Fusion Networking for IEC 61850 Inter Substation Communication: Use Case Applications

Charles M. Adrah, Steinar Bjørnstad, and Øivind Kure
NTNU, Trondheim N-7491, Norway
Email: {charles.adrah; steinar.bjornstad; okure}@ntnu.no

Abstract —In this paper, Fusion networking technology is proposed as a solution for transporting time critical traffic in wide area network power system protection applications among utility substations, to attain deterministic low delay, zero packet loss and ultra-low packet delay variation. Use case applications are explained for communication between two substations and more than two substations using the Fusion networking technology. In addition, the requirements for inter substation communications are presented with focus on the IEC 61850 protocols of Generic Object Oriented Substation Event (GOOSE) and Sampled Values (SMV) and their adaptability to the traffic classes of guaranteed service transport (GST) and statistically multiplexed (SM) in Fusion networking technology.

Index Terms—Communication, power systems protection, IEC 61850, Hybrid networks, circuit-switched, packet-switched

I. Introduction

In recent years, traditional relay protection devices are being replaced with digital relays called Intelligent Electronic Devices (IEDs) in the substations. The IEDs are built on advanced communication technologies to develop communication-assisted protection schemes within the smart grid context. The IEC 61850 [1] is the resultant standardization efforts in substation automation and to address the issues in communication for protection purposes.

The scope of IEC 61850 was originally specified for communication within the substation. It includes two real-time, peer-to-peer communications protocols that are designed particularly for protection applications: Generic Object Oriented Substation Event (GOOSE) messages and Sampled Values (SV) messages [2]. GOOSE and SV messages are link layer protocols that use a publisher/subscriber architecture. This multicast structure works by sending to the multiple subscribed nodes fast and reliable messages.

GOOSE is event driven and supports the point-to-point communication among multiple nodes. The high speed and reliability requirements makes it impractical to use confirmation services in its protocol. GOOSE solves this with a pragmatic approach by assuming subscribers did not receive the message and hence retransmit quickly notwithstanding the reality. This retransmission mechanism also increases the dependability of the protocol. SV is not event driven but sampled whereby configurable datasets are transmitted on a multicast basis from a publisher to multiple subscribers. Although the initial scope of IEC 61850 was within the substation, it is now seen as the future for digital substation as well as inter-substation automation. IEC 61850 90-1 [3] has defined specifications for communication between substations.

Furthermore, IEC 61850 is deployed with Ethernet technology. IEEE 802.1Q [4] specifies functions of Virtual LAN tagging of Ethernet packets and the methods used by network switches to handle packets such that GOOSE and SV messages flooding the wide area networks can be avoided. To lower the latencies of protection application messages which are mostly higher priority traffic, priority scheduling in addition to techniques of Quality of Service (QoS) prioritization are recommended for communication between substations. However, these techniques do not provide hard QoS of a dedicated circuit, e.g. like a dedicated wavelength light-path in an optical wavelength routed optical network [5].

When transporting protection application messages across two or more substations, over provisioning of bandwidth is one method to lower delay. Transporting other kinds of traffic such as IP-telephony, video, metering, Supervisory Control and Data Acquisition (SCADA) will lead to demand for increased bandwidth which presents challenges in cost-efficiency. Maximizing the bandwidth utilization while maintaining the strict QoS requirements for protection applications messages therefore provides a motivation in improving the network throughput in addition to reducing the cost per bit for utilities.

Fusion networking technology is an implementation of Integrated Hybrid Optical Networks (IHONs) [6]. This seeks to combine the circuit and packet networks in the same wavelength to achieve circuit quality transport of high priority services referred to as guaranteed service transport (GST) streams, and statistical multiplexing of best effort services referred to as Statistical Multiplex (SM) streams enabling the high throughput efficiency of packet networks. In [7], an experiment using two Ethernet based Fusion nodes with dedicated interface support for both high priority GST and lower priority SM streams was performed. It was demonstrated that GST enables connections with circuit-switched QoS of no

Manuscript received May 20, 2017; revised September 25, 2017.
Corresponding author email: charles.adrah@ntnu.no.
doi:10.12720/jcm.12.9.510-517

©2017 Journal of Communications

packet loss and ultra-low Packet Delay Variation (PDV) with the unutilized capacity being filled through statistical multiplexing of streams from lower priority SM class.

In this paper, Fusion networking technology is proposed as a solution to transport time critical power system protection data with hard QoS requirements mixed with other types of traffic that are typically running between substations. In addition, we propose an architecture of mixed traffic priorities on the aggregation and deaggreation interfaces, and estimate and analyze the performance on the time critical protection data.

The rest of the paper is structured as follows; Section II summarizes the requirements in the standardization efforts for inter substation communication specified in [3]. Section III introduces the Fusion networking concept. In section IV, scenarios are presented to show the application of fusion nodes in transporting protection application messages in inter substation communication and in addition, how protection messages can be classified. Section V explains the principles of the combining mixed traffic on Fusion nodes and we evaluate performance of a chosen scenario and finally conclusions are presented in section VI.

II. Requirements For Substation-To-Substation Communication

A. Background

The need to exchange standardized information directly between substations for power system protection purposes is increasing. IEC 61850 protocol originally made for exchange of information among devices within a substation provides features which can be used to extend beyond substations. It is expected that IEC 61850 will become the bedrock for a globally standardized utility communication network.

The different kinds of protection applications impose different communication constraints such as communication channel failure, timing, propagation delay, reliability, redundancy, data synchronization (e.g. less than 0.1ms), frequency of data exchange, data bandwidth to transmit three-phase current/voltage data, and data size.

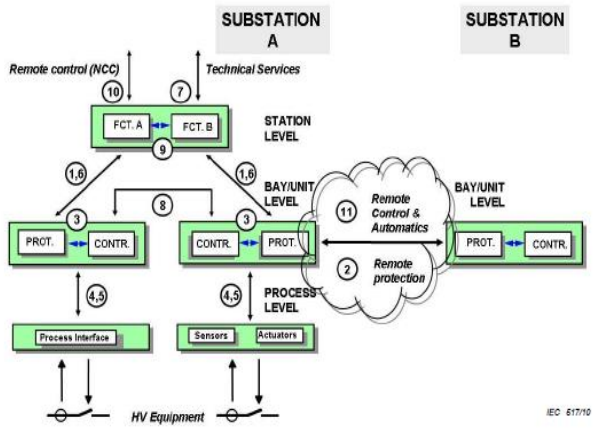

Fig. 1. Logical allocation of functions and interfaces [3].

A substation-to-substation (SS-SS) communication refers to functions in Substation Automation Systems (SASs) that are either distributed between two substations or functions in one substation that require some information from another substation. Fig. 1 shows the logical allocation of functions and interfaces in an SAS. Interface 2 and 11 are the focus of SS-SS communication. Protection related functions are defined on interface 2 and includes analogue data for line differential protection applications as well as digital data for line distance protection applications. The control related functions are defined on interface 11 and are mainly digital data for interlocking functions or inter-substation communication data. Both interfaces are expected to be dedicated communication paths for their respective functions.

B. Message Types and other Performance Requirements

Due to the different requirements of the functions in and between substations, IEC 61850 message types are divided into Message Performance Classes (MPC). Table I shows the message performance classification of different kinds of traffic that can exist between substations. MPC Type 1 are the high-speed messages that typically contain simple binary information of a short or simple message such as "Trip", "Reclose order", "Start". These message types are mission critical for the performance of the supported application function hence the receiving IED needs to act immediately upon receipt of such message. An MPC specialized Type 1A is mostly used to send "Trip" binary signal which is the most important fast binary message.

Table I: IEC 61850 Message Types [3].

Traffic (By protocol)	Type	Applications	Performance Class	Transfer times
GOOSE	1A	Fast messages "Trip"	P1	10 *ms*
			P2/P3	3 *ms*
	1B	Other fast messages	P1	100 *ms*
		Normal messages	P2/P3	20 *ms*
SV	4	Raw Data	P1	10 *ms*
			P2/P3	3 *ms*
Others (e.g. TCP/IP)	2	Medium speed		100 *ms*
	3	Low speed		500 *ms*
	6	File transfers		1000 *ms*

The transfer times for Type 1A varies depending on supported application function between 3 *ms* to an upper limit of 10 *ms*. Type 1B is another MPC that is for both fast and normal messages relevant for automation functions but with less stringent requirements compared to Type 1A. For this MPC, transfer time requirements are between 20 *ms* to 100ms. MPC Type 4 which are raw data messages including SV messages or phasors also have stringent transfer times between 3 *ms* and 10 *ms*.

MPC Types 2, 3 and 6 for medium speed, low speed and file transfers can be messages such as commands and

reports like station level database update, update of the single line display at a screen, update of alarm and event lists. Transfer times for these kinds of messages are between the bounds of 100 *ms* to 1000 *ms*.

C. Integrity, Security and Dependability

The communication link between SS-SS has high requirements on bit-error-ratio and signal-to-noise ratio. Three integrity classes have been specified for different types of messages in the standard IEC 60870 [8]. Protection safety related messages which are the most time critical messages, i.e. MPC type 1A, have the highest integrity class 3 prescribed. All other messages can be transmitted with lower data integrity in a class 2.

Security and dependability requirements are very high as well. Security "S", against unwanted commands, i.e. unwanted trips of protection if they are not requested by the protection scheme in the actual situation. Hence given P_{uc} as the probability for unwanted commands, then Security, $S = 1 - P_{uc}$. It is recommended that protection application in the tripping IED should have $P_{uc} < 10^{-8}$, and blocking schemes $P_{uc} < 10^{-4}$.

Dependability "D" means the dependability against "missing commands" i.e. for protection missing trips if these are requested from the protection scheme in the actual situation. Given probability for missing commands as P_{mc}, $D = 1 - P_{mc}$. It is prescribed a $P_{mc} < 10^{-4}$ within a 10ms duration. Table II lists the security, dependability and bit-error-ratio metrics recommended for GOOSE and SV traffic types.

TABLE II: SECURITY, DEPENDABILITY AND BER METRICS

Traffic Type	Security	Dependability	Error rate (BER)
GOOSE	$<10^{-8}$	$<10^{-4}$	$<10^{-6}$
SV	$<10^{-8}$	$<10^{-4}$	$<10^{-6}$ to $<10^{-8}$

D. Ethernet Communication for IEC 61850

Tele protection systems rely on telecommunication channels that provide a deterministic signal transmission delay and have a constant bandwidth or bit rate over time, without any delay variation [9]. Legacy technologies of SONET/SDH and PDH have been used by utilities to build wide-area communications networks for inter substation communication. Ethernet technology with its statistical multiplexing transmission mechanism and use of bandwidth-on-demand or "best effort" techniques have brought challenges to the performance requirements that protection applications must conform. Statistical multiplexing, which offers the main benefit of exploiting the network capacity efficiently, also imposes a crucial drawback: Ethernet networks are high bandwidth-delay product networks. Delay and packet delay variations (PDV) are normally imposed on the traffic because buffering is needed for handling the statistical variations in the traffic pattern. While the high-throughput is welcomed by bandwidth hungry applications and data centric technologies, the delay and PDV characteristic is not well- fitted for the transport of time-sensitive information [5].

IEC 61850 is deployed on an Ethernet Local Area Network (LAN). Traffic dependability problems emanate from congestion that arise from competing Ethernet packets for a network path. A solution for this is to use several priority-dependent queues at each egress port to lower the latencies of the higher-priority traffic. Another solution to address the security and dependability issues using Ethernet, is to avoid GOOSE packets flooding the wide area networks. This is achieved by configuring flow restrictions using Virtual LANs (VLANs). VLAN identifiers (VIDs) are configured between all IEDs needing certain messages or belonging to a certain application working with a specific kind of message hence using different VLANs for a substation internal traffic and substation-to-substation inter traffic.

[3] lists recommendations for using Ethernet for communication between substations as follows:

- If the Ethernet telecommunication network is outside the utility's "security perimeter", the Ethernet links through such equipment should be secured through technology such as "L2TP" (layer 2 tunneling protocol) to create a "VPN".
- Ethernet should recover (restore traffic) from a fiber failure within 10ms, unless dual-port IEC 61850 IEDs are used with physically separate paths.
- All the network switches "drop" ports connected to IEC 61850s should be configured for memberships only in the VLANs supported by the connected IEDs.
- All network switches "drop" ports shall be configured to block ingress traffic with VIDs for the critical VLANs.
- Probability of a GOOSE packet taking more than 10ms to traverse the network should be constrained to less than 10^{-4} by limiting the number of switches on the longest path and limiting the traffic loading.

III. FUSION NETWORKING CONCEPT

Fusion is a technology solving the problem of providing packet networks with the advantages of circuit switched networks [10]. The technology is built on the architecture of integrated hybrid optical Networks (IHON).

A. Introducing Integrated Hybrid Optical Networks

IHON is a concept that attempts to bring packet and circuit network domains together. IHON supports two main classes of service: the circuit- service class referred to as guaranteed service transport (GST) offering hard quality of service (QoS) and packet-service class referred to as statistically multiplexed (SM) with lower QoS [11]. The two classes of service share the same physical wavelength resource. The GST traffic offers hard QoS including: zero packet jitter, zero packet loss, and low deterministic delay while the SM traffic is statistically multiplexed, accepting lower priority QoS.

Provisioning circuits of wavelength granularity leads to the well-known issue of low resource utilization in optical circuit switching and wavelength routed optical networks (WRONs) [7] because statistical multiplexing is not available. Therefore, to optimize the wavelength capacity, IHON uses the established GST wavelength to transport SM traffic whenever there is an idle time gap between GST packets. The GST traffic is not affected by this technique since the SM traffic is only added in between vacant gaps not used by the GST packets.

B. Introducing Fusion Node

The TransPacket H1 prototype node [12], is a Fusion networking add-drop Ethernet muxponder which enables Ethernet packet transport of the two types of traffic classes; GST with circuit QoS and the statistically multiplexed SM class for high wavelength capacity utilization. TransPacket H1 10 Gigabit Ethernet (GE) add/drop Fusion muxponder introduces high density 10x1GE channels with transparent Ethernet transport, ultralow delay and zero packet loss. While the processing in the node follows the Fusion principle, all data signals into and out of the node is Ethernet compliant.

IV. SS-SS Communication Usng Fusion

In this section, we show the application of Fusion nodes in a first scenario as a direct link between two substations. We then show a second scenario involving more than two substations. We also show how traffic exchanged between substations can be classified using the Fusion traffic classes.

A. Fusion Node as Direct Link betweeen Two Substations

In the first scenario shown in Fig. 2, a Wide Area Network (WAN) communication setup between two substations is established. We assume that there is a direct Ethernet connection between the two substations hence the substations use the tunneling approached described in [3] for SS-SS communication. Tunneling is a method that connects multiple substation networks by allowing “direct access” to functions in a remote station. The station network becomes extended to include the remote station. Higher bandwidth is normally required to achieve low delay. Even for low data volume of GOOSE traffic, a higher bandwidth of the communication mechanism correlates with lower delay [3]. Tunnels are normally established by means of network switches or routers.

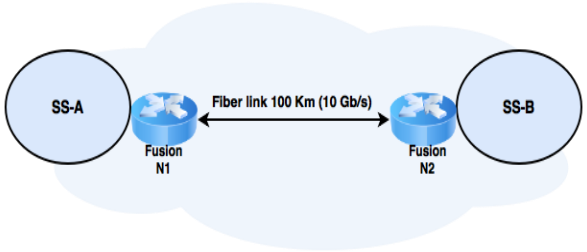

Fig. 2. SS-to-SS communication structure with fusion nodes

In each substation, we consider a Fusion node connected through a fiber link with a 10 Gb/s Ethernet wavelength. The 10Gb/s link is configured as the trunk port that connects the two substations. It is assumed that messages enter input ports of 1 Gb/s on each node and are then aggregated into the 10 Gb/s Ethernet output link. The Fusion node acts as a Substation Edge Node (SEN) coupling the WAN connection between the two substations. The SEN aggregates different traffic streams from each substation.

B. Three or More SS - Optical Ring Add/Drop

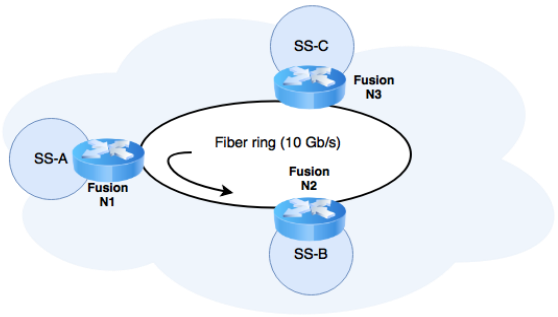

Fig. 3. SS-to-SS communication structure with 3 substations

In our second scenario, we extend the setup shown in Fig. 2 with an additional substation. Using the Fusion nodes, a ring topology is implemented such that the Fusion nodes acts as add/drop multiplexers, with large aggregate capacity suitable for a wide area network architecture. Using Fusion nodes for add/drop, aggregation rings with low delay and ultra-low PDV can be implemented, avoiding unnecessary routing or switching at intermediate nodes. In Fig. 3, the substations A, B, and C are connected by a 10 Gb/s fiber ring. Traffic directed from SS-A to SS-C will pass through an intermediate node, N2 at SS-B. N2 acting as a bypass node. Directed traffic to SS-B will be dropped at N2. In addition, traffic from SS-B can be added at N2, onto the 10 Gb/s aggregate link and routed to SS-C or SS-A based on the protection application requirements.

C. Use Case 1 – Protection vs Non-Protection Traffic.

TABLE III: MAPPING BETWEEN SS-SS TRAFFIC AND IHON TRAFFIC

SS-SS traffic types	IHON traffic types
Protection traffic - GOOSE (Type 1A 1B – fast, normal) and SV Type 4	GST
Non-protection traffic - Other traffic (TCP/IP)	SM

In the first use case, two types of traffic between substations are defined. All the protection traffic i.e. GOOSE and SV, as one type of traffic. The second type of traffic are non-protection traffic which may be client-server communications running on TCP/IP. This is the simplest case of traffic segregation where all data for protection applications between the two substations are considered to offer time critical services. The protection

traffic entering the Fusion node will be classified as GST streams while the non-protection traffic will be classified as SM streams. A mapping of the defined traffic types between the substations and supported classes by Fusion nodes is shown in Table III.

D. Use Case 2 – Clasification by Message Performance Classes

I the second use case, we consider the different IEC 61850 message performance classes for the protection traffic between substations shown in Table I. The messages are marked as either GST or SM streams on arrival at the Fusion node. The reason for classification of traffic types is based on the transfer time requirements for such message types. Table IV shows a mapping of the classes of services supported by the Fusion nodes and the IEC 61850 traffic types defined between substations.

The GOOSE Type 1A and Type 4 SV messages are classified as GST when entering the port of the Fusion node. These messages are the most time critical of the protection traffic, hence are marked as such. The GOOSE Type 1B (fast and normal), control messages or other traffic types running on TCP/IP that are exchanged between the two substations are classified as SM. We consider these traffic types to be less demanding on transfer time requirements for our use case, hence are marked as such.

TABLE IV: MAPPING BETWEEN IEC 61850 MESSAGE TYPES AND IHON TRAFFIC TYPES

SS-SS traffic types	IHON traffic types
GOOSE Type 1A	GST
SV Type 4	GST
GOOSE Type 1B - fast	SM
GOOSE Type 1B - normal	SM
Other traffic (TCP/IP)	SM

In Fusion, the high priority traffic (GST) is given a fixed delay through the node corresponding to the duration of a maximum sized SM frame. The purpose of the delay is the ability of detecting gaps in the GST traffic sufficiently large to insert a maximum sized SM packet. In this configuration, the fixed delay δ is set to 1.21μs to accommodate an SM maximum-length lower priority packet of 1518 bytes. The aim is to show that we can achieve aggregation of GST connections, transport and deaggregation with circuit QoS: low deterministic delay, ultralow PDV, and no packet loss.

V. COMBINING TRAFAFIC PRIORITIES ON INTERFACES, EVALUATION AND DISCUSSION

In this section, we explain the principles of the proposed combination of mixed traffic classes on aggregate nodes and evaluate performance effects on the GST traffic class. Furthermore, we discuss the effects the classification choices have on the GST streams and SM performance.

A. Combining Traffic Priorities on Interfaces

In the field trial setup in [7], the experiment considered nodes of dedicated traffic for the different traffic classes of GST and SM streams as shown in Fig. 4.

In our proposed architecture, traffic arriving and departing a node could be from a mix of different priority classes. Fig. 5 shows the mechanism of combining traffic priorities at the interfaces of the nodes. Suppose we have two 1 Gb/s ports of N1, with mix traffic priorities arriving on their ports, i.e. GST1/SM1 on *ge0* and GST2/SM2 on *ge1*, for the aggregation process into the 10GE wavelength channel. After deaggregation by N2, it is expected a different mix of traffic priorities at the corresponding ports, i.e. GST2/SM1 on *ge0* and GST1/SM2 on *ge1*.

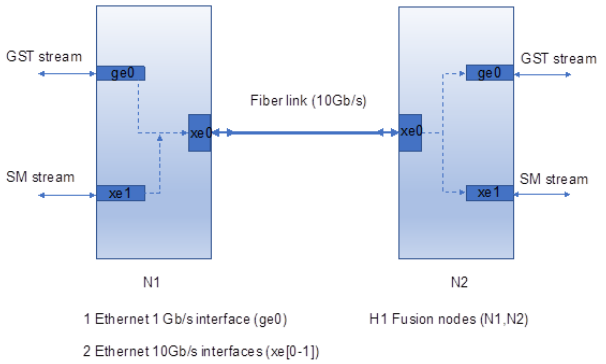

Fig. 4. Dedicated interface for traffic priorities [7].

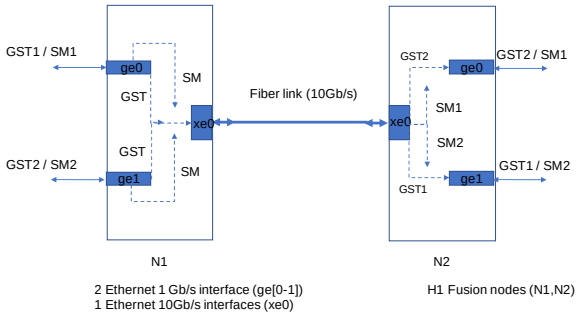

Fig. 5. Setup with mixed traffic at aggregation and deaggregation interfaces.

The aggregation scheme in N1 for the proposed architecture will behave similarly as shown in [7]. The SM streams from ports *ge0* and *ge1* are filtered into internal buffers from where they are scheduled only if they fit into the available of unutilized GST capacity. The GST packets received at the 10GE input interface pass through to the other 10GE output interface with absolute priority and light processing in the node [7].

In the deaggregation process, a mix of traffic priorities are expected on the interfaces of *ge0* and *ge1*. An additional delay will be incurred on the GST packets when combining with SM traffic on 1GE output, for achieving zero PDV from contending packets. The delay is fixed and influenced by the maximum packet length of the SM packet.

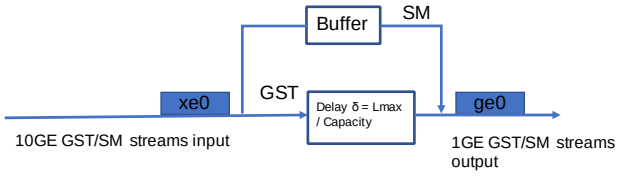

Fig. 6. Deaggregation from 10Gb/s to 1Gb/s.

In addition, since the deaggregation is from a 10 Gb/s port interface to a 1 Gb/S interface ports, it will take 10 times slower to clock out a packet on the 1 Gb/s ports. Fig. 6 shows a schematic of the deaggregation process and mechanism of combining mixed traffic on the 1Gb/s interface.

B. Performance Analysis on GST Traffic

To estimate the delay budget for the scenario in Fig. 2, we consider the following equation:

$$C_D = N\ x\ (N_D + T_{ProD})$$

C_D, is the delay budget. N, is the number of nodes. N_D, is the nodal delays which consists of transmission delay, processing delays and queuing delays. T_{ProD}, is the propagation delay.

The propagation delay for a fiber link is estimated to be *5us* per km [13]. We consider the SS-SS link in Fig. 2 to be of a transmission grid spanning 100 Km. A fixed delay δ is incurred by the GST packets before accessing the 10 Gb/s and 1 Gb/s output channels in both the aggregation and deaggregation process. This fixed delay is determined by the channel capacity C and the maximum length SM packet L_{max}, i.e. $\delta = L_{max} / C$. Assuming the maximum SM packet size of 1518 bytes, the GST marked packets will experience a fixed delay of 1.21 *us* during the aggregation process into the 10 Gb/s channel port and add fixed delay of 12.1 *us* due to combining traffic priorities on the 1 Gb/s channel ports of N2. The total end-to-end fixed delay for GST streams will then be 13.31 *us.*

The rest of the delay budget is constituted by propagation delay of 500 *us* (100 *Km* x 5 *us/Km*) plus some nodal processing delays. In the field trial demonstrated in [7], the end-to-end nodal processing delay recorded was 43.3 *us.* The total delay budget using Fusion with the proposed mix of traffic on interfaces will be:

$$C_D = (13.31 + 43.3 + 500)\ us = 556.6\ us$$

IEC 61850-90-1 [3] states that the requirements for the transfer time i.e. the communication performance are basically the same in one bay, between bays and between substations. Therefore, the same classification scheme shall be used for all links compliant with IEC 61850. For digital communication beyond the substation, transfer times ≤ 10 *ms* may be accepted according to the message performance class TR2 [14]. In addition, other less demanding performance classes may be acceptable if the protection application function will work with these transfer times. Hence from the delay budget of 556.6 *us* estimated when using Fusion, it can be a suitable solution in the transport of protection traffic between substations.

It was also shown in [7] that, the average delay of the GST streams will be deterministic independent of the amount of GST or SM load. The principle allows packet delay variation of the GST streams to be zero, but some PDV is added due to imperfect implementation issues in the node. The peak-to-peak PDV for GST in the experiment of [7] was however shown to have an average of 320 *ns.*

C. Discussions

The estimated delay budget obtained for the GST traffic will be the same for the traffic classification use cases explained in Sec. IV, C and D. Marking all protection traffic as GST and non-protection traffic as SM in one case versus only some message performance class as GST will not affect the delay performance of the GST traffic. This is because the only influence the Fusion node has on the GST circuit stream is that bypassing packets are given a fixed delay δ corresponding to the transmission time of the maximum length SM Ethernet packet [5].

Deciding on how to classify substation traffic either as GST or SM stream depends on what data is viewed as performing time-critical service. In addition, it depends on the total amount of data exchanged between the substations i.e. total network load. If a higher portion of total network load between the substations are classified as time-critical and hence marked as GST streams, this will have a corresponding effect on the offered load of SM traffic. This is because there will be a higher bandwidth utilization by the GST traffic which could lead to lower offered load of SM streams. Therefore, it is important to consider this before marking streams as either GST or SM.

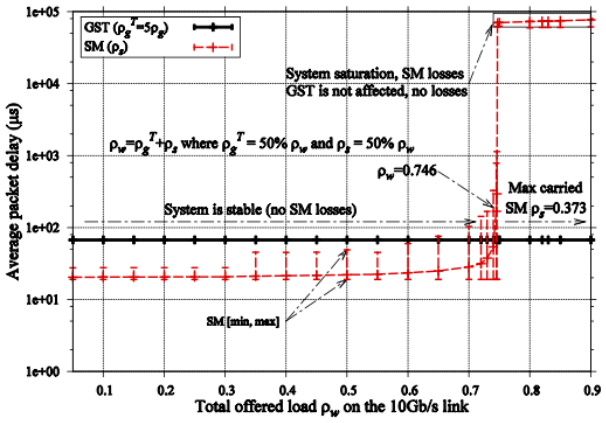

Fig. 7. Packet delays as function of the normalized offered load on the 10 Gb/s Ethernet wavelength [7].

In [7], it was shown that when the total offered load ρ_W is equally offered by the GST aggregate and SM such that $\rho_T = \rho_G + \rho_S$, $\rho_G = \rho$, the system goes into saturation at a point where SM traffic starts experiencing packet delays and losses. Illustrated in Fig. 7 are end-to-end delay results for GST and SM traffic. The minimum and

maximum boundary, plus their averages, SM delay values are plotted to show how the increase in GST load influences the SM performance. It is seen that as both GST and SM loads increase, the GST average delay is constant. At 0.75 of ρ_T with 0.38 GST, the system saturates and the end-to-end delay of the SM traffic increases. It was also observed SM traffic experienced congestion and packet losses.

VI. Conclusion

This paper presents the requirements in the IEC 61850 90-1 standard for communication between substations and proposes the use of Fusion networking technology based on the IHON architecture, for transporting time critical power system protection traffic together with other types of traffic between substations. The application of Fusion nodes in a wide area network setting was demonstrated in a first scenario involving two substations and a second scenario using more than two substations. In addition, two use cases showed how protection application traffic can be classified per the Fusion traffic classes. In one use case, classification of messages as GST or SM are based on the message performance classes of IEC 61850. GOOSE Type 1A and Type 4 SV messages are marked as GST streams which maintain the stream characteristic with zero packet loss, low delay and ultralow PDV. This provides circuit-switching properties with a low deterministic delay. The other IEC 61850 message types, i.e. Type 1B (fast and normal) plus traffic types running on TCP/IP which we consider less time critical are marked as SM streams and are statistically multiplex on to the same wavelength. This enables an efficient utilization of the wavelength.

Furthermore, we proposed an architecture of mixed traffic priorities on the aggregation interfaces and estimated the delay values incurred on GST streams in combining different traffic priorities on interfaces of both arrival and departure nodes. The delay is different for combined GST and SM within one interface versus dedicated GST and SM on two different interfaces, i.e. when traffic priorities are combined within the same interface there is an additional delay incurred due to the combination process. In a network architecture scenario including 100 km transmission distance it was found that a delay of 556.6 *us* for the GST traffic, significantly lower than the acceptable transfer time of maximum 10 *ms*, can be reached.

Applying the Fusion concept is therefore found to be a feasible solution for transport of time critical data across substations with guaranteed QoS of low deterministic delay and ultra-low PDV. In future, we intend to investigate the effect on offered load of SM traffic due to the combined traffic priorities on the proposed aggregation interface.

References

[1] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in *Proc. IEEE PES Power Systems Conference and Exposition*, Atlanta, GA, 2006, pp. 623-630.

[2] I. Xyngi and M. Popov, "IEC61850 overview - where protection meets communication," in *Proc. 10th IET International Conference on Developments in Power System Protection*. *Managing the Change*, Manchester, 2010, pp. 1-5.

[3] IEC/TR 61850-90-1, Communication Networks and Systems for Power Utility Automation – Part 90-1: Use of IEC 61850 for the Communication between Substation.

[4] IEEE Standard for Local and metropolitan area networks, Virtual Bridged Local Area Networks, IEEE 802.1Q-2005, December 2005.

[5] R. Veisllari, S. Bjornstad, K. Bozorgebrahimi, and N. Stol, "Providing ethernet circuit quality of service and high bandwidth efficiency through fusion networking," *Norsk Informatikkonferanse NIK*, 2013.

[6] S. Bjornstad, D. R. Hjelme, and N. Stol, "A packet switched hybrid optical network with service guarantees," *IEEE J. Sel. Areas Commun*., vol. 24, no. 8, pp. 97–107, 2006.

[7] R. Veisllari, S. Bjornstad, J. P. Braute, K. Bozorgebrahimi and C. Raffaelli, "Field-trial demonstration of cost efficient sub-wavelength service through integrated packet/circuit hybrid network [invited]," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 7, no. 3, pp. A379-A387, March 2015.

[8] IEC 60870-4, Telecontrol Equipment and Systems, Part 4: Performance Requirements, 1990.

[9] Advanced Power Grid Protection Next Generation Tele Protection Solutions. [Online]. Available: http://studylib.net/doc/8743237/advanced-power-grid-protection

[10] Fusion networking explained. TransPacket White Paper [Online]. Available: http://subsystems.transpacket.com/wpcontent/uploads/2016/09/White_paper_fusion_intro_12062012.pdf

[11] R. Veisllari, N. Stol, S. Bjornstad, and C. Raffaelli, "Scalability analysis of SDN-controlled optical ring MAN with hybrid traffic," in *Proc. IEEE International Conference on Communications*, Sydney, NSW, 2014, pp. 3283-3288.

[12] TRANSPACKET H1: A fusion networking add-drop mux-ponder. TransPacket White Paper [Online]. Available: http://www.transpacket.com/fusionh1/fusion‐ethernet‐h1/

[13] Application Considerations of IEC 61850/UCA 2 for Substation Ethernet Local Area Network Communication for Protection and Control, IEEE PSRC H6: SPECIAL REPORT.

[14] C. H. R. de Oliveira and A. P. Bowen, "Iec 61850 goose message over wan," in *Proc. International Conference on Wireless Networks*, 2012.

Charles M. Adrah was born in Ho, Ghana, in 1986. He received the B.S. degree from the Kwame Nkrumah University of Science and Technology (KNUST), Ghana, in 2008, in Electrical Engineering, and the M.S. degree from the Norwegian University of Science and Technology (NTNU), Trondheim, in 2012, in Telematics. He is currently pursuing the Ph.D. degree with the Department of Information Security and Communication Technology, NTNU. His research interests include smart grid communication networks, quality of service and performance evaluation.

Steinar Bjørnstad is a professor with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim. He is also with TransPacket AS, Oslo 0277, Norway. His research interests include optical networks, performance evaluation, QoS, wireless networks.

Øivind Kure is a professor with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim. He got his Ph.D. from the University of California, Berkeley in 1988. His current research interest is in various aspects of QoS performance analysis, multicast protocols, and ad hoc networks.