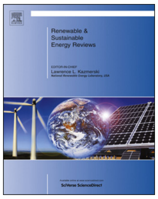
Renewable and Sustainable Energy Reviews 54 (2016) 1552–1562

Contents lists available at ScienceDirect

Renewable and Sustainable Energy Reviews

journal homepage: www.elsevier.com/locate/rser



Cyber-security in substation automation systems

Naiara Moreira*, Elías Molina, Jesús Lázaro, Eduardo Jacob, Armando Astarloa

Department of Electronics Technology, University of the Basque Country UPV/EHU, Spain

ARTICLE INFO

Article history:
Received 12 January 2015
Received in revised form
10 August 2015
Accepted 26 October 2015
Available online 11 November 2015

Keywords:
Cyber-security
SAS
IEC 61850
IEC 62351
IEEE 1588

ABSTRACT

The cyber-security of several industrial plants has been compromised for last years by some worms and viruses, such as Stuxnet, which was able to take control of the Supervisory Control And Data Acquisition (SCADA) system of a nuclear plant in Iran. The research community and the international standardization committees raised their awareness about protecting information in Substation Automation Systems (SAS). IEC 61850-5 and IEC 62351-6 standards respectively describe communication models and the security mechanisms to be deployed in current substations, but they present some inconsistencies. On the one hand, this standard mandates that RSA cryptosystem must be used to provide source authenticity of GOOSE and SV messages. However, despite expensive processors with crypto accelerators were utilized, execution times would exceed the maximum transfer times stated in the standard for most time critical applications. On the other hand, the recommended synchronization solution is the Precision Time Protocol (PTP), as defined in IEEE 1588-2008, which introduced an optional security extension based on old keyed hash algorithms that has also been demonstrated to be suboptimal due to latency times and required resources. The aim of this paper is to explore current available security solutions and study their applicability to the substation environment. Furthermore, as part of the future security framework, a MACsec-based security approach that allows different communication services with diverse performance and security requirements to live together within the substation network is proposed.

Contents

1. Introduction

The tendency in energy production from renewable energy resources is increasing worldwide. Therefore, the Smart Grid defined as the next-generation electrical power system has to fulfil strong requirements regarding reliability, flexibility, efficiency and environmentally friendly operation. Management and control functions in the electric grid depend on the real time information that is shared among systems through an advance digital communications network, which must be protected against attacks from hackers.

Several significant events have exhibited the vulnerabilities of the communication framework in power systems since 2003. A

* Corresponding author. Tel.: +34 946017243.
E-mail address: naiara.moreira@ehu.es (N. Moreira).

http://dx.doi.org/10.1016/j.rser.2015.10.124
1364-0321/© 2015 Elsevier Ltd. All rights reserved.

nuclear plant crashed because its control system network was infected by the Slammer worm. This virus bypassed firewalls causing the safety monitoring system to be disabled for nearly five hours [1]. Similarly, the computer worm Stuxnet infected the software of many industrial sites in Iran, including a nuclear plant which uses Siemens industrial control programs based on Microsoft Windows [2]. Stuxnet was the first worm known to attack Supervisory Control And Data Acquisition (SCADA) systems. It spies on the operations of the system and, then, uses this information to take control of the machines turning them into failure. The worm is believed to have been created with the support of a nation-state in an attempt of starting a cyberwar caused by geopolitical conflicts. After that, other variants of the Stuxnet worm were discovered such as Duqu, Flame and Gauss with the aim of spying on industries, people and banks. These worms can be quickly spread over USB sticks and networks without being detected by automated detection systems.

In last ten years, several organisms, such as those that formed the International Council on Large Electric Systems (in French, *Conseil International des Grands Réseaux Électriques or CIGRÉ*) and the International Electrotechnical Commission (IEC) have put a great effort concerning cyber-security on power systems [3]. IEC 62351 Security Standards address security issues for the different power system operations and communication standards defined by the IEC Technical Committee 57 (IEC TC57) [4].

This paper sets focus on the protection of information that is exchanged in substation networks, and is structured as follows. Section 2 outlines the evolution of communication systems in substations. The IEC 61850 is presented as current family of standards for power utility communications in Section 3, and Section 4 introduces the corresponding security standard. Other additional protocols and standards for a reliable and efficient operation are briefly described in Section 5. Then, guidelines for protecting future SASs are presented in Section 6 and, in Section 7, a MACsec based security approach is introduced. Finally, Section 8 summarizes the conclusions of this work.

2. The evolution of communication systems in substations

Conventional power generation, transmission and distribution networks are naturally evolving to Smart Grid technologies and consequently, the interest of the research community in the development of new functions has been growing considerably. Smart Grids are defined by the European Technology Platform as “an electricity network that can intelligently integrate the actions of all users connected to it (generators, consumers and those that do both) in order to efficiently deliver sustainable, economic and secure electricity supplies” [5]. In order to optimize the operation of the interconnected elements in power systems, a two-way flow of power, in electrical network, and information, in communication network, is required [6].

Substations are the nodes in the electrical power network that connect the lines and cables for transmission and distribution of electricity. In substations, local functions, such as data acquisition from the power grid via the switchgear (sensors) and activation of changes by commands to switchgear devices (actuators), are performed. For instance, a protection function issues a trip command to the allocated circuit breaker in case of fault detection.

In the eighties, the substation architecture gradually evolved from rigid parallel copper wiring to some proprietary solutions based on telephone, teletype or modem technologies [7]. Also, some standard protocols for industrial automation were employed in power systems, such as the Distributed Network Protocol version 3 (DNP3). Local functions in substations were performed through centralized SCADA systems which consisted of a Master Terminal Unit (MTU) and several Remote Terminal Units (RTUs) geographically distributed. RTUs were devices that gathered data and send control commands to switchgear components. The MTU continuously checked the state of the RTUs and if they have intentions to use the shared bus, by sending them messages periodically.

Modern SASs consist of a variety of microprocessor based Intelligent Electronic Devices (IEDs) and primary equipment (high-voltage circuit breakers, disconnectors, earthing switches, gas insulators, transformers, etc.) that provide local and remote access to the power system, manual and automatic functions and communication links and interfaces to the switchgear. In contrast to RTUs, SAS performs all local tasks in a more decentralized structure and the communication function of the RTU is often implemented in a gateway IED, which should convert communication protocols in both directions. Thus, the information collected and stored in IEDs is transferred to the SCADA master via this gateway [8]. SASs improve the control of the network, allowing a quick self-response to problems in few seconds. Hence, the highest benefits of SAS are the minimization of the number of outages and outage times, the reduction of operating costs, the increase of productivity and the improvement of power system performance [8]. In addition, since SASs improve the quality of the service and the power quality, the positive impact on end customer experience increases his satisfaction.

In traditional SCADA systems, the existence of many proprietary solutions made difficult the interoperability between devices, even between different versions of devices from the same supplier. Expensive protocol converters or re-engineering were needed to mitigate the problem of interoperability. In 1994, the IEC started to work on developing a common standard for substation communications, while the IEEE started a similar work on developing a common communication framework called Utility Communication Architecture (UCA). After that, in 1997, both organisms started to work together on the development of the standard IEC 61850 *Communication networks and systems for power utility automation* [6]. The different parts of the standard were first published between 2002 and 2005 becoming the only standard that provides an open architecture and assures interoperability with IEDs from different vendors. The main objectives of the standard were interoperability, free architecture and long term stability [9].

3. IEC 61850 standard general overview

While communication technologies change very rapidly, primary equipment in substations have lifetimes of 30–40 years and secondary equipment and IEDs are replaced between one and four times in this period of time [7]. Consequently, the standardization was focused on the domain specific object data model rather than the communication technology, which separated communication services from protocols and ensured interoperability through the definition of different mappings of data models into communication layers. Objects are breakers, controllers or other protection elements that exchange data with each other using standardized services [8].

Although the IEC 61850 standard was initially oriented to communications within the substation, it has been expanded to the whole power system including communications between substations and other inter-domain communications, as shown in Fig. 1. IEC 61850 parts are listed in Table 1. Parts from 3 to 5 define general and functional requirements as well as project management. Part 6 defines the Substation Configuration Language (SCL) that is based on Extensible Mark-Up Language (XML) and is used to exchange configuration information. The rest of the parts define communication services, data models and the mapping of services

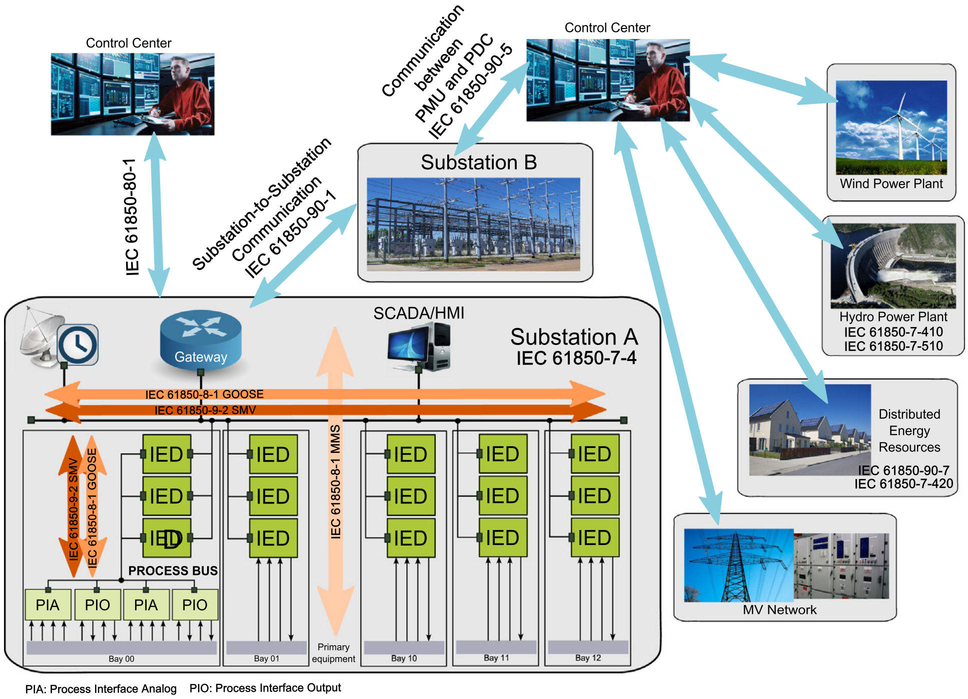


Fig. 1. IEC 61850 standards family scope [10,11].

Table 1
IEC 62351 standard parts.

IEC 61850 Parts	Title	Version	Date
Part 1 (TR)	Introduction and overview	ed2.0	2013/03
Part 2 (TS)	Glossary	ed1.0	2003/03
Part 3	General requirements	ed2.0	2013/12
Part 4	System and project management	ed2.0	2011/04
Part 5	Communication requirements for functions and device models	ed2.0	2013/01
Part 6	Configuration description language for communication in electrical substations related to IEDs	ed2.0	2009/12
Part 7-1	Basic communication structure – Principles and models	ed2.0	2011/07
Part 7-2	Basic communication structure – Abstract communication service interface (ACSI)	ed2.0	2010/08
Part 7-3	Basic communication structure – Common Data Classes	ed2.0	2010/12
Part 7-4	Basic communication structure – Compatible logical node classes and data classes	ed2.0	2010/03
Part 7-410	Basic communication structure – Hydroelectric power plants - Communication for monitoring and control	ed2.0	2012/10
Part 7-420	Basic communication structure – Distributed energy resources logical nodes	ed1.0	2009/03
Part 7-510 (TR)	Basic communication structure – Hydroelectric power plants - Modelling concepts and guidelines	ed1.0	2012/03
Part 8-1	Specific communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3	ed2.0	2011/06
Part 9-2	Specific communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3	ed2.0	2011/09
Part 10	Conformance testing	ed2.0	2012/12
Part 80-1 (TR)	Guideline to exchanging information from a CDC-based data model using IEC 60870-5-101 or IEC 60870-5-104	ed1.0	2008/12
Part 90-1 (TR)	Use of IEC 61850 for the communication between substations	ed1.0	2010/03
Part 90-4 (TR)	Network engineering guidelines	ed1.0	2013/08
Part 90-5 (TR)	Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118	ed1.0	2012/05
Part 90-7 (TR)	Object models for power converters in distributed energy resources (DER) systems	ed1.0	2013/02

to different network protocols for both intra- and inter-substation communication.

In order to meet the free configuration and long-term stability requirements, the IEC 61850 standard follows an Open Systems Interconnection (OSI) 7 layer model, where substation data services and applications are built above the application layer. The communication stack is represented in Fig. 2. The Abstract Communication Service Interface (ACSI) is a virtual interface to an IED that provides abstract services independent of the communication stack and the Specific Communication Service Mapping (SCSM) defines the concrete mapping of ACSI services and objects into a particular protocol (IEC 61850-8-1 [12], IEC 61850-9-2 [13]).

The standard specifies three types of communication models for these ACSI services: client/server communication, publisher/subscriber

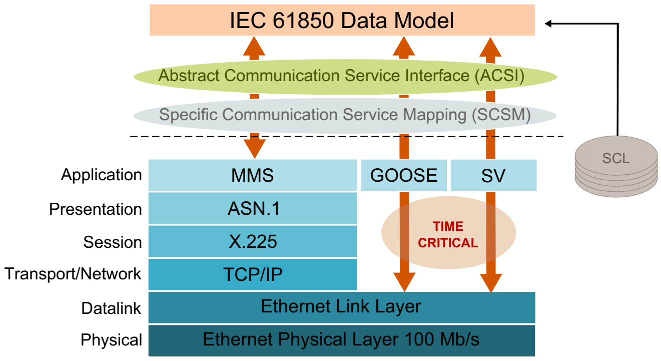


Fig. 2. IEC 61850 communication stack.

model with Generic Object Oriented Substation Events (GOOSE) messages and multicast Ethernet based Sample Values (SV) model. Most of IEC 61850 communications are based on client/server communication using the Manufacturing Message Specification (MMS) standard (as defined in ISO 9506 standard [14]) over TCP/IP, which provides a more reliable data transfer. An example of these services is the fault/event recording. For time critical applications, such as a protection function issuing a trip command, data is directly mapped to the Ethernet data link layer as GOOSE messages or SVs transmission using connectionless multicast addressing of frames. For instance, a protection function issuing a trip command requires transfer times below 3 ms and hence, information is directly mapped into a GOOSE message. While GOOSE messages generally transmit binary data such as indications, alarms and tripping signals, SVs are used to transfer current/voltage raw samples from Current/Voltage Transformers (CTs/VTs) to IEDs.

Fig. 3 shows the logical view of an example substation network architecture [15], commonly known as the IEC 61850 substation automation model, where there are three different levels: the station level, the bay level and the process level. The process bus is the communication network which connects IEDs at primary equipment level, whereas the station bus connects IEDs at bay level and IEDs at station level. While process level devices are typically switchyard apparatus, remote I/Os, intelligent sensors and actuators and CTs/VTs for measurements, bay level devices are needed for control, protection and monitoring functions. Thus, the primary equipment and the protection and control IEDs are in the process and bay levels respectively. The station level consists of a computer with a database and a Human Machine Interface (HMI) to be controlled by an operator, as well as the interfaces for remote communication as it has been represented in Fig. 1. Originally, the process bus was specified as the carrier of the SV traffic and the station bus as the carrier of MMS and GOOSE traffic, but both can carry the three types of traffic.

4. Cyber-security for IEC 61850 communications

The interest of research community in the protection of critical infrastructures, and specially the electricity generation and distribution grids, has increased over the past decade: when the electricity stops, everything stops [16]. As it has been introduced in Section 1, power systems are becoming computerized and control equipment interconnection is evolving from proprietary solutions to standard communication networks. This evolution reduces the costs of deployment but also open up new digital vulnerabilities, since clear information packets can be easily sniffed, altered or recorded and played black. Examples of real-world cases of cyber-security intrusions have already been described previously.

A lot of effort has been put on preventing that people from the Internet could gain unauthorized access to substation control systems. Therefore, the use of firewalls and other boundary control devices, like the Waterfall Unidirectional Security Gateway [17], has been the highest priority. In contrast to common firewalls, which are pure software systems, this Waterfall gateway achieves security at the physical layer: a transmitting device in the control system network contains a laser and a receiving device in the corporate network contains a photocell. As a consequence, the transmitter can send to the receiver, but not vice versa and, therefore, an attacker from the Internet cannot exploit software vulnerabilities to threat the control system. However, this perimeter defences are not sufficient as it was demonstrated with the

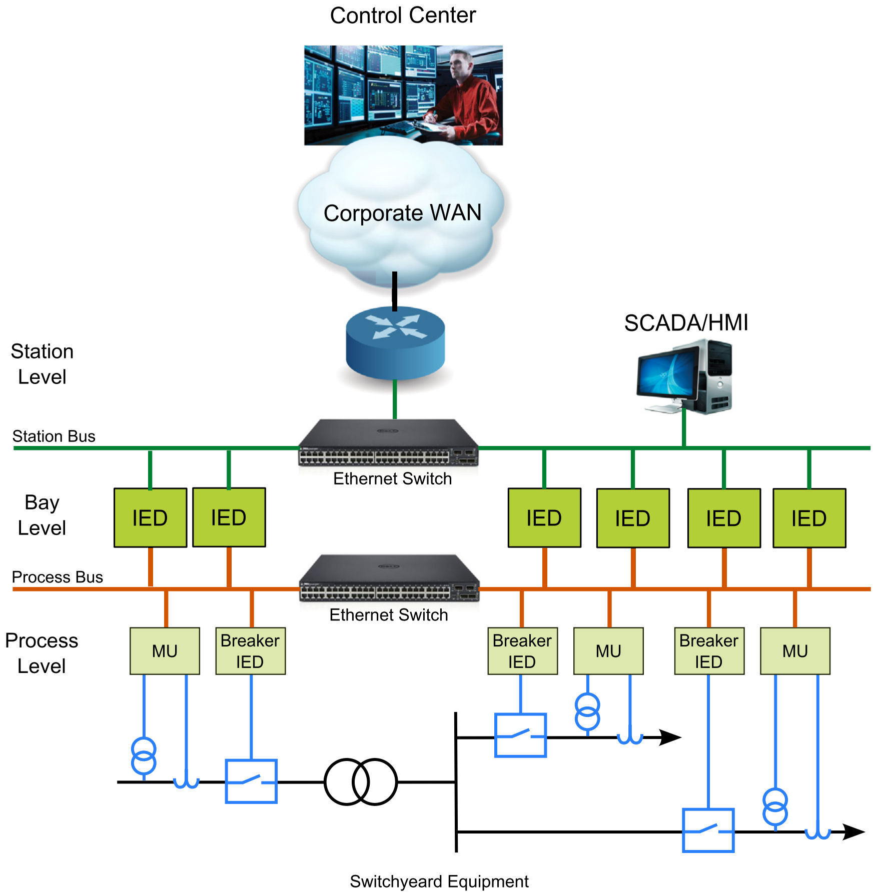


Fig. 3. Substation automation model [15].

infection of SCADA control systems via USB flash drives, where no Internet access was needed. The ideal scenario would be the protection of each individual device within the control network. In addition, security firewalls and gateways are very difficult to maintain since devices and networks in power systems are managed by multiple firms and constantly require changes in network configurations [16].

The IEC TC57 Working Group 15 works in the development of cyber-security standards for power system communications, with the aim of covering both information infrastructure and communication security [4]. In particular, they focused in the communication protocols defined in IEC 60870-5/6, 61850, 61970 and 61968 series. In 2007, the IEC 62351 security standard for the power system information infrastructure was first published and the work is still in process. Table 2 lists the parts that currently compose the standard. The first part describes the background on security for power system operations as well as introduces the remaining parts [18]. Parts 3–6 specify how to provide security services for the protocols mentioned above and listed in Table 1.

In particular, IEC 62351-6 [19] specifies the security mechanisms for protecting communications defined in the IEC 61850 family of standards. The implementation of cryptographic algorithms in power system devices with constrained memory and processing power is a challenge that is partially acknowledged in this part. Thereby, applications based on GOOSE and SVs, which require short transfer times, should only use authentication for ensuring data integrity and source authenticity, but not confidentiality. This standard proposes protecting GOOSE and SV messages with Message Authentication Codes (MAC) using the Secure Hash Algorithm (SHA), which are digitally signed using RSA (Rivest, Shamir and Adleman) public-key cryptosystem to provide source authenticity.

The main drawback of RSA digital signatures is the long execution times for both computation and verification of the signature. Thus, even though a high-end ARM processor with a crypto accelerator core was utilized in substation equipment, RSA signature with 1024-bit keys cannot be computed and verified within 3 ms, which is the maximum transfer time required by some GOOSE messages. In addition, deployment costs would increase considerably. Another alternative to that proposed in the standard would be the implementation of Elliptic Curve Digital Signature Algorithms (ECDSA) in dedicated crypto cores, which could offer latency times required by IEC 61850 for fast messages [16].

The IEC working group is now working on the first edition of the Part 9 regarding key management, which is expected to be published as an international standard in late 2015. This standard will be based on the Group Domain of Interpretation (GDOI). Similarly, Part 6 is planned to be updated shortly as a second edition based on security requirements defined in IEC 61850-90-5 for synchrophasor communications over wide area networks [20]. In this case, communications are based on UDP/IP that also allows multicast transmission and, in addition to integrity and authenticity, also confidentiality is required. In order to minimize the security impact on the performance of field devices, symmetric cryptography rather than digital signatures is proposed as the protection mechanism, using HMAC or AES-GMAC to compute the MAC. A shared group key should be distributed from a key centre to the group participants after being authenticated using GDOI protocol [21].

The rest of applications based on MMS, which should include data confidentiality in addition to authentication, are secured at application and transport levels as described in IEC 62351-3 and IEC 62351-4. End-to-end authentication is provided using Transport Layer Security (TLS) Version 1.0, as defined by RFC 2246 [22]. Some of the included cryptographic algorithms are RSA for key exchange, Advanced Encryption Standard (AES) for data encryption and SHA for message authentication.

Table 2
IEC 62351 standard parts.

IEC 62351 Parts	Title	Version	Date
Part 1	Communication network and system security – Introduction to security issues	ed1.0	2007/05
Part 2	Glossary of terms	ed1.0	2008/08
Part 3	Communication network and system security – Profiles including TCP/IP	ed1.0	2014/10
Part 4	Profiles including MMS	ed1.0	2007/06
Part 5	Security for IEC 60870-5 and derivatives	ed2.0	2013/04
Part 6	Security for IEC 61850	ed1.0	2007/06
Part 7	Network and System Management (NSM) data object models	ed1.0	2010/07
Part 8	Role-based access control	ed1.0	2011/09
Part 9	Key Management	ed1.0	Pending
Part 10	Security architecture guidelines	ed1.0	2012/10

5. Other communication protocols for efficient and reliable SAS

Apart from cyber-security mechanisms to prevent attacks against the legitimacy of the exchanged information and in order to deploy reliable and efficient communication networks in substations, additional protocols are required to provide precise time synchronization and redundancy.

5.1. Synchronization protocols in substations

When the blackout from August 2003 in the Northeast United States and Ontario [23] occurred, the alignment of fault records from different locations in the post-fault analysis was so difficult that time synchronization became the focus of such systems. In the past, the identification of simultaneous incidents was done by skilled personnel who looked continuously at the waveforms. However, an automated evaluation of these incidents could quickly deliver hints that could immediately be used for remedial action, not just for post-fault analysis. This automated evaluation is only possible by assigning accurate timestamps during the recording of faults, and thus, a powerful time synchronization system is required [24].

All devices in the SAS must have the same time reference so as to analyse globally the response of the system and, in case of fault, analyse precisely why, where and when this fault occurred [8]. For current and voltage samples, a time synchronization accuracy in the order of 1 μs is required. Even for fault detection and location on the transmission lines of the power grid, in order to measure the time that a travelling wave takes to traverse the line, a precise synchronization accuracy below 1 μs is desired. As an example, a time error of 1 μs results in a fault location error of 300 m.

Traditionally, IRIG-B was the common synchronization scheme in substations, which provides 1 μs accuracy using dedicated cabling infrastructure that is normally not redundant, increasing considerably implementation and maintenance costs. Normally, substations need long cables, in the range of 300-400 m, from control building to instrument transformers resulting in varying propagation delays that must be compensated with complicated and bothersome calibration processes.

In addition, the tendency is to gather all communications over the same Ethernet based data network, particularly over a shared network process bus in SAS. The 1 ms accuracy needed for post-event fault analysis may be achieved using the Simple Network

Time Protocol (SNTP). However, the IEC Smart Grid Strategy Group and the NIST [25] recommend the Precision Time Protocol (PTP), as defined in IEEE 1588-2008 standard [26], for high precision time synchronization in substation automation systems. Concretely, with the introduction of field specific profiles, the IEEE firstly published a PTP Power Profile as the IEEE C37.238 standard [27] for Power Systems.

PTP automatically compensates for propagation delays and distributes absolute time across a substation directly over Ethernet providing accuracies in the range of nanoseconds. Furthermore, in contrast to IRIG-B systems, time can be transmitted over redundant Ethernet networks to increase the reliability of time distribution.

PTP systems follow a master–slave hierarchy, where the master imposes the time by sending regular Sync messages with accurate timestamps and the slaves synchronize to it in both phase and frequency. In the slave, the syntonization or frequency adjustment is reached by measuring the time difference between consecutive received Sync messages, which allows the device to adjust its clock frequency until time intervals are equal on both the master and slave clocks. The frequency of the slave clock can be controlled by a servo loop which accelerates or slows the clock period. In Fig. 4, the protocol message exchange pattern is presented. The synchronization, or offset adjustment, is computed as the difference between the master and slave times: $t_2 - t'_1$, where t_2 is the slave ingress timestamp and t'_1 is the master egress timestamp t_1 but compensated by the propagation delay. This propagation delay can be computed by slaves using the delay request–response mechanism, following Eq. (3) as defined in the standard:

$$Delay + Offset = t_2 - t_1 \quad (1)$$

$$Delay - Offset = t_4 - t_3 \quad (2)$$

$$Delay = \frac{(t_2 - t_1) + (t_4 - t_3)}{2} \quad (3)$$

In Fig. 5 an example of IEEE 1588-aware substation network is shown, where end devices are called Ordinary Clocks (OCs) and intermediate nodes can be Boundary Clocks (BCs) or Transparent Clocks (TCs) [28]. BCs synchronize to grandmaster and do not forward PTP messages. They send new Sync messages to share its own timing reference with the rest of the slaves. Otherwise, TCs modify the content of PTP messages so as to consider latencies introduced by network nodes when computing the propagation delay and forward them to the slaves. End-to-End (E2E) TCs measure the time the message takes to traverse the TC, named residence time, and accumulate it in a special PTP field called the *correctionField*. Otherwise, Peer-to-Peer (P2P) TCs use the peer delay mechanism to measure the link delay and update the *correctionField* with both the residence time and the link delay associated with the ingress transmission path of Sync messages. P2P TCs allow a faster reconfiguration after network topology changes.

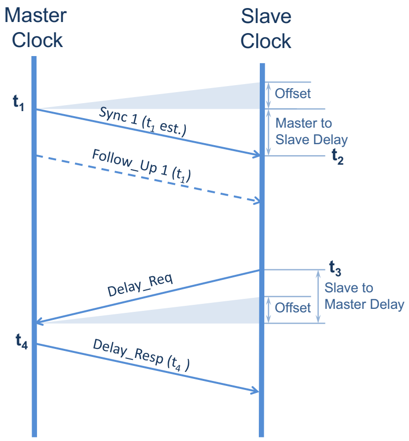


Fig. 4. Delay request–response mechanism message exchange pattern [26].

PTP firstly introduced security as an optional extension in Annex K of the second version of the standard. This Annex provides authentication, message integrity and replay protection using a new authentication Type-Length-Value (TLV) field that includes an Integrity Check Value (ICV), which is computed using symmetric HMAC functions. However, PTP security vulnerabilities have been studied during last years [29–31], which might lead PTP systems to different attacks ranging from Denial of Service (DoS) to selective packet delay attacks passing through clock manipulation by inserting, removing or modifying PTP packets. As a consequence, a slave clock could be forced to be aligned to a false time or interruptions of PTP protocol could be occasioned, causing failures and wrong operation of substation control systems.

The 1588 committee is now working on the third edition of the standard. Concretely, the security subcommittee is immerse in specifying the PTP security solution taking into account the security requirements defined in the RFC 7384 [32]. Both a specific security mechanism integrated in PTP protocol and the utilization of external security solutions are being considered in the standardization process.

5.2. High availability communication networks in substations

Apart from precise time synchronization, there are other critical issues in SAS such as the need for high available communication networks. For instance, no traffic interruption is allowed for busbar protection functions in case of link failure. IEC 61850-90-4 considers the Rapid Spanning Tree Protocol (RSTP), the Parallel Redundancy Protocol (PRP) and the High-availability Seamless Redundancy (HSR) for IEC 61850-8-1 and IEC 61850-9-2 substation communications. The ideal scenario is that providing seamless redundancy, with zero switch-over time and no frame losses, and this can be achieved using both HSR and PRP [33]. RSTP does not provide seamless recovery but recovers fast enough for most applications that use the station bus.

In this section, both PRP and HSR are considered, as defined in IEC 62439-3 standard [34]. On the one hand, the PRP protocol uses a completely doubled network topology and Doubled Attached Nodes (DANs) as network interfaces. DANs send and receive all network traffic over both networks all at once. Frame duplication, that is duplicate detection and removal, is handled by protocol interfaces in a completely transparent way to the rest of devices [35]. On the other hand, HSR protocol only needs one additional link to build a ring topology where DANs are daisy-chained. The sender sends two copies of the Ethernet frame in both directions of the ring and the destination passes the first arrived frame to the upper layers, while the second one is discarded.

The topology of substation communication networks may differ depending on the physical location of IEDs as a consequence of electrical primary equipment configuration. Normally, a group of IEDs per bay is attached to a bridge as shown in Fig. 1, although exceptions with IEDs serving several bays are also possible. Thus, the interconnection of IEDs in substations vary from a star topology to a daisy-chain or a ring. With the aim of increasing the resiliency of the substation network, it can be segmented into multiple redundancy domains (e.g. two separate redundancy domains for station and process bus separated through a bridge with multicast filtering). In Fig. 6, the block diagram of PRP/HSR nodes and PTP clocks of a complex substation is represented. A double Local Area Network (LAN) network is used on the station bus, which consists of two RSTP rings. The process bus is a HSR

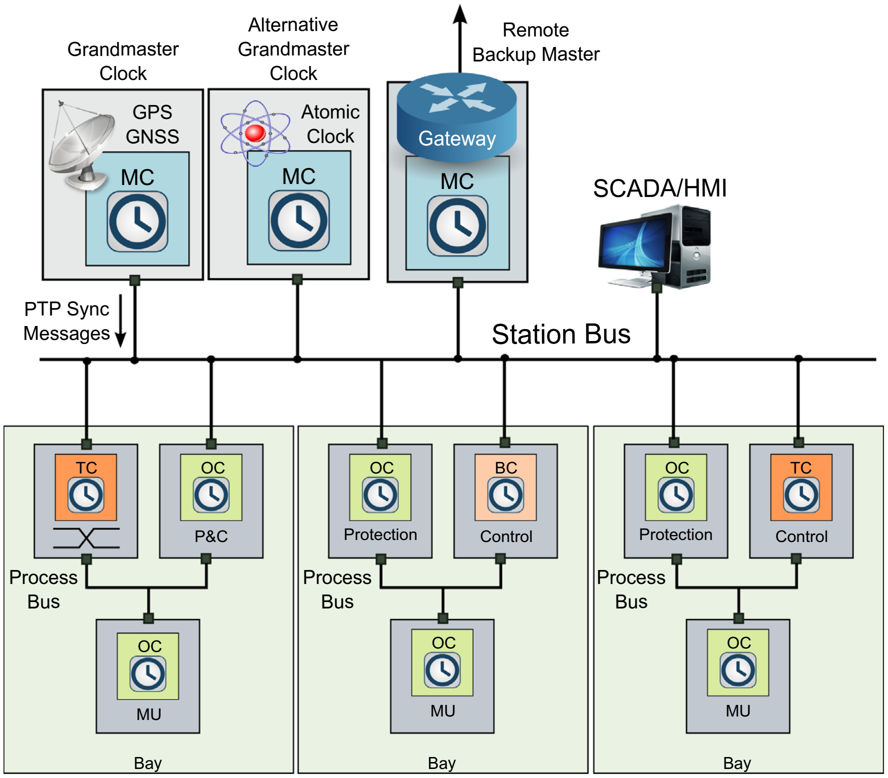


Fig. 5. Example of a PTP network within the substation [11].

ring per each bay. In small substations, also HSR could fit in the station bus.

In order to couple non-redundant network nodes, such as a Grandmaster clock or the substation gateway, and couple PRP and HSR networks, Redundancy Boxes (RedBoxes) are used. In the example network in Fig. 6, there are two RedBoxes in each bay: RedBox A couples the orange RSTP ring in the station bus with the HSR ring in the process bus, while the RedBox B couples the green one with the same HSR ring. Although RedBoxes can also be TCs, in this case they are BCs and they are treated as redundant clocks in the HSR ring. This means that only one of them sends Sync messages. Otherwise, in case they were TCs, they would inject four Sync messages with the same sequence number into the HSR ring. HSR end nodes in the process bus have an Hybrid Clock (HC) that is a combination of a TC and an OC.

5.3. *Incompatibility issues between communication protocols in substations*

PRP and HSR assume some principles about message propagation over the network that are quite incompatible to PTP [36,37]. Annex A of IEC 62439-3 [34] defines how redundant PTP messages must be handled. This Annex also specifies that PTP messages must be directly transported in multicast Ethernet frames and Peer-to-Peer (P2P) TC functionality must be included in intermediate nodes. The P2P TC is a type of transparent clock that use the peer delay mechanism to measure the link delay and update the *correctionField* with both the residence time and the link delay associated with the ingress transmission path of Sync messages.

The IEC SC 65C subcommittee has continued working on these incompatibility issues and on a new edition of IEC 62439-3 standard, which is expected to be released in 2015. From the draft of this third edition, it can be concluded that a new PTP profile for Power Systems is emerging from IEC groups, named Utility profile and specified as an Annex. Consequently, the existence of two different PTP profiles for Power Systems, the Power Profile defined in IEEE C37.238 standard [27] and this Utility Profile, arises a new incompatibility problem. Since the Utility Profile also considers the utilization of redundancy protocols, IEC and IEEE recently agreed on the utilization of the Utility Profile for SAS. In the near future, the definition of this unique profile will be moved from IEC SC 65C to IEC TC57 WG10 and it will be published as the IEC 61850-9-3 standard.

In [38], authors firstly implemented a full hardware solution with IEC 62439-3 and IEEE 1588 support. They demonstrated to be cost effective and fast. In the worst case, the propagation delay through a HSR ring would be the product of each node bridging delay by the number of nodes. Since this delay must be acceptable for time critical messages in SAS, IEC 62439-3 estimates that each node in the HSR ring should forward the frames within 5 μs, when there is no other traffic, so a cut-through bridging is suggested. Even though cut-through switching is implemented, where the frame is forwarded before it is entirely received, only the average forwarding delay is improved. In the worst case of all nodes injecting a maximum size frame at the same time, the overall propagation delay would not experience any reduction. In order to overcome this problem and fully exploit the cut-through properties, a pre-allocated time window would restrict the nodes to send frames in particular moments and hence, a common precision clock is needed.

However, the utilization of PTP in secured HSR networks implies that all nodes in the ring must recalculate the authentication code while the message passes through the nodes, in order to consider changes in *correctionField*. P2P TC functionality modifies the content of this field by adding the residence time and the link delay and, therefore, cryptographic units in ingress and egress ports must respectively verify and recalculate security checksums that protect the integrity of PTP messages. In fact, the main drawback of implementing security mechanisms in substation redundant networks is the increased propagation delays of

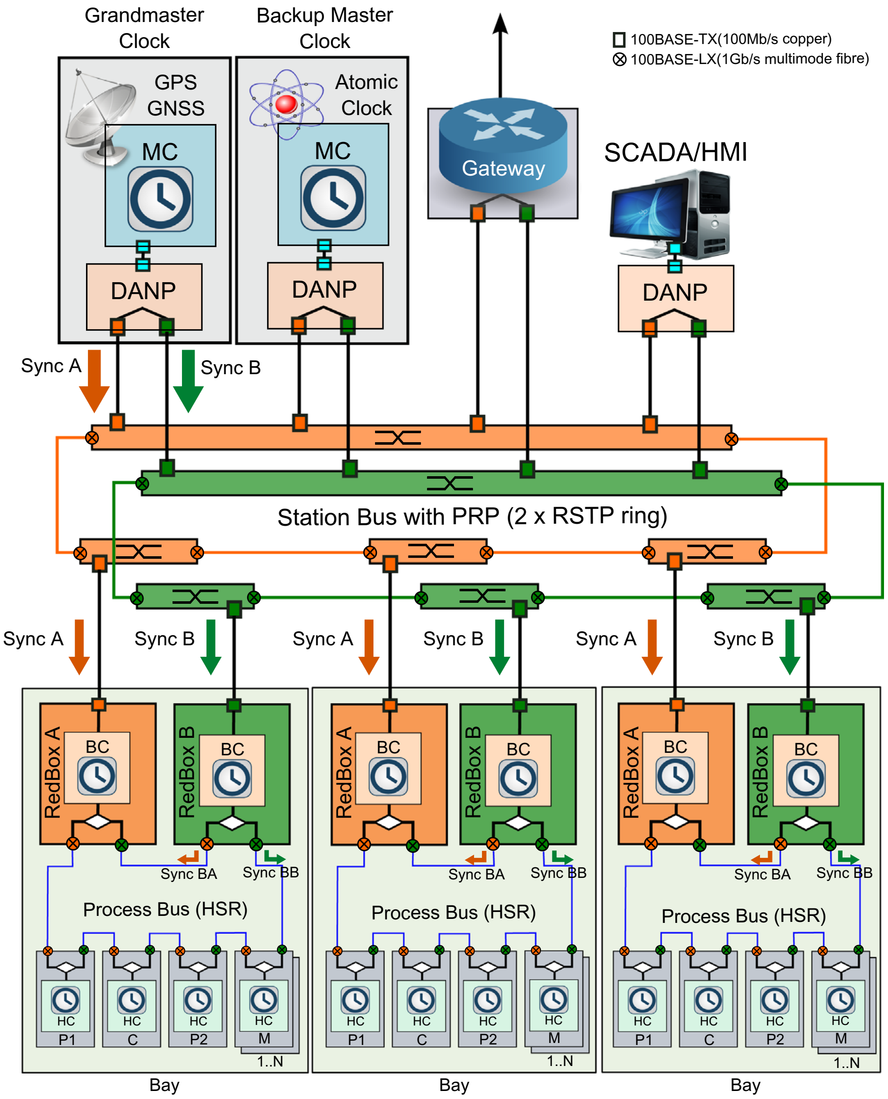


Fig. 6. Station and process bus with redundancy and synchronization [11]. (For interpretation of the references to colour in this figure, the reader is referred to the web version of this paper.)

packets, which should be considered and minimized. Otherwise, GOOSE or SV messages will suffer long transfer times that will not meet timing requirements.

6. The future of cyber-security in SAS

Since the security mechanisms specified in both IEC 62351-6 and Annex K of IEEE 1588-2008 standards have been demonstrated to be suboptimal, a dramatic change should be carried out in future versions. On the one hand, the use of digital signatures to protect GOOSE and SV messages is computationally expensive and presents long execution times that are not permissible for time critical applications. IEC is currently considering the utilization of symmetric cryptography and GDOI protocols to protect communications within the substation as mentioned in Section 4. To provide source authenticity using symmetric cryptography, authors in [20] proposed the utilization of Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol, where each key is valid for sending during a limited time interval and, once this time expires, the key is delivered to destination nodes.

On the other hand, Annex K of IEEE 1588-2008 standard presents several vulnerabilities that have been analysed in the literature, as stated in Section 5.1. The third edition of the standard, on which 1588 working group is now intensively working, will include a set of security mechanisms to be used individually or in combination to address security requirements of each particular specific application. A new TLV-based security mechanism to be integrated into PTP messages will be defined to provide end-to-end security, whereas the utilization of external security protocols like MACsec [39] has been considered to provide hop-by-hop security required by messages that must be modified in transit.

Rather than specifying an independent security mechanism to each communication service in SAS, in order to save computational resources in restricted IEDs, the utilization of a common security framework to protect all substation communications should be considered in future versions of standards. However, different types of traffic in SAS should meet different timing requirements, as well as different security requirements. Before continuing with the specification and development of a new security solution for SAS communications, it is worth performing a preliminary study about how Information Technology (IT) security solutions might help to fulfil them. Fig. 7 shows available security protocols and standards in the Open Systems Interconnection (OSI) model that provide security services on each layer independently. Security services offered by these security suites are very similar and also the cryptographic mechanisms they use are often the same. However, they differ in the applicability scope: while TLS provides security at application and transport layers, network and data link layers are protected by IPsec and MACsec respectively.

Table 3 summarizes the general security requirements for different communication services found in substations. Apart from the three communication models described in Section 3, also PTP synchronization service is included. In fact, PTP messages have been classified into two categories. While peer-to-peer (P2P) PTP messages are those involved in the peer delay mechanism and exchanged between peer nodes, end-to-end (E2E) PTP messages are those addressed from the master to the slave through the network.

TLS was already considered by IEC 62351-6 standard to provide end-to-end authentication of MMS-based client–server communications, as mentioned in Section 4. IPsec and MACsec, in contrast, have not been considered to protect substation communications yet. When their applicability to SAS is analysed, they show some drawbacks. While IPsec provides a great security solution in almost all IT applications, it is limited to data traffic that is transported over IP at network layer. In the case of real time communications within the substation, all events need to be rapidly handled not to lose information and data is transported directly over Ethernet at link layer, as it has been seen in Section 3. Therefore, security at network layer is not feasible. On the other hand, MACsec provides hop-by-hop integrity and authenticity, but not end-to-end source authenticity. Moreover, since each node in the path has to verify the integrity and authenticity of the message in the reception, and regenerate the authentication code in the transmission, long latencies could be introduced in cascaded topologies such as star or ring network configurations.

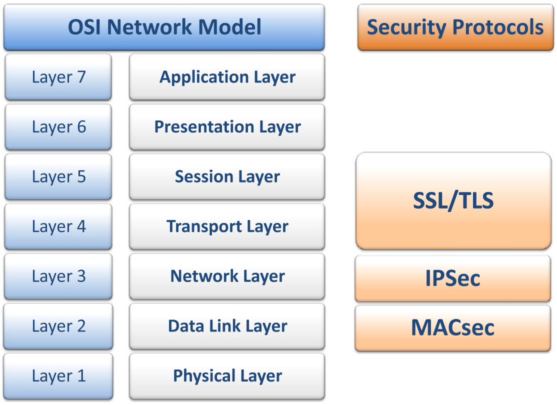


Fig. 7. Security protocols in the OSI model.

The common security framework should consider a hybrid solution with hop-by-hop group authentication and integrity protection using symmetric cryptography and end-to-end source authentication using efficient cryptographic methods. Data that is not modified by TC functionality in network nodes should not rise a problem if a suitable key management scheme is used and symmetric cryptographic algorithms are efficiently implemented in end nodes. The real challenge is the integration of a hop-by-hop security solution without compromising the SAS performance. In fact, one of the main problems of deploying secured and redundant substation networks is the increased propagation delays of packets due to cryptographic units in TCs: since they modify the content of PTP messages, they must recalculate the associated security checksums before retransmitting the messages. At the same time, the need for the participation of intermediate nodes makes difficult the management and distribution of cryptographic keys.

7. MACsec based security approach for SAS

MACsec provides hop-by-hop security, so each node in the path has to verify the integrity and authenticity of the message in the reception block, and regenerate the MAC in the transmission block. Hence, long latencies could be introduced in substation ring network configurations. In order to minimize the impact of security mechanisms on propagation delays, traffic separation could be performed in HSR nodes. According to substation security requirements summarized in Section 6 two different logical paths to be implemented have been identified:

1. A *fast logical path* with cut-through switches and cryptographic units only within end nodes for time critical messages protected by end-to-end security mechanisms, which are out of scope of this work.
2. A *robust logical path* with possible store-and-forward switches and optimized cryptographic units in all nodes for messages that are not time critical but must be modified in transit by hop-by-hop security mechanisms.

MACsec could provide hop-by-hop security for the robust path, using either pairwise or group keys. MACsec frames are identified by the Ethertype (0xh‘88E5) and they include a security tag, called SecTAG, and an Integrity Check Value (ICV), as shown in Fig. 8 [39]. These parameters are employed by the MACsec entity, named SecY, to decide if frames received from the common port must be forwarded through the controlled port and check/compute the ICV

Table 3
Summary of security requirements for SAS communication services.

Security requirements	Communication services in SAS					Security protocols		
	MMS	GOOSE	SVs	E2E PTP	P2P PTP	TLS	IPsec	MACsec
Source authentication	MUST	MUST	MUST	MUST	–	×	×	–
Group authentication	–	–	–	MUST	MUST	–	–	×
Hop-by-hop integrity	–	MAY	MAY	MUST	MUST	–	–	×
End-to-end integrity	MUST	MUST	MUST	MUST	–	×	×	–
Confidentiality	MUST	–	–	–	–	×	×	×
Unicast key management	MUST	–	–	SHOULD	–	×	×	–
Multicast key management	–	MUST	MUST	SHOULD	SHOULD	–	–	×

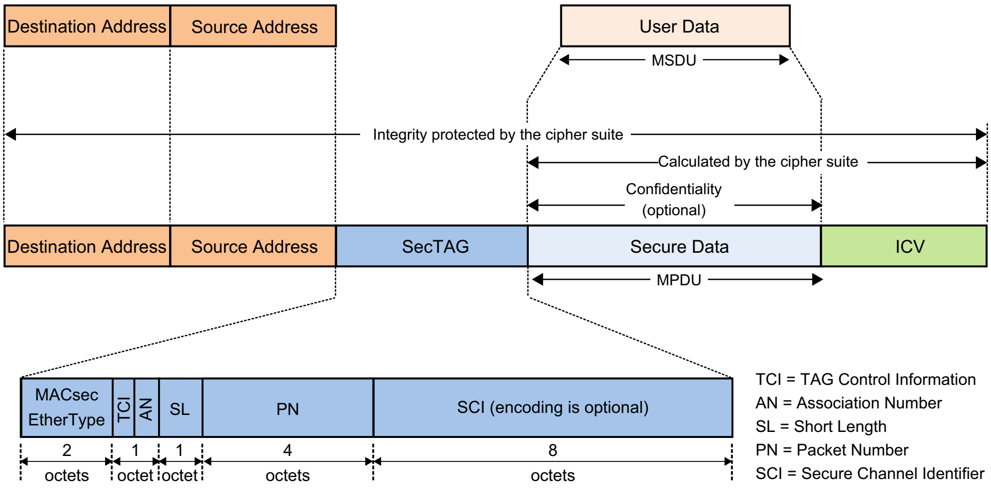


Fig. 8. MACsec frame format.

if needed.[1] Frames discarded by the SecY are delivered through the uncontrolled port to upper layers in order to be used by other protocol entities, such as key management applications.

In this proposal, cryptographic units across the robust path implement SecY functionality in hardware. They must also filter and reroute time critical messages through the fast logical path, so as not to apply cryptographic algorithms and maintain short processing times. MACsec standard specifies several processing rules to discard frames in the controlled port and, therefore, neither secure frame verification nor generation processes are performed in the SecY. For example, frames with an Ethertype other than 0xh'88E5', such as key agreement frames, are discarded in the controlled port. In this case, GOOSE and SV messages would be transmitted with an Ethertype=0xh'892F' within the HSR tag immediately after the source address, and without SecTAG-ICV fields. In intermediate nodes, frames discarded by ingress SecY entities in the controlled port will be forwarded through the uncontrolled port to the HSR switch and SecY will only forward valid frames through the controlled port without the SecTAG-ICV. Therefore, the HSR switch must not have to be MACsec-aware, since frames arrive as normal HSR frames.

Software support is also needed for MACsec, since the protocol relies on the IEEE 802.1X standard [40] to authenticate stations against an authentication server and dynamically establish and manage secure relationships.

8. Conclusions

In this paper, the protection of substation communications is outlined. On the one hand, the communication model and the related families of standards have been presented to understand the problem of securing information that is exchanged between participants in such substation communications. Concretely, real time communications in substations need minimum delays introduced by IEDs and network elements which, at the same time, have limited resources. IEC 62351 proposed the utilization of SHA-based MACs with symmetric encryption to provide authenticity and integrity protection of GOOSE messages and SVs in substations. Confidentiality is not provided due to real time requirements. However, using symmetric encryption only provides group authentication as described in Section 6, and therefore, the current version of the standard demands these MACs should be digitally signed using asymmetric encryption. Since digital signatures are computationally expensive, they have been demonstrated to be suboptimal in substation communications. Hence, another alternatives for source authenticity will have to be included in future versions of the standard.

On the other hand, the applicability of common security protocols in the OSI model have been considered. While TLS and IPsec are the most extended security solutions in almost all communication systems, in substations, they have a limited use because they work above Layer 3 in the OSI model and need unreasonable resources that field devices do not necessarily accomplish. Considering that the tendency is to gather all substation communications over the same Ethernet network, the use of hop-by-hop security as defined in MACsec could be advantageous in some cases. That is not the case for GOOSE/SVs messages that cannot present long transfer times due to encryption units in network nodes. But, for PTP messages that must be modified by intermediary nodes to take into account the propagation delay, it could be an appropriate solution.

In this sense, it is very important to study how the combination of all these different types of traffic, and the used cyber-security mechanisms, affect the performance of real time communications in substations. In order to save computational resources, using a common security framework to protect all SAS communications seems to be the necessity in future deployments. This framework should consider a hybrid solution that could involve hop-by-hop group authentication using symmetric encryption for traffic that must be modified in transit, in conjunction with source authentication for end-to-end communications using key chains for example. Since intermediary nodes will behave different depending on the message destination scope, they need to perform a proper traffic separation. A novel approach based on MACsec protocol has been introduced in the article to separate end-to-end traffic and protect the robust path in substation communications.

New hardware architectures for substation nodes should be developed making the most of new technologies, such as last generation FPGAs. FPGAs allow low-latency, flexible and scalable designs to address strict requirements in SAS and provide the ability to adapt to future versions of standards that are under construction. Furthermore, FPGA technology is moving forward to the next level to provide cost-affordable System-On-Chip devices. For instance, Zynq device by Xilinx consists of a double core Cortex-ARM9 processor with powerful peripherals (Gigabit Ethernet, memory controllers, etc.) in a single chip. Such a powerful

[1] The mandatory cipher suite in the standard is the Galois Counter Mode of Operation with the AES-128 symmetric block cipher (AES-128-GCM), and there is an amendment to use the AES-256 block cipher (AES-256-GCM).

platform enables to the power industry and the research community new possibilities in the field of substation communication networks, since both hardware and software designs might be directly developed and tested on target device at the same time. Future work needs to concentrate on implementing SoC IED architectures with MACsec support and analysing the performance results deeply. Particularly, the effect of MACsec cryptographic units on PTP performance should be tested, as well as the operation of traffic separation techniques to minimize GOOSE and SV message propagation delays.

Acknowledgements

This work has been supported by the Ministerio de Economía y Competitividad of Spain within the project TEC2014-53785-R and it has been carried out inside de Research and Education Unit UFI11/16 of the UPV/EHU and partially supported by the Basque Government within the fund for research groups of the Basque university system IT394-10 and within the project TFactory ER-2014/0016. Also, FEDER funds and UPV/EHU Ph.D. scholarship funding are acknowledged.

References

[1] Poulsen K. Slammer worm crashed Ohio nuke plant network. Online. URL ⟨http://www.securityfocus.com/news/6767⟩; August 2003.

[2] Kushner D. The Real Story of Stuxnet. IEEE Spectr 2013;50(March (3)):48–53.

[3] Ericsson G. Cyber security and power system communication-essential parts of a smart grid infrastructure. IEEE Trans Power Deliv 2010;25(July (3)):1501–7.

[4] Cleveland F. IEC 62351 security standards for the power system information infrastructure. White paper, ver. 14. International Electrotechnical Commission; June 2012.

[5] ETP SmartGrids. The SmartGrids European technology platform. Online. URL ⟨http://www.smartgrids.eu/ETPSmartGrids⟩.

[6] Kanabar M, Voloh I, McGinn D. Reviewing smart grid standards for protection, control, and monitoring applications. In: Proceedings of IEEE PES innovative smart grid technologies conference; January 2012. p. 1–8.

[7] ABB review special report IEC 61850, Technical report; August 2010.

[8] Brand K, Lohmann V, Wimmer W. Substation automation handbook. Utility automation consulting Lohmann; 2003.

[9] Sidhu T, Gangadharan P. Control and automation of power system substation using IEC61850 communication. In: Proceedings of IEEE conference on control applications; August 2005. p. 1331–6.

[10] IEC 61850-1 Standard ed2.0. Communication networks and systems for power utility automation—Part 1: Introduction and overview; March 2013.

[11] IEC 61850-90-4 Standard ed1.0. Communication networks and systems for power utility automation—Part 90-4: Network engineering guidelines; August 2013.

[12] IEC 61850-8-1 Standard ed2.0. Communication networks and systems for power utility automation—Part 8-1: Specific communication service mapping (SCSM)—mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3; June 2011.

[13] IEC 61850-9-2 Standard ed2.0. Communication networks and systems for power utility automation—Part 9-2: Specific communication service mapping (SCSM)—sampled values over ISO/IEC 8802-3; September 2011.

[14] ISO 9506-1 Standard ed2. Industrial automation systems—manufacturing message specification; August 2003.

[15] McGhee J, Goraj M. Smart high voltage substation based on IEC 61850 process bus and IEEE 1588 time synchronization. In: Proceedings of the IEEE international conference on smart grid communications (SmartGridComm); 2010.

[16] Fuloria S, Anderson R, McGrath K, Hansen K, Alvarez F. The protection of substation communications. In: Proceedings of SCADA security scientific symposium; January 2010. p. 1–13.

[17] Introduction to waterfall unidirectional security gateways: true unidirectionality, true security. Technical report. Waterfall Security Solutions Ltd.; August 2012.

[18] IEC/TS 62351-1 Standard ed1.0. Power systems management and associated information exchange—data and communications security—Part 1: Communication network and system security—introduction to security issues; May 2007.

[19] IEC/TS 62351-6 Standard ed1.0. Power systems management and associated information exchange—data and communication security—Part 6: Security for IEC 61850; June 2007.

[20] Fries S, Falk R. Security considerations for multicast communication in power systems. Int J Adv Secur 2013;6(3–4):111–21.

[21] Weis B, Rowles S, Hardjono T. RFC 6407: the group domain of interpretation; October 2011.

[22] Dierks T, Allen C. RFC 2246: the TLS protocol version 1.0; January 1999.

[23] U.S.-Canada Power System Outage Task Force. Final report on the August 14th blackout in the United States and Canada: causes and recommendations. Technical report; April 2004.

[24] Steinhauser F, Riesch C, Rudigier M. IEEE 1588 for time synchronization of devices in the electric power industry. In: Proceedings of the international IEEE symposium on precision clock synchronization for measurement control and communication (ISPCS); October 2010. p. 1–6.

[25] NIST Special Publication 1108. Framework and roadmap for smart grid interoperability standards, release 1.0; January 2010.

[26] IEEE 1588-2008 standard for a precision clock synchronization protocol for networked measurement and control systems; July 2008.

[27] IEEE C37.238-2011. Standard profile for use of IEEE 1588 precision time protocol in power system applications; July 2011.

[28] Moreira N, Astarloa A, Lazaro J, Garcia A, Ormaetxea E. IEEE 1588 transparent clock architecture for fpga-based network devices. In: Proceedings of the IEEE international symposium on industrial electronics (ISIE); May 2013. p. 1–6.

[29] Treytl A, Gaderer G, Hirschler B, Cohen R. Traps and pitfalls in secure clock synchronization. In: Proceedings of the international IEEE symposium on precision clock synchronization for measurement, control and communication; October 2007. p. 18–24.

[30] Treytl A, Hirschler B. Security flaws and workarounds for IEEE 1588 (Transparent) clocks. In: Proceedings of the international symposium on precision clock synchronization for measurement, control and communication; October 2009. p. 1–6.

[31] Onal C, Kirrmann H. Security improvements for IEEE 1588 Annex K: implementation and comparison of authentication codes. In: Proceedings of the international IEEE symposium on precision clock synchronization for measurement control and communication; September 2012. p. 1–6.

[32] Mizrahi T. IETF RFC 7384 security requirements of time synchronization protocols in packet switched networks; 2014.

[33] Kirrmann H, Weber K, Kleineberg O, Weibel H. Seamless and low-cost redundancy for substation automation systems (high availability seamless redundancy, HSR). In: Proceedings of the IEEE power and energy society general meeting; July 2011. p. 1–7.

[34] IEC 62439-3 ed2.0. Industrial communication networks—high availability automation networks—Part 3: Parallel redundancy protocol (PRP) and high-availability seamless redundancy (HSR); July 2012.

[35] Araujo J, Lazaro J, Astarloa A, Zuloaga A, Moreira N. Duplicate and circulating frames discard methods for PRP and HSR (IEC62439-3). In: Proceedings of the IEEE conference on industrial electronics society (IECON); November 2013. p. 4451–6.

[36] De Dominicis C, Ferrari P, Flammini A, Rinaldi S, Quarantelli M. On the use of IEEE 1588 in existing IEC 61850-based SASs: current behavior and future challenges. IEEE Trans Instrum Meas 2011;60(September (9)):3070–81.

[37] Abdul A, Ng G, Lupas P. Integration of HSR and IEEE1588 over Ethernet networks. In: Proceedings of the international IEEE symposium on precision clock synchronization for measurement control and communication (ISPCS); September 2010. p. 77–82.

[38] Kirrmann H, Honegger C, Ilie D, Sotiropoulos I. Performance of a full-hardware PTP implementation for an IEC 62439-3 redundant IEC 61850 substation automation network. In: Proceedings of the international IEEE symposium on precision clock synchronization for measurement control and communication (ISPCS); September 2012. p. 1–6.

[39] IEEE 802.1AE-2006. Standard for local metropolitan area networks: media access control (MAC) security; 2006.

[40] IEEE 802.1X-2010. Standard for port-based network access control; February 2010.