UNIVERSITATEA TEHNICĂ
“GHEORGHE ASACHI” DIN IAŞI
Facultatea de
Inginerie Electrică, Energetică şi
Informatică Aplicată

TEZĂ DE DOCTORAT
REZUMAT

Cercetari privind realizarea de aplicatii IT pentru cladiri inteligente

Conducător de doctorat:
Prof. dr. ing. Schreiner Cristina-Mihaela

Doctorand:
Olteanu Alin-Alexandru

Septembrie 2024

UNIVERSITATEA TEHNICĂ "GHEORGHE ASACHI" DIN IAŞI

R E C T O R A T U L

Către

_____

_____

Vă facem cunoscut că, în ziua de 30 Septembrie 2024 la ora 11.00 în Sala de Conferințe "Dragomir Hurmuzescu" a Facultății de Inginerie Electrică, Energetică și Informatică Aplicată, va avea loc susţinerea publică a tezei de doctorat intitulată:

" Cercetări privind realizarea de aplicații IT pentru clădiri inteligente"

elaborată de domnul **OLTEANU ALIN ALEXANDRU** în vederea conferirii titlului ştiinţific de doctor.

Comisia de doctorat este alcătuită din:
1. Prof.dr.ing. Maricel Adam, Universitatea Tehnica "Gheorghe Asachi" din Iași, preşedinte
2. Prof.dr.ing. Cristina Mihaela Schreiner, Universitatea Tehnica "Gheorghe Asachi" din Iași, conducător de doctorat
3. Prof.dr.ing. Laurenţiu Marius Dumitran, Universitatea Națională de Știință și Tehnologie POLITEHNICA București, referent oficial
4. Prof.dr.ing. Laurențiu Dan Milici, Universitatea „Ștefan cel Mare" din Suceava, referent oficial
5. Conf.dr.ing. Sebastian Teodor Arădoaei, Universitatea Tehnica "Gheorghe Asachi" din Iasi, referent oficial

Cu această ocazie vă invităm să participaţi la susţinerea publică a tezei de doctorat.

RECTOR,

Prof.univ. dr.ing. Dan Caşcaval

ROMÂNIA UNIVERSITATEA TEHNICĂ „GHEORGHE ASACHI" DIN IAȘI ISTERUL EDUCAȚIEI

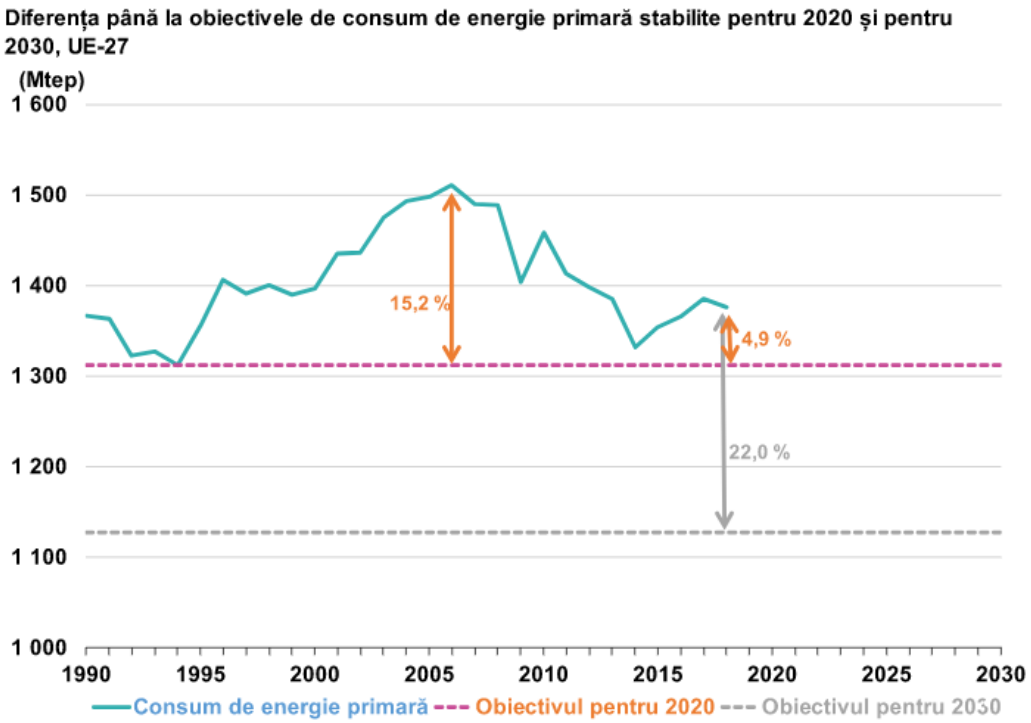
Secretar universitate,

ing. Cristina Nagîț

Introducere

Managementul energetic reprezintă într-o manieră economică acțiuni organizatorice și tehnice având ca scop îmbunătățirea continuă a performanței energetice a organizației și totodată de a menține îmbunătățirile obținute. Organizația parcurge în mod continuu ciclul de elaborare a politicilor; aici sunt incluse evaluarea obiectivelor, planificarea obiectivelor, implementarea obiectivelor, verificarea rezultatelor, revizuirea progreselor și actualizarea politicilor și a obiectivelor, după caz.

În 2012, Directiva 2012/27/UE[2] privind eficiența energetică a integrat obiectivul privind îmbunătățirea eficienței energetice cu 20% până în 2020 (în comparație cu consumul de energie preconizat pentru 2020). Directiva revizuită 2018/2002/UE[3] privind eficiența energetică a reflectat un obiectiv principal al UE în materie de eficiență energetică mai ambițios pentru 2030, de cel puțin 32,5 %.[2],[3],[6],[7].



Sursa: Statisticile Eurostat privind economiile de energie – Consumul de energie primară în 2018.

Figura nr.1.2: Consumul de energie primară în materie de eficiență energetică stabilite pentru 2020 și pentru 2030 [2]

Capitolul 1

Introducere in conceptul de structura a sistemului BMS

(building management system)

Strategiile de management implementate într-un sistem BMS variază în funcție de producător, însă unele dintre ele sunt fundamentale și se regăsesc în majoritatea cazurilor. Este importantă corelarea între sistemele de iluminat artificial și cel natural, astfel încât nivelul de iluminare artificială, atât interior cât și exterior, să se ajusteze automat în funcție de lumina naturală.

Totodată, funcționarea corpurilor de iluminat trebuie să fie sincronizată cu senzorii de prezență. În absența ocupanților, nivelul de iluminare trebuie redus sau, după caz, sistemul de iluminat trebuie oprit. În ceea ce privește instalațiile electrice de forță, este necesară o monitorizare constantă a consumului de energie activă și reactivă. În perioadele de consum maxim, când energia reactivă este ridicată, trebuie implementate măsuri pentru îmbunătățirea factorului de putere prin activarea automată a bateriilor de condensatoare.

Strategiile de management pentru instalațiile HVAC sunt diverse, iar cele mai comune includ:

- programarea optimă pentru oprirea/pornirea echipamentelor;
- utilizarea aerului exterior pentru răcire (free cooling) atunci când temperatura acestuia este mai scăzută decât cea a aerului introdus în interior;
- automatizarea centralelor de tratare a aerului și a unităților terminale în funcție de entalpie;
- adaptarea continuă și localizată a sistemului la sarcina termică de răcire/încălzire, renunțând la soluția clasică a încăperilor etalon;
- utilizarea ventilării în anumite situații (zero energy band[1]), cum se arată în figura 3: când temperatura ajunge în intervalul 23-24°C, instalațiile de încălzire/răcire sunt oprite, folosindu-se doar unitățile de ventilare;
- optimizarea funcționării chillerelor și creșterea graduală, pe cât posibil, a temperaturii apei răcite;

[1] https://byjus.com/physics/what-are-energy-bands/

- controlul funcționării unităților terminale prin intermediul senzorilor de prezență.

Clădirile cu eficiență energetică sunt văzute ca o componentă esențială a viitoarelor orașe inteligente. De obicei, prin clădiri inteligente, se înțeleg clădiri care au instalat **un sistem de management al clădirii** (**BMS** - în limba engleză **Building Management System**[2]).

Un astfel de sistem BMS vizează în mod obișnuit controlul tuturor echipamentelor instalate într-o clădire, **sistemul de iluminare și încălzire, ventilație și aer condiționat (HVAC), contorizările electrice și termice, sistemul de ascensoare, interfațarea cu sisteme de detecție a incendiului, supraveghere video și control al accesului** și e bazat pe anumite strategii de control, avand ca scop **reducerea consumurilor și optimizarea funcționării acestor sisteme** în condiții maxime de confort si siguranta. Un sistem BMS performant este capabil să minimizeze pierderile energetice, să colecteze energie solară sau apă pluvială, să înmagazineze aceste resurse pentru a avea un consum ulterior când condițiile sunt mai puțin favorabile, să programeze anumite activități pentru perioade în care condițiile sunt optime (de exemplu tarif de noapte sau producție sau rezerve de resurse crescute).

Se urmărește **minimizarea consumului de resurse de la rețea** iar în condiții extreme, de injectarea de energie electrică verde înapoi la furnizor, eficientizând astfel și activitatea acestuia.

Structura sistemului BMS

Structura hardware a unui sistem BMS variază semnificativ din cauza diversității producătorilor și soluțiilor disponibile. Până la mijlocul anilor 1990, sistemul era organizat pe trei niveluri distincte: aparatura de câmp (field level), automatizarea (automation level) și managementul (management level), fiecare având funcții și moduri de comunicare specifice. La nivelul de bază, traductoarele și elementele de execuție erau conectate individual la controllere, formând astfel o separare clară între echipamentele tehnologice (cazane, chillere, centrale de tratare a aerului etc.) și controllere, prin intermediul aparaturii de câmp.

După anul 2000, odată cu adoptarea pe scară largă a standardelor LONMARK și BACNet în echipamentele tehnologice și de automatizare, nivelul aparaturii de câmp a fost integrat în cel de automatizare în ceea ce privește comunicația. Această integrare a fost posibilă datorită includerii unor module de comunicație integrate în traductoare și elemente de execuție, având ca element central cipul Neuron, ceea ce a permis formarea unei rețele unice de tip peer-to-peer[3] cu

[2] https://www.sciencedirect.com/topics/engineering/building-management-system
[3] https://www.spiceworks.com/tech/networking/articles/what-is-peer-to-peer/

rețelele de controllere. De asemenea, echipamentele tehnologice au fost dotate cu module de comunicație compatibile cu sistemele BMS.

Problemele specifice

Majoritatea soluțiilor de gateway[4] de acasă de pe piață în prezent sunt un ecosistem închis, iar principala problemă a acestor soluții este compatibilitatea dispozitivelor. Cu alte cuvinte, atunci când un client decide să cumpere un nou dispozitiv inteligent pentru casă, trebuie să întrebe dacă acesta va funcționa cu gateway-ul lor (deoarece este posibil ca noul dispozitiv să nu funcționeze). Este important să rețineți că un sistem modern de casă inteligentă poate conține mai multe tipuri diferite de dispozitive (de exemplu, iluminat, comutatoare, senzori, dispozitive de securitate și alte aparate de uz casnic). Aparent, fiecare tip de dispozitiv are caracteristici și scopuri diferite. Chiar și dispozitivele din același tip pot avea funcții diferite. De exemplu, un bec inteligent ar putea oferi funcții de pornire și oprire, în timp ce un alt bec ar putea oferi funcții suplimentare, cum ar fi schimbarea culorii și clipirea. Un alt exemplu sunt dispozitivele cu senzori. Există mai multe tipuri de senzori, precum senzori de ușă, mișcare, temperatură și gaz. Drept urmare, va fi din ce în ce mai dificil să sprijiniți fiecare dispozitiv nou din rețelele eterogene [11] deținând proliferarea dispozitivelor de acasă conectate.

Capitolul 2
Analiza modului de integrare a BMS cu serviciile externe

Integrări cu servicii externe

Sunt oportune integrări cu mai multe tipuri de servicii:

1. Servicii de alertă (SMS, telefonice cu voce)
2. Servicii de comunicare umană precum Alexa, Google Home, Siri
3. Servicii de comandă externe tip ITTT (if this then that)[5] care pot comanda acțiuni în alte sisteme, altele decât BMS

Hardware. În afara costurilor de achizitie menționate în proiect, alte costuri adiționale în dezvoltarea unei platforme comprehensive pot fi generate de sisteme compatibile de monitorizare

[4] https://www.techtarget.com/iotagenda/definition/gateway
[5] https://www.spiceworks.com/tech/tech-general/articles/what-is-ifttt/

și control tip IoT, care pot costa de la câteva sute la câteva mii de euro. Sau de dispozitive și accesorii HVAC nou apărute, care nu au fost prezente pe piață la momentul conceperii acestui proiect. Întrucât se va lucra cu versiunile minimale ale acestora, pentru a demonstra viabilitatea produsului, costurile adiționale pot fi similar de la câteva sute la câteva mii de euro.

Tehnologia de automatizare inteligentă a clădirilor constă într-o rețea integrată de componente hardware și software care monitorizează și gestionează mediul intern al clădirilor. Sistemul de automatizare asigură funcționarea continuă și eficientă a sistemelor de încălzire, ventilație și aer condiționat (HVAC), electricitate, iluminat, instalații sanitare, precum și a sistemelor de siguranță și protecție ale unei clădiri.

Cele mai importante sunt tendințele care se cristalizeaza în zona de clădiri inteligente și care includ în tehnologiile folosite și Internetul Lucrurilor (IoT).

Platformele scalabile și sigure ale acestor soluții inteligente generează economii de costuri, îmbunătățind **eficiența energetică și durabilitatea** și sporind satisfacția utilizatorilor.

Internetul obiectelor (IoT) continuă să aibă un impact semnificativ asupra automatizării clădirilor. Clădirile inteligente se sprijină pe o varietate de tehnologii, cum ar fi comunicațiile fără fir, cloud computing-ul și administrarea datelor. Aceste dispozitive sunt concepute special pentru a oferi precizie, scalabilitate și versatilitate în managementul clădirilor.

Aplicațiile IoT permit managerilor de facilități să efectueze diferite experimente pentru a verifica rezultatul optimizării. De asemenea, le oferă un spațiu pentru a utiliza dispozitivele IoT în monitorizarea sistemelor clădirilor folosind un singur panou.

Cel mai important impact pe care IoT îl are asupra clădirilor este eficiența energetică. Utilizarea senzorilor în rețea ajută la furnizarea de informații care ar ajuta managerii să își controleze mai bine activele și, de asemenea, să reducă deșeurile dăunătoare din mediu.

Exemple de utilizare a IoT pentru eficiența energetică.

- Folosirea senzorilor pentru controlul temperaturii
- Utilizarea dispozitivelor de acționare pentru comenzile HVAC
- Aplicații complexe, cum ar fi asigurarea automatizării energetice complete pentru o clădire
- Permite atât comunicarea offline cât și în timp real
- Consideră prognozele meteo pentru a economisi costurile energiei în timp real

Cercetarea și dezvoltarea de noi strategii de control folosind tehnici de logică fuzzy[6] pentru serviciile de construcții se referă la trei aspecte de bază ale controlului clădirilor:

- controlul automat al zonelor individuale prin control termostatic (fan coil[7], amortizor de zonă etc.);
- control automat al centralei centrale și al sistemelor centrale HVAC (încălzire ventilație și aer condiționat) (temperatura apei, temperatura bobinei, rația de amestecare a aerului proaspăt etc.);
- control global al confortului termic, al confortului vizual (Daylight Glare Index[8]) și al calității aerului din interior (CO2), inclusiv integrarea controlului componentelor clădirii și utilizarea surselor regenerabile de energie (solare pasive, ventilație naturală etc.) [9]

Capitolul 3
Studiu privind abordările curente privind interfeţele de management al clădirilor

Indicații: Interfețele (UI - user interface[9], UX - user experience[10]) trebuie să fie clare, intuitive, neaglomerate și să inducă ideea de eficiență.

Designul UI/UX implică crearea interfețelor pentru utilizatori, unde ușurința de interacțiune cu informațiile afișate este la fel de esențială ca și estetica. Obiectivul acestuia este de a facilita rapid și eficient realizarea acțiunilor necesare pe portal (plasarea comenzilor, subscrierea, achizițiile, căutarea produselor/serviciilor) prin intermediul interfeței.

Diferențele principale între UI și UX sunt următoarele: în cazul UI, designerul evaluează modul în care vizitatorii sau utilizatorii vor interacționa cu interfața și care sunt pașii necesari pentru a obține un rezultat specific. În cadrul UI, specialistul determină aspectul vizual al fiecărui pas. Fundamental, UI cuprinde o serie de interfețe, pagini și componente vizuale, precum butoane

[7] https://www.designingbuildings.co.uk/wiki/Fan_coil_unit
[8] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.fedoa.unina.it/1312/1/Bellia_paper.pdf
[9] https://www.geeksforgeeks.org/user-interface-ui/
[10] https://www.workshopper.com/post/what-is-ux-and-why-is-it-important

și icoane, ce facilitează interacțiunea unei persoane cu un produs sau serviciu. În schimb, experiența utilizatorului (UX) se referă la percepția internă formată de o persoană în timpul interacțiunii cu diversele aspecte ale produselor și serviciilor unei companii. Următoarele sunt câteva diferențe între UX și UI: Designul UX, sau crearea experienței utilizatorului, începe cu identificarea unei dificultăți sau nevoi specifice utilizatorului. Pe baza acestei identificări, se construiește un prototip preliminar care ulterior este testat pentru a fi validat sau respins. După ce modelul de afaceri și propunerea de valoare sunt verificate, se trece la dezvoltarea produsului.

În ceea ce privește ordinea, inițial se dezvoltă componenta vizuală, conform principiilor User Experience, urmată apoi de User Interface. Totuși, elementul esențial de care trebuie să ne preocupăm este rezultatul obținut – o interfață care este compatibilă și ușor de folosit de către utilizatori. Pe scurt, UI reprezintă aspectul vizual al unei aplicații. Aceasta cuprinde totul, de la ecrane simple la ecrane tactile, tastaturi, sunete și chiar lumini.

Sistemele inteligente au devenit utilizate pe scară largă în clădiri cu capacități crescute ale tehnologiilor internetului obiectelor. Majoritatea acestor sisteme sunt scumpe; prin urmare, alegerea celei mai bune combinații a sistemelor pentru o proprietate este importantă.

Cinci obiective de proiectare pentru clădirile inteligente:

1. Interoperabilitate: Capacitatea sistemelor cibernetice și a oamenilor de a se conecta și comunica între ei prin internetul lucrurilor (IOT).

2. Virtualizare: O imagine virtuală a clădirii inteligente care este creată prin conectarea senzorului date cu modele virtuale și modele de simulare.

3. Descentralizare: Capacitatea sistemelor cibernetice fizice din clădirile inteligente de a lua decizii pe cont propriu.

4. Capacitate în timp real: Capacitatea de a colecta și analiza date și de a furniza idei derivate instantaneu.

5. Orientarea serviciilor: oferirea și consumul de servicii.

Interfețele trebuie sa fie eficiente să arate în timp real fluxurile de consum, economisire sau de returnare în rețea (la furnizor) a energiei generate în surplus care depășesc capacitatea bateriilor de la locație. Măsurarea netă (cunoscută și sub numele de **măsurare a energiei nete** sau

NEM) este un stimulent solar care va permite stocarea energiei în rețeaua electrică. Când panourile solare produc mai multă energie electrică decât este nevoie, energia respectivă este trimisă la rețea în schimbul certificatelor verzi/creditelor.[5]

Prin urmare, este crucial să se identifice cea mai avantajoasă balanță între costuri și mărimea necesară a sistemului în etapa de proiectare; acesta trebuie să incorporeze cel mai eficace dintre toate subsistemele, astfel încât:

1. Captarea și depozitarea energiei solare să fie optimizată;
2. Sursele de energie solară și cele auxiliare să fie separate;
3. Energia solară să fie utilizată cu prioritate;
4. Sursa de energie auxiliară să fie utilizată doar ca un supliment.

SPECIFICAȚII STANDARD PENTRU BMS

Un BMS are cel puțin o stație de lucru pentru operator permanent conectată printr-o rețea de comunicații la un număr de controlere de control digital direct (DDC) care sunt adesea denumite controlere de teren.

Sisteme DDC de rețea. Sistemele DDC în rețea cuprind două sau mai multe controlere DDC care sunt conectate împreună printr-o rețea de comunicații în același mod ca un BMS, totuși nu este prevăzută o stație de lucru pentru operator permanent.

Controlere DDC independente. Un sistem de control DDC autonom cuprinde unul sau mai multe controlere care nu sunt conectate împreună printr-o rețea de comunicații. Controlerele funcționează independent unul de celălalt și nu există o stație de lucru cu operator permanent.

Capitolul 4

Obiectivele de proiectare pentru aplicațiile IT ale clădirilor inteligente

Cele mai importante tendințe IoT Smart Building

Inteligență artificială (AI) și Big Data[11]

IoT permite AI și Big Data. Senzorii wireless captează cantități masive de date în timp real pentru analiză. Scopul IoT nu a fost niciodată datele în sine. Mai degrabă, potențialul de a produce informații inteligente derivate din date IoT, acestea oferă una dintre cele mai convingătoare teme ale IoT. AI poate furniza analize care schimbă jocul, bazate pe învățarea automată, detectarea anomaliilor, detectarea și diagnosticarea defectelor (FDD), întreținerea predictivă și multe altele.

Digitalizarea activelor

Consumăm informații digitale zilnic, este noul normal. Digitalizarea activelor revoluționează CRE, deoarece ajunge la restul economiei de piață. IoT facilitează digitalizarea activelor la întreaga clădire sau la nivelul activelor individuale. Luăm în considerare, de exemplu, monitorizarea stării activelor (ACM). Majoritatea organizațiilor au o vizibilitate redusă sau nulă asupra activelor critice HVAC, cum ar fi sistemul de răcire, turnurile de răcire. Este posibil să aibă o oarecare înțelegere a consumului lunar de energie electrică, dar nu au nicio perspectivă asupra stării operaționale în timp real a acestor active. Pentru activele considerate critice și care reprezintă cei mai mari consumatori de energie electrică și apă dintr-o clădire, acest lucru pare dificil de înțeles.

Vizualizări Cloud în timp real

Livrarea în cloud de produse și servicii în timp real este de asemenea noul normal. Digitalizarea activelor permite accesul la platformă pentru vizualizări în timp real în cloud. Cu toții ne-am obișnuit să avem la îndemână date și servicii în timp real. Așteptările noastre s-au schimbat, deoarece acum ne asumăm accesul oricând și oriunde la produse și servicii în timp real.

[11] https://www.oracle.com/big-data/what-is-big-data/

Eficiența energetică

IoT va continua să producă rezultate foarte mari în căutarea eficienței energetice, deoarece penetrarea pieței abia a început. Un procent alarmant de scăzut al clădirilor de astăzi are acces la orice formă de raportare a energiei în timp real. Prea multe clădiri se bazează în continuare pe citirea manuală a contoarelor. Clădirile sunt cea mai mare sursă de consum de energie la nivel mondial. Cu toate acestea, o mare parte din această energie este irosită, în principal din cauza gestionării deficitare a clădirilor. Prin urmare, a fi informați cu exactitate despre consumuri și detectarea anomaliilor sunt pași esențiali pentru a depăși această problemă.

Monitorizarea calității aerului interior (IAQ)

IoT oferă cea mai rapidă și cea mai economică metodă de creștere a infrastructurii clădirii pentru a permite monitorizarea IAQ în timp real. Chiar și BAS-ul (cel mai avansat, abia va sprijini măsurile moderne de IAQ, cum ar fi materia particulelor (PM) și compușii organici volatili (COV). Certificările, cum ar fi WELL, au identificat strategii pentru a limita concentrațiile de poluanți și contaminanți utilizând orientări bazate pe dovezi.

Iluminare inteligentă

Una dintre cele mai mari revoluții în modul în care ne luminăm clădirile a fost invenția iluminatului cu LED-uri de aproximativ treizeci de ani. Luminile cu LED pentru a consuma mai puțin de 80% din energia electrică a becurilor tradiționale și au o durată de viață de zece ori mai mare. Cu toate acestea, LED-urile reprezintă astăzi doar 10% din toate sistemele de iluminat, astfel încât multe clădiri au posibilitatea de a economisi energie și costuri doar prin schimbarea becurilor.

Icoane skeuomorfe

Skeuomorfismul este direcția de proiectare cumva opusă planului. Se bazează pe ideea de a reflecta imaginile în aspect 3D foarte aproape de aspectul natural original al obiectelor fizice. A fost popular pentru GUI de diferite tipuri și funcționalități în urmă cu câțiva ani. Dar apoi a fost înlocuit treptat cu un design plat în UI, care este mai simplu și, prin urmare, mai flexibil și practic pentru nevoile interfețelor digitale. Cu toate acestea, pictogramele skeuomorfe sunt încă utilizate pe scară largă în designul jocului și în pictogramele aplicațiilor din sectorul jocurilor.

Pictograme SVG

Pictogramele SVG, decodate ca grafică vectorială scalabilă, sunt pictograme receptive construite pe imagini vectoriale 2D bazate pe XML. Acestea sunt proiectate și integrate conform unui standard deschis dezvoltat de World Wide Web Consortium (W3C) din 1999 și susținut de toate browserele majore. Pictogramele SVG își cresc popularitatea, deoarece astăzi site-urile web sunt utilizate pe diversitatea platformelor și dispozitivelor și trebuie să fie receptive pentru a oferi un UX pozitiv.[20]

Capitolul 5

Studiu privind analiza diferitelor protocoale de comunicare, comparând principalele protocoale folosite în sistemele de automatizare a clădirilor

Protocoalele deschise pot fi clasificate în principal ca protocoale **prin cablu** (Wired Protocols[12]) și protocoale **fără cablu** (Wireless Protocols). Ambele au propriile avantaje și dezavantaje. În timp ce protocoalele wireless sunt de preferat pentru clădirile existente datorită ușurinței instalării lor, clădirile noi în care performanța și fiabilitatea sunt printre cele mai importante folosesc protocoale prin cablu. Comunicarea wireless este destul de ieftină în comparație cu comunicarea prin cablu. Astfel, în funcție de situația concretă trebuie să decidem dacă vom utiliza comunicații fără fir sau prin cablu. Se poate opta și pentru o combinație între acestea.

Compararea diferitelor protocoale ne va ajuta să alegem cel mai bun protocol care ar trebui utilizat în diferite situații și regiuni. Protocoalele vor fi comparate în funcție de tipul lor (cu fir sau fără fir), topologia rețelei pe care o utilizează, moduri de transmisie, diferitele lor aplicații în automatizarea clădirilor, securitate, avantajele lor și regiunile în care acestea sunt cele mai populare.

PROTOCOALE DE COMUNICARE IoT

Protocoalele de comunicare IoT sunt moduri de comunicare care protejează și asigură o securitate optimă a datelor schimbate între dispozitivele conectate.

[12] Wired Protocols

Dispozitivele IoT sunt de obicei conectate la Internet printr-o rețea IP (Internet Protocol). Cu toate acestea, dispozitivele precum Bluetooth și RFID permit dispozitivelor IoT să se conecteze local. În aceste cazuri, există o diferență de putere, autonomie și memorie utilizată. Conexiunea prin rețele IP este relativ complexă, necesită memorie și putere sporită de la dispozitivele IoT, în timp ce gama nu reprezintă o problemă. Pe de altă parte, rețelele non-IP necesită relativ mai puțină energie și memorie, dar au o limitare a intervalului.

Protocoalele și standardele IoT pot fi clasificate în **două** categorii separate:

1. Protocoale de rețea IoT

Protocoalele de rețea IoT sunt utilizate pentru a conecta dispozitive prin rețea. Acestea sunt setul de protocoale de comunicații utilizate de obicei pe internet. Folosind protocoale de rețea IoT, este permisă comunicarea de date de la un capăt la altul în sfera rețelei. Următoarele sunt diferitele protocoale de rețea IoT:

• HTTP (HyperText Transfer Protocol[13])

HyperText Transfer Protocol este cel mai bun exemplu de protocol de rețea IoT. Acest protocol a constituit baza comunicării datelor pe web. Este cel mai comun protocol care este utilizat pentru dispozitivele IoT atunci când există o mulțime de date de publicat. Cu toate acestea, protocolul HTTP nu este preferat din cauza costului său, a duratei de viață a bateriei, a economiei de energie și a mai multor constrângeri.

• LoRaWan[14] (rețea pe distanțe mari)

Este un protocol cu rază lungă de acțiune, care oferă detectarea semnalului sub nivelul de zgomot. LoRaWan conectează wireless dispozitivele cu baterie la Internet, fie în rețele private, fie în rețele globale. Acest protocol de comunicare este utilizat în principal de orașele inteligente, unde există milioane de dispozitive care funcționează cu mai puțină energie și memorie.

• Bluetooth

Protocolul Bluetooth este utilizat în principal în articole portabile inteligente, smartphone-uri și alte dispozitive mobile, unde fragmente mici de date pot fi schimbate fără putere și memorie

[13] https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview
[14] https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/

mare. Oferind ușurință în utilizare, Bluetooth ocupă primul loc în lista protocoalelor de conectivitate a dispozitivelor IoT.

2. Protocoale de date IoT

Protocoalele de date IoT sunt utilizate pentru a conecta dispozitive IoT de consum redus. Aceste protocoale asigură o comunicare punct-la-punct cu hardware-ul din partea utilizatorului, fără nicio conexiune la Internet. Conectivitatea în protocoalele de date IoT se face printr-o rețea cu fir sau celulară. Unele dintre protocoalele de date IoT sunt:

• **Transport de telemetrie a cozii de mesaje (MQTT)**

Unul dintre cele mai preferate protocoale pentru dispozitivele IoT, MQTT colectează date de la diferite dispozitive electronice și acceptă monitorizarea dispozitivelor la distanță. Este un protocol de abonare / publicare care rulează peste Transmission Control Protocol[15] (TCP), ceea ce înseamnă că acceptă schimbul de mesaje bazat pe evenimente prin rețele fără fir.

• **Protocol de aplicare restricționat (CoAP)**

CoAP este un protocol de utilitate de internet pentru gadgeturi restricționate. Folosind acest protocol, clientul poate trimite o cerere către server, iar acesta poate trimite înapoi răspunsul către client în HTTP. Pentru implementarea ușoară, folosește UDP (User Datagram Protocol[16]) și reduce utilizarea spațiului. Protocolul utilizează formatul de date binare EXL (Efficient XML Interchanges).

• **Protocol avansat de așteptare a mesajelor (AMQP)**

AMQP este un protocol de strat software pentru mediu middleware orientat către mesaje, care oferă rutare și coadă. Este utilizat pentru o conexiune fiabilă punct-la-punct și acceptă schimbul de date fără probleme și sigur între dispozitivele conectate și cloud. AMQP constă din trei componente separate și anume Exchange, Message Queue și Binding. Toate aceste trei componente asigură un schimb și stocare sigură și de succes a mesajelor. De asemenea, ajută la stabilirea relației unui mesaj cu celălalt.

[15] https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/
[16] https://www.geeksforgeeks.org/user-datagram-protocol-udp/

• Protocolul de comunicare Machine-to-Machine[17] (M2M)

Este un protocol industrial deschis construit pentru a oferi gestionarea de la distanță a aplicațiilor dispozitivelor IoT. Protocoalele de comunicații M2M sunt rentabile și utilizează rețele publice. Creează un mediu în care două mașini comunică și fac schimb de date. Acest protocol acceptă auto-monitorizarea mașinilor și permite sistemelor să se adapteze în funcție de mediul în schimbare.Protocoalele de comunicații M2M sunt utilizate pentru case inteligente, autentificare automată a vehiculelor, distribuitoare automate și bancomate.

• Protocol extensibil de mesagerie și prezență (XMPP)

XMPP este proiectat unic. Folosește un mecanism push pentru schimbul de mesaje în timp real. XMPP este flexibil și se poate integra perfect cu modificările. Dezvoltat folosind XML deschis (Extensible Markup Language[18]), XMPP funcționează ca un indicator de prezență care arată starea disponibilității serverelor sau dispozitivelor care transmit sau primesc mesaje.

PROTOCOALE FOLOSITE PENTRU AUTOMATIZAREA CLADIRILOR

BACnet

BACnet reprezintă Rețeaua de automatizare și control a clădirilor (Building Automation and Control Network). Se concentrează exclusiv pe automatizarea clădirilor. Acesta este cel mai popular protocol de rețea utilizat de producătorii de sisteme de automatizare a clădirilor din întreaga lume și este folosit în comunicarea dintre dispozitive diferite. Este susținut și actualizat de ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers).

LonWorks

Lonworks este o abreviere pentru rețeaua locală de operare (local operating network-LON). Este un sistem de control al rețelei. Este bazat pe protocolul proprietar LonTalk. LonWorks este practic o tehnologie care constă din diferite cipuri de la diferiți furnizori, protocolul LonTalk, mediul fizic prin care se conectează dispozitivele, diverse instrumente de gestionare a rețelei și

[17] https://www.techtarget.com/iotagenda/definition/machine-to-machine-M2M
[18] https://w3schools.com/xml/xml_whatis.asp

toate produsele care sunt construite în jurul acestei platforme. A fost dezvoltat special pentru automatizarea clădirilor.

DALI

DALI asigură un control eficient asupra iluminatului accesând fiecare dispozitiv separat. Acceptă setarea a 256 de niveluri de luminozitate. Nivelul semnal-zgomot superior duce la o comunicare fiabilă. Comunicarea rămâne bidirecțională astfel încât putem primi feedback despre starea de funcționare a lămpii. Flexibilitatea sa poate fi recunoscută prin faptul că se poate schimba ușor lampa în caz de defecțiune a acesteia.

KNX

KNX este un standard acceptat la nivel internațional pentru automatizarea clădirilor. Este rezultatul combinării a trei diferite standarde: European Home Systems Protocol (EHS), BatiBUS și European Installation Bus (EIB). Scopul său este de a standardiza universal comunicarea între dispozitivele de automatizare a clădirilor pentru dezvoltări ulterioare. Sprijină comunicarea multicast, precum și comunicarea punct-la-punct.

EnOcean

Tehnologia EnOcean este o tehnologie de comunicații wireless eficientă din punct de vedere energetic, care a fost dezvoltată în principal pentru automatizarea clădirilor. Protocolul definește utilizarea dispozitivelor de recoltare a energiei care nu necesită baterii sau orice altă sursă de energie. Peste 800 de produse certificate au fost dezvoltate pe baza acestui protocol. Dispozitivele Enocean folosesc tehnici de recoltare a energiei termice și cinetice care, la rândul lor, duc la eficientizarea cheltuielilor și sunt printre cele mai ecologice

Zigbee

Zigbee este din nou un standard wireless pentru automatizarea locuințelor și a clădirilor, bazat pe un standard IEEE 802.15.4 .

Una dintre caracteristicile importante ale acestui protocol este topologia rețelei de tip plasă (mesh) care presupune rutarea automată (auto routing) și auto-vindecarea (self-healing).

Principalul avantaj în rețeaua mesh este că, dacă comunicarea este întreruptă, atunci dispozitivele pot căuta prin rețeaua mesh un traseu nou. Acest lucru face comunicarea să fie fiabilă și flexibilă. Fiecare dispozitiv Zigbee poate suporta până la 240 de aplicații și, prin urmare, are 240 de puncte finale. Standardul Zigbee are, de asemenea, o acoperire largă, ceea ce îl face potrivit pentru clădiri mari și campusuri. Adăugarea unui dispozitiv nou este simplă și economică.

Capitolul 6
Aplicația practica a platformei de management si modul de comunicare cu display-ul

Vulnerabilitatea reprezintă o deficiență într-un sistem hardware sau software care facilitează accesul utilizatorilor neautorizați la acesta. Cele mai frecvente tipuri de vulnerabilități în sistemele informatice includ cele fizice, hardware, software și umane.

Sistemele informatice sunt primele ținte ale atacurilor tradiționale, atunci când un atacator reușește să acceseze fizic spațiile unde se află echipamentele de calcul și să extragă informații sensibile. Pentru a contracara acest risc, este esențial să se garanteze securitatea fizică a hardware-ului plasându-l în zone protejate, inaccesibile personalului neautorizat. Accesul în aceste zone se realizează prin utilizarea interfoanelor, cardurilor de acces sau tehnologiilor de identificare biometrică pentru autentificarea persoanelor autorizate să intre. O altă vulnerabilitate majoră a sistemelor informatice este reprezentată de dezastrele naturale (cum ar fi cutremurele, inundațiile, incendiile) sau accidentele tehnice, cum ar fi fluctuațiile de tensiune, care pot cauza distrugeri fizice ale echipamentelor. Astfel, este crucială și evaluarea amplasării echipamentelor pentru minimizarea riscurilor asociate cu amenințările ambientale.

Din perspectiva software, există diverse categorii de vulnerabilități:

➢ care conferă utilizatorilor locali neautorizați privilegii sporite;

➢ care le permit utilizatorilor externi să intre în sistem fără permisiune;

➢ care fac posibil ca sistemul să fie folosit într-un atac împotriva unui al treilea utilizator, cum ar fi atacul DDoS (Distributed Denial of Service).

Creșterea atacurilor asupra aplicațiilor web coincide cu avansul remarcabil al tehnologiilor web, care a permis crearea unor platforme interactive cu conținut dinamic și o interacțiune intensă cu utilizatorii. Aceste platforme moderne expun, totuși, vulnerabilități ce pot fi exploatate de atacatorii cibernetici pentru a ocoli măsurile de securitate și a accesa neautorizat datele din bazele de date.

Întrucât este mult mai dificilă abordarea securităţii după ce utilizarea şi implementarea au avut loc, securitatea trebuie avută în vedere din faza iniţială de planificare. Organizațiile au mai multe şanse să ia decizii despre configurarea computerelor în mod corespunzător şi constant dacă dezvoltă şi utilizează un plan de implementare detaliat, bine conceput. Dezvoltarea unui astfel de plan va sprijini administratorii serverelor web în luarea deciziilor inevitabile de compromis între utilitate, performanţă şi risc.

Organizațiile trebuie, de asemenea, să aibă în vedere cerinţele de resurse umane pentru implementarea şi operarea continuă a serverului web şi a infrastructurii de support.

Internetul obiectelor (IoT) este viitorul internetului care va interconecta miliarde de lucruri comunicante inteligente pentru a furniza zilnic servicii diverse utilizatorilor tehnologiei informației (IT). IoT continuă să afecteze toate aspectele vieții private și profesionale. În sectorul industrial, de exemplu, dispozitivele inteligente vor evolua pentru a deveni contribuabili activi la procesul de afaceri, îmbunătățind veniturile producătorilor de echipamente, furnizorilor de servicii bazate pe internet și dezvoltatorilor de aplicații. Securitatea IoT este zona de efort care se ocupă cu protejarea dispozitivelor și rețelelor conectate în mediul internetului obiectelor. Portabilele sunt un semn distinctiv al IoT, cu modele care încorporează funcții și caracteristici practice. De la sănătate la dispozitive orientate către modă și fitness, dispozitivele portabile fac tehnologia răspândită prin împletirea ei în viața de zi cu zi. Scopul principal al acestor aparate este să adune date precum bătăile inimii, caloriile arse, temperatura corpului sau a mediului ambiant și așa mai departe și să le trimită utilizatorului în scop informativ. Portabilele trebuie să stocheze datele local sau în cloud, pentru a genera rapoarte istorice despre progresul realizat al utilizatorului.

În sistemele încorporate, cum ar fi gateway-urile, hub-urile și punctele de intrare în rețea similare pentru dispozitive și lucruri care se conectează la acestea, este necesar să se ia în considerare o abordare diferită la îmbunătățirea securității, care începe de la planificarea timpurie a produsului cu securitate prin concept de proiectare (SbD). Practicanții de securitate trebuie să construiască o abordare multistratificată a ecosistemului IoT chiar de la pornirea inițială sigură

până la stabilirea încrederii și integrității software-ului pe dispozitivul IoT. Pentru a le stabili, controlul accesului bazat pe roluri (RBAC) asigură faptul că utilizatorii accesează doar acele privilegii și aplicații de care au nevoie ca parte a rolului lor de serviciu.

De asemenea, încorporarea principiului minimului privilegiu, autentificarea persistentă a dispozitivului și construirea de firewall-uri adecvate bazate pe gazdă și capacitatea de inspecție profundă a pachetelor vor spori încrederea și integritatea. Această integrare profundă a dispozitivelor interconectate care se încorporează în viața noastră de zi cu zi înseamnă că securitatea este de o importanță capitală. Aplicarea controalelor de securitate suplimentare fiecărui dispozitiv IoT nu este practic și pierde resurse. Securitatea trebuie să fie încorporată, să se potrivească mediului și să susțină funcționalitatea sistemului fără restricții. Când dispozitivele bazate pe System-on-Chip (SoC) pornesc sistemul, autenticitatea și integritatea software-ului, componentele firmware și hardware sunt verificate cu mijloace diferite. Modalitățile de asigurare a pornirii sigure și de verificare a integrității software-ului și firmware-ului instalat sunt importante pentru a garanta fiabilitatea acestuia în contextul marketingului. Metode precum Elliptic Curve Digital Signature Algorithm (ECDSA), Secure Hash Algorithm (SHA), acces direct la memorie (DMA) și funcția fizică neclonabilă (PUF) sunt utilizate pentru bootarea sigură și atestarea de la distanță. Încorporarea acestor metode pentru procesele de încărcare a încărcării este atenuarea scenariilor de atac plauzibile cu agenții de încărcare rău intenționați. Ca atare, bazele încrederii se stabilesc, dar dispozitivul are încă nevoie de protecție împotriva diverselor amenințări în timp de execuție și a intențiilor rău intenționate.

Controalele de acces încorporate ale sistemului de operare, obligatorii sau bazate pe roluri, au avantajul de a gestiona privilegiile pentru componentele și aplicațiile dispozitivului, astfel încât acestea să acceseze doar acele resurse atribuite acestora. În cazul unei intruziuni, controlul accesului asigură că intrusul are acces minim la alte părți ale sistemului. Mecanismele de control al accesului bazate pe dispozitive sunt similare cu sistemele de control al accesului bazate pe rețea, cum ar fi Microsoft Active Directory. Dacă cineva reușește să fure acreditări corporative și obține mijloace de intrare în rețea, accesul la astfel de informații compromise se limitează doar la acele segmente ale rețelei, autorizate de acele acreditări corespunzătoare. Principiul comenzilor cu cel mai mic privilegiu conform căruia trebuie să fie permis accesul minim necesar pentru a îndeplini o funcție, pentru a minimiza eficacitatea unei încălcări a securității.

Autentificarea dispozitivului trebuie declanșată atunci când activul este adăugat la rețea pentru prima dată, chiar înainte de a primi sau transmite date. Dispozitivele încorporate nu așteaptă

ca utilizatorii să introducă acreditările necesare pentru accesarea rețelei, dar identificarea lor trebuie să se facă corect înainte de autorizare. Similar cu modul în care mecanismul de autentificare a utilizatorului permite utilizatorului să acceseze rețeaua corporativă cu un nume de utilizator și o parolă, autentificarea mașinii permite dispozitivelor să acceseze rețeaua cu o pereche de acreditări stocate într-o zonă de stocare securizată. Aceste mecanisme de autentificare sunt denumite în cea mai mare parte autentificare de la dispozitiv la dispozitiv (D2D), unde acreditările de autentificare sunt schimbate printr-un canal de la mașină la mașină (M2M). Natura constrânsă a resurselor dispozitivelor IoT încurajează abordări ușoare pentru a menține eficiența transmisiei la un nivel satisfăcător. În plus, va îmbunătăți timpul de funcționare al dispozitivelor cu baterie. Astfel, încorporarea unui protocol de autentificare adecvat prin proiectarea circumspectă este vitală atât din perspectiva securității, cât și din perspectiva transmisiei.

Integrare protocoale de securitate - PGP encryption for offline temporary data storage[19]

PGP key generator (cpp)

#include "key_generation.h"

namespace OpenPGP {

namespace KeyGeneration {

bool complete_key_signatures(SecretKey & privateKey, const std::string & password) {

if (!privateKey.is_valid()) {

// "Error: Invalid key.\n";

return false;

}

#include "key_generation_helpers.h"

[19] https://www.varonis.com/blog/pgp-encryption

```
namespace OpenPGP {

namespace KeyGeneration {


bool complete_key_signatures(SecretKey &secretKey, const std::string &password) {

if (!secretKey.is_valid()) {

// "Error: Invalid key.\n";

return false;

    }


const std::string keyId = secretKey.get_key_id();


// Fetch the first packet which is expected to be a primary key packet

auto primaryKey = std::static_pointer_cast<Packet::Tag5>(secretKey.get_packets().front());


 // Clone packets for manipulation

PGP::Packets packets = secretKey.clone_packets();


Packet::Key::Ptr currentKey = nullptr;

Packet::User::Ptr currentUser = nullptr;


 for (auto &packet : packets) {

if (Packet::is_key_packet(packet->get_tag())) {

currentKey = std::static_pointer_cast<Packet::Key>(packet);
```

```
currentUser = nullptr;
} else if (Packet::is_user_packet(packet->get_tag())) {
currentUser = std::static_pointer_cast<Packet::User>(packet);
} else if (packet->get_tag() == Packet::SIGNATURE) {
 auto signature = std::static_pointer_cast<Packet::Tag2>(packet);

// Validate signatures using the primary key
if (signature->get_keyid() == keyId && Signature_Type::is_certification(signature->get_type())) {
if (currentKey->get_tag() == Packet::SECRET_KEY) {
signature = Sign::primary_key(primaryKey, password, std::static_pointer_cast<Packet::Tag5>(currentKey), currentUser, signature);
} else {
// "Error: Invalid key type for certification signature.\n";
return false;
}
}
// Other signature types processing...
}
}

secretKey.set_packets(packets);
return true;
}
```

```
SecretKey generate_key(Config &config) {
if (!config.is_valid()) {
// "Error: Invalid configuration for key generation.\n";
return SecretKey();
}

PGP::Packets packets;
uint32_t currentTime = now();

PKA::Values publicKeyValues, privateKeyValues;
if (!PKA::generate_keypair(config.pka_type, config.get_key_params(), privateKeyValues,
publicKeyValues)) {
// "Error: Failed to generate keypair.\n";
return SecretKey();
}

// Process private key values into a string
std::string secretValues;
 for (const auto &value : privateKeyValues) {
secretValues += serialize_MPI(value);
}

// Create and set up the primary Secret Key packet
auto primary = std::make_shared<Packet::Tag5>();
primary->set_time(currentTime);
```

```
primary->set_public_key_algorithm(config.pka_type);
primary->set_public_key_values(publicKeyValues);
configure_s2k(primary, config);

// Primary key processing
packets.push_back(primary);
const std::string keyId = primary->get_key_id();

// User ID and Signature packet generation
for (const auto &uid : config.user_ids) {
auto userIDPacket = create_user_id_packet(uid);
packets.push_back(userIDPacket);
auto signaturePacket = create_signature_packet(config, keyId, currentTime);
packets.push_back(signaturePacket);
}

// Generate subkeys
 for (const auto &subkeyConfig : config.subkeys) {
auto subkey = generate_subkey(subkeyConfig, currentTime);
packets.push_back(subkey.first);
packets.push_back(subkey.second);
}

// Compile all into a SecretKey object
```

SecretKey newSecretKey;

newSecretKey.set_packets(packets);

return newSecretKey;

}

}

}

Metode de comunicare cu perifericele; senzori, ecran, butoane, module de transmisie

Comunicarea cu perifericele la nivel hardware se face prin magistrale de date de tip I2C, SPI, UART. De regulă I2C pentru senzori, SPI pentru ecrane și UART pentru module de transmisie. Pentru butoane, în mod uzual se folosesc pini GPIO (General Purpose Input/Output[20]) unde se detectează semnal SUS (3.3 sau 5V) sau JOS (0V).

Peste acest layer de comunicație se pot folosi librării și wrappere a.î. schimbarea soluției tehnice să nu conducă la rescrierea firmware-ului.

Moduri de transmisie

Modul rapid:

Dispozitivele cu modul rapid pot primi și transmite la 400 kbit/s. Trebuie să se poată sincroniza cu o transmisie de 400 kbit/s și să prelungească perioada scăzută a semnalului SCL pentru a încetini transmisia.

Mod de mare viteză:

Dispozitivele în modul Hs pot transmite informații la rate de biți de până la 3,4 Mbit/s și rămân complet compatibile cu dispozitivele în mod rapid sau în mod standard (mod F/S) care

[20] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.egr.msu.edu/classes/ece480/capstone/fall09/group03/AN_balachandran.pdf

pot comunica bidirecțional într-un sistem de magistrală mixtă cu viteză. Transmisia în modul Hs are același principiu de magistrală serială și același format de date ca sistemul de mod F/S, cu excepția arbitrajului și a sincronizării ceasului care nu este efectuată.

Scrierea de firmware

Microcontrolerele au atins capacități hardware avansate, iar dezvoltatorii pentru multe aplicații nu mai trebuie să scrie cod *low-level*[21]. În schimb, dezvoltatorii pot scrie cod la un nivel superior similar cu modul în care un dezvoltator de aplicații scrie codul pentru computere. Pentru a face acest lucru, există două mecanisme diferite disponibile dezvoltatorilor de software încorporat: API-urile și HAL-urile.

Programare Firmware

Prin utilizarea API-ului pentru firmware, se pot dezvolta diverse metode de scriere a firmware-ului. În funcție de capabilitățile hardware ale microcontroller-ului, se pot dezvoltate metode mai simple sau mai complexe.

Detalierea caracateristicilor protocolului de comunicare cu display-ul

Comunicarea cu afișajul se realizează prin intermediul protocolului I2C (Inter-Integrated Circuit). Protocolul I2C (sau IIC - Inter-Integrated Circuit) este un standard de comunicație serială sincronă, multi-master - multi-slave, creat de Phillips în 1982. O magistrală I2C constă în următoarele semnale: SDA - linia de date și SCL - semnalul de ceas. Semnalul de ceas este generat de master, în timp ce linia de date este gestionată atât de master, cât și de slave. La un moment dat, doar un singur dispozitiv de pe magistrală poate controla linia de date, motiv pentru care protocolul I2C este considerat half-duplex.

Detalierea caracateristicilor protocolului de comunicare cu microSD-ul

Comunicarea cu microSD-ul se realizează prin intermediul protocolului SPI (Serial Peripheral Interface). SPI este un standard sincron dezvoltat de Motorola, care operează în mod full-duplex, permițând transferul de date în ambele direcții simultan. Dispozitivele care comunică prin SPI folosesc o arhitectură de tip Master-Slave, unde un singur dispozitiv Master

[21] https://www.geeksforgeeks.org/what-is-a-low-level-language/

și unul sau mai multe dispozitive Slave pot fi conectate. Master-ul este responsabil pentru inițierea comunicării. SPI este cunoscut și sub denumirea de "four wire" (patru fire), datorită celor patru semnale utilizate: MOSI, MISO, SCLK, CS/SS.

Plan de testare manuala a functionalitatii de baza a modulului de redundanță și backup-uri automate

1. Dashboard

Se verifica prezenta graficelor %CPU, %Mem, %Storage si uptime.

Se verifica corectitudinea informațiilor afișate.

2. Breakdown simulator

Se va verifica prezenta listei de noduri.

Se va verifica opțiunea de online/offline pentru fiecare nod.

3. Backup

Se va verifica existenta backup-urilor automate.

Se va verifica posibilitatea de a programa backup-urile cu o anumită frecvență, la anumite ore și cu specificatie locală sau la distanță(SFTP sau AWS S3).

Se va verifica existenta listei de backup-uri. Se vor verifica acțiunile listei de backup-uri(Restore, Download, Delete).

Se va verifica posibilitatea de a crea backup-uri manuale prin actionarea butoanelor.

Se va verifica existenta functionalitatii de refacere, restaurand un backup local, unul la distanța și/sau sincronizare cu celelalte servere pentru actualizarea tuturor datelor.

4. Redundanta

Se poate crea un nou nod de redundanță.

Se va verifica opțiunea de Enable/Disable în cazul unui nod.

Într-o listă se pot vizualiza toate nodurile existente.

Se va verifica opțiunea de Delete.

Filtrele funcționează și sorteaza corect datele conform condițiilor aplicate.

Câmpul de cautare nod funcționează prin introducerea succesiva de litere care va activa afișarea în timp real a sugestiilor de nume găsite pe baza caracterelor introduse.

5. Reports

Sistemul va avea un sistem granular de alertare a unor responsabili umani (administratori de sistem, operatori, etc.)

Plan de testare manuala a functionalitatii de baza a modulului aplicație software pentru panourile de afișaj pentru utilizatorii finali

1. Afisarea

Se va verifica afișarea parametrilor și a valorilor înregistrate de senzori(Temperatură, Umiditate, Luminozitate).

Se va verifica afisarea programului incaperii si a activitatii curente.

Se va verifica afișarea indicatiilor de evacuare.

Există buton pe ecranul tactil pentru confirmarea prezenței personale în clădire, la o anumită locație.

Un buton permite semnalarea unei probleme de evacuare (cale de acces blocată, etc.).

De pe panoul de afișaj se va verifica inițierea unei alerte pentru situațiile de urgență.

Plan de testare manuala a functionalitatii de baza a modulului de integrare

Modulul de integrare va fi optimizat în sensul de comunicare și control cu cel puțin următoarele sisteme:

1. Google Assistant
2. Apple Siri
3. Amazon Alexa
4. Microsoft Cortana
5. Home assistant API
6. Apple HomeKit
7. Caret API
8. Wink API

1. Acoperirea

Se va verifica acoperirea funcționalităților suportate de către componentele externe (termostate, lumini, uși de garaj, valve, senzori proximitate, temperatură, umiditate, gaze, flux de apă, ușă închisă/deschisă, etc.) care se va face fie vocal, fie prin intermediul interfețelor de monitorizare și control ale platformei.

Se va verifica că există interfață vizuală integrată care să poată controla toate dispozitivele în tandem (ex: trecut în modul noapte, stins toate luminile neesentiale, setat o anumită temperatură în toată clădirea indiferent de ce produse sunt folosite de la ce furnizori).

Se va verifica posibilitatea de a activa / inactiva o conexiune cu un serviciu terț.

Se va verifica păstrarea unui istoric (log) al tuturor datelor trimise/primite cu serviciile terțe.

Se va verifica ca exista un istoric (log) al tuturor acțiunilor personalului de administrare cu cel puțin următoarele date:

- Autor
- Dată/oră
- Locație/IP
- Acțiune
- Parametri anteriori
- Parametri curenți

Se pot detecta tentativele de acces neautorizat prin interfețe vizuale sau non- vizuale. Emiterea de alerte și blocarea automată a secțiunii respective în cazul unor anomalii în fluxurile de informație sau de comandă.

Testarea beta

Testarea beta este unul dintre tipurile de testare a acceptării, care adaugă valoare produsului, deoarece utilizatorul final (utilizator real destinat) validează produsul pentru funcționalitate, utilizare, fiabilitate și compatibilitate. Contribuțiile furnizate de utilizatorii finali ajută la îmbunătățirea calității produsului și duc la succesul acestuia. Acest lucru ajută și la luarea deciziilor de a investi în continuare în produsele viitoare sau în același produs pentru improvizație.

Testarea beta este una dintre metodologiile de validare a clienților pentru a evalua nivelul de satisfacție a clienților cu produsul, lăsând să fie validat de către utilizatorii finali, care îl folosesc efectiv, pe o perioadă de timp.

Experiența produsului câștigată de utilizatorii finali este solicitată feedback cu privire la design, funcționalitate și utilizare și acest lucru ajută la evaluarea calității produsului.

Testarea beta se efectuează întotdeauna imediat după finalizarea testării Alpha, dar înainte ca produsul să fie lansat pe piață (lansarea producției / Go Live). În acest caz, dezideratul este ca produsul să fie cel puțin 90% - 95% finalizat (suficient de stabil pe oricare dintre platforme, toate caracteristicile fiind aproape sau complet complete).

Aplicația software pentru panourile de afișaj

Descriere generală

Panoul de afișaj permite consultarea atributelor diverșilor senzori care sunt alocați zonei curente, se pot vizualiza programele de temperatură, umiditate, lumină, calitatea aerului și activitățile programate. Adițional se pot vizualiza indicații de orientare către puncte de interes, iar în caz de alertă, indicații de evacuare.

Redundanță și backup-uri automate

Descriere generală

Obiectivul modulului de redundanță este de a asigura permanența serviciului BMS. Pentru aceasta sunt adăugate două sau mai multe servere disponibile pentru productivitatea sistemului. Astfel se asigură că defecțiunea sau întreruperea unui server nu duce la oprirea sistemului.

Modul integrare (inclusiv senzori și alte kit-uri)

Descriere generală

Modulul perminte integrarea unor senzori și kit-uri cu API-uri deschise. Se pot folosi diverși asistenți personali în cadrul sistemului pentru a cere informații de la senzori și a comanda diverse elemente de acționare. Deciziile sunt aprobate sau nu tot de către sistem în baza configurărilor interne. Toate informațiile, inclusiv comenzile sunt înregistrate de către platformă.

Concluzii

Capitolul 1 ne introduce in conceptul de structura a sistemului BMS (building management system), cu problemele sale specifice. Majoritatea soluțiilor de tip gateway de pe piață în prezent sunt

ecosisteme închise, iar principala problemă a acestor soluții este legata de compatibilitatea dispozitivelor. Sunt descrise specificațiile funcționale si asigurarea managementului fluxurilor informaționale si energetice prin structura sistemelor de automatizare BMS. Din punct de vedere software, al tipului de protocol de comunicaţie utilizat în reţele, la nivel de automatizare, cele mai cunoscute sunt LON (Local Operating Network), EIB (European Installation Bus) si PROFIBUS (Process Field Bus). Au fost luate în considerare numai protocoalele deschise (open protocol), pentru că numai utilizarea lor oferă caracterul de versatilitate al unui sistem BMS, în detrimentul protocoalelor proprietar care condiţionează apartenenţa controlerelor şi a echipamentelor de comunicaţie la acelaşi proprietar.

Capitolul 2 analizează modul de integrare cu serviciile externe: Servicii de alertă (SMS, telefonice cu voce); Servicii de comunicare umană gen Alexa, Google Home, Siri; Servicii de comandă externe tip ITTT (if this then that) care pot comanda acțiuni în alte sisteme, altele decât BMS; Rețele interconectate de hardware și software care monitorizează și controlează mediul clădirilor; Aplicații care includ în tehnologiile folosite și Internetul Lucrurilor (IoT).

Capitolul 3 este dedicat unui studiu privind abordările curente din interfeţele de management al clădirilor, cu designul UI/UX pentru elaborarea interfețelor pentru utilizatori, unde comoditatea interacțiunii cu informațiile prezentate joacă un rol la fel de important ca și aspectul exterior. Scopul este de a efectua fără probleme acțiunea necesară pe portal (înregistrarea comenzii, abonarea, cumpărarea, căutarea produselor/serviciilor) prin intermediul interfeței.

Capitolul 4 abordează obiectivele de proiectare pentru aplicațiile IT al clădirilor inteligente: Interoperabilitatea - capacitatea sistemelor cibernetice și a oamenilor de a se conecta și comunica între ei prin internetul lucrurilor (IOT); Virtualizarea - O imagine virtuală a clădirii inteligente care este creată prin conectarea senzorului date cu modele virtuale și modele de simulare; Descentralizarea - Capacitatea sistemelor cibernetice fizice din clădirile inteligente de a lua decizii pe cont propriu; Capacitatea în timp real - Capacitatea de a colecta și analiza date și de a furniza decizii derivate în timp real / instantaneu; Orientarea serviciilor - Accesul personalizat la servicii.

Capitolul 5 este dedicat unui studiu privind analiza diferitelor protocoale de comunicare, comparând principalele protocoale folosite în sistemele de automatizare a clădirilor, respectiv BACnet, LonWorks, DALI, KNX, EnOcean și Zigbee. Aici sunt analizate si principalele aspecte privind securitatea cibernetică, care presupune asigurarea următoarelor obiective: confidențialitatea - proprietatea ca informațiile, serviciile sau resursele sistemelor informatice să nu fie disponibile unor persoane sau procese neautorizate; integritatea - proprietatea de păstrare a acurateței informațiilor, serviciilor sau resurselor sistemelor informatice; disponibilitatea - proprietatea ca informațiile, serviciile sau resursele sistemelor informatice să fie accesibile persoanelor sau proceselor autorizate; autenticitatea - proprietatea de

asigurare a identificării și autentificării persoanelor, dispozitivelor și serviciilor sistemelor informatice și de comunicații; non-repudierea - proprietatea ca o acțiune sau un eveniment să nu poată fi repudiat (negat, contestat) ulterior.

Capitolul 6 descrie aplicația practica a platformei de management cu modul de comunicare cu display-ul. Comunicarea cu display-ul este de tip I2C, un protocol de comunicație serială sincron, multi-master - multi-slave. Sunt descrise: condiția de start, cadrul de adresă, cadrele de date, condiția de stop, TWI Control Register, conectarea mai multor dispozitive Slave – inclusiv cu ajutorul topologiei SPI Daisy Chain; aspecte referitoare la transmiterea datelor folosind SPI – in diverse configurări; integrarea API între modulele software corespunzătoare dispozitivelor din platforma. In final s-a prezentat planul de testare a funcționalității de baza a modulului de redundanță și backup-uri automate, a modulului de integrare / Testarea beta, si a aplicației software pentru panourile de afișaj.

Activitatea științifică

Rezultatele cercetărilor efectuate de către autor în perioada pregătirii tezei de doctorat s-au concretizat în elaborarea a 6 lucrări publicate ca autor şi coautor, în reviste de specialitate sau în volumele unor conferinţe internaţionale de prestigiu.

Articole publicate

1. Mihaela Aradoaei, Oliver Schreiner, Ionel Alexa, Alin Olteanu, Madalina Ancuta Pintilei, Romeo Cristian Ciobanu, Sebastian Teodor Aradoaei, Simulating the Interaction of Electromagnetic Radiation with Matter, Within Nano/Micro-Conductive Composite, 2023 International Conference on Electromechanical and Energy Systems (SIELMEN), 11-03 October 2023, Chisinau, Modova, DOI: 10.1109/SIELMEN59038.2023.10290731, indexat IEEE Xplore

2. Alexandru Trandabat, Alexandru Arcire, Romeo Cristian Ciobanu, Olga Plopa, Mihaela Aradoaei, Alin Olteanu, Mosneagu Andrei Adriana Mona, Design and modeling considerations for developing a millimolar Oxalic Acid detection sensor based on screen-printed carbon electrode and methilbenzenpirol, 2022 International Conference and Exposition on Electrical And Power Engineering (EPE), 20-22 Octombrie EPE 2022 - Iaşi, DOI: 10.1109/EPE56121.2022.9959778, indexat IEEE Xplore

3. Madalina Ancuta Pintilei, Ileana Ursu, Sebastian Pascu, Cristina Mihaela Schreiner, Mihaela Aradoaei, Alin Olteanu, Compression Of Acquired Data In Order To Make Transmission And

Processing More Efficient, 2022 International Conference and Exposition on Electrical And Power Engineering (EPE), 20-22 Octombrie EPE 2022 - Iaşi, DOI: 10.1109/EPE56121.2022.9959083, indexat IEEE Xplore

4. Ileana Ursu, Alin Olteanu, Vlad Morosanu, Cristina Mihaela Schreiner, Mihaela Aradoaei, Technical Analysis Regarding The Implementation Of A Building Management System, 2022 International Conference and Exposition on Electrical And Power Engineering (EPE), 20-22 Octombrie EPE 2022 - Iaşi, DOI: 10.1109/EPE56121.2022.9959794, indexat IEEE Xplore

5. Vlad Morosanu, Alin Oltenu, Cristina Schreiner, Maria Georgiana Gheorghian, Smart building software simulator, The 13th IEEE International Conference and Exposition on Electrical and Power Engineering (EPEi 2024), articol acceptat, în curs de publicare.

6. Alin Olteanu, Vlad Morosanu, Cristina Schreiner, Madalina Ancuta Pintilie, Firmware programming for smart buildings, The 13th IEEE International Conference and Exposition on Electrical and Power Engineering (EPEi 2024), articol acceptat, în curs de publicare.