grid stability have typically the most demanding requirements for communication and accordingly they need special attention. Protection applications are such critical applications since they protect the primary infrastructure of the electrical grid such as Transformers or Power Lines. Protection applications demand very distinct requirements on communication performance. Traditionally these required performance parameters have been guaranteed by time division multiplexing (TDM) based communication networks together with special devices guaranteeing performance parameters using mentioned TDM networks. An example for this is Teleprotection (distance protection), where often dedicated Teleprotection equipment is used to guarantee application specific performance parameters (e.g. dependability, security, latency) as well as convert the binary (Trip) signal to analogue or digital transport technology (e.g. G.703 64 kbit/s). With today's situation,

¹ Ramon Baechli, ABB Switzerland Ltd., ramon.baechli@ch.abb.com

where packet switched solutions have found its way into IT networks and are discussed also for operational wide area networks, this is not the case anymore. This paper will evaluate how essential performance parameters of today's protection systems are potentially influenced by migrating to new wide area network (WAN) technology. It further shows how edge of technology solutions can circumvent problems caused by the emigration and ensure that Teleprotection applications via packet switched wide area network achieve guaranteed performance parameters, in line with the Teleprotection standard IEC 60834-1 or recommendations issued by CIGRE.

First the requirements of operational utility networks, especially the communication channel performance for guaranteed correct operation of critical protection applications are summarized. Usually focus is mainly on differential protection application, which demands very critical performance parameters, and not on distance protection application. This is potentially critical since new WAN technologies also affect the performance of distance protection, not only for latency aspects, which have been analyzed so far, but also for dependability and security parameters, which are often not looked at. That is why this paper will, beside differential protection requirements, specifically look in details of distance protection requirements and the implications driven by WAN technology migration, as well as summarizing results of extensive test series done with this critical application.

Different possible approaches enabling protection applications via new PSN WAN technologies are analyzed such as TDM based Teleprotection using standard circuit emulation or new application specific solutions for distance- as well as differential protection applications.

The new solutions provides superior performance, full Teleprotection standard compliance (IEC 60834-1) in case of distance protection application and guaranteed and symmetrical latency times in case of differential protection. Hence, they enable the migration to new packet switched wide area networks (PSN) with guaranteed performance for critical protection applications.

Finally, a new generic packet based protection solution is presented making the use of recent developments in the area of IEC 61850. The new solution provides significant optimization potential and even improves the performance of the protection system.

KEYWORDS

Teleprotection, time division multiplexing, packet switched wide area networks, dependability, security, IEC 60834-1, asymmetry, jitter & wander, technology migration, IEC 61850, GOOSE

1 Introduction

Operational networks of power utilities are typically multiservice networks offering communication services to various different applications (Figure 1). Many of them still use traditional communication interfaces, such as RS-232, IEEE C37.94 or 2/4 wire E&M, which will remain in use for many years due to the life cycles of substations being long and refurbishment being complex in operational systems [1]. Application specific performance requirements need to be met in any case. If the network is not capable to do so correct operation of the end application is in danger and grid stability is at stake. This is fully independent on the implemented technology of the wide area communication network. Never the less traditionally the application specific performance parameters have been supported by the used network technology and specific adaptations have been implemented in order to guarantee the performance parameters. This lead to optimized systems for TDM WAN, which might be suboptimal for other networking technologies.

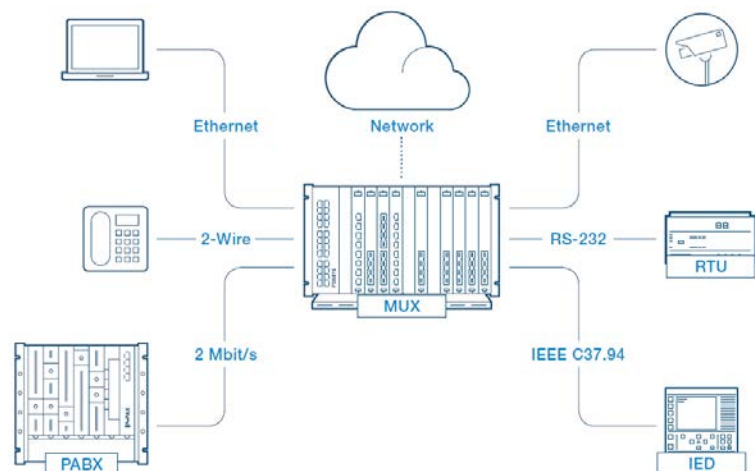


Figure 1: Typical applications and corresponding interfaces in electrical high voltage substations

Distance- and differential protection applications have been used for many years and are vital for reliable power grid operation. Due to their importance and the implications in case of none- or wrong operation they need special focus. Looking at protection systems we see that they consist of various different types of equipment connected together with distinct functionality. Each of the subsystems needs to provide the required performance in order to ensure that fault clearing times are short and damage to primary equipment due to faults is not happening. For both styles of protection schemes traditional TDM networks (e.g. SDH or SONET) have proven to comply with the stringent requirements. With the upcoming migration to new packet switched WAN the same is not guaranteed anymore. For differential protection application implications on the critical performance parameters latency, asymmetry as well as jitter and wander will be analyzed. For distance protection the implication of technology changes on latency, dependability and security will be looked at and compared with the requirements defined in the Teleprotection standard IEC 60834-1. Compliance to the application specific requirements are essential since the overall protection system only performs as expected if all the subsystems perform accordingly. Teleprotection systems (distance protection) can be built with dedicated external Teleprotection equipment or with multiplexer in built Teleprotection interface solutions allowing a more optimized setup and better visibility of the overall solution. Figure 2 shows the components of the Teleprotection system (in this picture with a dedicated Teleprotection equipment).

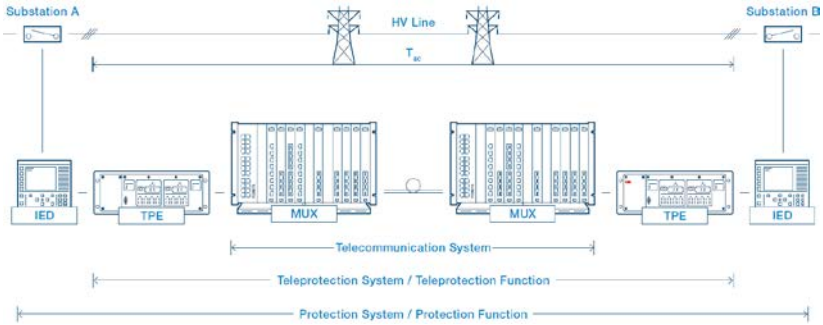


Figure 2: Protection system and split up in individual subsystems

In any case the Teleprotection system needs to guarantee application specific performance parameters (e.g. dependability, security and latency) as well as conversion from binary inputs to analogue or digital transport technology usually by using TDM interfaces (e.g. E1/ T1 or G.703 64 kbit/s). For differential protection systems the setup is very similar. A protection relay can be either connected to a dedicated converter box where relay specific protocols (e.g. IEEE C37.94) are converted to telecom equipment offered interface types (e.g. E1/ T1 or X.21) or a direct integration to the telecom equipment is possible if the same offers the required interface directly (e.g. IEEE C37.94). In both cases the external or internal Teleprotection function has typically be connected to wide area communication networks using TDM technology. The main performance parameters for distance- and differential protection applications have been optimized to the underlying WAN technology (e.g. by supporting error correction capabilities in TDM networks or using the echo timing methods for latency measurement). With today's situation, where packet switched solutions are discussed for operational wide area networks, implications on such performance parameters need to be analyzed in details. The main question to be asked is, if and how the technology change of the WAN from TDM to Packet Switched Network (PSN) influences the critical performance parameters of the Teleprotection system. The "if" is easy to answer. The fundamental and drastic change in communication technology as we see it with the migration from TDM systems to a PSN systems (e.g. MPLS-TP) influence the performance for sure, the question is just how. For differential protection it is usually understood that implications are severe and need special attention. For distance protection application often only analysis on latency implications are done. Considering the magnitude of change happening by migrating from TDM to PSN it might not be enough to just focus on latency and assume other critical performance parameters (e.g. dependability and security) are not changed, hence still in line with IEC 60834-1 requirements as before. The dependability and security values measured and approved in the TDM communication system must be reevaluated for PSN networks. In general, the conclusion that Distance Protection is easy to migrate from TDM communication networks to PSN and only latency needs to be considered is misleading and not considering the complexity behind this critical application.

2 Requirements of Teleprotection (distance and differential protection application)

The requirements of the most critical application for reliable grid operation, the protection of the high voltage powerlines, Transformers and other primary equipment, are summarized in this section. They are taken as a basis for the evaluation of technologies and solutions, which potentially enables the use of packet switched wide area communication networks, are suitable.

The fault clearance time (T_c) is a critical performance parameter of any protection system and defined in the IEC 60834-1 standard. A typical value for a high voltage transmission line is 3-6 power frequency cycles [2]. T_c is broken down in requirements for all the different subsystems. For Teleprotection systems, the maximum transmission time (T_{ac}) is the critical performance criterion when it comes to latency. For digital communication systems, T_{ac} should be < 10 ms [2], which is recommended for all kind of line protection schemes of HV lines, independent of the type of communication interface. Other organizations issue recommendations for Teleprotection communication channel latency, which go even beyond the requirements defined by IEC. For example, CIGRE recommends to have a maximum latency time of 5 ms [3].

2.1 Differential Protection

Differential protection demands very stringent requirements on signal transfer delay, delay variation and delay symmetry. It relies on the comparison of simultaneous (synchronized) samples of currents from the line ends and any time deviation imitates a virtual fault current, which could lead to unwanted tripping of circuit breakers. Figure 3 shows the typical tripping characteristics of current differential protection relays.

The no-trip (restrain area) safeguards against unwanted operation due to errors and tolerances of various system components, with communication delay asymmetry being one of these when sampling synchronization is based on echo principles. CIGRE Technical Brochure 192 “Protection using Telecommunications” [2] requests that a high performing line carrying differential protection provides a maximum delay asymmetry and delay time variance of < 0.1 ms, though more-recent publications accept values of < 0.2 ms considering that lower values

are very difficult to achieve with communication circuits other than direct fibers [3]. For sampling synchronization based on echo principles 0.4 ms of communication delay asymmetry means 3.6° phase angle error or 6.3% virtual fault current for a 50 Hz system amplitude error (4.4° or 7.7% for 60 Hz respectively), which will eventually affect the relay sensitivity setting. Delay asymmetry issues become even more prominent when switching between routes in redundant systems occur. Potential workarounds are time stamped samples using GPS synchronisation or dedicated fibres between differential protection relays. Both options are not ideal with respect to the availability, resources efficiency and operation & maintenance cost.

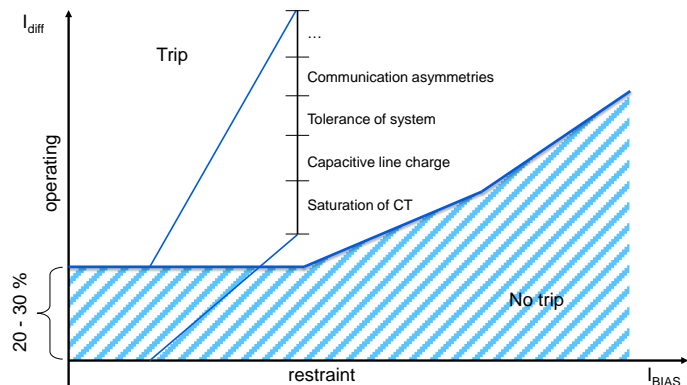


Figure 3: Tripping characteristics of differential protection relay

2.2 Distance Protection

Distance protection is based on the transfer of binary commands. In comparison to differential protection no direct comparison of current values happens on both sides, which relaxes the requirements in terms of symmetrical and jitter & wander free communication channels. The already mentioned communication channel latency is critical and results in Teleprotection command transmission times. Beside this dependability (P_{mc}) (dependability relates to the ability to issue and receive a valid command in the presence of interference and/ or noise) and security (P_{uc} = probability of an unwanted command), are critical performance parameters of a Teleprotection system and defined in the IEC 60834-1 standard. Compliance to the same ensures that the overall protection system performs as expected. Typically the

provider of the Teleprotection device confirms compliance to the IEC 60834-1 standard by performing relevant tests and sharing the results in specific diagrams as part of the technical data or user manual. Table 1 summarizes the relevant Teleprotection performance parameters for command based protection schemes based on IEC 60834-1 and a bit error rate of 10^{-6} .

Protection scheme	Trip transmission time (T_{ac})	Dependability (P_{mc})	Security (P_{uc})
Blocking	< 10 ms	< 10^{-3}	< 10^{-4}
Permissive underreach	< 10 ms	< 10^{-2}	< 10^{-7}
Permissive overreach	< 10 ms	< 10^{-3}	< 10^{-7}
Intertripping	< 10 ms	< 10^{-4}	< 10^{-8}

Table 1: Distance protection performance parameters @ BER 10^{-6}

3 Enabling transmission of traditional protection signals via packet switched wide area networks

Communication channel behaviour of TDM and PSN networks are significantly different. An example for this is the inherent Quality of Service (QoS) offering of TDM networks which packet switched networks (PSN) do not provide. In order to provide communication channels for traditional protection applications over PSN interworking function (IWF) are required. The IWF needs to map the TDM data into packets which can be transmitted via PSN and regenerate the TDM data streams again at the remote end. Such IWF are commonly used in public telecom environment, named circuit emulation (CE) and are standardized for interoperability. Other IWFs are based on application specific migration (e.g. conversion from voice to VoIP or direct conversion of Teleprotection commands to packets). In the following sections, the different approaches are explained more in details for differential- and distance protection applications.

3.1 Differential protection signals via packet switched wide area networks

For differential protection digital values have to be transported via the network, which requires an IWF. Two different IWF variants are analysed.

3.1.1 Standard based CE IWF

Two commonly used protocols are SAToP (IETF RFC 4553) and CESoPSN (IETF RFC 5086). Both CE solutions, in accordance with ITU-T G.8261, cannot guarantee maximum asymmetry values in case

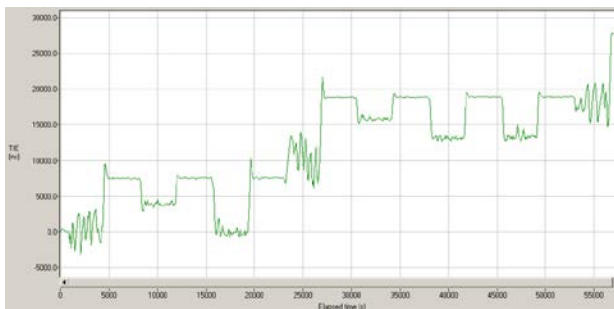


Figure 4: Accumulation of long term residential jitter buffer delay depending on traffic pattern

of long operation periods. In ITU-T G.8261 either a defined observation period is specified², or the observation period is at the same time a parameter to calculate the mask value³. This does not guarantee long-term phase stability under all conditions. Figure 4 shows a long-term Time Interval Error (TIE) measurement of accumulated jitter. Nicely visible is the missing phase adjustment, which makes it impractical for differential protection. As standard telecommunication application are typically tolerant against jitter/wander and asymmetric delay, the stand-

ard CE method is not taking care of such effects. Therefore, this approach is not suitable for utility specific HV-line differential protection applications.

² e.g. MRTIE of a 2048 kbit/s interface wander budget is based on a window of 1000 seconds (ITU-T G.8261, 9.1.1.2)

³ e.g. TDEV maximum value shall be below $3.1623\tau^{0.5}$ for $10 \text{ s} < \tau \leq 1000 \text{ s}$ for EEC-Option 2 (ITU-T G.8261, 9.2.1.2)

3.1.2 Application specific IWF

As shown before very stringent application requirements have to be met if differential protection signals are transmitted via fibre optical wide area communication networks. Without packet synchronization, CE methods rely on adaptive timing circuitry to derive the clock from the incoming packet stream.

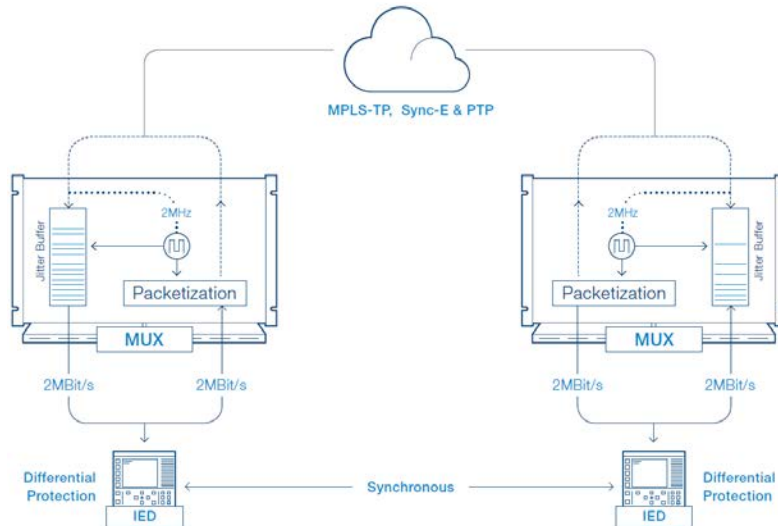


Figure 5: CE jitter buffer phase (re-) synchronization for differential protection application

Frequency stability implemented in state-of-the-art switch hardware with similar performance to SDH networks is provided by means of synchronous Ethernet (Sync-E) according to ITU-T G.8262/Y.1362 and ITU-T G.8264/Y.1364. Strengths of this technology are the physical layer implementation where it is not subject to load impairments, the link based nature as well as the stable holdover during topology changes. The drawback is that no phase information is available among the network elements, which may lead to a phase jump after a source switch or to a long-term wander

resulting in virtual fault currents on the differential protection relay.

Another widely deployed and well-standardized technology to distribute frequency and/or phase information with sub-microsecond precision within a network is IEEE 1588v2. The protocol is partially hardware supported to allow high precision time stamping, however it requires bidirectional packet exchange of synchronization and timing messages processed by a CPU. While the advantage is the high precision and the availability of Time of Day (ToD) information, the disadvantage is that the phase learning algorithm and re-learning after a source switch takes up to several minutes due to the limited frequency of received timing information.

The proposed application specific IWF solution for differential protection provides various traditional access ports, which can be used for any kind of protection relay type and interface. While every synchronisation technology discussed above has its shortcomings in regards to the demanding requirements of differential protection services, the assessed solution provides CE jitter buffer phase (re-) synchronization by means of hybrid Sync-E/ PTP operation. This approach allows phase adjusted data payout at both ends of the circuit via a jitter buffer (Figure 5).

The approach also takes advantage of the fine bandwidth granularity of packet technologies optimizing bandwidth usage compared to TDM solutions, wire speed hardware supported packet switching and packet duplication of the traffic streams to enable hitless redundancy. This guarantees the required performance parameters for differential protection.

Presentation of field test

A field test using the specific IWF for differential protection has been implemented within the network of a Swiss utility and consists of five TDM/ PSN hybrid multiplexer platforms distributed over about 50 km of the fiber optic network (Figure 6).

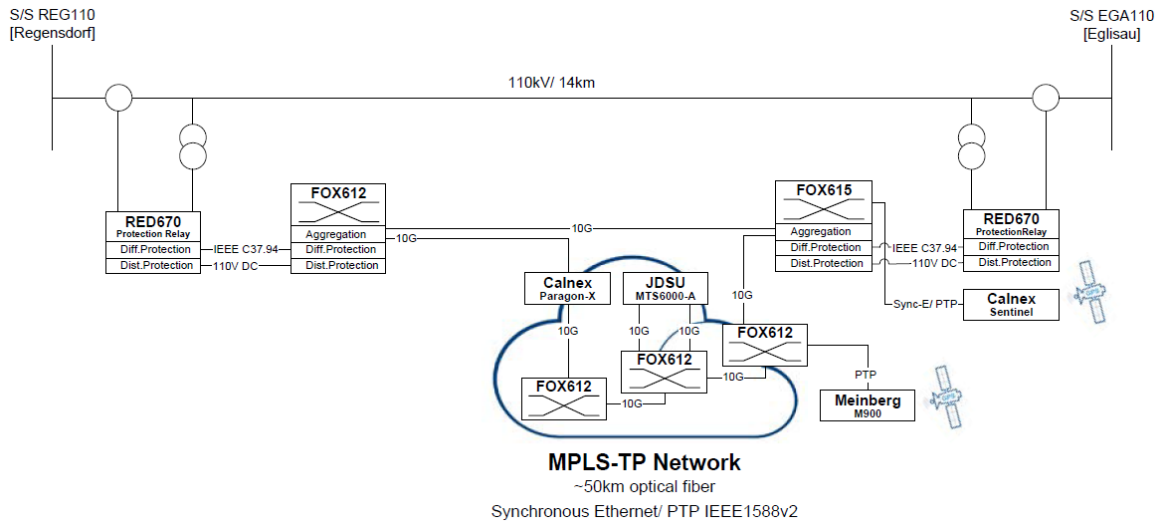


Figure 6: Field test system layout

WAN capacity is chosen at 10 Gigabit Ethernet using MPLS-TP technology providing bidirectional paths. The protection relays in the left and right substations (Figure 6) protect a 110 kV high voltage line and are equipped with IEEE C37.94 interfaces for differential protection and 110 VDC contact interfaces for distance protection. Sync-E as well as PTP is fed by a grandmaster device (Meinberg) and propagated by the multiplexer platforms throughout the network. PTP is realized as a chain of boundary clocks. Both, Sync-E as well as PTP, operated in a hybrid mode, are clocked from a single source.⁴ Redundancy for data and synchronization is given by the ring structure of the network.

For differential protection the authenticated, phase timed CE deployed provides a cyber secure, bidirectional, symmetrical point-to-point wire service over MPLS-TP. The service is assigned to the highest priority multiplexer queue without compromising on system protocols and stability. The CE buffer size was engineered to 6 ms, which typically provides stable functionality with a reasonable differential protection performance. The CE timing is coupled with the frequency and phase information available within the multiplexer to provide end-to-end delay symmetry. The communication module of the line differential protection relay deduct the synchronization from the C37.94 signal on both ends.

Strict scheduling of the queues is applied and hitless protection by traffic duplication at the service end-points is used. The benchmarking goals for this field test are to reach or exceed the requirements of the protection standards as well as the known long-term TDM network performance not only under normal conditions but as well under stress and fault conditions:

- *System phase stability in the sub-micro second range during stable operation*
- *Channel delay asymmetry below 0.1 ms under all conditions*
- *Absolute channel delay below 10 ms*

To verify system phase stability and service performance a Calnex Sentinel synchronization tester is used. By applying specific fault conditions and with

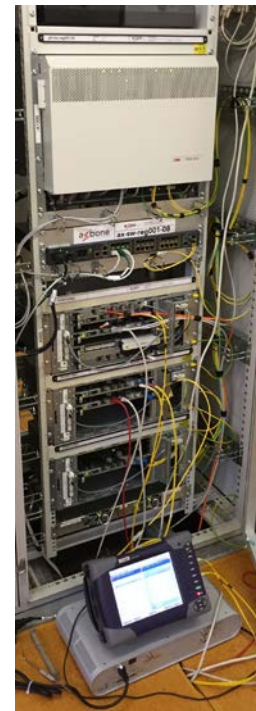


Figure 7: Field installation in one of the substations

⁴ This provides GPS independency and adds resiliency to GPS spamming and spoofing effects.

the help of a JDSU MTS6000-A traffic generator as well as the Calnex Paragon-X network emulator, the system is assessed.

Results of field tests

Under normal operation

TIE measurements with the Sentinel are performed to prove long-term phase stability from a communication perspective. The test intervals are set to seven days at a time (due to measurement device memory limitations) and repeated over months (Figure 8, also includes stress test with forced fiber break). These measurements reflect the inaccuracy of Sync-E and PTP over the five synchronization hops against GPS, which is the common time source of the grandmaster and the Sentinel. Accuracy of the measurements narrows down to the accuracy of GPS, which is sufficient in this case. The synchronization chain is stable, it regulates around the reference grandmaster ToD. A system phase stability below $1 \mu\text{s}$ is reached over the total observation time of several months. *The values lie within any network limit or standardization masks and the sub-micro-*

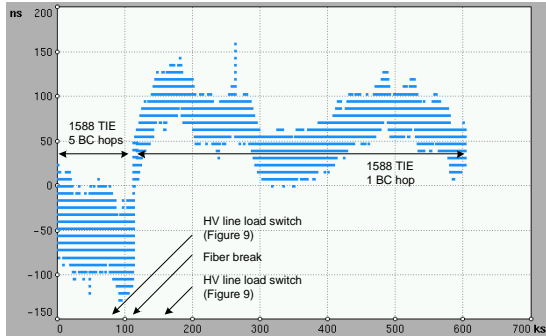


Figure 8: Measured communication network TIE (y-axis) stability (\rightarrow max. CE asymmetry) over time (x-axis)

second long-term phase stability goal is fulfilled. The phase stability of the CE end-points has a direct relation to the delay asymmetry of the differential protection service. *Therefore, the benchmark to reach below 0.1 ms path differential delay between the two multiplexer IEEE C37.94 interfaces was far exceeded*⁵.

In parallel, the perceived differential current is measured and recorded on the protection relays. The main contributor of the measured differential currents is typically the capacitive line charge. Figure 9 underlines the above-analysed values as the accumulation or variation of communication asymmetry would be indicated by a variation of I_{Diff} . *End-to-end delay measurements performed in the differential protection relays (echo timing) show that the absolute communication channel delay fulfils the requirement of $< 10 \text{ ms}$.*

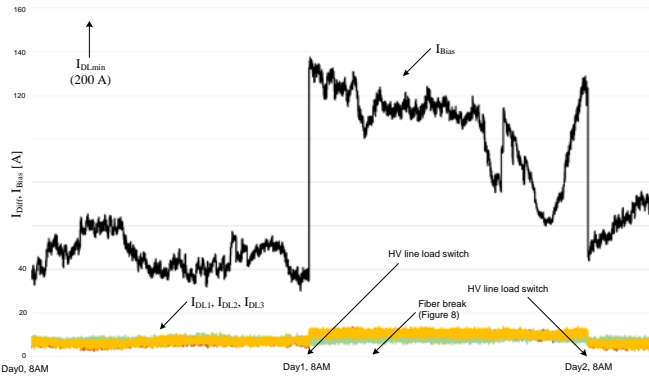


Figure 9: Protection relay differential currents I_{dL1} , I_{dL2} , I_{dL3} and I_{Bias} over time

During the complete observation period no loss of service was registered. Event and fault recorder read-out on the protection relay showed zero trip conditions over the total observation time (Table 2).

Multiplexer CE settings		Differential Protection Relay Measurements		
Buffer size/ end-to-end delay	Bandwidth	Transmission delay (incl. differential protection relay interface)	No. of communication interruptions	No. of trips
6 ms	1.248 Mbps	6.301 ... 6.306 ms	0	0

Table 2: Differential protection CE settings and protection relay measurements

Operation under stress & fault conditions

In a second step, different failure conditions were applied and immunity to the same was verified. The focus lay on the differential protection channel being a continuous data stream as it is much more sensitive to failure conditions. The below listed stress and failure scenarios were assessed:

⁵ The known electrical delay introduced by the IEEE C37.94 interface circuitry is compensated in the CE jitter buffer to meet the engineered end-to-end delay value (Table 2).

- **Fiber breaks** leading to path switchover under congestion
- **Random packet size congestion** on low priority queues
- **Channel and PTP delay asymmetries**

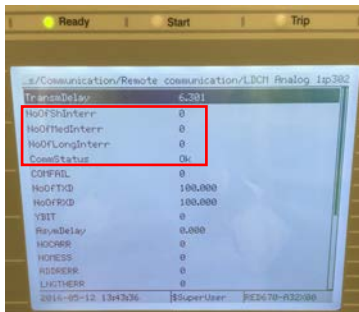


Figure 10: Continuous protection relay communication during fiber break

Impact of fiber breaks

The implemented packet duplication at the service end-points guaranteed in all fiber break test cases a hitless path switchover and continuous service operation. Differential protection CE synchronization during holdover relied on the physical layer Sync-E frequency until phase was regained on the backup path and the system recovered (Figure 8, Figure 10).

Impact of random packet size congestion (traffic overload)

Congestion showed no impact on Sync-E and a negligible one on PTP. No applied congestion scenario applied with the JDSU traffic generator had an impact on the differential protection service. By

controlling quality of service and the traffic load in the highest priority queues continuous service operation was guaranteed (Figure 10).

Impact of channel and PTP delay asymmetries

Demanding conditions present delay asymmetries introduced on CE and PTP streams. As long as only

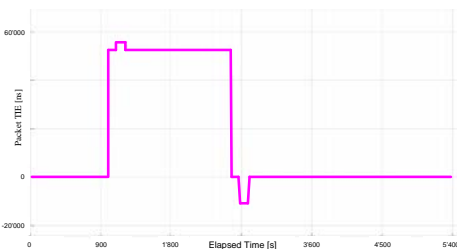


Figure 11: Sentinel measurement unidirectional PTP stream delay jump and restoration (53 μ s). Channel suppression threshold set to 50 μ s.

CE streams were impaired, e.g. due to asymmetric congestion or path switchovers, while phase stability remained, the jitter buffers compensated for the introduced delay (up to 6 ms, Table 2). The protection relay continued normal operation (Figure 10). Above 6 ms delay, CE buffer over-run was experienced. Consequently, the service was suppressed and an alarm indication signal (AIS) was played out to the protection relay until channel performance could be guaranteed again. The protection relay operated during this time in its fallback mode, distance protection.

In case PTP packet streams experienced an asymmetric delay or a phase jump (Figure 11), e.g. due to GPS signal recovery after an antenna fault, a threshold in the multiplexer set to 50 μ s (below the postulated tolerable asymmetry of 0.1 ms) guaranteed avoidance of a trip condition. Below the threshold, continuous operation of the channel was supported (Figure 10). Above the threshold, the service was suppressed until the phase shifts/ asymmetries were eliminated by the PTP protocol (Figure 12).

Under no circumstances an unwanted trip condition, e.g. caused by phase shifts or asymmetrical channel delay, occurred. If communication network performance was within expected variations continuous service operation was guaranteed even in heavily compromised networks. If performance exceeded engineered levels (e.g. asymmetry or latency > jitter buffer size) the system was put to a save state which led to a controlled service interruption. In all cases the system recovered by itself.

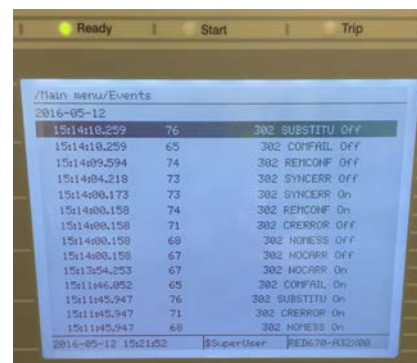


Figure 12: Protection relay communication loss during phase adjustments > 50 μ s

3.2 Distance Protection

In order to see the implications of WAN technology migration first the well known solutions in TDM WAN are described. A comparison of the same with different approaches using PSN WAN follows later in section 3.2.2.

3.2.1 Command based Teleprotection systems in TDM networks

As mentioned in the introduction, the solution provider of Teleprotection solutions needs to guarantee relevant standard compliance. This is done by performing extensive measurements with setups defined in the IEC 60834-1 standard.

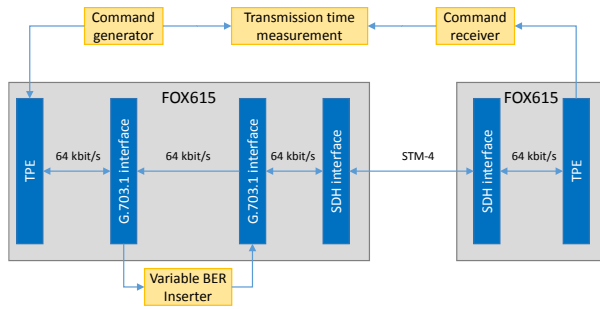


Figure 13: Test setup for dependability measurement

Dependability is $1 - P_{mc}$. With the results of this, the curves as seen in Figure 14 are generated, which simply tell how many commands have been received after $n \times T_0$ at a specific BER. The rest of the commands might come later ($> n \times T_0$), or in worst case never.

Teleprotection configuration: Permissive (speed)

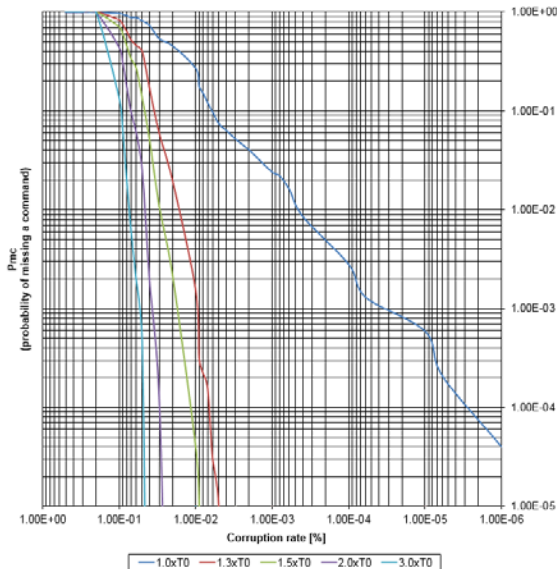


Figure 14: Probability of missing commands (P_{mc}) versus Bit Error Rate (BER) $T_0 = 4.6$ ms

curve since bit failures do have the same effect in any kind of TDM system. Of course, transmission delay times caused e.g. by fiber- or multiplexing delay change the T_0 time, but the curve as such stays valid means the dependability values stay the same just the transmission time needs to be added.

The last important performance parameter is security (P_{uc}), means the probability of an unwanted

in the IEC 60834-1 standard. Figure 13 shows the test setup used for measurement of the dependability values in Figure 14. The variable BER inserter generates random bit failures at a certain bit error rate, the transmission time measurement measures how many commands sent out are received after which time by the other device. As per IEC 60834-1 the same is scaled in $n \times T_0$ (n being 1 to 3), whereby T_0 is the back-to-back latency without any bit failures. For practical reasons the probability of a missing command (P_{mc}) is usually measured.

Figure 14 shows the results of the probability of a missing command measurements of the ABB FOX615 with the integrated Teleprotection module TEPI1 using an SDH network. Bit errors have been inserted on a 64 kbit/s electrical link. *Clearly visible is that the solution complies with the requirements defined in IEC 60834-1 by having a P_{mc} of $< 10^{-4}$ at a BER of 10^{-6} (compare with Table 1).* The estimated probability of a missing command (P_{mc}) is calculated as follows:

$$P_{mc} \approx \frac{N_T - N_R}{N_T}$$

N_T is the number of commands sent; N_R is the number of commands received after the defined time (e.g. $1.5 \times T_0$) [2].

Fiber optic delay or additional repeaters/ multiplexers do not change the fundamental shape of the

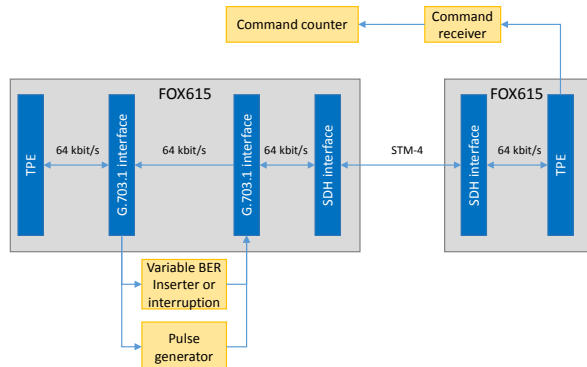


Figure 15: Test setup for security measurement

command due to burst disturbances or sudden signal interruptions. Figure 15 shows the test setup for measuring the security value. In the specific case of FOX615 with TEPI1 Teleprotection interface over SDH network, configured in blocking protection scheme, 8'981'200 BER bursts have been sent and no wrong trip has been detected, which confirms the requirement defined in the standard and shows a P_{uc} of $< 1.11 \times 10^{-7}$ for blocking schemes.

3.2.2 Command based Teleprotection systems in packet switched networks

How does the above explained behavior change when migration to packet switched networks happens? Various items are important to understand when migration of Teleprotection applications from TDM to PSN is looked at.

As already mentioned in section 3 interworking functions are needed to adapt and enable distance protection applications over packet switched networks. But what consequences does the technology migration have? Important to understand is the fact that the implication of a bit failure is significantly different in PSN compared to TDM networks. In TDM networks, a bit failure does not cause any action on transport layer. Bit failures are simply passed on and cause problems on application layer (e.g. requiring a retransmission of a file or a click in a voice conversation). Due to this communication channel behavior Teleprotection equipment typically includes additional security mechanism protecting the application from mal-operations due to bit failures⁶. The reasoning for TDM networks passing on bit failures is simple. TDM communication technologies have mainly be invented for efficient voice communication. Since this is a real time application, there is simply no time to retransmit corrupted information, rather accept the click in the voice conversation or apply coding schemes being able to correct bit failures then get high latency compromising on the voice conversation quality. This is very much comparable with real time applications in power grids, where data not received correctly loses its value hence retransmission is not an option (a trip signal is worthless ones the transformer burns).

For packet-based communication (e.g. Ethernet & IP) the background is different. Those protocols have the origin in the Internet world, where bit failures cause corruption of complete files and applications. Accordingly, it makes sense to discard corrupted packets as early as possible to save bandwidth and retransmit the same. This is why in Ethernet a bit failure causes the discarding of the entire frame.

Standard based circuit emulation interworking function

This setup is based on conventional Teleprotection as used in section 3.2.1 and standard based circuit emulation as IWF to transmit the TDM data over packet switched networks.

First, the implications on latency and raw data rate (bandwidth) needed for signal transmission are analyzed. In order to get a good communication channel performance packet size needs to be chosen small. To quantify the implications of circuit emulation on latency and bandwidth, the following Teleprotection channel is taken as an example:

- Teleprotection signals are mapped into 1 x 64 kbit/s channel
- For optimized latency the entire 2 Mbit/s frame is then mapped into 1 packet in the circuit emulation (structure agnostic CE)⁷
- Packet delay variation (PDV) tolerance is set to 4 ms
- Payload size: 32 bytes
- SAToP (CESoETH MEF 8 is used)
- The overhead with SAToP (CESoETH MEF 8) is 54 byte in an MPLS-TP link⁸

With these values, we can calculate the resulting bandwidth in the packet switched WAN using the following formula:

⁶ As an example, the NSD570 from ABB with the G.703.1 64 kbit/s interface can correct 1 Bit failure

⁷ Please note that it is not advisable to map more than 1 frame into a packet. Usual Teleprotection solutions evaluate received trip signals various times in order to guarantee required dependability and security values. If several frames are mapped into 1 frame a packet loss results in loosing multiple trip signal information with severe implication on dependability

⁸ Outer Ethernet Framing, 2 x MPLS headers, inner Ethernet framing incl. VLAN

$$\text{Bandwidth} = \frac{(\text{Payload} + \text{Overhead}) * 2048}{\text{Payload}} \left[\frac{\text{kbit}}{\text{s}} \right]$$

For the example given, this results in the following bandwidth:

$$\text{Bandwidth} = \frac{(32 + 54 \text{ bytes}) * 2048}{32} \frac{\text{kbit}}{\text{s}} = 5504 \frac{\text{kbit}}{\text{s}}$$

This means, for 1 x 64 kbit/s TDM data channel containing command based protection information 5.504 Mbit/s raw data rate is generated and needs to be transmitted through the packet switched network. Since it is not easy to bundle the Teleprotection data channel with other services due to service distinct routing, the resulting 5.5 Mbit/s⁹ are really just there for 1 x 64 kbit/s Teleprotection channel and the rest of the timeslots is typically unused¹⁰. This leads to a bandwidth efficiency of only 1.2%.

The latency consists out of the packetization delay and the packet delay variation tolerance (jitter buffer delay). Store and forward delay contributes only minor if traffic priorities, as well as network load is properly controlled and fiber delay can be neglected in case of back to back setup as used for T₀ measurement. In the given example, a packetization delay of 125 μs applies (1 frame per packet) and a packet delay variation tolerance of 4 ms¹¹. This results in an additional introduced delay due to circuit emulation of 4.125 ms.

Secondly, the different reaction to bit failures of TDM and PSN network results in a completely different behavior of the communication channel. Accordingly, we cannot take the TDM performance parameters of a command based Teleprotection scheme and assume that they are similar in packet switched networks. Just looking at the fact that, with the parameters used above, a 64 kbit/s data channel will result in 5.504 Mbit/s Ethernet data rate shows the different channel behavior. The different latency times of the two 64 kbit/s channels are easy to understand and explained above. Other communication channel parameters are more difficult to determine and need detailed analysis. As an example, the reaction on bit failures of the above mentioned channel is taken. Sending a 64 kbit/s channel through a TDM network means actually 8 bits (1 timeslot) every 125 μs. If an error on those 8 bits happens, it is simply passed on to the end application. If now the same 64 kbit/s channel is sent through a PSN, CE has to be applied. In order to get the best performance out of it, 1 frame per packet should be transmitted. This means that 688 bits are sent out every 125 μs. First of all, it is much more likely that a channel with a BER of e.g. 10⁻⁶, as defined in IEC 60834-1 as reference value, corrupts a bit. Secondly, in case of a TDM network, the corrupted data is simply passed on to the end application whereby in PSN the packet is immediately discarded. This makes it impossible to predict what happens with Teleprotection relevant performance parameters, especially dependability, when the service is migrated from TDM to PSN using standard based CE and measurement of the same is required.

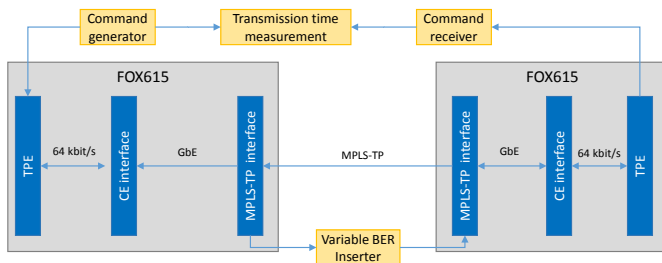


Figure 16: Dependability measurement setup for CE based solution

The implication on latency and dependability of a Teleprotection channel using standard based CE has been verified in measurements as shown in Figure 16. Table 3 compares the performance of a native TDM based solution as shown in section 3.2.1 with similar Teleprotection solution

⁹ The actual value depends on the configuration of the CE as described earlier in this document

¹⁰ Packetization of less than an entire 2 Mbit/s frame does not improve the situation since minimum Ethernet packet length is not reached

¹¹ It is possible to configure smaller packet delay variation tolerance values at the costs of resiliency of the solution (network problems cause faster a service interruption due to extended PDV)

but this time via packet switched network by using circuit emulation as described in this section. Nicely visible is that not only the back-to-back Transmission time (T_0) is affected by the circuit emulation¹² but also the probability of a missing command (P_{mc}) is changed completely. Taking a BER of 1.45×10^{-6} , which is equal to 0.1% packet loss rate¹³ and a comparable latency for both solutions, the resulting dependability is significant different in TDM as well as PSN-based systems. In case of the TDM solution the P_{mc} value is $< 1 \times 10^{-5}$ for a latency of $1.5 \times T_0$ (6.9 ms), which is fully compliant to IEC 60834-1. In case of the standard CE based solution the performance of the solution is severely impacted by the circuit emulation functionality. Latency is significantly changed (see Table 3) and comparing the resulting probability of a missing command values of the same Teleprotection implementation, just using now a packet switched network with circuit emulation, a significant change is visible. For a latency of 7.3 ms the resulting probability of a missing command for the standard based CE solution is 2×10^{-2} . This value is measured with the same BER as in the generic TDM based system. Hence, it is possible to compare it with the measured $< 1 \times 10^{-5}$ at a T_{ac} of 6.9 ms, which is even slightly faster than the 7.3 ms from the standard based CE solution. Clearly visible is the significantly increased probability of a missing command in the standard based circuit emulation solution, which is even not in line with the IEC 60834-1 standard requirements anymore. This is only caused by the different communication channel behavior of the TDM and PSN based communication channels since the Teleprotection function itself is identical for both measurements. The probability of a missing command values $P_{mc} < 10^{-4}$ could potentially be met in a standard based CE solution at the costs of longer T_{ac} (> 7.3 ms).

	TDM solution	CE solution
Latency (T_0)	4.6 ms	7.3 ms
BER	1.45×10^{-6}	1.45×10^{-6}
T_{ac}	6.9 ms	7.3 ms
P_{mc}	$< 1 \times 10^{-5}$	2×10^{-2}

Table 3: Comparison of performance of TDM- and CE based Teleprotection solution

Specific command based Teleprotection solution for packet switched networks

Considering the fact that any kind of circuit emulation based solution provides suboptimal performance for a command based Teleprotection scheme, up to a level where necessary standard requirements cannot be met anymore, new solutions need to be considered. Such a new solution has to provide a specific IWF fulfilling the distinct requirements of command based Teleprotection schemes. Such a solution is presented in this section. The specific IWF is a sequence number based packet generator, which uses the fact that command based Teleprotection schemes require event driven signal transmission (when a Trip signal needs to be transmitted) and continuous supervision information checking the availability and performance of the communication channel (guard packets). This actually does not require a classical circuit emulation solution of a TDM data channel as described in the previous section since no phase or frequency synchronization is required. With the specific IWF approach, many of the above seen drawbacks can be avoided. Teleprotection system performance increase is possible due to the shorter processing times and lack of framing which causes fix defined time intervals of 125 μ s as well as improved redundancy schemes making switchover from a main channel to a backup channel void. The specific IWF used in this solution generates a burst of packets ones a trip signal is detected at the input. This burst of packets ensures, that even in disturbed communication channels Trip information is received at the other end and dependability requirements can be met as defined in IEC 60834-1. To increase channel availability, Trip information is duplicated and can be sent twice via diverse data channels. Applying this principle reduces the probability of a missing command massively since it is unlikely that exactly the same packet is compromised on both channels simultaneously. The communication channels are supervised by sending guard packets around which are not only checking if the communication channel is still available, but also measuring the latency of the same as well as packet loss and packet delay variation.

In order to confirm the assumption of having a significantly improved dependability measurements of the same have been performed. Figure 17 shows the probability of a missing command curve for the solution applying the specific IWF over a packet switched wide area network. T_0 , which is the nominal transmission time under error free conditions, is set to 2.5 ms, which is extremely low. Figure 17 shows

¹² The 7.3 ms T_0 consist out of 4.125 ms latency introduced by the circuit emulation and 3.175 ms latency from the Teleprotection function. The discrepancy to the 4.6 ms latency using the TDM solution is internal optimization given by the integrated Teleprotection approach

¹³ 1 frame is 86 bytes including all the headers and labels, frame size for both is equal, the minimum Ethernet frame size

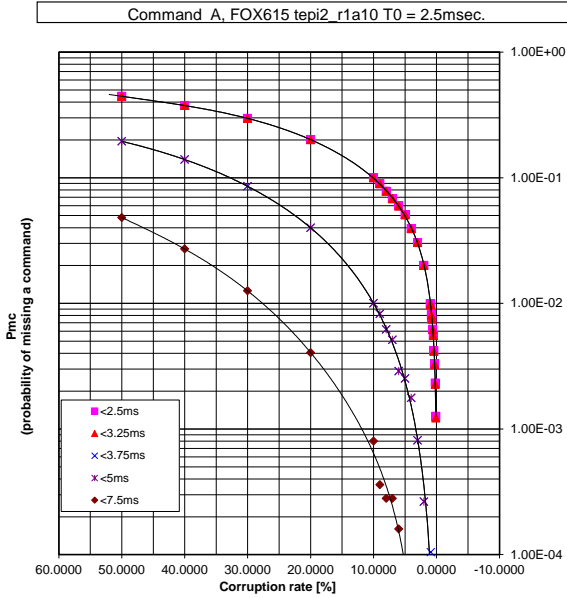


Figure 17: Probability of missing commands (P_{mc}) versus Bit Error Rate (BER) of the specific IWF based solution with non redundant WAN channel configuration

probability of a missing command of $< 1 \times 10^{-5}$ with a T_{ac} of 3.8 ms^{14} . The standard based CE approach provides a much worse probability of a missing command of 2×10^{-2} at a T_{ac} of 7.3 ms at the same BER of 1.45×10^{-6} (as summarized in Table 4). In other words, the specific IWF based solution transmits the Trip signals faster, much more reliable (more than a factor 1000) under similar impaired communication channel conditions (means BER).

Security narrows down to the probability of having an error affected frame being accepted at receiver side. For packet switched networks on Layer 2 bases, a CRC-32 checksum at the end of each packet secure the data integrity. The probability for a CRC-32 protected packet to be accepted would be close to the 1 in 2^{32} . This gives the probability as low as 2.33×10^{-10} hence fulfilling the specified security value.

The solution uses in addition to the CRC-32 of Layer 2 Ethernet packets an additional field in the payload to authenticate each packet with a SHA256 hash. This further increases the security of the signal as meant in IEC 60834-1 and gives the benefit of being protected against cyber security attacks since data modifications and repeated frames would be recognized. With this additional field is it very unlikely that errored packets are accepted on receiver side.

4 Optimization potential

Bandwidth optimization

As we have seen in Section 3.2.1 the required bandwidth for distance protection application using high performing CE configuration parameters is significant. Optimization potential is very limited since latency requirements are tight and mapping several frames into 1 packet leads to a risk of even further compromising the dependability performance values. Usage of more time slots is also difficult due to the fact that limited amount of signals need to be shared between neighboring substations (mainly protection signals). The actual bandwidth used is not a problem if you only look at a particular link. But as soon as you take a network approach, where e.g. 20 electrical substations form a big ring like topology

under which packet loss rates (corruption rate) which T_{ac} can be achieved. As an example, the probability of a missing command (P_{mc}) with the presented solution is $< 10^{-4}$ for packet loss rate of 1% and a T_{ac} of $< 2 \times T_0$ (5 ms). Taking the simplified approach of a bit failure leading to a packet loss (discarded due to checksum failure) and a packet length of 86 byte (which is implemented in the presented solution including all the headers for MPLS signal transmission) we have a total of 688 bits to consider. With a BER of 10^{-6} this results in a packet loss rate (PLR) of 6.88×10^{-4} or 0.0688%. Therefore, the presented solution's performance parameters are much better than the performance parameters for P_{mc} as well as T_{ac} defined in the standard [2]. The performance can be further increased by using redundant communication paths as explained before.

Comparing now the circuit emulation based approach with the specific IWF based approach we see the following improvement:

The specific IWF based approach provides with a PLR of 0.1% (resulting in a BER of 1.45×10^{-6}) a

	standard based CE solution	specific IWF based solution
BER	1.45×10^{-6}	1.45×10^{-6}
PLR	0.1%	0.1%
T_{ac}	7.3 ms	3.8 ms
P_{mc}	2×10^{-2}	$< 1 \times 10^{-5}$

Table 4: Comparison of probability of a missing command of standard CE and specific IWF based solution

¹⁴ Values taken from specific dependability measurements

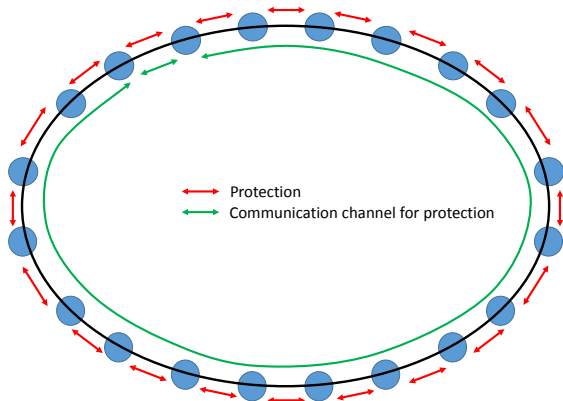


Figure 18: Sample setup for bandwidth consideration

with protection on all the lines and redundant communication channels are present (see Figure 18) we talk about significant amount of bandwidth used for Teleprotection only. In this example, it would be 20 x 5.5 Mbit/s or 110 Mbit/s Teleprotection traffic, which due to its time criticality and importance, would of course be high priority traffic.

The data rate of the specific IWF based approach is significantly reduced compared to the circuit emulation based solution. The bandwidth required depends if just guard packets are exchange or an actual Trip signal is sent. During Trip transmission times a bandwidth of < 400 kbit/s is re-

quired. Taking the above shown example again, we would only need 8 Mbit/s bandwidth for Teleprotection application and this is the worst-case scenario where all the 20 lines would be tripped at the same time. This is a bandwidth reduction of > 90% for high priority services compared to the assumed CE based approach. Comparable improvements for differential protection applications are not possible since TDM data streams need to be transmitted between the remote ends. This always requires CE and results in significant bandwidth requirements. Optimization is only possible at the costs of performance implications (e.g. longer latency).

Increasing the availability

Optimizing the Teleprotection solution for command based systems with a specific IWF based approach simplifies the setup of the overall solution with corresponding positive implications on system availability. The following sample calculation should make this better visible. Figure 19 shows the function blocks of a standard based CE IWF solution. An external Teleprotection equipment is connected to a

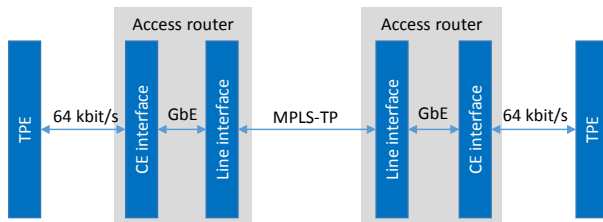


Figure 19: Function blocks of CE based system

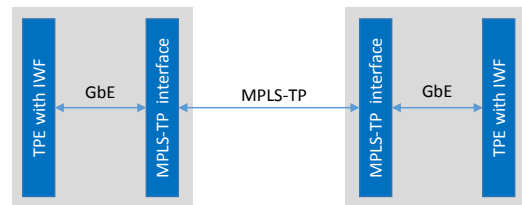


Figure 20: specific IWS based solution

networking device (access router). In typical networking devices dedicated hardware needs to be used for offering serial interfaces towards application which might or might not include CE functionality as well. For the considerations here, the CE functionality is on the same HW as the serial interface ports. Figure 20 shows the function blocks of the specific IWF based solution, where no CE in a classical way is required. In this case a Multiplexer integrated Teleprotection solution is considered which further improves the availability.

Component	MTBF
TPE	60 years
TPE with IWF	60 years
CE interface	30 years
Line interface	30 years
Backplane	200 years
Cables	1000 years

Table 5: MTBF values for sample calculation

For comparison, the following values summarized in Table 5 are considered. The values are of theoretical nature and not related to a specific device. In order to just see the effect of simplifying the setup the same MTBF for the external Teleprotection Equipment (TPE) and the integrated TPE with IWF has been considered. In reality, this will not be the case since a TPE itself consists of various parts reducing the MTBF compared to an integrated solution.

Taking an average time to repair of 4 hours, this leads to the following results (Table 6):

The positive effect on average yearly downtime of the integrated solution with the specific IWF function is nicely visible. As already mentioned, the approach is simplified, no protection of the data channels, as well as different MTBF values for the different Teleprotection approaches has been considered. For line differentials protection comparable effects exist. In case of dedicated IEEE C37.94 to e.g. E1 converter similar setups and improvements of availability are possible.

	Availability	Downtime per year (min)
CE based system	99.992%	42.9
specific IWF based solution	99.995%	26.4

Table 6: Availability comparison of different solutions

There are other positive effects of such an integrated solution. The visibility of the status of the overall Teleprotection solutions is much higher since the Teleprotection part is truly included in the multiplexer and alarms are automatically passed on to the network management system. Also fault finding is simplified since less systems are involved and remedial actions can be initiated much faster through reconfiguration from remote. Last but not least the operation gets simplified since less tools, software programs are involved (Teleprotection solution is part of the network element configuration) and complexity of overall solution is reduced (CE configurations are complex and require a deep know how of the communication network performance and its limitations).

5 Outlook

All the so far presented solutions are using conventional protection signals such as electrical inputs and outputs or TDM protocols (e.g. IEEE C37.94). In this section an outlook towards generic packet based protection solutions is made. The main idea of generic packet based protection solutions is to use well proven concepts and apply them for new application. The main idea is to use IEC 61850 based protocols for the same. This provides many benefits such as simplification of protection solutions, performance improvements or vendor interoperability.

5.1 Inter-substation GOOSE transmission

Solutions proposed in IEC 61850-90-1

Using GOOSE signals between substations generates requirements not seen before. The IEC technical report 61850-90-1 defines two possible approaches of how GOOSE signals can be used for trip command transmission between substations. The first approach is the tunnel approach connecting two substations directly together with a high speed Ethernet connection (Figure 21)¹⁵. This means actually building of one bigger station bus covering now both the substations. The second approach is the proxy-gateway approach which clearly separates the station bus from each other and introducing a gateway IED at the borders. This approach terminates the GOOSE message on the substation boarder, transmitting the trip command through any kind of technology to the remote end and generate a new GOOSE message at the remote end (Figure 22)¹⁶. The proxy gateway approach is used typically if narrowband communication channels are available. It is configuration intensive and requires significant processing time due to the requirement of decomposing and recomposing the GOOSE message. The tunnel approach generates challenges on many other aspects and are mainly driven by the proposed direct and transparent

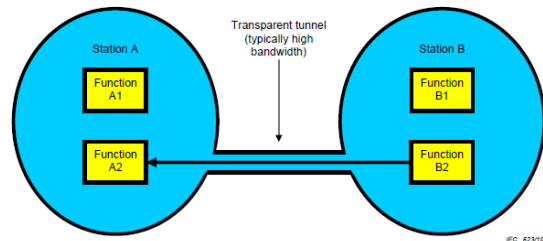


Figure 21: Tunnel approach defined in IEC TR 61850-90-1

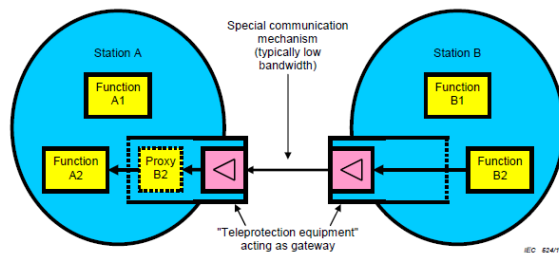


Figure 22: Proxy gateway approach defined in IEC TR 61850-90-1

¹⁵ Picture taken from IEC TR 61850-90-1 [6], page 57

¹⁶ Picture taken from IEC TR 61850-90-1 [6], page 58

interconnection of the two substations with corresponding extension of the broadcast domain. The main challenges for the tunnel approach are:

- Both substations need to be defined right from the beginning for direct interconnection with the tunnel approach. Otherwise it is very likely that reconfiguration with corresponding efforts is required due to conflicting or mismatching configurations.
- Extending the broadcast domain from one substation to another one enables direct, unprotected access from the local station bus to the remote one. Usually substation boundaries are considered as a security perimeter meaning that a transparent tunnel approach would contradict with this requirement.
- The wide area network is potentially not secured against data modification (e.g. man in the middle attacks). Modification of critical data, such as IEC 61850 GOOSE signals, is a scenario with tremendous implications for grid stability and needs prevention.

5.2 Changes on substation design driven by usage of IEC 61850 GOOSE messages

Using GOOSE based line protection simplifies the design of substations. It not only makes the conversion from electrical inputs to digital signals void with corresponding reduction on devices needed for this, but also replaces bulky copper cables transmitting high voltage trip commands by fibre optical cables. Finally it also enables new protection and control applications by exchanging additional signals or sending trip commands not only to protection relays but also other IEC 61850 IEDs such as breaker controller units or other GOOSE capable devices. Figure 23 shows a traditional substation configuration, where line distance protection (21) sends trip commands to the remote end using 110 VDC electrical signals. Dedicated Teleprotection equipment converts those signals a standard protocol and interface type (e.g. G.703 codir or IEEE C37.94), which then is connected to the multiplexer. Individual connections between protection relay and Teleprotection equipment per command are mandatory, but do not provide redundancy. Additionally one connection between Teleprotection equipment and multiplexer is needed per direction since the multiplexer cannot de-multiplex the information received and send it in different directions due to the proprietary packaging of Teleprotection information into the standardized protocol (e.g. IEEE C37.94). For various high voltage power lines (e.g. in the Figure 23 three power lines are indicated by three individual relays equal to three bays) typically multiple Teleprotection equipment is required.

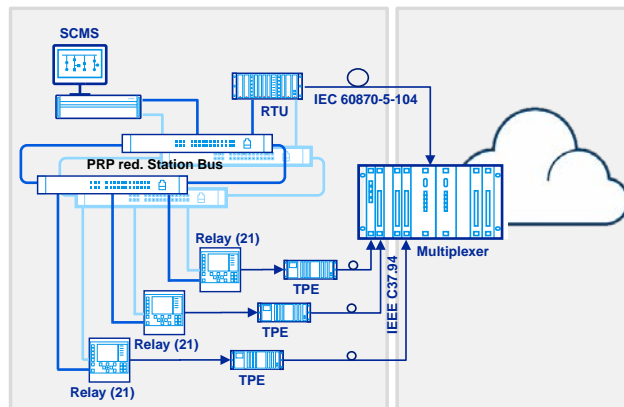


Figure 23: Substation design including dedicated Teleprotection equipment (TPE)

The result are rather complicated substation designs with corresponding limited availability due to more potential failure sources in the system. Fault finding in case of service interruption is complex since information cannot be shared easily and end to end service view is not given.

Using GOOSE based commands for line distance protection application changes the substation design considerably. Figure 24 shows such a setup where the multiplexer is acting as a GOOSE gateway connecting the station bus of one substation to the station bus of another substation through the wide area communication network.

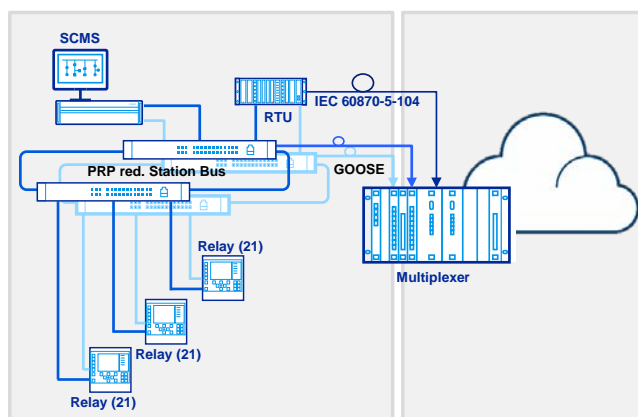


Figure 24: Substation design using GOOSE for line protection (21)

Using GOOSE based protection provides a possibility for fibre optic based command transmission without the need for external Teleprotection equipment. This simplifies the on-site installation substantially. Providing the option to connect redundantly to a PRP (Parallel Redundancy Protocol) redundant station bus removes the single point of failures existing in the other setup examples (e.g. cabling or Teleprotection equipment) and hence increases the availability of the line distance protection application. Using the presented solution, the GOOSE gateway will act as an IED in the substation being connected to the IEC 61850 station bus. As an IED the GOOSE gateway provides all the functions defined by the IEC 61850 standard, which for example includes reporting of the status to the substation configuration and monitoring system (SCMS). This means that the local substation now receives all of the relevant information relating to the status of the IEC 61850 smart GOOSE gateway (before Teleprotection equipment), which increases the visibility as well as allows to take actions in case of communication channel failures in the wide area communication network.

Finally, typical substation design includes one - often PRP redundant – station bus where all IEDs are connected. Protection signals based on GOOSE can be transmitted through this station bus for all powerlines leaving a substation. This means that all protection signals will be connected through the same (PRP redundant) fibre connection from the station bus to the GOOSE gateway interface where commands are identified by individual GOOSE messages to be sent to different remote ends. This simplifies the substation design for trip command signals transmission substantially as two fibre optic cables replace all copper cables that were used previously and are connected to one (or two redundant) interface card(s) [4].

5.3 Proposed solution based on IEC 61850 smart GOOSE gateway

As we have seen both proposed solutions have certain strength and weaknesses. The IEC 61850 smart gateway approach is focusing on broadband communication systems and is based on the IEC 61850-90-1 tunnel approach. The same has been enhanced with essential gateway elements combining the strength of both solutions and helps to overcome the main disadvantages of the tunnel approach. The IEC 61850 smart gateway solution addresses exactly the above listed challenges of the tunnel approach by providing the following key functionality:

- Tunnelling functionality of GOOSE messages as proposed in IEC TR 61850-90-1
- Wire speed translation functionality of GOOSE message fields such as VLAN or multicast addresses without decomposing the complete GOOSE message
- Filtering functionality for GOOSE messages to control the flow of GOOSE messages and apply good cyber the security practice of least privilege principle
- L2 based firewall functionality using white listing functionality to restrict access to the station bus from the wide area network
- Authentication of GOOSE messages for man in the middle- and replay attack protection

Thanks to these measures, GOOSE message security can be guaranteed and broadcast domains are limited to the corresponding station bus. This is due to the filtering function, which will only forward relevant GOOSE messages to the corresponding remote end. The wire speed translation functionality enables connection of IEC 61850 substations without any need for reconfiguration. On top the IEC 61850 smart GOOSE gateway solution provides additional functionality useful for Teleprotection application such as:

- Continuous communication channel supervision
- Hitless redundancy on wide area network side for highest availability of the communication channel
- PRP support for connection to redundant station bus configuration
- Integration into the local Substation Control and Monitoring System (SCMS) system for local alarming and communication status reporting
- Full integration into the communication network management system for supervision purposes
- WAN connection to a number of remote ends for multiple line protection schemes

5.4 IEC 61850 smart GOOSE gateway based distance protection solution performance

In order to confirm suitability of the GOOSE gateway based solution extensive testing on the performance has been done in a laboratory environment. This section summarizes the test results of those tests.

Delay of the IEC 61850 smart gateway based solution

The latency of the IEC 61850 smart GOOSE gateway was measured in a special setup. The test was performed using GOOSE messages generated by a specialised traffic generator. These got time tagged before injection into the GOOSE gateway. The IEC 61850 smart GOOSE gateway performed the translation of GOOSE fields and forwarded the same via an MPLS-TP link to the remote device, where the GOOSE message got re-injected using a local loopback on the front port. In a real world application, the receiving station bus would be connected here. The time tagged messages are processed once more through the complete system and - upon egress at the original device - they are time tagged again (see Figure 25 for a conceptual view on the test setup).

Analysis of the packet capture on the receiving side allowed for the readout of both the sent and received packet and therefore the roundtrip delay of the link.

The result of the round-trip delay measurements showed a consistent value $\leq 180\mu\text{s}$. The measured delay mainly consists of the store-and-forward delay of the involved nodes. With this the application requirements in terms of maximum transmission time delay is fulfilled completely.

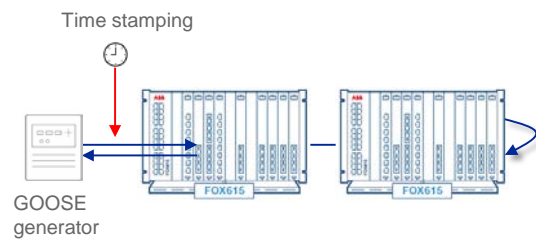


Figure 25: Delay measurement setup

Comparison to contact based solutions

To reflect a real use-case, a setup was prepared with two RED670 relays and parallel transmission paths using once contact based and once GOOSE communication to transfer a binary signal (representing a distance protection trip signal). The effect of jitter in the execution logic of the IEDs out- and inputs has been included by looping back both paths on the receiving side using contact based wiring of dedicated

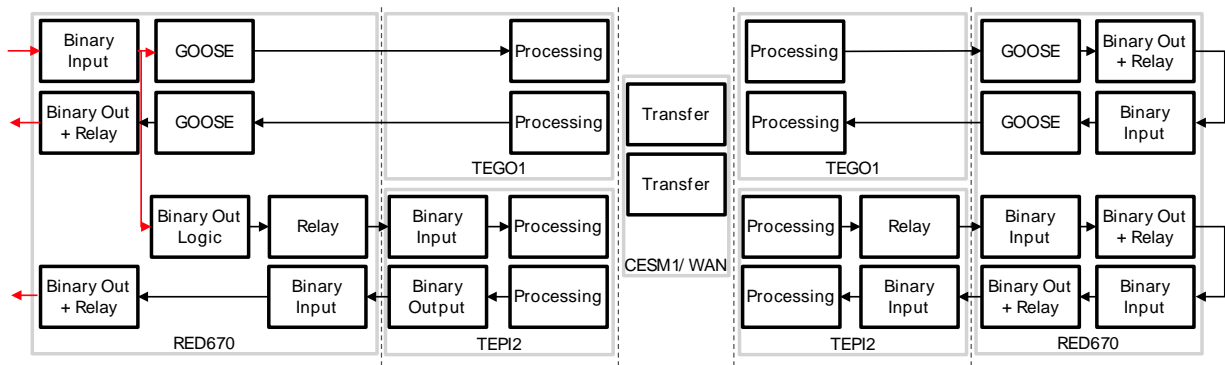


Figure 26: Comparison of contact and GOOSE based solutions

binary outputs to binary inputs (see Figure 26).

Upon triggering a single binary input, both message paths were activated. As a result, the loop delay of both paths could be directly measured. With multiple measurements the statistical effect of jitter should be levelled out and the latency values of the individual paths get comparable.

An average delta $\Delta t_{\text{Loop}} = t_{\text{Loop,Contact}} - t_{\text{Loop,GOOSE}}$ of $\Delta t_{\text{Loop}} \approx 10\text{ms}$ could be measured. Based on the setup, making, the valid assumption of symmetrical delays, the single trip delay can be estimated as $\Delta t_{\text{Single}} \approx \Delta t_{\text{Loop}}/2 \approx 5\text{ms}$.

The delay difference is mainly defined by the physics of the electromechanical relays used in today's IEDs¹⁷ as well as the processing delay of the conventional Teleprotection function on the respective interface card of the multiplexer.

Controlled access to the IEC 61850 station bus

As previously mentioned, interconnecting the station bus of two different substations can be critical and special measures to control the traffic flow from one substation to the other needs to be taken. To prevent operational issues such as unauthorised access to the station bus, flooding of multicast messages from one substation to another or broadcast storms in interconnected substation networks, the IEC 61850 smart gateway provides a controlled access to the station bus.

At ingress (data entering from the WAN to the LAN) whitelisting is used to ensure that only desired messages can enter towards the station bus of a substation. The IEC 61850 smart GOOSE gateway hereby serves as a L2 firewall operating at wire speed and hence does not affect the performance of the protection system. This approach works on a “deny by default” principle and provides a high level of security. At the egress side (data leaving the substation) filtering of relevant GOOSE messages is performed. This ensures that only relevant information is transmitted to the remote end and follows good practice by applying the least privilege principle.

Additionally front-ports support storm control by selectively limiting incoming L2 broadcast, multicast or unknown unicast frames to a settable threshold based on the total port bandwidth.

As part of the system test of the device, these two aspects have been extensively and successfully tested for both positive (e.g. whitelisted traffic passing through) and negative (e.g. non-GOOSE or non-whitelisted packets are dropped, stability during storm conditions) scenarios.

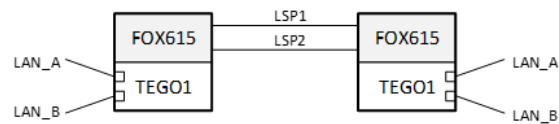


Figure 27: Example application of LAN and WAN redundancy

Operation under stress and fault conditions

Failure conditions such as link failures or traffic overload are a common appearance in today's communication networks. As a result a wide array of tests is performed to guarantee uninterrupted operation as well as correct indication and controlled transitions during faults.

Special focus shall be put on two failure modes: The impact of fiber breaks and traffic congestion.

Fiber breaks are handled both on the station bus and the WAN side, but by using different approaches. On the station side the application of the Parallel Redundancy Protocol (PRP) offers seamless switchover in case of failure. On the WAN side, redundant WAN channels providing hitless switchover are applied. The seamless switchover on both LAN and WAN side was extensively verified. Traffic congestion and storm scenarios were successfully tested both manually and in automated tests for stability. Correct behaviour of the filtering, authentication and prioritization of the device was proven using traffic generators and devices for robustness testing.

6 Conclusion

The technology migration presently ongoing in wider area communication networks from conventional TDM networks to next generation PSN networks provides many challenges for real time applications. Approaches focusing on some specific performance parameters (e.g. latency) oversimplify the problem at the risk of non-performance of the protection applications when needed or mal-operation when not needed. The paper analyzed the challenges of conventional Teleprotection applications (distance and differential) in packet switched networks in details as well as presented various migration options up to a scenario where the actual protection application migrates generically to packet switched networks making specific interworking functions void.

¹⁷ Solid state outputs of protection relays would also improve the latency to a certain extent but a significant difference to the GOOSE based approach would remain

For differential protection this paper elaborates why the standard implementations of CE technologies are not suitable since they cannot provide guaranteed symmetry as well as jitter and wander values resulting in potential mal-operation of the differential protection application. However, the tests performed in the field (supported by the tests in the laboratory) proved that the specific IWF for line differential protection with enhanced synchronisation capabilities as described in this paper can provide reliable transport of differential protection over PSNs. The assessed interworking of CE, MPLS-TP, Sync-E and PTP ensures guaranteed performance for this critical application even under network failure conditions.

For distance protection the implications of wide area network technology migration from traditional TDM networks to modern packet switched networks were analyzed. Conventional command based protection schemes are not only affected by increased latency times but also severely impaired on the critical performance criterion dependability if standard based circuit emulation is used for the same. This might be up to a level where compliance to Teleprotection standard IEC 60834-1 cannot be met anymore. The different critical performance parameters also depend on each other, latency time, bandwidth used, implications of bit failures (dependability) and availability of service influence each other. Optimizing on one of them can lead to severe implications on another parameter. This makes it almost impossible to give generic statements about the performance of a Teleprotection system and if IEC 60834-1 compliance is ensured when conventional TDM based Teleprotection systems are migrated using standard based CE in PSN. However, the packet generator based approach, as used in the presented specific IWF for command-based protection signals can overcome such problems. The specific IWF based approach greatly improves the dependability of the Teleprotection command signal transmission as well as reduces the command transmission time and bandwidth requirements due to native packet based Trip signal handling. With this approach, it is possible to achieve full compliance to IEC 60834-1 also in packet switched wide area networks. Finally, the enhanced redundancy possibilities as well as the optimized setup with the integrated solution greatly improves the availability of the overall solution.

Looking towards new ways of protecting electrical high voltage powerline shows interesting concepts with significant optimization potential. The IEC 61850 smart gateway is an essential element of such concepts and has been successfully tested in the laboratory as well as first field installation. It unveils several advantages against the traditional approach. Cabling efforts of protection application can be reduced, availability increased by enabling redundant connection to the IEC 61850 station bus and hitless redundancy of signal transmission through the WAN. Notification and alarming is ensured by integration to the IEC 61850 substation control and monitoring system (SCMS). Protection schemes get flexible since changes can be implemented by means of software changes and multiple protection signals can be transmitted on the same fibre pair reducing interface requirements on multiplexer side.

The measurements performed in ABB's laboratories, as well as in field clearly showed that the new IEC 61850 smart gateway based solution also complies with the requirements for distance protection applications by using IEC 61850 GOOSE messages for trip signal transmission.

The IEC 61850 smart GOOSE gateway based solution provides shorter trip information delay times compared to conventional Teleprotection schemes using either external Teleprotection equipment or multiplexer integrated contact based Teleprotection interfaces. The overall protection performance can be significantly improved by a latency reduction of 5 ms. Additionally, the possibility to connect redundantly to the substation bus (by means of PRP) as well as the hitless redundancy on the WAN side with duplicated signal transmission, increases the availability of the solution considerably.

Is it important to mention that cyber security requirements are covered with the described features. Via the integrated firewall functionality access to the station bus from the WAN is controlled and filtering ensures that only relevant GOOSE messages are transmitted to the respective remote substation.

The results prove the robustness and performance of the proposed solutions. It provides an attractive option for future IEC 61850 GOOSE line distance protection based on a mature and highly scalable approach.

All together it is possible to successfully migrate protection applications to new PSN based wide area network either by using specific IWF based solutions or migrate the application itself to generic packet switched technologies. Deep domain expertise, as well as specific solutions guarantee that performance is not compromised and electrical grid stability is not affected by the technology migration.

7 Bibliography

- [1] R. Bächli, M. Kranich, M. Häusler, M. Graf and U.Hunn, "Teleprotection ensuring highest performance of the protection system using packet switched wide area networks (D2/B5)," CIGRE, Vancouver, 2016.
- [2] "CIGRE Technical Brochure 192 "Protection using Telecommunications"," August 2001.
- [3] "CIGRE Technical Brochure 521 "Line and System Protection using digital circuit and packet communication"," CIGRE, December 2012.
- [4] R. Bächli, M. Kranich, R. Chowdhury, M. Häusler and Y. Al Jassasi, "IEC 61850-GOOSE based inter substation protection," CIGRE-GCC, Muscat, 2017.
- [5] "IEC 60834-1: Teleprotection equipment of power systems – Performance testing," IEC, Geneva, Switzerland, October 1999.
- [6] "IEC TR 61850-90-1: Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for communication between substations," IEC, 2010.

Authors



Ramon Bächli graduated from the University of Applied Sciences of Northwestern Switzerland in electrical engineering in 2002 and holds an EMBA in general management. He has extensive experience in the design of communication networks for power utilities. Presently he is working as a product manager responsible for broadband systems. In this position he is not only investigating in future technologies for utility communication networks, but also driving innovations towards all digital solutions.



Mathias Kranich graduated from the University Karlsruhe in electrical engineering in 1994 and earned a diploma in economic sciences in 1995. He has worked for over 18 years in the field of product management in utility communication and has vast experience in different communication applications and technologies. He is currently head of product management for telecommunication solutions in ABB.



Adolf Frei graduated from the University of Applied Sciences of Eastern Switzerland in electrical engineering in 2008 and holds an EMBA in Business Innovation. He has extensive experience in the design of time synchronization of packet switched communication networks for power utilities. Presently he is working as a senior development engineer within the R&D of wired communication products in ABB.