A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid

Jesús Lázaro 1,*, Armando Astarloa 1, Mikel Rodríguez 2, Unai Bidarte 1 and Jaime Jiménez 1

1 UPV/EHU, 48015 Bilbao, Spain; armando.astarloa@ehu.eus (A.A.); unai.bidarte@ehu.eus (U.B.); jaime.jimenez@ehu.eus (J.J.)
2 System-on-Chip Engineering, 48950 Erandio, Spain; mikel.rodriguez@soc-e.com
* Correspondence: jesus.lazaro@ehu.eus

Abstract: Since the 1990s, the digitalization process has transformed the communication infrastructure within the electrical grid: proprietary infrastructures and protocols have been replaced by the IEC 61850 approach, which realizes interoperability among vendors. Furthermore, the latest networking solutions merge operational technologies (OTs) and informational technology (IT) traffics in the same media, such as time-sensitive networking (TSN)—standard, interoperable, deterministic, and Ethernet-based. It merges OT and IT worlds by defining three basic traffic types: scheduled, best-effort, and reserved traffic. However, TSN demands security against potential new cyberattacks, primarily, to protect real-time critical messages. Consequently, security in the smart grid has turned into a hot topic under regulation, standardization, and business. This survey collects vulnerabilities of the communication in the smart grid and reveals security mechanisms introduced by international electrotechnical commission (IEC) 62351-6 and how to apply them to time-sensitive networking.

Keywords: IEC 62351-6; smart grid; time-sensitive networking; IEC 61950

1. Introduction

IEC 61850 [1], the standard for automating power substations, enables an interoperable digitalization of power substations and many smart grid premises [2,3], critical in the energy sector. It defines the data models, services, and communication protocols. Since 2004, when the 14 parts of the standard were released, most of the digitalization effort in the electrical field has followed this approach.

The aim of IEEE for industrial-grade communications has been to enhance the proven Ethernet standard in the industrial world. For this purpose, time-sensitive networking (TSN) offers the possibility of routing different traffic classes over the same network without low-priority traffic affecting high-priority ones. It allows critical data to be sent over the same communication link as the rest of the traffic without causing delays or disturbances, thus eliminating the need to create industrial networks independent of each other. These traffic classes facilitate data exchange between production sites and enterprises by making factory networks fully interoperable with the Internet [4]. The advent of TSN allows deterministic data to be transmitted by means of conventional Ethernet. However, TSN demands security against potential new cyberattacks; primarily, to protect real-time critical messages.

Since the definition of IEC 61850 and the first implementations of power substation networks based on the standard, several real-world security attacks have proven the lack of protection of the infrastructure, devices, and some protocols used [5]. In this scenario, where substation communications may be exposed to the Internet, security becomes crucial. Our paper reveals that another standard, IEC 62351-6, complements this by introducing security mechanisms. It also presents how to apply them to time-sensitive networking (TSN).
Section 2 includes a summary of previous surveys in the area. Section 3 presents IEC 61850 with its characteristics to automate power substations. Section 4 describes TSN, an Ethernet technology to integrate operation and information data that ensures compatibility among vendors. On the other hand, Section 5 uncovers the telematics vulnerabilities of the IEC 61850 and the resulting dangers. Next, Section 6 explains the impediments to leverage usual cyber countermeasures in TSN and other specific needs for its security. The solution, IEC 62351, is introduced in Section 7. Finally, the article is concluded by Section 8.

2. Related Surveys

Other surveys about security in the smart grid focus on different aspects of the smart grid. In particular:

- Kawoosa et al. [6] offer a comprehensive survey of types of attacks and classify them;
- Guduz et al. [7] also classify the attacks and explain the fundamentals of the cyber security in the smart grid;
- Kotut et al. [8] focus on the entire grid, instead of specific components;
- Rawat et al. [9] include a section about challenges and future research directions;
- Komninos et al. [10] focus on issues related to the security of the smart grid and the smart home;
- Yan et al. [11] explore the challenges for a communication infrastructure as part of a complex smart grid system; since this might have millions of consumers and devices, the demand for its reliability and security is highly critical;
- Baig et al. [12] perform a classification according to the different communication layers;
- Wang et al. [13] provide several clear objectives and requirements in the smart grid and an assessment of the security threats.

Unlike these surveys, ours exploits TSN as a critical enabler of the smart grid, provides an insight into the current standards for security in power grids and describes how to apply them to TSN.

3. IEC 61850

IEC 61850-based substations are divided into three logical levels, as shown in Figure 1: station, bay, and process levels. The process bus interconnects intelligent electronic devices (IEDs) at the primary equipment level. On the other hand, the station bus connects intelligent electronic devices (IEDs) at the bay level and station level. Devices at the process level are used to measure the status of the substation and actuate if required. Devices located at the bay level are used to control, monitor, and protect the substation. The station level provides remote access to the substation to allow remote configuration and supervision.

![Figure 1. IEC 61850 substation logical distribution [1].](image)
The standard is divided into 10 sections that describe the communications within the scope of a substation.

Sections 3–5 [14–16] specify the functional requirements for communications in a substation used to identify the services, data models, application protocols, transport, network, data link, and physical layers that meet the communication requirements of a substation. As modern substations are composed of numerous devices with specific functions and services, it is required to establish a configuration procedure that automates and simplifies the configuration process. Section 6 [17] of the standard presents an XML-based substation configuration language (SCL) to specify the relations between each substation automation system (SAS) and the substation control center.

Since electric substations have long service periods over 30 years, standardization was mainly focused on the object data model instead of any specific communication technology. Therefore, IEC 61850 defines objects and services that are independent of underlying protocols. The definition of services can be found in Section 7.2 [18] of the standard. The concept of common data classes (CDCs) is introduced in Section 7.3 [19] and defines common generic blocks that allow the creation of larger data objects. On the other hand, the definition of data objects (logical nodes) is described in Section 7.4 [20]. Specifically, according to IEC 61850, any device in the network that exchanges data using standardized services is considered an object [21]. The mapping of objects and services into messaging specification (MMS) messages is described in Section 8.1 [22] of the standard. According to Sections 9.1 and 9.2 [23], sampled value (SV) can be transmitted over unidirectional point-to-point links or bidirectional multipoint Ethernet links (process bus), respectively.

Having defined IEC 61850 as the standard communication protocol for substation automation systems (SASs), [24] provides several features and benefits as follows:

- **Flexibility**: the standard has been designed to support different services with different performance requirements;
- **Configurability**: substation configuration language (SCL) is used to describe the substation’s network and the services offered by all the devices;
- **Interoperability**: devices from different vendors can provide any service needed in the scope of a substation, which reduces configuration time and reliability issues.

IEC 61850 follows the open systems interconnection (OSI) model. Figure 2 shows the seven open systems interconnection (OSI) layers and the five types of communication services defined by IEC 61850. They can be divided into the following two main groups:

- OSI layer-2 messages with stringent time requirements considered as real-time traffic — process and bus level;
- OSI layer-3 and higher messages with low or no time requirements — station level.

![Figure 2. IEC 61850 communication models.](figure2.jpg)
4. Time-Sensitive Networking: The Interoperable Deterministic Ethernet Standard

The IEC61850 architecture requires mixing operational technologies (OTs) with information technology (IT). Therefore, a common Ethernet technology, able to merge operational technologies (OT) and IT worlds, would be a significant forward step to ensure interoperability among vendors and standardization. Effective development of this technology shall offer a significant cost reduction in equipment, maintenance, seamless integration of advanced analysis services, and a reduction of dependence on a single vendor.

TSN [25] is a comprehensive option for a unique Ethernet-based solution. The original audio–video bridging (AVB) working group evolved to the IEEE TSN Task Group, which is in charge of developing the standards related to TSN. These propose enhancements for IEEE 802.3 networks, and as it has happened in the electric sector, have enabled digitalization in all the sectors. For example, it is typical for the massive interconnection of cyber–physical systems combined with a big data analysis [26–30]. There are many working groups for the definition of the set of standards that make up TSN. Some standards are almost complete, although always subject to possible changes or improvements, while others are under development. Table 1 presents the functions and features of TSN that will enable the introduction of security mechanisms [4].

| Standard          | Description                                                                 | Status                      |
|-------------------|-----------------------------------------------------------------------------|-----------------------------|
| IEEE 802.1Q       | forwarding and transmission mechanisms and reservation protocols            | base standard—pub. in 2018  |
| IEEE 802.1AB      | specifying the link recovery protocols                                      | base standard—pub. in 2016  |
| IEEE 802.1AS      | time synchronization for TSN                                                | base standard—pub. in 2020  |
| IEEE 802.1AX      | link aggregation to increase the throughput                                | base standard—pub. in 2014  |
| 802IEEE 802.1CB   | frame replication and elimination for reliability                         | base standard—pub. in 2017  |
| IEEE 802.1CM      | mechanisms to enable TSN for Fronthaunal                                    | base standard—pub. in 2018  |
| P802.1CS          | link-local registration protocol                                           | ongoing                     |
| P802.1CQ          | multi-cast addressing and local address allocation                          | ongoing                     |
| P802.1DC          | provisioning of quality of service in the network                          | ongoing                     |
| P802.1DF          | the profile for TSN service providers                                       | ongoing                     |
| P802.1DG          | automotive in-vehicle communication                                         | ongoing                     |
| IEEE 802.1Qbu     | frame preemption support                                                    | 2016—IEEE 802.1Q-2018      |
| IEEE 802.1Qbv     | enhancements for scheduled traffic                                          | 2015—IEEE 802.1Q-2018      |
| IEEE 802.1Qca     | path control and reservation                                                | 2015—IEEE 802.1Q-2018      |
| IEEE 802.1Qav     | forwarding and queuing enhancements for time-sensitive streams             | 2009—IEEE 802.1Q-2018      |
| IEEE 802.1Qch     | cyclic queuing and forwarding                                               | 2017—IEEE 802.1Q-2018      |
| IEEE 802.1Qcc     | SRP enhancements and performance improvements                               | 2018—IEEE 802.1Q-2018      |
| IEEE 802.1Qci     | per-stream filtering and policing                                          | 2017—IEEE 802.1Q-2018      |
| IEEE 802.1Qat     | stream reservation protocol (SRP)                                           | 2010—IEEE 802.1Q-2018      |

The fundamental base of TSN is the time-aware shaper [31]. It is designed to separate the communication on the Ethernet network into a fixed length, repeating time cycles. These cycles are divided into time slots according to the TSN configuration agreed between peers. The different time slots can be configured and assigned to one or several of the eight Ethernet priorities. The operation of the time-aware shaper is defined in IEEE 802.1Qbv.

Considering time-aware shaper functionality, three basic traffic types are defined: scheduled, best-effort, and reserved traffic. Scheduled traffic type is appropriated for the hard real-time messages. The best-effort traffic is the general Ethernet packets that are not sensitive to any other quality of service metrics. The reserved traffic type is for frames allocated in different time slots but with a specified bandwidth reservation for each priority type. Figure 3 is an example that summarizes this slot distribution and traffic type. Authors have collaborated in an electronic design with smart grid network equipment manufacturers, in which the layer-2 messages have been allocated in scheduled traffic of TSN [32].
The time-aware shaper allows defining the number of time slots available in each cycle, their duration, and which priorities can be transmitted. Owing to this mode of operation, the scheduled traffic has dedicated time slots to ensure the expected deterministic behavior. The best-effort traffic is accommodated in the remaining time slots of each cycle of operation. A significant improvement for the prioritization and bandwidth use optimization in TSN is the support of credit-based shaper, as defined in IEEE 802.1Qav. This functionality allows using reserved traffic type, upgrading the priority of designed traffic in a state between the scheduled traffic and the best-effort one. Authors have faced the technical challenge of providing nanosecond range synchronization accuracy among the TSN devices that compose the network employing the IEEE 1588 synchronization protocol [33]. Owing to the accuracy provided by this technology, it is feasible ensuring controlled network delay and jitter implanting an effective time-triggered Ethernet-based solution. The specific IEEE 1588 profile for TSN is IEEE 1588ASrev.

On the other hand, layer-2 messages in the IEC 61850 provide services that require high-speed (low-delay) message delivery. Specifically, these messages must be generated, transmitted, received, and processed by the receiver in less than 3 ms, as shown in Table 2. IEC 61850 defines that real-time services must be mapped directly to the data link layer (layer-2) to reduce protocol overhead and achieve required performance levels.

Within this group of services, generic substation events (GSEs) provide a mechanism to share event and status data between substation automation systems (SAS). GSEs can be subdivided into two status/event transmission protocols: generic substation state events (GSSEs) and generic object-oriented substation events (GOOSEs). GOOSE messages are generated and received by intelligent electronic devices (IEDs) in a publisher/subscriber multicast model. These messages do not use delivery confirmation mechanisms. Therefore, GOOSEs are retransmitted several times to provide a certain level of redundancy [34]. Abstract syntax notation one (ASN.1) is used to define and encode the structure of the payload of the message. GOOSE messages generally transmit binary data such as indications or alarms. Examples of GOOSE usage are breaker failure or automatic transfer of lines.

Table 2. IEC 61850 time requirements [35].

| Application                  | Message Type | Time Requirement |
|------------------------------|--------------|------------------|
| Fast Messages                | GOOSE        | ≤3 ms            |
|                              | GSSEs        | ≤10 ms           |
| Raw Data                     | SV           | ≤3 ms            |
| Medium-Speed Messages        | MMS          | ≤100 ms          |
| Low-Speed Messages           | MMS          | ≤500 ms          |
| Time Synchronization         | IEEE 1588    | >500 ms          |
| File Transfer                | MMS          | >500 ms          |

SV messages [23] allow the transmission of sampled digital values over Ethernet networks, such as TSN. Data are sent in a continuous stream that is divided into Ethernet frames. merging units (MUs) perform raw voltage and current measurements in different points of the substation (from current and voltage transformers) and are transmitted in SV messages—bay level. This type of message is also based on a publisher/subscriber model
and is encoded using ASN.1. Therefore, IEDs can be subscribed to streams belonging to selected MUs to control switch breakers or other types of devices using GOOSE messages.

5. Security Threats in Substation Automation Systems

From the security point of view, the electric sector is identified as a critical system, similar to other energy facilities. The power plants and the electric substations are considered critical infrastructures [36–42]. Therefore, the digitalization of these premises has included, as potential threats, cyberattacks. Although IEC 61850 was not focused on security, the regulation and the evident exposure of the current electric system to these threats have pushed the international standardization community to work on a detailed security solution for the sector. This effort is compiled in IEC 62351 Standard to improve security in automation systems for the power system domain.

IEC 61850 defines the communication protocols used in the scope of a substation and opens the path of digitalization and standardization. On the other hand, it also opens the door to new vulnerabilities. Information between devices is distributed in Ethernet frames, such as TSN, which can be easily sniffed, altered, or recorded and played back. Recently, much effort has been put into preventing unauthorized people from accessing substation networks and control systems. In [43], the Waterfall Unidirectional Security Gateway is proposed to prevent attackers from accessing the substation by implementing a new type of physical firewall. However, this type of solution only protects the substation from certain types of cyberattacks. The ideal scenario would be to protect devices within the control network individually.

IEC 61850 does not specify any cybersecurity mechanism, as this task was left to be later defined by the IEC 62351 family of standards. The problem with this approach is that, as IEC 62351 was released several years after IEC 61850, many IEDs from different vendors do not support IEC 62351 [44]. Therefore, it is necessary to use alternative security solutions combined with the security mechanisms defined in IEC 62351 to protect current and future IEC 61850 based substations.

There are several types of attacks that can prevent IEC 61850 IEDs from operating as expected. Some of them are specific to SAS, while others are well-known threats already found in Ethernet-based networks [45–47]:

- Denial of service: IED is virtually disconnected from the network since it cannot send or receive Ethernet frames;
- Spoofing: IED can be physically or virtually spoofed to send erroneous commands or status events to other devices in the network;
- Unauthorized access: IED is accessed by an attacker to modify its configuration or its behavior, or to obtain sensitive data that can compromise the device or the substation;
- Data interception: critical data are intercepted to obtain information about the devices or the substation;
- Man-in-the-middle: communications between IEDs and monitoring systems are intercepted and modified by an attacker to pretend that the attacker is one of the end nodes of the communication;
- Stepping stone: an attacker compromises an IED and takes control of it to launch a logical attack on other IEDs or devices in the network.

Previously defined types of attacks can be performed from within the substation’s local area network (LAN) or accessed over a wide area network (WAN) from a remote location if the substation is connected to an external network such as the Internet [41,48–51]. According to the network layers, smart grid cyberattacks can be classified as shown in Table 3 [47].
Table 3. Smart grid cyberattacks according to network layers [47].

| Network Layer | Attack Type |
|---------------|-------------|
| Application Layer | CPU Exhaustring, LDoS, HTTP Flooding, Protocol, Stack Buffer Overflow, Data Injection Attacks |
| Transport Layer | IP Spoofing, Packet Sniffing, Wormhole, Data Injection, Traffic Flooding, Buffer Flooding, Buffer Overflow, DoS/DDoS, MITM, Covert Attack, Replay Attack |
| MAC Layer | Traffic Analysis, Masquerading, ARP Spoofing, MITM, TSA, MAC DoS Attack, Flooding attacks, Jamming Attack |
| Physical Layer | Eavesdropping, Smart Meter, Tampering Attacks, TSA, Jamming Attacks |

Since the definition of IEC 61850 and the first implementations of power substation networks based on the standard, several events have proven that previously defined types of attacks have been used in the real world. Slammer worm infected a nuclear plant’s control system that caused its failure. This cyberattack bypassed the protection mechanisms and disabled the safety monitoring system for nearly five hours [52]. Similarly, several industrial sites in Iran were infected by a computer worm called Stuxnet. Among them, there was a nuclear plant that used Siemens industrial control programs based on Microsoft Windows [5]. Stuxnet was the first known cyberattack on SCADA systems; it was used to gain knowledge about the operation of the system and then used to take control of devices in the network and cause their failure. After Stuxnet, several modifications of the worm have been identified: Duqu, Flame, or Gauss [53]. These variations of the original cyberattack were used to spy on industries, people, and banks. The peculiarity of this type of worms is that they have been designed to spread over networks and storage devices (such as USB sticks) without being detected by security systems [54].

As demonstrated by previously discussed cyberattacks to SAS, they may impact diversely on the behavior of the substation, which can cause malfunction, performance issues, or even total failure of part of the communications system or even the whole substation. The most common impacts of cyber-attacks are listed below [55]:

- Interruption of monitoring system: IED cannot receive data from MUs or other IEDs, data are corrupted, or it cannot process them as expected;
- Denial of service to control system: IED cannot send control commands to circuit breakers or protection devices, or an attacker has modified its operation;
- Interruption of protection communication: protection device cannot receive commands from IEDs;
- Undesirable protection operation: protection device receives fake commands, or it does not respond accordingly;
- Network interruption: devices in the substation are unable to communicate with each other. This represents a high-risk situation for the integrity of the facility and the service provided;
- Synchronization tampering: control center receives wrongly time-stamped data, which may source false alarms or hide true ones.

6. Time-Sensitive Networking and Security

Cybersecurity in critical systems in general, and in industrial control systems (ICS), in particular, is a vast and complex topic that is out of the scope of this paper. However, it is worth mentioning that there is an intensive activity defining secure architecture designs (e.g., [56]) for ICS that defined how to merge securely internal and external networks and benefit from DMZ areas and IT world field-proven technologies (firewalls, VPN, etc.). TSNs can benefit from these security mechanisms. Especially if the security mechanisms are applied using best-effort traffic [57]. For example, security protocols, such as IPsec or TLS, or any other security application can run over this deterministic Ethernet.

However, TSN has some particularities that need to be taken into account. The synchronization is the base of its functionality, and this depends on IEEE 1588. The security of IEEE 1588 is not straightforward, and the current commercial equipment cannot ensure adequate protection over the multiple vulnerabilities of this standard.
Moreover, some TSN traffic, such as the scheduled type, is strict real time that requires arriving at the listener before a definite time boundary. Therefore, the latency introduced by every node must be minimized (and globally deterministic). If encryption and authentication need to be applied to this traffic, the performance of regular microprocessor-based embedded systems is no longer valid [58].

Although the “cut-through” operation with the scheduled traffic would be desirable for minimizing the latency in delivering the message, from the security point of view, it could be a severe drawback to admit [59]. This switching approach implies that the messages cannot be thoroughly analyzed before being forwarded. Therefore, non-authenticated traffic could be injected into the network for malicious purposes.

6.1. Secure IEEE 1588 Precise Time Protocol

In the scope of the new digital protocols used in the sector, it is worth mentioning the precise time protocol (PTP) [33] used to distribute an accurate timing reference between the different equipment and event among the whole electric grid. This protocol is very vulnerable from the security point of view, and its protection is a challenge for the current state of the art [60–62]. The PTP algorithm uses a master–slave scheme; the slaves are synchronized and syntonized by time-stamped frames interchanged with the master. However, to obtain the requested timing accuracy level, all the network elements, including the switches and bridges, should modify these frames. Therefore, an end-to-end security approach is not enough due to the need for security in all devices.

PTP presents some security vulnerabilities and threats that 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 [63,64]. Consequently, a slave clock could be forced to be aligned to a false time, or interruptions of PTP protocol could be forced. Although PTP first introduced security as an optional extension in Annex K of the second version of the standard, it was never formalized into an adequately defined security protocol due to its limitations.

To protect IEEE 1588 systems, version 3 of the standard will include some security recommendations. Additionally, authors have proposed enhancements to the resilience of IEEE 1588 implementations against complex cyberattacks [65].

6.2. Wire-Speed Cryptography for Real-Time Traffic

As presented in this paper, the security means for stringent real-time traffic requires wire-speed cryptography to ensure low and deterministic latency times and robust security key management schemes [66]. For example, in the context of the electric sector, the scheduled traffic in a TSN network can be composed of layer-2 GOOSE and sampled measured value (SMV), previously described. The security has been addressed following the approach described in IEC 62351-6 and IEC 62351-9, which defines the frame format for the secure frames and the security key management system, respectively. On the other hand, the computation capabilities included in all the equipment must allow low-latency wire-speed cryptography that requires specific computation modules to support datastream processing [67]. Datastream processing is capital, both for the encryption (that may be optional in most of the scenarios) and for the authentication and integrity analysis of all the messages to block the propagation of non-authorized ones immediately.

Figure 4 depicts our schematic setup for secure real-time traffic implementing IEC 62351-6 and IEC 62351-9 standards. A TSN setup benefits from this approach, applying wire-speed cryptography for the deterministic traffic and implementing an agile security key management mechanism [68].
7. IEC Security Standards

IEC 62351 is the suite of standards that define the security considerations and requirements that must be met to protect IEC 61850 based communications in the scope of a substation. It is composed of 13 sections.

Section 3 [69] provides security for any profile that includes TCP/IP. It uses the widely adopted TLS protocol to provide authentication, confidentiality, and integrity. Specific parameters and settings for TLS that should be used are covered in this section. Section 4 [70] of the document provides security for profiles that include MMS. In this case, TLS is used to authenticate two entities interacting with each other. The standard allows both secure and non-secure profiles to operate simultaneously. Section 5 [71] defines the security mechanisms for serial communications (such as IEC 60870-5-101). These channels usually only support low bit rates or are constrained by the computing performance of the devices that implement them. Thus, TLS would not be a feasible solution for these classes of communications. Instead, the only security measure provided is some lightweight authentication mechanisms.

This last protocol, IEC 62351-6, is specific for the electric sector and aims to define security for very stringent real-time messages used for control purposes (GOOSE messages) and the distribution over the network of the current and voltage digitized values (sampled measured values). The latency introduced by the security mechanisms within these messages must be minimal so that it does not disturb the system’s proper operation. This requirement has influenced the final form of the standard, which defines as mandatory authentication and the integrity of the messages. Confidentiality through encryption has been defined as an optional feature.

Section 6 [72] defines the security procedures for peer-to-peer and layer-2 profiles such as GOOSE or SV. Instead of using general-purpose security mechanisms as TLS, a specific solution has been designed to ensure that messages with stringent time requirements are delivered on time. In this case, authentication is defined as mandatory. On the other hand, encryption is defined as optional because the added computational overload could prevent slow devices from meeting the time requirement of 3 ms to deliver the messages.

IEC 62351-7 [73] focuses on the network and system management (NSM) of the information infrastructure, such as communication networks, IEDs, and self-defining communication protocols. Secure management of the information infrastructure becomes critical to provide the levels of security and reliability needed in power system operations. The ISO CMIP and SNMP standards are proposed to monitor the health of the network and the systems. Section 8 [74] specifies the access control of users and automated agents.
to the data object in power systems employing role-based access control (RBAC). IEC 62351-9 [75] is an important part that enables other security standards such as IEC 62351-6. This section defines how to generate, distribute, revoke, and handle digital certificates and cryptographic keys to protect IEC 61850 based communications.

Section 10 [76] describes security architecture guidelines for power systems based on essential security controls. Their mapping and relation to the general system architecture of power systems allows system integrators to securely deploy power generation, transmission, and distribution systems. IEC 62351-11 [77] defines the security for XML-based files. The main objective of the document is to provide mechanisms to authenticate the source of the file and tamper detection. Figure 5 summarizes the mapping of each IEC 62351 security standard to its corresponding security layer.

| Security Layers       | IEC Security Standards                      |
|-----------------------|---------------------------------------------|
| Security Policies     | IEC 62351-10 Security Architecture         |
| Security Procedures   | IEC 62351-8 Role-Based Access Control       |
| Message Security      | IEC 62351-4 MMS Security                   |
| Transport Security    | IEC 62351-6 Layer-2 GOOSE & SV Security     |
|                       | IEC 62351-9 Secure Key Management           |
|                       | IEC 62351-11 XML File Security              |
| Network & Media Security | IEC 62351-7 Network and System Management |
|                       | VPNs, Firewalls, SNMP                       |

Figure 5. IEC 62351 security layers.

Figure 6 summarizes the applications of IEC 62351 standards and others to the different system layers found in a typical critical infrastructure of the smart grid. The bottom part of the pyramid represents how the specific standards for cryptographic equipment and modules are now applied to critical equipment such as protections in the grid. Furthermore, standards such as IEEE 1686 applied to the embedded software of the IEDs. IEC 62351 [78] covers general system security architectures (-10), role definitions for the sector (-8), and adoptions of well-known security mechanisms used in the IT world, such as IPsec or TLS, (-3, -4). It is worth mentioning the proposals for the security key exchange mechanism defined in (-9) and for the security of real-time traffic in the SAS (-6).

All these standards defined in IEC 62351, including IEC 62351-6, can be applied to Ethernet communications. Over the network link layer, layer-3 and upper protocols may include robust security features exploited in IT networks [79]. All these security mechanisms can be used over the high-availability Ethernet alternatives defined in IEC 61850, such as with parallel redundancy protocol (PRP) or with high-availability seamless redundancy (HSR) if the “cut-through” switching approach is not applied in this last one [80].

In a more general industrial scenario, we can find similarities to these approaches [81,82]. On the one hand, the low-latency traffic involved in the control operations is generally constrained with time response limitations, and on the other, there is the best-effort general and non-real-time traffic. Typically, both types have been implemented separately within industrial premises: the real-time traffic is carried out by proprietary field-buses in OT networks, and the best-effort traffic by conventional Ethernet-based switching and routing systems in the IT networks. In some critical infrastructures, these OTs and ITs are maintained isolated. However, in most cases, due to the need for accessing the “data,” it is clearly a merging process.
8. Conclusions

IEC 61850 has been the standard to digitize power substations, independent of underlying protocols. It provides flexibility, reconfigurability, and interoperability. On the other hand, Time-sensitive networking, the deterministic Ethernet solution has merged operational and information technologies in those digitized substations. Nevertheless, both standards have open the door to new specific vulnerabilities in this critical energy sector, such as potential cyberattacks on the synchronization plane and the real-time traffic—“scheduled” in TSN. This survey has introduced security mechanisms against them, collected in IEC 62351-6, and applied to time-sensitive networking.

Since TSN separates real-time data from the rest, it allows for the exploitation of usual security resources on non-critical traffic, in addition to its normal redundancy, as another protection. IEC 62351 sets some security features as optional “encryption”, not to delay critical traffic and offers specific measures. Last but not least, IEC 62351-6 is compatible with TSN, as Ethernet standard; thus, integrating both is straightforward, for example, in wire-speed cryptography and strong security key management.

In summary, the digitizing process leads to the need to use different kinds of standards. IEC 61850 provides the data interoperability layer. TSN provides the ability to isolate time critical from non-time-critical traffic. Customary IT resources can protect non-time-critical traffic. Smart-grid-related time-critical traffic, on the other hand, can be protected by the use of IEC 62351.

Author Contributions: Research and original draft preparation, J.L.; TSN fundamentals, A.A.; 61850 fundamentals, M.R.; writing—review and editing, U.B. and J.J.; state-of-the-art research, J.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been supported by the Ministerio de Economía y Competitividad of Spain within the project TEC2017-84011-R and FEDER funds, as well as by the Department of Education of the Basque Government within the fund for research groups of the Basque university system IT978-16.

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

| Abbreviation | Description |
|--------------|-------------|
| ASCI         | Abstract Communication Service Interface |
| ASN.1        | Abstract Syntax Notation One |
| AVB          | Audio Video Bridging |
| CDC          | Common Data Classes |
| DER          | Distributed Energy Resources |
| DoS          | Denial of Service |
| GOOSE        | Generic Object Oriented Substation Events |
| GSE          | Generic Substation Events |
| GSSE         | Generic Substation State Events |
| HSR          | High-availability Seamless Redundancy |
| ICS          | Industrial Control Systems |
| IEC          | International Electrotechnical Commission |
| IED          | Intelligent Electronic Devices |
| IT           | Information Technology |
| LAN          | Local Area Network |
| MMS          | Messaging Specification |
| MU           | Merging Units |
| NSM          | Network and System Management |
| OSI          | Open Systems Interconnection |
| OT           | Operational Technologies |
| PRP          | Parallel Redundancy Protocol |
| PTP          | Precise Time Protocol |
| RBAC         | Role-Based Access Control |
| SAS          | Substation-Automation-Systems |
| SCL          | Substation Configuration Language |
| SCSM         | Specific Communication Service Mapping |
| SMV          | Sampled Measured Value |
| SV           | Sampled Value |
| TSN          | Time-Sensitive Networking |
| WAN          | Wide Area Network |

## References

1. International Electrotechnical Comission (IEC). IEC 61850, Standard for the Design of Electrical Substation Automation. 2013. Available online: [https://webstore.iec.ch/publication/6028](https://webstore.iec.ch/publication/6028) (accessed on 2 August 2021).

2. Obaidli, S.A.; Subramaniam, V.; Alhuseini, H.; Gupta, R.; Dolezilek, D.; Kalra, A.; Sankar, P. IEC 61850 beyond compliance: A case study of modernizing automation systems in transmission power substations in Emirate of Dubai towards smart grid. In Proceedings of the Saudi Arabia Smart Grid (SASG), Jeddah, Saudi Arabia, 12–14 December 2017. doi:10.1109/sasg.2017.8356501.

3. Aguilar, R.; Ariza, J. Testing and configuration of IEC 61850 multivendor protection schemes. In Proceedings of the IEEE PES T&D 2010, New Orleans, LA, USA, 19–22 April 2010. doi:10.1109/tdc.2010.5484210.

4. Hallmans, D.; Ashjaei, M.; Nolte, T. Analysis of the TSN Standards for Utilization in Long-life Industrial Distributed Control Systems. In Proceedings of the 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 8–11 September 2020. doi:10.1109/etfa46521.2020.9212162.

5. Kushner, D. The real story of stuxnet. *IEEE Spectr.* 2013, 50, 48–53. doi:10.1109/mspec.2013.6471059.

6. Kawoosa, A.I.; Prashar, D. A Review of Cybersecurities in Smart Grid Technology. In Proceedings of the 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 19–21 January 2021. doi:10.1109/iccakm50778.2021.9357698.

7. Gunduz, M.Z.; Das, R. Analysis of cyber-attacks on smart grid applications. In Proceedings of the International Conference on Artificial Intelligence and Data Processing (IDAP), Malatya, Turkey, 28–30 September 2018. doi:10.1109/idap.2018.8620728.

8. Kotut, L.; Wahsheh, L.A. Survey of Cyber Security Challenges and Solutions in Smart Grids. In Proceedings of the Cybersecurity Symposium (CYBERSEC), Coeur d’Alene, ID, USA, 18–20 April 2016. doi:10.1109/cybersec.2016.013.

9. Rawat, D.B.; Bajracharya, C. Cyber security for smart grid systems: Status, challenges and perspectives. In Proceedings of the SoutheastCon 2015, Fort Lauderdale, FL, USA, 9–12 April 2015. doi:10.1109/secon.2015.7132891.

10. Komninos, N.; Philippou, E.; Pitsillides, A. Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *IEEE Commun. Surv. Tutor.* 2014, 16, 1933–1954. doi:10.1109/comst.2014.232093.

11. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Commun. Surv. Tutor.* 2013, 15, 5–20. doi:10.1109/surv.2012.021312.00034.
12. Baig, Z.A.; Amoudi, A.R. An Analysis of Smart Grid Attacks and Countermeasures. JCM 2013, 8, 473–479.
13. Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. Comput. Netw. 2013, 57, 1344–1371.
14. International Electrotechnical Comission (IEC). IEC 61850-3, “Communication Networks and Systems for Power Utility Automation—Part 3: General Requirements”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2013.
15. International Electrotechnical Comission (IEC). IEC 61850-4, “Communication Networks and Systems for Power Utility Automation—Part 4: System and Project Management”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2011.
16. International Electrotechnical Comission (IEC). IEC 61850-5, “Communication Networks and Systems for Power Utility Automation—Part 5: Communication Requirements for Functions and Device Models”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2013.
17. International Electrotechnical Comission (IEC). IEC 61850-6, “Communication Networks and Systems for Power Utility Automation—Part 6: Configuration Description Language for Communication in Power Utility Automation Systems Related to IEDs”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2020.
18. International Electrotechnical Comission (IEC). IEC 61850-7-2, “Communication Networks and Systems for Power Utility Automation—Part 7-2: Basic Information and Communication Structure—Abstract Communication Service Interface (ACSI)”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2020.
19. International Electrotechnical Comission (IEC). IEC 61850-7-3, “Communication Networks and Systems for Power Utility Automation—Part 7-3: Basic Communication Structure—Common Data Classes”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2020.
20. International Electrotechnical Comission (IEC). IEC 61850-7-4, “Communication Networks and Systems for Power Utility Automation—Part 7-4: Basic Communication Structure—Compatible Logical Node Classes and Data Object Classes”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2020.
21. McGhee, J.; Goraj, M. Smart High Voltage Substation Based on IEC 61850 Process Bus and IEEE 1588 Time Synchronization. In Proceedings of the First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010. doi:10.1109/smartgrid.2010.5622092.
22. International Electrotechnical Comission (IEC). IEC 61850-8-1, “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”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2020.
23. International Electrotechnical Comission (IEC). IEC 61850-9-2, “Communication Networks and Systems for Power Utility Automation—Part 9-2: Specific Communication Service Mapping (SCSM)—Sampled Values over ISO/IEC 8802-3”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2020.
24. Aftab, M.A.; Hussain, S.S.; Ali, I.; Ustun, T.S. IEC 61850 based substation automation system: A survey. Int. J. Electr. Power Energy Syst. 2020, 120, 106008. doi:10.1016/j.ijepes.2020.106008.
25. IEEE Time Sensitive Networking Task Group. IEEE 802.1 Standards. 2018. Available online: http://www.ieee802.org/1/pages/ tsn.html (accessed on 2 August 2021).
26. Sanchez, M.; Esposito, E.; Aguilar, J. Industry 4.0: Survey from a system integration perspective. Int. J. Comput. Integr. Manuf. 2020, 33, 1017–1041. doi:10.1080/0951192x.2020.1775295.
27. ur Rehman, M.H.; Yaqoob, I.; Salah, K.; Imran, M.; Jayaraman, P.P.; Perera, C. The role of big data analytics in industrial Internet of Things. Future Gener. Comput. Syst. 2019, 99, 247–259. doi:10.1016/j.future.2019.04.020.
28. Aceto, G.; Persico, V.; Pesce, A. A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-art, Taxonomies, Perspectives, and Challenges. IEEE Commun. Surv. Tutor. 2019, 21, 3467–3501. doi:10.1109/comst.2019.2938259.
29. Atlat, R.; Liu, L.; Wu, J.; Li, G.; Ye, C.; Yang, Y. Big Data Meet Cyber-Physical Systems: A Panoramic Survey. IEEE Access 2018, 6, 73603–73636. doi:10.1109/access.2018.2878681.
30. Babiceanu, R.F.; Seker, R. Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. Comput. Ind. 2016, 81, 128–137. doi:10.1016/j.compind.2016.02.004.
31. Pruski, A.; Berger, M. Design considerations for high-performance Time Sensitive Networking switches. In Proceedings of the 10th International Conference on Networks of the Future (NoF), Rome, Italy, 1–3 October 2019. doi:10.1109/nof47743.2019.9014950.
32. Muguira, L.; Lazaro, J.; Alonso, S.; Astarloa, A.; Rodriguez, M. Secure Critical Traffic of the Electric Sector over Time-Sensitive Networking. In Proceedings of the XXXV Conference on Design of Circuits and Integrated Systems (DCIS), Segovia, Spain, 18–20 November 2020. doi:10.1109/dcisc1330.2020.9268613.
33. Institute of Electrical and Electronics Engineers (IEEE). IEEE 1588-2008—IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. 2008. Available online: https://www.smartgrid.com/documents/ieee_1588_2008_ieee_standard_precision_clock_synchronization_protocol_networked_measurement (accessed on 2 August 2021).
34. International Electrotechnical Comission (IEC). IEC 61850-8-1, “Communication networks and systems in substations —Part 8-1: Specific Communication Service Mapping (SCSM)—Mapping to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2020.
35. International Electrotechnical Comission (IEC). IEC, “Substation Automation System Configuration Description Language”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2018.
37. Adepu, S.; Kandasamy, N.K.; Zhou, J.; Mathur, A. Attacks on smart grid: Power supply interruption and malicious power generation. *Int. J. Inf. Secur.* 2019, 19, 189–211. doi:10.1017/s10207-019-00452-2.

38. Nguyen, T.; Wang, S.; Alhazmi, M.; Nazemi, M.; Estebasi, A.; Dehghanian, P. Electric Power Grid Resilience to Cyber Adversaries: State of the Art. *IEEE Access* 2020, 8, 87592–87608. doi:10.1109/access.2020.2993233.

39. Samiannu, R.; Sampath Kumar, V.; Prasad, J. A critical review of cyber security and cyber-terrorism-threats to critical infrastructure in the energy sector. *IJCS 2018*, 14, 101. doi:10.1504/ijcs.2018.10013025.

40. Bartman, T.; Carson, K. Securing communications for SCADA and critical industrial systems. In Proceedings of the 69th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 4–7 April 2016. doi:10.1109/cpre.2016.7914914.

41. Zhang, Y.; Wang, L.; Xiang, Y.; Ten, C.W. Power System Reliability Evaluation With SCADA Cybersecurity Considerations. *IEEE Trans. Smart Grid* 2015, 6, 1707–1721. doi:10.1109/tsg.2015.2396994.

42. Briesemeister, L.; Cheung, S.; Lindqvist, U.; Valdes, A. Detection, correlation, and visualization of attacks against critical infrastructure systems. In Proceedings of the Eighth International Conference on Privacy, Security and Trust, Ottawa, ON, Canada, 17–19 August 2010. doi:10.1109/pst.2010.5593242.

43. Waterfall Security Solutions Ltd. *Introduction to Waterfall Unidirectional Security Gateways: True Unidirectionality, True Security*; Waterfall Security Solutions Ltd.: Rosh Ha’aiyin, Israel, 2012.

44. Carmo, U.; Sadok, D.H.; Kelner, J. IEC 61850 traffic analysis in electrical automation networks. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, USA, 2–5 November 2015. doi:10.1109/smartgridcomm.2015.7436344.

45. 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. doi:10.1109/tpwrd.2010.2050076.

46. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* 2019, 25, 36–49. doi:10.1016/j.ijcip.2019.01.001.

47. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* 2020, 169, 107094. doi:10.1016/j.comnet.2019.107094.

48. Mashima, D. Securing smart-grid infrastructure against emerging threats. In *Solving Urban Infrastructure Problems Using Smart City Technologies*; Elsevier: Amsterdam, The Netherlands, 2021; pp. 359–382. doi:10.1016/b978-0-12-816816-5.00016-4.

49. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Mali, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* 2020, 77, 103201. doi:10.1016/j.micro.2020.103201.

50. Hong, J.; Chen, Y.; Liu, C.C.; Govindarasu, M. Cyber-Physical Systems Testbed for substations in a power grid. *IEEE Trans. Power Deliv.* 2020, 25, 2376–2383. doi:10.1109/tpwrd.2010.2050076.

51. Wei, M.; Chen, Z. Reliability analysis of cyber security in an electrical power system associated WAN. In Proceedings of the IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 22–26 July 2012. doi:10.1109/pesgm.2015.7286357.

52. Poulsen, K. Slammer Worm Crashed Ohio Nuke Plant Network. 2003. Available online: http://www.securityfocus.com/news/6767 (accessed on 2 August 2021).

53. Al-Rabiaah, S. The “Stuxnet” Virus of 2010 As an Example of A “APT” and Its “Recent” Variances. In *Proceedings of the 15th International Conference on Information and Communications Security*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 261–301. doi:10.1007/978-3-662-45928-7_10.

54. Li, P.; Salour, M.; Su, X. A survey of internet worm detection and containment. *IEEE Commun. Surv. Tutor.* 2008, 10, 20–35. doi:10.1109/comst.2008.4483668.

55. Yang, Y.; Jiang, H.; McLaughlin, K.; Gao, L.; Yuan, Y.; Huang, W.; Sezer, S. Cybersecurity test-bed for IEC 61850 based smart substations. In Proceedings of the IEEE Power & Energy Society General Meeting, Denver, CO, USA, 26–30 July 2015. doi:10.1109/pesgm.2015.7286357.

56. U. S. Department of Homeland Security. ICS-CERT: Industrial Control Systems: Secure Architecture Design. 2018. Available online: https://ics-cert.us-cert.gov/Secure-Architecture-Design (accessed on 2 August 2021).

57. Gavrilut, V.; Pop, P. Traffic-type Assignment for TSN-based Mixed-criticality Cyber-physical Systems. *ACM Trans. Cyber Phys. Syst.* 2020, 4, 1–27. doi:10.1145/3371708.

58. Braendle, M.; Hohlbaur, F.A.F. Cyber Security Practical Considerations for Implementing IEC 62351. 2010. Available online: https://library.e.abb.com/ (accessed on 2 August 2021).

59. Zhou, Z.; Yan, Y.; Ruepp, S.; Berger, M. Analysis and implementation of packet preemption for Time Sensitive Networks. In Proceedings of the IEEE 18th International Conference on High Performance Switching and Routing (HPSR), Campinas, Brazil, 18–21 June 2017. doi:10.1109/hpsr.2017.7968677.

60. Itkin, E.; Wool, A. A Security Analysis and Revised Security Extension for the Precision Time Protocol. *IEEE Trans. Dependable Secur. Comput.* 2020, 17, 22–34. doi:10.1109/tdsc.2017.2748583.

61. Moussa, B.; Robillard, C.; Zugenmaier, A.; Kassouf, M.; Debbabi, M.; Assi, C. Securing the Precision Time Protocol (PTP) Against Fake Timestamps. *IEEE Commun. Lett.* 2019, 23, 278–281. doi:10.1109/11001.2018.2883287.

62. Tsang, J.; Beznosov, K. A Security Analysis of the Precise Time Protocol (Short Paper). In *Information and Communications Security*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 50–59. doi:10.1007/11935308_4.
63. Alghamdi, W.; Schukat, M. Cyber Attacks on Precision Time Protocol Networks—A Case Study. *Electronics* 2020, 9, 1398. doi:10.3390/electronics9091398.

64. DeCusatis, C.; Lynch, R.M.; Kluge, W.; Houston, J.; Wojcik, P.A.; Guendert, S. Impact of Cyberattacks on Precision Time Protocol. *IEEE Trans. Instrum. Meas.* 2020, 69, 2172–2181. doi:10.1109/tim.2019.2918597.

65. Moreira, N.; Lazaro, J.; Jimenez, J.; Idirin, M.; Astarloa, A. Security mechanisms to protect IEEE 1588 synchronization: State of the art and trends. In Proceedings of the IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), Beijing, China, 11–16 October 2015; pp. 115–120. doi:10.1109/ispcs.2015.7324694.

66. Rodriguez, M.; Astarloa, A.; Lazaro, J.; Bidarte, U.; Jimenez, J. System-on-Programmable-Chip AES-GCM implementation for wire-speed cryptography for SAS. In Proceedings of the Conference on Design of Circuits and Integrated Systems (DCIS), Lyon, France, 14–16 November 2018. doi:10.1109/5dcis.2018.8681469.

67. System-on-Chip engineering S.L. SASCrypt: Iec 62351 Substation Automation Systems Cryptographic IP Core. 2018. Available online: https://soc-e.com/products/sascrypt-iec-61850-62351-substation-automation-systems-cryptographic-ip-core/ (accessed on 2 August 2021).

68. Tawde, R.; Nivangune, A.; Sankhe, M. Cyber security in smart grid SCADA automation systems. In Proceedings of the International Conference on Innovations in Electronics, Embedded and Communication Systems (ICIECES), Coimbatore, India, 19–20 March 2015. doi:10.1109/iciiec.2015.7192918.

69. International Electrotechnical Comission (IEC). IEC 62351-3, “Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 3: Communication Network and System Security—Profiles including TCP/IP”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2018.

70. International Electrotechnical Comission (IEC). IEC 62351-4, “Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 4: Profiles Including MMS and Derivatives”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2018.

71. International Electrotechnical Comission (IEC). IEC 62351-5, “Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 5: Security for IEC 60870-5 and Derivatives”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2013.

72. International Electrotechnical Comission (IEC). IEC 62351-6, “Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 6: Security for IEC 61850”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2007.

73. International Electrotechnical Comission (IEC). IEC 62351-7, “Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 7: Network and System Management (NSM) Data Object Models”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2017.

74. International Electrotechnical Comission (IEC). IEC 62351-8, “Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 8: Role-Based access Control”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2011.

75. International Electrotechnical Comission (IEC). IEC 62351-9, “Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 9: Cyber Security Key Management for Power System Equipment”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2017.

76. International Electrotechnical Comission (IEC). IEC 62351-10, “Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 10: Security Architecture Guidelines”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2012.

77. International Electrotechnical Comission (IEC). IEC 62351-11, “Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 11: Security for XML Documents”; International Electrotechnical Comission (IEC): Geneva, Switzerland, 2016.

78. International Electrotechnical Comission (IEC). IEC 62351, Security Standards for the Power. System Information Infrastructure. 2017. Available online: https://webstore.iec.ch/publication/6912 (accessed on 2 August 2021).

79. Kanabar, M.; Cioraca, A.; Johnson, A. Wide Area Protection & Control using high-speed and secured Routable GOOSE Mechanism. In Proceedings of the 69th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 4–7 April 2016. doi:10.1109/cpre.2016.7914928.

80. Urbina, M.; Moreira, N.; Rodriguez, M.; Acosta, T.; Lazaro, J.; Astarloa, A. Secure Protocol and IP Core for Configuration of Networking Hardware IPs in the Smart Grid. *Energies* 2018, 11, 510. doi:10.3390/en11030510.

81. Yiming, A.; Eisaka, T. Support Industrial Hard Real-Time Traffic with Switched Ethernet. In *Embedded Software and Systems*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 671–682. doi:10.1007/11599555_64.

82. Varadarajan, S. Experiences with EtbeReal: A fault-tolerant real-time Ethernet switch. In Proceedings of the EFTF A 2001. 8th International Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No.01TH8597), Antibes-Juan les Pins, France, 15–18 October 2001. doi:10.1109/etfa.2001.996368.