Migration of distance protection application from TDM- to packet based wide area networks

R. BAECHLI[1], A. FREI, M. KRANICH

ABB Switzerland Ltd.
Switzerland

SUMMARY

Reliable operation of electrical grids depends on a variety of applications working together seamlessly and with an extraordinary high level of availability. The various applications have completely different requirements for communication, such as latency, bandwidth, availability, and symmetry. Failing on this results in critical power grid conditions, lack of visibility, the ability for remote control or even large-scale blackouts resulting in substantial financial losses and reputation damage.

Applications, which have an immediate impact on grid stability have typically the most demanding requirements on communication, and accordingly they require special attention. Failing to meet these requirements would put the power system at risk. Protection applications are the most critical applications in electrical grids. Traditionally required performance parameters of such critical applications have been guaranteed by TDM based communication networks, and special devices guaranteeing performance parameters using such TDM networks. An example for this is Teleprotection (distance protection), where often dedicated Teleprotection equipment has been used to guarantee application specific performance parameters (e.g. dependability, security as well as latency) as well as perform the conversion from binary inputs to analogue or digital transport technology. With today's situation, 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 migration to new WAN technology, and how edge of technology solutions can circumvent such problems, and ensure Teleprotection applications via packet switched wide area network achieving guaranteed performance parameters in line with the Teleprotection standard IEC 60834-1.

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 applications. This is potentially critical since new WAN technologies also affect distance protection application, not only for latency aspects, which have been analyzed so far, but also for dependability and security parameters not being analyzed typically. This paper will close this gap by summarizing and presenting results of extensive test series with a special focus on dependability in different setups and with different solutions and present an application specific

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

solution enabling distance protection applications to use communication channels via new WAN technologies. The new solution provides superior performance and full Teleprotection standard compliance (IEC 60834-1), hence enabling the migration to new packet switched wide area networks (PSN) with guaranteed performance.

KEYWORDS

Teleprotection, time division multiplexing, packet switched wide area networks, dependability, security, IEC 60834-1, technology migration

1 Introduction

Protection applications are vital for reliable power grid operation. Protection systems consist of various different types of equipment connected together. Each of the subsystems needs to provide the required performance in order to ensure the clearing of faults within a reasonable time [1]. Distance- and differential protection applications have been used for many years. In both cases traditional TDM networks (SDH or SONET) have proven to comply with the stringent requirements. With the upcoming migration to new packet switched wide area networks implications need to be evaluated carefully. For differential protection application the same has been analyzed in details and will not be further discussed here. For more information on this please refer to: [1].

For distance protection the implication of technology changes in the communication infrastructure, providing the communication channels between the remote ends, have not been analyzed in details so far. Dependability and security are, beside latency, the critical performance parameters, which have been defined in IEC 60834-1. Compliance to this standard is essential since the overall protection system only performs as expected if all the subsystems perform accordingly. IEC 60834-1 splits down the overall requirements to the relevant subsystems.

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 1 shows the components of the Teleprotection system (in this picture with a dedicated Teleprotection equipment). 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 or G.703 64 kbit/s). That Teleprotection equipment has typically be connected to wide area communication networks using TDM technology. The main performance parameters for distance protection applications have been optimized traditionally adapt to the undelaying WAN technology (e.g. by supporting error correction capabilities in TDM networks). 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 PSN influences the critical performance parameters of the Teleprotection system. The fundamental and drastic change in communication technology as we see it with the migration from Time Division Multiplexing (TDM) systems (e.g. SDH/SONET) to a Packet Switched Network (PSN) systems (e.g. MPLS-TP) influence the performance for sure, the question is just how. Considering this, it might not be enough to just measure the latency and assume dependability and security performance are not changed and 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 a TDM to PSN communication networks and only latency needs to be considered is misleading and not considering the complexity behind this critical application.

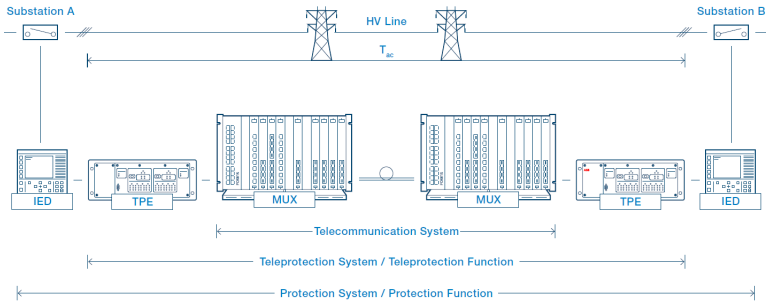

Figure 1: Protection system and split up in individual subsystems

Requirements of Teleprotection (distance protection application)

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

Critical performance parameters

The fault clearance time (T_c) is a critical performance parameter of the 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].
There are additional performance criteria to be fulfilled for reliably performing distance protection applications. We will now focus on those ones in more details.
Distance protection is based on the transfer of binary commands. The already mentioned command transmission times, as well as the dependability ($1-P_{mc}$[2]) and security ($1-P_{uc}$[3]), 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, which obviously can only be the case if all the subsystems contribute their parts as defined in the standard. 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}

2 Command based Teleprotection systems in TDM networks

As mentioned above, 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 2 shows the basic test setup. 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 x T_0 (n being 1 to 3), whereby T_0 is the back-to-back latency without any bit failures. With the results of this, the curves as seen in Figure 3 are generated, which simply tell how many commands have been received after n x T_0 at a

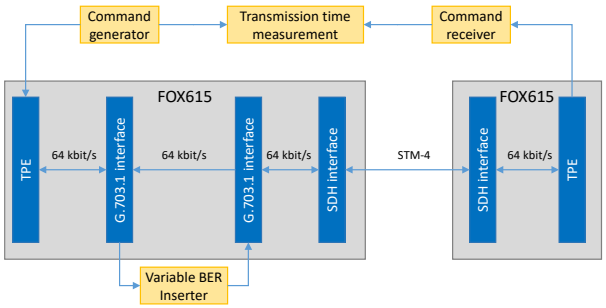

Figure 2: Test setup for dependability measurement

[2] probability of missing a command
[3] probability of an unwanted command

certain BER. The rest of the commands might come later (> n x T_0), or in worst case never.

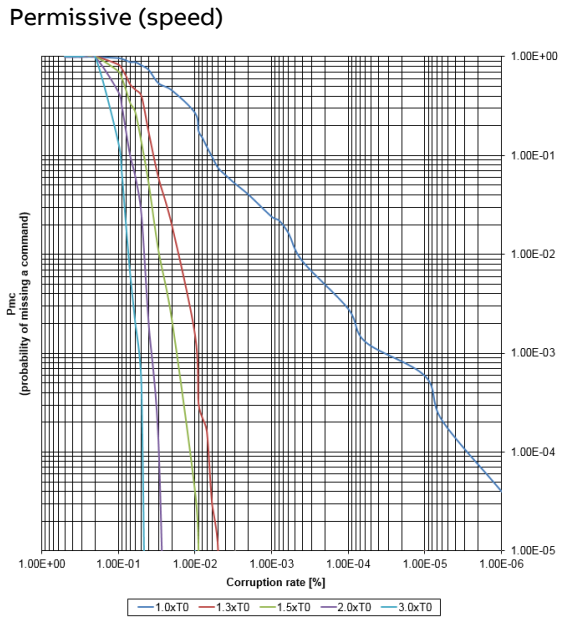

Figure 3: Probability of missing commands (P_{mc}) versus Bit Error Rate (BER) T_0 = 4.6 ms

values stay the same just the transmission time needs to be added.

The last important performance parameter is security (1-P_{uc}), means the probability of an unwanted command due to burst disturbances or sudden signal interruptions. Figure 4 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 x 10^{-7} for blocking schemes.

Figure 3 shows the results of such measurements. In this particular case, the ABB FOX615 with the integrated Teleprotection module TEPI1 has been measured and 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 (Table 1) by having a P_{mc} of < 10^{-4} at a BER of 10^{-6}. The probability of missing a 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 x T_0) [2].

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

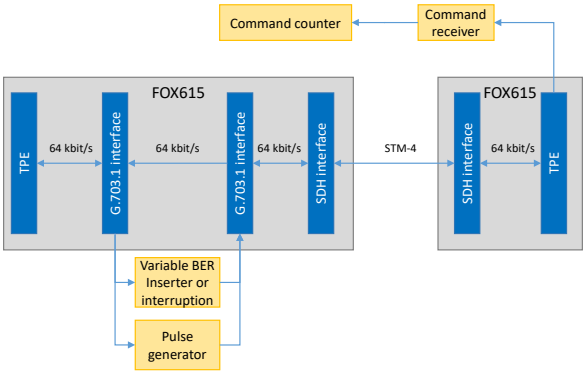

Figure 4: Test setup for security measurement

3 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.

First the need for a interworking function (IWF) enabling Trip transmission via PSN. When TDM signals are transmitted via packet switch networks the IWF needs to map the TDM data into packets and regenerate TDM data streams again at the remote end. Such IWF are commonly used in public telecom environment, named circuit emulation and are standardized for interoperability (e.g. CESoPSN RFC5086 or SAToP RFC4553). 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.

Second, the implication of a bit failure in both network types is significantly different in TDM networks compared to packet switched 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 transfer or a click in a voice conversation). Due to this communication channel

behavior Teleprotection equipment typically includes additional security mechanisms protecting the application from mal-operations due to bit failures[4]. 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 than 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.

3.1 Standard based circuit emulation interworking function

This setup is based on conventional Teleprotection as used in section 3 and standard based circuit emulation as interworking function 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. In order to quantify the implications of circuit emulation on latency and bandwidth better, 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)[5]
- 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

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

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

For the example given this results in the following bandwidth:

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

This means, for 1 x 64 kbit/s TDM data channel containing command based protection information 5.054 Mbit/s raw data rate is generated and needs to be transmitted through the packet switched network. Considering the fact that one (1) Teleprotection channel today uses typically 64 kbit/s the resulting 5.5 Mbit/s[6] lead 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 as long as 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 T_0 measurement. In the given example, a packetization delay of 125 µs applies (1 frame per packet) and a

[4] As an example, the NSD570 from ABB with the G.703.1 64 kbit/s interface can correct one (1) Bit failure
[5] Please note that it is not advisable to map more than one (1) frame into a packet. Usual Teleprotection solutions evaluate received trip signals various times in order to guarantee required dependability values. If several frames are mapped into one (1) frame a packet loss results in loosing multiple trip signal information with severe implication on dependability
[6] The actual value depends on the configuration of the CE as described earlier in this document

packet delay variation tolerance of 4 ms[7]. This results in an additional introduced delay due to circuit emulation of 4.125 ms.

Secondly,
The different reaction to bit failures in TDM and PSN network results for obvious reasons 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 mainly caused by the additional delay introduced by the CE function. Other communication channel parameters are more difficult to determine and need detailed measurement. As an example the reaction on bit failures of the above mentioned channel shall be looked at. 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 (refer to section 3.1). 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 in the second case and 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 PWN using standard based CE.

The implication on latency and dependability of a Teleprotection channel using standard based CE has been verified in measurements as shown in Figure 5.

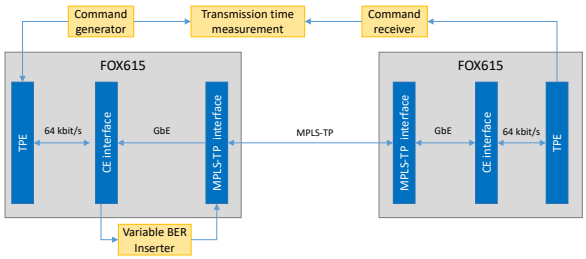

Figure 5: Dependability measurement setup for CE based solution

Table 2 compares the performance implication of a native TDM based solution as shown in section 2 with similar Teleprotection solution but this time via packet switched network by using circuit emulation as described in this section[8]. Nicely visible is that not only the actual Transmission time (T_{ac}) is affected by the circuit emulation but also the probability of missing a command (P_{mc}) is changed completely. Taking a BER of 1.45 x 10^{-6}, which is equal to 0.1% packet loss rate 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 probability of missing a command value is < 1 x 10^{-5} for a latency of 1.5 x 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 dependability 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 missing a command for the standard based CE solution is 2 x 10^{-2}. This value is measured with the same with BER as in the generic TDM based system. Hence, it is possible to compare it with the measured <1 x 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 higher probability of missing a command in the standard based circuit emulation solution, which is clearly not in line with the IEC 60834-1

	TDM solution	CE solution
Latency (T_0)	4.6 ms	7.3 ms
BER	1.45 x 10^{-6}	1.45 x 10^{-6}
Tac	6.9 ms	7.3 ms
Pmc	< 1 x 10^{-5}	2 x 10^{-2}

Table 2: Comparison of dependability of TDM- and CE based solution

[7] 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)

[8] 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

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 missing a command value $P_{mc} < 10^{-4}$ could potentially be met in a standard based CE solution at the costs of longer T_{ac} (> 7.3 ms).

3.2 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 (as seen in previous section), new solutions need to be considered. Such a new solution has to provide a specific interworking function (IWF) fulfilling the specific requirements of command based Teleprotection schemes. Such a specific 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 signals 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 µs 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 probability of missing a command 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 increases the dependability 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 6 shows the probability of missing a 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 6 shows 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 688 x 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.

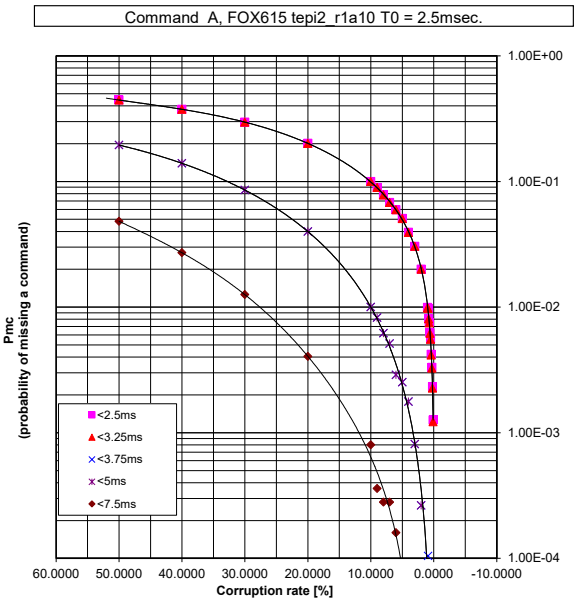

Figure 6: Dependability curve of specific IWF based solution with

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 x 10^{-6}) a probability of missing a command of < 1 x 10^{-5} with a T_{ac} of 3.8 ms[9]. The standard based CE approach provides a much worse probability of missing a command of 2 x 10^{-2} at a T_{ac} of 7.3 ms and a BER of 1.45 x 10^{-6} (as summarized in Table 4). In other words, the specific IWF based solution transmits the Trip signals faster, much more reliable under comparable impaired communication channel conditions (means BER).

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

Table 3: Comparison of dependability of standard CE and specific IWF based solution

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 x 10^{-10} hence fulfilling the specified security/ probability of an unwanted command requirement.
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

4.1 Bandwidth optimization

As we have seen in Section 3.1 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 on a particular link. But as soon as you take a network approach, where e.g. 20 electrical substations form a big ring like topology with protection on all the lines and redundant communication channels are present (see Figure 7) 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.

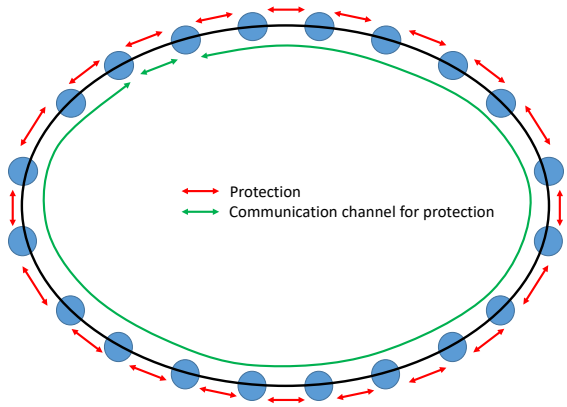

Figure 7: Sample setup for bandwidth consideration

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 required. 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.

[9] Values taken from specific probability of missing a command measurements measurements

4.2 Increasing the availability

Optimizing the Teleprotection solution with a specific IWF based simplifies the setup of the overall solution with corresponding positive implications on system availability. The following sample calculation should make this better visible. Figure 8 shows the function blocks of a standard based CE IWF solution. An external Teleprotection equipment is connected to a 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 9 shows the function blocks of the specific IWF base solution, where no CE in a classical way is required. In this case a Telecom equipment integrated Teleprotection solution is considered which further improves the availability.

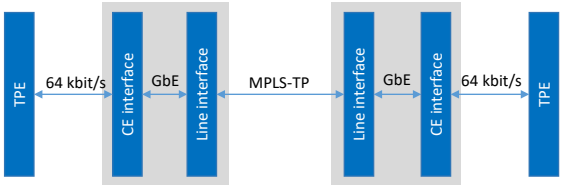

Figure 8: Function blocks of CE based system

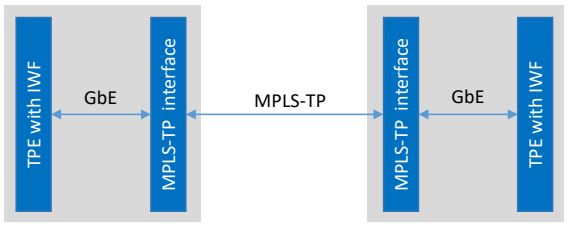

Figure 9: specific IWS based solution

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 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 one.

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 4: MTBF values for sample calculation

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

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

Table 5: Availability comparison of different solutions

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.

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 simplified (CE configurations are complex and require a deep know how of the communication network performance and its limitations).

5 Conclusions

The paper analyzed the challenges Teleprotection applications are facing when they are migrated from traditional TDM networks to modern packet switched networks. Conventional command based protection schemes are not only affected by increased latency times but also severely impaired on the critical performance criteria 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 Teleprotection systems and the level of IEC 60834-1 compliance 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 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.
Migration of command based protection systems from traditional TDM WAN to PSN needs deep application expertise. Implications on performance go much further than simple latency change. Solutions developed to provide such application specific migration scenarios show clear benefits compared to standard based circuit emulation solutions and prove to be able to provide required performance parameters also in modern packet switched wide area networks.

6 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] "IEC 60834-1: Teleprotection equipment of power systems – Performance testing," IEC, Geneva, Switzerland., October 1999.

[3] "CIGRE Technical Brochure 521 “Line and System Protection using digital circuit and packet communication”," CIGRE, December 2012.

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.