Wire-speed Cryptographic Technology for Substation Automation Systems

System-on-Chip engineering
Web: http://soc-e.com | Email: info@soc-e.com

***Abstract*—Nowadays, cyber-security in critical infrastructures is more and more important. Most governments have launched specific security programs to define the protection of the Electric Grid, and some recent attacks like the one suffered by Ukrainian Grid emphasize this need for security. In these critical systems, it is necessary to define a complex multi-layered cyber-security approach that covers from the electronic device up to the cloud. SoCe proposes an innovative technology to face the challenge of securing Time Critical Layer 2 communications like GOOSE and SMV messages used in the context of IEC 61850 and Smart Grid.**

I. Introduction

Communication networks in conjunction with cyber-security are critical parts in the deployment of reliable and efficient Substation Automation Systems (SAS). More recently, a serious attack to Ukrainian Electric Grid has revealed the importance of enforcing security policies in critical infrastructures [1].

Figure 1. Electric Substation.

This security issue is very complex and it needs to be faced from a multi-layered approach: devices, systems, networks, users, software applications, etc. In last ten years, the International Electrotechnical Commission (IEC) have put a great effort concerning cyber-security on the electric utility industry [2]. IEC 62351 family of standards addresses security issues for the different power system operations and communication standards defined by the IEC TC57 working group [3].

These standards have focused on the specific protocols and applications used in SAS. The applications based on MMS should include data confidentiality in addition to authentication and they are secured at application and transport levels as described in IEC 62351-3/4 [3]. End-to-end authentication is provided using Transport Layer Security (TLS) and some of the included cryptographic algorithms are RSA for key exchange, Advanced Encryption Standard (AES) for data encryption and SHA for message authentication.

Furthermore, the IEC working group is now working on the IEC 62351-9 standard regarding the utilization of the Group Domain of Interpretation (GDOI) for key management, which is expected to be published in 2017.

In particular, IEC 62351-6 [4] standard specifies the security mechanisms for protecting IEC 61850 communications [5] that are not based on TCP/IP. It specifies the protection of GOOSE and SV messages with message authentication codes using the Secure Hash Algorithm (SHA), which are digitally signed using RSA (Rivest, Shamir and Adleman) public-key cryptosystem to provide source authenticity. However, RSA digital signatures have long execution times that do not allow to meet timing requirements: even though a high-end ARM processor with a crypto accelerator were employed, RSA signature with 1024-bit keys cannot be computed within the maximum transfer time required by some GOOSE messages [6].

The IEC 62351-6 is planned to be updated shortly based on security requirements defined in IEC 61850-90-5 [7], where symmetric cryptography rather than digital signatures is proposed in order to minimize the negative impact of security measures on field devices performance.

II. Substation Automation Systems (SAS) Crypto-core IP for wire-speed processing

Taking into the account the context of SAS, the applications with strong timing requirements use GOOSE messages and SMV, in which data is directly mapped to the Ethernet data link layer in order to facilitate an agile processing. A critical example is a GOOSE tripping message in Class P2/3 Substations with a response time of less than 3 ms between applications in two different IEDs. For the Sample Measured Value (SVM) messages, in addition to the response time requirement, high volumes of data are generated by the Merging Unit under regular operation.

The need for security in these time-critical messages has generated an out-standing technical challenge that needs to be solved using innovative hardware and software

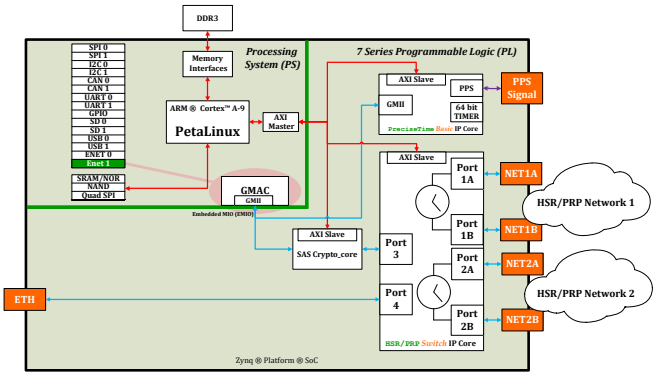

Figure 2. New generation SoC based IEDs.

approach.

SoCe **proposal to secure the frames is based on integrating the frame processing in the same Silicon area where the switching logic is implemented. Therefore, cipher and decipher operations are done within the same datapath of the information, by hardware and at wire-speed. This architecture is deterministic and it is able to fulfil the strict Real Time timing requirements defined in the SAS standard in contrast with the acceleration provided by the general purposed crypto-cores embedded in many microprocessors.**

Thanks to this approach, the complexity of the security is abstracted for the IEC 61850 Software. The implementation of this solution takes benefit from the latest technology on embedded devices. Newest IEDs have adopted reconfigurable platforms to implement the FPGA section the signal processing, synchronization and low latency and high availability networking combined with these on-the-fly ciphers. Indeed, SoCe switching IPs for high-availability Ethernet (HSR/PRP) networking and for synchronization (IEEE 1588) are widely integrated worldwide in products for the the Electric Sector (IEDs, MUs, Relays, Gateways, Smart-Transformers, etc.).

Figure 2 shows a high-level block diagram of SoC implementation for a new-generation IED including the IEEE 1588 support, HSR/PRP and SAS Crypto-core IP.

SAS Crypto-core IP includes a high-level configuration tool that can be used to define the format of the Layer 2 Frame that should be processed for ciphering and deciphering purposes. This tool configures the *generics* infrastructure for the IP that is used at synthesis time to generate an specific hardware IP customized for that frame format. This flexibility will be extremely useful to adapt SAS IP to the changes on IEC 62351-6 standard (new version currently in draft).

In order to illustrate the applicability of this approach, an specific configuration of this IP to support Configuration-over-Ethernet (COE) SoCe frame format is presented in the next Section.

III. SAS Crypto-core IP use case: COEsec

COE is a light chip-to-chip communication channel over Ethernet used in many implementations of our IPs to communicate CPUs with the switch using the Interlink Data link. In many embedded equipments the system design is simplified if the access to the internal registers of the IPs (networking, synchronization, etc.) is implemented over the same Ethernet channel used to communicate the CPU unit with the switching infrastructure implemented on the FPGA. COE removes the need for additional configuration links like SPI or MDIO. However, nowadays, in some installations it is not feasible ensuring that a chip-to-chip link is safe. Indeed, in some installations COE protocol is used as a communication between boards set in different physical locations.

COEsec (Configuration Over Ethernet Secure) is a protocol developed by SoCe that allows secure configuration communications over Ethernet. **This IP includes a SAS crypto-core IP module and it is presented in this paper as a field proven example of the proposed approach**.

This protocol makes use of private key cryptography, relying on the AES-GCM algorithm to provide data encryption and authentication. Although the protocol could support almost any cryptographic algorithm, AES-GCM has been selected due to its cryptographic capabilities, resource utilization and performance achieved, especially in hardware implementations.

SoCe networking IPs implemented in a FPGA can be securely configured by a remote CPU located in the same network. In this scenario, the CPU is responsible for generating and receiving COEsec messages in order to configure the desired networking IPs. Furthermore, it acts as a server that allows remote configuration in WAN making use of higher level protocols like HTTPS.

COEsec messages are based on Ethernet frames that contain several specific fields within the payload that provide all the cryptographic information as well as configuration data. The Figure 3 shows a COEsec frame including protocol-specific fields and Ethernet fields.

This frame is divided in three main sections. The first one contains the data required for encryption/decryption tasks. The second one includes the encrypted configuration data. Finally, there is a tag that provides authentication and integrity to the messages. All the fields that composes the COEsec frame are described below:

- *Channel ID:* each COEsec communication is identified with a channel ID. This field is used to associate the sender/receiver to its secret key that is used to encrypt, decrypt and authenticate the messages. It is 2 octets long.
- *Reserved:* 4 octets long field reserved for future use. All of them must be set to zero.
- *IV:* 12 octets long Initialization Vector used for the encryption/decryption of the messages. It provides randomness to the messages and ensure confidential-

Preamble	Start of frame delimiter	MAC destination	MAC source	Ethertype	Payload						Frame check sequence
					Channel ID	Reserved	IV		Payload	Authentication Tag	
							Random Number	Frame Number			
7 octets	1 octet	6 octets	6 octets	2 octets	2 octets	4 octets	8 octets	4 octets	16 – 80 octets	16 octets	4 octets

Figure 3. COEsec frame format.

ity. It is divided in two subfields: a random number and a frame number.

  - *Random Number:* 8 octets long random number that allows the encryption algorithm to achieve semantic security and prevents an attacker from inferring relationships between segments of different encrypted messages.
  - *Frame Number:* 4 octets long frame number that identifies each couple of messages (petition and response) exchanged between a sender and a receiver and associated to a certain channel ID. The sender must increase the frame number with each new frame. In case of the sender uses an invalid frame number, an automatic response message will be generated containing the same frame number that the petition received and whose payload will contain the valid frame number expected to receive for that channel ID. When the maximum frame number value is reached, the value should be reset to zero.

- *Payload:* it contains the encrypted configuration commands (both read and write operations) and their respective responses.
- Authentication Tag: in order to prevent an attacker from modifying the messages, an authentication tag is used (16 octets long). This tag has been generated using a Hash function that assures that if any of the bits of the authenticated fields changes, the tag will take a different value. The authenticated fields are: Channel ID, Reserved, IV and Payload as well as the Ethernet header (MAC destination, MAC source and Ethertype).

IV. Implementation

The block diagram draw inside the FPGA depicted in Figure 4 represents the implementation of the COEsec concept-proof design. It is composed by a 4-port IEEE1588-aware Managed Ethernet Switch (MES) IP [8], an IEEE1588 Timer and Timestamping IP, a COEsec IP instance and simple Wishbone system interconnection architecture.

The IP switching and timing infrastructure implemented in the FPGA can be configured using any of the Ethernet ports due to all COE frames are addressed to the COEsec IP that processed them and configures the IP through the Wishbone Master interface.

This design has been implemented on a XC7Z020 Zynq-700 All Programable SoC device from Xilinx, which is used to validate the architecture.

The values presented in Table I represent the resource percentage used in the proposed design on this device. As it can be observed the worst case implies the use of 23.77 % of the total available resources of the FPGA and it includes all IP infrastructure described previously.

Resources	Used	Available	Percent
Slice Registers	13293	106400	12.49 %
Slice LUT	12645	53200	23.77 %
Block RAMs	26	140	18.57 %

Table I
FPGA resources used for the concept-proof design.

V. Validation

In order to analyze the timing behaviour of the proposed architecture, an experimental set-up has been built. Figure 4 summarizes this set-up. It is composed by a PC, an FPGA based card (SMARTzynq Industrial Networking card [9]) and by a multiport oscilloscope.I n this scenario, a PC is responsible for sending and receiving the COEsec frames, which are generated by means of Python scripts.

In order to measure the 'real' processing times (including the Ethernet phyters and additional logic) an oscilloscope has been included in the set-up. The first channel of the oscilloscope is responsible of capturing the Ethernet frame before entering the PHY in the Rx+ pin. The second channel is connected to the FPGA pin linked to the state of the register, which is being configured. In addition, the second channel is used as a trigger signal.

The test sequence has been defined as follows:

First, a ciphered writing frame to one internal register of the IP in the FPGA is sent from the PC. This frame is deciphered by the COEsec implementation of the SAS crypto-core. Next, a reading frame to the previous register is sent from the PC. This command triggers a response from the FPGA to the PC that it is ciphered. This response (reply) frame is captured using the WireShark software. Finally, the frame is decrypted using a Python script that includes a third party-implementation of the cipher suite, which delivers the value of the register that should coincide to the value sent in the writing frame.

The simulations are used to determine the processing time of a COEsec frame from it entering the core until the data is saved in the IP core register to be configured. In addition, simulations for writing and reading frames using different transmission rates (e.g. 10 Mbps, 100 Mbps, 1 Gbps) are performed, which results are summarized in Table II.

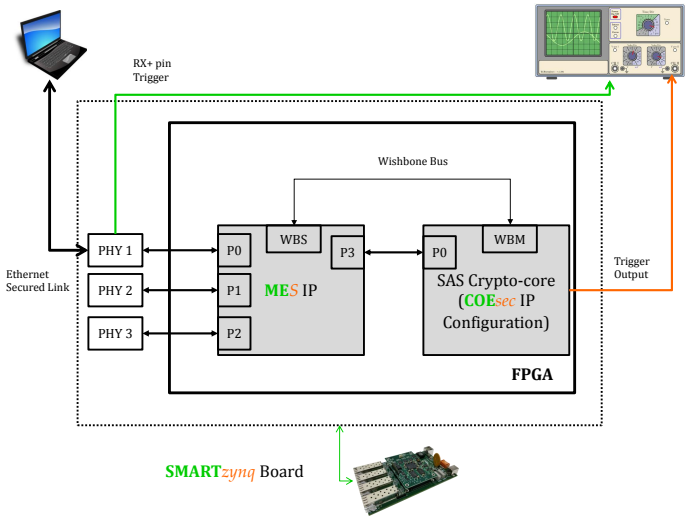

Figure 4. Experimental Setup to measure COEsec timing.

Type	10 Mbps	100 Mbps	1 Gbps
Reading	70.860 μs	9.296 μs	3.156 μs
Writing	78.196 μs	10.152 μs	3.364 μs

Table II
COEsec PROCESSING TIMES.

The difference between the time obtained by simulation (i.e. 78.196 μs) and the time obtained by the oscilloscope are the result of the latency produced in the PHY from entering the first bit to the output of the first data through the Rdx(3:0) bus. In this case the delay is 2.324 μs, which is approximated to 2.18 μs according to the value specified in the datasheet of the PHY shown in Table III.

	Parameter	Typ	Units
1000 BASE-T	Star of Packet to RX_CTL Asserted	236	ns
100 BASE-T	Star of Packet to RX_CTL Asserted	357	ns
10 BASE-T	Star of Packet to RX_CTL Asserted	2.18	μs

Table III
PHY RECEIVE LATENCY TIMING.

Additionally, measurements at rates of 100 Mbps and 1 Gbps have been performed and summarized in Table IV summarizes the results obtained in the simulation and in the real set-up.

	Frame writing	
Rates	Simulation+PHY-latency(μs)	Measurement(μs)
10 Mbps	80.376	80.520
100 Mbps	10.509	10.650
1 Gbps	3.600	3.583

Table IV
DATA OF SIMULATION VS. MEASUREMENT.

VI. CONCLUSIONS

The technology presented in this paper focuses on providing a solution for on-the-fly processing of secured time critical Layer-2 frames. It is based on a hardware implementation on reconfigurable devices able to cipher and decipher the communication link inside the chip between the CPU unit and the networking IP.

Due to the frame format for secure GOOSE and SMV format is nowadays not fully defined by the standard, a specific use-case based on a SoCe protocol used to access the switch IP registers on the FPGA from a remote CPU unit has been reported. The implementation results highlight the small silicon footprint required to implement the solution, enabling it for cost-sensitive CPU-less solutions but applying the state-of-the-art cryptographic algorithms. On the other hand, the timing obtained for the on-the-fly decryption of the frames enables the extension of this approach to secure other critical control frames used in SAS environment.

REFERENCES

[1] P. Fairley, "Cybersecurity at u.s. utilities due for an upgrade," *IEEE Spectrum*, March 2016.
[2] G. Ericsson, "Cyber Security and Power System Communication - Essential Parts of a Smart Grid Infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, 2010.
[3] F. Cleveland, "Iec tc57 wg15: Iec 62351 security standards for the power system information infrastructure," International Electrotechnical Commission, White Paper ver 14, June 2012. [Online]. Available: http://xanthus-consulting.com/Publications/documents/IEC%20_TC57_WG15_White_Paper.pdf
[4] *IEC/TS 62351-6 ed1.0 Power Systems Management and Associated Information Exchange - Data and Communication Security - Part 6: Security for IEC 61850*, IEC Std., 2007.
[5] *IEC 61850-1 ed2.0 Communication Networks and Systems for Power Utility Automation - Part 1: Introduction and Overview*, IEC Std., 2013.
[6] S. Fuloria, R. Anderson, K. McGrath, K. Hansen, and F. Alvarez, "The Protection of Substation Communications," in *Proceedings of SCADA Security Scientific Symposium*, 2010.
[7] S. Fries and R. Falk, "Security Considerations for Multicast Communication in Power Systems," *International Journal On Advances in Security*, vol. 6, no. 3 and 4, pp. 111–121, 2013.
[8] SoC-e, "MES, Managed Ethernet Switch IP Core ," http://soc-e.com/mes-managed-ethernet-switch-ip-core/, 2016.
[9] ——, "SMARTzynq module: 5 Port Gigabit Ethernet Industrial Embedded Switch Module," http://soc-e.com/products/smart-zynq-module/, 2016.