UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE POLITEHNICA BUCUREŞTI

Școala Doctorală de Electronică, Telecomunicații și Tehnologia Informației

Decizie nr. 49 din 20.05.2024

REZUMAT TEZĂ DE DOCTORAT

Ing. Ionuț RĂDOI

CONTRIBUȚII LA PROCESAREA DATELOR ÎN SISTEME MULTISENZOR FOLOSIND CIRCUITE HARDWARE RECONFIGURABILE

CONTRIBUTIONS TO DATA PROCESSING IN MULTISENSOR SYSTEMS USING RECONFIGURABLE HARDWARE CIRCUITS

COMISIA DE DOCTORAT

Prof. Dr. Ing. Mihai CIUC Universitatea Națională de Știință și Tehnologie Politehnica București	Președinte
Prof. Dr. Ing. Lidia DOBRESCU Universitatea Națională de Știință și Tehnologie Politehnica București	Conducător de doctorat
Prof. Dr. Ing. Daniela TĂRNICERIU Universitatea Tehnică "Gheorghe Asachi" din Iași	Referent
Prof. Dr. Ing. Radu Mihnea UDREA Universitatea Națională de Știință și Tehnologie Politehnica București	Referent
CSI Dr. Ing. Mihail-Liviu COȘEREANU Institutul Național de Cercetare-Dezvoltare Aerospațială	Referent

BUCUREŞTI 2024

Cuprins

Capitolul 1

Introducere

1.1 Prezentarea domeniului tezei de doctorat

Progresele din ultimii ani făcute în domeniul circuitelor electronice și a rețelelor de date, au permis utilizarea rețelelor de senzori fără fir (WSN) la scară largă și au determinat dezvoltarea unor noi generații de rețele care oferă avantaje copleșitoare comparativ cu rețelele wireless dezvoltate în trecut și au schimbat modul în care trăim [1].

Concomitent cu evoluția rețelelor de senzori, este de așteptat ca piața circuitelor reconfigurabile să atingă valoarea de 11,7 miliarde de dolari în 2027, după ce în 2020 a fost evaluată la 5,7 miliarde [2].

Pentru a se adapta la cererea crescută de dispozitive portabile, companiile producătoare de circuite reconfigurabile au introdus în portofoliul lor și circuite cu consum redus de energie. Capabilitatea de procesare în paralel al datelor califică circuitele reconfigurabile pentru a fi folosite la dezvoltarea unor noi tipuri de noduri care folosesc aceste circuite pentru procesarea datelor citite de la senzori [3].

1.2 Scopul tezei de doctorat

Scopul principal al tezei constă în aducerea unor contribuții viabile pentru evoluția rețelelor de noduri de senzori, folosind circuite hardware reconfigurabile. Aceasta este o problemă spinoasă deoarece se încearcă utilizarea unor circuite cunoscute pentru consumul lor de energie într-un domeniu în care consumul este un factor important.

Al doilea scop este de a găsi soluții pentru a securiza nodurile de senzori și comunicațiile în interiorul rețelei și pentru a oferi o protecție cât mai bună împotriva atacurilor de orice fel.

Validarea soluțiilor este completată de verificarea funcțională folosind diverse metode precum: estimarea consumului de putere folosind instrumente specifice furnizate de la producătorii de circuite reconfigurabile, simularea modulelor hardware în faza de dezvoltare și testare post implementare folosind aparatură de măsură și control de ultimă generație.

1.3 Conținutul tezei de doctorat

Lucrarea este planificată astfel încât să prezinte gradual mecanismele și modulele hardware dezvoltate, pornind de la un studiu al circuitelor reconfigurabile și terminând cu identificarea unei soluții complete. După capitolul introductiv teza este organizată după cum urmează:

Al doilea capitol al tezei începe cu o scurtă prezentare a evoluției circuitelor reconfigurabile care evidențiază progresul tehnologic la care s-a ajuns în ziua de azi în domeniul circuitelor reconfigurabile. Prezentarea continuă cu enumerarea principalelor tipuri de circuite reconfigurabile existente pe piață în momentul actual iar apoi sunt prezentate rezultatele unui studiu comparativ unic prin prisma numărului mare de circuite incluse în studiu și a al orientării lui. După studierea parametrilor de funcționare ai acestor circuite se trece la identificarea acelora care îndeplinesc cerințele specifice utilizării lor pentru dezvoltarea de noi noduri de senzori. De asemenea, se vor prezenta și câteva metode de reducere a consumului de energie care trebuie respectate de dezvoltatorii de noduri de senzori atunci când implementează module hardware care vor fi incluse în astfel de noduri.

În capitolul trei sunt prezentate trei arhitecturi inovative de noduri de senzori proiectate și realizate fizic pentru fi folosite în rețelele de senzori moderne. De asemenea, mai prezint și o metodă inovativă de control al activităților nodurilor care are ca scop reducerea consumului de energie al nodului plus un model unic de simulare parametrizabil pentru testarea platformelor multisenzor.

Capitolul patru tratează problema securității rețelelor de noduri de senzori. În cadrul acestui capitol sunt prezentate mecanisme inovative, care au ca scop protejarea nodurilor de senzori împotriva atacurilor informatice. Primul mecanism dezvoltat abordează problematica generării numerelor aleatorii pe platforme care nu oferă suficiente resurse de procesare, iar al doilea prezintă o modalitate unică care folosește tehnologii moderne pentru securizarea rețelelor de senzori. De asemenea este prezentată și o metodă de implementare care permite utilizarea algoritmilor criptografici puternici în noduri cu resurse limitate și o metodă care permite folosirea nodurilor de senzori în zone critice.

În capitolul 5 este prezentat un nod de senzori securizat și cu performanțe ridicate. Pentru a asigura un nivel de securitate cât mai înalt, este propusă o arhitectură nouă, realizată cu o singură unitate de procesare a datelor, un sistem de management al cheilor criptografice și un model de stocare a datelor cu mecanisme de criptografice sub controlul strict al utilizatorului. Pentru protecția fizică pe lângă diverse mecanisme specifice este prezentat și modelul unei carcase capabile să asigure un nivel ridicat de protecție împotriva radiațiilor compromițătoare. Acest model a fost testat întru-un laborator acreditat.

În ultimul capitol se vor prezenta rezultatele obținute pe parcursul stagiului de studiu doctoral, contribuțiile originale, lista lucrărilor și câteva direcții de dezvoltare ulterioară care derivă din rezultatele prezentate în cadrul acestei teze.

Capitolul 2

Circuite reconfigurabile utilizate la dezvoltarea rețelelor de senzori fără fir

2.1 Tipuri de circuite reconfigurabile

Resursele logice ale circuitelor reconfigurabile au crescut exponențial în timp ce procesul de fabricație a scăzut în același mod atingând în 2019 valoarea de 7nm reducând astfel consumul de energie și calificând circuitele hardware reconfigurabile pentru includerea lor domeniul dezvoltării nodurilor de senzori.

2.1.1 Circuite CPLD

Circuitele CPLD sunt folosite în general în aplicații precum: programarea circuitelor FPGA, decodare, automate digitale, aplicații mobile.

2.1.2 Circuite FPGA

Circuitele FPGA sunt circuite integrate realizate din siliciu care pot fi reprogramate astfel încât ele pot înlocui aproape orice circuit integrat sau chiar sistem. Aceste circuite sunt alcătuite dintr-o matrice de blocuri logice complexe înconjurate de o "țesătură" de căi de rutare care permit interconectarea blocurilor prin programare.

2.2 Tehnologii de programare

În tabelul 2.1 [4], sunt prezentate principalele proprietăți ale celor mai folosite tehnologii de programare.

Tabelul 2.1 Proprietățile tehnologiilor de programare

	SRAM	FLASH	Anti-fuse
Reprogramabilitate	Da	Da	Nu
Volatilitate	Da	Nu	Nu
Arie ocupată	Mare	Moderată	Mică
Programare în sistem	Da	Da	Nu
Proces de fabricație utilizat	CMOS	Flash	Polisiliciu
Rezistența comutatoarelor	Mare	Mare	Mică

2.3 Parametri și familii de circuite

Pentru a alege circuitul potrivit în procesul de proiectare a nodurilor de senzori trebuie studiate o serie de parametri ai tuturor familiilor de circuite.

2.3.1 Parametrii circuitelor reconfigurabile

Parametrii circuitelor reconfigurabile pot fi grupați în două mari categorii: **parametrii intrinseci** care caracterizează resursele interne ale circuitelor reconfigurabile și **parametrii extrinseci** care caracterizează circuitele din punct de perspectivă electrică, al condițiilor de mediu și al gabaritului.

2.3.2 Familii de circuite reconfigurabile

Pentru identificarea circuitelor reconfigurabile care se califică pentru dezvoltarea arhitecturilor de senzori, am efectuat studiu comparativ unic prin prisma numărului mare de circuite incluse și a al orientării lui. Acest studiu clasează toate familiile de la principalii producători de circuite reconfigurabile în funcție de resurse logice reconfigurabile relevante pentru dezvoltarea nodurilor de senzori.

2.4 Circuite reconfigurabile și sisteme mulisenzor

2.4.1 Aplicații ale circuitelor reconfigurabile

În această secțiune sunt sintetizate rezultatele studiului asupra aplicațiilor moderne care folosesc circuite reconfigurabile. În acest studiu au fost alese pentru fiecare domeniu cele mai semnificative aplicații care folosesc circuite reconfigurabile

și care specifică tipul de circuit folosit . Studiul reprezintă stadiul actual al aplicațiilor cu circuite reconfigurabile.

2.4.2 Aplicații ale sistemelor multisenzor

În această secțiune sunt sintetizate rezultatele studiului asupra aplicațiilor moderne ale sistemelor mutisenzor.

2.4.3 Sisteme multisenzor cu circuite reconfigurabile

Dacă intersectăm domeniile în care sunt aplicate circuitele reconfigurabile și sistemele multisenzor, se pot trage concluzii despre modul în care circuitele reconfigurabile pot fi folosite pentru a implementa aplicații, platforme și module care pot contribuii la dezvoltarea sistemelor moderne cu mai mulți senzori.

2.5 Metode de reducere a consumului de energie

Pentru proiectarea nodurilor de senzori inginerii sunt obligați să dezvolte sisteme optimizate pentru un consum cât mai mic de energie. Pentru a minimiza consumul de energie al circuitelor reconfigurabile trebuie mai întâi să analizăm cu atenție consumul total de energie.

2.5.1 Metoda reducerii prin constrângeri de sinteză și rutare

Cea mai practică metodă de reducere a consumului este folosirea diferitelor strategii de sinteză și rutare oferite de producătorii de circuite prin intermediul mediilor de dezvoltare. Aceste programe oferă opțiuni de optimizare a consumului sau a resurselor logice folosite.

2.5.2 Metoda reducerii prin tehnici de codare și utilizare a resurselor

În această secțiune sunt prezentate tehnicile de programare prin care dezvoltatorii de aplicații din domeniul nodurilor de senzori care au la bază circuite reconfigurabile trebuie să le folosească pentru a minimiza consumul de energie al nodului.

Capitolul 3

Arhitecturi de noduri bazate pe circuite reconfigurabile

3.1 Topologia rețelelor de senzori

În prezent există mai multe topologii de rețele de senzori dintre care cele mai întâlnite sunt: punct la punct, stea, arbore și plasă.

În funcție de domeniul de aplicare rețelele de senzori fără fir pot fi mobile, statice, "single" sau "multi hop". De asemenea pot avea una sau mai multe stații de bază.

3.2 Arhitecturi de nodurilor de senzori

3.2.1 Modelul de bază

Este prezentată arhitectura de bază a unui nod de senzori în care unul sau mai mulți senzori conectați la o unitate centrală de procesare prin intermediul magistralelor de comunicare cu viteză redusă (de exemplu, SPI, I2C, UART, CAN etc.) [6].

3.2.2 Arhitectura Single Chip Full HW - SCFHW

Această arhitectură folosește un singur circuit reconfigurabil care îndeplinește toate funcțiile unității centrale de procesare.

În general, la nivelul unui nod de senzori, unitatea centrală de procesare citește date de la senzori la intervale regulate de timp, pe care le procesează și apoi le transmite mai departe către alte noduri.

- **Nodul HWP-CPLD-2018**

Plecând de la informațiile prezentate mai sus am proiectat și realizat fizic două noduri de senzori care au ca unitate de procesare doar cu un circuit reconfigurabil. Prima variantă are la bază un circuit CPLD.

Pentru testarea nodului într-o configurație normală de lucru am montat la porturile GPIO ale nodului un modul care conține un singur senzor de monitorizare ambientală și un modul de transmisie cu consum redus de energie care transmite și recepționează date în banda ISM-868MHz. Modulele hardware interne sunt controlate cu ajutorul unui automat finit care asigură următoarele funcții: configurează nodul cu parametrii de funcționare, citește date de la senzori de trei ori pe oră și le transmite la stația de bază.

Rezultatele experimentale sunt prezentate în tabele 3.3 și 3.4.

Tabelul 3.1 *Consumul mediu de curent pe oră în funcție de frecvență în regim normal de funcționare al nodului HWP-CPLD-2018*

	Curent static (µA)	**Curent fix (µA)**	**Consumul mediu de curent pe oră în etapele care depind de frecvența de tact**				
			32.768KHz	**100KHz**	**1MHz**	**8MHz**	**50MHz**
CPLD	33	-	0.040 mA	0.1 mA	0.77 mA	5.6 mA	40 mA
OSCILATOR	0.1÷10	-	0.9 µA	0.75 µA	3 mA	3 mA	19 mA
SENZOR	1	0.3	2.2 nA	732 pA	73 pA	9 pA	0.4 pA
Modul Comunicații	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

Pentru nodul HWP-CPLD-2018 am testat și metoda cu modul de management al activităților. În cazul acesta am obținut un consum mediu de **43µA** rezultând un timp de funcționare de aproximativ 6 ani. Platforma de testare este prezentată în figura 3.8.

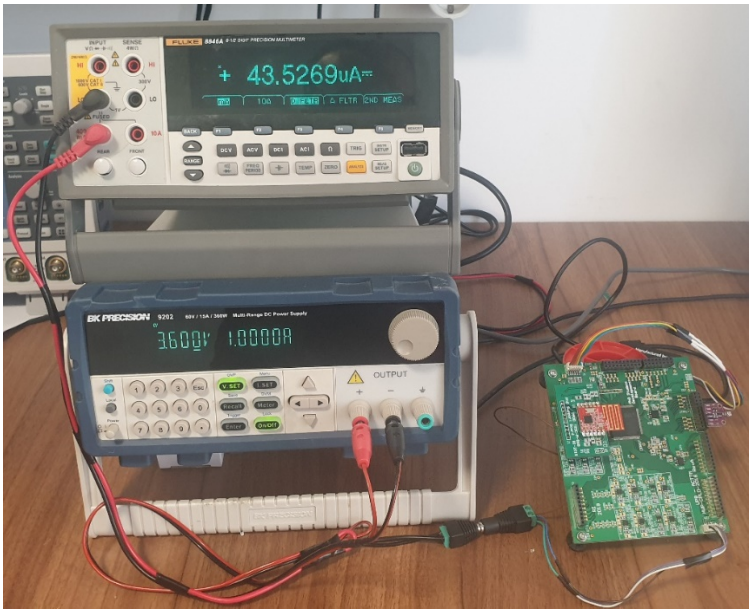


Figura 3.1 *Platforma de testare a nodului HWP-CPLD-2018*

Tabelul 3.2 *Situația resurselor logice utilizate pentru nodul HWP-CPLD-2018*

Modul \ Resurse	Macrocelule (disponibile 384)	Registre (disponibile 384)
Controler sistem	38 (9.9%)	34 (9%)
Controler SPI	82 (21.3%)	96 (25%)
Controler I2C	108 (28%)	80 (21%)
Management activitate	7 (1.8%)	4 (1%)
Total	**235 (61%)**	**214 (56%)**

- **Nodul de senzori HWP-S6-2018**

Acest nod de senzori folosește ca circuit de procesare un circuit FPGA Spartan-6 care are mult mai multe resurse logice decât circuitul CPLD.

În figura 3.10 este ilustrat nodul de senzori care are conectat la porturile sale doi senzori pentru monitorizarea calității aerului și un modul de comunicații cu protocol SubGHz pentru transmiterea și recepția datelor în banda ISM-858MHz.

Figura 3.2 *Nodul de senzori HWP-S6-2018*

În tabelele 3.5 și 3.6 sunt prezentate rezultatele experimntale.

Tabelul 3.3 *Consumul mediu de curent pe oră în funcție de frecvență în regim normal de funcționare al nodului HWP-S6-2018*

	Curent static (µA)	Curent fix (µA)	Consumul mediu de curent pe oră în etapele care depind de frecvența de tact				
			32.768KHz	**100KHz**	**1MHz**	**8MHz**	**50MHz**
FPGA		-	5mA	5.1 mA	5.5mA	6 mA	50 mA
OSCILATOR	0.1÷10	-	0.9 µA	0.75 µA	3 mA	3 mA	19 mA
SENZOR	1	0.3	2.2 nA	732 pA	73 pA	9 pA	0.4 pA
Modul Comunicații	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**

Așa cu se observa în tabelul 3.6, 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.

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

Modul \ Resurse	LUT (5720 disponibile)	Registre (11440 disponibile)
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%)**

În tabelul 3.7 sunt prezentate mai multe noduri disponibile pe piață sau prezentate în lucrări științifice care au ca circuit de procesare atât microcontrolere cât și circuite reconfigurabile.

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

Denumire	Circuit procesare	Componente auxiliare	Modul comunicație	Putere medie consumată (mW)	Putere consumată în transmisie (mW)	Referință
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	[7]
Telos–B (Comercial)	MSP430	SRAM–20KB FLASH–60KB	CC2420	6.5	76.5	[7]
Beagle Bone Black	ARM Cortex-A8	SDRAM–512MB FLASH–2GB	-	2200	-	[7]
Spartan–3E	XC3S1600E	-	-	2850		[7]
Spartan–3	XC3S2000	-	-	1000		[7]
Spartan–6	XC6SLX150	SDRAM–256Mb	-	462	-	[7]
Artix–7	XC7A35T	SRAM-1.8Mb	-	5000	-	[7]
Cyclone-II	EP2C70	-	ZigBee	221	-	[7]

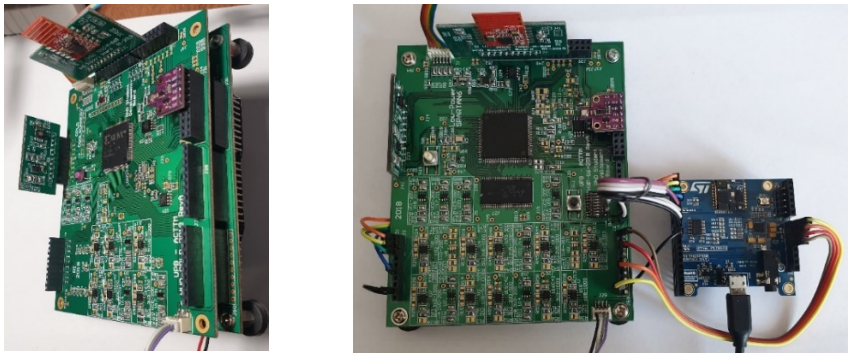
3.2.3 Arhitecturi tip hibrid

În cadrul acestor arhitecturi circuitele reconfigurabile au rol de coprocesor sau accelerator hardware. Funcțiile principale ale nodului sunt asigurate de un circuit cu consum mic de energie dar cu resurse de procesare insuficiente. Configurarea nodului, citirile de date de la senzori și transmiterea lor este executată de către circuitul cu consum mic de energie, care poate activa circuitul reconfigurabil doar atunci când este nevoie de executarea unor funcții care necesită putere mare de procesare precum funcții criptografice, procesare de semnal audio-video sau chiar funcții din domeniul inteligenței artificiale.

Pentru a testa performanțele acestei arhitecturi, am dezvoltat două noduri de senzori folosind plăcile prezentate în secțiunea anterioară și o placă de dezvoltare care are ca circuit de bază un microcontroler. În primul nod circuitul principal este circuitul CPLD al plăcii HWP-CPLD-2018 în timp ce pentru al doilea am folosit ca circuit

principal microcontrolerul plăcii STEVAL-STLKT01V1 “SensorTile development kit”.

Pentru testare am ales să folosesc circuitul FPGA pe post de accelerator criptografic, acesta având rolul să cripteze folosind algoritmul de criptare AES-256 în modul ECB datele primite de la circuitul principal și apoi să le trimită înapoi pentru a fi transmise prin intermediul modulului de comunicație. Cele două montaje sunt ilustrate în figura 3.13.



a) b)

Figura 3.3 *Noduri de senzori cu arhitecturi hibride*

Gradul de ocupare al circuitului Spartan 6 după adăugarea modulului criptografic este **36.7% LUT** și **6.9% registre** logice.

Pentru determinarea consumului am folosit același scenariu și aceeași platformă de testare pe care le-am folosit pentru testarea nodurilor realizate folosind arhitectura SCFHW. În tabelul 3.8 sunt prezentate rezultatele experimentale la diferite frecvențe de lucru ale celor două configurații pentru o singură activare a circuitului FPGA într-o oră.

Tabelul 3.6 *Rezultate experimentale pentru nodurile de senzori cu arhitecturi hibride*

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**

În tabelul 3.9. sunt prezentate câteva noduri cu arhitecturi similare, unde consumul circuitului FPGA este dat pentru cazul în care acesta funcționează permanent.

Tabelul 3.7 *Exemple de noduri de senzori cu arhitecturi hibride*

Denumire	**Circuit principal**	**FPGA**	**Puterea consumată de circuitul principal (mW)**	**Puterea consumată de FPGA (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	[5]
Senito32-Igloo	AVR32	IGLOO	77.5	5.93	[5]
MSP-IGLOO	MSP430	AGL125	20	5	[5]

3.2.4 Arhitecturi tip SoC

Aceste arhitecturi sunt folosite pentru dezvoltarea nodurilor cu performanțe ridicate, unde datorită fluxului mare de date, a protocoalelor de comunicații utilizate și a funcțiilor executate, doar aria logică a circuitelor FPGA cu consum mic de energie nu este suficientă pentru asigura funcționarea în bune condiții rețelelor cu nodurilor..

Există două tipuri de noduri care pot fi folosite la dezvoltarea acestor tipuri de noduri de senzori cu nuclee de procesare „soft" și „hard".

Placa HWP-S6-2018 poate fi folosită pentru a dezvolta noduri de senzori cu arhitecturi SoC, deoarece circuitul Spartan 6 suportă implementarea de procesoare soft.

Pentru a testa cel de-al doilea tip de nod (cu procesor hard) am folosit placa de dezvoltare MiniZED ilustrată în figura 3.16.

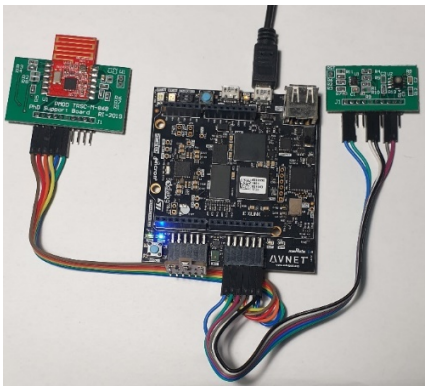


Figura 3.4 *Nod de senzori realizat cu placa de dezvoltare MiniZed*

În urma experimentelor a rezultat un consum de **800mW** pentru placa HWP-S6-2018 și **1.8W** pentru placa MiniZed, ambele plăci fiind alimentate de la o sursă de 5V. În tabelul 3.10 este prezentată situația utilizării resurselor logice.

Tabelul 3.8 *Rezultate experimentale pentru nodurile de senzori cu arhitecturi SoC*

Nod de senzori	**LUT**		**Registre**		**Blocuri Memorie**	
	Disponibile	Utilizate	Disponibile	Utilizate	Disponibile	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 Managementul activității nodurilor de senzori

Consumul de energie al nodurilor poate fi redus considerabil dacă la nivelul nodului se implementează un modul hardware care are rolul de a controla la nivel macro celelalte module hardware.

Modulul care gestionează managementul activităților este prezentat în figura 3.18. Pentru a reduce consumul de energie acesta folosește două generatoare de semnal de tact. Primul cu frecvență mică are rol de timer și este folosit pentru a monitoriza și activa celelalte module și oscilatorul cu frecvență mai mare activat doar atunci când este nevoie.

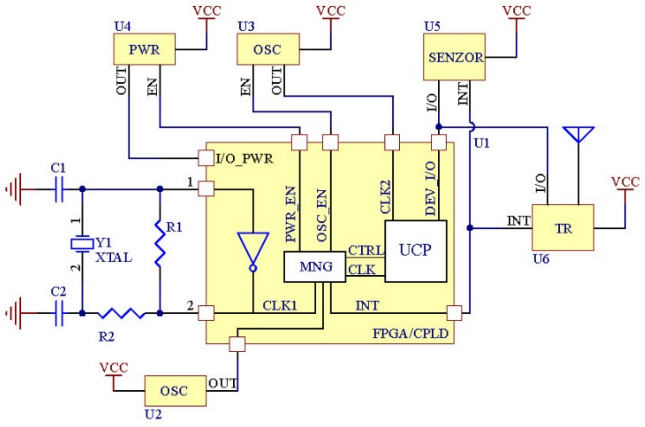


Figura 3.5 *Sistem de management al activităților*

Folosind această metodă de management al activității am obținut rezultatele prezentate în tabelul 3.11.

Tabelul 3.9 *Rezultate experimentale obținute în cazul folosirii modulului pentru managementul activităților*

Nod	**Fără management de activitate**		**Cu management de activitate (32.768KHz/8MHz)**		
	Consum în funcționare la 32.768KHz	Consum în funcționare la 8MHz	Consum mediu pentru 3 operații pe oră	Consum mediu pentru 10 operații pe oră	Consum mediu pentru 100 operații pe oră
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 Model parametrizabil de simulare pentru testarea arhitecturilor multisenzor

Modelarea și simularea comportamentală este necesară pentru caracterizarea teoretică a dispozitivelor și sistemelor înainte de fabricație, sau chiar înainte de realizarea prototipului, din mai multe motive printre care se numără reducerea costurilor și a timpului de producție [8].

Deoarece majoritatea senzorilor folosiți sunt de tipul SiP am decis să dezvolt un model de simulare care să modeleze senzorii de tipul SiP.

3.4.1 Structura modelului de simulare

După studierea celor mai reprezentative familii de senzori, de mai multe, am stabilit o structură care poate descrie cât mai precis toți acești senzori, chiar dacă sunt de tipuri diferite. Această structură prezentată în figura 3.20 conține toate mecanismele și parametrii necesari pentru ca modelul de simulare propus să ofere cercetătorilor

posibilitatea de a-și testa modulele de control sau fuziune a datelor cât mai bine posibil [9].

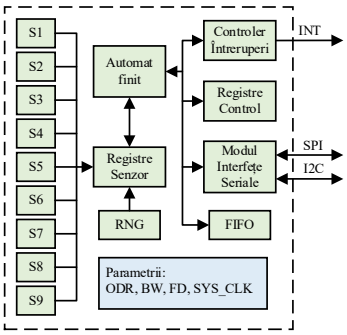


Figura 3.6 *Structura modelului de simulare*

Acest model poate fi sintetizat și implementat în aria logică a circuitelor FPGA folosind mediul de dezvoltare Vivado. În tabelul 3.13 este prezentată utilizarea resurselor FPGA.

Tabelul 3.10 *Situația resurselor logice în cazul implementării hardware a modelului de simulare*

Modul hardware	**LUT**	**Registre**	**BRAM**
Automat finit	11	14	0
Interfețe seriale	204	222	0
Mecanismul de întreruperi	10	5	0
Registre interne	2	5	0
RNG	120	105	0
FIFO	2	2	2
Total	**349**	**353**	**2**

3.4.2 Metode de simulare și implementare

Modelul a fost implementat și testat folosind două metode diferite. În prima metodă, prezentată în figura 3.21, modelul a fost simulat folosind un modul de testare tip "testbench HDL" care include atât modelul de simulare, cât și controlere hardware de comunicații seriale.

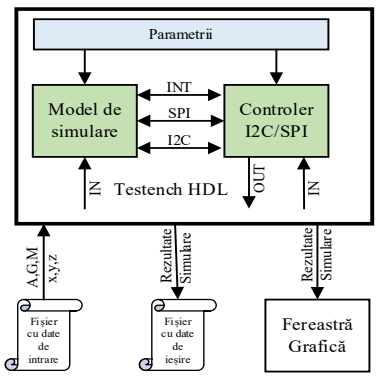


Figura 3.7 *Schema platformei pentru simulare*

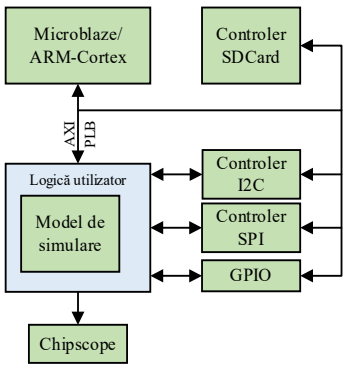


Figura 3.8 *Platformă pentru testarea hardware a modelului*

În a doua metodă, prezentată în figura 3.22, modelul a fost emulat în hardware folosind metode tip embedded care includ atât instrumente hardware cât și software.

3.5 Nod de senzori cu consum redus de energie pentru monitorizarea temperaturii pacientului

În această secțiune este prezentat conceptul și implementarea unui senzor wireless de temperatură pentru monitorizarea pacienților folosind dispozitive hardware reconfigurabile ca o alternativă la utilizarea dispozitivelor clasice. Sistemul a fost dezvoltat folosind plăci de dezvoltare și apoi implementat pe platforma HWP-CPLD-2018.

Sistemul propus poate fi alimentat folosind diferite tipuri de baterii sau acumulatori cu tensiuni cuprinse între 3.6 V - 5 V.

Deoarece CPLD-ul și senzorul pot lucra cu frecvența de 32.768KHz am folosit un singur oscilator. În tabelul 3.14 este prezentat consumul de energie al componentelor și consumul total de energie al nodului [10].

Tabelul 3.11 *Consumul de curent al nodului în diferite moduri de funcționare*

Dispozitiv	**Consum în modul inactiv**	**Consum în modul activ**
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

Deoarece în timpul unui ciclu de 10 minute, sistemul efectuează 5 operații de citire și o transmisie și ținând cont de consumul circuitului CPLD și al regulatoarelor, atunci rezultă un consum mediu pe oră de aproximativ **46.38 µA**. Dacă este folosită o baterie cu capacitate de 1000 mAh, atunci din calcule folosind formula 3.1 rezultă că sistemul poate funcționa aproximativ **3 ani** fără a schimba bateria [10].

Capitolul 4

Securitatea nodurilor de senzori

4.1 Mecanisme de securitate

În tabelul 4.1 sunt prezentați principalii algoritmi criptografici implementați împreună resursele pe care aceștia le utilizează.

Tabelul 4.1 *Utilizarea resurselor în urma implementării principalilor algoritmi de criptare*

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

4.2 Generator de numere aleatorii

În această secțiune prezint o metodă care folosește senzorii nodurilor ca sursă de zgomot pentru a genera numere aleatorii. Pentru evaluare am implementat două platforme: prima are la bază un microcontroler iar cea de-a doua are la bază un circuit FPGA.

Pentru testarea datelor extrase, am utilizată o metodologie acreditată de NIST, care include un număr de 10 estimatori care sunt calculați pentru seturi de date de cel puțin 1.000.000 de eșantioane.

4.2.1 Evaluarea entropiei folosind platforme cu microcontroler

În cazul experimentelor efectuate pe platforma cu microcontroler, am folosit placa de dezvoltare B-L475E-IOT01A1 produsă de STMicroelectronics. Această placă este dezvoltată ca nod IoT și este echipată cu un microcontroler plus o serie de senzori de tip IMU și monitorizare parametrii ambientali.

Analiza entropiei a fost efectuată prin mai multe experimente.

- Experimentul 1
  - Scop: evaluarea entropiei senzorilor IMU în două cazuri de utilizare: în staționare și în deplasare.
  - Rezultate: Tabelul 4.2 prezintă valorile entropiei în cazul celor cei trei senzori pentru fiecare axă (X,Y și Z) în cele două cazuri de utilizare [11].

Tabelul 4.2 *Valorile estimate ale entropiei pentru senzorul IMU*

Senzor	În staționare			În deplasare		
	axa X	axa Y	Axa Z	axa X	axa Y	Axa Z
Accelerometru	0.46	0.41	0.30	0.82	0.82	0.82
Giroscop	0.25	0.36	0.26	0.53	0.54	0.39
Magnetometru	0.47	0.46	0.62	0.56	0.48	0.59

- Experimentul 2:

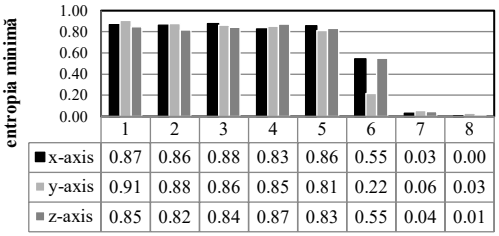
- Scop: evaluarea entropiei senzorilor pentru monitorizarea parametrilor de mediu în două cazuri de utilizare: interior și exterior.
- Rezultate: Tabelul 4.3 prezintă valorile entropiei pentru cei patru senzori în cele două cazuri de utilizare [11].

Tabelul 4.3 *Valorile estimate ale entropiei pentru senzorul de monitorizare a mediului*

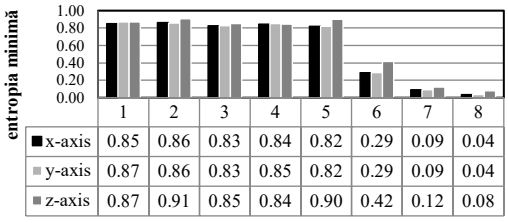
Locul testării	HTS221		LPS22HB	
	Umiditate	Temperatură	Presiunea aerului	Temperatură
Interior	0.0321	0.0041	0.3067	0.0004
Exterior	0.0405	0.0078	0.3028	0.0019

- Experimentul 3

- Scop: identificarea pozițiilor biților care contribuie cel mai mult la entropia datelor extrase;
- Rezultate: în figurile 4.1 sunt prezentate valorile entropiei pentru accelerometru [11].



(a)



(b)

Figura 4.1 *Valorile entropiei pentru fiecare bit al datelor citite de la accelerometru: (a) în staționare, (b) în mișcare*

Pentru ceilalți senzori rezultatele sunt asemănătoare de unde se trage concluzia că primii 4 biți contribuie cel mai mult la valoarea entropiei.

4.2.2 Evaluarea entropiei folosind circuite reconfigurabile

Pentru determinarea valorilor entropiei folosind circuite hardware reconfigurabile am folosit platforma ilustrată în figura 4.5. Componenta principală a acestei platforme este placa de dezvoltare CMOD-A7 produsă de compania Digilent. Placa este dotată cu un circuit FPGA Artix7 - XC7A15T-1CPG236C.

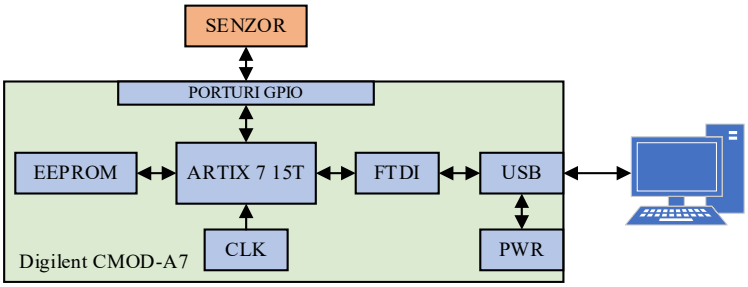


Figura 4.2 *Schema bloc a platformei cu circuite reconfigurabile folosite pentru evaluarea entropiei*

Toate modulele hardware au fost implementate cu ajutorul mediului de dezvoltare Vivado 2018.3. În tabelul 4.4 [6] este prezentată situația utilizării resurselor logice după implementare.

Tabelul 4.4 *Gradul de utilizare a resurselor logice pentru platforma de testare cu circuite reconfigurabile*

Controler	LUT		Registre	
	Folosite	Grad de utilizare (%)	Folosite	Grad de utilizare (%)
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

S-a folosit aceeași baterie de teste ca și în primul caz.

- Experimentul 1

Evaluarea entropiei datelor extrase de la senzorul IMU.

Tabelul 4.5 *Valorile entropiei pentru senzorul IMU*

Senzor/Parametrii de configurare	**axa x**	**axa y**	**axa z**
Accelerometru: ODR=1333, Fs=16, Delay=3500	0.59	0.52	0.51
Giroscop: ODR=1333, Fs=16, Delay=3500	0.45	0.44	0.4
Magnetometru: ODR=1000, Fs=8, Delay=1500	0.5	0.45	0.58

- Experimentul 2

Pentru această etapă am utilizat aceiași senzori cu aceeași configurație ca la experimentul 1. Singura diferență a fost că în acest experiment s-au efectuat două citiri de la doi senzori in același ciclu, biții datelor extrase de la senzori au fost concatenați folosind următoarea relație:

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

Rezultatele experimentale sunt prezentate în tabelul 4.6 [6].

Tabelul 4.6 *Valorile entropiei pentru senzorul IMU obținute prin aplicarea relației de concatenare*

Senzor/Parametrii de configurare	**H{x,y}**	**H{x,z}**	**H{y,z}**
Accelerometru: ODR=1333, Fs=16, Delay=3500	**0.9**	0.87	0.72
Giroscop: ODR=1333, Fs=16, Delay=3500	0.74	0.68	0.51
Magnetometru: ODR=1000, Fs=8, Delay=1500	0.58	0.7	0.68

- Experimentul 3

În acest experiment s-au folosit microfonul MEMS și senzorul de monitorizare a calității aerului. Pentru acest caz, entropia a fost analizată în trei cazuri: interior (I), exterior (II) și cu sursă de poluare (III).

Rezultatele experimentale sunt prezentate în tabelul 4.7 [6].

Tabelul 4.7 *Valorile entropiei pentru microfon și senzorul de monitorizare a calității aerului*

Senzor	**Cazul I**	**Cazul II**	**Cazul III**
Microfon	0.3	0.47	0.6
Senzor pentru monitorizarea calității aerului	0.32	0.5	0.55

4.3 Securizarea rețelelor de senzori prin baze de date distribuite (blockchain)

Tehnologia blockchain poate fi folosită pentru securizarea rețelelor de senzori cu circuite FPGA folosind arhitecturile de tip SoC la care am adăugat două module care au rolul de a mina și a valida blocurile din blockchain.

În tabelul 4.8 sunt prezentate rezultatele experimentale.

Din datele experimentale rezultă că nodul HWP-S6-2018 care folosește circuitul XC6SLX9 poate fi folosite pentru implementarea tehnologiei blockchain pentru securizarea datelor.

Tabelul 4.8 *Rezultatele experimentale obținute în urma implementării arhitecturii de securizare prin tehnologie blockchain*

Familie de circuite FPGA	**Circuit FPGA**	**Tip Circuit**	**Resurse logice (LUT)**	**Număr de module SHA2**	**Frecvență maximă**	**Viteză 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 Metodă de implementare a algoritmilor criptografici în nodurile cu resurse hardware insuficiente

Pentru a satisface cerințele implementării unor algoritmi criptografici performanți pe circuite reconfigurabile mai puțin performante, am dezvoltat o metodă inovativă de implementare care reduce semnificativ gradul de utilizare a ariei logice interne.

Prin această metoda se elimină necesitatea folosirii resurselor interne ale circuitelor pentru a implementa tabelele S-Box. Pentru degreva circuitul reconfigurabil de această sarcină am folosit o memorie externă de tip SRAM pentru a stoca la adrese succesive cheile de rundă derivate în prealabil din cheia criptografică și valorile $b_{n,n}$ ale tabelei S-Box.

Pentru testarea metodei am folosit nodul HWP-S6-2018. Schema platformei de testare este indicată în figura 4.10.

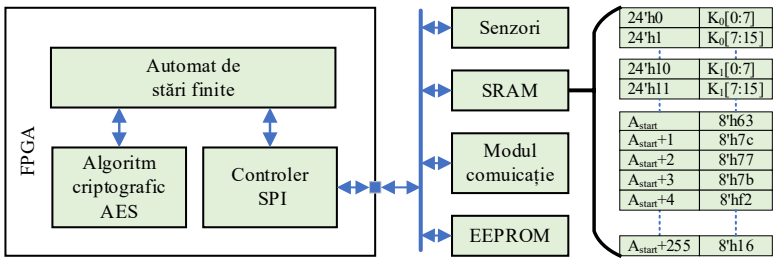


Figura 4.3 *Schema bloc a platformei de testare*

În tabelul 4.9 sunt prezentate rezultatele implementării algoritmului AES-128/256 atât în varianta optimizată pentru viteză cât și pentru varianta optimizată pentru a fi folosită în noduri cu resurse logice limitate.

Tabelul 4.9 *Utilizarea resurselor logice*

Algoritm	**Optimizare pentru viteză**			**Optimizare pentru resurse logice puține**		
	Cicluri	**LUT**	**Registre**	**Cicluri**	**LUT**	**Registre**
AES-128	10	638(11%)	281(2%)	8560	254(4%)	269(2%)
AES-256	14	1543(26%)	425(3%)	11984	364(6%)	416(3%)

Datele referitoare la utilizare prezentate în tabel sunt date doar pentru algoritm și nu includ și resursele utilizate de controlerul SPI și de automatul de stări finite.

4.5 Nod de senzori securizat pentru monitorizarea parametrilor medicali

Pentru a demonstra posibilitatea folosirii circuitelor FPGA la implementare unor sisteme care pot fi purtate de utilizatori, am dezvoltat o un nod de senzor unic datorită mobilității, a domeniului de aplicare și a utilizării circuitelor reconfigurabile ca circuit

principal de procesare. Acest nod de senzori are ca scop principal monitorizarea parametrilor biomedicali al oamenilor în timpul unor exerciții care presupun efort fizic intens (de exemplu monitorizarea parametrilor soldaților în timpul misiunilor de luptă).

Sistemul propus este alcătuit din unul sau mai multe noduri purtabile de senzori care măsoară parametrii biomedicali umani și apoi trimite datele colectate la o stație de bază pentru a fi analizate de personal calificat. Domeniul în care este folosit acest senzor impune necesitatea securizării comunicației dintre noduri și stația de bază. Parametrii monitorizați sunt: temperatura corpului, nivelul de oxigen din sânge, ritmul cardiac, frecvența respiratorie, mișcarea și poziția subiectului.

Pentru securizarea comunicației între stația de bază și nodurile de senzori am ales algoritmul AES-256 deoarece raportul dintre tăria criptografică și resurse utilizate este cel mai bun [12].

Pentru implementare am folosit nodul HWP-S6-2018 prezentat în capitolul 3 la care am conectat senzorii enumerați mai sus. Placa MiniZed la care am conectat modulul TSRC-ST-868 îndeplinește funcțiile stației de bază.

Circuitul Spartan 6 funcționează cu 32.768KHz în modul timer și 8MHz în modul activ. În tabelul 4.11 prezintă consumul componentelor în ambele moduri de lucru, consumul mediu de energie pentru 25 de cicluri pe secundă (citire date de la cei trei senzori și transmiterea datelor) și consumul total al nodului [12].

Tabelul 4.10 Consumul mediu de energie al nodului securizat

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

Funcționarea corectă a sistemului am verificat-o prin afișarea datelor în fereastra ILA, înainte de criptare, după criptare și la recepție.

Utilizarea resurselor după implementare este prezentată în tabelul 4.11.

Tabelul 4.11 Situația utilizării resurselor în urma implementării nodului securizat

Modul	**LUT**	**Registre**
Controler sistem	320	256
Controler SPI	75	69
Controler I2C	177	97
Modul Criptare - Decriptare	3122	812
Total	**3694 (64%)**	**1234 (10%)**

Consumul mediu al stației de bază este de 280 mA. Dar, în această configurație stația de bază dispune de o sursă de energie. Numărul de resurse utilizate la nivelul stației este aproximativ egal cu cel al nodului.

Capitolul 5

Nod de senzori securizat cu performanțe ridicate de procesare

În acest capitol sunt prezentate metode și mecanisme originale care pot fi integrate în arhitecturile de noduri de senzori cu performanțe ridicate de procesare. Mecanismele prezentate au rolul de a interconecta modulele nodului asigurând în același timp viteze mari de procesare și de a mări nivelul de securitate al nodului.

5.1 Arhitectura nodului

Componentele principale ale arhitecturii sunt prezentate în figura 5.1. Arhitectura prezentată conține toate modulele necesare pentru a obține performanțe înalte de procesare și o securitate sporită împotriva atacurilor informatice.

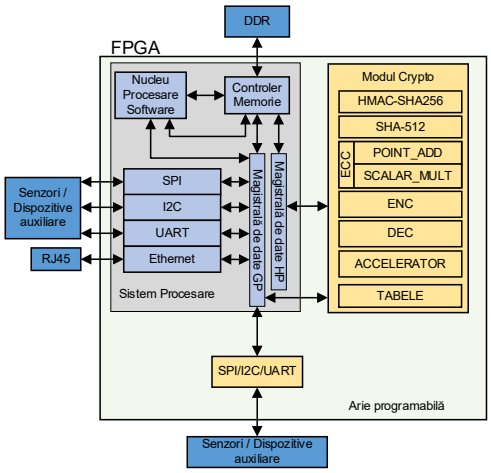


Figura 5.1 *Arhitectura nodului de senzori cu performanțe ridicate de procesare*

Pentru a asigura cerințele de performanță și securitate, am implementat la nivelul nodului folosind limbaje de programare de tip HDL modulul hardware Crypto care conține cele mai utilizate mecanisme criptografice și un accelerator hardware.
În tabelul 5.1 sunt prezentate resursele utilizate după implementarea modulelor.

Modulele au fost implementate și testate folosind o platformă experimentală alcătuită din modulul Trenz TE0715-15-04 și placa suport TE0703-06. Aria programabilă are 46200 LUT, 92400 registre și 95 module RAMB36. În timpul testelor consumul de curent maxim a fost de **300mA**.

Tabelul 5.1 *Situația utilizării resurselor în urma implementării nodului cu performanțe ridicate*

Modul	LUT	Registre	Memorie BRAM
HMAC-SHA256	2152	1910	0
SHA-512	3810	2244	0
ECC	7949	7507	0
ENC-DEC	7312	5559	16
ACCELERATOR	1671	1988	2
TABELE	753	1232	8
BLOCURI AUXILIARE	6421	8980	2
Total	**30068**	**29420**	**28**

5.1.1 Accelerator hardware de mare viteză

Această componentă hardware permite conectarea mai multor module specializate la un singur port HP al procesorului folosind un singur bloc AXI_DMA. Blocurile acceleratorului și conexiunile între ele sunt prezentate în figura 5.3.

Blocul CAM este un modul hardware care permite determinarea rapidă a poziției la care se află datele de intrare, iar blocul TABELA CHEI este o memorie de tipul BRAM cu două porturi care permit controlarea memoriei de către două module hardware diferite.

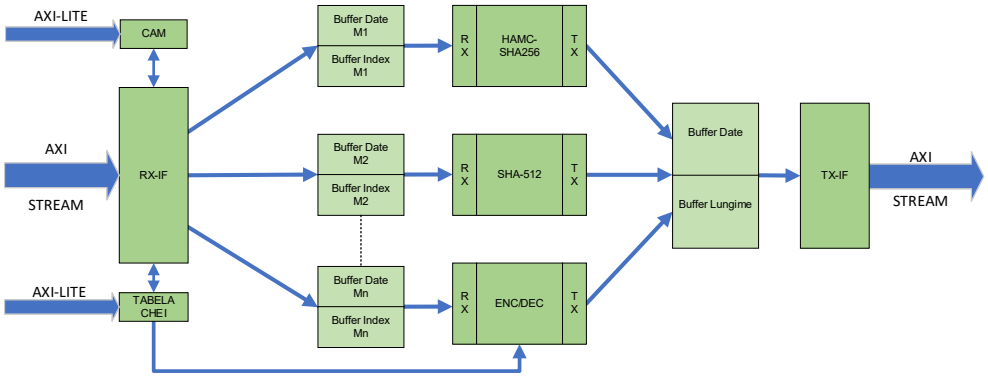


Figura 5.2 *Structura internă a acceleratorului*

Blocului INDEX după care se face determină blocul care va fi folosit este alcătuit din: SM indică sub-modulul care se dorește a fi utilizat, ADDR este adresa nodului sursă, NM este un flag care indică faptul că adresa nu a fost găsită în CAM și LEN reprezintă lungimea pachetului ce urmează a fi procesat. R este rezervat pentru diferite semnalizări definite de utilizator.

5.2 Metode de transfer a datelor

În această secțiune sunt prezentate o serie de informații utile rezultate în urma efectuării unor teste inovative care au ca scop identificarea soluției optime de transfer a datelor dintre procesor și modulele hardware folosite pentru procesarea acestor date.

Pentru a testa aceste metode într-un scenariu cât mai apropiat de cel real, am ales configurația procesor-accelerator hardware (AES256) deoarece este cea mai folosită. [13]

După ce au fost studiate mai multe protocoale și specificații disponibile pentru a transfera și recepționa date de la sau către procesor, am considerat că numai trei dintre ele merită luate a fi prezentate.

Metodele alese sunt următoarele: PowerPC440 DMA, PowerPC440 APU și Zynq-7000 DMA- HP.

Metodele de transfer propuse au fost implementate și testate folosind plăcile de dezvoltare ML507 și MiniZed.

Rezultatele experimentale sunt prezentate în figura 5.11.

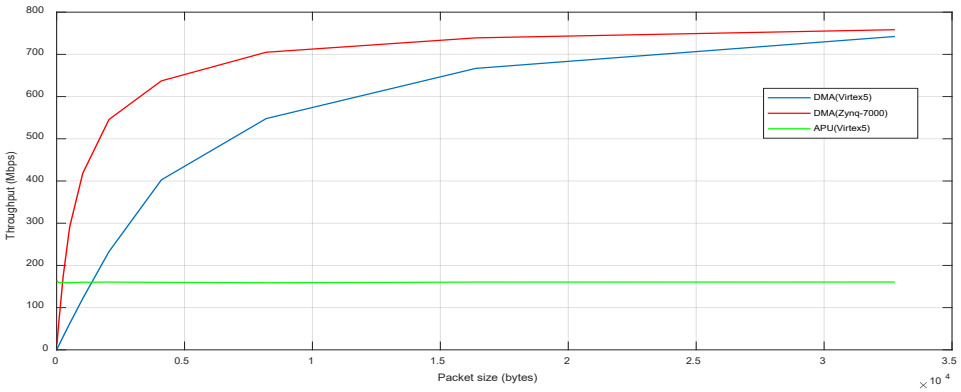


Figura 5.3 *Viteza de transfer a datelor în funcție de lungimea pachetului pentru cele trei metode de transfer*

5.3 Mecanism de stabilire a cheilor criptografice

În această secțiune este prezentat un mecanism original de stabilire a cheilor criptografice de sesiune, dezvoltat în timpul studiului doctoral care poate fi folosit cu succes pentru a securiza comunicațiile în rețelele de senzori cu topologii stea.

Cheia de sesiune este stabilită între cele două entități în urma unor schimburi de mesaje prin care se stabilește un index de cheie care este echivalent cu o adresă de memorie din memoria flash.

5.4 Mecanism de protecție la nivel 4 FIPS

În cazurile în care cerințele de securitate sunt mari, se impune implementarea la nivelul nodului al unor mecanisme suplimentare de securitate care să asigure monitorizarea în timp real a tensiunilor de alimentare și a temperaturii din interiorul circuitului reconfigurabil. Pentru a satisface și aceste cerințe extinse de securitate, am dezvoltat un modul hardware inovativ care folosește modulele dedicate ale circuitelor FPGA pentru a monitoriza permanent parametrii de funcționare ai circuitului și de a genera semnale de alarmă atunci când sunt depășite pragurile definite de utilizator [14].

Modulul generează semnale de alarmă atunci când mărimile monitorizate se află în afara pragurilor specificate.

5.5 Protecția nodurilor de senzori împotriva radiațiilor compromițătoare

În cazul nodurilor de senzori care fac parte din rețelele de senzori care au ca scop monitorizarea obiectivelor critice, sunt formulate și cerințe de protecție împotriva radiațiilor compromițătoare. În această secțiune este prezentată o metodă de inovativă prin care inginerii pot reduce considerabil timpul de implementare a mecanismelor protecție împotriva radiațiilor compromițătoare prin folosirea modelelor PCB ale nodurilor de senzori și a programului de simulare ANSYS HFSS. Prin această metodă se poate determina eficacitatea soluțiilor de ecranare înainte de realizarea lor în ateliere de prelucrări mecanice.

Pentru a testa eficacitatea soluției am ales nodul de senzori HWP-S6-2018.

După validarea modelului prin simulare s-a trecut la următoarea etapă în care a carcasa a fost realizată fizic și apoi s-au montat componentele nodului de senzori. După ce nodul a fost asamblat și testat din punct de vedere funcțional, acesta a fost supus testării într-un laborator acreditat pentru măsurarea nivelului de emisii compromițătoare [15].

5.6 Model de stocare a datelor cu mecanisme criptografice sub controlul strict al utilizatorului

În această secțiune este tratată problema stocării securizate în cloud a datelor de la nodurile de senzori [16][17][18] și este propus un sistem pentru securizarea prin criptare a datelor stocate care utilizatorul controlează cheile criptografice și ciclul lor de viață și are posibilitatea de alege între diferite metode de criptare în funcție de cerințele acestora [19].

Soluția de stocare securizată în cloud dezvoltată este de asemenea bazată pe schema de criptare la client, dar care îi permite utilizatorului să facă acest lucru cu control complet atât asupra cheilor de criptare, cât și asupra algoritmilor de criptare pe care doresc să-i utilizeze pentru protejare datele. Pentru a atinge nivelul de încredere dorit, este propusă de asemenea o arhitectură de tipul "zero-knowledge", în care datele și cheile nu sunt cunoscute de către sistemul de stocare în cloud.

Capitolul 6

Concluzii

Concluzionând, această teză prezintă gradual o serie de soluții originale care au condus în final la implementarea unor noduri de senzori cu un nivel de securitate sporit și cu performanțe mari de procesare, dar cu o eficiență energetică care permite alimentarea lor de la baterii sau acumulatori și montarea în zone izolate. În urma testării acestor soluții au fost obținute rezultate remarcabile în ceea ce privește eficiența energetică și puterea de procesare.

6.1 Rezultate obținute

În fiecare capitol al acestei teze au fost prezentate soluții viabile care pot contribuii la dezvoltarea rețelelor de senzori fără fir care folosesc noduri bazate pe circuite reconfigurabile. Fiecare soluție prezentată a fost implementată și testată obținând rezultate care le validează pentru a fi folosite nu doar în laborator ci și în lumea reală.

6.2 Contribuții originale

În timpul efectuării studiului doctoral, contribuțiile inovative pot fi sintetizate astfel:

1. Efectuarea unui studiu comparativ în funcție de parametrii care au relevanță în domeniul nodurilor de senzori. Acest studiu include toate circuitele reconfigurabile produse de principalii producători de astfel de circuite;
2. Proiectarea și fabricarea nodului de senzori HWP-CPLD-2018 care are la bază un circuit CPLD pentru procesarea datelor;
3. Proiectarea și fabricarea nodului de senzori HWP-S6-2018 care dispune pentru procesarea datelor de un circuit Spartan 6 în variantă cu consum redus de energie;
4. Implementarea și testarea arhitecturilor SCFHW care utilizează un singur circuit reconfigurabil pentru procesarea datelor provenite de la senzori și care prin comparare cu alte arhitecturi le clasează drept arhitecturi optime în legătură cu consumul;
5. Implementarea și testare arhitecturilor de tip hibrid care folosesc mai multe circuite reconfigurabile sau le combină cu microcontrolere pentru a obține

resurse mari de procesare dar în același timp asigură un consum redus de energie. Prin comparare cu alte noduri similare și punând în balanță raportul consum de energie-resurse logice rezultă că arhitecturile și modulele hardware prezentate în această teză sunt cele mai performante;

6. Implementarea și testare unei arhitecturi de tip SoC care poate fi folosită în rețelele de noduri de senzori oferind resurse uriașe de procesare prin conectarea ariilor reprogramabile la procesoare de tip “hard” sau “soft”;
7. Dezvoltarea unui mecanism hardware pentru management al activităților în cadrul nodurilor de senzori prin care se reduce considerabil consumul de energie;
8. Implementarea unui model parametrizabil de simularea arhitecturilor multisenzor. Modelul oferă posibilitatea simulării sau emulării senzorilor de tip SiP în timpul dezvoltării modulelor care controlează sau procesează date în sisteme cu mai mulți senzori [A9];
9. Implementarea și testarea unui nod de senzori cu consum redus de energie destinat monitorizării temperaturii pacienților [A1];
10. Am dezvoltat o platformă de testare cu microcontroler pentru evaluarea entropiei datelor culese de la senzori. Prin utilizarea unor metodologii NIST, am validat metoda și am identificat senzorii care pot genera suficientă entropie pentru a putea fi utilizați pentru generarea de numere aleatorii [A7];
11. Pentru a demonstra superioritatea circuitelor reconfigurabile în procesul de culegere a datelor de la senzori, am implementat o platformă de testare care are la bază un circuit FPGA. Cu această platformă au fost testați numai senzorii validați cu platforma de la punctul anterior [A8];
12. Am demonstrat posibilitatea utilizării tehnologiei blockchain pentru securizarea rețelelor de noduri de senzori [A4];
13. Am dezvoltat o metodă de implementare a algoritmilor criptografici complecși pe circuite reconfigurabile care nu au disponibile multe resurse logice;
14. Combinând soluțiile propuse anterior am implementat un nod de senzori securizat care are la bază circuite reconfigurabile pentru monitorizarea parametrilor biomedicali [A6];
15. Am implementat un modul hardware care permite conectarea mai multor acceleratoare la un singur port HP al procesoarelor reducând astfel resursele logice utilizate pentru implementarea nodurilor care asigură performanțe ridicate de procesare;
16. Am dezvoltat o metodă rapidă de atribuire a cheilor criptografice în funcție de adresa nodului de unde vine pachetul. Folosind această metodă atribuirea cheilor se face în paralel cu procesarea datelor din pachet, cheile fiind disponibile atunci când se începe procesul de decriptare;
17. Implementarea și compararea mai multor metode de transfer a datelor în sisteme de tip embedded reprezintă o contribuție deoarece prin acest studiu am demonstrat că în cazul utilizării circuitelor FPGA mai puțin performante care pot fi folosite în domeniul nodurilor de senzori, este posibilă obținerea unor

viteze de transfer la fel de mari ca și în cazul utilizării unor circuite mult mai performante [A2];

18. Dezvoltarea unui protocol de stabilire a cheilor criptografice prin care se asigură comunicația securizată între nodurile unei rețele de senzori;
19. Implementarea unui mecanism care poate fi configurat dinamic și care folosește senzorii din interiorul circuitului FPGA pentru a asigura o protecție la nivel 4 FIPS [B1];
20. Proiectarea, simularea, realizarea și validarea prin testare în cadrul unui laborator acreditat a unei carcase care asigură protecția nodului de senzori împotriva radiațiilor compromițătoare [A5]. Contribuția mea la realizarea carcasei a constat în generarea cu programul Altium Designer a modelului 3D al nodului de senzori care conține caracteristicile fizice și electrice ale nodului, necesare simulării electromagnetice efectuată cu programul ANSYS HFSS plus coordonarea echipei care a simulat și testat carcasa;
21. Dezvoltarea unui model de stocare a datelor cu mecanisme criptografice sub controlul strict al utilizatorului [A3].

6.3 Lista lucrărilor originale

6.3.1 Articole științifice indexate ISI

[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, în curs de indexare 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, în curs de indexare WOS, 2023.

6.3.2 Articole științifice indexate BDI

[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 Perspective de dezvoltare ulterioară

Odată cu apariția onor noi circuite și a unor noi cerințe de procesare, se pot dezvolta noi tehnici de reducere a consumului de energie care să permită amplasarea în zone izolate și o funcționare cât mai îndelungată.

Informațiile prezentate în prima parte a capitolului 3 reprezintă punctul de plecare spre dezvoltarea unor noi tipuri de noduri de senzori care au la bază circuite hardware reconfigurabile. Menținerea consumului mic de energie se poate face prin perfecționarea modulului de management al activităților prezentat in capitolul 3. Modelul de simulare prezentat poate fi completat prin adăugarea unor noi funcționalități specifice noilor senzori de tip SoC.

Deoarece amenințările de securitate asupra nodurilor și a rețelelor de senzori vor evolua permanent, dezvoltarea unor noi mecanisme de securitate care să contracareze aceste amenințări, devine obligatorie.

Sursele de entropie prezentate pot fi folosite împreună cu modulele hardware care folosesc baze de date distribuite pentru a dezvolta noduri de senzori care datorită gradului ridicat de securitate pot fi folosiți în multe aplicații în care securitatea datelor este esențială.

Modulele hardware prezentate în capitolul 5 pot fi folosite în dezvoltările ulterioare ale nodurilor de senzori cu capacități ridicate de procesare.

Bibliografie

[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