CERCETĂRI ȘI SOLUȚII PENTRU REȚELELE DE CONTORIZARE INTELIGENTĂ

Teză destinată obținerii

titlului științific de doctor inginer
la
Universitatea Politehnica Timișoara
în domeniul Ingineria Sistemelor
de către

Ing. Paul-Onuț NEGÎRLA

Președintele comisiei:	prof.univ.dr.ing……..
Conducător științific:	prof.univ.dr.ing. Ioan SILEA
Referenți științifici:	prof.univ.dr. ……...
	prof.univ.dr.ing. …….
	conf.univ.dr.ing. …….

Ziua susținerii tezei: ……..

Seriile Teze de doctorat ale UPT sunt:

1. Automatică
2. Chimie
3. Energetică
4. Inginerie Chimică
5. Inginerie Civilă
6. Inginerie Electrică
7. Inginerie Electronică și Telecomunicații
8. Inginerie Industrială
9. Inginerie mecanică
10. Știința Calculatoarelor
11. Știința și Ingineria Materialelor
12. Ingineria Sistemelor
13. Inginerie Energetică
14. Calculatoare și Tehnologia Informației
15. Ingineria Materialelor
16. Inginerie și Management
17. Arhitectură
18. Inginerie Civilă și Instalații
19. Inginerie Electronică, Telecomunicații și Tehnologii Informaționale

Universitatea Politehnica Timișoara a inițiat seriile de mai sus în scopul diseminării expertizei, cunoștințelor și rezultatelor cercetărilor întreprinse în cadrul Școlii doctorale a universității. Seriile conțin, potrivit H.B.Ex.S Nr. 14 / 14.07.2006, tezele de doctorat susținute în universitate începând cu 1 octombrie 2006.

România, 300223 Timișoara, Bd. Vasile Pârvan 2B
Tel./fax 0256 404677
e-mail: editura@upt.ro

Cuvânt înainte

Teza de doctorat a fost elaborată pe parcursul activității mele de cercetare în cadrul Departamentului de Automatică și Informatică Aplicată al Universității Politehnica Timișoara.

Pentru îndrumarea și sprijinul oferit, mulțumiri deosebite se cuvin coordonatorului de doctorat, prof. univ. dr. ing. Ioan SILEA, căruia îi sunt recunoscător pentru răbdarea și profesionalismul cu care m-a ghidat pe parcursul anilor de cercetare necesari elaborării prezentei teze.

Mulţumirile mele se îndreaptă și către cadrele didactice din cadrul Universităţii Politehnica Timişoara, pentru susținerea continuă și pentru colaborările care au contribuit la dezvoltarea mea profesională.

În final, aș dori să mulțumesc familiei mele pentru sprijinul continuu și pentru că a fost aproape de mine pe tot parcursul studiilor doctorale.

Timișoara, 2022 NEGÎRLA Paul-Onuț

NEGÎRLA, Paul-Onuț
Titlul tezei
Teze de doctorat ale UPT, Seria X, Nr. YY, Editura Politehnica, 2022, 140 pagini, 56 figuri, 14 tabele.
ISSN:
ISBN:

Cuvinte cheie
……
……
Rezumat

CUPRINS

LISTA DE FIGURI

LISTA DE TABELE

LISTA DE ABREVIERI

AC	Alternating current
ANRE	Autoritatea Națională de Reglementare în domeniul Energiei
CBA	Cost Benefit Analysis
CC2500	Emitor-receptor de joasă putere de 2,4 Ghz (de la Chipcon Company)
CE	Consiliul European
CENELEC	Comité Européen de Normalisation Électrotechnique;
COSEM	Companion Specification for Energy Metering
CPCS	Construction Plant Competence Scheme
CPU	Central Processing Unit
DLMS	Device Language Message Specification
ECC	Error Correction Codes
EEPROM	Electrically Erasable Programmable Read-Only Memory
ERBD	European Bank for Reconstruction and Development
FTP	File Transfer Protocol
G3	Protocol de comunicație prin PLC
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
ISM	Benzile radio industriale, științifice și medicale
ITU	International Telecommunication Union
JTAG	Joint Test Action Group
LED	Diodă emițătoare de lumină
LQI	Indicator pentru calitatea legăturii
LTE	Long-Term Evolution
M-Bus	Meter-Bus
MCU	Microcontroller unit
MD-5	Message Digest Algorithm 5
MMU	memory management unit
MSDU	Media Access Control Service Data Unit
MSP430F2274	Microcontroler de joasă putere (de la Texas Instruments Company)
MTU	Maximum transmission unit
NOR	Operator SAU-NU logic
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
OTA	Over The Air
OTP	One Time Programmable
PDU	Protocol Data Unit
PLC	Power Line Communications
PRIME	PoweRline Intelligent Metering Evolution
RAM	Random Access Memory
ROM	Read-only memory
RS232	Standardul 232-Interfață recomandată EIA (din standardele Alianței

	Industriilor Electronice)
RS-232	Recommended Standard 232–Interface EIA
RSSI	Received Signal Strength Indicator
SHA-2	Secure Hash Algorithm 2
SPI	Serial Peripheral Interface
SSL	Secure Sockets Layer
ST	STMicroelectronics
TCP	Transmission Control Protocol
TDMA	Acces multiplu cu diviziune în timp
TLS	Transport Layer Security
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Datagram Protocol

1. INTRODUCERE

1.1. Actualitatea temei și motivația autorului în alegerea ei

Teza aleasă are ca scop analiza metodelor de actualizare a sistemelor integrate folosite în contoarele inteligente instalate în rețelele de energie, identificarea carențelor acestor procese și propunerea unor tehnici de contracarare a problemelor identificate.

Contoarele inteligente au fost adoptate în multe țări în ultimii ani deoarece oferă beneficii economice, sociale și ecologice, iar instalarea lor la nivel național duce la transformarea rețelei energetice într-o rețea energetică inteligentă. Rețeaua energetică inteligentă conferă un management și control eficient al energiei, reduce costurile de producție, economisește energie și este mai fiabilă în comparație cu rețeaua convențională.

Dacă într-o rețea convențională procesul de citire a consumurilor înregistrate de contoare, tarifarea și facturarea clienților finali se face printr-un proces anevoios, în rețelele de contorizare inteligentă fluxul de date și arhitectura contoarelor oferă rezultate mai rapid, într-un mod automatizat și cu un grad de precizie ridicat. Printre avantajele contoarelor inteligente se numără: facturarea exactă fără valori estimative și fără să fie necesar accesul unor angajați ai furnizorilor pe proprietățile clienților, vizualizarea consumurilor și costurilor instantanee, lucru ce duce la o mai buna înțelegere a modului în care energia este consumată de către utilizatori, putând astfel să reducă amprenta emisiilor de carbon și să economisească bani în același timp. Tarifarea dinamică și personalizată pentru fiecare locuință sau consumator este de asemenea importantă pentru ca astfel se poate reduce încărcarea rețelelor la ore de vârf, iar clienții pot beneficia de tarife preferențiale în anumite intervale orare. Totodată, prin instalarea unor contoare inteligente se urmărește integrarea mai ușoară a surselor regenerabile de energie rezidențiale în rețea prin monitorizarea transferului bidirecțional de energie precum și identificarea pofilelor de consum ale utilizatorilor pentru o predictibilitate mai bună a importurilor din rețea.

Protecția contoarelor inteligente este o provocare specială, deoarece accesul sau manipularea neautorizată pot duce la daune financiare sau chiar blocaje strategice la nivel național. La aceste provocări se adaugă și costul implementării atât a rețelelor electrice cât și a rețelelor de date. Aceste implementări sunt costisitoare și necesită investiții mari în domenii care sunt departe de competențele companiilor de utilități publice. Chiar dacă protocoalele folosite în rețelele inteligente sunt de cele mai multe ori unele deschise publicului și testate în mai multe ramuri ale industriei, schimbul sigur de date nu este ferit de vulnerabilitățile descoperite în diferite componente ale sistemului de-a lungul timpului.

Dacă în mediul privat vulnerabilitățile descoperite în calculatoarele sau rețelele instituțiilor și companiilor sunt corectate în timp util și sunt instalate sub formă de actualizări software în cel mai scurt timp posibil, limitările sistemelor integrate din contoarele inteligente și disponibilitatea redusă la o rețea de date ale

acestora duc la o creștere considerabilă a vulnerabilităților într-un mediu strategic precum rețeaua energetică națională.

Această lucrare își propune să analizeze metodele de actualizare a software-ului folosit în prezent în echipamentele rețelei energetice inteligente, iar apoi să ofere o soluție generică optimizată pentru a îmbunătăți fiabilitatea și rapiditatea actualizărilor software în mediile dificile unde disponibilitatea sistemelor este limitată.

Adoptarea directivei 2009/72/CE privind normele comune pentru piața internă a energiei electrice și a directivei 2009/73/CE privind normele comune pentru piața internă în sectorul gazelor naturale a declanșat necesitatea efectuării unei analize a costurilor și beneficiilor (CBA) privind implementarea și instalarea unor sisteme inteligente de contorizare în fiecare stat membru al Uniunii Europene. Momentan la nivelul Uniunii Europene, până la începutul anului 2018, erau instalate aproximativ 100 de milioane de contoare inteligente.

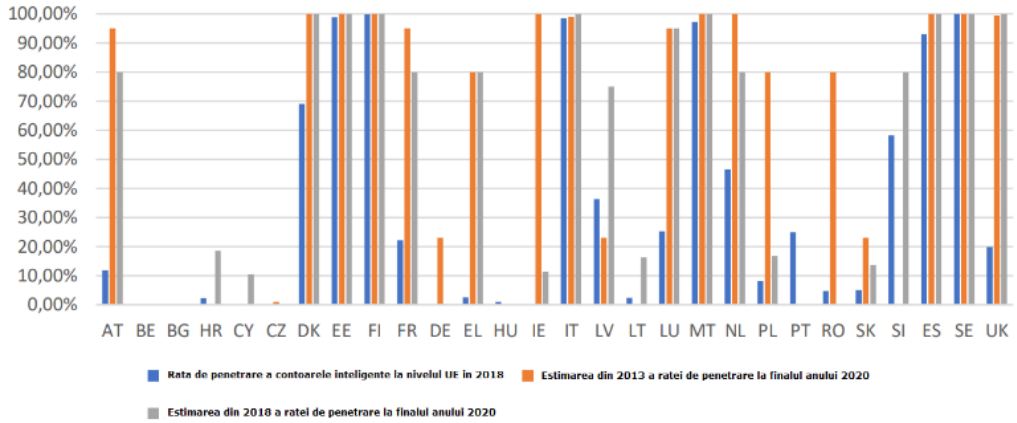

Fig. 1.1. - Rata de penetrare a contoarele inteligente la nivelul UE

Având în vedere numărul locuințelor din uniune, există momentan peste 300 de milioane de locuri de consum. Conversia a doar o treime din spațiul european la rețeaua energetică inteligentă a întâmpinat deja probleme tehnice substanțiale, iar echipamentele deja instalate necesită actualizări pentru a îmbunătăți experiența utilizatorului și pentru a corecta vulnerabilitățile descoperite de la instalare până în prezent. Conform ANRE, România avea în anul 2019 puțin peste 500.000 de contoare inteligente instalate în cele 9.23 milioane de locuri de consum. Inițial, planul urmărea acoperirea a cel puțin 78% din teritoriul țării până în 2020, dar datorită factorilor tehnici și economici acest termen a fost amânat pentru 2028 [1]. Chiar și păstrând ritmul actual (fig. 1.1), până la finalul anului 2024 se estimează un număr de 243 de milioane de noi contoare instalate (fig. 1.2).

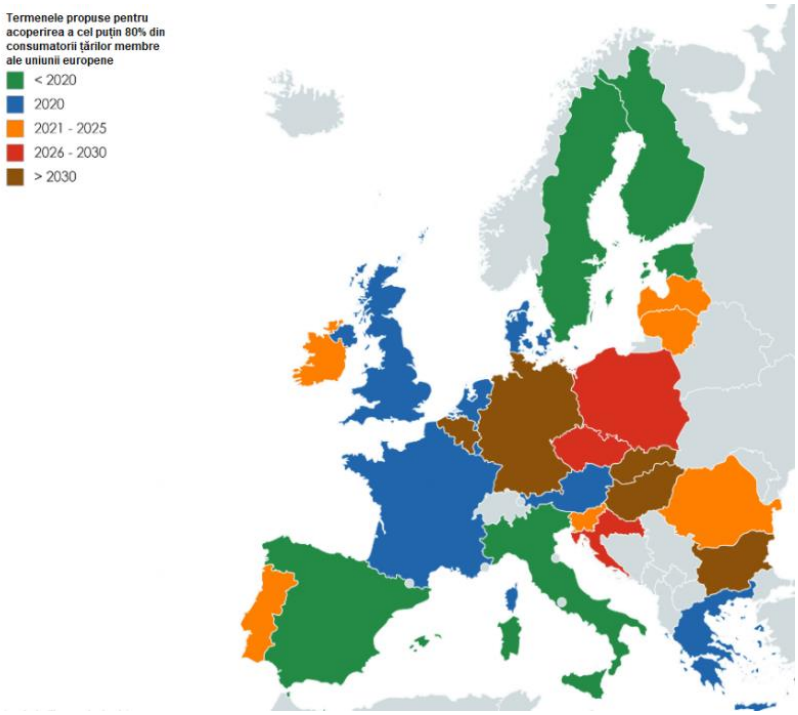

Fig. 1.2. - Termenele propuse pentru instalarea contoarelor inteligente la cel puțin 80% din consumatorii țărilor membre ale uniunii europene

Costurile implementării proiectului de modernizare și de conversie a rețelei energetice la una inteligentă nu sunt acoperite decât parțial de către reglementator, iar prețul de distribuție va conține diferența de preț. Companiile de furnizare și de distribuție a energiei nu vor acoperi costurile contoarelor inteligente, astfel că piața va opta pentru costul cel mai mic de instalare a unui contor inteligent fără a urmări în mod explicit ce tip de tehnologii se vor folosi și dacă acestea vor fi încă de actualitate la finalul termenului conversiei naționale.

Gestionarea datelor transportate în rețeaua inteligentă nu are o arhitectură bine definită, iar managementul acestor date se face într-un mod descentralizat astfel că dezvoltatorii de contoare inteligente și furnizorii de energie își pot defini propriul protocol de transport și de accesare a acestor date. Odată cu creșterea volumului de date și a surselor de date, integritatea datelor, disponibilitatea și confidențialitatea lor devin din ce în ce mai dificil de asigurat.

Autorii specificațiilor tehnice ale echipamentelor inteligente de măsurare nu au acordat o importanță suficientă reglementărilor privind securitatea informatică a acestor sisteme. Deși actualizarea acestor reglementări a început sa fie luată în considerare, numărul echipamentelor care vor fi deja instalate în locuințele rezidențiale va face din actualizarea acestora o sarcină imperios necesară.

În industria tehnologiilor informației, probabilitatea apariției unor vulnerabilități de securitate este luată în calcul încă de la fazele incipiente ale dezvoltării unui nou proiect. De aceea, arhitecții de sistem se asigură că aceste

programe pot fi actualizate în viitor printr-un proces care nu necesită interacțiunea manuală a unui operator. Acest proces poartă denumirea de OTA upgrade sau "Over The Air" upgrade și este singurul mod prin care actualizările pot ajunge la milioane de echipamente în timp util și cu costuri minimale. Dacă acest proces nu funcționează, ar însemna că operatori ai companiilor se deplasează la fiecare consumator pentru o actualizare manuală a fiecărui echipament. În contextul în care avem zeci de milioane de contoare inteligente instalate pe teritoriul unei țări, costurile și timpul necesar pentru a actualiza manual aceste dispozitive nu fac fezabilă o astfel de abordare.

Actualizarea de tip OTA ar fi o sarcină ușoară dacă echipamentele inteligente de măsurare ar dispune de conexiuni de date rapide, dar pentru a minimiza costurile de întreținere și de instalare, operatorii au optat pentru tehnologii de comunicație care pot transfera doar câteva sute de octeți într-o zi, astfel că actualizarea echipamentelor ar putea dura luni sau ani de zile, iar în anumite cazuri contoarele inteligente pot rămâne blocate pentru perioade de timp determinate.

Plecând de la analiza problemelor contoarelor inteligente, motivația cercetării constă în găsirea unor soluții de actualizare rapidă în masă, sigură, folosind infrastructura actuală pentru a proteja sistemele integrate în cazul unor defecte sau a unor probleme de securitate.

1.2. Scopul și obiectivele cercetării

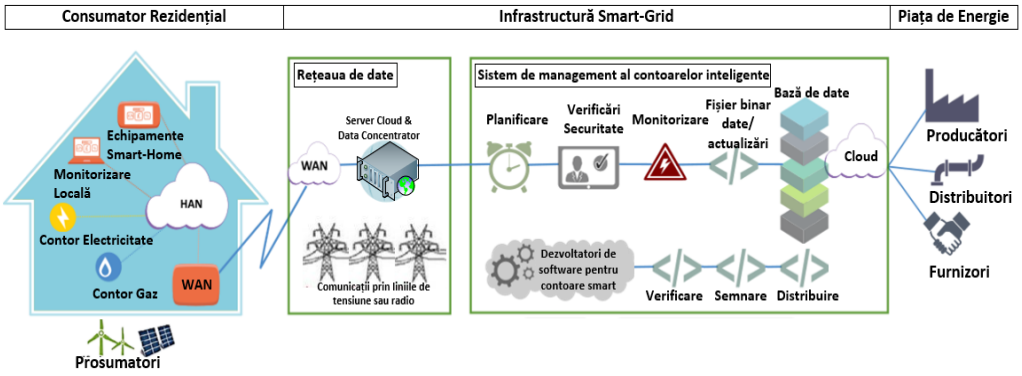

Fig. 1.3. – Vedere de ansamblu a sistemului de contorizare inteligentă

În figura 1.3 se prezintă o vedere de ansamblu a întregului sistem de contorizare energetică, de la producător la consumatorul final. Piața de energie este compusă din trei entități, producători, distribuitori și furnizori. Infrastructura de contorizare este asigurată de către distribuitori și furnizori în colaborare cu companiile producătoare de contoare inteligente, companii care au în sarcină mentenanța, actualizarea echipamentelor de contorizare, precum și asigurarea fluxului de date de la utilizatorii finali către furnizorii contractați de aceștia.

Puternica interconectare dintre componentele sistemului energetic fac din gestionarea riscului unei funcționări defectuoase a contoarelor inteligente în cazul unui atac sau a unei defecțiuni majore o sarcină deosebit de importantă. Oprirea coordonată, datorită unui atac cibernetic sau a unui defect, a unor porțiuni semnificative din rețea va avea repercusiuni majore asupra stabilității întregului sistem național și nu numai.

Preîntâmpinarea celor mai multe atacuri coordonate se poate face prin asigurarea actualizărilor de securitate în bibliotecile de criptografie și rețelistică sau a oricărei alte componente care a devenit vulnerabilă. Actualizările trebuie transportate într-un mod securizat și fiabil pentru a asigura atât confidențialitatea utilizatorului final cât și proprietatea intelectuală și siguranța furnizorilor de echipamente de contorizare inteligentă. Procesul de actualizare fiind unul dintre cele mai invazive procese în sistemele integrate, riscul unui defect crește de-a lungul procesului de actualizare și ingineria sistemelor trebuie să ia în considerare toate condițiile posibile la locul de consum la care echipamentul este instalat. Cele mai des întâlnite astfel de condiții sunt întreruperea temporară a canalului de comunicare cu serverul ce furnizează actualizările programelor sau întreruperea alimentării sistemelor integrate în timpul descărcării sau scrierii noului program.

Tema cercetării tratează metodele prin care fiabilitatea și securitatea sistemelor integrate folosite în contoarele inteligente pot fi îmbunătățite prin tehnici de actualizare, validare și protecție a programelor încărcate în memoriile interne ale acestora.

Scopul principal al acestei lucrări este dezvoltarea unui sistem de actualizare fiabil și securizat în rețelele de distribuție cu acoperire limitată a comunicațiilor de date vizând cercetări asupra următoarelor elemente din structura sa:

- componentele software și hardware necesare la nivel local în cadrul fiecărui sistem integrat pentru asigurarea fiabilității și a securității programelor rulate;
- metodele de transport a actualizărilor software prin medii cu semnal radio slab sau prin liniile de înaltă tensiune supuse interferențelor;
- optimizarea transportului și efectuarea actualizărilor la nivel local între nodurile adiacente în funcție de calitatea semnalului.

1.3. Structura tezei de doctorat

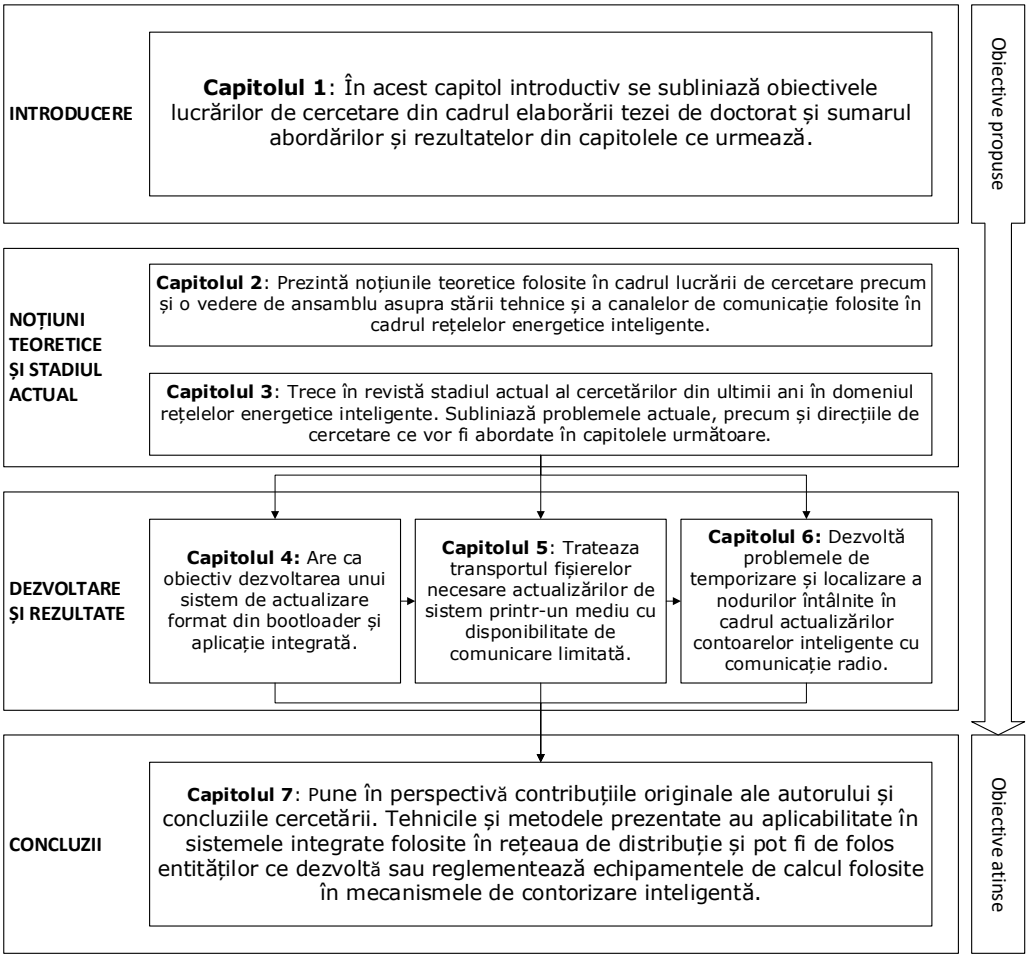

Fig. 1.4. - Structura tezei de doctorat

Structurată pe 7 capitole, teza de doctorat, ilustrată in figura 1.4, acoperă în **primul capitol** tematica aleasă, motivația autorului și încadrarea acesteia în actualul context social și economic. În acest capitol introductiv se subliniază obiectivele lucrărilor de cercetare din cadrul elaborării tezei de doctorat și sumarul abordărilor și rezultatelor din capitolele ce urmează. De asemenea se pune accent pe actualitatea subiectului ales și pe perspectivele de cercetare deschise de tratarea subiectului ales.

În cel de-al **doilea capitol** se prezintă noțiunile teoretice folosite în cadrul lucrării de cercetare, precum și o vedere de ansamblu asupra stării tehnice și a canalelor de comunicație folosite în cadrul rețelelor energetice inteligente. În analiza

inițială se concluzionează limitările echipamentelor instalate în teren și se subliniază durata de viață tehnologică de cel puțin 30 de ani de funcționare pe care acestea trebuie sa o îndeplinească după instalare. Tot în cadrul aceluiași capitol, începe analiza stadiului actual al standardelor tehnologice folosite în industrie pentru actualizarea sistemelor integrate de la distanță. Capitolul descrie procesul de stocare, descărcare și de instalare a actualizărilor prin metodele cunoscute momentan. Se menționează două categorii de probleme:

(i) În prima categorie se discută problema rulării programelor de actualizare la nivel local în cadrul sistemelor integrate, protejarea conținutului intern precum și a fiabilității și a verificărilor de autenticitate necesare în execuția aplicațiilor de contorizare inteligentă.

(ii) În cea de-a doua categorie se discută problema transportului securizat și optim al fișierelor de actualizare sub format binar prin mediile de transport cu disponibilitate redusă, remarcându-se performanța scăzută oferită de metodele uzuale.

În **capitolul 3** se trec în revistă lucrările de specialitate publicate în ultimul deceniu în domeniul rețelelor energetice inteligente. Se subliniază neajunsurile industriei și domeniile de cercetare descrise de literatura recentă, iar astfel se observă că există încă provocări majore legate de managementul și actualizarea contoarelor inteligente instalate în teren precum și provocările legate de infrastructura de comunicații de date atât pentru tehnologiile prin fir cât și pentru cele radio.

Capitolul 4 are ca obiectiv studiul impactului procesului de actualizare asupra contoarelor inteligente și dezvoltarea unui sistem de actualizare format din bootloader și aplicație integrată. Aplicația acoperă atât nevoile de fiabilitate precum și cele de securitate folosind o combinație de metode uzuale optimizate pentru mediul actual al rețelei energetice, totodată încadrându-se în cerințele de sistem uzuale ale unui contor inteligent.

În cadrul **capitolului 5** se tratează problema transportului fișierelor necesare actualizărilor de sistem printr-un mediu cu disponibilitate de comunicare limitată prin metode de secționare a fișierelor la dimensiuni egale cu unitatea de transmisie maximă acceptată de către rețelele de comunicație prin liniile de înaltă tensiune sau prin medii de comunicație radio.

În **capitolul 6** se dezvoltă problemele de localizare a nodurilor întâlnite în cadrul actualizărilor contoarelor inteligente cu comunicație radio. Localizarea contoarelor radio și algoritmii de estimare a distanței au, ca puncte de plecare, informații diferite furnizate de echipamentele de transmisie/recepție integrate. În acest capitol, a fost proiectat și implementat un sistem pentru achiziționarea indicatorului puterii semnalului recepționat (RSSI). S-a pus accent pe variația indicatorului de putere a semnalului recepționat (RSSI) în funcție de distanța și orientarea geometrică a nodurilor și a mediului, atât în spații interioare, cât și în cele exterioare.

În ultimul capitol, **capitolul 7**, se pun în perspectivă contribuțiile originale ale autorului și concluziile cercetării. Tehnicile și metodele prezentate au aplicabilitate în sistemele integrate folosite în rețeaua de distribuție și pot fi de folos entităților ce dezvolta sau reglementează echipamentele de calcul folosite în mecanismele de contorizare inteligentă. Capitolul se încheie cu perspectivele de cercetare ulterioară și concluziile finale.

Luând în considerare scopul și obiectivele tezei enunțate anterior, lucrarea de cercetare și contribuțiile aduse vor putea fi întrebuințate în dezvoltarea continuă a sistemelor de contorizare inteligentă. De asemenea, cercetarea întreprinsă în elaborarea acestei teze deschide o serie de perspective de continuare a prezentei lucrări, cum ar fi: continuarea cercetărilor în domeniul fuziunii tehnologiilor de contorizare inteligentă și a tehnologiilor de tip Internet of Things, perspective privind standardizarea actualizărilor la distanță în domeniul energetic sau aprofundarea studiilor privind algoritmii de localizare a echipamentelor de contorizare inteligentă. Perspectivele pot fi elaborate atât sub forma unor viitoare lucrări de cercetare științifică cât și sub forma unor proiecte de dezvoltare a unor soluții tehnice implementate de către producătorii de echipamente integrate destinate sistemelor energetice rezidențiale.

2. NOȚIUNI TEORETICE

2.1. Introducere în actualizarea sistemelor integrate de la distanță (OTA)

Actualizările sistemelor integrate de la distanță prin metoda OTA se adresează dispozitivelor instalate deja pe teren care au acces la un gateway. Acest gateway poate fi conectat la un sistem de asistență prin internet sau prin alte mijloace în așa fel încât dispozitivele să nu necesite un operator uman pentru a fi aplicate noile actualizări. Programul principal din interiorul dispozitivului este înlocuit prin procesul de actualizare permițând o dezvoltare rapidă și implementarea de noi capabilități, remedieri de erori sau îmbunătățiri de securitate care urmează să fie instalate. Aceasta este o sarcină esențială în dispozitivele electronice din zilele noastre, care au termene foarte stricte de punere pe piață și în care capacitățile de asistență oferite de actualizările OTA extind durata de viață a dispozitivelor existente. Acest lucru permite producătorilor să urmărească dezvoltarea durabilă a noilor dispozitive, permițând în același timp utilizatorilor să beneficieze de o durată de viață prelungită a dispozitivelor.

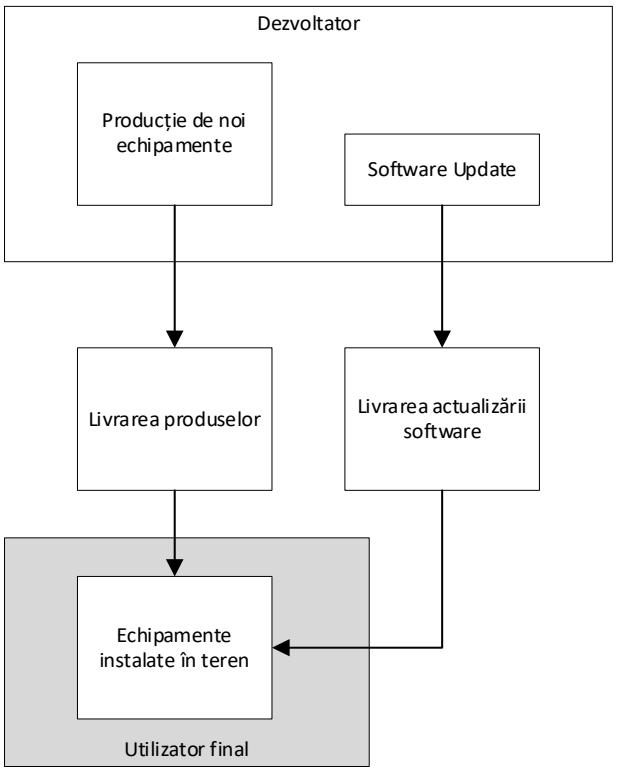

Fig. 2.1. - Schema conceptului de actualizare a sistemelor integrate

După cum arată figura 2.1 de mai sus, dispozitivele fabricate părăsesc fabrica în timpul fazei de livrare a produselor și acestea sunt instalate de către utilizatorul final sau de către un terț contractat de către dezvoltator. Odată ce aplicația trebuie să sufere ajustări, depinde de producător să pună acest lucru la dispoziția clienților săi printr-o operațiune de actualizare a sistemelor integrate.

Constrângerile de resurse determinate de economia de piață fac ca proiectarea unei actualizări software robuste să fie foarte dificilă, așa cum vom sublinia în următoarele subcapitole. În afară de parcurgerea unora dintre proiectele de referință ale producătorilor consacrați, cum ar fi Analog Devices [2] sau Atmel [3], vom atrage atenția și asupra problemelor majore cu care se confruntă această procedură, precum și a compromisurilor fiecărei tip de implementare.

Toate proiectele urmează același ciclu de viață al dispozitivului. Odată ce este necesară o actualizare a software-ului, aceasta trebuie să fie exclusiv responsabilitatea producătorilor și va necesita cât mai puțină interacțiune umană posibilă din partea utilizatorului final. Prin urmare, un proces simplu de actualizare a software-ului ar trebui să asigure urmarea acestor pași de concept:

1. Producătorii proiectează și dezvoltă dispozitive
2. Dispozitivele sunt vândute și distribuite clienților
3. Utilizatorii finali instalează dispozitivele cu software-ul implementat inițial v.1.0
4. Producătorii implementează o actualizare software v.2.0 pentru a sprijini noi caracteristici sau pentru a remedia problemele de securitate
5. Dispozitivele instalate primesc v.2.0
6. Utilizatorii finali pot folosi acum un produs actualizat

2.2. Fundamente legate de programul permanent (firmware) folosit in sistemele integrate

Înainte de a aprofunda noțiuni mai complexe ale sistemelor de actualizare a programelor permanente din sistemele integrate, trebuie să definim ce este un program permanent și cum este acesta creat.

Fișierele de tip firmware, ce conțin programul sistemului integrat, sunt instrucțiuni cod mașină pentru procesor codate binar. Acestea cuprind întreaga aplicație executată de un sistem încorporat și rezidă într-o memorie nevolatilă a microcontrolerului sau a microprocesorului. Fișierul binar rulat de către sistemul integrat este rezultatul procesului de compilare.

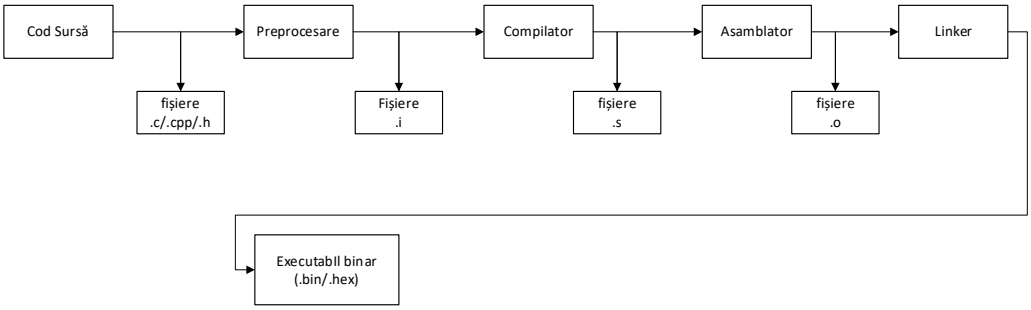

Fig. 2.2. - Diagrama procesului de compilare

Aplicația începe cu scrierea codului acesteia într-un limbaj de programare standardizat, aici vom discuta despre aplicații scrise în limbajul de programare C, dar toate limbajele de programare compilate urmează același proces.

Odată ce codul a fost finalizat, fișierele sursă (.c) și fișierele antet (.h) sunt transformate individual de către preprocesor în fișiere intermediare „.i", numite formal unități de translatare. În această etapă, toate directivele preprocesorului au fost extinse, macro-comenzile sunt înlocuite cu echivalentele lor textuale, fișierele #include sunt copiate și încorporate în fișierele sursă și condiționalele #if/#ifdefs sunt evaluate și pe baza simbolurilor preprocesatorului din proiectul selectat vor produce fișierele „.i" pregătite pentru inserarea in următoarea faza a compilatorului. Pentru a opri compilatorul gcc în stadiul preprocesorului, se poate utiliza semnalizatorul „-E". (e.g. gcc -E main.c -o main.o).

Compilatorul preia fișierele intermediare produse anterior și traduce limbajul de programare în instrucțiuni de asamblare care sunt specifice procesorului pentru care compilăm. În timp ce codul sursă utilizat în preprocesor este agnostic față de arhitectura hardware care urmează să fie utilizată, compilatorul trebuie să cunoască setul de instrucțiuni specifice pe care le poate folosi înainte de a putea produce fișiere asamblabile utilizabile („.s").

Odată ce fișierele sursa de timp assembler sunt procesate, acestea trec prin asamblator, care le transformă în fișiere obiect „.o". Fișierele obiect sunt colecții de simboluri, cum ar fi funcțiile și variabilele, acestea fiind structurate în diferite zone de memorie, cum ar fi „.text" pentru instrucțiuni și „.data" pentru variabile.

Fiecare fișier obiect începe cu un cuprins, care conține o structură numită tabel de simboluri. Acest tabel descrie ce variabile sau funcții sunt conținute în fișierul obiect și în ce locație pot fi găsite. Aceste informații vor fi utilizate ulterior în procesul de linkare.

Linkerul preia toate fișierele obiect produse anterior și își dă seama ce trebuie lipit (legat; linked) împreună pentru a forma un program care să satisfacă toate dependențele de cod. Locațiile finale ale obiectelor sunt decise de un relocator în interiorul linker-ului care creează o hartă de memorie. Aceasta plasează codul fie în RAM (spațiu de memorie virtuală), fie în memorie Flash (spațiu de memorie folosit la încărcare), în funcție de tipul de variabile, de necesitatea schimbării valorilor în timpul rulării sau în funcție de tipul de instrucțiuni executate de microcontroler [4].

Rezultatul final al procesului de conectare este un fișier binar executabil, codificat fie ca fișier .bin brut, fie ca fișier .hex. Acest fișier conține și prima instrucțiune care va fi rulată, iar aceasta este rutina de tratare a întreruperii de reset [5] [6].

2.2.1. Topologii de sistem

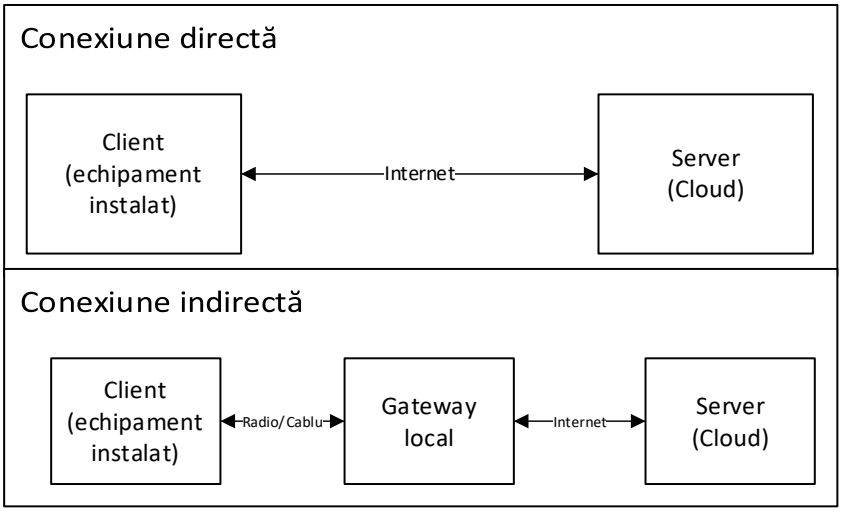

Fig. 2.3. - Tipuri de topologie bazate pe tipul de interconectare a dispozitivelor.

Părțile implicate în procesul de actualizare, producătorul și utilizatorul final, sunt uneori diferențiate bazându-ne pe poziționarea lor topologică în rețea. Astfel, utilizatorul final va fi denumit partea client și producătorul și sistemul său de distribuție a aplicațiilor actualizate, ca partea server sau partea cloud în dispozitivele conectate la internet. Arhitecturile pe care le vom discuta ulterior sunt sisteme ce nu țin cont de tipul tehnologiei de comunicații utilizate între cele două părți și se pot conecta direct la serverul de internet / cloud sau pot utiliza o conexiune indirectă cu un gateway(poartă de acces) conectat la internet care facilitează comunicarea cu dispozitivele finale locale conform figurii 2.3.

Conexiunile directe se bazează pe dispozitivul final că va gestiona, printr-o conexiune la internet, comunicația cu o soluție de tip server/cloud. Acest lucru se face, de obicei, având dispozitivul final (client) conectat direct la un router de internet prin conexiune ethernet sau Wi-Fi, iar pe unele sisteme ce necesită o conexiune dedicată comunicația se face prin comunicații de bandă largă ce pot fi încorporate în soluția finală direct de către producător. Această metodă de comunicare este des întâlnita în cadrul dispozitivelor instalate în aer liber, iar acestea pot să ”vorbească” în continuare direct cu serverul la cerere și este principala soluție utilizată în dispozitivele de măsurare inteligentă a consumului de gaz sau de apă.

Conexiunile indirecte au început să piardă teritoriu în ultimii câțiva ani [7], în primul rând datorita noilor familii de microcontrolere ce permit dezvoltarea de

dispozitive mai ieftine și conectate direct la internet, într-un mod rentabil și fiabil. Cu toate acestea, conexiunea indirectă este încă principala tehnologie utilizată de soluțiile Internet of Things (IoT) și de echipamentele de contorizare inteligentă cu capacități de comunicare prin liniile electrice (PLC) [8]. În sistemele indirecte, gateway-ul menține comunicarea cu serverul cloud pentru a-l informa despre starea dispozitivului local (i.e. versiunile firmware-ului, citirile jurnalului de erori, starea generală de sănătate și capabilitățile de actualizare ale echipamentului), precum și pentru a descărca noi actualizări ale aplicației când acestea sunt disponibile. Odată ce noul software ajunge la gateway, serverul nu mai este implicat în procesul de actualizare și aceasta se desfășoară mai departe doar la nivel local. Ultimul salt al software-ului de la gateway la dispozitivele finale se face folosind un protocol de comunicație din sistemul local (de ex. ZigBee, Wi-Fi, PLC). În câteva cuvinte, dispozitivul gateway va acționa ca o copie (umbră) locală a serverului, fiind acum responsabil cu supravegherea procedurii de instalare a noului program.

Provocările de transport cu care se confruntă fiecare topologie fac obiectul unui capitol ulterior și ambele tipuri de sistem vor fi acoperite. Vom analiza avantajele și dezavantajele acestor tipuri de sisteme pe baza cerințelor aplicației și vom analiza modul în care acestea pot fi încorporate într-un mecanism robust de actualizare.

2.2.2. Provocări uzuale în procesul de actualizare

Pe măsură ce sistemele încorporate sunt supuse actualizării de la distanță, siguranța și securitatea dispozitivelor sunt cei doi factori cheie pe care trebuie să îi luăm în considerare. Starea de funcționare a dispozitivului trebuie menținută înainte și după actualizare și funcționarea corectă a dispozitivului nu poate fi periclitată. Accesul fizic la dispozitivele instalate deja pe teren este rareori o abordare fezabilă pentru efectuarea actualizărilor de firmware, iar prin urmare fiabilitatea și robustețea dispozitivului sunt concepte de proiectare care nu trebuie compromise în niciun caz în timpul planificării dezvoltării. Pe de altă parte, producătorii trebuie să se asigure că dispozitivul va fi utilizat numai în scopul pentru care a fost construit și reconvertirea acestuia pentru alte scopuri, de cele mai multe ori rău intenționate, trebuie prevenită, iar logica internă a dispozitivului nu trebuie să permită acest lucru.

Întrucât am acoperit în linii mari securitatea și siguranța sistemului integrat, trebuie să luăm în considerare și fișierele de actualizare și alte programe software care părăsesc serverul producătorului împreună cu o proprietate virtuală care trebuie protejată cu aceleași principii de securitate și siguranță.

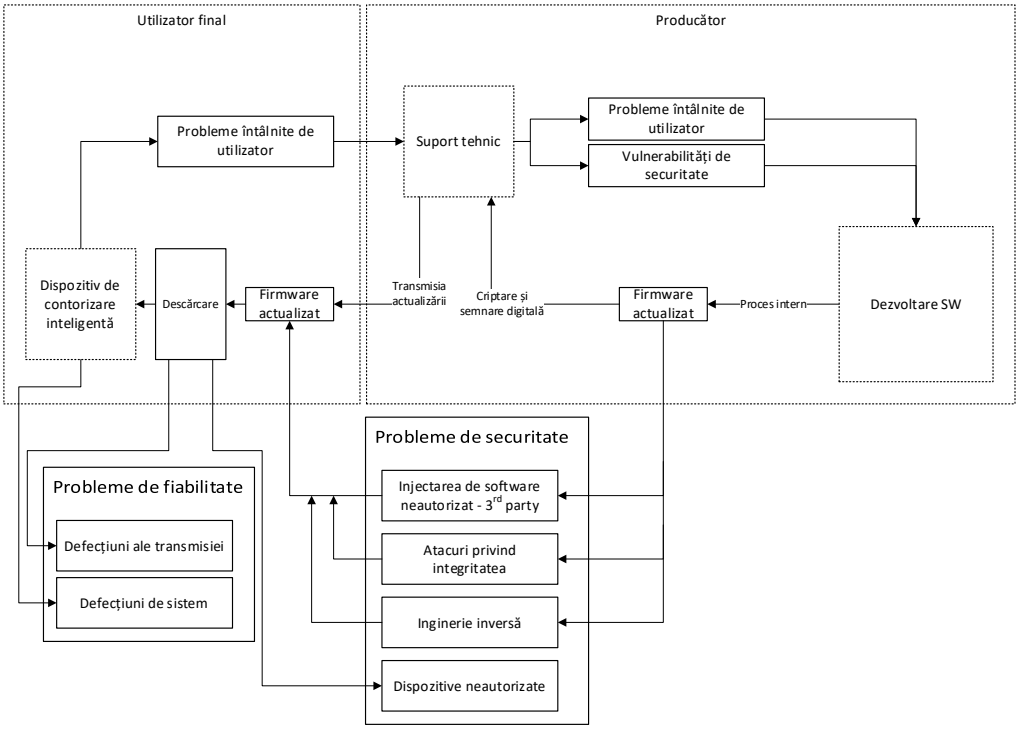

Fig. 2.4. - Problemele majore din procesul de instalare și dezvoltare a noului firmware.

Figura 2.4. prezintă delimitările procesului de actualizare între entitățile principale implicate, utilizatorul final și compania producătoare de contoare inteligente. Actualizările de program apar de cele mai multe ori ca urmare a unui defect de tip software sau ca urmare a unei vulnerabilități de securitate descoperite în industrie. În urma dezvoltării software a unui nou program firmware în cadrul companiei de producției a contoarelor inteligente, va rezulta un fișier binar criptat și semnat digital cu chei specifice fiecărui producător. Fișierul binar ce conține actualizarea ajunge apoi la serviciul de suport tehnic, iar acesta va decide ce lot de contoare trebuie să fie actualizate și va indica acestor contoare disponibilitatea descărcării unui nou firmware. De asemenea, figura prezintă și principalele puncte de atac în timpul procedurii de actualizare a firmware-ului, puncte pe care le vom aborda în următoarele capitole. Se vor discuta problemele de fiabilitate a echipamentelor de contorizare și problemele de fiabilitate a procesului de descărcare, precum și problemele de securitate apărute de-a lungul întregului proces de actualizare.

2.2.2.1. Probleme de fiabilitate

Eșecuri de transmisie a fișierelor folosite în procesul de actualizare

Pe măsură ce noul firmware se deplasează de la serviciul de asistență cloud al producătorului la dispozitivele instalate pe teren, acesta se confruntă cu aceleași provocări pe care le întâlnim in cadrul oricărui protocol de descărcare a fișierelor. Protocolul utilizat de către producător trebuie să fie pregătit să gestioneze întreruperile transmisiei, descărcările incomplete ale fișierelor sau corupția fișierelor descărcate. Astfel de scenarii sunt adesea întâlnite din cauza unei conexiuni de rețea instabile, a resetărilor sistemului sau a întreruperilor de alimentare.

În timp ce HTTP, HTTPS, FTP sunt protocoale deja consacrate folosite de către industrie, iar TCP, UDP, sunt protocoalele utilizate la nivelul OSI de transport, aplicația principală software care gestionează fișierele de actualizare trebuie sa gestioneze la rândul ei, descărcarea corectă și recuperarea acestora în cazul unor problemele de transmisie. Trebuie sa ne asigurăm ca o actualizare software nu va începe niciodată cu o descărcare incompletă a fișierelor OTA și nici cu un fișier corupt sau trunchiat.

Defecte de sistem

Al doilea tip de probleme de siguranță acoperă defecțiunile specifice sistemului integrat. Acestea cuprind atât defecțiuni hardware, precum și probleme cauzate de întreruperi de alimentare neprevăzute sau alte defecțiuni interne. Măsurile de siguranță implementate la nivelul bootloaderului trebuie să protejeze procedura de pornire a aplicației astfel încât aplicația să nu poată afecta componentele hardware și viceversa.

2.2.2.2. Sumar al problemelor de securitate întâlnite in sistemele integrate

Deoarece problemele de siguranță discutate mai sus sunt măsuri luate pentru a evita interferențele naturale în instalarea actualizărilor software, securitatea are ca scop protejarea echipamentelor, a utilizatorului și a producătorului împotriva atacurilor rău intenționate și a altor riscuri de piratare. Problemele de securitate sunt clasificate pe baza tipurilor de atac în probleme de control al accesului, probleme de confidențialitate și probleme de integritate [9] [10].

Controlul accesului

Pentru a evita accesul la serverul producătorului, contoarele inteligente instalate pe teren care solicită o actualizare trebuie mai întâi să fie autentificate. Autentificarea este procedura supusă unui dispozitiv în comunicarea cu serverul pentru a verifica revendicarea identității sale ca produs autentic. Acest lucru interzice dispozitivelor care sunt falsificate sau clonate să obțină acces în serverul de asistență înainte de a începe orice altă comunicare. Dispozitivele rulează, de

asemenea, propriul proces de autentificare al serverului cu care fac schimb de informații. Prin mijloace specifice, un server imitat ar putea fi folosit pentru a citi sau scrie informații pe dispozitivele care sunt deja în teren. Pentru a ne asigura că sistemele integrate instalate in contoarele inteligente vor verifica autentificarea serverului cu care comunică se vor folosi certificate de securitate tranzacționate de obicei printr-o comunicație securizată de tip SSL [11].

Dacă dispozitivul a trecut controlul de autentificare, va trece acum printr-o verificare a autorizării acestuia, care verifică faptul că acestui tip de dispozitiv i se permite să acceseze caracteristici specifice de pe server la un moment dat. Acest proces ar putea fi utilizat pentru a restricționa accesul la actualizări unei game de produse bazat pe diferite valori, valori ce pot începe de la categoriile de preț ale dispozitivului până la poziția geografică actuală a dispozitivului.

Autorizarea este utilizată pentru a verifica dacă un anumit dispozitiv are acces de citire sau scriere pe serverele de asistență pe care producătorul le-a configurat. În mod similar cu paradigma de autentificare, dispozitivul în sine trebuie să autorizeze și el la rândul sau serverul atât pentru drepturi de citire cat și pentru cele de scriere. Uneori, s-ar putea să fie cazuri în care există mai multe servere configurate de către producător și fiecare dintre acestea ar putea avea niveluri diferite de acces la citire și scriere bazate pe propria certificare de securitate sau bazate pe locația de instalare a acestora.

Integritatea și confidențialitatea programelor și a datelor din sistem

Imaginile software instalate pe contoarele inteligente sau fișierele binare transferate de pe servere sunt toate supuse legilor de proprietate intelectuală și aparțin producătorului. Entitățile sau utilizatorii neautorizați nu pot accesa aceste informații și nu vor fi puse la dispoziția terților neautorizați fără acordul corespunzător al proprietarului proprietății intelectuale. Acesta este un subiect larg care trebuie abordat încă din fazele inițiale de proiectare. Începe de la controlul accesului fizic asupra echipamentelor, la hardware-ul ales astfel încât acesta să aibă mecanisme specifice de protecție pentru a evita accesul la memorie odată ce contoarele au părăsit fabrica. Un mecanism tipic pentru o astfel de protecție îl constituie siguranțele (virtuale) programabile de unica folosință care sunt arse la ieșirea de pe linia de producție blocând citirea fizică a informațiilor din sistem odată ce controlul calității a aprobat dispozitivul pentru vânzare și instalare. Deoarece contoarele ajung mai târziu sa fie instalate pe teren sau pe măsură ce fișierele cu programele actualizate se deplasează prin servere și medii ce nu se află sub controlul și incidența producătorului, trebuie să luam în considerare adăugarea unui nou nivel de securitate pentru a proteja confidențialitatea informațiilor stocate în memoria contoarelor sau în fișierele OTA.

Prin criptare, informațiile valoroase sunt transformate în date ilizibile, inaccesibile, și care vor fi inutilizabile pentru orice terț neautorizat. Criptografia protejează informațiile sensibile din spațiul de stocare intern sau informațiile comunicate dinspre și către servere prin utilizarea cheilor de criptare împreună cu un sistem de gestionare a cheilor ales de către producător [11].

2.3. Inițializarea sistemului de operare și procesul de încărcare a aplicației

Fiecare dispozitiv electronic bazat pe un microprocesor prinde viață printr-o procedură de pornire bine definită. Odată ce dispozitivul a fost alimentat, o serie de sarcini sunt efectuate de către sistem înainte ca acesta să intre într-o stare permanentă de funcționare. Sarcina principală a unui bootloader (încărcător de program) este de a se asigura că întreg sistemul se află într-o stare corectă înainte de a continua procedura de lansare a pașilor de inițializare a sistemului de operare. Deși acest lucru ar putea părea un proces banal, conceptul de pornire, numit boot-up, este un proces complex și acoperă numeroase tipuri de configurații și de implementări potențiale pentru a permite unui sistem să fie flexibil și robust în același timp.

Inițial sistemele integrate nu aveau un bootloader în memoria ROM și codul ar era pur și simplu executat dintr-o anumită locație fixă din memorie imediat după resetarea procesorului. În prezent, bootloader-urile au fost extinse pe mai multe etape de procesare, iar fiecare etapă are o sarcină specifică cu roluri precum cel de a asigura verificările de securitate, rolul de a instala configurația potrivita echipamentului folosit sau doar rolul de a executa pașii operaționali care vor aduce codul aplicației în poziția finala de unde acesta va fi executat de unitatea de procesare. Acele sisteme care trec direct la executarea codului aplicației dintr-o sursă externă (de obicei memorii flash externe de tip NOR) trebuie, prin implementarea lor, să ia în considerare situațiile de concurență dintre sarcinile executate de procesor și disponibilitatea accesului de citire a instrucțiunilor din memoria externă. De asemenea, un alt dezavantaj al faptului că unele sisteme nu folosesc un bootloader este dat de limitarea locației unde poate fi scris programul final al aplicației în memorie, lucru ce duce de cele mai multe ori la rate mai mici de acces către memoriile de stocare externe și implicit și a vitezei de execuție a aplicațiilor.

Alteori, pentru a evita prețul ridicat al memoriilor externe cu viteză de citire mai rapidă, o cantitate mică de cod care rulează în timpul fazei de pornire din memoria internă poate pregăti memoria RAM cu instrucțiunile de program aflate în memoria externă și poate ulterior sări la codul de inițializare a aplicației când transferul a fost finalizat.

În sistemele moderne pe lângă gestionarea memoriilor, configurația sistemului face și ea parte din bootloader. Pentru optimizările de cost, companiile pot opta pentru același tip de hardware în toate produsele lor, lăsând la latitudinea bootloaderului să înceapă o aplicație diferită pe baza unor pini de configurație sau pe baza datelor stocate extern care ar putea face diferența între un produs low-end sau high-end . Alte produse ar putea utiliza hardware diferit cu aceeași aplicație lăsând bootloaderului sarcina de a afla ce tip de aplicație trebuie să inițializeze. [12]

Bootloaderul inițial denumit bootloader de primă etapă, rulează primul nivel de instrucțiuni din procesul de inițializare a sistemului. Acesta este instalat de către furnizorii de microcontrolere sau microprocesoare într-o memorie de tip ROM și are un număr limitat de configurații ce pot fi realizate prin arderea siguranțelor programabile OTP sau prin conectarea semnalelor hardware la anumiți pini. Acei pini sunt utilizați în mod obișnuit pentru a selecta un mod de încărcare descris în

manualul tehnic al utilizatorului sau în fișa tehnică a microcontrolerului. Producătorii de cipuri nu oferă o mare flexibilitate în bootloader-ul ROM atât din motive de cost cât și din motive de securitate. Prin urmare, pentru a obține mai multe funcționalități, cum ar fi upgrade-uri de firmware, autentificări, verificări de securitate, etc., trebuie să ne deplasăm către o a doua etapă a bootloader-ului.

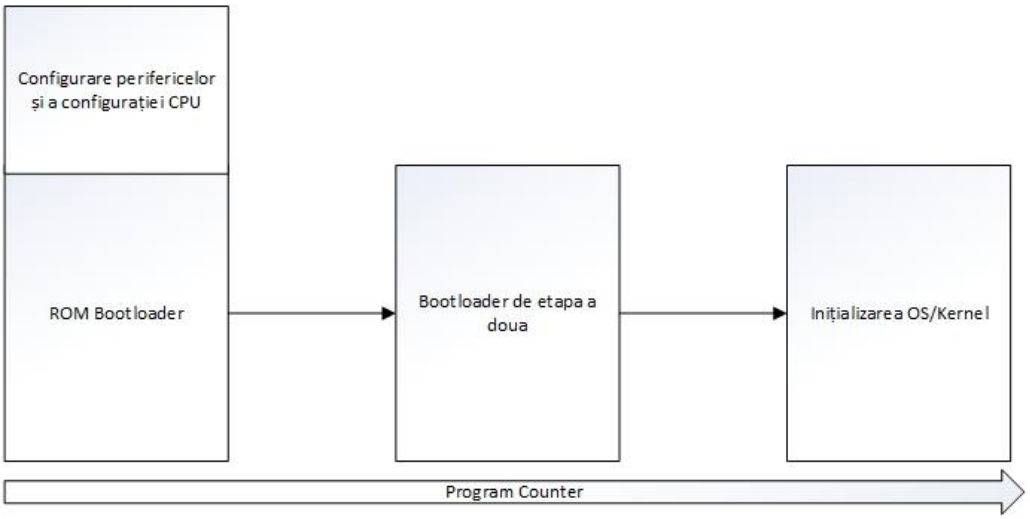

Fig. 2.5. - Structura bootloaderelor in funcție de etapele de inițializare

Figura 2.5. arată pașii de execuție întâlniți în toate sistemele cu încărcător de program cu etape multiple. Toate programele din sistemele integrate pornesc prin încărcarea vectorului de întreruperi și prin configurarea ceasurilor interne, apoi la nivelul bootloaderului de primă etapă se pot face verificări minimale de hardware urmând ca apoi să se facă saltul la prima adresă din bootloaderul de etapă secundară. Program counterul sistemului i-a valoarea adresei la care este stocată funcția de inițializare a bootloaderului de etapa a doua, iar după ce întreg procesul dedicat acestei etape a fost finalizat cu succes se face un ultim salt către pornirea sistemului de operare.

2.4. A doua etapă de inițializare a sistemului din cadrul bootloaderului

Cea de-a doua etapă de încărcare a programului principal din sistemele integrate constă în codul de program scris de dezvoltatorii de aplicații pentru a îndeplini sarcinile de inițializare specifice fiecărui produs și este plasat în locația fixă aleasă de către producătorii microprocesoarelor in implementarea primei etape de încărcare. Aceasta locație fixă va fi folosită pentru primul salt din codul aplicației.

Sarcinile de inițializare a sistemului în cea de-a doua etapă variază de la inițializarea memoriei externe până la stabilirea comunicației cu perifericele de interfațare. Periferice precum SPI FLASH, memorii EEPROM sau protocoale precum USB, I2C, Ethernet sunt doar câteva dintre modulele ce pot fi inițializate în acest moment și ce pot fi utilizate pentru alte etape ulterioare de configurare sau validare.

Dezvoltatorii de aplicații vor trebui să proiecteze această etapă în funcție de nevoile aplicației lor, iar sistemul va trebui sa treacă prin mai multe sarcini înainte de inițializarea sistemului de operare al sistemului integrat sau înainte de a declanșa nucleul(kernel) sistemului într-o mașină bazată pe Linux.

Pe lângă ceea ce a fost deja verificat în prima etapă de inițializare, această etapă ar trebui să se ocupe de funcții mai avansate printre care amintim:

- Configurarea registrelor de control ale procesorului
- Inițializarea sistemelor critice și a perifericelor
- Configurarea întreruperilor și configurarea MMU
- Încărcarea stack-pointer-ului și a configurației memoriei RAM
- Verificări de integritate a firmware-ului
- Verificări de autentificare firmware
- Verificări generale de securitate de inițializare
- Actualizări de firmware
- Moduri de recuperare firmware
- Încărcarea kernelului sau a sistemului de operare

Bootloader-urile implementate in cea de-a doua etapă de inițializare a sistemelor integrate au foarte puține seturi de operații specifice hardware-ului, singurele astfel de instrucțiuni fiind folosite pentru configurarea perifericelor și a ceasurilor interne utilizate în această etapă. Acest lucru face ca scrierea unui bootloader proprietar să fie adecvat pentru o portabilitate bună ce poate fi refolosit pe mai multe tipuri de aplicații sau hardware, oferind dezvoltatorilor șansa de a reutiliza acest program pe întreaga bază de produse.

Având în vedere că portabilitatea a fost luată în considerare la implementările anterioare din comunitatea open source, unele bootloadere au devenit mai populare și sunt acum disponibile în mod implicit în majoritatea mediilor de dezvoltare furnizate de producătorii care fabrică hardware destinat sistemelor încorporate bazate pe Linux. Unul dintre acestea este proiectul open source Universal Bootloader sau pe scurt, U-Boot.

2.4.1. Încărcătorul de program U-boot

U-Boot oferă un cadru de interacțiune integrat care oferă o versatilitate considerabilă și numeroase opțiuni pentru configurarea unui bootloader generic. Acest lucru conferă dezvoltatorilor un mediu în care detaliile hardware ale microprocesoarelor folosite nu influențează etapele de inițializare a sistemului. U-Boot își începe execuția cu un program interactiv ce rulează imediat după inițializarea simplă a procesorului și care permite utilizatorilor să interacționeze cu configurațiile necesare inițializării sistemului printr-o interfață de comunicație serială-caracteristică de tip consolă. Utilizatorul are, de asemenea, opțiunea de a rula Universal Bootloader într-un mod automat, fără a necesita intervenția manuală, acesta rulând dintr-o memorie flash sau altă memorie internă, după care se mută în RAM și va executa funcții mai avansate. În afară de încărcarea sistemului de operare, interfața serială poate oferi funcții complexe, cum ar fi:

- Încărcarea memoriei și accesarea/citirea, ștergerea și programarea prin intermediul interfeței seriale
- U-Boot permite, de asemenea, sistemului să pornească de la o varietate de interfețe, cum ar fi USB (Universal Serial Bus), SD (securizat digital), PCIe (Peripheral Component Interconnect Express), SATA sau chiar Ethernet sau alte interfețe de rețea [13].
- U-Boot este, în ultima perioadă, opțiunea preferată de către dezvoltatorii de sisteme încorporate bazate pe sistemul de operare Linux. Deoarece acesta este un bootloader open source, Universal Bootloader adună continuu contribuțiile comunității sale și are suport actualizat pentru toate arhitecturile obișnuite ale CPU-urilor și respectă standardele de securitate cerute de piață.

2.5. Procedură de bază pentru actualizarea firmware-ului

Orice proces reușit de actualizare a firmware-ului unui sistem integrat se încheie cu scrierea unui nou software într-o locație fixă dintr-o memorie nevolatilă a sistemului. Memoria respectivă va fi folosită ulterior de către bootloader pentru a inițializa software-ul proaspăt instalat, rezultând într-un sistem actualizat ce l-a înlocuit pe cel învechit.

Pentru a realiza cele de mai sus, noul software trebuie să ajungă la dispozitivul nostru prin interacțiune fizică (USB, interfețe serializate, carduri de memorie etc.) sau printr-o interfață virtuală Over-The-Air, OTA. În toate cazurile, actualizările încapsulate sub forma unor date binare sunt mutate de la o sursa de furnizare a actualizărilor, fie ea locală sau nu, într-o memorie internă pe care sistemul o va utiliza ulterior pentru a rula mai multe rutine de securitate și validare. Dacă totul merge bine, sistemul va putea finaliza acum procesul de actualizare scriind peste vechiul software sau lângă acesta, în funcție de topologia de memorie aleasa in implementarea bootloaderului.

2.6. Structurarea memoriilor interne

Structurarea memoriilor nevolatile folosite în procedura de actualizare a sistemelor integrate se face ținând cont de nevoile sistemului. În memoriile nevolatile folosite de către microcontroler se vor păstra zone pentru stocarea bootloaderului (încărcătorului), zone pentru stocarea aplicației curente sau a aplicației ce urmează sa fie descărcată sau alte zone pentru configurații și setări interne folosite de către sistem. In alegerea unei structuri se vor lua in considerare limitările hardware-ului folosit precum și necesarul de spațiu al aplicației, sistemele simple vor avea o structură rudimentară cu o singură partiție, iar sistemele complexe se vor întinde pe multiple sectoare în care fiecare are un rol bine definit.

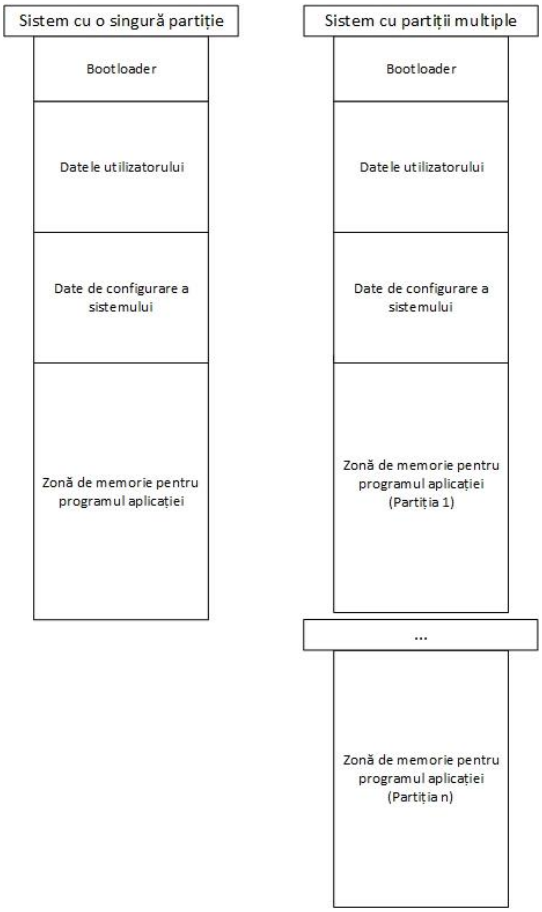

Fig. 2.6. - Structuri tipice pentru sisteme cu o singură partiție sau cu partiții multiple

Figura 2.6. prezintă cele două tipuri de structuri ale memoriei interne folosite în sistemele de actualizare la distanță. Ambele structuri au în componență un încărcător de program (bootloader) și un sector de memorie destinat datelor necesare configurării sistemului și a datelor de utilizator. Diferența majoră o constituie partiționarea sistemului de stocare a aplicației. Cele mai simpliste sisteme au un singur sector destinat programului aplicației, iar complexitatea crește pentru sistemele cu partiții multiple.

2.6.1. Sisteme integrate bazate pe o singura partiție pentru aplicație

Sistemele încorporate care, de cele mai multe ori din motive economice, nu pot aloca o zonă de memorie swap-out pentru schimbul de aplicații între cea curentă și cea actualizata, se bazează pe o singură partiție. Acest lucru elimină flexibilitatea săriturilor între partiții sau sectoare flash atunci când lucrurile nu merg conform planului și de cele mai multe ori pot scădea fiabilitatea întregului sistem. Dezvoltatorii trebuie să opteze pentru acest tip de sisteme din motive de reducere a costurilor sau atunci când dezvoltarea unor mecanisme de recuperare mai complexe nu sunt necesare. Exista și cazuri când s-ar putea ca un coprocesor să utilizeze una dintre aceste abordări și să se bazeze pe controlerul principal pentru a reprograma sistemul atunci când este detectat un defect în procesul de actualizare a aplicației.

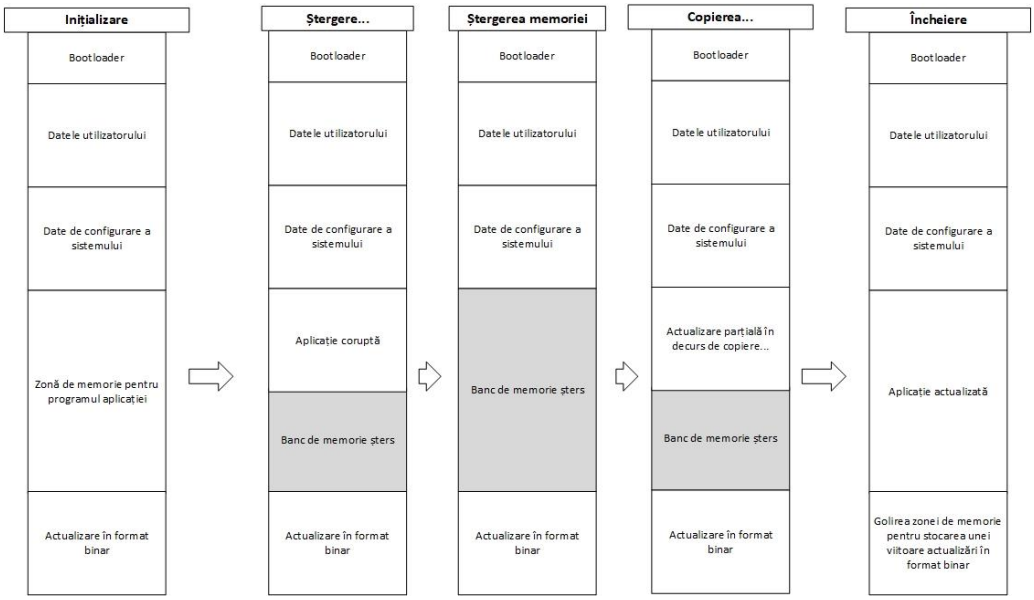

Fig. 2.7. - Etapele de actualizare a unui sistem integrat cu o singura partiție

După cum se vede în fig. 3, detaliile de implementare ale unui sistem cu o singură partiție sunt simple și ușor de dezvoltat. Bootloader-ul va șterge la un moment dat aplicația care rulează pentru a crea spațiu liber pentru noul software

(de la pasul de ștergere până la pasul de copiere). Acesta este un punct vulnerabil în care defecțiunile pot opri sistemul și există riscul ca sistemul să rămână cu o memorie goală. O întrerupere a alimentarii sau repornirea sistemului după ștergere sau în timpul acesteia trebuie luată în considerare atunci când se dezvoltă un nou bootloader pentru un sistem integrat cu o singură partiție. Această perioadă de interschimbare a aplicației curente cu cea actualizată nu ar trebui să împiedice sub nici o formă reluarea procesului de actualizare la următoarea pornire a bootloaderului.

În cazul in care procesul de actualizare a fost întrerupt sistemul va reporni doar cu bootloaderul intact, acesta va porni automat un nou proces de actualizare pentru a încerca să recupereze aplicația și totodată întregul sistem.

Platformele educaționale sau chiar și cele industriale au dezvoltat sisteme bazate pe o partiție unică cu bootloadere care acceptă programarea printr-o comunicație serială (de cele mai multe ori o comunicație serială simplă UART). Acest lucru menține cerințele de memorie scăzute, permițând în același timp reprogramarea plăcilor fără un instrument de programare sau un depanator flash. Unul dintre cele mai populare produse care utilizează acest tip de abordare este familia Arduino bazată pe MCU-uri Atmel sau sistemele WiFi Espressif ESP32 sau ESP8266 [16][17].

2.6.2. Sisteme integrate bazate pe două partiții

În sistemele integrate cu memoria programului intern împărțita în mai multe partiții, exista secțiuni de memorie identice ca structură, iar comutarea între partiții se poate face instant într-o singură operațiune conferind astfel atomicitate transferului de la aplicația curentă la aplicația actualizată.

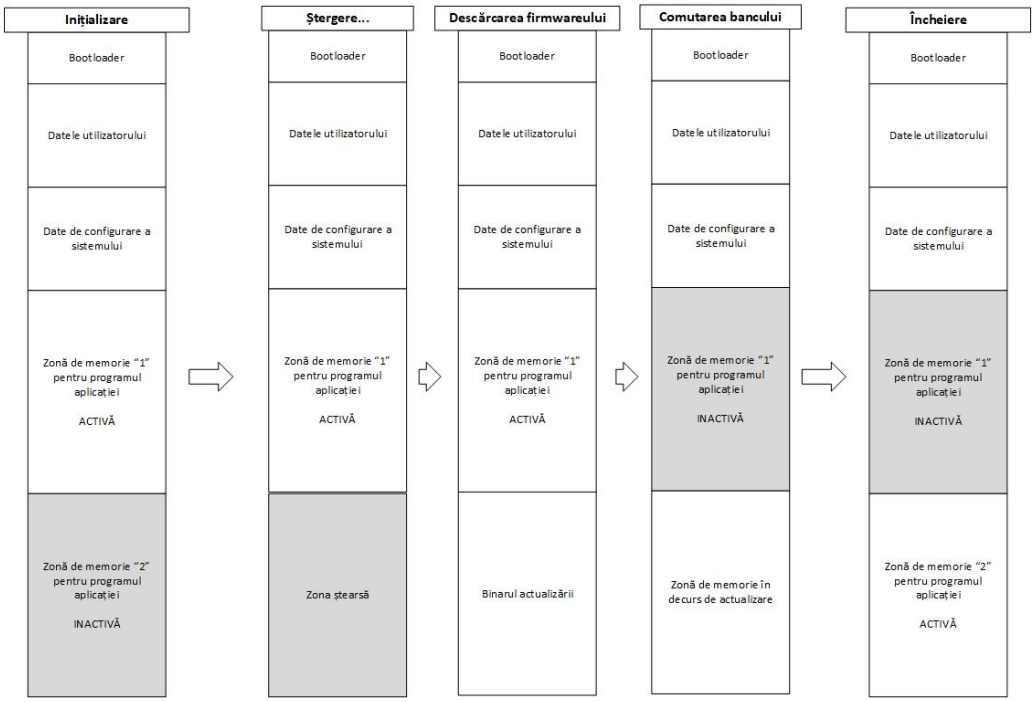

Fig. 2.8. - Etapele procesului de actualizare într-un sistem integrat cu două partiții

Figura 2.8 descrie un proces simplu de actualizare a aplicației într-un mediu cu partiție dublă, iar spre deosebire de sistemul cu o singură partiție se pot observa avantaje de performanță și de robustețe a procesului de actualizare specifice sistemelor cu partiții multiple, precum și dezavantajele legate de spațiul de memorie necesar, aspecte ce urmează a fi explicate în detaliu mai jos. Avantajul de a avea un sector de stocare secundar face ușoară evitarea oricărei interferențe cu aplicația care rulează în momentul actualizării. Prin urmare, nu există nicio etapă intermediară în care se modifică software-ul activ principal, iar riscul de corupere a programului curent este inexistent. În același timp trebuie amintit și faptul că software-ul actual este păstrat ca o copie de rezervă pe tot parcursul procesului de actualizare.

În prima partiție, avem un software care rulează versiunea 1.0, pe care dorim să îl actualizăm la o versiune software 2.0 superioară. Tot ce trebuie să facem este să începem descărcarea în cea de-a doua partiție inactivă. Odată ce descărcarea s-a terminat și sectorul a trecut peste toate verificările necesare, bootloader-ul va primi un set de semnalizări. Aceste fanioane trimise către bootloader indică faptul că la următoarea repornire, în loc să pornim partiția 1, activăm partiția 2 cu noua aplicație. Dacă nu sunt descoperite probleme în timpul primului boot-up al programului actualizat, partiția 1 rămâne inactivă si așteaptă să fie suprascrisă într-un upgrade viitor. Pe de altă parte, dacă se detectează o defecțiune pe programul actualizat, partiția 2 devine din nou dezactivată și putem reveni la versiunea inițială de software 1.0 pentru a recupera sistemul general.

Din aceste procese putem vedea că principalele avantaje ale unui sistem de partiție dublă sunt:

- Rularea software-ului nu este afectată în procesul de actualizare
- Actualizările se fac într-un mod atomic (i.e. într-o singură operațiune se poate comuta între programul actualizat sau cel curent)
- Sistemul partiționat astfel este tolerant la erori de scriere si este pretabil pentru mecanisme de revenire la un software funcțional in caz de avarie

Acest tip de structură de partiție dublă oferă numeroase avantaje față de sistemele cu o partiție unică, dar toate acestea vin cu costul unei facturi crescute de componente (BOM). Costul crescut este cauzat de memoria suplimentară necesară pentru a duplica zona de memorie și acesta este un factor important care trebuie luat în considerare de către echipa de dezvoltare atunci când se alege o noua structură, deoarece are un impact direct și imediat în planul de afaceri. Prin urmare, toate avantajele de mai sus pot fi uitate dacă este necesară alegerea unei noi memorii flash sau a unui SOC superior (i.e. cu mai mult spațiu de stocare intern).

2.7. Probleme de securitate ale bootloadere-lor folosite in sisteme integrate

În 2016, Mirai Botnet [18] a modificat software-ul dispozitivelor IOT slab protejate deși erau conectate la internet. Aceasta a inclus dispozitive precum termostate inteligente, sisteme inteligente de iluminat și alte aparate, cum ar fi mașini de spălat conectate la WiFi sau frigidere. Firmware-ul modificat a transformat aceste dispozitive în entități înrobite numite roboți [19], care emiteau cereri TCP coordonate către un server DynDNS lucru ce a rezultat în aducerea offline a unor servicii populare precum Twitter sau Netflix. Atacurile de acest tip pot fi evitate în viitor, atât în cadrul dispozitivelor IoT cat si în contextul contoarelor inteligente, prin implementarea unor măsuri de securitate consacrate la nivelul încărcătorului de program [20]. În următoarele subcapitole vom sublinia importanța verificării integrității programelor stocate în sistemele integrate precum și importanța verificării autenticității acestora.

2.7.1. Verificarea integrității firmware-ului stocat și transportat

Modificările involuntare ale conținutului spațiului de stocare folosit de către firmware-ul sistemului integrat se pot produce din cauza unor defecțiuni neașteptate sau ca urmare a executării unui cod de program neautorizat. Acest lucru va putea lăsa sistemul într-o stare inconsistentă, ceea ce înseamnă că funcționalitățile cheie ar putea fi dezactivate sau, mai îngrijorător, funcționalitatea s-ar putea transforma într-un comportament nedefinit.

Modificări involuntare în timpul transmisiilor de date se pot întâmpla, de regulă, din cauza condițiilor de transport prin medii zgomotoase sau nesigure. Cel mai simplu algoritm pentru a preveni modificările accidentale este implementarea unui cod de corectare a erorilor sau abreviat, ECC de la Error Correction Code[21].

Datele redundante împreună cu informațiile permit receptorului să corecteze problemele survenite în timpul transportului fără a fi nevoie de retransmisii. Unul dintre cele mai simple coduri de corecție a erorilor ce pot fi implementate într-un sistem integrat sunt protocoalele bazate pe conceptul de cod Hamming [22].

Deoarece modificările voluntare ale software-ului au un impact mai mare asupra securității generale a dispozitivului, bootloader-ul trebuie să implementeze mai mult decât simpla verificare a erorilor. Modificările voluntare sunt un tip de atac care au la bază o entitate rău intenționată ce încearcă să adauge cod la o aplicație existentă. Apoi, aceasta poate să facă parte dintr-un atac direct sau deschide vulnerabilități ce pot fi folosite ulterior pentru o operațiune coordonată în care mai multe dispozitive instalate deja în teren pot fi îndreptate concomitent către o singură destinație producând un atac de tip Denial of Service (DOS) [23] [24].

Protecția împotriva modificărilor intenționate a firmware-ului care rulează pe un dispozitiv nu poate fi oprită numai prin verificarea sumelor de control sau a codurilor de eroare și de cele mai multe ori trebuie implementată o soluție mai avansată. Una dintre cele mai comune modalități de a proteja aplicația împotriva modificărilor nedorite este oferită de funcțiile de securitate de tip hash. Aceasta clasă de funcții matematice mai poartă în literatura de specialitate si denumirea de funcții de dispersie sau funcții de rezumat [25][26].

2.7.2. Asigurarea integrității datelor cu ajutorul funcțiilor de dispersie

Verificările de integritate pot fi făcute într-un sistem integrat utilizând o funcție hash criptografică (CHF) care produce într-un mod determinist o corelație între datele unui mesaj de intrare și o matrice de biți de ieșire de dimensiune fixă (de ex. 256 biți / 512 biți). Cele mai populare funcții hash utilizate pentru verificarea integrității în industrie în acest moment sunt funcțiile MD-5, SHA-1 și SHA-2. [27]

Funcțiile criptografice de tip hash utilizate pentru verificarea integrității trebuie să aibă două proprietăți si anume să fie unidirecționale și fără coliziuni. Prin unidirecțional, înțelegem că funcția hash poate produce o valoare matematică hash pentru un mesaj introdus într-un mod ușor si rapid, dar încercarea de a scoate mesajul original dintr-o valoare hash nu va fi o operațiune fezabilă. De asemenea, prin coliziune, înțelegem că este imposibil să găsim două mesaje care să producă aceeași valoare criptografică hash.

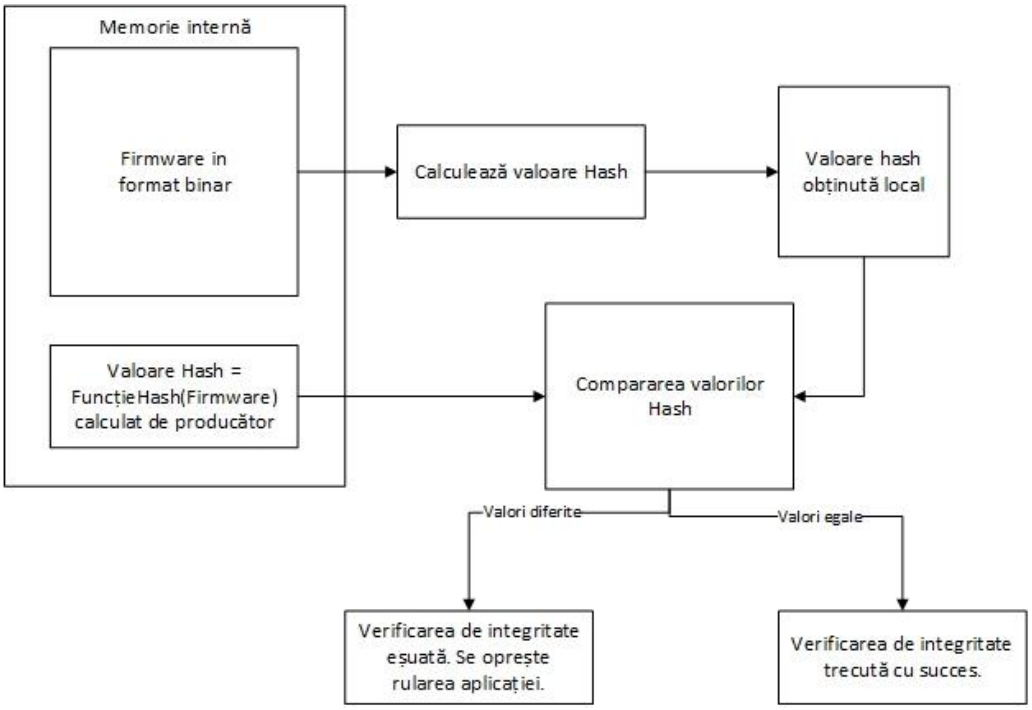

Fig. 2.9 - Procesul de verificare a integrității programului stocat într-un sistem integrat

Conform figurii 2.9, pentru a verifica integritatea firmware-ului, o valoare hash este stocată într-o locație nevolatilă care nu este accesibilă în timpul rulării. Apoi, la fiecare pornire, hash-ul întregului firmware este recalculat din nou și, dacă nu se potrivește cu amprenta salvată în memorie, înseamnă că firmware-ul a fost modificat și executarea va fi oprită.

2.7.3. Protejarea proprietății intelectuale prin procedee criptografice

Software-ul salvat în sistemele încorporate necesită o protecție adecvată împotriva accesului la citire de către entități neautorizate. Securizarea informațiilor stocate în memoriile flash interne sau informațiile care tranzitează canalele de comunicație de la server la dispozitivele client este o sarcină preocupantă pentru producători atât din punct de vedere economic cât si din punct de vedere al securității informatice a contoarelor inteligente.

Din punct de vedere economic producătorii vor să evite clonarea dispozitivelor de către o terță parte care ar putea produce echipamente identice la un preț mult mai mic folosind etapele de cercetare și dezvoltare copiate din echipamentele vândute. Pe de cealaltă parte, dacă atacatorii au acces la programul intern stocat în memoriile contoarelor, aceștia ar putea găsi vulnerabilități deja cunoscute ale bibliotecilor integrate în program sau ar putea descoperi noi puncte de

slăbiciune printr-un proces de tip pen-test (i.e. penetration testing). Un program lizibil într-un mediu ce nu adoptă filozofia open-source se expune la toate dezavantajele pe care le expune cunoașterea codului de către atacator fără a beneficia de eventualele actualizări de securitate pe care comunitățile open-software le-ar putea oferi. Toate acestea afectează atât activitatea producătorului, cât și securitatea utilizatorului final, iar pentru a proteja codul aplicației de entități neaprobate, acesta trebuie să fie criptat atât în timpul stocării în memoriile interne ale sistemului integrat, cât și în timpul transporturilor la care acesta este supus in procesul de actualizare.

În funcție de tipul de chei utilizate în procesul de criptare și decriptare, algoritmii criptografici pot fi simetrici sau asimetrici. În criptarea simetrică, aceeași cheie care a convertit binarul într-un format ilizibil este utilizată pentru decriptare. În binarele criptate asimetrice, o cheie publică este trimisă de server către hardware-ul clientului, care apoi folosește o cheie privată pentru a decripta aplicația primită.

2.8. Concluzii parțiale

Noțiunile teoretice enumerate în acest capitol subliniază faptul că un mecanism de actualizare software adecvat pentru sistemele cu disponibilitate redusă trebuie să asigure următoarele cerințe:

1. Trebuie să fie tolerant la erori de sistem și să poată relua procesul de actualizare de unde a fost oprit anterior. Integritatea sistemului nu trebuie să fie afectată de către întreruperile bruște ale surselor de alimentare.
2. Dispozitivul va putea reveni la o versiune anterioară corectă când acest lucru se impune de către starea defectuoasă a echipamentului actualizat. Modurile de recuperare sunt acceptabile în anumite situații, dar nu pe dispozitive care necesită întreținere redusă sau dispozitive cu acces fizic dificil.
3. Echipamentul va fi protejat împotriva executării programelor malițioase care nu au fost semnate de o sursă de încredere sau de către producător.
4. Sistemul integrat va fi protejat împotriva pirateriei software și a atacurilor de acest tip. Se impun implementarea mecanismelor de protecție criptografice și dezactivarea tuturor interfețelor de citire fizică a memoriilor hardware.
5. Cerințele de resurse trebuie menținute la minimum pe dispozitivele integrate, iar unde este disponibil, se vor utiliza resursele unui server extern cât mai mult posibil.
6. Sistemele de actualizare trebuie să se asigure că procesul nu se va bloca într-o stare intermediară. Procesul de actualizare trebuie să folosească o arhitectură cu caracter atomic.

3. STADIUL ACTUAL – METODE ȘI SISTEME UTILIZATE ÎN REȚELELE DE CONTORIZARE INTELIGENTĂ

3.1. Introducere

Pentru a putea asigura îmbunătățiri în ceea ce privește eficiența, fiabilitatea, flexibilitatea și rentabilitatea investițiilor pentru toți producătorii, operatorii și clienții implicați într-o rețea inteligentă de distribuție a energiei, este necesară dezvoltarea unor soluții informatice moderne la nivelul tuturor elementelor ce o alcătuiesc. O astfel de infrastructură de comunicații trebuie sa fie robustă, fezabilă și suficient de rapidă pentru a putea asigura schimbul de date în timp util de la furnizor la clientul final și invers. Acest capitol trece în revistă stadiul actual al cercetărilor în cadrul arhitecturilor de rețele de distribuție inteligentă subliniind cercetările privind procesul de actualizare a programelor integrate și a capabilităților de comunicații necesare pentru asigurarea performanței, fiabilității și economiei rețelei de contorizare inteligentă.

Rețeaua de distribuție inteligentă este gândită pentru a rezolva problemele rețelei de energie printre care amintim: fiabilitatea scăzută, întreruperile dese, emisiile mari de gaze cu efect de seră, siguranța și securitatea energetică [28]. Una dintre definițiile pentru rețeaua inteligentă cunoscută și sub denumirea de „smart grid" este aceea că rețeaua inteligentă este o rețea de comunicații suprapusă rețelei energetice prin ajutorul căreia se colectează și analizează datele de la diferite componente ale unei rețele pentru a prezice oferta și cererea de energie. În final, aceste informații pot fi utilizate pentru gestionarea și controlul distribuției de energie. [29]

Problemele și soluțiile studiate în literatura recentă acoperă atât avantajele și dezavantajele contoarelor inteligente cât și problemele nerezolvate. Printr-un proces stabil de actualizare a programelor integrate în contoarele inteligente, utilizatorii și furnizorii vor putea primi acces la o multitudine de funcționalități și îmbunătățiri pe măsură ce acestea vor fi implementate de către industrie. [30]

După expunerea stadiului actual al tehnologiilor și a funcționalităților așteptate în rețeaua contorizare inteligentă, vor fi expuse principalele tipuri de canale de comunicație prin care furnizorul poate transmite noi programe către contoarele inteligente. Se vor analiza diferite topologii si vor fi prezentate avantajele și dezavantajele tehnologiilor folosite în acest moment în structurile naționale precum și direcțiile de cercetare disponibile.

Figura 3.1 de mai jos prezintă o vedere de ansamblu a subiectelor de cercetare în cadrul rețelelor de contorizare inteligentă precum și a legăturilor dintre acestea. Se observă că în sistemul energetic se dezvoltă noi funcționalități și îmbunătățiri tehnologice care pot fi implementate sub forma de software de către dezvoltatorii contoarelor inteligente. Prin intermediul rețelei de date funcționalitățile și modificările ajung sub forma unor actualizări de software sau de configurație la contoarele inteligente, iar acestea transmit înapoi date și parametri de consum ce vor fi folosiți în viitoare cercetări reluând întregul proces.

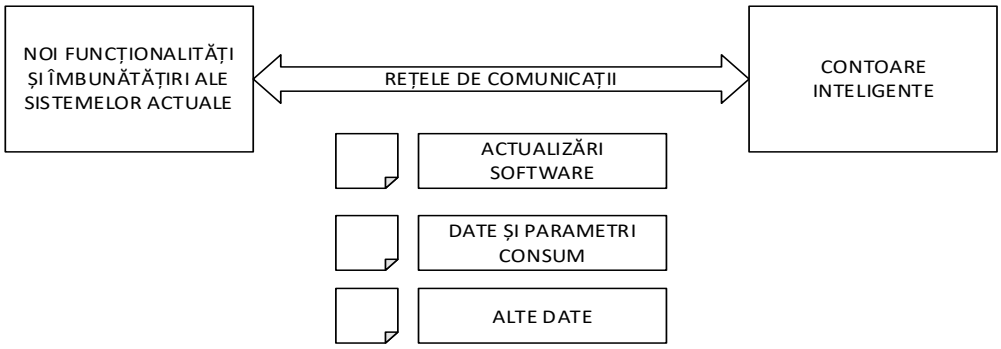

Fig. 3.1. – Vedere de ansamblu a subiectelor de cercetare în cadrul rețelelor de contorizare inteligentă precum și a legăturilor dintre acestea

În final, se vor aborda metodele curente de actualizare implementate la nivelul contoarelor instalate în sistemele naționale și se vor analiza cerințele acestor metode atât din considerente tehnologice ce țin de securitate, ușurința de implementare și constrângeri hardware, cât și din alte puncte de vedere ce pot sublinia fezabilitatea sau neajunsurile cu care industria se confruntă în mod curent.

3.2. Funcționalități și oportunități în viitorul contoarelor inteligente

În ultimii ani evoluțiile tehnologice și contextul economic și social au dus la apariția unor multitudini de noi tehnologii încorporate în echipamentele de contorizare inteligentă. În figura 3.2 am prezentat un scurt istoric al contoarelor inteligente și progresul acestora până în prezent.

Institutul Național de Standarde și Tehnologie (NIST) al SUA, a propus in 2014 [31] o listă de funcționalități cheie ce trebuie implementate într-un timp cât mai scurt de către industria energetică. Ulterior acestea au fost preluate și la nivel european și național [32].

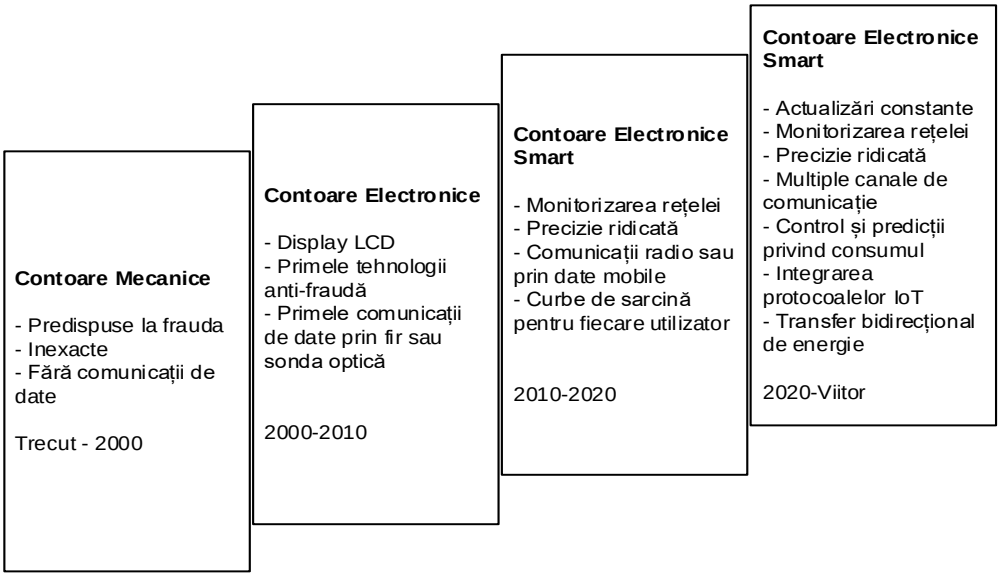

Fig. 3.2. - Evoluția în timp a funcționalităților oferite de rețeaua de contoare inteligente

3.2.1. Răspuns adecvat la cererea energetică și îmbunătățirea eficienței energetică a consumatorilor

Răspunsul adecvat la cererea energetică dintr-un anumit nod de rețea este necesar pentru optimizarea echilibrului dintre cererea și oferta de energie electrică. Acest răspuns presupune ca rețeaua de distribuție și furnizorii să ofere mecanisme și stimulente pentru ca clienții din sectorul comercial, industrial și rezidențial să își modifice consumul de energie în perioadele de vârf de cerere sau ori de câte ori fiabilitatea energiei este în pericol datorită consumului distribuit neuniform în timp și spațiu. De asemenea, se impun metode prin care consumatorul să aibă acces la informații detaliate privind consumul de energie și costul acesteia. Aceste acțiuni urmărind schimbarea modului in care utilizatorul folosește energia furnizată și eventual identificarea echipamentelor ineficiente conectate la rețea.

3.2.2. Monitorizarea rețelei la scară largă

Prin monitorizarea în timp real a performanțelor sistemului de alimentare pe zone geografice extinse, se pot conștientiza situații critice și în cele din urmă se pot optimiza performanțele rețelelor precum se poate și anticipa, preveni sau răspunde unor probleme înainte de apariția întreruperilor de furnizare a energiei. Problemele de monitorizare includ atât metodele de urmărire a caracteristicilor rețelei cât și metodele de localizare a defectelor, ambele conlucrând la construcția unor rețele cât mai robuste și la o mentenanță cât mai eficientă.

3.2.3. Resurse energetice distribuite (RED)

Problema cuprinde sistemele de generare și/sau de stocare a energiei electrice care sunt interconectate cu sistemele de distribuție. Această funcționalitate acoperă inclusiv dispozitivele care se află în incinta clientului. Sistemele RED utilizează o gamă largă de tehnologii de generare și stocare, cum ar fi energia din surse regenerabile, generatoarele de cogenerare de căldură și energie electrică, stocarea fixă în baterii și vehiculele electrice cu încărcătoare bidirecționale. Sistemele RED pot fi utilizate pentru generare/stocare locală, sau pot fi agregate ca centrale electrice virtuale. Funcționalitățile avansate de RED interactive cu rețeaua, activate de echipamentele inteligente de interconectare a invertoarelor, devin din ce în ce mai răspândite și asigură calitatea energiei electrice și stabilitatea rețelei, respectând în același timp cerințele de siguranță ale sistemului de distribuție. Funcționalitățile avansate ale RED permit, de asemenea, noi arhitecturi de rețea care încorporează "micro-rețele" care pot funcționa într-un mod independent atunci când alimentarea cu energie electrică este întreruptă și care pot interacționa pentru a forma un sistem energetic mai adaptabil și mai fiabil.

3.2.4. Metode și mijloace de stocarea a energiei

Mijloace de stocare a energiei, în mod direct sau indirect. Deși cea mai frecventă tehnologie de stocare a energiei în masă utilizată în prezent este tehnologia de stocare hidroelectrică prin pompare. Noile capacități de stocare - în special pentru stocarea distribuită - ar fi benefice pentru întreaga rețea, de la generare până la utilizarea finală cu condiția ca rețeaua inteligentă de distribuție să poată monitoriza și controla mijlocul de stocare.

3.2.5. Integrarea vehiculelor electrice

Se referă în primul rând la facilitarea integrării pe scară largă a vehiculelor electrice plug-in (PEV). Transportul electric ar putea reduce în mod semnificativ dependența țărilor de petrolul străin, ar putea crește utilizarea surselor regenerabile de energie, ar putea asigura stocarea energiei electrice pentru a ameliora solicitările de vârf de sarcină și ar putea reduce în mod dramatic amprenta de carbon.

3.2.6. Rețele de comunicații

Se referă la o varietate de rețele de comunicații publice și private, cu și fără fir, care vor fi utilizate pentru domeniile și subdomeniile rețelelor de distribuție inteligente. Se va avea în vedere varietatea de medii de rețea, identificarea parametrilor de performanță și a elementelor operaționale ale diferitelor aplicații, actori și domenii. Pe lângă acestea, dezvoltarea, implementarea și întreținerea unor controale de securitate adecvate este considerată esențială pentru rețeaua inteligentă.

3.2.7. Infrastructura de contorizare avansată (AMI)

Oferă o monitorizare aproape în timp real a consumului de energie electrică. Aceste rețele avansate de contorizare ar putea fi utilizate pentru punerea în aplicare a răspunsului dinamic la cererea rezidențială și implicit a tarifării dinamice. AMI este compus din hardware și software de comunicații, precum și din sistemele asociate de software pentru gestionare datelor în serverele furnizorilor. Acestea creează împreuna o rețea bidirecțională între sistemele de contoare inteligente și sistemele informatice ale furnizorilor, permițând colectarea și distribuirea de informații.

3.2.8. Inter-conectivitatea rețelelor energetice

Se concentrează pe maximizarea performanței alimentatoarelor, transformatoarelor și a altor componente ale sistemelor de distribuție în rețea și pe integrarea acestora cu sistemele de transport și cu operațiunile clienților. Pe măsură ce se dezvoltă capacitățile rețelelor inteligente, cum ar fi AMI și răspunsul la cerere și pe măsură ce se implementează un număr mare de resurse energetice distribuite și de PEV-uri, automatizarea sistemelor de distribuție devine din ce în ce mai importantă pentru funcționarea eficientă și fiabilă a întregului sistem energetic. Printre beneficiile anticipate ale gestionării rețelei de distribuție se numără creșterea fiabilității, reducerea vârfurilor de sarcină, creșterea eficienței sistemului de distribuție și îmbunătățirea capacităților de gestionare a surselor distribuite de energie regenerabilă.

3.2.9. Securitatea cibernetică

Cuprinde măsuri de asigurare a confidențialității, integrității și securității precum și a disponibilității sistemelor electronice de comunicare a informațiilor și a sistemelor de control necesare pentru gestionarea, exploatarea și protecția energiei din rețeaua inteligentă și a infrastructurilor de telecomunicații.

Stabilirea acestor priorități în industria rețelelor energetice smart a dus la un influx sporit de lucrări de cercetare, iar câteva dintre cele mai importante lucrări din ultimii ani sunt menționate în tabelul 3.1, de mai jos.

Tabelul 3.1. - Lista de lucrări de cercetare din domeniul rețelelor energetice inteligente.

Funcționalități	**Referințe bibliografice**	**Anul Publicării**	**Subiectul abordat**
Monitorizarea rețelelor de distribuție	McBee et al. [33]	2012	Monitorizarea căderilor de tensiune, metode de prevenție a golurilor sau a problemelor în rețea.
	Bhor et al. [34]	2016	Metode de simulare și monitorizare a calității energiei într-o rețea de mari dimensiuni.
	Zhang et al. [35]	2012	Sunt rezumate mecanismele și algoritmii aplicați în sistemul de monitorizare inteligentă.
	Khan et al. [36]	2020	Integrarea echipamentelor și a senzorilor IoT în pachetele de date folosite în monitorizarea rețelei.
Răspuns dinamic la cererea energetică	R Lu et al. [37]	2018	Un algoritm de răspuns la cerere cu prețuri dinamice: abordare de învățare prin întărire.
	Haider et al. [38]	2016	O trecere în revistă a studiilor asupra răspunsului la cererea energetică rezidențială, propune utilizarea unei scheme de tarifare adaptivă.
	Paterakis et al. [39]	2017	Examinarea amănunțită a programelor existente în diferite regiuni geografice.
	Jordehi [40]	2019	Analiza metodelor de optimizare folosite in DR.
	Uddin et al. [41]	2018	Prezintă strategii de reducere a vârfurilor de sarcină.

	R Lu et al. [42]	2019	Răspuns la cerere bazat pe o rețea inteligentă cu învățare prin întărire și rețea neuronală.
	Faruqui et al.[43]	2010	Furnizarea de preturi dinamice și implicațiile economice la nivel de uniune europeană.
Sisteme de generare distribuită	Pipattanasomporn et al. [44]	2009	Proiectarea și implementarea unui sistem multi-agent pentru rețele inteligente distribuite.
	Järventausta et al. [45]	2010	Exemple de funcții și caracteristici ale unor rețele inteligente cu generare distribuită.
	Arritt et al. [46]	2011	Instrumente de analiză necesare în integrarea sistemelor de generare rezidențiale.
Integrarea vehiculelor electrice	Kong et al. [47]	2016	Studiu privind metode de încărcare pentru vehiculele electrice plug-in în rețele inteligente.
	Couillet et al. [48]	2012	Vârfuri de cerere cauzate de încărcarea mașinilor electrice și metode de combatere a acestora.
	Xue et al. [49]	2014	Integrarea vehiculelor electrice în rețelele inteligente.
	Xu et al. [50]	2021	Interacțiunea dintre vehiculele electrice conectate prin rețeaua inteligentă.
	Rana et al. [51]	2018	Sisteme energetice interconectate care încorporează turbine și vehiculele electrice.
Rețele de comunicații	Saputro et al. [52]	2012	Protocoale de rutare în rețelele smart grid.

	Hossain et al. [53]	2012	Un studiu privind tehnologiile actuale de comunicații folosite în rețelele energetice.
	Yan et al. [54]	2012	Studiu privind securitatea cibernetică în rețelele smart grid.
	Chinet al. [55]	2017	Rețele ce integrează tehnologii Internet of Things si provocările acestora.
	Lopez et al. [56]	2019	Comunicații prin liniile de înaltă tensiune.
	Dragičević et al. [57]	2019	Comunicații wireless bazate pe tehnologia 5G aplicate rețelelor smart grid.
	Tightiz et al. [58]	2020	Stadiul actual și viitorul IoT în rețelele energetice.
Infrastructura de contorizare avansată	Saleh et al. [59]	2019	Integrarea principiilor BigData în sistemele de contorizare inteligentă.
	Gosal et al. [60]	2019	Stadiul actual al sistemelor de contorizare inteligentă.
	Siqueira et al. [61]	2018	Sistem de comunicații pentru contoarele inteligente.
Interconectivitatea rețelelor energetice	DK Kim et al. [62]	2017	Studiu privind interoperabilitatea rețelelor inteligente
Securitatea cibernetică	Kim et al. [63]	2018	Îmbunătățirea securității rețelelor smart grid prin tehnologii blockchain
	Gunduz et al. [64]	2020	Stadiul actual al securității în rețelele inteligente, amenințări și soluții
	Kimani et al. [65]	2019	Provocările securității cibernetice în rețele energetice bazate pe echipamente IoT

3.3. Înglobarea tehnologiei IoT in rețelele de tip smart grid

Conceptul de echipamente IoT (Internet of Things), presupune integrarea coordonată și colaborarea obiectelor din mediul înconjurător prin intermediul internetului pentru a realiza diverse sarcini într-un mod mai eficient și mai inteligent [66, 67]. Cercetările în acest domeniu au cunoscut o expansiune fulminantă, iar abordările sunt întinse asupra multor alte domenii de cercetare precum amintește și L. Atzori în [68]. Amintim doar câteva domenii abordate, precum cel medical [69-71], domeniul transporturilor [72, 73] și cel educațional [74-76]. Domeniul energetic a început să înglobeze aceste tehnologii în cercetările sale, iar ideea unei rețele energetice de tip smart grid interconectată cu echipamente IoT și cercetările din acest domeniu au fost cuprinse în [77], [78], [79] și [80].

În [81], Miao amintește cele trei motive principale prin care tehnologia IoT poate îmbunătăți rețelele smart:

- Înțelegerea mediului înconjurător: Utilizarea senzorilor pentru a colecta informații de la orice obiect, în orice moment și oriunde.
- Procesare inteligentă: Utilizarea unor tehnici precum cloud computing pentru a analiza cantități uriașe de date.
- Transmisie fiabilă: Transmitere precisă și în timp real a datelor prin intermediul comunicațiilor rețele de comunicații și internet.

Iar, în [82] Singh împarte abordările IoT în trei categorii precum urmează:

- Orientat spre internet: În viziunea orientată spre internet, este necesară crearea de obiecte inteligente și obiectele trebuie să utilizeze specificațiile protocoalelor IP.
- Orientat spre percepție: În viziunea orientată spre percepție, numărul de senzori disponibili va fi foarte mare, iar cantitățile de date colectate de aceștia vor fi uriașe. Astfel, datele brute trebuie să fie gestionate și procesate pentru o mai bună reprezentare și o înțelegere mai bună.
- Orientată spre lucruri: În viziunea orientată pe lucruri, putem urmări orice obiect folosind senzori și tehnologii omniprezente. Orice obiect poate fi identificat în mod unic cu ajutorul unui cod specific fiecărui produs.

Marile cantități de date produse de contoarele inteligente pot beneficia de infrastructurile Internet of Things, iar capabilitățile de procesare locale prin intermediul gatewayurilor IoT trebuie luate în considerare în viitorul apropiat. Dacă luăm în considerare estimările specialiștilor [83], în anul 2030 la nivel global se va depăși numărul de o mie de miliarde de dispozitive IoT conectate la internet. Acest lucru ne obligă la a lua cel puțin în considerare această resursă omniprezentă în dezvoltarea viitoarelor tehnologii smart grid. Dintre avantajele imediate de care echipamentele de contorizare inteligentă pot beneficia amintim capabilitățile de a realiza comunicații fiabile, procesarea de date, capabilitatea de control a consumatorilor și o senzoristică avansată.

În 2018, Bedi et al. [84] propune înglobarea tehnologiilor IoT în sistemele de transport și producție a energiei electrice, aceștia emulând modelul unui sistem nervos biologic peste o rețea de senzori IoT cu capabilități de calcul distribuite la nivelul fiecărui nod. Aceștia subliniază impactul economic și social pe care un sistem energetic, capabil de conexiuni cu rețeaua de internet, îl poate avea. Alte lucrări propun metode de contorizare inteligentă bazate pe conexiuni mobile sau satelit [85], iar în [86] și [77] autorii prezintă implementări IPv6 aplicate rețelelor smart grid IoT.

Sisteme smart grid asistate de senzori și actuatori de tip Internet of Things deși par o combinație naturală prin perspectiva simbiozei de informații și infrastructurii de comunicații de care fiecare parte poate beneficia, este umbrită de o lipsă acută de standardizare [78] în această direcție. De asemenea, deși principiile prin care rețelele energetice inteligente se pot interconecta cu echipamente IoT sunt trecute în revistă de mai mulți autori în literatura recentă, volumul de lucrări cu aplicații concrete implementate în rețelele smart grid sunt încă într-un număr foarte redus, iar potențialul de cercetare în această direcție este unul ridicat.

3.4. Rețele de comunicație folosite în rețelele smart grid

Deși există o gamă largă de tehnologii disponibile pentru rețelele de comunicații a sistemelor de contorizare inteligentă, nu există în prezent o tehnologie de comunicații care să răspundă tuturor nevoilor și, uneori, în cadrul aceleiași implementări sunt utilizate mai multe tehnologii [87][88]. În analiza stadiului actual al tehnologiilor folosite am împărțit observațiile în funcție de mediul de transmisie folosit astfel avem comunicații fără fir (radio, satelit, date mobile) și comunicații prin fir care folosesc liniile de alimentare cu energie sau un circuit auxiliar pentru transmisia datelor.

Tehnologia PLC în bandă îngustă (NB-PLC), este una dintre cele mai populare alegeri în rețelele smart din Europa și se aplică de obicei pentru legătura de telecomunicații dintre contorul inteligent și concentratorul de date [89].

Tehnologiile G3 [90] și Prime [91] sunt cele mai cunoscute protocoale NB-PLC. Acestea utilizează metoda de transmisie (OFDM) și tehnica de modulație DBPSK/DQPSK. Diferența constă în faptul că în PRIME conceptul DPSK este utilizat în domeniul frecvență, în timp ce în G3-PLC este utilizat în domeniul timp. Peste acestea se aplică standardul IEC 62056 care specifică formatul datelor transmise de către contoarele inteligente, dar limitările impuse prin standard și natura fizică a acestor două protocoale au dezavantajul unor viteze de transmisie reduse, dar și avantajul unui cost de instalare și de mentenanță redus [92].

Alte soluții de comunicații prin medii solide precum tehnologii DSL vin cu costuri de mentenanță ridicate și viteze mici de transmisie a datelor, iar tehnologiile bazate pe fibra optică deși au avantajul unor viteze ridicate, nu sunt fezabile din punct de vedere economic și nici nu sunt potrivite pentru mediile în care sunt instalate contoarele inteligente [93][94].

Protocolul radio ZigBee [95], reprezintă una dintre cele mai răspândite soluții fără fir integrate în rețelele energetice inteligente. La baza acestuia stă standardul IEEE 802.15.4 și, la fel ca în cazul tehnologiilor PLC, este un protocol

folosit la scara largă pentru realizarea conexiunilor între contoarele inteligente și concentratoarele de date. Având o rază de acțiune destul de redusă, de aproximativ 100m, concentratoarele trebuie instalate în perimetrul locuințelor. Folosind frecvențe de 2.4GHz este un protocol afectat de alte echipamente rezidențiale ce ocupă același spectru, dar are în același timp avantajul că ar putea duce ușor la o integrare între rețelele smart-grid și cele IoT [96]. În momentul de față protocolul stă la baza întregii infrastructuri de date din contoarele inteligente instalate în programul SMETS [97] pe teritoriul Regatului Unit.

Concentratoarele de date sau unele contoare inteligente au abordat o implementare bazată pe datele mobile prin tehnologii 2G, 3G, LTE, iar mai nou 5G [98][99]. Principalele avantaje ale acestor tehnologii sunt infrastructura deja existentă la care se pot lega ușor, latența redusă pe care o oferă și consumul redus de energie, dar principala problemă o reprezintă costul ridicat al echipamentelor de transmisie-recepție și costurile abonamentelor necesare pentru fiecare echipament din rețea [100].

Stadiul actual al tehnologiilor folosite pentru comunicațiile de date în rețelele energetice inteligente, împreună cu avantajele si dezavantajele descrise de literatură în [78], [101], [102] și [103] au fost rezumate și cuprinse in tabelul 3.2.

Tabelul 3.2. - Rezumatul stadiului actual al tehnologiilor folosite în rețelele smart grid.

Mediu	Protocolul de comunicație	Frecvența	Viteza maximă de transfer	Distanța acoperită	Avantaje	Dezavantaje	Rețele ce înglobează protocolul
Comunicații prin fir	NB-PLC	500 kHz	300 kbps	3 km	Costul foarte redus pentru implementare.	Mediu predispus interferențelor.	Folosit la scară largă pe întreg teritoriul uniunii europene (UE)
	BB-PLC	150 MHz	100 Mbps	0.5 km	Viteze de transfer foarte mari.	Distanță mică de acoperire.	HomeGrid (SUA și Germania), doar la nivel de data concentratoare.
	ADSL	1 MHz	800 kbps	4 km	Viteze de transfer suficient de mari.	Costuri mari de instalare și mentenanță.	Infrax (Belgia)
	PON	500 MHz	2.5 Gbps	40 km	Viteze de transfer foarte mari. Tehnologie robustă.	Infrastructură deosebit de costisitoare.	Boulder Smart City Grid (SUA)
	IEC62056-31	80 MHz	9.6 kbps	0.5 km	Tehnologie robustă și ușor de instalat.	Viteze de transfer foarte scăzute.	Euridis (Franța)
Comunicații fără fir	GSM	1800 MHz	14.4 kbps	35 km	Arie mare de acoperire. Costuri de mentenanță reduse.	Consum ridicat de energie pentru transmisia datelor. Costuri mari pentru abonamentele fiecărui contor inteligent.	Telegestore (Italia)
	3G	2100 MHz	60 kbps	20 km	Arie mare de acoperire. Costuri de mentenanță reduse.		China Southern Power Grid (China)
	LTE	2500 MHz	240 kbps	5 km	Viteze mari de transfer. Costuri de mentenanță reduse.	Costuri mari pentru abonamentele fiecărui contor inteligent. Arii mici de acoperire pentru o singură celulă.	Smart Grid Smart City (Australia) Essential Energy (Australia)
	5G	30-300 GHz	50 Gbps	0.5 km	Viteze foarte mari de transfer. Costuri de mentenanță reduse.		State Grid Corporation of China (China)

	ZigBee	2.4 GHz	250 kbps	0.1 km	Costuri mici de implementare. Consum redus de energie.	Mediu predispus interferențelor. Arie mică de acoperire.	Energy Demand Research Project (Marea Britanie) National Smart Metering Programme, (Irlanda)
	Wi-Fi	2.4 GHz	54 Mbps	0.1 km	Tehnologie robustă. Viteze de transfer foarte mari.	Predispus interferențelor. Consum ridicat de energie.	Central Maine Power Company (SUA)
	Bluetooth	2.4 GHz	1 Mbps	0.05 km	Consum redus de energie.	Predispus interferențelor. Arie mică de acoperire.	Smart Energy Study Group (SUA)

Infrastructura deja prezentă și ușurința cu care se pot adaugă noi contoare inteligente în rețea au făcut ca la nivel european tehnologiile NB-PLC să fie preponderent alese. În tabelul 3.3, am rezumat tehnologiile implementate [102] la nivel național pe teritoriul uniunii europene.

Tabelul 3.3. - Tehnologiile alese la nivel național în rețelele smart grid europene.

Țara	**Protocoalele implementate**	**Standardele de contorizare inteligentă implementate**
Franța	NB-PLC, IEC 62056-31	G1, G3-PLC, IEC 62056-21
Italia	NB-PLC, GSM, 3G	IEC 62056-21
Germania	BB-PLC, NB-PLC	G3-PLC, G.Hn
Suedia	NB-PLC, GSM, 3G	IEC 62056-21, IEC 14908
Spania	NB-PLC	PRIME, T5
România	NB-PLC,	IEC 62056-21, PRIME, T5
Grecia	NB-PLC, GSM, 3G	IEC 62056-21
UK (non-UE)	ZigBee, 3G, GSM	SMETS1, SMETS2

Se poate observa că la nivel global, tehnologiile NB-PLC și ZigBee sunt cele mai populare datorită costurilor mici necesare instalării în teren. Aceste protocoale pot face comunicația posibilă doar pe raze restrânse, iar datele sunt adunate în echipamente de tip „data concentrator” care comunică la rândul sau cu serverele furnizorilor prin intermediul datelor mobile.

3.5. Metode de localizare a echipamentelor în rețelele smart grid

Pornind de la problemele de monitorizare și mentenanță a rețelelor energetice descrise anterior, în cazul unui defect, pentru a putea acționa cât mai repede este necesară identificarea defectului și localizarea acestuia.

Dacă în alte medii industriale folosirea tehnologiilor GPS este metoda cel mai des folosită [94], în cadrul rețelelor de joasă tensiune acest lucru nu este posibil datorită instalării echipamentelor de contorizare inteligentă în medii închise fără vizibilitate către un sistem de sateliți. Una din aceste abordări a fost prezentată în [95], această lucrare propune localizarea în mediile rezidențiale prin folosirea tehnologiei ultra-wide band. Deoarece această tehnologie are o durată scurtă a impulsurilor de frecvență radio și o lățime de bandă largă, se pot minimiza efectele interferențelor multipath și astfel se poate obține o localizare de înaltă rezoluție. Având în vedere și caracterul economic al rețelelor energetice o astfel de abordare nu este încă pregătită să înlocuiască metodele clasice de localizare în interior puse în revistă de A Yassin în [106].

Folosindu-ne de parametri fizici măsurați în mod continuu de fiecare contor inteligent, precum puterea consumată și tensiunea și frecvența rețelei, Jiang propune în [107] o abordare bazată pe analiza wavelet (WTC) a acestor parametri. Apoi, caracteristicile rețelei de la nodurile cu poziție cunoscută, formează o hartă zonală a echipamentelor implicate într-un anumit defect, care pe urmă poate fi utilizată pentru a localiza cu precizie defectele din sistemul energetic. De asemenea, în [108], o abordare similară se folosește de modemurile de comunicație PLC conectate în rețeaua energetică. Folosind semnale de diferite frecvențe pentru a comunica între două noduri NB-PLC, Passerini și Tonello [108] au arătat că defectele pot fi identificate ușor cu ajutorul celor doi algoritmi propuși de aceștia, cu condiția ca topologia rețelei să fie cunoscută în prealabil.

Dacă tehnologiile bazate pe echipamente PLC se bucură de o multitudine de algoritmi de localizare ce pot fi ușor implementați în cadrul rețelelor smart, acest lucru nu este adevărat și în cadrul echipamentelor de contorizare bazate pe tehnologii radio (e.g. ZigBee) care împart același spectru radio cu echipamentele IoT sau Wi-Fi și implicit sunt predispuse interferențelor. În [109], autorii arată variația măsurătorilor RSSI în funcție de tipul de transmițător sau de tipul de antenă ales și impactul deloc neglijabil pe care temperatura mediului ambiant o poate avea asupra acestor măsurători. Lucrarea concluzionează că parametrul RSSI folosit în algoritmii de localizare a echipamentelor fără fir poate fi folosit doar prin intermediul unui set de corecții matematice și doar după ce cunoaștem impactul avut de mediul intrinsec și extrinsec asupra măsurătorilor făcute.

3.6. Metode de actualizare a contoarelor inteligente

Pentru ca funcționalitățile descrise anterior să poată ajunge la contoarele inteligente odată ce vor fi implementate sau de fiecare dată când se dorește schimbarea modului de funcționare al acestora, managementul rețelei inteligente poate lansa noul software sub forma unor actualizări de program integrat. Actualizarea programelor integrate ce rulează în contoarele inteligente presupune

înlocuirea aplicației curente cu una nouă ce are capabilități software îmbunătățite și poate cuprinde noi funcționalități, noi parametrizări sau uneori pot corecta defecte ce periclitau siguranța cibernetică a întregii rețele smart.

Deoarece actualizările software au dimensiuni considerabile și călătoresc de la serverul furnizorului de energie prin întreaga rețea, dintr-un nod în altul, acestea sunt predispuse interferențelor și sunt afectate de numeroase imperfecțiuni ale rețelei de comunicații de date. De asemenea, actualizările software transmise prin smart grid pot fi afectate și de atacuri cibernetice ce pot expune unor potențiale pericole atât proprietatea intelectuală a programelor, cât și intimitatea clienților finali sau chiar, în cazuri extreme, integritatea întregii rețele energetice [110][111].

3.6.1. Provocări și probleme întâlnite în procesul de actualizare

Lipsa unei standardizări a procesului de actualizare la nivelul dezvoltatorilor de contoare inteligente duce la numeroase probleme pe care fiecare producător, din motive economice, încearcă să o rezolve într-un mod proprietar. La această lipsă se mai adaugă și capabilitățile hardware reduse ale echipamentelor de contorizare precum și disponibilitatea precară a rețelelor de date în anumite noduri de rețea [112].

Metodele descrise de Kolehmainen [113] includ atât metode bazate pe acceleratoare criptografice hardware cât și soluții software open-source precum distribuțiile NanoBSD bazate pe modelul cu o partiție inactivă așa cum a fost descris și în capitolul teoretic sau modele bazate pe fragmentarea flash propuse de Schimdt et al. sub denumire SecFota [114]. Pe partea de disponibilitate a rețelei și în funcție de tehnologia de comunicație aleasă pentru contoarele inteligente problemele enumerate încep de la Feng [115] care subliniază că metodele standard de actualizare prin tehnologii radio vor crea congestii și vor duce la procese lente, iar Galli menționează probleme similare și în rețelele bazate pe tehnologii PLC în [116].

Din punctul de vedere al securității cibernetice problemele sunt numeroase, dar în general actualizărilor de software li se aplică 4 categorii de amenințări precum sunt descrise și în tabelul 3.4 așa cum sunt subliniate și în [117] și [126].

Tabelul 3.4. - Categorii de amenințări ale securității cibernetice în contextul actualizărilor software.

Categorie	**Descriere**	**Lucrări științifice**
Alterarea programului integrat	Modificarea parțială a funcționalității programelor integrate. Pot fi afectate inclusiv părțile legate de tarifare și facturare.	Lee[118], Keleman[119]
Pierderea proprietății intelectuale	Poate duce la pierderea programului scris în memoriile interne și permite copierea neautorizată a acestuia. De asemenea accesul la codul	Lee[120], Kumar[121]

	sursă poate expune vulnerabilități sau date private.	
Rularea programelor neautorizate	Adăugarea unor bucăți noi de cod ce va fi executat într-un mod transparent fără a afecta funcționarea normală. Acest lucru poate duce la construcția unor structuri masive de tip bot-net.	Guillen[122], Jain[123]
Rularea pe dispozitive neautorizate	Instalarea unui firmware primit de la producător în echipamente neconforme.	Hagan[124], Shepherd [125]

Pentru a putea proteja contoarele inteligente de aceste amenințări, au fost descrise, în capitolul teoretic, măsurile criptografice propuse în literatură pentru protejarea integrității firmwareului. Metodele includ metode bazate pe semnăturile digitale, coduri MAC de autentificare sau simple sume de control și valori hash [127-131]. Dar, nevoia de standardizare în acest domeniu a dus la formarea unor protocoale specifice precum *ASSURED* [132] sau *SFOTA* [133]. Autorii descriu o structură fixă cu pachete ce pot fi criptate în mod individual, iar oprirea comunicației și reluarea acesteia mai târziu se poate face fără a afecta securitatea canalului de comunicație sau a echipamentelor integrate. Se asigură confidențialitatea, autenticitatea și integritatea datelor în ambele protocoale, dar trebuie sa amintim că *ASSURED* este pretabil în special pentru echipamente cu două niveluri de protecție. Această abordare este potrivită pentru contoarele inteligente care folosesc o parte a memoriei pentru programele supuse certificărilor metrologice și o altă parte izolată ce nu va fi supusă certificărilor. Această bucată de program, bine izolată, va fi mai puțin orientată spre securitate și mai mult orientată spre funcționalități ușor accesibile utilizatorilor finali. La nivel de confidențialitate se folosesc algoritmi criptografici bazați pe curbe eliptice, iar simultan se asigură prin același mecanism și verificările de integritate necesare înainte de încărcarea programelor la pornire. La nivel de rețea propunerile din literatură se îndreaptă de la abordările clasice spre abordări bazate pe tehnologii blockchain [134][135], acest lucru este posibil în cadrul rețelelor IoT, dar momentan nu este fezabil în contorizarea inteligentă datorită cerințelor ridicate date de complexitatea ciclomatică a proceselor implicate [136].

În [137], Arakadakis et al. trece în revistă pe lângă problemele de securitate descrise anterior și problemele de ordin fizic cu care echipamentele integrate se întâlnesc în mediile în care sunt instalate. Dintre acestea autorii menționează limitările hardware precum spațiul redus al memoriilor EEPROM [138] sau al limitărilor memoriilor Flash[139].

Folosirea memoriilor Flash în procesul de actualizare software solicită ciclurile de scriere și citire lucru ce poate duce la degradarea paginilor de memorie în memoriile bazate pe porți logice NOR și mai rar și în memoriile bazate pe porți NAND [140]. Prin rotația zonelor de memorie folosite pentru stocarea segmentelor din binarele destinate actualizării, se pot proteja blocurile de memorie obținând o degradare

uniformă sau putem evita acest impediment folosind scheme propuse pentru actualizări bazate doar pe stocarea temporară a segmentelor în memoria RAM [141]. De asemenea, scrierea în memoriile externe necesită cantități de energie consistente lucru pe care dezvoltatorii contoarelor inteligente trebuie să îl ia în considerare. Autorii recenziei [137] menționează că transportul radio al unui singur bit de informație din descărcarea unei actualizări consumă o cantitate de energie echivalentă cu executarea a 1000 de instrucțiuni de procesor [142]. În [143], autorii arată că traversarea dintre pagini în memoria flash determină un consum suplimentar de energie din cauza circuitelor implicate în acest proces. Acest lucru implică faptul că dezvoltatorii de actualizări trebuie să țină cont de acest lucru, iar segmentele descărcate să fie aliniate corespunzător într-o singură pagină, dacă este posibil, pentru a evita un consum excesiv de energie.

În funcție de topologia rețelei, numărul de vecini disponibili și tipul rețelei de date, metodele de actualizare trebuie să ia in considerare ordinea în care nodurile vor fi actualizate, algoritmii de comprimare a actualizărilor și modul de transport a binarelor. Alegerea nodurilor în funcție de versiunea curentă și de dispersarea nodurilor vecine este discutat în [144]. Rutele alese de la server către sistemele integrate sunt o problemă tratată în literatura IoT, iar Aschenbruck [145] trece în revistă mai multe abordări potrivite și pentru rețelele smart grid.

O altă provocare, găsită preponderent în dezvoltarea actualizărilor contoarelor inteligente, o constituie timpul de inoperabilitate cauzat de trecerea de la versiunea curentă la noua versiune. Furnizorii impun producătorilor de contoare inteligente să dezvolte programe ce nu opresc contorizarea consumului de energie atunci când se face trecerea de la o versiune veche la una actualizată, iar soluțiile propuse sunt atât hardware[146] cât și software[145].

3.6.2. Metode și platforme pentru construcția și distribuția actualizărilor

În tabelul T5 am prezentat un sumar al soluțiilor date de literatura de specialitate pentru problemele menționate anterior. Au fost amintite atât avantajele cât și dezavantajele fiecărei metode, iar subiectele abordate acoperă atât partea de dezvoltare și implementare cât și partea de transport și management necesar procesului de actualizare a contoarelor inteligente. Metode similare au fost trecute în revistă de Arakadakis în [137], de Halder et al. în [148] și de Villegas et al. în [149].

Tabelul 3.5: Metode de dezvoltare și distribuție a actualizărilor inteligente

Subiectul abordat	**Referințe bibliografice**	**Anul Publicării**	**Descrierea metodei**
Metode pentru securizarea	Kim et al. [150]	2013	Echiparea sistemelor integrate cu module de
	Metke et al. [151]	2010	

programelor	Nicanfar et al. [152]	2013	accelerare criptografică hardware. Presupune un cost ridicat, dar conferă un mediu deosebit de sigur pentru stocarea cheilor criptografice și un mediu de rulare izolată a porțiunilor de program considerate critice.
	Butin [153]	2017	Sume de control de tip hash folosite în criptografie în contextul creșterii bruște a puterii de calcul prin calculatoarele cuantice.
	Kumar et. al [121]	2018	Implementarea unui bootloader securizat pentru actualizarea sistemelor la distanță.
	Huynh-Van et al. [154]	2019	Integrarea algoritmilor AES în metodele de optimizare Deluge folosite în actualizarea firmware.
	Sun et al. [155]	2017	
Metode de compresie a actualizărilor	Wang et al. [156]	2019	Mecanisme de compresie a programelor integrate pentru optimizarea procesului de upgrade.
	Onuma et al. [157]	2018	Metode de compresie folosite în cadrul computerelor de bord din domeniul automotive.
	Lehniger et al. [158]	2019	Metode de update incrementale și impactul acestora asupra sistemelor integrate.
	Zhang et al. [159]	2016	Aplicarea unor segmente de cod diferențiale în sisteme ce nu necesită repornirea.
Metode de actualizare centralizată (server-client)	Dalai et al. [160]	2015	Sistem de actualizare prin canalul de voce al rețelei celulare.
	Perito et al. [161]	2010	Actualizare securizată a codului pentru dispozitive încorporate prin intermediul dovezilor de ștergere sigură.
	Karame et al. [162]	2015	

	Aman et al. [163]	2021	Studiu privind atacurile de securitate și metode de actualizare a mașinilor autonome.
	Pham et al. [164]	2021	Metode centralizate de actualizare în rețelele IoT.
	Jurkovic et al. [165]	2014	Actualizare de la distanță pentru sisteme încorporate cu resurse hardware limitate
	Zandberg [127]	2019	Standarde open source pentru actualizările centralizate.
Metode de actualizare descentralizată	Lee B. et al. [166]	2016	Metodă de actualizare a firmwareului dispozitivelor prin metode blockchain.
	Casino et al. [167]	2019	Trecere în revistă a aplicațiilor bazate pe tehnologii descentralizate.
	Lee Y. et al. [168]	2020	Prevenirea accesului neautorizat în timpul actualizărilor folosind tehnologii blockchain.
Platforme de actualizare a sistemelor integrate	Toiviainen [169]	2020	Mender – Serviciu complet de actualizare la distanță a unei flote de echipamente embedded.
	Krishnamurthi et al. [170]	2019	Amazon AWS – Grasshopper - Sistem de management a unei flote de echipamente bazate pe AWS și FreeRTOS
	Botez [171]	2020	Balena – Soluție de distribuție a programelor prin containere.

3.7. Concluzii parțiale și contribuții

În acest capitol au fost prezentate lucrări și metode din literatura de specialitate publicate în perioada 2010-2021, referitoare la viitorul rețelelor de contorizare inteligentă și provocările ce trebuie depășite pentru implementarea pe scară largă a noilor funcționalități propuse de către industrie.

Rețelele de tip Smart Grid pot rezolva problemele legate de fluxul bidirecțional de informații și energie, problemele de fiabilitate și de securitate ale rețelelor energetice tradiționale. Utilizarea și producția energiei într-un mod inteligent atât la nivel național cât și rezidențial pot pune capăt risipei de energie și pot rezolva problemele cauzate de cererea crescândă de energie. Acest lucru este posibil prin

tehnicile de monitorizare, analiza și control prezentate la începutul capitolului. Așadar, se poate desprinde concluzia că pentru gestionarea și economisirea energiei contoarele inteligente joacă un rol esențial, iar până la finalul anului 2022 se preconizează că vor fi instalate 200 de milioane de noi contoare inteligente pe parcursul implementării a mai mult de 50 de proiecte derulate la nivel european.

Pentru transmiterea datelor se remarcă două tehnologii populare în implementarea acestor proiecte și anume: tehnologii radio sub protocolul ZigBee și tehnologii de comunicație prin liniile de alimentare electrică sub protocolul NB-PLC. Ambele tehnologii folosesc concentratoare de date ce deservesc o anumită arie, iar conexiunea de la concentrator către serverele centrale se face prin tehnologii de date mobile. Aceste alegeri au la bază costurile reduse de implementare și flexibilitatea relativ ridicată a protocoalelor alese, dar acestea se confruntă cu provocări de coexistență într-un domeniu frecvență deja aglomerat, provocări legate de securitatea canalului de comunicație și provocări legate de congestii de date și lipsa unei metode de comunicație în timp real.

Un nou domeniu de cercetare apărut recent, ia în considerare atât problemele apărute în rețelele de contorizare inteligentă, cât și problemele întâlnite în echipamentele de tip Internet of Things (IoT) folosite în automatizările proiectelor de tip smart home. Propunerile generale sunt acelea de standardizare și înglobare a celor două tehnologii într-un sistem smart grid asistat de IoT care adresează problemele de interoperabilitate și integrare a noilor dispozitive, folosirea distribuită a puterii de procesare pentru analiza volumului uriaș de date și utilizarea unei topologii de comunicații hibride ce poate adresa problemele de congestie și securitate a datelor informatice. Sistemele de contorizare inteligentă asistate de echipamentele IoT reprezintă o integrare a două lumi emergente și promițătoare.

Aplicațiile de contorizare și control rulate în programele contoarelor inteligente necesită o rețea rapidă, fiabilă și securizată. Literatura studiată menționează că localizarea nodurilor de rețea poate conferi un suport adițional algoritmilor de optimizare, dar poate îmbunătăți atât deciziile luate în direcționarea pachetelor prin rețea, cât poate și reduce timpii de rezolvare a unui defect fizic prin identificarea rapidă a acestuia în spațiul geografic. În mediile fizice ce nu permit instalarea echipamentelor GPS localizarea se face pe baza indicatorilor de semnal radio, iar deși autorii propun mai multe metode de localizare a contoarelor inteligente, acestea se confruntă cu o complexitate de calcul ridicată și de multe or se bazează doar pe indicatorul de semnal RSSI ce poate suferi modificări semnificative în funcție de factorii de mediu.

O parte esențială în proiectele de contorizare inteligentă aflate în derulare o constituie metodele și sistemele de actualizare a firmware-ului la distanță. Deoarece tehnologiile implicate în rețelele energetice inteligente evoluează în mod accelerat este important ca fiecare echipament instalat în teren să aibă ulterior acces la actualizări software ce pot aduce funcționalități adiționale sau pot îmbunătăți securitatea contoarelor și implicit a întregii rețele. Au fost analizate multiple tehnici și structuri standardizate de actualizare la distanță a sistemelor integrate precum au fost și evidențiate principalele provocări și limitări care pornesc de la constrângerile echipamentelor hardware sau ale rețelei de comunicație. În plus, au fost discutate schemele de securizare a întregului proces de update prin criptare, semnare și alte procese de verificare a integrității și autenticității programelor rulate de contoarele inteligente. De asemenea, în cadrul acestui capitol, au fost analizate instrumente de

analiză și metode de optimizare a transmisiei de date ce pot juca un rol important în actualizarea contoarelor inteligente instalate în zone cu acces redus la rețelele de date și s-au sugerat direcțiile de cercetare în acest domeniu.

În concluzie, există încă provocări majore care necesită investigarea în continuare a unor probleme importante de cercetare deschise în domeniul rețelelor de contorizare inteligentă și managementul contoarelor inteligente deja instalate. În capitolele următoare sunt prezentate metodele propuse pentru actualizarea contoarelor inteligente într-un mod securizat chiar și în cazul sistemelor integrate cu capabilități de calcul reduse. Se vor prezenta metode de transmitere a acestor actualizări prin canale de comunicație PLC supuse interferențelor precum va fi tratat și subiectul localizării contoarelor pe baza calității semnalului RSSI. În final, se vor analiza rezultate obținute în urma experimentelor și se va putea ajunge la o concluzie mai clară asupra unui sistem standardizat de contorizare inteligentă.

4. CERCETĂRI PRIVIND IMPACTUL METODELOR DE ACTUALIZARE DE LA DISTANȚĂ A CONTOARELOR INTELIGENTE

4.1. Introducere

Pornind de la contextul actual al rețelelor de contorizare inteligentă, împreună cu concluziile conceptelor teoretice descrise anterior, în prezentul capitol se vor propune și cerceta metode prin care procesul de actualizare poate fi implementat la nivel software fără compromisuri de funcționalitate sau securitate venite din constrângerile tipului de hardware utilizat.

Întrucât costurile directe cu modernizarea rețelei de distribuție și implicit a contoarelor inteligente sunt suportate de către furnizori, soluțiile tehnice vor fi întotdeauna axate spre o variantă cât mai economică și cât mai cuprinzătoare, deoarece clientul final nu își poate procura singur un contor inteligent, iar funcționalitățile adiționale sau implementările bazate pe securitate hardware nu fac parte din obiectivele imediate ale furnizorilor. Așadar propunem o soluție de implementare a cerințelor de autentificare a softwareului ce rulează pe contorul inteligent prin măsurile criptografice descrise anterior în capitolele 3.2.9 și 2.7, totodată conferind și suport pentru actualizări de la distanță într-o manieră ce protejează atât clienții finali cât și proprietatea intelectuală ce aparține producătorilor de contoare inteligente. Metodele criptografice folosite în acest capitol folosesc funcții de dispersie pentru implementarea algoritmului de verificare a integrității programului firmware, criptarea memoriilor de stocare prin standardul avansat de criptare (AES) cu chei de până la 256 biți pentru protejarea proprietății intelectuale, iar pentru transportul fișierelor securitatea va fi asigurată de canale de comunicație bazate pe chei simetrice și prin protocolul HTTPS.

Pentru îndeplinirea acestui obiectiv, vom avea nevoie de două componente software optimizate pentru contoarele inteligente și resursele hardware de care acestea dispun. Prima componentă a sistemului de actualizare la distanță a contoarelor inteligente este acoperită de o soluție de tip bootloader secundar (încărcător de program) cu funcții de decriptare a imaginilor, autentificare digitală a acestora precum și instalare a noului software. Cea de-a doua componentă software va fi integrată în aplicația contorului inteligent și aceasta se va ocupa de autentificarea cu serverul producătorului pentru a putea descărca într-un mod sigur o imagine software, apoi se va ocupa de stocarea acesteia și va urmări în același timp să nu influențeze în niciun fel mărimile contorizate în tot procesul de actualizare.

După prezentarea și analiza stadiului actual și a cerințelor standardizate la nivel arhitectural, am prezentat structura și pașii de implementare a sistemului de

actualizare al unui prototip de contor inteligent bazat pe microcontrollerul STM32L475 precum și metodele de testare a soluției propuse.

În finalul capitolului se prezintă rezultatele obținute de sistemul de actualizare format din bootloader și partea de aplicație precum și evaluarea proprietăților de siguranță cibernetică. Astfel, am ajuns la concluzia că este posibilă implementarea unui sistem de actualizare la distanță chiar și pentru sistemele low-power cu resurse hardware limitate (ie. 64 KB RAM și 256 KB Flash), îndeplinind totodată și cerințele de funcționalitate și securitate cerute de industrie.

4.2. Problema standardizării și stadiul actual

În [172], Moran et al., se propune o arhitectură standardizată folosită în prezent în industria IoT, care prezintă cerințele de sistem minimale și o arhitectură de nivel înalt a întregului sistem de actualizare la distanță folosit în echipamentele integrate conectate. Amintim cerințele esențiale într-un sistem de actualizare la distanță așa cum apar în manifestul SUIT (Software Updates for Internet of Things) [173]:

- Distribuirea imaginilor folosite în procesul de actualizare trebuie să nu se bazeze pe măsurile de securitate dezvoltate la nivelul straturilor fizice, de transport sau de rețea, iar soluția aleasă trebuie să nu țină cont de mediul hardware prin care are loc actualizarea (ie. Bluetooth, Wi-Fi, USB, sondă optică, etc.)
- Mecanismele de securitate folosite trebuie să fie de ultimă generație și să includă metode de autentificare a autorului imaginilor descărcate, metode de protecție a integrității imaginii pentru a garanta că nicio terță parte nu poate modifica imaginea originală și, nu în ultimul rând, mecanismul de actualizare trebuie să asigure protecția confidențialității imaginii firmware.
- Sistemul de actualizare trebuie să includă și un bootloader capabil să verifice integritatea software a contorului inteligent la fiecare pornire cu ajutorul mecanismelor criptografice. Acest bootloader poate conține și mecanisme de recuperare în cazul în care procesul de actualizare nu reușește să ajungă la final.
- Fiabilitatea întregului dispozitiv nu trebuie să fie afectată de mecanismul de actualizare. O pană de curent, condiții nefavorabile ale rețelei de alimentare sau de comunicații, precum și un eventual eșec de validare nu trebuie să provoace o defecțiune a dispozitivului actualizat.

Deși standardul propus nu impune algoritmii criptografici necesari validării imaginilor, în lucrarea [174], Banegas face o analiză a mai multor mecanisme ce pot

fi folosite pentru a obține un grad ridicat de protecție chiar și in cazul unor contoare inteligente ce nu dispun de resurse hardware de ultimă generație.

În [175], se arată apropierea dintre echipamentele de contorizare și echipamentele folosite în casele inteligente, iar soluția de actualizare prezentată de Sahlmann et al. este bazată pe protocolul MQTT. Tot din domeniul Internet of Things, soluții similare au fost abordate în [176], [177] și [178].

Kolehmainen descrie în [179] mai multe probleme întâlnite în mecanismele de update ale echipamentelor încorporate, iar acesta propune un model în patru părți pentru rezolvarea celor mai des întâlnite probleme de securitate. Cele patru categorii propuse sunt: împachetarea, transportul, autentificare și atestarea. Soluțiile descrise au ca punct comun un sistem de actualizare ce încearcă să distribuie uniform actualizările ce au loc la un moment dat în rețeaua de dispozitive astfel încât să se evite problemele de tip DOS. De asemenea, abordările propuse consideră procesul de actualizare ca fiind unul intensiv pentru sistemul de calcul, astfel că actualizările sunt planificate să aibă loc atunci când sistemul se află într-o stare de repaus, minimizând astfel un posibil impact asupra performanțelor dispozitivelor aflate în proces de actualizare.

Constrângerile venite din resursele hardware limitate au fost o problemă dezbătută intens în literatura de specialitate. În [180], [181] și [182] sunt prezentate strategii de implementare a cerințelor SUIT chiar și în echipamentele cu memorie RAM sau flash de dimensiuni reduse. Mai mult, în [183] o soluție economică completă pentru echipamente de tip ZigBee este descrisă de către Uddin et al., dar aceasta presupune standardizarea la nivel de rețea pentru o descentralizare completă a procesului de actualizare.

Soluții pentru implementarea unui sistem de încărcare a programului principal, îndeplinind în același timp și cerințele SUIT au fost pe rând descrise în [184] pentru un sistem de tip MSP430 foarte limitat ca resurse hardware și funcționalități, iar apoi în [185] și [186] autorii au descris un bootloader specializat pentru actualizări software de tip IoT păstrând totodată consumul de energie la un nivel minim.

Metodele de instalare a noului program, descărcat în procesul de actualizare, au fost descrise în [187]. Yuan et al. trec în revistă metode de instalare potrivite pentru programele structurate pe două sau mai multe partiții, iar în [188] Schmidt et al. prezintă algoritmi criptografici și principii prin care stocarea actualizărilor pe memorii externe poate fi protejată împotriva potențialilor atacatori.

4.3. Structura soluției propuse

Pentru dezvoltarea unui sistem de actualizare pentru contoarele inteligente, dar care să fie totodată și compatibil cu cerințele standardului SUIT, am ales un sistem bazat pe microcontrollerul STM32L475 ce beneficiază de 128 KB memorie

RAM și 256 KB memorie Flash. Pentru descărcarea imaginilor de update și pentru comunicațiile dintre furnizor și contorul inteligent am ales modulul cu capabilități 3G și GPS, SIM808, produs de SimCom, unul din principalii furnizori ai constructorilor de echipamente de contorizare pentru rețeaua smart.

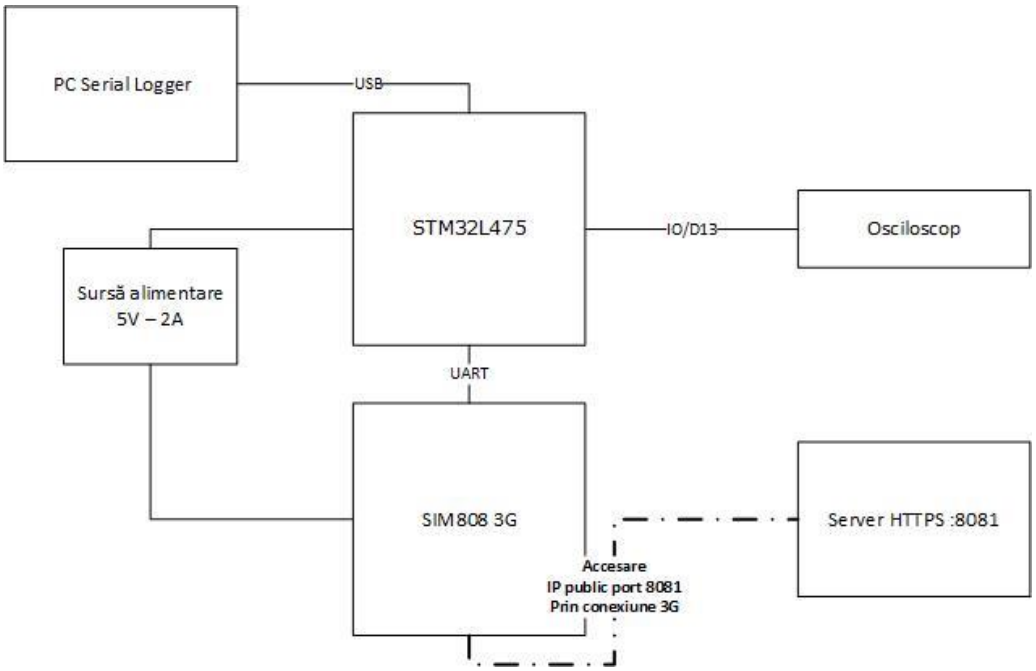

Fig. 4.1. - Schema bloc a sistemului experimental folosit pentru evaluarea procesului de actualizare la distanță a contoarelor inteligente

În figura 4.1 se observă schema bloc a sistemului experimental propus, având ca piese centrale placa de dezvoltare bazată pe STM32L475 și modulul de comunicație SIM808. Acestea sunt interconectate printr-o interfață UART, 115200bps, 8N1. Ambele subsisteme sunt alimentate de la sursă de curent continuu de 5V-2A, iar pentru o cronometrare exactă a timpilor de execuție din bootloader, un semnal GPIO de la pinul D13 al controllerului STM32, a fost conectat la un osciloscop Keysight DSOX1102A. Programarea inițială a programului principal pentru un contor inteligent generic [189] a fost pus la dispoziție de către furnizorul STMicroelectronics și a fost scris în memoria flash folosind J-Link programatorul inclus în placa de dezvoltare. Comenzile AT transmise prin interfața serială ce leagă cele două plăci, fac legătura cu un server expus pe un IP public de pe care se pot descărca noi actualizări. Întregul ansamblu fizic se poate vedea în figura 4.2, de mai jos.

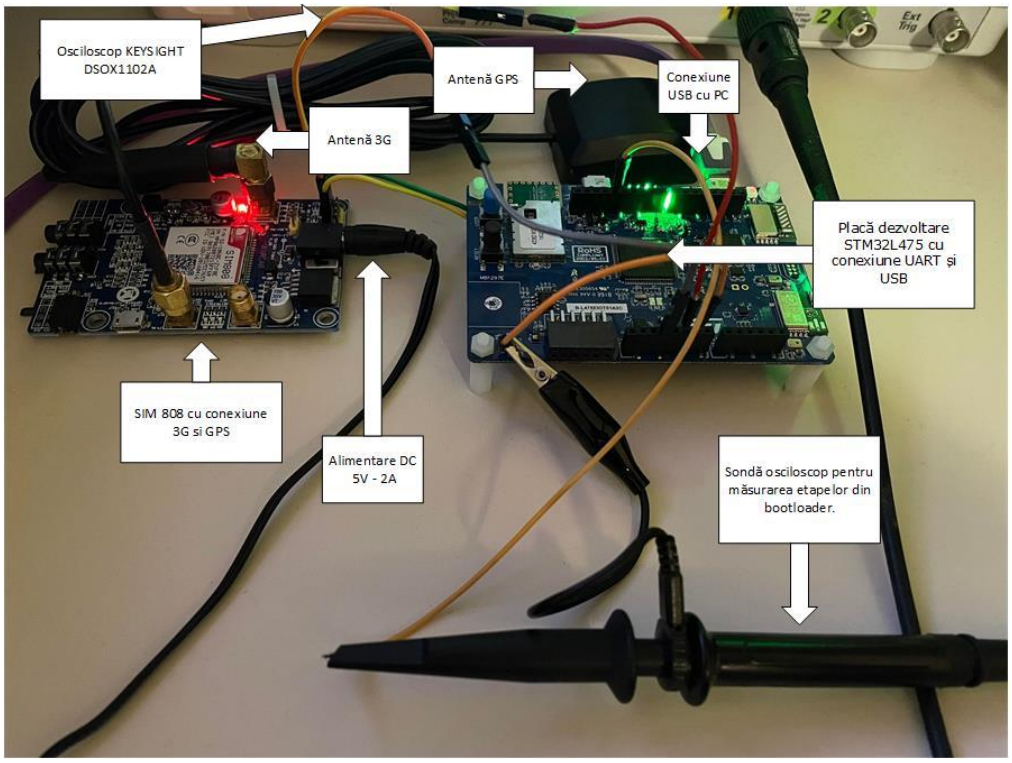

Fig. 4.2. - Standul experimental cu echipamentele integrate interconectate prin interfețe seriale.

Vitezele reduse de scriere în memoria flash internă, prezentate și în figura 4.3, ar duce la timpi de nefuncționare de aproximativ 60 de secunde pentru scrierea și ștergerea întregii aplicații. Acest lucru nu este acceptat de către standardul european ce reglementează caracteristicile tehnice ale echipamentelor de măsurare a energiei electrice [190], astfel că cea mai potrivită abordare este cea a unui sistem de actualizare bazat pe două partiții de memorie pentru programul prinicipal, iar bootloaderul va face tranziția într-un mod rapid la pornire între aplicația veche și cea actualizată.

Flash memory characteristics

Table 53. Flash memory characteristics(1)

Symbol	Parameter	Conditions	Typ	Max	Unit
t_{prog}	64-bit programming time	-	81.69	90.76	µs
t_{prog_row}	one row (32 double word) programming time	normal programming	2.61	2.90	ms
		fast programming	1.91	2.12	
t_{prog_page}	one page (2 Kbyte) programming time	normal programming	20.91	23.24	
		fast programming	15.29	16.98	
t_{ERASE}	Page (2 KB) erase time	-	22.02	24.47	

Fig. 4.3. - Caracteristicile tehnice ale memoriei interne de tip flash folosite de către microcontrollerul STM32L475.

O hartă a memoriei flash este ilustrată în figura 4.4. Aceasta prezintă memoria flash pornind de la prima adresă cu programul de tip bootloader, urmat pentru câteva sectoare flash de către datele nevolatile ce conțin informații scrise pe linia de producție cum ar fi coduri unice de identificare, configurații, chei de criptare/decriptare a actualizărilor, certificate digitale pentru verificarea autenticității imaginilor descărcate sau certificate digitale folosite pentru accesul la un server securizat. Pe lângă datele specifice aplicației de contorizare și cele instalate de producător, bootloaderul va trebui să păstreze în acest sector de memorie date privind algoritmii criptografici, sume de control precum și un identificator al partiției considerată activă la un moment dat.

Întrucât cerințele SUIT nu permit transportul unei imagini software în moduri nesecurizate, pachetul firmware va fi stocat într-o a 3-a zonă de memorie, destinată descărcărilor de imagini criptate și semnate. Transferul imaginii actualizate în sectorul inactiv se va face de către aplicație atunci când toate etapele de verificare și validare au fost finalizate.

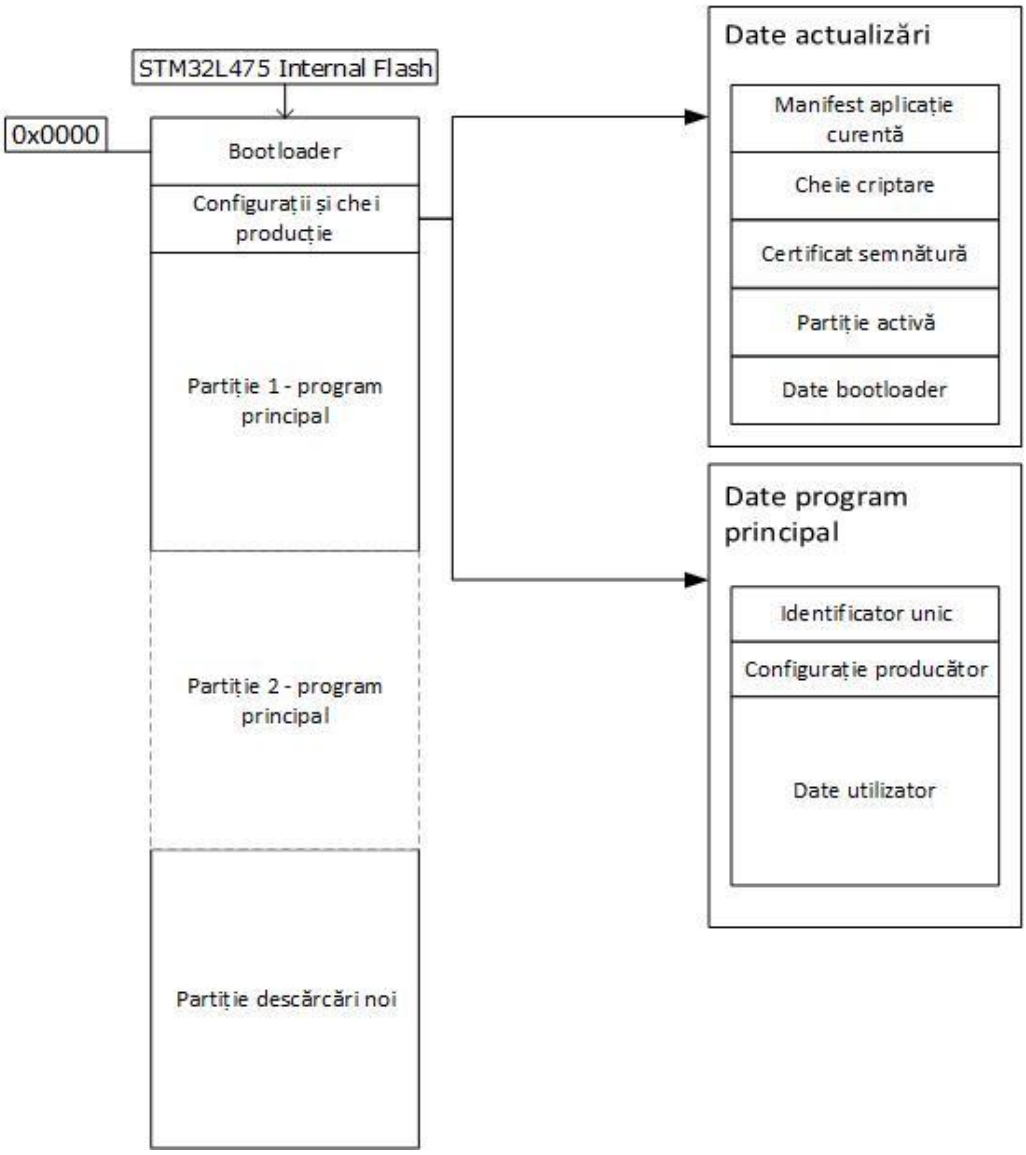

Fig. 4.4. - Structura memoriei nevolatile de tip flash din cadrul microcontrollerului STM32L475.

4.4. Bootloaderul Smart-Grid și procesul de încărcare a programului de contorizare actualizat

În cadrul oricărui echipament integrat, bootloaderul este primul program care se rulează de către procesor, iar acesta alege apoi aplicația ce urmează să fie rulată de către dispozitiv de îndată ce verificările de securitate și integritate au fost completate. Echipamentele de contorizare inteligentă au pe lângă cerințele de fiabilitate și securitate obișnuite și cerințe stricte legate de timpul necesar bootloaderului să parcurgă toate etapele și să ruleze aplicația de contorizare corespunzătoare [191]. Așadar, odată descărcată imaginea firmware ce conține actualizarea contorului, verificarea integrității imaginii, verificarea semnăturii autorului și decriptarea într-o partiție inactivă se vor face la nivelul aplicației și nu la nivelul procesului de boot, pentru a nu întârzia pornirea aplicației de contorizare. Bootloaderul va fi responsabil doar de alegerea partiției active și de verificarea integrității aplicației ce urmează să fie rulate. Integritatea nu poate fi verificată doar pe baza unei sume de control fie ea chiar si CRC32, lucru amintit si de Chakravarty et al. în [192], iar folosirea algoritmilor criptografici avansați este de preferat [193]. Întregul proces de încărcare și verificare a aplicației actualizate nou instalată este descris în figura 4.5 mai jos.

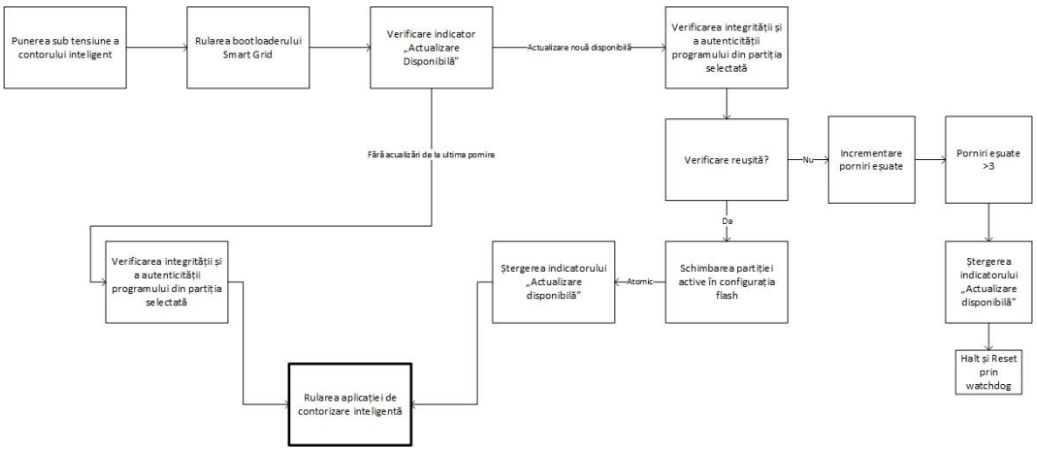

Fig. 4.5. - Diagrama de proces a încărcătorului (i.e. bootloader) de tip smart-grid propus.

La pornirea încărcătorului de program, acesta inițializează un număr minim de periferice, păstrând consumul de energie și timpii necesari inițializărilor cât mai scăzuți. Apoi, din memoria flash se citește un indicator de tip „fanion” care are rolul de a indica dacă o nouă actualizare a fost decriptată și proaspăt salvată în partiția inactivă. Dacă acest fanion nu este valid, atunci se pornește aplicația deja marcată ca activă și se rulează programul curent de contorizare inteligentă. Dar, dacă acest fanion are o valoare considerată validă, acest lucru semnalează nevoia unor verificări suplimentare de integritate și autenticitate. Dacă toate verificările au fost finalizate cu succes, aplicația poate porni, partiția activă va fi actualizată în memoria flash, iar fanionul va fi distrus marcând finalul unui proces de actualizare încheiat cu succes. În schimb, dacă procesul de validare a noii actualizări eșuează în mod repetat, la cel de-al patrulea eșec se ia decizia ca fanionul să fie distrus fără actualizare partiției active, astfel noua actualizare nu este considerată validă, iar procesul de actualizare ia sfârșit fără modificarea programului curent.

Acest proces de contorizare a validărilor eșuate asigură robustețea procesului de actualizare și astfel ne-am asigurat că funcționalitatea contorului inteligent nu este întreruptă, revenindu-se imediat la programul anterior așteptând o nouă actualizare.

Simplitatea și păstrarea proceselor ce au loc în cadrul încarcatorului de program la un nivel minim vin din nevoia păstrării unui program cât mai robust întrucât bootloaderele de acest tip nu pot fi actualizate și sunt scrise o singură dată în toată durata de operabilitate a contorului inteligent, iar al doilea motiv este strâns legat de viteza cu care acești pași trebuie executați pentru a putea rula programul de contorizare cât mai repede, evitând pierderi și goluri în curbele de profil de consum.

4.5. Modulul software responsabil de descărcarea și salvarea actualizărilor prin echipamentele Smart-Grid

În diagrama din figura 4.6, am descris pașii executați la nivelul aplicației de contorizare în cadrul modului software responsabil de descărcarea și salvarea actualizărilor.

Modulul interoghează periodic, la fiecare 24 de ore, un server oferit de producător. Serverul oferă un răspuns privind actualizările disponibile într-un pachet criptat cu o cheie prestabilită încă din timpul producției contorului inteligent. Mai mult, înainte de a furniza răspunsul criptat, contorul trebuie să se autentifice la rândul său folosind metoda descrisă în [194] și folosind un certificat SSL stocat în memoria internă.

Odată ce a fost găsită o actualizare compatibilă, contorul descarcă în partiția destinată noilor actualizări, o imagine criptată prin același canal de comunicație criptat. Structura memorie a fost descrisă anterior, iar partiția la care facem referire aici se află la capătul memoriei flash din controllerul STM32L475 așa cum se observă și în figura 4.4.

La finalul descărcării imaginii criptate, se execută o verificare de integritate a pachetului descărcat prin calculul unei sume de control MD5 [195], de 128 de biți. Dacă verificarea s-a finalizat cu succes și sumele coincid cu cele descrise în antetul

imaginii și cu cele disponibile pe serverul ce a furnizat imaginea, atunci programul ia decizia de a curăța partiția inactivă din memoria flash pentru a o pregăti pentru stocarea imaginii de actualizare decriptate. Criptarea se face cu chei AES-128 CBC [196] și folosind un vector de inițializare aleatoriu aflat în antetul imaginii.

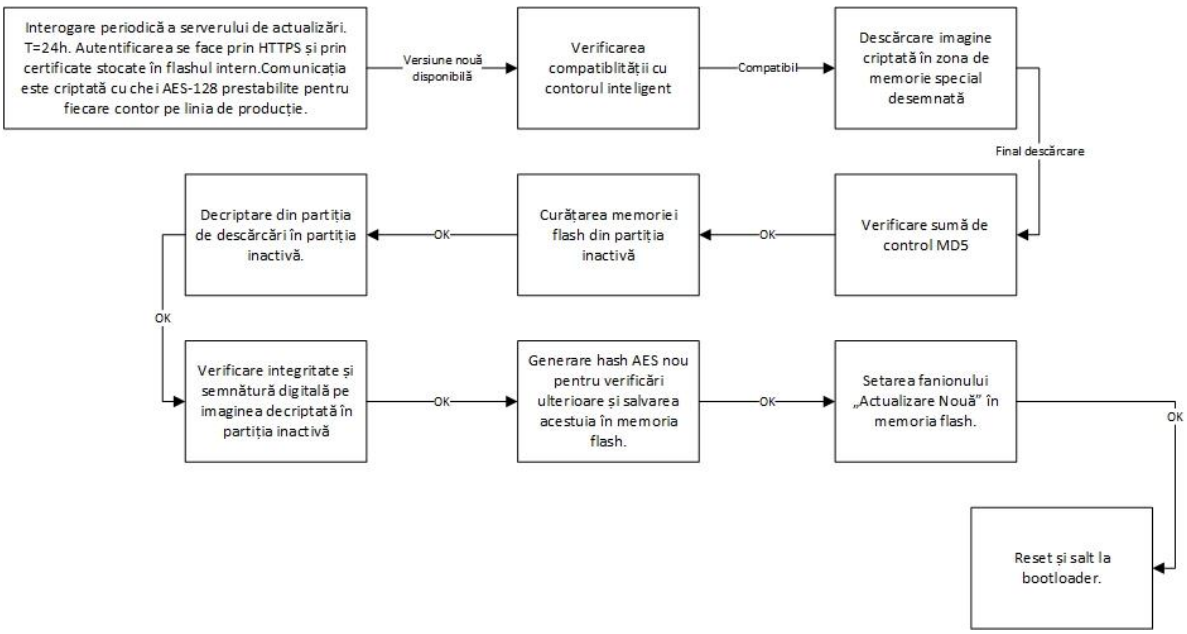

Fig. 4.6. - Diagrama de proces a aplicației de actualizare a echipamentelor de tip smart-grid.

La finalizarea decriptării imaginii în partiția inactivă, se verifică pentru prima dată autenticitatea softwareului proaspăt instalat. Așadar, se rulează rutinele de verificare a semnăturii digitale cu care a fost semnată imaginea firmware și se verifică astfel și integritatea acesteia. Algoritmii folosiți sunt cei descriși de Rahul et al. în [197] și fac uz de capabilitățile criptografice ale acestei familii de microcontrollere produse de STMicrolectronics.

Folosind cheia de decriptare anterioară și un vector IV generat aleatoriu folosind mai multe surse de entropie [198], se generează și salvează într-o zonă protejată a memoriei flash, un manifest, sau o așa zisă valoare hash ce va fi folosită de către bootloader ulterior.

Dacă toți pașii descriși anterior au fost rulați cu succes și nu au fost întâlnite nici un fel de erori de calcul sau de execuție, se setează o valoare pe 32 biți în cuvântul fanion ce indică prezența unei noi actualizări în partiția inactivă. Acesta, așa cum am descris deja în subcapitolul anterior, va fi citit de către încărcătorul de aplicații și va face tranziția de la aplicația curentă la cea actualizată.

În final, se transmite un semnal de resetare a programului principal pentru a porni tranziția la noul firmware. Programul principal poate lua decizia de a executa acest salt la bootloader, imediat sau la o oră la care consumul de energie contorizat este minim și riscul ca un utilizator sau tehnician să necesite acces la contor să fie cât mai redus. În mod alternativ, furnizorul poate emite o comandă ce oprește

actualizările software pentru un număr stabilit ore pe un anumit contor sau un set de contoare inteligente, tocmai pentru a evita schimbarea versiunii curente în mijlocul unor operațiuni tehnice planificate.

4.6. Analiza timpilor de execuție și a impactului acestora în procesul de actualizare a contoarelor inteligente

Pe baza standului experimental descris în figura 4.2, au fost rulate teste experimentale de tip end-to-end, prin care aplicația de bază a microcontrollerului STM32L475 a fost actualizată în mod repetat, iar cu ajutorul osciloscopului și a unor semnale digitale au fost măsurați timpii de execuție pentru fiecare etapă din procesele descrise în diagrama de proces a încărcătorului de program (figura 4.5) și în diagrama e proces a modului software responsabil de actualizările firmware a contorului inteligent (figura 4.6).

Tabelul 4.1. - Durata de descărcare și instalare a actualizărilor efectuate prin standul experimental.

Test	Durata de descărcare a actualizării (s)	Durata de instalare după repornire (s)	Dimensiunea fișierului de actualizare (bytes)
1	61.62	7.588	484,572
2	57.64	6.842	484,572
3	69.96	6.851	484,572
4	67.69	6.838	484,572
5	63.58	7.029	484,572
6	66.28	6.611	484,572
7	63.21	6.923	484,572
8	66.37	7.619	484,572
9	63.01	6.794	484,572
10	65.85	7.493	484,572
11	59.74	6.806	484,572
12	63.95	6.633	484,572
13	60.63	7.593	484,572
14	64.39	6.843	484,572
15	63.62	6.844	484,572
16	64.50	6.823	484,572
17	60.73	7.657	484,572
18	62.43	7.070	484,572
19	66.71	7.052	484,572
20	63.17	6.669	484,572
21	66.92	6.515	484,572
22	63.77	6.922	484,572
23	64.37	7.221	484,572
24	60.69	7.441	484,572
25	60.79	6.695	484,572

Actualizările au fost efectuate într-un mediu controlat, iar rezultatele experimentale au fost trecute în tabelul 4.1. Timpii de descărcare a actualizărilor nu impactează modul de funcționare a contoarelor inteligente, aceste măsurători au doar rol de control și pot conferi un grad sporit de încredere în interpretarea rezultatelor finale. Pe de altă parte, timpii de instalare sunt timpi de execuție în care contorul inteligent nu poate executa alte operațiuni, iar consumul de energie nu este înregistrat în această perioadă.

Tabelul 4.2. - Analiza statistică a măsurătorilor experimentale efectuate.

Timp execuție	Media (s)	Deviație	Varianță Eșantion	Interval de încredere (95%)
Descărcare actualizare	63.6648 s	2.811	7.903	de la 61.56 s la 65.76 s
Instalare actualizare	7.0148 s	0.351	0.123	de la 6.87 s până la 7.15 s

În tabelul 4.2, am prezentat analiza statistică a rezultatelor experimentale. Timpii de descărcare a unui nou program firmware s-a încadrat cu un interval de încredere de 95%, între 61.51 secunde și 65.76 secunde, iar timpul de instalare a acestor actualizări s-a încadrat între 6.87 secunde și 7.15 secunde pentru același interval de încredere.

4.7. Concluzii parțiale și contribuții

Rezultate prezentate arată că este posibilă implementarea unui sistem de actualizare la distanță chiar și pentru sistemele low-power cu resurse hardware limitate cum sunt cele găsite în cadrul echipamentelor instalate în rețeaua inteligentă. Pentru îndeplinirea cerințelor minime de securitate și pentru a acoperi toate mecanismele de protecție la defect este necesar un microcontroller cu minim 128 KB RAM și minim 256 KB Flash. Sistemul prezentat bazat pe microcontrollerul STM32L475 a îndeplinit toate cerințele de funcționalitate și securitate cerute de standardul SUIT și este o soluție potrivită pentru contoarele inteligente conectate în rețelele de tip smart grid.

Impactul asupra operaționalității contorului inteligent în procesul de actualizare a fost redus folosind metodele prezentate, iar timpul mediu de instalare a unui nou firmware în condiții de laborator a fost de 7.0148 secunde.

Metodele prezentate în acest capitol subliniază importanța standardizării procesului de actualizare în rețelele de contorizare inteligentă. Coexistența echipamentelor de contorizare în rețeaua de date a sistemului energetic poate fi puternic afectată de soluțiile alese de producătorii de contoare inteligente. Sincronizarea tehnologiilor alese de dezvoltatori poate avea un impact major asupra întregii rețele, iar interconectarea acestor contoare în sistemul energetic într-un mod coerent poate îmbunătăți atât viteza de transmisie cât și capacitatea de acoperire a zonelor greu accesibile, subiecte ce vor fi tratate în capitolul următor. De asemenea, la nivel de încărcător de program (bootloader), alegerile tehnice trebuie sa sporească în primul rând robustețea procesului de actualizare întrucât această

porțiune de program nu poate fi actualizată, iar mecanismele de recuperare, alese de dezvoltatorii de contoare inteligente, pot evita defectarea prematură a echipamentelor instalate fără a necesita intervenția locală a unui operator atunci când procesul de actualizare este întrerupt.

5. ÎMBUNĂTĂȚIREA DISPONIBILITĂȚII PRIN SEGMENTAREA DATELOR ÎN REȚELELE SMART GRID PLC

5.1. Introducere

Rețelele electrice variază în mărime, de la acoperirea unei singure clădiri la cele naționale care acoperă țări întregi sau chiar la rețele transnaționale care pot traversa continentele. O dată cu lansarea de contoare inteligente în întreaga lume, există cazuri de utilizare în care soluțiile obișnuite eșuează și disponibilitatea în rețea a anumitor contoare este foarte scăzută din cauza condițiilor de comunicație precare. Acest capitol propune un model de segmentare a datelor pentru fișiere de date mari, care trebuie să călătorească în siguranță și în mod fiabil prin rețeaua inteligentă de distrbuție. Metoda propusă abordează, în special, îmbunătățirile disponibilității rețelei de tip PLC PRIME prin folosirea adecvată a unor algoritmi de segmentare a datelor la nivelul aplicației și calibrarea acestora pentru rate de transmisie în conformitate cu nivelurile de zgomot prezente în rețeaua electrică. Îmbunătățirea ratei de succes în cererile de date informatice de la echipamentele inteligente instalate pe rețeaua electrică, chiar și la rate de transmisie mai mici, înseamnă că nu este necesară o interacțiune manuală a operatorilor furnizorilor de energie, reducând costurile de întreținere atât pentru companiile energetice, precum și pentru utilizatorul final. De-a lungul dezvoltării capitolului, au fost efectuate experimente pe o rețea electrică de mică putere pentru a evalua îmbunătățirile disponibilității prin metoda propusă precum și fezabilitatea actualizărilor de firmware la distanță în cazul unor echipamente ce comunică prin rețele cu un nivel de zgomot ridicat. Rezultatele au arătat că actuala abordare are rezultate similare cu o actualizare manuală a firmware-ului efectuată de către un operator deplasat la locul de consum. Mai mult, rezultatele arată că metoda prezentată, de actualizare a firmware-ului la distanță, este fiabilă și practică în zonele în care disponibilitatea echipamentelor inteligente este scăzută.

Prezentul capitol este o versiune extinsă a lucrărilor anterioare publicate în [200] și [201], iar conceptul inițial a fost extins inclusiv prin experimente și metode de analiză statistică a actualizărilor de firmware la distanță în rețelele energetice inteligente bazate pe protocoale de comunicații prin liniile de alimentare.

Odată cu dezvoltarea tehnologiilor din domeniul energiilor regenerabile și odată ce colectarea energiei solare și eoliene prin soluțiile instalate în medii rezidențiale, necesitatea comunicării fiabile cu distribuitorii de energie electrică în timp real este mai mare ca niciodată. Contoarele inteligente permit o gestionare eficientă a fiecărei gospodării, iar companiile de utilități pot aduna mai multe date despre consumul și producția de energie din fiecare punct de consum. Distribuitorii sunt informați automat cu privire la orice întreruperi și pot fi furnizate noi funcții sau scheme de tarifare de la distanță către utilizatorii finali atunci când este necesar. Contoarele inteligente sunt puternic conectate de-a lungul rețelei electrice pentru a forma o rețea inteligentă care are ca scop controlul dinamic al importurilor și exporturilor de energie într-un mod optimizat având ca scop final producerea unei

amprente de carbon cât mai reduse, iar totodată reducând costurile utilizatorilor și îmbunătățind, în același timp, fiabilitatea rețelei.

Pentru a putea optimiza consumul de energie într-o rețea inteligentă, este necesară instalarea de echipamente de contorizare inteligentă, echipamente ce pot aduna cantități mari de informații care apoi pot fi transmise spre analiză de-a lungul liniilor electrice către un furnizor de energie. După analiza curbelor de sarcină și a altor metode de analiză și reprezentare a consumului de energie, distribuitorul poate dezvolta scheme de tarifare sau chiar programe software optimizate pentru un anumit profil de consum, urmând apoi să le transmită către contoarele inteligente din punctele de consum în diferite formate. Actualizările transmise către contor pot conține doar seturi de parametri sau pot conține pachete software complet noi care se potrivesc profilului de consum din gospodăria vizată.

Pentru a face față tranziției accelerate către o rețea de distribuție inteligentă, este important să putem face actualizări software ale contoarelor inteligente de la distanță, fără a schimba echipamentul sau fără a necesita intervenția manuală a unui operator al distribuitorului la locul de consum vizat. Funcționalitatea de încărcare și descărcare de la distanță a imaginilor binare permite obținerea unor contoare particularizate și actualizate în funcție de necesitățile din teren descoperite într-un moment ulterior instalării [202].

În timp ce desfășurarea contoarelor inteligente în rețelele inteligente urmărește în special acordarea posibilității pentru clienți de a opta pentru o anumită opțiune de economisire a energiei, provocarea de a obține informații, într-un mod robust, de la și către utilizatorii finali din rețeaua inteligentă, a fost evidențiată frecvent în literatura de specialitate ca fiind o sarcină dificilă [203].

Contoarele inteligente pot comunica cu centrele informatice ale furnizorilor principali de energie electrică prin liniile de tensiune, prin radio sau cu ajutorul datelor mobile. Adesea, unele noduri din rețeaua de energie inteligentă dispun de o disponibilitate redusă la aceste medii de comunicare, iar linia de date în regiunile izolate ale rețelei sau în medii foarte zgomotoase, reușește să transmită cu succes doar câteva cadre de date pe zi în cel mai fericit caz.

Capitolul curent este structurat după cum urmează: introducerea evidențiază scopul, semnificația și importanța subiectului ales, apoi secțiunea context menționează stadiul actual al tehnicii și prezintă o comparație rapidă a publicațiilor cheie privind provocările transmisiilor de date pe liniile electrice de-a lungul modelelor propuse în prezent. A treia secțiune, materiale și metode, enumeră materialele și echipamente utilizate pe tot parcursul implementării modelului de segmentare. Metodele descrise acoperă, de asemenea, testele de descărcări și încărcări de date de la contoare inteligente către un concentrator de date și testele ratelor de transfer necesare în timpul unui proces de actualizare a firmware-ului. Secțiunea de rezultate acoperă prezentarea rezultatelor experimentelor descrise anterior. În total au fost rulate 20 de teste de încărcare a curbelor de sarcină și au fost realizate 60 de descărcări de imagini firmware atât prin intermediul liniilor de alimentare cât și prin intermediul sondei optice. În cele din urmă, discuțiile și secțiunile de concluzii încheie lucrarea cu o vedere amplă a implicațiilor constatărilor actuale.

5.2. Protocoale de comunicație folosite în rețelele de energie electrică

Al treilea pachet energetic aflat în derulare la nivel european [204] cere statelor membre ale Uniunii Europene să asigure introducerea unor scheme inteligente de măsurare a consumului de energie. Există aproape 60 de milioane contoare inteligente instalate deja în doar trei state membre [205] (Finlanda, Italia și Suedia) și, în timp ce 95% [206] din incinte sunt acoperite de tehnologiile curente fără probleme, vor fi câteva mii de gospodării care sunt lăsate într-o parte inaccesibilă a rețelei de energie inteligentă unde abordările standard întâmpina mari dificultăți de comunicare.

Problema îmbunătățirii securității rețelei inteligente a fost un subiect activ de cercetare în ultimii ani și soluțiile acoperă atât îmbunătățiri la nivel fizic, cum ar fi soluțiile prezentate de Passerini in [207] până la cele de la nivel de aplicație software în care firmware-ul conectat la internet se actualizează așa cum este descris de Jang si Jung în [208]. Literatura evidențiază în primul rând, problemele care apar într-o rețea inteligentă nesecurizată corespunzător și riscul pe care aceasta îl prezintă permițându-le atacatorilor în cazul unui potențial atac să destabilizeze o rețea energetică prin controlul de la distanță asupra unor noduri cheie. Acest capitol își propune să confere suportul pentru o îmbunătățire a securității contoarelor inteligente cu disponibilitate redusă la o rețea de date, permițând fiecărui nod să primească actualizări de la distanță într-un mod practic și într-un timp util.

Într-o astfel de rețea, atacatorii pot reduce lățimea de bandă a rețelei sau pot obține acces inclusiv la date private, cum ar fi istoricul consumului de energie, informații legate de utilizator sau chiar tiparele de utilizare a energiei și profilul de utilizator casnic atribuit unei locuințe, prin exploatarea unor vulnerabilități sau chiar prin instalarea unui firmware malițios [208]. Mlynek și colab. [209] arată ratele de transfer a datelor pentru diferite protocoale de comunicații folosite în cadrul liniilor electrice utilizate în contorizarea inteligentă, dar concluzionează că toate echipamentele ce comunică prin liniile de înaltă tensiune vor avea pierderi de date la nodurile care nu sunt suficient de apropiate și vor depinde foarte mult de calitatea energiei electrice și a rețelei dintr-o anumită zonă. Soluția propusă, de a adăuga echipamente noi la mijlocul distanței, cu rol de repetor de semnal, nu este fezabilă întrucât lucrarea prezentă își propune o îmbunătățire a comunicației prin actuala rețea fără intervenții asupra echipamentelor hardware sau a mediilor fizice de comunicare, iar toate soluțiile propuse trebuie să funcționeze doar cu echipamentele deja instalate pe teren. În [210], Andreadou subliniază deciziile luate de marile companii europene de distribuție a energiei electrice în timpul expansiunilor Smart Grid. Tehnologia PRIME a fost una dintre cele mai frecvente alegeri datorită performanțelor ș a costurilor relativ reduse de instalare în rețeaua de joasă tensiune.

Așteptările curente sunt ca aproximativ 200 de milioane de contoare inteligente să fie instalate până în anul 2021. Totodată, există mai mul de 50 de proiecte europene care sunt legate direct sau indirect de aplicații de contorizare inteligentă, toate acestea necesitând o întreținere corespunzătoare pentru o perioada prelungită de timp, lucru ce implică printre altele și actualizări de firmware

ale contoarelor inteligente de fiecare dată când o nouă funcționalitate este adăugată sau când o actualizare de securitate este necesară. În plus, lansările paralele fără un protocol sincronizat de comunicație au atras atenția asupra unei posibile abordări standardizate. În [211], standardul de comunicare IEC 61850 este recomandat pentru comunicarea în rețelele locale (LAN) și protocolul eXtensible Messaging and Presence Protocol (XMPP) în rețele extinse (WAN). Această propunere rezolvă parțial problema de standardizare, dar încă suferă de latențe de până la câteva minute, precum și de lățimi de bandă foarte mici lucru ce face adoptarea ei greoaie și puțin fezabilă la momentul actual.

O revizuire a literaturii privind securitatea cibernetică în rețelele Smart Grid efectuată de Baumeister [212] evidențiază riscul de a avea contoare inteligente care nu vor mai beneficia de upgrade-uri de securitate în rețea datorită problemelor de disponibilitate. Studii privind infrastructura contoarelor inteligente [213-216] atrag atenția asupra riscului de securitate prezentat prin disponibilitatea redusă la o rețea de comunicații de date și oferă soluții de la cele de tip VSAT [217] care conferă o acoperire înaltă sau LTE și soluții mobile [218] cu disponibilități de aproape 99,9%. Problema este că o parte din contoarele inteligente sunt deja instalate și adăugarea de noi tehnologii nu ar fi fezabilă din punct de vedere tehnic și nici din punct de vedere al costurilor. Așadar, soluția propusă trebuie să fie pe cât posibil doar la nivelul aplicației și trebuie să fie compatibilă cu capacitatea redusă de a transmite date prin rețelele problematice amintite mai sus. O astfel de soluție trebuie să folosească la maxim fiecare bit de transmisie, evitând pe cât posibil retransmisiile.

Pentru piața energetică din România s-a ales un model de implementare bazat pe concentratoare de date conectate prin liniile de tensiune direct la contoarele inteligente. Comunicarea datelor se face în primul rând prin protocoale PLC (power line communication), iar de la concentrator către serverele furnizorilor transmisia se face prin internet. În ceea ce privește protocoalele de comunicare alese până acum, cea mai mare parte a pieței folosește PLC, M-Bus, WiFi, RS-485 și rețele celulare. Sistemele PLC au o piață divizată între protocoalele PLC G3 și PRIME Narrow Band [219]. Aceste ultime tehnologii, deși au marele avantaj de a nu necesita instalarea unei noi infrastructuri comunicând prin rețeaua electrică, au dezavantajul că rata de succes în transmisia datelor este afectată de interferențele generate de consumatori sau de distanța nodurilor de transmisie dintre gospodăriile adiacente. Cerințele echipamentelor alese de ERBD și Autoritatea Națională de Reglementare în domeniul Energiei sunt potrivite pentru zonele dens populate , dar limitările comunicațiilor prin liniile de tensiune se văd când avem de a face cu un volum foarte mare de date, iar deși instalarea echipamentelor la nivel național încă nu se apropie de sfârșit deja avem nenumărate situații în care cerințele inițiale se dovedesc acum insuficiente.

Standardul global DLMS / COSEM (IEC 62056, EN13757-1) pentru măsurarea energiei inteligente solicită anumite structuri de date, cum ar fi tarifele care se pot schimba dinamic la fiecare două minute sau alegerea contractului prin contor din mai mulți furnizori de energie sau chiar profilarea curbelor de sarcină pentru tarifele din contract suportat la o rezoluție de 1 min pentru toate tipurile de energii (activă, reactivă, importată / exportată). Astfel de structuri complexe copleșesc de obicei protocoalele alese și pot ușor ajunge la dimensiuni de mai mulți megabyțes. Pe de altă parte, evaluările de performanță ale celor două benzi din sistemele PLC (PRIME și G3) arată că această transmisie poate fi realizată la o viteză

mai mare pe PRIME, dar se comportă mai nefavorabil în prezența interferențelor sau a zgomotului pe rețea[220, 221].

Rata de eroare a pachetelor în rețelele PRIME crește odată cu dimensiunea pachetelor, după cum a demonstrat Farias în [222]. Contoarele PRIME înregistrează o disponibilitate scăzută tot mai des, deoarece dimensiunea pachetelor transmise a crescut semnificativ, iar soluțiile hardware propuse în literatura de specialitate nu pot îmbunătății un contor deja instalat care înâmpină pierderi semnificative de pachete. Prin urmare, capitolul curent își propune să îmbunătățească rata de eroare a pachetelor transmise prin rețelele PRIME, care ulterior ar putea duce la îmbunătățirea ratei de succes a actualizărilor la distanță a firmwareului din contoarele inteligente.

Segmentarea datelor la o dimensiune adecvată într-un mod dinamic, fiecărui canal de comunicație, ar putea duce la îmbunătățirea protocoalelor actuale, iar contoarele inteligente, care arareori păstrează o conexiune solidă cu furnizorul de energie, vor putea astfel să obțină actualizări de software într-un mod practic. Folosind această abordare furnizorii pot evita cazurile în care operatorii sunt nevoiți să recurgă la o actualizare sau citire a contorului manuală pe teren. În final, acest lucru poate duce la un cost de mentenanță mai redus, lucru de care vor beneficia atât furnizorii de energie cât și utilizatorii finali.

5.3. Materiale și metode de testare a soluției

Pentru a atinge o rată de succes a actualizărilor software la distanță, contoarele inteligente aflate într-o zonă cu disponibilitate redusă trebuie să evite retransmisiile pe cât posibil, să aibă o toleranță ridicată la erorile de transmisie și în sfârșit, să fie capabile să reasambleze fișierul inițial ori de câte ori detectează o transmisie completă. Segmentele pot fi livrate pe canale de comunicație separate, acolo unde acest lucru este disponibil pe contorul inteligent sau prin cadrul echipamentelor adiacente din aceeași rețea inteligentă.

În dezvoltarea aplicației s-au folosit tehnologiile sugerate de către autoritățile de reglementare și anume, comunicații de tip PLC utilizând protocoale PRIME aplicate pe platforma de evaluare ST EVL-KSTCOMET10-1 bazată pe un nucleu Cortex-M4. Configurația implicită este potrivită pentru protocolul PRIME (UIT G.9904) CENELEC de banda A, iar conexiunea PLC permite dispozitivului să transmită și să recepționeze date pe linia de curent alternativ utilizând protocoalele de bandă îngustă modulate OFDM cu frecvențe de până la 500kHz [223]. Terminalele ce simulează contoarele inteligente sunt conectate în serie și rețeaua este controlată de o a treia placă de dezvoltare care acționează ca un data concentrator PRIME. Toate dispozitivele au avut instalat un modul de memorie externă de tip W25Q16JV pentru stocarea a 16 megabytes de profiluri de curbă de sarcină în format DLMS.

Fiecare tip de rețea de date are o cantitate maximă de date ce pot fi mutate prin nodurile rețelei într-un interval de timp dat. În rețelele de calculatoare, unitatea de transmisie maximă (MTU) este de dimensiunea celei mai mari unități de date din protocolul ales (PDU), ce poate fi comunicată într-o singură tranzacție. Metoda de transport abordează de obicei o segmentare a datelor ce ține cont de constrângerile rețelei, astfel într-o conexiune tipică de tip Ethernet v2, este de așteptat un MTU de

1500 octeți [224], iar ori de câte ori mai multe tipuri de protocol sunt înseriate, considerentele MTU trebuie făcute având o imagine de ansamblu completă asupra protocoalelor și a mediilor fizice implicate în procesul de comunicare a datelor informatice de la un capăt la altul al rețelei.

Deși pachete mai mari înseamnă implicit și mai puține transmisii independente, există anumite compromisuri de care trebuie să ținem cont. Dacă viteza de procesare a unui pachet mare este redusă, rețeaua va rămâne ocupată pentru o perioadă mai lungă de timp, reducând astfel disponibilitatea celorlalte noduri până când tranzacția aflată în desfășurare ia sfârșit. O alta problemă cunoscută ce poate apărea odată cu creșterea dimensiunii unui pachet este că șansa apariției unei erori crește direct proporțional cu dimensiunea acestuia, iar orice eroare detectată va duce la retransmiterea întregului pachet. În mediile care sunt predispuse la apariția erorilor de transmisie și la corupția datelor, se vor folosi așadar, transmisii cu segmente de date cu dimensiuni reduse. Soluția propusă constă în împărțirea pachetelor de date mari în bucăți de dimensiuni egale cu unitatea maximă de transmisie din lanțul de comunicație. Acest lucru permite, în teorie, unui pachet să ajungă la destinație într-un mod cât mai robust. Prin acest mod ne asigurăm că lățimea de bandă disponibilă la locația unui contor inteligent nu este irosită prin retransmisii ale unor structuri de dimensiuni mari și aceasta este folosită în totalitate de segmentele redimensionate după condițiile din rețeaua PLC.

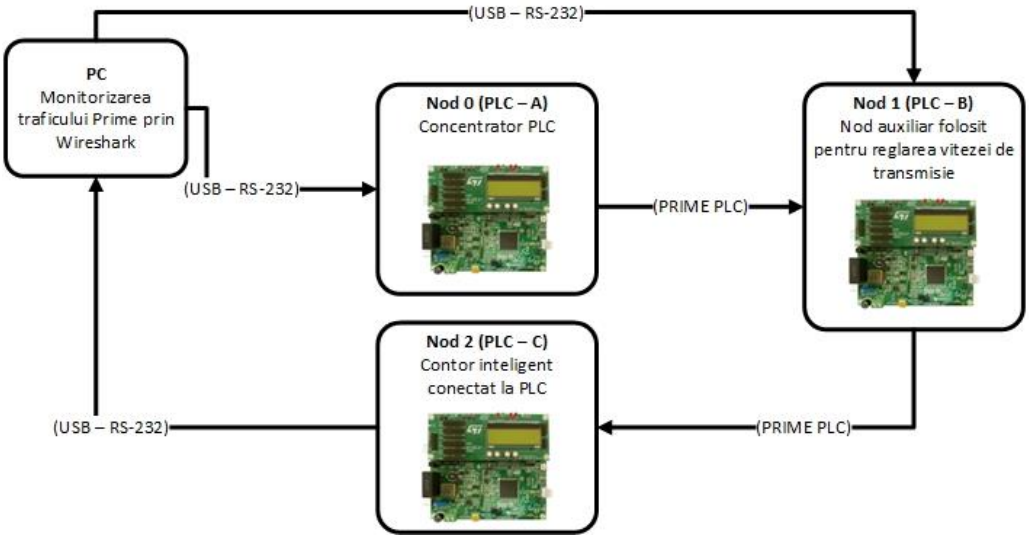

Fig. 5.1. - Topologia rețelei de evaluare a metodei de segmentare a datelor PoweRline Intelligent Metering Evolution (PRIME).

Figura 5.1 ilustrează topologia rețelei folosită la evaluarea soluției de segmentare a datelor. Această topologie constă în trei noduri de comunicație conectate la liniile de tensiune bazate pe platformele de evaluare a protocolului de comunicație PRIME, EVL-KSTCOMET1-1 [225]. Platformele de evaluare sunt de asemenea conectate la un computer ce poate monitoriza întregul sistem printr-o interfață de diagnoză încorporată expusă printr-un port USB. Interfața USB

utilizează o aplicație personalizată dezvoltată special pentru acest test și dispune de comenzi ce pot simula o anumită calitate a rețelei sau ce poate analiza ratele de succes a transmisiilor PRIME între nodurile experimentale. Nodul 2, PLC-C, va fi examinat ca dispozitiv principal în timp ce celelalte două noduri au un rol auxiliar. Nodul 0, rulează o aplicație generică de tip data concentrator PLC-PRIME menținând funcțiile corespunzătoare unei rețele de tip mesh, iar nodul 1 are pe lângă funcțiile de bază capabilitatea de a simula o rată de succes a transmisiilor de pachete putând astfel să simuleze condițiile dintr-o rețea cu performanțe scăzute [226].

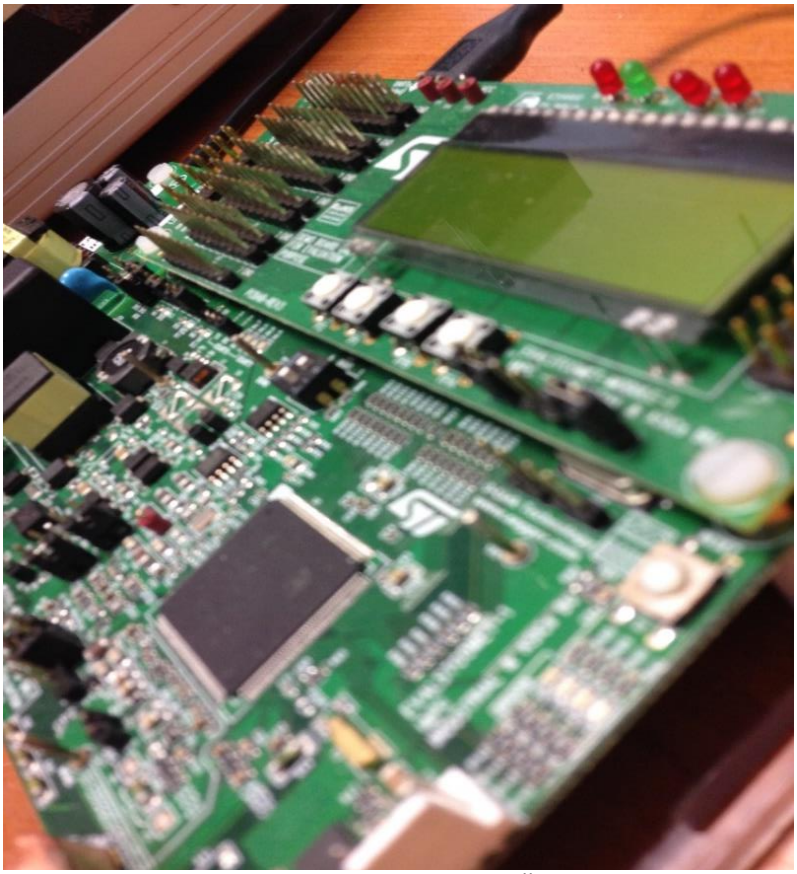

Fig. 5.2. - Platforma de evaluare pentru contorizare inteligentă PLC STMicroelectronics (ST)

Figura 5.2 ilustrează dispozitivul testat și se pot observa conexiunile USB ce conferă atât suportul necesar depanării aplicațiilor prin interfața JTAG încorporată pe platformă cât și accesul la interfața serială asincronă.

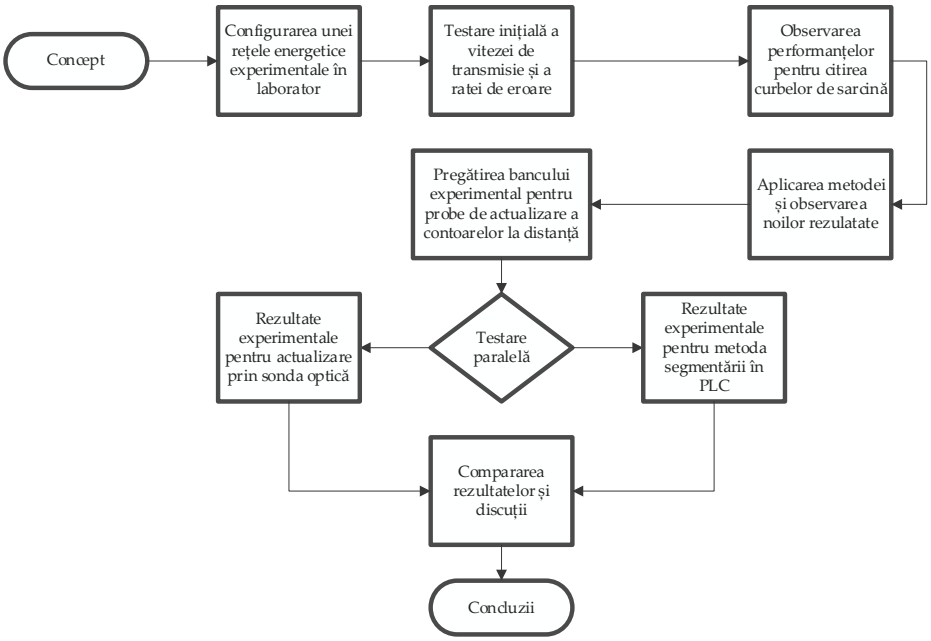

Fig. 5.3. - Diagrama de proces și metodele de evaluare a soluției propuse

O reprezentare a diagramei de proces și a metodelor de evaluare propuse este expusă în figura 5.3. Aceasta conține pașii urmați de-a lungul experimentelor, precum și o prezentare pe scurt a modului în care au fost analizate rezultatele experimentale.

5.3.1. Propuneri privind structura pachetelor

Pentru a putea implementa metoda de segmentare propusă fiecare bloc de date transmisie prin rețea este precedat de un antet generic. Așadar, fiecare pachet are două secțiuni, un antet și un corp de date. Antetul conferă detalii legate de protocolul specific rețelei în timp ce corpul conține datele transmise în format binar - acesta alcătuind marea majoritate din spațiul fiecărui pachet încapsulat pentru transmisie. În protocolul prezentat, corpul conține informații în format binar, iar antetul oferă suficiente informații pentru ca receptorul să poată procesa, valida și controla reconstrucția fișierului final. Acest lucru se realizează în mod obișnuit prin adăugarea unui identificator numeric de secvență și a numărului total de segmente așteptat în întregul proces de transmisie a unui fișier de date.

PRIME v1. 4.6 utilizat în contoarele inteligente implementate până în prezent folosește modulație diferențială cu una dintre cele trei variante posibile: DBPSK, DQPSK sau D8PSK. Dacă mediul canalului este bun și nu este necesară codificarea convoluțională a transmisei, protocolul poate suporta viteze de până la 47 Kbps, 94 Kbps și 141 Kbps respectiv. Tabelul 5.1 ilustrează viteza datelor brute teoretice suportate într-o rețea PRIME comună [227].

Tabelul 5.1. - Viteza de transmisie a datelor și parametrii pachetelor pentru diverse scheme de codificare.

Encoding	DBPSK	DBPSK	DQPSK	DQPSK	D8PSK	D8PSK
Convolutional Code (1/2)	On	Off	On	Off	On	Off
Raw data rate (Kbps approx.)	21.4	42.9	42.9	85.7	64.3	128.6
Maximum MSDU length with 63 symbols (in bits)	3016	6048	6040	12096	9064	18144
Maximum MSDU length with 63 symbols (in bytes)”	377	756	755	1512	1133	2268

Având în vedere faptul că ratele expuse mai sus sunt teoretice și pot fi atinse doar într-un mediu ideal, iar transmisia unor pachete de dimensiuni consistente vor fi fragmentate la nivelul fiecărui strat OSI ne așteptăm ca transmisia prin rețeaua PRIME a contoarelor inteligente folosite mai sus să aibă structura descrisă în tabelul 5.2:

Tabelul 5.2. - Corespondenți straturi de interconectare a sistemelor deschise (OSI) și sisteme smart grid.

Nivel OSI	Strat Smart Metering PLC
Application	Segmentare la nivel DLMS
Presentation	COSEM
Transport	TCP/UDP
Network	IPv6
Data Link & Phy	PLC PRIME

Modulația D8PSK fără cod convoluțional a fost aleasă pentru a obține cea mai ridicată viteză de transmisie prin PRIME cu un MSDU = 2268 octeți. Pentru a evita orice segmentare și reasamblare prin nivelul PRIME, trebuie să ne uităm la sub-stratul său comun de convergență a părților, CPCS. Funcționalitatea CPCS este responsabilă pentru divizarea datelor de ieșire în segmente constante ClMTU de 256 de octeți fiecare. PRIME 1.3.6 acceptă până la 64 de segmente ale ClMTUSize. Aceasta duce la o lungime maximă de transmisie de 16.384 de octeți, după care straturile superioare trebuie să gestioneze segmentarea și reasamblarea ulterioară. Segmentarea la nivel de aplicație va urma aceeași structură ca cea de la nivelul fizic PRIME, iar substratul comun de convergență a părților (CPCS) este descris în standardul R1.3.6 și urmărește același format cu cel descris în tabelul 5.3:

Tabelul 5.3. - Câmpurile și structura antetului de segmentare.

Denumire	Lungime	Descriere
Tip	2 bits	Tipul de segment. 0b00:primul segment; 0b01: segment intermediar; 0b10: ultimul segment; 0b11: rezervat
NSegs	N bits	Număr total de segmente – 1.
SEQ	N bits	Număr de secvență a segmentului curent.

Pentru a defini un număr N adecvat de segmente acceptate, ne vom uita la unul dintre cele mai comune transmisii eșuate în rețele inteligente PLC, care constă în citirea curbelor de sarcină a energiei consumate în ziua precedentă cu o rezoluție de 5 minute. Fiecare înregistrare din curba de sarcină constă în valori care acoperă atât energia electrică activă importată și exportată, cât și toate energiile reactive pe toate cele patru cadrane. Numărul maxim de contracte de tarifare suportate de contorul ST și numărul tarifelor acceptate de aplicația de contorizare are următoarele limitări: 6 contracte independente fiecare putând avea 16 scheme de tarifare distincte. Putem astfel calcula dimensiunea maximă a unei citiri complete de curbă de sarcină de la un punct de consum cu o configurație completă:

$$LoadProfileDaySize = NumTypesOfEnergyRegisters * RegisterSize * NumOfSupportedTariffs * NumOfSupportedContracts * MinTimeResolution$$

$$LoadProfileDaySize = 6 * 8\ bytes * 16 * 6 * 288$$

$$LoadProfileDaySize = \ 1327104\ bytes$$

$$NSegs_{min} = \ LoadProfileDaySize / \ \mathrm{ClMTUSize}_{*}$$

$$NSegs_{min} = 1327104\ bytes\ /\ 256\ \mathrm{bytes}$$

$$NSegs_{min} = \ 5184$$

Având în vedere cele de mai sus, un număr N = 16 biți va fi suficient, ducând la un consum de 34 biți pentru logica segmentării, iar pentru a obține cel mai mare randament, toate testele se execută folosind modulația și encodarea D8PSK cu cod convoluțional.

5.3.2. Definirea metodelor experimentale pentru descărcarea curbelor de sarcină prin noduri PRIME

Pentru evaluarea performanțelor obținute prin segmentarea curbelor de sarcină am simulat o clădire rezidențială folosind un data concentrator DLMS PLC PRIME prezentat anterior în figura 5.2, iar topologia desfășurată este cea descrisă în figura 5.1. Pentru a simula condițiile de comunicare precare întâlnite în teren în zonele care întâmpină tulburări ale calității energiei, am folosit echipamentul Integra GP 3050/3 ce poate furniza alimentarea cu sarcini simulate la nivelul contoarelor inteligente și poate oscila tensiunea de alimentare în intervalul 180-230V AC. Deoarece platforma de dezvoltarea aleasă nu dispune de funcționare pe baterie, sursa de alimentare de pe echipamentele de măsură inteligentă folosite, VIPER26H, poate menține active canalele de comunicație și procesorul principal chiar și în cazul unor goluri de tensiune. Într-o rețea problematică, golurile de tensiune sunt des întâlnite la nodurile aflate la o distanță mare de centrul de distribuție, iar scenariul evaluat va simula un gol de tensiune de 180V pe perioada comunicației. Tensiunea nominală a rețelei este 230V AC, iar la nivelul rețelei nu a fost aplicată intenționat nici o altă sursă de distorsiuni armonice și nici nu au existat alte echipamente conectate în apropierea sistemului experimental. În acest mediu, și folosind parametrii descriși mai sus, viteza teoretică ar putea ajunge la 128,6 kbps, dar dimensiunea înregistrărilor din curba de sarcină și zgomotul simulat în rețea au făcut ca pierderile de transmisie frecvente să facă nepractică această abordare. Folosind segmentarea datelor cu modelul propus anterior, transferurile de date au devenit fiabile, curbele de sarcină fiind transferate de la platforma contorului PLC-C PRIME înainte și înapoi la concentratorul PLC-A PRIME prin contorul PRIME PLC-B. După ce am ales o dimensiune a segmentelor conform mărimilor MTU din tabelul 5.2, următoarele teste au fost efectuate:

Test 1. Viteza inițială, cu accent pe viteza la care segmentele au avut nevoie de retransmisie în timpul unei transmisii normală a unei citiri zilnice a curbei de sarcină care are o dimensiune LoadProfileDaySize = 1.327.104 octeți.

Test 2. Test cu segmentarea datelor folosind citiri de curbă de sarcină zilnice configurate pentru un segment de date de dimensiune = 256 octeți. Această abordare împarte datele formatate în 5184 segmente.

5.3.3. Fezabilitatea actualizărilor de firmware prin comunicații PRIME bazate pe segmente de date

Având în vedere rezultatele preliminare obținute prin descărcarea curbelor de sarcină cu segmente de date, am luat în considerare impactul unei abordări similare într-o operațiune de descărcare de firmware la distanță, precum și într-o actualizare de firmware post-producție, pentru cazurile în care o actualizare prin PLC este mai convenabilă decât o actualizare manuală prin intermediul interfeței optice. Pentru aceste teste, a fost utilizat un contor generic bazat pe controllerul ST-COM pe care am comparat viteza de finalizare a procesului actualizare a firmware-ului prin PRIME cu segmente de date față de o descărcare convențională IEC 62056-1-0:2014 prin intermediul unei comunicări optice în infraroșu prin interfața izolată galvanic.

Testul ales este unul cu un singur nod de comunicație și nu adresează metodele și strategiile gândite pentru întreaga rețea de contorizare inteligentă prin optimizări la nivelul rutelor dintre noduri [229] și nu ia în considerare nici impactul adăugării de măsuri de securitate [230] în procesul general de actualizare, dar ambele vor fi luate în considerare pentru cercetări ulterioare.

Deoarece dispozitivele testate utilizează o memorie flash internă de 1 MB, va trebui să simulăm o actualizare completă care umple întreaga memorie, deoarece aceasta abordare acoperă și scenariul unei actualizări parțiale în cazul echipamentelor care acceptă funcții de separare legală a firmware-ului. Toate testele au fost executate în aceleași condiții descrise în iterațiile anterioare de încărcare a curbelor de sarcină, iar din etapele de actualizare a contoarelor inteligente, au fost luate în considerare doar etapele de transfer a imaginii nu și transferul între memoriile interne ale contorului. Etapele sunt: Etapa 1 – Citirea mărimii imaginii ce urmează să fie transferată, Etapa 2 – Inițializarea transferului, Etapa 3 – Transferul propriu-zis al segmentelor, așa cum sunt descrise și în [231].

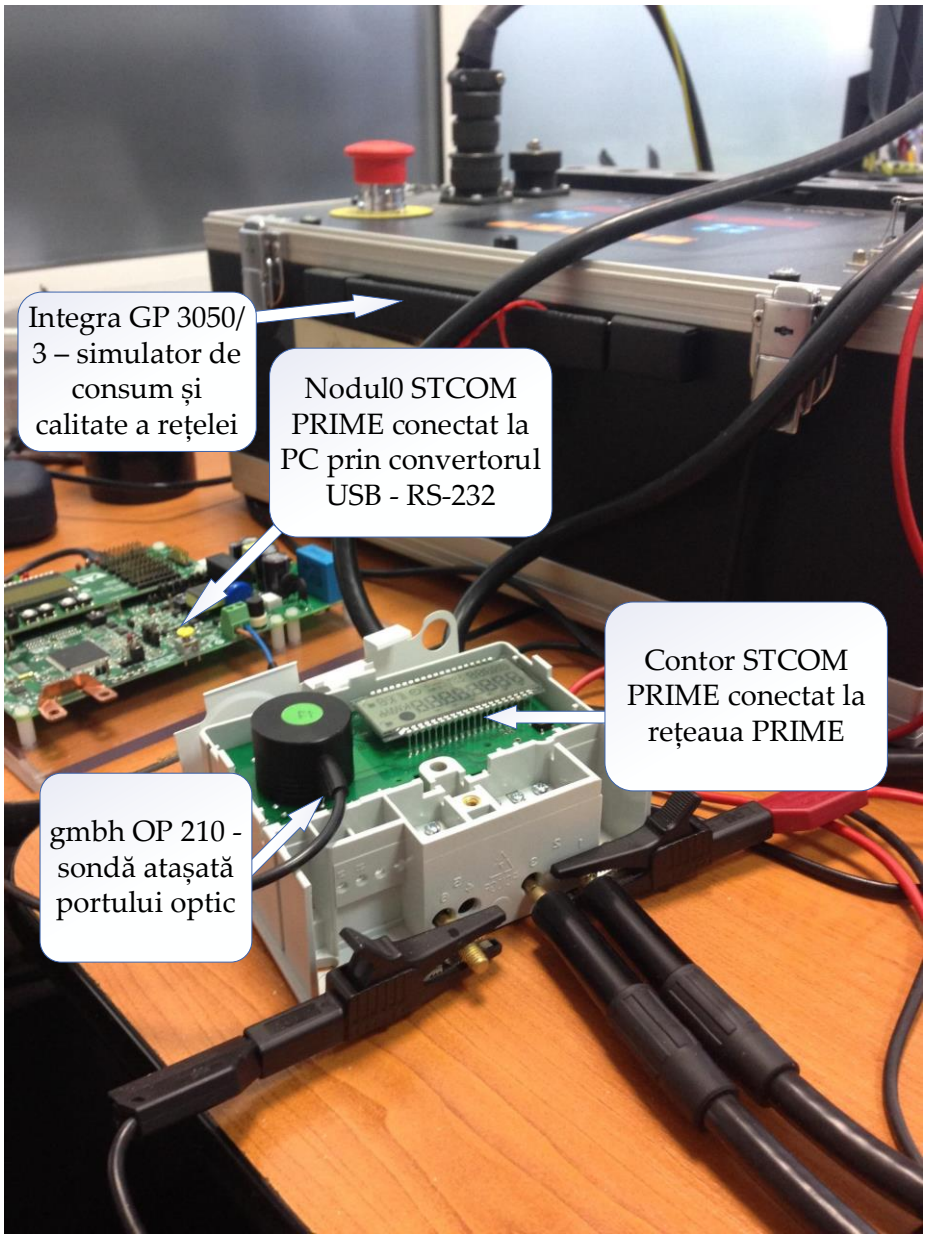

Fig. 5.4. - Contor inteligent ST-COM conectat concomitent la concentratorul PLC și la sonda optică.

Fig. 5.4 prezintă mediul de testare cu contorul PRIME conectat atât la un nod STCOM PRIME, cât și la o sondă optică. Transmisiunile optice au fost realizate prin intermediul protocolului standard COSEM IEC 62056-1-0:2014 utilizând o sondă

USB gmb - OP 210 la viteza sa maximă de 19200 biți/s. Nivelul de aplicație a rămas neschimbat și nu a fost modificat între testarea interfeței optice și, respectiv, a celei electrice.

5.4. Rezultate

După rularea comenzilor COSEM prin configurația descrisă în secțiunea anterioară, am adunat rezultate de la 10 citiri unice ale curbei de sarcină din același nod, prima dată fără a utiliza secționarea datelor și apoi cu segmente de 256 de octeți. De fiecare dată când protocoalele au semnalat pierderea unui pachet în transmisia PRIME, în instrumentul de monitorizare a fost marcată o reîncercare, care apoi marchează pachetul de date ca fiind un pachet ce nu a fost transmis la prima încercare. Acest lucru este important, deoarece pierderea de pachete este principala metrică pe care protocolul urmărește să o îmbunătățească, iar viteza de transmisie nu este esențială atunci când nodurile sunt oricum greu accesibile.

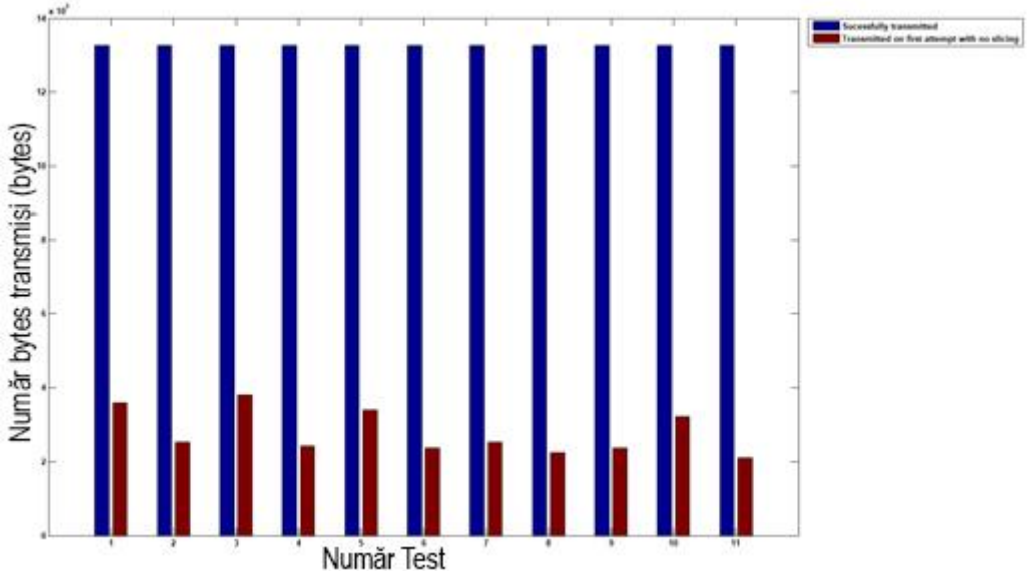

Fig. 5.5. - Rezultatele inițiale privind citirea curbei de sarcină zilnică prin PLC-PRIME de la PLC-A la PLC-C.

Înainte de a trece la testarea soluțiilor propuse, trebuie să măsurăm care sunt limitările rețelei la nivelul nodului 1. Fig. 5.5 arată că, în medie, 13% din curbele de sarcină citite au necesitat retransmiteri prin protocolul PLC lucru ce poate fi observat și printr-o scurtă analiză a capturilor PLC Wireshark. Așadar testul inițial dovedește că structura aleasă în mediul experimental prezintă probleme de disponibilitate, iar topologia din Fig. 5.1 poate fi utilizată în continuare pentru a analiza modul în care funcționează un dispozitiv cu disponibilitate redusă, precum cel din Nodul 2. Acest nod va fi modificat astfel încât programul de transmisie să

comunice cu segmente de date de dimensiuni egale cu *CIMTUSize,* adică mărimea maxim admisă la nivelul protocolului Prime.

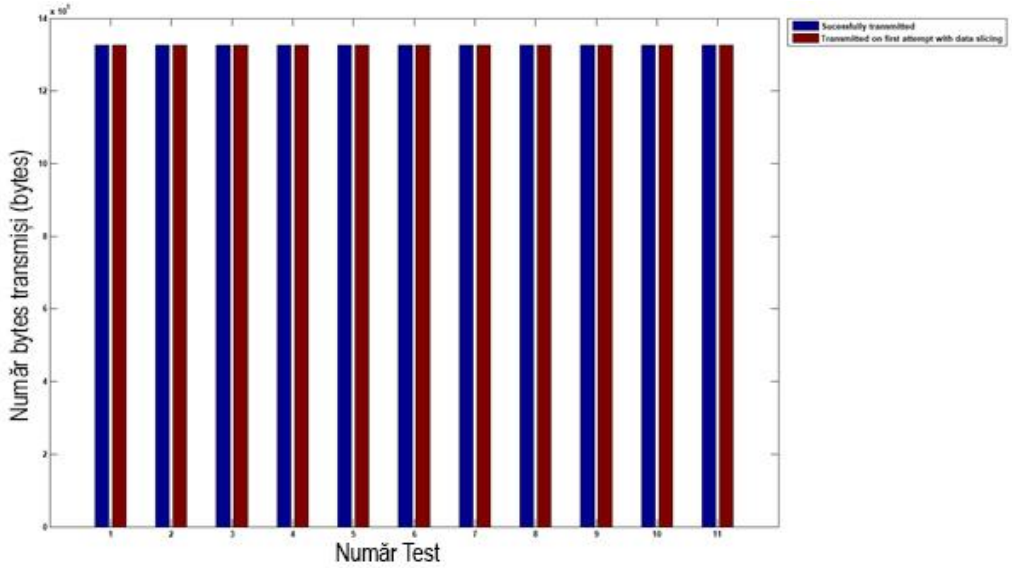

Fig. 5.6. - Transmiterea citirilor zilnice ale curbei de sarcină prin segmente limitate la nivel de aplicație.

În Fig. 5.6, datele au arătat că nu a fost necesară nicio retransmitere pe toată durata comunicării cu Nodul 2 în timpul comenzii de citire a curbelor de sarcină pe întreg parcursul celor zece iterații separate ale testului. Citirile curbelor de sarcină au ajuns cu succes la destinația vizată, fără pierderi de pachete iar, mai mult, fiecare segment a fost transmis în mod corespunzător într-o singură fereastră de transmisie, fără a fi necesare reîncercări sau retransmisii. Cu toate acestea, viteza de transmisie a scăzut semnificativ în timpul analizei noastre experimentale, prin urmare, acest aspect a fost analizat în etapele următoare. În figură se observă numărul transmisiilor egal cu numărul transmisiilor ce au ajuns cu succes la destinație din prima încercare de transmisie.

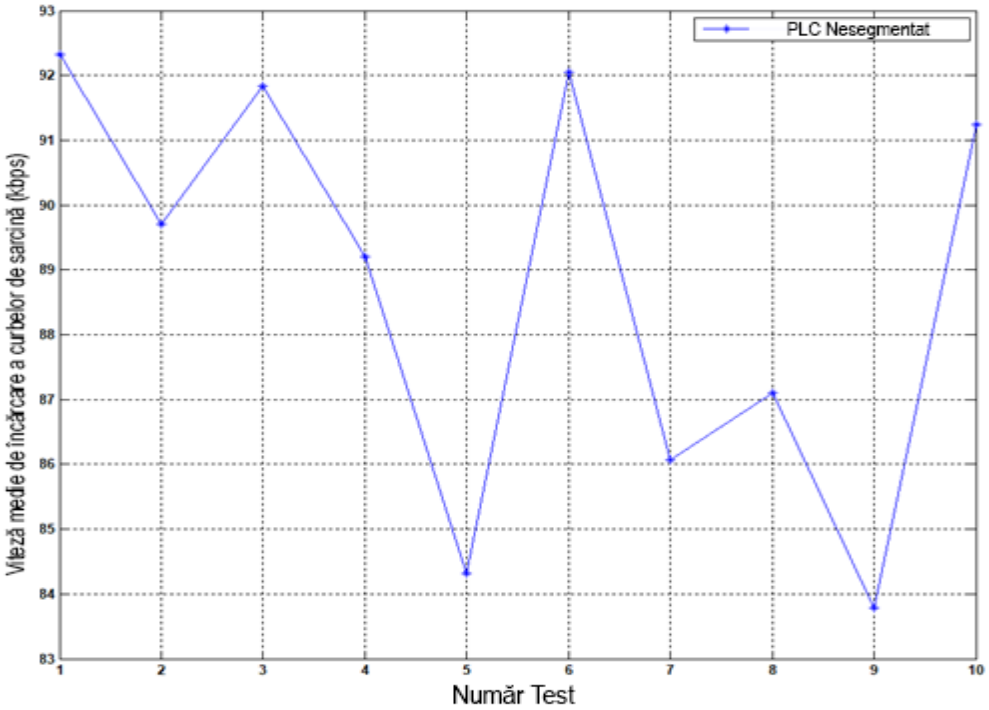

Fig. 5.7. - Viteze de transmisie observate pe un canal de comunicație PLC ce nu folosește segmentarea datelor la nivel de aplicație.

În figura 5.7 sunt prezentate rezultatele testelor vitezei de transmisie prin protocolul de comunicație PRIME fără segmentare, nod ce are o conexiune directă cu Nodul 2. Inițial viteza de transmisie s-a încadrat în intervalul [83 kbps, 93 kbps], ceea ce nu este neobișnuit pentru o rețea de linii de joasă tensiune ce nu suferă de interferențe sau de alte probleme de calitate a rețelei.

Având ca obiectiv o rețea ce necesită retransmisia pachetelor cât mai rar posibil și o comunicație cât mai apropiată de modul în care arăta o comunicație de date într-un mediu lipsit de interferențe, am analizat impactul soluției cu segmente de date care îmbunătățește semnificativ disponibilitatea rețelei, dar cu o viteză vizibil mai mică în comparație cu protocoalele standardizate. În cazul dispozitivelor care ar rămâne pentru o perioadă mai lungă de timp la un nivel de disponibilitate de 0%, viteza de transmisie nu este o problemă imediată, deoarece aceste dispozitive ar fi oricum inaccesibile pentru o perioadă lungă de timp.

În cele din urmă, Fig. 5.8 arată costul plătit pentru a crește disponibilitatea rețelei, viteza de transmisie a scăzut de la o valoare medie de 88,761 kbps la 6,763 kbps, permițând transmiterea unei curbe de sarcină, în formatul cel mai complex, pentru întreaga perioadă a unei zile, în aproximativ 20 de minute.

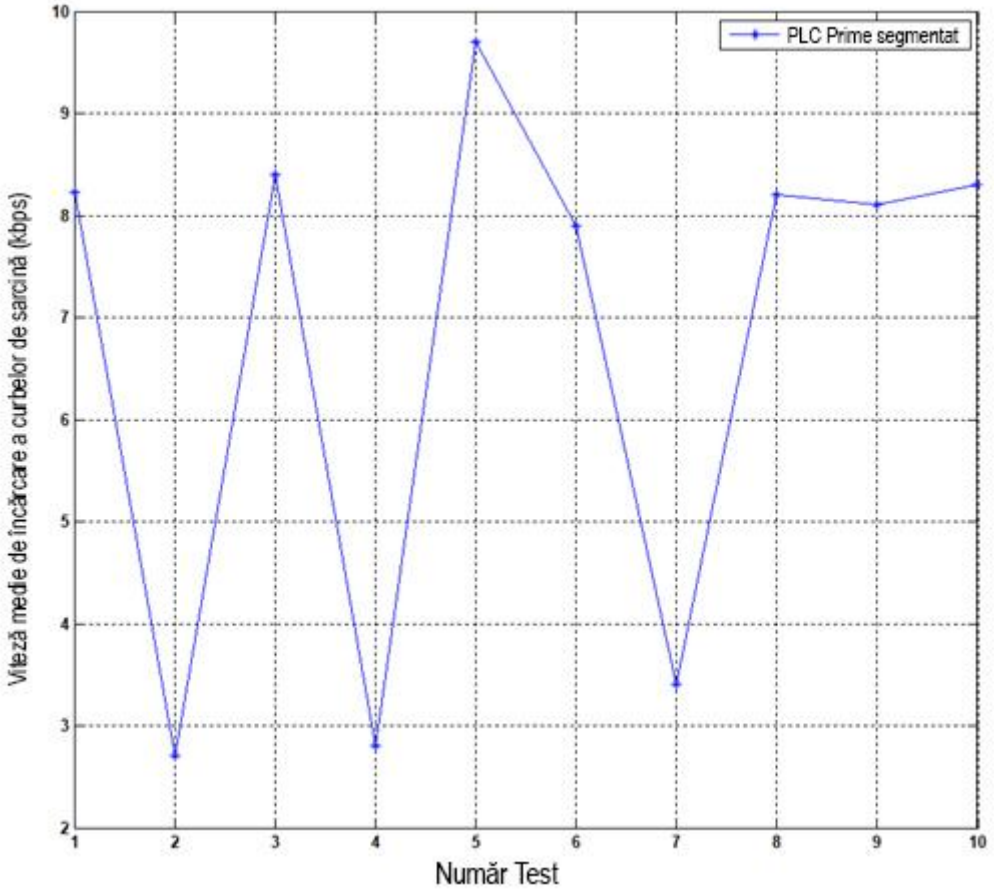

Fig. 5.8. - Viteze de transmisie observate pe canalul de comunicație de la PLC-A către PLC-C folosind segmentarea datelor la nivel de aplicație.

Viteza de transmisie obținută prin menținerea gestionării segmentelor de comunicare de către așa-numita aplicație de segmentare a datelor este suficientă pentru a se realiza suficiente transmisii reușite de la contoarele inteligente către furnizori, iar furnizorul de energie va dispune astfel de suficiente date din curbele de sarcină pentru a putea construi o schemă tarifară optimizată pentru fiecare client. Totodată, ne așteptăm ca facturarea să poată fi si ea automatizată chiar și pentru dispozitivele ce nu reușeau să comunice, deoarece curbele de sarcină reprezintă împreună cu imaginile pentru actualizările de software, cele mai mari bucăți de informații care trebuie să călătorească prin întreaga rețea Prime. Aplicația trebuie să fie capabilă să se adapteze și să recurgă la acest mod de comunicație ori de câte ori este necesar, acesta putând fi un mecanism de siguranță pe care nodurile s-ar putea baza în ultimă instanță după ce un număr de transmisii clasice au eșuat.

Mergând mai departe, trebuie să analizăm dacă această metodă de segmentare este potrivită pentru actualizările de firmware, deoarece studiile de securitate efectuate de Baumeister [212] și Asghar [213] indică faptul că procesul de actualizare este cel mai critic pas într-o rețea de contoare inteligente. Deoarece dispozitivele fără disponibilitate sunt de obicei actualizate manual de către un operator pe teren, la locul unde este instalat contorul inteligent, am comparat procesul de actualizare în rețea cu o actualizare manuală prin intermediul interfeței sondei optice. În cazul în care această metodă obține rezultate similare, înseamnă că nodurile neactualizate care au fost lăsate nesecurizate în rețea vor putea primi un nou firmware care să conțină actualizări de securitate, precum și funcționalități noi.

Tabelul 5.4. - Rezultatele testelor de viteza de actualizare a firmware-ului pentru fișiere de 1 MB prin intermediul comunicației optice respectiv al comunicării prin PLC PRIME.

Test	Optic (bps)	Optic (kbps)	PLC segmente (bps)	PLC segmente (kbps)
1	17622	17.21	6813	6.65
2	12978	12.67	7624	7.45
3	17300	16.89	4301	4.20
4	17313	16.91	8016	7.83
5	15566	15.20	9933	9.70
6	17091	16.69	8670	8.47
7	15893	15.52	10079	9.84
8	14091	13.76	6142	6.00
9	13276	12.96	8201	8.01
10	12738	12.44	6787	6.63
11	15369	15.01	6311	6.16
12	14977	14.63	9926	9.69
13	13064	12.76	8959	8.75
14	13458	13.14	10287	10.05
15	17860	17.44	9851	9.62
16	13827	13.50	7223	7.05
17	15302	14.94	9774	9.54
18	15062	14.71	4968	4.85
19	14129	13.80	9932	9.70
20	12904	12.60	5680	5.55
21	18152	17.73	3987	3.89
22	15318	14.96	10131	9.89
23	14678	14.33	8379	8.18
24	14550	14.21	4076	3.98
25	12783	12.48	7966	7.78
26	12912	12.61	5866	5.73
27	18391	17.96	5222	5.10
28	13046	12.74	7469	7.29
29	13565	13.25	10098	9.86
30	17274	16.87	10411	10.17

Tabelul 5.4 prezintă iterația experimentală a descărcării fișierului de imagine firmware de 1 MB prin PRIME, prin comunicarea prin linia electrică, precum și vitezele obținute de interfața optică pentru același fișier. În timpul testelor ilustrate în tabelul 5.4, viteza medie de descărcare a actualizării firmware-ului prin intermediul interfeței optice a fost de 15016,3 bps (14,66 kbps), în timp ce prin abordarea PLC cu segmentare de date s-a obținut o viteză medie de 7769,4 bps (7,59 kbps).

O comparație vizuală a vitezelor este reprezentată în figura 5.9, în timp ce aceasta arată că interfața optică funcționează la viteze ușor mai bune, am arătat că abordarea prin segmentare de date este încă o soluție viabilă, cu viteze într-un interval de valori similar.

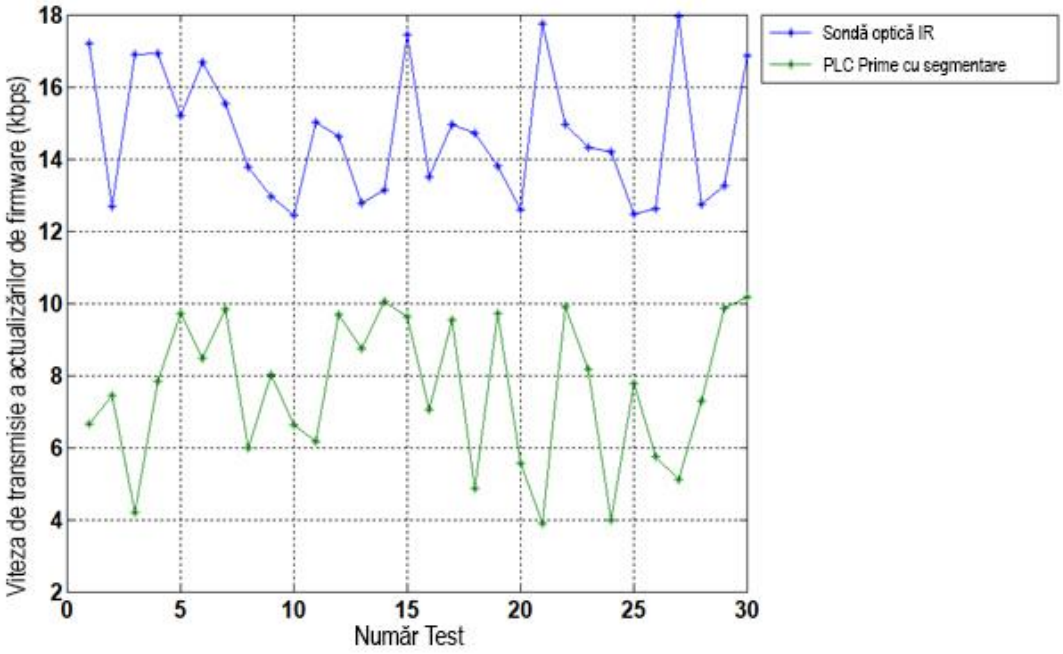

Fig. 5.9. - Reprezentarea vizuală a rezultatelor testelor de viteză de actualizare a firmware-ului pentru fișiere de 1 MB prin intermediul comunicațiilor optice și a celor cu PLC PRIME cu segmente de date.

După cum o arată și rezultatele prezentate anterior, prin reducerea segmentelor transmise într-o anumită fereastră de timp, am arătat că rata de retransmisie a fost redusă semnificativ, iar comunicarea PLC cu segmente de date poate îmbunătăți disponibilitatea prin transmiterea a cel puțin un segment de la contorul inteligent vizat ori de câte ori există o scurtă fereastră de disponibilitate. În plus, procesul de actualizare a firmware-ului poate atinge în continuare viteze comparabile cu aceeași operațiune efectuată manual de un operator din teren, fără costurile de logistică pe care le implică această metodă. Acest lucru înseamnă că nodurile care se află la capătul rețelei într-o rețea PRIME pot fi actualizate și nu mai sunt lăsate nesecurizate din cauza imposibilității de a obține o actualizare completă în aceeași fereastră de disponibilitate.

Tabelul 5.5. - Analiza statistică a măsurătorilor de testare a debitului.

Interfață de măsurare	Media (kbps)	Deviație	Varianță Eșantion	Coeficientul de variație	Interval de încredere (95%)
Optic	14.66	1.804	3.2632	0.1231	de la 14.01 la 15.31
Date feliate PRIME PLC	7.59	2.024	4.0864	0.2664	6,86 până la 8,31

Tabelul 5.5 prezintă o analiză statistică a datelor experimentale și evidențiază o viteză medie de 7,59 kbps pentru dispozitivele PRIME cu segmente de date, având o abatere standard a eșantioanelor de 2,02 și un interval de încredere (95%) între 6,86 kbps și 8,31 kbps.

De asemenea viteza de descărcare a actualizărilor software este comparabilă cu o actualizare manuală efectuată de un operator din teren prin intermediul unei sonde optice izolate galvanic, ceea ce face ca o abordare de actualizare prin PLC să fie mai apropiată de nevoile actuale ale industriei.

Comparația acestei abordări cu soluțiile specializate analizate în literatura de specialitate în [232] subliniază faptul că orice tehnologie care îmbunătățește disponibilitatea generală face ca rețeaua inteligentă să fie mai performantă și mai sigură, iar întrucât niciun sistem nu poate fi mai sigur decât veriga sa cea mai slabă, prin adăugarea mai multor abordări în setul de instrumente disponibil echipamentelor pentru contorizarea inteligentă se poate garanta, în cele din urmă, o soluție cât mai completă.

Diferite tipuri de topologii ale rețelelor smart includ inclusiv tehnologii radio care prin diferite protocoale concurează pentru lățimea de bandă disponibilă lucru ce poate afecta disponibilitatea întregului sistem pe termen lung [233], dar în prezent, există puține standarde care să acopere mai mult de un singur tip de comunicație în cadrul rețelei inteligente. Implementarea unui model ce folosește segmente de date la nivelul aplicației sau a unuia similar poate fi abordată în prezent doar de anumiți producători, iar coexistența unor contoare de la producători diferiți în rețeaua inteligentă nu poate funcționa într-un mod complet standardizat. Standardele trebuie să devină mai flexibile, permițând ca noile tehnologii să fie implementate la nivelurile OSI inferioare, în loc ca producătorii să se bazeze pe implementări software la nivel de aplicație. În cele din urmă, o rețea inteligentă care poate beneficia de toate avantajele diferitelor tipuri de transmisii de date poate crea o soluție hibridă în care o rețea de tip mesh poate beneficia de mici îmbunătățiri, cum ar fi cea prezentată mai sus, pentru a crea protocoale de comunicații mai cuprinzătoare cu cât mai multe noduri sau cu mai multe straturi de comunicație, cum ar fi cele prezentate în [229] și [234].

5.5. Concluzii parțiale și contribuții

Acest capitol propune o metodă de creștere a disponibilității contoarelor inteligente conectate prin intermediul protocolului de comunicare prin linii electrice PRIME. Prin creșterea disponibilității, furnizorii de energie electrică pot ajunge la un număr mai mare de contoare inteligente, iar profilurile de consum de energie, cum ar fi curbele de sarcină zilnică, pot fi colectate într-un mod fiabil și robust, dar, mai important, contoarele inteligente care rareori păstrează o conexiune de date solidă cu distribuitorul de energie pot fi acum actualizate de la distanță, contoarele primind actualizări de securitate în timp util îmbunătățind astfel securitatea întregii rețele de contorizare inteligentă. Acest lucru înseamnă că în locații îndepărtate cu conectivitate slabă la rețelele de date se pot evita operațiunile de actualizare manuală sau cazurile unde fiecare echipament de contorizare inteligentă trebuie vizitat în teren pentru citirea manuală a consumurilor de energie. Această îmbunătățire poate duce la costuri de întreținere mai mici de care pot beneficia atât furnizorii de energie, cât și utilizatorii finali.

Rezultatele testelor experimentale efectuate pe contoare inteligente care utilizează modelul descris mai sus au dovedit că abordarea funcționează corect în mediile cu disponibilitate redusă, iar prin utilizarea segmentării datelor la nivel de aplicație folosind modelul propus, transferurile de date au devenit mai stabile, fără a mai fi nevoie de încercări de retransmitere. În plus, dispozitivele instalate în cadrul unei rețele afectate de interferențe au înregistrat o creștere notabilă a ratei de transmitere cu succes a curbelor de sarcină, precum și o creștere a ratelor de succes pentru actualizarea firmware-ului la distanță.

Având în vedere necesitatea unei rețele de distribuție electrică mai sigure, conceptul de îmbunătățire a metodologiilor de actualizare a firmware-ului pentru echipamentele de contorizare inteligentă este un subiect cheie care trebuie urmărit în cadrul viitoarelor lucrări de cercetare. O altă abordare dezirabilă ar fi îmbunătățirea disponibilității în cazul contoarelor inteligente care beneficiază de mai multe medii fizice de transmisie a comunicațiilor și modul în care acestea pot fi îmbinate pentru a obține rețele de contorizare inteligentă hibridă prin intermediul unei metode de fuziune a rețelelor de date.

La o scară mai mare, tehnologiile alese pentru implementarea la nivel național ar trebui să fie bine analizate înainte de a impune o soluție unică pentru întreaga industrie, iar actorii trebuie să aibă o strategie comună pentru a depăși provocările fizice întâlnite în teren. Toate implementările din țările analizate au obținut acoperirea a unei bune părți din utilizatorii casnici prin intermediul contoarelor inteligente, dar această acoperire poate fi îmbunătățită mai departe prin intermediul actualizărilor software, precum și a noilor tehnologii care se pot îmbina cu cele existente, păstrând un cost unitar eficient și conferind totodată o experiență de utilizare îmbunătățită pentru fiecare gospodărie. În cele din urmă, companiile de electricitate și producătorii de contoare inteligente nu pot rezolva singuri problemele, iar cercetările în vederea unei standardizări a protocoalelor trebuie să continue. Prin îmbinarea abordărilor actuale cu alte îmbunătățiri, cum ar fi cea prezentată în acest capitol, se poate crea, prin actualizarea software-ului de la distanță și citirea automată a contoarelor, o rețea de contorizare inteligentă mai sigură, cu dispozitive cu disponibilitate ridicată și costuri de întreținere reduse,

permițând implicit utilizatorilor să aibă un firmware personalizat care să se potrivească formatului de consum de energie din fiecare gospodărie.

6. CONSIDERAȚII PRIVIND MĂSURAREA NIVELULUI SEMNALULUI ÎN REȚELELE DE CONTORIZARE FĂRĂ FIR PENTRU ESTIMAREA POZIȚIEI NODURILOR

6.1. Introducere

Rețelele de senzori fără fir (WSN) sunt utilizate pe scară largă în diferite sisteme de monitorizare inclusiv în sistemele de contorizare si monitorizare a consumului de energie. Având în vedere natura distribuită a acestor rețele, un număr tot mai mare de studii de cercetare se concentrează asupra unor aspecte importante precum: maximizarea autonomiei rețelei, localizarea nodurilor și securitatea accesului la date. Algoritmii de localizare a nodurilor și de estimare a distanței au ca punct de plecare diferite informații furnizate de noduri, iar nivelul intensității semnalului este adesea un astfel de punct de plecare. În acest capitol a fost proiectat, implementat și testat un sistem de achiziție a indicatorului de intensitate a semnalului recepționat (RSSI). De asemenea, au fost efectuate experimente în diferite medii de operare pentru a arăta variația indicatorului de intensitate a semnalului recepționat (RSSI) în funcție de distanță și de orientarea geometrică a nodurilor precum și a mediului, atât în interior, cât și în exterior. Algoritmii de transmitere a datelor cu consum redus de energie ajustează puterea consumată de noduri în funcție de distanța relativă dintre noduri. Au fost efectuate experimente pentru a măsura curentul consumat de nod în funcție de puterea de transmisie ajustată. Pentru a utiliza valorile RSSI ca date de intrare pentru algoritmi de detectare a distanței sau a locației, acestea nu pot fi utilizate fără etape intermediare de procesare pentru a atenua neliniaritatea valorilor măsurate. Rezultatele măsurătorilor au confirmat că nivelul RSSI variază în funcție de distanță, de orientarea geometrică a senzorilor precum și în funcție de caracteristicile mediului.

Indicatorul de intensitate a semnalului recepționat (RSSI) reprezintă o măsură a puterii semnalului dintr-o legătură radio între două noduri ale rețelei. Într-o legătura radio, calitatea transmisiei poate fi afectată de mai mulți parametri de canal, cunoscuți și sub numele de condiții de canal, care determină variații ale nivelului RSSI, cum ar fi distanța dintre noduri, mediul de transmisie radio (de exemplu, aer, apă), obstacolele fizice, orientarea geometrică a nodurilor și interferențele cu alte echipamente de transmisie radio și undele radio reflectate. Având în vedere această sensibilitate la diverși parametri, RSSI este ales pe scară largă de către industrie pentru estimarea distanței, localizarea nodurilor, detectarea mișcărilor [235], precum și pentru algoritmi de urmărire și mecanisme de securitate (de exemplu, detectarea intrușilor), ca în [236].

Rețelele de senzori fără fir trec încet de la mediile academice și industriale la viața de zi cu zi tot mai des, de la rețelele energetice inteligente, monitorizarea urbană, dezvoltarea durabilă [237] și, în cele din urmă, în casele inteligente ca dispozitive Internet of Things [238]. Aceste medii sunt predispuse la diferite interferențe și fiecare factor de ambianță trebuie tratat separat. În plus, impactul mediului radio asupra factorului RSSI [239, 240], prin variații ale temperaturii și a umidității [241] trebuie să fie luate în considerare în special în cazul rețelelor WSN cu o distanță mare între noduri cum sunt de exemplu rețelele de contorizare inteligentă bazate pe tehnologii radio. În cele din urmă, trebuie amintit și faptul că monitorizarea configurațiilor de calitate a serviciilor, QoS [242] în aceste procese a devenit o parte esențială a soluțiilor bazate pe RSSI. Împreună cu considerațiile de mediu de mai sus, acești factori au stabilit, în rețelele WSN, metode de localizare fiabile și bine fundamentate atât în sistemele bidimensionale, cât și în cele tridimensionale [243].

În ciuda lipsei de precizie, factorul RSSI este utilizat pe scară largă în prezent în majoritatea algoritmilor de localizare în rețelele de tip WSN [244]. O analiză cuprinzătoare a principiilor și tehnicilor de bază utilizate în algoritmii de localizare, a categoriilor acestor algoritmi și a schemelor de localizare a fost abordată în [245,246]. Deși aceste metode sunt afectate de subiectul prezentei lucrări, ele nu au fost analizate comparativ și nici nu au fost detaliate pe parcursul studiului făcând parte din planul unor cercetări ulterioare.

Noi scheme de calibrare și soluții de filtrare au fost dezvoltate în ultimii ani, iar o nouă metodă descrisă în [247] se concentrează pe localizarea din rețelele WSN a surselor radio cu rază lungă de acțiune, utilizând o metodă cu o complexitate de calcul redusă totodată atingând o precizie ridicată în condiții de zgomot alb gaussian. De asemenea, în [248] este propus un algoritm cu o precizie ridicată de localizare atunci când raportul semnal/zgomot este ridicat, această metodă poate îmbunătăți precizia fără a fi necesară modificarea hardware-ului de bază de asemenea un lucru de interes pentru rețelele de contorizare inteligentă cu echipamente deja instalate în teren. Modelele propuse anterior pe baza soluțiilor de reducere a zgomotului Bayesian sau a filtrului de particule [249] sunt încă costisitoare din punct de vedere computațional și nu sunt întotdeauna potrivite pentru mediile interioare [250, 251].

Prima problemă într-o aplicație cu noduri de senzori este localizarea sau estimarea poziției acestora. Conceptele de bază ale estimării locației pornesc de la ipoteza că există un nod central, numit și stație de bază, și noduri suplimentare fixe sau mobile care comunică cu stația de bază și iau măsurători ale diferiților parametri, cum ar fi RSSI, unghiul de sosire (AoA), timpul de sosire (ToA) și diferența de timp de sosire (TDoA), așa cum este descris în [252]. O analiză comparativă a acestor parametri este documentată în [253].

În circumstanțe ideale, numite și modelul spațiului liber, relația dintre atenuarea semnalului și distanță poate fi exprimată prin (6.1), conform [254], care descrie cu o precizie limitată atenuarea semnalului pe traseu, bazată doar pe distanță și frecvență.

$$PL(d_0) = -32.44 - 20\log(f_c) - 20\log(d_0), <dB> \quad (6.1)$$

PL reprezintă atenuarea sau pierderea puterii semnalului radio pe parcursul unui traseu, f_c - frecvența centrală și d_0 - distanța dintre noduri. În afară de RSSI,

celelalte măsurători sunt mai dificil de realizat, deoarece necesită componente hardware specializate care, de obicei, nu se găsesc în cazul senzorilor fără fir din cauza constrângerilor de proiectare, a constrângerilor de cost și a eforturilor de miniaturizare. Mecanismele de măsurare RSSI sunt în prezent caracteristici comune integrate în chip-urile emițătoarelor-receptoarelor radio, ceea ce face din RSSI o soluție tehnică accesibilă. Cu toate acestea, măsurătorile RSSI sunt foarte sensibile la schimbările de mediu și necesită adesea procese de calibrare intensive, atât offline cât și online, așa cum este descris în [255].

O a doua problemă în rețelele fără fir este estimarea distanței dintre noduri pentru a crește eficiența energetică a rețelei. Rețelele de senzori fără fir eficiente din punct de vedere energetic sunt caracterizate de o autonomie sporită dată de consumul redus de energie și de mecanisme auxiliare de colectare a energiei. Într-un sistem tradițional, un senzor fără fir este alimentat de baterii sau acumulatori ca sursă principală de energie. Fiecare senzor fără fir include următoarele patru blocuri principale: bloc emițător-receptor radio, unitate de procesare (de obicei un microcontroler), circuite de achiziție și filtrare a semnalelor și un etaj de ieșire (pentru controlul local al procesului).

Pentru a minimiza consumul de energie al microcontrolerului, se pot aplica diferite tehnici, de obicei activarea modurilor de tip *sleep* sau alte moduri de reducere a consumului de energie, reducerea frecvenței de operare și oprirea perifericelor neutilizate. Moduri similare de reducere a consumului de energie pot fi activate pentru emițătorul-receptor radio, care poate ajusta, de asemenea, puterea de transmisie, reducând astfel consumul de curent.

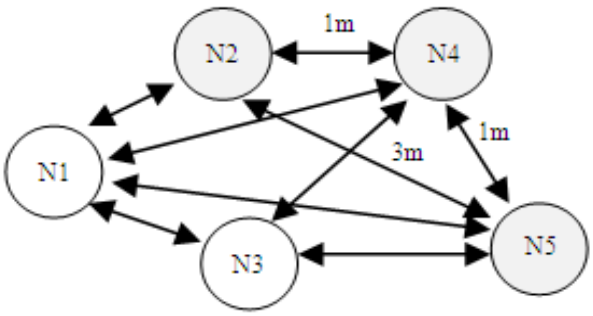

Fig. 6.1. - Exemplu de rețea de senzori fără fir cu distanțe diferite.

În figura 6.1, este reprezentat un exemplu de rețea de senzori fără fir de mici dimensiuni, cu diferite distanțe între nodurile rețelei. Pornind de la un tabel de interpolare construit pe baza informațiilor RSSI, disponibil la momentul execuției programului, care arată puterea necesară pentru a transmite un pachet pe o distanță dată, sunt posibile următoarele scenarii de reducere a consumului de energie:

Nodul N2 transmite un pachet către nodul N5 cu un anumit nivel de putere (L5), fiind capabil să ajungă la nodul N5 situat la 3 m distanță.

Nodul N2 transmite un pachet către nodul N4 cu un anumit nivel de putere (L4), unde L4 < L5, fiind capabil să ajungă la nodul N4 situat la numai 1 metru

distanță. În acest fel, deducem că este posibilă ajustarea dinamică a puterii de transmisie.

În plus, dacă autonomia întregii rețele este critică, transmisiile cu un singur salt care necesită un consum de energie mai mare pot fi înlocuite cu transmisii multi-salt pe baza unui algoritm de maximizare a autonomiei rețelei.

Cu toate acestea, sistemele de rețele de noduri fără fir sunt scalabile între anumite limite, impuse pe de o parte de spațiul de adresare (numărul de octeți disponibili), iar pe de altă parte de algoritmii de detectare și localizare a nodurilor pentru a restabili rețeaua, atunci când un nod dispare (semnalul de la acesta este prea mic).

Capitolul curent arată că, folosind o configurație simplă, se pot efectua măsurători care validează (nod cu nod) o arhitectură de rețea de senzori fără fir, totodată luând în considerare o operațiune prin care se permite, de fapt, testarea scalabilității hardware și implicit a stabilității algoritmilor software, adică a limitelor bunei funcționări a unei rețele date. Prin cercetările efectuate, se recomandă efectuarea de măsurători de semnal, la fața locului, atunci când se are în vedere extinderea ariei rețelei de senzori sau scalarea numărului de senzori. În lucrare sunt prezentate aspecte legate de măsurătorile nivelului semnalului (utilizând RSSI) atunci când tensiunea de alimentare a nodurilor și orientarea senzorilor (în aceeași locație) nu rămân întotdeauna aceleași.

6.2. Materiale și metode experimentale pentru studiul indicatorilor de semnal

Rezultatele și experimentele prezentate în lucrare sunt utile pentru realizarea a cel puțin două aplicații precum urmează:

- un sistem de identificare a poziției contoarelor inteligente pe teren sau a consumatorilor casnici într-o locuință dotată cu senzori inteligenți/prize inteligente.
- un sistem de citire a consumului de energie de la fiecare dintre apartamentele de pe scara unei clădiri cu mai multe niveluri.

Arhitectura ambelor aplicații se bazează pe un nod principal și mai multe noduri secundare fixe sau mobile. Între noduri, în diferite variante, se stabilesc legături. Legătura poate fi afectată de mai mulți parametri de canal, cunoscuți și sub numele de condiții de canal, care determină variații ale nivelului RSSI.

În această lucrare, a fost proiectat, implementat și testat un sistem de achiziție RSSI pentru a utiliza această măsură ca un set de date de intrare pentru dezvoltarea viitoare a algoritmilor de estimare a distanței și a locației contoarelor inteligente. Scopul sistemului este de a permite utilizatorului să măsoare nivelurile RSSI între nodurile active din sistem și în ambele direcții de transmisie. Adică, înțelegem prin aceasta că este interesant nu numai să se măsoare nivelul RSSI pentru o transmisie între nodul N2 și nodul N4 (din figura 6.1), ci și pentru o transmisie între nodul N4 și nodul N2. Acest aspect a fost luat în considerare pentru situațiile în care cele două măsurători ar fi diferite, deoarece parametrii senzorilor fără fir sunt diferiți pentru operațiuni de transmisie față de parametrii folosiți în

operațiunile de recepție. Două exemple de astfel de parametri sunt nivelul puterii de transmisie și tensiunea de alimentare.

Având în vedere sistemul din figura 6.1, nodul N1 este nodul central, iar nodurile N2, N3, N4 și N5 sunt noduri la distanță. Sistemul trebuie să fie capabil să măsoare distanța de la nodul central la fiecare nod secundar plasat la o anumită distanță, dar și între oricare alte două noduri secundare. Diferența dintre nodurile centrale și cele aflate la distanță constă în faptul că nodul central are o conexiune UART (Universal Asynchronous Receiver/Transmitter) cu un alt dispozitiv, în acest caz, un PC (Personal Computer). Această legătură de comunicare prin cablu este utilizată pentru a declanșa comenzi și pentru a colecta date din rețeaua fără fir cu ajutorul unei interfețe de utilizator desktop dedicate.

În afară de nivelul puterii de emisie și de nivelul tensiunii de alimentare, direcția în care este trimis/recepționat semnalul influențează foarte mult calitatea comunicării. Experimentele prezentate în lucrare evidențiază importanța acesteia, în special pentru aplicațiile bazate pe noduri mobile.

6.2.1 Descrierea sistemului cu noduri radio mobile

Figura 6.2 descrie arhitectura sistemului de măsurare și achiziție a datelor. Sistemul are n noduri notate cu nodul 0, ... , Nod n, iar Nodul 0 comunică cu un PC prin intermediul unei interfețe RS232. Nodurile N1, N2, ... , Nn, sunt noduri mobile care vor putea fi amplasate în diferite puncte din zona/clădirea în care se efectuează experimentele. Configurația noastră experimentală a utilizat nodul principal (N0) și, succesiv, un nod mobil pentru a efectua măsurătorile. Nodul mobil este plasat în poziția și cu orientarea dorită. Am procedat astfel pentru a avea rezultate pentru același nod în diferite poziții/locații conferind suportul necesar studierii comportamentului unui nod. Bineînțeles, prin utilizarea tuturor nodurilor se pot face determinări asupra întregii rețele de senzori. Deși sistemul este distribuit fizic, accesul la datele din rețea se face prin intermediul unui nod central, Nodul 0.

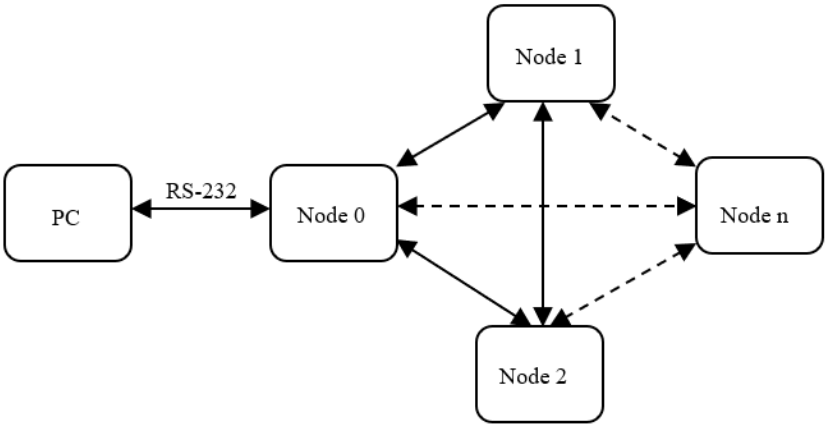

Fig. 6.2. - Arhitectura sistemului de măsurare a indicatorului de intensitate a semnalului recepționat (RSSI).

Senzorii fără fir utilizați în sistem sunt eZ430-RF2500T de la Texas Instruments. Aceștia sunt construiți în jurul unui microcontroler cu consum redus de energie, derivatul MSP430F2274, de la Texas Instruments și a unui transceiver de 2,4 GHz cu consum redus de energie, CC2500 de la Chipcon. Senzorul este alimentat de un pachet de baterii de 3 V (2 baterii AAA de 1,5 V). Nodul fără fir fiind prezentat în figura 6.3.

Fig. 6.3. - Nodul fără fir eZ430-RF2500T.

Nodul are o antenă radio încorporată, LED-uri, pini de intrare-ieșire digitală și o interfață de programare/depanare, oferind posibilități de extindere. Frecvența de funcționare a microcontrolerului este de 1 MHz. CC2500 este un emițător-receptor de 2400-2483,5 MHz care funcționează în banda ISM, cu o viteză de transmisie a datelor programabilă între 1,2-500 kBaud, un nivel de putere de transmisie programabil și ieșiri digitale RSSI și LQI (Link Quality Indication), conform descrierii din [255].

6.2.2 Protocolul de comunicație propus

Au fost implementate două protocoale de comunicație similare. Unul se ocupă de comunicarea prin cablu pe interfața RS232 între PC și nodul central, iar celălalt se ocupă de comunicarea fără fir între nodurile ce comunică wireless.

Protocoalele se bazează pe următoarele telegrame.
(a) Telegrama de control
(b) Telegrama de răspuns

Figura 6.4 descrie structura telegramei de control.

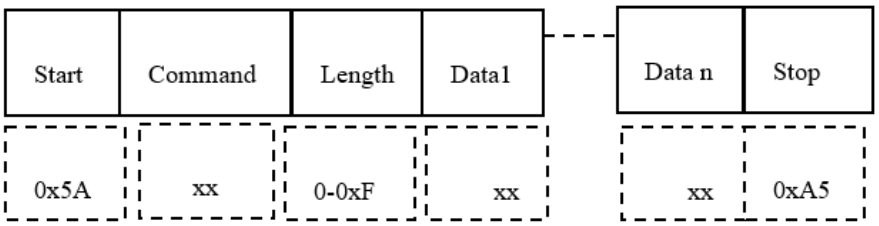

Fig. 6.4. - Structura unei telegrame de control.

Observăm octetul de start, apoi octetul de comandă, urmat de lungimea câmpului de date (octeți), de octeții de date (Data 0, ..., Data n) și de octetul de oprire.

În continuare, figura 6.5 descrie structura telegramei de răspuns.

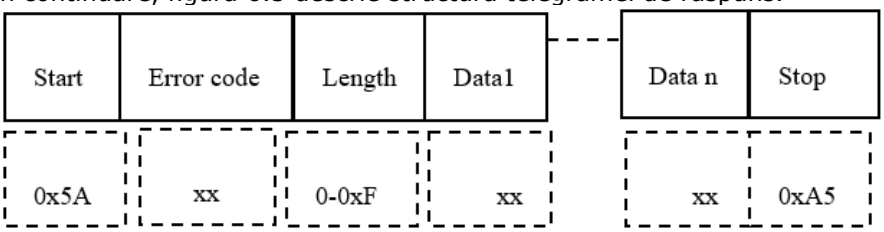

Fig. 6.5. - Structura unei telegrame de răspuns.

Telegrama de răspuns este delimitată de un indicator Start și Stop. *Codul de eroare* este codificat pe un octet, urmat de lungimea care indică numărul de octeți de date primite. Datele sunt trimise în modul MSB, iar transmisia datelor are loc doar în cazul în care comanda a fost executată cu succes. Același format al telegramei de răspuns este păstrat atât pentru protocolul cu fir, cât și pentru cel fără fir. Tabelul 6.1. prezintă comenzile de control acceptate.

Tabelul 6.1. - Comenzi de control.

Comandă	Descriere
NODE_INFO	Obțineți informații despre noduri
PART_NUM	Obțineți numărul componentei și versiunea HW
GET_RSSI	Obțineți RSSI
NET_SCAN	Scanarea rețelei
FLASH	Operațiuni flash
TX_LEVEL	Setați nivelul de putere TX
TX_STRESS	Trimiterea a N cadre de date (test de rezistență)

Softwareul comenzilor de control poate fi preconfigurat pentru fiecare nod, permițând utilizatorului să ajusteze numărul de servicii în funcție de capacitățile hardware în ceea ce privește componentele de memorie RAM și ROM disponibile.

O comunicare este întotdeauna declanșată de aplicația software de pe PC, iar nodul central execută comanda la nivel local, în cazul în care nodul central este destinația sau transmite comanda către alte noduri la distanță din rețea. La un moment dat, doar un singur nod are voie să trimită date, astfel încât se evită interferențele de canal. O excepție de la această regulă a fost permisă pentru punerea în aplicare a comenzii NET_SCAN (Network scan) care interoghează rețeaua pentru a găsi nodurile disponibile. Pentru a evita interferențele, a fost implementat un mecanism de acces multiplu cu diviziune în timp (TDMA), după cum se arată în figura 6.6. Nodul central scanează rețeaua timp de 2 secunde și obține numărul total de noduri găsite și numerele de identificare asociate acestora. Fiecărui nod i se atribuie un număr de identificare (ID) pe 8 biți. ID-ul este programat în memoria flash și nu poate fi suprascris în timpul execuției.

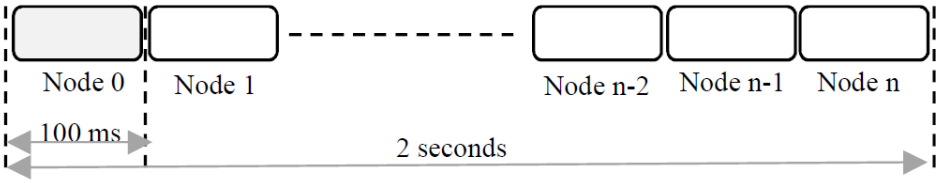

Fig. 6.6. - Mecanismul TDMA utilizat pentru scanarea rețelei.

Nodul central trimite un mesaj de tip broadcast în intervalul de timp 0. Fiecare nod primește mesajul și trimite înapoi răspunsul în propriul interval de timp de 100 de milisecunde.

6.2.3 Parametrii protocolului de comunicare

Comunicarea prin cablu utilizează interfața RS-232 și protocolul UART, iar configurația folosită pentru cadrele UART este 8N1, ceea ce înseamnă 8 biți de date, LSB, fără paritate și 1 bit de stop.

Comunicarea fără fir este setată la o frecvență de 2400 MHz și o rată de 250 kBaud. Numărul maxim de octeți de date într-o transmisie este setat la 16 octeți. Limitarea este necesară din cauza constrângerilor legate de memoria RAM redusă a chipului MSP430F2274. Software-ul permite ajustarea tampoanelor de transmisie și recepție a datelor, asigurând o portare ușoară la alte arhitecturi hardware dacă acest lucru este necesar.

6.2.4 Indicatorul RSSI

Atunci când se primește un pachet, datele sunt stocate în memoria internă RAM a emițător-receptorului și pot fi recuperate pentru utilizare ulterioară prin intermediul interfeței SPI. CC2500 poate fi configurat să adauge informații privind factorul RSSI calculat în memoria tampon a pachetelor primite. Valoarea este stocată în complement de 2 și este necesară o prelucrare ulterioară a acestei valori, deoarece există un decalaj care depinde de viteza de transmisie ce trebuie să fie ulterior sustras pentru a obține valoarea finală. Pentru o rată de transmisie de 250 kBaud, trebuie să se sustragă un decalaj de 72 dBm din valoarea RSSI brută, în conformitate cu [256]. În figura 6.7, este descrisă structura unui pachet.

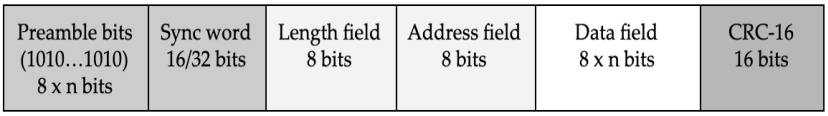

Fig. 6.7. - Structura pachetelor de transmisie radio CC2500.

Există 4 octeți de preambul și 4 octeți de sincronizare configurați pentru fiecare transmisie. Protocolul de comunicație adaugă un overhead de 4 octeți la fiecare pachet transmis. Prin urmare, durata de transmisie (D) a unui singur cadru de date, care transportă n octeți de date, la o rată de transmisie de 250 kBaud, poate fi calculată cu ajutorul (6.2).

$$D(s) = [16 \times 8(\text{biți header}) + n \times 8(\text{biți de date})] \times 4 \times 10^{-6}, <s>. \quad (6.2)$$

6.3. Rezultate experimentale și cercetări suplimentare privind indicatorii nodului radio

Pornind de la ideea că diagrama de radiație a unui nod senzorial nu este izotropă, cercetarea prezintă rezultatele măsurătorilor factorului RSSI în mai multe situații de aranjament geometric: în interior și în exterior, într-un mediu real. Pentru senzorii menționați mai sus a fost determinată interdependența dintre nivelurile de tensiune ale sursei de alimentare, variația neliniară a nivelului de putere de emisie în funcție de setările regiștrilor interni.

Deoarece experimentele nu au fost efectuate în condiții de laborator, iar factorii de mediu (temperatură, umiditate, presiune, etc.) nu pot fi controlați/modificați, rezultatele reflectă situația măsurătorilor doar din perspectiva distanței și a orientării geometrice a nodurilor senzoriale în mediul real.

6.3.1. Cercetări privind consumul de curent al fiecărui nod.

Consumul total de curent este dat de (6.3).

$$C_{Total}\,(mA) = C_{CPU} + C_{Outputs} + C_{Transceiver},\ <mA>. \quad (6.3)$$

C_{CPU} este curentul consumat de CPU și de periferice și este definit, de obicei, de viteza de funcționare a procesorului, de circuitele externe și de perifericele activate (alimentate). $C_{Outputs}$ este curentul consumat de ieșirile controlate de CPU, iar în acest caz, există o singură ieșire, un LED utilizat ca indicator vizual al pachetului primit, care comută de fiecare dată când un nou pachet a fost primit cu succes. În cele din urmă, $C_{Transceiver}$ este curentul consumat de emițătorul-receptor radio de la bord, care poate fi influențat de modul de funcționare al emițătorului-receptor: oprire, inactivitate, RX activ sau TX activ, pe de o parte, și de nivelul puterii de transmisie, în cazul în care modul de funcționare este TX activ.

Valoarea de interes este consumul total de curent al nodului atunci când se află în modul TX activ, deoarece aceasta constituie singura valoare ce ar putea fi modificată în mod dinamic de un algoritm de transmisie de date eficient din punct de vedere energetic.

Protocolul de comunicare conferă două comenzi de control, care pot fi utilizate pentru a măsura și controla consumul de curent în timpul unei transmisii.

Utilizând comanda TX_LEVEL, utilizatorul poate controla nivelul de putere TX cu o granularitate de 192 de trepte de nivel de putere. CC2500 oferă un registru de control pe 8 biți inscriptibil de către utilizator pentru setarea nivelului de putere TX, iar Figura 6.8 prezintă dependența dintre valoarea registrului și nivelul de putere TX.

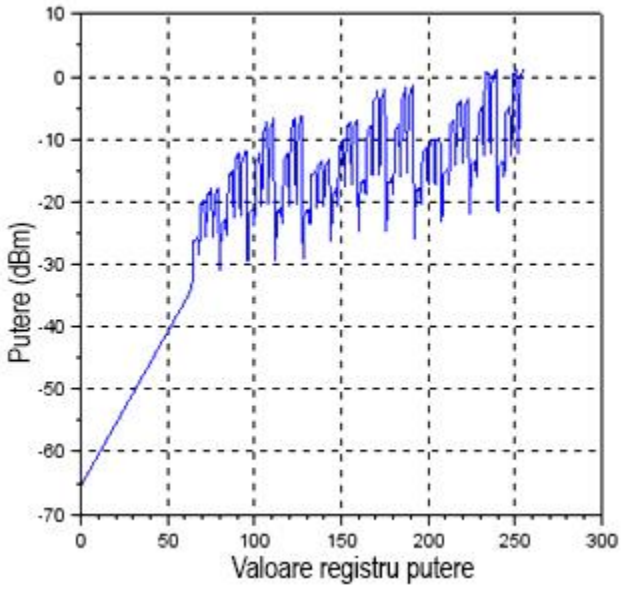

Fig. 6.8. - Variația neliniară a nivelului de putere de transmisie în funcție de setarea registrului.

Deoarece caracteristica nu este liniară, a fost necesară implementarea unui tabel de căutare în aplicația software, astfel încât caracteristica neliniară să nu fie vizibilă utilizatorului final. În figura 6.9 este prezentată caracteristica liniară obținută.

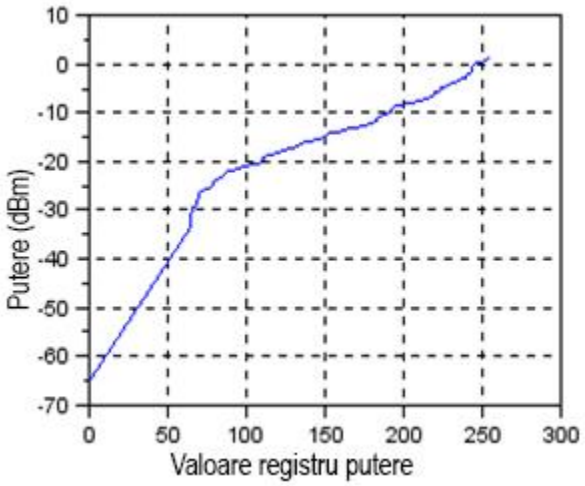

Fig. 6.9. - Liniarizarea nivelului de putere de transmisie în funcție de setarea registrului de putere al emițătorului.

Utilizând comanda TX_STRESS, un set de cadre de date predefinite sunt trimise de un nod secundar, în timp ce se măsoară consumul de curent al nodului în timpul transmisiei. Dispozitivul de măsurare a curentului utilizat în aceste experimente este multimetrul Agilent 34401a. Dispozitivul este capabil să efectueze măsurători la o rată de 200 de eșantioane/secundă, rezultând o perioadă de eșantionare de 5 milisecunde.

Durata unei singure transmisii de 10 octeți, la o rată de 250 kBaud, calculată cu ajutorul ecuației 6.2, este egală cu 832 microsecunde. Deoarece durata unei singure transmisii de cadre este mai mică decât perioada de eșantionare a dispozitivului de măsurare, a fost necesară forțarea transmițătorului CC2500 în modul de transmisie continuă de date pentru a mări fereastra de timp pe care se face măsurarea. Prin urmare, dispozitivul va rămâne în starea activă TX pentru un număr de transmisii de pachete definit de utilizator și astfel au fost efectuate două seturi de măsurători de curent în modul TX pentru toate cele 192 de setări diferite ale nivelului de putere, iar pentru fiecare măsurătoare, au fost transmise 1000 de pachete.

Pentru primul set, nodul fără fir a fost alimentat cu două baterii AAA de 1,5 volți, complet încărcate, iar în figura 6.10 sunt prezentate rezultatele măsurătorilor inițiale.

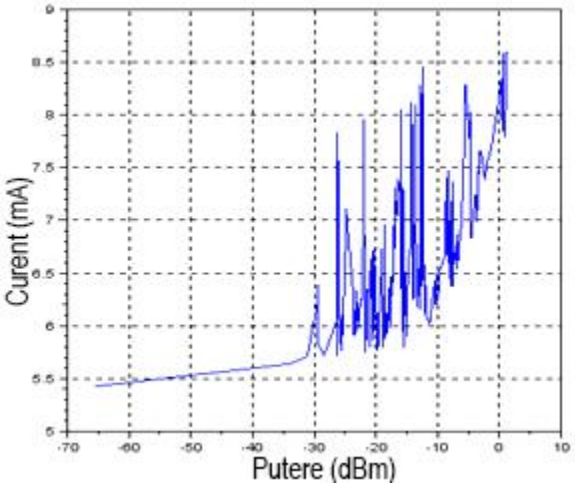

Fig. 6.10. - Curentul în funcție de puterea de transmisie pentru baterii complet încărcate (VBAT = 3,16 V).

Se poate observa faptul că graficul reprezentat arată din nou o caracteristică neliniară. Pentru cel de-al doilea set, nodul fără fir a fost alimentat cu două baterii AAA de 1,5 volți descărcate (i.e. V_{bat} = 2,768 V), iar în figura 6.11 sunt prezentate rezultatele măsurătorilor.

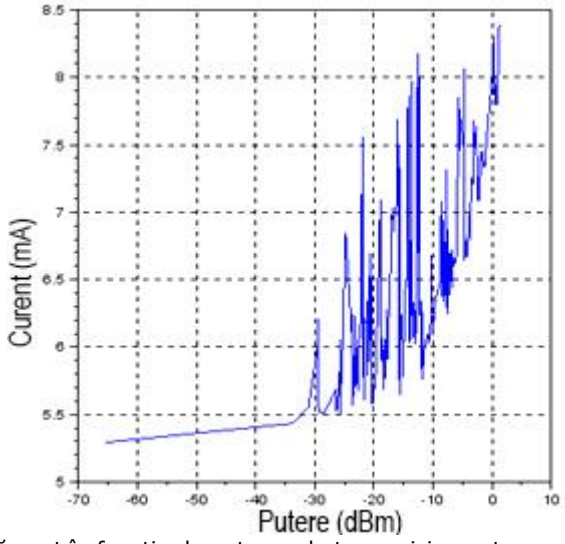

Fig. 6.11. - Curentul măsurat în funcție de puterea de transmisie pentru cazul alimentării cu baterii descărcate (Vbat = 2,768 volți).

Graficul din figura 6.11 arată din nou o caracteristică neliniară (lucru confirmat și de [256]), iar prin suprapunerea figurilor 6.10 și 6.11, diferența de

consum de curent poate fi observată în figura 6.12. Așa cum era de așteptat, consumul de curent în cazul bateriilor descărcate este mai mic.

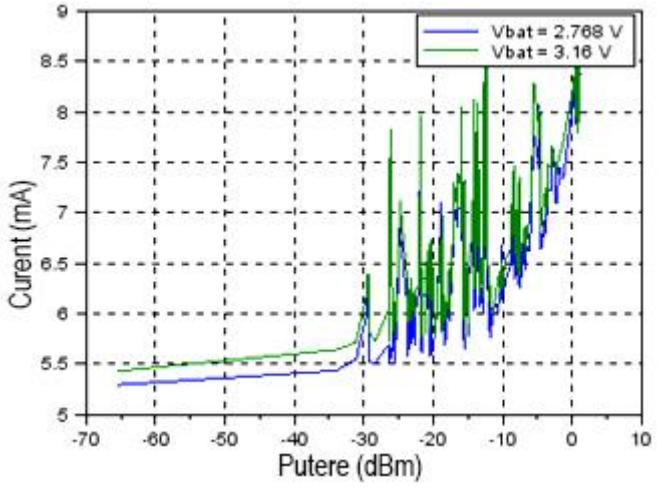

Fig. 6.12. - Curentul măsurat în funcție de puterea de transmisie. Comparație între baterii complet încărcate și baterii descărcate.

În cazul unui senzor, măsurătorile de curent efectuate în funcție de puterea de emisie diferă în funcție de nivelul de încărcare a bateriei folosite, prin urmare, autonomia unui astfel de senzor sau contor, estimată prin măsurarea tensiunii bateriei, influențează acuratețea estimării distanței, pe baza măsurătorii RSSI.

Figura 6.13 arată diferența de consum de curent atunci când există o scădere de 0,48 volți în sursa de alimentare.

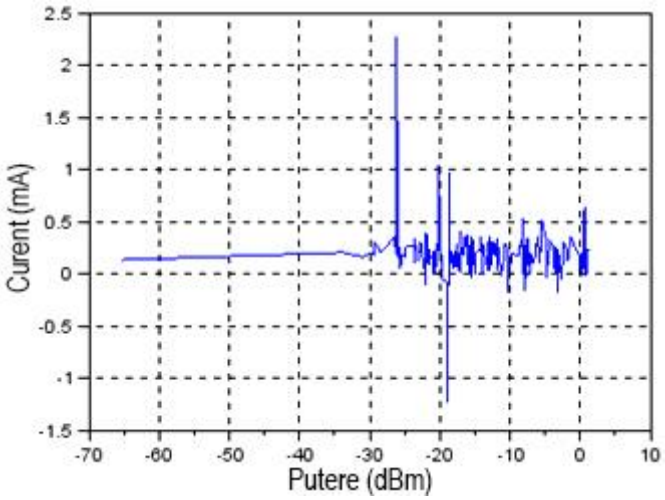

Fig. 6.13. - Consumul de curent în funcție de puterea de transmisie. Diferența de consum de curent cauzată de o cădere de tensiune de 0,48 volți.

6.3.2. Măsurători RSSI

S-au efectuat mai multe seturi de măsurători pentru a evalua nivelul RSSI în diferite condiții. Măsurătorile au fost declanșate cu ajutorul a două comenzi de control ale protocolului fără fir prezentat anterior. În primul rând, a fost trimisă o comandă NET_SCAN pentru a căuta noduri active în raza de acțiune, iar apoi după ce s-a obținut lista modurilor disponibile, comanda GET_RSSI a fost utilizată pentru a prelua nivelul RSSI. Comanda GET_RSSI funcționează în două moduri, direct și indirect. Modul direct se aplică dacă nodul sursă este același cu nodul central și atunci se măsoară nivelurile RSSI între nodul central și un nod secundar, iar măsurarea indirectă a nivelului RSSI se efectuează între oricare două noduri diferite de nodul central. Folosind cele două moduri, se poate măsura orice nivel RSSI între orice nod din rețea. Pentru măsurătorile în aer liber și în interior, s-a utilizat sistemul de poziționare a nodurilor descris în figura 6.14.

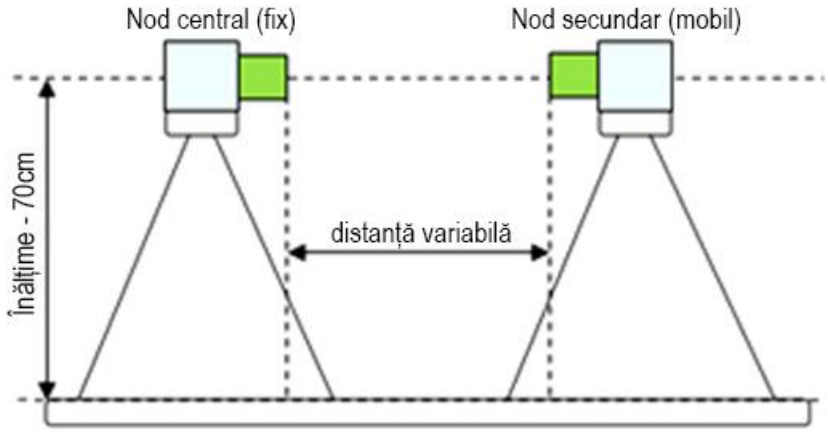

Fig. 6.14. - Configurația de măsurare în interior/exterior.

6.3.2.1. Măsurători în aer liber

Utilizând configurația sistemului descrisă în figura 6.14, primul set de măsurători a fost efectuat pe un câmp deschis acoperit de o suprafață de beton (parcare). Pe o rază circulară de 31 m, niciun obstacol nu se afla în linia de vizibilitate, astfel că a fost considerat un mediu cu o probabilitate minimă de interferență.

Poziția stației de bază a fost stabilă în timpul măsurătorilor, iar stația de la distanță a fost deplasată în pași de 1 m față de stația de bază. Teoretic, în această

configurație, singura perturbare ar trebui să fie reflectarea undei radio de la solul (suprafața) de beton. În figura 6.15 sunt prezentate rezultatele măsurătorilor.

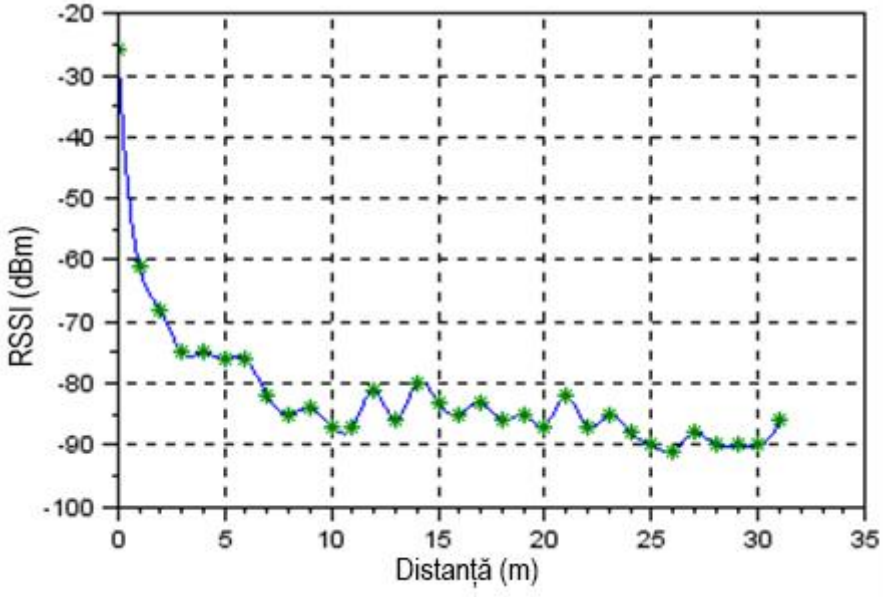

Fig. 6.15. - Nivelul RSSI în funcție de distanță. Măsurători în câmp deschis.

Este vizibil faptul că, în câmp deschis, pentru o distanță de până la 10 m, caracteristica este liniară, dar măsurătorile se degradează pe măsură ce distanța crește. Cu nivelul maxim de putere de transmisie setat, măsurătorile au fost posibile pentru o distanță de până la 31 m, iar la o distanță mai mare, semnalul a fost prea slab și pachetele au fost pierdute. Raza de acțiune poate fi extinsă prin utilizarea unei antene externe și a unor circuite adecvate de adaptare a antenei, dar nu fac obiectul prezentului experiment.

6.3.2.2. Măsurători în interior

Utilizând configurația sistemului descrisă în figura 6.14, primul set de măsurători a fost efectuat în interiorul unui coridor cu o lungime de 14 m și o lățime de 1,5 m. Ansamblul de măsurare a fost centrat pe axa longitudinală. Stația secundară aflată la distanță a fost deplasată în pași de 1 m față de stația de bază. Teoretic, în această configurație, măsurătorile sunt afectate de reflexiile undelor de la podea, tavan și pereții din jur. În figura 6.16, sunt prezentate rezultatele măsurătorilor în interior.

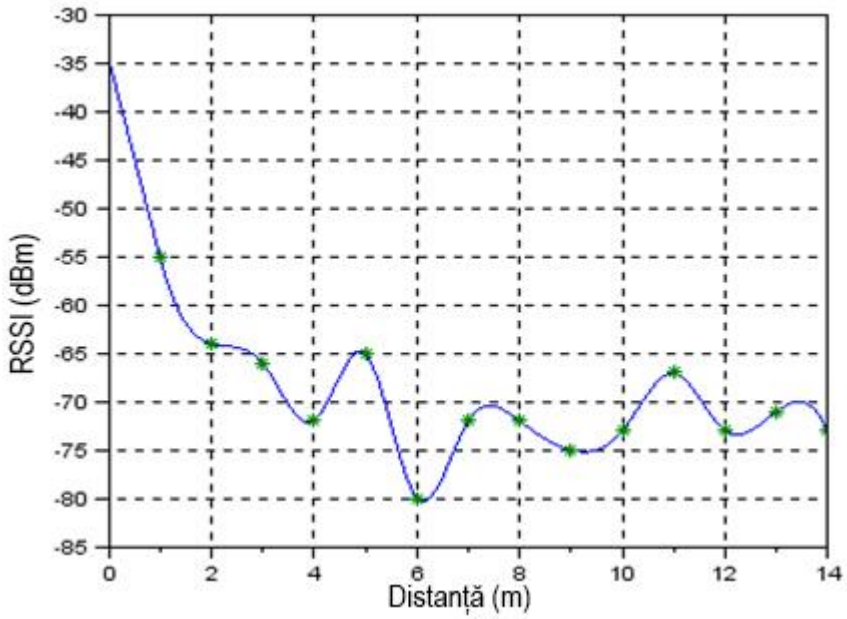

Fig. 6.16. - Nivelul RSSI în funcție de distanță. Măsurători în interior pe un coridor de 14 m lungime și 1,5 m lățime.

Comparând figurile 6.15 și 6.16, se observă că, pentru aceeași distanță, nivelul RSSI într-un mediu interior este mai mare. Se presupune că, datorită căilor multiple de reflexie a undelor radio, pierderea de putere a semnalului este redusă.

6.3.2.3. Măsurători de orientare orizontală în interior

Pentru efectuarea măsurătorilor de orientare geometrică, a fost utilizat sistemul din figura 6.14, cu o distanță fixă de 1 m între stația de bază și stația la distanță. Aceste experimente indică dacă există o modificare a nivelurilor RSSI în cazul unei poziționări diferite a stației secundare față de stația de bază.

Au fost efectuate două seturi de măsurători, unul cu nodurile față în față și unul cu nodurile poziționate spate în spate. S-a efectuat un set de unsprezece măsurători pentru a acoperi o zonă de 360 de grade în jurul stației de bază, cu o granularitate de α = 30 de grade, după cum se arată în figurile 6.17 și 6.18.

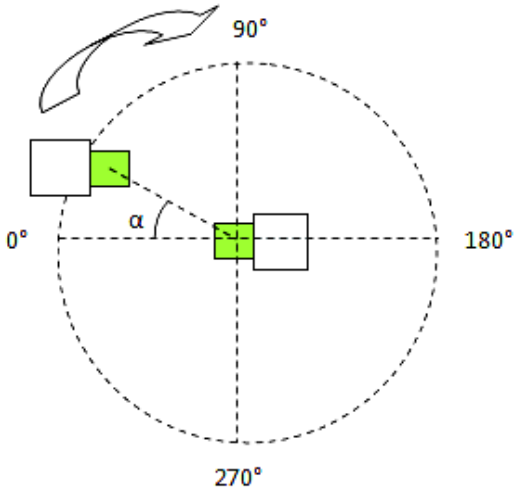

Fig. 6.17. - O configurație de măsurare cu nodurile față în față pe parcursul a 360°.

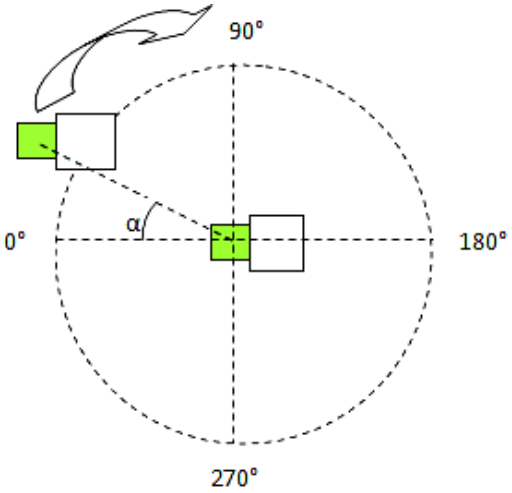

Fig. 6.18. - O configurație de măsurare cu nodurile spate în spate pe parcursul a 360°.

Figura 6.19 prezintă rezultatele măsurătorilor efectuate cu ajutorul configurației de măsurare cu nodurile aflate față în față, iar distanța dintre noduri fiind de 1 metru.

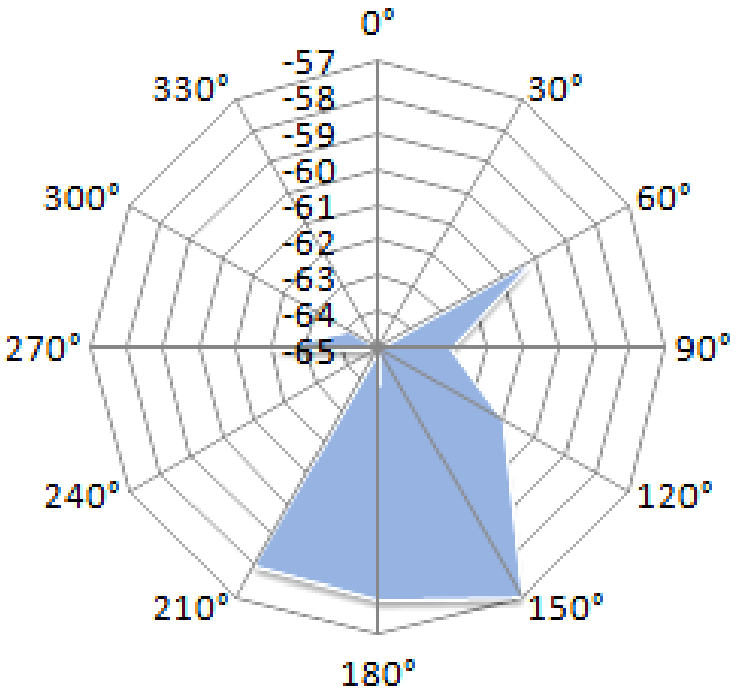

Fig. 6.19. - Nivelul RSSI în funcție de orientarea nodului într-o configurație de măsurare cu nodurile aflate față în față.

Prin menținerea nodului de bază fix și rotirea nodului mobil, se poate observa pe graficul de măsurare că nivelul RSSI diferă considerabil. Măsurătorile au fost efectuate la fiecare 30 de grade.

Figura 6.20 prezintă rezultatele măsurătorilor efectuate cu ajutorul configurației de măsurare poziționate spate în spate, iar distanța dintre noduri a fost de 1 m. Configurații experimentale similare sunt documentate în [235, 257 și 258]. Dacă senzorul de bază și senzorul mobil sunt plasate spate în spate, diagrama RSSI nu se schimbă prea mult ca formă (este în continuare direcțională), dar nivelul RSSI este mai mic. Din fiecare diagramă pot fi citite nivelurile semnalului indicate de RSSI, la diferite valori ale poziției unghiulare.

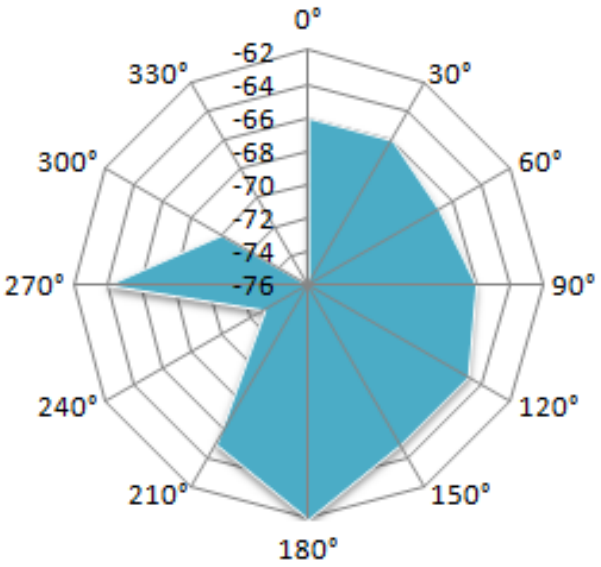

Fig. 6.20. - Nivelul RSSI în funcție de orientarea nodului într-o configurație de măsurare cu nodurile spate în spate.

În figura 6.21 sunt afișate rezultatele măsurătorilor efectuate în [235], redesenate în același format ca în figura 20 pentru o comparație mai ușoară a rezultatelor. În [235], măsurătorile au fost efectuate numai pe 4 unghiuri.

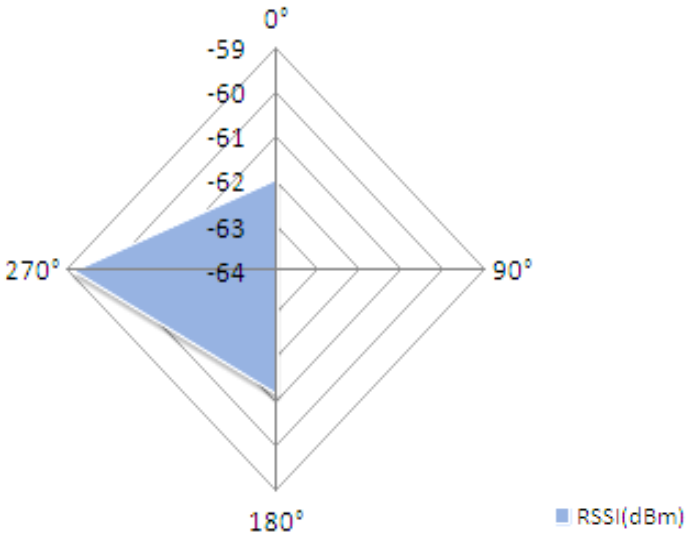

Fig. 6.21. - Nivelul RSSI în funcție de orientarea nodului într-o configurație de măsurare spate în spate.

Distanța dintre noduri este de 1,5 metri, iar valorile RSSI reprezintă media a 50 de măsurători în fiecare direcție.

Pentru analiza statistică, folosind configurația din figura 6.17, măsurătorile factorului RSSI au fost repetate într-un nou mediu interior în condiții diferite. Testul a fost repetat de 30 de ori, pentru fiecare poziție unghiulară, iar rezultatele se regăsesc în Tabelul 6.2. - Rezultatele măsurătorilor RSSI.

Tabelul 6.2. - Rezultatele măsurătorilor RSSI.

#	0 DEG (dBm)	30 DEG (dBm)	60 DEG (dBm)	90 DEG (dBm)	120 DEG (dBm)	150 DEG (dBm)	180 DEG (dBm)	210 DEG (dBm)	240 DEG (dBm)	270 DEG (dBm)	300 DEG (dBm)	330 DEG (dBm)
1	−56	−53	−56	−47	−48	−49	−56	−59	−46	−44	−51	−51
2	−54	−53	−56	−47	−48	−49	−61	−58	−46	−46	−51	−51
3	−53	−53	−56	−47	−48	−49	−62	−59	−44	−47	−50	−49
4	−54	−53	−67	−47	−48	−49	−60	−60	−46	−47	−50	−49
5	−54	−53	−68	−48	−48	−52	−60	−58	−46	−47	−50	−49
6	−54	−53	−68	−48	−48	−50	−60	−59	−46	−47	−49	−49
7	−54	−53	−68	−48	−48	−50	−61	−59	−46	−47	−50	−49
8	−54	−56	−68	−48	−48	−49	−60	−59	−42	−47	−50	−49
9	−54	−58	−68	−48	−48	−49	−60	−59	−46	−47	−51	−49
10	−54	−58	−68	−48	−48	−49	−60	−58	−46	−47	−50	−50
11	−55	−58	−68	−48	−48	−50	−60	−58	−44	−47	−50	−49
12	−55	−58	−68	−48	−48	−51	−60	−59	−46	−47	−50	−49
13	−55	−58	−63	−48	−48	−49	−59	−59	−46	−47	−49	−49
14	−55	−58	−65	−48	−48	−49	−60	−59	−46	−48	−50	−49
15	−55	−58	−65	−48	−48	−50	−60	−59	−46	−49	−50	−50
16	−55	−58	−65	−48	−48	−50	−60	−59	−46	−49	−50	−50
17	−55	−58	−65	−48	−48	−50	−60	−58	−46	−49	−50	−50
18	−55	−58	−65	−48	−48	−50	−60	−56	−44	−50	−50	−53
19	−55	−58	−65	−48	−48	−50	−68	−56	−46	−49	−50	−48
20	−56	−58	−65	−48	−48	−50	−60	−58	−46	−50	−51	−47
21	−55	−58	−65	−48	−48	−50	−60	−58	−46	−50	−51	−48
22	−55	−58	−71	−48	−48	−50	−60	−58	−44	−49	−49	−47
23	−55	−58	−72	−48	−48	−50	−60	−58	−46	−49	−49	−48
24	−55	−58	−72	−48	−48	−50	−63	−58	−47	−49	−49	−47
25	−55	−58	−72	−48	−48	−50	−63	−58	−46	−49	−49	−48
26	−55	−59	−72	−48	−48	−50	−60	−59	−47	−49	−49	−47
27	−55	−56	−72	−48	−48	−50	−63	−59	−46	−49	−49	−47
28	−55	−56	−72	−48	−48	−50	−62	−58	−47	−49	−49	−47
29	−54	−56	−72	−48	−48	−50	−67	−58	−47	−48	−50	−47
30	−54	−56	−68	−48	−48	−51	−60	−58	−44	−48	−49	−47

Prelucrarea statistică a acestor informații este prezentată în tabelul 6.3 și reprezentată grafic astfel: RSSI mediu-Figura 6.22, abaterea standard a eșantionului-Figura 6.23, coeficientul de variație-Figura 6.24 și în sfârșit variația eșantionului-Figura 6.25. (Prelucrarea statistică a fost realizată cu ajutorul instrumentelor WolframAlpha).

Tabelul 6.3. - Analiza statistică a măsurătorilor RSSI.

Angle (DEG)	Mean (RSSI)	Sample Std. Deviation	Sample Variance	Coefficient of Variation	Confidence Interval (95%)
0	−54.65	0.6607	0.4366	−0.01209	−54.878 to −54.413
30	−56.52	2.096	4.391	−0.03708	−57.254 to −55.778
60	−66.86	4.237	17.95	−0.06337	−68.261 to −65.454
90	−47.78	0.3408	0.1161	−0.007119	−47.9909 to −47.7510
120	−47.77	0.5603	0.314	−0.01173	−47.971 to −47.577
150	−49.84	0.6878	0.4731	−0.0138	−50.081 to −49.597
180	−60.84	2.208	4.873	−0.03628	−61.616 to −60.062
210	−58.35	0.8386	0.7032	−0.01437	−58.650 to −58.060
240	−45.71	1.131	1.28	−0.02475	−46.108 to −45.311
270	−48.03	1.291	1.666	−0.02687	−48.463 to −47.596
300	−49.76	0.6989	0.4884	−0.01404	−50.000 to −49.530
330	−48.12	1.394	1.943	−0.02897	−48.513 to −47.732

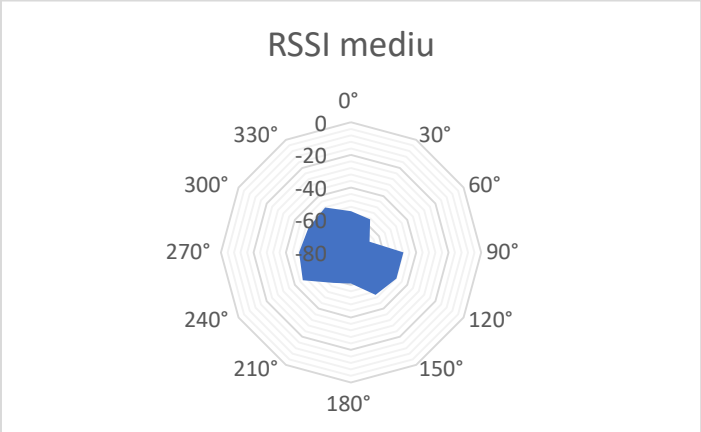

Fig. 6.22. - Analiza statistică. Valoarea medie RSSI a măsurătorilor.

Valoarea medie RSSI, prezentată în figura 6.22, a fost obținută prin calcularea mediei a 30 de măsurători într-o configurație cu nodurile poziționate față în față. Fiecare măsurătoare constă în 11 măsurători distincte, iar stația de bază a

rămas într-o poziție fixă, în timp ce nodul mobil a fost deplasat manual în sensul acelor de ceasornic cu 30 de grade la fiecare minut, menținând constantă raza de un metru. Citirea RSSI a fost înregistrată la 30 de secunde după ce nodul a fost plasat în noua poziție. În acest fel, s-a evitat orice perturbare a măsurătorilor produsă de către experimentator.

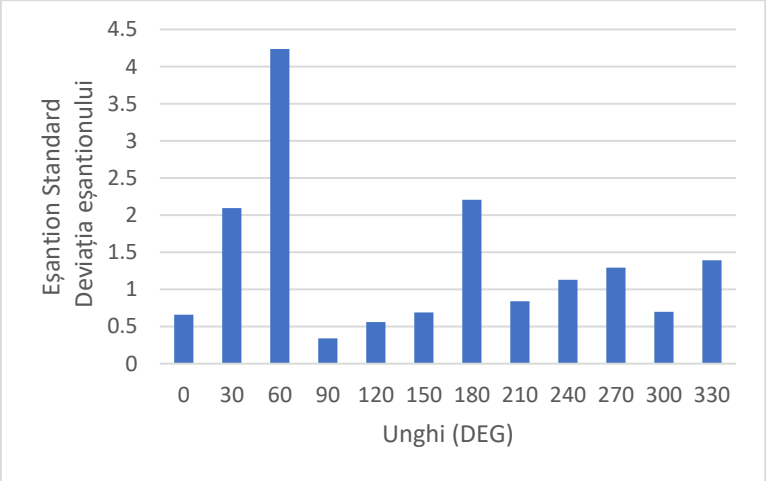

Fig. 6.23. - Analiza statistică. Exemplu de deviație standard a măsurătorilor RSSI.

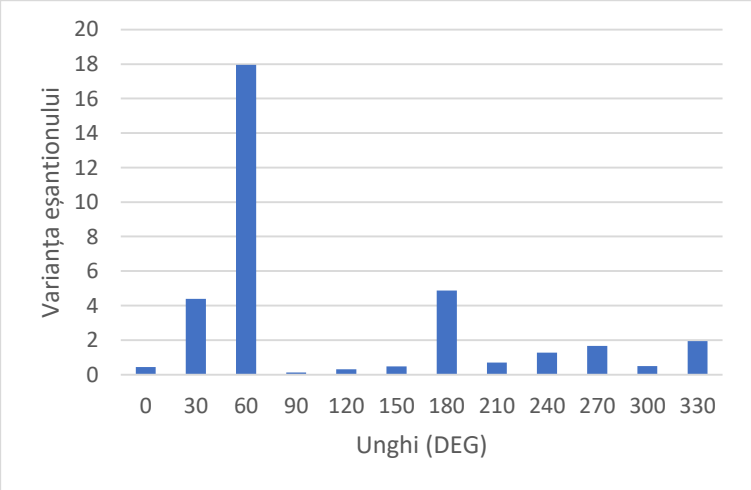

Fig. 6.24. - Analiza statistică. Variația eșantioanelor de măsurători RSSI.

Pentru a exclude interferențele cauzate de factorii de mediu care s-ar putea modifica în timp, s-au repetat periodic seturi complete de măsurători. Un set complet constă în unsprezece măsurători care acoperă 360 de grade în jurul stației de bază. Reprezentarea variației standard a eșantionului din figura 6.23 și varianța

corespunzătoare a eșantionului din figura 6.24 arată o răspândire minimă în distribuția măsurătorilor RSSI corespunzătoare fiecărui unghi.

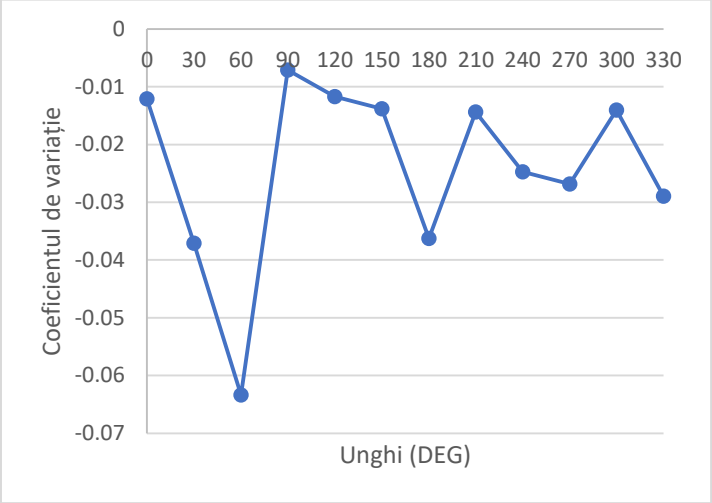

Fig. 6.25. - Analiza statistică. Coeficientul de variație al măsurătorilor RSSI.

Atât acuratețea, cât și fiabilitatea măsurătorilor din timpul experimentelor sunt validate cu ajutorul coeficientului de variație (CV) ilustrat în figura 6.25. Având în vedere dispersia scăzută în timpul acestor măsurători, studiile ulterioare privind orientarea geometrică a RSSI în același mediu ar putea fi repetate folosind un număr mai mic de eșantioane colectate, considerând că vor avea același grad de încredere.

Toate aceste rezultate dovedesc variația nivelului semnalului indicat de RSSI pentru aceeași distanță între senzori, dar cu orientări unghiulare diferite.

6.3.2.4. Măsurători de orientare verticală în interior

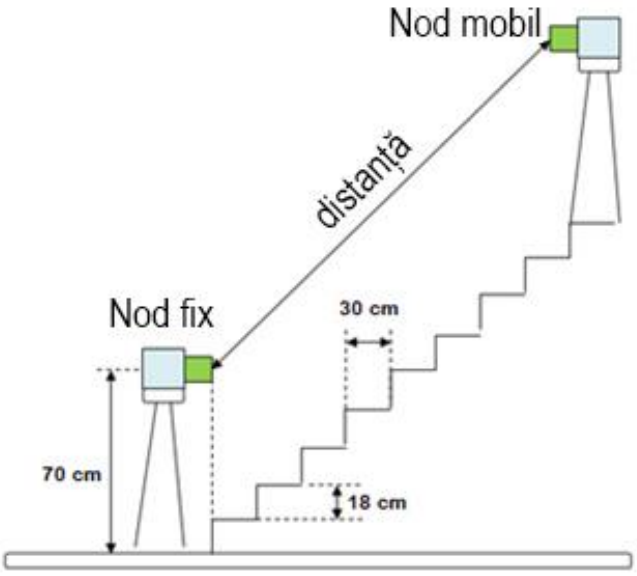

Fig. 6.26. - Un montaj de măsurare verticală cu nodurile poziționate față în față.

Scopul acestor măsurători este de a evalua nivelul RSSI între două noduri poziționate la înălțimi diferite și sub un anumit unghi. În figura 6.26 este ilustrată configurația experimentelor de măsurare. Stația de bază este fixă, iar stația secundară (nodul mobil) se deplasează treptat în sus, câte o treaptă pe rând. Scările sunt situate într-un coridor cu lățimea de 1,3 m și lungimea de 3 m.

În figura 6.27, sunt prezentate rezultatele măsurătorilor obținute cu ajutorul configurației de măsurare față în față pe verticală din figura 6.26.

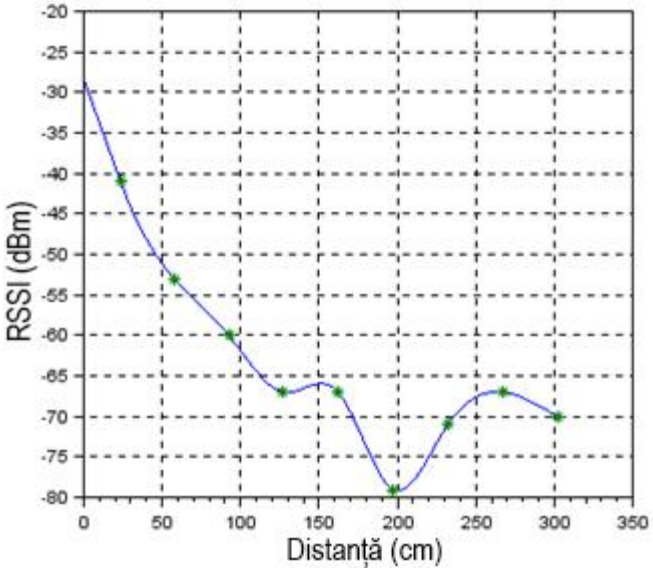

Fig. 6.27. - Nivelul RSSI în funcție de orientarea nodului într-o configurație de măsurare verticală cu nodurile poziționate față în față.

Comparând valorile de la 1 m, 1,5 m, 2 m, 2,5 m și 3 m prezentate în figurile 6.16 și 6.27, se observă diferențe considerabile, iar rezultatele prezentate arată în mod clar că caracteristicile de orientare ale modulului radio de pe senzor nu sunt izotrope.

6.4. Discuție privind rezultatele experimentale

Scopul acestui capitol a fost de a evidenția în ce măsură rezultatele experimentelor științifice pot diferi în rețelele de contorizare inteligentă fără fir în funcție de orientarea unui nod față de alte noduri. Ca urmare, într-o aplicație în care se utilizează rețele de noduri fără fir, în funcție de modulul radio folosit, există implicații pentru problemele de autonomie și problemele de localizare în special în cazurile în care poziția și orientarea nodurilor nu este cunoscută.

Sistemul de măsurare RSSI descris în această lucrare, bazat pe protocolul de comunicare cu fir și fără fir propus, și-a dovedit fiabilitatea și compatibilitatea cu rețelele de contorizare fără fir. Prin proiectarea sa, sistemul software este scalabil din punct de vedere al caracteristicilor și al resurselor hardware, ceea ce îl face potrivit pentru o gamă mai largă de senzori sau dispozitive fără fir cu arhitectură hardware și amprentă de resurse de calcul diferite.

Pentru a utiliza valorile RSSI ca date de intrare pentru algoritmi de detectare a distanței sau a locației, valorile RSSI nu pot fi utilizate fără etape intermediare de procesare pentru a atenua neliniaritatea valorilor măsurate. Rezultatele măsurătorilor au confirmat că nivelul RSSI variază în funcție de distanță, de orientarea geometrică a senzorilor și de caracteristicile mediului.

Având în vedere rețelele de echipamente fără fir eficiente din punct de vedere energetic cum ar putea fi contoarele inteligente de gaz, este de așteptat ca factorul RSSI să fie o soluție pentru detectarea distanței dintre noduri și, ulterior, să ajusteze puterea de transmisie la o valoare specifică corespunzătoare distanței măsurate. Prin reducerea puterii de transmisie, se reduce consumul de curent al emițătorului-receptorului și, prin urmare, crește autonomia nodului, dar totodată rezultatele experimentale arată că eZ430-RF2500T are o caracteristică neliniară între curent și puterea de transmisie, așa cum se arată în figurile 6.10-6.12, ceea ce dovedește că nu este cea mai potrivită platformă hardware pentru acest tip de aplicații.

6.5. Concluzii parțiale și contribuții

Experimentele și interpretarea rezultatelor din prezentul capitol arată că sistemul RSSI poate fi utilizat pentru a estima distanța dintre nodurile unei rețele fără fir cum ar fi contoarele inteligente bazate pe tehnologii radio. Cu toate acestea, precizia măsurătorilor este puternic afectată de orientarea nodurilor în fiecare locație, iar pe lângă considerarea factorilor de mediu, o analiză atentă a fișei tehnice a fiecărui nod radio poate scuti proiectanții de probleme care pot fi descoperite doar în timpul instalării în teren.

Același nivel al semnalului măsurat de la aceleași două noduri nu înseamnă că distanța dintre cei doi senzori este aceeași, dar e posibil ca senzorii ce au caracteristica de emisie izotropă a semnalului să confere informații ușor îmbunătățite. Cu toate acestea, sunt implicați și alți factori de mediu care pot influența nivelul semnalului indicat de măsurătorile RSSI. Menționăm că în experimentele prezentate nu am efectuat măsurători cu astfel de senzori (cu emisie izotropică) și nici în condiții de mediu diferite.

Sistemul conceput și implementat experimental pentru un tip de parametru și un tip de nod radio poate fi ușor adaptat la studiul altor noduri din echipamente fără fir, iar studiul practic al altor parametri care furnizează date pentru algoritmii de localizare a nodurilor poate fi realizat prin adaptarea sistemului prezentat.

Rezultatele finale ale acestor studii ne pot conduce la estimări mai precise ale autonomiei și a poziționării unui nod sau a unei întregi rețele de echipamente de contorizare inteligentă fără fir.

Experimentele prezentate au utilitate practică deosebit de mare pentru preluarea consumului energetic de la consumatorii situați pe o scară în blocurile cu mai multe niveluri.

7. CONCLUZII FINALE ȘI CONTRIBUȚII PERSONALE

7.1. Concluzii

Acest capitol final sintetizează un șir de concluzii privind obiectivele tezei de doctorat, actualitatea temei abordate, respectiv a contribuțiilor personale prezentate în cadrul capitolelor anterioare. De asemenea, capitolul este destinat și prezentării modurilor de valorificare a rezultatelor și a unor elemente tehnice propuse în cadrul lucrărilor de cercetare din domeniul abordat. Capitolul conchide prin enumerarea direcțiilor de studiu identificate pentru viitor și a lucrărilor publicate în urma cercetării doctorale.

În contextul actual, premergător crizei sanitare COVID-19, dar și a creșterii costului energiei, sectorul energetic joacă un rol deosebit de important atât din punct de vedere economic cât și politic. Producția de energie electrică din surse regenerabile face ca utilizarea pe scară largă a contoarelor inteligente să fie esențială datorită flexibilității și performanțelor conferite de o rețea inteligentă de distribuție capabilă să transmită informații în timp real de la fiecare punct de consum și totodată să primească actualizări de program de la distanță fără a fi necesară intervenția unor operatori în teren. Capacitatea de a putea actualiza echipamentele rețelei inteligente de distribuție într-un mod eficient și robust stă la baza dezvoltării continue a capabilităților tehnologice și a siguranței cibernetice a întregii rețele.

În capitolul introductiv a fost analizată problema actualizării la distanță și a fost descris scopul lucrării de cercetare doctorală în acest domeniu. S-a propus analiza metodelor de actualizare folosite în prezent în echipamentele rețelei energetice inteligente, iar apoi găsirea unei soluții generice, optimizată pentru îmbunătățirea fiabilității și performanțelor procesului de actualizare software a contoarelor inteligente. Obiectivul general al cercetării a constat în găsirea unor soluții de actualizare rapidă și sigură, folosind doar infrastructura actuală, pentru a proteja astfel și sistemele integrate de contorizare deja instalate în rețeaua energetică.

Tema de cercetare aleasă a dus la stabilirea următoarelor obiective intermediare:

- Dezvoltarea și analiza unui sistem de actualizare viabil, compus din aplicație și încărcător de program, compatibile cu capabilitățile hardware de care dispun echipamentele de contorizare uzuale.

- Propunerea unor metode de transport a actualizărilor software prin medii cu semnal radio slab sau prin liniile de înaltă tensiune supuse interferențelor.

- Analiza capabilităților de localizare a echipamentelor de contorizare inteligentă, precum și analiza posibilității de optimizare a actualizărilor la

nivel local între nodurile adiacente în funcție de calitatea semnalului dată de indicatorii RSSI.

Această teză a fost structurată în șapte capitole, stadiul actual al cercetării fiind descris în capitolul 3, iar lucrările de specialitate menționate sunt publicate in perioada 2016 - 2021. Cele mai recente lucrări amintesc ca direcție de cercetare problema actualizărilor la distanță în sistemele integrate, subliniind astfel actualitatea temei alese.

Capitolele 4-6 reprezintă tematica de cercetare, fiecare capitol urmărind ca temă generală obiectivele principale enumerate anterior. Capitolul 4 are ca obiectiv elaborarea și soluționarea unui sistem de actualizare la distanță a contoarelor inteligente cu resurse hardware limitate. Implementarea îndeplinește cerințele de performanță și de securitate cerute de ultimele standarde publicate în domeniu. S-a subliniat în primul rând importanța standardizării mecanismelor de actualizare la distanță în domeniul energetic și a fost elaborată o implementare compatibilă atât cu cerințele rețelelor de tip SMART GRID cât și cu cerințele standardului SUIT. Sistemul de actualizare descris a avut ca obiectiv principal și un impact cât mai redus asupra mecanismelor de contorizare ce nu pot fi întrerupte pentru perioade lungi de timp.

În cadrul capitolului 5 s-a tratat problema transportului fișierelor necesare actualizărilor de sistem printr-un mediu cu disponibilitate de comunicare limitată. S-a propus o metoda de transport prin secționare a fișierelor la dimensiuni egale cu unitatea de transmisie maximă acceptată de către rețelele de comunicație prin liniile de înaltă tensiune. Procedeul propus a fost implementat și aplicat asupra unor contoare inteligente instalate într-un mediu controlat. Rezultatele obținute în nodul de rețea experimental au arătat că sistemul este pretabil în special pentru capetele de rețea sau pentru echipamentele de contorizare aflate în locații greu accesibile.

În capitolul 6 se analizează problemele de localizare a contoarelor inteligente cu comunicație radio folosind indicatorii de calitate a semnalului la nivelul fiecărui nod. În acest capitol a fost proiectat și implementat un sistem pentru achiziționarea indicatorului puterii semnalului recepționat (RSSI). S-a pus accent pe variația indicatorului de putere a semnalului recepționat (RSSI) în funcție de distanța și orientarea geometrică a nodurilor și a mediului, atât în spații interioare, cât și în cele exterioare. Datele analizate în acest capitol deschid multiple direcții de cercetare privind localizarea echipamentelor de contorizare adiacente și implicit, optimizarea actualizărilor de la distanță folosind noduri alăturate.

Obiectivele principale urmărite în cadrul tezei doctorale au dus la obținerea următoarelor contribuții personale:

S-a elaborat o analiză comprehensivă a tehnologiilor folosite, la nivel global, în rețelele energetice atât din punct de vedere al tehnologiilor folosite de sistemele de contorizare cât și din punct de vedere al tehnologiilor de comunicație alese pentru digitalizarea rețelelor energetice.

A fost realizat un sistem de actualizare pentru sisteme încorporate, acesta fiind compatibil cu caracteristicile tehnice ale contoarelor inteligente aflate în producție. Sistemul este format din bootloader (fig. 4.5.) și aplicație de proces (fig. 4.6.) și are ca obiectiv îndeplinirea tuturor cerințelor din standardul SUIT [173]. Elaborarea sistemului a pus accent pe o fiabilitate ridicată și un grad crescut de securitate informatică atât la nivelul nodului de rețea cât și la nivelul procesului de distribuție a actualizărilor. În procesul de design software s-a avut în vedere

obținerea unui sistem de actualizare cu un impactul minimal asupra procesului de contorizare a energiei.

Pentru validarea sistemului mai sus creat a fost realizată o arhitectură completă client (contor inteligent) – server (cloud), iar sistemul de distribuție a fișierelor necesare actualizării software poate converti aplicații în format binar în fișiere criptate și semnate la standardele de securitate actuale. Programele și procesul de distribuție au fost apoi folosite în lucrările experimentale efectuate în publicarea lucrării [262] și în elaborarea capitolelor ulterioare.

Cel de-al doilea obiectiv de cercetare a dus la elaborarea unei analize critice privind frecvența și volumul de date transportat de la contoarele inteligente către furnizor prin intermediul liniilor de tensiune.

S-a elaborat un sistem experimental pentru simularea nodurilor de rețea PRIME, în vederea evaluării obiective a metodelor de optimizare propuse ulterior pentru transportul de date prin acest tip rețele.

S-a dezvoltat un algoritm de segmentare a datelor la nivel de aplicație de contorizare. Algoritmul optimizează transportul fișierelor de dimensiuni mari prin rețelele PRIME, iar cazurile cele mai uzuale în care acesta poate fi folosite sunt transportul fișierelor necesare actualizărilor sau transportul pachetelor de date ce conțin curbele de sarcină ale fiecărui loc de consum. Algoritmul urmărește creșterea ratei de transmisii reușite pentru a reduce erorile de comunicație în zonele în care calitatea rețelei PRIME este puternic afectată de perturbații. Prin utilizarea segmentării datelor la nivel de aplicație folosind modelul propus, transferurile de date au devenit mai stabile, fără a mai fi nevoie de încercări de retransmitere. În plus, dispozitivele instalate în cadrul unei rețele afectate de interferențe au înregistrat o creștere notabilă a ratei de transmitere cu succes a curbelor de sarcină, precum și o creștere a ratelor de succes pentru actualizarea firmware-ului la distanță. Rezultatele au fost publicate în jurnale de specialitate, iar algoritmul și detaliile standului de simulare a nodurilor de rețea au făcut parte din conținutul articolelor ”Web of Science” [259], [261] și [262].

Cercetările și analiza indicatorului de semnal RSSI emis de contoarele inteligente bazate pe tehnologii radio au stabilit că acesta poate fi utilizat pentru a estima distanța dintre nodurile rețelei.

S-a conceput și implementat experimental un sistem pentru analiza algoritmilor de localizare bazați pe parametrul de semnal, RSSI. Detaliile privind implementarea acestuia, precum și măsurătorile experimentale și observațiile finale au fost publicate într-un jurnal ”Web of Science” prin articolul [260].

Standurile și metodele experimentale au dus la facilitarea susținerii unor lucrări de laborator din cadrul Universității Politehnica din Timișoara, iar rezultatele didactice obținute au fost publicate în [262] și [264].

Validarea cercetării elaborate în urma prezentei teze de doctorat a fost dobândită prin publicarea unui număr de 10 lucrări științifice, enumerate in anexa A1. Publicațiile privind domeniul de cercetare ales au fost prezentate la jurnale și conferințe internaționale de prestigiu, iar 4 lucrări, [259-262], au fost indexate în baza de date ”Web of Science”.

7.2. Perspective de cercetare

Prin rezultatele obținute și prin analiza teoretică și practică a cercetărilor elaborate în cadrul tezei de doctorat s-au observat mai multe direcții și perspective de studiu în domeniul tezei doctorale.

O primă direcție de cercetare se îndreaptă spre extinderea sistemului de actualizare propus pentru o și mai bună reducere a impactului avut de acest proces asupra aplicațiilor de contorizare inteligentă. Se vor avea în vedere actualizări prin sisteme de operare desemnate echipamentelor integrate.

Un nou orizont de cercetare deosebit de complex îl constituie problema înglobării tehnologiilor de tip Internet of Things în cadrul rețelelor inteligente de distribuție. Actualizările de program ale contoarelor de energie ar putea beneficia de conexiunea de bandă largă a echipamentelor casnice conectate din proximitate prin standardizarea coexistenței celor două familii de echipamente.

Cercetările din teza doctorală au arătat, de asemenea, că există oportunitatea unor optimizări a transportului de date în funcție de topologia rețelei și de calitatea semnalului.

În final, securizarea și digitalizarea întregii rețele de distribuție este un domeniu vast, iar subiectul actualizării contoarelor inteligente de la distanță într-un mod robust și sigur necesită aprofundare în lucrări de cercetare viitoare.

ANEXE

A1. LISTA PUBLICAŢIILOR REZULTATE ÎN URMA CERCETĂRII DOCTORALE, PUBLICATE SAU ACCEPTATE SPRE PUBLICARE, SUB AFILIERE UPT

Lucrarea 1: "Availability Improvements through Data Slicing in PLC Smart Grid Networks"

Negîrla, P., Druta, R., & Silea, I. (2019). Availability Improvements through Data Slicing in PLC Smart Grid Networks. Sensors, 20 (24), 7256. Journal: Sensors 2020, 20(24), 7256; (Switzerland)

Lucrarea 2: "Considerations about the Signal Level Measurement in Wireless Sensor Networks for Node Position Estimation"

Dolha, S., Negîrla, P., Alexa, F., & Silea, I. (2019). Considerations about the Signal Level Measurement in Wireless Sensor Networks for Node Position Estimation. Sensors, 19(19), 4179. Journal: Sensors 2019, 19(19), 4179; (Switzerland)

Lucrarea 3: "Data Slicing Model Proposals for Low-availability Smart Metering Equipment"

P. Negirla and I. Silea (2020). Conference: 6th International Conference on Sensors and Electronic Instrumentation Advances, Porto, Portugal, Proceedings of the 2nd IFSA

Lucrarea 4: "Another approach regarding the balance between natural and manufactured ecosystems"

Paul Negirla, Sorin Nanu, Ioan Silea, Octavian Stefan (2019). Another approach regarding the balance between natural and manufactured ecosystems., SIM 2019: 15th International Symposium in Management, Sustainable management

Lucrarea 5: "A Review on Methods and Systems for Remote Collaboration"

Druta, R., Druta, C., Negirla, P., & Silea, I. (2021). A Review on Methods and Systems for Remote Collaboration. Applied Sciences, 11(21), 10035., Journal: Applied Sciences 2021, (Switzerland)

Lucrarea 7: "Students Training Through Applied Activities at Department of Automation and Applied Informatics, University Politehnica Timișoara"

Silea I., Negirla, P., & Korodi, A. (2019). Students Training Through Applied Activities at Department of Automation and Applied Informatics, University Politehnica Timișoara. *European Journal of Engineering and Formal Sciences*, *3*(2), 11-19.

Lucrarea 6: "Automatic Mapping of a Room Using LIDAR-Based Measuring Sensor."

Ungureanu, V. I., Trutiu, B. A., Silea, I., Negîrla, P., Zimbru, C., & Miclea, R. C. (2019, May). Automatic Mapping of a Room Using LIDAR-Based Measuring Sensor. In 2019 22nd International Conference on Control Systems and Computer Science (CSCS) (pp. 689-695). IEEE.

Lucrarea 8: "Guidance and control of autonomous robot in agricultural field."

S Nanu, P Negirla, S Bungescu (2019), "Guidance and control of autonomous robot in agricultural field", INMA Bucharest 2019, International Symposium, ISB-INMA-TEH, Agricultural and Mechanical Engineering, Bucharest, Romania, 31 October-1 November 2019.

Lucrarea 9: "Mobile robot platform for studying sensor fusion localization algorithms"

Paul Negirla and Mariana Nagy (2018), "Mobile robot platform for studying sensor fusion localization algorithms", SOFA 2018, Springer, Advances in Intelligent Systems and Computing

Lucrarea 10: "Sensor fusion for accurate human body temperature measurement at a distance"

P. Negirla, P. Radu and V. Suta (2020). Conference: 6th International Conference on Sensors and Electronic Instrumentation Advances, Porto, Portugal, Proceedings of the 2nd IFSA

REFERINȚE BIBLIOGRAFICE

[1] Alaton Clément, Tounquet Frédéric, Benchmarking smart metering deployment in the EU-28 with a focus on electricity, Publications Office of the European Union, 2020
[2] Over-the-Air (OTA) Updates in Embedded Microcontroller Applications: Design TradeOffs and Lessons Learned, Benjamin Bucklin Brown, Analog Dialogue 52-11, November 2018
[3] Atmel AT02333: Safe and Secure Bootloader Implementation for SAM3/4, APPLICATION NOTE, 42141A–SAM–06/2013
[4] Leon Presser and John R. White. 1972. Linkers and Loaders. ACM Comput. Surv. 4, 3 (Sept. 1972), 149–167. DOI:https://doi.org/10.1145/356603.356605
[5] David W. Barron. 2003. Linkers and loaders. Encyclopedia of Computer Science. John Wiley and Sons Ltd., GBR, 988–991.
[6] Salomon, D, 1992. Assemblers and Loaders. Chichester: Ellis Horwood
[7] H. Hejazi, H. Rajab, T. Cinkler and L. Lengyel, "Survey of platforms for massive IoT," 2018 IEEE International Conference on Future IoT Technologies (Future IoT), Eger, 2018, pp. 1-8, doi: 10.1109/FIOT.2018.8325598.
[8] J. Zheng, D. W. Gao and L. Lin, "Smart Meters in Smart Grid: An Overview," 2013 IEEE Green Technologies Conference (GreenTech), Denver, CO, 2013, pp. 57-64, doi: 10.1109/GreenTech.2013.17.
[9] Bayuk, J. (2009). "Chapter 4: Information Classification". In Axelrod, C.W.; Bayuk, J.L.; Schutzer, D. (eds.). Enterprise Information Security and Privacy. Artech House. pp. 59–70. ISBN 9781596931916.
[10] Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress. p. 240. ISBN 9780128008126.
[11] Akpeninor, James Ohwofasa (2013). Modern Concepts of Security. Bloomington, IN: AuthorHouse. p. 135. ISBN 978-1-4817-8232-6. Retrieved 18 January 2018.
[12] David Katz, Rick Gentile, Fundamentals of Booting for Embedded Processors, 2009
[13] Mohit Arora and Varun Jain, Understanding embedded system boot techniques, EDN, February 2011
[14] Wheat D. (2011) Arduino Software. In: Arduino Internals. Apress. https://doi.org/10.1007/978-1-4302-3883-6_5]

[15] Pan T., Zhu Y. (2018) Getting Started with Arduino. In: Designing Embedded Systems with Arduino. Springer, Singapore. https://doi.org/10.1007/978-981-10-4418-2_1
[16] Wheat D. (2011) Arduino Software. In: Arduino Internals. Apress. https://doi.org/10.1007/978-1-4302-3883-6_5]
[17] Pan T., Zhu Y. (2018) Getting Started with Arduino. In: Designing Embedded Systems with Arduino. Springer, Singapore. https://doi.org/10.1007/978-981-10-4418-2_1
[18] Kuzmanovic, Aleksandar; Knightly, Edward W. (2003-08-25). Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. ACM. pp. 75–86. CiteSeerX 10.1.1.307.4107. doi:10.1145/863955.863966. ISBN 978-1581137354.
[19] Burhan, Muhammad & Rehman, Rana Asif & Kim, Byung-Seo & Khan, Bilal. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors. 18. 10.3390/s18092796.
[20] Boritz, J. Efrim (2005). "IS Practitioners' Views on Core Concepts of Information Integrity". International Journal of Accounting Information Systems. Elsevier. 6 (4): 260–279. doi: 10.1016/j.accinf.2005.07.001.
[21] Glover, Neal; Dudley, Trent (1990). Practical Error Correction Design for Engineers (Revision 1.1, 2nd ed.). CO, USA: Cirrus Logic. ISBN 0-927239-00-0. ISBN 978-0-927239-00-4.
[22] Hamming, R. W. (April 1950). "Error Detecting and Error Correcting Codes". Bell System Technical Journal. USA: AT&T. 29(2): 147–160. doi:10.1002/j.1538-7305. 1950.tb00463. x.
[23] "Understanding Denial-of-Service Attacks". US-CERT. 6 February 2013. Retrieved 26 May 2016.
[24] Kumar, Bhattacharyya, Dhruba; Kalita, Jugal Kumar (2016-04-27). DDoS attacks: evolution, detection, prevention, reaction, and tolerance. Boca Raton, FL. ISBN 9781498729659. OCLC 948286117.
[25] Knuth, D. 1973, The Art of Computer Science, Vol. 3, Sorting and Searching, p.527. Addison-Wesley, Reading, MA., United States
[26] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A (1996). Handbook of Applied Cryptography. CRC Press. ISBN 978-0849385230.
[27] - Schneier, Bruce. "Cryptanalysis of MD5 and SHA: Time for a New Standard". Computerworld. 2016

[28] Ghasempour, Alireza. "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges." *Inventions* 4.1 (2019): 22.
[29] Ghasempour, Alireza. "Optimum number of aggregators based on power consumption, cost, and network lifetime in advanced metering infrastructure

architecture for Smart Grid Internet of Things." *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2016.
[30] Barai, Gouri R., Sridhar Krishnan, and Bala Venkatesh. "Smart metering and functionalities of smart meters in smart grid-a review." *2015 IEEE Electrical Power and Energy Conference (EPEC)*. IEEE, 2015.
[31] Greer, Christopher, et al. "Nist framework and roadmap for smart grid interoperability standards, release 3.0." (2014).
[32] Ministerul Energiei, "Planul Național De Acțiune În Domeniul Eficienței Energetice IV", 2020
[33] McBee, Kerry D., and Marcelo G. Simões. "Utilizing a smart grid monitoring system to improve voltage quality of customers." *IEEE Transactions on Smart Grid* 3.2 (2012): 738-743.
[34] Bhor, Dhananjay, Kavinkadhirselvan Angappan, and Krishna M. Sivalingam. "Network and power-grid co-simulation framework for Smart Grid wide-area monitoring networks." *Journal of Network and Computer Applications* 59 (2016): 274-284.
[35] Zhang, Hao-Tian, and Loi-Lei Lai. "Monitoring system for smart grid." *2012 International Conference on Machine Learning and Cybernetics*. Vol. 3. IEEE, 2012.
[36] Khan, Fahad, et al. "IoT based power monitoring system for smart grid applications." *2020 International Conference on Engineering and Emerging Technologies (ICEET)*. IEEE, 2020.
[37] Lu, Renzhi, Seung Ho Hong, and Xiongfeng Zhang. "A dynamic pricing demand response algorithm for smart grid: reinforcement learning approach." *Applied Energy* 220 (2018): 220-230.
[38] Haider, Haider Tarish, Ong Hang See, and Wilfried Elmenreich. "A review of residential demand response of smart grid." *Renewable and Sustainable Energy Reviews* 59 (2016): 166-178.
[39] Paterakis, Nikolaos G., Ozan Erdinç, and João PS Catalão. "An overview of Demand Response: Key-elements and international experience." *Renewable and Sustainable Energy Reviews* 69 (2017): 871-891.
[40] Jordehi, A. Rezaee. "Optimisation of demand response in electric power systems, a review." *Renewable and sustainable energy reviews* 103 (2019): 308-319.
[41] Uddin, Moslem, et al. "A review on peak load shaving strategies." *Renewable and Sustainable Energy Reviews* 82 (2018): 3323-3332.
[42] Lu, Renzhi, and Seung Ho Hong. "Incentive-based demand response for smart grid with reinforcement learning and deep neural network." *Applied energy* 236 (2019): 937-949.
[43] Faruqui, Ahmad, Dan Harris, and Ryan Hledik. "Unlocking the€ 53 billion savings from smart meters in the EU: How increasing the adoption of dynamic tariffs

could make or break the EU's smart grid investment." *Energy Policy* 38.10 (2010): 6222-6231.
[44] Pipattanasomporn, Manisa, Hassan Feroze, and Saifur Rahman. "Multi-agent systems in a distributed smart grid: Design and implementation." *2009 IEEE/PES Power Systems Conference and Exposition*. IEEE, 2009.
[45] Järventausta, Pertti, et al. "Smart grid power system control in distributed generation environment." *Annual Reviews in Control* 34.2 (2010): 277-286.
[46] Arritt, Robert F., and Roger C. Dugan. "Distribution system analysis and the future smart grid." *IEEE Transactions on Industry Applications* 47.6 (2011): 2343-2350.
[47] Kong, Peng-Yong, and George K. Karagiannidis. "Charging schemes for plug-in hybrid electric vehicles in smart grid: A survey." IEEE Access 4 (2016): 6846-6875.
[48] Couillet, Romain, et al. "Electrical vehicles in the smart grid: A mean field game analysis." IEEE Journal on Selected Areas in Communications 30.6 (2012): 1086-1096.
[49] Xue, Yusheng, Shumei Cui, and Qun Niu. Intelligent Computing in Smart Grid and Electrical Vehicles. Springer, 2014.
[50] Xu, Haitao, et al. "Charging control of electric vehicles in smart grid: A stackelberg differential game based approach." Mobile Networks and Applications 26.2 (2021): 562-570.
[51] Rana, Md M., et al. "Monitoring the smart grid incorporating turbines and vehicles." IEEE access 6 (2018): 45485-45492.
[52] Saputro, Nico, Kemal Akkaya, and Suleyman Uludag. "A survey of routing protocols for smart grid communications." *Computer Networks* 56.11 (2012): 2742-2771.
[53] Hossain, Ekram, Zhu Han, and H. Vincent Poor, eds. *Smart grid communications and networking*. Cambridge University Press, 2012.
[54] Yan, Ye, et al. "A survey on cyber security for smart grid communications." *IEEE Communications Surveys & Tutorials* 14.4 (2012): 998-1010.
[55] Chin, Wen-Long, Wan Li, and Hsiao-Hwa Chen. "Energy big data security threats in IoT-based smart grid communications." *IEEE Communications Magazine* 55.10 (2017): 70-75.
[56] Lopez, Gregorio, et al. "The role of power line communications in the smart grid revisited: Applications, challenges, and research initiatives." *IEEE Access* 7 (2019): 117346-117368.
[57] Dragičević, Tomislav, Pierluigi Siano, and S. R. Prabaharan. "Future generation 5G wireless networks for smart grid: A comprehensive review." *Energies* 12.11 (2019): 2140.,

[58] Tightiz, Lilia, and Hyosik Yang. "A comprehensive review on IoT protocols' features in smart grid communication." *Energies* 13.11 (2020): 2762.
[59] Saleh, Mohammed, Thair Khdour, and Mahmoud Qasaymeh. "Analysis of AMI, Smart Metering Deployment and Big Data Management Challenges." *Proceedings of the 3rd International Conference on Big Data and Internet of Things*. 2019.
[60] Ghosal, Amrita, and Mauro Conti. "Key management systems for smart grid advanced metering infrastructure: A survey." *IEEE Communications Surveys & Tutorials* 21.3 (2019): 2831-2848.
[61] Siqueira de Carvalho, Ricardo, et al. "Communication system design for an advanced metering infrastructure." *Sensors* 18.11 (2018): 3734.
[62] Kim, Dae-Kyoo, et al. "Toward interoperability of smart grids." *IEEE Communications Magazine* 55.8 (2017): 204-210.
[63] Kim, Seong-Kyu, and Jun-Ho Huh. "A study on the improvement of smart grid security performance and blockchain smart grid perspective." *Energies* 11.8 (2018): 1973.
[64] Gunduz, Muhammed Zekeriya, and Resul Das. "Cyber-security on smart grid: Threats and potential solutions." *Computer networks* 169 (2020): 107094.
[65] Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International Journal of Critical Infrastructure Protection* 25 (2019): 36-49.
[66] Sarma, Sanjay. "The networked physical world-proposal for engineering the next generation of computing, commerce and automatic-identification." (2000).
[67] Gershenfeld, Neil, Raffi Krikorian, and Danny Cohen. "The internet of things." *Scientific American* 291.4 (2004): 76-81.
[68] L. Atzori, A. Iera, and G. Morabito, "The Internet-of-Things: A Survey," Computer Networks, vol. 54, no. 15, Oct. 2010, pp. 2787–805.
[69] Babu, B. Sobhan, et al. "IoT for healthcare." *International Journal of Science and Research* 5.2 (2016): 322-326.
[70] Kodali, Ravi Kishore, Govinda Swamy, and Boppana Lakshmi. "An implementation of IoT for healthcare." *2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*. IEEE, 2015.
[71] Darshan, K. R., and K. R. Anandakumar. "A comprehensive review on usage of Internet of Things (IoT) in healthcare system." *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*. IEEE, 2015.
[72] Zantalis, Fotios, et al. "A review of machine learning and IoT in smart transportation." *Future Internet* 11.4 (2019): 94.

[73] He, Wu, Gongjun Yan, and Li Da Xu. "Developing vehicular data cloud services in the IoT environment." *IEEE transactions on industrial informatics* 10.2 (2014): 1587-1595.
[74] Al-Emran, Mostafa, Sohail Iqbal Malik, and Mohammed N. Al-Kabi. "A survey of internet of things (IoT) in education: opportunities and challenges." *Toward social internet of things (SIoT): Enabling technologies, architectures and applications* (2020): 197-209.
[75] Zhamanov, Azamat, et al. "IoT smart campus review and implementation of IoT applications into education process of university." *2017 13th International Conference on Electronics, Computer and Computation (ICECCO)*. IEEE, 2017.
[76] Marquez, Jack, et al. "IoT in education: Integration of objects with virtual academic communities." *New Advances in Information Systems and Technologies*. Springer, Cham, 2016. 201-212.
[77] Viswanath, Sanjana Kadaba, et al. "System design of the internet of things for residential smart grid." *IEEE Wireless Communications* 23.5 (2016): 90-98.
[78] Saleem, Yasir, et al. "Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions." *IEEE Access* 7 (2019): 62962-63003.
[79] Hashmi, Shahwaiz Ahmed, Chaudhry Fahad Ali, and Saima Zafar. "Internet of things and cloud computing-based energy management system for demand side management in smart grid." *International Journal of Energy Research* 45.1 (2021): 1007-1022.
[80] Li, Wenjia, Houbing Song, and Feng Zeng. "Policy-based secure and trustworthy sensing for internet of things in smart cities." *IEEE Internet of Things Journal* 5.2 (2017): 716-723.
[81] Yun, Miao, and Bu Yuxin. "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid." *2010 International Conference on Advances in Energy Engineering*. IEEE, 2010.
[82] Greer, Christopher, et al. "Nist framework and roadmap for smart grid interoperability standards, release 3.0." (2014).
[83] Lu, Yang, Savvas Papagiannidis, and Eleftherios Alamanos. "Internet of Things: A systematic review of the business literature from the user and organisational perspectives." *Technological Forecasting and Social Change* 136 (2018): 285-297.
[84] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks and K. Wang, "Review of Internet of Things (IoT) in Electric Power and Energy Systems," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 847-870, 2018
[85] Sohraby, Kazem, et al. "A review of wireless and satellite-based m2m/iot services in support of smart grids." *Mobile Networks and Applications* 23.4 (2018): 881-895.

[86] Al-Ali, A. R. "Role of internet of things in the smart grid technology." *Journal of Computer and Communications* 3.05 (2015): 229.
[87] Lo, Chun-Hao, and Nirwan Ansari. "The progressive smart grid system from both power and communications aspects." *IEEE Communications Surveys & Tutorials* 14.3 (2011): 799-821.
[88] Xiang, Wang, Marc St-Hilaire, and Thomas Kunz. "Roadmap of future smart grid, smart home, and smart appliances." *Carleton University: Canada* (2011).
[89] Yousuf, Muhammad Salman, and Mustafa El-Shafei. "Power line communications: An overview-part i." *2007 Innovations in Information Technologies (IIT)*. IEEE, 2007.
[90] Vigneron, J., and K. Razazian. "G3-PLC Powerline Communication Standard for Todays Smart Grid." *G3-PLC Alliance, 2012, Maxim Integrated* (2012).
[91] PRIME Alliance Technical Working Group, "Draft Standard for PoweRline Intelligent Metering Evolution (PRIME) " , 1.3A ed., (2010)
[92] Sendin, Alberto, Ivan Peña, and Pablo Angueira. "Strategies for power line communications smart metering network deployment." *Energies* 7.4 (2014): 2377-2420.
[93] Covrig, Catalin Felix, et al. "Smart grid projects outlook 2014." *Joint Research Centre of the European Commission: Petten, The Netherlands* (2014).
[94] Sood, Vijay K., et al. "Developing a communication infrastructure for the smart grid." *2009 IEEE Electrical power & energy conference (EPEC)*. IEEE, 2009.
[95] Safaric, Stanislav, and Kresimir Malaric. "ZigBee wireless standard." *Proceedings ELMAR 2006*. IEEE, 2006.
[96] Geelen, Daniel, et al. "A wireless mesh communication protocol for smart-metering." *2012 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2012.
[97] Thomas, Lee, and Nicholas Jenkins. "Smart metering for development and operation of the GB power system." *HubNet Website* (2014).
[98] Dragičević, Tomislav, Pierluigi Siano, and S. R. Prabaharan. "Future generation 5G wireless networks for smart grid: A comprehensive review." *Energies* 12.11 (2019): 2140.
[99] Leligou, Helen C., et al. "Smart Grid: a demanding use case for 5G technologies." *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 2018.
[100] Sofana, Reka S., et al. "Future Generation 5G Wireless Networks for Smart Grid: A Comprehensive Review." *Energies* 12.11 (2019): 2140.
[101] Uribe-Pérez, Noelia, et al. "State of the art and trends review of smart metering in electricity grids." *Applied Sciences* 6.3 (2016): 68.

[102] Andreadou, Nikoleta, Miguel Olariaga Guardiola, and Gianluca Fulli. "Telecommunication technologies for smart grid projects with focus on smart metering applications." *Energies* 9.5 (2016): 375.
[103] Yigit, Melike, et al. "Power line communication technologies for smart grid applications: A review of advances and challenges." *Computer Networks* 70 (2014): 366-383.
[104] Wang, Jing, Ratan K. Ghosh, and Sajal K. Das. "A survey on sensor localization." *Journal of Control Theory and Applications* 8.1 (2010): 2-11.
[105] Cheng, Long, et al. "Real time indoor positioning system for smart grid based on UWB and artificial intelligence techniques." *2020 IEEE Conference on Technologies for Sustainability (SusTech)*. IEEE, 2020.
[106] Yassin, Ali, et al. "Recent advances in indoor localization: A survey on theoretical approaches and applications." *IEEE Communications Surveys & Tutorials* 19.2 (2016): 1327-1346.
[107] Jiang, Huaiguang, Jun Jason Zhang, and David W. Gao. "Fault localization in smart grid using wavelet analysis and unsupervised learning." *2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*. IEEE, 2012.
[108] Passerini, Federico, and Andrea M. Tonello. "Smart grid monitoring using power line modems: Anomaly detection and localization." *IEEE Transactions on Smart Grid* 10.6 (2019): 6178-6186
[109] Sandoval, Ruben M., Antonio-Javier Garcia-Sanchez, and Joan Garcia-Haro. "Improving RSSI-based path-loss models accuracy for critical infrastructures: A smart grid substation case-study." *IEEE Transactions on Industrial Informatics* 14.5 (2017): 2230-2240.
[110] Langer, Lucie, et al. "From old to new: Assessing cybersecurity risks for an evolving smart grid." *computers & security* 62 (2016): 165-176.
[111] Ray, Partha Datta, Rajgopal Harnoor, and Mariana Hentea. "Smart power grid security: A unified risk management approach." *44th Annual 2010 IEEE international Carnahan conference on security technology*. IEEE, 2010.
[112] Kolehmainen, Antti. "Secure firmware updates for IoT: a survey." *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018.
[113] Gerzo, Daniel. "Introduction to NanoBSD." *The FreeBSD Documentation Project* (2006).
[114] Schmidt, Silvie, et al. "Secure firmware update over the air in the internet of things focusing on flexibility and feasibility." *Internet of Things Software Update Workshop (IoTSU). Proceeding*. 2016.

[115] Feng, Tuo. *Zigbee-based firmware updating algorithms in smart home environment*. Diss. University of Essex, 2017.
[116] Galli, Stefano, and Thierry Lys. "Next generation narrowband (under 500 kHz) power line communications (PLC) standards." *China Communications* 12.3 (2015): 1-8.
[117] Herbold, Florian, et al. "Secure Software Updates: Challenges and Solutions for Embedded IoT Systems." *9 th Prague Embedded Systems Workshop*. 2021.
[118] Lee, Boohyung, et al. "Firmware verification of embedded devices based on a blockchain." *international conference on heterogeneous networking for quality, reliability, security and robustness*. Springer, Cham, 2016.
[119] Keleman, Levon, et al. "Secure firmware update in embedded systems." *2019 IEEE 9th International Conference on Consumer Electronics (ICCE-Berlin)*. IEEE, 2019.
[120] Lee, Robert P., Konstantinos Markantonakis, and Raja Naeem Akram. "Binding hardware and software to prevent firmware modification and device counterfeiting." *Proceedings of the 2nd ACM international workshop on cyber-physical system security*. 2016.
[121] Kumar, Sudeendra K., et al. "A novel holistic security framework for in-field firmware updates." *2018 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)*. IEEE, 2018.
[122] Guillen, Oscar, et al. "Crypto-Bootloader–Secure in-field firmware updates for ultra-low power MCUs." *Texas Instruments Incorporated* (2015).
[123] Jain, Neha, Swapnil G. Mali, and Suhas Kulkarni. "Infield firmware update: Challenges and solutions." *2016 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, 2016.
[124] Hagan, Matthew, et al. "Enforcing policy-based security models for embedded SoCs within the internet of things." *2018 IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE, 2018.
[125] Shepherd, Carlton, et al. "Secure and trusted execution: Past, present, and future-a critical review in the context of the internet of things and cyber-physical systems." *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, 2016.
[126] Bettayeb, Meriem, Qassim Nasir, and Manar Abu Talib. "Firmware update attacks and security for IoT devices: Survey." *Proceedings of the ArabWIC 6th Annual International Conference Research Track*. 2019.
[127] Zandberg, Koen, et al. "Secure firmware updates for constrained iot devices using open standards: A reality check." *IEEE Access* 7 (2019): 71907-71920.
[128] Toiviainen, Aarno. "Over-the-air firmware update for mission critical embedded devices." (2020).

[129] Obermaier, Johannes, and Stefan Tatschner. "Shedding too much light on a microcontroller's firmware protection." *11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17)*. 2017.
[130] Benkraouda, Hadjer, et al. "Snifu: Secure network interception for firmware updates in legacy plcs." *2020 IEEE 38th VLSI Test Symposium (VTS)*. IEEE, 2020.
[131] Zhu, Ruijin, et al. "A methodology for determining the image base of ARM-based industrial control system firmware." *International Journal of Critical Infrastructure Protection* 16 (2017): 26-35.
[132] Asokan, N., et al. "ASSURED: Architecture for secure software update of realistic embedded devices." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 37.11 (2018): 2290-2300.
[133] Doddapaneni, Krishna, et al. "Secure fota object for iot." *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*. IEEE, 2017.
[134] Yohan, Alexander, Nai-Wei Lo, and Suttawee Achawapong. "Blockchain-based firmware update framework for internet-of-things environment." *Proceedings of the International Conference on Information and Knowledge Engineering (IKE)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2018
[135] He, Xinchi, et al. "Securing Over-The-Air IoT Firmware Updates using Blockchain." *Proceedings of the International Conference on Omni-Layer Intelligent Systems*. 2019.
[136] Ortu, Marco, Matteo Orrú, and Giuseppe Destefanis. "On comparing software quality metrics of traditional vs blockchain-oriented software: An empirical study." *2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE, 2019.
[137] Arakadakis, Konstantinos, et al. "Firmware over-the-air programming techniques for IoT networks--a survey." *arXiv preprint arXiv:2009.02260* (2020).
[138] Panta, Rajesh Krishna, and Saurabh Bagchi. "Hermes: Fast and energy efficient incremental code updates for wireless sensor networks." *IEEE INFOCOM 2009*. IEEE, 2009.
[139] Frisch, Dustin, Sven Reißmann, and Christian Pape. "An over the air update mechanism for ESP8266 microcontrollers." *Proc. 12th Int. Conf. Syst. Netw. Commun.(ICSNC)*. 2017.
[140] Tal, Arie. "Two flash technologies compared: NOR vs NAND." *White Paper of M-SYstems* (2002).
[141] Kachman, Ondrej. "Effective Multiplatform Firmware Update Process for Embedded Low-Power Devices." (2018).
[142] Reijers, Niels, and Koen Langendoen. "Efficient code distribution in wireless sensor networks." *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*. 2003.

[143] Pallister, James, et al. "A high-level model of embedded flash energy consumption." *2014 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES)*. IEEE, 2014.
[144] Zhu, Hongliang, et al. "Detection of selective forwarding attacks based on adaptive learning automata and communication quality in wireless sensor networks." *International Journal of Distributed Sensor Networks* 14.11 (2018): 1550147718815046.
[145] Aschenbruck, Nils, et al. "Selective and secure over-the-air programming for wireless sensor networks." *2012 21st International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2012.
[146] Farooq, Muhammad Omer, and Thomas Kunz. "Operating systems for wireless sensor networks: A survey." *Sensors* 11.6 (2011): 5900-5930.
[147] Hahm, Oliver, et al. "Operating systems for low-end devices in the internet of things: a survey." *IEEE Internet of Things Journal* 3.5 (2015): 720-734.
[148] Halder, Subir, Amrita Ghosal, and Mauro Conti. "Secure over-the-air software updates in connected vehicles: A survey." *Computer Networks* 178 (2020): 107343.
[149] Villegas, Mónica M., and Hernán Astudillo. "OTA updates mechanisms: a taxonomy and techniques catalog." *XXI Simposio Argentino de Ingeniería de Software (ASSE 2020)-JAIIO 49 (Modalidad virtual)*. 2020.
[150] Kim, Jin Cheol, Young Eok Kim, and Tae Hun Kim. "Implementation of Secure GOOSE Protocol using HSM." Applied Mechanics and Materials. Vol. 260. Trans Tech Publications Ltd, 2013.
[151] Metke, Anthony R., and Randy L. Ekl. "Security technology for smart grid networks." IEEE Transactions on Smart Grid 1.1 (2010): 99-107.
[152] Nicanfar, Hasen, et al. "Efficient authentication and key management mechanisms for smart grid communications." IEEE systems journal 8.2 (2013): 629-640.
[153] Butin, Denis. "Hash-based signatures: State of play." IEEE security & privacy 15.4 (2017): 37-43.
[154] Huynh-Van, Dang, et al. "Towards an integration of AES cryptography into Deluge dissemination protocol for securing IoTs reconfiguration." 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF). IEEE, 2019.
[155] Hyun, Sangwon, Kun Sun, and Peng Ning. "FEC-Seluge: Efficient, reliable, and secure large data dissemination using erasure codes." Computer Communications 104 (2017): 191-203.
[156] Wang, Yinfang, et al. "FIRMWARE COMPRESSION MECHANISM FOR SPEEDING UP FIRMWARE UPDATING IN A RESOURCE RESTRICTED NETWORK." (2019).

[157] Onuma, Yutaka, Yoshiaki Terashima, and Ryozo Kiyohara. "Compression method for ECU software updates." 2017 Tenth International Conference on Mobile Computing and Ubiquitous Network (ICMU). IEEE, 2017.
[158] Lehniger, Kai, and Stefan Weidling. "The Impact of Diverse Execution Strategies on Incremental Code Updates for Wireless Sensor Networks." SENSORNETS. 2019.
[159] Zhang, Chi, et al. "Live code update for IoT devices in energy harvesting environments." 2016 5th Non-Volatile Memory Systems and Applications Symposium (NVMSA). IEEE, 2016.
[160] Dalai, Sovan, et al. "Microcontroller based remote updating system using voice channel of cellular network." 2015 IEEE Power, Communication and Information Technology Conference (PCITC). IEEE, 2015.
[161] Perito, Daniele, and Gene Tsudik. "Secure code update for embedded devices via proofs of secure erasure." European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2010.
[162] Karame, Ghassan O., and Wenting Li. "Secure erasure and code update in legacy sensors." International Conference on Trust and Trustworthy Computing. Springer, Cham, 2015.
[163] Aman, Muhammad Naveed, Uzair Javaid, and Biplab Sikdar. "IoT-Proctor: A Secure and Lightweight Device Patching Framework for Mitigating Malware Spread in IoT Networks." IEEE Systems Journal (2021).
[164] Pham, Minh, and Kaiqi Xiong. "A survey on security attacks and defense techniques for connected and autonomous vehicles." Computers & Security (2021): 102269.
[165] Jurkovic, Goran, and Vlado Sruk. "Remote firmware update for constrained embedded systems." 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2014.
[166] Lee, Boohyung, et al. "Firmware verification of embedded devices based on a blockchain." international conference on heterogeneous networking for quality, reliability, security and robustness. Springer, Cham, 2016.
[167] Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: Current status, classification and open issues." Telematics and informatics 36 (2019): 55-81.
[168] Lee, Younghun, et al. "A blockchain-based smart home gateway architecture for preventing data forgery." Human-centric Computing and Information Sciences 10.1 (2020): 1-14.
[169] Toiviainen, Aarno. "Over-the-air firmware update for mission critical embedded devices." (2020).

[170] Krishnamurthi, Rajalakshmi, Raghav Maheshwari, and Rishabh Gulati. "Deploying Deep Learning Models via IOT Deployment Tools." 2019 Twelfth International Conference on Contemporary Computing (IC3). IEEE, 2019.
[171] Botez, Robert, et al. "Containerized Application for IoT Devices: Comparison between balenaCloud and Amazon Web Services Approaches." 2020 International Symposium on Electronics and Telecommunications (ISETC). IEEE, 2020.
[172] Moran, Brendan, et al. A Firmware Update Architecture for Internet of Things. RFC 9019. IETF, 2021.
[173] Moran, Brendan, et al., A Concise Binary Object Representation (CBOR)-based Serialization Format for the Software Updates for Internet of Things (SUIT) Manifest, IETF, 2021
[174] Banegas, Gustavo, et al. "Quantum-Resistant Security for Software Updates on Low-power Networked Embedded Devices." arXiv preprint arXiv:2106.05577, 2021.
[175] Sahlmann, Kristina, et al. "MUP: Simplifying Secure Over-The-Air Update with MQTT for Constrained IoT Devices." Sensors 21.1, 2021: 10.
[176] Hernández-Ramos, José L., et al. "Updating IoT devices: challenges and potential approaches." 2020 Global Internet of Things Summit (GIoTS). IEEE, 2020.
[177] Pukkila, Sami-Petteri. "Secure over-the-air updates for wireless Internet-of-Things devices.", 2020.
[178] Gündoğan, Cenk, et al. "Reliable firmware updates for the information-centric internet of things." Proceedings of the 8th ACM Conference on Information-Centric Networking. 2021.
[179] Kolehmainen, Antti. "Secure firmware updates for IoT: a survey." 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018.
[180] Zandberg, Koen, et al. "Secure firmware updates for constrained iot devices using open standards: A reality check." IEEE Access 7 (2019): 71907-71920.
[181] Alladi, Tejasvi, et al. "Consumer IoT: Security vulnerability case studies and solutions." IEEE Consumer Electronics Magazine 9.2, 2020: 17-25.
[182] Felser, Meik, et al. "Dynamic software update of resource-constrained distributed embedded systems." Embedded System Design: Topics, Techniques and Trends. Springer, Boston, MA, 2007. 387-400.
[183] Uddin, Muhammad Inshal, and Muhammad Khurram. "Over-the-air Programming for Low Cost, Small Scale WSNs based on ZigBee Protocol."
[184] Mischie, Septimiu, and Robert Pazsitka. "Designing a MSP430 Bootloader." 2019 International Conference on Applied Electronics (AE). IEEE, 2019.
[185] Guillen, Oscar, et al. "Crypto-Bootloader–Secure in-field firmware updates for ultra-low power MCUs." Texas Instruments Incorporated (2015).

[186] Vasile, Sebastian, David Oswald, and Tom Chothia. "Breaking all the things—A systematic survey of firmware extraction techniques for IoT devices." International Conference on Smart Card Research and Advanced Applications. Springer, Cham, 2018.
[187] Yuan, Shenghao, and Jean-Pierre Talpin. "Verified functional programming of an IoT operating system's bootloader." MEMOCODE 2021-19th ACM-IEEE International Conference on Formal Methods and Models for System Design. 2021.
[188] Schmidt, Silvie, et al. "Secure firmware update over the air in the internet of things focusing on flexibility and feasibility." Internet of Things Software Update Workshop (IoTSU). Proceeding, 2016.
[189] UM1530 Smart meter demonstration board with DLMS/COSEM using ST7570 S-FSK modem with STM32™ and SPEAr™, Doc ID 022957 Rev 1, 2012. DS10969 Rev 5, Datasheet STM32L475xx, STMicroelectronics, Rev 5, 2019.
[190] SR EN 50470-1:2007 EN 50470-1:2006 Echipamente de măsurare a energiei electrice (c.a.). Standard european, 2007
[191] IEC 62053:1998, Electricity metering equipment (a.c.) - Particular requirements, IEC, 1998
[192] Chakravarty, Tridib, and Phil Koopman. "Performance of cyclic redundancy codes for embedded networks." (2001).
[193] Urien, Pascal. "Integrity Issues for IoT: From Experiment to Classification Introducing Integrity Probes." IoTBDS. 2019.
[194] Ge, Qianqian, and Feng Chen. "Strategies for Implementing SSL on Embedded System." 2008 International Seminar on Future BioMedical Information Engineering. IEEE, 2008.
[195] Rivest, Ronald, and S. Dusse. "The MD5 message-digest algorithm." (1992): 330-344.
[196] Osvik, Dag Arne, et al. "Fast software AES encryption." International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 2010.
[197] Dhobi, Rahul, et al. "Secure Firmware Update over the Air using TrustZone." 2019 Innovations in Power and Advanced Computing Technologies (i-PACT). Vol. 1. IEEE, 2019.
[198] Pareschi, Fabio, Gianluca Setti, and Riccardo Rovatti. "A macro-model for the efficient simulation of an ADC-based RNG." 2005 IEEE International Symposium on Circuits and Systems. IEEE, 2005.
[199] Negirla, P.; Silea, I. Data Slicing Model Proposals for Low-availability Smart Metering Equipment. In Proceedings of the 6th International Conference on Sensors Engineering and Electronics Instrumentation Advances (SEIA' 2020), Porto, Portugal, 23–25 September 2020; pp. 123–126.
[200] Negirla, P., Druță, R., & Silea, I. (2020). Availability Improvements through Data Slicing in PLC Smart Grid Networks. Sensors, 20(24), 7256

[201] Snyder, A.F.; Rankin, B.; Snyder, I.B.; Swain, T. The Realities of Testing Meter Firmware Upgradeability. In Proceedings of the 2014 Clemson University Power Systems Conference, Institute of Electrical and Electronics Engineers (IEEE), Clemson, SC, USA, 11–14 March 2014; pp. 1–5.
[202] Chan, J.; Ip, R.; Cheng, K.; Chan, K.S. Advanced Metering Infrastructure Deployment and Challenges. In Proceedings of the 2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia), IEEE, Bangkok, Thailand, 20–23 March, 2019; pp. 435–439.
[203] Gupta, B.B.; Akhtar, T. A survey on smart power grid: Frameworks, tools, security issues, and solutions. Ann. Telecommun. 2017, 72, 517–549.
[204] European Commission. Benchmarking Smart Metering Deployment in the EU-27 with a Focus on Electricity; Publications Office of the European Union: Luxembourg, 2016.
[205] European Comission. Staff Working Document, Cost-benefit Analyses & State of Play of Smart Metering Deployment in the EU-27; Publications Office of the European Union: Luxembourg, 2016.
[206] Data Communication Company. Consultation on the Delivery Plan for DCC Release 2.0, Version 1.0; 2020.
[207] Passerini, F.; Tonello, A.M. Secure PHY layer key generation in the asymmetric power line communication channel. Electronics 2020, 9, 605.
[208] Jang, J.; Jung, I.Y. Sustainable and practical firmware upgrade for wireless access point using password-based authentication. Sustainability 2016, 8, 876.
[209] Mlynek, P.; Misurec, J.; Silhavy, P.; Fujdiak, R.; Slacik, J.; Hasirci, Z. Simulation of achievable data rates of broadband power line communication for smart metering. Appl. Sci. 2019, 9, 1527.
[210] Andreadou, N.; Guardiola, M.O.; Fulli, G. Telecommunication technologies for smart grid projects with focus on smart metering applications. Energies 2016, 9, 375.
[211] Tightiz, L.; Yang, H. A comprehensive review on IoT protocols' features in smart grid communication. Energies 2020, 13, 2762.
[212] Baumeister, T. Literature Review on Smart Grid Cyber Security; Collaborative Software Development Laboratory at the University of Hawaii: Honolulu, HI, USA, 2010.
[213] Asghar, M.R.; Dan, G.; Miorandi, D.; Chlamtac, I. Smart meter data privacy: A survey. IEEE Commun. Surv. Tutor. 2017, 19, 2820–2835.
[214] Ahmed, S.; Gondal, T.M.; Adil, M.; Malik, S.A.; Qureshi, R. A Survey on Communication Technologies in Smart Grid. In Proceddings of the 2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia), IEEE, Bangkok, Thailand, 20–23 March, 2019; pp. 7–12.

[215] Arnold, G.W.; Wollman, D.A.; FitzPatrick, G.J.; Prochaska, D.; Holmberg, D.G.; Su, D.H.; Hefner, Jr, A.R.; Golmie, N.T.; Brewer, TL.; et al. NIST Framework and Roadmap for Smart Grid Interoperability Standards; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2010.
[216] Fang, Xi; Misra, S.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. IEEE Commun. Surv. Tutor. 2011, 14, 944–980.
[217] Mahadevan, R.; Kadati, S.H.; Chandrasekhar S.; Sindganhupe, S. Satellite communications for rural smart grid. J. Commun. 2012, 2012, 19-30.
[218] Ritoša, P.; Pikl, P.; Mlinar, R.; Jenko, P.; Droftina, U.; Anzic, J.; Sernec, R.; Pratas, N.; Skrt, G.; Jurse, J.; et al. Traffic Modelling, Communication Requirements and Candidate Network Solutions for Real-Time Smart Grid Control; Sunseed Deliverable Report: Ljubljana, Slovenia, 2015.
[219] Kearney, A.T. Smart Metering in Romania, 3 September 2012. Romanian Authority for Energy Regulation: Bucharest, Romania, 2012.
[220] Hoch, M. Comparison of PLC G3 and PRIME. In Proceedings of the 2011 IEEE International Symposium on Power Line Communications and Its Applications, IEEE, Udine, Italy, 3–6 April 2011; pp. 165–169.
[221] Matanza, J.; Alexandres, S.; Rodriguez-Morcillo, C. Performance evaluation of two narrowband PLC systems: PRIME and G3. Comput. Stand. Interfaces 2013, 36, 198–208.
[222] A Da Rocha Farias, L.; Monteiro, L.F.; Leme, M.O.; Stevan, S.L., Jr. Empirical Analysis of the Communication in Industrial Environment Based on G3-Power Line Communication and Influences from Electrical Grid. Electronics 2018, 7, 194.
[223] Guyard, P.; Fiorelli, R.; Houee, J. AN4732 Application Note STCOMET Smart Meter and Power Line Communication System-on-Chip Development Kit; STMicroelectronics: Geneva, Switzerland, 2017.
[224] Hornig, C. A Standard for the Transmission of IP Datagrams over Ethernet Networks, STD 41, RFC 894; Symbolics Cambridge Research Center: Cambridge, MA, USA, 1984.
[225] STMicroelectronics. EVLKSTCOMET10-1 ST Smart Meter System-on-Chip Development Kit Data Brief, Doc ID028546 Rev 2; STMicroelectronics: Geneva, Switzerland, 2017.
[226] Sendin, A.; Berganza, I.; Arzuaga, A.; Pulkkinen, A.; Kim II, H. Performance Results from 100,000+ PRIME Smart Meters Deployment in Spain. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), IEEE, Tainan, Taiwan, 5–8 November 2012; pp. 145–150.
[227] Prime Alliance Technical Working Group. Draft Specification for Powerline Intelligent Metering Evolution. versión 1.3, 2013, 6.

[228] Jalil, S.Q.; Chalup, S.; Mubashir, R.H. A Smart Meter Firmware Update Strategy Through Network Coding for AMI Network. In Proceedings of the International Conference on Smart Grid and Internet of Things, Niagara Falls, ON, Canada, 11 July 2018; pp. 68–77.
[229] Katzir, L.; Schwartzman, I. Secure Firmware Updates for Smart Grid Devices. In Proceedings of the 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, IEEE, Manchester, UK, 5–7 December, 2011; pp. 1–5.
[230] Kim, Y.-J.; Oh, D.-E.; Ko, J.-M.; Kang, S.-J.; Choi, S.-H. A Remote Firmware Upgrade Method of NAN and HAN Devices to Support AMI's Energy Services. In Proceedings of the International Conference on Hybrid Information Technology, Daejeon, Korea, 22–24 September 2011; pp. 303–310.
[231] Rinaldi, S.; Ferrari, P.; Flammini, A.; Rizzi, M.; Sisinni, E.; Vezzoli, A. Performance analysis of power line communication in industrial power distribution network. Comput. Stand. Interfaces 2015, 42, 9–16.
[232] Sörries, B. Communication Technologies and Networks for Smart Grid and Smart Metering. Rapport for CDMA Development Group 450 Connectivity Special Interest Group (450 SIG), 2013.
[233] Kabalci, Y. A survey on smart metering and smart grid communication. Renew. Sustain. Energy Rev. 2016, 57, 302–318.
[234] El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. Comput. Electr. Eng. 2018, 67, 469–482.
[235] Erdogan, S.Z.; Hussain, S.; Park, J.-H. Intelligent Monitoring using Wireless Sensor Networks. In Emerging Directions in Embedded and Ubiquitous Computing; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4809, pp. 389–400, doi:10.1007/978-3-540-77090-9_35.
[236] Hussain, S.; Peters, R.; Silver, D. Using Received Signal Strength Variation for Surveillance in Residential Areas. In Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security; SPIE: Orlando, FL, USA, 2008; Volume 6973, p. 1982, doi:10.1117/12.778008.
[237] Moreno, C.D.; Brox-Jiménez, M.; Gersnoviez-Milla, A.A.; Márquez-Moyano, M.; Ortiz-López, M.A.; Quiles-Latorre, F.J. Wireless Sensor Network for Sustainable Agriculture. Proceedings 2018, 2, 1302.
[238] Sadowski, S.; Spachos, P. RSSI-Based Indoor Localization with the Internet of Things. IEEE Access 2018, 6, 30149–30161, doi:10.1109/ACCESS.2018.2843325.
[239] LN Nguyen, T.; Shin, Y. An Efficient RSS Localization for Underwater Wireless Sensor Networks. Sensors 2019, 19, 3105, doi:10.3390/s19143105.
[240] Han, Y.; Zhang, J.; Sun, D. Error control and adjustment method for underwater wireless sensor network localization. Appl. Acoust. 2018, 130, 293–299, doi:10.1016/j.apacoust.2017.08.007.

[241] Guidara, A.; Fersi, G.; Derbel, F.; Jemaa, M. Impacts of Temperature and Humidity variations on RSSI in indoor Wireless Sensor Networks. Procedia Comput. Sci. 2018, 126, 1072–1081, doi:10.1016/j.procs.2018.08.044.
[242] Mitton, N. QoS in Wireless Sensor Networks. Sensors 2018, 18, 3983, doi:10.3390/s18113983.
[243] Zhang, L.; Yang, Z.; Zhang, S.; Yang, H. Three-Dimensional Localization Algorithm of WSN Nodes Based on RSSI-TOA and Single Mobile Anchor Node. J. Electr. Comput. Eng. 2019, 2019, 1–8, doi:10.1155/2019/4043106.
[244] Bianchi, V.; Ciampolini, P.; de Munari, I. RSSI-Based Indoor Localization and Identification for ZigBee Wireless Sensor Networks in Smart Homes. IEEE Trans. Instrum. Meas. 2019, 68, 1–10, doi:10.1109/TIM.2018.2851675.
[245] Farooq-i-Azam, M.; Ayyaz, M.N. Location and position estimation in wireless sensor networks. In Wireless Sensor Networks: Current Status and Future Trends; CRC Press: 2012, doi:10.1201/b13092-12.
[246] Jia, Z.; Guan, B. Received signal strength difference–based tracking estimation method for arbitrarily moving target in wireless sensor networks. Int. J. Distrib. Sens. Netw. 2018, 14, doi:10.1177/1550147718764875.
[247] Sun, Y.; Zhang, F.; Wan, Q. Wireless Sensor Network Based Localization Method Using TDOA Measurements in MPR. IEEE Sens. J. 2019, 19, 3741–3750, doi:10.1109/JSEN.2019.2892652.
[248] Chen, H.; Tan, G. Adaptive iteration localization algorithm based on RSSI in wireless sensor networks. Clust. Comput. 2018, 1–9, doi:10.1007/s10586-018-1875-y.
[249] Schulten, H.; Kuhn, M.; Heyn, R.; Dumphart, G.; Trosch, F.; Wittneben, A. On the Crucial Impact of Antennas and Diversity on BLE RSSI-Based Indoor Localization. In Proceedings of the IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019.
[250] Ahmadi, H.; Viani, F.; Bouallegue, R. An accurate Prediction Method for Moving Target Localization and Tracking in Wireless Sensor Networks. Ad Hoc Netw. 2018, 70, 14–22.
[251] Goldoni, E.; Prando, L.; Vizziello, A.; Savazzi, P.; Gamba, P. Experimental data set analysis of RSSI-based indoor and outdoor localization in LoRa networks. Internet Technol. Lett. 2019, 2, e75, doi:10.1002/itl2.75.
[252] Mazuelas, S.; Bahillo, A.; Lorenzo, R.; Fernandez, P.; Lago, F.; Garcia, E.; Blas, J.; Abril, E. Robust Indoor Positioning Provided by Real-Time RSSI Values in Unmodified WLAN networks. IEEE J. Sel. Top. Signal Process. 2009, 3, 821–831, doi:10.1109/JSTSP.2009.2029191.
[253] Liu, Q.; Ren, P.; Zhou, Z. Three-dimensional Accurate Positioning Algorithm Based on Wireless Sensor Networks. J. Comput. 2011, 6, 2582–2589, doi:10.4304/jcp.6.12.2582-2589.

[254] Shu, J.; Gong, J.; Chen, Y.; Liu, L. BR2OM: RSSI Based Refinement and Optimization Mechanism for Wireless Sensor Networks. J. Netw. 2009, 4, 1017–1025, doi:10.4304/jnw.4.10.1017-1025.
[255] Texas Instruments. Low Cost, Low Power 2.4 Ghz RF Transceiver. Available online: http://www.ti.com/lit/ds/symlink/cc2500.pdf (accessed on 24 September 2019).
[256] Texas Instruments. Programming Output Power on CC2500 and CC2550. Available online: http://www.ti.com/lit/an/swra152/swra152.pdf (accessed on 24 September 2019).
[257] Zafer, S.; Hussain, S. Using Received Signal Strength Variation for Energy Efficient Data Dissemination in Wireless Sensor Networks. In Proceedings of the 18th International Conference on Database and Expert System Applications, Regensburg, Germany, 3–7 September 2007; pp. 620–624, doi:10.1109/DEXA.2007.149.
[258] Malajner, M.; Benkic, K.; Planinsic, P. A New Study Regarding the Comparison of Calculated and Measured RSSI Values under Different Experimental Conditions. Prz. Elektrotechniczny 2013, 89, 214–219.
[259] Negirla, Paul, Romina Druță, and Ioan Silea. "Availability Improvements through data slicing in PLC smart grid networks." *Sensors* 20, no. 24, 2020;
[260] Dolha, Stelian, Paul Negirla, Florin Alexa, and Ioan Silea. "Considerations about the signal level measurement in wireless sensor networks for node position estimation." *Sensors* 19, no. 19, 2019;
[261] Negirla, P.; Silea, I. Data Slicing Model Proposals for Low-availability Smart Metering Equipment. In Proceedings of the 6th International Conference on Sensors Engineering and Electronics Instrumentation Advances (SEIA' 2020), Porto, Portugal, 23–25 September 2020;
[262] Druta, Romina, et al. "A Review on Methods and Systems for Remote Collaboration." *Applied Sciences* 11.21, 2021;
[263] Negirla, Paul, Sorin Nanu, Ioan Silea, and Octavian Stefan. "Another Approach Regarding the Balance Between Natural and Manufactured Ecosystems." In *International Symposium in Management Innovation for Sustainable Management and Entrepreneurship*, pp. 171-181. Springer, Cham, 2019;
[264] Silea, Ioan, Negirla, Paul. "Students Training Through Applied Activities at Department of Automation and Applied Informatics, University Politehnica Timisoara." *European Journal of Engineering and Formal Sciences* 3, no. 2, 2020;