Investigating the Impact of Network Security on the Line Current Differential Protection System

A. Aichhorn*, A. Unterweger †, D. Engel †, and R. Mayrhofer ‡

*Sprecher Automation GmbH, Linz, Austria, andreas.aichhorn@sprecher-automation.com
†Fachhochschule Salzburg, Center for Secure Energy Informatics, Salzburg, Austria
{andreas.unterweger, dominik.engel}@fh-salzburg.ac.at
‡Johannes Kepler University, Linz, Austria, rene.mayrhofer@jku.at

Keywords: Line Current Differential Protection, Network Security, IPsec, Clock Synchronization, WAN

Abstract

This paper analyzes the influence of network security measures on the system behavior of a power system protection device. In this particular case, an IP-based Ethernet protection interface of a line current differential protection system is considered. IPsec has previously been proposed to be part of the security concept of the protection interface. Therefore, we conduct a trade-off analysis regarding the influence of IPsec on the protection function and consequently on the system safety. This work shows that the protection function of the relay is not impaired as long as the additional CPU performance for the encryption by the protection relay is available and the necessary bandwidth on the communication channel is provided.

1 Introduction

Various protection schemes are known to protect power lines from faults, i.e., earth faults or short circuits. The line current differential protection scheme, also known as 87L protection according IEEE C37.2-2008, is one of the fastest and a very sensitive protection algorithm. Also advantageous is the absolute selective operation in its protection area. The basic principle of 87L protection is to observe the difference current between both ends of a power line, referring to Kirchhoff's current law, where the sum of currents at a junction has to be equal to zero. As soon as a fault current exceeds a pre-defined threshold, the protection relays send a tripping signal to the circuit breaker to switch off the affected power line. To be able to calculate this tripping criterion, the measurement data of the remote station is required. Consequently, a communication between the 87L protection relays, also known as the protection interface, is necessary. Fig. 1 illustrates the arrangement of such a protection system.

1.1 System safety

The 87L protection system has two operation modes. The main protection mode uses the differential current for the tripping criterion, where the protection interface is necessary. The back-up protection mode uses a protection scheme which does not require such a protection interface, e.g., overcurrent or distance protection.

The measurement data must be transferred within a pre-defined time limit t_{limit}, depending on the path delay of the communication latency t_{PD}, which is illustrated in Fig. 1 by the condition $t_{PD} < t_{limit}$. According to the technical report of the IEC 61850-90-1 [1], this limit is specified to be between 5 and 10 ms depending on the applied voltage level.

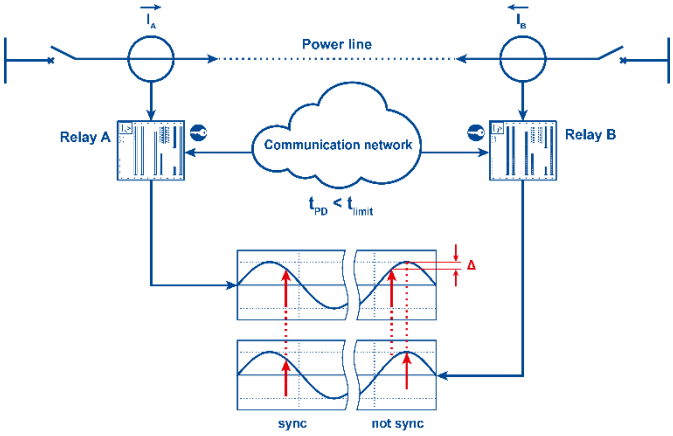

Fig. 1: Arrangement of an 87L protection system.

To get an accurate calculation result, the measurement values are assigned with a timestamp to correctly match the local with the remote data. Fig. 1 illustrates the consequence of synchronized and not accurately synchronized clocks in the diagrams, placed on the bottom of the figure. The left part shows the case of accurately synchronized clocks, whereas the right part depicts the result of not accurately synchronized clocks with the consequence of a spuriously calculated difference current in the case of a healthy state.

Consequently, accurate clock synchronization of the relays is required. The design consideration from the IEC 61850-90-1 [1] recommends a synchronization accuracy of at least 10 µs for high fault current sensitivity.

Several methodologies can be used to realize accurate clock synchronization, e.g., GPS receiver, dedicated fiber for the synchronization pulse or Ethernet-based synchronization methods. Since a network connection is necessary in any case for the measurement data exchange, it is beneficial to use this communication network for the clock synchronization.

We introduced a new concept for the protection interface of an 87L protection system over Ethernet-based networks in [6], [7] to enable the use of standard Ethernet-based Wide Area Networks (WANs). In order for the system to ensure a holistic system safety, a security concept to protect from malicious attacks has to be developed.

1.2 Security against malicious attacks

Since the electrical power system serves to ensure the societal needs, it is classified as a critical infrastructure. Consequently, the power system is an attractive target for attackers. Thus, it is very important that security measures are implemented to protect against malicious attacks, like Blackmailing or Nation-State Attacks. The C1 Working Group Members of Power System Relaying Committee published a report [20], which discusses the importance of cyber security for protection relays. Especially for 87L protection, the hazardous consequences are pointed out, i.e., that malicious attacks may result in losing the protection interface and therefore the differential protection function. Further, the risk of a malfunction due to an attack is hazardous as well for 87L protection.
We previously presented a threats analysis and proposed a security concept for the protection interface of an 87L protection system in [8], which basically introduces the use of IPsec as security protocol [11]. Extra system performance is required for applying such security measures to encrypt and decrypt the transferred data. Consequently, the necessary system performance of the protection relay is increased and the data transmission is at least influenced in terms of latency and bandwidth to an uncertain extent. Additionally, synchronization accuracy may be influenced as well as the continuity of the data stream.
This paper presents a trade-off analysis investigating the influence of the proposed network security measure on the protection function and consequently on the system safety. The analysis is performed on a standard protection relay, manufactured by the company Sprecher Automation GmbH.

1.3 Related work

Blair et al. [9] present a secure and reliable protection interface of an 87L protection system communicating over IP/MPLS, but no trade-off between security and safety has been discussed. Further related work in this field, e.g., [13], [17], evaluates the communication security of protection devices, but uses a different definition of the term security. They interpret it as reliability and dependability, respectively, and not as a protection against malicious attacks.
Therefore, the influence of network security on the protective function has not been discussed so far. This paper performs such a trade-off analysis to analyze the influence on the system safety by using the concept presented in [8].

1.4 Contributions

The main contributions of this paper are:

- An analysis of the real-time capability of IPsec, e.g., during rekeying;
- An investigation of the influence of encryption on the accuracy of channel-based clock synchronization;
- A trade-off analysis between network security and system safety of the protective function of an 87L protection system is performed.

The paper is organized as follows. Section 2 presents the implemented concept of the protection interface and Section 3 describes the applied security concept. Section 4 presents the trade-off analysis and the evaluation. The conclusion is subsequently presented in Section 5.

2 Protection interface

The protection interface is responsible for the measurement data exchange between the protection relays as depicted in Fig. 1. The used communication technology is an Ethernet-based WAN, e.g., Multi Protocol Label switching (MPLS). The transfer protocol is built on top of the IP layer, according to [5], to be routable and establish End-to-End encryption between the protection relays.
Clock synchronization to provide synchronous sampling and the measurement data exchange to calculate the difference current, like presented in [6], [7], is realized over the communication channel.
The remaining part of this section describes the synchronization and the measurement data exchange in detail.

2.1 Clock synchronization

The synchronization algorithm is implemented according to our previous published work [7]. There, a maximum likelihood estimator including a Kalman filter is proposed for accurate clock synchronization. The necessary timestamp exchange is realized by using UDP
[16] as transport protocol.
The convincing advantage of the implemented synchronization algorithm is that no correcting clocks, like boundary or transparent clocks, which are essential for the Precision Time Protocol (PTP) [3] along the communication path, are necessary for meeting the required synchronization accuracy of 10 μs required by [1].

2.2 Measurement data exchange

Measurement data is transferred by using SCTP [19] as transport protocol, according to our previous work [6]. Since momentary values at a frequency of $1\,kHz$ are sent, a continuous data stream is necessary for creating the tripping criterion with the consequence of a stringent timing criteria. The requirement of the communication latency is limited to $5\,ms$ in this work, which is the lowest limit for this application specified in [1]. This timing constraint is also set as the timeout requirement for the data stream. Further, the data stream continuously transmits measurement values with sample data at every $1\,ms$. Therefore, an uninterruptible data stream is a mandatory requirement for a proper operation of the 87L protection system.

2.3 Summary

In summary, the requirements which have to be fulfilled for the realization of an accurate and fast line current differential protection system are:

- Clock synchronization accuracy: $t_{Sync} \leq 10\ \mu s$;
- Providing new measurement data: $f_{data} = 1\ kHz$;
- End-to-End latency between the protection relays: $t_{limit} \leq 5\ ms$;
- Uninterruptible data stream.

To reach the best possible performance of the power grid, the goal is to provide a highly available protection system. Therefore, the protection interface must fulfil the above stated requirements. In order to be protected against malicious attacks, an additional security concept for the protection interface is inevitable.

3 Security concept

In order to protect from malicious attacks, a security concept is necessary. We previously developed a communication concept and a security strategy which fulfils the special needs of a protection interface for an 87L protection system [8]. According to the relating threats analysis, the network security measures have to guarantee availability, confidentiality, and integrity. The implementation consists of a state-of-the-art IPsec implementation and an asymmetric delay attack detection algorithm. Consequently, all threats are handled, whereas not all threats can be prevented. The concept is primarily designed to prevent threats, which is not possible for packet dropping and delay attacks. Therefore, it is important to detect these threats so that the protection relay can be operated in the less favorable back-up protection mode, so that the power line is still protected.

The remainder of this section describes the basic idea of the security concept and the specific implementation used for this system. Implementing a security concept is a major improvement for the overall system safety. Consequently, for a holistic safety investigation, the influence of the security measures on the system performance has to be performed. This trade-off analysis is subsequently presented in Sec. 4.

3.1 Functional principle

Based on the developed channel-based clock synchronization algorithm presented in [7], End-to-End encryption can be realized, as illustrated in Fig. 2 between Relay A and Relay B. Therefore, only the protection relays have to hold the cryptographic keys and not the whole network infrastructure needs to be confidential. Therefore, if the communication infrastructure were to be compromised, the differential protection system would not be affected.

This topology would not be possible with state-of-the-art synchronization methods, like PTP according to [3]. Fig. 2 illustrates the differences. The green line connects Relay A with Relay B and illustrates the proposed scheme, whereas the red line connects Relay C with Relay D and depicts the resulting topology when a state-of-the-art clock synchronization schemes for Ethernet-based networks is used. Therefore, the transferred data only has to be encrypted and decrypted at the end device and the relay, if the here proposed scheme is used. Otherwise, encryption and decryption have to be performed at each network device along the communication path. Furthermore, the proposed scheme decreases the overall computation effort and strengthens the security concept.

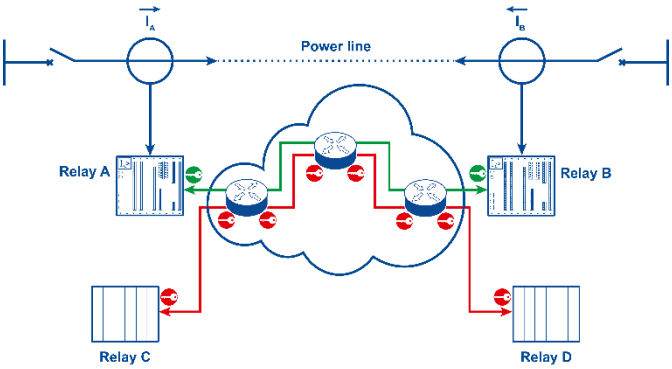

Fig. 2: Network security for protection interface

3.2 IPsec implementation

The implemented IPsec encryption solution is *strongSwan* [18]. *StrongSwan* is an open source implementation, originally designed for Linux systems, and has been ported to other platforms, like Android, Mac OS X and Windows. It includes IPsec as the encryption protocol and the Internet Key Exchange (IKE) [11] protocol for exchanging the private keys.

IPsec includes basically two cryptographic services, Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides integrity and authentication, whereas ESP provides confidentiality in addition. According to the requirements discussed, confidentiality and therefore ESP is necessary for this application. This service can be realized by two different modes, transport and tunnel mode. Basically, tunnel mode is used if two networks have to be connected, whereas transport mode is used if two single end devices have to be securely connected. Therefore, transport mode is applied here, since two protection relays, i.e., end devices, are connected.

For maintaining a long-lasting secure connection, the negotiated keys have to be renewed after a pre-defined amount of time or a pre-defined amount of transmitted bytes.

For this purpose, the key exchange protocol IKE is used. In this work, IKEv2 according to [18] is used, where state-of-the-art methods are implemented. Two phases are required, which are defined in [11]. In phase 1 (authentication phase), a secure connection is established by authentication of the peers. The established secure connection is called a Security Association (SA). Phase 2 uses this SA to negotiate keys for establishing the Encapsulating Security Payload (ESP). After negotiating the keys of phase 2, a secure connection has been built up.

Reauthentication (phase 1) of the SA verifies that the peers retain their access to authentication credentials and rekeying (phase 2) establishes for the ESP SA new keys and resets message ID counters. This procedure strengthens the security of such a connection, especially for a permanent data stream.

4 Trade-off analysis

As already stated, the implemented security increases the required system performance, including CPU usage, network bandwidth and communication latency (deterministic and stochastic part), which may have an impact on the protective function. The investigated parameter which may be affected are:

(a) CPU usage
(b) Bandwidth utilization
(c) Communication latency
(d) Clock synchronization accuracy
(e) Real-time requirements of the sensor data stream

These parameters have to be divided into their effect on the protection system into increased necessary system performance and endangering the protective function, the system safety, respectively. The first group applies to (a) and (b) whereas the second group applies to (c), (d) and (e).

4.1 Experimental setup

The trade-off analysis is performed on a standard protection relay from the company Sprecher Automation GmbH. The built-in processor is a Freescale i.MX 6 quad core CPU with a clock frequency of 800 MHz. The port speed of the fast Ethernet controller, attached to the CPU, is set to 100 $Mbit/s$ and supports hardware timestamping.

4.2 CPU usage

If the system is running under normal conditions, i.e., without activated IPsec, the average CPU load is 12%. If IPsec is activated on the protection device, the load increases to an average value of 19%.
Consequently, as long as the resources of the processor meet the demands of all remaining applications, IPsec encryption does not endanger the protection function. The used system has enough resources and therefore the system safety is not jeopardized.

4.3 Bandwidth utilization

The data encryption entails increased bandwidth demand due to packing of all IP data into a new IP frame. Fig. 3 shows on the top a generic Ethernet frame (without encryption), whereas on the bottom an Ethernet frame with IPsec/ESP (transport mode) encryption is illustrated. It is evident that there is a sufficient increase of the transferred data due to integrating the security layer.
Based on the transferred data, which consists of the timestamps at a frequency of 8 Hz and the measurement data at a frequency of 1 kHz, a bandwidth of 1.57 $Mbit/s$ (on wire for both directions) is necessary. If IPsec encryption is enabled, the required bandwidth is 2.28 Mbit/s, which corresponds to an increase of 45%.
Thus, as long as the communication channel provides the necessary bandwidth, the protection function is not endangered.

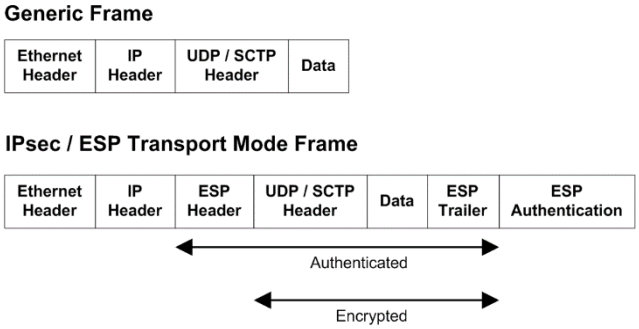

Fig. 3: Generic Ethernet and IPsec/ESP encrypted frame according to [15]

4.4 Communication latency

The communication latency can be divided into two different parts: the intrinsic and the routing delay according to [14]. The intrinsic delay is the deterministic part which is constant for one specific route. It consists of the propagation time of the signal in the media, e.g., Fiber Optical (FO) cable, and the processing time of the data packets within the network devices, defined by the packet size and the port speed. The routing delay is the stochastic part, which is caused by the queuing of messages in the network device. This part of the delay depends on the channel utilization.

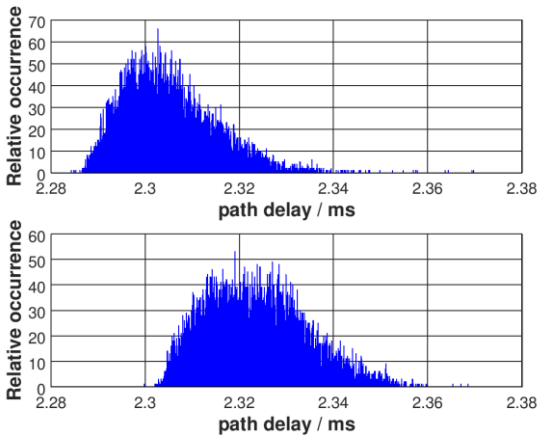

Fig. 4: Histogram of path delays without (top) and with (bottom) the use of IPsec.

Fig. 4 shows histograms of the communication latency, where the stochastic part of the delay is illustrated. The intrinsic delay is equal to the minimum measured delay.
Fig. 4 illustrates the path delays on the top without and on the bottom with IPsec encryption. The intrinsic delay without IPsec results in 2.285 ms, and with activated IPsec in 2.30 ms. The additional intrinsic delay is equal to 15 µs and is caused by the additional frame / header data due to IPsec. The standard deviation, which represents the routing delay, changes from 9.76 µs to 10.65 µs. This slight change is not caused by the encryption, but solely by the stochastic occurrence of this delay type.

The security lead to an increase of the communication latency, but only a slight increase. Since the test was performed with upper bound condition ($t_{limit} = 5\,ms$), communication latency does not endanger the protection function.

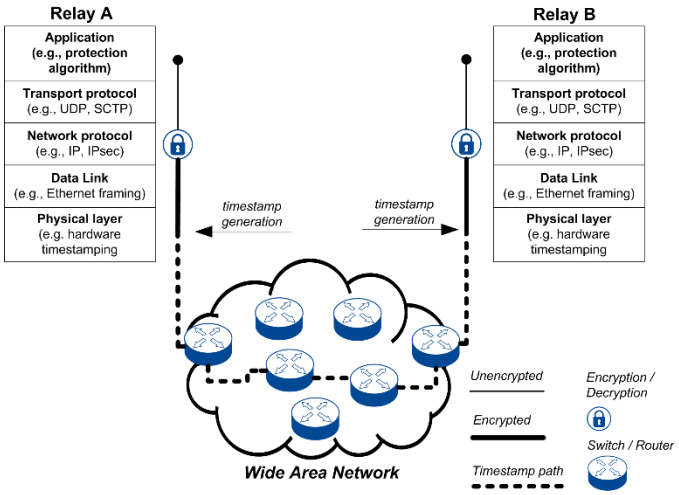

Fig. 5: Timestamp path

4.5 Clock synchronization accuracy

The implemented clock synchronization method uses the communication channel for the timestamp exchange, following [7]. Therefore, the synchronization accuracy is influenced by the communication channel characteristics, the stochastic delay, respectively occurring in the channel between the generation of these timestamps. Fig. 5 illustrates the resulting timestamp path.
It is clearly visible, that this concept of timestamp generation does not influence the accuracy if IPsec is used, since the additional jitter due to packing the IP payload into the IPsec/ESP frame, is performed in the chain before the packet is time-stamped in the sending and after it is time-stamped at the receiving device, according to Fig. 5. Accuracy measurements with and without IPsec, are shown in Fig. 6. Here, no influence of the encryption is present and the synchronization accuracy stays in between a limit of $\leq 3\,\mu s$ for both measurements. If software timestamps, generated at the application layer, would be used, encryption would degrade the synchronization accuracy.

4.6 Sensor data stream

In order to protect the power line without interruption, the difference current has to be calculated continuously. Therefore, an uninterruptible data stream of the measurement values between the protection relays has to be guaranteed. Thus, if the security measure, i.e., IPsec in this work, violates the timing constraints, the protection function would not work properly anymore in the main protection mode of the 87L relay.
As the previous sections already presented, the system needs additional resources, but is not endangering the differential protection algorithm so far. However, one aspect of this setup has not been investigated yet – the renewing of the security keys of the IPsec connection of phase 1 and phase 2.

Reauthentication is necessary to prove if the peer/user still has access to the authentication credentials. Data may be lost during reauthentication where a new security association is built up, depending from the timing constraints. Despite the option of IKEv2 [18] to reauthenticate before the keys are deleted (make-before-break), it is still possible that packages are lost while the new keys are installed. In this specific application a continuous data stream is using the secured channel and as soon as the data stream is interrupted, the connection has to be built up from scratch and has to be authenticated anyway. Therefore, the device or user does not change during an active connection and no reauthentication is required and the continuity of the data stream is not endangered.

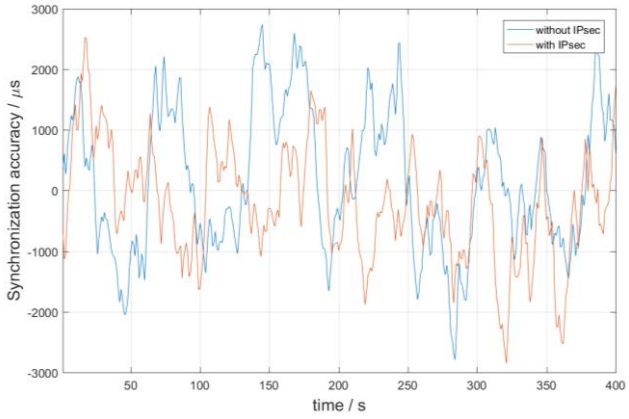

Fig. 6: Measurement of clock synchronization accuracy without and with the use of IPsec

Rekeying, compared to reauthentication, is necessary to avoid the use of compromised keys and therefore to maintain a secure connection. Therefore, after a pre-defined time or after a pre-defined amount of data traffic, a new key has to be used for the encryption of the transferred data.
Rekeying was a major issue in previous versions of IPsec for the use in combination with real-time constraints, since there was only a single key valid at a time and the key update caused data loss or re-transmissions of a data stream, respectively. Also, if the key was synchronously updated at both relays, the rekeying process could cause data loss due to the fact that there may still exist messages encrypted with the previous key, which cannot be decrypted with the renewed one after rekeying.
Since *strongSwan* version 5.5.3 [18], inline rekeying of SAs is supported to provide a seamless renewal of the necessary keys. Thus, by using this version, rekeying can be enabled without endangering the system safety and a secure uninterruptible data stream can be provided.

4.7 Summary

The CPU usage is increased, additional bandwidth is necessary, the communication latency slightly increased and the clock synchronization accuracy as well as the timing constraint of the sensor data stream is not influenced by the applied security measures. The results of the performed trade-off analysis are summarized in Tab. 1.

Attribute	Required	No encryption	IPsec / ESP
CPU usage		12%	19%
Necessary Bandwidth	$\geq$ 1.57 $MBit/s$	1,57 $Mbit/s$	2,28 $Mbit/s$
Communi-cation latency	$\leq$ 5 ms	2.285 ms	2,30 ms
Clock synch-ronization accuracy	$\leq$ 10 μs	$\leq$ 3 μs	$\leq$ 3 μs
Sensor data stream	*continuous*	*continuous*	*continuous*

Tab. 1: Summary of the requirements for the protection interface and the results of the trade-off analysis

5 Conclusion

This paper investigated the influence of network security measures at the protection interface of an 87L protection system on the protective function. IPsec with ESP encryption in transport mode is used as the security protocol. The implementation *strongSwan* [18] is used as IPsec encryption. The results show that if the extra performance of the CPU and the necessary bandwidth is provided and the resulting communication latency does not exceed the specified limits, the security measures do not jeopardize the protective function and therefore the system safety. The clock synchronization accuracy is not influenced by using IPsec if hardware timestamps are used. Further, the sensor data stream is not interrupted by IPsec, not even during the renewal of the keys when using inline rekeying, which is supported since *strongSwan* version 5.5.3. Finally, by using the concept proposed in this paper, the security measures do not jeopardize the protective function and consequently the differential protection relay is continuously working including the security measures.

Acknowledgements

This research is performed within the research project SmartProtect, supported by The Austrian Research Promotion Agency (FFG), project no. 848911. The financial support by the Austrian Federal Ministry of Science, Research and Economy,the Austrian National Foundation for Research, Technology and Development and the Federal State of Salzburg is gratefully acknowledged.

References

[1] Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations, IEC TR 61850-90-1, Mar. 2010.

[2] IEEE Guide for Protective Relay Applications to Transmission Lines, IEEE Std C37.113-2015, Jun. 2016

[3] IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, IEEE Std 1588-2008, Jul. 2008.

[4] IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, IEEE Std 1686-2013, Jan. 2014.

[5] ISO/IEC Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model, ISO/IEC 7498-1:1994, Nov. 1994

[6] A. Aichhorn, R. Mayrhofer, H. Krammer and T. Kern, "Realization of Line Current Differential Protection over IP-based Networks using IEEE 1588 for Synchronous Sampling", in IET DPSP, Mar. 2016.

[7] A. Aichhorn, B. Etzlinger, R. Mayrhofer and A. Springer, "Accurate Clock Synchronization for Power Systems Protection Devices over Packet Switched Networks", Springer Link, Computer Science - Research and Development, Vol. 32, Issue 1-2, pp. 147-158, Mar. 2017.

[8] A. Aichhorn, B. Etzlinger, S. Hutterer and R. Mayrhofer, "Secure communication interface for line current differential protection over Ethernet-based networks", in 12th IEEE PES PowerTech Conference, pp. 1-6, Jun. 2017.

[9] S. M. Blair, C. D. Booth, B. De Valck, D. Verhulst, C. Kirasack, K. Y. Wong, and S. Lakshminarayanan, "Validating Secure and Reliable IP/MPLS Communications for Current Differential Protection", in IET DPSP, pp. 1-6, Mar. 2016.

[10] S. M. Blair, C. D. Booth, B. D. Valck, D. Verhulst and K. Y. Wong, "Modelling and Analysis of Asymmetrical Latency in Packet-Based Networks for Current Differential Protection Application", in IEEE Transactions on Power Delivery, *to appear*.

[11] S. Frankel and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", RFC 6071, Feb. 2011.

[12] P. Hitchin, "Keeping the lights on", E & T magazine, Engineering and Technology, Volume 9, Issue 4, pp. 36-39, May 2014.

[13] J. Holbach, N. Schuster and A. Struecker, "Secure Data Communication for Line Differential Relays," in Power Systems Conference 2009, pp. 1-6, Mar. 2009.

[14] T. Holleczek, V. Venus and S. Naegele-Jackson, "Statistical analysis of IP delay measurements as a basis for network alert systems," in IEEE ICC, pp. 1-6, Jun. 2009.

[15] S. Kent, "IP Encapsulating Security Payload (ESP)", RFC 4303, Dec. 2005.

[16] J. Postel, "User Datagram Protocol", RFC 768, Aug. 1980.

[17] E. O. Schweitzer, K. Behrendt and T. Lee, "Digital Communications for Power System Protection: Security, Availability, and Speed," SEL Journal of Reliable Power, Volume 1, Number 1, pp. 1-25, July 2010.

[18] A. Steffen, "strongSwan - the OpenSource IPsec-based VPN Solution," [Online]. Available: http://www.strongswan.org, Sep. 2017.

[19] R. Stewart, "Stream Control Transmission Protocol", RFC 4960, Sep. 2007.

[20] S. Ward et al., "Cyber Security Issues for Protective Relays; C1 Working Group Members of Power System Relaying Committee", IEEE Power Engineering Society General Meeting, pp. 1-8, Jun. 2007.