Master in Electronic Engineering

Implementation of the Parallel Redundancy Protocol (PRP) with encryption of frames using the Advanced Encryption Standard (AES)

Marco Andrés Ortiz Niño

Bogotá, D.C., 13-01-2021

ESCUELA COLOMBIANA DE INGENIERÍA
JULIO GARAVITO

Implementation of the Parallel Redundancy Protocol (PRP) with encryption of frames using the Advanced Encryption Standard (AES)

Thesis work to obtain a master's degree in Electronic Engineering, with an emphasis on Telecommunications.

Supervisor: Eng. Hernán Paz Pengos. PhD
Co-Supervisor: Eng. Javier Evandro Soto Vargas. PhD.

Implementation of the Parallel Redundancy Protocol (PRP) with encryption of frames using the Advanced Encryption Standard (AES)

Jury:

Bogotá, D.C., 13-01-2021

ESCUELA COLOMBIANA DE INGENIERÍA
JULIO GARAVITO

The Master Thesis, *Implementation of the Parallel Redundancy Protocol (PRP) with encryption of frames using the Advanced Encryption Standard (AES)*, presented by Marco Andrés Ortiz Niño meets the requirements established to obtain the title of Magister in Electronic Engineering with emphasis on telecommunications.

Jury:

Supervisor: Eng. Hernán Paz Penagos. PhD.
Co-Supervisor: Eng. Javier Evandro Soto Vargas. PhD.

Bogotá, D.C., 13-1-2021

Abstract

As industrial Networks progressively migrate their communications infrastructure to IP and Ethernet set of protocols, threads and vulnerabilities also appear to disrupt operation of infrastructure with serious repercussions. To minimize these, authentication, encryption, integrity and availability must be taken in consideration at every layer of the communication architecture. Security can be achieved by numerous algorithms and set protocols that are continuously tested and implemented to be supported on current links, networks and applications. Their implementations are performed to accomplish high throughput and reduced logic utilization depending on industry or sector requirements. Particularly, this work deals with confidentiality and availability at data link layer where Ethernet resides. Advanced Encryption Standard (AES) with Counter mode (CTR) are used for confidentiality and the Parallel Redundancy Protocol (PRP) for redundancy. These are selected due to their communication orientation, broad operation lifetime expectancy, and their direct relation to secure industrial networks for critical and non-critical infrastructures. Advanced Encryption Standard (AES)-Counter mode (CTR) logic an its Intellectual Property (IP) Cores are created using Very High Speed Integrated Circuit Hardware Description Language (VHDL) within Xilinx Vivado and tested using the Zynq7000 System on Chip (SoC)-Field Programable Gate Array (FPGA) and Kintex 7 FPGA. Parallel Redundancy Protocol (PRP) is implemented on software to govern the protocol algorithm, data encryption operation and packet framing. To test integration between these components, the embedded processor of the Zynq 7000 (ARM) and Microblaze are used. This work presents a non-pipelined AES implementation for confidentiality, its logic utilization, maximum frequency and throughput. Results for AES are also presented in simulation for 128, 192 and 256 bit-length key sizes. At implementation, the 128 bit key is used. For redundancy, on the other hand, the PRP is implemented on software, which creates the header and trailer according to International Electrotechnical Commission (IEC) specification, and, a packet format is proposed to encrypted payloads. Integration results of AES-PRP are seen as packets that were captured in between of the communication devices.

Contents

List of Tables

List of Figures

Introduction

Security threats are continuously found in form of sophisticated attacks, which often are aimed to harm critical and non-critical infrastructure of both, public or private sectors. Based on these, governments and organizations develop standards and guidelines that establish requirements to prevent incidents that may affect public or private entities. Generally, requirements are achieved by defense systems, devices and protocols to enhance confidentiality, authentication and availability for data transmitted between end nodes. These data may contain classified information, supervisory and control commands among others. Several countermeasures are commonly established by means of security devices and protocols. These allow compliance of a single or set of requirements, so to improve a security scheme, protocols are combined on top of software and hardware components, allowing traditional security devices as Firewalls, Intrusion Detection Systems (IDS), Virtual Private Network (VPN) servers or antivirus software, coupling with advanced services like data loss prevention and detection of malware (Rubio, Manulis, Alcaraz, & Lopez, 2019).

In many cases, the inclusion of devices would not be advisable for many situations because: 1. Many communications devices in power industry use limited memory and processing resources, thus the overhead needed for encryption and key exchanges are not allowed (IEC 62351-1 sec. 5.6.1) as these are commonly implemented on the application, transport or network layer (upper layers); and 2. Information in a telecommunication scheme protected by cryptography, is done from source to destination point, hence, adding devices in between does not accurately secure end-to-end. Nevertheless, advanced services and devices are being adapted to industrial networks due to its migration from isolated infrastructures to interconnected systems that use protocols commonly seen in Information Technology (IT), thus, reducing operational costs and improving time response when a failure occurs, with the downside of importing IT threats which, in turn, are reported frequently with a growing trend (Rubio et al., 2019).

Internet of Things (IoT) is another extension of Industrial Networks with continuous development and innovation, modifying processes in many industries (Rost et al., 2018). Some definitions of Industrial Internet of Things (IIoT) and, mainly, an analysis framework are shown in (Boyes, Hallaq, Cunningham, & Watson, 2018). Requirements for the IIoT, as presented by (Urbina et al., 2018), are: Real-time operation, High availability, Interoperability, Data analysis and Cyber-security.

Characteristics of devices in this context can be categorized, as Boyes et al. (2018) propose: by its function, critically, easy of repair, management interface and relationship between devices, sensor and actuators. Thus, to fulfill these requirements and characteristics within industrial networks, a versatile and re-configurable approach can be made by means of FPGAs and FPGA-SoCs, as these have transformed to be a fundamental solution for development that requires high availability, high processing, real-time conditions, interoperability, resilience and security (Urbina et al., 2018).

This work includes an integrated approach for confidentiality and availability requirements by implementing the PRP protocol and AES. The Parallel Redundancy Protocol (PRP) defined by IEC 62439-3 standard is intended to industrial communications with high availability in Local Area Networks (LANs). Provides fault tolerance with adjustable time requirements according to specific implementation and available hardware. It resides at link layer, taking advantage of Ethernet that, among others, allows process devices to be interconnected with other devices, reducing the use of gateways that could limit real time requirements (Urbina et al., 2018). Data contained in the PRP packet, which is framed on an Ethernet frame, has vulnerabilities in networks as its load content is not authenticated nor encrypted. AES is implemented as it allows a robust and widely used confidentiality system that can be integrated along multiple sets of protocols that are currently used and in continuous evaluation according to the target application. Because of this, AES encryption is included in the Link Redundancy Entity (LRE) which is a key component of PRP end nodes. In this implementation, framing and a discard algorithm of PRP are performed based on packets formats that are proposed to include AES-CTR within its payload. For AES data encryption beyond the block size, the CTR is implemented as this mode is essential for encrypted-authenticated operations (not covered in this work), and is designed for high data rates encrypted communication.

In this context, the main objective of this work is to implement on a FPGA, the Advanced Encryption Standard (AES) and the Parallel Redundancy Protocol (PRP); and, based on IEC62439-3, evaluate the compatibility of PRP with AES for its payload confidentiality. Evaluation is made using international standard IEC62439-3 for framing correctness by comparing the PRP frame structure with an encrypted/decrypted packet transmitted from the FPGA, captured by an intermediate Ethernet Switch and decoded on Wireshark packet analyzer. Frame formats and its size restrictions are discussed. Tests for PRP performance and recovery time, as documented in IEC62438-part1, are not presented in this work due to the time cost required for development of related components. The Link Redundancy Entity (LRE) of PRP is implemented as a basic DANP or RedBox with the duplicate discard mode principle (IEC62439-3, 2016). AES IP Cores are implemented using combinational and sequential methodologies. The later is used to form an AES-CTR IP.

Physical implementation use a Xilinx® Zynq7000 FPGA-SoC (xc7z020clg484-1), embedded on a ZedBoard with an Ethernet port expansion. This device is used to report timing and utilization of IP Cores Programable Logic (PL) and, also, as the PRP RedBox cipher sender. To complete the communication scheme, a Xilinx® Kintex®-7 (xc7k325tffg676-1) FPGA integrated on a NetFPGA 1G-CML is used as the PRP RedBox decipher receiver. PRP framing and AES control are implemented on the Processing System (PS) of the Zynq7000 (ARM) and Kintex 7 (Microblaze)

This document has the following structure: Chapter 1 presents the literature review and a context of this implementation, Chapter 2 describes the methodology using for implementing the components such as the elaboration of AES cores with Counter mode (CTR), the packets with PRP included AES for payload encryption and the algorithm that governs the operation. Chapter 3 presents the results separately for AES IP core, its Throughput, maximum frequencies and utilization showing that, to allow integration with softprocessor and other hardware components, utilization should be kept at minimum avoiding, as far as possible, decrease of throughput. Also, this chapter presents the PRP packets with its trailer and encrypted payload sent over an Ethernet network. chapter 3.5 presents the conclusions and future work regarding this implementation.

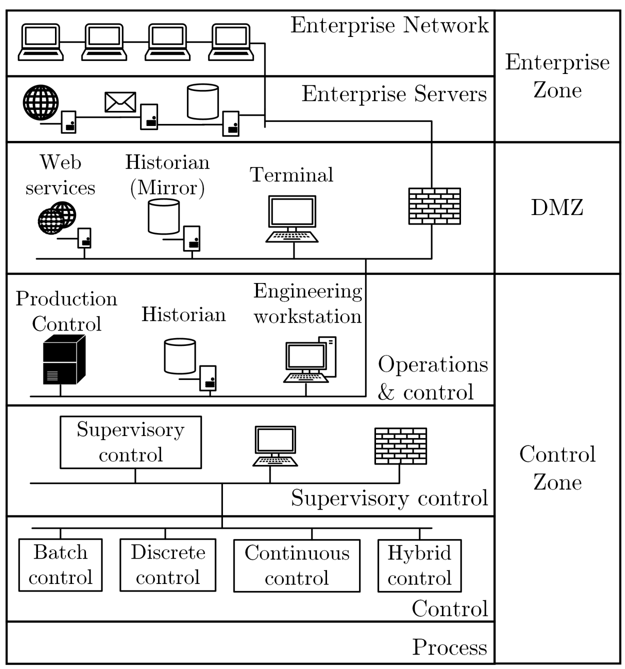
Chapter 1

Literature Review

1.1 Industrial networks security

An industrial data network is based on models such as Computer Aided Manufacturing (CAM) and the more detailed version developed by the International Purdue Workshop on Industrial Computer Systems (Buse & Wu, 2006), adopted as an Industrial Automation and Control Systems (IACS) security standard known as ISA/IEC 62443. This model is represented in levels as shown in the Figure 1. It outlines the tasks of an integrated information management and automation system. However, the number of levels used in an industry model may vary (Buse & Wu, 2006), but each has its own policies related to physical and logical security (Knapp & Langill, 2011).

Figure 1. Reference Model for industrial control systems.



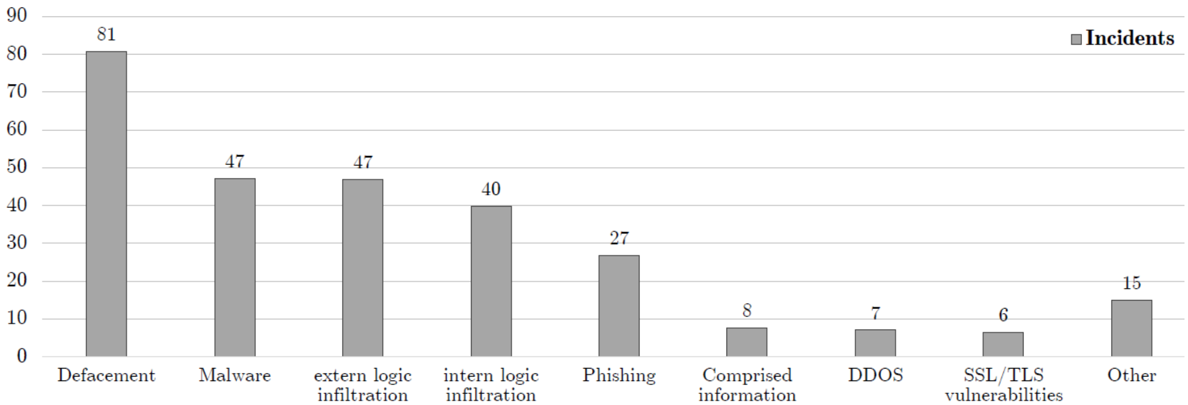
Source: Bodungen, Singer, Shbeeb, Wilhoit, and Hilt (2016).

Industrial Automation and Control Systems (IACS) have expanded from isolated networks to interconnected systems using Commercial off-the-Shelf (COTS) protocols and operating systems. IACS also are integrated with enterprise systems through different communication networks (IEC/TS62443-1-1, 2009) according to standards that allow systems to exchange information consistently. However, this increases vulnerability to attacks and introduces potential risk in IACS with effects that include the following (IEC/TS62443-1-1, 2009):

- Unauthorized access to confidential information.
- Loss of integrity or reliability of process data and production information.
- Loss of system availability.
- Equipment damage.
- Personal injury.
- Violation of legal and regulatory requirements.
- Risk to public health and confidence.
- Threat to a nation's security.

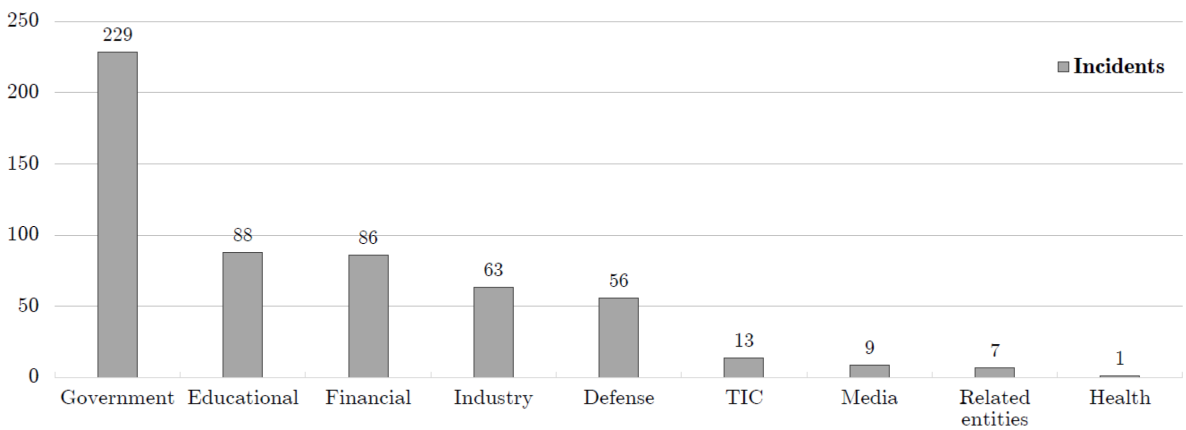
Security consultant at Red Tiger Security showed in 2010 that after testing approximately 100 North American electric power generation infrastructure, more than 38000 security warning and vulnerabilities were encountered (Knapp & Langill, 2011), and "*the average number of days between the time when the vulnerability was disclosed publicly and the time when the vulnerability was discovered in a control system was 331 days*" (Knapp and Langill,2011,p.32). Vulnerabilities allows sophisticated *malware* to be implanted on equipment, also with effects listed above and incidents with critical consequences. Several worldwide incidents can be found in Bodungen et al. (2016) and Knapp and Langill (2011). In Colombia, Comando Conjunto Cibernético (CCOC) and Colombian Computer Emergency Readiness Team (ColCERT) worked on 769 national-defense incidents on 2014 and 957 during 2015. This later year showed that $27,4\%$ of the incidents correspond to defacement, 16% to malware, $15,9\%$ to logic extern infiltration and $13,5\%$ to intern logic (Figure 2). Incidents by sectors are presented in the Figure 3.

Figure 2. Incidents managed by CCOC and ColCERT in Colombia, 2015.



Source: *Conpes-3854 Consejo Política Nacional de Seguridad Digital* (2016).

Figure 3. Incidents by sector in Colombia, 2015.



Source: *Conpes-3854 Consejo Política Nacional de Seguridad Digital* (2016).

In order to enhance security for data communications systems, public and private organizations have developed guidelines and standards which are intended to avoid incidents by means of establishing security requirements, which traditionally are focused on achieving confidentiality, integrity, and availability. Detailed requirements for security in Industrial Automation and Control Systems (IACS) are presented in Table 1. Security standards for industrial systems are shown in Appendix A.1.

Table 1. Security requirements for IACS.

Requirement	**Description**
Access Control	Control access to selected devices, information or both to protect against unauthorized interrogation of the device or information.
Use Control	Control use of selected devices, information or both to protect against unauthorized operation of the device or use of information.
Data Integrity	Ensure the integrity of data on selected communication channels to protect against unauthorized changes.
Data Confidentiality	Ensure the confidentiality of data on selected communication channels to protect against eavesdropping.
Restrict Data Flow	Restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources.
Timely Response to Event	Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission-critical or safety-critical situations.
Resource Availability	Ensure the availability of all network resources to protect against denial of service attacks.

Source: IEC IEC/TS62443-1-1 (2009).

Several protocols are standardized and documented to achieve these requirements. But as these do not have security measures included in the original standards (IEC/TS62351-1, 2007) and could be hacked by sophisticated *malware*, novel approaches are continuously developed to comply with a specific or set of requirements. Particularly, this work deals with data **confidentiality** and **availability** requirements using PRP and AES. Commercial implementations that meet high availability requirements using PRP are presented in the Table 2.

Table 2. PRP commercial devices.

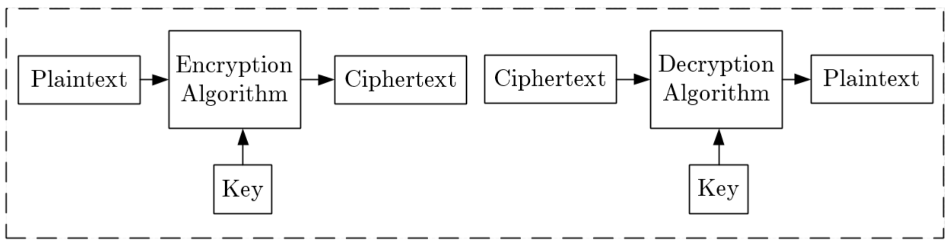
Device	Manufacturer	Security
IE 4000	Cisco	IEEE802.1AE MacSec
IE 5000	Cisco	IEEE802.1AE MacSec
2000U	Cisco	IEEE802.1AE MacSec
SCALANCE X204RNA	Siemens	Not specified
RED25	Hirschmann - Blenden	Not specified

As seen, PRP devices do not have a security mechanism by itself. It uses protocols as MACSec to fulfill authentication and confidentiality but this is not present in all devices and limited to LAN domains which are frequently secured by obscurity, as this type of network remains on a single administration domain. Despite PRP and MACSec are constrained to LAN networks, modern transmission and distribution automation systems requires data transmission over WAN networks. These data (control, protection, supervisory) should be secured in terms of availability and confidentiality with IP support. Thus, two issues arise: availability over WAN networks using PRP and securing PRP. For the first issue, three proposals were found in (Stefanka, 2016), (Popovic, Mohiuddin, & Tomozei, 2015) and (Rentschler & Heine, 2013) but no devices nor implementations were found; for later issue, confidentiality is made based on AES with crypto engines. To propose a solution, a programable platform is mandatory. This includes hardware and software components to accelerate processes that guarantee time responses according to specifications. For this matter, Texas Instruments provides a platform based on software for developing and investigation named The Programmable Real-Time Unit Subsystem and Industrial Communication SubSystem (PRU-ICSS). But, to provide a more complex and robust programable platform that exploits both, hardware and software, FPGAs and dedicated processors are needed.

1.2 Cryptography

Cryptography, part of cryptology discipline, studies the techniques to create from plain text, non-comprehensible data for anyone who does not know the appropriate key. Thus, data encoded can securely be stored or transferred via any communication channel (Koscielny, Kurkowski, & Srebrny, 2013) providing confidentiality, integrity, authentication, nonrepudiation and anonymity among others (Vaudenay, 2006), depending on the encryption algorithm implemented which in general consists of the Plain text that is the data content being transferred (input); key that must remain secret for unauthorized parties (input); the process of protect the data content called encryption and the resulting encrypted message called ciphertext (Output). The encryption and decryption algorithms are assumed publicly known with private key or public-private pair keys. Both algorithms form a cipher (Koscielny et al., 2013). General components are presented in the Figure 4.

Figure 4. Cipher components.



Source: Author.

There are two types of ciphers: Symmetric and Asymmetric. The first use duplicate Keys for encryption and decryption while second, also referred as public-key ciphers, use a different pair of keys for each algorithm named public and private keys. “The first of them is publicly available. Everybody can use it to encrypt messages. But only the corresponding private key allows decryption. Thus the only person able to run decryption is the one who has the private key” (Koscielny et al., 2013).

1.2.1 Symmetric algorithms

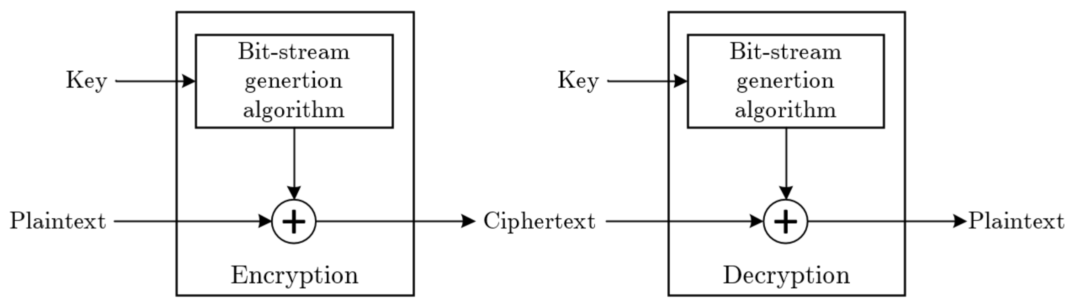
“Symmetric algorithms are fast and are used for encrypting - decrypting high volume data” (Rodriguez-Henriquez, Saqib, Pérez, & Koc, 2006), encode Plaintext by **stream** (Figure 5a) when one of its bits or bytes is processed by the algorithm at a time, or by **block** (Figure 5b) when a set of bytes are processed producing an output block of equal length. “Typically, a block size of 64 or 128 bits is used” (Stallings, 2013). Block ciphers ”seem applicable to a broader range of applications than stream ciphers. The vast majority of network-based symmetric cryptographic applications make use of block ciphers” (Stallings, 2013). In the Table 3, examples of stream and block ciphers are shown.

Table 3. Stream and block ciphers.

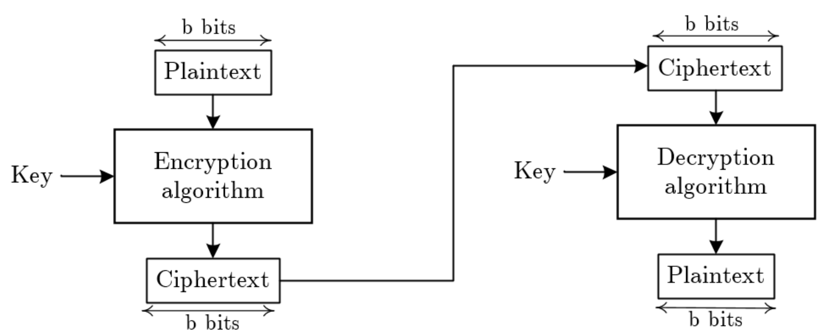
Symmetric type	**Algoritmhs**
Stream ciphers	Vigenère, Vernam, SEAL, TWOPRIME, WAKE, RC4, A5
Block ciphers	DES, AES Rijndael, Serpent, RC5, RC6, MARS, IDEA, Twofish, Blowfish, CAST, FEAL, GOST, TEA, SAFER k64, Twofish, DEAL, LOKI97, LOKI91, MISTY, MMB, Madryga, ICE

Figure 5. Stream cipher and Block cipher.

(a) Stream cipher.



(b) Block cipher.



Source: Stallings (2013).

One of the most popular symmetric block cipher is the Data Encryption Standard (DES). "In 1973 the US National Bureau of Standards (NBS) solicited proposals for a uniform and reliable encryption algorithm that could be applied, among other places, in commercial communication systems" (Koscielny et al., 2013). The algorithm developed at IBM by Horst Feistel and Dan Coppersmith in 1974 was accepted and became widely deployed in many applications despite its 56-bit key length that nowadays can be discovered in hours by a brute force attack

(Rodriguez-Henriquez et al., 2006). Because this vulnerability, a variation of DES called Triple-DES or 3DES that uses three 56-bit keys and may offer a security of a 112-bit key is widely used (Rodriguez-Henriquez et al., 2006). But DES is destined to be replaced by the Advanced Encryption Standard (AES) in order to improve confidentiality.

1.2.2 AES and the Rijndael Algorithm

Rijndael algorithm, developed by Joan Daemen and Vincent Rijmen, became the Advanced Encryption Standard (AES) in November 2001 after a selection process initiated in January 1997 by the National Institue of Standards and Technology (NIST). AES is a byte-oriented symmetric block cipher that requires 10, 12 or 14 rounds of encryption for key sizes of 128, 192 or 256 bits respectively, operating as a classic substitution/permutation relying on operations in the field GF(2^8) (Dobbertin, Rijmen, & Sowa, 2005). AES is composed with an input block, four transformation modules, a key generator and an output block. The **input block** is a 128 bit-lenght of plain data, arranged in a matrix as described in the Figure 6, where each column forms a 4 byte word called N_b-word.

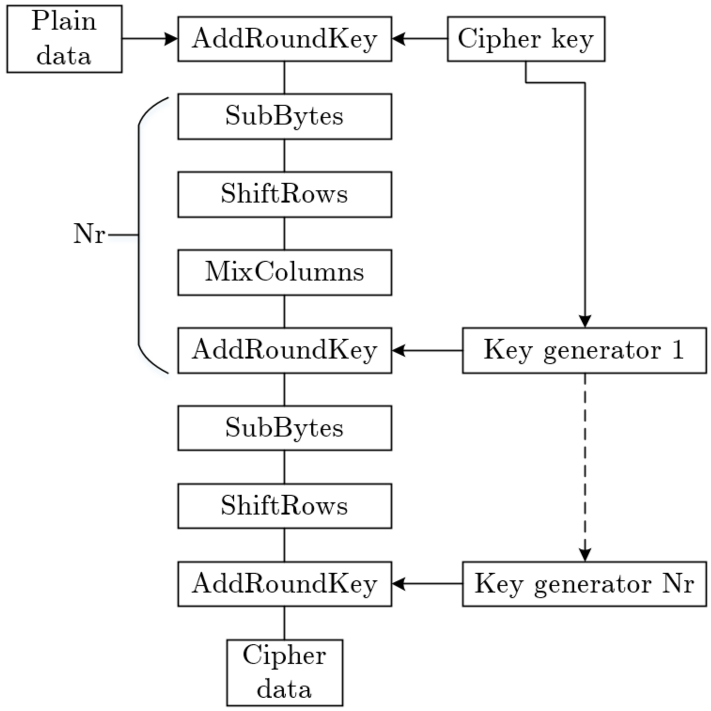
Figure 6. AES input block to cipher.

a_0	a_4	a_8	a_{12}
a_1	a_5	a_9	a_{13}
a_2	a_6	a_{10}	a_{14}
a_3	a_7	a_{11}	a_{15}

source: Dobbertin et al. (2005)

Transformation modules, named *SubBytes*, *ShiftRows*, *MixColumns* and *AddRoundKey* (NIST, 2001a) form a round of the cipher with some variations at start and end rounds. The key-expansion module or **key generator**, generates a key per round until completion of the encryption process. Figure 7 presents the AES parts integrated, where N_r is the number of rounds modules should be repeated according to the cipher-key being used, which is arranged in a matrix where each column is 32-bit length with N_k columns.

Figure 7. AES cipher.



Source: Author.

The relation between the number of rounds N_r and the key size N_k is shown in the Table 4.

Table 4. Key-Block-Round Combinations.

Name	**Key length (N_k words)**	**Block size (N_b words)**	**Number of rounds (N_r)**
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Source: IEC - IEC/TS62443-1-1 (2009).

Detailed AES components and operations are presented in NIST (2001a) and Daemen and Rijmen (2002). AES encryption is currently active and presents a usable time estimation of years ahead as defined by NIST and seen in the Table 5.

Table 5. Approval Status of Symmetric Algorithms Used for Encryption and Decryption.

Algorithm	**Use**
AES-128	Acceptable
AES-192	Acceptable
AES-256	Acceptable

Source: SP800131A (2015).

Besides, AES uses the three key lengths that are also acceptable by National Institue of Standards and Technology (NIST) and widely deployable. Table 6 shows the recommendation for key management.

Table 6. Recommendation for key management.

Security Strength	**Through 2030**	**2031 and Beyond**
128	Acceptable	Acceptable
192	Acceptable	Acceptable
256	Acceptable	Acceptable

Source: SP80057Part1 (2016).

1.2.3 Modes of operation

Modes of operation allows block ciphers to encrypt data that must cope beyond the block size. For example, AES block size is 128 bit, so to encrypt data grater than 128 bits, is necessary to partition it in blocks of the same size. But if these partitioned blocks use the same key, security vulnerabilities increase (Stallings, 2013), so a mode of operation is required to enhance security of a cryptography algorithm. Modes of operation are divided according to the application. Seven parts are defined by the NIST and presented in the Table 7.

Table 7. Block cipher's Modes of operation.

Part	**service**	**Name**	**Standard**
1	Confidentiality	Electronic CodeBook mode (ECB)	SP800-38A
		Chiper Block Chaining mode (CBC)	
		Chiper Feedback mode (CFB)	
		Output Feedback mode (OFB)	
		Counter mode (CTR)	
2	Authentication	cipher-based message authentication code (CMAC)	SP800-38B
3	Authentication Confidentiality	Counter with Cipher Block Chaining-Message Authentication Code (CCM)	SP800-38C
4	High-Throughput Authentication confidentiality	Galois/Counter Mode (GCM)	SP800-38D
5	Storage Confidentiality	XEX Tweakable Block Cipher with Ciphertext Stealing (XTS) (XTS-AES)	SP800-38E IEEE1619-2007
6	Key Wrapping	Key Wrap (KW) Key Wrap Padding (KWP)	SP800-38F
7	Format-Preserving Encryption	format-preserving, Feistel-based encryption (FF1)	SP800-38G

As this work attempts to provide a confidentiality -and redundancy- mechanism for data transmissions, part 1 is considered for implementation process, specifically, the Counter mode (CTR) mode as this best fits the requirements and is scalable in a way that can be used for other modes of operation as Galois/Counter Mode (GCM) or Counter with Cipher Block Chaining-Message Authentication Code (CCM). In Table 8, a description of the modes of operation related strictly to confidentiality are shown.

Table 8. Modes of operation Part 1 description.

Mode	**Description**	**Typical application**
Electronic Code-Book mode (ECB)	Input data (plain text) of blocks are encoded separately using the same key.	Transmission of unique values as an encryption key.
Chiper Block Chaining mode (CBC)	Input data (plaintext) is the xor of the plain data of the next block and the previous block output data(cipher text).	Block-oriented for communication and authentication
Chiper Feedback mode (CFB)	Input data is processed a set of bits at once. Output data of previous block, is passed as input to the cipher to generate pseudorandom output data. This is xored with the input data to produce subsequent set of ciphertext.	Stream-oriented communication and authentication.
Output Feedback mode (OFB)	Like CFB, except that the input data is the preceding cipher output. Uses all available blocks.	Stream-oriented communication.
Counter mode (CTR)	Blocks of input data are xored independently with a ciphered counter. For each next block, the counter is incremented.	Block-oriented transmission. Used for high speed requirements

Source: Stallings (2013).

Currently, new proposals are being presented for authentication and encryption in the Competition for Authenticated Encryption: Security, Applicability,and Robustnes (CAESAR). These proposals aim to improve AES-GCM performance for lightweight devices and include both, block and stream ciphers. Detailed information and implementation is beyond the scope of this work, but can be found in (Farzaneh Abed, 2016) and in the International-Cryptologic-Research-Community (2017).

1.3 Redundancy in communication networks

In order to accomplish high availability in networks, a redundancy scheme is implemented according to specific application requirements such as topology, recovery time, data-packet losses and devices involved in the redundancy process. Applications such as enterprise networks are considered non-critical for recovery time and packet losses at network layer or lower.

For automation networks, requirements meet enhanced performance. See Table 9.

Table 9. grace time per application examples.

Applications	Typical grace time (s)
Uncritical automation	20
Automation management	2
General automation	0.2
Time-critical automation	0.020

Source: IEC62439-1 (2013).

Redundancy can be dynamic or static. On dynamic redundancy, devices react to failures within the network. On the other hand, static redundancy acts in a parallel manner as devices are active concurrently. In the Table 10, a list o protocols for redundancy are shown.

Table 10. Examples of redundancy protocols.

Protocol	Solution	Frame loss	Redundancy Protocol	End node attachment	Network topology	Recovery time
IP	IP routing	Yes	Within the network	Single	Single meshed	> 30s typical not deterministic
STP	IEEE 802.1D	Yes	Within the network	Single	Single meshed	> 20s typical not deterministic
RSTP	IEEE 802.1D	Yes	Within the network	Single	Single meshed, ring	Can be deterministic

Source: IEC62439-1 (2013).

Table 10. (Continued) Examples of redundancy protocols.

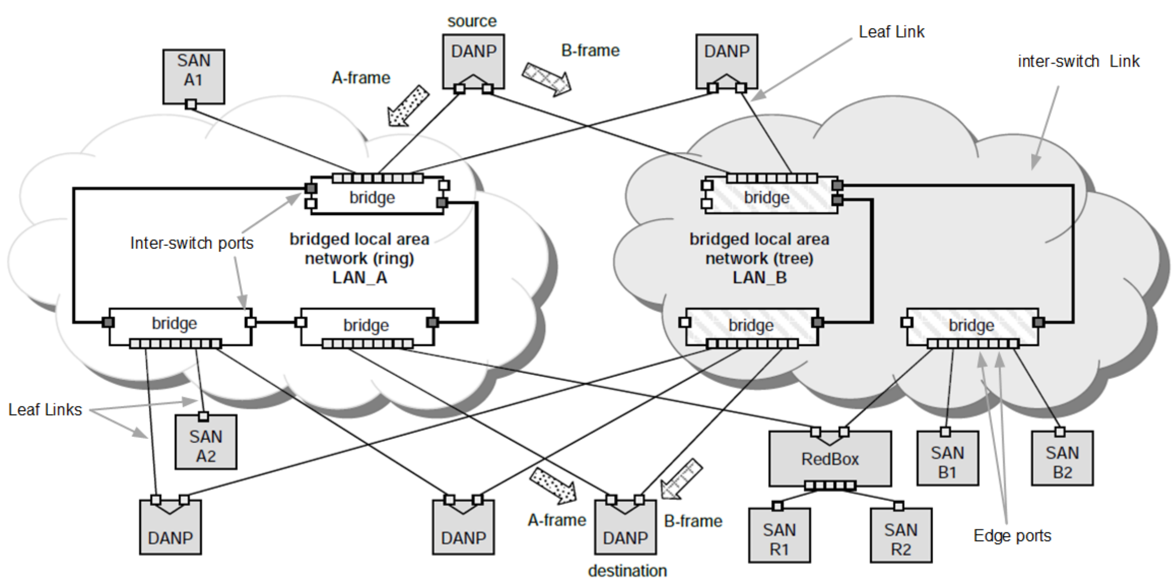
Protocol	Solution	Frame loss	Redundancy Protocol	End node attachment	Network topology	Recovery time
CRP	IEC 62439-4	Yes	In the end nodes	Single and double	Doubly meshed, crossconnected	1s worst case for 512 end nodes
DRP	IEC 62439-6	Yes	Within the network	Single and double	Ring, double ring	100 ms worst case for 50 switches
MRP	IEC 62439-2	Yes	In the end nodes	Single	Ring	500 ms, 200 ms, 30 ms or 10 ms worst case for 50 switches depending on the parameter set
BRP	IEC 62439-5	Yes	In the end nodes	Double	Doubly meshed, connected	4,8 ms worst case for 500 end nodes
PRP	IEC 62439-3	No	In the end nodes	Double	Doubly meshed, independent	0s
HSR	IEC 62439-3	No	In the end nodes	Double	Ring, meshed	0s

Source: IEC62439-1 (2013).

1.3.1 The Parallel Redundancy Protocol - PRP

The Parallel Redundancy Protocol (PRP) is defined in the Section 4 of the IEC62439-3 (2016) standard for high availability in automation networks. PRP is implemented in end nodes, avoids frame losses and guarantees seamless recovery time (IEC62439-1, 2013). PRP allows high availability services by duplicating a packet and sending it over two independent LAN networks to only one destination at a time. Provides redundancy in end devices rather than in network components using nodes called DANPs (IEC62439-3, 2016). Thus, source DANP sends two frames in a parallel manner to a destination DANP that receives those frames in a time lapse depending on the two LAN topologies involved, passing the Link Service Data Unit (LSDU) contained in the first received frame to upper layers and discarding the second frame. LANs attached to a DANP must be identical in the suite of protocols at the Logical Link Control (LLC) data-link sublayer, specifically IEEE802.3 and IEEE802.1D, to accomplish the resilience specified by IEC62439-1 (2013), but each LAN can be different in topology and performance (IEC62439-3, 2016). These LANs named LAN A and LAN B (as the standard call them), should operate simultaneously and be "fail-independent". Figure 8 presents a PRP network with the elements that compose it such as: end nodes like SANs, RedBox and DANPs; elements within the LANs like IEEE802.1D bridges, edge ports, inter-switch ports and inter-switch links; and the leaf-links between LANs and end nodes. Particularly, DANP and RedBox nodes need a Link Redundancy Entity (LRE) in their protocol stack for adequate operation of PRP.

Figure 8. PRP Redundancy Network.

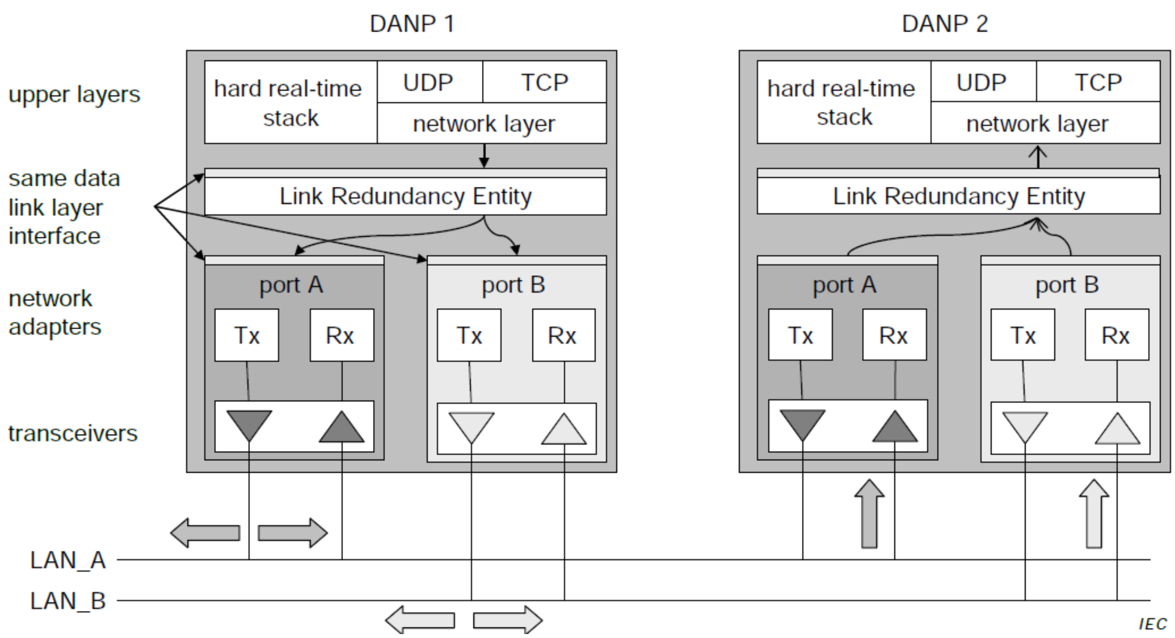


Source: IEC62439-3 (2016).

1.3.1.1 Link Redundancy Entity - LRE

End nodes have a single connection as the SAN node or more than one as the DANP and RedBox nodes. These later nodes require a Link Redundancy Entity (LRE) in their link layer to hide redundancy from upper layers (IEC62439-1, 2013) and operate ports in parallel. LRE in DANP nodes interfaces two ports with one upper layer stack (Figure 9). It handles duplicated frames and redundancy management (IEC62439-3, 2016).

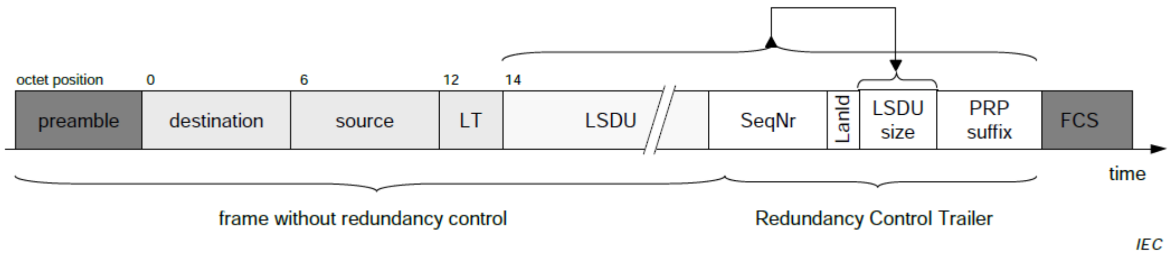
Figure 9. PRP with two DANP.



Source: IEC62439-3 (2016).

When sending data at the link layer, the LRE inserts six bytes called Redundancy Control Trailer (RCT) between the Ethernet Frame Check Sequence (FCS) and LSDU (Figure 10). Considerations for tagged and padded frames are also considered by the IEC62439-3 (2016). A IEEE802.1Q tagged frame is modified like regular Ethernet frames with the RCT, but padded frames, when required should be filled before adding the RCT, thus avoid scanning it twice (IEC62439-3, 2016). RCT has four fields that allows redundancy to be achieved using PRP. These are shown in the Table 11.

Figure 10. PRP with RCT.



Source: IEC62439-3 (2016).

Table 11. Redundancy Control Trailer (RCT) fields.

Field	**Length (bit)**	**Name**
SeqNr	16	Sequence Number
LanId	4	LAN Identifier
LanId	4	LAN Identifier
PRPsuffix	16	PRP suffix at RCT

"Sequence Number (SeqNr) is incremented for each frame a DANP sends. The doublet source MAC address, sequence number uniquely identifies copies of the same frame"IEC62439-3 (2016). The LAN Identifier (LanId) field allows a receiver to know which LAN the frame is received from. LAN˙A, has the value 1010 (xA) and LAN˙B 1011 (xB). when receiving a LanId different than expected an error is noticed with monitoring purposes.

1.4 NetFPGA and ZedBoard

Some features provided by the ZedBoard and NetFPGA are listed in Table 12.

Table 12. Zedboard and NetFPGA features.

Feature	**NetFPGA**	**ZedBoard**
	Xilinx® Kintex®-7 XC7K325T-1FFG676 FPGA	Xilinx® XC7Z020-1CLG484C Zynq-7000 AP SoC
Memory	X16 4.5 MB QDRII+ static RAM (450 MHz)	512 MB DDR3 (128M x 32)

Table 12. (Continued) Zedboard and NetFPGA features.

Feature	**NetFPGA**	**ZedBoard**
	X8 512 MB DDR3 dynamic RAM (800 MHz)	256 Mb QSPI Flash
	1-Gbit BPI Flash	
Interfaces	SD card slot	SD Card
	Four 10/100/1000 Ethernet PHYs with RGMII	10/100/1G Ethernet
	X4 Gen 2 PCI Express	USB 2.0 FS USB-UART bridge
	FMC connector	LPC FMC connector
	Two Pmod ports	USB-JTAG Programming
Oscillator	200 MHz	100 MHz (PL)
		33.333 MHz (PS)
Other	32-bit PIC microcontroller	HDMI Output
	USB microcontroller	VGA (12-bit Color)
	Real time clock	128x32 OLED Display
	Crypto-authentication chip	Audio Line-in, Line-out, headphone, microphone
	Four on-board LEDs and four on-board general-purpose buttons	Two Reset Buttons
		Seven Push Buttons
		Eight dip/slide switches
		Nine User LEDs

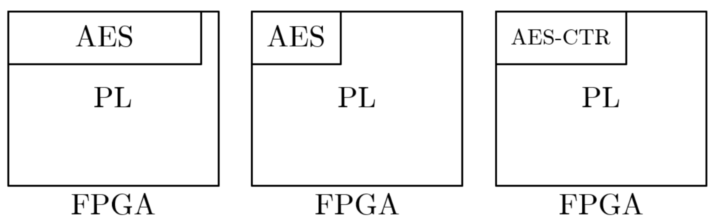
Detailed information can be found on the *"NetFPGA-1G-CML™ Board Reference Manual"* Digilent (2016) and *"Zynq™ Evaluation and Development Hardware User's Guide"* Xilinx (2014).

Chapter 2

Methodological Design of the Implementation

To implement confidentiality and high-availability over a Gigabit Ethernet (GigaE) environment, the Parallel Redundancy Protocol (PRP) and Advanced Encryption Standard (AES) with Counter mode (CTR) of operation are selected. First, AES with CTR blocks are designed. AES, based in standard (SP800131A, 2015), is designed using combinational and sequential-combinational methods separately and implemented on the Programable Logic (PL) of the FPGA. Then, Counter mode (CTR) is added as documented in (NIST, 2001a). These blocks are presented in the Figure 11.

Figure 11. Blocks of AES combinational (left), sequential (center) and sequential AES with CTR (right).



Source: Author.

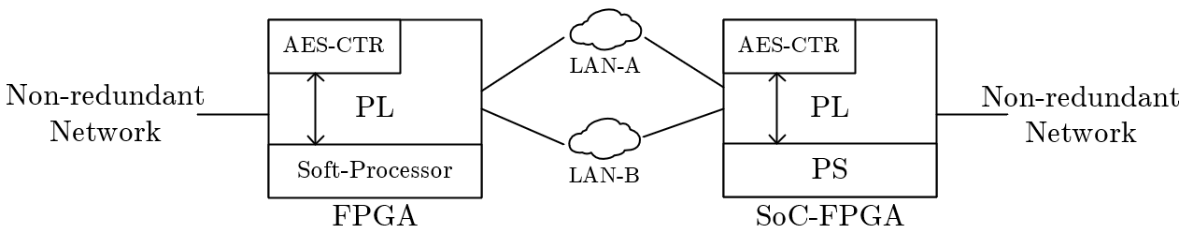
Sequential design method, as found in the documentation available for AES on FPGA, can be divided in pipelined and non-pipelined. This work shows the non-pipelined implementation for the Sequential method. AES and CTR performance are measured in terms of FPGA utilization and timing using Vivado's Synthesis and implementation as presented in chapter 3. For pipelined designs, higher utilization and throughput are expected compared to the same parameters on non-pipelined designs. Thus, the later uses lower FPGA area utilization with the disadvantage of limited throughput (in the order of Giga-bits per seconds), while pipelined throughput achieves tens or hundreds of Giga-bits per second (Silitonga, Jiang, Khan, & Becker, 2019). Chapter 3 presents a comparative of implementations based on similar devices as those used here and the reports for timing and utilization.

Framing and operation related to the Parallel Redundancy Protocol (PRP) are then designed based in standard (IEC62439-1, 2013). Its integration with AES-CTR is made by taking the encrypted data and place it within a PRP packet. Two pair of packets are proposed, the first transmits plain PRP parameters and an encrypted Link Service Data Unit (LSDU). For the second pair of packets, PRP parameters and LSDU are encrypted.

Operation for transmission and reception of encrypted PRP packets are designed to be implemented on the Processing System (PS) of the SoC-FPGA or soft-processor on the FPGA.

The described components and PRP related elements (subsection 1.3.1) are presented in the Figure 12.

Figure 12. System block components.



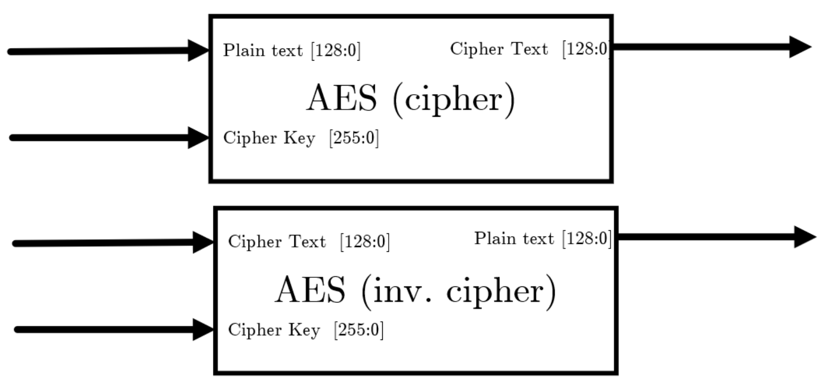
Source: Author.

To verify the operation of the implemented modules and interconnections, specifically, to verify encryption and redundancy, packets are sent between the Non-redundant networks and analyzed in the redundant network. The following sections show these components design in detail.

2.1 AES combinational and non-pipelined (sequential) design

Cipher and its inverse design are based on the transformations specified in NIST named (inv)SubBytes, (inv)ShiftRows, (inv)MixColumns and (inv)AddRoundKey. Both with the same Key Expansion. Pure combinational blocks are represented in the Figure 13.

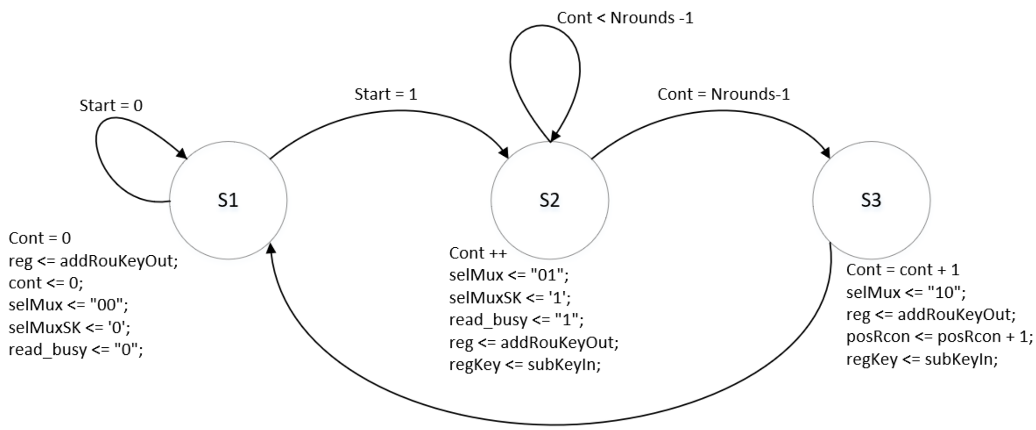
Figure 13. AES Cipher and inverse cipher combinational blocks.



Source: Author.

Unlike combinational method which only requires connections of combinational-elements, sequential strategy presents more timing complexity, thus requiring deeper design considerations as described in the Figure 15 for the system process blocks and Figure 14 for state machine.

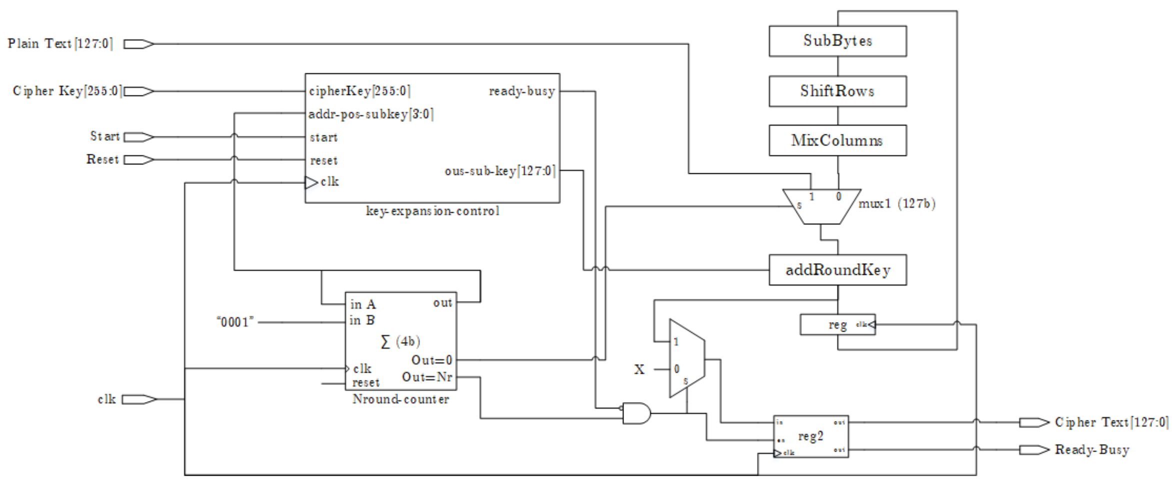
Figure 14. Process blocks state machine.



Source: Author.

The encryption process of sequential AES is straight forward. For each cycle SubBytes, ShiftRows, MixColumns and AddRoundKey are performed, and, Key generation is done once every cycle. The quantity of cycles depends on the key being used. Despite NIST (2001a) defines 10, 12 and 14 cycles for 128, 192 and 256 bit-length keys respectively, this work results (Chapter 3) requires an extra cycle in order to load data on the encryption core. The block diagram is presented in the Figure 15.

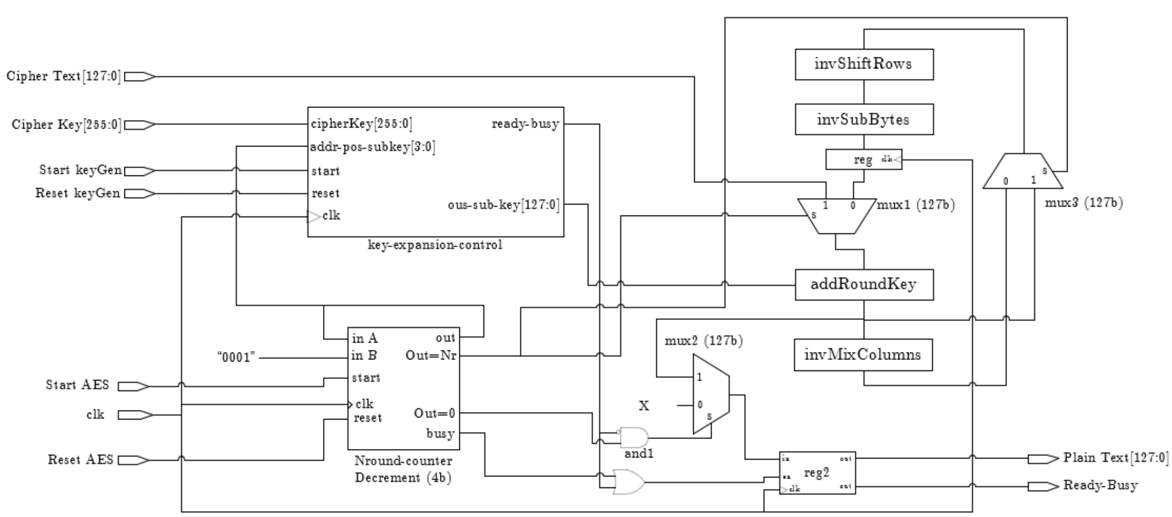
Figure 15. AES process blocks.



Source: Author.

Inverse sequential AES requires that the key generation encounters all subkey to start backwards. As a result, all subkeys are first generated and stored in a custom RAM memory. Once the key generation process is finished, the inverse cipher submodules start. Figure 16 presents its block diagram.

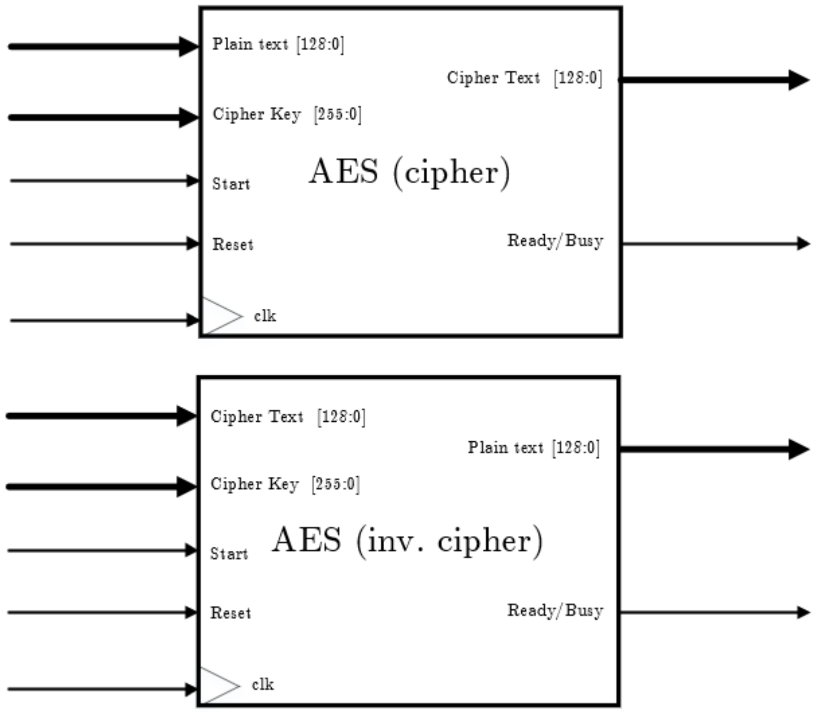
Figure 16. Inverse AES process blocks.



Source: Author.

Sequential method requires three additional inputs to control the AES process. These are the *clock* signal, *start* and *reset* ports. Also it has an extra output that allows monitoring of process completion, this is named *Ready/Busy*. These are represented in the Figure 17.

Figure 17. AES Cipher and inverse cipher Sequential-combinational blocks.



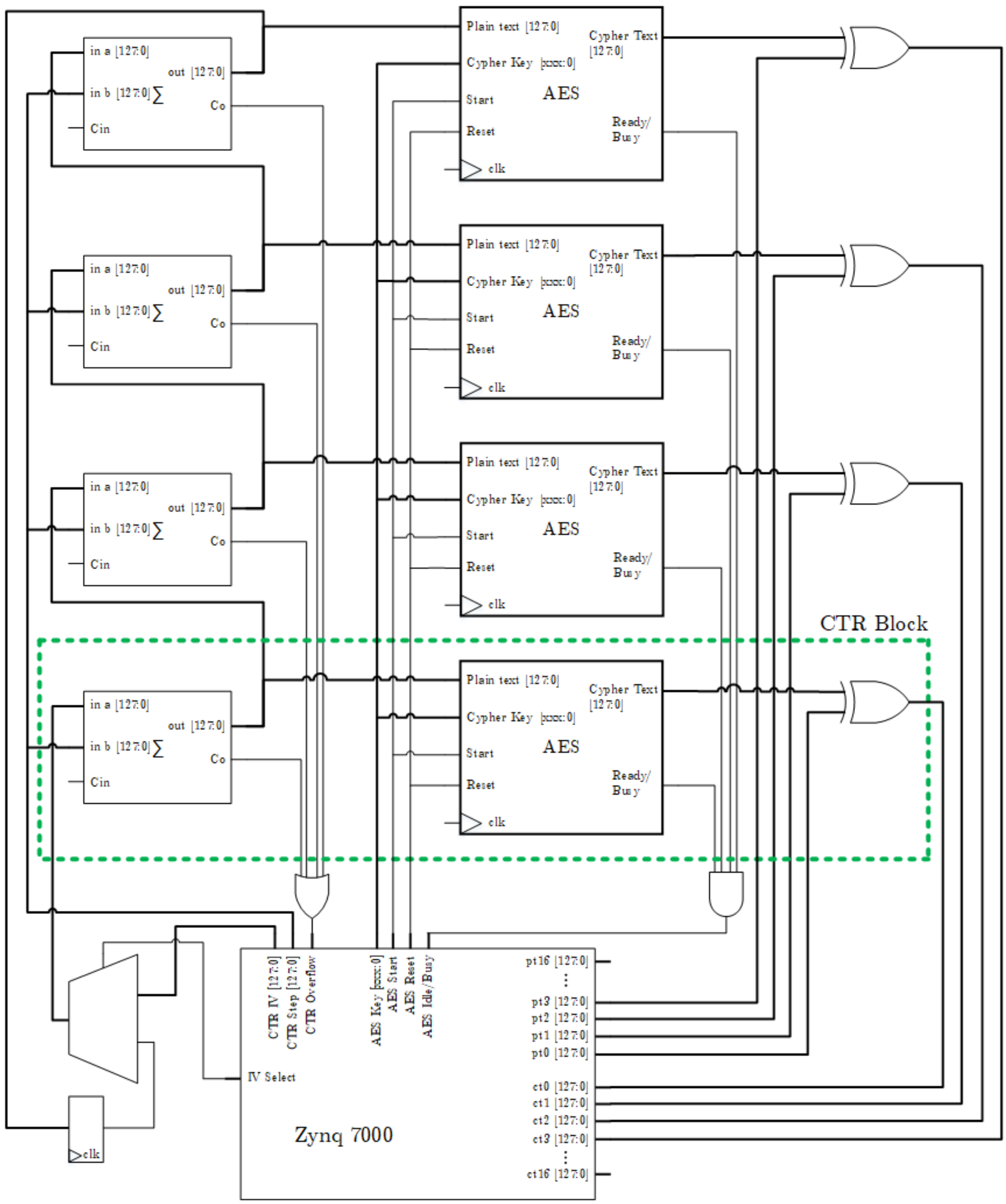
Source: Author.

After AES design, the CTR mode of operation is included into sequential AES. Combinational AES is excluded for CTR operation due to its high utilization and the fact that the implemented design requires four AES blocks.

2.2 AES (sequential) integrated blocks for CTR

According to the properties of CTR mode of operation, the cipher block is applied for encryption and decryption, thus, sequential AES-128 is grouped with a counter to form a CTR Block. Four blocks are connected in parallel and its inputs and outputs are connected to the processing system as seen in the Figure 18.

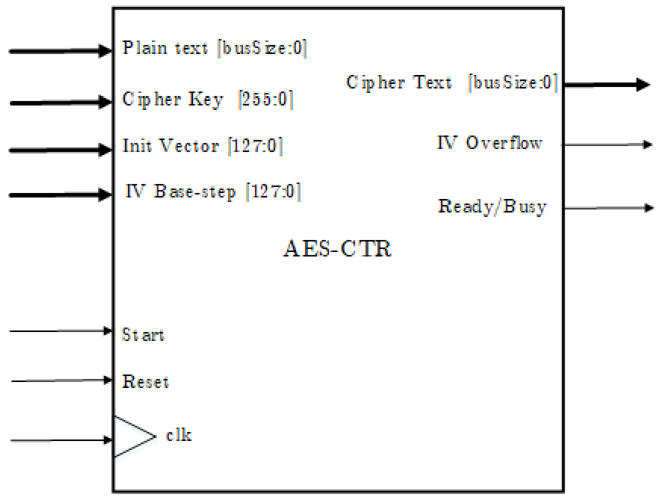
Figure 18. AES-CTR, Ethernet and processing system block diagram.



Source: Author.

IP Core design for AES-128-CTR is presented in the Figure 19.

Figure 19. AES-CTR, block diagram.



Source: Author.

2.3 PRP framing and algorithm

PRP implementation is performed entirely at Processing System (PS) for framing and discarding algorithm. Supervisory frames are not included in this work. Based on the following frame packet, formats are proposed to extend this implementation for further integration with key exchanges and VLANs. First PRP trailer gets incorporated into the IEEE802.3 frame with its documented minimum and maximum LSDU sizes. This is shown in the Figure 20. The PRP trailer is implemented according to its structure and bit sizes as described in the Figure 21.

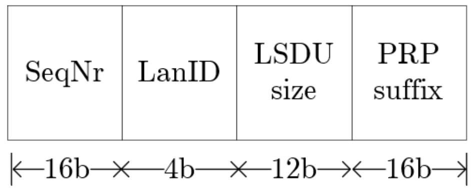
Figure 20. Ethernet frame with PRP trailer.

Dest. Addr.	Src. Addr.	Lenght Type	LSDU	IEEE 802.3 Padding	PRP trailer	FCS
6B	6B	2B	40B to 1976B		6B	4B

Source: Author.

PRP trailer description and sizes are presented in the Figure 21, where SeqNr is the sequence number of each redundant packet, LanID is the LAN identification that can be LANA or LANB, and, the LSDU size with the PRP suffix are used to validate a valid PRP trailer.

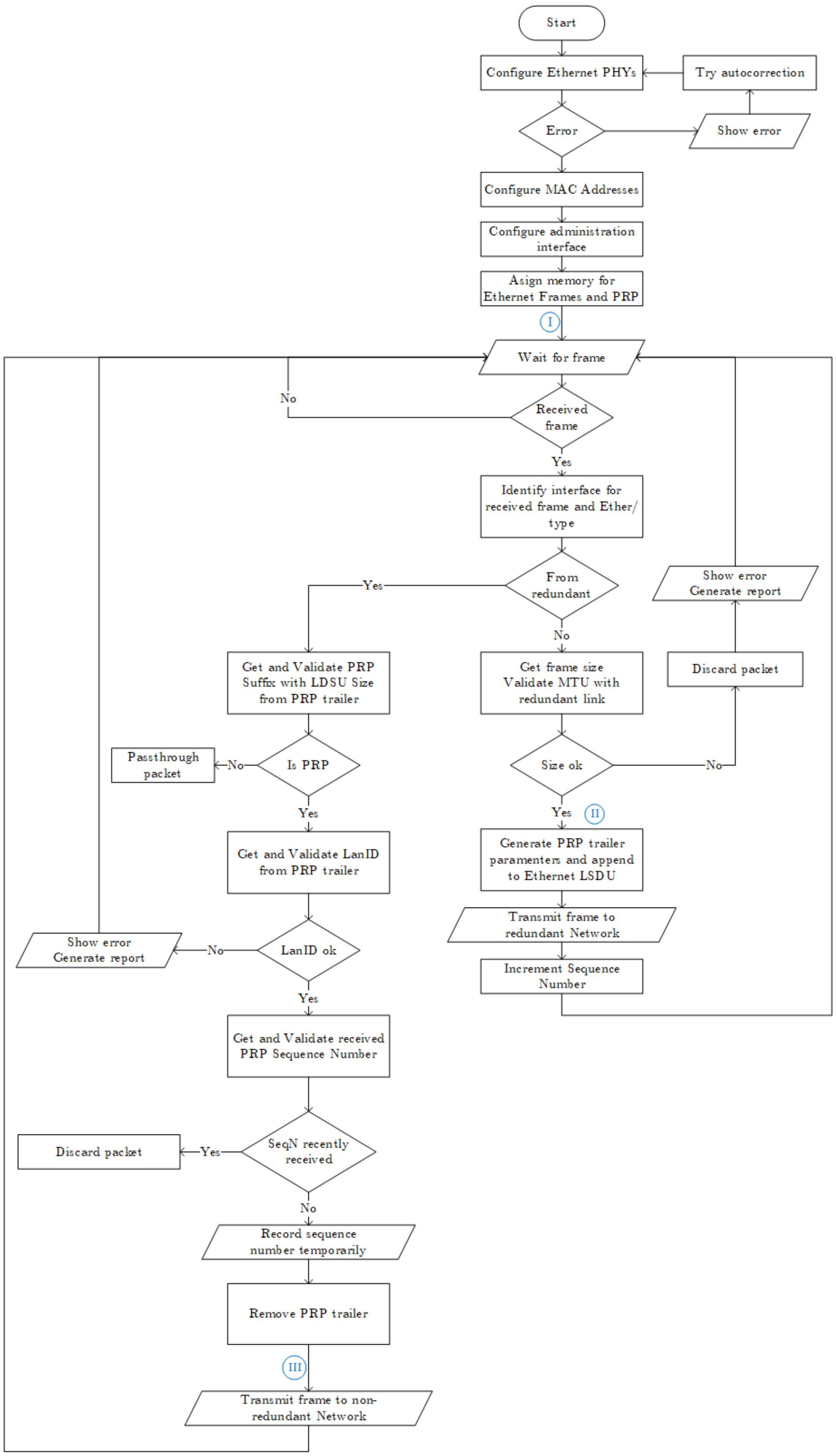
Figure 21. PRP trailer details.



Source: Author.

PRP Link Redundancy Entity (LRE) capabilities for this work, are designed based on the diagram flow presented in the Figure 22.

Figure 22. PRP LRE Flow diagram on the Processing System (PS).



Source: Author.

2.4 PRP and AES-CTR integration design

Integration of AES-CTR with PRP is designed based on its packet structure. The Figure 23 presents the design for the frame with encrypted payload. This do not interfere with Ethernet header nor PRP trailer.

Figure 23. Ethernet frame with encrypted LSDU and plain PRP trailer.

Dest. Addr.	Src. Addr.	Lenght Type	AES Encrypted	PRP trailer	F C S
6B	6B	2B	40B to 1976B	6B	4B

Source: Author.

The Figure 24 shows the design and lengths of an Ethernet frame with the IEEE802.1Q tag and the PRP trailer.

Figure 24. Ethernet with VLAN tag and encrypted LSDU and plain PRP trailer.

Dest. Addr.	Src. Addr.	IEEE 802.1Q Tag	Lenght Type	AES Encrypted	PRP trailer	F C S
6B	6B	4B	2B	36B to 1972B	6B	4B

Source: Author.

As an alternative, the PRP trailer is encrypted to hide redundancy information, but this implies to generate a PRP secure tag which allows the receiver node to multiplex and decipher at Data-link layer. The Figure 25 presents the design for this packet with its bit sizes.

Figure 25. Ethernet frame with encrypted LSDU and PRP trailer.

Dest. Addr.	Src. Addr.	PRP Secure Tag	Lenght Type	AES Encrypted	F C S
6B	6B	4B	2B	42B to 1978B	4B

Source: Author.

The Figure 26 shows the same scenario of encrypted PRP trailer and PRP secure tag for multiplexing with the addition of the IEEE802.1Q tag for VLANs.

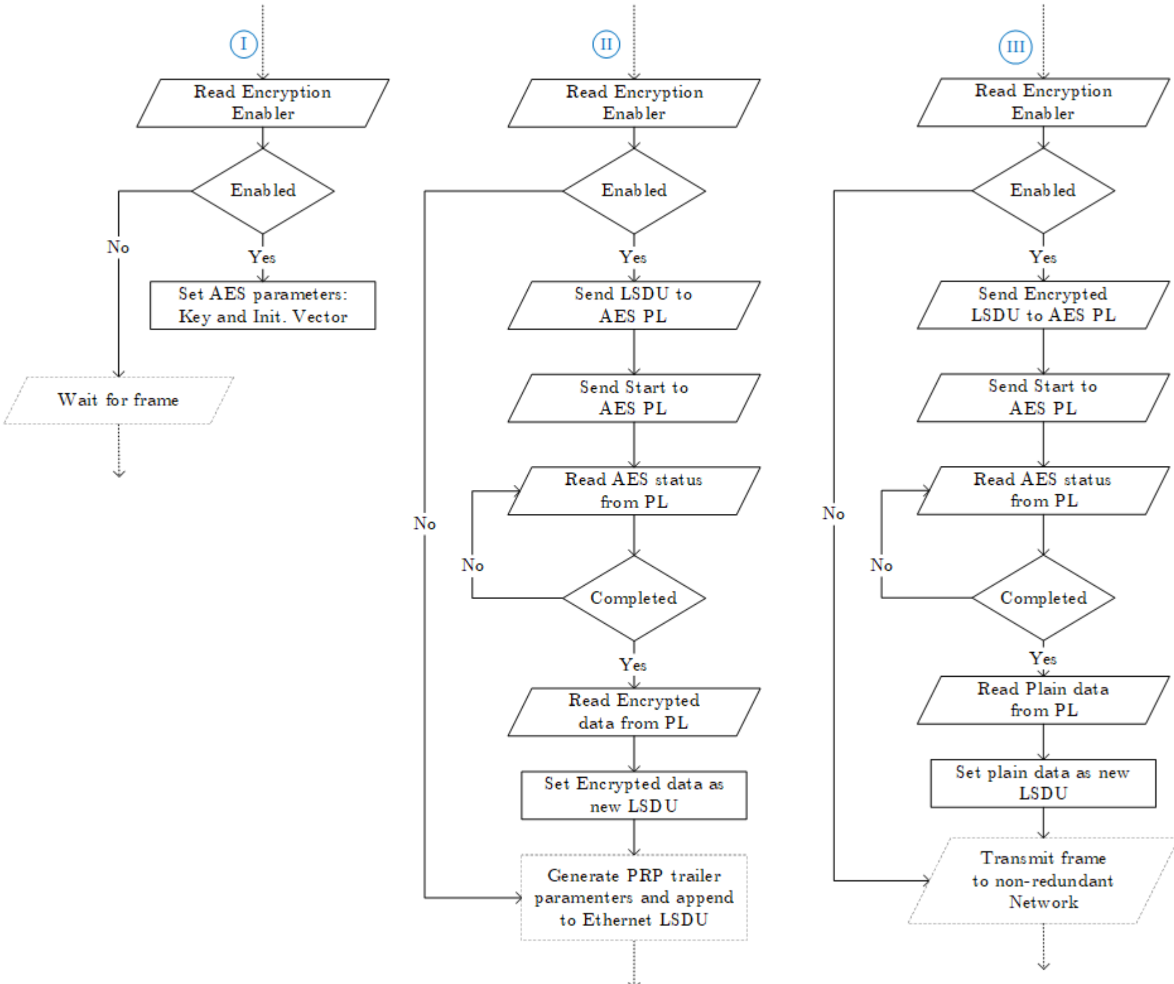
Figure 26. Ethernet and VLAN tag frame with encrypted LSDU and PRP trailer.

Dest. Addr.	Src. Addr.	IEEE 802.1Q Tag	PRP Secure Tag	Lenght Type	AES Encrypted	F C S
6B	6B	4B	4B	2B	38B to 1974B	4B

Source: Author.

Once integrated in the packet, AES is controlled from PRP Link Redundancy Entity (LRE) by adding the corresponding code described in the Figure 27 and connected to previously LRE flow (Figure 22).

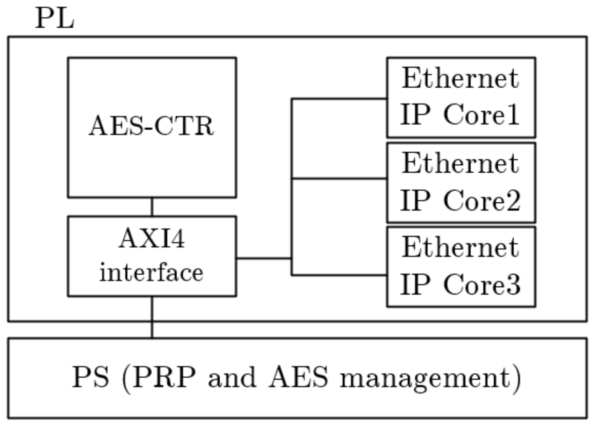
Figure 27. PRP with AES integration flow diagram on the Processing System (PS).



Source: Author.

Hardware integration of PRP and AES-CTR is elaborated by the interconnection of Programable Logic (PL) elements with the Processing System (PS). This interconnection is made by using the Advanced eXtensible Interface (AXI) interface, which permits the communication between the Ethernet interfaces and the AES-CTR Cores, with the Processing System. The Figure 28 shows the diagram with the elements required.

Figure 28. PRP with AES-CTR Hardware integration.



Source: Author.

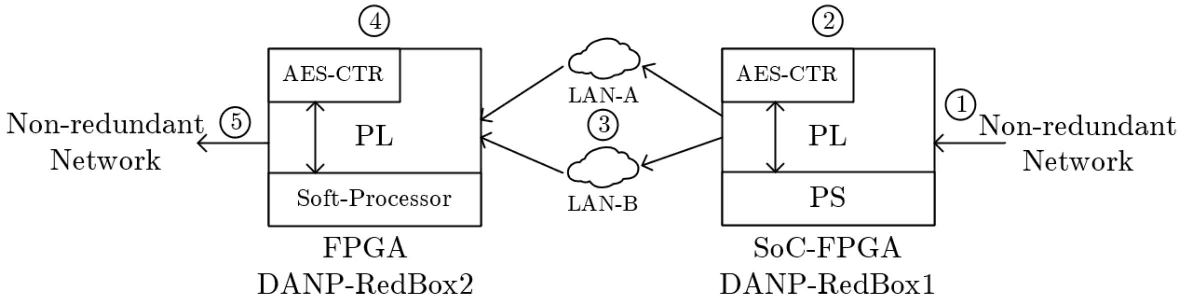
2.5 PRP and AES-CTR integration verification

To verify operation of the system, two devices are required (Figure 12). Each device is described previously Figure 28, where the Ethernet Cores are used to connect to the redundant and non-redundant networks.

Two tests are identified to verify and evaluate the implementation: a simple communication to verify correctness of PRP framing and its encrypted payload using different packet sizes; and, a Unit Under Test (UUT) methodology to evaluate the performance of the complete system.

In the simple communication scheme (Figure 29), a packet is sent from the non-redundant network and received in the device (step 2 in the figure), then, (step 3) this device send the packets with their PRP trailers and ciphered LSDU to the redundant network by using parts of the operation flow as described in the Figure 22 and Figure 27. At step 4, the device apply the discarding algorithm (Figure 22 and Figure 27), decipher the payload (LSDU) and send to the non-redundant network (Step 5).

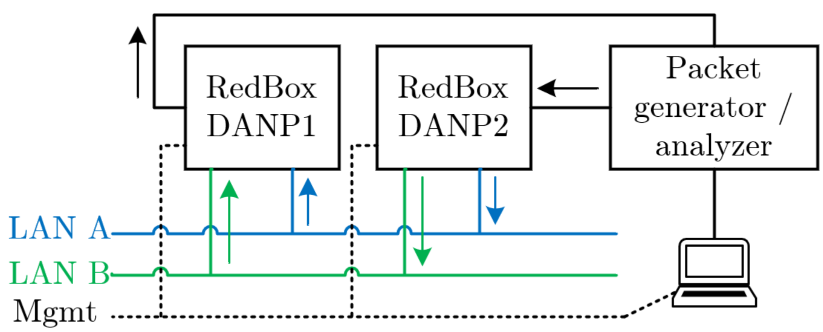
Figure 29. PRP with AES-CTR simple communication verification.



Source: Author.

This communication verification is used in this work, and its results are shown in Chapter 3. On the other hand, the UUT scheme (Figure 30) let the performance parameters of the integrated system be evaluated on physical implementation. The parameters that can be physically tested (including PL and PS), among others, are the throughput, transmission rates and packet losses.

Figure 30. PRP with AES-CTR UUT test.



Source: Author.

The UUT test requires a packet generator and analyzer, which transmits an specific packet data and expects to receive the same packet on its other interface to compare quantity of transmitted packets versus received, latency and loss rate, among others. Although the benefits of the UUT test, this is not presented in this work considering availability of the packet analyzer, the time extension required to develop the current work and the enhancements identified for the AES-CTR Core. These considerations are left for future work and explained in the section 3.5.

Chapter 3

Results and Analysis

The physical implementation use a Xilinx® Kintex®-7 XC7K325T Net-FPGA and Xilinx® Zedboard with FMC ports. Those physical components are named DANP-RedBox. Zedboard implements DANP-RedBox-1 for cipher and to send to PRP redundant network. On the other hand, NetFPGA implements DANP-RedBox-2 to decryption process and PRP-LRE discarding algorithm.

Also, extracted from the physical devices, these nodes have two general components: software and hardware. So implementation of *main-DANP* and *test-DANP*, and, in order to comply with the objectives of this work, is achieved with the following. First, AES is implemented on hardware using a combinational and sequential-combinational using a non-pipelined strategy to compare time performance and hardware utilization which allows to select the one that best fits the design. Then, CTR mode of operation is implemented for data streams with a fixed bit-length. Second, the Link Redundancy Entity (LRE) algorithm, which defines PRP operation, is implemented on software and hardware. The software part, on top of the processor, interfaces the Link Redundancy Entity (LRE) with Network layer, has some functionalities of LRE, controls AES blocks for cipher-decipher and registers Ethernet status among others. Hardware part, manages link layer framing and LRE functions.

The implementation of AES hardware is made on *Xilinx* development environment, particularly *Vivado* 2019.2 for AES hardware description, communication and processing logic; and *Vitis* 2019.2 for software and communication testing over the $ZYNQ-7000$ processor. AES results are presented in behavioral simulation and implementation using the generated *bitstream* for each IP. The synthesis with timing results are shown as presented in *Vivado* table reports.

3.1 AES results

The AES IPs, generated using VHDL, are evaluated by Vivado 2019 Simulation, Synthesis and Implementation. Simulation results shows the behavior of VHDL implemented, Synthesis presents the timing reports to obtain maximum frequency and throughput, and, Implementation is made by an Out of Context (OOC) hierarchical methodology that allows to obtain more accurate Slices utilization reports. VHDL Entities and hardware description are presented in Appendix A.2.

3.1.1 Combinational AES IP Cores

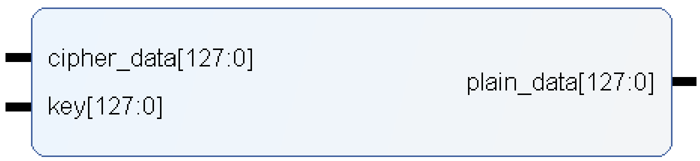
The IP cores for both cipher and decipher are implemented using VHDL and generated independently using the IP *Vivado packager* that uses *IP-XACT* standard (ug1118). The

Figure 31 shows the IP for combinational AES cipher and Figure 32 for AES inverse cipher.

Figure 31. IP AES cipher port diagram.

Source: Author.

Figure 32. IP AES inverse cipher port diagram.



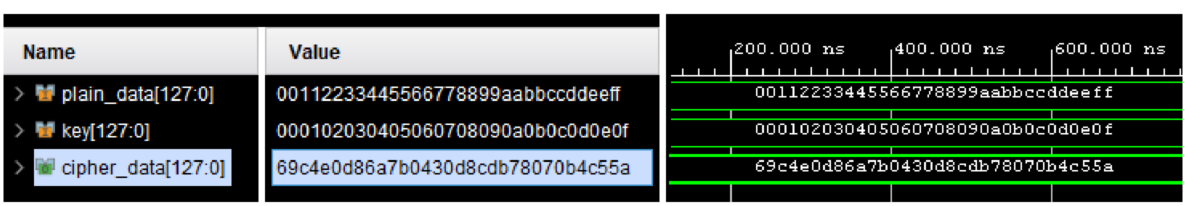
Source: Author.

The following AES combinational results are tested on the Zynq7000 SoC (xc7z020clg484-1) using Vivado 2019-2.

3.1.1.1 Combinational AES IP Cores behavioral simulation

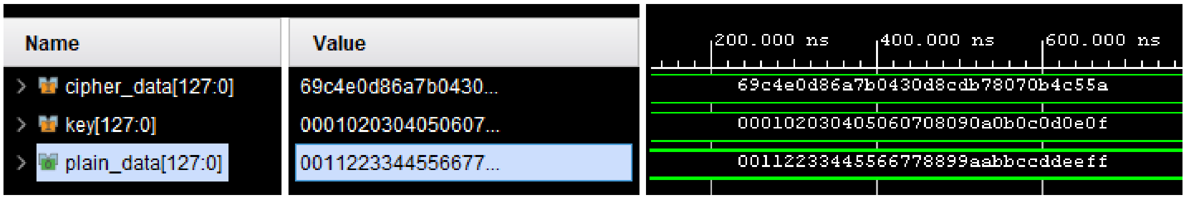
Behavioral simulation is presented for AES IP with a key of 128 bit-length size. Key sizes of 192 and 256 are not tested due to the high utilization report presented in the following subsection. The Figure 33 and Figure 34 presents the encryption and decryption results respectively using the test vectors documented in NIST (2001a).

Figure 33. Behavioral simulation for combinational AES-128 cipher.



Source: Author.

Figure 34. Behavioral simulation for combinational AES-128 inverse cipher.



Source: Author.

3.1.1.2 Combinational AES IP Cores Timing

Timing results are extracted from Vivado Systhesis report. As no Clock is included in this combinational design, only the throughput is presented and calculated by Equation 3.1 (Soltani & Sharifian, 2015). Results do not include Hold and Setup configurations for IO and are left for future work analysis.

$$Throughput = \frac{Outputed\_bits}{Delay\_of\_critical\_path} \tag{3.1}$$

For AES cipher, Total delay Path, from input source to output destination taken from Synthesis timing report is 42.378nS (Figure 35), thus, with a bit length of 128 bits, the throughput is 3.02$Gbps$.

Figure 35. Cipher worst path delay.

Name	Levels	From	To	Net Delay	Logic Delay	Total Delay
Path 1	53	plain_data[59]	cipher_data[48]	30.512	11.866	42.378

Source: Author.

For inverse cipher Delay is 82.571nS (Figure 36) obtaining a throughput of 1.55$Gbps$.

Figure 36. Inverse cipher worst path delay.

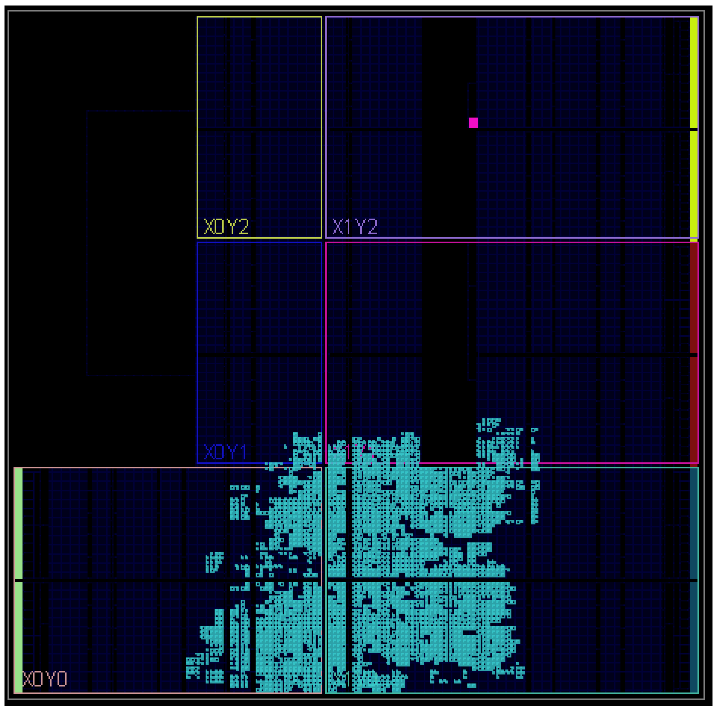
Name	Levels	From	To	Logic Delay	Net Delay	Total Delay
Path 1	97	key[16]	plain_data[24]	18.745	63.826	82.571

Source: Author.

3.1.1.3 Combinational AES IP Cores Utilization

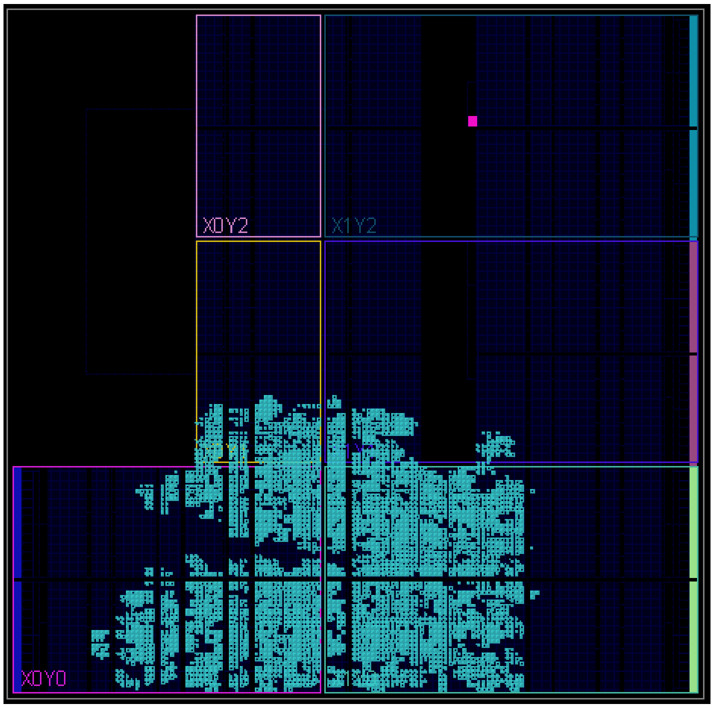
Utilization of slices is taken from implementation reports configured with the hierarchical methodology named Out of Context (OOC). The Figure 37 and Figure 38 presents the area utilized for cipher and it inverse. For these results, floor-planning are not considered and are left for future work.

Figure 37. Utilization space of combinational AES-128.



Source: Author.

Figure 38. Utilization space of combinational inverse AES-128.



Source: Author.

The Slice Logic distribution is shown in the Table 13 for both, cipher and its inverse. The detailed utilization report can be found in Appendix A.3.

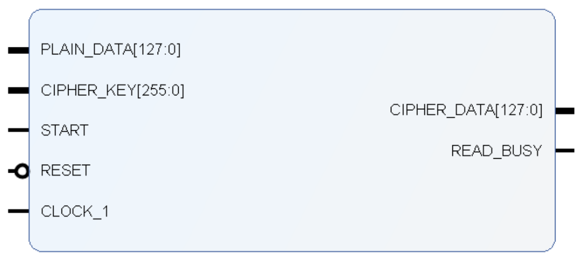
Table 13. Slice utilization for combinational AES.

		Cipher		Inverse cipher	
Site Type	**Available**	**Used**	**Util%**	**Used**	**Util%**
Slice	13300	2541	19.11	3451	25.95
LUT as Logic	53200	9280	17.44	12249	23.02
LUT as Memory	17400	0	0	0	0
Slice Registers	106400	0	0	0	0

3.1.2 Sequential AES IP Cores

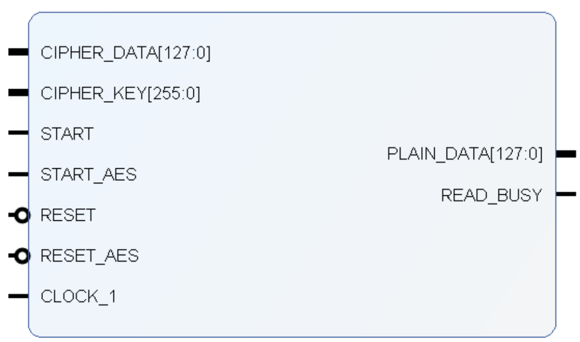
The IP cores for both cipher and decipher are implemented using VHDL and generated independently using the IP *Vivado packager* that uses *IP-XACT* standard (ug1118). Its hardware description has an asynchronous reset and the generics that allow the selection of 128, 192 or 256 bit-length key. The Figure 39 shows the IP for sequential AES cipher and the Figure 40 for its inverse.

Figure 39. AES cipher IP port diagram.



Source: Author.

Figure 40. AES inverse cipher IP port diagram.



Source: Author.

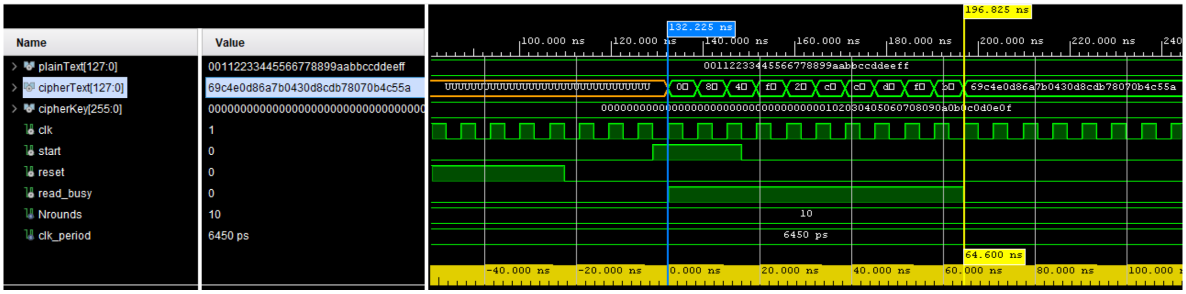
The following results for sequential AES are tested on the Zynq7000 SoC (xc7z020clg484-1) using Vivado 2019-2

3.1.2.1 Sequential AES IP Cores behavioral simulation

Behavioral simulations for AES IP are done by configuring VHDL generic to 128, 192, and 256 bit-length. Test vectors presented in this simulation are verified according to NIST (2001a). These test vectors are taken from NIST (2001a).

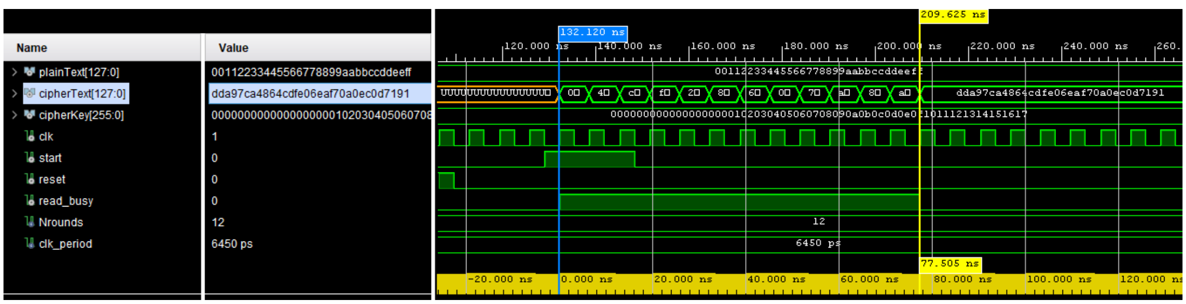
the Figure 41, Figure 42 and Figure 43 show the behavior for AES cipher.

Figure 41. Behavioral simulation for sequential AES-128 cipher.



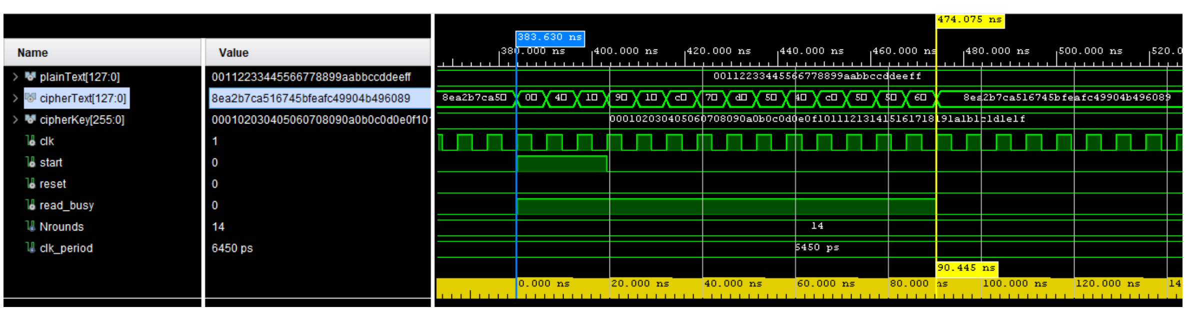
Source: Author.

Figure 42. Behavioral simulation for sequential AES-192 cipher.



Source: Author.

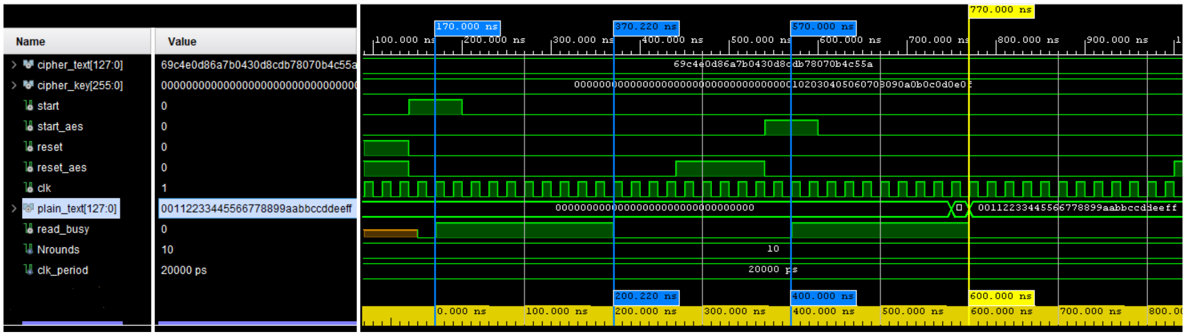
Figure 43. Behavioral simulation for sequential AES-256 cipher.



Source: Author.

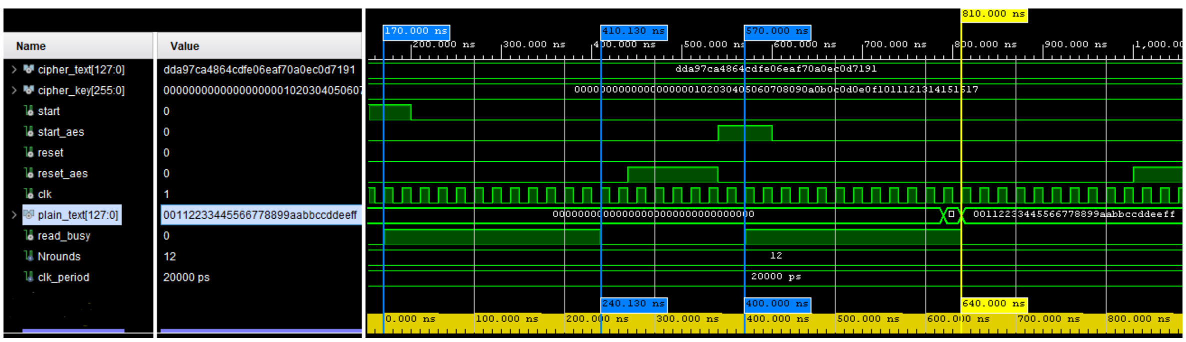
The Figure 44, Figure 45 and Figure 46 show the behavior for AES inverse cipher.

Figure 44. Behavioral simulation for sequential AES-128 inverse cipher.



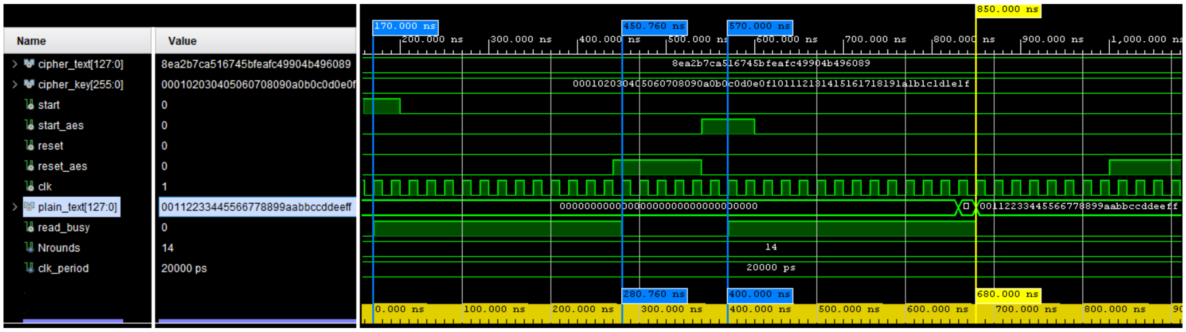
Source: Author.

Figure 45. Behavioral simulation for sequential AES-192 inverse cipher.



Source: Author.

Figure 46. Behavioral simulation for sequential AES-256 inverse cipher.



Source: Author.

3.1.2.2 Sequential AES IP Cores Timing

Timing results are taken from Vivado Synthesis. With a Clock period constrained in the Xilinx Design Constraints (XDC) file, a Worst Negative Slack (WNS) is found to calculate, using Equation 3.2 (Xilinx, 2019), the Maximum Frequency supported by the AES Core.

$$Max\_Freq = \frac{1}{T - WNS} \tag{3.2}$$

AES cipher, with a Clock period of $6.450nS$, sets the maximum frequency to $155MHz$ and the WNS to $0.001nS$ as presented in Figure 47. The detailed timing report can be found on Appendix A.4.

Figure 47. AES-128 cipher Synthesis Timing summary.

Setup		Hold		Pulse Width	
Worst Negative Slack (WNS):	0,001 ns	Worst Hold Slack (WHS):	0,150 ns	Worst Pulse Width Slack (WPWS):	2,725 ns
Total Negative Slack (TNS):	0,000 ns	Total Hold Slack (THS):	0,000 ns	Total Pulse Width Negative Slack (TPWS):	0,000 ns
Number of Failing Endpoints:	0	Number of Failing Endpoints:	0	Number of Failing Endpoints:	0
Total Number of Endpoints:	534	Total Number of Endpoints:	534	Total Number of Endpoints:	270

Source: Author.

Thus, AES cipher Throughput of $1.8Gbps$ is obtained from Equation 3.3 (Chhabra & Lata, 2018).

$$Throughput = \frac{Block\_length \times Max\_Freq}{Cycle\_Count} \tag{3.3}$$

Inverse AES has a maximum frequency of $93.65MHz$, throughput of $1.09Gbps$ and WNS of $0.002nS$ as presented in Figure 48. The detailed timing report can be found in Appendix A.4.

Figure 48. AES-128 inverse cipher Synthesis Timing summary.

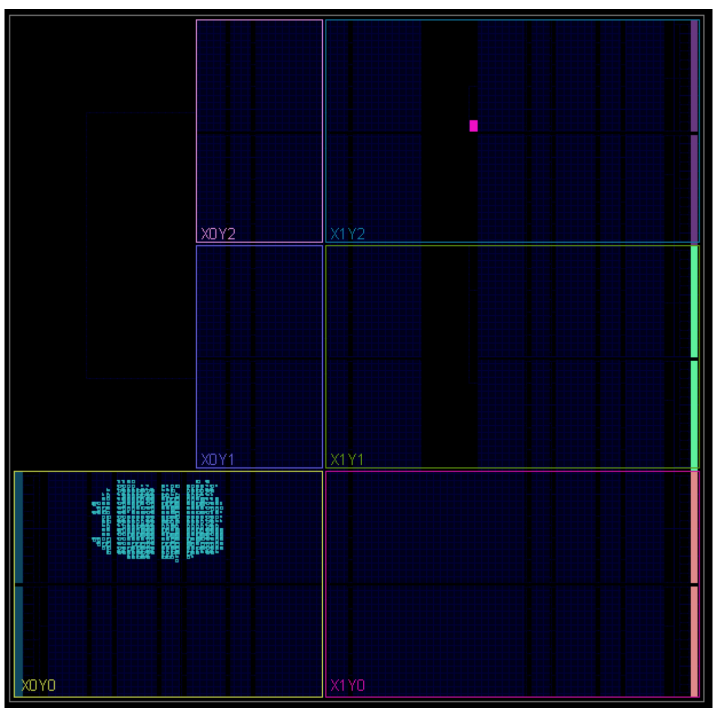
Setup		Hold		Pulse Width	
Worst Negative Slack (WNS):	0,002 ns	Worst Hold Slack (WHS):	0,140 ns	Worst Pulse Width Slack (WPWS):	4,840 ns
Total Negative Slack (TNS):	0,000 ns	Total Hold Slack (THS):	0,000 ns	Total Pulse Width Negative Slack (TPWS):	0,000 ns
Number of Failing Endpoints:	0	Number of Failing Endpoints:	0	Number of Failing Endpoints:	0
Total Number of Endpoints:	857	Total Number of Endpoints:	857	Total Number of Endpoints:	423

Source: Author.

3.1.2.3 Sequential AES IP Cores Utilization

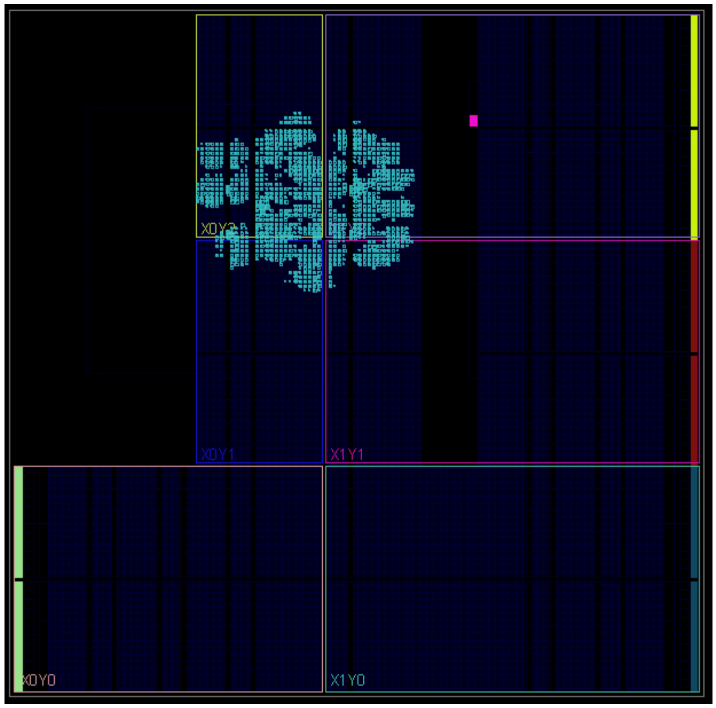
Slice utilization is reported by Vivado Implementation using the Out of Context (OOC) hierarchy. The Figure 49 and Figure 50 show the area utilized for cipher and its inverse. For these results, floor-planning is not considered and left to future work.

Figure 49. Utilization space of sequential AES-128.



Source: Author.

Figure 50. Utilization space of sequential inverse AES-128.



Source: Author.

The Sequential AES Slice logic distribution is presented in the Table 14. The detailed utilization report can be found in Appendix A.5.

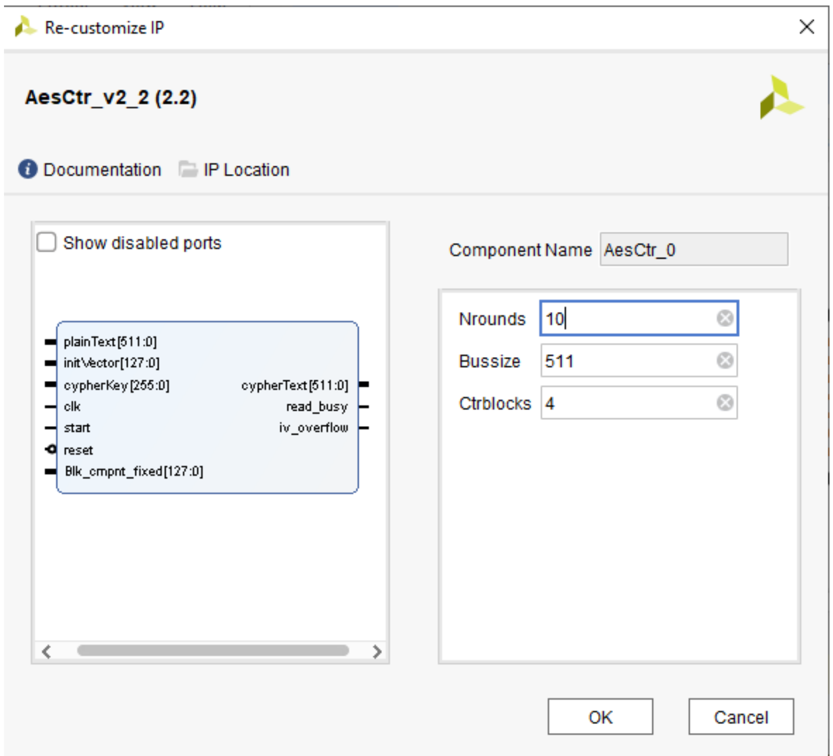
Table 14. Slice and BRAM utilization for sequential AES-128.

		Cipher		Inverse cipher	
Site Type	**Available**	**Used**	**Util%**	**Used**	**Util%**
Slice	13300	363	2.73	966	7.26
LUT as Logic	53200	1314	2.52	3409	6.41
LUT as Memory	17400	0	0	0	0
Slice Registers	106400	269	0.25	413	0.39
Block RAM	140	0	0	2	1.43

3.1.3 AES-CTR IP Cores

IP cores for both cipher and decipher are implemented using VHDL and generated independently using the IP *Vivado packager* that uses *IP-XACT* standard (ug1118). Its hardware description has an asynchronous reset and the generics that allow the selection of key and blocks sizes for CTR mode. The Figure 51 shows the IP for AES-CTR cipher / decipher.

Figure 51. IP AES-CTR cipher port diagram and generics.



Source: Author.

These generics are *Nrounds* to select the key size; *Bussize* to configure the maximum value for the position of Most Significant bit (MSb) of plain and encrypted data bits; and *Ctrblocks* that defines the quantity of AES blocks. *Nrounds* can be set to 10, 12 or 14 to select key sizes of 128, 192 or 256 respectively. *Bussize* represents the MSb position value: 511 *downto* 0, which is directly related to *Ctrblocks* value because each block, as standardized in NIST (2001a) , has 128 bits for either encrypted and plain data, thus $4x128 = 512$ or 511 *downto* 0. Table 15 describe ports used.

Table 15. IPs ports.

Port	**Type**	**Size**	**Description**
plain_text	Input/Output	$Bussize/[511:0]$	readable plain data
cipher_text	Input/Output	$Bussize/[511:0]$	Encrypted data
init_vector	Input	[127 : 0]	Initialization Vector. see NIST (2001b)
key	Input	[255 : 0]	Key for encryption and decryption. Least Significant bit (LSb) are used for each key length.
ctr_step	Input	[127 : 0]	An increment step between each block. $0x1$ by default
reset	Input	[0 : 0]	Asynchronous reset active high
start	Input	[0 : 0]	Start of encryption/decryption process by setting bit
clk	Input	[0 : 0]	Clock
ready_busy	Output	[0 : 0]	Set when busy, cleared when idle
iv_overflow	Output	[0 : 0]	Set when an initialization vector overflow occurs

The following AES results are tested on the Zynq7000 SoC (xc7z020clg484-1) and Kintex 7 (xc7k325tffg676-1) using Vivado 2019-2.

3.1.3.1 AES-CTR IP Cores behavioral simulation

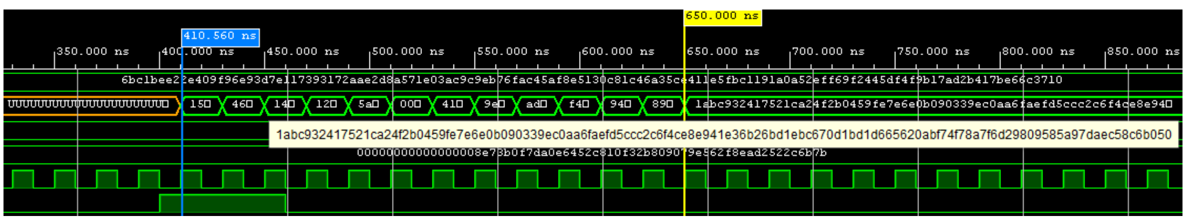
Behavioral simulations for AES IP are done by configuring VHDL generic to 128, 192, and 256 bit-length. Test vectors presented in this simulation are verified according to NIST (2001a). These test vectors, are taken from NIST (2001b).
The Figures 52, 53 and 54 show the behavioral simulation for cipher AES-CTR with key lengths of 128, 192 and 256 respectively. The Clock cycles required for each key are 11, 13 and 15. Simulations are made with a 20ns period clock.
AES-CTR encryption is verified with the test vectors used in standard (NIST, 2001b). The

Figures 52, 53 and 54 show the behavioral encrypted data resulted for AES-CTR with key lengths of 128, 192 and 256 respectively.

Figure 52. Behavioral simulation for AES-CTR-128 cipher.

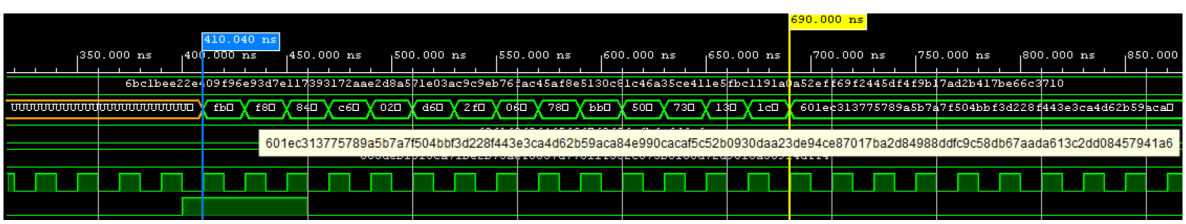
Source: Author.

Figure 53. Behavioral simulation for AES-CTR-192 cipher.



Source: Author.

Figure 54. Behavioral simulation for AES-CTR-256 cipher.



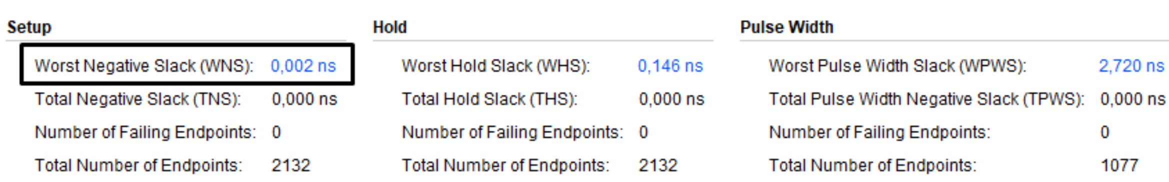
Source: Author.

3.1.3.2 AES-CTR IP Cores Timing

Timing results are taken from Vivado Synthesis. The Equation 3.2 and Equation 3.3 are used to find the maximum frequency and throughput with a WNS of $0.002nS$ (Figure 55) for

Zynq7000 and $0.005nS$ (Figure 56) for Kintex 7. There results do not include Tcl commands for Hold neither Setup configurations for IO and are left for future work analysis.

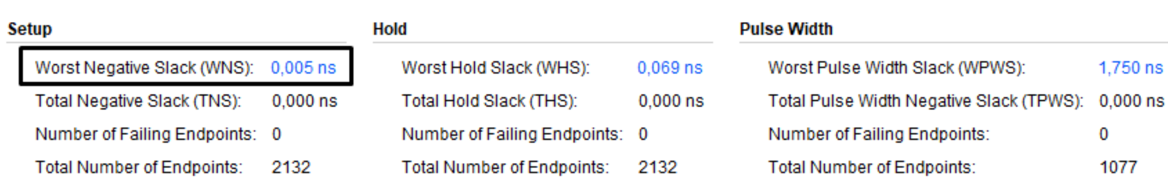
Figure 55. Zynq 7000 AES-128-CTR Synthesis Timing Summary.



Setup		Hold		Pulse Width	
Worst Negative Slack (WNS):	0,002 ns	Worst Hold Slack (WHS):	0,146 ns	Worst Pulse Width Slack (WPWS):	2,720 ns
Total Negative Slack (TNS):	0,000 ns	Total Hold Slack (THS):	0,000 ns	Total Pulse Width Negative Slack (TPWS):	0,000 ns
Number of Failing Endpoints:	0	Number of Failing Endpoints:	0	Number of Failing Endpoints:	0
Total Number of Endpoints:	2132	Total Number of Endpoints:	2132	Total Number of Endpoints:	1077

Source: Author.

Figure 56. Kintex 7 AES-128-CTR Synthesis Timing Summary.



Setup		Hold		Pulse Width	
Worst Negative Slack (WNS):	0,005 ns	Worst Hold Slack (WHS):	0,069 ns	Worst Pulse Width Slack (WPWS):	1,750 ns
Total Negative Slack (TNS):	0,000 ns	Total Hold Slack (THS):	0,000 ns	Total Pulse Width Negative Slack (TPWS):	0,000 ns
Number of Failing Endpoints:	0	Number of Failing Endpoints:	0	Number of Failing Endpoints:	0
Total Number of Endpoints:	2132	Total Number of Endpoints:	2132	Total Number of Endpoints:	1077

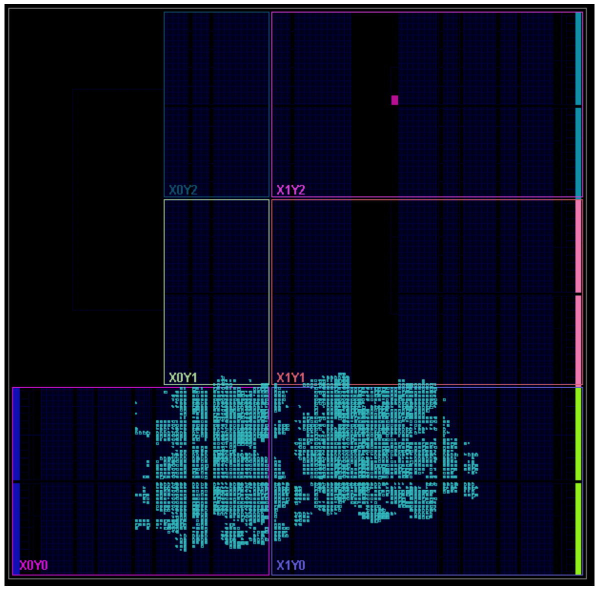
Source: Author.

For Zynq7000, Maximum frequency reported is $155.327MHz$ and, with 4 blocks of 128 bit each, Throughput calculated for 512 bit-length output is $7.22Gbps$. Kintex 7 presents a Maximum Frequency of $237.37MHz$ and Throughput of $11.11Gbps$. Complete reports are generated using the Tcl command report_timing. These can be found in Appendix A.6 for Zynq 7000 and Kintex 7.

3.1.3.3 AES-CTR IP Cores utilization

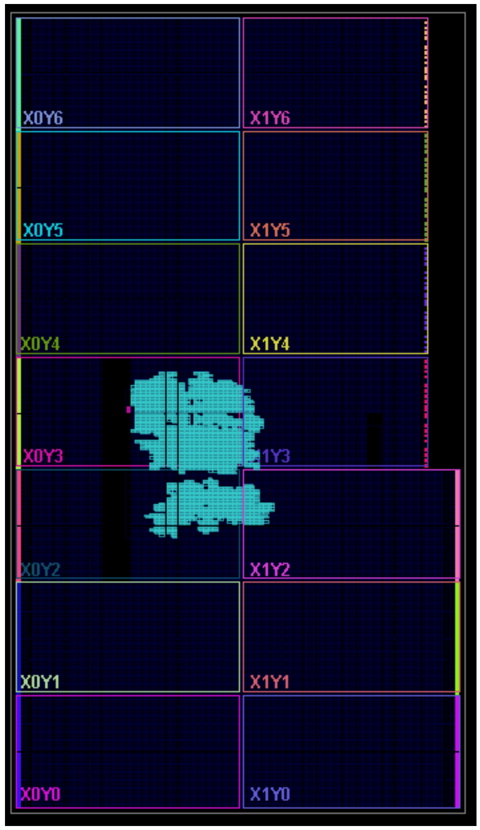
Utilization of slices is taken from implementation reports configured with the hierarchical methodology named Out of Context (OOC). The Figure 57 presents the area utilized for AES-128-CTR. For these results, floor-planning are not considered and are left for future work.

Figure 57. Zynq 7000 Utilization space of AES-128-CTR.



Source: Author.

Figure 58. Kintex 7 Utilization space of AES-128-CTR.



Source: Author.

The Slice Logic distribution is shown in the Table 16. Complete reports are generated using the Tcl command report_utilization. These can be found in Appendix A.7 for Zynq 7000 and Kintex 7.

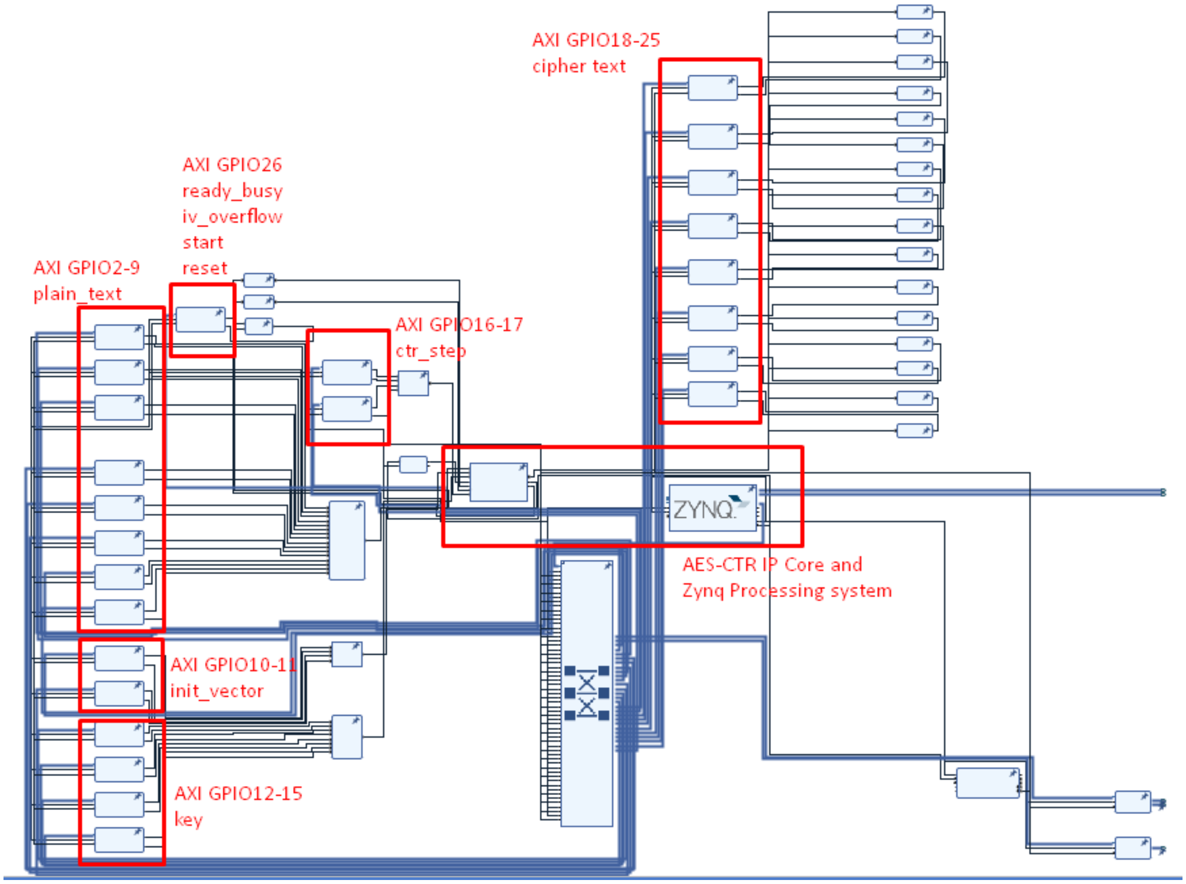
Table 16. Slice utilization for AES-CTR.

	Zynq 7000			Kintex 7		
Site Type	**Available**	**Used**	**Util%**	**Available**	**Used**	**Util%**
Slice	13300	2275	17.11	50950	2276	4.47
LUT as Logic	53200	8178	15.37	203800	8116	3.98
LUT as Memory	17400	0	0	64000	0	0
Slice Registers	106400	1076	1.01	407600	1076	0.26
Block RAM	140	0	0	445	0	0

3.1.3.4 AES-CTR IP Core implementation

The test of IP for both, cipher and inverse cipher, are based on the schematic presented in the Figure 59. Connections between the Zynq processing system and AES-CTR IP are made by AXI interconnect elements. The name of processing-relevant AXI ports can be seen in Figure 59 also.

Figure 59. AES-CTR IP test schematic.



Source: Author.

After successful bitstream generation (Figure 60), hardware is exported to Vitis. Software to control AES-CTR block is made on C programming language.

Figure 60. Synthesis, Implmentation and Bitstream generation status.

Source: Author.

Within Vitis automatically-generated files, two source files and a library are implemented in order to access AXI ports (*gpio_mgmt.c*, *gpio_mgmt.h*) and to control the encryption/decryption process (*main.c*). *gpio_mgmt.h* defines the constants used to relate the data ports with its corresponding AXI-GPIO port (Figure 61). These lines are also related to the block diagram presented in the Figure 59.

Figure 61. *gpio_mgmt.h* fragment.

```
/*********************************************************************/
/*********************************************************************/
    #define AES_PLAIN_TEXT_511_448  XPAR_AXI_GPIO_2_DEVICE_ID
    #define AES_PLAIN_TEXT_447_384  XPAR_AXI_GPIO_3_DEVICE_ID
    #define AES_PLAIN_TEXT_383_320  XPAR_AXI_GPIO_4_DEVICE_ID
    #define AES_PLAIN_TEXT_319_256  XPAR_AXI_GPIO_5_DEVICE_ID
    #define AES_PLAIN_TEXT_255_192  XPAR_AXI_GPIO_6_DEVICE_ID
    #define AES_PLAIN_TEXT_191_128  XPAR_AXI_GPIO_7_DEVICE_ID
    #define AES_PLAIN_TEXT_127_64   XPAR_AXI_GPIO_8_DEVICE_ID
    #define AES_PLAIN_TEXT_63_0     XPAR_AXI_GPIO_9_DEVICE_ID
/*********************************************************************/
/*********************************************************************/
    #define AES_KEY_255_192 XPAR_AXI_GPIO_12_DEVICE_ID
    #define AES_KEY_191_128 XPAR_AXI_GPIO_13_DEVICE_ID
    #define AES_KEY_127_64  XPAR_AXI_GPIO_14_DEVICE_ID
    #define AES_KEY_63_0    XPAR_AXI_GPIO_15_DEVICE_ID
/*********************************************************************/
/*********************************************************************/
    #define AES_IV_127_64   XPAR_AXI_GPIO_10_DEVICE_ID
    #define AES_IV_63_0     XPAR_AXI_GPIO_11_DEVICE_ID
/*********************************************************************/
/*********************************************************************/
    #define AES_BLK_CMPNT_FIXED_127_64  XPAR_AXI_GPIO_16_DEVICE_ID
    #define AES_BLK_CMPNT_FIXED_63_0    XPAR_AXI_GPIO_17_DEVICE_ID
/*********************************************************************/
/*********************************************************************/
    #define AES_CONTROL_STATUS  XPAR_AXI_GPIO_26_DEVICE_ID
/*********************************************************************/
/*********************************************************************/
    #define AES_CYPHER_TEXT_511_448 XPAR_AXI_GPIO_25_DEVICE_ID
    #define AES_CYPHER_TEXT_447_384 XPAR_AXI_GPIO_24_DEVICE_ID
    #define AES_CYPHER_TEXT_383_320 XPAR_AXI_GPIO_23_DEVICE_ID
    #define AES_CYPHER_TEXT_319_256 XPAR_AXI_GPIO_22_DEVICE_ID
    #define AES_CYPHER_TEXT_255_192 XPAR_AXI_GPIO_21_DEVICE_ID
    #define AES_CYPHER_TEXT_191_128 XPAR_AXI_GPIO_20_DEVICE_ID
    #define AES_CYPHER_TEXT_127_64  XPAR_AXI_GPIO_19_DEVICE_ID
    #define AES_CYPHER_TEXT_63_0    XPAR_AXI_GPIO_18_DEVICE_ID
```

Source: Author.

The *gpio_mgmt.c* implements the functions to configure ports and set or read its data. *gpio_mgmt* files are attached to this document. AES-CTR parameters are created in *main.c* with the test vectors values used in the standard NIST (2001b) (Figure 62).

Figure 62. *main.c* fragment with test vectors.

```
#ifdef AES_CTR_128_VECTORS
	unsigned int key[8] = {0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x2b7e1516, 0x28aed2a6, 0xabf71588, 0x09cf4f3c};
	int key_size = 128;
#endif

#ifdef AES_CTR_192_VECTORS
	unsigned int key[8] = {0x00000000, 0x00000000, 0x8e73b0f7, 0xda0e6452, 0xc810f32b, 0x809079e5, 0x62f8ead2, 0x522c6b7b};
	int key_size = 192;
#endif

#ifdef AES_CTR_256_VECTORS
	unsigned int key[8] = {0x603deb10, 0x15ca71be, 0x2b73aef0, 0x857d7781, 0x1f352c07, 0x3b6108d7, 0x2d9810a3, 0x0914dff4};
	int key_size = 256;
#endif

	unsigned int ptext[16] = {0x6bc1bee2, 0x2e409f96, 0xe93d7e11, 0x7393172a, 0xae2d8a57, 0x1e03ac9c, 0x9eb76fac, 0x45af8e51, 0x30c81c46,
	                          0xa35ce411, 0xe5fbc119, 0x1a0a52ef, 0xf69f2445, 0xdf4f9b17, 0xad2b417b, 0xe66c3710};

	unsigned int iv[4] = {0xf0f1f2f3, 0xf4f5f6f7, 0xf8f9fafb, 0xfcfdfefe};

	unsigned int blk_cmpnt_fixed[4] = {0x00000000, 0x00000000, 0x00000000, 0x00000001};

	unsigned int ctext[16];
```

Source: Author.

The Figure 63 shows a fragment of the process that controls AES-CTR.

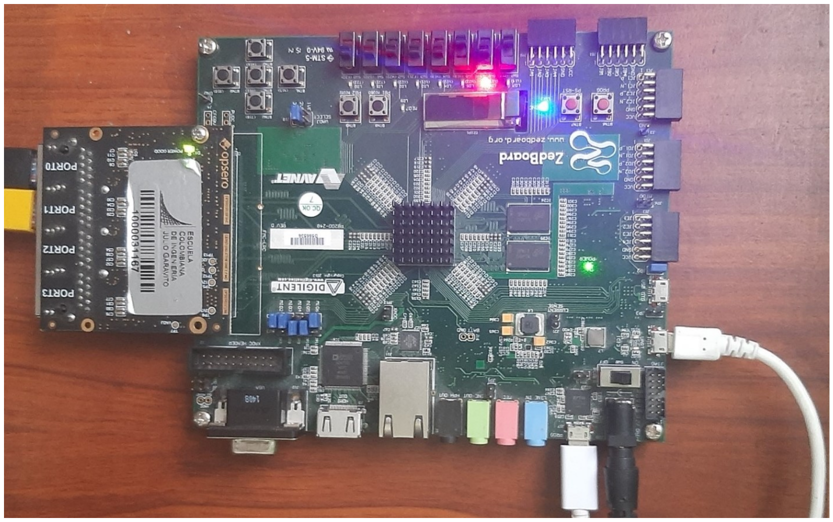
Figure 63. *main.c* fragment with test vectors.

```
reset_aes ();
set_plainText(ptext);
set_key(key);
set_iv(iv);
set_blk_cmpnt_fixed(blk_cmpnt_fixed);

xil_printf("\r\nPLAIN TEXT AES-CTR (test vector): \r\n");
print_arrays (ptext,16);

xil_printf("\r\nKEY AES-CTR %d (test vector): \r\n", key_size);
print_arrays (key,8);

xil_printf("\r\nINIT. VECTOR AES-CTR (test vector): \r\n");
print_arrays (iv,4);

xil_printf("\r\nStarting AES-CTR...\r\n");

start_aes ();

while (is_aes_ready ()); //1 busy - 0 ready

stop_aes();

xil_printf("\r\nAES-CTR ready!\r\n");
read_aes_cyphered (ctext);

xil_printf("\r\nCIPHER TEXT AES-CTR:\r\n");
print_arrays (ctext,16);
```

Source: Author.

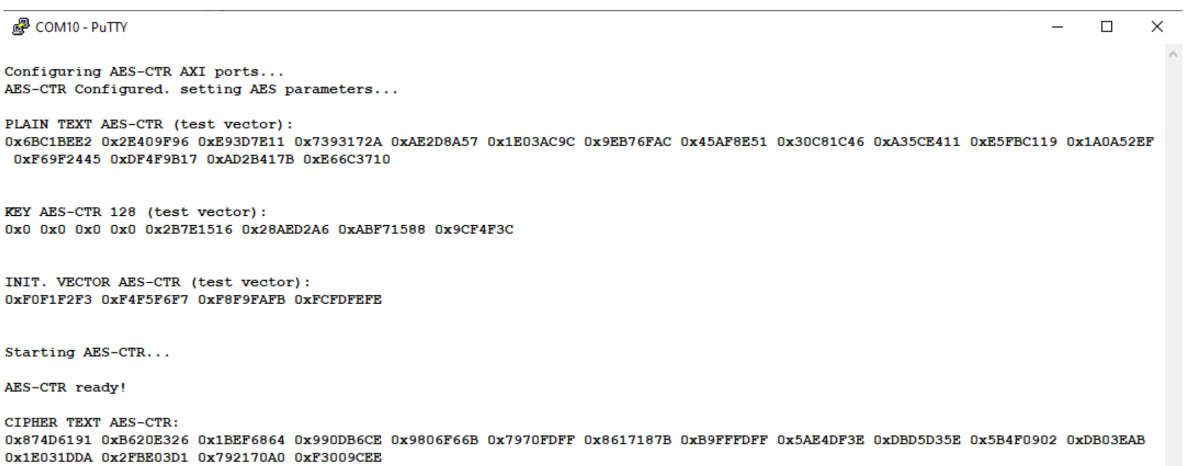
After building Vitis application, the process is then programmed onto the Zedboard (Figure 64). To verify cipher process, data is sent serial through a COM port from the Zedboard at 115200 bps. This is presented in the Figure 65 with successful result as the data obtained is the same showed as a test vector in standard NIST-FIPS197.

Figure 64. *Zedboard* programmed.



Source: Author.

Figure 65. AES-CTR-128 result.



Source: Author.

As mentioned earlier, despite the AES-CTR IPs support all key lengths, this work presents FPGA implementation results only for AES-CTR with key size of 128. Key sizes of 192 and 256 are tested behaviorally and at post-synthesis only. These longer keys are not taken for consideration as further timing analysis must be realized to constraint properly for those cases.

3.1.3.5 AES IP Cores Comparative

Table 17. Slice utilization for AES IP Cores.

Device	Zynq 7000					Kintex 7
AES Type	Combinational (Util. %)		Sequential (Util. %)		CTR (Util. %)	CTR (Util. %)
	cipher	inverse cipher	cipher	inverse cipher		
Slice	19.11	25.95	2.73	7.26	17.11	4.47
LUT as Logic	17.44	23.02	2.52	6.41	15.37	3.98
LUT as Memory	0	0	0	0	0	0
Slice Registers	0	0	0.25	0.39	1.01	0.26
Block RAM	0	0	0	1.43	0	0

Table 18. Timing for AES IP Cores.

Device	Zynq 7000					Kintex 7
AES Type	Combinational		Sequential		CTR	CTR
	cipher	inverse cipher	cipher	inverse cipher		
Max. Freq (MHz)	-	-	155	93.65	155.327	237.37
Throughput (Gbps)	3.02	1.55	1.8	1.09	7.22	11.11

The data for the AES-CTR timing and utilization within the FPGA are presented in the Table 19 along with implementation of other authors that use Kintex and SoC FPGA.

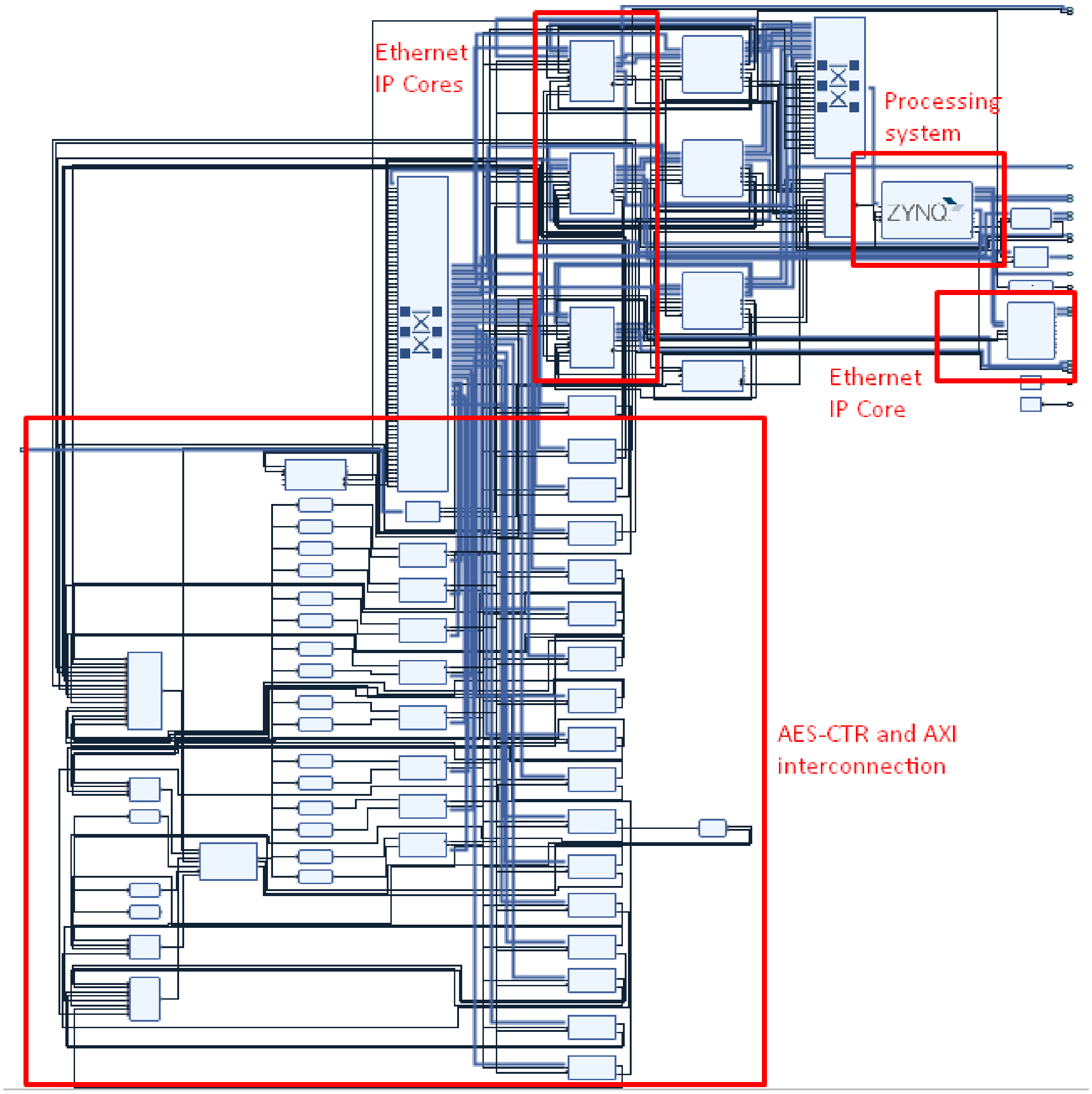
Table 19. Comparison of AES-CTR implementation.

Reference	Device	Encrypt.		Utilization			Tp	Max
		Mode	Blocks	Slice Register	Slice LUT	Slices	(Gbps)	Freq (MHz)
Daoud, Hussein, and Rafla (2019)	XC7Z020-1CLG484C	AES	-	830	1417	431	1,29	192
This work	XC7Z020 CLG484-1	AES	-	269 (0,25%)	1314 (2,47%)	363 (2,73%)	1,8	155,06
Visconti, Capoccia, Venere, Velázquez, and de Fazio (2020)	XCZU9EG-2FFVB1156E	AES	-	0,71%	4,76%	-	28	220
Chen, Hu, and Li (2019)	XC7K325 TFFG676-2l	AES	-	8311	19312	-	17,8	139
Silitonga et al. (2019)	Zynq7000 Zedboard	AES-CTR	4	6%	46%	-	538,38	-
This work	XC7Z020 CLG484-1	AES-CTR	4	1076 (1,01%)	8178 (15,37%)	2275 (17,11%)	7,22	155.33
Sikka, Asati, and Shekhar (2020)	XC7K70T-FBG676	AES-CTR	1	449	585	-	38,05	297,3
This work	XC7K325 TFFG676-1	AES-CTR	4	1076 (0,26%)	8116 (3,98%)	2276 (4,47%)	11,11	237.37

3.2 AES and PRP converged results

As PRP relies on Institute of Electrical and Electronics Engineers (IEEE)-802.3 data link protocol, 4 Ethernet IP are added to the block design described previously, particularly the AXI 1G2.5G Ethernet Subsystem. The AXI connection process is heavily automated by Vivado. Other ports are connected according to baseline designs. considerations as physical constraints and ports configuration are based each on hardware specification. The Figure 66 shows the block diagram with all elements.

Figure 66. AES-CTR, Ethernet and processing system block diagram.



Source: Author.

There are three clocks. Two asynchronous primary clock generated from FPGA processing system at 200MHz and 125MHz for processor and Ethernet blocks; and a third synchronous generated clock for AES-CTR IP of 50 MHz. Implementation utilization reports are in the Table 20. Detailed reports can be found in appendixes and attached project.

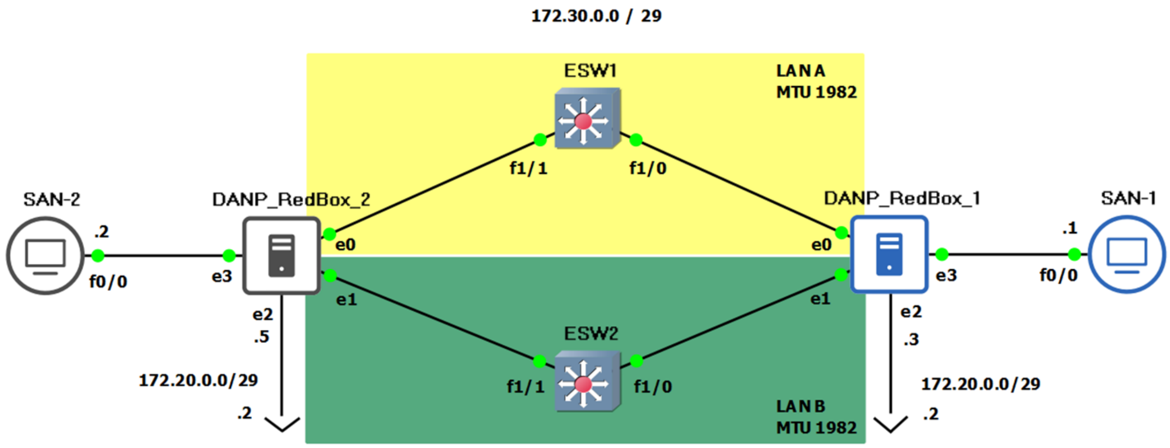
Table 20. Comparative of post-synthesis utilization.

Device	**Site type**	**Used**	**Available**	**Utilization %**
Zynq7000	Slice LUTs	35381	53200	66.51
	LUT as Logic	32344	53200	60.80
	LUT as Memory	3037	17400	17.45
	Slice Registers (FF)	50141	106400	47.13
	Block RAM Tile	18	140	12.86
Kintex-7 XC7K325T	Slice LUTs	33251	203800	16.32
	LUT as Logic	30965	203800	15.2
	LUT as Memory	3028	64000	4.7
	Slice Registers (FF)	46825	407600	11.5
	Block RAM Tile	22	445	4.9

3.3 PRP results

Implementation of PRP shows the following results using the topology presented in the Figure 67 and Wireshark as the packet capture analyzer software. Three components are presented in this section: first, the frame flow communication results at logic layers with non-encrypted packets as these do not differentiate logically from encrypted ones, demonstrated later on this chapter; second, the resulting algorithm that governs the PRP process and its execution platform; and third, redundancy tests are exhibited.

Figure 67. PRP logic implementation.



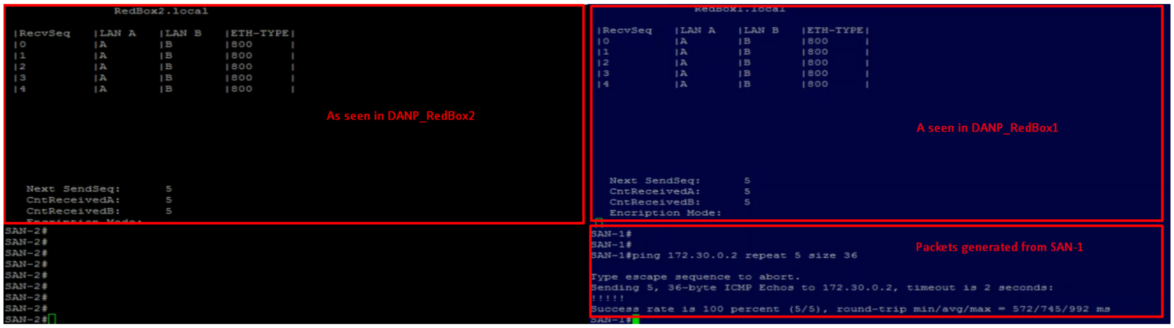
Source: Author.

Test of PRP consists in the transmission of Internet Control Message Protocol (ICMP) packets bidirectionally between SAN-1 and SAN-2 (Figure 67) using minimum and maximum packet sizes. Packets are captured in both LANs. These are shown in yellow for LAN-A and green for LAN-B in the Figure 67.

3.3.1 Packet flow

Communication flow starts at SAN-1 in the non-redundant network with the transmission of ICMP packets. At link level, this packet is received and duplicated at RedBox-1 whom send it through both interfaces attached to redundant LAN. At network level these packets are expected to be received at SAN-2. The Figure 68 shows the generation of these bidirectional packets using ICMP ping tool. This figure also shows RedBox-1 and RedBox-2 console to monitor redundancy operation.

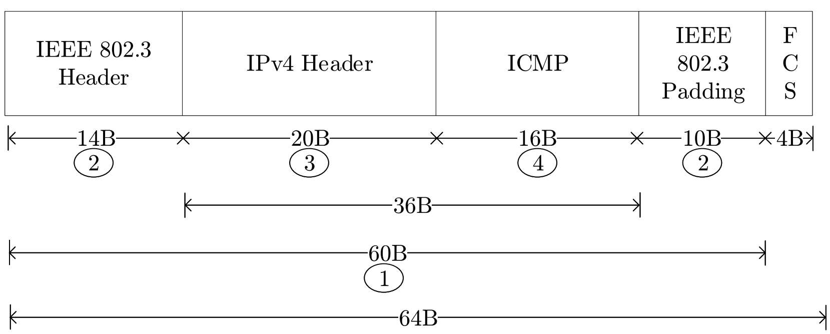
Figure 68. Packets in the non-redundant link with SAN-1



Source: Author.

The size of each transmitted packet is 36B at network level. These Bytes are then encapsulated to form a 64B frame packet which is the minimum size according to iieee802.3 specification. See Figure 69.

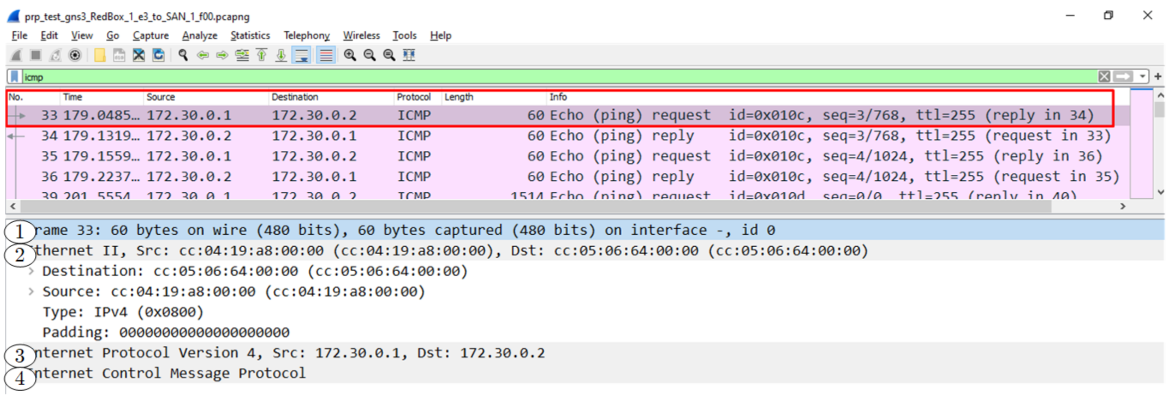
Figure 69. Packet in non-redundant link with SAN-1.



Source: Author.

A packet capture of these packets is presented in the Figure 70. Cyclic Redundancy Check (CRC) is hardware offloaded thus not present in Wireshark.

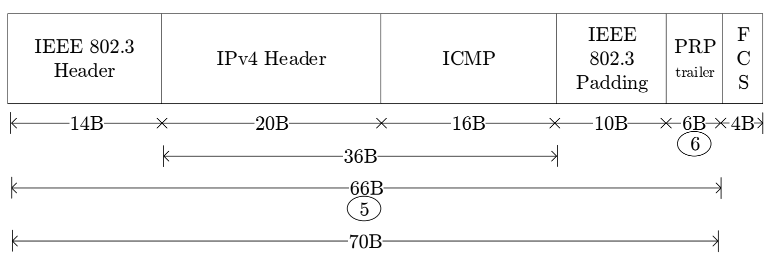
Figure 70. Packet in non-redundant link attached to SAN-1 .



Source: Author.

When received at RedBox-1 its PRP algorithm process (IEC62439-1, 2013) duplicates the packet, appends LANs PRP trailers accordingly and -try to- transmits them on LAN-A and LAN-B nearly at the same time. When transmitted, the next sequence number gets updated and printed on DANP console (Figure 68). Packet structure on redundant network is exposed in the Figure 71

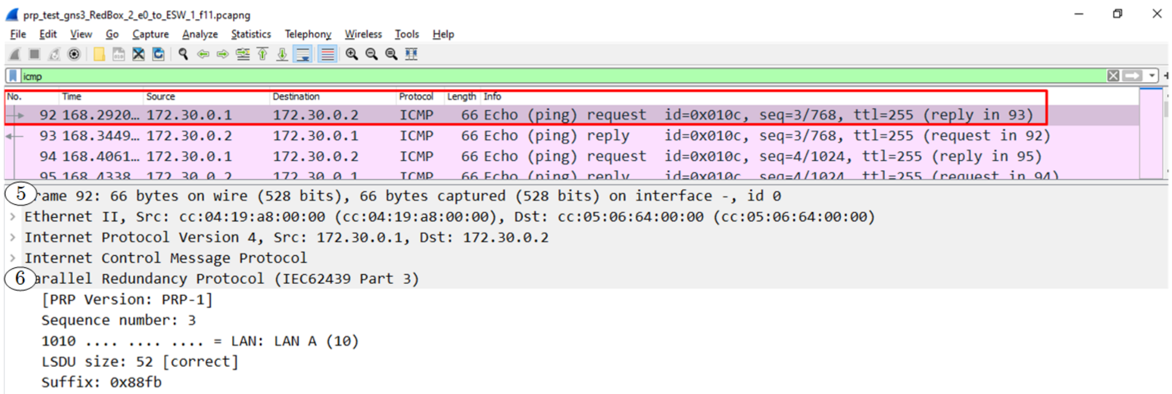
Figure 71. Packet format in redundant LANs.



Source: Author.

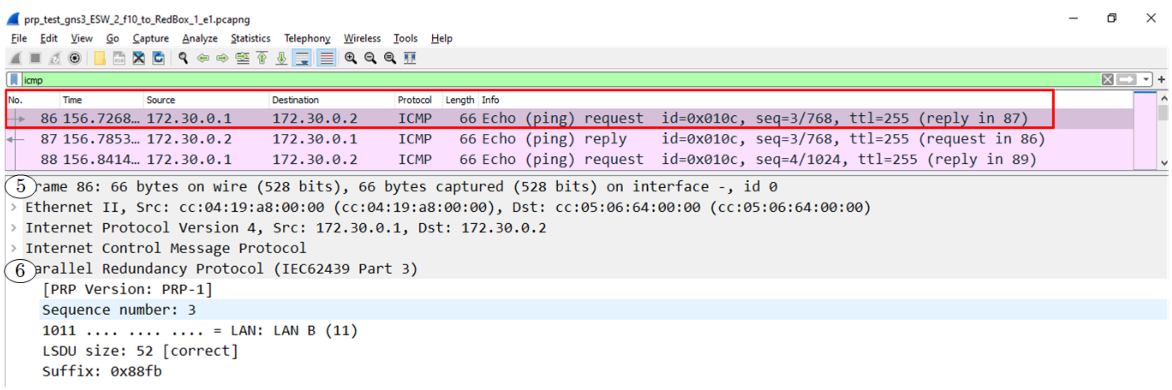
Packet captures of these PRP packets are presented in the Figure 72 and Figure 73.

Figure 72. Packet in redundant LAN-A.



Source: Author.

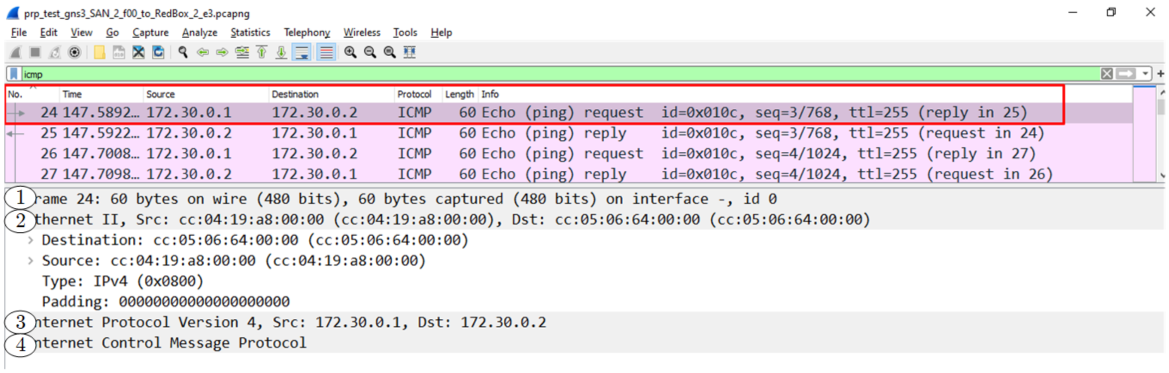
Figure 73. Packet in redundant LAN-B.



Source: Author.

At RedBox-2, the PRP process awaits for the first correctly PRP received packet from either redundant LAN to start the duplicate handling algorithm (IEC62439-1, 2013). This states that the first received packet must be transmitted immediately to its attached non-redundant network after removing the PRP trailer and minimum-required redundant status is printed on DANP console (Figure 68). The Figure 74 exhibits the packet transmitted from RedBox-2 to SAN-2.

Figure 74. Packet in non-redundant link with SAN-2.



Source: Author.

After received at SAN-2, an ICMP echo-reply packet is automatically generated and transmitted back to SAN-1 at network level. The flow described above is then mirrored and bidirectional communication verified as seen in the Figure 74.

3.3.1.1 maximum packet size considerations

The maximum frame size allowed for transmission from a node connected to a non-redundant network is constrained by the Maximum Transmission Unit (MTU) configured on redundant LANs due to the six bytes overhead added by the PRP trailer and DANP behavior as a link layer device without fragment capabilities. According to 802.3, maximum frame size is 2000B IEEE802.3 (2015), thus, maximum MTU permitted is 1982B, which is implemented here on the redundant network (figure) and should be implemented on related real implementations. Hence, maximum allowed MTU on non-redundant links is 1976. Packet flow is the same as described previously for the minimum frame size.

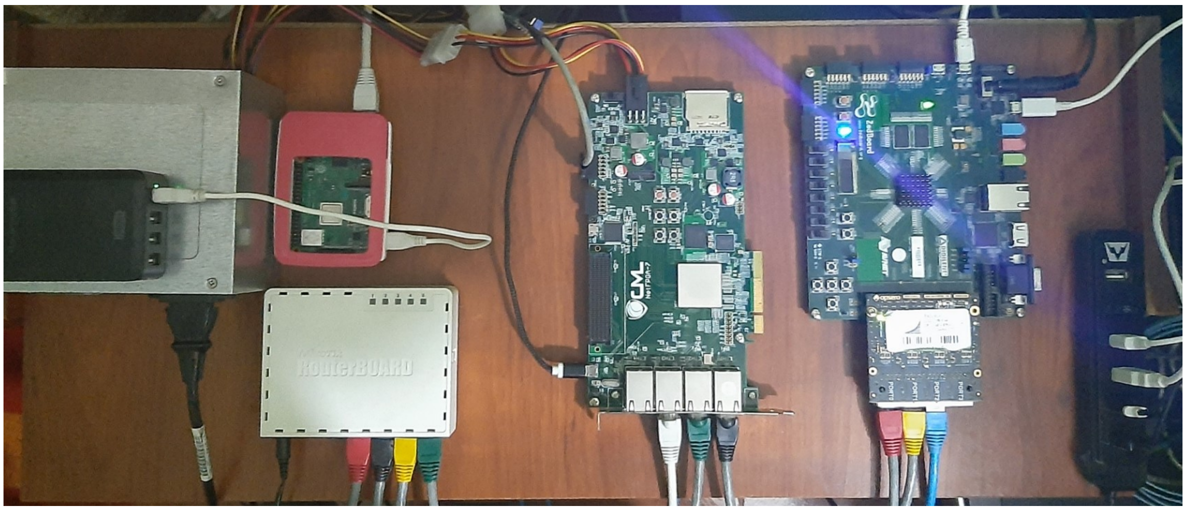
3.3.2 PRP algorithm

As shown in the PRP algorithm features included are the duplicate generation on both LANs with its trailed verified in IEC62439-3 (2016) ; also, at receiver the discarding algorithm selects the first received frame, validates the PRP trailer and passes it to the non-redundant interface. Source code can be found in appendix and attached files.

3.4 Encrypted PRP frame

The Figure 75 present devices and connections used to test the entire system, PRP with AES-CTR and a 128 key length. Physical devices and system components are the DANP-RedBox-1, DANP-RedBox-2, SAN-1, SAN-2 and an administrative switch to create two bridges for each redundant LAN.

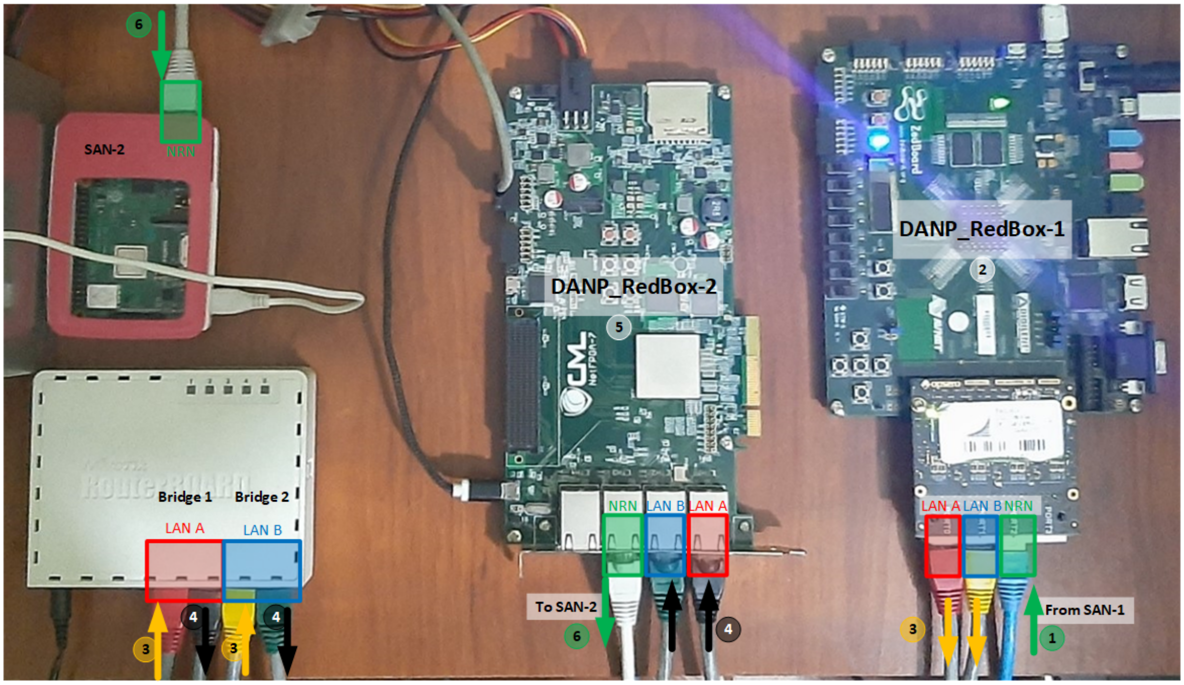
Figure 75. Physical components and connections for DANPs with AES-CTR.



Source: Author.

DANP-RedBoxs each have three interfaces. Colors in the Figure 76 represents the zones attached to them. Selected in green are the interfaces attached to the Non-Reduntant Network. Red and blue belong to reduntant LAN-A and LAN-B respectively. These LANs are implemented using the RouterOS device RB-9512n with two separate bridges. DANP-RedBox-1 implemented within the Zedboard receive plain data from SAN-1 (step 1 in green), then encrypts the payload of received packet, generates and appends the PRP trailer (step 2 in white) to finally send to redundant interfaces (step 3 in yellow). At DANP-RedBox-2, implemented using the NetFPGA, packets are received (step 4 in black). The PRP packet gets identified an the discarding algorithm is applied. Then, payload gets decrypted and framed to immediately send to SAN-2 (step 6 in green).

Figure 76. Communication flow of SANs and DANPs.

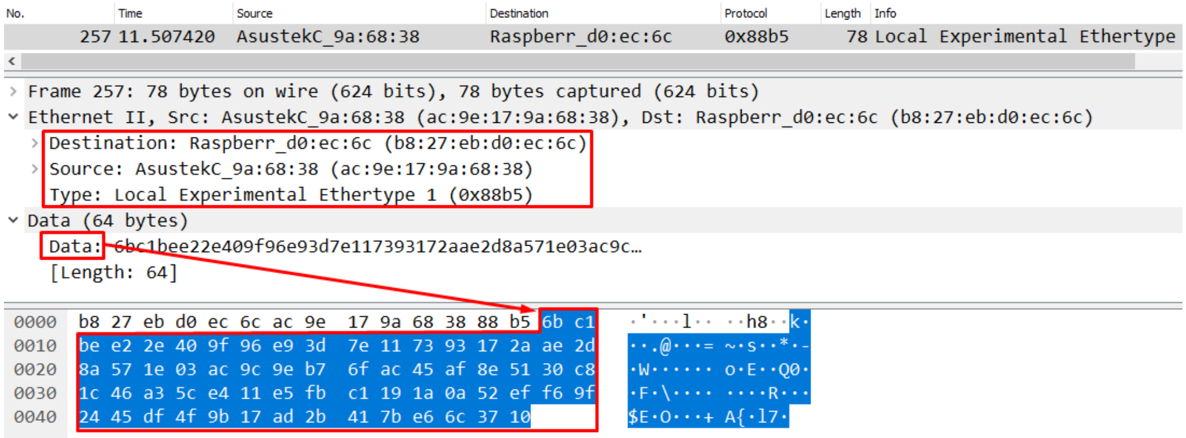


Source: Author.

SAN-1 is a virtual machine with a RouterOS operating system from which the plain text packet is sent using the command
/tool traffic-generator inject interface=ether1
data="B827EBD0EC6CAC9E179A683888b5
6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411e5fbc1191a0a52ef
f69f2445df4f9b17ad2b417be66c3710"

Plain data packet is presented in Figure 77.

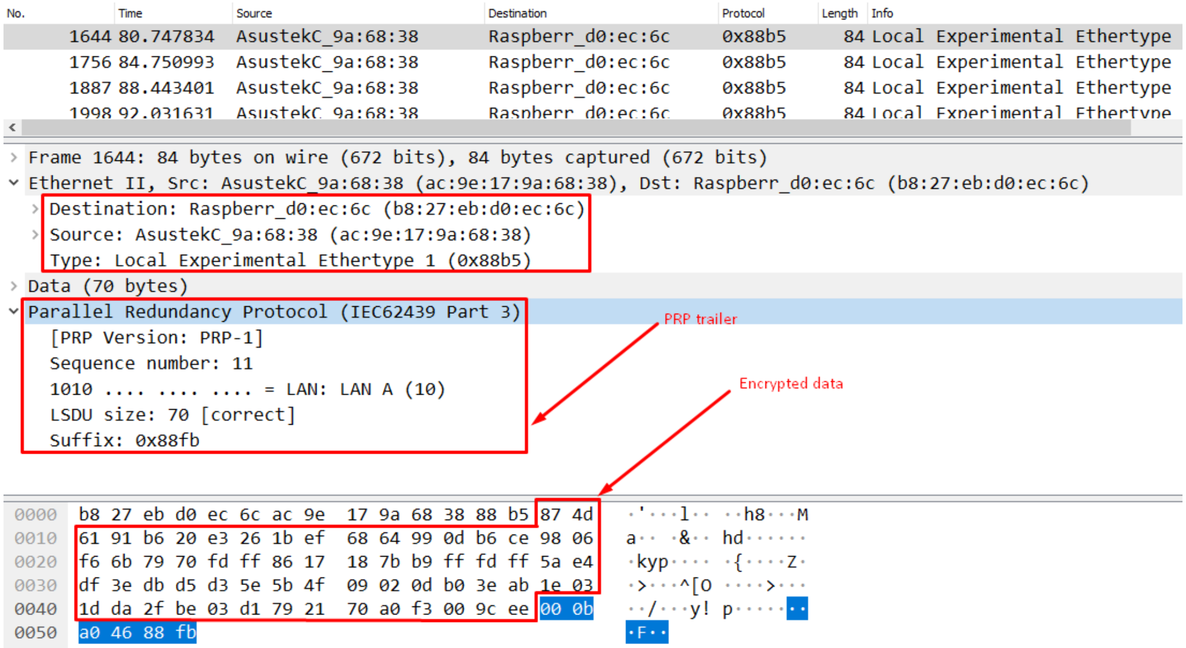
Figure 77. Packet sent by SAN-1 with plain data.



Source: Author.

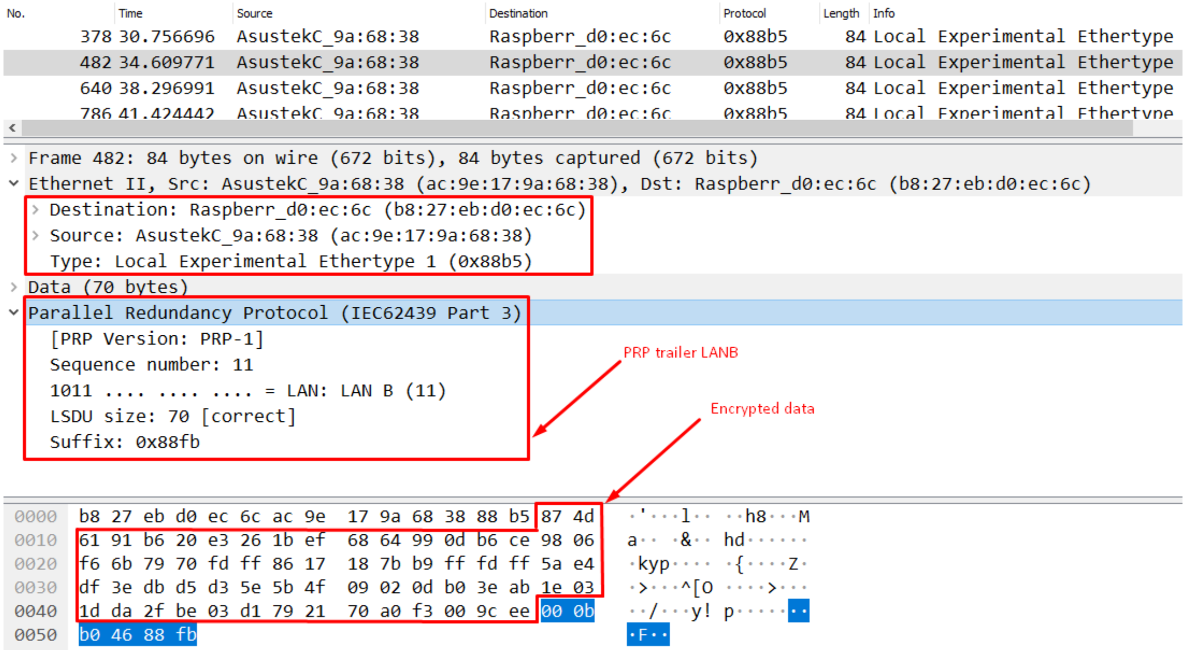
At the same time RouterOS device RB-9512n has its bridges running (redundant zone) and all packets gets sniffed. The Figures 78 and 79 present the encrypted packet payload with its respective PRP trailer appended.

Figure 78. Packet sent by DANP-RedBox-1 with cipher data and PRP trailer on LAN-A.



Source: Author.

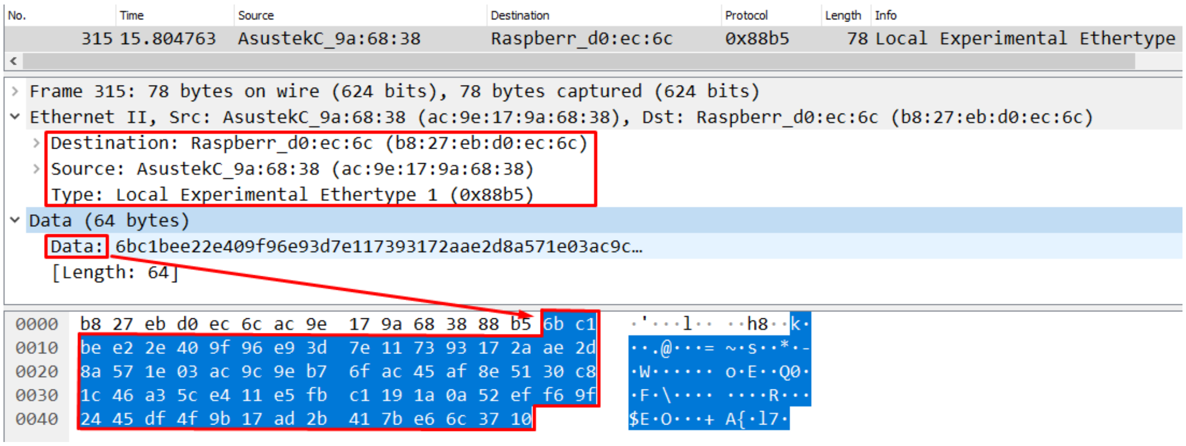
Figure 79. Packet sent by DANP-RedBox-1 with cipher data and PRP trailer on LAN-B.



Source: Author.

After received by DANP-RedBox-2, the packets are passed to the discarding PRP algorithm, decrypted and sent to SAN-2. SAN-2 is a Raspberry PI3 device with *tcpdump* installed to capture the incoming data in its interface. This is done by issuing the following command on SAN-2: *sudo tcpdump -w /tmp/testNRN.pcap*. See Figure 80.

Figure 80. Packet received on SAN-2 with original plain data.



Source: Author.

3.5 Analysis, Discussion of Results and Future Work

System on Chip (SoC) devices are deployed in different applications such as IoT and industrial networks for its adaptability when integrating software and hardware elements is required. For AES, a combinational-sequential implementation, particularly a non-pipelined as the presented in this work, is preferred in terms of used hardware space, allowing optimal cycle times that can be enhanced as higher clock frequency can be configured on devices. Besides, a pure-combinational AES or even a pipelined, exhausts almost all logic resources limiting IP integration as commonly occurs in practice. To enhance throughput minimizing utilization, and, to support high data rates more efficiently with packets that can be up to 2000B, the non-pipelined AES core gets grouped to encrypt bigger chunks of data using the CTR mode of operation, which is the base for other confidentiality authenticated modes like GCM, and also has the advantage to reduce AES vulnerabilities as each block have different input value due to its interconnected configuration.

Implemented AES-CTR IP shows a correct behavior for 128, 192 and 256 key sizes with four CTR blocks. The cipher process with 192 and 256 sizes require additional cycles that affect timing performance and hardware utilization. These cases should be analyzed beyond this work by improving Logic floor-planning. Also, the AES-CTR block can be resized to test utilization in FPGA for a faster and longer packet encryption. AES-CTR IP can be improved unifying the Key Expansion entity for all blocks, and also, as devices should perform cipher and decipher functions, integration of both processes are required but not implemented in this work.

Despite that the throughput for the IPs were measured by Vivado Synthesis, a complete physical system throughput between FPGAs devices is not tested here and is left for future implementation after IPs optimization. A problem encountered that limited a complete system throughput measurement was the configuration of the Ethernet Cores used. Soft-processors included on the FPGA are used here, have the disadvantage of constraint Logic components, thus, for Kintex 7 board, the PCI port should be included for future works for communication with external processors, and, for Zynq7000, an AXI communication interface needs to be studied further to include it into the IP implemented to enhance efficiency at the moment to interconnect the encryption/decryption logic to a processing system, avoiding the use of several default AXI interfaces to connect all IP inputs and outputs to the processing system.

Redundancy and encryption are meant to provide high availability of resources and data confidentiality. PRP by itself guarantees high availability only through two independent LANs. AES-CTR is used to provide data confidentiality. This adds an additional security layer at link for Local Area Network (LAN), thus further studies regarding this are recommended for broader networks at 2.5 and Internet Protocol (IP) layers generating new set of protocols based on one or combinantion of Multiprotocol Label Switching (MPLS), IP or IPSec protocols, as these, normally known as Wide Area Networks (WANs), commonly operate over public networks which has more threats than LANs. Future works about redundancy, not included here, but can be extended from this work, are the completion of PRP functions like secure multi-cast supervisory frame and interoperation with other link protocols as MACSec, Rapid Spanning tree protocol (STP) and High-availability Seamless Redundancy (HSR). The later, documented in the same standard as PRP for ring networks.

PRP adds 6 bytes to a link packet generating over-heading when transmitted on a redundant network. Maximum Ethernet protocol supported MTU value, if used, must be reduced in non-redundant network to 1976B. Packet encryption do not generate over-heading. Also, PRP trailer isn't encrypted, so in order to provide extra confidentiality by encrypting it, an Ethertype should be requested to IEEE authority for a receiver DANP-RedBox demultiplexing process. Besides, other frame packet formats should be proposed to add Hashes, initialization Vector or information for key exchange that grant, additionally to confidentiality and High Availability, authenticated packets as long as unnecessary excessive shrinking of payload are avoided. As PRP presented in this document is implemented entirely on software, hardware offload is also considered for future work, thus, increasing performance of the complete system taking advantage of the reduced utilization that this non-pipelined achieves, allowing flexible combination with different Logic elements.

Conclusions

To achieve the objective of this work, a widely variety of background concepts are required. These, among others, are: FPGA detailed features, VHDL, Xilinx's Vivado and Vitis usage, communication interfaces as AXI4 and Ethernet at physical and data-link layers, C programming and networking. During implementation, concepts are acquired for AES design, which is based on combinational or sequential (Pipelined, Non-pipelined) methodologies at FPGA Programable Logic (PL).

On the other hand, PRP concepts, based in IEC62439 part 3, are accomplished for framing and the discarding algorithm. Due to complexity and developing time restrictions, other relevant concepts are left aside in this work, including those related to PRP supervisory frames and logging data, evaluation of redundancy protocol performance with the Unit Under Test (UUT) method as described in IEC62439 part 1 and IEC/TR61158 (all parts) and section 2.5. UUT is left for future work as described in section 3.5

The implementation of AES IP Cores show the correct behavior at simulation for 128 bit-length key using the combinational methodology, and the same occurs for keys of 128, 192 and 256 bit-length by applying the sequential approach, which is based on an iterative non-pipelined design. CTR mode of operation also shows the expected behavioral results for those keys as it is based on sequential AES. Although correctness of simulation, at physical implementation only AES-128 and AES-128-CTR present the expected value according to test vectors. This is caused by the extended Key-Expansion required for 192 and 256 bit-length keys and the lack of floor-planning for this design. Also, AES IP Cores can be extensively analyzed using Xilinx Vivado before passing it bit stream onto the FPGA.

The PRP evaluation of the frame format is accomplished by transmitting from the RedBox device to the redundant network that includes a packet analyzer, and, for this implementation, AES-CTR within PRP frame, does not present Ethernet header modifications. Considerations observed regarding this implementation are for the maximum frame size allowed when a packet that is received from the non-redundant is sent to the redundant one as the CTR trailer must be appended to Ethernet payload. Other frames formats are not implemented in this work but would be considered for future works to manage VLANs and AES extensions.

DANP RedBoxs includes a processor and Programmable Logic, both included in each FPGA. For zynq7000 SoC, the dual core ARM Cortex A9 processor is used for PRP process. Kintex 7 Microblaze softprocessor also performs PRP related operations, but no comparison is presented here as just the frame is tested. In other words, PRP is implemented at software and no hardware offload is made.

Physical tests for GigaE environments are not performed here due to the detailed configuration required that goes beyond the scope of this work, but test are made on an Ethernet environment.

In this context, implementation and integration of AES-CTR are accomplished by means of the FPGAs described earlier and tests show accurately results which are based mainly on a comparative of real packets captured with international standard IEC62439-3 (2016), NIST-FIPS197 (2001) and NIST-SP-800-38A (2001).

References

Bodungen, C., Singer, B., Shbeeb, A., Wilhoit, K., & Hilt, S. (2016). *Hacking exposed industrial control systems: Ics and scada security secrets & solutions.* McGraw-Hill Education.

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018, oct). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1–12. doi: 10.1016/j.compind.2018.04.015

Buse, D. P., & Wu, Q. (2006). *Ip network-based multi-agent systems for industrial automation: Information management, condition monitoring and control of power systems.* Springer.

Chen, S., Hu, W., & Li, Z. (2019, may). High performance data encryption with AES implementation on FPGA. In *2019 IEEE 5th intl conference on big data security on cloud (BigDataSecurity), IEEE intl conference on high performance and smart computing, (HPSC) and IEEE intl conference on intelligent data and security (IDS).* IEEE. doi: 10.1109/bigdatasecurity-hpsc-ids.2019.00036

Chhabra, S., & Lata, K. (2018, dec). Hardware software co-simulation of obfuscated 128-bit AES algorithm for image processing applications. In *2018 IEEE international symposium on smart electronic systems (iSES) (formerly iNiS).* IEEE. doi: 10.1109/ises.2018.00049

Conpes-3854 consejo política nacional de seguridad digital. (2016). Retrieved from `https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf`

Daemen, J., & Rijmen, V. (2002). *The design of rijndael: Aes - the advanced encryption standard (information security and cryptography).* Springer.

Daoud, L., Hussein, F., & Rafla, N. (2019, 03). Optimization of advanced encryption standard (aes) using vivado high level synthesis (hls)..

Digilent. (2016, April). Netfpga-1g-cml™ board reference manual [Computer software manual].

Dobbertin, H., Rijmen, V., & Sowa, A. (Eds.). (2005). *Advanced encryption standard - aes: 4th international conference, aes 2004, bonn, germany, may 10-12, 2004, revised selected and invited papers (lecture notes in computer science).* Springer.

Farzaneh Abed, S. L., Christian Forler. (2016). General classification of the authenticated encryption schemes for the caesar competition. *Computer Science Review*, *22*, 13-26.

IEC62439-1. (2013). *Industrial communication networks – high availability automation networks – part 1: General concepts and calculation methods.*

IEC62439-3. (2016). *Industrial communication networks - high availability automation networks - part 3: Parallel redundancy protocol (prp) and high-availability seamless redundancy (hsr).*

IEC/TS62351-1. (2007). *Power systems management and associated information exchange –*

data and communications security part 1: Communication network and system security – introduction to security issues.

IEC/TS62443-1-1. (2009). *Industrial communication networks – network and system security – part 1-1: Terminology, concepts and models.*

IEEE802.3. (2015). *Ieee standard for ethernet. ieee std 802.3-2015 (revision of ieee std 802.3-2012).*

International-Cryptologic-Research-Community. (2017). *Caesar submissions* (Tech. Rep.).

Knapp, E. D., & Langill, J. T. (2011). *Industrial network security: Securing critical infrastructure networks for smart grid, scada, and other industrial control systems*. Syngress.

Koscielny, C., Kurkowski, M., & Srebrny, M. (2013). *Modern cryptography primer: Theoretical foundations and practical applications*. Springer.

NIST. (2001a, November). *Fips197.* Retrieved from `https://csrc.nist.gov/publications/detail/fips/197/final`

NIST. (2001b, December). *Sp-800-38a* (No. SP-800-38A). Retrieved from `https://csrc.nist.gov/publications/detail/sp/800-38a/final`

Popovic, M., Mohiuddin, M., & Tomozei, D.-C. (2015). iprp: Parallel redundancy protocol for ip networks. *IEEE*. doi: 10.1109/WFCS.2015.7160549

Rentschler, M., & Heine, H. (2013). The parallel redundancy protocol for industrial ip networks. *IEEE*. doi: 10.1109/ICIT.2013.6505877

Rodriguez-Henriquez, F., Saqib, N., Pérez, A. D., & Koc, C. K. (2006). *Cryptographic algorithms on reconfigurable hardware (signals and communication technology)*. Springer.

Rost, P., Breitbach, M., Roreger, H., Erman, B., Mannweiler, C., Miller, R., & Viering, I. (2018, oct). Customized industrial networks: Network slicing trial at hamburg seaport. *IEEE Wireless Communications*, *25*(5), 48–55. doi: 10.1109/mwc.2018.1800045

Rubio, J. E., Manulis, M., Alcaraz, C., & Lopez, J. (2019). Enhancing security and dependability of industrial networks with opinion dynamics. In *Lecture notes in computer science* (pp. 263–280). Springer International Publishing. doi: 10.1007/978-3-030-29962-0_13

Sikka, P., Asati, A. R., & Shekhar, C. (2020, July). High-throughput field-programable gate array implementation of the advanced encryption standard algorithm for automotive security applications. *Journal of Ambient Intelligence and Humanized Computing*. Retrieved from `https://doi.org/10.1007/s12652-020-02403-2` doi: 10.1007/s12652-020-02403-2

Silitonga, A., Jiang, Z., Khan, N., & Becker, J. (2019, oct). Reconfigurable module of multimode AES cryptographic algorithms for AP SoCs. In *2019 IEEE nordic circuits and systems conference (NORCAS): NORCHIP and international symposium of system-on-chip (SoC)*. IEEE. doi: 10.1109/norchip.2019.8906923

Soltani, A., & Sharifian, S. (2015, oct). An ultra-high throughput and fully pipelined implementation of AES algorithm on FPGA. *Microprocessors and Microsystems*, *39*(7), 480–493. doi: 10.1016/j.micpro.2015.07.005

SP800131A. (2015, November). *Nist special publication 800 131a revision 1. transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths.* Retrieved from `http://dx.doi.org/10.6028/NIST.SP.800-131Ar1`

SP80057Part1. (2016, November). *Recommendation for key management.* Retrieved from `http://dx.doi.org/10.6028/NIST.SP.800-131Ar1`

Stallings, W. (2013). *Cryptography and network security: Principles and practice.* Pearson.

Stefanka, M. (2016). The parallel redundancy protocol over wide area networks. *ABB Inc.*. doi: 10.4236/sgre.2016.74011

Urbina, M., Moreira, N., Rodriguez, M., Acosta, T., Lázaro, J., & Astarloa, A. (2018, feb). Secure protocol and IP core for configuration of networking hardware IPs in the smart grid. *Energies*, *11*(3), 510. doi: 10.3390/en11030510

Vaudenay, S. (2006). *A classical introduction to cryptography.* Springer US.

Visconti, P., Capoccia, S., Venere, E., Velázquez, R., & de Fazio, R. (2020, oct). 10 clock-periods pipelined implementation of AES-128 encryption-decryption algorithm up to 28 gbit/s real throughput by xilinx zynq UltraScale+ MPSoC ZCU102 platform. *Electronics*, *9*(10), 1665. doi: 10.3390/electronics9101665

Xilinx. (2014, January). Zynq™ evaluation and development hardware user's guide [Computer software manual].

Xilinx. (2019). *Vivado timing - where can i find the fmax in the timing report?* (Tech. Rep.). Retrieved from `https://www.xilinx.com/support/answers/57304.html`

Acronyms

AES Advanced Encryption Standard. 1–8, 10–15, 17, 18, 22, 26–30, 37–43, 46–76, 82, 83, 88–91, 101–133

AXI Advanced eXtensible Interface. 48, 68, 70, 75, 89

plus5minus3

BRP Beacon Redundancy Protocol. 32

plus5minus3

CAESAR Competition for Authenticated Encryption: Security, Applicability,and Robustnes. 30

CBC Chiper Block Chaining mode. 29, 30

CCM Counter with Cipher Block Chaining-Message Authentication Code. 29

CCOC Comando Conjunto Cibernético. 10, 20, 21

CFB Chiper Feedback mode. 29, 30

CMAC cipher-based message authentication code. 29

ColCERT Colombian Computer Emergency Readiness Team. 10, 20, 21

COTS Commercial off-the-Shelf. 19

CRC Cyclic Redundancy Check. 79

CRP Cross-network Redundancy Protocol. 32

CTR Counter mode. 4–8, 10–15, 17, 18, 29, 30, 37, 41–43, 46, 48–51, 62–74, 76, 82, 83, 88–91, 120–133

plus5minus3

DANP Dual Attached Node using PRP. 10, 13, 17, 33–35, 51, 80–84, 86, 87, 89, 90

DRP Distributed Redundancy Protocol. 32

plus5minus3

ECB Electronic CodeBook mode. 29, 30

plus5minus3

FCS Frame Check Sequence. 34

FF1 format-preserving, Feistel-based encryption. 29

FPGA Field Programable Gate Array. 4, 16, 17, 37, 51, 72, 73, 76, 88–91

plus5minus3

GCM Galois/Counter Mode. 29, 30, 88

GigaE Gigabit Ethernet. 37, 90

plus5minus3

HSR High-availability Seamless Redundancy. 32, 89

plus5minus3

IACS Industrial Automation and Control Systems. 8, 19–22

ICMP Internet Control Message Protocol. 78, 82

IDS Intrusion Detection Systems. 16

IEC International Electrotechnical Commission. 4, 22, 27, 32, 100

IEEE Institute of Electrical and Electronics Engineers. 31, 75, 89

IIoT Industrial Internet of Things. 16

IoT Internet of Things. 16, 88

IP Intellectual Property. 4, 6, 8, 11, 12, 17, 42, 51–54, 56, 59, 60, 62–65, 68, 69, 72, 73, 75, 76, 88–90

IP Internet Protocol. 31, 89

IT Information Technology. 16

plus5minus3

KW Key Wrap. 29

KWP Key Wrap Padding. 29

plus5minus3

LAN Local Area Network. 13, 33, 35, 78, 80–83, 86, 87, 89, 96

LanId LAN Identifier. 35

LLC Logical Link Control. 33

LRE Link Redundancy Entity. 11, 17, 33, 34, 44, 45, 47, 51

LSb Least Significant bit. 63

LSDU Link Service Data Unit. 11, 33, 34, 37, 43, 46, 47, 49

plus5minus3

MRP Media Redundancy Protocol. 32

MSb Most Significant bit. 62

MTU Maximum Transmission Unit. 82, 89

plus5minus3

NIST National Institue of Standards and Technology. 26–28, 99

plus5minus3

OFB Output Feedback mode. 29, 30

OOC Out of Context. 51, 54, 60, 65

plus5minus3

PL Programable Logic. 17, 37, 48, 50, 90

PRP Parallel Redundancy Protocol. 1–6, 8, 10, 11, 13, 17, 18, 22, 23, 32–35, 37, 38, 43–51, 75, 77, 78, 80–83, 85–87, 89, 90

PS Processing System. 11, 18, 37, 43, 45, 48, 50

plus5minus3

RCT Redundancy Control Trailer. 8, 10, 34, 35

RedBox Redundancy Box. 13, 17, 33, 34, 51, 78, 80–83, 86, 87, 89, 90

RSTP Rapid Spanning tree protocol. 31

plus5minus3

SAN Single Attached Node. 13, 33, 34, 78–85, 87, 88

SeqNr Sequence Number. 35

SoC System on Chip. 4, 16, 17, 35, 37, 52, 63, 73, 88

STP Spanning tree protocol. 31, 89

plus5minus3

UUT Unit Under Test. 11, 49, 50, 90

plus5minus3

VHDL Very High Speed Integrated Circuit Hardware Description Language. 4, 7, 51, 56, 62, 63, 90, 101

VLAN Virtual LAN. 11, 43, 46, 47

VPN Virtual Private Network. 16

plus5minus3

WAN Wide Area Network. 89

WNS Worst Negative Slack. 59, 64

plus5minus3

XDC Xilinx Design Constraints. 59

XTS XEX Tweakable Block Cipher with Ciphertext Stealing. 29

Appendices

A.1. Standards and guidelines for security on industrial networks

Table 21. Standards and guidelines.

Standard	**Description**	**Region**
Conpes-3701	Consejo Nacional de Política Económica y Social: Lineamientos de política para Ciberseguridad y Ciberdefensa	Colombia
Conpes-3854	Consejo Nacional de Política Económica y Social: Política nacional de seguridad digital	Colombia
HSPD-7	Homeland Security Presidential DirectiveSeven. Attempts to distinguish the critical versus noncritical systems. Does not include specific security recommendations	U.S
NIST-800	Best practices and information of general interest to information security	U.S
	Part: SP 800-53. Recommended Security Controls for Federal Information Systems defines many aspects of information security procedures and technologies. Applicable to the protection of critical infrastructures	U.S
	Part: SP 800-82. Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. Details control system architectures, protocols, vulnerabilities, and security controls	U.S
NERC CIP	North American Electric Reliability Corporation - Critical Infrastructure Protection. Identifies security measures for protecting critical infrastructure with the goal of ensuring the reliability of the bulk power system	U.S
NRC	Nuclear Regulatory Commission. Responsible for ensuring the safe use of radioactive materials for beneficial civilian (nonmilitary) purposes by licensed nuclear facilities	U.S
FISMA	**Part:** 10 CFR 73.54. Title 10 Code of Federal Regulations (CFR), section 73.54	U.S

Table 21. (Continued) Standards and guidelines.

Standard	**Description**	**Region**
	Part: RG 5.71. Office of Nuclear Regulatory Research's Regulatory Guide 5.71 . Provides recommendations to nuclear agencies or "licensees" in how to secure their facilities against cyber attack	U.S
CFATS	Chemical Facility Anti-Terrorism Standards. set of risk-based performance guidelines published by the Department of Homeland Security	U.S
ISA-99	Industrial control security standard created by the International Society of Automation (ISA) to protect SCADA and process control systems	Global
ISO-27002	Security recommendations published by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). "Information technology - Security techniques- Code of practice for information security management," and is not specific to industrial network security	Global
IEC/TS 62351	International Electrotechnical Commission. Power systems management and associated information exchange - Data and communications security	Global
IEC 62439	International Electrotechnical Commission. Industrial communication networks - high availability automation networks	Global
IEC/TS 62443	International Electrotechnical Commission. Industrial communication networks - Network and system security	Global

A.2. VHDL AES entities

A.3. Combinational AES utilization report

Figure 81. Utilization combinational AES-128 report part 1.

```
Copyright 1986-2019 Xilinx, Inc. All Rights Reserved.
------------------------------------------------------------------------
------------------------------------------------------------------------
-
| Tool Version : Vivado v.2019.2 (win64) Build 2708876 Wed Nov  6
21:40:23 MST 2019
| Date         : Thu Nov 12 07:11:30 2020
| Host         : DESKTOP-GLRI1LS running 64-bit major release  (build
9200)
| Command      : report_utilization -file E:/OneDriveECI/prp-
aes/Entregable/figures/resultados/aes_comb_utilization_report.txt -name
utilization_1
| Design       : aes128c
| Device       : 7z020clg484-1
| Design State : Routed
------------------------------------------------------------------------
------------------------------------------------------------------------
-

Utilization Design Information

Table of Contents
-----------------
1. Slice Logic
1.1 Summary of Registers by Type
2. Slice Logic Distribution
3. Memory
4. DSP
5. IO and GT Specific
6. Clocking
7. Specific Feature
8. Primitives
9. Black Boxes
10. Instantiated Netlists

1. Slice Logic
--------------

+-------------------------+------+-------+-----------+-------+
|        Site Type        | Used | Fixed | Available | Util% |
+-------------------------+------+-------+-----------+-------+
| Slice LUTs              | 9280 |     0 |     53200 | 17.44 |
|   LUT as Logic          | 9280 |     0 |     53200 | 17.44 |
|   LUT as Memory         |    0 |     0 |     17400 |  0.00 |
| Slice Registers         |    0 |     0 |    106400 |  0.00 |
|   Register as Flip Flop |    0 |     0 |    106400 |  0.00 |
|   Register as Latch     |    0 |     0 |    106400 |  0.00 |
| F7 Muxes                | 2932 |     0 |     26600 | 11.02 |
| F8 Muxes                | 1426 |     0 |     13300 | 10.72 |
+-------------------------+------+-------+-----------+-------+


1.1 Summary of Registers by Type
--------------------------------
```

Figure 82. Utilization combinational AES-128 report part 2.

Total	Clock Enable	Synchronous	Asynchronous
0	_	-	-
0	_	-	Set
0	_	-	Reset
0	_	Set	-
0	_	Reset	-
0	Yes	-	-
0	Yes	-	Set
0	Yes	-	Reset
0	Yes	Set	-
0	Yes	Reset	-

2. Slice Logic Distribution

Site Type	Used	Fixed	Available	Util%
Slice	2541	0	13300	19.11
SLICEL	1964	0		
SLICEM	577	0		
LUT as Logic	9280	0	53200	17.44
using O5 output only	0			
using O6 output only	8525			
using O5 and O6	755			
LUT as Memory	0	0	17400	0.00
LUT as Distributed RAM	0	0		
LUT as Shift Register	0	0		
Slice Registers	0	0	106400	0.00
Register driven from within the Slice	0			
Register driven from outside the Slice	0			
Unique Control Sets	0		13300	0.00

Figure 83. Utilization combinational AES-128 report part 3.

+--+------+-------+-----------+-------+

* Note: Available Control Sets calculated as Slice Registers / 8, Review the Control Sets Report for more information regarding control sets.

3. Memory

Site Type	Used	Fixed	Available	Util%
Block RAM Tile	0	0	140	0.00
RAMB36/FIFO*	0	0	140	0.00
RAMB18	0	0	280	0.00

* Note: Each Block RAM Tile only has one FIFO logic available and therefore can accommodate only one FIFO36E1 or one FIFO18E1. However, if a FIFO18E1 occupies a Block RAM Tile, that tile can still accommodate a RAMB18E1

4. DSP

Site Type	Used	Fixed	Available	Util%
DSPs	0	0	220	0.00

5. IO and GT Specific

Site Type	Used	Fixed	Available	Util%
Bonded IOB	0	0	200	0.00
Bonded IPADs	0	0	2	0.00
Bonded IOPADs	0	0	130	0.00
PHY_CONTROL	0	0	4	0.00
PHASER_REF	0	0	4	0.00
OUT_FIFO	0	0	16	0.00
IN_FIFO	0	0	16	0.00
IDELAYCTRL	0	0	4	0.00
IBUFDS	0	0	192	0.00
PHASER_OUT/PHASER_OUT_PHY	0	0	16	0.00
PHASER_IN/PHASER_IN_PHY	0	0	16	0.00
IDELAYE2/IDELAYE2_FINEDELAY	0	0	200	0.00
ILOGIC	0	0	200	0.00
OLOGIC	0	0	200	0.00

Figure 84. Utilization combinational AES-128 report part 4.

```
6. Clocking
-----------

+------------+------+-------+-----------+-------+
|  Site Type | Used | Fixed | Available | Util% |
+------------+------+-------+-----------+-------+
| BUFGCTRL   |    0 |     0 |        32 |  0.00 |
| BUFIO      |    0 |     0 |        16 |  0.00 |
| MMCME2_ADV |    0 |     0 |         4 |  0.00 |
| PLLE2_ADV  |    0 |     0 |         4 |  0.00 |
| BUFMRCE    |    0 |     0 |         8 |  0.00 |
| BUFHCE     |    0 |     0 |        72 |  0.00 |
| BUFR       |    0 |     0 |        16 |  0.00 |
+------------+------+-------+-----------+-------+


7. Specific Feature
-------------------

+-------------+------+-------+-----------+-------+
|  Site Type  | Used | Fixed | Available | Util% |
+-------------+------+-------+-----------+-------+
| BSCANE2     |    0 |     0 |         4 |  0.00 |
| CAPTUREE2   |    0 |     0 |         1 |  0.00 |
| DNA_PORT    |    0 |     0 |         1 |  0.00 |
| EFUSE_USR   |    0 |     0 |         1 |  0.00 |
| FRAME_ECCE2 |    0 |     0 |         1 |  0.00 |
| ICAPE2      |    0 |     0 |         2 |  0.00 |
| STARTUPE2   |    0 |     0 |         1 |  0.00 |
| XADC        |    0 |     0 |         1 |  0.00 |
+-------------+------+-------+-----------+-------+


8. Primitives
-------------

+----------+------+---------------------+
| Ref Name | Used | Functional Category |
+----------+------+---------------------+
| LUT6     | 6912 |                 LUT |
| MUXF7    | 2932 |               MuxFx |
| MUXF8    | 1426 |               MuxFx |
| LUT2     | 1147 |                 LUT |
| LUT4     |  895 |                 LUT |
| LUT3     |  544 |                 LUT |
| LUT5     |  535 |                 LUT |
| LUT1     |    2 |                 LUT |
+----------+------+---------------------+


9. Black Boxes
--------------
```

Figure 85. Utilization combinational inverse AES-128 report part 1.

```
Copyright 1986-2019 Xilinx, Inc. All Rights Reserved.
------------------------------------------------------------------------
------------------------------------------------------------------------
----
| Tool Version : Vivado v.2019.2 (win64) Build 2708876 Wed Nov  6
21:40:23 MST 2019
| Date         : Thu Nov 12 07:13:05 2020
| Host         : DESKTOP-GLRI1LS running 64-bit major release  (build
9200)
| Command      : report_utilization -file E:/OneDriveECI/prp-
aes/Entregable/figures/resultados/aesDec_comb_utilization_report.txt -
name utilization_1
| Design       : aes_128_c_dec
| Device       : 7z020clg484-1
| Design State : Routed
------------------------------------------------------------------------
------------------------------------------------------------------------
----

Utilization Design Information

Table of Contents
-----------------
1. Slice Logic
1.1 Summary of Registers by Type
2. Slice Logic Distribution
3. Memory
4. DSP
5. IO and GT Specific
6. Clocking
7. Specific Feature
8. Primitives
9. Black Boxes
10. Instantiated Netlists

1. Slice Logic
--------------

+-------------------------+-------+-------+-----------+-------+
|        Site Type        |  Used | Fixed | Available | Util% |
+-------------------------+-------+-------+-----------+-------+
| Slice LUTs              | 12249 |     0 |     53200 | 23.02 |
|   LUT as Logic          | 12249 |     0 |     53200 | 23.02 |
|   LUT as Memory         |     0 |     0 |     17400 |  0.00 |
| Slice Registers         |     0 |     0 |    106400 |  0.00 |
|   Register as Flip Flop |     0 |     0 |    106400 |  0.00 |
|   Register as Latch     |     0 |     0 |    106400 |  0.00 |
| F7 Muxes                |  2660 |     0 |     26600 | 10.00 |
| F8 Muxes                |   799 |     0 |     13300 |  6.01 |
+-------------------------+-------+-------+-----------+-------+


1.1 Summary of Registers by Type
--------------------------------
```

Figure 86. Utilization combinational inverse AES-128 report part 2.

Total	Clock Enable	Synchronous	Asynchronous
0	_	-	-
0	_	-	Set
0	_	-	Reset
0	_	Set	-
0	_	Reset	-
0	Yes	-	-
0	Yes	-	Set
0	Yes	-	Reset
0	Yes	Set	-
0	Yes	Reset	-

2. Slice Logic Distribution

Site Type	Used	Fixed	Available	Util%
Slice	3451	0	13300	25.95
SLICEL	2526	0		
SLICEM	925	0		
LUT as Logic	12249	0	53200	23.02
using O5 output only	0			
using O6 output only	10158			
using O5 and O6	2091			
LUT as Memory	0	0	17400	0.00
LUT as Distributed RAM	0	0		
LUT as Shift Register	0	0		
Slice Registers	0	0	106400	0.00
Register driven from within the Slice	0			
Register driven from outside the Slice	0			
Unique Control Sets	0		13300	0.00

Figure 87. Utilization combinational inverse AES-128 report part 3.

```
+----------------------------------------+-------+-------+-----------+-
------+
* Note: Available Control Sets calculated as Slice Registers / 8, Review
the Control Sets Report for more information regarding control sets.


3. Memory
---------

+----------------+------+-------+-----------+-------+
|    Site Type   | Used | Fixed | Available | Util% |
+----------------+------+-------+-----------+-------+
| Block RAM Tile |    0 |     0 |       140 |  0.00 |
|   RAMB36/FIFO* |    0 |     0 |       140 |  0.00 |
|   RAMB18       |    0 |     0 |       280 |  0.00 |
+----------------+------+-------+-----------+-------+
* Note: Each Block RAM Tile only has one FIFO logic available and
therefore can accommodate only one FIFO36E1 or one FIFO18E1. However, if
a FIFO18E1 occupies a Block RAM Tile, that tile can still accommodate a
RAMB18E1


4. DSP
------

+-----------+------+-------+-----------+-------+
| Site Type | Used | Fixed | Available | Util% |
+-----------+------+-------+-----------+-------+
| DSPs      |    0 |     0 |       220 |  0.00 |
+-----------+------+-------+-----------+-------+


5. IO and GT Specific
---------------------

+-----------------------------+------+-------+-----------+-------+
|          Site Type          | Used | Fixed | Available | Util% |
+-----------------------------+------+-------+-----------+-------+
| Bonded IOB                  |    0 |     0 |       200 |  0.00 |
| Bonded IPADs                |    0 |     0 |         2 |  0.00 |
| Bonded IOPADs               |    0 |     0 |       130 |  0.00 |
| PHY_CONTROL                 |    0 |     0 |         4 |  0.00 |
| PHASER_REF                  |    0 |     0 |         4 |  0.00 |
| OUT_FIFO                    |    0 |     0 |        16 |  0.00 |
| IN_FIFO                     |    0 |     0 |        16 |  0.00 |
| IDELAYCTRL                  |    0 |     0 |         4 |  0.00 |
| IBUFDS                      |    0 |     0 |       192 |  0.00 |
| PHASER_OUT/PHASER_OUT_PHY   |    0 |     0 |        16 |  0.00 |
| PHASER_IN/PHASER_IN_PHY     |    0 |     0 |        16 |  0.00 |
| IDELAYE2/IDELAYE2_FINEDELAY |    0 |     0 |       200 |  0.00 |
| ILOGIC                      |    0 |     0 |       200 |  0.00 |
| OLOGIC                      |    0 |     0 |       200 |  0.00 |
+-----------------------------+------+-------+-----------+-------+
```

Figure 88. Utilization combinational inverse AES-128 report part 4.

```
6. Clocking
-----------

+------------+------+-------+-----------+-------+
|  Site Type | Used | Fixed | Available | Util% |
+------------+------+-------+-----------+-------+
| BUFGCTRL   |    0 |     0 |        32 |  0.00 |
| BUFIO      |    0 |     0 |        16 |  0.00 |
| MMCME2_ADV |    0 |     0 |         4 |  0.00 |
| PLLE2_ADV  |    0 |     0 |         4 |  0.00 |
| BUFMRCE    |    0 |     0 |         8 |  0.00 |
| BUFHCE     |    0 |     0 |        72 |  0.00 |
| BUFR       |    0 |     0 |        16 |  0.00 |
+------------+------+-------+-----------+-------+


7. Specific Feature
-------------------

+-------------+------+-------+-----------+-------+
|  Site Type  | Used | Fixed | Available | Util% |
+-------------+------+-------+-----------+-------+
| BSCANE2     |    0 |     0 |         4 |  0.00 |
| CAPTUREE2   |    0 |     0 |         1 |  0.00 |
| DNA_PORT    |    0 |     0 |         1 |  0.00 |
| EFUSE_USR   |    0 |     0 |         1 |  0.00 |
| FRAME_ECCE2 |    0 |     0 |         1 |  0.00 |
| ICAPE2      |    0 |     0 |         2 |  0.00 |
| STARTUPE2   |    0 |     0 |         1 |  0.00 |
| XADC        |    0 |     0 |         1 |  0.00 |
+-------------+------+-------+-----------+-------+


8. Primitives
-------------

+----------+------+---------------------+
| Ref Name | Used | Functional Category |
+----------+------+---------------------+
| LUT6     | 8372 |                 LUT |
| MUXF7    | 2660 |               MuxFx |
| LUT4     | 2483 |                 LUT |
| LUT3     | 1321 |                 LUT |
| LUT5     | 1308 |                 LUT |
| LUT2     |  854 |                 LUT |
| MUXF8    |  799 |               MuxFx |
| LUT1     |    2 |                 LUT |
+----------+------+---------------------+


9. Black Boxes
--------------
```

A.4. Sequential AES timing report

Figure 89. AES timing reports. Part 1

```
Copyright 1986-2019 Xilinx, Inc. All Rights Reserved.
------------------------------------------------------------------------
-----------
| Tool Version : Vivado v.2019.2 (win64) Build 2708876 Wed Nov  6
21:40:23 MST 2019
| Date         : Mon Nov 16 12:04:05 2020
| Host         : DESKTOP-GLRI1LS running 64-bit major release  (build
9200)
| Command      : report_timing
| Design       : aes_sec
| Device       : 7z020-clg484
| Speed File   : -1  PRODUCTION 1.11 2014-09-11
------------------------------------------------------------------------
-----------

Timing Report

Slack (MET) :             0.001ns  (required time - arrival time)
  Source:                 cont_reg[3]/C
                            (rising edge-triggered cell FDRE clocked by
clk_aes  {rise@0.000ns fall@3.225ns period=6.450ns})
  Destination:            reg_reg[2][25]/D
                            (rising edge-triggered cell FDRE clocked by
clk_aes  {rise@0.000ns fall@3.225ns period=6.450ns})
  Path Group:             clk_aes
  Path Type:              Setup (Max at Slow Process Corner)
  Requirement:            6.450ns  (clk_aes rise@6.450ns - clk_aes
rise@0.000ns)
  Data Path Delay:        6.313ns  (logic 1.517ns (24.030%)  route
4.796ns (75.970%))
  Logic Levels:           7  (LUT3=2 LUT6=5)
  Clock Path Skew:        -0.145ns (DCD - SCD + CPR)
    Destination Clock Delay (DCD):    2.078ns = ( 8.528 - 6.450 )
    Source Clock Delay      (SCD):    2.406ns
    Clock Pessimism Removal (CPR):    0.183ns
  Clock Uncertainty:      0.035ns  ((TSJ^2 + TIJ^2)^1/2 + DJ) / 2 + PE
    Total System Jitter     (TSJ):    0.071ns
    Total Input Jitter      (TIJ):    0.000ns
    Discrete Jitter          (DJ):    0.000ns
    Phase Error              (PE):    0.000ns

    Location             Delay type                Incr(ns)  Path(ns)
Netlist Resource(s)
  -------------------------------------------------------------------
-------------------
                         (clock clk_aes rise edge)    0.000     0.000 r
                                                      0.000     0.000 r
CLOCK_1 (IN)
                         net (fo=0)                   0.000     0.000
CLOCK_1
                         IBUF (Prop_ibuf_I_O)         0.921     0.921 r
CLOCK_1_IBUF_inst/O
                         net (fo=1, unplaced)         0.800     1.721
CLOCK_1_IBUF
```

Figure 90. AES timing reports. Part 2

```
                         BUFG (Prop_bufg_I_O)        0.101     1.822 r
CLOCK_1_IBUF_BUFG_inst/O
                         net (fo=269, unplaced)      0.584     2.406
CLOCK_1_IBUF_BUFG
                         FDRE                                        r
cont_reg[3]/C
  -------------------------------------------------------------------
-------------------
                         FDRE (Prop_fdre_C_Q)        0.478     2.884 r
cont_reg[3]/Q
                         net (fo=6, unplaced)        0.773     3.657
cont_reg_n_0_[3]
                         LUT3 (Prop_lut3_I0_O)       0.295     3.952 r
reg[1][23]_i_2/O
                         net (fo=115, unplaced)      0.552     4.504
reg[1][23]_i_2_n_0
                         LUT3 (Prop_lut3_I1_O)       0.124     4.628 r
reg[3][19]_i_2/O
                         net (fo=34, unplaced)       1.184     5.812
inKey[19]
                         LUT6 (Prop_lut6_I1_O)       0.124     5.936 f
regKeyActual[121]_i_5/O
                         net (fo=1, unplaced)        0.902     6.838
regKeyActual[121]_i_5_n_0
                         LUT6 (Prop_lut6_I1_O)       0.124     6.962 r
regKeyActual[121]_i_2/O
                         net (fo=1, unplaced)        0.449     7.411
regKeyActual[121]_i_2_n_0
                         LUT6 (Prop_lut6_I0_O)       0.124     7.535 r
regKeyActual[121]_i_1/O
                         net (fo=8, unplaced)        0.487     8.022
carryKeyOut[121]
                         LUT6 (Prop_lut6_I2_O)       0.124     8.146 r
reg[2][25]_i_4/O
                         net (fo=1, unplaced)        0.449     8.595
subKeyIn[2][25]
                         LUT6 (Prop_lut6_I5_O)       0.124     8.719 r
reg[2][25]_i_1/O
                         net (fo=1, unplaced)        0.000     8.719
addRouKeyOut[2][25]
                         FDRE                                        r
reg_reg[2][25]/D
  -------------------------------------------------------------------
-------------------

                         (clock clk_aes rise edge)   6.450     6.450 r
                                                     0.000     6.450 r
CLOCK_1 (IN)
                         net (fo=0)                  0.000     6.450
CLOCK_1
                         IBUF (Prop_ibuf_I_O)        0.788     7.238 r
CLOCK_1_IBUF_inst/O
                         net (fo=1, unplaced)        0.760     7.998
CLOCK_1_IBUF
```

Figure 91. AES timing reports. Part 3

```
                         BUFG (Prop_bufg_I_O)         0.091     8.089 r
CLOCK_1_IBUF_BUFG_inst/O
                         net (fo=269, unplaced)       0.439     8.528
CLOCK_1_IBUF_BUFG
                         FDRE                                         r
reg_reg[2][25]/C
                         clock pessimism              0.183     8.711
                         clock uncertainty           -0.035     8.676
                         FDRE (Setup_fdre_C_D)        0.044     8.720
reg_reg[2][25]
  -------------------------------------------------------------------
                         required time                          8.720
                         arrival time                          -8.719
  -------------------------------------------------------------------
                         slack                                  0.001
```

A.5. Sequential AES utilization reports

Figure 92. AES utilization report. Part 1

```
Copyright 1986-2019 Xilinx, Inc. All Rights Reserved.
-------------------------------------------------------------------------
-------------------------------------------------------------------------
--------
| Tool Version : Vivado v.2019.2 (win64) Build 2708876 Wed Nov  6
21:40:23 MST 2019
| Date         : Mon Nov 16 14:20:06 2020
| Host         : DESKTOP-GLRI1LS running 64-bit major release  (build
9200)
| Command      : report_utilization -file E:/OneDriveECI/prp-
aes/Entregable/figures/resultados/aes_sec/aes_sec_utilization_report.txt
-name utilization_1
| Design       : aes_sec
| Device       : 7z020clg484-1
| Design State : Routed
-------------------------------------------------------------------------
-------------------------------------------------------------------------
--------

Utilization Design Information

Table of Contents
-----------------
1. Slice Logic
1.1 Summary of Registers by Type
2. Slice Logic Distribution
3. Memory
4. DSP
5. IO and GT Specific
6. Clocking
7. Specific Feature
8. Primitives
9. Black Boxes
10. Instantiated Netlists

1. Slice Logic
--------------

+-------------------------+------+-------+-----------+-------+
|        Site Type        | Used | Fixed | Available | Util% |
+-------------------------+------+-------+-----------+-------+
| Slice LUTs              | 1314 |     0 |     53200 |  2.47 |
|   LUT as Logic          | 1314 |     0 |     53200 |  2.47 |
|   LUT as Memory         |    0 |     0 |     17400 |  0.00 |
| Slice Registers         |  269 |     0 |    106400 |  0.25 |
|   Register as Flip Flop |  269 |     0 |    106400 |  0.25 |
|   Register as Latch     |    0 |     0 |    106400 |  0.00 |
| F7 Muxes                |  251 |     0 |     26600 |  0.94 |
| F8 Muxes                |  102 |     0 |     13300 |  0.77 |
+-------------------------+------+-------+-----------+-------+


1.1 Summary of Registers by Type
--------------------------------
```

Figure 93. AES utilization report. Part 2

Total	Clock Enable	Synchronous	Asynchronous
0	_	-	-
0	_	-	Set
0	_	-	Reset
0	_	Set	-
0	_	Reset	-
0	Yes	-	-
0	Yes	-	Set
0	Yes	-	Reset
0	Yes	Set	-
269	Yes	Reset	-

2. Slice Logic Distribution

Site Type	Used	Fixed	Available	Util%
Slice	363	0	13300	2.73
SLICEL	214	0		
SLICEM	149	0		
LUT as Logic	1314	0	53200	2.47
using O5 output only	7			
using O6 output only	1224			
using O5 and O6	83			
LUT as Memory	0	0	17400	0.00
LUT as Distributed RAM	0	0		
LUT as Shift Register	0	0		
Slice Registers	269	0	106400	0.25
Register driven from within the Slice	238			
Register driven from outside the Slice	31			
LUT in front of the register is unused	4			

Figure 94. AES utilization report. Part 3

```
|     LUT in front of the register is used   |   27 |       |           |
|
| Unique Control Sets                        |    5 |       |     13300 |
0.04 |
+--------------------------------------------+------+-------+-----------
+-------+
* Note: Available Control Sets calculated as Slice Registers / 8, Review
the Control Sets Report for more information regarding control sets.


3. Memory
---------

+----------------+------+-------+-----------+-------+
|    Site Type   | Used | Fixed | Available | Util% |
+----------------+------+-------+-----------+-------+
| Block RAM Tile |    0 |     0 |       140 |  0.00 |
|   RAMB36/FIFO* |    0 |     0 |       140 |  0.00 |
|   RAMB18       |    0 |     0 |       280 |  0.00 |
+----------------+------+-------+-----------+-------+
* Note: Each Block RAM Tile only has one FIFO logic available and
therefore can accommodate only one FIFO36E1 or one FIFO18E1. However, if
a FIFO18E1 occupies a Block RAM Tile, that tile can still accommodate a
RAMB18E1


4. DSP
------

+-----------+------+-------+-----------+-------+
| Site Type | Used | Fixed | Available | Util% |
+-----------+------+-------+-----------+-------+
| DSPs      |    0 |     0 |       220 |  0.00 |
+-----------+------+-------+-----------+-------+


5. IO and GT Specific
---------------------

+-----------------------------+------+-------+-----------+-------+
|          Site Type          | Used | Fixed | Available | Util% |
+-----------------------------+------+-------+-----------+-------+
| Bonded IOB                  |    0 |     0 |       200 |  0.00 |
| Bonded IPADs                |    0 |     0 |         2 |  0.00 |
| Bonded IOPADs               |    0 |     0 |       130 |  0.00 |
| PHY_CONTROL                 |    0 |     0 |         4 |  0.00 |
| PHASER_REF                  |    0 |     0 |         4 |  0.00 |
| OUT_FIFO                    |    0 |     0 |        16 |  0.00 |
| IN_FIFO                     |    0 |     0 |        16 |  0.00 |
| IDELAYCTRL                  |    0 |     0 |         4 |  0.00 |
| IBUFDS                      |    0 |     0 |       192 |  0.00 |
| PHASER_OUT/PHASER_OUT_PHY   |    0 |     0 |        16 |  0.00 |
| PHASER_IN/PHASER_IN_PHY     |    0 |     0 |        16 |  0.00 |
| IDELAYE2/IDELAYE2_FINEDELAY |    0 |     0 |       200 |  0.00 |
```

Figure 95. AES utilization report. Part 4

```
| ILOGIC                      |    0 |     0 |       200 |  0.00 |
| OLOGIC                      |    0 |     0 |       200 |  0.00 |
+-----------------------------+------+-------+-----------+-------+


6. Clocking
-----------

+------------+------+-------+-----------+-------+
|  Site Type | Used | Fixed | Available | Util% |
+------------+------+-------+-----------+-------+
| BUFGCTRL   |    0 |     0 |        32 |  0.00 |
| BUFIO      |    0 |     0 |        16 |  0.00 |
| MMCME2_ADV |    0 |     0 |         4 |  0.00 |
| PLLE2_ADV  |    0 |     0 |         4 |  0.00 |
| BUFMRCE    |    0 |     0 |         8 |  0.00 |
| BUFHCE     |    0 |     0 |        72 |  0.00 |
| BUFR       |    0 |     0 |        16 |  0.00 |
+------------+------+-------+-----------+-------+


7. Specific Feature
-------------------

+-------------+------+-------+-----------+-------+
|  Site Type  | Used | Fixed | Available | Util% |
+-------------+------+-------+-----------+-------+
| BSCANE2     |    0 |     0 |         4 |  0.00 |
| CAPTUREE2   |    0 |     0 |         1 |  0.00 |
| DNA_PORT    |    0 |     0 |         1 |  0.00 |
| EFUSE_USR   |    0 |     0 |         1 |  0.00 |
| FRAME_ECCE2 |    0 |     0 |         1 |  0.00 |
| ICAPE2      |    0 |     0 |         2 |  0.00 |
| STARTUPE2   |    0 |     0 |         1 |  0.00 |
| XADC        |    0 |     0 |         1 |  0.00 |
+-------------+------+-------+-----------+-------+


8. Primitives
-------------

+----------+------+---------------------+
| Ref Name | Used | Functional Category |
+----------+------+---------------------+
| LUT6     | 1006 |                 LUT |
| FDRE     |  269 |        Flop & Latch |
| MUXF7    |  251 |               MuxFx |
| LUT3     |  178 |                 LUT |
| MUXF8    |  102 |               MuxFx |
| LUT5     |   78 |                 LUT |
| LUT2     |   69 |                 LUT |
| LUT4     |   66 |                 LUT |
+----------+------+---------------------+
```

Figure 96. inverse AES utilization report. Part 1

```
Copyright 1986-2019 Xilinx, Inc. All Rights Reserved.
------------------------------------------------------------------------
------------------------------------------------------------------------
-----------
| Tool Version : Vivado v.2019.2 (win64) Build 2708876 Wed Nov  6
21:40:23 MST 2019
| Date         : Mon Nov 16 14:37:21 2020
| Host         : DESKTOP-GLRI1LS running 64-bit major release  (build
9200)
| Command      : report_utilization -file E:/OneDriveECI/prp-
aes/Entregable/figures/resultados/aes_sec/aesDec_sec_utilization_report.t
xt -name utilization_1
| Design       : aes_inv_chipher
| Device       : 7z020clg484-1
| Design State : Routed
------------------------------------------------------------------------
------------------------------------------------------------------------
-----------

Utilization Design Information

Table of Contents
-----------------
1. Slice Logic
1.1 Summary of Registers by Type
2. Slice Logic Distribution
3. Memory
4. DSP
5. IO and GT Specific
6. Clocking
7. Specific Feature
8. Primitives
9. Black Boxes
10. Instantiated Netlists

1. Slice Logic
--------------

+-------------------------+------+-------+-----------+-------+
|        Site Type        | Used | Fixed | Available | Util% |
+-------------------------+------+-------+-----------+-------+
| Slice LUTs              | 3409 |     0 |     53200 |  6.41 |
|   LUT as Logic          | 3409 |     0 |     53200 |  6.41 |
|   LUT as Memory         |    0 |     0 |     17400 |  0.00 |
| Slice Registers         |  413 |     0 |    106400 |  0.39 |
|   Register as Flip Flop |  413 |     0 |    106400 |  0.39 |
|   Register as Latch     |    0 |     0 |    106400 |  0.00 |
| F7 Muxes                |  260 |     0 |     26600 |  0.98 |
| F8 Muxes                |   24 |     0 |     13300 |  0.18 |
+-------------------------+------+-------+-----------+-------+


1.1 Summary of Registers by Type
--------------------------------
```

Figure 97. inverse AES utilization report. Part 2

Total	Clock Enable	Synchronous	Asynchronous
0	_	-	-
0	_	-	Set
0	_	-	Reset
0	_	Set	-
0	_	Reset	-
0	Yes	-	-
0	Yes	-	Set
0	Yes	-	Reset
4	Yes	Set	-
409	Yes	Reset	-

2. Slice Logic Distribution

Site Type	Used	Fixed	Available	Util%
Slice	966	0	13300	7.26
SLICEL	672	0		
SLICEM	294	0		
LUT as Logic	3409	0	53200	6.41
using O5 output only	0			
using O6 output only	2633			
using O5 and O6	776			
LUT as Memory	0	0	17400	0.00
LUT as Distributed RAM	0	0		
LUT as Shift Register	0	0		
Slice Registers	413	0	106400	0.39
Register driven from within the Slice	400			
Register driven from outside the Slice	13			
LUT in front of the register is unused	1			

Figure 98. inverse AES utilization report. Part 3

```
|     LUT in front of the register is used   |   12 |       |           |
|
| Unique Control Sets                        |    7 |       |     13300 |
0.05 |
+--------------------------------------------+------+-------+-----------
+-------+
* Note: Available Control Sets calculated as Slice Registers / 8, Review
the Control Sets Report for more information regarding control sets.


3. Memory
---------

+-------------------+------+-------+-----------+-------+
|     Site Type     | Used | Fixed | Available | Util% |
+-------------------+------+-------+-----------+-------+
| Block RAM Tile    |    2 |     0 |       140 |  1.43 |
|   RAMB36/FIFO*    |    0 |     0 |       140 |  0.00 |
|   RAMB18          |    4 |     0 |       280 |  1.43 |
|     RAMB18E1 only |    4 |       |           |       |
+-------------------+------+-------+-----------+-------+
* Note: Each Block RAM Tile only has one FIFO logic available and
therefore can accommodate only one FIFO36E1 or one FIFO18E1. However, if
a FIFO18E1 occupies a Block RAM Tile, that tile can still accommodate a
RAMB18E1


4. DSP
------

+-----------+------+-------+-----------+-------+
| Site Type | Used | Fixed | Available | Util% |
+-----------+------+-------+-----------+-------+
| DSPs      |    0 |     0 |       220 |  0.00 |
+-----------+------+-------+-----------+-------+


5. IO and GT Specific
---------------------

+-----------------------------+------+-------+-----------+-------+
|          Site Type          | Used | Fixed | Available | Util% |
+-----------------------------+------+-------+-----------+-------+
| Bonded IOB                  |    0 |     0 |       200 |  0.00 |
| Bonded IPADs                |    0 |     0 |         2 |  0.00 |
| Bonded IOPADs               |    0 |     0 |       130 |  0.00 |
| PHY_CONTROL                 |    0 |     0 |         4 |  0.00 |
| PHASER_REF                  |    0 |     0 |         4 |  0.00 |
| OUT_FIFO                    |    0 |     0 |        16 |  0.00 |
| IN_FIFO                     |    0 |     0 |        16 |  0.00 |
| IDELAYCTRL                  |    0 |     0 |         4 |  0.00 |
| IBUFDS                      |    0 |     0 |       192 |  0.00 |
| PHASER_OUT/PHASER_OUT_PHY   |    0 |     0 |        16 |  0.00 |
| PHASER_IN/PHASER_IN_PHY     |    0 |     0 |        16 |  0.00 |
```

Figure 99. inverse AES utilization report. Part 4

```
| IDELAYE2/IDELAYE2_FINEDELAY |    0 |     0 |       200 |  0.00 |
| ILOGIC                      |    0 |     0 |       200 |  0.00 |
| OLOGIC                      |    0 |     0 |       200 |  0.00 |
+-----------------------------+------+-------+-----------+-------+


6. Clocking
-----------

+------------+------+-------+-----------+-------+
|  Site Type | Used | Fixed | Available | Util% |
+------------+------+-------+-----------+-------+
| BUFGCTRL   |    0 |     0 |        32 |  0.00 |
| BUFIO      |    0 |     0 |        16 |  0.00 |
| MMCME2_ADV |    0 |     0 |         4 |  0.00 |
| PLLE2_ADV  |    0 |     0 |         4 |  0.00 |
| BUFMRCE    |    0 |     0 |         8 |  0.00 |
| BUFHCE     |    0 |     0 |        72 |  0.00 |
| BUFR       |    0 |     0 |        16 |  0.00 |
+------------+------+-------+-----------+-------+


7. Specific Feature
-------------------

+-------------+------+-------+-----------+-------+
|  Site Type  | Used | Fixed | Available | Util% |
+-------------+------+-------+-----------+-------+
| BSCANE2     |    0 |     0 |         4 |  0.00 |
| CAPTUREE2   |    0 |     0 |         1 |  0.00 |
| DNA_PORT    |    0 |     0 |         1 |  0.00 |
| EFUSE_USR   |    0 |     0 |         1 |  0.00 |
| FRAME_ECCE2 |    0 |     0 |         1 |  0.00 |
| ICAPE2      |    0 |     0 |         2 |  0.00 |
| STARTUPE2   |    0 |     0 |         1 |  0.00 |
| XADC        |    0 |     0 |         1 |  0.00 |
+-------------+------+-------+-----------+-------+


8. Primitives
-------------

+----------+------+---------------------+
| Ref Name | Used | Functional Category |
+----------+------+---------------------+
| LUT6     | 2083 |                 LUT |
| LUT5     |  670 |                 LUT |
| LUT3     |  587 |                 LUT |
| LUT4     |  553 |                 LUT |
| FDRE     |  409 |        Flop & Latch |
| LUT2     |  292 |                 LUT |
| MUXF7    |  260 |               MuxFx |
| MUXF8    |   24 |               MuxFx |
| RAMB18E1 |    4 |        Block Memory |
```

A.6. AES-CTR timing reports

Figure 100. AES-CTR Zynq7000 timing report. Part 1

```
Copyright 1986-2019 Xilinx, Inc. All Rights Reserved.
------------------------------------------------------------------------
-----------
| Tool Version : Vivado v.2019.2 (win64) Build 2708876 Wed Nov  6
21:40:23 MST 2019
| Date         : Mon Nov 16 23:07:31 2020
| Host         : DESKTOP-GLRI1LS running 64-bit major release  (build
9200)
| Command      : report_timing
| Design       : AesCtr
| Device       : 7z020-clg484
| Speed File   : -1  PRODUCTION 1.11 2014-09-11
------------------------------------------------------------------------
-----------

Timing Report

Slack (MET) :             0.002ns  (required time - arrival time)
  Source:                 block_ctr0/aes/cont_reg[1]/C
                            (rising edge-triggered cell FDRE clocked by
clk_aes  {rise@0.000ns fall@3.220ns period=6.440ns})
  Destination:            block_ctr0/aes/reg_reg[2][6]/D
                            (rising edge-triggered cell FDRE clocked by
clk_aes  {rise@0.000ns fall@3.220ns period=6.440ns})
  Path Group:             clk_aes
  Path Type:              Setup (Max at Slow Process Corner)
  Requirement:            6.440ns  (clk_aes rise@6.440ns - clk_aes
rise@0.000ns)
  Data Path Delay:        6.302ns  (logic 1.567ns (24.865%)  route
4.735ns (75.135%))
  Logic Levels:           7  (LUT3=2 LUT4=1 LUT5=2 LUT6=2)
  Clock Path Skew:        -0.145ns (DCD - SCD + CPR)
    Destination Clock Delay (DCD):    2.078ns = ( 8.518 - 6.440 )
    Source Clock Delay      (SCD):    2.406ns
    Clock Pessimism Removal (CPR):    0.183ns
  Clock Uncertainty:      0.035ns  ((TSJ^2 + TIJ^2)^1/2 + DJ) / 2 + PE
    Total System Jitter     (TSJ):    0.071ns
    Total Input Jitter      (TIJ):    0.000ns
    Discrete Jitter          (DJ):    0.000ns
    Phase Error              (PE):    0.000ns

    Location             Delay type                Incr(ns)  Path(ns)
Netlist Resource(s)
  -------------------------------------------------------------------
-------------------
                         (clock clk_aes rise edge)    0.000     0.000 r
                                                      0.000     0.000 r
clk (IN)
                         net (fo=0)                   0.000     0.000
clk
                         IBUF (Prop_ibuf_I_O)         0.921     0.921 r
clk_IBUF_inst/O
                         net (fo=1, unplaced)         0.800     1.721
clk_IBUF
```

Figure 101. AES-CTR Zynq7000 timing report. Part 2

```
                          BUFG (Prop_bufg_I_O)        0.101     1.822 r
clk_IBUF_BUFG_inst/O
                          net (fo=1076, unplaced)     0.584     2.406
block_ctr0/aes/CLK
                          FDRE                                        r
block_ctr0/aes/cont_reg[1]/C
  -------------------------------------------------------------------
-------------------
                          FDRE (Prop_fdre_C_Q)        0.478     2.884 f
block_ctr0/aes/cont_reg[1]/Q
                          net (fo=8, unplaced)        0.779     3.663
block_ctr0/aes/cont_reg_n_0_[1]
                          LUT3 (Prop_lut3_I0_O)       0.319     3.982 r
block_ctr0/aes/regKeyActual[95]_i_2/O
                          net (fo=70, unplaced)       0.540     4.522
block_ctr0/aes/inKey1
                          LUT3 (Prop_lut3_I2_O)       0.124     4.646 r
block_ctr0/aes/regKeyActual[27]_i_2/O
                          net (fo=36, unplaced)       1.185     5.831
block_ctr0/aes/suKy_conn/inKey[27]
                          LUT6 (Prop_lut6_I1_O)       0.124     5.955 r
block_ctr0/aes/suKy_conn/i_/regKeyActual[102]_i_5/O
                          net (fo=1, unplaced)        0.902     6.857
block_ctr0/aes/suKy_conn/i_/regKeyActual[102]_i_5_n_0
                          LUT5 (Prop_lut5_I1_O)       0.124     6.981 r
block_ctr0/aes/suKy_conn/i_/regKeyActual[102]_i_2/O
                          net (fo=3, unplaced)        0.437     7.418
block_ctr0/aes/suKy_conn/regKeyActual_reg[25]
                          LUT6 (Prop_lut6_I2_O)       0.124     7.542 r
block_ctr0/aes/suKy_conn/i_/regKeyActual[38]_i_1/O
                          net (fo=4, unplaced)        0.473     8.015
block_ctr0/aes/suKy_conn/posRcon_reg[1][38]
                          LUT5 (Prop_lut5_I4_O)       0.124     8.139 r
block_ctr0/aes/suKy_conn/i_/reg[2][6]_i_4/O
                          net (fo=1, unplaced)        0.419     8.558
block_ctr0/aes/subKeyIn[2]_12[6]
                          LUT4 (Prop_lut4_I3_O)       0.150     8.708 r
block_ctr0/aes/reg[2][6]_i_1/O
                          net (fo=1, unplaced)        0.000     8.708
block_ctr0/aes/addRouKeyOut[2]_5[6]
                          FDRE                                        r
block_ctr0/aes/reg_reg[2][6]/D
  -------------------------------------------------------------------
-------------------

                          (clock clk_aes rise edge)    6.440     6.440 r
                                                       0.000     6.440 r
clk (IN)
                          net (fo=0)                  0.000     6.440
clk
                          IBUF (Prop_ibuf_I_O)        0.788     7.228 r
clk_IBUF_inst/O
                          net (fo=1, unplaced)        0.760     7.988
clk_IBUF
```

Figure 102. AES-CTR Zynq7000 timing report. Part 3

```
                         BUFG (Prop_bufg_I_O)         0.091     8.079 r
clk_IBUF_BUFG_inst/O
                         net (fo=1076, unplaced)      0.439     8.518
block_ctr0/aes/CLK
                         FDRE                                         r
block_ctr0/aes/reg_reg[2][6]/C
                         clock pessimism              0.183     8.701
                         clock uncertainty           -0.035     8.666
                         FDRE (Setup_fdre_C_D)        0.044     8.710
block_ctr0/aes/reg_reg[2][6]
  -------------------------------------------------------------------
                         required time                          8.710
                         arrival time                          -8.708
  -------------------------------------------------------------------
                         slack                                  0.002
```

Figure 103. AES-CTR Kintex7 timing report. Part 1

```
Copyright 1986-2019 Xilinx, Inc. All Rights Reserved.
------------------------------------------------------------------------
-----------
| Tool Version : Vivado v.2019.2 (win64) Build 2708876 Wed Nov  6
21:40:23 MST 2019
| Date         : Mon Nov 16 22:56:46 2020
| Host         : DESKTOP-GLRI1LS running 64-bit major release  (build
9200)
| Command      : report_timing
| Design       : AesCtr
| Device       : 7k325t-ffg676
| Speed File   : -1  PRODUCTION 1.12 2017-02-17
------------------------------------------------------------------------
-----------

Timing Report

Slack (MET) :             0.005ns  (required time - arrival time)
  Source:                 block_ctr0/aes/cont_reg[1]/C
                            (rising edge-triggered cell FDRE clocked by
clk_aes  {rise@0.000ns fall@2.100ns period=4.200ns})
  Destination:            block_ctr0/aes/reg_reg[1][25]/D
                            (rising edge-triggered cell FDRE clocked by
clk_aes  {rise@0.000ns fall@2.100ns period=4.200ns})
  Path Group:             clk_aes
  Path Type:              Setup (Max at Slow Process Corner)
  Requirement:            4.200ns  (clk_aes rise@4.200ns - clk_aes
rise@0.000ns)
  Data Path Delay:        4.052ns  (logic 0.746ns (18.411%)  route
3.306ns (81.589%))
  Logic Levels:           7  (LUT3=2 LUT5=1 LUT6=4)
  Clock Path Skew:        -0.145ns (DCD - SCD + CPR)
    Destination Clock Delay (DCD):    1.933ns = ( 6.133 - 4.200 )
    Source Clock Delay      (SCD):    2.191ns
    Clock Pessimism Removal (CPR):    0.113ns
  Clock Uncertainty:      0.035ns  ((TSJ^2 + TIJ^2)^1/2 + DJ) / 2 + PE
    Total System Jitter     (TSJ):    0.071ns
    Total Input Jitter      (TIJ):    0.000ns
    Discrete Jitter          (DJ):    0.000ns
    Phase Error              (PE):    0.000ns

    Location             Delay type                Incr(ns)  Path(ns)
Netlist Resource(s)
  -------------------------------------------------------------------
-------------------
                         (clock clk_aes rise edge)    0.000     0.000 r
                                                      0.000     0.000 r
clk (IN)
                         net (fo=0)                   0.000     0.000
clk
                         IBUF (Prop_ibuf_I_O)         0.903     0.903 r
clk_IBUF_inst/O
                         net (fo=1, unplaced)         0.584     1.487
clk_IBUF
```

Figure 104. AES-CTR Kintex7 timing report. Part 2

```
                         BUFG (Prop_bufg_I_O)        0.120     1.607 r
clk_IBUF_BUFG_inst/O
                         net (fo=1076, unplaced)     0.584     2.191
block_ctr0/aes/CLK
                         FDRE                                        r
block_ctr0/aes/cont_reg[1]/C
  -------------------------------------------------------------------
-------------------
                         FDRE (Prop_fdre_C_Q)        0.269     2.460 f
block_ctr0/aes/cont_reg[1]/Q
                         net (fo=8, unplaced)        0.570     3.030
block_ctr0/aes/cont_reg_n_0_[1]
                         LUT3 (Prop_lut3_I0_O)       0.153     3.183 r
block_ctr0/aes/regKeyActual[119]_i_2/O
                         net (fo=150, unplaced)      0.450     3.633
block_ctr0/aes/regKeyActual[119]_i_2_n_0
                         LUT3 (Prop_lut3_I2_O)       0.056     3.689 r
block_ctr0/aes/regKeyActual[19]_i_2/O
                         net (fo=34, unplaced)       0.737     4.426
block_ctr0/aes/suKy_conn/inKey[19]
                         LUT6 (Prop_lut6_I1_O)       0.053     4.479 f
block_ctr0/aes/suKy_conn/i_/regKeyActual[121]_i_5/O
                         net (fo=1, unplaced)        0.521     5.000
block_ctr0/aes/suKy_conn/i_/regKeyActual[121]_i_5_n_0
                         LUT6 (Prop_lut6_I1_O)       0.053     5.053 r
block_ctr0/aes/suKy_conn/i_/regKeyActual[121]_i_2/O
                         net (fo=1, unplaced)        0.340     5.393
block_ctr0/aes/suKy_conn/i_/regKeyActual[121]_i_2_n_0
                         LUT6 (Prop_lut6_I0_O)       0.053     5.446 r
block_ctr0/aes/suKy_conn/i_/regKeyActual[121]_i_1/O
                         net (fo=8, unplaced)        0.378     5.824
block_ctr0/aes/suKy_conn/posRcon_reg[1][110]
                         LUT5 (Prop_lut5_I4_O)       0.056     5.880 r
block_ctr0/aes/suKy_conn/i_/reg[1][25]_i_4/O
                         net (fo=1, unplaced)        0.310     6.190
block_ctr0/aes/subKeyIn[1]_10[25]
                         LUT6 (Prop_lut6_I5_O)       0.053     6.243 r
block_ctr0/aes/reg[1][25]_i_1/O
                         net (fo=1, unplaced)        0.000     6.243
block_ctr0/aes/addRouKeyOut[1]_4[25]
                         FDRE                                        r
block_ctr0/aes/reg_reg[1][25]/D
  -------------------------------------------------------------------
-------------------

                         (clock clk_aes rise edge)    4.200     4.200 r
                                                      0.000     4.200 r
clk (IN)
                         net (fo=0)                  0.000     4.200
clk
                         IBUF (Prop_ibuf_I_O)        0.827     5.027 r
clk_IBUF_inst/O
                         net (fo=1, unplaced)        0.554     5.581
clk_IBUF
```

Figure 105. AES-CTR Kintex7 timing report. Part 3

```
                         BUFG (Prop_bufg_I_O)         0.113     5.694 r
clk_IBUF_BUFG_inst/O
                         net (fo=1076, unplaced)      0.439     6.133
block_ctr0/aes/CLK
                         FDRE                                         r
block_ctr0/aes/reg_reg[1][25]/C
                         clock pessimism              0.113     6.246
                         clock uncertainty           -0.035     6.211
                         FDRE (Setup_fdre_C_D)        0.037     6.248
block_ctr0/aes/reg_reg[1][25]
  -------------------------------------------------------------------
                         required time                          6.248
                         arrival time                          -6.243
  -------------------------------------------------------------------
                         slack                                  0.005
```

A.7. AES-CTR utilization reports

Figure 106. AES-CTR Zynq7000 utilization report. Part 1

```
Copyright 1986-2019 Xilinx, Inc. All Rights Reserved.
------------------------------------------------------------------------
------------------------------------------------------------------------
---------------
| Tool Version : Vivado v.2019.2 (win64) Build 2708876 Wed Nov  6
21:40:23 MST 2019
| Date         : Mon Nov 16 21:38:31 2020
| Host         : DESKTOP-GLRI1LS running 64-bit major release  (build
9200)
| Command      : report_utilization -file E:/OneDriveECI/prp-
aes/Entregable/figures/resultados/aes_ctr/aes128_ctr_ooc_utilization_repo
rt.txt -name utilization_1
| Design       : AesCtr
| Device       : 7z020clg484-1
| Design State : Routed
------------------------------------------------------------------------
------------------------------------------------------------------------
---------------

Utilization Design Information

Table of Contents
-----------------
1. Slice Logic
1.1 Summary of Registers by Type
2. Slice Logic Distribution
3. Memory
4. DSP
5. IO and GT Specific
6. Clocking
7. Specific Feature
8. Primitives
9. Black Boxes
10. Instantiated Netlists

1. Slice Logic
--------------

+-------------------------+------+-------+-----------+-------+
|        Site Type        | Used | Fixed | Available | Util% |
+-------------------------+------+-------+-----------+-------+
| Slice LUTs              | 8178 |     0 |     53200 | 15.37 |
|   LUT as Logic          | 8178 |     0 |     53200 | 15.37 |
|   LUT as Memory         |    0 |     0 |     17400 |  0.00 |
| Slice Registers         | 1076 |     0 |    106400 |  1.01 |
|   Register as Flip Flop | 1076 |     0 |    106400 |  1.01 |
|   Register as Latch     |    0 |     0 |    106400 |  0.00 |
| F7 Muxes                | 1092 |     0 |     26600 |  4.11 |
| F8 Muxes                |  376 |     0 |     13300 |  2.83 |
+-------------------------+------+-------+-----------+-------+


1.1 Summary of Registers by Type
--------------------------------
```

Figure 107. AES-CTR Zynq7000 utilization report. Part 2

Total	Clock Enable	Synchronous	Asynchronous
0	_	-	-
0	_	-	Set
0	_	-	Reset
0	_	Set	-
0	_	Reset	-
0	Yes	-	-
0	Yes	-	Set
0	Yes	-	Reset
0	Yes	Set	-
1076	Yes	Reset	-

2. Slice Logic Distribution

Site Type	Used	Fixed	Available	Util%
Slice	2275	0	13300	17.11
SLICEL	1696	0		
SLICEM	579	0		
LUT as Logic	8178	0	53200	15.37
using O5 output only	8			
using O6 output only	7266			
using O5 and O6	904			
LUT as Memory	0	0	17400	0.00
LUT as Distributed RAM	0	0		
LUT as Shift Register	0	0		
Slice Registers	1076	0	106400	1.01
Register driven from within the Slice	919			
Register driven from outside the Slice	157			
LUT in front of the register is unused	13			

Figure 108. AES-CTR Zynq7000 utilization report. Part 3

```
|     LUT in front of the register is used   |  144 |       |           |
|
| Unique Control Sets                        |   17 |       |     13300 |
0.13 |
+--------------------------------------------+------+-------+-----------
+-------+
* Note: Available Control Sets calculated as Slice Registers / 8, Review
the Control Sets Report for more information regarding control sets.


3. Memory
---------

+----------------+------+-------+-----------+-------+
|    Site Type   | Used | Fixed | Available | Util% |
+----------------+------+-------+-----------+-------+
| Block RAM Tile |    0 |     0 |       140 |  0.00 |
|   RAMB36/FIFO* |    0 |     0 |       140 |  0.00 |
|   RAMB18       |    0 |     0 |       280 |  0.00 |
+----------------+------+-------+-----------+-------+
* Note: Each Block RAM Tile only has one FIFO logic available and
therefore can accommodate only one FIFO36E1 or one FIFO18E1. However, if
a FIFO18E1 occupies a Block RAM Tile, that tile can still accommodate a
RAMB18E1


4. DSP
------

+-----------+------+-------+-----------+-------+
| Site Type | Used | Fixed | Available | Util% |
+-----------+------+-------+-----------+-------+
| DSPs      |    0 |     0 |       220 |  0.00 |
+-----------+------+-------+-----------+-------+


5. IO and GT Specific
---------------------

+-----------------------------+------+-------+-----------+-------+
|          Site Type          | Used | Fixed | Available | Util% |
+-----------------------------+------+-------+-----------+-------+
| Bonded IOB                  |    0 |     0 |       200 |  0.00 |
| Bonded IPADs                |    0 |     0 |         2 |  0.00 |
| Bonded IOPADs               |    0 |     0 |       130 |  0.00 |
| PHY_CONTROL                 |    0 |     0 |         4 |  0.00 |
| PHASER_REF                  |    0 |     0 |         4 |  0.00 |
| OUT_FIFO                    |    0 |     0 |        16 |  0.00 |
| IN_FIFO                     |    0 |     0 |        16 |  0.00 |
| IDELAYCTRL                  |    0 |     0 |         4 |  0.00 |
| IBUFDS                      |    0 |     0 |       192 |  0.00 |
| PHASER_OUT/PHASER_OUT_PHY   |    0 |     0 |        16 |  0.00 |
| PHASER_IN/PHASER_IN_PHY     |    0 |     0 |        16 |  0.00 |
| IDELAYE2/IDELAYE2_FINEDELAY |    0 |     0 |       200 |  0.00 |
```

Figure 109. AES-CTR Zynq7000 utilization report. Part 4

```
| ILOGIC                      |    0 |     0 |       200 |  0.00 |
| OLOGIC                      |    0 |     0 |       200 |  0.00 |
+-----------------------------+------+-------+-----------+-------+


6. Clocking
-----------

+------------+------+-------+-----------+-------+
|  Site Type | Used | Fixed | Available | Util% |
+------------+------+-------+-----------+-------+
| BUFGCTRL   |    0 |     0 |        32 |  0.00 |
| BUFIO      |    0 |     0 |        16 |  0.00 |
| MMCME2_ADV |    0 |     0 |         4 |  0.00 |
| PLLE2_ADV  |    0 |     0 |         4 |  0.00 |
| BUFMRCE    |    0 |     0 |         8 |  0.00 |
| BUFHCE     |    0 |     0 |        72 |  0.00 |
| BUFR       |    0 |     0 |        16 |  0.00 |
+------------+------+-------+-----------+-------+


7. Specific Feature
-------------------

+-------------+------+-------+-----------+-------+
|  Site Type  | Used | Fixed | Available | Util% |
+-------------+------+-------+-----------+-------+
| BSCANE2     |    0 |     0 |         4 |  0.00 |
| CAPTUREE2   |    0 |     0 |         1 |  0.00 |
| DNA_PORT    |    0 |     0 |         1 |  0.00 |
| EFUSE_USR   |    0 |     0 |         1 |  0.00 |
| FRAME_ECCE2 |    0 |     0 |         1 |  0.00 |
| ICAPE2      |    0 |     0 |         2 |  0.00 |
| STARTUPE2   |    0 |     0 |         1 |  0.00 |
| XADC        |    0 |     0 |         1 |  0.00 |
+-------------+------+-------+-----------+-------+


8. Primitives
-------------

+----------+------+---------------------+
| Ref Name | Used | Functional Category |
+----------+------+---------------------+
| LUT6     | 3738 |                 LUT |
| LUT4     | 2810 |                 LUT |
| LUT2     | 1186 |                 LUT |
| MUXF7    | 1092 |               MuxFx |
| FDRE     | 1076 |        Flop & Latch |
| LUT5     |  838 |                 LUT |
| LUT3     |  490 |                 LUT |
| MUXF8    |  376 |               MuxFx |
| CARRY4   |  132 |          CarryLogic |
| LUT1     |   20 |                 LUT |
```

Figure 110. AES-CTR Kintex7 utilization report. Part 1

```
Copyright 1986-2019 Xilinx, Inc. All Rights Reserved.
-------------------------------------------------------------------------
-------------------------------------------------------------------------
----------------------
| Tool Version : Vivado v.2019.2 (win64) Build 2708876 Wed Nov  6
21:40:23 MST 2019
| Date         : Mon Nov 16 22:37:24 2020
| Host         : DESKTOP-GLRI1LS running 64-bit major release  (build
9200)
| Command      : report_utilization -file E:/OneDriveECI/prp-
aes/Entregable/figures/resultados/aes_ctr/aes128_ctr_ooc_utilization_repo
rt_kintex.txt -name utilization_1
| Design       : AesCtr
| Device       : 7k325tffg676-1
| Design State : Routed
-------------------------------------------------------------------------
-------------------------------------------------------------------------
----------------------

Utilization Design Information

Table of Contents
-----------------
1. Slice Logic
1.1 Summary of Registers by Type
2. Slice Logic Distribution
3. Memory
4. DSP
5. IO and GT Specific
6. Clocking
7. Specific Feature
8. Primitives
9. Black Boxes
10. Instantiated Netlists

1. Slice Logic
--------------

+-------------------------+------+-------+-----------+-------+
|        Site Type        | Used | Fixed | Available | Util% |
+-------------------------+------+-------+-----------+-------+
| Slice LUTs              | 8116 |     0 |    203800 |  3.98 |
|   LUT as Logic          | 8116 |     0 |    203800 |  3.98 |
|   LUT as Memory         |    0 |     0 |     64000 |  0.00 |
| Slice Registers         | 1076 |     0 |    407600 |  0.26 |
|   Register as Flip Flop | 1076 |     0 |    407600 |  0.26 |
|   Register as Latch     |    0 |     0 |    407600 |  0.00 |
| F7 Muxes                | 1092 |     0 |    101900 |  1.07 |
| F8 Muxes                |  376 |     0 |     50950 |  0.74 |
+-------------------------+------+-------+-----------+-------+


1.1 Summary of Registers by Type
--------------------------------
```

Figure 111. AES-CTR Kintex7 utilization report. Part2

Total	Clock Enable	Synchronous	Asynchronous
0	_	-	-
0	_	-	Set
0	_	-	Reset
0	_	Set	-
0	_	Reset	-
0	Yes	-	-
0	Yes	-	Set
0	Yes	-	Reset
0	Yes	Set	-
1076	Yes	Reset	-

2. Slice Logic Distribution

Site Type	Used	Fixed	Available	Util%
Slice	2276	0	50950	4.47
SLICEL	1592	0		
SLICEM	684	0		
LUT as Logic	8116	0	203800	3.98
using O5 output only	0			
using O6 output only	7154			
using O5 and O6	962			
LUT as Memory	0	0	64000	0.00
LUT as Distributed RAM	0	0		
LUT as Shift Register	0	0		
Slice Registers	1076	0	407600	0.26
Register driven from within the Slice	939			
Register driven from outside the Slice	137			
LUT in front of the register is unused	9			

Figure 112. AES-CTR Kintex7 utilization report. Part 3

```
|     LUT in front of the register is used   |  128 |       |           |
|
| Unique Control Sets                        |   17 |       |     50950 |
0.03 |
+--------------------------------------------+------+-------+-----------
+-------+
* Note: Available Control Sets calculated as Slice Registers / 8, Review
the Control Sets Report for more information regarding control sets.


3. Memory
---------

+----------------+------+-------+-----------+-------+
|    Site Type   | Used | Fixed | Available | Util% |
+----------------+------+-------+-----------+-------+
| Block RAM Tile |    0 |     0 |       445 |  0.00 |
|   RAMB36/FIFO* |    0 |     0 |       445 |  0.00 |
|   RAMB18       |    0 |     0 |       890 |  0.00 |
+----------------+------+-------+-----------+-------+
* Note: Each Block RAM Tile only has one FIFO logic available and
therefore can accommodate only one FIFO36E1 or one FIFO18E1. However, if
a FIFO18E1 occupies a Block RAM Tile, that tile can still accommodate a
RAMB18E1


4. DSP
------

+-----------+------+-------+-----------+-------+
| Site Type | Used | Fixed | Available | Util% |
+-----------+------+-------+-----------+-------+
| DSPs      |    0 |     0 |       840 |  0.00 |
+-----------+------+-------+-----------+-------+


5. IO and GT Specific
---------------------

+-----------------------------+------+-------+-----------+-------+
|          Site Type          | Used | Fixed | Available | Util% |
+-----------------------------+------+-------+-----------+-------+
| Bonded IOB                  |    0 |     0 |       400 |  0.00 |
| Bonded IPADs                |    0 |     0 |        26 |  0.00 |
| Bonded OPADs                |    0 |     0 |        16 |  0.00 |
| PHY_CONTROL                 |    0 |     0 |        10 |  0.00 |
| PHASER_REF                  |    0 |     0 |        10 |  0.00 |
| OUT_FIFO                    |    0 |     0 |        40 |  0.00 |
| IN_FIFO                     |    0 |     0 |        40 |  0.00 |
| IDELAYCTRL                  |    0 |     0 |        10 |  0.00 |
| IBUFDS                      |    0 |     0 |       384 |  0.00 |
| GTXE2_COMMON                |    0 |     0 |         2 |  0.00 |
| GTXE2_CHANNEL               |    0 |     0 |         8 |  0.00 |
| PHASER_OUT/PHASER_OUT_PHY   |    0 |     0 |        40 |  0.00 |
```

Figure 113. AES-CTR Kintex7 utilization report. Part 4

```
| PHASER_IN/PHASER_IN_PHY     |    0 |     0 |        40 |  0.00 |
| IDELAYE2/IDELAYE2_FINEDELAY |    0 |     0 |       500 |  0.00 |
| ODELAYE2/ODELAYE2_FINEDELAY |    0 |     0 |       150 |  0.00 |
| IBUFDS_GTE2                 |    0 |     0 |         4 |  0.00 |
| ILOGIC                      |    0 |     0 |       400 |  0.00 |
| OLOGIC                      |    0 |     0 |       400 |  0.00 |
+-----------------------------+------+-------+-----------+-------+


6. Clocking
-----------

+------------+------+-------+-----------+-------+
|  Site Type | Used | Fixed | Available | Util% |
+------------+------+-------+-----------+-------+
| BUFGCTRL   |    0 |     0 |        32 |  0.00 |
| BUFIO      |    0 |     0 |        40 |  0.00 |
| MMCME2_ADV |    0 |     0 |        10 |  0.00 |
| PLLE2_ADV  |    0 |     0 |        10 |  0.00 |
| BUFMRCE    |    0 |     0 |        20 |  0.00 |
| BUFHCE     |    0 |     0 |       168 |  0.00 |
| BUFR       |    0 |     0 |        40 |  0.00 |
+------------+------+-------+-----------+-------+


7. Specific Feature
-------------------

+-------------+------+-------+-----------+-------+
|  Site Type  | Used | Fixed | Available | Util% |
+-------------+------+-------+-----------+-------+
| BSCANE2     |    0 |     0 |         4 |  0.00 |
| CAPTUREE2   |    0 |     0 |         1 |  0.00 |
| DNA_PORT    |    0 |     0 |         1 |  0.00 |
| EFUSE_USR   |    0 |     0 |         1 |  0.00 |
| FRAME_ECCE2 |    0 |     0 |         1 |  0.00 |
| ICAPE2      |    0 |     0 |         2 |  0.00 |
| PCIE_2_1    |    0 |     0 |         1 |  0.00 |
| STARTUPE2   |    0 |     0 |         1 |  0.00 |
| XADC        |    0 |     0 |         1 |  0.00 |
+-------------+------+-------+-----------+-------+


8. Primitives
-------------

+----------+------+---------------------+
| Ref Name | Used | Functional Category |
+----------+------+---------------------+
| LUT6     | 3884 |                 LUT |
| LUT4     | 2698 |                 LUT |
| LUT2     | 1164 |                 LUT |
| MUXF7    | 1092 |               MuxFx |
| FDRE     | 1076 |        Flop & Latch |
```

A.8. Verification of submitted paper

Figure 114. Submitted paper to *Computers and Electrical Engineering* journal