Study Committee B5 Colloquium
June 24-28, 2019
Tromsø, Norway

300

Preferential Subject 3

Future technologies for inter-substation communication, Migrating Digital Teleprotection Channels to Packet-Based Networks

Special Report

Fred Steinhauser
AUSTRIA

Summary

For this preferential subject, nine papers from seven countries were selected from the submitted abstracts.
Not surprising, some common topics could be identified. Five papers refer to the application of inter-substation communication for line protection. Also, six papers deal with MPLS or at least mention it as an option, whereas three of them emphasize on the migration from classical communication systems to MPLS.
Two papers go into the usage of routable GOOSE messages (R-GOOSE) for inter substation communication.
Also not surprising in this context, many of the papers touch the topics of time synchronization, be it self-synchronizing via the communication link or using PTP and GPS. To have some kind of time synchronization mechanism in place is essential for such distributed protection and automation systems communication via inter-substation links.

Consolidated Keywords

Line Differential Protection, SONET, SDH, PDH, TDM, IEEE C37.94, IEEE 1588, PTP, IEC 61850-90-12, R-GOOSE, MPLS, Wavelength Division Multiplexing, Optical Transport Network

Contributions focusing on Line Differential Protection and MPLS

A clear trend in the utility industry is outlined in three papers: the era of SDH networks is coming to an end. The components in these networks have reached end of life, the former suppliers are not interested in supporting this technology anymore and spare parts are no longer available. The most dominant alternative is to move to MPLS networks. Depending on the preferences, different migration strategies are possible.

Paper 301 from Germany is centred about line differential protection that utilized SDH for communication before and how this is to be migrated to MPLS networks. A brief intro to MPLS is provided, which is just adequate for power system engineers. The protection relays remain unchanged and still utilize protection communication via IEEE C37.94 and are not yet communicating "natively" packet-based. Thus, the edge routers to the MPLS network must provide IEEE C37.94 interfaces. Where this is not provided, even converters between IEEE C37.94 and G.703.6 are to be used. Laboratory tests showed that the MPLS communication is capable to handle the communication for line differential protection and based on this, the first differential line protection system vial MPLS were put in operation.

Paper 303 from Japan is as well driven by the line differential protection application, but it focuses on the innovative approach of utilizing "native" Ethernet interfaces and Ethernet packets for the information exchange between the protection relays. This removes the need to convert the legacy protocols supported by formerly existing relays to a packet-based communication. The communication channels need to be Ethernet (ISO layer 2) links, which then also opens further options for the application of other, Ethernet based features and services. For providing redundancy, the Parallel Redundancy Protocol (PRP) is an option that is as well based on international standards and endorsed by IEC 61850. Also, with high bandwidth channels (in this case, 1Gbps links were used) and sufficiently defined signal propagation properties, the Precision Time Protocol (IEEE 1588, PTP) is a straight forward solution for time synchronizing the protection devices.

Paper 305 from the USA also describes the potentials of moving protection communication from established TDM communication systems to packet-based communication. The course of the paper leads to a virtual synchronous network (VSN), either over MPLS or Carrier Ethernet. The communication channel requirements are discussed related to IEEE 1646 and IEC 61850-90-12. Metrics like latency, asymmetry, and jitter are explained and put in relation with the requirements and typically achievable figures. To avoid modification of the protection devices, converters between IEEE C37.94 and Ethernet were used. Extensive laboratory tests were conducted with the packet-based communication architectures. Interestingly, the probable reason for the only communication interruption recorded during an experiment was a firmware upgrade to the core switches. This indicates that such actions must be carefully coordinated in multi-purpose utility networks. The proposed VSN technology proved to be well suited for mission-critical protection.

Paper 307 from Sweden starts with the statement that SDH/PDH networks are sometimes maintained solely for the line differential protection, while all other services in a utility are already migrated to state-of-the-art technologies such as MPLS.
For the time synchronization, the considerations were based on the condition that GPS is not to be used and all line protection relays must operate self-synchronized (Echo Timing). The figures used for evaluation the time synchronization inaccuracy and differential current magnitude error are almost identical to those laid out in paper 301. Again, the protection devices remained unchanged, still operating with IEEE C37.94 interfaces. For connecting them to the MPLS network, converters (multiplexers with IEEE C37.94 and G.703 E1 interfaces) were used.
A laboratory test setup was connected to the actual existing MPLS network to achieve significant test conditions. This network connects 22 operational 130 kV substations, partly via optical fibres but also via microwave links. Considerations regarding synchronization,

path redundancy, and route and path switching complement the topics covered. The new system has first been rolled out in three stations (protecting two lines) for a pilot phase and the migration is now completed in nine substations.

Paper 308 from Russia considers migration strategies from the SDH/PDH communication systems to MPLS from the view of a communication services consultant for power utilities. Several different migration strategies are described with their pros and cons. Not surprising, all of them are associated with cost considerations, mentioning that the CAPEX and OPEX of the MPLS solutions are high.
The paper states that there are no obvious advantages of MPLS from the point of view of implementing synchronous channels for line differential protection and teleprotection equipment. Four different migration strategies are discussed in detail. The strategies focus on providing synchronous communication channels. In a further test with protection equipment, again converters for interfacing with the IEEE C37.94 are employed. Laboratory tests worked out the conditions for providing suited channels for protection and control applications and conclusions for commissioning and maintenance are drawn as well.
As one conclusion, the advantage of MPLS is mainly seen on the side of the suppliers of telecommunications equipment and for that reason the Russian utilities might still stick with SDH/PDH and direct optical fibres for a while.

Questions

Question 3-1: In the majority of the contributions, the legacy interfaces (IEEE C37.94) are still used at the protection devices, so converters have to be used to interface these devices to packet-based networks.
Given the general trend to packed-based networks and for streamlining the systems by eliminating the converters, is it now time to request "native" packed-based interfaces and protocols also in the protection and control devices?

Question 3-2: The line protection relays still exchange the current and voltage information in a proprietary format. The Sampled Values formats as in IEC 61869-9 used for merging units in local networks are unlikely to be used for wide area applications. Even though the available bandwidth is ever-increasing, it seems unreasonable in most cases to dedicate a bandwidth in the order of 10 Mbps for such purposes. A profile for wide area applications should use a sampling rate in the range of what perfectly works for line differential protection (well below 1 kHz). Together with an optimized coding, the bandwidth requirements could be shifted into the range of 1 Mbps, which could be transmitted over a T1 link.
Would it be beneficial for wide area applications to standardize a new Sampled Values profile as indicated above for such applications? When using such an interoperable communication interface, are line differential protection schemes with relays from different vendors on opposite ends imaginable?

Question 3-3: The protection performance and the communication channel performance are closely related to each other. The evaluations of the system performance is mostly done in a merged and interdependent setup, assessed from a protection point of view.
Would it be beneficial if the protection experts learn to formulate their requirements on the communication channels in the language of the IT/OT experts, so the IT/OT experts could independently evaluate and provide suitable communication channels?

Question 3-4: Paper 308 contains a chapter about issues of commissioning.
Is it now time to introduce the commission of the communication infrastructure for protection and automation as an explicit, independent task to be performed solely based on requirements on the communication, even without presence of the protection and control devices?

Contributions focusing on Routable GOOSE

There are already many implementations existing that exchange "normal" GOOSE messages over WAN links between substations. But all of these implementations require the involvement of some translation or tunnelling devices. IEC 61850-90-5 (now migrated to IEC 61850-7-2 Ed.2), triggered by a requirement for transmitting synchrophasors, defined routable flavours of Sampled Values and GOOSE.
The R-GOOSE is an IP based communication service which can make use of the more commonly available IP communication services. This opens a wider scope of applications as soon the protection and control devices support the R-GOOSE communication

Paper 302 from the USA covers the usage of GOOSE messages over wide area networks for protection communication. MPLS, with its ability to provide layer 2 (Ethernet) paths is one option to transmit the "normal" GOOSE over WAN links. But layer 3 (IP) routes, which are as well supported by MPLS, will be much more commonly available than the layer 2 paths. By utilizing the R-GOOSE, these communication options can be exploited for protection and control applications. System Integrity Protection Schemes (SIPS) with their high number of potential data sources in many different locations with often limited communication capabilities are prominent candidates for utilizing R-GOOSE.
The paper also outlines test systems and methods to measure the performance of wide area communication channels to assess if they are suited for specific protection and control applications.

Paper 304 from Argentina describes a prototyping of a concept utilizing a so-called "R-GOOSE Gateway" in a laboratory test. The paper describes the use of "R-GOOSE gateways". Contrary to proprietary GOOSE encapsulation techniques of IP or otherwise established layer 2 tunnels, the use of these R-GOOSE gateways relies simply on the availability of IP routes. The protection devices interfacing with the R-GOOSE gateways remain unchanged and communicate via "normal" GOOSE messages. This may also be a migration path. As protection devices become equipped with built-in R-GOOSE capabilities, they can then simply become re-connected to bypass the gateway. In this example, the R-GOOSE gateway also includes a logic to evaluate the GOOSE messages from the local protection devices to create a consolidated R-GOOSE that is transmitted to the remote stations.

Questions

Question 3-5: The current R-GOOSE pilot installations do not include any cyber security measures in order to keep the complexity for the proof of concept as low as possible. This might not be an issue within a closed communication network privately owned by the utility or when using a VPN. But when exploiting the option of sending R-GOOSE via public networks ("over the internet"), cyber security measures, e.g. as proposed in IEC 62351 need to be applied. For this, a security key/certificate management and distribution system is to be implemented.
Are there established systems in the electrical power industry or at least role models to be adopted from other industries for implementing such a system for managing and distributing the security keys/certificates? Is there a best practice for administering such security measures for wide area protection communication?

Question 3-6: Besides synchrophasors, which other applications for routable Sampled Values (R-SV) are imaginable? Would a R-SV profile, probably with even lower sampling rates than indicated in question 3-2, be beneficial for the proliferation of applications based on routable Sampled Values?

Contributions focusing on Networking Technology and Data Management

These two contributions remain on a more general level, both in a different way. While one expands the scope of the possible performance of communications channels far into high bandwidth regions, the other one emphasizes on the classification of data for purpose related communication channels.

Paper 306 from the USA goes deep into the data transfer capacity an optical fibre provides, starting at the physical level. Modern communication equipment is able to exploit much of this enormous bandwidth potential, then breaking it down to pieces that are assigned to communication services. The technically available bandwidth is 5 to 9 orders of magnitudes larger than what is typically used for protection communication today. By selecting the adequate option, new advanced protection concepts such as travelling wave protection can be successfully applied. This opens the fantasy for further innovative protection concepts. The identified opportunities for the relay design include using PTP and the related profiles for the electrical power industry for time synchronization.

Paper 309 from Switzerland emphasizes on the fact that the data exchanged between the parts of the automation and control system for electrical power system have very different nature. Segregating the data into classes according to urgency and significance allows to assign them to communication services and communication channels of adequate behaviour and performance.

Question

Question 3-7: According to paper 306, there are enormous gains in communication bandwidth (exceeding the bandwidth typically requested by present day protective relay designs by as much as 5 to 9 orders of magnitude) possible. This makes new protection principles feasible and provides a lot of room for fantasy. As an example, travelling-wave-based differential protection is mentioned.
In addition to the abovementioned applications, which further innovative protection, automation and control functions are imaginable if the current bandwidth restrictions were waived?