Article

MACsec Layer 2 Security in HSR Rings in Substation Automation Systems

Jesús Lázaro [*,†], Armando Astarloa, José Angel Araujo, Naiara Moreira and Unai Bidarte

Universidad del País Vasco/Euskal Herriko Unibertsitatea (UPV/EHU), 48013 Bilbao, Spain;
armando.astarloa@ehu.eus (A.A.); joseangel.araujo@ehu.es (J.A.A.); naiara.moreira@ehu.eus (N.M.);
unai.bidarte@ehu.eus (U.B.)

[*] Correspondence: jesus.lazaro@ehu.eus; Tel.: +34-946017344

[†] Current address: Plaza Ingeniero Torres Quevedo, 1, 48013 Bilbao, Spain.

Academic Editor: Josep M. Guerrero
Received: 9 November 2016; Accepted: 12 January 2017; Published: 31 January 2017

Abstract: The smart-grid concept takes the communications from the enclosed and protected environment of a substation to the wider city or nationwide area. In this environment, cyber security takes a key role in order to secure the communications. The challenge is to be able to secure the grid without impacting the latency while, at the same time, maintaining compatibility with older devices and non secure services. At the lower level, added security must not interfere with the redundancy and the latency required for the real-time substation automation communications. This paper studies how to integrate IEEE MAC Security standard (MACsec) in the substation environment, especially when used in substation system communications that have stringent response time requirements and zero recovery time as defined in IEC 62439-3.

Keywords: smart-grid; industrial communication; substation automation; cryptography

1. Introduction

Smart grids are gaining more and more importance in the electricity sector. One part of the electric distribution smart grid network is the automation network in substations, governed by the IEC 61850 [1]. It helps to secure the interconnection and interoperability of devices made by several different manufacturers. Moreover, using and integrating local area network (LAN) in industrial systems and using Ethernet and TCP/IP technologies allows offices to be interconnected with automation networks, which provides business resource planning systems with industrial process data for operational and decision-making purposes. Ethernet offers high throughput and has a dominant position in the LAN technologies. However, using Ethernet for industrial automation networks involves adding new, strict requirements and dealing with new challenges [2].

The introduction of standard communication protocols and mediums has also increased the need for greater security [3–6]. It must be noted that the use of proprietary communication protocols is not a guarantee of security as the Stuxnet attack on Siemens proprietary devices [7,8] showed. In the effort to make the smart-grid cyber secure, the IEC 62351 standard [9] introduces mechanisms to guarantee end-to-end security. Specifically, part 6 is dedicated to security for IEC 61850 profiles.

This security mechanism works modifying some reserved fields of the standard frame and adding an authentication tag using RFC 2104 [10], RFC 2437 [11] and RFC 3174 [12]. This standard requires the modification of all end equipment that requires security while, at the same time, maintains compatibility with non-secure devices. Besides substation automation communications, it does not introduce any security mechanism for other protocols that may exist for the correct functioning of the device, such as synchronization or configuration [13,14]. The complex security scheme introduces big delays that may render this standard not useful [15] in some approaches, especially the asymmetric cryptography required. Substation automation requires 3 ms latency at most, and even high-end processors such as the 32-bit cores from Intel and ARM cannot in general compute and verify a digital signature using RSA with 1024-bit keys within 3 ms. For example, an RSA 1024-bit private key signature operation takes 8 ms on a single 1.7 GHz Intel core using the OpenSSL library.

This paper focuses on the use of IEEE MAC Security 802.1AEstandard [16] as a way of securing the communication at the lowest possible level (see Figure 1). This point-to-point securization happens at level 2, and this means that higher level protocols or applications are completely unaffected by the security protocol. At the same time, the use of this standard does not mean that IEC 62351 should not be used, and both can coexist at the same time. IEC 62351 is focused on end-to-end security of the substation automation protocols while 802.1AE is in charge of securing communication in every Ethernet connection. The proposed approach is interesting when legacy devices are used or when we want to secure other protocols apart from IEC 61850. An interesting point is that, since the use of redundancy protocols requires the use of specialized switches, security may be added at the same time without the need of already changing working devices.

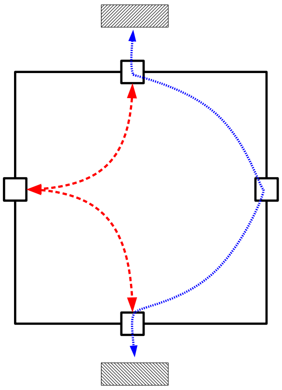

Figure 1. IEC 62351 end-to-end security (short dashed line) and 802.1AE point-to-point security (long dashed line).

2. Background Information

2.1. IEC 61850 Security Considerations

IEC 61850 substations provide several advantages over traditional ones. Nevertheless, one of the problems of a highly connected substation are the cybersecurity requirements. There are several possible attacks [17], for example:

- Attacks on IEC 61850
    - Denial of Service (DoS) Attacks: the effect of a DoS attack to an IEC 61850 substation network is the disruption to the availability of the network in the substation. Availability in the substation is disrupted by disabling and shutting down the IED operation [18,19].
    - Password Cracking Attacks: the purpose of this attack is for the attacker to gain unauthorized access to a system or device.
    - Packet Sniffing Attacks: when the packet sniffing attack is launched within the IEC 61850 substation network, the attacker will gain the ability to steal transmitted data and perform certain attacks such as the man-in-the middle attack.
- Attacks on GOOSE and Sample Values (SV)
    - GOOSE and SV Modification Attack: In [20], an attack is proposed. In this attack, the GOOSE control message packet is captured and then modified with a message that will allow the attacker to gain control and operate circuit breakers in a substation. For an SV packet,

an attacker could generate a fabricated analog value, and this value is sent to a control center in a substation that leads to undesirable operations. This attack will enable the attacker to gain control of IEDs and cause unplanned power outage or even damage the substation field devices.

- GOOSE and SV DoS Attacks: a DoS attack will cause an IED to stop responding to legitimate requests made by other IEDs. This will prevent the IED from performing its intended function and may lead to many other consequences such as power failure and equipment damage. A DoS attack can be conducted in several ways. The simplest way is to just send a large number of GOOSE or SV messages to an IED so that it becomes overwhelmed and no longer able to respond to legitimate requests.
- GOOSE and SV Replay Attack: in a reply attack, the GOOSE messages used to send this tripping signal is captured and kept by the attacker. The attacker would then send the exact same message to cause the circuit breaker to trip when it is not supposed to. This will cause an unintentional power outage. For SV message replay attack, the attacker can capture an SV packet containing a certain power and voltage values, and then replay this same SV packet to other IEDs in the substation multiple times. SV packets with the same power and voltage values circulating inside the substation can lead to undesirable operation.

As mentioned, IEC 61850 [1] includes security mechanisms. The standard addresses several information security aspects for power systems control operations. The aim is to provide confidentiality, integrity, availability and non-repudiation in a system.

Part 6 of the standard deals with the security in generic object oriented substation events (GOOSE) and sample values (SV). The extension is intended to authenticate a protocol data unit (PDU) by containing a signed hash of the PDU. The main issue is that some applications within IEC 61850 require response times of 4 ms, and IEC 62351-6 does not recommend encryption for these applications as the cryptographic overhead might already incur delays of more than 4 ms [21]. This, in turn, makes the security standard not usable in the most demanding applications.

Studies by ABB Switzerland [22] state that the only way to get to the desired level of speed would be the use of RSA dedicated chips. Even with the use of this specialized hardware, the solution would not be available in the short- or mid-term. Fuloria et al. [15] show different cryptographic chips and their performance. One interesting point is that there is not a great availability of them, and reliance on a single product would exacerbate concerns about competition, pricing and lock-in. Apart from that, some of them are also strictly export-controlled.

In Table 1, different RSA chips are described. Fuloria et al. [15] further describe problems of similar chips, and this table has new chips that offer higher speeds but are focused onPCIe cards for servers. A typical product could be SUN Crypto Accelerator 6000 PCIe card, not so much dedicated hardware in a substation.

Table 1. RSA (Rivest-Shamir-Adleman) performance for different devices.

Device	1024 RSA Performance
SafeXcel-1741	119 op/sec sign, 1176 op/sec verify
SafeXcel-1841	1220 op/sec sign, 3790 op/sec verify
BCM5860	4600 op/sec
BCM5861	7000 op/sec
BCM5862	15,224 op/sec

2.2. High-Availability Seamless Redundancy

The IEC 61850 standard series for communications networks and systems for power utility automation establishes requirements in terms of real-time operation communications protocols and availability. Regarding the network infrastructure, the recently published IEC 61850-90-4 [23] has adopted Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), both defined in the IEC 62439-3 [24], as the preferred Ethernet-based protocols for Station Bus (SB) and Process Bus (PB) in substations. They provide hot-plugging, zero recovery time and frame loss protection in the case of a network failure.

HSR is based on sending two copies of every frame via two independent paths, so that, if one of them is lost, the other one arrives and there is no break in communication. The redundancy that has been introduced is in the Link layer of the Open System Interconnection (OSI) reference model. These protocols add a Link Redundancy Entity (LRE), which manages protocols, functions and frames transparently for the other layers, with which the interface is standard Ethernet. This feature allows the use of existing upper stack protocols and applications, which is required for the use of Ethernet for industrial automation networks in general [25].

The basic topology, a ring, uses two independent paths (clockwise and counterclockwise) as depicted in Figure 2. Double Attached Nodes (DANs) forward frames from one port to the other, unless they are the sole destination of the frame, or unless they have already sent the same frame in the same direction. HSR networks do not accept Single Attached Nodes (SANs) connected directly because they cannot forward frames; therefore, Redundancy Boxes (RedBoxes) become necessary. A RedBox is a three input switch, two of the ports are connected to the HSR ring while the third (called interlink) is connected to a standard Ethernet network. A key point in this kind of networks is that every node must eliminate duplicate and circulating frames. A duplicate is a frame that has already been received through a port in the destination node, while a circulating frame is one that has already been sent through a port and should not be sent again uncontrolled (for example, in a single ring, because it has lost its origin -multicast-, or origin and destination -unicast-).

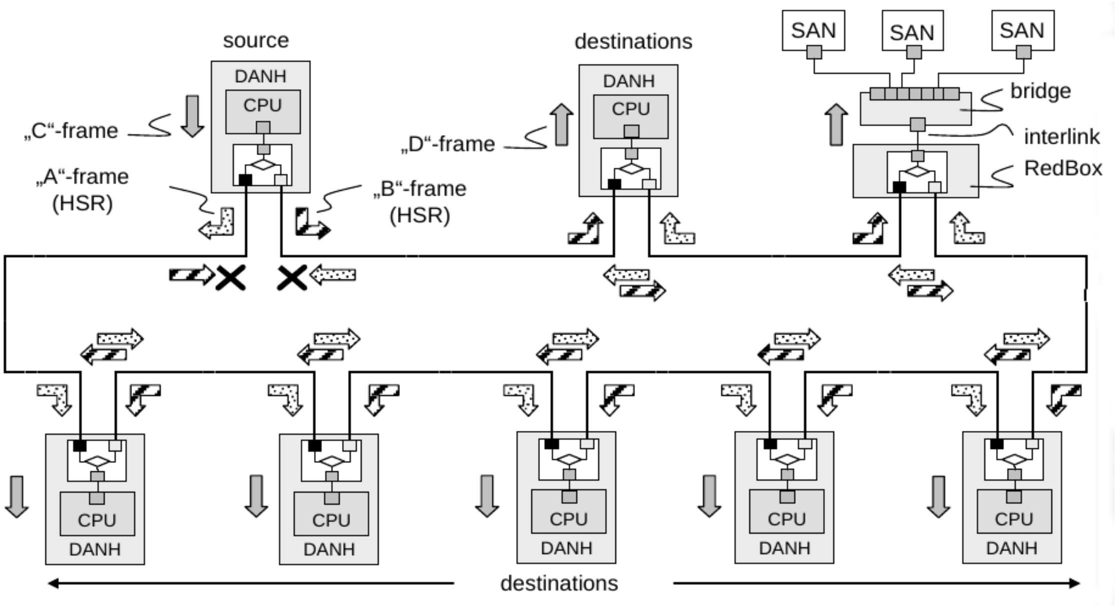

Figure 2. HSR (High-availability Seamless Redundancy) basic topology. Multicast frame example pictured.

The topology of substation communication networks may differ depending on the physical location of intelligent electronic devices (IED) as a consequence of electrical primary equipment configuration. Normally, a group of IEDs per bay is attached to a bridge, although exceptions with IEDs serving several bays are also possible. Thus, the interconnection of IEDs in substations varies 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 Figure 3, the block diagram of PRP/HSR nodes and precise time protocol (PTP) clocks of a complex substation is represented. A double LAN network is used on the station bus, which consists of two rapid spanning tree protocol (RSTP) rings. The process bus is an HSR ring per each bay. In small substations, HSRs could fit in the station bus.

In order to couple non-redundant network nodes, such as a Grandmaster clock or the substation gateway, and a couple of PRP and HSR networks, In addition, RedBoxes are used. In the example network in Figure 3, there are two RedBoxes in each bay: RedBox A couples the orange RSTP LAN 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.

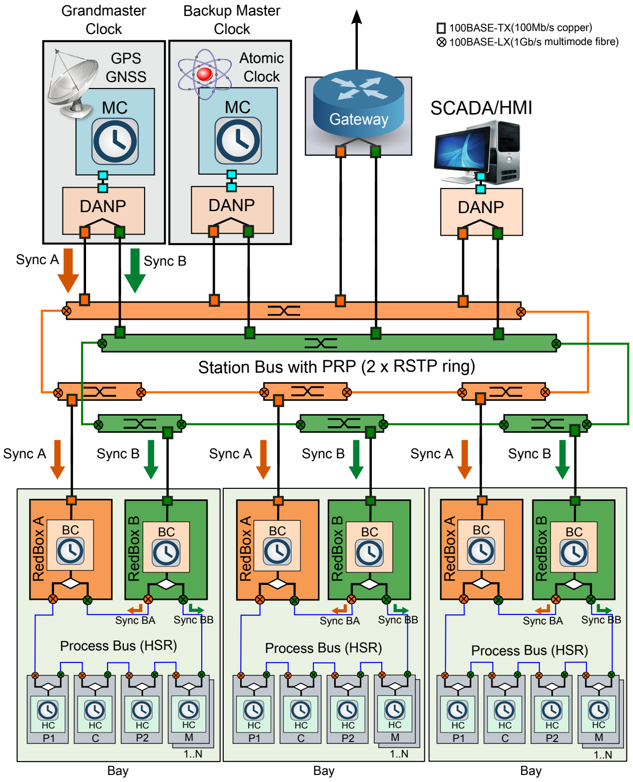

Figure 3. Station and process bus with redundancy and synchronization [23].

2.3. MACsec

There are several standards for securing and authenticating data in an Ethernet network. One of these standards is the IEEE MAC Security 802.1AE standard (also known as MACsec) [16], which defines connectionless data confidentiality and integrity for media access independent protocols. This is the only IEEE sponsored standard for authentication and encryption inside the 802.1 working group. MACsec is already in use in telecommunication infrastructure, and there is a lot of network equipment compatible with the standard.

One advantage of this standard is that it works at OSI Level 2, the same level that substation communications work. Key management and the establishment of secure associations is outside the scope of 802.1AE but is specified by 802.1X-2010. Since it works at Level 2, the rest of the protocols are completely unaffected.

The 802.1AE standard provides a way of securing MAC service to the client. The standard defines:

- MACsec frame format;
- Secure Connectivity Associations that represent groups of stations connected via unidirectional Secure Channels;
- Two ciphers that provide encryption and authentication at the same time: GCM-AES128 and GCM-AES-256 [26].

The MACsec frame format is depicted in Figure 4. The frame is composed of a security tag (SecTAG), the secured data and an integrity check value (ICV).

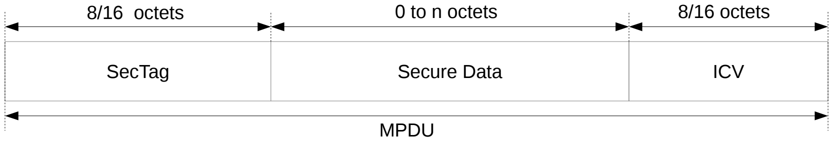

Figure 4. MACsec frame format.

The security tag (see Figure 5) is composed of the following fields:

- TCI: Tag Control Information. This field facilitates version numbering, determine whether confidentiality or integrity alone are in use, option inclusion, etc.
- AN: Association Number. It identifies up to four different secure associations within the context of a secure channel.
- SL: Short Length. This integer encodes the number of octets in the secure data field if that number is less than 48.
- PN: Packet Number. This field provides a unique initialization vector for all data transmitted using the same secure association, and, at the same time, it supports replay protection.
- SCI: Optionally encoded Secure Channel Identifier. This facilitates the identifications of the secure channel when there are three or more peers.

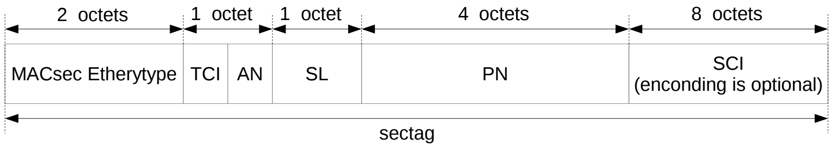

Figure 5. Security tag format.

This tag allows the coexistence of MACsec capable systems in the same environment as other systems. Concurrent operation of Key Agreement protocols is independent of the MACsec protocol and the Current Cipher Suite. It also allows non-secure and secure communications to make use of the same communication medium. The packet number is used as initialization vector for some operations of the cipher as well as replay protection support, that is, protect the system against the retransmission of a valid message.

In the context of substation automation, the replay protection is of key importance. There are two main types of messages across the network, SV and action messages (GOOSE). A retransmission of a SV frame out of context may lead the protection decision equipment to think that the current has dropped too quickly and take appropriate action. A retransmission of a trip message would lead the protection relay to open and cut electrical supply to a large area.

The Galois Counter Mode (GCM) encryption operation is defined by several equations [26]. Due to the internal structure of the algorithm, the decryption is done in the same way as encryption. A simplified diagram is depicted in Figure 6.

The tag that is computed by the decryption operation is compared to the tag associated with the message. If the two tags match (in both length and value), the message is returned as valid.

MACsec is a secure protocol provided the keys are managed correctly requiring a cautious deployment [27]. Another point to take into account is the security of the encryption algorithm. For now, the AES-GCM combination is considered safe [28] and is actively used in many scenarios such as IPsec Encapsulating Security Payload, TLS (transport layer security), Secure storage, fibre channel security and secure RTP (rapid spanning tree).

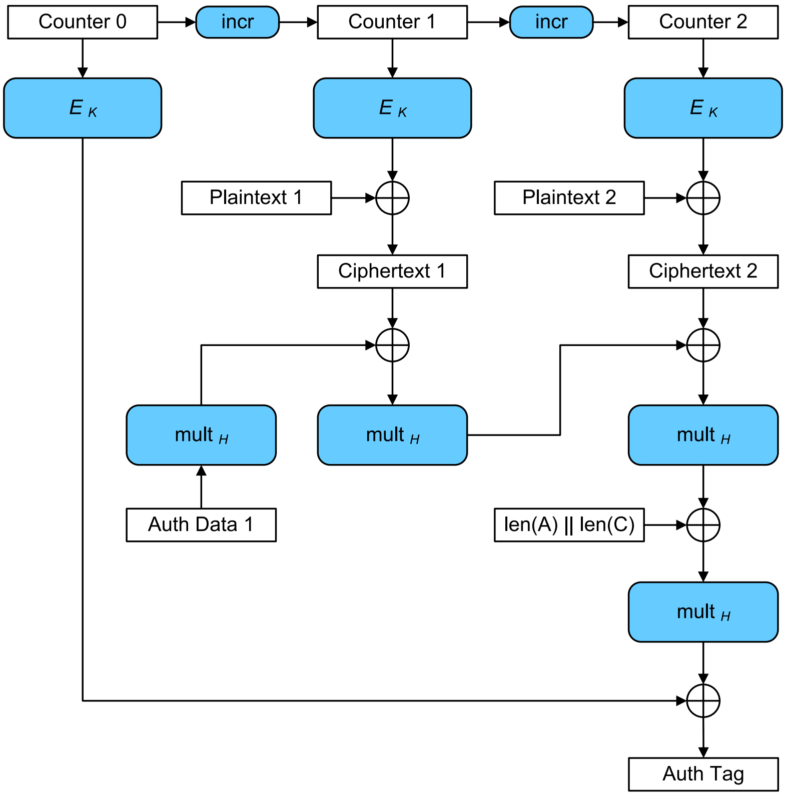

Figure 6. Galois Counter Mode encryption operation.

3. Communication Protection Alternatives

As we have previously seen, both HSR and MACsec embed a normal L2 packet into their payload. This presents a complication to the use of both protocols at the same time. Should we embed HSR into MACsec or MACsec into HSR? The following sections discuss these alternatives. One common and important point is the key distribution among all the elements in the network. MACsec states that key distribution is done using 802.1X-2010 [29] authentication.

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1X Extensible Authentication Protocol (EAP) framework. Only host facing links (links between network access devices and endpoint devices such as a PC or IP phone) can be secured using MACsec.

A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the client. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the client, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The switch compares that ICV to the ICV within the frame. If they are not identical, the frame is dropped. The switch also encrypts and adds an ICV to any frames sent over the secured port (the access point used to provide the secure MAC service to a client) using the current session key.

The MKA Protocol manages the encryption keys used by the underlying MACsec protocol. The basic requirements of MKA are defined in 802.1X-2010. The MKA Protocol extends 802.1X to allow peer discovery with confirmation of mutual authentication and sharing of MACsec secret keys to protect data exchanged by the peers.

3.1. HSR in MACsec

One way of solving this problem is to create a valid HSR frame and secure it using MACsec as in Figure 7. The ICV tag protects the whole message from the destination address to the payload.

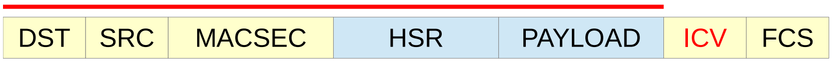

Figure 7. HSR frame embedded in MACsec frame. ICV (integrity check value) protects the whole frame.

This mechanism offers several advantages. First of all, the resulting frame fully complies with the 802.1AE, and this means that 802.1AE capable net equipment can deal with these frames (see Figure 8). Another interesting point is that all communication can be secured, if so desired. With this configuration, all attacks commented in Section 2.1 are defeated except for DoS. DoS attacks are more complicated to perform since the hardware in charge of 802.1AE will drop the attack packets; nevertheless, if the attack is capable of filling the Ethernet bandwidth, correct frames will not arrive even if the IED is capable of processing them.

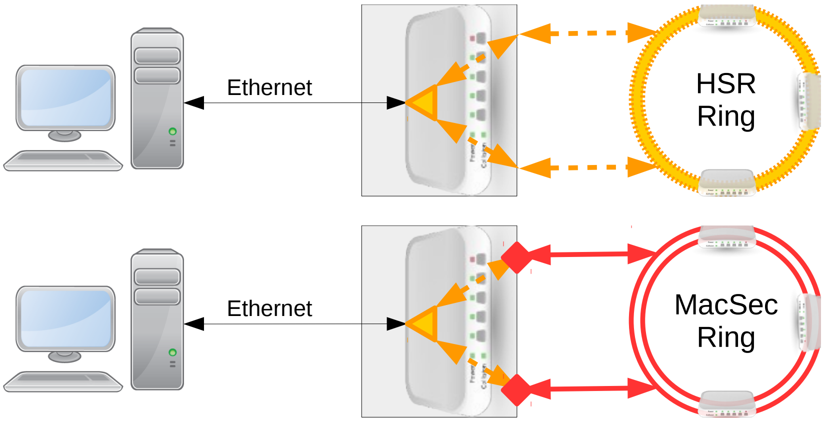

Figure 8. Standard DAN (top) and HSR in MACsec enabled DAN (bottom). Short dashed lines indicate standard HSR traffic. The MACsec header is included as the last element so the traffic in the ring is MACsec compliant.

The disadvantages are also clear. The use of legacy HSR switches, RedBoxes or DANs is prevented since they cannot understand the MACsec header. HSR switching requires MACsec processing, which will add latency as described in Section 4. For example, as can be seen in Table 2, the maximum number of elements can be halved.

Table 2. Maximum number of nodes for different communication protection according to maximum latency allowed by IEC 61850 in Cut Through mode for Fast Ethernet and (Gigabit Ethernet).

	t_{3Min}	t_{3SV}	t_{3Max}
MACsec in HSR	289 (2885)	41 (404)	5 (48)
Signed HSR in MACsec	179 (1786)	38 (372)	5 (48)
Encrypted HSR in MACsec	145 (1443)	36 (354)	5 (47)

3.2. MACsec in HSR

The other way of solving this problem is to create a valid MACsec frame and send it using HSR as depicted if Figure 9. In this case, the HSR tag would not be secured.

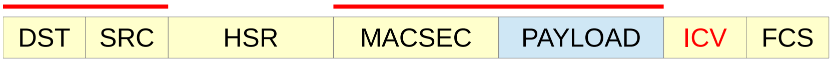

Figure 9. MACsec frame embedded in HSR frame. ICV does not protect the HSR tag.

This can be done at two levels (as detailed in Figure 10). The first level is securing what enters through the interlink. The second level is securing both ring ports before adding HSR related tags. The first approach reduces the required resources since a single MACsec instance is required in the interlink. Furthermore, if the RedBox is connected to MACsec capable devices in the interlink, standard RedBoxes can be used. The second secures point-to-point communications in the HSR rings that are not part of the device to device communications, like HSR supervision frames and peer-to-peer synchronization messages.

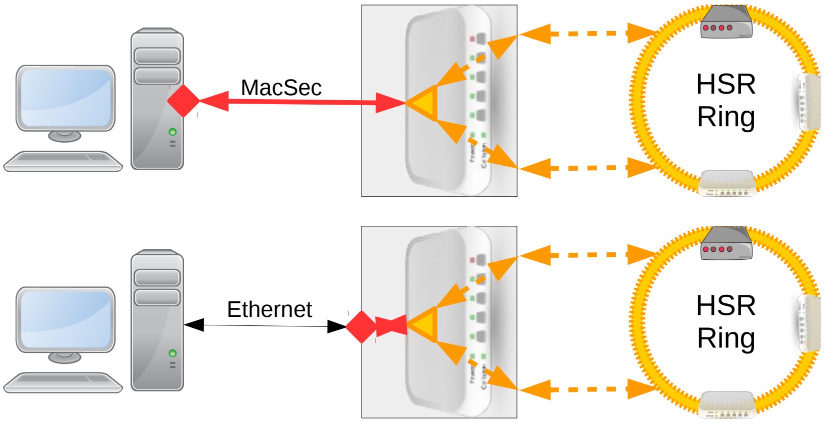

Figure 10. MACsec in HSR can be done at two different levels. (Top) MACsec added in the processing unit. (Bottom) tag added in the switch interlink port. Dashed lines indicate standard HSR traffic. Continuous lines indicate standard Ethernet. MACsec header is inserted before HSR processing; all the traffic in the ring is HSR compliant. If the MACsec tag is inserted inside the switch, some of the HSR related communications may also be protected. Since the traffic is HSR, legacy HSR equipment can be used, and it will not have any access to secured communications but otherwise is fully functional. It can transmit information to other equipment (both legacy and MACsec capable) and secure information can pass through it.

This mechanism offers several advantages. The frames in the HSR ring fully comply with the standard. This means that legacy HSR communication equipment can be used, and, since it is a standard HSR ring, there is no added latency compared with non secured HSR rings.

There are also several disadvantages. The HSR header is not protected, and, thus, HSR related attacks can be generated. Another problem is that HSR switching is not aware if a packet is discarded by the end node because it is a forge. This could lead to a packet loss because HSR thinks that they have already arrived while, in reality, they have not (see Figure 11). This could be a special case of DoS attack in which you trick the system into dropping good packets. Depending on where the securing block is included, HSR supervision messages are also not protected and time synchronization may not be completely secured. These disadvantages can be solved using the third method proposed in this paper (see Section 3.3).

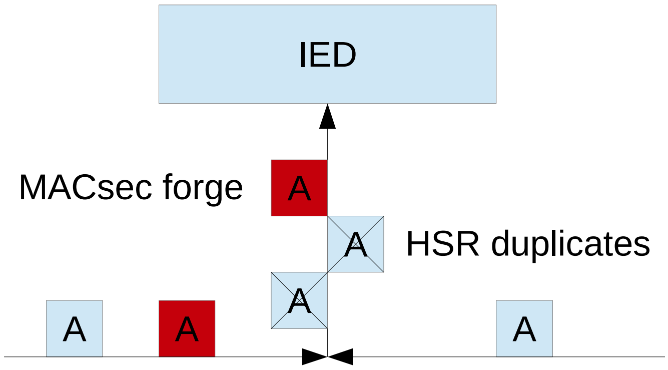

Figure 11. An HSR frame is forged, and correct frames are discarded by HSR processing because they have already arrived. MACsec processing in the end node discards the frame because it is a forge. Frame A never arrives to the intended destination.

3.3. MACsec into Protected HSR

Although there are only two possibilities (HSR in MACsec and MACsec in HSR), there is a third way of solving the problem. In this case, we can embed an MACsec frame inside HSR but making the ICV protection cover the HSR frame as seen in Figure 12.

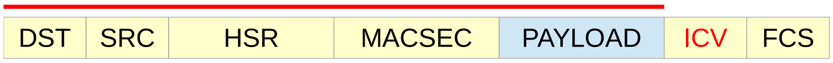

Figure 12. MACsec frame embedded in the HSR frame. ICV also protects the HSR header.

This mechanism offers several advantages. The resulting frame is fully compliant with the HSR standard (see Figure 13). All HSR tags are located in the standard positions with standard values. As in the previous case, this means that non security aware equipment may be used and that the standard HSR latency is applied. At the same time, all communication can be secured if desired. In this way, the protection scheme is complete and all attacks mentioned in Section 2.1 are defeated.

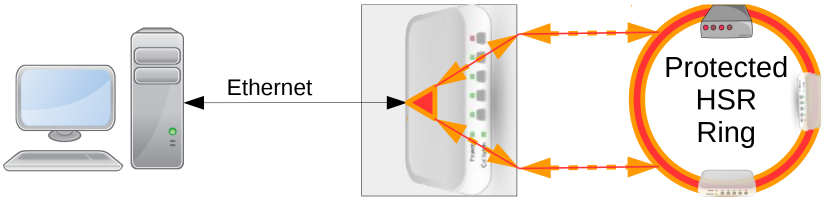

Figure 13. MACsec into protected HSR maintains HSR compatibility in the ring. Short dashed lines indicate standard HSR traffic. Black lines indicate standard Ethernet. MACsec and HSR tags are included at the same point so that MACsec can secure HSR, and the outermost layer is HSR so the traffic in the ring is HSR compliant. Legacy equipment (top switch/DAN) can communicate using non secure channels with any other equipment in the network.

The main disadvantage is that the MACsec implementation is not standard. This means that standard equipment like MACsec aware Ethernet phyters may not be used. Although not standard, it is by no means strange since similar approaches are used in EoMPLS (Ethernet over Multiprotocol Label Switching) communications [30].

One key point in this approach is that the frame must be processed to see not only that the frame check sequence (FCS) field is correct but to see if the ICV is valid before it is added to the correctly received packet memory.

4. Impact of Protection Schemes in Communications

This section will study the impact of MACsec in the maximum number of nodes. We will study the maximum latency allowed by the IEC 61850 standard as well as the throughput implications. This study is of great importance since a security scheme that renders the network unusable is of no interest. These kinds of studies are normally focused on special cases of IEC 61850 and different network types [31]. In this case, we will focus on studying worst/best case scenarios; due to this fact no statistical analysis has been performed. Our efforts are focused on obtaining the maximum number of nodes in a network that guarantees a correct functioning of the network under any conditions.

4.1. Latency

Latency, the worst delay of all possible associations, becomes a factor to control in HSR in which every node adds a delay to the frames that crosses it. IEC 61850-5 [32] establishes different types of traffic based on latency, with the most restrictive latency of 3 ms for TT6 traffic type in substations. It includes GOOSE traffic and Sample Value traffic. According to the IEC 61850-90-4 [23], each node concerned, source and destination has a maximum processing time of 1.2 ms. Thus, the remaining time to cross the network will be given by Equation (1):

$$latency_{max} = 3 - 2 \times 1.2 = 0.6 \text{ ms}. \tag{1}$$

The delay added by each HSR node, T_1, can be broken down into three parts (Equation (2)) as depicted in Figure 14:

$$T_1 = t_1(receiving) + t_2(switching) + t_3(waiting). \tag{2}$$

These terms refer to parts of the reception/forwarding operation process of the frames in nodes. The following time calculations are for fast Ethernet (FEth) and must be divided by 10 for gigabit Ethernet (GEth):

- t_1 depends on the operation mode used, for standard HSR without MACsec:
  - Store-and-Forward (SF): the whole frame is received before switching. This depends on the size of the frame: from 70 octets up to 1528 octets plus preamble and start of frame (P&SoF). It results in a time range from 6.24 µs to 122.88 µs.
  - Cut-Through (CT): switching starts after receiving P&SoF, addresses and HSR Tag to minimize the delay added in the nodes. The theoretical value is 2.08 µs for the regular HSR frame.
- t_2 is the time taken to decide whether to forward/receive/discard a frame, and it depends fundamentally on the time needed to check whether the frame has arrived before or not.
- t_3 is the time a frame has to wait to be sent because another frame is being sent. We have tested three different scenarios:
  - $t_{3Min} = 0$: no waiting time. In other words, no frame is being sent. This is the best case scenario. In the case of synchronized traffic, this would be the normal situation.
  - $t_{3SV} = 12.8$ µs: in an IEC 61850 process bus network, most traffic is of sample value type. These frames do not have a constant length, but 160 octets (8 octets P&SoF + 12 octets interframe gap + 140 SV frame) is quite common, and this frame would allow to send a single value.
  - $t_{3max} = 123.84$ µs: the worst case scenario appears when the longest frame (1528 octets + 8 octets P&SoF + 12 octets interframe gap) is being transmitted and a new frame arrives from a different port.

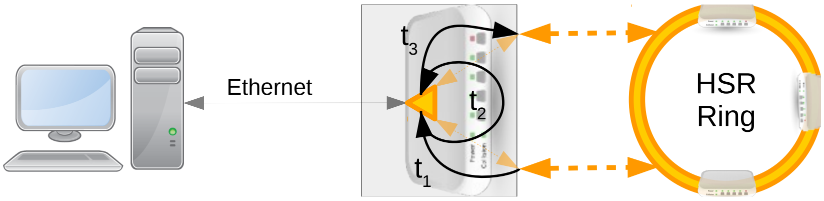

Figure 14. Delays in HSR node. Source node includes t_3, and destination $t_1 + t_2$.

Latency can be reduced in several ways, t_1 is made minimum using CT, which entails hardware implementation, e.g., field programmable gate arrays (FPGAs). This term varies according to the different approaches discussed in Section 3:

- *MACsec inside HSR* or *MACsec into protected HSR*: the standard HSR times apply since HSR tag is in the same position and is not encrypted: 2.08 µs 26 octets: 8 octets P&SoF + 6 destination MAC address + 6 source MAC address + 6 HSR tag.
- *HSR inside MACsec*: the HSR tag is buried inside the MACsec payload, depending on whether the payload is encrypted or only signed for authentication:
    - Signed: 3.36 µs 42 octets: 8 octets P&SoF + 6 destination MAC address + 6 source MAC address + 16 MACsec header + 6 HSR tag.
    - Encrypted: 4.16 µs 52 octets: 8 octets P&SoF + 6 destination MAC address + 6 source MAC address + 16 MACsec header + 16 MACsec decryption block, assuming a heavily pipelined decryption algorithm that results in negligible decryption time.

t_3 is reduced by avoiding waiting times in nodes. It may be improved by synchronized traffic generation on nodes and by controlling frame size. If delivered frames were limited in length, the waiting times would be shorter. On the other hand, if traffic generation is controlled and synchronized in the network, waiting times in the nodes can be avoided or reduced. The IEC 62439-3 includes the use of IEEE 1588 (PTP) [33] to ensure accurate synchronization.

t_2 is the last term with which the delays in nodes can be reduced. It is directly related to the way of checking whether a frame is new or a duplicate or circulating frame. A correct design of the switch can make this term negligible at FEth. In GEth, this may be one of the key points. For the rest of our discussion, we will focus on an ideal system with zero search time.

The maximum number of nodes, N, of a HSR ring is given by Equation (3) in this theoretical worst scenario, when the largest Ethernet frame is transmitted with the latency restrictions imposed by TT6 traffic:

$$N = 1 + \frac{latency_{max}}{t_1 + t_2 + t_3 + t_l}, \tag{3}$$

where t_l is the delay of the signal in each link. Since the delay in the medium is negligible in comparison to the rest of the terms, it will ideally be taken as zero. Table 2 shows a comparison of the different approaches. It has been made for three different scenarios, synchronized traffic (t_{3Min}), IEC 61850 sample value (t_{3SV}) and worst case scenario (t_{3max}).

As it can be seen, the use of HSR embedded in MACsec can heavily reduce the amount of available nodes due to the increase of the latency in each of them. The difference in the worst case scenario is halving the maximum number of nodes. Although this scenario is highly unlikely, a 10% reduction is more than possible in networks where SV messages are dominant.

4.2. Throughput

The throughput is defined as the amount of data that can be transported by a unit of time. In the context of Power Utility Automation, each node, in the process bus, generates a sample value every 250 µs for 50 Hz line frequency. This means that 4000 SV frames per second per node are generated.

Additionally, Manufacturing Message Specification (MMS) and GOOSE messages can be included in the communication. In order to allow for periodic (SV) and sporadic (GOOSE) traffic, only 125 µs of every period are left for SV traffic. The addition of HSR and MACsec increases the amount of data transmitted, and, thus, reduces the maximum number of nodes. The SV frame size is variable, but if we take a standard length of 140 octets (160 octets taking into account P&SoF) as a reference for the calculations, Table 3 shows the results. The number of nodes is reduced since the frame is increased. HSR requires six extra octets while MACsec needs 32 more.

From the table, we can see that the introduction of MACsec reduces the amount of nodes by 20%.

Table 3. Maximum number of nodes for different communication protection according to throughput estimated from IEC 61850. Frame sizes are 160 (IEC 61850), 166 (HSR) and 198 (HSR + MACsec) octets.

	IEC 61850	**HSR**	**HSR + MACsec**
FEth	9	9	7
GEth	97	94	78

5. Hardware Implementation

One of the motivations for this work is the inability of current devices to perform RSA based security on real-time data like GOOSE. This work proposes the use of MACsec, which, in turn, is based on AES-GCM. If AES-GCM cannot be performed faster than RSA, all this work could be meaningless. The key point is that AES-GCM can be highly parallelized. There are, at least, two possible ways of managing this high speed AES-GCM flow, one through the use of AES-GCM capable Ethernet controllers and the other by the use of dedicated blocks in FPGAs.

In the area of MACsec capable Ethernet controllers, there are multiple possibilities from different vendors. All of them are capable of securing 1 Gbps traffic on the fly. Examples could be the Intel 82576EB [34], Broadcom BCM54380 [35] or Vitesse VSC8584 [30].

Even more interesting that a dedicated "phy" is the use of a specialized core in the switching element. This element normally is a FPGA that can have added modules. There are plenty of modules for AES-GCM in FPGA. Examples include CAST GCM-AES Authenticated Encrypt/Decrypt Core [36], Heliontech AES-GCM family of cores [37], BarcoSilex Scalable AES-GCM/GMAC/CTR IP Core [38], and Algotronix MACsec Core [39].

6. Conclusions

This paper presents an approach to use MACsec as a security communication means in a substation automation network. Although the use of an information technology standard may seem straightforward, the considerations that have to been taken into account to guarantee the maximum allowed delay for real-time traffic require some thought. This paper presents three different approaches to securing substation automation communication. This effort is proposed at OSI Level 2 using the international MACsec standard. This is done to minimize latency issues. Special attention has been given to the negative latency and throughput impact. This impact leads to different maximum number of nodes in the network that may render a solution not appropriate for the low latency IEC 61850 traffic.

This approach is not meant as a replacement of proposed end-to-end security schemes as IEC 62351 but as a complementary measure and as a way of securing existing equipment by the addition of the MACsec core at the HSR switch level. This approach also secures non end-to-end communication such as synchronization. Each of the presented approaches has its own advantages and disadvantages and has an impact on the maximum number of nodes that the resulting network may have to still comply with the tight requirements of the IEC 61850.

The different approaches presented reduce the number of nodes in the network and the best achievable cases are when MACsec is embedded into HSR.

Acknowledgments: 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 the Research and Education Unit UFI11/16 of the UPV/EHU and partially supported by the Basque Government within the funds for research groups of the Basque University system IT978-16 and within the project TFactory ER-2014/0016. In addition, FEDER funds and UPV/EHU Ph.D. scholarship funding are acknowledged.

Author Contributions: The overall research has been performed by J.L. A.A. provided all the required knowledge and development in the area of redundant ethernet. J.A.A. is the main contributor in the area of latency and throughput calculations. N.M. has been in charge of the cryptographical part. U.B. has provided feedback on multiple areas and has developed many of the ring models.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. International Electrotechnical Commission. *IEC 61850: Power Utility Automation*; International Electrotechnical Commission: Geneva, Switzerland, 2016.
2. Skeie, T.; Johannessen, S.; Brunner, C. Ethernet in substation automation. *IEEE Control Syst.* **2002**, *22*, 43–51.
3. Cleveland, F. IEC TC57 Security Standards for the Power System's Information Infrastructure—Beyond Simple Encryption. In Proceedings of the 2005/2006 IEEE PES Transmission and Distribution Conference and Exhibition, Dallas, TX, USA, 21–24 May 2006; pp. 1079–1087.
4. Ray, P.; Harnoor, R.; Hentea, M. Smart power grid security: A unified risk management approach. In Proceedings of the 2010 IEEE International Carnahan Conference on Security Technology (ICCST), San Jose, CA, USA, 5–8 October 2010; pp. 276–285.
5. Wang, Y.; Ruan, D.; Gu, D.; Gao, J.; Liu, D.; Xu, J.; Chen, F.; Dai, F.; Yang, J. Analysis of Smart Grid security standards. In Proceedings of the 2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE), Shanghai, China, 10–12 June 2011; Volume 4, pp. 697–701.
6. Kanabar, M.; Voloh, I.; McGinn, D. Reviewing Smart Grid Standards for Protection, Control, and Monitoring Applications. In Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies Conference, Washington, DC, USA, 16–20 January 2012; pp. 1–8.
7. Chen, T.; Abu-Nimeh, S. Lessons from Stuxnet. *Computer* **2011**, *44*, 91–93.
8. Langner, R. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51.
9. International Electrotechnical Commission. *IEC 62351 Power Systems Management and Associated Information Exchange—Data and Communications Security*; International Electrotechnical Commission: Geneva, Switzerland, 2007.
10. Krawczyk, H.; Bellare, M.; Canetti, R. HMAC: Keyed-Hashing for Message Authentication (RFC 2104). Frebruary 1997. Available online: https://www.ietf.org/rfc/rfc2104.txt (accessed on 24 January 2017).
11. Jonsson, J.; Kaliski, B. Public-Key Cryptography Standards (PKCS) 1: RSA Cryptography Specifications. RFC 3447. February 2003. Available online: https://tools.ietf.org/html/rfc3447 (accessed on 24 January 2017).
12. Eastlake, D.E., 3rd; Jones, P.E. Secure Hash Algorithm 1 (SHA1), RFC 3174. September 2001. Available online: https://tools.ietf.org/html/rfc3174 (accessed on 24 January 2017).
13. Moreira, N.; Astarloa, A.; Kretzschmar, U. SHA-3 Based Message Authentication Codes to Secure IEEE 1588 Synchronization Systems. In Proceedings of the IEEE Conference on Industrial Electronics Society (IECON), Vienna, Austria, 10–13 November 2013; pp. 2323–2328.
14. Treytl, A.; Gaderer, G.; Loschmidt, P.; Kerö, N. Investigations on Security Aspects in Clock Synchronized Industrial Ethernet. In Proceedings of the Precise Time and Time Interval Systems and Applications Meeting, Reston, VA, USA, 7–9 December 2006; pp. 232–240.
15. Fuloria, S.; Anderson, R.; McGrath, K.; Hansen, K.; Alvarez, F. The Protection of Substation Communications. In Proceedings of the SCADA Security Scientific Symposium, Miami, FL, USA, 10–12 January 2010.
16. *IEEE 802.1AE-2006 Media Access Control (MAC) Security*; IEEE Standards Department: Piscataway, NJ, USA, 2006.
17. Rashid, M.T.A.; Yussof, S.; Yusoff, Y.; Ismail, R. A review of security attacks on IEC 61850 substation automation system network. In Proceedings of the 6th International Conference on Information Technology and Multimedia, Putrajaya, Malaysia, 18–20 November 2014; pp. 5–10.
18. Premaratne, U.K.; Samarabandu, J.; Sidhu, T.S.; Beresh, R.; Tan, J.C. An Intrusion Detection System for IEC61850 Automated Substations. *IEEE Trans. Power Deliv.* **2010**, *25*, 2376–2383.

19. Premaratne, U.; Samarabandu, J.; Sidhu, T.; Beresh, R.; Tan, J.C. Security Analysis and Auditing of IEC 61850-Based Automated Substations. *IEEE Trans. Power Deliv.* **2010**, *25*, 2346–2355.
20. Hong, J.; Liu, C.C.; Govindarasu, M. Integrated Anomaly Detection for Cyber Security of the Substations. *IEEE Trans. Smart Grid* **2014**, *5*, 1643–1653.
21. Schlegel, R.; Obermeier, S.; Schneider, J. Assessing the Security of IEC 62351. In Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015), Ingolstadt, Germany, 17–18 September 2015.
22. Hohlbaum, F.; Braendle, M.; Alvarez, F. *Cyber Security Practical Considerations for Implementing IEC 62351*; Technical Report; ABB: Zürich, Switzerland, 2010.
23. International Electrotechnical Commission. *IEC 61850-90-4 Ed.01: Communication Networks and Systems for Power Utility Automation;* International Electrotechnical Commission: Geneva, Switzerland, 2013.
24. International Electrotechnical Commission. *IEC 62439-3 Ed.02: Industrial Communications Networks—High Availability Automation Networks;* International Electrotechnical Commission: Geneva, Switzerland.
25. Felser, M. Real-Time Ethernet—Industry Prospective. *Proc. IEEE* **2005**, *93*, 1118–1129.
26. McGrew, D.; Viega, J. The Galois/Counter Mode of Operation (GCM), 2004. Available online: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf (accessed on 24 January 2017).
27. *Identity-Based Networking Services: MAC Security*; White Paper; Cisco: San Jose, CA, USA, 2011.
28. McGrew, D.A.; Viega, J. The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In *INDOCRYPT, Volume 3348 of LNCS*; Springer: Berlin, Germany, 2004; pp. 343–355.
29. *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*; IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004); IEEE Standards Association: Piscataway, NJ, USA, 2010; pp. 1–205.
30. Vitesse. Quad Port Dual Media QSGMII/SGMII GbE PHY with Intellisec and VeriTime. Available online: http://www.microsemi.com/products/ethernet-solutions/ethernet-phys/gigabit-ethernet-phys/vsc8584-quad-port-dual-media-qsgmii-sgmii-gbe-phy-with-intellisec-and-veritime (accessed on 24 January 2017).
31. Abdolkhalig, A.; Zivanovic, R. Simulation and testing of the over-current protection system based on IEC 61850 Process-Buses and dynamic estimator. *Sustain. Energy Grids Netw.* **2015**, *2*, 41–50.
32. International Electrotechnical Commission. *IEC 61850-5 Ed. 2: Communication Networks and Systems for Power Utility Automation—Part 5: Communication Requirements for Functions and Device7 Models*; International Electrotechnical Commission: Geneva, Switzerland, 2013.
33. *IEEE 1588-2008—Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*; IEEE Standards Association: Piscataway, NJ, USA.
34. Intel. Intel 82576EB Gigabit Ethernet Controller. Available online: http://ark.intel.com/products/series/32261/Intel-82576-Gigabit-Ethernet-Controller (accessed on 24 January 2017).
35. Broadcom. Octal-Port 10/100/1000BASE-T 40 nm Transceiver. Available online: https://www.broadcom.com/products/ethernet-connectivity/copper-phy/gigabit-phy/bcm54380 (accessed on 24 January 2017).
36. Inc, C. AES-GCM Authenticated Encrypt/Decrypt Core. Available online: https://www.design-reuse.com/sip/?q=gcm+aes+authenticated+encrypt+decrypt+core (accessed on 24 January 2017).
37. Heliontech. AES-GCM Core. Available online: http://www.latticesemi.com/en/Products/DesignSoftwareAndIP/IntellectualProperty/IPCore/HelionTechCores/AESGCMCore.aspx (accessed on 24 January 2017).
38. Scalable AES-GCM/GMAC/CTR IP Core, BA415. Available online: http://www.barco-silex.com/products/security/high-speed-aes/ (accessed on 24 January 2017).
39. Algotronix. Multiple SecY IEEE 802.1ae MACSEC IP Core for 1Gbit Ethernet. Available online: https://www.xilinx.com/products/intellectual-property/1-4pilr2.html (accessed on 24 January 2017).