P31

Solutions for the Alternative Route of the Teleprotection Communication Channel

V. ČELEBIĆ, A. KABOVIĆ, M. KABOVIĆ, J. GAJICA, I. SALOM
Institute "Mihajlo Pupin", Belgrade,
Serbia

SUMMARY

Transmission of the teleprotection signals must meet very stringent requirements such as dependability, security and transmission time. The most stringent requirement is the dependability, defined as the ability to provide uninterrupted relay communication during a recovery in the communication network due to a fiber break or component failure. Dependability relates to the ability to issue and receive a valid command in the presence of interference and/or noise, by minimizing the probability of missing a command. This requires the use of redundant backup communication paths.

With the aim of increasing the availability of the communication path, optimal alternative communication paths for the teleprotection signals were considered within the company JP EMS (Serbian Transmission System and Market Operator). Considering the existing network infrastructure in order to reach the optimal solution, several possibilities were analyzed which differ in the type of the communication path used, and interfaces on the teleprotection terminal. The main communication path for teleprotection in JP EMS is OPGW. Analyzing the availability of the existing JP EMS communication network, the most suitable solutions are considered to be: E12 (ITU-T G.703-2 Mbps) and Ethernet interfaces, and TDM and Ethernet communication paths. Using Ethernet interface with the transmission of the packets over the SDH network was concluded as the best solution for the redundant path in most cases. VLAN network configuration was used in order to separate teleprotection service from other services. Tests were carried out to determine whether the proposed solution meets the requirements for transmission of the teleprotection signals. During testing, three types of messages were used: GOOSE, dedicated and ping messages. Testing showed that such a solution can meet the requirements expressed in the IEC-60834 standard.

KEYWORDS

teleprotection, Ethernet over SDH, E12 interface, VLAN, GOOSE.

vladimir.celebic@pupin.rs

1. Introduction

Solving the problem of the redundant communication path for the teleprotection signals is very important, and related to the development of the communication technology and its application in the telecommunication system of the power utilities. This communication system is expected to support not only low bandwidth applications, but also high bandwidth applications such as (video, corporate data etc.). Communication technologies have evolved during the years, but the requirements for the transmission of the teleprotection signals (transmission time, dependability, and security) have not been changed, and are defined by the standard IEC-60834 (Table 1).

Protection scheme	Maximum actual transmission time T_{ac} (ms)	Channel quality (BER)	Noise duration T_B (ms)	Security P_{uc}	Dependability P_{mc}
Blocking	10	10^{-6}	Continous	N/A	$< 10^{-3}$
Blocking	10	Worst case	200	$< 10^{-4}$	N/A
Permissive underreach	10	10^{-6}	Continous or pulsed	N/A	$< 10^{-2}$
Permissive underreach	10	Worst case	200	$< 10^{-7}$	N/A
Permissive overreach	10	$< 10^{-6}$	Continous or pulsed	N/A	$< 10^{-3}$
Permissive overreach	10	Worst case	200	$< 10^{-7}$	N/A
Intertripping	10	$< 10^{-6}$	Continous or pulsed	N/A	$< 10^{-4}$
Intertripping	10	Worst case	200	$< 10^{-8}$	N/A
Note – All values refer to digital communication channels, and applications for EHV systems					

Table 1: Requirements for the teleprotection signals and communication channel [1]

Analysing the existing communication network of the JP EMS company as well as location of the communication and teleprotection equipment in substations, two interfaces were considered as optimal solutions for the redundant communication path:

- E12 (ITU-T G.703-2 Mb/s)
- Ethernet (IEEE 802.3).

Emphasis was put on analysing the combination of the Ethernet interface and the SONET/SDH as the transmission path. Transmission of the packet traffic over the SDH system is very frequently used in power utilities thanks to the advances in technology in both domains [2] [3].

2. Interfaces Considered in Redundant Communication Path for Teleprotection Signals

2.1 E12 (ITU-T G.703-2 Mb/s) Interface

Depending on the location of the teleprotection terminal, the E12 wired interface can be connected to the SDH multiplexer directly in case the teleprotection equipment is not situated far from the multiplexer, or the connection can be realized by the conversion of the E12 wired interface to fiber optic by using a fiber optic modem, or using the interface according to the standard IEEE C37.94.

Standard IEEE C37.94 defines a programmable n x 64 kbps (n = 1,…,12) multimode optical fiber interface to provide communication between teleprotection and multiplexer equipment for distances up to 2 km. Later on, a monomode optical fiber is also adopted in order to reach longer distances. The last version of this standard was accepted in 2013 as IEC62843-2013. The advantage of this type of interface is that it enables interoperability.

2.2 Ethernet (IEEE802.3) Interface

The Ethernet interface was also considered as another option for a backup interface. It is important to emphasize that the best teleprotection performance over Ethernet is realized when Ethernet is the native protocol of the teleprotection device [3].

Ethernet is the broadband communication network which belongs to the second layer of the OSI communication model. Ethernet has become a popular networking technology because of its low cost (eliminating the need for using different equipment for different service types), high bandwidth and versatile support for multiple applications. It is used in power utilities for the transmission of the operational and business services. When considering operational services, it is used for monitoring, control, transmission of the measuring data and teleprotection commands. Standard IEC61850 is established for regulating these types of communication in the substations (LAN networks), and also among the substations (MAN and WAN networks), with device interoperability as its main goal. It is realized with copper cables or optical fibers, and many articles such as [4], describe what is important when designing this type of network. Parameters to be taken into account are: network availability, security and the mechanism for reconstruction and recovery. Because of the great traffic diversity, the information must be separated according to priority, so the expected quality of service could be accomplished. In the previous generation of the communication systems SDH network is widespread, and is still in function. One of the methods which proved to be convenient for connection SDH and packet networks is Ethernet over SDH, which is one of the reasons it was chosen for testing.

To test the validity of this solution, the measurements of the transmission delay between two distant points were done, by software simulation of the teleprotection commands generation.

2.3 Testing Ethernet over SDH as the Alternative Transmission Path for the Teleprotection Signals

For testing purposes, the LAN is realized, which includes two distant locations, simulating where the teleprotection terminals could be placed in the near worst case. Testing is carried out by simulating the teleprotection commands generation, and measuring transmission delay, using the software installed on the computers set up at the terminals. Measurement of the transmission delay in the LAN network requires the test terminals to be time synchronized. Various methods for time synchronization could be applied, but to simplify the test, the circular transfer time measurement was chosen. This means that commands are generated and received on the same terminal. In addition, the generated messages contain the information about the time of sending. Software which works on the other terminal is used only for receiving and forwarding commands back to the starting location. When the message is received, the time of the receipt is recorded, message validity is tested, sending time is extracted, and finally the circular transmission time is calculated.

Hardware configuration for the test follows the configuration when the teleprotection terminals would be connected to the network. Test terminals are connected to the Ethernet using switches, connected in the ring topology. This configuration is further connected to the SDH device. The connection is the same at both locations, as it is shown in Figure 1.

Three types of messages were used for the test: dedicated, GOOSE (Generic Object Oriented Substation Message), and ping (Packet Internet Groper). Dedicated and GOOSE messages were generated by the software using protocols from the second and third layer of the OSI model. The main difference between them is that the dedicated messages are transferred unicast, while GOOSE messages are transferred multicast. Ping messages are the standard tool for testing computer networks, and they are generated using ICMP (Internet Control Message Protocol) Echo function. Separate software applications were made for the transmission and the reception of both types of messages. They are running on the same test terminal on one location, while the software for forwarding messages is running at the other location. Testing consisted of generating a certain number of messages of the selected type with the chosen time interval, and if the message was correctly received, travel time through the network is calculated.

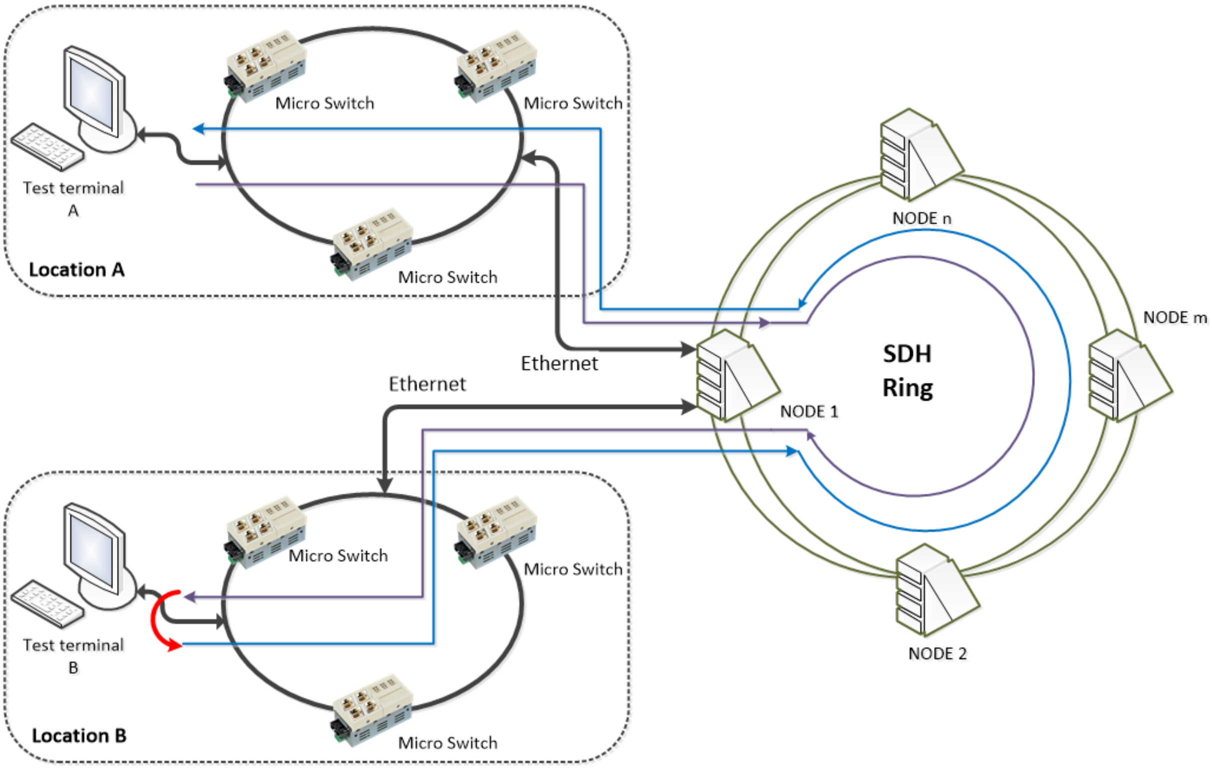

Figure 1 – Configuration of the VLAN for testing the round trip delay of the teleprotection messages

2.4 Short Description of the Software Applications

Block diagram representing the position of the realized software applications is shown in Figure 2.

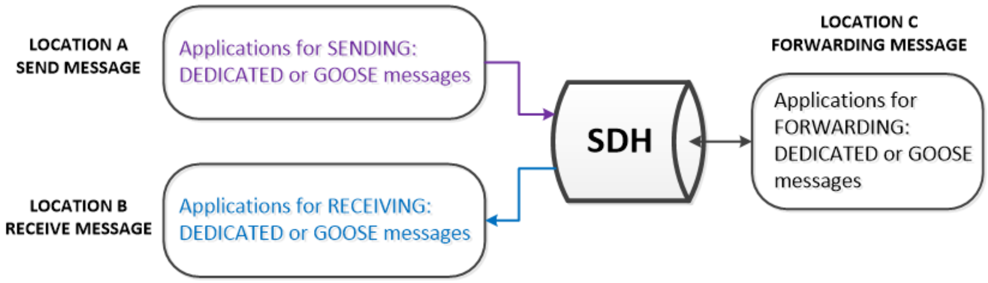

Figure 2 – Block diagram of the position and names of the software for testing propagation of the dedicated and GOOSE messages through the network

In Figure 2, the upper block “Location A Send Message” represents the applications for generating and sending teleprotection commands of the dedicated or GOOSE type respectively, while the lower block “Location A Receive Message” represents the applications for receiving these commands. As previously mentioned these blocks work on the same test terminal and send/receive data over the same Ethernet interface. The block “Location B Forwarding Message” represents the applications for forwarding dedicated or GOOSE messages respectively, which are running on the terminal at the remote location.

2.4.1 Software Applications for Dedicated Messages

The application for dedicated message generation, “SendAFPacketSockRaw”, has the following input parameters: number of messages that will be generated, time interval between two messages, and the hardware address of the interface at the remote site. Communication is carried over a network connection created in the domain of the second level of the OSI communication model, the so called packet interface with the socket type – “SOCK_RAW”, and implemented protocol – “IPPROTO_RAW“. The message has a fixed structure which consists of the following parts: the first byte defines the beginning of the message, next eight bytes define the type of the signal sent on each teleprotection channel (command or guard message), followed by the sending time and the message number in the sequence.

The application "ReceiveAFPacketSockRaw" for dedicated message reception, has the following input parameters: maximum number of messages to be received (that is equal to the number of sent messages), and hardware address of the interface at the remote site that delivers the message. The type of network connection created for reception of data is the same as in the "SendAFPacketSockRaw" application. After the message arrives in the reception buffer, the hardware address from the Ethernet frame is first checked. If the destination and the source address are correct, the checking of the message is continued to determine whether the received message is the same as the one submitted. If it is established, the round trip delay and transmission time is calculated.

The application "RecSenAFPacketSockRaw" is running on the test terminal at a distant location (location B), and is intended for receiving/sending messages from/to the location A (see Figure 1). Input parameters of this application are: maximum number of messages which are expected to be forwarded, and hardware address of the interface at location A which sends/receives messages. The type of network interface is the same as the network interfaces created in previously mentioned applications. When the message is received, first the addresses from the Ethernet frame are checked, after which the rest of the message is checked. If the checked data are correct, the message is sent to location A, where the complete testing is done.

2.4.2 Software Applications for the GOOSE Messages

Standard IEC61850 has designed GOOSE message to replace dc control wiring between devices. It is a mechanism for the fast transmission of substation events and the performance requirement for GOOSE is an operation time of 4 ms in the LAN. The message of this type is initiated by the monitored events of the equipment in the substation. Besides transferring teleprotection commands, GOOSE messages could be used for the transmission of the control commands, as well as measured values of the voltage or current. When there is a change of at least one monitored data, the message is sent. They are sent to the multicast address of the local network. When they are used in the WAN network, the multicast address is not used. The messages are sent repeatedly, and in the steady state the repetition interval is 1s. The equipment which receives the message must be configured for its reception. Every message has the data named "ttl" – time allowed to live, which determines the repetition time. The recipient of the message calculates the time of arrival for the next message based on this data. For the network load less than 70%, and without the presence of noise, the probability of the lost commands must be less than 0.001. For testing the transmission of the teleprotection commands using GOOSE messages, special applications were realized to run on test terminals as shown in Figure 2.

The application "SendGooseMessage" is dedicated for generating teleprotection commands as GOOSE messages, while "ReceiveGooseMessage" represents the application for its reception. As it is previously mentioned for the dedicated commands, they work on the same terminal and send/receive data over the same Ethernet interface. Block "RecSenGooseMessage" represents the application for message forwarding, and works on the terminal situated at the distant location.

The application "SendGooseMessage" has the following input parameters: number of messages that will be generated, and the time interval between two generated messages. The network connection and implemented protocols are almost the same as for the generation of the dedicated messages. The only difference is that the message is sent multicast.

The structure of the message and the control block for transmission are as defined in the IEC61850 standard. The main set of the data transmitted by the command, represents the state on the monitored sections, that is, whether the command or guard signal is sent. Besides these data, the message contains other important data such as: the hardware address of the destination interface, the identification of the application which sends the message, time when the next message would be received in sequence and etc. [6].

The application "ReceiveGooseMessage" is running on the same test terminal at location A, as "SendGooseMessage". Its input parameters are: the maximum number of messages expected, and the hardware address of the interface from which the messages are sent (MAC address of the interface at the location B). The type of network connection, and the used protocol for reception are the same as in the application for sending messages. After the message reception, and address checking, it is tested whether the message has arrived in the defined time interval. If it has, parts of the messages are extracted and tested. Testing is done according to the equipment's configuration for receiving this type of message, and the data from the previous correctly received message. If the message is correctly received, the round trip delay is calculated.

The application "RecSenGooseMessage" is running on the test terminal at a distant location (B), and is intended for receiving/sending messages from/to the location A. Input parameters of this application are: maximum number of messages which are expected for forwarding, and hardware address of the interface at location A which sends/receives messages. The type of network interface is the same as the network interfaces created in the previously mentioned applications for the GOOSE messages. Message checking is done partially, and if the message is correct it is sent back to location A.

3. The results of testing

The transmission time, dependability and security of the Ethernet over SDH as the communication path, were tested using the previously described method and using the configuration which provides the worst case, in terms of the transmission time. The switches for connection test terminals with SDH multiplexers were connected in the ring configuration (Figure 1). Testing was done with the message sequences of various lengths such as 500, 1000, 10000 and 100000 messages, and with various message intervals: 2, 5, 10, 50, 100, 200 and 1000 ms. The obtained data were statistically processed in order to calculate various data such as the maximum and minimum value of the transmission time from location A to location B, the mean value, and the standard deviation. The results for the statistically obtained parameters are summarized below in Tables 2 and 3, and in Figure 3 as well.

MESSAGE TYPE	INTERVAL [ms]	TRANSMISSION TIME [ms]			NUMBER OF MESSAGES
		MAX	MEAN VALUE	MIN	
GOOSE	2	4.752	4.188	3.973	260 980
	5	4.644	4.190	3.978	50 990
	10	6.260	4.187	3.981	110 989
	50	4.498	4.197	3.990	30 990
	100	4.981	4.191	3.968	570 959
DEDICATED	2	4.601	3.727	3.504	397 985
	5	4.078	3.757	3.513	77 985
	10	5.718	3.729	3.513	30 990
	50	5.899	3.766	3.568	34 990
	100	5.836	3.736	3.513	15 990
	2000	4.023	3.771	3.555	99 995
PING	1000	4.011	3.863	3.692	500
	200	4.021	3.868	3.667	11 000

Table 2: Summarized results for the maximum, minimum, mean value and the standard deviation of the transmission delay of the messages from A to B for each message interval

Table 2 shows the comparison of the previously mentioned statistical parameters for various message intervals and all types of messages. From these results it can be concluded that the mean value of the transmission time does not depend on the interval of the message generation. On the basis of the data from the tables, it can be concluded that the maximum transmission delay is significantly below the limit of 10 ms. According to the test results, the dependability and the security of the transmission meet the requirements of the standard IEC 60834.

	TRANSMISSION TIME [ms]				
MESSAGE TYPE	MAX	MEAN VALUE	MIN	STDEV	NUMBER OF MESSAGES
GOOSE	6.26	4.19	3.97	0.0639	1 024 908
DEDICATED	5.90	3.74	3.50	0.0640	641 935
PING	4.02	3.87	3.67	0.0630	11 500

Table 3: Summarized results for the maximum, minimum, mean value and the standard deviation of the transmission time of the messages from A to B, for all three tested types of messages

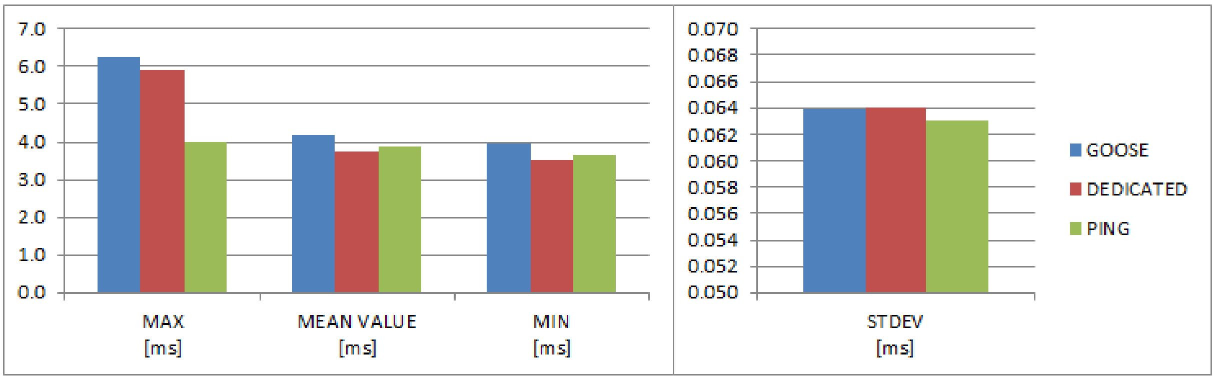

Figure 3 – Graphical presentation of the results shown in Table 3 for three types of the messages

In order to determine the delay of certain parts of the network shown in Figure 4, another test was carried out. The transmission time for all three types of messages was measured for three network configurations:

- With SDH ring and switches – complete configuration (where $T_{SUM} = 2 * T_{PROC} + 2 * T_{SW} + T_{SDH}$),
- With SDH ring and without switches (where $T_{SUM} = 2 * T_{PROC} + T_{SDH}$),
- Without SDH ring and switches (where $T_{SUM} = 2 * T_{PROC}$).

The messages were generated with the time interval of 200 ms and test results for all types of network configurations are given in Table 4.

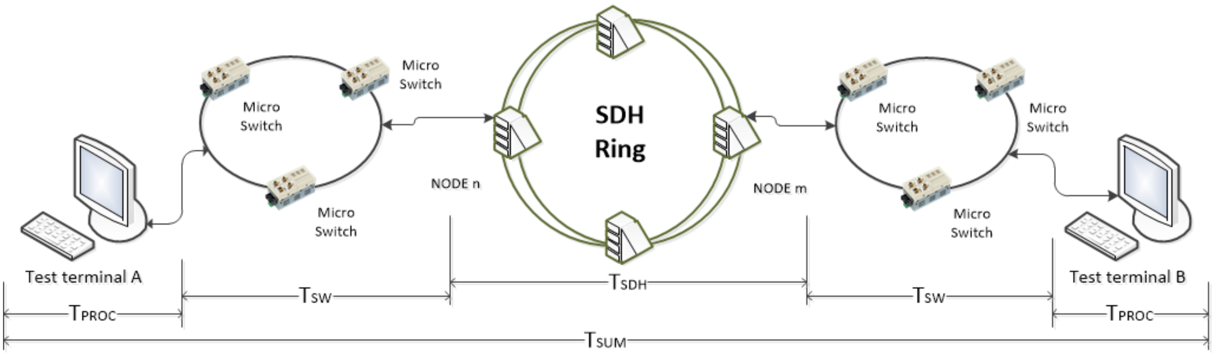

Figure 4 – Transmission delay in the parts of the communication network

One more test type was carried out. The test consisted of generating messages in packs of 3 posts, 2 ms apart, with a package separation of 200 ms. The results showed that GOOSE messages had slightly longer transmission time values than dedicated messages. The probability of the values of the transmission delay greater than 8 ms is the same – zero, which is the most important fact (Figure 5). Generally, the variation of the standard deviation can be considered negligible for any type of message with which it was tested.

		TRANSMISSION TIME [ms]				
TYPE	SWITCHES	MAX	AVERAGE	MIN	STDEV	NUMBER OF COMMANDS
GOOSE	no	7.40	4.17	3.96	0.0730	10 000
	yes	6.16	4.22	4.02	0.0691	10 000
DEDICATED	no	7.59	3.70	3.51	0.0908	10 000
	yes	7.29	3.74	3.53	0.0942	10 000
PING	no	4.07	3.82	3.65	0.0666	10 000
	yes	4.08	3.86	3.67	0.0687	10 000

		NUMBER OF COMMANDS				
TYPE	SWITCHES	< 4 ms	4-5 ms	5-8 ms	> 8 ms	SUM
GOOSE	no	22	9 976	2	0	10 000
	yes	0	9 998	2	0	10 000
DEDICATED	no	9 991	3	6	0	10 000
	yes	9 986	7	7	0	10 000
PING	no	9 999	1	0	0	10 000
	yes	9 875	125	0	0	10 000

		PROBABILITY			
TYPE	SWITCHES	< 4 ms	4-5 ms	5-8 ms	> 8 ms
GOOSE	no	2.200E-3	9.976E-1	2.000E-4	0
	yes	0	9.998E-1	2.000E-4	0
DEDICATED	no	9.991E-1	3.000E-4	6.000E-4	0
	yes	9.986E-1	7.000E-4	7.000E-4	0
PING	no	9.999E-1	1.000E-4	0	0
	yes	9.875E-1	1.250E-2	0	0

Table 4: Transmission delay measurements for all three types of messages and for network configurations with and without switches

It can be calculated that the transmission time for the message processing in the switches is approximately $T_{SW} \approx 20$ µs. Processing times in the terminals are approximately 150 µs and $T_{PROC} + T_{SW} << 1$ ms. Most of the transmission time is through the SDH equipment and is approximately 3 - 3.5 ms.

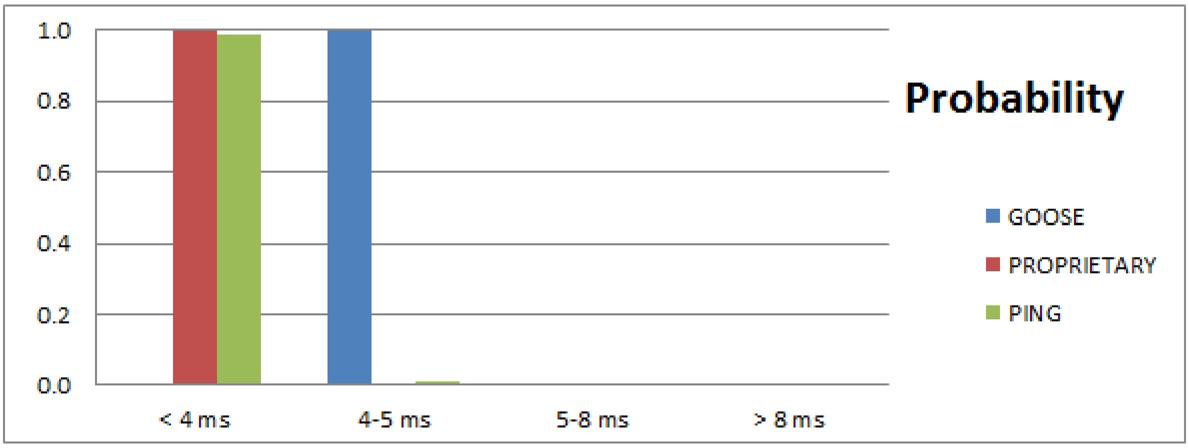

Figure 5 – Graphical representation of the probability of certain transmission delay values for all three types of commands obtained from the results shown in Table 4

4. Conclusion

After reviewing the JP EMS telecommunication network, several solutions for the alternative route of the teleprotection commands were taken into consideration. When it comes to the choice of the interface, we decided to use Ethernet interface for several reasons. This solution does not require an upgrade of existing telecommunication equipment in the substations. Packet networks are increasingly used in substations, so the coexistence of the packet and the SDH network is utilised in this way. Also the conversion of the interface in order to use packet network is not needed. It turned out that acceptable implementation is the transmission of the teleprotection signals using Ethernet over SDH, in the configuration where the teleprotection equipment is connected in the VLAN network. High performance of the teleprotection system (high dependability, security, transmission time, in accordance with the IEC 60834-1) was satisfied. Test results had shown that regardless of the message type, the maximum time for the transmission of the teleprotection commands in the test configuration was significantly below the limit of the 10 ms. The probability that the transmission time is greater than 5 ms was less than 10^{-5} for dedicated messages, and less than 10^{-6} for GOOSE messages. The dependability and the security of the commands transmission was completely satisfied.

BIBLIOGRAPHY

[1] "IEC 60834-1, Teleprotection Equipment of Power Systems – Performance and Testing.Part 1: Command Systems". International Electrotechnical Commission, October 1999.

[2] Skendzic, V.; Moore, R., "Extending the Substation LAN Beyond Substation Boundaries: Current Capabilities and Potential New Protection Applications of Wide-Area Ethernet," in *Power Systems Conference and Exposition, 2006. PSCE '06. 2006 IEEE PES* , vol., no., pp.641-649, Oct. 29 2006-Nov. 1 2006

[3] Edmund O. Schweitzer, David Whitehead, Ken Fodero, Paul Robertson, "Merging SONET and Ethernet Communications For Power System Applications"**,** SEL Journal of Reliable Power, Volume 3, Number 2, August 2012

[4] "The Use of Ethernet Technology in the Power Utility Environment", Technical Brochure 460 WG D2.23,April 2011

[5] "Network Migration for Utilities – Teleprotection Over Packet", RAD DATA Communications Ltd 2011

[6] C. Kriger, S. Behardien, J.Retonda-Modiya, "A Detailed Analysis of the Goose Message Structure in an IEC61850 Standard-Based Substation Automation System", INT. J. COMPUT. COMMUN.,8(5): October 2013

[7] Garry W. Scheer, Darold A. Woodward, "Speed and Reliability of Ethernet Networks for Teleprotection and Control",3rd Annual Western Power Delivery Automation Conference, Spokane, Washington, April 10-12 2001.