Fault Tolerant Ethernet Based Network for Time Sensitive Applications in Electrical Power Distribution Systems

Leos BOHAC, Jiri VODRAZKA

Department of Telecommunications Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Technicka 2, 160 00 Prague, Czech Republic

bohac@fel.cvut.cz, vodrazka@fel.cvut.cz

Abstract. *The paper analyses and experimentally verifies deployment of Ethernet based network technology to enable fault tolerant and timely exchange of data among a number of high voltage protective relays that use proprietary serial communication line to exchange data in real time on a state of its high voltage circuitry facilitating a fast protection switching in case of critical failures. The digital serial signal is first fetched into PCM multiplexer where it is mapped to the corresponding E1 (2 Mbit/s) time division multiplexed signal. Subsequently, the resulting E1 frames are then packetized and sent through Ethernet control LAN to the opposite PCM demultiplexer where the same but reverse processing is done finally sending a signal into the opposite protective relay. The challenge of this setup is to assure very timely delivery of the control information between protective relays even in the cases of potential failures of Ethernet network itself. The tolerance of Ethernet network to faults is assured using widespread per VLAN Rapid Spanning Tree Protocol potentially extended by 1+1 PCM protection as a valuable option.*

Keywords

E1, PCM, protective switch, RSTP, smart grid, time sensitive applications.

1. Introduction

The foreseen concept of Smart Grid technology, which promises highly efficient and dynamic energy systems in Europe, has to be backed by suitable information and communication system. From this perspective it is more than obvious to take already acquired knowledge from well-developed ordinary information and communication systems and apply it to the realm of the power energy system.

However, the energy systems like the power electrical grids have more stringent requirements on the performance factors of the communication system, at least in terms of reliability, than is generally required and expected from ordinary information systems.

There has been a growing interest in recent couple of years to apply already existing ICT technology in an electrical power industry. The main stimulus behind these activities can be primarily seen in the lower and continually decreasing capital costs, strong technology standardization and its maturity. What is not also negligible is that one can select the particular devices from a broader range of manufacturers avoiding potential vendor lock as often seen in the power distribution industry today. Ethernet technology, originally developed and targeted specifically only for the local area network segment, is nowadays very mature, low cost, scalable and reliable communication network platform that is easily upgradable to speeds of tens of gigabits. Thus, it is not surprising there is a great effort to lay this network as a foundation for the future integrated communication system of the power electricity engineering industry [1], [11].

However, Ethernet technology is not alone as the candidate considered replacing the legacy systems in an electrical power industry. Its combination with IP and MPLS (Multiprotocol Label Switching) is also taken into account [2] to specifically cover communication needs in an extended geographical domain rather than a small area of only one substation as is most common in Ethernet's deployment today [5], [10]. This extended communication coverage is very typical for deployment in large SCADA systems (Supervisory Control and Data Acquisition) [8].

The basic Ethernet technology is well suited for supporting the data transfer for classical information tech-

nology applications running in the campus or office environment or accessing Internet resources, but not so much for the process automation or device monitoring in real time. Also, though the reliability of the basic Ethernet technology is sufficient for aforementioned office applications it is not as well for the control data exchange in the electrical power industry. Thus, the efforts have been made to alter or supplement the function of basic Ethernet technology to provide a better reliability figures particularly in the area of the substation deployment [4], [6].

As was already stated, one of the most important applications in the electrical power distribution systems is that of providing the protection relay intercommunication that is very demanding as regards the guarantee of reliability and minimum delay. Several papers [3], [7], [9], [12], [13] have already addressed these issues in different ways. It is possible either to define new protocol to deal with a potential node or link failure or use one from already existing set of standardized protocols. Implementing new algorithms is quite complicated and also in the very pragmatic world of an electrical power industry challenging to enforce. In our work we target first choice and analyze a situation where there in Ethernet based network is deployed the per VLAN (Virtual Local Area Network) Spanning Tree Protocol (RSTP) in combination with 1+1 PCM (Pulse-code Modulation) protection scheme in addition to the dedicated primary communication line among protection relays themselves. This protocol selected was well in line with one of our practical projects we have dealt with where there was a requirement to use already existing protocol (if possible) in the network (in this case the per VLAN RSTP) and validate its practicability for the protection relay traffic in the network with multiple VLANs.

2. Network Test Arrangement

The laboratory test interconnection of the network devices is depicted on Fig. 1. In order to stay more aligned with real practical situations, our intention was to use such a network arrangement that would be more relevant to a similar network topology deployed in one electrical power distribution company in Czech republic. All devices in our testbed are manufactured by Cisco and the network is strictly based on Ethernet L2 switching of data frames. The laboratory network architecture also follows the standard layered approach recommended by Cisco for enterprise/campus-like networks where switches SW11 and SW21 represent the core or distribution layer and all others are part of the access layer.

In practice, each electrical substation site is connected to the network core through two identical local Cisco switches (e.g. SW12 and SW13 in our lab) to ensure both communication device and medium redundancy needed in case of the fiber or access device failure. The issues related to other potential single points of failures, like common installation of both uplink fiber cables in the same duct or feeding both redundant switches from a single power supply source were not considered.

In the paper we have strictly concentrated only on studying the effects of the dynamic network reconfiguration on the data transport interruption when one of the uplink-fiber fails (e.g. fiber cut). At the very bottom of the Fig. 1 there are two boxes named Siprotec. They represent the real high voltage remote differential protection relays from Siemens communicating in real time between each other at the electrical power distribution network to protect the electrical grid from detrimental failures that may cause the potential damage to the power lines or other power grid devices. The data communication between these relays is very important in the power distribution engineering field and as such it makes very sensitive issue to deal with. The communication requirement of the protection relays belongs to the low-bandwidth high-response real time category that is generally difficult to support unless the network is able to guarantee some sort of the priority dispatching schema of frames corresponding to this type of service.

In our case the electrical power distribution company has been using historically for ensuring the protection relays communication two independent lines, one primary optical fiber based line (blue arrowed line in Fig. 1) and second redundant PCM E1 based line (yellow line connecting PCM muldexes). If primary optical fiber line is not interrupted the relays communicate only through them. When the primary line fails the traffic is automatically rerouted to the secondary line hosted by PCM transmission system. The serial data of relays are first mapped in PCM muldex to the corresponding E1 frame channel of E1 and then are sent to the opposite PCM muldex through another pair of fibers. The direct primary and secondary optical fibers (via PCM) pass along the different pathways to tackle forming a single point of failure at common duct/cable level.

Our goal was to check whether the PCM can be potentially replaced by Ethernet based network without incurring unacceptable transit delay and decreased reliability. The laboratory testbed corresponding to the Ethernet network is also depicted in Fig. 1. Four Ethernet switches form a representative part of entire Ethernet metropolitan network. This network is also used for other applications, particularly SCADA, to move data from Remote Terminal Units (RTU's) installed in appropriate substations (the pair of switches SW12/SW13 is in practice installed in the place of one

substation and SW22/SW23 in another) to the central SCADA servers connected to the core switches SW11 and SW21. In other words, the interconnection of switches is not purpose built only for the relays, but the network as a whole must support also hub-and-spoke type of communication. A key design requirement was to preserve currently running resilience protocol in the network, which is per VLAN RSTP, and check its reconfiguration/interruption time in the case of link failure. As can be seen from network topology, there is potentially a number of possible failures, both on the side of the devices and connecting fibers.

However, most probable failures come from the uplink fibers (e.g. from SW11 to SW12) as they are relatively long (several kilometers) and pass through various pathways that may be cut or another way interrupted. Other fiber segments in the network (e.g. SW11-SW21, SW12-13 and SW22-23) are only short local interconnection of switches not posing a great reliability issue if properly treated. The device failures were not extensively studied here thought in some cases they can be simulated by the node's concurrent multiple fiber failure model.

3. RSTP Convergence Time

Ethernet technology historically supported only active tree topology. This requirement resulted in only one active pass permissible for any pair of communicating in the entire bounded switched network. If this rule was not adhered to, the potential loop in the network would leave network totally inoperable causing endless circulation of the data frames and inducing excessive load on the switches that forced very quickly reindex station's position in the network. Sooner or later this way looped Ethernet network is sentenced to its own load collapse. However, the impossibility to intentionally introduce the loops in the network topology significantly affects its resilience as there is only one path available between any two communicating devices and when any component of this path fails the path fails fully disabling any subsequent data transfer. In this sense the loops are very vital providing standby paths in case the active ones fail.

The ability of the Ethernet to resist the line or node failures is very significant for applications that operate in the real time and do not tolerate long traffic disruption. For the classical office and campus network applications Ethernet was supplemented by the distributed algorithm called Spanning Tree Protocol (STP) that enabled design of Ethernet network topology with multiple physical loops. However, in this case STP dynamically builds up logical tree topology above the physical one by blocking specific segments between switches and thus disconnecting loops holding operational topology again as the tree. If the failure of the switch or any segment occurs in the active logical tree, the STP progressively builds up a new and different active logical tree out of still operating parts (i.e. switches and segments) of the network.

The STP has been standardized and implemented for years in accordance with the document known as IEEE 802.1D. However, the main drawback of this historically first standard has been a low convergence speed of the algorithm leading in the event of the failure to a very long traffic disconnection time in the order of tens of seconds, which is not acceptable for mission critical applications like the ones used in the process control of utility systems.

RSTP protocol was specifically designed to tackle slow convergence of its predecessor. In our project we have used this protocol because it can support very short outage of data packet streams in case of network failures.

4. RSTP Convergence Measurement

In our situation of the laboratory tests we have used aforementioned network topology in Fig. 1. The core switches were Cisco Catalyst C3560 and all access switches Cisco Catalyst C2960. The software images we have used ordinarily supported the rapid spanning tree protocol. Though better choice was to implement multiple spanning tree protocol (MSTP), we have rather concentrated on the tests and verification of per VLAN rapid spanning tree protocol (per VLAN RSTP) as this one was required to be checked in our project. The slowest convergence of RSTP protocol is when the root switch fails and hence the remaining switches are forced to elect new root switch to continue to support a logical spanning tree in the network. However, this event was not considered for it has a lower probability to occur than the uplink fiber failures.

We have configured the network in such a way that SW11 played a role of active root switch in our topology and SW21 as a standby root bridge for the case of the primary is lost. The star-type topology was dictated by the design of the production network, traffic patterns in the network and the primary requirement to have minimum devices between substations and the substations and the network center, here represented by SW11 and SW21 switches. Thought this double-star like topology is very demanding as the number of the optical fibers and lengths required it does not make a big trouble in our case as the corresponding distribution company already had its own very rich optical network with a plenty of the optical fibers already installed. Alternative topologies can be considered,

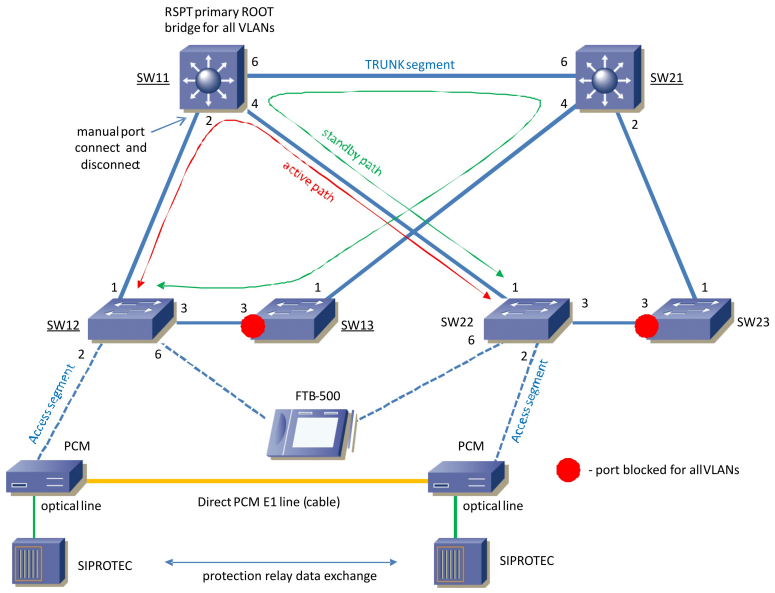

Fig. 1: The laboratory test topology; the core and access switches from Cisco were used (C3560 and C2960 respectively); for the measurement of the traffic disruptions we used professional network analyzer form EXFO, FTB 500; the network was configured to support the increasing number of VLANs; port #2 on SW11 was repeatedly disconnected and connected to simulate break of fiber between switches SW11 a SW12; the red line represents the active path and green standby path respectively that is activated by RSTP in case of disconnection of port#2 on SW11.

of course (like the ring), but redesigning this critical network was not welcomed at all by the distribution company as it is very pragmatic to any considerable changes in any system if these are not absolutely necessary bringing clear benefit for the potential failure of the network is in stake anytime when any configuration and hardware change are made. These type of networks and systems fall under strict rules of reconfiguration, testing and management procedures and thus it is not easy to do some experiments in live there.

The test procedure of our measurement was quite simple. We used a professional EXFO analyzer FTB 500 to inject repeated train of Ethernet frames of 200 bytes long to the port #6 of SW12 every 1 ms in time and at the SW22 this sequence was received and lost frames counted. The disruption time is then given by the number of lost frames multiplied by frames sending period at the transmitter site using the formula

$$t_{dis} = N_{lost} T_p, \tag{1}$$

where t_{dis} is time of traffic disruption in the case of the port#6 connect or disconnect event, N_{lost} is the number of lost Ethernet frames and T_p is the period of time forframes are sent to the port#6 on SW12 (in our case 1 ms).

We used the physical access speed of 100 Mb·s^{-1} on all ports in the network in our test. The processing delay at the transmitter and receiver site of the analyzer and the length of frames were neglected as they are in the order of microseconds and we are dealing here with disruption times in the order of tens of milliseconds and even more, see further.

The precision of our measurement is primarily dictated by a finite time of sending frames in the network, in this case it is ±2 ms. Again it can be neglected in comparison with the average disruption times measured.

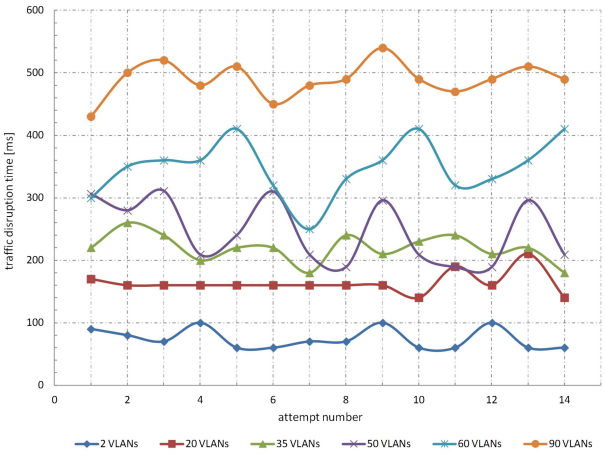

Fig. 2: The plot of traffic disruption time in case of port#2 disconnection versus the number of the attempt tried and number of VLANs.

The number of VLANs was changed in each step on the switch SW11 and using VTP protocol the list of VLANs was distributed to remaining switches in the network followed by other cycle of the experiment. One experiment consisted of 14 cycles of port#2 disconnect/reconnect events at SW11 and results were plotted in graphs shown in Fig. 2 and Fig. 3. Fig. 2 corresponds to disconnect events and Fig. 3 reconnect

events. As can be seen when a number of VLANs is kept low the disruption time is also low and has even small variance.

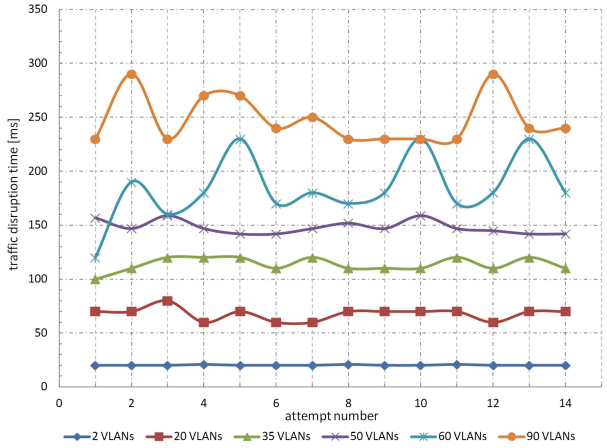

Fig. 3: The plot of traffic disruption time in case of port#2 reconnection versus the number of the attempt tried and number of VLANs.

However, as the number of VLANs increases the disruption time as well and also its variance. The reason for that behavior can be attributed to how multiple control messages of RSTP are processed inside the switches. The similar curves corresponding to the reconnection events are shown in Fig. 3. As can be seen, the reconnection disruption times are shorter than disconnection ones, and again a larger variance is evident when the number of VLANs is increasing. In order to

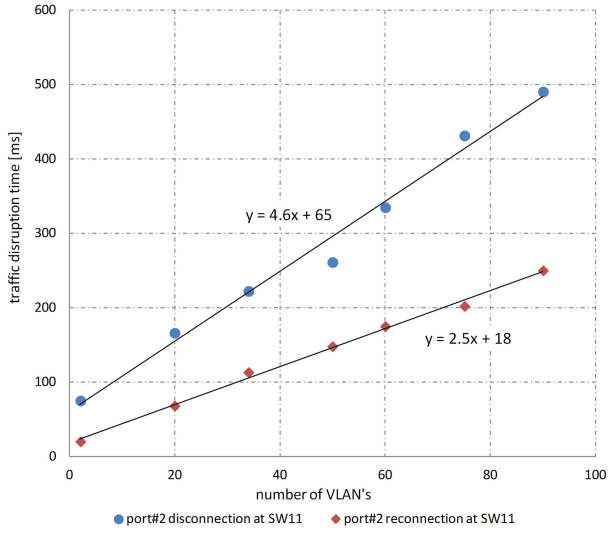

Fig. 4: The plot of traffic disruption time in case of the port #2 disconnect (blue) and connect (red) events versus the number of VLANs in the network.

better understand dependence of the disruption time on the number of VLANs we have plotted the average values of disruption times for all cycles in other plot shown in Fig. 4, where a nearly linear dependence of the disruption time on the number of VLANs can be seen.

5. Conclusion

In the paper we have summarized measurements done in a laboratory environment to check the feasibility of RSTP and Ethernet network for deployment in demanding electrical power distribution network. We have found that performance of per VLAN RSTP protocol as implemented by Cisco switched is linearly dependent on the number of VLANs configured in the network and that time of traffic disruption grows faster in the case of uplink disconnect than reconnect event. Thus, to use per Vlan RSTP the number of VLANs has to be considered even in a very simple hub-and-spoke topology. Also, the more VLANs in the network the larger variance in disruption traffic was found.

When the protective relay's communication is considered in this scenario, it is evident that in the moment of the uplink fiber cut (disconnect) the communication line is not available at least for 80 ms at the average time and with only one VLAN in the network configured that is not typical situation in practice at all. In many case such a long disruption time is not tolerated by most differential protection relays where the required ranges are in the fraction up to the order of a few milliseconds (0,5–5 ms) depending on the type of protection. Thus, in the failure scenario the relays are not able to communicate among each other. In order to make communication more robust, it is possible to send relay's data along two separate paths and hence use 1+1 protection or to strictly keep communication fiber's or equipment's failures independent of those in the electrical power system to ensure a break in power distribution system will not cause at the same time a failure at communication network.

Acknowledgment

This work was supported by the Grant of the Ministry of the Interior of the Czech Republic, No. VG20132015104, "Research and development of secure and reliable communications network equipments to support the distribution of electric energy and other critical infrastructures", and was researched in cooperation with TTC Telecomunikace.

References

[1] JANCA, T. R. Utility Ethernet network architecture: Networked Electrical eXchange Topology-

NEXT. In: *Sarnoff Symposium (SARNOFF)*. Newark: IEEE, 2012, pp. 1–6. ISBN 978-1-4673-1465-7. DOI: 10.1109/SARNOF.2012.6222721.

[2] FUJIKAWA, F., K. KUWABARA, Y. KODA and M. KIUCHI. Examination of electric power utility network applying IP router/MPLS router/wide-area Ethernet. In: *Power Engineering Society General Meeting*. Denver: IEEE, 2004, pp. 901–904. ISBN 0-7803-8465-2. DOI: 10.1109/PES.2004.1372956.

[3] BRUNELLO, G., R. SMITH and C. B. CAMPBELL. An application of a protective relaying scheme over an ethernet LAN/WAN. In: *Transmission and Distribution Conference and Exposition*. Atlanta: IEEE, 2001, pp. 522–526. ISBN 0-7803-7285-9. DOI: 10.1109/TDC.2001.971288.

[4] MIDANCE, R. and D. IADONIS. Ethernet networks redundancy with focus on IEC 61850 applications. In: *20th International Conference and Exhibition on Electricity Distribution*. Prague: Curran, 2009, pp. 1–4. ISBN 978-184919126-5. DOI: 10.1049/cp.2009.0637.

[5] QUERASHI, M., A. RAZA and D. KUMAR. A survey of communication network paradigms for substation automation. In: *Power Line Communications and Its Applications*. Jeju City: IEEE, 2008, pp. 310–315. ISBN 978-1-4244-1975-3. DOI: 10.1109/ISPLC.2008.4510445.

[6] HEINE, H. and O. KLEINEBERG. The High-Availability Seamless redundancy protocol (HSR): Robust fault-tolerant networking and loop prevention through duplicate discard. In: *Factory Communication Systems (WFCS)*. Lemgo: IEEE, 2012, pp. 213–222. ISBN 978-1-4673-0693-5. DOI: 10.1109/WFCS.2012.6242569.

[7] WARD, S. and W. HIGIBHOTAN. Network errors and their influence on current differential relaying. In: *Protective Relay Engineers*. College Station: IEEE, 2011, pp. 79–90. ISBN 978-1-4577-0494-9. DOI: 10.1109/CPRE.2011.6035607.

[8] KWOK-HONG, M. and B. L. HOLLAND. Migrating electrical power network SCADA systems to TCP/IP and Ethernet networking. *Power Engineering Journal*. 2002, vol. 16, iss. 6, pp. 305–311. ISSN 0950-3366. DOI: 10.1049/pe:20020604.

[9] DEMETER, E., S. FARIED and T. S. SIDHU. Power System Protective Functions Performance Over an Ethernet-based Process Bus. In: *Electrical and Computer Engineering*. Vancouver: IEEE, 2007, pp. 264–267. ISBN 1-4244-1020-7. DOI: 10.1109/CCECE.2007.72.

[10] VASEL, J. One plant, one system: Benefits of integrating process and power automation. In: *Protective Relay Engineers*. College Station: IEEE, 2012, pp. 215–250. ISBN 978-146731841-9. DOI: 10.1109/CPRE.2012.6201235.

[11] POZZUOLI, M. P. and R. MOORE. Ethernet in the substation. In: *Power Engineering Society General Meeting*. Montreal: IEEE, 2006, pp. 1–7. ISBN 1-4244-0493-2. DOI: 10.1109/PES.2006.1709165.

[12] MOXLEY, R., K. FODERO and H. J. ALTUVE. Updated transmission line protection communications. In: *Power Systems Conference*. Austin: IEEE, 2009, pp. 394–401. ISBN 978-1-4244-4182-2. DOI: 10.1109/CPRE.2009.4982528.

[13] CHLUMSKY, P., Z. KOCUR and J. VODRAZKA. Comparison of Different Scenarios for Path Diversity Packet Wireless Networks. *Advances in Electrical and Electronic Engineering*. 2012, vol. 10, iss. 4, pp. 199–203. ISSN 1336-1376.

About Authors

Leos BOHAC received the M.Sc. and Ph.D. degrees in electrical engineering from the Czech Technical University, Prague, in 1992 and 2001, respectively. Since 1992, he has been teaching optical communication systems and data networks with the Czech Technical University, Prague. His research interest is on the application of high-speed optical transmission systems in a data network. He has also participated in the optical research project Czech Education and Scientific NETwork (CESNET) - the academic data network provider to help implement a long-haul high-speed optical research network. Currently, he has been actually involved in and led some of the projects on optimal protocol design, routing, high speed optical modulations and industrial network design.

Jiri VODRAZKA was born in Prague, Czech Republic in 1966. He joined the Department of Telecommunication Engineering, Faculty of Electrical Engineering, Czech Technical University, Prague in 1996 as a research assistant and received his Ph.D. degree in electrical engineering in 2001. He has been the head of the Transmission Media and Systems scientific group since 2005 and became Associate Professor in 2008. He participates in numerous projects in cooperation with external bodies. Currently he acts also as vice-head of the Department.