Teleprotection solutions with guaranteed performance using packet switched wide area communication networks

Ramon Bächli
ABB Switzerland
Baden, Switzerland
ramon.baechli@ch.abb.com

Martin Häusler
Mathias Kranich
ABB Switzerland
Baden, Switzerland

Abstract—This paper is presenting how teleprotection applications via packet switched wide area networks can be implemented guaranteeing required application specific performance parameters. The following different approaches are analyzed for differential protection:

a. ITU-T compliant standard circuit emulation (CE) using SAToP/ CESoPSN.
b. A novel approach of CE technology, using explicit clocks, developed for protection signal transmission via packet switched wide area networks

For distance protection, the following approach is assessed:

c. Applying an interworking function (IWF) based on a packet generator

The analysis is completed with supporting results from the field, in addition to lab tests of the specific solutions (b+c). Tests not only include the normal operation of the wide area network but also stress tests for various scenarios like traffic overload conditions, excessive jitter and wander, delay asymmetries, packet loss and protection switching of communication paths.

The tests proved the capabilities and superior performance of the specific solution (b+c) compared to other solutions.

***Index Terms*-- Circuit emulation, multiprotocol label switching, synchronization, teleprotection, wide area network**

I. INTRODUCTION

The availability of power grids depends on correct operation of various applications installed in control centers, electrical substations and power plants. Many of them require real time status information and immediate action in case of abnormal situations. Key performance parameters are bandwidth requirements and latency of the communication channel as well as its stability regarding symmetry, jitter and wander. For critical applications, the latter parameters need to be guaranteed on a sub millisecond timescale. Operational communication networks based on established technologies such as TDM have proven to fulfil such requirements perfectly. Driven by public communication networks, having completely different characteristics in terms of communication channel performance, new packet switched communication technologies, such as MPLS, have found their way into operational communication networks of power utilities.

Another important aspect is that in many cases large parts of the electrical infrastructure already exists. Installed devices often 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 (Figure 1). The substation environment, where communication devices for operational networks are installed, requires high EMC/EMI immunity as well as an extended temperature

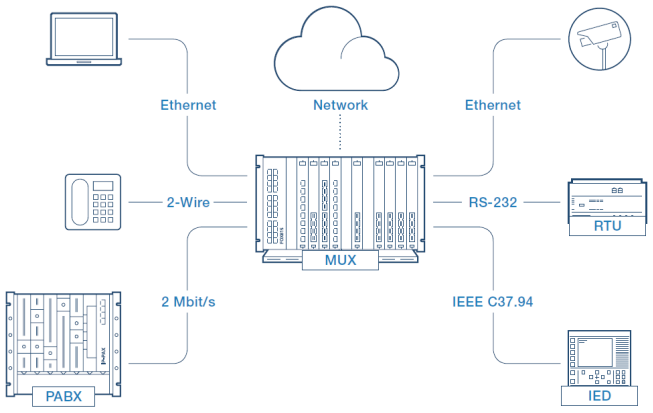

Figure 1: Typical applications and corresponding interfaces in electrical high voltage substations

range, avoiding moving parts (cooling fans) whenever possible.

A. *Requirements from Protection*

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

Protection systems consist of various different types of equipment connected together (Figure 2). Each of the subsys-

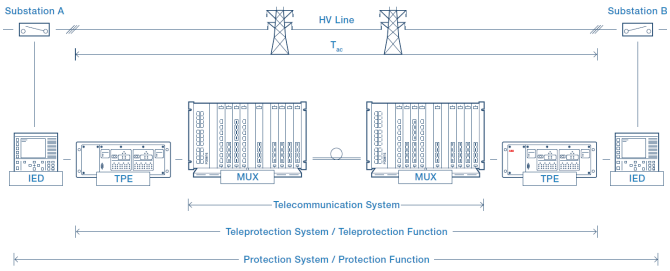

Figure 2: Protection system and split up in individual subsystems

tems needs to provide the required performance in order to ensure the clearing of faults within a reasonable time. Fault clearance time (T_c) is defined in the IEC 60834-1 report and a typical value for a high voltage transmission line is 3-6 power frequency cycles [2]. For teleprotection systems, the maximum transmission time (T_{ac}) is the critical performance criterion. For digital communication systems, T_{ac} should be < 10 ms [3], which is recommended for all kind of line protection schemes of HV lines, independent of the type of communication interface.

B. *Distance Protection*

Distance protection is based on the transfer of binary commands. Command transmission times, as well as the dependability (P_{mc}) and security (P_{uc}), are critical for the overall performance of the distance protection application, defined in the IEC 60834-1 standard, and need to be fulfilled by the teleprotection system for correct operation. The transmission time (T_{ac}) has to be within defined limits depending on the protection scheme and voltage level. The tolerance of commands on variations of the signal transfer delay makes the migration of such teleprotection applications to packet-switched (Ethernet/IP) networks feasible if the network guarantees the requested maximum end-to-end latency as well as dependability and security [1]. Table 1 summarizes the relevant teleprotection performance parameters for command based protection schemes.

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

C. *Differential Protection*

Differential protection operating in "echo principle mode" relies on the comparison of simultaneous (synchronized) samples of currents from the line ends and hence demands very stringent requirements on signal transfer delay, delay variation and delay symmetry. Any time deviation imitates a virtual fault current potentially leading to unwanted tripping of circuit breakers. The tripping characteristics of differential protection relays include a no-trip (restrain) area, which 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 [7]. Requirements vary based on publications. E.g. CIGRE Technical Brochure 192 "Protection using Telecommunications" [2] requests for high performing channel carrying differential protection data provides a maximum delay asymmetry and delay time variance of < 0.1 ms where more-recent publications accept values of < 0.2 ms which considers lower values are very difficult to achieve with communication circuits other than direct fibers [5]. In order to visualize the effect of asymmetry a short example is included here 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 amplitude error for a 50 Hz system (4.4° or 7.7% for 60 Hz respectively), such values might affect the relay sensitivity settings. Delay asymmetry issues become even more prominent when switching between routes in redundant communication systems occur. Potential workarounds are time stamped samples using GPS synchronization or dedicated fibers between differential protection relays. Both options are not ideal with respect to the availability, resources efficiency and O&M cost [7].

II. ENABLING TRANSMISSION OF TRADITIONAL PROTECTION SIGNALS VIA PACKET SWITCHED WIDE AREA NETWORKS

Packet switched networks (PSN) do not offer inherent Quality of Service (QoS) as TDM networks do, and add accordingly additional challenges for communication networks. Special measures have to be taken in order to reach or exceed the performance of traditional TDM networks especially under the aspect that today nearly all protection signals are connected via a traditional TDM interface (e.g. IEEE C37.94 or X.21). These measures are discussed in the following sections.

A. *Differential protection signals via packet switched wide area networks*

As explained differential protection requires digital, synchronized data for correct operation. In order to transmit this data via the PSN CE is required. Two variants are analyzed:

1) Standard CE (Variant a)

Two commonly used protocols are SAToP [8] and CESoPSN [9]. Both CE solutions, in accordance with ITU-T G.8261, cannot guarantee maximum asymmetry values in case of long operation periods since either a defined observation period is specified[1], or the observation period is at the same time a parameter to calculate the mask value[2]. Without packet synchronization, CE methods rely on adaptive timing

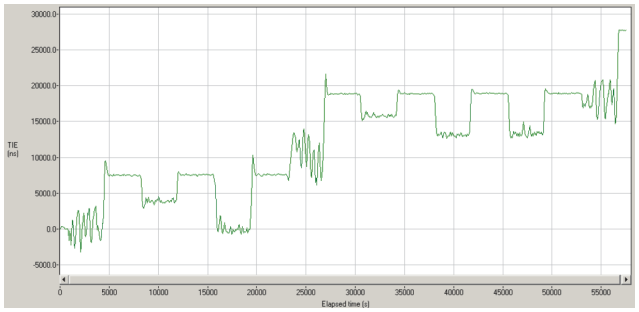

Figure 3: Accumulation of long-term residential jitter buffer delay depending on traffic pattern

circuitry to derive the clock from the incoming packet stream, which limits the long-term phase stability. The same can be seen in Figure 3, which shows a long-term Time Interval Error (TIE) measurement of accumulated jitter. The accumulated Jitter and Wander makes it impractical for differential protection. State-of-the-art switch hardware supports frequency stability with similar performance as SDH networks by means of synchronous Ethernet (Sync-E) [9][10][11]. Strengths of this technology include the physical layer implementation, which 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.

Therefore, neither SAToP nor CESoPSN is considered as suitable for utility specific HV-line protection applications but perfectly fit for less demanding applications in public telecom environment.

2) A novel approach to differential protection signal transmission over PSN (Variant b)

The proposed CE solution provides various traditional access ports for connection to any kind of protection relay type and interface. The assessed solution provides CE jitter buffer phase (re-) synchronization by means of hybrid Sync-E/ PTP operation, which is fundamentally different to circuit emulation technology discussed above. This approach allows phase adjusted data playout at both ends of the circuit via a jitter buffer and meets the stringent requirements of protection applications, hence enabling the same to use new PSN infrastructure.

III. DISTANCE PROTECTION SIGNALS VIA PACKET SWITCHED WIDE AREA NETWORKS

The chosen approach for distance protection does not rely on CE, but is based on an IWF, a sequence number based packet generator, which is independent of the system phase stability. This approach has been chosen to comply with the corresponding requirements of distance protection application as well as the teleprotection standard IEC 60834-1 [3] with the defined command transmission times, dependability (P_{mc}) and security (P_{uc}). The packet generator based approach for distance protection signals greatly improves the dependability of the teleprotection command as well as reduced the command transmission time due to less processing. Figure 4 shows the dependability curve for the packet generation based teleprotection solution. T_0, which is the nominal transmission time under error free conditions, is set to 2.5 ms, which is extremely low. The figure 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

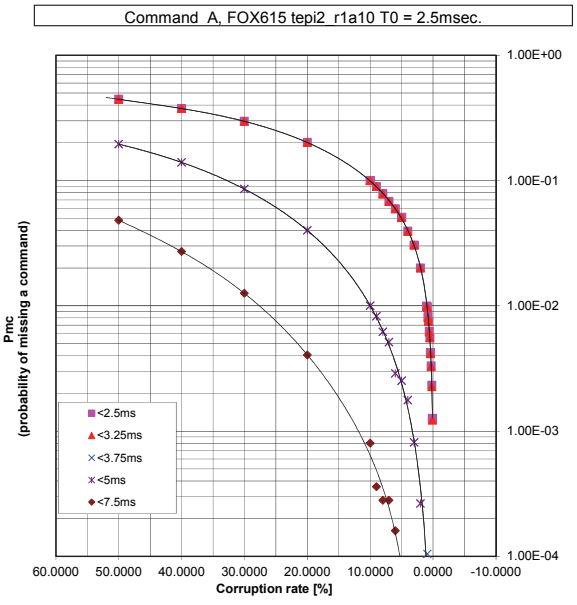

Figure 4: Dependability curve of presented solution

the presented solution is $< 10^{-4}$ for packet loss rate of 1% and a T_{ac} of $< 2 \times T_0$ (5 ms). The Teleprotection standard asks for $P_{mc} < 10^{-4}$ for a bit error rate (BER) of 10^{-6} and a maximum transmission time (T_{ac}) of < 10 ms. Taking the simplified approach of having a bit failure leading to a packet loss (discarded due to checksum failure) and a packet length of 70

[1] 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)

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

byte (which is implemented in the presented solution) we have a total of 560 bits to consider. With a BER of 10^{-6} this results in a packet loss rate of 5.6 x 10^{-4} or 0.056%. 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 [3]. The performance can be further increased by using redundant communication paths where it is very unlikely that bit failures happen at the same packet on main and backup path.

Security narrows down the probability of having an error affected frame being accepted at receiver side. For the used approach this is as low as 2.33 x 10^{-10} hence fulfilling the specified security value [6].

IV. FIELD TEST SETUP

A field test of both presented solutions has been done within the network of Swiss utility. The same consists of five TDM/ PSN hybrid multiplexer platforms operated at 10 Gigabit Ethernet using MPLS-TP technology providing bidirectional paths (Figure 5). The protection relays at either end of

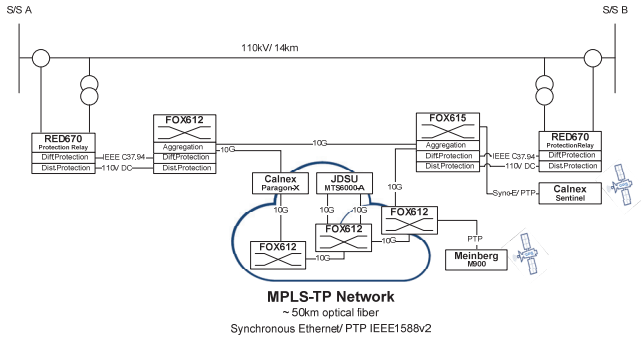

Figure 5: Field test system layout

the powerline are protecting a 110kV high voltage line. They are connected to the multiplexer with IEEE C37.94 interfaces for differential protection and 110V DC contact interfaces for distance protection. The system is synchronized by Sync-E as well as PTP from a grandmaster device (Meinberg). 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.[3] Redundancy for data and synchronization achieved by the ring structure of the network.

For differential protection the authenticated, phase timed CE (novel approach) 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 latency of the CE service was defined as 6 ms, which typically provides stable functionality with a reasonable differential protection performance. The specific CE solution uses the frequency and phase information available within the multiplexer to guarantee 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 [7].

For distance protection dedicated packet generation interworking functions are in place to provide a high-speed, secure, bidirectional service and the service is assigned to the second highest priority multiplexer queue.

Strict scheduling of the queues is applied and both teleprotection types ensure hitless protection by traffic duplication at the service end-points. 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:

For differential protection:

- *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*

For distance protection:

- *Absolute channel delay below 5 ms*
- *Dependability and Security values as per relevant IEC 60834-1 standard*

A Calnex Sentinel synchronization tester is used to verify the system phase stability and service performance. The network behavior, as well as other traffic being transmitted on the network, is simulated using JDSU MTS6000-A traffic generator as well as the Calnex Paragon-X network emulator. Since Dependability performance verification requires a high amount of commands sent the same could not be verified in the field. The lab test results summarized in Figure 4 are taken as Dependability values. The Security is proofed by not having any wrong distance protection trip signal during the entire test period.

V. RESULTS OF FIELD TESTS

A. Under normal operation

The TIE measurements are done using the Sentinel to prove the long-term phase stability from a communication perspective. Test device memory limitations limit the test

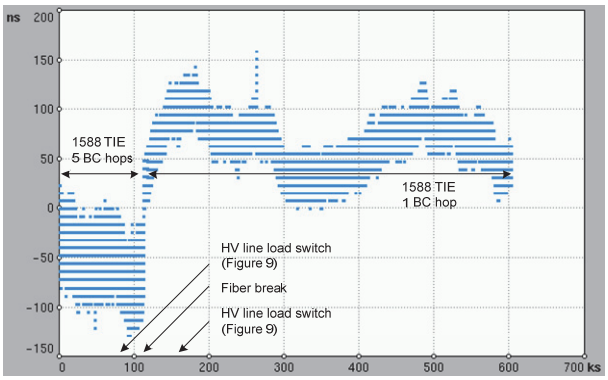

Figure 6: Measured network TIE (y-axis) stability (→ max. CE asymmetry) over time (x-axis)

[3] This provides GPS independency and adds resiliency to GPS spamming and spoofing effects.

intervals to seven days at a time. The same are repeated over months. Figure 6 shows such an interval, which also includes stress test with a forced fibre 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. As it can be seen in Figure 6 a stable synchronization chain present and the hybrid multiplexers regulate around the reference grandmaster ToD. A system phase stability below 1 µs is reached over the total observation time of several months. *The values lie within any network limit or standardization masks and the sub-microsecond 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 C37.94 interfaces was far exceeded*[4]*. 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 ms.* 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.

Event recorder entries of the field test confirm the back-to-back delay values for distance protection measured in the laboratory to be around 3 ms end-to-end. No wrong trip signals were recorded at the protection relay, confirming the security calculations. Dependability has been proofed in laboratory testing with a high amount of commands sent and with corresponding compromised communication channels simulated [7].

B. Operation under stress & fault conditions

To prove the robustness of the solution different failure conditions were applied and immunity to the same was verified. The below listed stress and failure scenarios were assessed:

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

1) 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 6), Distance protection signal packet generation continued on the redundant path without any service interruption.

[4] The known electrical delay introduced by the C37.94 interface circuitry is compensated in the CE jitter buffer to meet the engineered end-to-end delay value

2) Impact of random packet size congestion

Congestion showed no impact on Sync-E and a negligible one on PTP. No congestion scenario applied with the JDSU traffic generator had an impact on the distance and differential protection service either. By controlling quality of service and the traffic load in the highest priority queues continuous service operation was guaranteed.

3) Impact of channel asymmetries

Demanding conditions present delay asymmetries introduced on CE streams. As long as only 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). The protection relay continued normal operation. 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. The distance protection application worked successfully during this entire test since the application is less affected by asymmetrical communication channels or latency variations.

Under no circumstances an unwanted trip condition, e.g. caused by 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 safe state which led to a controlled service interruption. In all cases the system recovered by itself.

VI. 6. CONCLUSION

The paper analyzed the challenges teleprotection applications are creating when connected through packet switched networks. In the case of differential protection, this paper elaborated on why the standard implementations of CE technologies are not suitable. However, the novel solution with enhanced synchronization capabilities as described in this paper can provide reliable transport of differential protection over PSNs. The tests performed in the field (supported by the tests in the laboratory) proved this. The assessed interworking of CE, MPLS-TP, Sync-E and PTP allowed guaranteed performance for this critical application even under extreme conditions.

In addition, the presented solution for distance protection signaling based on packet generators met and exceeded the Dependability, Security and trip transmission time requirements defined in the standard.

The presented solution cannot only enable the migration of critical protection services from traditional TDM networks to PSNs but can also help to improve the performance of the protection system overall, e.g. based on the lower protection channel asymmetry or lower transmission times (T_{ac}) with guaranteed Dependability (P_{mc}) and Security (P_{uc}).

REFERENCES

Periodicals:

[1] R. Comino, M. Strittmatter: "Advanced power grid protection" ABB Review 3/11.

Technical Reports:

[2] CIGRE Technical Brochure 192 "Protection using Telecommunications", August 2001.

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

[4] IEC TR 61850-90-1: Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations 2010-3

[5] CIGRE Technical Brochure 521 "Line and System Protection using digital circuit and packet communication", December 2012

Books:

[6] A. Tannenbaum, Computer Networks, Prentice Hall PTR, 2003.

Papers from Conference Proceedings (Published):

[7] R. Bächli, M. Kranich, M. Häusler, M. Graf, U. Hunn: Teleprotection ensuring highest performance of the protection system using packet switched wider area networks (D2/B5), presented at CIGRE Canada Conference, Vancouver, Canada, 2016, Cigre-764

Standards:

[8] The Internet Engineering Task Force (IETF), RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP), June 2006

[9] The Internet Engineering Task Force (IETF), RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN), Dec. 2007

[10] International Telecommunication Union (ITU-T), G.8262/ Y.1362 Timing Characteristics of Synchronous Ethernet Equipment Slave Clock, Jan. 2015

[11] International Telecommunication Union (ITU-T), ITU-T G.8264/ Y.1364 Distribution of timing information through packet networks, May 2014

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 also investigating in future technologies for utility communication networks.

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 14 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 communication networks in ABB.

Martin Häusler graduated from the Zurich University of Applied Sciences, Switzerland in electrical engineering in 2003. He has extensive experience in the design of communication networks for power utilities. Presently he is working as a product prime responsible for broadband systems at ABB.