NATIONAL UNIVERSITY OF SCIENCE
AND TECHNOLOGY POLITEHNICA
BUCHAREST

Doctoral School of Electronics, Telecommunications and Information Technology

Decision No. 49 from 20.05.2024

Ph.D. THESIS SUMMARY

Ionuț RĂDOI

CONTRIBUȚII LA PROCESAREA DATELOR ÎN SISTEME MULTISENZOR FOLOSIND CIRCUITE HARDWARE RECONFIGURABILE

CONTRIBUTIONS TO DATA PROCESSING IN MULTISENSOR SYSTEMS USING RECONFIGURABLE HARDWARE CIRCUITS

THESIS COMMITTEE

Prof. Dr. Ing. Mihai CIUC National University Of Science And Technology Politehnica Bucharest	President
Prof. Dr. Ing. Lidia DOBRESCU National University Of Science And Technology Politehnica Bucharest	PhD Supervisor
Prof. Dr. Ing. Daniela TĂRNICERIU Gheorghe Asachi Technical University of Iaşi	Referee
Prof. Dr. Ing. Radu Mihnea UDREA National University Of Science And Technology Politehnica Bucharest	Referee
CSI Dr. Ing. Mihail-Liviu COȘEREANU National Institute for Aerospace Research	Referee

BUCHAREST 2024

Table of contents

Chapter 1

Introduction

1.1 Presentation of the field of the doctoral thesis

In recent years, advances in electronic circuitry and data networks have enabled the use of wireless sensor networks (WSNs) on a large scale and prompted the development of new generations of networks that offer overwhelming advantages over wireless networks developed in the past and have changed the way we live [1].

Concomitant with the evolution of sensor networks, the market for reconfigurable circuits is expected to reach $ 11.7 billion in 2027, after being valued at $ 5.7 billion in 2020 [2].

To adapt to the increased demand for portable devices, companies producing reconfigurable circuits have also introduced low-power circuits in their portfolio. The parallel data processing capability qualifies reconfigurable circuits for use in the development of new types of nodes that use these circuits to process data read from sensors [3].

1.2 Scope of the doctoral thesis

The main goal of the thesis is to make viable contributions to the evolution of sensor node networks using reconfigurable hardware circuits. This is a thorny issue because it attempts to use circuits known for their energy consumption in an area where consumption is an important factor.

The second goal is to find solutions to secure sensor nodes and communications inside the network and provide the best protection against attacks of any kind.

The validation of solutions is complemented by functional verification using various methods such as: estimating power consumption using specific instruments provided from manufacturers of reconfigurable circuits, simulation of hardware modules in the development phase and post-implementation testing using state-of-the-art measuring and control equipment.

1.3 Content of the doctoral thesis

The work is planned to gradually present the mechanisms and hardware modules developed, starting from a study of reconfigurable circuits and ending with the identification of a complete solution. After the introductory chapter, the thesis is organized as follows:

The second chapter of the thesis begins with a brief presentation of the evolution of reconfigurable circuits that highlights the technological progress reached today in the field of reconfigurable circuits. The presentation continues with the enumeration of the main types of reconfigurable circuits currently on the market and then the results of a unique comparative study, in terms of the large number of circuits included in the study and its orientation, are presented. After studying the operating parameters of these circuits, we proceed to the identification of those that meet the specific requirements of their use for the development of new sensor nodes. It will also present some methods to reduce energy consumption that must be followed by sensor node developers when implementing hardware modules that will be included in such nodes.

In chapter are presented three innovative sensor node architectures designed and physically built for use in modern sensor networks. I also present an innovative method of controlling node activities that aims to reduce node power consumption and a unique parameterizable simulation model for testing multisensor platforms.

Chapter four addresses security issues of sensor node networks. Within this chapter are presented innovative mechanisms aimed at protecting sensor nodes against cyber attacks. The first mechanism developed addresses the problem of generating random numbers on platforms that do not provide sufficient processing resources and the second presents a unique way that uses modern technologies to secure sensor networks. Also, is presented an implementation method that allows the use of powerful cryptographic algorithms in nodes with limited resources and a method that allows the use of sensor nodes in critical areas.

Chapter 5 shows a secure sensor node with high performance. In order to ensure the highest level of security, a new architecture is proposed, made with a single data processing unit, a cryptographic key management system and a data storage model with cryptographic mechanisms under the strict control of the user. For physical protection, in addition to various specific mechanisms, the model of a housing capable of providing a high level of protection against compromising radiation is also presented. This model has been tested in an accredited laboratory.

In the last chapter will be presented the results obtained during the doctoral study stage, the original contributions, the list of papers and some directions of further development deriving from the results presented within this thesis.

Chapter 2

Reconfigurable circuits used in the development of wireless sensor networks

2.1 Types of reconfigurable circuits

The logic resources of reconfigurable circuits have grown exponentially, while the manufacturing process has decreased in the same way, reaching in 2019 the value of 7nm, thus reducing power consumption and qualifying reconfigurable hardware circuits for their inclusion in the field of sensor node development.

2.1.1 CPLD circuits

CPLD circuits are generally used in applications such as: FPGA circuit programming, decoding, digital controllers, mobile applications.

2.1.2 FPGA circuits

FPGA circuits are integrated circuits made of silicon that can be reprogrammed so that they can replace almost any integrated circuit or even system. These circuits are made up of an array of complex logic blocks surrounded by routing paths that allow blocks to be interconnected programmatically.

2.2 Programming technologies

Table 2.1 [15] presents the main properties of the most commonly used programming technologies.

Tabelul 2.1 Proprietățile tehnologiilor de programare

	SRAM	FLASH	Anti-fuse
Reprogrammability	Yes	Yes	No
Volatility	Da	Nu	No
Area	High	Moderate	Low
In system programming	Yes	Yes	No
Fabrication process	CMOS	Flash	Polysilicon
Switch resistance	High	High	Low

2.3 Parameters and circuit series

In order to choose the right circuit in the process of designing sensor nodes, a number of parameters of all circuit families must be studied.

2.3.1 Parameters of reconfigurable circuits

The parameters of reconfigurable circuits can be grouped into two broad categories: intrinsic parameters characterizing the internal resources of reconfigurable circuits and extrinsic parameters characterizing circuits from an electrical, environmental and gauge perspective.

2.3.2 Reconfigurable circuit series

In order to identify the reconfigurable circuits that qualify for the development of sensor architectures, I conducted a unique comparative study in terms of the large number of circuits included and its orientation. This study ranks all families from major manufacturers of reconfigurable circuits according to reconfigurable logic resources relevant to sensor node development.

2.4 Reconfigurable circuits and multisensor systems

2.4.1 Applications of reconfigurable circuits

In this section, the results of the study on modern applications using reconfigurable circuits are summarized. In this study, the most significant applications using reconfigurable circuits and specifying the type of circuit used were chosen for each domain. The study represents the current state of play in applications with reconfigurable circuits.

2.4.2 Applications of multisensor systems

In this section are summarized the results of the study on modern applications of mutissensor systems.

2.4.3 Multisensor systems with reconfigurable circuits

If we intersect the areas where reconfigurable circuits and multisensor systems are applied, conclusions can be drawn about how reconfigurable circuits can be used to implement applications, platforms, and modules that can contribute to the development of modern multisensor systems.

2.5 Methods to reduce power consumption

For the design of sensor nodes, engineers are obliged to develop systems optimized for the lowest possible energy consumption. To minimize the power consumption of reconfigurable circuits, we must first carefully analyze the total power consumption.

2.5.1 Synthesis and routing constraint reduction method

The most practical method of reducing consumption is to use various synthesis and routing strategies offered by circuit manufacturers through development environments. These programs offer options to optimize consumption or logical resources used.

2.5.2 Reduction method by coding techniques and resource controll

This section presents programming techniques by which application developers in the field of sensor nodes based on reconfigurable circuits must use them to minimize the power consumption of the node.

Chapter 3

Node architectures based on reconfigurable circuits

3.1 Wireless sensor networks topology

Currently, there are several topologies of sensor networks, of which the most common are: point to point, star, tree and mesh.

Depending on the scope of application, wireless sensor networks can be mobile, static, "single" or "multi hop". They may also have one or more base stations.

3.2 Sensor node architectures

3.2.1 Base model

The basic architecture of a sensor node where one or more sensors are connected to a central processing unit via low-speed communication buses (e.g. SPI, I2C, UART, CAN, etc.) is presented [58].

3.2.2 Single Chip Full HW – SCFHW architecture

This architecture uses a single reconfigurable circuit that performs all the functions of the central processing unit.

Generally, at the level of a sensor node, the central processing unit reads data from the sensors at regular intervals, which it processes and then transmits to other nodes.

- **HWP-CPLD-2018 sensor node**

Starting from the information presented above, I designed and physically built two sensor nodes that have as processing unit only a reconfigurable circuit. The first node is based on a CPLD circuit.

For testing the node in a normal operating configuration, I mounted to the GPIO ports of the node a module containing a single ambient monitoring sensor and a low-power transmission module that transmits and receives data in the ISM-868MHz band. The internal hardware modules are controlled by the FSM that provides the following functions: it configures the node with operating parameters, reads data from sensors three times an hour and transmits it to the base station.

The experimental results are presented in tables 3.3 and 3.4.

Table 3.1 *Average current consumption per hour by frequency in normal operation of node HWP-CPLD-2018*

	Quiescent current (μA)	Fix current (μA)	The average current consumption per hour in steps that depend on the clock frequency				
			32.768KHz	**100KHz**	**1MHz**	**8MHz**	**50MHz**
CPLD	33	-	0.040 mA	0.1 mA	0.77 mA	5.6 mA	40 mA
OSCILLATOR	0.1÷10	-	0.9 μA	0.75 μA	3 mA	3 mA	19 mA
SENSOR	1	0.3	2.2 nA	732 pA	73 pA	9 pA	0.4 pA
Communication module	1	0.23	0.75 nA	0.25 nA	25 pA	10 pA	0.1 pA
TOTAL	33÷45	0.53	43.5μA	103.5 μA	3.77 mA	8.6 mA	59 mA

For the HWP-CPLD-2018 node I also tested the method with the activity management module. In this case, I obtained an average consumption of 43μA, resulting an operating time of approximately 6 years. The test platform is shown in figure 3.8.

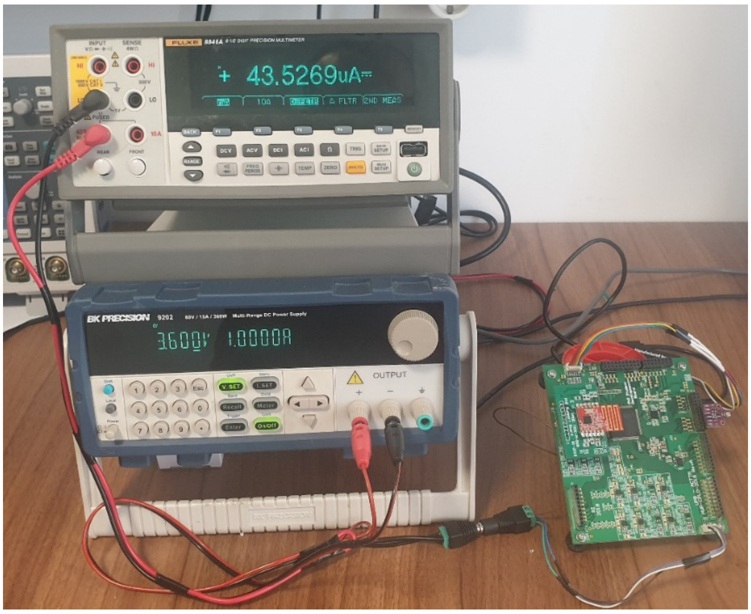


Figure 3.1 *HWP-CPLD-2018 node test platform*

Table 3.2 *Status of logical resources used for node HWP-CPLD-2018*

Resources Module	Macrocells (available 384)	Registers (available 384)
System controller	38 (9.9%)	34 (9%)
SPI controller	82 (21.3%)	96 (25%)
I2C controller	108 (28%)	80 (21%)
Activity management	7 (1.8%)	4 (1%)
Total	**235 (61%)**	**214 (56%)**

- **HWP-S6-2018 sensor node**

This sensor node uses as a processing circuit a Spartan-6 FPGA circuit that has much more logical resources than the CPLD circuit.

Figure 3.10 illustrates the sensor node which has connected to its ports two sensors for air quality monitoring and a communication module with SubGHz protocol for data transmission and reception in the ISM-858MHz band.

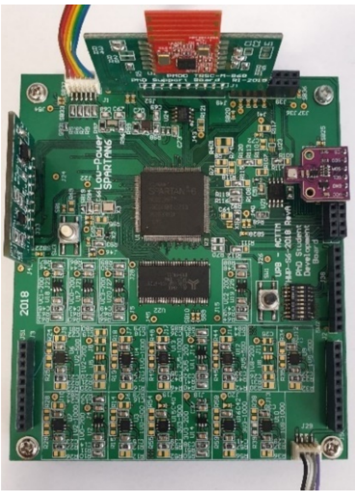


Figure 3.2 *HWP-S6-2018 sensor node*

The experimental results are presented in tables 3.5 and 3.6.

Table 3.3 *Average current consumption per hour by frequency in normal operation of node HWP-S6-2018*

	Quiescent current (µA)	**Fix current (µA)**	**The average current consumption per hour in steps that depend on the clock frequency**				
			32.768KHz	**100KHz**	**1MHz**	**8MHz**	**50MHz**
FPGA		-	5mA	5.1 mA	5.5mA	6 mA	50 mA
OSCILLATOR	0.1÷10	-	0.9 µA	0.75 µA	3 mA	3 mA	19 mA
SENSOR	1	0.3	2.2 nA	732 pA	73 pA	9 pA	0.4 pA
Communication module	1	0.23	0.75 nA	0.25 nA	25 pA	10 pA	0.1 pA
TOTAL		**0.53**	**5.009 mA**	**5.1007**	**8.5 mA**	**9 mA**	**69 mA**

În tabelul 3.6. este prezentată utilizarea resurselor logice. Așa cu se observa în tabel, pentru acest nod blocurile principale utilizează foarte puține resurse, mai puțin de 10% din totalul disponibil, restul de 91.5 rămân disponibile pentru a implementa module hardware care asigură funcții mai complexe.

Table 3.4 *Situația resurselor logice utilizate pentru nodul HWP-S6-2018*

Module / **Resources**	**LUT (5720 available)**	**Registers (11440 available)**
Controler sistem	198 (3.5%)	126 (1.1%)
Controler SPI	75 (1.3%)	69 (0.6%)
Controler I2C	177 (3%)	97 (0.85%)
Management activitate	38 (0.7%)	17 (0.15%)
Total	**488 (8.5%)**	**309 (2.7%)**

Table 3.7 presents several nodes available on the market or presented in scientific papers that have both microcontrollers and reconfigurable circuits as processing circuit.

Table 3.5 Exemple de noduri de senzori cu un singur circuit de procesare

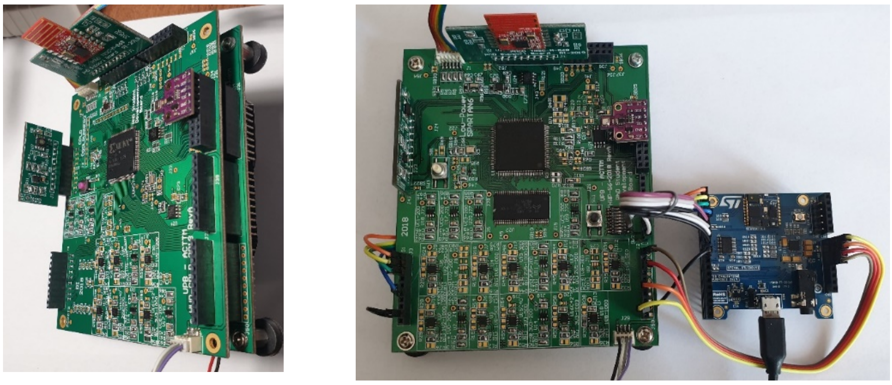
Name	**Processing circuit**	**Auxiliary components**	**Comm. module**	**Average power (mW)**	**Transmission power (mW)**	**Ref.**
HWP-CPLD-2018	XC2C384	SRAM–1Mb EEPROM–1Kb	MRF89XAM8A	**0.156**	25	-
HWP-S6-2018	XC6LX9-1L	SRAM–1Mb FLASH–16MB EEPROM–256Mb	MRF89XAM8A	**18.36**	25	-
Mica (Comercial)	ATMega128L	SRAM–4KB FLASH–128KB	CC1000	43.2	27.8	[67]
Telos–B (Comercial)	MSP430	SRAM–20KB FLASH–60KB	CC2420	6.5	76.5	[67]
Beagle Bone Black	ARM Cortex-A8	SDRAM–512MB FLASH–2GB	-	2200	-	[67]
Spartan–3E	XC3S1600E	-	-	2850		[67]
Spartan–3	XC3S2000	-	-	1000		[67]
Spartan–6	XC6SLX150	SDRAM–256Mb	-	462	-	[67]
Artix–7	XC7A35T	SRAM-1.8Mb	-	5000	-	[67]
Cyclone-II	EP2C70	-	ZigBee	221	-	[68]

3.2.3 Hybrid architectures

Within these architectures, reconfigurable circuits act as a coprocessor or hardware accelerator. The main functions of the node are provided by a circuit with low power consumption but insufficient processing resources. The configuration of the node, the data readings from the sensors and their transmission are executed by the low-power circuit, which can activate the reconfigurable circuit only when it is necessary to perform functions that require high processing power such as cryptographic functions, audio-video signal processing or even functions in the field of artificial intelligence.

To test the performance of this architecture, we developed two sensor nodes using the boards shown in the previous subsection, and a development board that has a microcontroller as its base circuit. In the first node the main circuit is the CPLD circuit of the HWP-CPLD-2018 board, while for the second we used as the main circuit the microcontroller of the STEVAL-STLKT01V1 board "SensorTile development kit".

For testing, I chose to use the FPGA circuit as a cryptographic accelerator, which has the role of encrypting using the AES-256 encryption algorithm in ECB mode the data received from the main circuit and then sending it back to be transmitted through the communication module. The two assembly are illustrated in figure 3.13.



a) b)

Figure 3.3 *Sensor nodes with hybrid architectures*

The use of logical resources for the Spartan 6 circuit after adding the cryptographic module is 36.7% LUT and 6.9% logical registers.

For determining power consumption I will use the same scenario and the same theater platform that I used to test nodes made using the SCFHW architecture.

Table 3.8 shows the experimental results at different frequencies of the two configurations for a single FPGA circuit activation in one hour.

Table 3.6 *Experimental results for sensor nodes with hybrid architectures*

Parametru	**Frecvență de lucru**		
	32.768KHz	**8MHz**	**50MHz**
Consum curent FPGA în modul activ	5 mA	10.8 mA	63 mA
Consum curent CPLD	56 µA	49.3 µA	50 µA
Consum curent µC (microcontroler)	75 µA	75 µA	75 µA
Total consum nod în configurație CPLD-FPGA	**61.6 µA**	**50.5 µA**	**52.2 µA**
Total consum nod în configurație µC-FPGA	**80.6 µA**	**82.8 µA**	**115.1 µA**

In Table 3.9. several nodes with similar architectures are shown, where the consumption of the FPGA circuit is given for the case when it operates all time.

Table 3.7 *Examples of sensor nodes with hybrid architectures*

Name	**Main circuit**	**FPGA**	**Main circuit power consumption (mW)**	**FPGA power consumption (mW)**	**Ref.**
HWP-CPLD-S6	XC2C384	XC6LX9-1L	0.049	39	-
HWP-µC-S6	STM32	XC6LX9-1L	0.075	39	-
ATMega-Igloo	ATMega	AGL600	382.94	12.36	[16]
Senito32-Igloo	AVR32	IGLOO	77.5	5.93	[16]
MSP-IGLOO	MSP430	AGL125	20	5	[16]

3.2.4 SoC architectures

These architectures are used for the development of high-performance nodes, where due to the high data flow, communication protocols used, and functions performed, the logic area of low-power FPGA circuits alone is not sufficient to ensure operation of node networks.

There are two types of nodes that can be used to develop these types of sensor nodes with "soft" and "hard" processing cores.

The HWP-S6-2018 board can be used to develop sensor nodes with SoC architectures, as the Spartan 6 circuit supports the implementation of soft processors.

To test the second type of node (with hard processor) we used the MiniZED development board illustrated in figure 3.16.

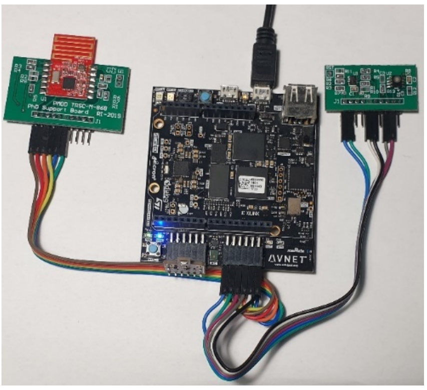


Figure 3.4 *Sensor node with MiniZed development board*

The experiments resulted in a consumption of **800mW** for the HWP-S6-2018 board and **1.8W** for the MiniZed board, both boards being powered from a 5V source. Table 3.10 presents the situation of use of logical resources.

Table 3.8 *Experimental results for sensor nodes with SoC architectures*

Sensor node	**LUT**		**Registers**		**Memory block**	
	Available	Utilizate	Available	Utilizate	Available	Utilizată
HWP-S6-2018	5720	2764 (48%)	11440	1899 (16%)	32 (16Kb)	12 (37%)
MiniZed	14400	2358 (16%)	28800	1756 (6%)	50 (36Kb)	0

3.3 Sensor node activity management

The power consumption of nodes can be considerably reduced if a hardware module is implemented at the node level that has the role of controlling the other hardware modules at macro level..

The module that does the management of activities is shown in Figure 3.18. To reduce power consumption, it uses two clock signal generators. The first low-frequency oscillator acts as a timer and is used to monitor and activate the other modules and the higher-frequency oscillator when needed.

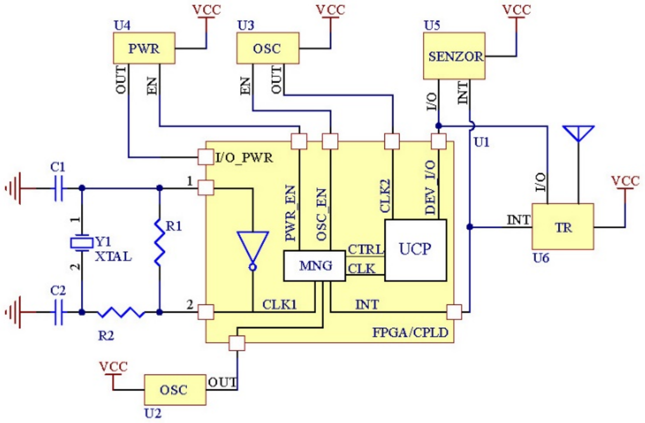


Figure 3.5 *Activity management system*

Using this method of activity management I obtained the results presented in table 3.11.

Table 3.9 *Experimental results obtained when using the module for activity management*

Node	**Without activity management**		**With activity management (32.768KHz/8MHz)**		
	Current consumption at 32.768KHz	Current consumption at 8MHz	Average consumption for 3 operations per hour	Average consumption for 10 operations per hour	Average consumption for 100 operations per hour
HWP-CPLD-2018	43.5µA	8.6mA	43.83µA	44.6µA	53.6µA
HWP-S6-2018	5mA	9mA	5.00057mA	5.0019mA	5.019mA

3.4 Parameterizable simulation model for testing multisensor architectures

Behavioural modelling and simulation is necessary for the theoretical characterisation of devices and systems prior to manufacture, or even before prototype, for several reasons including reduced costs and production time [83].

Since most of the sensors used are of the SiP type, I decided to develop a simulation model to model the SiP type sensors.

3.4.1 Simulation model structure

After studying the most representative sensor families, I have established a structure that can describe as accurately as possible all these sensors, even if they are of different types. This structure shown in Figure 3.20 contains all the mechanisms and parameters necessary for the proposed simulation model to enable researchers to test their data control or fusion modules as best as possible [84].

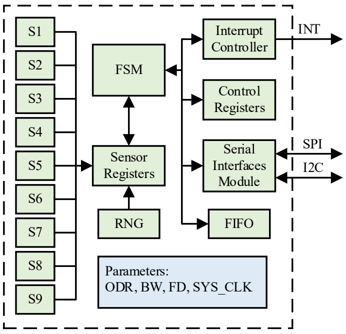


Figura 3.6 *Simulation model structure*

This model can be synthesized and implemented in the logical area of FPGA circuits using the Vivado development environment. Table 3.13 shows the use of FPGA resources.

Tabelul 3.10 *Use of logical resources in case of hardware implementation of the simulation model*

Modul hardware	**LUT**	**Registers**	**BRAM**
FSM	11	14	0
Serial interfaces	204	222	0
Interrupt controller	10	5	0
Internal registers	2	5	0
RNG	120	105	0
FIFO	2	2	2
Total	**349**	**353**	**2**

3.4.2 Simulation and implementation methods

The model was implemented and tested using two different methods. In the first method, shown in figure 3.21, the model was simulated using an HDL testbench test module that includes both the simulation model and serial communications hardware controllers.

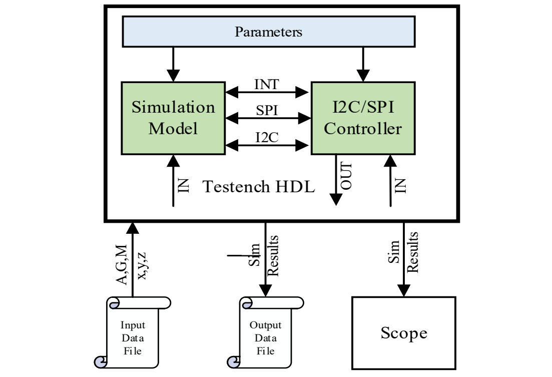


Figure 3.7 *Simulation platform diagram*

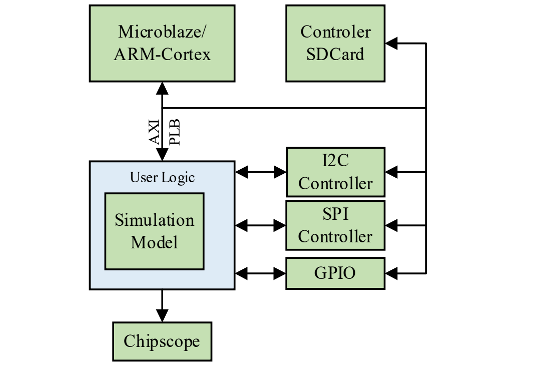


Figure 3.8 *Hardware testing diagram*

In the second method, shown in figure 3.22, the model was emulated in hardware using embedded methods that include both hardware and software tools.

3.5 Low-Power Wireless Temperature Sensor for Health Monitoring

In this section is presented the concept and implementation of a wireless temperature sensor for monitoring patients with reconfigurable hardware devices as an alternative to using classic devices. The system was implemented using development boards and then implemented on the HWP-CPLD-2018 platform.

The proposed system can be powered using different types of batteries or accumulators with voltages ranging from 3.6 V - 5 V.

Since the CPLD and sensor can work with the frequency of 32.768KHz, we used only one oscillator. Table 3.14 shows the power consumption for each component and the total power consumption of the node [88].

Table 3.11 *Node current consumption in different operating modes*

Component	Stand-by	Active mode
CPLD	43 µA	43 µA
MAX30205	1.65 µA	600 µA
MRF89XAM8A	0.1 µA	1.3 mA
TCR2LF18LMCT	0.1 µA	0.1 µA
TCR2LF33LMCT	0.1 µA	0.1 µA
SIT1532AC-J5-DCC-32.768E (OSC)	0.1 µA	0.1 µA
24LC01B/SN (EEPROM)	1 µA	3 mA

Since during a 10-minute cycle, the system performs 5 reading operations and one transmission, and taking into account the consumption of the CPLD circuit and regulators, then it results in an average consumption per hour of about **46.38 µA**. For a battery with a capacity of 1000 mAh, the system can work for about 3 years without changing the battery [88].

Chapter 4

Sensor node security

4.1 Security algorithms

Table 4.1 shows the main implemented cryptographic algorithms together with the resources they use.

Table 4.1 *Resource utilization after implementation of the main encryption algorithms*

Algorithm	AES 128	AES 256	AES GCM 128	Twofish 256	Camelia 256	ECC 163	Present (LC) 80
Reosurce (LUT)	638	1453	2684	3551	7617	25394	153

4.2 Random number generator

n this section I present a method that uses node sensors as a noise source to generate random numbers. For evaluation, I have implemented two platforms: the first is based on a microcontroller and the second is based on an FPGA circuit..

For testing the extracted data, I used a NIST accredited methodology that includes a number of 10 estimators that are calculated for datasets of at least 1000000 samples.

4.2.1 Entropy evaluation using microcontroller platforms

For the experiments performed on the microcontroller platform, I used the B-L475E-IOT01A1 development board manufactured by STMicroelectronics. This board is developed as an IoT node and is equipped with a microcontroller and a series of IMU-type sensors and environmental parameters monitoring.
The board is equipped with the following sensors:

Entropy analysis was performed through several experiments.

- First Experiment
- Purpose: entropy evaluation of IMU sensors in two use cases: stationary and moving;
- Results: Table 4.2 shows the entropy values for the three sensors for each axis (X,Y and Z) in the two cases of use [96].

Tabelul 4.2 *Estimated entropy values for the IMU sensor*

Sensor	**Stationary**			**Moving**		
	X axis	Y axis	Z axis	X axis	Y axis	Z axis
Accelerometer	0.46	0.41	0.30	0.82	0.82	0.82

Gyroscope	0.25	0.36	0.26	0.53	0.54	0.39
Magnetometer	0.47	0.46	0.62	0.56	0.48	0.59

➢ Second experiment:

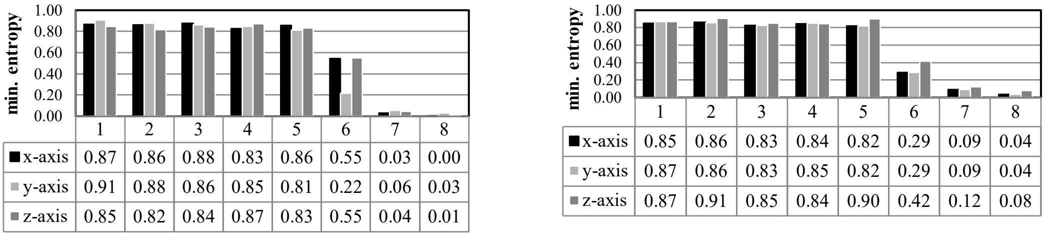
- Purpose: entropy assessment of sensors for monitoring environmental parameters in two use cases: indoor and outdoor;
- Results: Table 4.3 shows the entropy values for the four sensors in the two cases of use [96].

***Tabelul 4.3** Estimated entropy values for the environmental monitoring sensor*

Place	**HTS221**		**LPS22HB**	
	Humidity	Temperature	Air pressure	Temperature
Inside	0.0321	0.0041	0.3067	0.0004
Outside	0.0405	0.0078	0.3028	0.0019

➢ Third experiment

- Purpose: identifying the bit positions that contribute the most to the entropy of the extracted data;
- Results: Figures 4.1 show the entropy values for the accelerometer [96].



(a) (b)

***Figura 4.1** Entropy values for each bit of data read from the accelerometer:*

(a) stationary, (b) moving

For the other sensors the results are similar, from which the conclusion is drawn that the first 4 bits contribute the most to the entropy value.

4.2.2 Entropy evaluation using reconfigurable circuits

To determine the entropy values using reconfigurable hardware circuits we used the platform illustrated in figure 4.5. The main component of this platform is the CMOD-A7 development board produced by Digilent. The board is equipped with a circuit FPGA Artix7 - XC7A15T-1CPG236C.

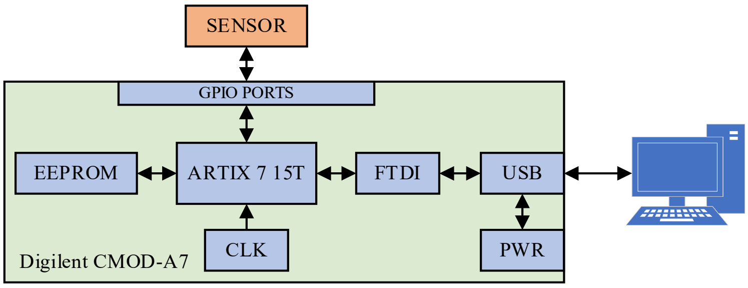


Figura 4.2 *Block diagram of the platform with reconfigurable circuits used for entropy evaluation*

All hardware modules were implemented using the Vivado 2018.3 development environment. Table 4.4 [58] shows the utilization of logical resources after implementation.

Table 4.4 *Logical resource utilization for the test platform with reconfigurable circuits*

Controller	LUT		Registers	
	Used	Utilization (%)	Used	Utilization (%)
SISTEM	14	0.13	11	0.05
SPI	42	0.40	98	0.47
IIC	139	1.34	119	0.57
UART	49	0.47	77	0.37

To perform the tests, I have generated datasets of 1000000 samples. The same test suite was used.

- First experiment

Evaluation of the entropy of data extracted from the IMU sensor.

Table 4.5 *Entropy values for the IMU sensor*

Sensor/Configuration parameters	**x axis**	**y axis**	**z axis**
Accelerometer: ODR=1333, Fs=16, Delay=3500	0.59	0.52	0.51
Gyroscope: ODR=1333, Fs=16, Delay=3500	0.45	0.44	0.4
Magnetometer: ODR=1000, Fs=8, Delay=1500	0.5	0.45	0.58

- Second experiment

For this stage we used the same sensors with the same configuration as in the first experiment. The only difference was that in this experiment two readings were taken from two sensors in the same cycle, the bits of data extracted from the sensors were concatenated using the following relationship:

$$H\{a,b\} = \{b[3:0]; a[2:0]; a[4]\} \tag{4.1}$$

The experimental results are presented in table 4.6 [58].

Table 4.6 *Entropy values for the IMU sensor obtained by applying the concatenation relation*

Sensor/Configuration parameters	**H{x,y}**	**H{x,z}**	**H{y,z}**
Accelerometer: ODR=1333, Fs=16, Delay=3500	**0.9**	0.87	0.72
Gyroscope: ODR=1333, Fs=16, Delay=3500	0.74	0.68	0.51
Magnetometer: ODR=1000, Fs=8, Delay=1500	0.58	0.7	0.68

- Third experiment 3

The MEMS microphone and air quality monitoring sensor were used in this experiment. For this case, the entropy was analyzed in three cases: indoor, outdoor and with pollution source.

The experimental results are presented in table 4.7 [58].

***Table 4.**7 Entropy values for microphone and air quality monitoring sensor*

Sensor	**Case I**	**Case II**	**Case III**
Microphone	0.3	0.47	0.6
Air quality monitoring sensor	0.32	0.5	0.55

4.3 Securing sensor networks with blockchain technology

Blockchain technology can be used to secure sensor networks with FPGA circuits using SoC architectures to which I have added two modules that have the role of mining and validating blocks in the blockchain.

Table 4.8 presents the experimental results.

The experimental data shows that the HWP-S6-2018 node using the XC6SLX9 circuit can be used to implement blockchain technology to secure data.

***Table 4.8** Experimental results obtained from the implementation of the security architecture through blockchain technology*

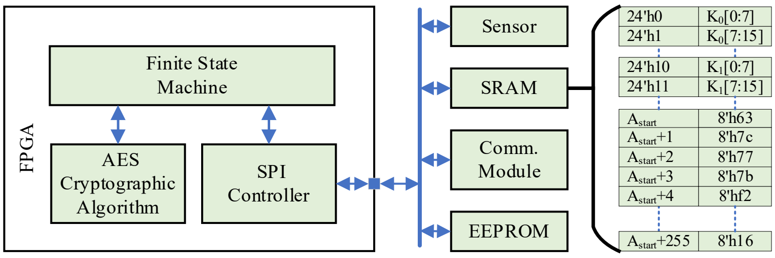
FPGA Series	**FPGA Circuit**	**Circuit Type**	**Logic Reources (LUT)**	**Numer of SHA2 module s**	**Max. Freq.**	**Speed Gbit/sec**	**Iccq (mA)**
Spartan 6	XC6SLX9	FPGA	5720	3	69.46	1.66	4.9
Spartan 6	XC6SLX150	FPGA	92152	78	69.46	43.44	63
Artix 7	XC7A12T	FPGA	8000	5	138.7	5.5	51
Artix 7	XC7A200T	FPGA	134600	115	138.7	127.6	268
Zynq-7000	XC7Z007S	FPGA SoC	14400	12	138.7	13.3	172
Zynq-7000	XC7Z020	FPGA SoC	53200	46	138.7	51.3	330
Kintex 7	XC7K70T	FPGA	41000	34	151.5	41.2	208
Kintex 7	XC7K480T	FPGA	298600	257	151.5	311.4	840
Zynq-7000	XC7Z030	FPGA SoC	76600	66	151.5	79.9	437
Zynq-7000	XC7Z100	FPGA SoC	277400	240	151.5	290.8	1095
Virtex 7	XC7V585T	FPGA	364200	314	196.1	492.6	1597
Virtex 7	XC7VX1140	FPGA	712000	473	196.1	966.3	3698

4.4 Method of implementing cryptographic algorithms in nodes with insufficient hardware resources

In order to meet the requirements of implementing high performance cryptographic algorithms on less powerful reconfigurable circuits, we have developed an innovative implementation method that significantly reduces the usage of the internal logic area.

To relieve the reconfigurable circuit of this task, we used an external SRAM memory to store at successive addresses the round keys previously derived from the cryptographic key and the $b_{n,n}$ values of the S-Box table.

For testing the method I used node HWP-S6-2018. The diagram of the test platform is shown in figure 4.10.



24'h0	K_0[0:7]
24'h1	K_0[7:15]
24'h10	K_1[0:7]
24'h11	K_1[7:15]
A_{start}	8'h63
A_{start}+1	8'h7c
A_{start}+2	8'h77
A_{start}+3	8'h7b
A_{start}+4	8'hf2
A_{start}+255	8'h16

***Figure 4.3** Block diagram of the test platform*

Table 4.9 presents the results of the implementation of the AES-128/256 algorithm both in the optimized version for speed and for the variant optimized to be used in nodes with limited logical resources.

***Tabelul 4.9** Logical resources utilization*

Algorithm	**Speed optimization**			**Optimization for area reduction**		
	Cycles	**LUT**	**Registers**	**Cycles**	**LUT**	**Registers**
AES-128	10	638(11%)	281(2%)	8560	254(4%)	269(2%)
AES-256	14	1543(26%)	425(3%)	11984	364(6%)	416(3%)

The usage data presented in the table is given for the algorithm only and does not include resources used by the SPI controller and FSM.

4.5 Secure sensor node for medical parameters monitoring

In order to demonstrate the possibility of using FPGA circuits to implement wearable devices, I have developed a unique sensor node due to its mobility, scope, and use of reconfigurable circuits as the main processing circuit. The main purpose of this sensor node is to monitor people's biomedical parameters during exercises that involve intense physical effort (e.g. monitoring soldiers' parameters during combat missions).

The proposed system consists of one or more wearable sensor nodes that measure human biomedical parameters and then send the collected data to a base station to be analyzed by qualified personnel. The domain in which this sensor is used imposes the need to secure communication between the nodes and the base station. The monitored parameters are: body temperature, blood oxygen level, heart rate, respiratory rate, movement and position of the subject.

To secure communication between the base station and sensor nodes, I chose the AES-256 algorithm because the ratio of cryptographic strength to resources used is the best.

For implementation we used node HWP-S6-2018 presented in chapter 3 to which we connected the sensors listed above. The MiniZed board to which we connected the TSRC-ST-868 module performs the functions of the base station.

The Spartan 6 circuit operates with 32.768KHz in timer mode and 8MHz in active mode. Table 4.11 shows current consumption in both operating modes, average energy consumption for 25 cycles per second (reading data from the three sensors and data transmission) and total node consumption.

Table 4.10 Average power consumption of secure node

Circuit	Consum în modul timer	Consum în modul activ	Consum mediu
XC6SLX9-L1	5.1 mA	10 mA	5.15 mA
AFE9400	0,1 µA	20 mA	30 µA
MAX30205	1.65 µA	600 µA	18 µA
MAX86141	0.6 µA	31 mA	91 µA
TSRC-ST-868	0.1 µA	22 mA	9 mA
Total			14.3 mA

We checked the correct operation of the system by displaying data in the ILA window, before encryption, after encryption and at reception.

Utilizarea resurselor după implementare este prezentată în tabelul 4.11.

Tabele 4.11 The utilization of resources after implementation is shown in Table 4.11

Module	LUT	Registers
System Controller	320	256
SPI Controller	75	69
I2C Controller	177	97
Criptare-Decriptare Module	3122	812
Total	**3694 (64%)**	**1234 (10%)**

The average consumption of the base station is 280 mA. But in this configuration the base station has acess to high capacity power source. The number of resources used at the station level is approximately equal to that of the node.

Chapter 5

Secure sensor node with high processing performance

This chapter presents original methods and mechanisms that can be integrated into sensor node architectures with high processing performance. The presented mechanisms have the role of interconnecting the node modules while ensuring high processing speeds and increasing the security level of the node.

5.1 Node architecture

The main components of the architecture are shown in Figure 5.1. The presented architecture contains all the necessary modules to achieve high processing performance and increased security against computer attacks.

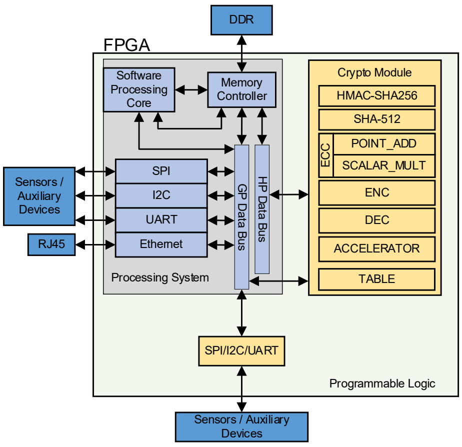


***Figure 5.1** Sensor node architecture with high processing performance*

In order to ensure performance and security requirements, we implemented at the node level using HDL programming languages the Crypto hardware module containing the most used cryptographic mechanisms and a hardware accelerator.

Table 5.1 shows the resources utilization after the implementation of the modules.

The modules were implemented and tested using an experimental The programmable area has 46200 LUT, 92400 registers and 95 RAMB36 modules. During tests the maximum current consumption was **300mA**.

Table 5.1 *Resource utilization status following high performance node deployment*

Module	LUT	Registers	BRAM
HMAC-SHA256	2152	1910	0
SHA-512	3810	2244	0
ECC	7949	7507	0
ENC-DEC	7312	5559	16
ACCELERATOR	1671	1988	2
TABELS	753	1232	8
AUXILIARY BLOCKS	6421	8980	2
Total	**30068**	**29420**	**28**

5.1.1 High speed hardware accelerator

This hardware component allows multiple specialized modules to be connected to a single HP port on the processor using a single block AXI_DMA. The accelerator blocks and connections between them are shown in figure 5.3.

The CAM block is a hardware module that allows quick determination of the position of the input data, and the KEY TABLE block is a BRAM memory with two ports that allow two different hardware modules to control the memory.

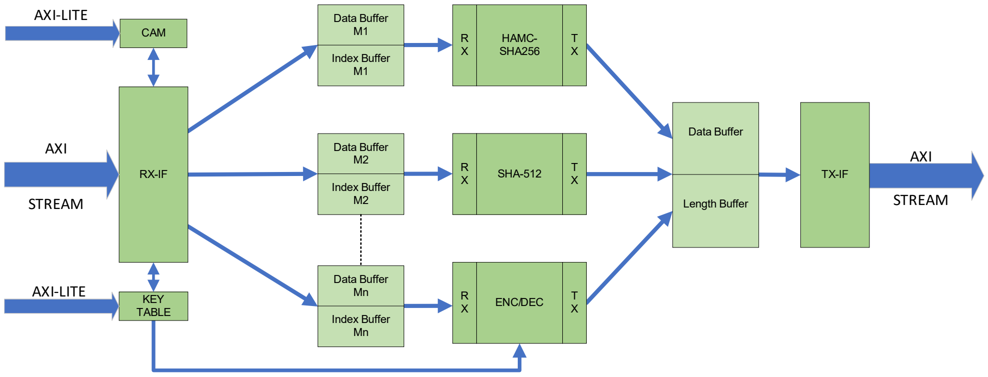


Figure 5.2 *Internal structure of the accelerator*

The INDEX block which indicates the path consists of: MS indicates the sub-module to be used, ADDR is the address of the source node, NM is a flag indicating that the address was not found in the CAM and LEN represents the length of the packet to be processed.

5.2 Data transfer methods

In this section are presented a series of useful information resulting from innovative tests aimed at identifying the optimal solution for data transfer between the processor and the hardware modules used to process this data.

To test these methods in a scenario as close to the real one as possible, we chose the processor-hardware accelerator configuration (AES256) because it is the most used. [108]

After studying several protocols and specifications available to transfer and receive data from or to the processor, we considered that only three of them were worth considering to be presented.

The methods chosen are: PowerPC440 DMA, PowerPC440 APU şi Zynq-7000 DMA- HP.

The proposed transfer methods were implemented and tested using ML507 and MiniZed development boards.

The experimental results are shown in Figure 5.11.

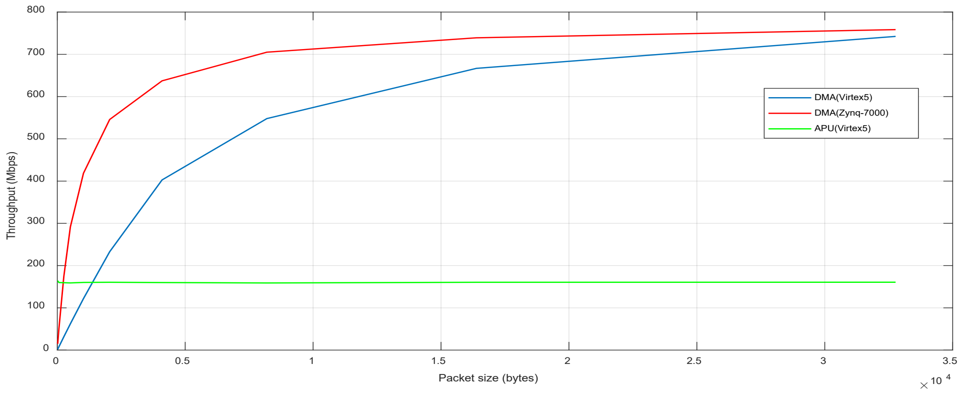


***Figure 5.3** Data transfer speed depending on packet length for the three transfer methods*

5.3 Cryptographic key establishment mechanism

In this section is presented an original mechanism for establishing cryptographic session keys, developed during the doctoral study that can be successfully used to secure communications in sensor networks with star topologies.

The session key is established between the two entities through message exchanges that establish a key index that is equivalent to a memory address in flash memory.

5.4 FIPS Level 4 Protection Mechanism

In cases where security requirements are high, it is necessary to implement additional security mechanisms at node level to ensure real-time monitoring of supply voltages and temperature inside the reconfigurable circuit. To meet these extensive safety requirements, we have developed an innovative hardware module that uses dedicated FPGA circuit modules to continuously monitor circuit operating parameters and generate alarm signals when user-defined thresholds are exceeded [113].

The module generates alarm signals when the monitored quantities are outside the specified thresholds.

5.5 Protection of sensor nodes against compromising radiation

In the case of sensor nodes that are part of sensor networks aimed at monitoring critical targets, protection requirements against compromising radiation are also formulated. In this section is presented an innovative method by which engineers can considerably reduce the implementation time of compromising radiation protection mechanisms by using PCB models of sensor nodes and ANSYS HFSS simulation program. By this method the effectiveness of shielding solutions can be determined before their realization in mechanical processing workshops.

To test the effectiveness of the solution, we chose the sensor node HWP-S6-2018.

After validating the model through simulation, we moved on to the next stage where the housing was physically made and then the components of the sensor node were mounted. After the node was assembled and functionally tested, it underwent testing in an accredited laboratory to measure the level of compromising emissions.

5.6 Data storage sodel with user sontrolled Cryptographic Mechanisms

This section addresses the issue of secure cloud storage of data from sensor nodes [16][17][18] and proposes a system for securing stored data through encryption that the user controls cryptographic keys and their lifecycle and has a choice between different encryption methods according to their requirements [19].

The secure cloud storage solution developed is also based on the encryption scheme at the client, but allows the user to do so with complete control over both encryption keys and encryption algorithms they want to use to protect data. To achieve the desired level of trust, a zero-knowledge architecture is also proposed, in which data and keys are not known by the cloud storage system.

Chapter 6

Conclusions

Concluding, this thesis gradually presents a series of original solutions that ultimately led to the implementation of sensor nodes with a high level of security and high processing performance, but with energy efficiency that allows their power supply from batteries or accumulators and installation in isolated areas Testing these solutions has yielded outstanding results in terms of energy efficiency and processing power.

6.1 Results

In each chapter of this thesis, viable solutions have been presented that can contribute to the development of wireless sensor networks using nodes based on reconfigurable circuits. Each solution presented has been implemented and tested, obtaining results that validate them for use not only in the laboratory but also in the real world.

6.2 Original contributions

During the doctoral study, innovative contributions can be synthesized as follows:

1. Conducting a comparative study according to parameters that are relevant in the field of sensor nodes. This study includes all reconfigurable circuits produced by major manufacturers of such circuits;
2. Design and manufacture of sensor node HWP-CPLD-2018 based on a CPLD circuit for data processing;
3. Design and manufacture of HWP-S6-2018 sensor node with a low-power Spartan 6 circuit for data processing;
4. Implementation and testing of SCFHW architectures that use a single reconfigurable circuit to process sensor data and that, when compared to other architectures, rank them as optimal consumption-related architectures;
5. Implementation and testing of hybrid architectures that use multiple reconfigurable circuits or combine them with microcontrollers to obtain high processing resources while ensuring low power consumption. By comparing with other similar nodes and balancing the ratio of energy consumption to logical resources, it results that the architectures and hardware modules presented in this thesis have the best performance;

6. Implementation and testing of a SoC architecture that can be used in networks of sensor nodes providing huge processing resources by connecting reprogrammable areas to "hard" or "soft" processors;
7. Development of a hardware mechanism for activity management within sensor nodes that considerably reduces energy consumption;
8. Implementation of a parameterizable model for simulation of multisensor architectures. The model offers the possibility of simulating or emulating SiP sensors during the development of modules that control or process data in multi-sensor systems [A9];
9. Implementation and testing of a low-power wireless temperature sensor node for health monitoring [A1];
10. Development of a microcontroller test platform for evaluating the entropy of sensor data. Using NIST methodologies, we validated the method and identified sensors that can generate enough entropy to be used to generate random numbers [A7];
11. In order to demonstrate the superiority of reconfigurable circuits in the process of collecting sensor data, we implemented a test platform based on an FPGA circuit. With this platform, only sensors validated with the platform from the previous point were tested [A8];
12. I have demonstrated the possibility of using blockchain technology to secure networks of sensor nodes [A4];
13. I have developed a method for implementing complex cryptographic algorithms on reconfigurable circuits that do not have many logical resources available;
14. Combining the solutions proposed above, I have implemented a secure wireless system based on reconfigurable devices for human biomedical parameters monitoring [A6];
15. Implementation of a hardware module that allows multiple accelerators to connect to a single HP port of processors, thereby reducing logical resources used to deploy nodes that ensure high processing performance;
16. I have developed a quick method of assigning cryptographic keys according to the address of the node where the package comes from. Using this method, key assignment is done in parallel with the processing of data in the package, the keys being available when the decryption process is started;
17. The implementation and comparison of several data transfer methods in embedded systems is a contribution because through this study we have demonstrated that in the case of using less powerful FPGA circuits that can be used in the field of sensor nodes, it is possible to achieve transfer speeds as high as when using much more efficient circuits [A2];
18. Development of a cryptographic key establishment protocol ensuring secure communication between nodes of a sensor network;
19. Implementation of a dynamically configurable mechanism that uses sensors inside the FPGA circuit to provide FIPS level 4 protection [B1];
20. Design, simulation, realization and validation by testing in an accredited laboratory of a housing that provides protection of the sensor node against

compromising radiation [A5]. My contribution to the realization of the housing consisted in generating with the Altium Designer program the 3D model of the sensor node containing the physical and electrical characteristics of the node, necessary for the electromagnetic simulation performed with the ANSYS HFSS program plus the coordination of the team that simulated and tested the housing;

21. Development of a data storage model with cryptographic mechanisms under strict user control [A3].

6.3 List of original works

6.3.1 ISI indexed scientific articles

[A1] I. Rădoi, L. Dobrescu, S. Pașca, Low-Power Wireless Temperature Sensor for Health Monitoring, The 13th International Symposium on Advanced Topics n Electrical Engineering, DOI: 10.1109/ATEE.2017.7905036, ISBN:978-1-5090-5160-1, ISSN: 1843-8571, WOS:000403399400050, 2017

[A2] I. Rădoi, F. Răstoceanu, D. Hritcu, Data Transfer Methods In FPGA Based Embedded Design For High Speed Data Processing Systems, International Conference on Communications (COMM), DOI: 10.1109/ICComm.2018.8484792, , ISBN978-1-5386-2350-3, ISSN1550-3607, WOS:000449526000098, 2018

[A3] S.C. Arseni, I. Rădoi, S.B. Maluțan, M. Lazar, R.I. Dragomir, A Data Storage Model with User Controlled Cryptographic Mechanisms for Data Processing, International Conference on Communications (COMM), DOI: 10.1109/ICComm.2018.8484804, ISBN978-1-5386-2350-3, ISSN1550-3607, WOS:000449526000099, 2018

[A4] F. Răstoceanu, I. Rădoi, FPGA based architecture for securing IoT with blockchain, International Conference on Speech Technology and Human-Computer Dialogue (SpeD), DOI: 10.1109/SPED.2019.8906595, ISBN 978-1-7281-0984-8, WOS:000571718700023, 2019

[A5] A. Boteanu, F. Răstoceanu, I. Rădoi, C. Rusea, Modeling and simulation of electromagnetic shielding for IoT sensor nodes case, International Conference on Speech Technology and Human-Computer Dialogue (SpeD), DOI: 10.1109 / SPED.2019.8906621, ISBN 978-1-7281-0984-8, WOS:000571718700030, 2019

[A6] I. Rădoi, L. Dobrescu, S.C. Arseni, F. Roman, D. Dobrescu, S. Halichidis, Secure Wireless System Based on Reconfigurable Devices for Human Biomedical Parameters Monitoring, Romanian Journal of Military Medicine, Vol. CXXII, No. 3, ISSN 1222-5126, eISSN 2501-2312, WOS:000506183500020, 2019

[A7] F. Răstoceanu, B.I. Ciubotaru, I. Rădoi, V.M. Constantin, Extended analysis using NIST methodology of sensor data entropy, U.P.B. Scientific Bulletin, Series C, Vol. 83, Iss. 2, ISSN 2286-3540, eISSN 2286-3559, WOS:000692193500010, 2021

[A8] I. Rădoi, L. Dobrescu, C. Rusea, Random number generation in hardware reconfigurable wireless sensor nodes, The 13th international symposium on advanced topics in electrical engineering, DOI: 10.1109 ATEE 58038.2023. 10108373, under indexing WOS, 2023

[A9] I. Rădoi, L. Dobrescu, C. Rusea, HDL simulation model for testing and verification of "system in package" sensor architectures, The 13th international symposium on advanced topics in electrical engineering, DOI: 10.1109 ATEE 58038.2023 .10108271, under indexing WOS, 2023.

6.3.2 BDI indexed scientific articles

[B1] I. Rădoi, L. Dobrescu, Real-time FPGA monitoring hardware module using on-chip sensors, Innovation and Sustainability in Technology, Business and Education, ISSN 2501-6095, 2017.

6.4 Future work

With the advent of new circuits and new processing requirements, new techniques can be developed to reduce energy consumption that allow placement in remote areas and longer operation.

The information presented in the first part of Chapter 3 is the starting point for the development of new types of sensor nodes based on reconfigurable hardware circuits. Maintaining low energy consumption can be done by improving the activity management module presented in Chapter 3. The simulation model presented can be completed by adding new functionalities specific to the new SoC sensors.

As security threats to nodes and sensor networks will constantly evolve, the development of new security mechanisms to counter these threats becomes mandatory.

The entropy sources presented can be used in conjunction with hardware modules that use distributed databases to develop sensor nodes which, due to their high degree of security, can be used in many applications where data security is essential.

The hardware modules presented in Chapter 5 can be used in further developments of sensor nodes with high processing capabilities.

References

[1] A. Malhotra, *Intensive Review on Hybrid Combination of WSN and IoT and its Impact*, 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, ISBN:979-8 -3503-9926-4, 2023.

[2] Mordor Intelligence, *Field Programmable Gate Array (FPGA) Market Size & Share Analysis - Growth Trends & Forecasts*, https://www.mordorintelligence.com/industry-reports/field-programmable-gate-array-fpga-market, 2020.

[3] A. Diaz-Perez, M. Morales-Sandoval, and C. Lara-Nino*, Use of FPGAs for enabling security and privacy in the IoT: features and case studies, FPGA Algorithms and Applications for the Internet of Things*, chapter 2, P. Sharma and R. Nair, Eds., pp. 26–45, IGI Global, 2020.

[4] P. Babu, E. Parthasarath, *Reconfigurable FPGA Architectures: A Survey and Applications*, Journal of The Institution of Engineers, 2020.

[5] A. Piedra, A. Braeken, A. Touhafi, *Sensor Systems Based on FPGAs and Their Applications: A Survey*, Sensors Journal, ISSN 1424-8220, 2012.

[6] I. Rădoi, L. Dobrescu, C. Rusea, *Random number generation in hardware reconfigurable wireless sensor nodes*, The 13th international symposium on advanced topics in electrical engineering, 2023.

[7] D.M. Pham, S.M. Aziz, *FlexiS-A Flexible Sensor Node Platform for the Internet of Things*, Sensors Journal, 2021.

[8] T.Sripriya, V.Jeyalakshmi, *Simulation of an Optical MEMS Pressure Sensor*, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN 2278 – 8875, 2014.

[9] I. Rădoi, L. Dobrescu, C. Rusea, *HDL simulation model for testing and verification of "system in package" sensor architectures,* The 13th international symposium on advanced topics in electrical engineering, 2023.

[10] I. Rădoi, L. Dobrescu, S. Pașca, *Low-Power Wireless Temperature Sensor for Health Monitoring*, The 13th international symposium on advanced topics in electrical engineering, 2017.

[11] F. Răstoceanu, B.I. Ciubotaru, I. Rădoi, *Extended analysis using nist methodology of sensor data entropy*, U.P.B. Scientific Bulletin, Series C, Vol. 83, Iss. 2, ISSN 2286-3540, 2021.

[12] I. Rădoi, L. Dobrescu, S.C. Arseni, F. Răstoceanu, F.M. Roman, *Secure Wireless System Based on Reconfigurable Devices for Human Biomedical Parameters Monitoring*, Romanian Journal of Military Medicine, Vol. CXXII, No. 3, 2019.

[13] I. Rădoi, F. Răstoceanu, D. Hrițcu, *Data Transfer Methods In FPGA Based Embedded Design For High Speed Data Processing Systems*, International Conference on Communications COMM, 2018.

[14] I. Rădoi, L. Dobrescu, *Real-time FPGA monitoring hardware module using on-chip sensors*, Innovation and Sustainability in Technology, Business and Education, 2017.

[15] A. Boteanu, F. Răstoceanu, I. Rădoi, C. Rusea, *Modeling and simulation of electromagnetic shielding for IoT sensor nodes case*, International Conference on Speech Technology and Human-Computer Dialogue (SpeD), 2019.

[16] T. Syamsundararao, D. Aswani, K. L. Prasad, G. R. Babu, B. Samatha, N. Karyemsetty, *Integrated Cloud Security for Data Storage and Access*, International Conference on Edge Computing and Applications, 2022.

[17] R. Eswari, A. Vamshi, M. S. Sultan, *An Efficient Data Storage Technique for User Files in Cloud*, International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security, 2023.

[18] H. Kui, X. Yi, *Secure Internet of Things in Cloud Computing via Puncturable Attribute-Based Encryption With User Revocation*, Internet of Things Journal, Volume 11, Ed. 2, 2024.

[19] S.C. Arseni, I. Rădoi, S.B. Maluțan, M. Lazar, R.I. Dragomir, *A Data Storage Model with User Controlled Cryptographic Mechanisms for Data Processing*, International Conference on Communications (COMM), 2018