Validating Secure and Reliable IP/MPLS Communications for Current Differential Protection

S.M. Blair*, C.D. Booth*, B. De Valck†, D. Verhulst†, C. Kirasack†, K.Y. Wong†, S. Lakshminarayanan†

**University of Strathclyde, UK, steven.m.blair@strath.ac.uk*
†Alcatel-Lucent, Belgium/Canada, bram.de_valck@alcatel-lucent.com

Keywords: Communications, current differential protection, encryption, IEC 61850, IEEE C37.94, teleprotection.

Abstract

Current differential protection has stringent real-time communications requirements and it is critical that protection traffic is transmitted securely, i.e., by using appropriate data authentication and encryption methods. This paper demonstrates that real-time encryption of protection traffic in IP/MPLS-based communications networks is possible with negligible impact on performance and system operation. It is also shown how the impact of jitter and asymmetrical delay in real communications networks can be eliminated. These results will provide confidence to power utilities that modern IP/MPLS infrastructure can securely and reliably cater for even the most demanding applications.

1 Introduction

Current differential protection, often referred to as teleprotection, has stringent real-time communications requirements: low-delay, symmetrical delay, and low jitter. Furthermore, it is critical for system stability that teleprotection traffic is transmitted securely [1], i.e., by using appropriate authentication and data encryption methods.

Conventionally, time-division multiplying (TDM) technologies, such as synchronous digital hierarchy (SDH), have been used by power utilities to provide wide-area communications for teleprotection services. However, a packet-based approach using Internet Protocol/MultiProtocol Label Switching (IP/MPLS) offers increased operational flexibility and efficiency [2], whilst still emulating the benefits of TDM-based services.

This paper demonstrates and analyses two methods for enhancing the delivery of teleprotection functionality in IP/MPLS networks:

1. Real-time encryption of an IP/MPLS-based service which transports teleprotection traffic. The paper analyses the impact of the above methods for both IEEE C37.94 and IEC 61850 – using Sampled Value (SV) and GOOSE protocols – approaches for current differential protection.
2. Compensation for asymmetrical delay (i.e., different communications delays in the "forward" and "reverse" directions) due to unavoidable jitter in packet-switched networks. The paper shows how the impact of asymmetrical delay can be minimised to prevent potential maloperation of teleprotection relays (i.e., false trips) under certain circumstances.

2 Validation Methodology

Figure 1 summarises the real-time, hardware-in-the-loop testing configurations which have been used, and Figure 2

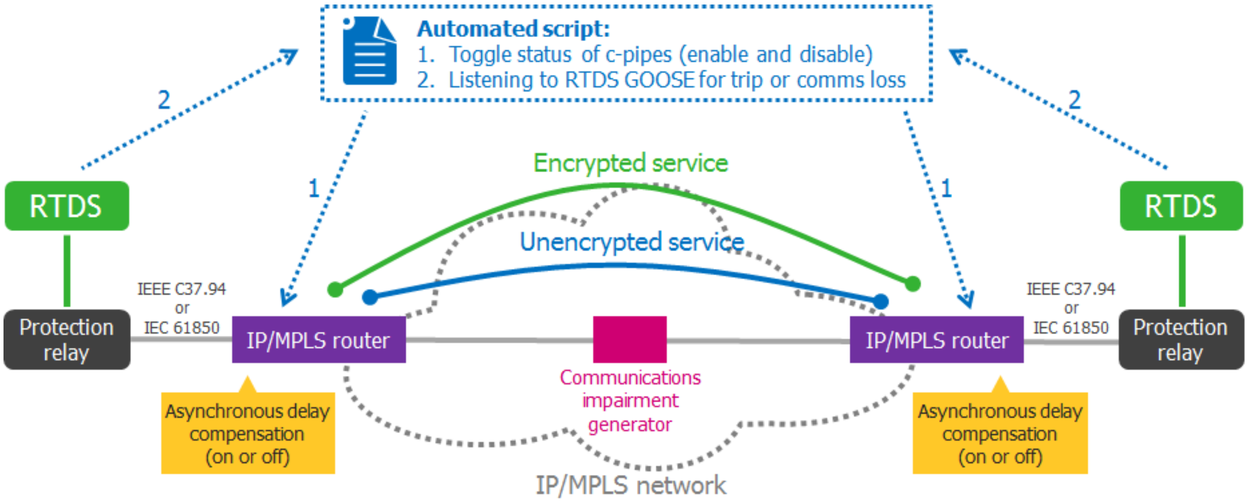

Automated script:
1. Toggle status of c-pipes (enable and disable)
2. Listening to RTDS GOOSE for trip or comms loss
2
2
1
1
Encrypted service
Unencrypted service
RTDS
RTDS
Protection relay
Protection relay
IEEE C37.94 or IEC 61850
IEEE C37.94 or IEC 61850
IP/MPLS router
IP/MPLS router
Communications impairment generator
Asynchronous delay compensation (on or off)
Asynchronous delay compensation (on or off)
IP/MPLS network

Figure 1: Overview of system used for validation

shows the laboratory devices. A two-terminal 400 kV transmission line has been simulated using a Real Time Digital Simulator (RTDS) [3]. The RTDS supplies three-phase current signals to two commercially-available current differential protection relays (Alstom P545). These relays natively communicate using IEEE C37.94 optical interfaces. The IP/MPLS routers (Alcatel-Lucent 7705 Service Aggregation Routers) packetize the IEEE C37.94 data and transport it over an emulated point-to-point connection in the wide-area communications network, as described in detail in [2] and [4].

A script, written in the Python programming language and based on the software reported in [5], has been used to fully automate the testing process. This is essential because multiple test iterations are required due to the stochastic nature of jitter, as described further in Section 4.1. In order to confidently establish whether or not false trips occur for a given scenario, the RTDS sends GOOSE messages containing each relay's trip status (which are obtained from the relays' digital output trip signals). The script is therefore able to both send commands to the IP/MPLS routers to initiate test iterations and to record any resulting GOOSE trip messages from the RTDS.

A key component in Figure 1 is the "communications impairment generator" which must inject precise and repeatable real-time Ethernet traffic delays. This component allows emulation of sub-optimal communications performance, such as asymmetrical delay. Both a commercial device (a Calnex Paragon-X) and a custom embedded platform have been used.

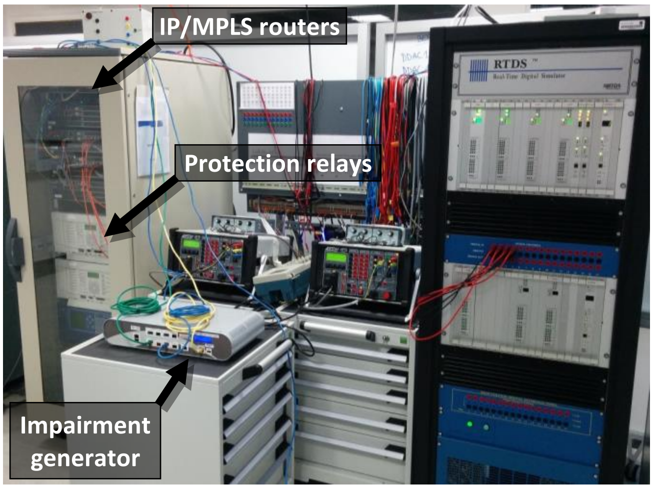


Figure 2: Laboratory testing arrangement

3 Real-Time Encryption

3.1 Impact of Encryption

As implied by Figure 1, the IP/MPLS routers have been configured to create an encrypted service between the end-points in the two (simulated) substations to transport protection traffic. The encryption and decryption is hardware-accelerated and is only performed at the end-points; i.e., the traffic remains encrypted throughout the entire wide-area communications network infrastructure, rather than being re-encrypted at each node. This approach is thereby designed to minimise the real-time latency resulting from encrypting traffic and implements a true end-to-end encrypted transport service.

This approach is known as Network Group Encryption (NGE) and involves encrypting IEEE C37.94 traffic at the MPLS layer. The AES256 algorithm has been used for encryption and HMAC-SHA-512 has been used for authentication [6].

Table 1, with some results from [2] and [4], demonstrates that encryption has negligible impact on protection performance. An additional delay of approximately 20 µs can be measured for the IEEE C37.94 protocol. No other impact on protection functionality was found, i.e., there was no measurable impact on tripping times for simulated short-circuit faults.

		Propagation delay	Typical trip time	Bandwidth required
IEEE C37.94	**No encryption**	1.68 ms	28.4 ms	0.2-2.7 Mbps
	With encryption	1.70 ms	28.4 ms	0.5-5.9 Mbps
IEC 61850	**No encryption**	Not measured	24.9 ms	~5.4 Mbps
	With encryption	Not measured	24.9 ms	~7.0 Mbps

Table 1: Comparison of protection performance with and without encryption

As noted in IEC 61850-90-5 [7] and IEC/TS 62351-6:2007 [8], there are concerns regarding the real-time performance of encrypted communications links for teleprotection functionality. However, as this section has demonstrated, an end-to-end and hardware-accelerated encryption approach avoids these concerns with a negligible performance impact.

The solution adopted by the IP/MPLS routers includes other practical factors such as automated key distribution and ensuring that there is no interruption of protection functionality during key updates [6].

3.2 Relationship to Other Approaches and Standards

The IEC 61850 GOOSE and SV protocols – designed to be used for protection applications – are mapped directly to Layer 2 Ethernet frames. For wide-area communications using these protocols, one of the following approaches must be adopted:

1. Use a gateway device to convert between suitable protocols, as described in IEC 61850-90-1. The use of a gateway is likely to involve a conversion delay and is therefore not suitable for real-time applications such as current differential protection or phasor measurement unit (PMU) data.

2. “Tunnel” the Ethernet traffic using IP and UDP, thereby creating so-called Routable-GOOSE and Routable-SV, as discussed in IEC 61850-90-1 and described in detail in IEC 61850-90-5. This was primarily designed to transport PMU data using the IEC 61850 data model and protocol mappings.
3. Use an “e-pipe” service or a virtual private LAN service (VPLS) over an IP/MPLS-based network. An e-pipe is an Ethernet point-to-point Layer 2 connection, while a VPLS provides a multipoint Layer 2 service to the connected endpoints as if they were connected on the same physical LAN infrastructure. This is the approach described in this paper.

Approaches 2 and 3 are compared in Table 2. The additions to the protocol stack required to achieve Routable-GOOSE and Routable-SV – particularly to cater for authentication and encryption – are relatively complex. Furthermore, the burden is left to each device vendor to implement the protocol stack, without compromising security; protection relay vendors may not conventionally have the required expertise. Conversely, for approach 3, the authentication and encryption functions can be delegated to the IP/MPLS infrastructure: individual wide-area services (whether Ethernet-based, IP-based, or otherwise) can be encrypted if required. Encryption is managed at a level which is not seen by the application (e.g. GOOSE or other traffic) which significantly reduces the complexity for device vendors, system integrators, and utilities. This approach also allows legacy devices to benefit from encryption.

	Approach 2: IEC 61850-90-5	**Approach 3: e-pipe or VPLS over IP/MPLS**
Complex protocol stack implementation required?	Yes, but an open source implementation exists [9]	No, the complexity of the encryption is hidden from users
Each device vendor must implement authentication and encryption software?	Yes	No, this is provided automatically by the communications infrastructure vendor
Supports legacy devices (i.e., non-Ethernet interfaces)?	No	Yes
Hardware-accelerated encryption?	Depends on vendor implementation	Yes

Table 2: Comparison of wide-area communications approaches for protection applications

4 Compensating for Asymmetrical Delay

Jitter is unavoidable in real communications networks, due queuing delays and the use of TDM-based links such as T1/E1. Furthermore, for low-bandwidth links, which is typical at the edge of a communications network for “last-mile” connectivity, greater jitter can be expected. Jitter can result in fluctuating differences between the “forward” and “reverse” delays, i.e., asymmetrical delay.

4.1 Problem Background

The process of transporting a TDM-based teleprotection service over a packet-based network requires that a buffer is used to control the egress of data to the protection relays – to ensure that a consistent stream of data is delivered. However, this buffer must be initialised, or “primed”, with data when the teleprotection service is started. Any communications jitter (i.e., random deviations from the mean latency) experienced during this initialisation period can be critical, and may result in the buffer “playing-out” data too early or too late. Therefore, there can be an inconsistency in the buffer residency time for the forward and reverse directions, which would be present until the service was stopped and reinitialised – which is clearly unacceptable for a teleprotection service. If the difference in the buffer residency times was substantial, a false trip could occur due to the delay asymmetry. This is because the protection relays “rotate” remote current phasors by the estimated propagation delay; however, this estimation is only valid for symmetrical delays.

A feature called Asymmetrical Delay Compensation (ADC) has been developed to address this issue. ADC is designed to further improve the performance of teleprotection services under non-ideal communications network conditions, such as asymmetric or “jittery” paths. ADC analyses the behaviour of traffic over time and adjusts the jitter buffer residency time accordingly to compensate for errors.

4.2 Protection Settings Analysis

For each testing method described in Section 4.3, the protection relay settings have been configured as shown in Table 3. Note that, for some tests, the value of $k1$ has been selected as 0% (i.e., no current bias) in order to make the relays more sensitive to asymmetrical delay.

Setting	**Typical value** [10]	**Value for high-sensitivity**
I_{s1}	400 A	400 A
I_{s2}	4000 A	4000 A
$k1$	30%	0%
$k2$	150%	150%

Table 3: Current differential protection settings

The theoretical maximum asymmetrical delay that can be tolerated for the selected protection settings can be calculated. Figure 3 illustrates the current phasors required for two-terminal differential protection.

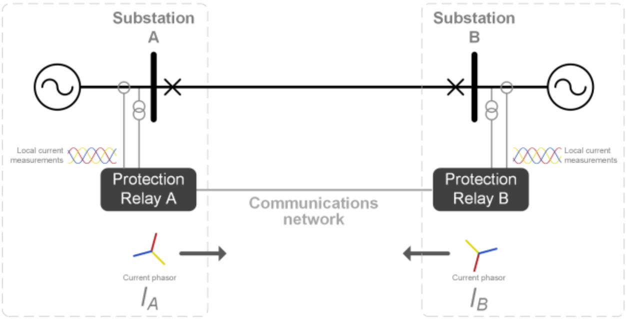


Figure 3: Definition of current phasors for a two-terminal protection scheme

Current phasors I_A and I_B can be defined as follows:

$$I_A = I_{A_m}\angle I_{A_\theta} = I_{A_m}\cos I_{A_\theta} + jI_{A_m}\sin I_{A_\theta}$$
$$I_B = I_{B_m}\angle I_{B_\theta} = I_{B_m}\cos I_{B_\theta} + jI_{B_m}\sin I_{B_\theta}$$

I_{diff} is the magnitude of the vector sum of I_A and I_B, which can be calculated from the real (re) and imaginary (im) components as follows:

$$\begin{aligned} I_{diff} &= \sqrt{\left(re(I_A)+re(I_B)\right)^2+\left(im(I_A)+im(I_B)\right)^2} \\ &= \sqrt{\begin{aligned}&\left(I_{A_m}\cos I_{A_\theta}+I_{B_m}\cos I_{B_\theta}\right)^2\\ &+\left(I_{A_m}\sin I_{A_\theta}+I_{B_m}\sin I_{B_\theta}\right)^2\end{aligned}} \end{aligned}$$

Assuming the load current is within the first region of the differential protection characteristic (i.e., $I_{A_m} < I_{s2}$) and that $k1 = 0\%$, a trip will occur when $I_{diff} \geq I_{s1}$.

Asymmetrical delay results in an error in the estimated phase of the remote current measurements. For a load current magnitude of 3900 A (i.e., I_{A_m} = 3900 A), a value of I_{B_θ} of 185.88º or 174.12º would cause a trip. This means that a phase error of 5.88º would result in a trip. At a 50 Hz fundamental frequency, this equates to a time error of 326.6 μs $(= 5.88° \times 0.02\ s \div 360°)$. However, for the relays to erroneously rotate current vectors by a given angle, the actual asymmetry must be twice this value. This is because the "ping-pong" time synchronisation algorithm [10] used by the relays calculates the total round-trip delay, which is divided by two to estimate the propagation delay in one direction.

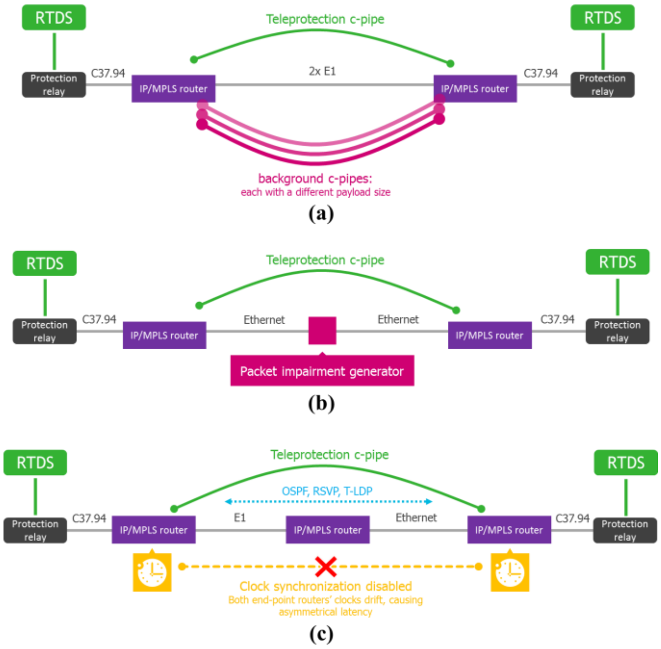
Therefore, for the "high-sensitivity" settings given in Table 3, an asymmetrical delay of approximately 653 μs would result in a false trip.

4.3 Testing Methodology

Three methods have been used to artificially create asymmetrical delay:

Method (a): Traffic congestion due to multiple circuit emulation services (known as "c-pipes") over TDM-based E1 links, with limited bandwidth
Method (b): Injection of jitter during c-pipe initialisation
Method (c): Clock drift due to loss of synchronisation

Each configuration is summarised in Figure 4 and is described in detail in the following subsections.



(a)

(b)

(c)

Figure 4: Asymmetrical delay testing configurations

4.3.1 *Method (a): traffic congestion*

Additional circuit-emulation services (c-pipes), with various payload sizes (ranging from 64 to 160 bytes), have been provisioned which compete for the limited total available bandwidth. This results in packet delay variation (PDV) for the teleprotection traffic. Therefore, there is a probability that, at the instant in time when the teleprotection jitter buffer is initialised, PDV will be present which will "degrade" the jitter buffer state in one or both directions. This may lead to a false trip, as described in Section 4.1. The script illustrated in Figure 1 controls multiple iterations of starting and stopping the teleprotection service to ensure that the worst-case PDV is likely to be experienced.

In practice, critical protection traffic would be prioritised above other services through the appropriate Quality-of-Service (QoS) profile, but PDV can still occur due to a high-priority packet arriving at a node just after the start of the transmission of a large packet from another service.

4.3.2 *Method (b): injection of jitter*

The impairment generator illustrated in Figure 1 has been configured to add additional latency to the packet flow in each direction, according to a Gaussian distribution. This allows jitter, according to the defined statistical distribution, to be “injected” into the Ethernet link carrying teleprotection traffic. Figure 5 illustrates a typical packet delay distribution.

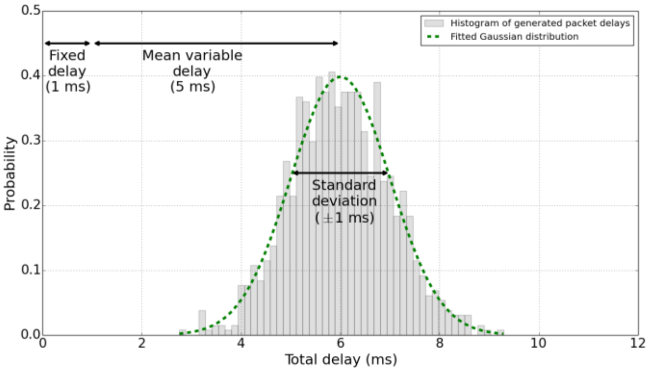


Figure 5: Typical packet delay injection distribution

The same delay distribution has been applied to traffic in both directions. As for test method (a), multiple iterations have been executed to ensure that worst-case jitter is experienced during initialization of the jitter buffers.

4.3.3 Method (c): clock drift

Multiple nodes in an IP/MPLS network must be synchronised – using Synchronous Ethernet (SyncE), IEEE 1588, or otherwise – to ensure that the teleprotection service functions correctly. By intentionally disabling this synchronisation, the local clocks of the IP/MPLS routers may drift differently over time, thereby injecting a gradual relative phase error between the two end-points. Therefore, one end-point delivers teleprotection traffic at a slightly faster rate than the other end-point; over time the phase error accumulates and would eventually result in a false trip due to the asymmetry.

This testing method involves disabling the IP/MPLS router synchronisation and recording false trips – if any – with the ADC feature disabled and enabled. In this case, stratum 3 clocks, with an accuracy of ±4.6 ppm, have been used in the IP/MPLS routers.

4.4 Results

4.4.1 Method (a): traffic congestion

For the specified combination of traffic from competing services, false trips have been observed in over 66% of test iterations without ADC enabled. With the ADC feature enabled, no false trips have been observed.

4.4.2 Method (b): injection of jitter

Table 4 summarises the results for several different test parameters. For each test, at least 10 iterations have been performed to ensure that – where expected – false trips occur without ADC enabled. Tests 1-5 illustrate the impact of different jitter profiles. Note that the fixed delay value is the minimum total delay, regardless of the calculated value of the variable delay component for a given packet. Tests 6-10 illustrate the effect of varying other parameters: MPLS payload size, jitter buffer size, and the number of packets sampled by the ADC analysis process.

In all cases, and for all parameter combinations, it has been demonstrated that the ADC feature prevents false trips.

4.4.3 Method (c): clock drift

Without the ADC feature, it has been observed that the protection relays would trip after approximately 40 minutes, due to excessive clock drift. However, with ADC enabled, no trips have been observed over several hours. Furthermore, using monitoring functionality within the IP/MPLS routers, automatic adjustments to the jitter buffer residency time have been observed approximately every 40 minutes – confirming that the ADC feature operated correctly.

5 Conclusions

This paper has described the validation and performance analysis of an encryption method and an asymmetrical delay compensation method for current differential protection in IP/MPLS networks.

It has been demonstrated that wide-area power system

	MPLS and ADC settings			**Jitter Gaussian distribution**			**Number of protection relay false trips**	
Test	**Packet size (bytes)**	**Buffer size (ms)**	**ADC sampled packets**	**Fixed delay (ms)**	**Mean variable delay (ms)**	**Standard deviation (ms)**	**ADC off**	**ADC enabled**
1	16	8	32,000	1.0	5.0	1.0	7 of 10	0 of 10
2	16	8	32,000	1.0	3.0	1.0	3 of 10	0 of 10
3	16	8	32,000	1.0	2.0	1.0	4 of 20	0 of 20
4	16	8	32,000	1.0	1.0	1.0	3 of 20	0 of 10
5	16	8	32,000	1.0	0.3	1.0	0 of 20	0 of 20
6	8	8	32,000	1.0	5.0	1.0	N/A	0 of 20
7	32	16	16,000	1.0	5.0	1.0	N/A	0 of 20
8	8	8	1,000	1.0	5.0	1.0	N/A	0 of 20
9	8	8	8,000	1.0	5.0	1.0	N/A	0 of 20
10	8	16	16,000	1.0	5.0	1.0	N/A	0 of 20

Table 4: Test summaries for jitter injection (method (b))

communications – including safety-critical teleprotection services – can be encrypted in real-time with negligible impact on performance. Furthermore, the approach described in the paper offers operational benefits for utilities and protection device vendors: authentication and encryption functionality is provided, without requiring a complex implementation within protection each protection relay, PMU, or other device; key generation can be managed automatically over time; and legacy devices and interfaces can be supported.

A method for avoiding the impact of jitter in real networks has been thoroughly tested using three methods. In all cases, even with relatively sensitive protection settings, no false trips occur with ADC enabled.

These results will be of interest to utilities looking to adopt packet-based technologies achieve a more efficient, flexible, and secure communications infrastructure.

References

[1] M. Anavi, “Cyber Security for Power Utilities - A defense primer for the operational network,” 2013.

[2] S. M. Blair and C. D. Booth, “Real-time teleprotection testing using IP/MPLS over xDSL,” *University of Strathclyde*, 2013. [Online]. Available: https://pure.strath.ac.uk/portal/files/26184600/001_DSL_Testing.pdf.

[3] RTDS, “Real Time Power System Simulation - RTDS Technologies,” 2011. [Online]. Available: http://www.rtds.com.

[4] S. M. Blair, F. Coffele, C. Booth, B. De Valck, and D. Verhulst, “Demonstration and analysis of IP/MPLS communications for delivering power system protection solutions using IEEE C37.94, IEC 61850 Sampled Values, and IEC 61850 GOOSE protocols,” in *CIGRE Paris Session B5*, 2014.

[5] S. M. Blair, F. Coffele, C. D. Booth, and G. M. Burt, “An Open Platform for Rapid-Prototyping Protection and Control Schemes with IEC 61850,” *IEEE Trans. Power Deliv.*, vol. 28, no. 2, pp. 1103–1110, 2013.

[6] Bell Labs, “Alcatel-Lucent network group encryption - Seamless encryption for mission-critical networks,” 2015.

[7] IEC TC 57, “IEC/TR 61850-90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118,” 2012.

[8] IEC TC 57, “IEC/TS 62351-6 Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850,” 2007.

[9] IEC 61850 Users Group, “IEC TR 61850-90-5 Open Source Project,” 2013. [Online]. Available: http://iec61850.ucaiug.org/90-5/default.aspx.

[10] Alstom Grid, *Network Protection & Automation Guide*. Alstom Grid, 2011.