Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems

MIKEL RODRÍGUEZ[1], JESUS LÁZARO[2], UNAI BIDARTE[2], JAIME JIMÉNEZ[2], ARMANDO ASTARLOA[2]

[1] System-on-Chip engineering, Ed. Udondo Planta 6, Ribera de Axpe 50, Erandio, Spain (e-mail: mikel.rodriguez@soc-e.com)
[2] University of the Basque Country UPV/EHU, Escuela de Ingenieria de Bilbao, Edificio I, Plaza Ingeniero Torres Quevedo 1, Bilbao, Spain (e-mail: jesus.lazaro@ehu.eus; unai.bidarte@ehu.eus; jaime.jimenez@ehu.eus; armando.astarloa@ehu.eus)

Corresponding author: Mikel Rodriguez (e-mail: mikel.rodriguez@soc-e.com).

This work has been supported by the Ministerio de Economía y Competitividad of Spain within the project TEC2017-84011-R and FEDER funds, Doctorados Industriales program DI-15-07857 and by the Department of Education, Linguistic Policy and Culture of the Basque Government within the fund for research groups of the Basque university system IT978-16

ABSTRACT International Electrotechnical Commission (IEC) 62351-6 standard specifies the security mechanisms to protect real-time communications based on IEC 61850. Generic Object Oriented Substation Events (GOOSE) and Sampled Value (SV) messages must be generated, transmitted and processed in less than $3\,\mathrm{ms}$, which challenges the introduction of IEC 62351-6. After evaluating the security threats to IEC 61850 communications and the state of the art in GOOSE and SV security, this work presents a novel architecture based on wire-speed processing able to provide message authentication and confidentiality. This architecture has been implemented and tested to evaluate its performance, resource usage, and the latency introduced. Other proposals in the scientific literature do not support real-time traffic, so they are not suitable for GOOSE and SV messages. Whereas the others exceed the target latency of $3\,\mathrm{ms}$ or do not comply with the standards, our design authenticates and encrypts real-time IEC 61850 data in less than $7\,\mu\mathrm{s}$ —predictable latency—, and complies with IEC 62351:2020.

INDEX TERMS Cybersecurity, GOOSE, IEC 61850, IEC 62351, SAS, SV

I. INTRODUCTION

Smart Grid and modern Substation-Automation-Systems (SAS) are considered critical infrastructures by governments and organizations [1]–[4]. Therefore, it is required that they accomplish strong requirements in the fields of reliability, flexibility, efficiency, and interoperability, to guarantee their correct operation. In terms of reliability and interoperability, communications take a key role. IEC has developed the IEC 61850 standard to overcome the interoperability issues in an automated substation among industrial and measurement equipment from different vendors [5]–[7].

IEC 61850 defines the data models, services, and communication protocols that enable the digitalization of electric infrastructures, and integrate the devices which are part of them and the communications within this type of facility. Layer-2 messages are used to provide services that require delivering high-speed (low delay) messages [8]. Specifically, frames must be generated, transmitted, received, and processed by the receiver in less than $3\,\mathrm{ms}$ as shown in table 1. 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.

TABLE 1. IEC 61850 time requirements [8].

Application	Message Type	Time Requirement
Fast Messages	GOOSE	$\leq 3\,\mathrm{ms}$
	GSSE	$\leq 10\,\mathrm{ms}$
Raw Data	SV	$\leq 3\,\mathrm{ms}$
Medium Speed Messages	MMS	$\leq 100\,\mathrm{ms}$
Low Speed Messages	MMS	$\leq 500\,\mathrm{ms}$
Time Synchronization	IEEE 1588	$> 500\,\mathrm{ms}$
File Transfer	MMS	$> 500\,\mathrm{ms}$

Within this group of low-delay services, Generic Substation Events (GSE) is used to provide a mechanism to share event and status data among SAS. GSE can be subdivided into two status/event transmission protocols: Generic Substation State Events (GSSE) and GOOSE. GOOSE messages are generated and received by Intelligent Electronic Devices (IED) in a publisher/subscriber multicast model. These messages do not use mechanisms to confirm delivery. Therefore, GOOSEs are retransmitted several times to provide a certain level of redundancy [9]. To define and encode the structure of the payload of the message, Abstract Syntax Notation One (ASN.1) is used. This way, GOOSE messages generally transmit binary data, such as indications or alarms. Examples of GOOSE usage are breaker failure or automatic transfer of lines.

SV messages allow transmitting sampled digital values in the form of raw data over Ethernet networks. Data are sent in a continuous stream that is divided into layer-2 Ethernet frames. These messages are also encoded using ASN.1 and must be delivered in less than $3\,\mathrm{ms}$. 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. These types of messages are also based on a publisher/subscriber model and are encoded using ASN.1. Therefore, IEDs can be subscribed to streams from selected MUs, to monitor the status of the substation through SVs and control switch breakers or other types of devices using GOOSE messages.

In this context, data authentication and confidentiality are highly desirable features. Unfortunately, the latter has proven to be a harder challenge than the former, since using asymmetric cryptography is not feasible to secure real-time traffic. Even in the newest hardware, the time required to compute Rivest-Shamir-Adleman (RSA) digital signature is still in the order of milliseconds, which is beyond the required latency for GOOSE and SV messages.

Therefore, our research aims to:

- Analyze security threats to IEC 61850 communications, vulnerable to cyber-attacks.
- Evaluate current security solutions for GOOSE and SV messages.
- Provide both data authentication and encryption for real-time IEC 61850 traffic.
- Comply with the suitable standard, IEC 62351:2020.
- Support, in the same Field Programmable Gate Array (FPGA), $1\,\mathrm{Gbit\,s^{-1}}$ of Ethernet data throughput.
- Integrate the design in commercial systems for SAS.

After validating both in simulation and in a real implementation, the resulting design has been made modular, to support future upgrades of the standards, protocols or algorithms. Required performance has been reached by means of parallelization and pipelining in powerful FPGAs. Last but not least, area usage figures show that our solution can be integrated into SAS.

Below, Section II describes potential cyber-threats to IEC 61850 SAS. Section III expounds the features of the IEC 62351-6 standard and its state of the art. The proposed solution is presented in Section IV, measures and results, in V, and is compared in VI. Section VII concludes the article.

II. SECURITY THREATS IN SAS

IEC 61850 defines the communication protocols used in the scope of a substation and opens the path of digitalization and standardization. The progressive integration of the Operational Technology (OT) with the Information Technology (IT) one introduces new vulnerabilities. Information between devices is distributed in the form of Ethernet frames, which can be easily sniffed, altered, or recorded and played back [10]–[12].

IEC 61850 does not specify any cybersecurity mechanism, since the standardization of the security aspects was left to be later defined by the IEC 62351 family of standards. However, IEC 62351 was released several years after IEC 61850, many IEDs from different vendors do not support IEC 62351 [13]. Therefore, alternative security solutions may be combined with the security mechanisms defined in IEC 62351 to protect current and future IEC 61850 based substations. After an extensive analysis of the IEC 62351, authors in [14] describe that the need to preserve partial backward-compatibility has led to some design choices related to the security protocols and standards described in IEC 62351 that provide less security than could have been achieved with a more ambitious approach.

A. HIGH LEVEL VULNERABILITIES

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 of the protocols used. Slammer worm infected a nuclear plant's control system that caused its failure. This cyber-attack bypassed the protection mechanisms and disabled the safety monitoring system for nearly five hours [15]. 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 [16]. Stuxnet was the first known cyber-attack on Supervisory Control And Data Acquisition (SCADA) systems. It was used to get knowledge about the operation of the system, and then to take control of devices in the network and cause their failure.

Previously described events are attacks to high-level communication protocols, devices, and systems that do not have low latency time requirements, as in the case of GOOSE and SV messages. In [17], firewalls, Intrusion Detection Systems (IDS), Anti-Malware software, or patches to the software packages are proposed as key elements to prevent these types of attacks. Furthermore, secure communication protocols, such as Internet Protocol security (IPsec), Media Access Control security (MACsec), or Transport Layer Security (TLS) have also been proposed in the past to protect messages with no real-time requirements [18]. In [19], the use of Virtual Private Networks (VPNs) or almost any kind of tunneling technology over Ethernet is proposed to secure communications between substations.

B. GOOSE AND SV VULNERABILITIES

There are several vulnerabilities of IEC 61850 GOOSE and SV messages that have been discovered by researchers and described in the literature. In [20], a spoofing attack is described where it is possible to send fraudulent GOOSE messages to a receiver. After recording GOOSE traffic, the attacker changes several fields of the messages, such as data values and Sequence Number Value (stNum). Modified messages are sent by the attacker and validated by the receiver if the stNum is higher than the last received message marked as valid and the timestamp of the frame is not older than two minutes. Similarly, authors in [21] and [22] analyze spoofing attacks against IEC 61850 systems.

The lack of security mechanisms for IEC 61850 in the form of message authentication or data encryption allows an attacker to perform injection attacks. As described in [23] and [24], capturing messages sent by a legitimate device in the network gives an attacker the required information to generate fraudulent messages with erroneous content that could cause undesired results such as equipment or service failure. Unlike in the case of spoofing attacks, knowing the stNum and the destination address of the message.

Modifications to the stNum field of GOOSE frames are also used in [25] to perform a Denial of Service (DoS) attack. In this case, the attacker changes the value of the stNum field to $(2^{32} - 1)$, which is the highest value before an overflow happens, forcing the receiver to set its internal counter to that value and rejecting all the legitimate messages received from the sender whose stNum value is smaller.

Flooding attacks in IEC 61850 communication systems are extensively studied in [26] and [27]. They allow an attacker to inject false messages in the network, which could be real messages previously captured with the sole purpose of consuming communication or processing resources that could prevent legitimate messages from being delivered or processed on time. Hussain et al. [28] have reviewed the different security threats and attacks that can be used to compromise IEC 61850 messages. Specifically, GOOSE and SV messages suffer from integrity and availability threats by the means of replay, integrity violation, masquerade, DoS, data manipulation, or false injection. Additionally, GOOSE and SV messages are also sensitive to confidentiality threats, since not having access to the content of the messages prevents an attacker from performing the majority of the attacks previously defined.

As demonstrated by previously discussed cyber-attacks to SAS, they may have several impacts on the behavior of the substation, which can cause malfunction, performance issues, or total failure of part of the communications systems, or even the whole substation. The most common impacts of cyber-attacks are listed below [29]:

- Interruption of monitoring system: IED is not able to receive data from MUs or other IEDs, data are corrupted or IED is unable to process data as expected.
- DoS to control system: IED cannot send control commands to circuit breakers and protection devices or its operation has been modified by an attacker.
- Interruption of protection communication: protection device cannot receive commands from IEDs.
- Undesirable protection operation: protection device receives fake commands or it does not operate 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 substation and the service provided.

III. GOOSE AND SV SECURITY

IEC 62351-6 [30] defines the security procedures for peer-to-peer and Layer-2 profiles such as GOOSE or SVs. On the other hand, IEC 62351-9 [31] defines how to generate, distribute, revoke and handle digital certificates as well as the cryptographic keys that are used to protect IEC 61850 based communications. Other sections of IEC 62351 provide security mechanisms to protect IEC 61850 related communications and services that do not have real-time requirements. Fig. 1 shows how the standards defined in IEC 62351 are mapped to the security layers.

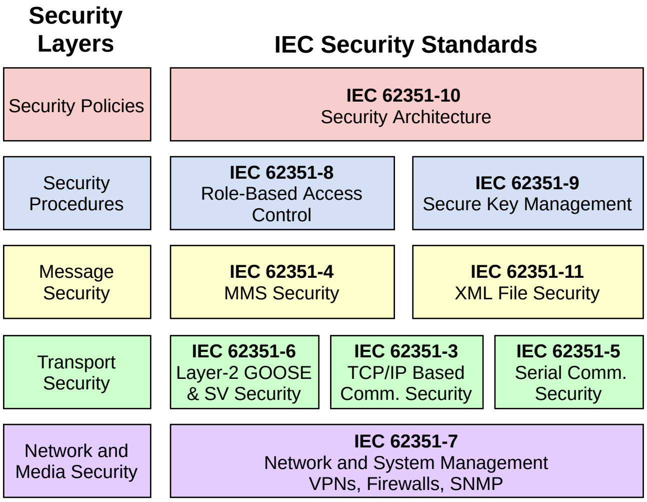

Security Layers
IEC Security Standards
Security Policies
IEC 62351-10 Security Architecture
Security Procedures
IEC 62351-8 Role-Based Access Control
IEC 62351-9 Secure Key Management
Message Security
IEC 62351-4 MMS Security
IEC 62351-11 XML File Security
Transport Security
IEC 62351-6 Layer-2 GOOSE & SV Security
IEC 62351-3 TCP/IP Based Comm. Security
IEC 62351-5 Serial Comm. Security
Network and Media Security
IEC 62351-7 Network and System Management VPNs, Firewalls, SNMP

FIGURE 1. IEC 62351 security layers.

A. IEC 62351-6

To address previously discussed attacks and vulnerabilities of GOOSE and SV messages, IEC released section 6 of the IEC 62351 document. This chapter [30] defines the security procedures for peer-to-peer and layer-2 profiles, such as GOOSE or SVs. Instead of using general-purpose security mechanisms, such as TLS, a specific solution has been designed to make sure that messages with stringent time requirements are delivered on time. In this case, authentication is defined as mandatory. On the other hand, encryption is optional, since the added computational overload could prevent slow devices from meeting the time requirement of $3\,\mathrm{ms}$ to deliver this type of messages. Message authentication is provided by the means of a digital signature using a hash function, which ensures that the data has not been modified by a third party (data integrity) and that the data has been sent by a legitimate device (data authenticity).

Implementing message authentication prevents an attacker from modifying or generating fake messages. However, as data confidentiality (encryption) is only set as optional by the standard, anyone with access to the substation network could capture all the GOOSE and SV messages in the network, to get information about the status and the behavior of the substation. That information could be used by an attacker to determine the best way to exploit possible vulnerabilities in other devices of the substation. Hence, data confidentiality is a highly desirable feature that presents an additional challenge in comparison with integrity and authenticity, as the additional computational overhead introduced needs to be small enough not to compromise the delivery time of the GOOSE and SV messages.

B. STATE OF THE ART IN IEC 62361-6

Since the first version of IEC 62351-6 released in 2007, the research community has analyzed and evaluated its feasibility. In [32], a report of the performance impacts of IEC 62351-6 is carried out. As described by the authors, asymmetric cryptography is not a viable choice for securing real-time traffic, especially in systems with limited computational resources, such as IEDs or MUs. They generate digital signatures using a software implementation of the RSA algorithm, as specified in the standard. Results show that the minimum time needed to generate the digital signature is 1.5 ms, and up to 4 ms when a recommended key length of 1024 bits is used. This demonstrates that implementations of the RSA algorithm for protecting GOOSE and SV messages are non-viable. In [33], the authors present a similar test using the latest hardware available with the aim of evaluating if using high-performance processors could make RSA implementations suitable for protecting GOOSE and SV messages. Results confirm that, even on the latest mainstream hardware, the time required for RSA digital signature computation is still in the order of milliseconds.

As an alternative to RSA, [34] proposes the usage of RSASSA-PSS digital signature algorithm based on RFC 3447. This algorithm demands less processing power and, therefore, is expected to improve the performance achieved with RSA implementations. Results confirm an improvement in comparison with RSA. However, neither RSA nor RSASSA-PSS are fast enough to secure GOOSE or SV messages without compromising the target delivery time of less than 3 ms.

After receiving all the feedback from the scientific and research community about the issues to generate digital signatures for GOOSE and SV messages using the RSA algorithm, IEC has been working on a new version of the current draft. IEC 62351:2020 was released in 2020 and replaced RSA with Secure Hash Algorithm-256 (SHA-256) and Advanced Encryption Standard (AES) Galois Message Authentication Code (AES-GMAC) algorithms as shown in Table 2. These two authentication algorithms are based on symmetric-key cryptography, which reduces computation load in comparison with asymmetric key cryptographic algorithms, such as RSA. Therefore, this change is expected to enable the generation of digital signatures without compromising the time requirements set by IEC 61850 for GOOSE and SV messages. However, symmetric-key cryptography requires that both ends of a communication share a secret key, which increases the complexity of key distribution [31].

TABLE 2. IEC 62351-6 cryptographic algorithms [35].

Algorithm	Bits	Usage	Security
SHA-256	80	Mandatory	Authentication
SHA-256	128	Mandatory	Authentication
SHA-256	256	Mandatory	Authentication
AES-GMAC	64	Mandatory	Authentication
AES-GMAC	128	Mandatory	Authentication
AES-GCM	64	Optional	Authentication & Encryption
AES-GCM	128	Optional	Authentication & Encryption

This new revision of the IEC 62351-6 standard includes AES Galois/Counter Mode (AES-GCM), to allow to provide both data authentication and encryption. This algorithm has proven to be extremely efficient and achieves both high data throughput and low latency when implemented in hardware [5], [36]–[38]. However, encryption is still a challenge. The industry forecasts difficulties to ensure that all the equipment can cipher the traffic. IEC 62351-6 includes encryption as an optional feature.

There are almost no proposals in the literature that have faced the challenge of authenticating and encrypting IEC 61850 GOOSE and SV messages as defined in IEC 62351-6. The majority of the presented solutions just provide data integrity and authentication, but not confidentiality. In [39] authors present a GOOSE and SV authentication framework based on a software implementation. They use the RSA-Probabilistic Signature Scheme based on Signature Scheme with Appendix (RSASSA-PKCS1-v1_5) as the digital signature algorithm. Results show that the RSASSA-PKCS1-v1_5 algorithm is too slow for real-time applications such as GOOSE and SV protection when executed in modern desktop-class processors. They also describe a message protection mechanism based on SHA-256. However, they do not provide performance results for digital signature calculation based on this algorithm. Additionally, in [32] and [33], RSA is used to generate digital signatures to authenticate GOOSE and SV messages. Authors use different families of processors to analyze how digital signature computation time is affected by the computational power of each device. Results show that just server-class Intel Xeon processors can generate the digital signature in less than 1 ms. Finally, GOOSE and SV digital signature based on AES-GMAC and Hash-based Message Authentication Code (HMAC) algorithms is also analyzed. These symmetric-key cryptographic algorithms allow that even low-performance hardware, such as a Raspberry Pi 2 or a BeagleBone, were able to compute the digital signature in a few microseconds. Similarly, in [40], authors use an Intel Celeron processor with 4 GB RAM to evaluate the performance of message authentication using AES-GMAC and HMAC-SHA256 algorithms in low-performance devices. Results show that end-to-end delays for GOOSE messages authenticated with previously described Medium Access Control (MAC) algorithms are within the requirement of 3 ms even in worst-case scenarios.

In [41] authors present their solution to provide authenticity and data encryption to GOOSE and SV messages. According to them, IEC 62351-6 does not specify any method for ensuring confidentiality. However, as shown in Table 2 and previously discussed, AES-GCM is used to provide data encryption and authentication. Furthermore, they propose 3 methods derived from IEC 62351-6 that use AES and SHA-256 to protect communications in three different ways. The first one, which they call Encrypt-then-MAC (EtM), encrypts the GOOSE Application Protocol Data Unit (APDU) using AES, and then calculates the digital signature over the encrypted data, using SHA-256. This requires encrypting data first, and then performing the digital signature calculation in transmission, whereas in reception data can not be decrypted until they have been used for calculating the digital signature. As a consequence, frame protection times can increase significantly. The second method, Encrypt and MAC (E&M), encrypts GOOSE APDU and calculates the digital signature over the unencrypted GOOSE APDU. The problem of this procedure, which is also applicable to EtM, is that, as the GOOSE APDU is encrypted with AES, certain parts of the frame with fixed values will always provide the same result, if they are encrypted with the same key. Therefore, an attacker could use this information to get the secret key and take access to communications. Finally, in MAC then Encrypt (MtE), the digital signature is calculated over GOOSE APDU, and then both GOOSE APDU and security extension are encrypted. This method makes decrypting the frame impossible for the receiver, as the IEC 62351-6 extension where the required cryptographic information is stored has also between encrypted. Additionally, they suggest exploiting several unused bits of the GOOSE and SV frames to specify which method of the three proposed is being performed in each case. As all the presented solutions are modifications of IEC 62351-6, interoperability among devices of different vendors can not be ensured, which is one of the main reasons for the introduction of IEC 61850.

C. IEC 62351-6 SECURITY EXTENSION

IEC 62351-6 presents, a frame extension over a regular GOOSE/SV frame. This security extension is located at the end of the frame and makes compatible the use of insecure IEC 61850 traffic and IEC 62351-6 protected one. Fig. 2 shows the main fields of a GOOSE/SV frame and all the relevant sub-fields necessary for frame protection.

According to the standard, the Ethernet MAC header, composed of the destination and source MAC addresses, as well as the Virtual LAN (VLAN) field, is kept unaltered and transmitted as plaintext to allow network devices, such as switches, to read these fields and forward the frame. The Extended Protocol Data Unit (EPDU) is composed of the Ethertype, Application Identifier (APPID), the length of the APDU, the length of the security extension, and the Cyclic Redundancy Check (CRC) of the Extended Protocol Data Unit (PDU). The main difference to a regular GOOSE/SV frame is that, instead of the length of the security extension and the CRC, those bytes are unused and marked as reserved. All the fields of the extended PDU are used to calculate the authentication signature.

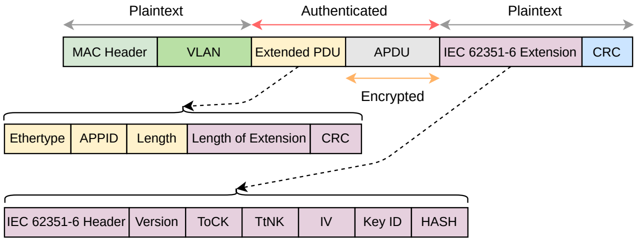


FIGURE 2. IEC 62351-6 security extension.

The GOOSE/SV APDU is not modified when the frame is protected with IEC 62351-6. However, if just authentication is used, all its content is used to calculate the authentication hash. On the other hand, if both encryption and authentication are used, the APDU will be also encrypted to hide its content. Finally, after the APDU there is the IEC 62351-6 security extension, which is encoded according to the ASN.1 Basic Encoding Rules (BER) and is composed of these fields:

- Header: it marks the start of the IEC 62351-6 security extension, as well as the security parameters used.
- Version: it contains the extension protocol version number.
- ToCK: Time of Current Key (ToCK) value represents the seconds since Epoch in which the last key used was marked as valid.
- TtNK: Time to Next Key (TtNK) value represents the seconds remaining until the next key to be used will be marked as valid.
- Initialization Vector (IV): It is an optional field, in case of the MAC or the encryption algorithm, such as AES-GMAC, needs an initialization value.
- Key ID: it identifies the key that has been used to protect the message. This is selected by the sender according to the ones distributed by the Key Distribution Center (KDC) and depending on the content of the frame. This field is required by the receiver to decrypt and authenticate the message.
- HASH: the calculated HMAC value that authenticates all the bytes of the frames starting from the Ethertype and until de APDU (included).

IV. PROPOSED SOLUTION

In this work, a novel hardware architecture in the form of Intellectual Property (IP) core, implementable in FPGA and able to process, cipher, decipher, sign and authenticate GOOSE and SV frames at wire-speed according to IEC 62351:2020 is presented. This proposal aims to overcome the limitations identified in the state of the art to protect this strict real-time traffic.

The proposed hardware architecture has been designed following three main guidelines to face the challenges previously stated:

- Modularity: it must be a modular design that allows future upgrades and modifications. This feature will allow implementing new revisions of the standard, new security algorithms or protocols, as well as modifications for protecting other types of traffic with real-time requirements, such as GOOSE and SV messages.
- Performance: the architecture must make use of advanced hardware designing techniques such as parallelization and pipelining for processing high volumes of data.
- Area usage: the proposed design must achieve the required area usage figures that make viable its implementation in SAS. Therefore, the architecture needs to provide enough computing power to process up to $1\,\mathrm{Gbit\,s^{-1}}$ of Ethernet data. Additionally, it must ensure the applicability of this approach in commercial systems used for SAS.

Secure key distribution is accomplished by a software implementation of IEC 62351-9. As defined by this standard, devices on the substation network are authenticated by the Public Key Infrastructure (PKI) using a one-time password that allows them to get a digitally signed certificate. Using it, the devices ask for the keys to the KDC using Internet Key Exchange (IKE) protocol as part of the Group Domain of Interpretation (GDOI) protocol. The IEC 62351-6 driver integrates the IEC 62351-9 stack to configure the keys and cryptographic information that is required by the proposed architecture to secure GOOSE and SV frames.

Fig. 3 shows the proposed architecture. It is divided into six main sections (represented by letters A-F) that perform a specific task of the process of authenticating and encrypting a GOOSE or SV frame. One of the key features of this architecture is that it follows a mirrored design with the aim of supporting full-duplex operation at wire-speed. Apart from section F, the rest of the architecture consists of 5 sections that are duplicated, one instance is for unprotected traffic that needs to be protected, and the second one is for protected traffic that needs to be unprotected. All these sections and the modules that compose them have been implemented using standard signals by the means of the Advanced eXtensible Interface Stream (AXI-S) interface, which eases the process of adding or replacing any part of the architecture, if required in the future. AXI-S is part of the Advanced Microcontroller Bus Architecture (AMBA) developed by Advanced RISC Machine (ARM) that defines an open-source standard for the connection and management of functional blocks in a SoC [42].

A. PORT INTERFACE

The port interface module implements several interfaces used for the communication between the MAC layer and the Physical (PHY) one, such as Media-Independent Interface (MII) or Gigabit Gigabit Media-Independent Interface (GMII), to name a few, and turn them into AXI-S. This provides an abstraction layer to the rest of the modules in other sections as they only need to implement a single interface. Furthermore, this section of the architecture is also responsible for checking and calculating the Ethernet CRC as well as the Inter-Frame Gap (IFG).

B. FRAME ANALYSIS

The frame analysis module is used to inspect the frames and extract the data. It analyzes each incoming frame to determine if it is a GOOSE, SV, or another type of frame. This task is performed by an advanced parser that can decode ASN.1 data structures, as defined for IEC 61850. The parser can also detect errors in the format or the content of the frame, as well as extract the required data that will be used to protect or verify the frame. In the case of a frame that needs to be protected, the parser divides the data into three types:

- Data that do not need to be processed (Ethernet header, IEC 62351-6 extension, and CRC).
- Data that must be authenticated but not encrypted (EPDU).
- Data that must be encrypted and authenticated (APDU).

On the other hand, in the case of a frame that is already protected and needs to be unprotected, the parser gets all the IEC 62351-6 extension fields in addition to the three data types previously defined. All this information is provided to the encryption/decryption controller module (C) to process it. If the received frame is not a GOOSE or SV frame, it will be directly forwarded to the output without further processing. Additionally, in the case of encryption, a random number generator module is included. It uses a ring oscillator, as defined in [43], to generate true random numbers that, in combination with a counter for each new frame, generate the initialization value required to protect the messages.

C. ENCRYPTION/DECRYPTION CONTROLLER

The encryption/decryption controller acts as an intermediate layer between modules B, D, and F. It gets all the information provided by frame analysis module (B) and generates a request to the lookup engine (section F) to get the cryptographic key associated with the dataset of the frame. If the lookup engine has been configured with a key for the dataset, it will provide it; otherwise, the frame will be forwarded to the output without further processing. If a key is available, this section provides to the AES-GCM engine all the parameters needed to perform frame protection.

D. AES-GCM ENGINE

Fig. 4 shows the internal architecture of the AES-GCM engine, which is a key part of the design. It has been extensively

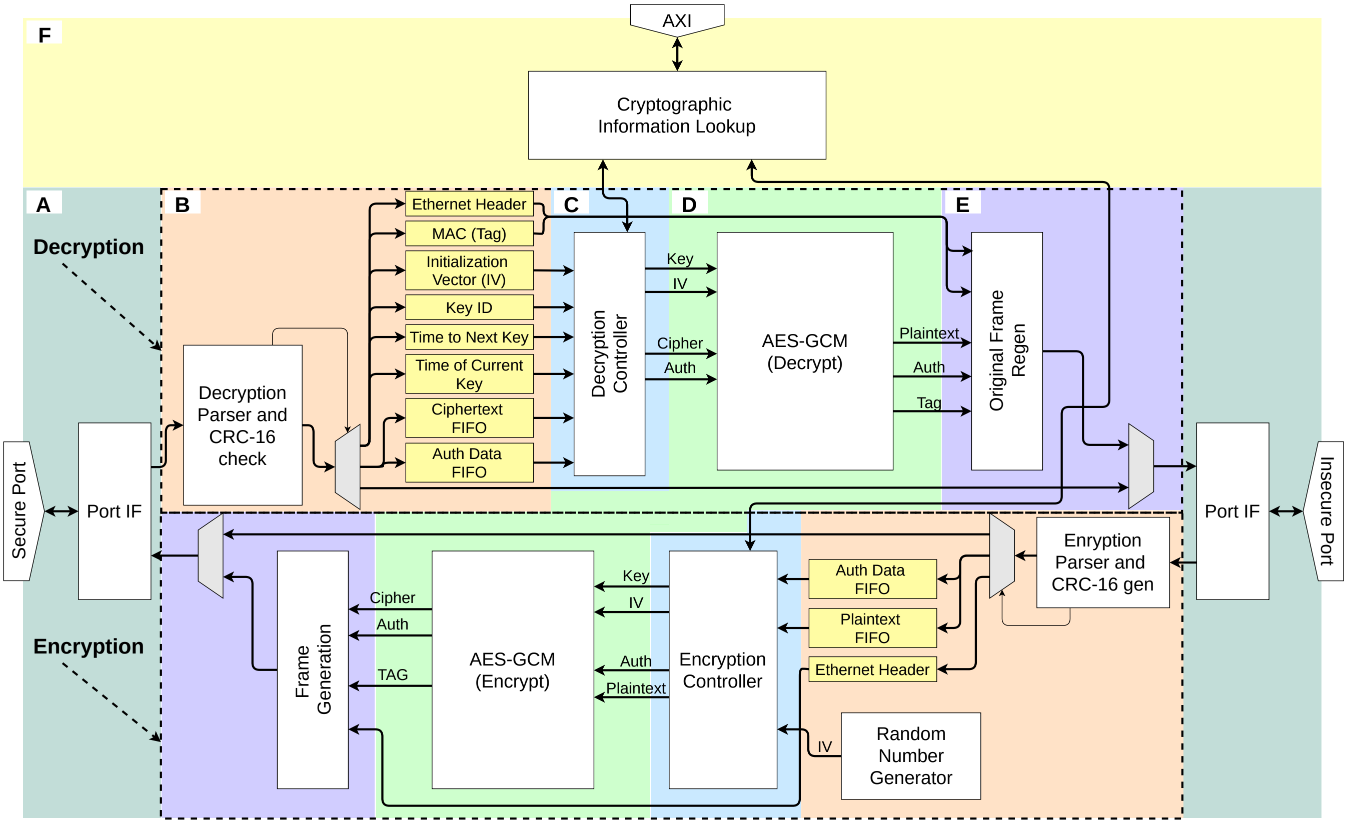


FIGURE 3. IEC 62351-6 proposed architecture.

analyzed in [5] and it has been specifically designed to support different latency/silicon-resources trade-off attending the targeted performance. It has four main phases that are carried out for each frame that needs to be processed:

1) The AES-GCM engine initializes the authentication tag computing logic with the key selected to protect the frame according to its dataset.
2) The data are encrypted/decrypted using the key and the Initialization Vector (IV), in addition to a counter that is set to zero with each new frame and incremented with each word of the frame.
3) The authentication tag is calculated with the data that only need to be authenticated (data that do not need to be encrypted).
4) The authentication tag computing logic is fed with the encrypted data, which are also authenticated.

This module provides as outputs the encrypted or decrypted data (depending on the operation carried out), the data that only has been authenticated, and the authentication tag. The AES-GCM engine can process a 128-bit word each clock cycle which represents a throughput of $16\,\mathrm{Gbit\,s^{-1}}$ with a clock frequency of $125\,\mathrm{MHz}$. As the required throughput is $1\,\mathrm{Gbit\,s^{-1}}$, an instance of the AES-GCM engine is used for encrypting and decrypting data, which reduces resource usage without compromising performance.

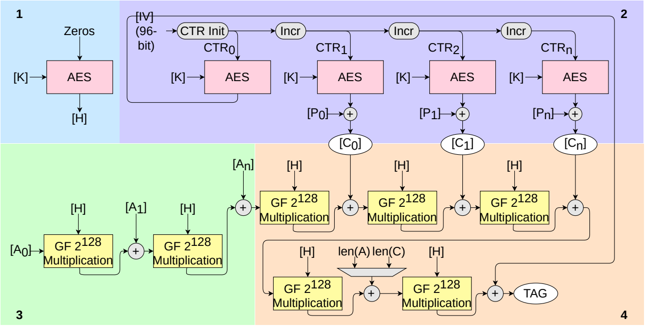


FIGURE 4. AES-GCM cryptographic engine internal architecture.

E. FRAME GENERATOR

The frame generator module receives data from the AES-GCM engine (D) and the frame analysis module (B) to generate the encrypted and authenticated frame or to regenerate the original unprotected frame depending on the use case. This section is also responsible for checking the authentication tag in the case of the decryption process. The received tag is compared to the tag computed by the AES-GCM engine. If they match each other, the frame is reconstructed and forwarded to the output. Otherwise, the frame is discarded as a security measure.

F. LOOKUP ENGINE

Finally, the lookup engine performs two main tasks. First of all, it provides the interface to configure the silicon IP and check its status. Among the configuration parameters, there is the possibility to set all the cryptographic parameters specified by IEC 62351-6 for each dataset that needs to be protected. It is important to note that, as a security measure, this information can only be written, to avoid undesired access to cryptographic keys or other sensitive information stored. The second task is searching the associated key for each GOOSE and SV frame that is received and determining if it must be protected or unprotected.

V. RESULTS

The proposed architecture has been evaluated and validated both in simulation and hardware implementations. To measure timing performance, two test setups are proposed. Simulation-based timing performance analysis allows making high precision timing measurements, within an accuracy level of a clock cycle. On the other hand, hardware testing validates latency measurements obtained in simulation. Finally, functional evaluation of the proposed architecture, as well as its resource usage, has been carried out using a hardware implementation of the silicon IP.

A. SIMULATION-BASED TIMING RESULTS

A simulation setup has been designed to check whether the proposed architecture achieves the low latency values for data protection that allow reaching the target delivery time of 3 ms as set by IEC 61850. The simulation environment has been created with Vivado 2018.3 and consists of 2 instances, A and B, of the IP core, which are interconnected in a daisy chain. Plain GOOSE and SV frames are received from the insecure port of instance A of the IP core. After being processed, protected frames are transmitted through the secure port of instance A of the IP core, which is connected to the secure port of instance B. Finally, after being analyzed and decrypted, unprotected GOOSE and SV frames are transmitted on the insecure port of instance B of the IP core. Result analysis is carried out using the waveform view of the simulation, whereas configuration is made by writing and reading the internal registers of the IP cores from the testbench. Time measurements are taken at the secure and insecure ports of both instances of the IP core.

The test consists of sending two sample frames: a GOOSE frame of 159 B and an SV frame of 156 B. The test is executed 4 times modifying the number of frames sent: 1, 100, 500, and 50000 respectively. Additionally, each test is repeated 5 times modifying the frame injection time to check if IP core performance is altered. To evaluate the proposed architecture in a worst-case scenario, frames are sent back-to-back with an interframe gap of 96 ns. Fig. 5 shows the results achieved from this test.

These results show that the proposed architecture has a predictable response time, achieving always the same latency value for a certain operation, ciphering and deciphering, and certain frame size. Frame encryption and authentication have a latency of 6.743 µs for the SV frame and a value of 6.815 µs for the GOOSE frame. On the other hand, frame decryption and authentication have a latency of 4.256 µs for the SV frame and 4.304 µs for the GOOSE frame. These results show that, for the worst case, which is GOOSE frame encryption and authentication, the latency introduced by the proposed architecture represents just 0.22 % of the target delivery time of 3 ms.

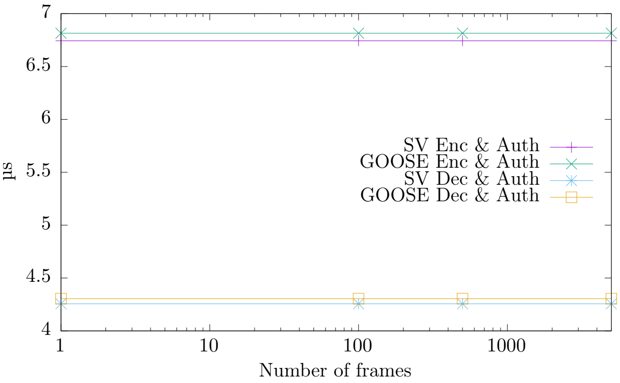


FIGURE 5. IEC 62351-6 encryption/decryption and authentication latency.

This test also shows the wire-speed capability of the proposed architecture. This guarantees resilience against DoS attacks since the core is capable of receiving, processing, and filtering every frame, without droping any.

B. HARDWARE-BASED TIMING RESULTS

This test aims to replicate the latency measurement process that has been carried out in the simulation-based timing test of the IP core. Apart from the IP cores, additional hardware has been added to the design that allows taking high precision timestamps of the inbound and outbound GOOSE and SV frames. Two evaluation boards from SoC-e based on Zynq 7020 FPGA from Xilinx are used. Fig. 6 shows the block diagram of the design implemented inside the FPGA in each board, which has been generated with Vivado 2018.3. The diagram is divided into two main sections: PL and PS. Located in the PL there is the IP core proposed to encrypt and decrypt GOOSE and SV frames. Additionally, four edge detectors have been included to generate a trigger when a frame is received or transmitted by the IP core. Using a 64 bit timer with an accuracy of 8 ns and the outputs from the edge detectors as input, 4 timestamping units store the value of the timer in 4 independent memories each time a frame is transmitted or received. In the ARM CPU located in the PS side of the FPGA, there is a standalone software running that, apart from providing the Command Line Interface (CLI) to configure and check the status of the IP core, also calculates the encryption and decryption latency of the IP core. As PS and PL are interconnected with an Advanced eXtensible Interface (AXI) bus, the CPU can read the timestamp values stored in the memories previously described. Therefore, encryption latency is obtained by calculating the difference between the reception timestamp of the insecure port and the transmission timestamp of the secure port. On the other hand, decryption latency is obtained by calculating the difference between the reception timestamp of the secure port and the transmission timestamp of the insecure port.

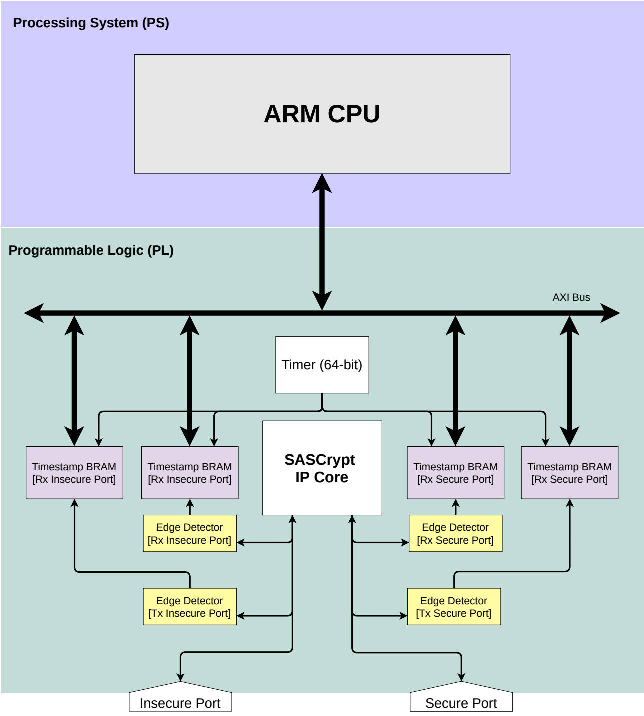

Processing System (PS)
ARM CPU
Programmable Logic (PL)
AXI Bus
Timer (64-bit)
Timestamp BRAM [Rx Insecure Port]
Timestamp BRAM [Rx Insecure Port]
SASCrypt IP Core
Timestamp BRAM [Rx Secure Port]
Timestamp BRAM [Rx Secure Port]
Edge Detector [Rx Insecure Port]
Edge Detector [Rx Secure Port]
Edge Detector [Tx Insecure Port]
Edge Detector [Tx Secure Port]
Insecure Port
Secure Port

FIGURE 6. Hardware-based latency measurement block diagram.

A PC is connected to the CLI of each board and sets the configuration parameters for the test. The same test described in the simulation-test is carried out. Results show a deviation of $\pm\ 8\,\mathrm{ns}$ (a clock period) regarding the latency measures obtained in simulation and represented in Figure 5. This deviation was expected and is caused by the clock domain changes that are necessary to capture the timestamps. Therefore, results show the correlation between simulation and hardware.

C. FUNCTIONAL RESULTS

Fig. 7 shows the test setup used to perform the functional evaluation of the proposed architecture. Devices A and B are two evaluation boards from System-on-Chip engineering (SoC-e) based on Zynq 7020 FPGAs from Xilinx. They implement the proposed architecture as well as standalone software running in the embedded ARM processor of the Zynq FPGA. This software provides a CLI for configuring and checking the status of the IP core. Additionally, a PC is used to get access to the IP core and to configure it. This PC also generates, receives, and captures the GOOSE and SV frames.

This test is divided into four sections. First, PC 1 is used to configure the IP cores on boards A and B using the CLI. The configuration parameters include the datasets to be protected as well as the cryptographic information associated with those datasets. After that, PC 2 is used to inject regular GOOSE and SV frames to the insecure port of device A. The IP core in this board analyzes incoming traffic and protects it according to the configuration. Protected GOOSE and SV frames are transmitted through the secure port of the same device. Next, PC 3 is connected to the path between the secure ports of boards A and B to capture and analyze secure traffic. Finally, device B receives traffic from device A on the secure port. It analyzes the received GOOSE and SV frames and unprotects them according to the configuration previously set. Unprotected GOOSE and SV frames are transmitted on the insecure port of device B and are received by PC 4 that captures them.

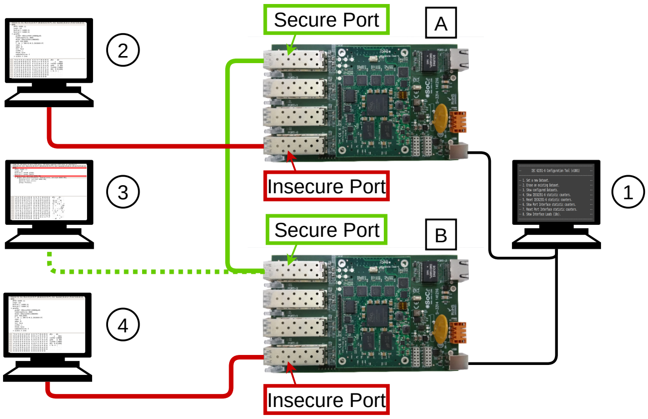
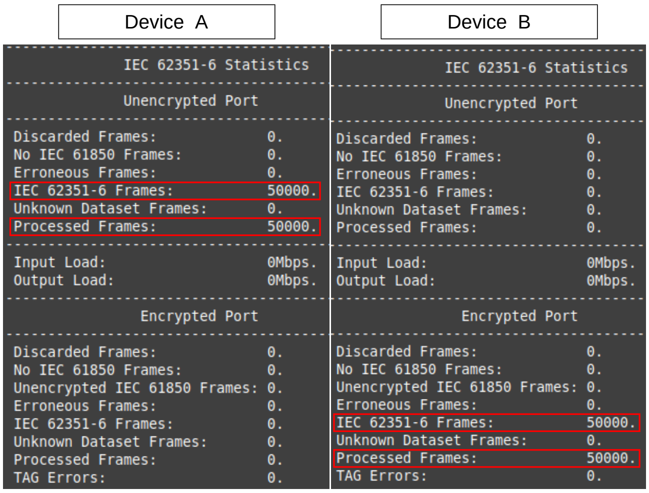


FIGURE 7. IEC 62351-6 test setup.

The test consists of sending 50000 GOOSE frames of the dataset “GEDeviceF650/LLN0$GO$gcb01”. Fig. 8 shows the status information of devices A and B. As it can be seen, device A has received 50000 frames on the insecure port (denoted as processed frames in the figure), all of them being IEC 61850 frames that have been protected (marked as IEC 62351-6 in the figure) and transmitted on the secure port. On the other hand, device B has received 50000 frames on the secure port (denoted as processed frames in the figure) from device A, being all of them IEC 61850 frames protected with IEC 62351-6:2020 security extension (marked as IEC 62351-6 in the figure) that have been unprotected and transmitted on the insecure port of the device.

Fig. 9 shows a Wireshark capture of one of the 50000 frames received by device A on the insecure port and injected by PC 2. It is a plain GOOSE frame. The frame has been divided into 3 sections on the figure. In yellow, there have been highlighted the source and destination MAC addresses. In brown, the extended PDU contains two reserved fields (that will be used in IEC 62351-6). Finally, in green, the GOOSE APDU is composed of several subfields that are the content of the GOOSE frame itself.

Fig. 10 shows a Wireshark capture of the frame shown in Fig. 9, made by PC 3 after it has been processed and secured



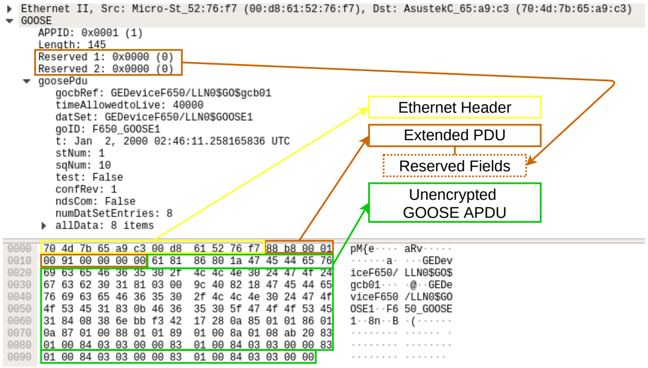
Device A

```
--------------------------------------------
          IEC 62351-6 Statistics
--------------------------------------------
          Unencrypted Port
--------------------------------------------
Discarded Frames:                 0.
No IEC 61850 Frames:              0.
Erroneous Frames:                 0.
IEC 62351-6 Frames:               50000.
Unknown Dataset Frames:           0.
Processed Frames:                 50000.
--------------------------------------------
Input Load:                       0Mbps.
Output Load:                      0Mbps.
--------------------------------------------
          Encrypted Port
--------------------------------------------
Discarded Frames:                 0.
No IEC 61850 Frames:              0.
Unencrypted IEC 61850 Frames:     0.
Erroneous Frames:                 0.
IEC 62351-6 Frames:               0.
Unknown Dataset Frames:           0.
Processed Frames:                 0.
TAG Errors:                       0.
```

Device B

```
--------------------------------------------
          IEC 62351-6 Statistics
--------------------------------------------
          Unencrypted Port
--------------------------------------------
Discarded Frames:                 0.
No IEC 61850 Frames:              0.
Erroneous Frames:                 0.
IEC 62351-6 Frames:               0.
Unknown Dataset Frames:           0.
Processed Frames:                 0.
--------------------------------------------
Input Load:                       0Mbps.
Output Load:                      0Mbps.
--------------------------------------------
          Encrypted Port
--------------------------------------------
Discarded Frames:                 0.
No IEC 61850 Frames:              0.
Unencrypted IEC 61850 Frames:     0.
Erroneous Frames:                 0.
IEC 62351-6 Frames:               50000.
Unknown Dataset Frames:           0.
Processed Frames:                 50000.
TAG Errors:                       0.
```

FIGURE 8. IEC 62351-6 test results (CLI).

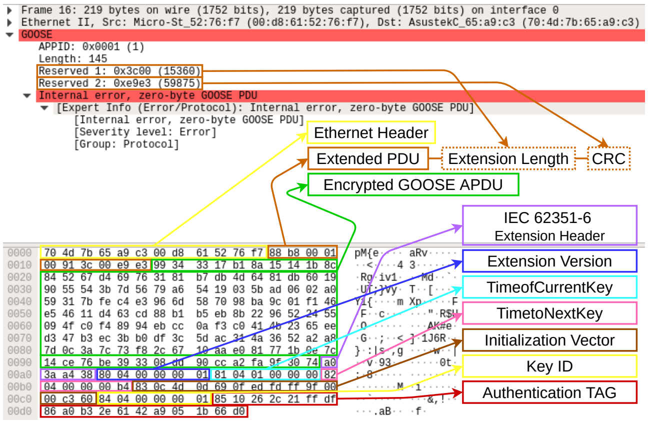


```
▸ Ethernet II, Src: Micro-St_52:76:f7 (00:d8:61:52:76:f7), Dst: AsustekC_65:a9:c3 (70:4d:7b:65:a9:c3)
▾ GOOSE
    APPID: 0x0001 (1)
    Length: 145
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ▾ goosePdu
      gocbRef: GEDeviceF650/LLN0$GO$gcb01
      timeAllowedtoLive: 40000
      datSet: GEDeviceF650/LLN0$GOOSE1
      goID: F650_GOOSE1
      t: Jan  2, 2000 02:46:11.258165836 UTC
      stNum: 1
      sqNum: 10
      test: False
      confRev: 1
      ndsCom: False
      numDatSetEntries: 8
    ▸ allData: 8 items

0000  70 4d 7b 65 a9 c3 00 d8  61 52 76 f7 88 b8 00 01   pM{e···· aRv·····
0010  00 91 00 00 00 00 61 81  86 80 1a 47 45 44 65 76   ······a· ···GEDev
0020  69 63 65 46 36 35 30 2f  4c 4c 4e 30 24 47 4f 24   iceF650/ LLN0$GO$
0030  67 63 62 30 31 81 03 00  9c 40 82 18 47 45 44 65   gcb01··· ·@··GEDe
0040  76 69 63 65 46 36 35 30  2f 4c 4c 4e 30 24 47 4f   viceF650 /LLN0$GO
0050  4f 53 45 31 83 0b 46 36  35 30 5f 47 4f 4f 53 45   OSE1··F6 50_GOOSE
0060  31 84 08 38 6e bb f3 42  17 28 0a 85 01 01 86 01   1··8n··B ·(······
0070  0a 87 01 00 88 01 01 89  01 00 8a 01 08 ab 20 83   ········ ······ ·
0080  01 00 84 03 03 00 00 83  01 00 84 03 03 00 00 83   ········ ········
0090  01 00 84 03 03 00 00 83  01 00 84 03 03 00 00      ········ ·······
```

FIGURE 9. IEC 61850 GOOSE unencrypted frame capture.

by device A. This has several modifications in comparison to the original frame, to be protected as specified in IEC 62351-6. First of all, the reserved fields of the extended PDU are used for the IEC 62351-6 extension length and the CRC respectively.



```
▸ Frame 16: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits) on interface 0
▸ Ethernet II, Src: Micro-St_52:76:f7 (00:d8:61:52:76:f7), Dst: AsustekC_65:a9:c3 (70:4d:7b:65:a9:c3)
▾ GOOSE
    APPID: 0x0001 (1)
    Length: 145
    Reserved 1: 0x3c00 (15360)
    Reserved 2: 0xe9e3 (59875)
  ▾ Internal error, zero-byte GOOSE PDU
    ▾ [Expert Info (Error/Protocol): Internal error, zero-byte GOOSE PDU]
        [Internal error, zero-byte GOOSE PDU]
        [Severity level: Error]
        [Group: Protocol]

0000  70 4d 7b 65 a9 c3 00 d8  61 52 76 f7 88 b8 00 01   pM{e···· aRv·····
0010  00 91 3c 00 e9 e3 99 34  33 17 b1 8a 15 14 1b 8c   ··<···4 3·······
0020  84 52 67 d4 69 76 31 81  b7 db 4d 64 81 db 60 19   ·Rg·iv1· ··Md··`·
0030  90 55 54 3b 7d 56 79 a6  54 19 03 5b ad 06 02 a0   ·UT;}Vy· T··[····
0040  59 31 7b fe c4 e3 96 6d  58 70 98 ba 9c 01 f1 46   Y1{····m Xp·····F
0050  e5 46 11 d4 63 cd 88 b1  b5 eb 8b 22 96 52 24 55   ·F··c··· ···"·R$U
0060  09 4f c0 f4 89 94 eb cc  0a f3 c0 41 4b 23 65 ee   ·O······ ···AK#e·
0070  d3 47 b3 ec 3b b0 df 3c  5d ac 31 4a 36 52 a2 a8   ·G··;··< ]·1J6R··
0080  7d 0c 3a 7c 73 f8 2c 67  10 aa e0 81 77 1b 0e 7c   }·:|s·,g ····w··|
0090  14 ce 76 be 39 33 08 dd  90 cc a2 fa 9f 30 74 a0   ··v·93·· ·····0t·
00a0  3a a4 38 80 04 00 00 00  01 81 04 01 00 00 00 82   :·8····· ········
00b0  04 00 00 00 b4 83 0c 4d  0d 69 0f ed fd ff 9f 00   ·······M ·i······
00c0  00 c3 60 84 04 00 00 00  01 85 10 26 2c 21 ff df   ··`····· ···&,!··
00d0  86 a0 b3 2e 61 42 a9 05  1b 66 d0                  ····.aB·· ·f·
```

FIGURE 10. IEC 61850 GOOSE encrypted frame capture (IEC 62351-6).

Furthermore, GOOSE APDU is now encrypted (content is unreadable), which is the reason why Wireshark marks that the frame has an internal error. Finally, after the encrypted GOOSE APDU, there is the IEC 62351-6:2020 security extension. It contains all the fields specified by the standard as shown in Fig. 2. It is important to note that, since AES-GCM has been chosen as the cryptographic algorithm, the optional IV field also needs to be used.

D. AREA OCCUPATION

Using the test setup presented in Fig. 7, the evaluation of the silicon (FPGA) resources for a complete implementation of the proposed architecture has been made. Apart from the IEC 62351-6 security IP core, the design includes a hardware IP for high-availability Ethernet networking supporting High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) protocols (IEC 62439-3). It also includes a hardware IP to provide sub-microsecond level time accuracy, using the IEEE 1588 mechanism. These functionalities are specified by IEC 61850 and must be implemented in IEDs of SAS.

Table 3 shows that GOOSE and SV frame security, communications redundancy as well as time synchronization can fit in a Xilinx Zynq-7020 device. This family of low-cost FPGAs is suitable for IEDs in SAS, due to their ability to provide hardware acceleration for several protocols; at the same time, they include an embedded dual-core ARM processor and low power consumption.

TABLE 3. Resource usage of each functionality for a Xilinx Zynq-7020.

Functionality	LUTs	Registers	BRAM
IEEE 1588	2631 (4.95 %)	1191 (1.12 %)	0
IEC 62439-3	13986 (26.29 %)	14431 (13.56 %)	41.5 (29.64 %)
IEC 62351-6	29071 (54.64 %)	29997 (28.19 %)	85.5 (61.07 %)

VI. COMPARISON

In this section results achieved by this work are compared with the state-of-the-art publications in the field of IEC 62351-6 GOOSE and SV frame security. The first five entries of Table 4 are software and hardware implementations of digital signatures to provide data authentication. None of them implements message encryption. Furthermore, the authors do not provide maximum throughput supported values, so it is not possible to know if the performance could be affected depending on the load. Additionally, all of the software-based implementations are not able to provide a fixed latency value: the results depend on the tasks being executed by the processor. Finally, all of them fail to generate the digital signature fast enough to meet the 3 ms delivery time, as almost all of them are well above 1 ms. In the context of delivering these messages without security, it is estimated in the Smart-Grid sector a computation time of 1.2 ms for the message processing by the sender and 1.2 ms for the message processing by the receiver. Therefore, only the remaining time (0.6 ms) is available for the communications.

The overhead added by the security mechanism shall fit in the minimum portion of these $0.6\,\mathrm{ms}$.

Therefore, none of the proposals presented in [32] - [34] are valid to protect GOOSE and SV messages.

Authors in [41] present the only proposal found in the literature for authenticating and encrypting GOOSE and SV messages. They describe three methods based on encryption, using AES and authentication generating a digital signature with SHA-256. Although the latency figures presented are low enough to allow frame encryption and authentication without compromising frame delivery time, all of the proposed methods use modifications over IEC 62351-6. However, the main drawbacks of these approaches are the lack of interoperability and their behavior at high-line rates. This second limitation impacts specifically when multiple SV streams are present in the same network. Therefore, it is impossible to evaluate if the solution is suitable for a real Ethernet network where a data throughput of hundreds of Mbps or even $1\,\mathrm{Gbit\,s^{-1}}$ can be reached. Finally, as AES is used as the encryption algorithm, the cryptographic keys are vulnerable to being known by an attacker. In AES, a certain plaintext input always produces the same ciphertext output. As GOOSE and SV frames have fixed fields that always contain the same value, an attacker could use that information to guess the cryptographic key used to protect the communications.

VII. CONCLUSIONS

This paper presents a novel hardware architecture that can provide data integrity and confidentiality without compromising the message delivery time of $3\,\mathrm{ms}$ set by IEC 61850. The presented solution is fully IEC 62351-6 compliant and only introduces a latency of a few microseconds, which is several orders of magnitude below the requirement, ensuring that messages are delivered on time even in worst-case scenarios. The proposed architecture always has a fixed latency for a certain frame size, which provides a predictable behavior, essential for real-time messages. Additionally, performance and resource usage tests have shown that the silicon IP can process up to $1\,\mathrm{Gbit\,s^{-1}}$ of sustained Ethernet traffic, and that it can be implemented in a cost-effective FPGA family, alongside other redundancy and synchronization protocols used for SAS. Therefore, this work shows for the first time that data authentication and encryption can be implemented for GOOSE and SV messages as defined in IEC 62351-6:2020 standard.

In the future, we plan to evaluate other security algorithms defined in the IEC 62351-6:2020 standard and check their feasibility to accomplish the mandatory delivery time of $3\,\mathrm{ms}$. At the same time, interoperability with other suppliers shall be always ensured.

REFERENCES

[1] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, “A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services,” IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3453–3495, 2018. [Online]. Available: https://doi.org/10.1109%2Fcomst.2018.2855563

[2] S. Adepu, N. K. Kandasamy, J. Zhou, and A. Mathur, “Attacks on smart grid: power supply interruption and malicious power generation,” International Journal of Information Security, vol. 19, no. 2, pp. 189–211, Jul. 2019. [Online]. Available: https://doi.org/10.1007%2Fs10207-019-00452-z

[3] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, “Electric power grid resilience to cyber adversaries: State of the art,” IEEE Access, vol. 8, pp. 87 592–87 608, 2020. [Online]. Available: https://doi.org/10.1109%2Faccess.2020.2993233

[4] R. Samikannu, V. S. Kumar, and J. Prasad, “A critical review of cyber security and cyber terrorism - threats to critical infrastructure in the energy sector,” International Journal of Critical Infrastructures, vol. 14, no. 2, p. 101, 2018. [Online]. Available: https://doi.org/10.1504%2Fijcis.2018.10013025

[5] M. Rodriguez, A. Astarloa, J. Lazaro, U. Bidarte, and J. Jimenez, “System-on-programmable-chip AES-GCM implementation for wire-speed cryptography for SAS,” in 2018 Conference on Design of Circuits and Integrated Systems (DCIS). IEEE, Nov. 2018. [Online]. Available: https://doi.org/10.1109%2Fdcis.2018.8681469

[6] R. P. Gupta, “Substation automation using iec 61850 standard,” in Fifteenth National Power Systems Conference (NPSC), IIT Bombay, Dec. 2008. [Online]. Available: http://www.krec.ir/Automation/Substation_Automation_Using_IEC61850_Standard.pdf

[7] R. E. Mackiewicz, “Overview of IEC 61850 and benefits,” in 2006 IEEE PES Power Systems Conference and Exposition. IEEE, 2006. [Online]. Available: https://doi.org/10.1109%2Fpsce.2006.296392

[8] 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.”

[9] ——, “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.”

[10] T. Bartman and K. Carson, “Securing communications for SCADA and critical industrial systems,” in 2016 69th Annual Conference for Protective Relay Engineers (CPRE). IEEE, Apr. 2016. [Online]. Available: https://doi.org/10.1109%2Fcpre.2016.7914914

[11] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, “Power system reliability evaluation with SCADA cybersecurity considerations,” IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 1707–1721, Jul. 2015. [Online]. Available: https://doi.org/10.1109%2Ftsg.2015.2396994

[12] L. Briesemeister, S. Cheung, U. Lindqvist, and A. Valdes, “Detection, correlation, and visualization of attacks against critical infrastructure systems,” in 2010 Eighth International Conference on Privacy, Security and Trust. IEEE, Aug. 2010. [Online]. Available: https://doi.org/10.1109%2Fpst.2010.5593242

[13] U. Carmo, D. H. Sadok, and J. Kelner, “IEC 61850 traffic analysis in electrical automation networks,” in 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, Nov. 2015. [Online]. Available: https://doi.org/10.1109%2Fsmartgridcomm.2015.7436344

[14] R. Schlegel, S. Obermeier, and J. Schneider, “A security evaluation of IEC 62351,” Journal of Information Security and Applications, vol. 34, pp. 197–204, Jun. 2017. [Online]. Available: https://doi.org/10.1016%2Fj.jisa.2016.05.007

[15] P. K, “Slammer worm crashed Ohio nuke plant network,” Aug. 2003. [Online]. Available: http://www.securityfocus.com/news/6767

[16] D. Kushner, “The real story of stuxnet,” IEEE Spectrum, vol. 50, no. 3, pp. 48–53, Mar. 2013. [Online]. Available: https://doi.org/10.1109%2Fmspec.2013.6471059

[17] A. Elgargouri, R. Virrankoski, and M. Elmusrati, “IEC 61850 based smart grid security,” in 2015 IEEE International Conference on Industrial Technology (ICIT). IEEE, Mar. 2015. [Online]. Available: https://doi.org/10.1109%2Ficit.2015.7125460

[18] N. R. Indukuri, “Layer 2 security for smart grid networks,” in 2012 IEEE International Conference on Advanced Networks and Telecommunciations Systems (ANTS). IEEE, Dec. 2012. [Online]. Available: https://doi.org/10.1109%2Fants.2012.6524237

[19] C. Diago and A. Forshaw, “Cybersecurity for shared infrastructure substation networks with IEC 61850 GOOSE and sampled values,” The

TABLE 4. Comparison of IEC 62351-6 GOOSE and SV frame security implementation proposals.

Reference	Algorithm	Functionality	Implementation	Max. Latency ms	Delivery Time Usage	Max. Throughput	Fixed Latency	IEC 62351-6 Compliant
[32]	RSA	Auth	SW	4.000	133.00 %	-	No	No (Time)
[32]	RSA	Auth	HW	1.917	63.90 %	-	Yes	No (Time)
[33]	RSA	Auth	SW	6.000	200.00 %	-	No	No (Time)
[34]	RSASSA-P	Auth	SW	0.942	31.40 %	-	No	No (Time)
[34]	KCS1-v1_5	Auth	SW	3.560	118.70 %	-	No	No (Time)
[41]	EtM (AES &SHA-256)	Auth & Enc	SW	0.242	8.07 %	-	No	No (Format)
[41]	E&M (AES &SHA-256)	Auth & Enc	SW	0.235	7.83 %	-	No	No (Format)
[41]	MtE (AES & SHA-256)	Auth & Enc	SW	0.284	9.47 %	-	No	No (Format)
This work	AES-GCM	Auth & Enc	HW	0.006	0.23 %	>1 Gbit s^{-1}	Yes	Yes

Journal of Engineering, vol. 2018, no. 15, pp. 1195–1198, Aug. 2018. [Online]. Available: https://doi.org/10.1049%2Fjoe.2018.0150

[20] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in 2012 IEEE Globecom Workshops. IEEE, Dec. 2012. [Online]. Available: https://doi.org/10.1109%2Fglocomw.2012.6477809

[21] M. Kabir-Querrec, S. Mocanu, P. Bellemain, J.-M. Thiriet, and E. Savary, "Corrupted GOOSE Detectors: Anomaly Detection in Power Utility Real-Time Ethernet Communications," in GreHack 2015. Grenoble, France: Verimag, Nov. 2015. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01237725

[22] J. Noce, Y. Lopes, N. C. Fernandes, C. V. N. Albuquerque, and D. C. Muchaluat-Saade, "Identifying vulnerabilities in smart gric communication networks of electrical substations using GEESE 2.0," in 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE). IEEE, Jun. 2017. [Online]. Available: https://doi.org/10.1109%2Fisie.2017.8001232

[23] J. G. Wright and S. D. Wolthusen, "Stealthy injection attacks against IEC61850's GOOSE messaging service," in 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, Oct. 2018. [Online]. Available: https://doi.org/10.1109%2Fisgteurope.2018.8571518

[24] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in 2016 IEEE Power and Energy Society General Meeting (PESGM). IEEE, Jul. 2016. [Online]. Available: https://doi.org/10.1109%2Fpesgm.2016.7741747

[25] N. Kush, M. Branagan, E. Foo, and E. Ahmed, "Poisoned goose : exploiting the goose protocol," vol. 149, 01 2014.

[26] F. Zhang, M. Mahler, and Q. Li, "Flooding attacks against secure time-critical communications in the power grid," in 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, Oct. 2017. [Online]. Available: https://doi.org/10.1109%2Fsmartgridcomm.2017.8340726

[27] Q. Li, C. Ross, J. Yang, J. Di, J. C. Balda, and H. A. Mantooth, "The effects of flooding attacks on time-critical communications in the smart grid," in 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, Feb. 2015. [Online]. Available: https://doi.org/10.1109%2Fisgt.2015.7131802

[28] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 5643–5654, Sep. 2020. [Online]. Available: https://doi.org/10.1109%2Ftii.2019.2956734

[29] Y. Yang, H. T. Jiang, K. McLaughlin, L. Gao, Y. B. Yuan, W. Huang, and S. Sezer, "Cybersecurity test-bed for IEC 61850 based smart substations," in 2015 IEEE Power & Energy Society General Meeting. IEEE, Jul. 2015. [Online]. Available: https://doi.org/10.1109%2Fpesgm.2015.7286357

[30] International Electrotechnical Comission (IEC), "IEC 62351-6, "Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850"," 2007.

[31] ——, "IEC 62351-9, "Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment"," 2017.

[32] M. Braendle and F. A. F. Hohlbaum, "Cyber security practical considerations for implementing iec 62351," https://library.e.abb.com/, 2010.

[33] D. Ishchenko and R. Nuqui, "Secure communication of intelligent electronic devices in digital substations," in 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). IEEE, Apr. 2018. [Online]. Available: https://doi.org/10.1109%2Ftdc.2018.8440438

[34] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages," IEEE Access, vol. 7, pp. 32 343–32 351, 2019. [Online]. Available: https://doi.org/10.1109%2Faccess.2019.2902571

[35] International Electrotechnical Comission (IEC), "IEC 62351-6, "Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850"," draft, 2020.

[36] E. B. Kavun, N. Mentens, J. Vliegen, and T. Yalcin, "Efficient utilization of DSPs and BRAMs revisited: New AES-GCM recipes on FPGAs," in 2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig). IEEE, Dec. 2019. [Online]. Available: https://doi.org/10.1109%2Freconfig48160.2019.8994730

[37] B. Buhrow, K. Fritz, B. Gilbert, and E. Daniel, "A highly parallel AES-GCM core for authenticated encryption of 400 gb/s network protocols," in 2015 International Conference on ReConFigurable Computing and FPGAs (ReConFig). IEEE, Dec. 2015. [Online]. Available: https://doi.org/10.1109%2Freconfig.2015.7393321

[38] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Efficient and high-performance parallel hardware architectures for the AES-GCM," IEEE Transactions on Computers, vol. 61, no. 8, pp. 1165–1178, Aug. 2012. [Online]. Available: https://doi.org/10.1109%2Ftc.2011.125

[39] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "S-GoSV: Framework for generating secure IEC 61850 GOOSE and sample value messages," Energies, vol. 12, no. 13, p. 2536, Jul. 2019. [Online]. Available: https://doi.org/10.3390%2Fen12132536

[40] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, "Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security," IEEE Access, vol. 7, pp. 80 980–80 984, 2019. [Online]. Available: https://doi.org/10.1109%2Faccess.2019.2923728

[41] ——, "A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages," IEEE Transactions on Power Delivery, vol. 35, no. 5, pp. 2565–2567, Oct. 2020. [Online]. Available: https://doi.org/10.1109%2Ftpwrd.2020.2990760

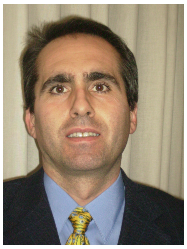
[42] ARM Inc. (2010) AMBA® 4 AXI4-Stream Protocol, Version 1.0. [Online]. Available: https://static.docs.arm.com/ihi0051/a/IHI0051A_amba4_axi4_stream_v1_0_protocol_spec.pdf

[43] N. N. Anandakumar, S. K. Sanadhya, and M. S. Hashmi, "FPGA-based true random number generation using programmable delays in oscillator-rings," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 3, pp. 570–574, Mar. 2020. [Online]. Available: https://doi.org/10.1109%2Ftcsii.2019.2919891

MIKEL RODRÍGUEZ received the B.S. in telecommunications engineering from the University of the Basque Country, Spain, in 2013 and the M.S. in telecommunications engineering from the University of Deusto, Spain, in 2015. He is currently pursuing a Ph.D. degree in telecommunications engineering at the University of the Basque Country, Spain. His research is based on the protection of real-time critical communications in the Electric sector. Since 2015 he has been working as a Research & Development engineer at System-on-Chip engineering S.L. (soc-e.com), a supplier of leading-edge networking and synchronization solutions based on FPGA technology. He has been involved in the development of new IP cores and technologies that enable secure and redundant communications as well as nanosecond level synchronization for a wide range of sectors, such as Aerospace or Industry.

DR. JESÚS LÁZARO received the M.S. and Ph.D. degrees in telecommunications engineering from the University of the Basque Country, Spain, in 2001 and 2005. In 2001, he started at the Telecommunications Department of the University of the Basque Country as a Researcher and Lecturer. Since 2019 hi is a Full Professor. In 2010, he was a Research Visitor at the Configurable Computing Lab of Virginia Tech. He is a member of the Applied Electronics Research Team and co-founder and entrepreneur of System-on-Chip engineering S.L. (soc-e.com). He has participated in 44 competitive research projects supported by public institutions and 44 private research contracts, in 19 of them as main researcher. He is the author or co-author of 4 patents, 35 articles in scientific international magazines, and 90 papers in national and international conferences. His main areas of research are high-speed circuits based on reconfigurable devices and communications devices.

DR. UNAI BIDARTE received the M.Sc. and Ph.D. degree in Telecommunication Engineering from the University of the Basque Country, Spain, in 1996 and 2004 respectively. From 1999 to 2008, he was an Assistant Professor in electronic technology at the Electronics and Telecommunications Department of the University of the Basque Country. In 2009, he became Associate Professor. He is a researcher of the Applied Electronics Research Team and he has participated in more than 30 research projects supported by public institutions and more than 20 by private companies. He is co-author of 3 patents, more than 10 papers in international magazines indexed in Journal Citation Reports (JCR) Science Citation Index of ISI Web of Knowledge, and more than 60 contributions to other magazines and conferences.



DR. JAIME JIMÉNEZ received the M.S. and Ph.D. degrees in telecommunications engineering from the University of the Basque Country, Spain, in 1991 and 2005, respectively. In 1998, he started at the Telecommunications Department of the University of the Basque Country as a Researcher and Lecturer. In 2007, he was a Research Visitor at the Ecole Supérieure des Technologies Industrielles Avancées (Bidart, France). He is a member of the Applied Electronics Research Team and co-founder and entrepreneur of System-on-Chip engineering S.L. (soc-e.com). He has participated in 45 competitive research projects supported by public institutions and in 39 private research contracts, in 11 of them as main researcher. He is the author or co-author of 23 articles in scientific international magazines and 77 papers in international conferences. His main areas of research are high-speed circuits based on reconfigurable devices and communications devices.

DR. ARMANDO ASTARLOA received the M.Sc. and Ph.D. degree in Electrical Engineering from the University of the Basque Country (UPV/EHU), Spain, in 1999 and 2005 respectively. After several years developing his professional career as hardware engineer in the private sector, in 2001 he joined the staff of the UPV/EHU in the School of Engineering of Bilbao as a full-time researcher and lecturer. He is founding member of the Research Applied Electronics Research Team (APERT) and his research topics include reliable electronic design for reconfigurable devices, industrial networking, and cybersecurity. He is author of dozens of technical contributions in international scientific journals, conferences, book chapters, patents and he collaborate as committee member in IEC working groups. In 2008 he enrolled in the Institute of Microelectronics and Wireless Systems in Ireland as a visiting researcher. In 2010, he launched System-on-Chip engineering S.L. (SoC-e.com) business project, and he hold the CEO position at this company from 2016 to 2020. In 2021, he achieved the position of Full Professor at the UPV/EHU.

• • •