UNIVERSITATEA „POLITEHNICA” din BUCUREȘTI

ȘCOALA DOCTORALĂ ETTI-B

Decizie nr. 515 din 01.07.2020

REZUMAT EXTINS

MODULE INTELIGENTE DESTINATE SECURIZĂRII ÎMPOTRIVA INTRUZIUNILOR ASUPRA ECHIPAMENTELOR ELECTRONICE

SMART MODULES FOR SECURING THE ELECTRONIC EQUIPMENT AGAINST TAMPERING

Doctorand: **Ing. Daniel-Ciprian Vasile**

COMISIA DE DOCTORAT

Președinte	**Prof. Dr. Ing. Gheorghe Brezeanu**	de la	**Univ. Politehnica București**
Conducător de doctorat	**Prof. Dr. Ing. Paul Svasta**	de la	**Univ. Politehnica București**
Referent	**Prof. Dr. Ing. Adriana Vlad**	de la	**Univ. Politehnica București**
Referent	**Prof. Dr. Ing. Alexandru Șerbănescu**	de la	**Academia Tehnică Militară**
Referent	**C. S. I. Dr. Fiz. Liviu Coșereanu**	de la	**INCD Aerospațială ”Elie Carafoli”**

BUCUREȘTI 2020

Cuprins

Lista figurilor

Lista abrevierilor

ADC - *Analog to Digital Converter*, convertor analog-digital
AI - *Artificial Intelligence*, inteligență artificială
ARM - familie de arhitecturi de procesoare (Arm Limited)
ASIC - *Application Specific Integrated Circuit*, circuit integrat specializat
CADI - circuit activ de detecție a intruziunilor
CDI - circuit de detecție a intruziunilor
CES - circuit electronic de securitate
DAC - *Digital to Analog Converter*, convertor digital-analogic
e-PTFE - *expanded-Polytetrafluoroethylene*, politetrafluoretilenă expandată
FLASH - memorie nevolatilă care poate fi ștearsă și reprogramată
FPGA - *Field Programmable Gate Array*, arie de porți programabile
GPIO - *General Purpose Input/Output*, port de intrare/ieșire de uz general
HASH - funcție de dispersie injectivă
HSM - *Harware Security Module* modul de securitate
Internet - sistem global de rețele de calculatoare interconectate
IoT - *Internet of Things*, interconectarea dispozitivelor prin Internet
IT - *Information Technology*, tehnologia informației
LDS - *Laser Direct Structuring*, imprimare 3D laser
LFSR - *Linear Feedback Shift Register*, registru de deplasare cu reacție liniară
NFSR - *Non-linear Feedback Shift Register*, registru de deplasare cu reacție neliniară
NVRAM - *Non-volatile RAM*, memorie RAM nevolatilă
PC - *Personal Computer*, calculator
PCB - *Printed Circuit Board*, circuit imprimat
PES - *Poly Ether Sulfone*, sulfonat polieter
POS - *Point Of Sale*, dispozitiv destinat plăților electronice
PWM - *Pulse Width Modulation*, modulația în durată a impulsurilor
RAM - *Random Access Memory*, memorie cu acces aleator
RF - radio-frecvență
SCA - *Side Channel Attacks*, atacuri pe canale colaterale
UART - *Universal Asynchronous Receiver-Transmitter*, comunicație serială asincronă

Capitolul 1

Introducere

1.1 Prezentarea domeniului de doctorat

Era digitală actuală are ca fundamente comunicațiile și procesarea datelor și este caracterizată de schimbări într-un ritm accelerat. Echipamentele electronice înglobează circuite electronice (*hardware*) și aplicații informatice (*software, firmware*) care implementează funcțiile acestora. Tehnologiile noi oferă nenumărate posibilități și domenii de dezvoltare, însă utilizarea lor poate expune utilizatorul la riscuri. Pentru resursele de valoare, precum informații, *hardware*, *software* și *firmware*, evaluarea acestor riscuri poate fi dificilă și depinde de mediul în care sunt localizate aceste resurse [1].

Securitatea resurselor informaționale face parte din evoluția oricărei organizații și este reprezentată prin protejarea profitului, asigurarea securității membrilor sau a valorilor deținute de aceștia. Acest profil poate fi definit, de asemenea, și pentru structuri și organizații de nivel național sau internațional. Costurile pe care le implică protejarea resurselor informaționale depind de fiecare sistem informatic și de comunicații. Pentru a fi un sistem eficient, costurile de securitate nu trebuie să depășească beneficiile realizate prin utilizarea resurselor protejate.

Circuitele electronice de securitate (CES) reprezintă modulele responsabile cu securitatea resurselor informaționale din cadrul echipamentelor electronice. Acestea conțin atât componente logice (precum porți logice, procesoare, memorii, circuite FPGA și CPLD, etc.) cât și componente analogice (surse de alimentare liniare, surse de zgomot, senzori etc.).

Datele de securitate reprezintă orice informație procesată în interiorul unui echipament electronic (date, funcții, protocoale, rutine *software* și *firmware*) pe care producătorul dorește să le protejeze împotriva accesului neautorizat. Aceste date de securitate sunt procesate în interiorul CES cu ajutorul circuitelor integrate dedicate care implementează aplicația informatică (*software* sau *firmware*).

Criptografia asigură mijloacele matematice necesare pentru protecția informațiilor în format digital (date de securitate). Acestea sunt formate din funcții, protocoale și principii pe care CES le implementează.

1.2 Scopul tezei de doctorat

Studiul cuprins în această teză de doctorat a avut ca scop găsirea de soluții inovatoare și eficiente pentru protejarea CES împotriva celor mai importante intruziuni, din punct de vedere al eficienței atacului criptanalitic, și anume intruziunile fizice și atacurile prin variația temperaturii. Soluţiile propuse în cadrul tezei constau în proiectarea unui înveliş cu caracteristici senzoriale care să protejeze CES, realizat dintr-o reţea conductivă, şi a unui circuit electronic care să analizeze modificarea caracteristicilor electrice ale reţelei conductive.

S-a urmărit ca structura fizică, ce constă într-o rețea conductivă specială, să asigure mai multe funcții de detecție, și anume: detecția scurt-circuitului și a întreruperii traseelor rețelei conductive, detecția variațiilor de temperatură și ecranarea circuitelor protejate.

În cazul circuitelor de detecție a intruziunilor s-au avut în vedere analizarea și testatarea experimentală a mai multor metode de detecție pentru stabilirea eficienței în cazurile de interes.

1.3 Conținutul tezei de doctorat

Capitolul 1 prezintă importanța circuitelor electronice de securitate în contextul comunicațiilor de date și al securității resurselor informaționale. Domeniile de utilizare ale acestor circuite sunt evidențiate în contextul tehnologiilor moderne.

Capitolul 2 conține un breviar al atacurilor asupra circuitelor electronice de securitate, precum criptanaliza, atacurile pe canale colaterale și intruziunile fizice.

Capitolul 3 descrie elementele componente ale unui circuit de detecție a intruziunilor și stadiul actual al soluțiilor disponibile în acest domeniu.

Capitolul 4 cuprinde contribuțiile aduse în dezvoltarea rețelelor conductive și a circuitelor active de detecție a intruziunilor, care funcționează în conjuncție cu acestea. Sunt studiate două tipuri de rețele conductive: rețea dublu strat și rețea triplu strat. Sunt prezentate metode de sondare a rețelelor conductive de către circuitele active de detecție a intruziunilor. Acestea pot detecta intruziunile fizice, tentativele de intruziuni și atacurile termice (variațiile de temperatură la nivelul rețelei conductive).

Capitolul 5 extinde domeniul de utilizare a sistemelor de detecție a intruziunilor, prezentate în capitolul 4, la protejarea circuitelor electronice de securitate sau a dreptului de autor asupra aplicațiilor informatice.

Capitolul 6 conține concluziile tezei de doctorat. Este structurat în subcapitole care evidențiază rezultatele obținute, contribuțiile originale, lista lucrărilor originale și perspectivele de dezvoltare ulterioară.

Bibliografia reprezintă ultimul capitol al tezei de doctorat și conține lucrările consultate în cadrul studiului doctoral.

Capitolul 2

Atacuri asupra circuitelor electronice de securitate

Un aspect important al securității CES este faptul că acestea trebuie să protejeze datele de securitate stocate sau utilizate în procesele din interiorul CES: chei criptografice, date secrete, parole, programe *firmware*, etc. Protecția trebuie să fie activă pe toată durata de viață a CES, necondiționat de prezența alimentării cu energie electrică. În acest sens, CES sunt protejate de circuite specializate, dotate cu senzori care monitorizează în permanență diferiți parametri de stare și detectează tentativele de intruziune, în condițiile asigurării unui consum redus de energie. Circuitele de detecție a intruziunilor sunt realizate cu elemente logice de tip circuite integrate specializate (ASIC), circuite programabile (FPGA, CPLD) sau microcontrolere, la care sunt atașați diferiți senzori dedicați acestui scop. În cazul detectării unei intruziuni, circuitul dedicat intreprinde acțiunea programată pentru a nu dezvălui datele de securitate, în general, constând în ștergerea rapidă a acestora. În mod uzual, datele de securitate sunt stocate într-o memorie volatilă de tip RAM iar ștergerea se execută prin întreruperea alimentării acesteia.

Tipuri de atacuri asupra circuitelor electronice de securitate.

Atacurile asupra CES pot fi grupate în următoarele categorii:

- **Criptanaliza sistemelor criptografice**;
- **Atacuri pe canale colaterale** (”*Side channel attacks*”);
- **Intruziuni fizice**.

2.1 Criptanaliza sistemelor criptografice

Criptanaliza studiază sistemele criptografice în scopul găsirii slăbiciunilor din funcțiile implementate în acestea ce ar putea ajuta la descifrarea datelor fără a se cunoaște cheia de cifrare [2]. În analiza de risc asociată atacurilor criptanalitice se consideră

că algoritmul de cifrare este cunoscut. Atacurile criptanalitice pot fi clasificate după tipul de informație pe care atacatorul o are la dispoziție [2], astfel:

- **Numai text cifrat (”*Ciphertext-only*”).** În cadrul acestui scenariu de atac se utilizează numai textul cifrat și se presupune că atacatorul are capabilități pasive de monitorizare a comunicației cifrate. Chiar dacă atacatorul nu cunoaște textul clar, el are totuși anumite informații despre textul clar.
- **Text în clar ales (”*Chosen-plaintext*”).** În acest scenariu, atacatorul are posibilitatea să aleagă textul în clar și să obțină textul cifrat corespunzător. În criptografia modernă criptanaliza diferențială este un exemplu tipic de atac cu text în clar ales. Acest atac este similar cu atacul cu text cifrat ales.
- **Text în clar ales, adaptiv (”*Adaptive chosen-plaintext*”).** Este asemănător cu atacul cu text în clar ales cu diferența că atacatorul alege textele în clar subsecvente pe baza informațiilor învățate din criptările anterioare.
- **Chei asociate (”*Related-keys*”).** Ca și în cazul atacului cu text în clar cunoscut, atacatorul obține acces la texte cifrate cu chei asociate. Cheile nu sunt cunoscute de atacator dar sunt într-o relație matematică cunoscută de acesta.

Atacurile criptanalitice pot fi caracterizate din punctul de vedere al resurselor necesare, astfel:

- **Timp.** Durata atacului depinde de numărul de pași ce trebuiesc efectuați.
- **Memorie.** Orice atac are nevoie de memorie pentru stocarea variabilelor și vectorilor de lucru. Fiecare tip de atac necesită un volum diferit de memorie.
- **Volumul de date necesar.** Funcție de tipul atacului, volumul de date necesar (text în clar, text cifrat) trebuie să aibă o anumită dimensiune.

2.2 Atacuri pe canale colaterale (”Side-channel attacks”)

Atacurile pe canale colaterale (”*Side-channel attacks*” - SCA) utilizează orice informație provenită, în mod neintenționat, din dispozitivele electronice care implementează funcții criptografice. Această informație poate fi sub următoarele forme [3] [4] [5]: durată de procesare, sunet, unde electromagnetice, putere disipată, curenți de alimentare, etc. Aceste atacuri depind de modul cum sunt proiectate CES și cum sunt implementate funcțiile criptografice.

În standardul FIPS 140-2 [6] sunt definite patru tipuri de atacuri SCA: analiza puterii, analiza duratelor de execuție, inducerea de erori și TEMPEST. Aceste atacuri sunt descrise astfel:

1. **Analiza puterii** (*"Power analysis"*). Atacurile bazate pe analiza puterii consumate pot fi împărțite în două categorii, **Analiza simplă a puterii** ("*Simple Power Analysis*" - SPA) și **Analiza diferențială a puterii** ("*Differential Power Analysis*" - DPA). SPA implică o analiză directă a formelor semnalelor ce caracterizează consumul de energie electrică și a duratelor de execuție a instrucțiunilor individuale de către un CES în cazul execuției unei funcții criptografice. DPA are același scop ca și SPA dar utilizează metode statistice avansate și tehnici specializate (de exemplu analiza timp-frecvență) pentru analiza variațiilor consumului de putere.

2. **Analiza duratelor de execuție** ("*Timing Analysis*"). Atacurile de tip analiză a duratelor se bazează pe măsurarea precisă a duratei de execuție a operațiilor matematice asociate cu o funcție criptografică. Informația de timp colectată este analizată pentru a determina relația dintre intrările CES și cheile criptografice utilizate de algoritmul sau procesul în cauză.

3. **Inducerea de erori** ("*Fault Induction*"). Atacurile de tip inducere de erori utilizează stimuli externi, cum ar fi, de exemplu, semnale radio din domeniul microundelor, temperaturi extreme și manipularea tensiunii de alimentare pentru a cauza erori de procesare ale CES. Analiza acestor erori și a modelului de apariție poate fi utilizată în ingineria inversă (*reverse engineering*) a aplicației care rulează în CES, în scopul dezvăluirii caracteristicilor de implementare a funcțiilor criptografice și, ulterior, a cheilor criptografice.

4. **TEMPEST**. Analiza TEMPEST implică detecția la distanță și colectarea informației din semnalele electromagnetice nedorite emise de un CES.

2.3 Intruziuni fizice

În afara măsurilor de protecție la atacuri criptanalitice sau atacuri pe canale colaterale, CES trebuiesc protejate la intruziuni fizice astfel încât accesul la componentele electronice ale acestuia să fie imposibil de realizat. Intruziunea fizică reprezintă orice acțiune ce are ca scop obținerea accesului la componentele electronice sau la traseele conductoare ce compun un circuit electronic. Conectarea la magistralele de date ale circuitelor logice din CES asigură obținerea de informații importante din cadrul proceselor interne ale acestuia.

Accesul neautorizat la circuitul electronic al CES poate produce daune însemnate, cum ar fi:

- Obținerea cheii secrete de cifrare. Acest fapt poate duce la descifrarea comunicațiilor dispozitivului care înglobează un CES sau descifrarea comunicațiilor din toată rețeaua la care este conectat modulul electronic. Astfel nu se mai poate asigura confidențialitatea datelor.

- Intervenția asupra mesajelor comunicate de CES prin modificarea lor în scopul obținerii de avantaje. Integritatea mesajelor nu mai poate fi asigurată.
- Asumarea identității CES de către o altă entitate. Un atacator poate transmite informații false către entitățile din rețea ca și cum ar fi transmise de CES în cauză.
- Modificarea mesajelor transferate în rețea în vederea introducerii de erori. Autenticitatea mesajelor este astfel compromisă.

2.3.1 Măsuri pentru reducerea atacurilor de tip intruziune fizică

Protecția împotriva atacurilor de tip intruziune fizică este caracterizată prin următoarele tipuri de acțiuni:

- *Detecția intruziunii (”**Tamper detection**”):* reprezintă determinarea automată, de către CES, a tentativei de compromitere a securității fizice.
- *Evidențierea intruziunii (”**Tamper evidence**”):* reprezintă indicația externă a echipamentului electronic ce conție CES referitoare la tentativa de compromitere a securității fizice.
- *Răspunsul la intruziune (”**Tamper response**”):* reprezintă acțiunea automată efectuată de CES imediat ce a detectat intruziunea. CES întreprinde acțiuni împotriva utilizării neautorizate sau dezvăluirii datelor de securitate stocate în acesta.

Capitolul 3

Circuite de detecție a intruziunilor - stadiul actual

3.1 Protecția circuitelor electronice de securitate împotriva intruziunilor fizice

Securitatea CES se realizează printr-un ansamblu de mecanisme de protecție organizate pe mai multe niveluri. Primul nivel este cel fizic: circuitele electronice componente sunt protejate de o carcasă specială, ce nu permite pătrunderea neautorizată la nivelul circuitului. Acestea sunt realizate din materiale metalice și îndeplinesc următoarele cerințe: sunt etanșe și nu prezintă fante sau perforații care ar putea favoriza accesul sondelor specializate (optice) la nivelul circuitelor electronice.

Al doilea nivel, cel mai important, îl reprezintă mecanismele de protecție ale circuitelor electronice și ale datelor de securitate. Un atacator nu trebuie să aibă acces la aceste circuite, însă, în cazul în care reușește să treacă de primul nivel de protecție, CES dispune de un circuit specializat care reacționează în vederea protejării datelor de securitate. Timpul de răspuns este foarte scurt iar efectul este complet, în sensul că toate datele de securitate sunt șterse.

Soluția care asigură acest nivel de protecție este introducerea, între carcasa metalică și circuitul protejat, a unui strat conductor special care este sensibil la intruziuni - rețeaua conductivă. Această rețea este sondată periodic cu semnale de circuitul de detecție a intruziunilor (CDI). În momentul în care acest circuit detectează o intruziune, execută funcțiile specifice de protecție a datelor de securitate: ștergerea rapidă a acestor date și executarea unei rutine speciale de ștergere a datelor sensibile din procesorul CES.

Funcție de modul în care sunt analizate semnalele de sondare a acestui strat de protecție, circuitele de detecție a intruziunilor se clasifică în circuite pasive și circuite active.

3.2 Rețele conductive

Pentru asigurarea unui nivel ridicat de protecție la intruziuni se folosesc rețelele conductive (*mesh networks*) realizate sub forma unui circuit imprimat care acoperă în întregime ansamblul format din CES și CDI [7]. Rețeaua conductivă poate fi flexibilă, realizată din folii imprimate subțiri, sau rigidă, realizată din cablaje imprimate (PCB) îmbinate astfel încât să nu rezulte fante care să faciliteze intruziunile sau introducerea de sonde pentru analizarea interiorului CES. Orice încercare de penetrare a acestor structuri determină generarea evenimentului de intruziune.

Pentru ca aceste rețele conductive să fie eficiente din punct de vedere al tentativelor de penetrare, atât lățimea traseelor cât și spațiul dintre ele trebuie să aibă dimensiuni reduse, în general mai mici de $0.2mm$.

3.3 Circuite pasive de detecție a intruziunilor

Circuitele pasive de detecție a intruziunilor se bazează pe monitorizarea unor mărimi electrice sau logice, variația acestor mărimi peste anumite limite determină declanșarea procesului de răspuns la intruziune (*"Tamper response"*). Funcție de regimul de consum utilizat, verificarea parametrilor se poate face în mod continuu sau la o perioadă predefinită.

Pentru asigurarea unei securități crescute a datelor de securitate (chei criptografice, secvențe aleatoare generate, alte date secrete), circuitele integrate destinate detecției intruziunilor pot fi dotate cu memorie RAM nevolatilă și ceas de timp real. Ceasul de timp real asigură marca de timp necesară în multe procese criptografice dar și înregistrarea momentului la care s-a detectat evenimentul de intruziune. Memoria RAM nevolatilă fiind parte componentă a circuitului integrat, este destinată stocării unei chei criptografice, necesară pentru cifrarea unor volume de date (programul *firmware* al CES, date de securitate, etc.).

3.4 Circuite active de detecție a intruziunilor

Circuitele active de detecție a intruziunilor (CADI) au la bază principiul testării rețelei conductive prin sondarea acesteia cu semnale având caracteristici alese în mod corespunzător. Semnalele de sondare sunt injectate în rețeaua conductivă, prin portul de intrare. La portul de ieșire al acesteia, semnalele sunt eșantionate și analizate, având ca referință semnalele inițiale. Schema de principiu a unui astfel de circuit este prezentată în figura 3.6.

În general, semnalele de sondare sunt impulsuri care au parametrii variabili (perioadă, durată, formă) pentru a face imposibilă reproducerea acestora în cazul unui atac de tip *bypass* (dezactivarea unei zone din rețeaua conductivă și injectarea unor impulsuri false).

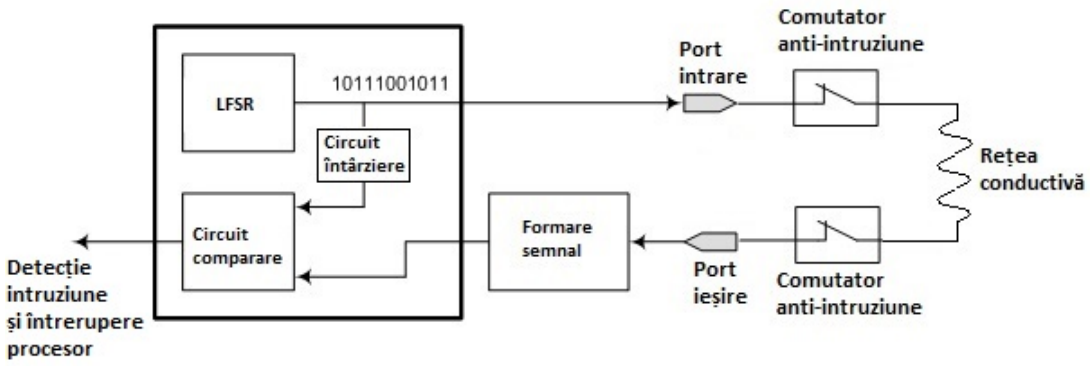


Figura 3.6: *Schema de principiu a unui circuit tamper activ.*

CADI analizează efectele pe care rețeaua conductivă le exercită asupra impulsurilor care se propagă prin aceasta. Pentru efectuarea acestei analize, semnalele rezultate la ieșirea rețelei conductive se eșantionează și se analizează în domeniile timp și frecvență. În acest mod, se poate exploata caracteristica dispersivă a rețelei conductive care protejează CES. Această metodă implică utilizarea unui convertor analog-digital rapid și efectuarea unui volum de calcule mai mare decât în cazul altor metode.

Ca și în cazul circuitelor pasive de detecție a intruziunilor, CADI poate fi afectat de perturbațiile electromagnetice atât din interiorul circuitului electronic protejat cât și din afara lui. Pentru a reduce acest efect este necesară ecranarea circuitului conductiv în interior și exterior. În acest fel, efectele perturbațiilor electromagnetice externe modulului format din CES și CADI vor avea un rol util în detecția intruziunilor prin afectarea semnalelor de sondare ca urmare a deteriorării voluntare a stratului extern de ecranare.

3.5 Structura unui circuit de protecție împotriva intruziunilor

CES sunt module care fac parte din echipamete electronice specializate, în principal dedicate protecției datelor și comunicațiilor. Modul în care CES interacționează cu circuitul de detecție a intruziunilor și a altor tipuri de atacuri este prezentat în figura 3.7. Circuitul de detecție monitorizează permanent senzorii, atât pe durata funcționării echipamentului cât și pe durata în care nu este alimentat. Pentru cazul în care acesta nu este alimentat (pe durata transportului, stocării sau a unor operații de mentenanță), circuitul de detecție se alimentează din bateria de rezervă. În cazul detecției unui astfel de acces (intruziune, modificarea în afara limitelor a temperaturii circuitului, modificarea tensiunii de alimentare, etc.), circuitul de detecție întrerupe alimentarea memoriei RAM nevolatile, pentru pierderea datelor de securitate, și generează o întrerupere către circuitul logic al CES (microprocesor, ASIC etc.) pentru executarea rutinei de ștergere a datelor din memoria RAM și regiștrii interni.

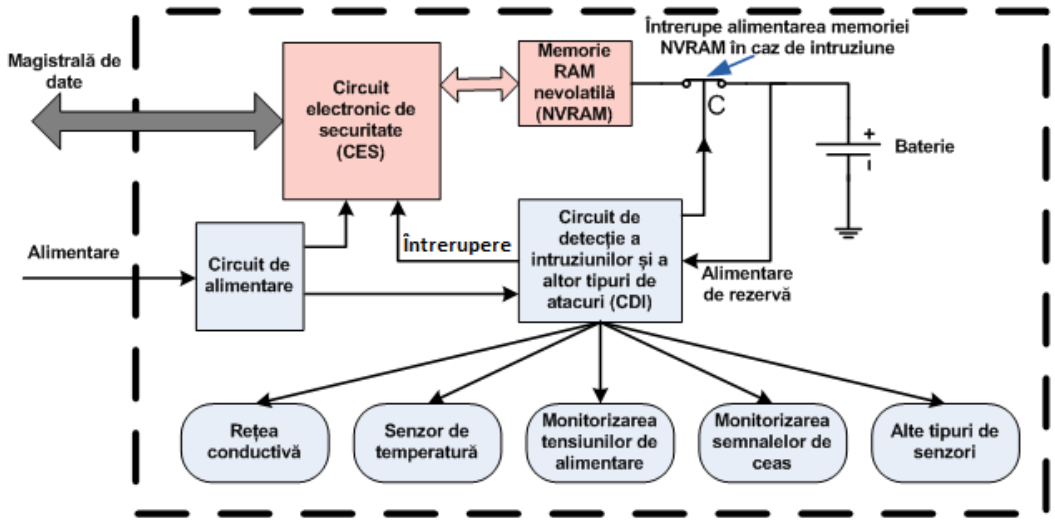


Figura 3.7: *Schema de principiu a unui circuit de protecție a CES.*

Senzorii utilizați de CDI sunt: rețeaua conductivă (pentru detecția intruziunilor fizice), senzori de temperatură, senzori pentru monitorizarea tensiunilor de alimentare, senzori pentru detecția variației frecvenței de ceas a procesorului și alte circuite cu funcții de monitorizare.

Pentru protejarea rețelei conductive față de factorii externi, inclusiv factori de natură electromagnetică, întreg circuitul de protecție al CES este introdus într-o incintă metalică rigidă. Această incintă protejează și împotriva intruziunilor fizice accidentale. În figura 3.8 este exemplificată această metodă de protecție a CES.

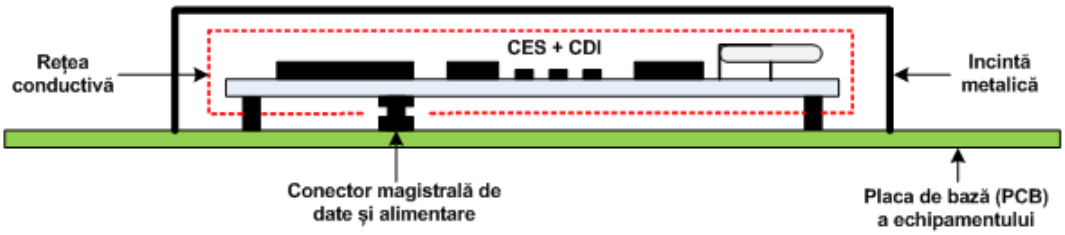


Figura 3.8: *Structura ansamblului format din CES și CDI.*

CES este acoperit complet de rețeaua conductivă, mai puțin conectorul prin care se alimentează acesta (în timpul funcționării) și se transferă datele. Incinta metalică, ce acoperă această structură, este conectată la planul de masă al echipamentului. Această incintă îmbunătățește stabilitatea în timp a circuitului de detecție a intruziunilor în sensul reducerii declanșărilor false ale evenimentelor de intruziune.

Capitolul 4

Circuite active de detecție a intruziunilor

4.1 Rețea conductivă inovativă dublu strat pentru circuite active de detecție a intruziunilor

Pentru izolarea traseelor conductive de eventualele perturbații electromagnetice proprii ale CES și CADI (acestea fiind protejate, ca ansamblu, de CADI), este necesară introducerea unui plan de masă de separație, conectat la potențialul de masă al CES și CADI. Astfel, circuitul imprimat va conține două straturi conductive (izolate printr-un strat dielectric): unul de masă și unul dedicat rețelei conductive. Stratul de masa va fi poziționat între modulul format din CES și CADI, și rețeaua conductivă.

Proiectarea ecranului electromagnetic flexibil

Pentru asigurarea unei flexibilități crescute a rețelei conductive, planul de masă este realizat sub formă hașurată cu perforații pătrate, cu latură de $0,5mm$, distanțate la $1mm$. Considerând că suprafețele ce compun rețeaua conductivă nu depășesc un pătrat cu laturile de $10cm$ (100 perforații / latură), eficiența de ecranare este de $89,5dB$.

Proiectarea rețelei conductive

Rețeaua conductivă are rolul de a împiedica efectuarea de intruziuni (perforări) în vederea obținerii accesului la CES și CADI. Este realizată sub forma unor trasee subțiri, având lățimea mai mică de $0.2mm$, cu spațiul dintre trasee de maxim $0,2mm$. Modelul traseelor este de tipul unor meandre ce acoperă întreaga suprafață, fără a lăsa spații neacoperite, și este realizat dintr-un singur circuit conductiv (prezintă o singură intrare și o singură ieșire accesibile la nivelul CADI). Un eșantion al rețelei conductive este prezentat în figura 4.1.

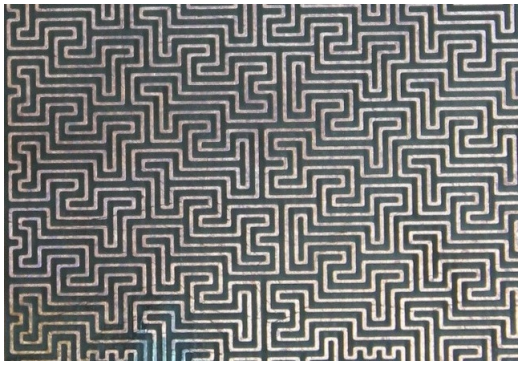


Figura 4.1: *Traseele rețelei conductive realizate pe un circuit PCB.*

Pentru efectuarea de teste experimentale, rețeaua conductivă a fost realizată dintr-un circuit imprimat (PCB) de tip sticlotextolit (FR4), cu două straturi de cupru, având grosimea de $0,035mm$. Circuitul imprimat are dimensiunea de $12,5 \times 25cm$, grosimea de $0.5mm$, iar traseele au lățimea și distanța dintre ele de $0,2mm$. Primul strat este format din trasee conductive cu modelul prezentat în figura 4.1, cel de-al doilea este format dintr-o folie completă de cupru conectat la planul de masă al CES și CADI.

4.2 Circuit activ de detecție a intruziunilor bazat pe generator LFSR

Circuitul de detecție a intruziunilor, studiat în cadrul lucrării [8], este compus dintr-un microcontroler, rețeaua conductivă prezentată în figura 4.1 și un circuit de formare a impulsurilor. Pentru realizarea testelor și măsurătorilor, s-a folosit placa de dezvoltare STM32F4-DISCOVERY (conține microcontrolerul STM32F407VG). Schema funcțională a acestui circuit este prezentată în figura 4.2.

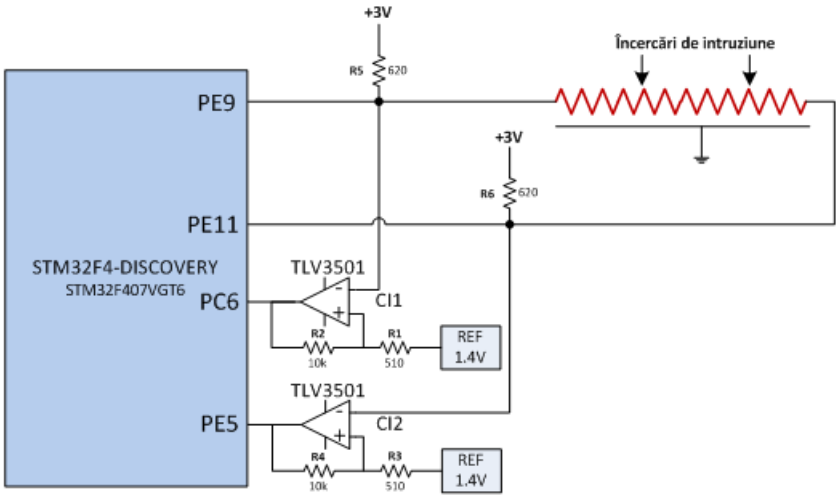


Figura 4.2: *Schema funcțională a CADI.*

Microcontrolerul generează impulsuri la ambele capete ale rețelei conductive în scopul mascării sursei impulsurilor de sondare și inducerii în eroare a unui eventual atacator care ar încerca simularea acestor impulsuri. Pinii GPIO PE9 și PE11 sunt conectați la rețeaua conductivă și sunt configurați ca ieșiri cu drenă deschisă (*open-drain*) pentru canalele 1 și 2 ale circuitului intern de ceas *Timer 1*, în modul PWM (*Pulse Width Modulation*). Acești pini de ieșire sunt configurați în modul *drenă deschisă* pentru a realiza funcția logică *ȘI* necesară în cadrul acestei aplicații. Schema echivalentă, cu parametrii concentrați, este prezentată în figura 4.3.

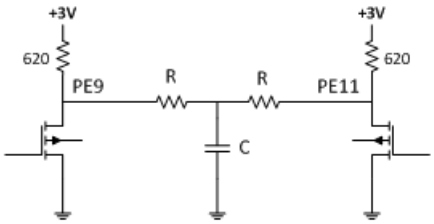


Figura 4.3: *Schema echivalentă a rețelei conductive conectate la pinii PE9 și PE11.*

Principiul de generare și achiziție al impulsurilor de sondare

Impulsurile de sondare sunt sincronizate cu ajutorul unui generator de secvențe pseudo-aleatoare LFSR (*Linear-Feedback Shift Register*). Pentru circuitul CADI s-a utilizat o configurație tip cascadă Gollmann modificată, așa cum este prezentată în [9]. Schema logică a acestui generator este prezentată în figura 4.4:

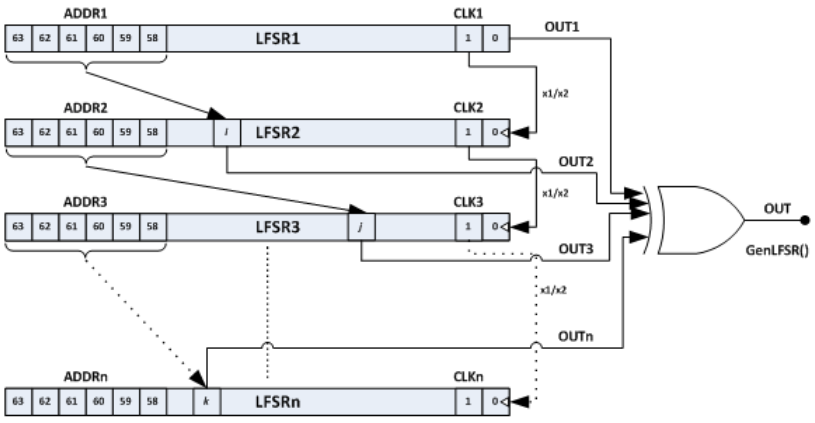


Figura 4.4: *Schema logică a generatorului pseudo-aleator bazat pe cascada Gollmann.*

Acest generator este utilizat pentru a decide care impulsuri sunt active la porturile de ieșire PE9 și PE11 (configurate ca funcție alternativă 1 - TIM1_CH1, respectiv, TIM1_CH2). *Timer 1* este configurat în modul generare PWM cu frecvența de 250kHz și este sincronizat de semnalul intern de ceas al microcontrolerului (cu frecvența de 168MHz). La fiecare perioadă de $4\mu s$, *Timer 1* intră în rutina de intrerupere și, pe baza ieșirii generatorului LFSR, programul stabilește dacă se

generează impulsul de sondare. Dacă generatorul LFSR produce un bit 0, atunci ieșirea *Timer 1* este dezactivată, în caz contrar generatorul LFSR furnizează doi biți ce vor determina parametrii impulsurilor generate.

Relația dintre $D1$ și $D2$ este $D2 = D1 + d$, unde d este durata de propagare a impulsurilor prin rețeaua conductivă, în acest caz particular $d = 162ns$.

Modul de compunere al impulsurilor este prezentat în figura 4.5 și este valabil în orice punct al rețelei conductive și se datorează faptului că porturile PE9 și PE11 sunt configurate în modul drenă deschisă pentru a obține funcția logică ȘI (*AND*).

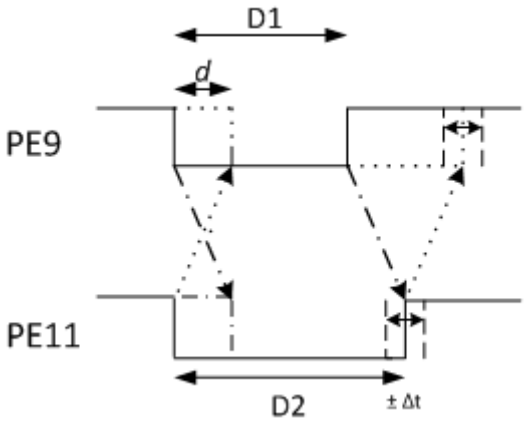


Figura 4.5: *Modul de compunere a impulsurilor de sondare a rețelei conductive.*

Formatorul de impulsuri

Circuitul de formare a impulsurilor este realizat cu ajutorul comparatorului TLV3501 [10] [11], folosit în configurație de comparator cu histerezis pentru a crește imunitatea la zgomot. Imunitatea la zgomot este necesară deoarece impulsurile au fronturi lente și comparatorul poate produce oscilații la ieșire în momentele în care semnalul de intrare are valori în apropierea nivelului de prag.

Analiza impulsurilor detectate

Impulsurile produse de circuitul de formare, realizat cu comparatoare, sunt analizate de circuitele de ceas *Timer 8*, canalul 1 (TIM8_CH1), și *Timer 9*, canalul 1 (TIM9_CH1), conectate la pinii PC6 și, respectiv, PE5 (configurați ca funcție alternativă 3). Aceste circuite de ceas sunt configurate în modul de analiză PWM și îndeplinesc funcția de detecție a perioadelor și duratelor impulsurilor.

Pentru demonstrarea funcționării CADI, a fost realizat circuitul experimental prezentat în figura 4.6. Acest circuit conține toate modulele prezentate anterior: circuitul imprimat (PCB) al rețelei conductive (partea stîngă a figurii), circuitul de formare a impulsurilor (partea dreaptă a figurii) și placa de dezvoltare STM32F4-Discovery (partea centrală a figurii).

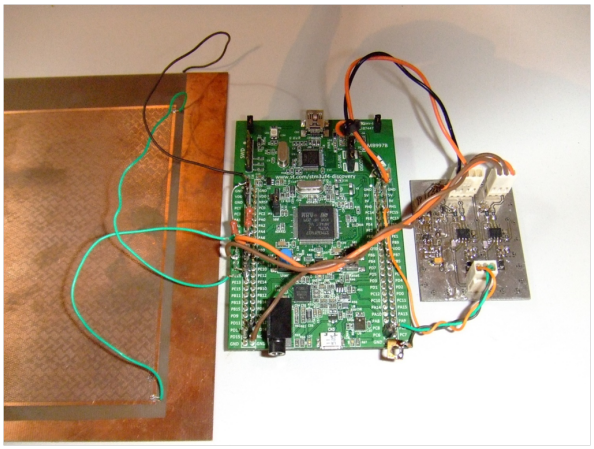


Figura 4.6: *Circuitul experimental de detecție a intruziunilor.*

Impulsurile măsurate la nivelul pinilor PE9, PE11, PC6 și PE5 sunt prezentate în figura 4.8, canalele 1 la 4.

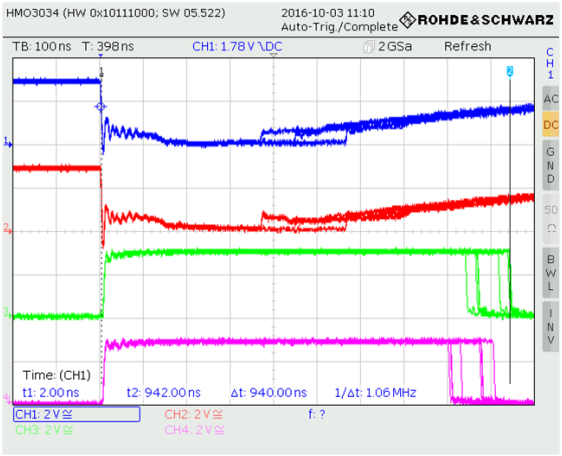


Figura 4.8: *Detaliu captură impulsuri la nivelul pinilor PE9, PE11, PC6 și PE5.*

Metoda propusă de generare a impulsurilor de sondare, bazată pe o schemă complexă de generator LFSR, împreună cu principiul de compunere a acestora pe durata propagării prin rețeaua conductivă nu permit determinarea parametrilor impulsurilor și simularea funcționării normale a circuitului de detecție.

În urma testelor experimentale, CADI atinge următoarele performanțe:

- detectează variații ale duratelor între impulsuri mai mari de $5,9ns$;
- detectează variații ale duratelor impulsurilor mai mari de $5,9ns$;
- detectează creșterea capacității totale a rețelei conductive cu cel puțin $22pF$;
- detectează intruziunile fizice realizate prin tăierea rețelei conductive și orice intervenție care poate modifica durata și amplitudinea semnalelor prin aceasta.

4.3 Circuit activ de detecție a intruziunilor bazat pe analiza răspunsului la impulsuri a rețelei conductive

Analiza impulsurilor de sondare de la ieșirea rețelei conductive prin măsurarea duratelor între fronturi poate fi îmbunătățită în sensul creșterii sensibilității în detectarea tentativelor de intruziune. Circuitul propus analizează întârzierea impulsurilor și puterea spectrală totală. CADI este compus dintr-un circuit de procesare, un circuit de achiziție și o rețea conductivă [12]. Schema de principiu este prezentată în figura 4.11.

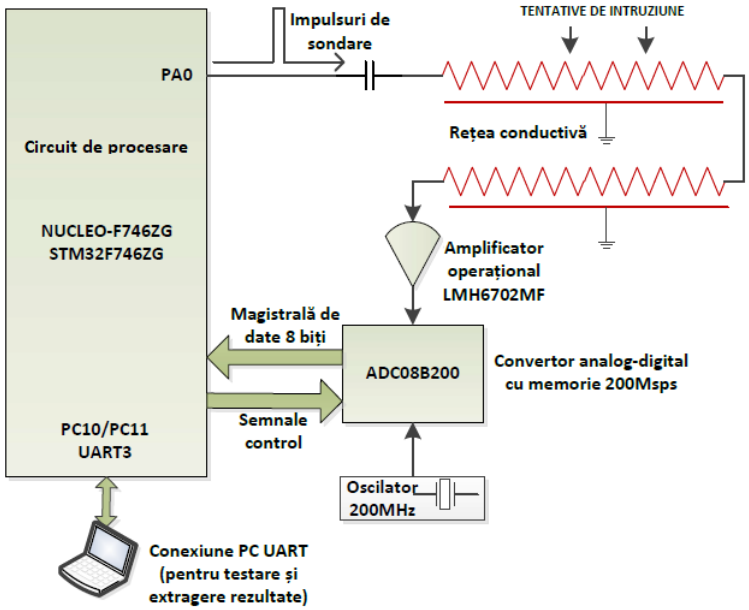


Figura 4.11: *Schema de principiu a CADI.*

Circuitul de procesare generează impulsuri cu durată variabilă, cu perioadă de o secundă, care sunt aplicate rețelei conductive pe portul de intrare, prin cuplaj capacitiv. Aceste impulsuri se propagă prin rețeaua conductivă iar semnalele de la portul de ieșire sunt amplificate și adaptate, utilizând un amplificator operațional, pentru a fi achiziționate de către convertorul analog-digital. Datele achiziționate sunt analizate pentru a detecta intruziunile fizice.

Circuitul de procesare

Placa de dezvoltare NUCLEO-F746ZG constituie circuitul de procesare, așa cum este prezentat în figura 4.11. Aceasta conține microcontrolerul STM32F746ZG. Portul de ieșire PA0 este utilizat pentru generarea de impulsuri scurte cu durate determinate de un generator LFSR, implementat în software. Microcontrolerul STM32F746ZG controlează convertorul analog-digital, stabilind momentele la care acesta începe conversia. Datele achiziționate sunt stocate temporar la nivelul convertorului analog-digital. La finalul achiziției, microcontrolerul citește din acesta

256 eșantioane a câte 8 biți fiecare.Eșantioanele sunt analizate în scopul măsurării întârzierilor și calculării puterii componentelor spectrale.

Circuitul de achiziție

Circuitul de achiziție este format din două componente: amplificatorul operațional LMH6702 și convertorul analog-digital ADC08B200. Circuitul de amplificare și achiziție este prezentat în figura 4.13.

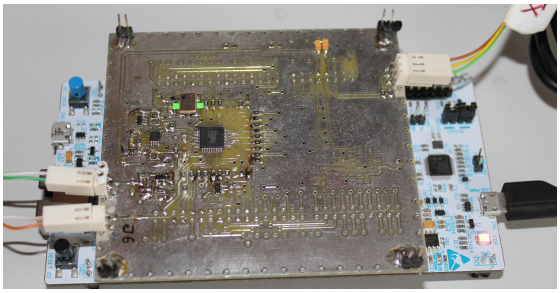


Figura 4.13: *Circuitul de amplificare și achiziție.*

ADC08B200 este un convertor analog-digital pe 8 biți cu frecvența maximă de eșantionare de 210Msps. Dispune de o memorie de stocare cu dimensiunea selectabilă de 256, 512 sau 1024 octeți. Pentru această aplicație au fost suficiente 256 de eșantioane, convertorul fiind configurat pentru această dimensiune.

Rețeaua conductivă utilizată este cea prezentată în secțiunea 4.1.

Principiul de funcționare

Circuitul de procesare (NUCLEO-F746ZG) generează impulsuri scurte, cu durate variabile, care alimentează portul de intrare al rețelei conductive prin cuplaj capacitiv. Semnalele rezultate la portul de ieșire al rețelei conductive sunt preluate de circuitul de achiziție. Acesta amplifică semnalele cu ajutorul amplificatorului operațional LMH6702 și apoi le eșantionează cu convertorul ADC08B200. Eșantioanele astfel rezultate (256 octeți) sunt citite de microcontrolerul STM32F746ZG, din cadrul circuitului de procesare.

În vederea detectării unei eventuale intervenții asupra rețelei conductive, eșantioanele sunt analizate urmărind două aspecte: întârzierea impulsurilor (domeniul timp) și puterea componentelor spectrale (domeniul frecvență).

Analiza în domeniul timp

Utilizând funcția *arm_max_f32*, microcontrolerul detectează poziția valorilor de vârf ale impulsurilor din datele achiziționate, reprezentând întârzierea impulsurilor la portul de ieșire al rețelei conductive.

Analiza în domeniul frecvență

CADI analizează răspunsul rețelei conductive în domeniul frecvență. Modificarea caracteristicilor impulsurilor de sondare poate fi analizată prin densități spectrale de energie a secvenței semnalului eșantionat. Pentru sondarea rețelei conductive s-au utilizat impulsuri cu durate de $13,6ns$, $22,4ns$, $35ns$ și $46,4ns$. Testarea rețelei conductive s-a făcut în următoarele condiții: nicio intervenție, adăugarea unui condensator în paralel (cu capacități de $8pF$, $22pF$ și $33pF$) și adăugarea unui rezistor în serie (cu rezistențe de 1Ω, 5Ω și 10Ω). Scopul acestor experimente este de a analiza răspunsul CADI la tentative de intruziune. În figurile 4.22 și 4.23 sunt prezentate grafic valorile puterii spectrale pentru impulsuri de $46,4ns$.

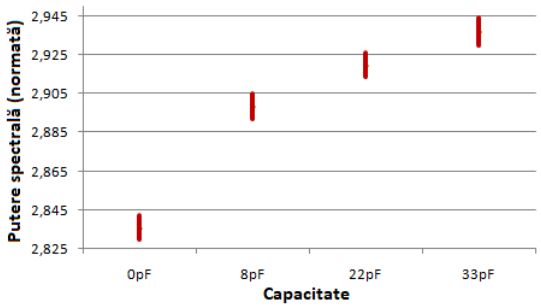


Figura 4.22: *Variația puterii spectrale pentru impulsuri de 46,4ns în cazul creșterea capacității în paralel cu rețeaua conductivă (putere normată, x10^{-4}).*

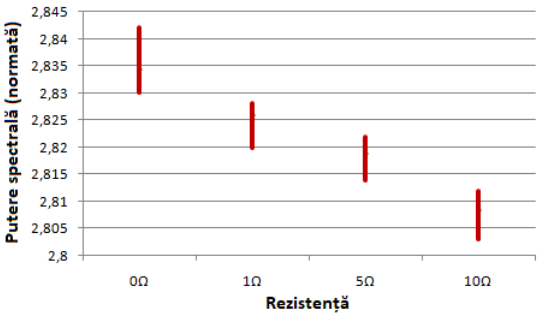


Figura 4.23: *Variația puterii spectrale pentru impulsuri de 46,4ns în cazul creșterii rezistenței în serie cu rețeaua conductivă (putere normată, x10^{-4}).*

Circuitul activ de detecție a intruziunilor (CADI) poate determina variații ale întârzierii impulsurilor mai mari de $5ns$.

Conform acestor rezultate, analiza semnalelor cu o sondă standard de osciloscop ($8pF/1M\Omega$) poate fi detectată prin utilizarea impulsurilor de sondare cu durate de $22,4ns$, $35ns$ și $46,4ns$. De asemenea, creșterea rezistenței totale a traseului rețelei conductive cu cel puțin 1Ω este detectată pentru impulsuri de cel puțin $22,4ns$. CADI poate detecta intruziunile și tentativele de intruziune cu un grad mare de certitudine pentru impulsuri de sondare cu durate de $22,4ns$, $35ns$ și $46,4ns$.

4.4 Circuit activ de detecție a intruziunilor cu funcție dublă: detecția variațiilor de temperatură și detecția intruziunilor prin metode statistice

În această secțiune este propus un CADI care, pe lângă detecția intruziunilor fizice, poate detecta variația temperaturii la nivelul învelișului de protecție format din rețeaua conductivă. Din punct de vedere al securității CES, este mult mai eficient a detecta depășirea limitelor temperaturii la nivelul învelișului exterior al ansamblului format din CES și CADI decât realizarea acestei funcții la nivelul circuitului imprimat (PCB).

În completarea măsurilor de protecție la atacurile pe canale colaterale bazate pe variația temperaturii, lucrarea oferă și o soluție pentru detecția intruziunilor prin analiza statistică a răspunsului rețelei conductive la sondarea cu impulsuri.

Analiza comportării CADI la variațiile de temperatură, la nivelul rețelei conductive, are la bază studiul realizat în cadrul lucrării [13]. Metodele statistice de detecție a intruziunilor au fost studiate în cadrul lucrării [14]. Analiza experimentală s-a realizat cu ajutorul circuitului electronic prezentat în figura 4.11.

Analiza răspunsului rețelei conductive la variații de temperatură

Având în vedere variația parametrilor rezistență și capacitate, ce caracterizează traseele rețelei conductive, impulsurile de sondare care se propagă prin această structură sunt afectate în mod diferit la temperaturi diferite. De aceea, calcularea puterii semnalelor, la ieșirea rețelei conductive, reprezintă o metodă eficientă de detecție a variațiilor caracteristicilor acestui mediu de propagare funcție de variația temperaturii. Calculele s-au efectuat în formatul virgulă flotantă, simplă precizie, utilizând instrucțiuni native ale microcontrolerului.

Analiza statistică a răspunsului rețelei conductive

Pentru detectarea intruziunilor fizice, o soluție mai economică din punct de vedere energetic (cu un număr redus de calcule) este abordarea statistică pentru analiza semnalelor eșantionate. Parametrii statistici utilizați în această lucrare sunt: media aritmetică, media rădăcină pătratică (RMS), deviația standard și varianța. CADI calculează acești parametrii statistici și îi compară cu valori de referință pentru a detecta tentativele de intruziune fizică.

Răspunsul CADI la variații de temperatură

Testele de variație a temperaturii au fost realizate utilizând camera termică ESPEC Temperature Chamber, model SH-241. Testele au fost efectuate prin variația temperaturii în domeniul $-20^oC \div 100^oC$, cu stabilizarea temperaturii la fiecare treaptă de temperatură (trepte de 10^oC).

Valorile achiziționate ale puterii normate a semnalului sunt prezentate în figura 4.26. Aceste valori sunt utilizate pentru comparații relative în scopul stabilirii apariției situației de intruziune fizică. Din datele analizate, se observă variația cvasi-liniară a puterii, cu pantă negativă în cazul creșterii temperaturii. CADI este capabil să detecteze fără ambiguitate temperatura la nivelul rețelei conductive.

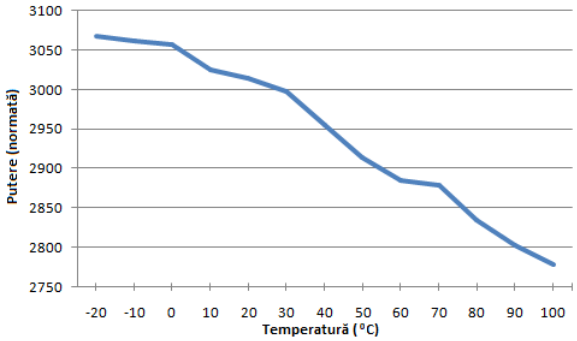
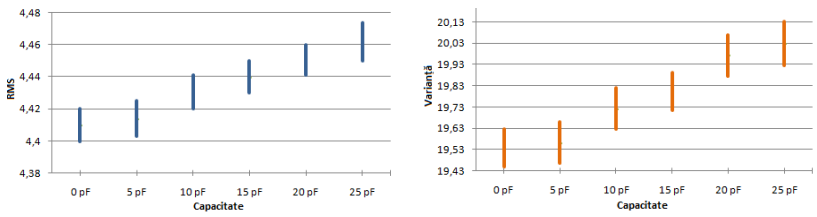


Figura 4.26: *Puterea normată a semnalului de sondare funcție de temperatură.*

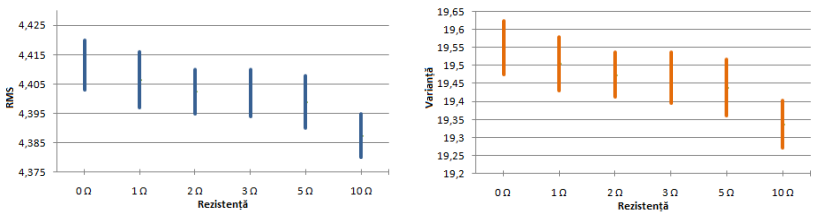
Detecția intruziunilor pe baza analizei statistice

Testarea experimentală a simulat o posibilă intervenție asupra rețelei conductive și constau în creșterea capacității în paralel cu rețeaua conductivă(condensatoare cu capacități de 5pF, 10pF, 15pF, 20pF, 25pF) și a rezistenței în serie cu rețeaua conductivă (rezistoare cu rezistențe de 1Ω, 2Ω, 3Ω, 5Ω, 10Ω). Rezultatele experimentale sunt reprezentate grafic în figurile 4.27 și 4.28. Rezultatele experimentale demonstrează eficiența CADI pentru creșterea rezistenței serie cu mai mult de 10Ω și creșterea capacității totale cu mai mult de 10pF.



(a) *RMS* ***(b)*** *varianță*

Figura 4.27: *Variația parametrilor statistici funcție de creșterea capacității.*



(a) *RMS* ***(b)*** *varianță*

Figura 4.28: *Variația parametrilor statistici funcție de creșterea rezistenței.*

4.5 Rețea conductivă inovativă cu structură triplu strat – creșterea eficienței în detecția intruziunilor

Rețelele conductive utilizate în protecția CES au ca cerințe principale asigurarea unei sensibilități crescute la tentativele de penetrare fizică a acesteia și imposibilitatea replicării semnalului de sondare folosit de CADI.

Studiul cuprins în această secțiune are la bază articolul [15] și propune un tip inovativ de rețea conductivă realizată din trei straturi conductive, izolate cu straturi dielectrice. Primul strat, dispus spre interior, este un strat compact conectat la potențialul de masă și are două roluri importante: plan de referință pentru semnalele de sondare și ecran electromagnetic între ansamblul format din CES și CADI și traseele conductive sondate cu semnale (straturile 2 și 3). Stratul 2 (intermediar), conține o rețea conductivă foarte fină (trasee cu grosime $<$ 0,2mm și cu distanțe între ele $<$ 0,2mm) cu model tip meandre. Acesta este stratul utilizat de CADI pentru analiza semnalelor de sondare. Cel de-al treilea strat, spre exterior, nu este sondat în mod direct de CADI însă este utilizat pentru a facilita detecția intruziunilor. Geometria traseelor de pe acest strat o copiază pe cea de pe stratul intermediar, cu diferența că acestea formează circuite închise. Pentru a determina modul de comportare al rețelei conductive în cazul intruziunilor fizice, s-a utilizat structura prezentată în figura 4.29.

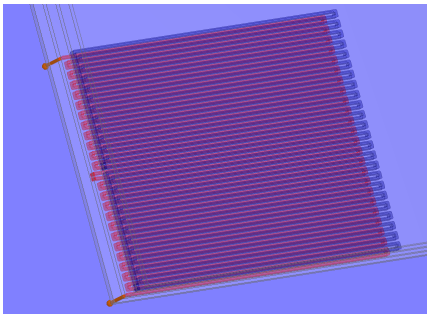


Figura 4.29: *Structura geometrică a rețelei conductive utilizate în simulare.*

Analizând semnalele induse în stratul 3, această structură nu permite determinarea caracteristicilor semnalelor de sondare utilizate de CADI. Aceste semnale au amplitudini foarte mici și nu dispun de un plan de masă de referință, fiind circuite izolate galvanic de restul structurii. În cazul în care un atacator ar încerca să se conecteze la traseele conductive ale stratului 2, ar trebui să dezafecteze zone ale rețelei conductive de pe stratul 3.

A fost proiectată o rețea conductivă cu dimensiunea de $30mm \times 30mm$ cu meandre ce realizează cuplaje inductive și capacitive la diferite lungimi de propagare ale semnalului în scopul producerii de rezonanțe multiple la frecvențe scăzute. Pentru simularea acestei rețele conductive, prezentată în figura 4.35, a fost utilizată aplicația ANSYS®SIwave 2016.2.0.

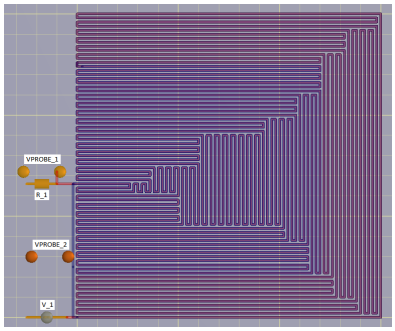


Figura 4.35: *Rețea conductivă îmbunătățită.*

Simularea s-a realizat în domeniul de frecvență $0Hz \div 500MHz$. Rezultatele simulării pentru această structură sunt prezentate în figura 4.36, pentru cazul în care stratul de detecție este neafectat, și în figura 4.37 pentru cazul în care s-a efectuat intruziunea fizică.

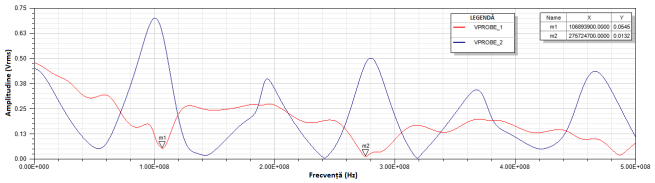


Figura 4.36: *Rețea conductivă neafectată de intruziune: traseul roșu - amplitudinea semnalului pe rezistorul R_1, traseul albastru - amplitudinea semnalului măsurat într-un punct pe traseul conductiv de pe stratul 3.*

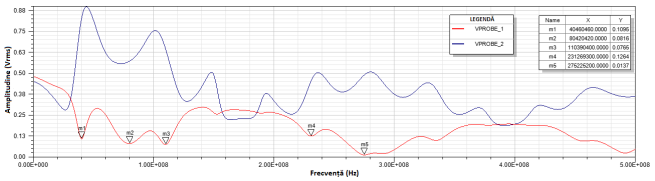


Figura 4.37: *Rețea conductivă afectată de intruziune: traseul roșu - amplitudinea semnalului pe rezistorul R_1, traseul albastru - amplitudinea semnalului măsurat într-un punct pe traseul conductiv de pe stratul 3.*

În momentul creării intruziunii, din cele două grafice, se observă creșterea punctelor de rezonanță și scăderea frecvențelor la care au loc aceste rezonanțe. Utilizând o metodă corespunzătoare pentru analiza acestor rezonanțe, un CADI poate detecta rapid o intruziune fără a expune calea de semnal către atacator. Structuri asemănătoare celei prezentate în figura 4.35 pot fi asociate pentru a obține suprafața necesară pentru acoperirea întregului CES. Pe stratul 2 traseele conductive se conectează în serie, pentru crearea căii de semnal, iar pe stratul 3 fiecare zonă formează câte un circuit închis.

Rețea conductivă triplu strat - structură extinsă

În cadrul lucării [16] s-a evaluat comportarea în domeniul frecvență a unei structuri formate din două zone pătrate, cu laturile de $30mm$, traseele și spațiile dintre ele având lățimea de $0,2mm$. Această structură este prezentată în figura 4.40. Principiul de utilizare al ansamblului format din această rețea conductivă și CADI a fost propus spre publicare în cadrul cererii de brevet de invenție [17].

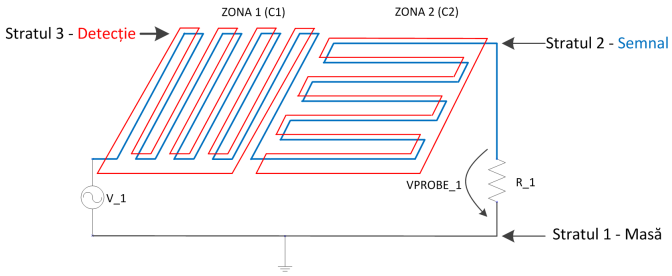


Figura 4.40: *Structura rețelei conductive formată din două zone active.*

După cum se observă în figura 4.40, pe stratul 2, traseele conductive ale celor două zone sunt conectate în serie iar cele de pe stratul 3 formează circuite închise, corespunzătoare fiecărei zone. Pentru validarea efectului de detecție al rețelei conductive, aceasta a fost realizată practic sub forma unui cablaj imprimat PCB, cu grosimea dielectricului de $0,3mm$, cu aceleași caracteristici ca modelul simulat. Au fost analizate următoarele cazuri: fără intruziuni, C1 afectat de intruziune și C2 afectat de intruziune. Rezultatele sunt prezentate în figura 4.43.

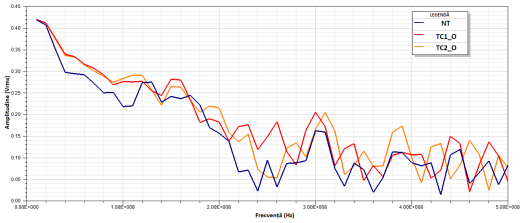


Figura 4.43: *Caracteristica de ieșire a rețelei conductive (simulare): NT - fără intruziune, TC1_O - C1 circuit deschis, TC2_O - C2 circuit deschis.*

Caracteristica de ieșire a rețelei conductive realizată practic este prezentată în figura 4.45. Așa cum se observă din figurile 4.43 și 4.45, începând cu frecvența de $30MHz$, rețeaua conductivă este eficientă în detectarea intruziunilor de tip circuit deschis. Diferențele de amplitudine între starea neafectată și cea afectată de intruziune a rețelei conductive sunt ușor cuantizabile pentru domenii extinse de frecvență.

Rețea conductivă triplu strat - analiza intruziunilor de tip scurt-circuit

Intruziunile fizice asupra rețelelor conductive se pot efectua, în afară de întreruperea traseelor conductive, și prin crearea de scurt-circuite între trasee alăturate.

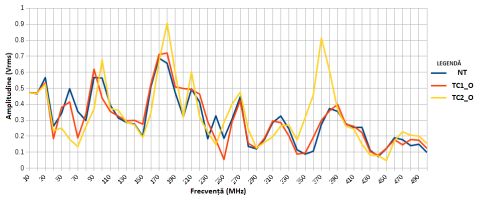


Figura 4.45: *Caracteristica de ieşire a reţelei conductive (testare experimentală): NT - fără intruziune, TC1_O - C1 circuit deschis, TC2_O - C2 circuit deschis.*

Considerând circuitul prezentat anterior, au fost analizate, prin simulare și testare experimentală [18], următoarele cazuri: rețea conductivă neafectată, scurt-circuit între două trasee alăturate și întreruperea traseului conductiv. S-a testat o rețea conductivă realizată pe folie PES (*Poly Ether Sulfone*) cu grosimea de $0,1mm$, imprimată cu pastă conductivă SW180 (Tatsuta Electric Wire & Cable Co. Ltd.). Rezultatul simulării este prezentat în figura 4.48.

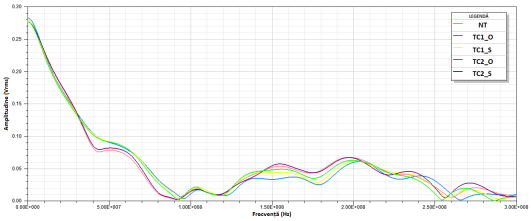


Figura 4.48: *Caracteristica de ieşire a reţelei conductive (simulare): NT - fără intruziune, TC1_O - C1 circuit deschis, TC1_S - C1 scurt-circuit între trasee, TC2_O - C2 circuit deschis, TC2_S - C2 scurt-circuit între trasee.*

Rețeaua conductivă prezintă domenii extinse de frecvență utile în detecția intruziunilor. Pentru validarea efectelor intruziunilor asupra rețelei conductive, aceasta a fost realizată practic și testată în aceleași condiții cu modelul utilizat în simulări. Măsurătorile efectuate sunt prezentate în figura 4.52.

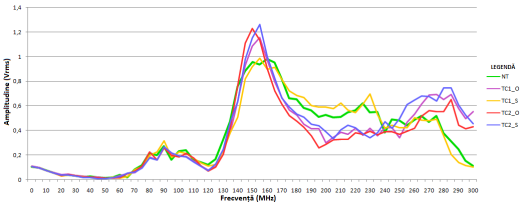


Figura 4.52: *Caracteristica de ieşire a reţelei conductive (testare experimentală): NT - fără intruziune, TC1_O - C1 circuit deschis, TC1_S - C1 scurt-circuit între trasee, TC2_O - C2 circuit deschis, TC2_S - C2 scurt-circuit între trasee.*

Începând cu frecvența de $85MHz$ această structură poate fi utilizată în detectarea sigură a intruziunilor de tip circuit deschis și scurt-circuit între trasee alăturate. Cele două moduri de analiză a rețelei conductive (simulare și testare experimentală) demonstrează eficiența acesteia în detectarea intruziunilor de tip întrerupere sau scurt-circuit efectuate pe stratul de detecție (3).

4.6 Aspecte tehnologice ale realizării rețelelor conductive pe folii flexibile dielectrice

Rețeaua conductivă imprimată pe folie PES a fost realizată cu ajutorul tehnologiei de imprimare serigrafică. Pentru realizarea rețelei conductive a fost conceput un proiect grafic care ulterior a fost transpus într-o sită serigrafică cu țesătură metalică. Imprimarea s-a realizat cu pasta conductivă SW180 (TATSUTA) și echipamentul de imprimarea tip DEK Horizon 08. În figura 4.56 sunt prezentate detalii ale foliilor imprimate cu pasta conductivă SW180 pe folie PES (trasee cu grosimea de $0.2mm$).

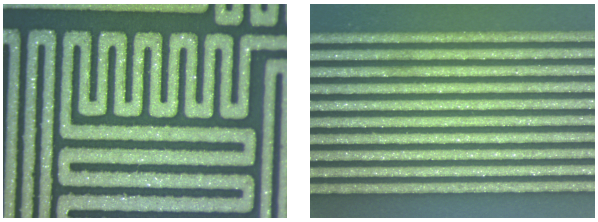
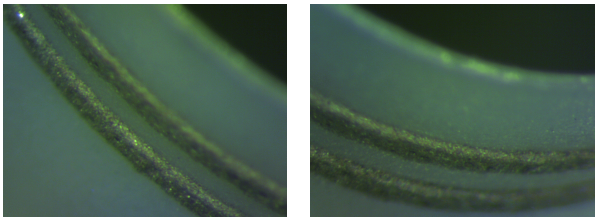
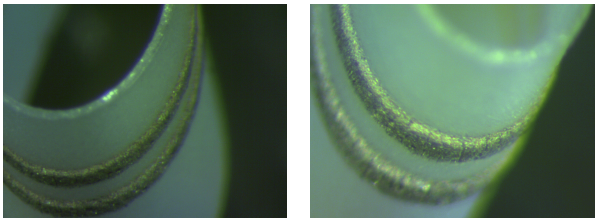


Figura 4.56: *Traseele conductive imprimate cu pasta SW180.*

O proprietate importantă a rețelei conductive este capacitatea acesteia de a fi împăturită fără a produce întreruperea traseelor conductive. A fost testată o mostră de rețea conductivă, formată din două trasee liniare, prin îndoire sub diferite raze. Testele, prezentate în figura 4.58, relevă faptul că rețeaua conductivă poate fi îndoită cu o rază minimă de 2mm fără producerea de fisuri.



(a) *rază* $3mm$. ***(b)*** *rază* $2mm$.



(c) *rază* $1mm$. ***(d)*** *rază* $0.5mm$.

Figura 4.58: *Testarea foliei PES* $0.1mm$ *la îndoire sub diferite raze de curbură. Pentru raze mai mici de* $2mm$ *apar fisuri ale traseelor conductive.*

Un aspect important al acestui tip de pastă conductivă este faptul că aceasta are o rezistență mecanică limitată, ceea ce constituie un avantaj în realizarea de rețele conductive pentru detecția intruziunilor.

4.7 Circuit activ de detecție a intruziunilor specializat, destinat rețelelor conductive triplu strat

Rețeaua conductivă cu structură triplu strat asigură funcția de detecție a intruziunilor prin analiza variației caracteristicii de ieșire amplitudine-frecvență. Pentru realizarea protecției anti-intruziune a CES, s-a proiectat un CADI [19] [20] ce utilizează acest tip de rețea conductivă. Schema de principiu este prezentată în figura 4.59.

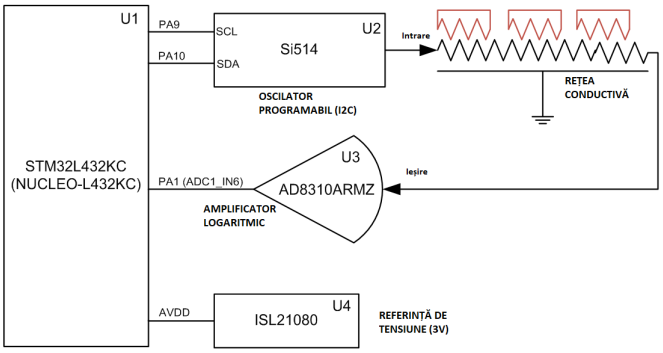


Figura 4.59: *Schema de principiu a CADI destinat sondării rețelei conductive triplu strat.*

CADI conține, ca element de procesare, microcontrolerul STM32L432KC (U1 în figura 4.59), parte componentă a modulului de dezvoltare NUCLEO-L432KC. Rețeaua conductivă este sondată cu impulsuri formate din semnale sinusoidale, cu frecvențe predefinite. Aceste impulsuri, cu frecvențe corespunzătoare sondării rețelei, sunt generate cu ajutorul oscilatorului programabil Si514, conectat la microcontroler prin intermediul unui port I2C (pinii $PA9$ și $PA10$).

Semnalele de la ieșirea rețelei conductive (impulsuri sinusoidale) sunt detectate cu ajutorul amplificatorului logaritmic AD8310. Ieșirea amplificatorului AD8310 este conectat la intrarea ADC1_IN6 a convertorului ADC1 (pinul PA1), parte componentă a microcontrolerului STM32L432KC.

Circuitul CADI este compus din două module: placa de dezvoltare NUCLEO-L432KC și circuitul de interfață cu rețeaua conductivă, așa cum este prezentat în figura 4.61.

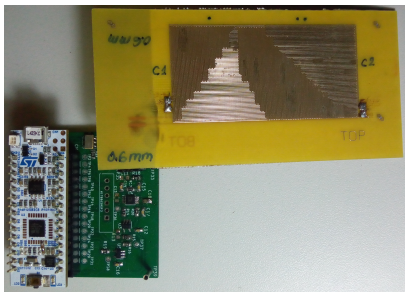


Figura 4.61: *CADI experimental format din placa de dezvoltare NUCLEO-L432KC, circuitul de interfață și rețeaua conductivă.*

Descrierea procesului de detecție a intruziunilor

Implementarea experimentală a acestui CADI a avut în vedere testarea a două caracteristici importante în protecția CES: detecția intruziunilor fizice și detecția variațiilor de temperatură. Pentru obținerea unei rezoluții optime în detecția intruziunilor, au fost utilizate 32 de frecvențe, cu un ecart de $5MHz$ între ele. Frecvența de început a fost aleasă $50MHz$, rezultând un domeniu cu frecvența maximă de $205MHz$. Programul din STM32L432KC controlează oscilatorul Si514 astfel încât acesta modifică frecvența la fiecare $250ms$. După o durată de $20ms$ de stabilizare internă a semnalului generat de Si514, se activează ieșirea acestuia pentru $300\mu s$, timp necesar pentru ADC1 să efectueze conversia. În figura 4.62 este prezentat un impuls generat de Si514 și impulsul la ieșirea AD8310.

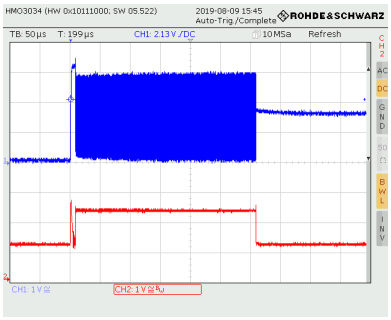


Figura 4.62: *Semnal de ieșire din rețeaua conductivă (canalul 1, traseul albastru) și semnalul detectat la ieșirea amplificatorului logaritmic (canalul 2, traseul roșu).*

Detecția intruziunilor fizice

Testarea CADI, împreună cu rețeaua conductivă triplu strat, a fost realizată în condiții reale de producere a intruziunilor fizice de tip întrerupere a traseului conductiv și scurt circuit între tresee alăturate pe stratul de detecție (3) al rețelei conductive. Au fost testate următoarele cazuri: rețea conductivă integră (NT), C1 deschis (TC1_O), C1 în scurt-circuit (TC1_S), C2 deschis (TC2_O), C2 în scurt-circuit (TC2_S). A fost analizată rețeaua conductivă realizată din folie PES cu grosime de $0,1mm$ imprimată cu pastă conductivă tip SW180. Rezultatul analizei este prezentat în figura 4.63.

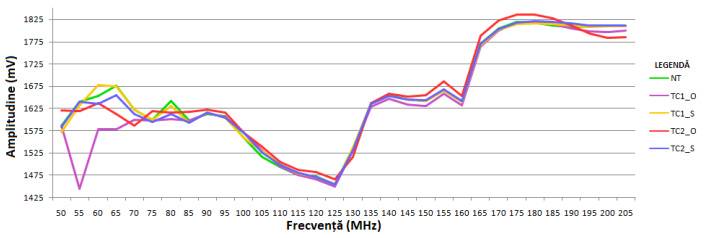


Figura 4.63: *Caracteristica de ieșire a rețelei conductive: NT - circuite neafectate de intruziune, TC1_O - C1 circuit deschis, TC1_S - C1 scurt-circuit, TC2_O - C2 circuit deschis, TC2_S - C2 scurt-circuit.*

Se observă că detecția intruziunilor de tip circuit deschis (întreruperea traseelor de pe stratul 3 al rețelei conductive) este posibilă în tot domeniul de frecvență analizat. În ceea ce privește detecția intruziunilor de tip scurt-circuit între trasee alăturate, sunt mai multe domenii distincte de frecvență în care se poate realiza detecția.

Detecția variațiilor de temperatură

Pentru a contracara atacurile de inducere a erorilor prin variația temperaturii, rețeaua conductivă triplu strat împreună cu CADI sunt capabile să detecteze variațiile de temperatură și să ia măsurile necesare pentru protecția datelor de securitate. Au fost realizate teste pentru un domeniu de temperaturi între $-20°C$ și $80°C$, utilizând camera termică (ESPEC SH_241). Rezultatele sunt prezentate în figura 4.66.

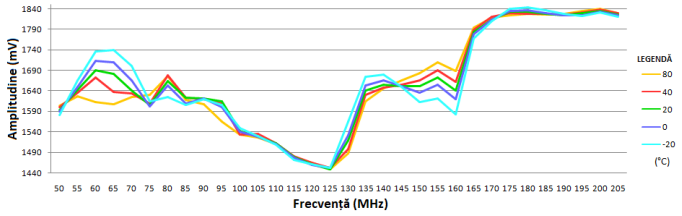


Figura 4.66: *Caracteristica de ieșire a rețelei conductive: comportarea la variații ale temperaturii.*

Analizând comportarea rețelei conductive la variații de temperatură, în cazul celor trei modele constructive, se observă că valorile pentru temperaturi din domeniul $> -20°C$ și $< 80°C$ sunt încadrate de traseele corespunzătoare temperaturilor limită de intruziune $-20°C$ și $80°C$. Pentru o funcționare eficientă a CADI este necesar ca acesta să permită detecția celor două tipuri de intruziuni: fizice și termice. Pentru verificarea eficienței CADI, s-au calculat diferențele între valorile rezultate în cazul intruziunilor fizice și valorile corespunzătoare limitelor de intruziune termică, iar modulul acestor diferențe este prezentat în figura 4.69. În cazul în care valorile de intruziune fizică sunt încadrate de cele de intruziune termică, valoarea afișată este 0.

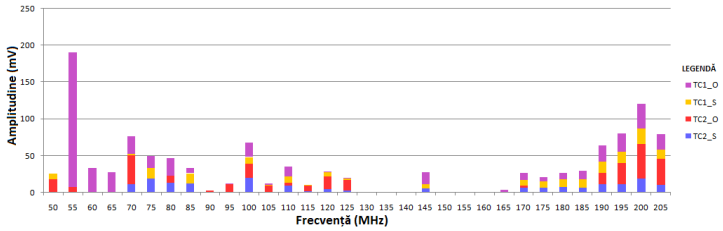


Figura 4.69: *Rețea conductivă PES $0,1mm$: diferențele de amplitudine (în modul) între intruziunile fizice și limitele de atac termic.*

Analizând figura 4.69, se observă că sistemul format din CADI și rețeaua conductivă detectează atât intruziunile fizice cât și cele termice în aproximativ 80% din spectrul de sondare. Pentru optimizarea funcționării CADI, frecvențele la care acesta nu este eficient în detecția intruziunilor se pot elimina din spectrul de sondare.

Capitolul 5

Funcții de securitate complementare ale rețelei conductive triplu strat

5.1 Securizarea circuitelor electronice de securitate

Caracteristica de ieșire a rețelei conductive poate fi utilizată într-un mod special pentru securizarea CES, astfel: nivelele de semnal achiziționate la frecvențe discrete sunt folosite în procesul de obținere a unei chei criptografice. Protecția CES de către CADI acoperă următoarele cazuri: la pornire (*boot*) și pe durata funcționării.

La momentul pornirii (*boot*), se procesează o cheie criptografică prin testarea rețelei conductive la frecvențe predefinite. Această cheie este utilizată la descifrarea programului (*firmware*) al CES. După încărcarea corectă a programului, programul verifică starea rețelei conductive prin sondarea ei la frecvențe predefinite.

Studiul acestui principiu a fost realizat în lucrarea [21], utilizând circuitul experimental prezentat anterior. Pentru ca acest principiu să fie eficient este necesar ca fiecare rețea conductivă să furnizeze o cheie criptografică nepredictibilă. Variația valorilor achiziționate este determinată de procesul de cuantizare al ADC, zgomotul CADI și răspunsul rețelei conductive funcție de temperatură.

Considerând domeniul termic operațional între valorile $-20°C$ și $80°C$, rețeaua conductivă este caracterizată de o bandă operațională, mărginită de traseele de maxim și de minim, așa cum este prezentat în figura 5.2.

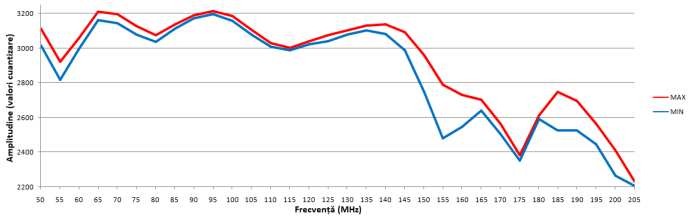
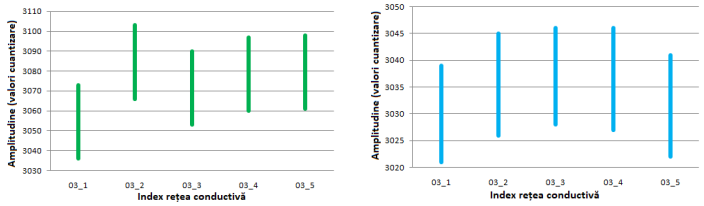


Figura 5.2: *Limitele valorilor achiziționate la ieșirea rețelei conductive PCB* $0,3mm$*, pentru variații ale temperaturii între* $-20°C$ *și* $80°C$*.*

În figura 5.4 sunt exemplificate, pentru două valori ale frecvențelor de sondare

($80MHz$ și $120MHz$), domeniile de valori de răspuns ale rețelelor conductive testate, corespunzătoare domeniului termic analizat (între $-20°C$ și $80°C$).



(a) *PCB* $0,3mm$, $80MHz$. ***(b)*** *PCB* $0,3mm$, $120MHz$.

Figura 5.4: *Exemple de răspunsuri ale rețelelor conductive la frecvențele 80MHz și 120MHz.*

Din figura 5.4 se observă că fiecare rețea conductivă testată are un răspuns unic, utilizabil în constituirea unei chei criptografice. Cheia criptografică se poate obține prin împărțirea spațiului amplitudinilor în cuante $Q_{i,j}$, cu i reprezentând frecvența F_i iar j reprezentând numărul cuantei. Fiecărei cuante îi corespunde o valoare binară, astfel încât, concatenarea acestor valori produce cheia criptografică K_D. Acest mod de împărțire a spațiului de amplitudini este prezentat în figura 5.5.

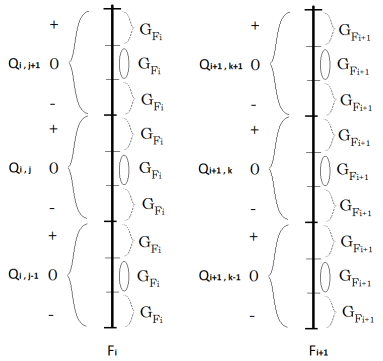


Figura 5.5: *Reprezentarea domeniilor de cuantizare corespunzătoare frecvențelor de sondare ale rețelei conductive* i *și* $i+1$.

Această secțiune propune o metodă inovativă de derivare a cheilor criptografice bazată pe caracteristica de ieșire amplitudine-frecvență a rețelei conductive și pe dispersia acestei caracteristici funcție de temperatură și de parametri de material.

5.2 Autentificarea circuitelor electronice de securitate

Datele de identificare, în cazul unei autentificări, pot fi obținute din răspunsul rețelei conductive prin cuantizarea acestuia la frecvențe discrete. Identificarea unică a echipamentelor ce conțin un CES, impune ca secvențele obținute din caracteristica amplitudine-frecvență să fie unice. Pentru asigurarea acestei unicități, se pot implementa următoarele diferite metode: rețele conductive unice, adăugarea de elemente RLC, aplicarea unei funcții HASH, sondarea la frecvențe diferite etc.

Capitolul 6

Concluzii

Acest capitol prezintă în mod sintetic concluziile rezultate în urma cercetării aplicate în cadrul tezei de doctorat. În prima secțiune, sunt enumerate contribuțiile originale ce reies din activitatea de cercetare. Secțiunea a doua cuprinde lista lucrărilor publicate de autor și rapoartele de cercetare din programul de doctorat.

6.1 Contribuții originale

Capitolul 2

1. Am studiat tipurile de atacuri asupra circuitelor electronice de securitate: criptanaliza sistemelor criptografice, atacuri pe canale colaterale și intruziuni fizice [11, 12, 13, 14, 15].

2. Am evidențiat necesitatea asigurării protecției fizice a circuitelor electronice de securitate [11, 12, 13, 14, 15].

Capitolul 3

1. Am analizat caracteristicile sistemelor de protecție a circuitelor electronice de securitate împotriva intruziunilor fizice [11].

2. Am documentat rolul și tipurile de rețele conductive utilizate în sistemele de protecție a circuitelor electronice de securitate [11, 12].

3. Am analizat proprietățile și neajunsurile circuitelor pasive de detecție a intruziunilor [11, 12, 13, 14, 15].

4. Am studiat circuitele active de detecție a intruziunilor. Am analizat principiul de funcționare și stadiul actual de dezvoltare [11, 12].

5. Am propus o schemă de principiu și o structură fizică a ansamblului format din circuitul electronic de securitate și circuitul de detecție a intruziunilor [11].

Capitolul 4

Secțiunea 4.1

1. Am realizat o rețea conductivă formată dintr-un strat de masă și un strat cu trasee conductive, destinat sondării cu semnale. Stratul de masă îmbunătățește proprietățile de detecție a intruziunilor. Acesta are două roluri: plan de referință pentru semnalele de sondare ce se propagă prin traseele conductive și ecran electromagnetic [1, 11].

Secțiunea 4.2

1. Am proiectat un circuit activ de detecție a intruziunilor format dintr-un circuit de procesare, bazat pe microcontrolerul STM32F407, și un circuit de interfață cu rețeaua conductivă, format din comparatoare cu histerezis [1, 11].

2. Am stabilit o metodă de generare a impulsurilor de sondare prin utilizarea unui generator de secvențe pseudoaleatoare, tip LFSR [1, 11].

3. Am stabilit o metodă de implementare a impulsurilor de sondare, caracterizată prin generarea simultană a acestora la cele două porturi ale rețelei conductive [1, 11].

4. Analiza impulsurilor de sondare am implementat-o într-un program executat în microcontroler [1, 11].

5. Circuitul experimental de detecție a intruziunilor împreună cu rețeaua conductivă dublu strat le-am testat și am determinat performanțele de detectare a intruziunilor și a tentativelor de intruziune fizică [1, 11].

Secțiunea 4.3

1. Am proiectat un circuit activ de detecție a intruziunilor compus dintr-un circuit de procesare (STM32F746), un amplificator operațional și un convertor analog-digital cu memorie (ADC08B200) [1, 2, 11, 12].

2. Am stabilit modul de analiză al rețelei conductive în vederea detecției intruziunilor, urmărindu-se două aspecte: întârzierea și puterea componentelor spectrale a impulsurilor [1, 2, 11, 12].

3. Am implementat funcțiile de detecție a intruziunilor în programul circuitului de procesare [1, 2, 11, 12].

4. Am efectuat teste experimentale cu semnale de sondare formate din impulsuri de diferite durate pentru a determina parametrii optimi de detecție a intruziunilor și a tentativelor de intruziune (afectarea nedistructivă a rețelei conductive) [1, 2, 11, 12].

5. Din testarea experimentală a întârzierii impulsurilor au reieșit performanțele acestui sistem în domeniul timp [1, 2, 11, 12].

6. Din testarea experimentală în domeniul frecvență s-au determinat limitele de la care pot fi detectate tentativele de intruziune [1, 2, 11, 12].

Secțiunea 4.4

1. Pentru circuitul activ de detecție a intruziunilor, prezentat în secțiunea 4.3, am implementat două categorii de metode de protecție a circuitului electronic de securitate: detecția variațiilor de temperatură (la nivelul rețelei conductive) și detecția intruziunilor fizice [1, 2, 3, 4, 11, 12, 13].

2. Variațiile de temperatură le-am analizat prin calculul puterii semnalului în domeniul timp [3, 13].

3. Detecția intruziunilor fizice am realizat-o prin calculul parametrilor statistici: medie, medie rădăcină pătratică, deviație standard și varianță [4, 13].

4. Am analizat răspunsul rețelei conductive la variații de temperatură în domeniul $-20°C \div 100°C$. Caracteristica rezultată este cvasiliniară, cu pantă negativă, și permite detecția variațiilor de temperatură. Detecția atacurilor termice se implementează prin stabilirea unui domeniu de operabilitate [3, 13].

5. Detecția intruziunilor fizice am extins-o la detecția tentativelor de intruziune prin testarea mai multor valori ale rezistorilor conectați în serie cu rețeaua conductivă sau ale condensatorilor conectați în paralel cu aceasta [4, 13].

6. În urma testelor, valori ale rezistențelor mai mari de 10Ω și valori ale capacităților mai mari de $10pF$ pot fi detectate prin calculul parametrilor statistici medie rădăcină pătratică, deviație standard și varianță [4, 13].

Secțiunea 4.5

1. Am propus o rețea conductivă inovativă formată din trei straturi conductive (strat de masă, strat de semnal și strat de detecție), izolate prin straturi dielectrice. Traseele conductive ce formează stratul de detecție, expus la exterior, sunt circuite închise [5, 14].

2. Am stabilit un mod de sondare cu semnale a rețelei conductive în vederea detectării intruziunilor fizice. Un atacator nu poate determina exhaustiv parametrii semnalelor de sondare prin analiza stratului conductiv expus, făcând astfel imposibilă simularea și injectarea de semnale false [5, 14].

3. Am analizat un circuit echivalent al traseelor conductive, ce formează stratul de semnal și cel de detecție, cuplate inductiv și capacitiv [5, 14].

4. O structură simplă, formată din meandre identice, am simulat-o în vederea obținerii caracteristicii amplitudine-frecvență de ieșire, în următoarele cazuri: rețea neafectată și intruziune fizică (întreruperea traseului conductiv al stratului de detecție) [5, 14]. Domeniul de frecvență în care s-a făcut simularea a fost $0Hz \div 1GHz$.

5. Caracteristicile amplitudine-frecvență corespunzătoare celor două cazuri diferă în mod substanțial, prin apariția a două puncte de minim suplimentare [5, 14].

6. Rețeaua conductivă anterioară am îmbunătățit-o prin extinderea suprafeței acoperite de traseele conductive la un pătrat cu latura de $30mm$, format din meandre complexe [5, 14].

7. Această structură îmbunătățită am simulat-o pentru obținerea caracteristicii de ieșire amplitudine-frecvență, pentru domeniul $0Hz \div 500MHz$, corespunzătoare cazurilor în care stratul de detecție este intact și cazul în care traseul de pe stratul de detecție formează un circuit deschis (intruziune) [5, 14].

8. În urma simulării, caracteristicile corespunzătoare celor două cazuri analizate diferă în mod consistent la frecvențe joase, mai mici de $300MHz$ [5, 14]. Acest comportament este util în proiectarea circuitelor active de detecție a intruziunilor deoarece detecția și analiza semnalelor de sondare nu necesită circuite complexe.

9. Am exemplificat un model de rețea conductivă, tip folie, destinată acoperirii complete a unui circuit electronic (format din circuitul electronic de securitate și circuitul activ de detecție a intruziunilor) [15].

10. Am proiectat o rețea conductivă formată din două zone alăturate, cu modele diferite ale traseelor conductive. Acestea le-am simulat și realizat practic sub forma a două cablaje imprimate cu grosimea dielectricului de $0,3mm$ și $0,6mm$ [6, 15]. Domeniul de frecvență de analiză a fost $0Hz \div 500MHz$.

11. Simulările corespunzătoare celor două tipuri de cablaje prezintă diferențe măsurabile între cazurile de rețea neafectată și rețea asupra căreia s-a efectuat o intruziune [6, 15].

12. Testele practice, realizate în aceleași condiții, prezintă un comportament diferit în frecvență față de simulări însă efectul intruziunilor este detectabil în aceeași măsură, începând cu frecvența de $30MHz$ [6, 15].

13. Principiul sistemului format din această rețea conductivă și circuitul activ de detecție a intruziunilor a fost propus spre publicare în cadrul unei cereri de brevet de invenție [16].

14. Pentru evidențierea intruziunilor de tip întreruperea circuitului și scurt-circuit între două trasee alăturate (pe stratul de detecție - 3), am simulat și testat practic aceste cazuri pentru trei tipuri de rețele conductive: cablaj imprimat cu grosimea dielectricului de $0,3mm$, cablaj imprimat cu grosimea dielectricului de $0,6mm$ și folie PES imprimată cu pastă conductivă SW180 [7].

15. Simulările efectuate pentru domeniu de frecvență $0Hz \div 300MHz$ au evidențiat detecția intruziunilor de tip circuit deschis pentru frecvențe mai mari de $30MHz$ și detecția intruziunilor de tip scurt-circuit pentru frecvențe mai mari [7].

16. Analiza circuitelor realizate practic a pus în evidență faptul că rețeaua conductivă de tip PES, cu dielectric de grosimea $0,1mm$, este eficientă începând cu frecvența de $85MHz$, rețeaua conductivă de tipă PCB, cu dielectric de grosimea $0,3mm$, este eficientă începând cu frecvența de $35MHz$ iar rețeaua conductivă de tipă PCB, cu dielectric de grosimea $0,6mm$, este eficientă începând cu frecvența de $15MHz$ [7].

Secțiunea 4.6

1. Am realizat proiectul grafic pentru fabricarea sitelor serigrafice necesare imprimării rețelei conductive pe folie PES cu ajutorul echipamentului DEK Horizon 08 [15].

2. Am executat procesele tehnologice pentru imprimarea foliilor PES cu pastă conductivă SW180 [15].

3. Am testat integritatea traseelor conductive la îndoire sub diferite raze de curbură. Rețeaua conductivă, imprimată cu pasta SW180 prin tehnologia serigrafică, permite îndoirea cu raze de cel puțin $2mm$ [15].

4. Acest tip de folie, împreună cu pasta conductivă SW180, reprezintă o soluție corespunzătoare pentru fabricarea rețelelor conductive pentru caracteristicile de semnal și pentru friabilitatea controlată, necesară protecției împotriva intruziunilor [15].

Secțiunea 4.7

1. Am proiectat un circuit activ de detecție a intruziunilor specializat pentru sondarea și analiza rețelei conductive triplu strat cercetate anterior [8, 9]. Structura este simplă și minimală pentru optimizarea dimensiunilor și consumului: un microcontroler cu consum redus de energie, un oscilator programabil și un amplificator logaritmic.

2. Am stabilit principiul de detecție al intruziunilor și am dezvoltat aplicația ce rulează în microcontroler. Rețelele conductive au fost sondate cu impulsuri

radio (trenuri de semnale sinusoidale) cu frecvențe în domeniul $50MHz \div 205MHz$ [8, 9].

3. Am testat experimental ansamblul format din circuitul activ de detecție a intruziunilor și rețeaua conductivă. Am utilizat cele trei tipuri de rețele conductive cercetate în secțiunea 4.5 (folie PES cu grosimea de $0,1mm$ imprimată cu pastă conductivă SW180, cablaj imprimat cu grosimea dielectricului de $0,3mm$ și cablaj imprimat cu grosimea dielectricului de $0,6mm$). Testele efectuate au vizat atât intruziunile fizice (întreruperea circuitului detector, scurt-circuit între trasee alăturate ale circuitului detector) cât și detecția veriațiilor de temperatură, în special depășirea limitelor termice operaționale [8, 9].

4. Testele pentru intruziuni fizice au pus în evidență detecția celor patru tipuri de intruziuni analizate (circuit deschis, respectiv, scurt-circuit în zonele 1 și 2) în majoritatea frecvențelor de test [8, 9].

5. Testele pentru detecția variațiilor de temperatură le-am efectuat în domeniul termic $-20°C \div 80°C$. Sistemul analizat poate detecta variații ale temperaturii în subdomenii ale domeniului de frecvență utilizat. Important este faptul că traseele corespunzătoare temperaturilor extreme ($-20°C$ și $80°C$) încadrează traseele temperaturilor intermediare. Detecția atacurilor pe canale colaterale de tip termic pot fi detectate într-o gamă de frecvențe [8, 9].

6. Având în vedere că circuitul activ de detecție a intruziunilor trebuie să răspundă la cele două tipuri de atacuri analizate, am identificat frecvențele la care rețeaua conductivă poate detecta concomitent intruziuni fizice și depășirea limitelor termice operaționale. Astfel, în mai mult de 80% din frecvențele de analiză sistemul a fost eficient în detecția celor două tipuri de atacuri [8, 9].

Secțiunea 5.1

1. Am identificat o procedură de securizare a programelor *firmware* ce are la bază proprietățile rețelelor conductive triplu strat studiate. Din sondarea rețelei conductive se procesează o cheie criptografică cu care se cifrează programul *firmware* [6, 10, 15].

2. Această metodă de protejare a programului *firmware* nu necesită utilizarea unei surse de energie de rezervă destinată asigurării funcționării fără întrerupere a circuitului activ de detecție a intruziunilor [6, 10, 15].

Secțiunea 5.2

1. Am identificat o procedură de autentificare a circuitelor de securitate bazată pe obținerea unei identități unice din caracteristica amplitudine-frecvență de ieșire a rețelei conductive triplu strat [7, 15].

2. Am propus mai multe metode de creștere a dispersiei acestei caracteristici pentru asigurarea identităților unice ale circuitelor electronice de securitate [7, 15].

6.2 Lista lucrărilor originale

Lucrări științifice publicate în cadrul conferințelor științifice și rapoarte de cercetare susținute pe parcursul programului de doctorat:

1. **D. C. Vasile, A. Marghescu, P. Svasta**, *Improved tamper detection circuit based on linear-feedback shift register*, 2016 IEEE 22nd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Oradea, Romania, 2016, DOI: 10.1109/SIITME.2016.7777261.

2. **D. C. Vasile, P. Svasta, N. Codreanu, M. Safta**, *Active tamper detection circuit based on the analysis of pulse response in conductive mesh*, Jubilee 40th International Spring Seminar on Electronics Technology, ISSE 2017, Sofia, Bulgaria, 2017, DOI: 10.1109/ISSE.2017.8000987.

3. **D. C. Vasile, P. Svasta**, *Temperature Sensitive Active Tamper Detection Circuit*, 2017 IEEE 23rd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Constanța, Romania, 2017, DOI: 10.1109/SIITME.2017.8259885.

4. **D. C. Vasile, P. Svasta**, *Active Tamper Detection Circuit Based on Statistical Analysis*, 2017 IEEE 23rd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Constanța, Romania, 2017, DOI: 10.1109/SIITME.2017.8259884.

5. **D. C. Vasile, P. Svasta**, *Innovative Conductive Mesh Structure for the Protection of Security Electronic Circuits*, 2018 7th Electronic System-Integration Technology Conference (ESTC), Dresden, Germany, 2018, DOI: 10.1109/ESTC.2018.8546366.

6. **D. C. Vasile, P. Svasta**, *Antitamper Conductive Mesh Used for Securing Cryptographic Modules*, 2018 IEEE 24th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Iași, Romania, 2018, DOI: 10.1109/SIITME.2018.8599284.

7. **D. C. Vasile, P. Svasta**, *Innovative Authentication Method for IoT Devices*, 2019 22nd European Microelectronics and Packaging Conference & Exhibition (EMPC), IEEE, Pisa, Italy, 2019, DOI: 10.23919/EMPC44848.2019.8951767.

8. **D. C. Vasile, P. Svasta**, *Protecting the Secrets: Advanced Technique for Active Tamper Detection Systems*, 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Cluj-Napoca, Romania, 2019, DOI: 10.1109/SIITME47687.2019.8990877.

9. **D. C. Vasile, P. Svasta, M. Pantazică**, *Preventing the Temperature Side Channel Attacks on Security Circuits*, 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Cluj-Napoca, Romania, 2019, DOI: 10.1109/SIITME47687.2019.8990788.

10. **D. C. Vasile, S. Chițu, P. Svasta**, *Criptographic Key Derivation from an Anti-Tamper Solution*, 2020 8th Electronic System-Integration Technology Conference (ESTC), Vestfold, Norway, 2020 (lucrare acceptată pentru prezentare în cadrul conferinței).

11. **D. C. Vasile**, *Sistem activ de detect, ie a intruziunilor destinat protecției circuitelor electronice de securitate*, Raport de cercetare nr. 1, 2017.

12. **D. C. Vasile**, *Circuit activ de detecție a intruziunilor bazat pe analiza răspunsului la impulsuri a rețelei conductive*, Raport de cercetare nr. 2, 2017.

13. **D. C. Vasile**, *Circuit activ de detecție a intruziunilor cu funcție dual: detecția variațiilor de temperatură și detecția intruziunilor prin metode statistice*, Raport de cercetare nr. 3, 2018.

14. **D. C. Vasile**, *Rețea conductivă inovativă pentru protecția circuitelor electronice de securitate*, Raport de cercetare nr. 4, 2019.

15. **D. C. Vasile**, *Securizarea circuitelor electronice de securitate: rețea conductivă inovativă pentru detecția intruziunilor*, Raport de cercetare nr. 5, 2019.

16. **D. C. Vasile, P. Svasta**, *Rețea conductivă de protecție a circuitelor electronice de securitate împotriva intruziunilor fizice*, Cerere de brevet de invenție A/00609, 30 septembrie 2019.

Bibliografie

[1] A. E. Hassanien and M. Elhoseny. *Cybersecurity and Secure Information Systems, Challenges and Solutions in Smart Environments*. Springer, 2019.

[2] H. C. A. Van Tilborg. *Encyclopedia of cryptography and security*. Springer Science and Business Media, 2014.

[3] D. Gritzalis, M. Theocharidou, and G. Stergiopoulos. *Critical Infrastructure Security and Resilience - Theories, Methods, Tools and Technologies*. Springer, 2019.

[4] N. P. Smart. *Physical side-channel attacks on cryptographic systems*. Software Focus 1.2, 2000.

[5] Y. Souissi, J. L. Danger, S. Guilley, S. Bhasin, and M. Nassar. *Embedded systems security: An evaluation methodology against side channel attacks*. Proceedings of the 2011 Conference on Design & Architectures for Signal & Image Processing (DASIP) IEEE, 2011.

[6] National Institute of Standards and Technology (NIST). *Security Requirements for Cryptographic Modules, FIPS 140-2*. 2001.

[7] Enevoldsen, M. T. and West, T. T. and Wesselhoff E. and Rasmussen, J. and Mikkelsen, D. B. *Security module for protection circuit components from unauthorized access, U.S. Patent No. US 10,009,995 B2*. 2018.

[8] D. C. Vasile, A. Marghescu, and P. Svasta. *Improved tamper detection circuit based on linear-feedback shift register*. 2016 IEEE 22nd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Oradea, România, 2016.

[9] A. Marghescu, P. Svasta, and Simion E. *High Speed and Secure Variable Probability Pseudo/True Random Number Generator Using FPGA*. 2015 IEEE 21st International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Oradea, România, 2015.

[10] Texas Instruments. *TLV350x 4.5-ns, Rail-to-Rail, High-Speed Comparator in Microsize Packages*. `http://www.ti.com`, 2016.

[11] Kay, A. and Claycomb, T. *Comparator with Hysteresis Reference Design, TIDU020A, Texas Instrumens*. `http://www.ti.com`, 2014.

[12] D. C. Vasile, P. Svasta, N. Codreanu, and M. Safta. *Active tamper detection circuit based on the analysis of pulse response in conductive mesh*. Jubilee 40th International Spring Seminar on Electronics Technology, ISSE 2017, Sofia, Bulgaria, 2017.

[13] D. C. Vasile and P. Svasta. *Temperature Sensitive Active Tamper Detection Circuit*. 2017 IEEE 23rd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Constanța, România, 2017.

[14] D. C. Vasile and P. Svasta. *Active Tamper Detection Circuit Based on Statistical Analysis*. 2017 IEEE 23rd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Constanța, România, 2017.

[15] D. C. Vasile and P. Svasta. *Innovative Conductive Mesh Structure for the Protection of Security Electronic Circuits*. Electronics System-Integration Technology Conference (ESTC), Dresden, Germany, 2018.

[16] D. C. Vasile and P. Svasta. *Antitamper Conductive Mesh Used for Securing Cryptographic Modules*. 2018 IEEE 24th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Iași, România, 2018.

[17] D. C. Vasile and P. Svasta. *Rețea conductivă de protecție a circuitelor electronice de securitate împotriva intruziunilor fizice*. Cerere de brevet de invenție A/00609, Oficiul de Stat pentru Invenții și Mărci, 30 septembrie 2019.

[18] D. C. Vasile and P. Svasta. *Innovative Authentication Method for IoT Devices*. 22nd Microelectronics and Packaging Conference (EMPC), IEEE, Pisa, Italia, 2019.

[19] D. C. Vasile and P. Svasta. *Protecting the Secrets: Advanced Technique for Active Tamper Detection Systems*. 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Cluj-Napoca, România, 2019.

[20] D. C. Vasile, P. Svasta, and M. Pantazică. *Preventing the Temperature Side Channel Attacks on Security Circuits*. 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Cluj-Napoca, România, 2019.

[21] D. C. Vasile, S. Chițu, and P. Svasta. *Cryptographic Key Derivation from an Anti-Tamper Solution*. 8th Electronics System-Integration Technology Conference (ESTC), Vestfold, Norvegia, 2020.