



**UNIVERSITATEA POLITEHNICA
DIN BUCUREȘTI**



**Școala Doctorală de Electronică, Telecomunicații
și Tehnologia Informației**

Decizie nr. 802 din 07-02-2022

REZUMAT TEZĂ DE DOCTORAT

Ing. Vlad-Valentin Fireșteanu

**STRUCTURAREA APLICAȚIILOR DE ANALIZA A
RISULUI PENTRU PROIECTELE IOT**

**DESIGNING RISK ASSESSMENT APPLICATIONS
FOR INTERNET OF THINGS PROJECTS**

COMISIA DE DOCTORAT

Prof. Dr. Ing. Ion Marghescu Univ. Politehnică din București	Președinte
Prof. Dr. Ing. Mihai CIUC Univ. Politehnică din București	Conducător de doctorat
Prof. Dr. Ing. Corneliu Rusu Univ. Tehnică din Cluj	Membru
Prof. Dr. Ing. Călin Vladeanu Univ. Politehnică din București	Membru
Prof. Dr. Ing. Dan Marius Dobrea Univ. Tehnică Gh. Asachi, Iași	Membru

BUCUREȘTI 2022

Cuprins

1. Introducere	1
1.1. Prezentarea domeniului de doctorat	1
1.2. Scopul tezei	3
1.3. Conținutul tezei	5
2. Zone majore de risc si analiza factorilor de risc	8
3. Agile pentru livrarea proiectelor de tip IoT.....	11
4. Tableau pentru monitorizarea proiectelor de tip IoT.....	13
5. Validarea ponderilor prin metoda chestionarului.....	14
5.1. Alegerea audienței	14
5.2. Alegerea setului de întrebări pentru chestionar.....	16
5.3. De la întrebare la variabila de pondere.....	18
6. Concluzii	22
6.1. Rezultate obținute	23
6.2. Contribuții originale	25
6.3. Lista lucrărilor originale	26
6.4. Perspective de dezvoltare ulterioară	27
Bibliografie	29

Capitolul 1

Introducere

În ultimii ani, numărul proiectelor de tip IoT a crescut considerabil. Așadar, numărul companiilor care folosesc aceste tehnologii a crescut de la 13% în 2014 la 25% atunci când aceasta a fost scrisă [1]. Având în vedere această creștere, direct proporțional s-au dezvoltat și eforturile în ceea ce privește cercetarea și optimizarea proceselor ce caracterizează acest trend. De asemenea, această creștere a dus și la un număr mare de provocări cum ar fi redactarea rapoartelor de fezabilitate și productivitate, proces ce ia în calcul multitudinea de factori de risc ce pot apărea.

Pe lângă numărul în continuă creștere al companiilor ce lucrează cu aceste tehnologii, este important să luăm în considerare și numărul echipamentelor hardware ce intră în componența proiectelor propriu zise. Aceste echipamente au o diversitate foarte mare, pornind de la periferice cu putere de procesare mică precum becuri, leduri, întrerupătoare până la echipamente cu putere mare de procesare (camere video, dispozitive de recunoaștere a vocii etc.). Doar în anul 2020 avem aproximativ 22 miliarde de astfel de echipamente. De aceea, odată cu numărul acestora, proporțional crește și numărul vulnerabilităților. Atacurile de tip ‘black hat hacking’ au demonstrat că ignorarea securității software duce la consecințe de o gravitate remarcabilă. În urma unei statistici, HP a concluzionat în 2015 că șapte din primele zece astfel de echipamente ce pot fi conectate la Internet sunt vulnerabile din punct de vedere al securității software [2].

Un exemplu mai apropiat de o piață mult mai largă de utilizatori finali vine în zona proiectelor de tip ‘Home Automation’. În 2015, în cadrul DEFCON au fost organizate atacuri de tip ‘white hat hacking’ ce au dus la compromiterea unei rețele prin intermediul dispozitivelor de achiziție ce intră în componența unei case inteligente. Exploatarea s-a produs la nivelul unui protocol de comunicare, reprezentat de ZigBee [3].

Un prim pas ar fi reprezentat de identificarea nevoii ce trebuie acoperită de proiectul pe care îl realizăm. După identificarea acestei nevoi, următorii pași sunt reprezentați de conturarea unui plan. Pentru o mai bună înțelegere a acestuia, lucrarea mapează pașii din care este alcătuit cu etapele concrete de dezvoltare a diferitelor proiecte de tip IoT.

1.1 Prezentarea domeniului tezei de doctorat

Prin definiție, IoT reprezintă o rețea de echipamente fizice, vehicule și alte entități cu capacitate de procesare, achiziție sau execuție (senzori, motoare, valve). Aceste entități permit conectarea lumii fizice la artefacte software. Un echipament de tip IoT presupune o resursă hardware la care nu ne așteptăm să aibă o conexiune la Internet, dar care comunică cu acesta fără intervenție umană. Ne putem gândi la această definiție ca diferență majoră dintr-un echipament hardware ce stă la baza IoT și un

laptop sau telefon ce necesită intervenția umană pentru actualizarea datelor sau trimiterea acestora pe un server [4].

Numărul considerabil de proiecte IoT este împărțit pe mai multe domenii de interes în funcție de nevoia ce trebuie acoperită. Fiecare acest domeniu de interes este caracterizat de diferite echipamente și arhitecturi. Printre cele mai importante proiecte avem:

- 1) ‘Orașe inteligente’ (Smart Cities) – proiecte care se ocupă cu automatizarea diferitelor procese din cadrul unor aglomerări urbane, având ca scop final îmbunătățirea calității vieții locuitorilor din orașul respectiv (parcări inteligente, calitatea aerului, congestia traficului, ridicare selectivă a deșeurilor).
- 2) ‘Mediu inteligent’ (Smart Environment)– proiecte care se ocupă cu optimizarea și eficientizarea proceselor din cadrul unui mediu ales (predicția avalanșelor, prevenirea avalanșelor, predicția alunecărilor de teren).
- 3) ‘Irigare inteligentă’ (Smart Water)– optimizarea acțiunilor de irigare având ca scop final creșterea diferitelor recolte, managementul resurselor umane, eficiența costurilor.
- 4) ‘Măsurare inteligentă’ (Smart Metering)– eficientizarea proceselor de măsurare pentru reducerea costurilor, siguranța resurselor umane, monitorizarea în siguranță a echipamentelor.
- 5) ‘Securitate și urgență’ (Security and Emergencies)– proiecte de monitorizare și alertă ce implică declanșarea automată a diferitelor proceduri/ răspunsuri în cazul unei urgențe.
- 6) ‘Retail și logistică’ (Retail and Logistics) – proiecte ce se ocupă cu optimizarea proceselor dintr-o companie ce are ca scop eficientizarea costurilor, protecția muncii.
- 7) ‘Control industrial’ (Industrial Control)– monitorizare inteligentă a liniilor de producție, respectiv a elementelor de achiziție și execuție ce sunt specifice unui cadru industrial.
- 8) ‘Agricultură inteligentă’ – atât proiecte de monitorizare pentru animale, cât și proiecte ce se ocupă cu eficientizarea proceselor agricole având ca scop final creșterea livrabilelor, managementul resurselor umane.
- 9) ‘Case inteligente’ – proiecte de monitorizare și procesare a informațiilor din cadrul unui domiciliu având ca scop final îmbunătățirea vieții, eficientizarea consumului.
- 10) ‘eHealth’ – pentru eficientizarea proceselor din cadrul sănătății.

Analiza riscului reprezintă o procedură prin care optimizăm siguranța aplicației dar și a resurselor hardware ce intră în cadrul unui proiect IoT. Acest lucru se face prin identificarea vulnerabilităților sau zonelor sensibile, determinând în cele din urmă structurarea unor măsuri care să prevină sau să atenueze efectele acestor vulnerabilități [5].

Mai mult, riscul unui proiect este dat și de caracteristicile tehnice ale acestor echipamente. Atât elementele de achiziție, cât și cele de execuție pot fi analogice sau digitale precum în Figura 1.1:



Figura 1.1 Echipamente IoT și clasificarea acestora

Pe lângă elementele de achiziție, respectiv de execuție un proiect IoT conține și unitățile de procesare, respectiv sursa de alimentare pentru ca întreg sistemul să funcționeze. Încadrată în chenarul roșu, această parte este reprezentată în Figura 1.2.

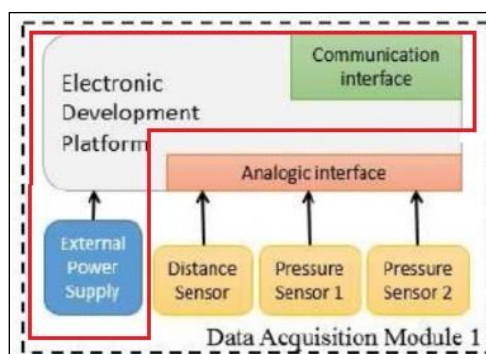


Figura 1.2 Arhitectura unui modul dintr-un proiect IoT

Vom discuta, astfel, despre riscurile ce pot apărea în zona echipamentelor pe care dorim să le achiziționăm pentru implementarea proiectului în sine (tip, cost, disponibilitate, complexitate etc.), dar și despre riscurile ce pot apărea atunci când optăm pentru o anumită soluție de alimentare a proiectului (disponibilitate, cost, scalabilitate). Totodată, prezența echipamentelor de execuție din Figura 1.1 duce la conturarea unei alte zone majore de risc, definită de factorii ce duc la prezența diferitelor accidente de muncă – un exemplu sugestiv este chiar prezența unghiurilor intrânde ce apar în cadrul instalațiilor ce conțin motoare.

1.2 Scopul tezei de doctorat

Noutatea acestei lucrări, pe lângă construirea unui framework unic de identificare a riscului, este reprezentată de intenția autorului de a explora, găsi și cuantifica riscul mai departe de partea de securitate informatică. Majoritatea lucrărilor, dar și a framework-urilor existente au fost construite în jurul vulnerabilităților de securitate

din cauza faptului că echipamentele pot fi compromise relativ ușor. Chiar dacă riscurile sunt în zona de securitate, trebuie să ne gândim și la riscurile ce vin din altă zonă ce caracterizează, în mod inevitabil, acest tip de proiecte. Un bun exemplu este reprezentat de factorii de risc ce vin din zona de mediu, și anume mediul unde proiectul nostru este instalat. Pe lângă mediu, trebuie să ne gândim și la partea de risc ce crește direct proporțional cu numărul echipamentelor hardware folosite sau la rutinele de hibernare ca parte din extinderea duratei de viață a bateriei, tipul de alimentare folosit etc. Un alt exemplu sugestiv este reprezentat și de riscul ce descrie partea de securitate în muncă și, implicit, siguranța factorului uman ce poate interfera cu aria de acțiune a proiectului. Bazându-ne pe articolele existente, aceste tipuri de risc sunt eclipsate de riscurile ce vin odată cu vulnerabilitățile software [6].

Metodele existente de cuantificare a riscului software încep să se înmulțească direct proporțional cu implementarea proiectelor de tip IoT. Nume mari, precum OWASP, au creat o listă specială IoT ce este actualizată periodic, listă ce conține primele zece amenințări software[7]. Un alt colos este reprezentat de Microsoft care a publicat o listă cu toți pașii recomandați ce ar trebui să caracterizeze un SDLC ¹pentru IoT. În linii mari, această listă conține un curs introductiv în securitatea informației, cinci repere de implementare împărțite în diferite perioade de timp, dar și o fază de răspuns. Cercetând aceste exemple, ne putem da seama că o abordare sănătoasă de implementare se realizează încă din faza de design a proiectului [8].

Trebuie, de asemenea, să înțelegem de ce anumite tipuri de risc sunt neglijate, iar un indiciu important este dat chiar de natura proiectelor în sine. Unul dintre scopurile proiectelor de tip IoT este ca momentul intrării pe piață să fie cât mai devreme. Cu cât un produs este mai devreme pe piață [9], cu atât îi este mai ușor să-și creeze un brand, o reputație etc.

Așadar, provocările acoperite în această lucrare sunt reprezentate de eficientizarea energiei în funcție de proiectul pe care îl alegem și deciziile ce stau în spatele acestui proces, gândirea proiectului pentru satisfacerea cerințelor necesare în ceea ce privește protecția muncii, dar și integritatea datelor din prisma interferenței factorilor externi[10]. Procesul în sine este structurat pe baza unui vector ce conține zone de risc major. Aceste zone de risc major au în componența lor, într-o abordare mai granulară, factorii de risc propriu-ziși. După ce cuantificăm aceste zone pe baza factorilor caracteristici, ne vom crea o imagine de ansamblu asupra proiectului. În cele din urmă, pe baza acestei imagini de ansamblu se va construi o decizie argumentată, relevantă în ceea ce privește costurile de implementare, dar și fezabilitatea propriu-zisă a proiectului. Având aceste informații, se va hotărî atât licitarea pentru un proiect software, cât și acceptarea acestuia. În urma citirii acestei lucrări, dar și a aplicării principiilor sau metodei de calcul prezentată, ne va fi mai ușor să răspundem unor întrebări practice precum: ‘Care zone din proiectul meu trebuie îmbunătățite pentru a avea șanse mai mari de succes?’ sau ‘Cum putem cuantifica riscul proiectului pe care dorim să-l implementăm, în ciuda impredictibilității acestuia?’ sau ‘Ce obstacole putem întâlni la implementarea proiectului?’. Putem observa că răspunsul la aceste întrebări se mulează foarte bine cu principiile metodologiei Agile, o metodă SDLC care este în continuă adaptare în funcție de cerințe pe măsură ce proiectul progresează. Mai mult, această metodă SDLC are la bază o multitudine de ședințe de proiect, printre care și ședințe concrete de estimare. De fapt, sunt multe similitudini

¹ SDLC este o abreviere pentru Software Development Life Cycle reprezentând ciclul de dezvoltare al proiectelor software. Un bun exemplu pentru un ciclu de dezvoltare este reprezentat de metodologia Agile SCRUM sau Waterfall, V-model etc.

între ritmul dinamic al proiectelor de tip IoT și acest tip de metodologie. Un capitol întreg va fi structurat pe baza acestor similitudini, metodologia de livrare fiind de asemenea inclusă în lista zonelor majore de risc. Stabilind încă de la început ce metodologie de livrare vom folosi, vom fluidiza considerabil procesul de dezvoltare.

În concluzie, ne dorim ca prin metoda documentată pe parcursul tezei să conturăm cele mai importante riscuri atunci când ne gândim la dezvoltarea unui proiect IoT. Totodată, conștientizându-le, ne va fi mai ușor să le adresăm pentru optimizarea proceselor de livrare, dar și a gestionării costurilor atât în ceea ce privește resursele tehnologice, cât și cele umane. Scopul nostru este să aducem un plus de valoare fiecărui business care se ocupă de livrarea proiectelor, dar și celor care, atrași fiind de natura practică a acestui domeniu, doresc să intre în rândul dezvoltatorilor prin intermediul proiectelor individuale. Este important ca metoda noastră să ofere indicații precise, în funcție de piața largă a proiectelor deja existente. Un alt factor important de care trebuie să ținem cont este domeniul și răspunsurile la diferite întrebări ce țin de implementarea unui proiect în cadrul acestuia. Ca un exemplu, intuim deja de ce un proiect de casa inteligentă poate fi afectat de mult mai puține riscuri decât un proiect din cadrul orașelor inteligente. Următorul pas este, totuși să avem o valoare orientativă cât mai aproape de adevăr, ideal procentuală, ce face diferența dintre acestea. Pe lângă stabilirea unor valori concrete, este important să găsim și o aplicație de afișare a datelor, deoarece vom lucra cu o suită de răspunsuri complexe achiziționate de la specialiști și generaliști din acest domeniu. Pentru acest ultim aspect am ales aplicația Tableau, aplicație ale cărei avantaje vor fi prezentate separat într-un capitol dedicat. Așa cum Agile poate acoperi ritmul foarte dinamic al evoluției pentru aceste proiecte, Tableau poate acoperi seturile complexe de date achiziționate atât de un proiect, cât și de aplicația noastră de risc. Ne va fi astfel, mult mai ușor să alocăm un buget inițial, să licităm în fața unui client atunci când dorim implementarea unui proiect sau pur și simplu să contribuim la o imagine generală asupra stadiului actual al relației dintre riscuri și proiectele IoT.

1.3 Conținutul tezei de doctorat

În aceasta secțiune, vom începe cu documentarea pașilor ce sunt considerați utili pentru a ne crea o imagine de ansamblu asupra riscului în ceea ce privește proiectele de tip Internet of Things. Principalele etape ale unui proiect de tip IoT sunt reprezentate de:

- identificarea unei nevoi a utilizatorului;
- identificarea echipamentelor ce trebuie achiziționate după înțelegerea arhitecturii de tip IoT;
- Alegerea unui mediu de dezvoltare pentru proiectele IoT;
- comunicarea cu echipamentele fizice, atât local cât și online;
- înțelegerea conceptului de serviciu Web și familiarizarea cu bibliotecile ce pot fi apelate din mediul de dezvoltare;
- rutine de hibernare și alte noțiuni de optimizare a consumului.

Pe baza acestor pași și după studierea structurilor deja existente de analiză a riscului, vom identifica alte zone majore de risc, exceptând riscurile ce țin de securitatea aplicațiilor. Există foarte puțină literatură de specialitate care tratează acest subiect al zonelor de risc mai departe de vulnerabilitățile software și tipurile de atacuri

deja existente. Din acest punct de vedere, teza se bazează în principal pe activități de cercetare fundamentală, unde am avut plăcerea să urmărim o ipoteză interesantă și să mergem pe acest drum al cunoașterii pentru definirea unor metode de gândire noi. Pe lângă acestea, domeniul fiind cel al ingineriei, teza trebuie să conțină și aspecte de cercetare aplicativă, scopul final fiind crearea unei metode de calcul ce aduce valoare fiecărui dezvoltator de proiecte IoT. Vom detalia în cele ce urmează unde se face trecerea de la partea fundamentală la cea aplicativă și care sunt activitățile specifice de cercetare.

Așadar, primele acțiuni au fost de cercetare fundamentală. Aici, pe baza cerințelor unui proiect de tip IoT, am identificat mai multe zone noi unde dorim să calculăm riscul. Printre acestea amintim de riscurile ce țin de mediul de instalare, soluția de alimentare a proiectului în sine, echipamentele fizice, siguranța și protecția muncii. Așa cum bine intuim, acestea au o pondere diferită în funcție de domeniul în cadrul căruia dorim să implementăm proiectul IoT. Pentru a înțelege mai bine nevoile și soluțiile IoT, în urma căutărilor am ales o listă ușor de urmărit și de înțeles ce se regăsește în cadrul furnizorilor de soluții IoT. Pe parcursul lucrării, vom vedea că rezultatele depind foarte mult de acest domeniu care poate fi militar, al sănătății, domenii ce țin de casa inteligentă, orașe inteligente, agricultură etc. Tot din punct de vedere fundamental, pentru a acoperi cât mai multe scenarii, am împărțit zonele majore de risc în categorii de risc, respectiv în factori de risc. Țin să mulțumesc, de asemenea, celor din spatele platformei OWASP pentru inspirația de a organiza ierarhic și granular riscurile ce țin de securitatea software. Totodată, deși am abordat și noi problema securității în funcție de primele amenințări la adresa proiectelor IoT, recomandăm servicii specializate care pot oferi consultanță strict pe această parte. Totuși, cât de departe trebuie să ne gândim și unde se oprește riscul unui astfel de proiect? Folosind maparea ierarhică amintită mai sus, ca un exemplu, zona majoră de risc de tip mediu de instalare este formată din mai multe categorii (condiții meteorologice sau factorul uman) care la rândul lor au la bază factori de risc (temperaturi ridicate, scăzute, vânt, sabotaj, corupere accidentală a datelor etc.). După organizarea domeniilor și a structurii zonelor majore de risc, începem să simțim nevoia acțiunilor de cercetare din punct de vedere aplicativ.

Trecerea la partea aplicativă a fost construirea unui chestionar îndreptat către specialiștii și generaliștii IoT pentru stabilirea unor ponderi în ceea ce privește categoriile principale de risc. Aceștia sunt reprezentați de ingineri software, autori de articole de specialitate din sfera IoT sau pur și simplu indivizi care au cochetat cu acest domeniu prin construirea unui proiect individual. Avem un capitol dedicat unde se prezintă audiența, dar și statistici demografice relevante ce țin de zona geografică, funcția pe care aceștia o dețin în cadrul echipei de livrare, conștientizare a riscului și domeniile unde au implementat proiectele. Pe lângă aceste statistici, cel mai important livrabil al acestui capitol sunt ponderile fiecărei categorii de risc în cadrul metodei noastre de calcul. După citirea ponderilor vom vedea cum proiecte dintr-un domeniu sunt mai predispuse la anumite riscuri decât alte proiecte din alte domenii. Cu toate acestea, în următorul capitol ne gândim și la beneficiarii metodei noastre de calcul și anume oricine este interesat de gestionarea riscului înainte de trecerea la procesele de livrare. De data aceasta, chestionarul nu este public și va fi îndreptat către cei care doresc să analizeze în detaliu nevoile și riscurile proiectelor specifice. Vom folosi ponderile din primul chestionar pentru a calcula o notă finală a proiectului, dar și pentru a furniza lămuriri detaliate. Beneficiarul, și anume respondentul celui de-al doilea chestionar va avea la dispoziție un număr de 70 de întrebări pentru a ne face o idee cât mai bună despre factorii de risc specifici. Cu ajutorul întrebărilor, vom asigura

o notă fiecărui factor. Dacă acesta este conștient deja de un factor sau a ales să îl trateze, îl vom considera element neutru. Dacă acesta nu a tratat un factor de risc, îi vom asigura o valoare în funcție de rapoartele de cercetare specializate deja existente. Vom vedea pe parcursul lucrării că am folosit rapoarte interesante de la Eurostat pentru stabilirea ratei de incidență în ceea ce privește siguranța și protecția muncii, dar și rapoarte de la companii specializate în managementul proiectelor. Dintre acestea amintim de cei de la Atlassian, un nume important în ceea ce ține de eficientizarea livrării software, sau Project Management Institute, Wellington etc. Acestea din urmă au fost folosite pentru a stabili rata de incidență a factorilor de risc ce privesc partea de SDLC, și anume ciclurile de livrare pentru proiecte software.

Din punct de vedere tehnic, această abordare de tip chestionar este foarte utilă pentru identificarea riscurilor înainte de lansarea în execuție a unui proces [11]. După ce toate întrebările au fost adresate, informația va trece printr-un nod de calcul ce va avea ca ieșire diferite livrabile pentru o citire mai ușoară. Prin livrabile înțelegem tipuri de fișiere cunoscute, precum .xml, .txt, .csv etc. Pe baza acestor livrabile o notă generală va fi asignată proiectului și prezentată, în același mod intuitiv, părților interesate. Rezultatele vor fi afișate într-o manieră ușor de citit folosind Tableau. Am explicat, de asemenea, de ce am ales să folosim această aplicație de monitorizare și care sunt avantajele acesteia atunci când dorim să o aplicăm în cadrul proiectelor IoT.

Concluzionând, teza de doctorat va conține statusul actualizat în ceea ce privește nevoile și domeniile IoT actuale bazate pe experiența specialiștilor și generaliştilor ce au participat la acest studiu, noi categorii de risc pe care dorim să le analizăm și ponderile lor în funcție de domeniu, metoda de calcul unde folosim ponderile respective și un sistem unic de notare a factorilor de risc în funcție de răspunsurile specifice ale fiecărui beneficiar. În plus, din punct de vedere al mitigării acestor riscuri, vom avea un capitol dedicat pentru a evidenția beneficiile Agile ca metodă de livrare, dar și beneficiile Tableau ca aplicație de procesare și monitorizare a datelor. Totodată, vom vedea cum ne putem folosi de capacitatea de procesare a acestei aplicații pentru a genera o interfață intuitivă chiar pentru metoda noastră de calcul. În plus, din punct de vedere al costurilor, metoda noastră este eficientă deoarece am folosit Tableau Public care este gratuit. Singurele investiții au fost în zona de campanii pe Facebook pentru a atrage oameni cu experiență relevantă, în aplicațiile de construire/editare diagrame și în aplicația de generare a chestionarelor. Aceasta din urmă a fost necesară, deoarece ne dorim în jur de 2700² de răspunsuri pentru a face studiul nostru cât mai exact. Relevanța începe, totuși, de la 384³ de răspunsuri în sus și vom vedea în capitolul detaliat cum am ales aceste valori. Chestionarul este activ, iar la momentul scrierii acestei lucrări am acumulat în jur de 700 de răspunsuri.

² Valoare țintă pentru a atinge un nivel de încredere de 99% cu un interval de eroare de $\pm 2.5\%$.

³ Valoare țintă pentru a atinge un nivel de încredere de 95% cu un interval de eroare de $\pm 2.5\%$.

Capitolul 2

Zone majore de risc și analiza factorilor de risc

Atunci când o echipă de dezvoltare acceptă un proiect este ideal să cunoască din timp resursele necesare, dar și obstacolele ce pot apărea atunci când proiectul este implementat. Putem spune că suntem mai aproape de acest obiectiv dacă reușim să ne creăm un framework general, dar și scalabil pentru cuantificarea acestui factor de risc. Este imperativ să realizăm eforturi de cercetare pentru o cât mai bună acuratețe a estimărilor. După cum vom vedea în cele ce urmează acest lucru se va realiza prin asignarea unei note/procent în funcție de natura fiecărui proiect și de studiul actual al fiecărei zone majore de risc în parte.

Înainte de a prezenta în detaliu cum calculăm riscul ce descrie zona majoră de risc reprezentată de ‘Mediu’, este important să știm care sunt zonele principale de interes, iar lista tratată în această lucrare este:

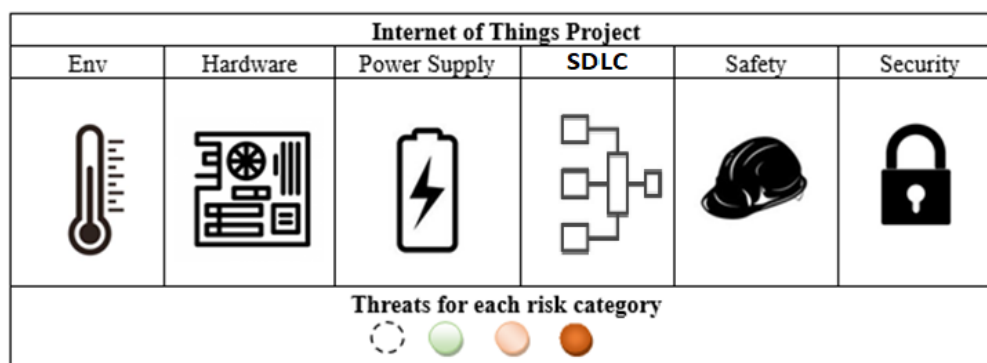


Figura 2.2 Zone majore de risc pentru proiectele IoT

După cum putem vedea mai sus, principalele zone majore de risc sunt reprezentate de:

- ‘Env’ – abbrev. **Environment** pentru riscuri privind mediul de instalare
- ‘Hardware’ - pentru zona de risc conturată în jurul echipamentelor fizice
- ‘Power Supply’ – pentru riscuri privind alimentarea
- ‘SDLC’ – pentru riscuri privind metodologia de livrare folosită
- ‘Safety’- riscuri privind protecția muncii
- ‘Security’ – riscuri privind securitatea informatică

Fiecare dintre aceste zone majore de risc este alcătuită din mai multe categorii de risc ce sunt împărțite în mod granular în factori de risc. Pe parcursul acestui capitol, am descris detaliat fiecare dintre factorii respectivi, dar și notarea acestora în funcție de proiectele pe care dorim să le implementăm. Pentru a ne face o idee despre tipul factorilor și ordinea ierarhică, avem următoarea figură unde sunt prezentate componentele zonei majore reprezentate de mediul de instalare al proiectului:

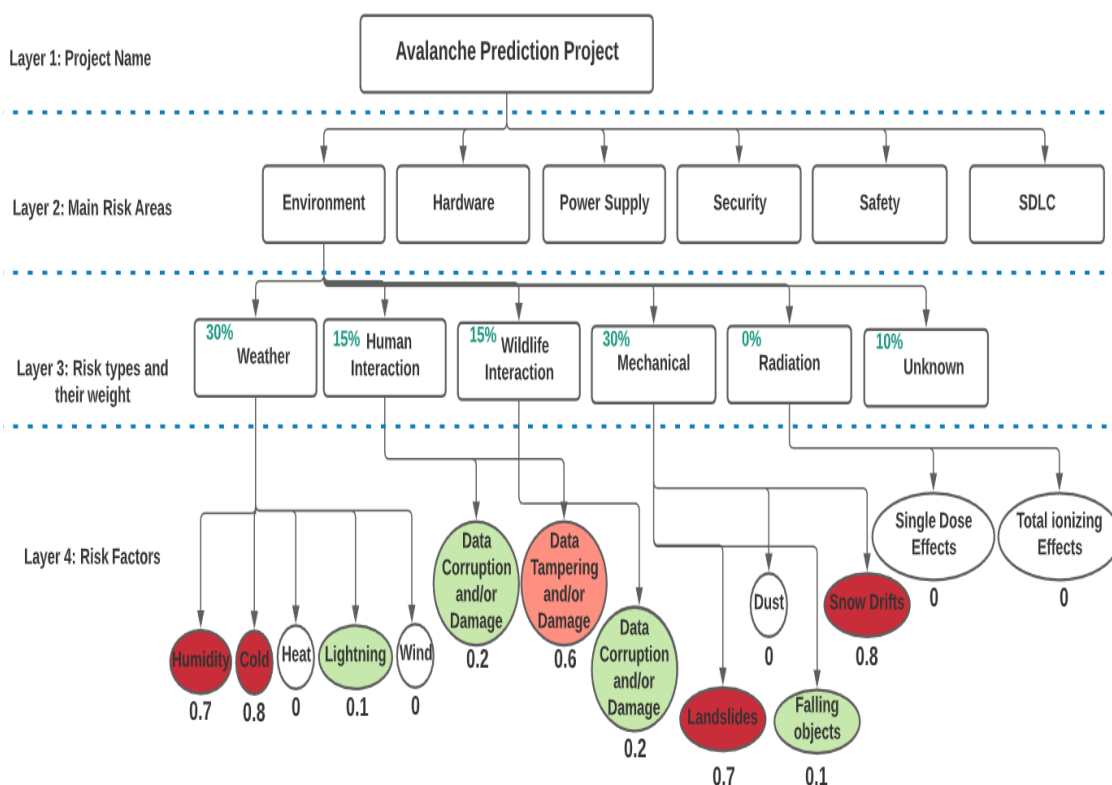


Figura 2.4 Zona majoră de risc 'Environment' pentru proiectul de predicție a avalanșelor

Observăm două tipuri de valori, și anume primul set de valori subunitare și al doilea set reprezentat de procente reprezentate cu verde. Valorile subunitare sunt rezultatul chestionarului pe care îl distribuim beneficiarilor metodei noastre de calcul, iar procentajele sunt ponderile fiecărei categorii în zona majoră de risc în funcție de natura proiectului. Acestea din urmă sunt rezultatul primului chestionar pe care l-am distribuit specialiștilor IoT pentru stabilirea ponderilor. Drumul de la răspunsul acestora până la stabilirea unui tabel de ponderi este descris detaliat în cadrul capitolului 5. Livrabilele acestui capitol sunt reprezentate de tabelele de ponderi pentru fiecare dintre zonele majore de risc enunțate anterior. Tabelele cu valorile actualizate se regăsesc în cadrul anexelor din teza principală. Pentru o înțelegere mai bună a abordării și a metodei de calcul, în cadrul capitolului am ales tabele populate cu date orientative, rotunjite care vor ajuta cititorul să înțeleagă legătura dintre zone majore de risc, categoriile de risc și factorii de risc pentru un proiect specific. Așadar fiecare tabel este conturat pe baza unui studiu de caz, în cadrul căruia am fost implicat în procesul de dezvoltare, respectiv livrare.

În figurile următoare avem exemple de astfel de tabele de ponderi și formulele cu ajutorul cărora le-am calculat în Tableau:

Environment Weights

Domain	Harsh_WeatherConditions	Mechanical_Hazards	Human_Interaction	Wildlife_Interaction	Radiation_Percentage
eHealth	14.81 %	7.41 %	55.56 %	11.11 %	11.11 %
Emergencies	18.60 %	30.23 %	34.88 %	9.30 %	6.98 %
Home_Automation	15.87 %	28.57 %	50.79 %	3.17 %	1.59 %
Industrial_control	9.68 %	32.26 %	41.94 %	6.45 %	9.68 %
Military	21.88 %	21.88 %	31.25 %	21.88 %	3.13 %
Retail_Logistics	3.57 %	35.71 %	53.57 %	3.57 %	3.57 %
Smart_Agriculture	35.48 %	25.81 %	29.03 %	9.68 %	0.00 %
Smart_Animal_Farming	12.50 %	25.00 %	50.00 %	12.50 %	0.00 %
Smart_city	26.67 %	32.00 %	33.33 %	6.67 %	1.33 %
Smart_env	21.62 %	24.32 %	32.43 %	18.92 %	2.70 %
Smart_meter	17.65 %	35.29 %	41.18 %	5.88 %	0.00 %

Figura A7.2 Tabel actualizat cu ponderile zonelor majore de risc în funcție de domeniu - 2

Environment:

```

AVG([Harsh weather conditions])
AVG([Mechanical Hazards])
AVG([Human Interaction])
AVG([Wildlife Interaction])
AVG([Radiation])
[Total_Env] = AVG([Harsh weather conditions]) + AVG([Mechanical
Hazards]) + AVG([Human Interaction]) + AVG([Wildlife Interaction]) +
AVG([Radiation])

Harsh_WeatherConditions = 100 * AVG([Harsh weather
conditions])/[Total_Env]
Mechanical_Hazards = 100 * AVG([Mechanical Hazards])/[Total_Env]
Human_Interaction = 100 * AVG([Human Interaction])/[Total_Env]
Wildlife_Interaction = 100 * AVG([Wildlife Interaction])/[Total_Env]
Radiation_Percentage = 100 * AVG([Radiation])/[Total_Env]

```

Figura A6.2 Formule Tableau pentru calcularea ponderilor - 2

În concluzie, acest capitol a fost dedicat documentării zonelor majore de risc pe care dorim să le acoperim, majoritatea ieșind din sfera securității informatice. Așadar, o analiză ca cea din figurile de mai sus a fost aplicată pe mai multe studii de caz, cu scopul de a înțelege necesitatea unei imagini de ansamblu asupra unor zone precum mediul de instalare și riscurile aferente, siguranță și protecția muncii, partea hardware împreună cu riscurile sale, soluțiile de alimentare și particularitățile lor, precum și vastul domeniu reprezentat de metodologiile de livrare folosite în ciclurile software.

Capitolul 3

Agile pentru livrarea proiectelor de tip IoT

În acest capitol, am explicat într-un mod obiectiv de ce metodologia Agile este recomandată pentru livrarea proiectelor IoT. Pentru o înțelegere mai bună a etapelor și a aplicării fundamentelor Agile, am utilizat, de asemenea, un studiu de caz, reprezentat de un proiect de automatizare a unui domiciliu (proiect de tip ‘Casa inteligentă’). Totodată, prin comparație cu alte metodologii precum binecunoscutele V-model sau Waterfall am evidențiat cum o parte din provocările unui proiect IoT pot fi abordate, chiar rezolvate numai prin alegerea unei metode potrivite de livrare. Firesc, după parcurgerea etapelor aplicate în cadrul studiului de caz ales, am sumarizat o listă cu avantajele acestei metode.

Principalul avantaj este reprezentat de calitatea produsului rezultat. Împărțind livrarea produsului în mai multe cicluri iterative, denumite sprinturi, sporim interacțiunea echipei de testare cu produsul nostru. Din punct de vedere al calității, echipa de testare are activități prezente pe tot parcursul procesului de livrare. Cu alte cuvinte, produsul este verificat în mod repetat, obligatoriu în fiecare sprint pentru a putea trece la următorul. Parcurgând lucrarea, vom observa o strânsă legătură între particularitățile Agile și riscurile ce pot fi mitigate din zona majoră de risc SDLC. Datorită faptului că defectele găsite pot fi adresate foarte devreme în SDLC, categoria principală de risc reprezentată de costuri scade semnificativ.

Următorul avantaj important este reprezentat de transparență. Aceasta este conferită de mai multe ședințe obligatorii atunci când folosim Agile Scrum ca metodă de livrare. Dezvoltând un proiect IoT, ne așteptăm la multiple schimbări pe parcursul proiectului, chiar la mai multe decât pentru un proiect obișnuit [12]. Acestea trebuie adresate din timp cu clientul pentru a vedea dacă influențează în orice fel scopul său inițial. Al doilea tip de transparență este cel din interiorul echipei de livrare. Acest lucru este datorat faptului că în orice moment pe parcursul proiectului, echipa de testare cunoaște activitățile echipei de dezvoltare și viceversa [13].

Legat de riscuri, îndeosebi de impactul lor asupra costurilor, găsirea timpurie a acestora este favorizată de adoptarea acestei metodologii. Capacitatea identificării, dar și a soluționării factorilor de risc ne duce cu gândul la alt avantaj și anume cel al flexibilității. În cadrul unui astfel de domeniu, trebuie să ne așteptăm la modificări dese și să ne adaptăm la acestea pe măsură ce livrăm. Totodată, dacă clientul dorește alte cerințe sau cere modificarea celor deja existente, o echipă de dezvoltare trebuie să aibă posibilitatea de a le actualiza.

Alt avantaj este rapiditatea intrării pe piață a produsului pe care dorim să îl dezvoltăm. De obicei, proiectele de tip IoT vin ca urmare a unor eforturi inovative de

acoperire a unor nevoi reale în piață, indiferent dacă vorbim despre case inteligente, orașe inteligente, eHealth etc. Venind din acest mediu inovativ, este puțin timp pentru analizarea competiției și primul pe piață dobândește un mare avantaj reputațional care de multe ori îl ajută să devină lider de piață. Spre deosebire de alte metodologii, Agile încurajează livrarea propriu zisă, chiar din stadii timpurii ale proiectelor. În momentul de față, ne confruntăm cu un număr sporit de nevoi pe piață, creșterea acestui domeniu fiind estimată la 26% până în anul 2026 [14]. O altă statistică interesantă este reprezentată de faptul că proiectele livrate folosind Agile Scrum ajung cu 37% mai repede pe piață decât proiectele care sunt livrate folosind Waterfall [15].

Un alt avantaj este feedback-ul constant prezent în această metodologie. Clientul este implicat încă de la sfârșitul primului sprint în eforturile de dezvoltare, aprobarea acestuia fiind unul dintre criteriile de finalizare cu succes a sprintului. Totodată, prin acest mod de interacționare, el este încurajat să descopere chiar și alte funcționalități la care nu s-a gândit atunci când proiectul a fost acceptat. Pe lângă aceste posibilități, clientul poate realiza la rândul lui eforturi de cercetare în piață, iar descoperirile pot fi adresate cu șeful de produs sau cu managerii de proiect. Ca o consecință a acestei interacțiuni, relația profesională cu clientul se va îmbunătăți, ducând la o mai bună reputație, respectiv vizibilitate a firmei care s-a ocupat cu dezvoltarea produsului. Pe lângă acestea, cresc și șansele de loializare a clientului datorită interacțiunilor repetate cu acesta. Toate acestea stau la baza unui portofoliu solid pentru firma de dezvoltare, dar încurajează și existența unei companii de încredere pe piață. Atât clienții, cât și firmele de implementare a proiectelor de tip IoT vor beneficia de pe urma acestei colaborări. Totuși, cuvântul cheie aici este flexibilitatea, iar clientul optează pentru gradul de interacțiune cu firmele de dezvoltare. Discuția rămâne una deschisă în funcție de nevoile acestuia. Ca o concluzie, comunicarea între client și echipa de dezvoltare este foarte importantă, iar flexibilitatea metodologiei Agile poate fi pusă în valoare foarte bine de proiectele IoT. Aplicând Agile, putem maximiza eficiența acestei metode și totodată putem mitiga o mare parte dintre riscurile prezente în SLDC (prezentate detaliat în capitolul cu zonele majore de risc). Domeniul IoT generează un mediu foarte sănătos de dezvoltare, care încurajează inovația într-un ritm rapid. Este important să ținem pasul cu aceste modificări și să optimizăm constant metodele de dezvoltare.

Capitolul 4

Tableau pentru monitorizarea proiectelor de tip IoT

În cadrul acestui capitol, am explicat de ce recomandăm Tableau pentru a mitiga riscurile din zona datelor pe care dorim să le prelucrăm pentru proiectele IoT. Din punct de vedere al funcționalității, Tableau poate parsa și prelucra fișiere mari de date ce pot fi stocate atât local, cât și pe servere dedicate. În majoritatea proiectelor de tip IoT, ne dorim ca datele să fie disponibile de fiecare dată când se dorește consultarea acestora. Putem afișa informații relevante de pe diferite servere de baze de date acoperind o arie mare de tehnologii precum Oracle, Microsoft SQL Server, Amazon Redshift [16]. Totodată, putem parsa cele mai cunoscute tipuri de fișiere precum text, JSON, Microsoft Excel, PDF.

Această diversitate largă în ceea ce privește sursele de date pentru aplicația noastră de citire se mulează foarte bine cu multitudinea de informații achiziționate de proiectele noastre de tip IoT. Acesta din urmă are capacitatea de a procesa structuri complexe de date [17]. După cum ne-am obișnuit, pentru a evidenția avantajele Tableau, pe parcursul capitolului am ales un studiu de caz cu un volum mare de date pe care trebuie să-l procesăm, necesitând ca informațiile achiziționate să fie în timp real. Integrarea proiectelor de tip IoT cu Tableau conferă mediului de dezvoltare diferite avantaje, precum:

Diversitate – conferită de cele două tipuri de conexiune ‘Live’ (pentru proiecte care necesită actualizarea constantă a datelor, cum ar fi Smart Parking, Smart Irrigation, Smart Metering, Traffic Management, Home automation projects) sau ‘Extract’ (pentru proiecte care folosesc date ce nu trebuie actualizate în timp real, cum ar fi ‘Avalanche Prediction’, ‘Weather Stations’, ‘Air Pollution Monitoring’, ‘Garbage Monitoring’).

Aplicabilitate - Tableau Dashboards poate fi rulat pe o varietate foarte mare de dispozitive. Atunci când creăm un dashboard putem selecta și dispozitivele pe care dorim să vizualizăm respectiva interfață. Printre cele mai cunoscute dispozitive care suportă această funcționalitate se numără PC-uri, tablete, telefoane etc.). Ca o paranteză, interfața pentru studiul nostru de caz a fost gândită pentru telefoanele mobile [18]. Nu mai este nevoie să creăm de la zero o pagină web folosind bibliotecile oferite de mediile de dezvoltare unde modelăm datele achiziționate (printre exemple se numără bibliotecile Xively).

Scalabilitate - de fiecare dată când avem nevoie să extindem proiectul, putem mări nedeterminat numărul de stații sau de senzori fără a afecta funcționalitățile de afișare. Chiar dacă spațiul pe disc este mai mare, deoarece achiziționăm mai multe date, funcționalitățile de parsare, sortare, modelare și afișare vor rămâne la fel.

Capitolul 5

Validarea ponderilor prin metoda chestionarului

În cadrul acestui capitol, vom explica legătura dintre răspunsurile participanților la studiu și stabilirea tabelului de ponderi. Vom vedea cum chestionarul nostru este împărțit în două zone principale.

Pe baza răspunsurilor la fiecare dintre cele două seturi de întrebări vom vedea cât de importantă este fiecare zonă majoră de risc și repartizarea acestora în funcție de domeniul de implementare, funcția ocupată de fiecare respondent în cadrul echipei de livrare, cum este perceput riscul de cei care livrează aceste proiecte, dar și distribuția proiectelor pe zonă geografică.

5.1 Alegerea audienței

Înainte de a prezenta chestionarul în sine, trebuie să înțelegem cum am ales populația pentru el. Scopul inițial a fost abordarea persoanelor tehnice ce au fost implicate în livrarea proiectelor de tip IoT. În cazul în care au livrat mai multe proiecte, este validă completarea chestionarului pentru fiecare dintre acestea. Deci, primul filtru a fost reprezentat de specialiști și generaliști IoT. Pentru a realiza acest lucru, contactarea specialiștilor (aceștia au fost reprezentați în mare parte chiar de autorii articolelor citate în referințe) s-a făcut și prin intermediul emailului.

Pentru abordarea generaliștilor am folosit campanii sponsorizate pe Facebook, postarea în grupuri specializate de IoT sau schimbul de chestionare pe website-uri construite în acest scop. În Figura 5.1 putem observa criteriile de selectare a populației din punct de vedere geografic pentru campania de pe Facebook, în timp ce în Figura 5.2 avem filtrele pe care le-am aplicat pentru o definiție cât mai precisă a populației. Este important de știut că relevanța datelor se păstrează prin cunoașterea și selectarea corectă a audienței.

Am tinde să credem că o audiență mai mare înseamnă mai multe răspunsuri pentru chestionar, dar trebuie să ne amintim că scopul este completarea acestuia doar de specialiștii care ne interesează din punct de vedere al relevanței.



Figura 5.1 Alegere audiență relevantă din punct de vedere geografic



Figura 5.2 Filtre pentru țintirea cât mai specifică a campaniei

După aplicarea filtrelor obținem o audiență mulțumitoare de 19 milioane de utilizatori care se mulează pe chestionarul nostru. Acest lucru este confirmat și de mesajul 'Your audience is defined' pe care îl putem vedea în Figura 5.1. Pentru demararea campaniei a fost nevoie să creăm o pagină de Facebook unde am postat progresul acesteia. Următorul pas este reprezentat de modul în care ne-am ales seturile de întrebări pentru a conferi relevanța necesară aplicației noastre de gestionare a riscului.

5.2 Alegerea setului de întrebări pentru chestionar

În cadrul acestui subcapitol vom vedea că avem diferite seturi de întrebări, fiecare cu un scop precis. Pentru o urmărire mai bună a acestui scop, în română vom prezenta următoarele seturi:

Setul 1 de întrebări își propune cunoașterea audienței și caracteristicile proiectului în care au fost implicați, acest set fiind împărțit în:

- Care a fost domeniul ultimului proiect IoT în care ați fost implicat?
Variante de răspuns: fiecare dintre domeniile pe care le-am abordat în capitolele anterioare (eHealth, SmartCity, Retail/Logistics, Military etc.)
- Care a fost rolul dumneavoastră în cadrul proiectului IoT?
Variante de răspuns: toate rolurile din cadrul unei echipe ce livrează IoT (Dezvoltator, Manager de proiect, Tester etc.) și proiecte individuale
- Care a fost numele sau funcționalitatea principală a proiectului IoT?
La această întrebare nu avem variante de răspuns, fiind un câmp obligatoriu care acceptă text. Vom folosi informația din acest câmp pentru prezentarea aplicației și a diversității funcționale ce caracterizează proiecte de acest tip.
- Credeți că gestionarea riscului aduce beneficii în cadrul proiectelor IoT?
Această întrebare are trei variante de răspuns (Da, Nu, Nu știu) și a fost adresată pentru a vedea dacă generaliștii/specialiștii au luat în considerare acest aspect.
- Ce știți despre analiza riscului pentru proiectele de tip Internet of Things?
Acesta nu este un câmp obligatoriu și nu are variante de răspuns. El poate fi completat la liber pentru a ne face o idee despre gradul de familiaritate al generaliștilor/specialiștilor cu subiectul principal al chestionarului/lucrării.
- Ce metodă de livrare ați folosit pentru proiectul vostru IoT?
Variante de răspuns: Agile, Waterfall, V-Model, Big-Bang, Alte metode
- V-ați gândit la normele de protecția muncii când ați livrat proiectul IoT?
Variante de răspuns: Da, Nu, Nu știu – pentru a ne face o impresie despre modul în care cei care răspund chestionarului abordează acest subiect.
- În ce țară trăiți?
Completarea acestei întrebări nu este obligatorie, dar ne ajută în a ne crea o impresie despre distribuția geografică a specialiștilor/ proiectelor IoT
- Dacă sunteți interesați de rezultatele acestui studiu, vă rugăm să introduceți adresa de email. La fel ca cea de mai sus, această întrebare nu este obligatorie. Cel care răspunde are ocazia de a primi rezultatele studiului după publicare dacă este interesat prin completarea acestui câmp.

Acesta a fost primul set de întrebări și-l vom folosi pentru a genera rapoartele demografice.

Unul dintre aceste rapoarte este cel din Figura 5.3, unde avem o distribuție relativ uniformă a proiectelor în funcție de domeniul lor de implementare. În Figura 5.4, observăm funcțiile ocupate de cei care au răspuns în cadrul proiectului IoT.

Project Distribution

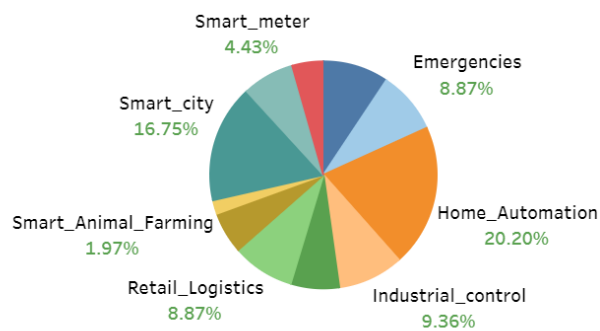


Figura 5.3 Reprezentare vizuală relevantă pentru distribuția proiectelor în funcție de domeniu

Job Description

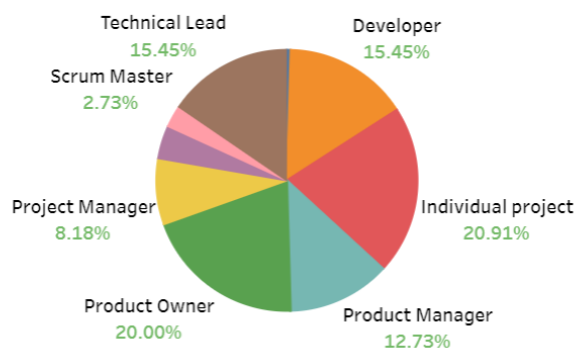


Figura 5.4 Raport demografic pentru distribuția funcțiilor în cadrul proiectului

Setul 2 de întrebări are ca scop popularea tabelor de ponderi pentru fiecare categorie majoră de risc. Valorile devin mai concludente direct proporțional cu numărul persoanelor care răspund la acest chestionar. Tot în ceea ce privește acest număr, putem considera ponderile satisfăcătoare atunci când atingem 2700 de respondenți. Acest număr este strâns legat de celelalte metrici care caracterizează chestionarul nostru. Printre cele mai relevante, amintim de nivelul țintă de încredere pe care ni-l dorim și anume de 99% cu o eroare de maxim 2.5%.

Revenind la al doilea set de întrebări, cu rezultate procentuale exacte pe care le putem varia în română a acestora este reprezentată de:

- Care a fost domeniul ultimului proiect IoT în care ați fost implicat?
Variante de răspuns: fiecare dintre domeniile pe care le-am abordat în capitolele anterioare (eHealth, SmartCity, Retail/Logistics, Military etc.). Observăm că această întrebare este comună cu setul 1. Pe lângă importanța sa demografică, acesta este principalul criteriu după care calculăm ponderile. Este de la sine înțeles de ce un proiect din zona de agricultură inteligentă este afectat mai mult de anumiți factori de risc de natură ambientală decât un proiect de casă inteligentă.
- După instalarea proiectului dumneavoastră, acesta va fi afectat de:
Variante de răspuns: condiții meteorologice extreme, faună, sabotaj etc. Această întrebare este adresată pentru a acoperi zona de 'Environment'
- Care dintre următoarele vulnerabilități au fost tratate când s-a dezvoltat proiectul? Variante de răspuns: Injecție SQL, Utilizare echipamente cu

vulnerabilități etc. Această întrebare este adresată pentru zona de ‘Security’

- Ce echipamente fizice ați folosit pentru construirea proiectului?
Variante de răspuns: echipamente de achiziție, echipamente de execuție, alte echipamente. Această întrebare este adresată pentru zona de ‘Hardware’
- Ce provocări ați întâmpinat pe parcursul livrării proiectului?
Variante de răspuns: Am avut nevoie de mai multe resurse pentru dezvoltare sau testare, estimarea costurilor, estimarea task-urilor etc. Această întrebare este adresată pentru acoperirea zonei de metodologie pentru livrarea IoT.
- Ce variante ați folosit pentru a alimenta proiectul pe care l-ați livrat?
Variante de răspuns: Baterii, Panouri fotovoltaice, Prize, Am folosit rutine de hibernare pentru prelungirea duratei de viață a bateriilor, am înlăturat consumatorii ce nu erau necesari etc. Această întrebare este adresată pentru a acoperi zona ‘Power Supply’
- Ce accidente de muncă poate cauza proiectul dumneavoastră? Variante de răspuns: Ciocniri, șocuri mecanice, tăieturi, electrocutare, incendii. Această întrebare a fost adresată pentru a acoperi zona de ‘Safety’.

După adresarea acestor întrebări, răspunsurile vor fi prelucrate cu ajutorul formulelor și se vor genera ponderile în funcție de domeniul de implementare. Acest lucru va duce la un proces foarte detaliat de gestionare a riscului ținând exact pe proiectul pe care dorim să-l evaluăm

5.3 De la întrebare la variabila de pondere

Un scenariu interesant este transformarea răspunsurilor în variabilele de pondere pe care le folosim în metoda noastră de calcul. Când vorbim despre aceste variabile, ne gândim la procentajele cu care am populat tabelele pentru fiecare zonă majoră de risc. Să luăm de exemplu ‘Environment’ ca zonă majoră de risc – ponderile pentru fiecare categorie de risc sunt evidențiate în Figura 5.5:

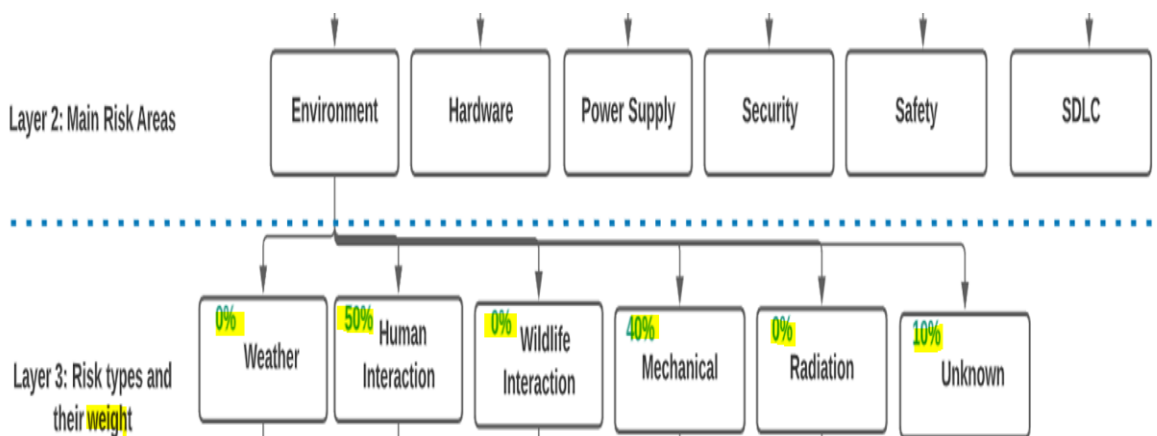


Figura 5.5 Exemplu valori finale pentru ponderile de risc

Primul pas pentru calcularea ponderilor este obținerea unui număr cât mai mare de răspunsuri la chestionar. Pentru această zonă majoră reprezentată de riscurile ce pot apărea în mediul de instalare a proiectului am adresat întrebarea din setul 2: „După instalarea proiectului dumneavoastră, va fi afectat de:”, bineînțeles cu variantele de răspuns reprezentate de condiții meteorologice nefavorabile, interacțiune nedorită, atât umană, cât și cu fauna, prezența unor riscuri mecanice și prezența radiației. Întrebarea din chestionar poate fi văzută în Figura 5.6.

* 6. After possible deployment of your project, it can be affected by: (tick the boxes that apply for your project)

- ☐ Harsh weather conditions (cold, heat, wind, lightning, humidity)
- ☐ Mechanical Hazards (landslides, snowdrifts, falling objects)
- ☐ Human Interaction (accidental data corruption, data tampering, vandalism, sabotage)
- ☐ Wildlife Interaction (data corruption, damage to components)
- ☐ Radiation
- ☐ Other Environment Hazards or None Environmental Hazards

Figura 5.6 Întrebare adresată audienței relevante pentru stabilirea ponderilor din zona majoră de risc reprezentată de mediu

În aceeași figură putem observa că fiecare variantă este explicată, încurajând persoana ce îl completează să se gândească la toate scenariile ce pot apărea după punerea în producție. Acest aspect contribuie și la creșterea gradului de familizare cu procesul de analiză a riscului, un proces foarte important în livrarea software. Pentru crearea și distribuirea chestionarului am folosit un tool plătit, reprezentat de serviciul celor de la SoGoSurvey. Am ales acest serviciu datorită unor avantaje precum paleta diversificată de funcționalități structurale pentru întrebări, dar și posibilitatea de a asigna valori dorite pentru fiecare dintre răspunsuri. Totodată, valorile pe care le asignăm sunt foarte utile atunci când folosim programe de generare a statisticilor, Tableau fiind unul dintre ele. După ce am prezentat întrebarea și am primit numărul de răspunsuri, următorul pas este exportul datelor și asignarea de valori. Vedem în Figura 5.7 datele pe care le-am considerat relevante pentru reprezentarea răspunsurilor:

i Codes are sometimes used by certain statistical programs for analysis.

Do you wish to assign codes? ☒

6. After possible deployment of your project, it can be affected by: (tick the boxes that apply for your project)

6 Environment

Harsh weather conditions (cold, heat, wind, lightning, humidity)	1
Mechanical Hazards (landslides, snowdrifts, falling objects)	1
Human Interaction (accidental data corruption, data tampering, vandalism, sabotage)	1
Wildlife Interaction (data corruption, damage to components)	1
Radiation	1

Figura 5.7 Asignare valori de tip boolean pentru generarea statisticilor relevante

Am asignat valoarea 1 pentru toate răspunsurile unde s-a ales respectiva variantă. Traducând, în exportul nostru reprezentat de fișierul Excel vom avea o listă cu toate răspunsurile la această întrebare și cu variantele pe care le-am ales. Dacă un respondent a ales doar prima și ultima variantă, pe coloanele respective vom avea valoarea 1. Pentru toate celelalte variante vom avea trei valori NULL. Pentru a realiza o statistică relevantă în funcție de domeniu, vom exporta și răspunsurile la prima întrebare din fiecare set. Am ales valorile 1 și 0, deoarece atunci când aplicăm media pe coloane avem o valoare subunitară care poate fi transformată foarte ușor într-un procent. Fiecare zonă majoră de risc este împărțită în categorii, apoi calculăm totalul acestor valori. După ce avem numărul total, și anume suma categoriilor, calculăm procentul fiecăreia în raport cu numărul total. Toate funcțiile pe care le-am aplicat asupra acestei variabile fac parte din procesul de agregare menit să genereze valori cât mai ușor de citit, respectiv de folosit în formula noastră de calcul. Prelucrarea valorilor asignate pentru fiecare răspuns se poate observa în Figura 5.9, acesta fiind pasul final din procesul de stabilire a ponderilor.

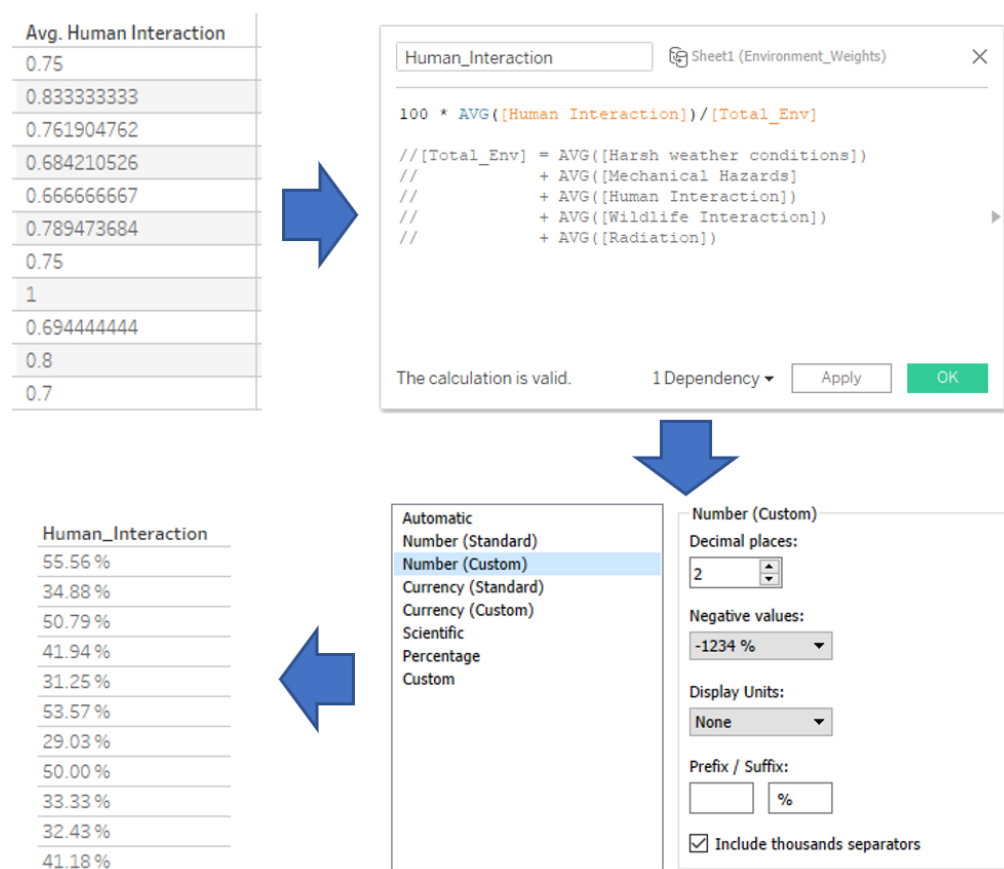


Figura 5.9 Prelucrarea datelor pentru obținerea unei valori procentuale relevante

Pentru interfața aplicației am optat tot pentru Tableau deoarece, pe lângă funcționalitățile complexe de monitorizare, avem predefinite și acțiuni. Fiecare tabel de pondere se află în pagini separate și este actualizat pe măsură ce primim mai multe răspunsuri la chestionarele noastre. Trimiterea la acestea se face prin intermediul butoanelor acționabile. Aceste tabele au rol informativ, iar pe baza valorilor cu care sunt populate calculăm nota finală de risc pentru aplicația/proiectul IoT pe care dorim să-l analizăm. Interfața poate fi observată în figura următoare:

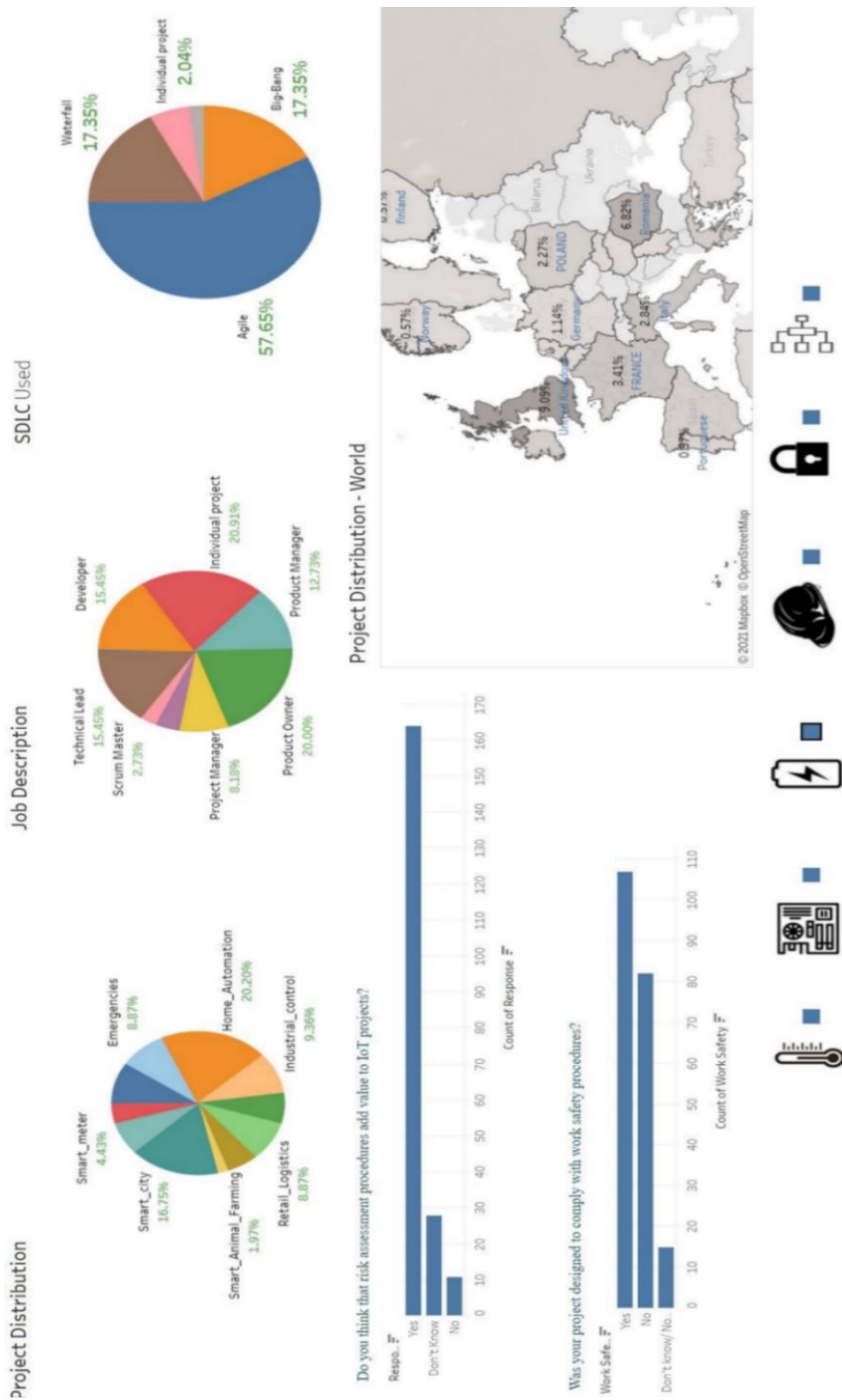


Figura A5.1 Interfața realizată în Tableau pentru aplicația de analiză a riscului

Capitolul 6

Concluzii

În primul rând, riscul total al aplicației trebuie să tindă către zero pentru orice proiect IoT. Parametrul asignat pentru acoperirea riscurilor neprevăzute este necesar, deoarece este evident faptul că nu există aplicație, respectiv proiect fără nici măcar un risc. În al doilea rând, procentul de acoperire al proiectului trebuie să tindă către 100%, valoare ce este, de asemenea, una ideală. Nu există aplicație [19] care să nu aibă vulnerabilități sau zone neacoperite.

În practică, persoanele ce sunt considerate manageri de proiect sau manageri tehnici ce coordonează echipele de livrare vor fi conștiente de aceste valori înainte să înceapă implementarea în sine. Descoperirea riscurilor cât mai devreme în SDLC duce la o eficientizare a costurilor, dar și a resurselor umane ce sunt asignate pe proiectul respectiv. Această abordare poate ajuta foarte mult activitățile de estimare, îndeosebi atunci când se livrează folosind Agile, metodă foarte la modă în zilele de astăzi [13]. Am explicat în capitolul 3 din teză de ce această metodă este preferată atunci când se structurează un proiect IoT. Pe lângă eficientizarea costurilor prin descoperirea timpurie a riscurilor, acest proces de analiză poate aduce valoare echipelor de livrare și dintr-o altă perspectivă indirectă ce constă în creșterea portofoliului de negociere în licitarea pentru un proiect. Beneficiile sunt și de partea clientului care este beneficiarul direct al rezultatelor echipei de dezvoltare. O analiză completă a riscului duce la o comunicare transparentă și o colaborare productivă prin expunerea unor indici de performanță ce se pot atinge mult mai ușor prin soluționarea specifică a problemelor din procesul de dezvoltare.

Aplicând fiecare etapă a acestui ‘framework’ când construim un proiect ne ajută să înțelegem de ce avem nevoie să cumpărăm sau să implementăm pentru a minimiza riscul, așadar pentru a contribui proactiv la succesul proiectului nostru (bazându-ne pe indicatori de performanță stabiliți în prealabil). Cu alte cuvinte, dacă observăm o valoare ridicată în cadrul unei zone majore de risc, ne putem gândi specific la măsurile concrete pe care le putem lua, nu pentru a obține un scor mai bun, ci pentru a minimiza componenta de risc respectivă, contribuind astfel în mod direct la succesul proiectului analizat. Un prim beneficiu al acestui proces de analiză este conștientizarea riscului ce iese din sfera securității informației. Următorul pas este reprezentat de specificitatea cu care alegem să tratăm riscul. În cele din urmă contribuim la crearea unei baze de date ce poate fi interogată oricând pentru a putea obține statistici utile (atât demografice, cât și tehnice acestea din urmă putând fi folosite ca repere în analiza proiectelor asemănătoare). Un exemplu de astfel de statistică arată că doar 26.78% dintre cei care au fost implicați în livrarea de proiecte IoT din sfera orașelor inteligente nu au avut probleme cu estimarea costurilor. În cazul acceptării sau licitării pentru un proiect din această sferă, este util, chiar imperativ să

prezentăm faptul că suntem constienți de acest aspect și avem soluții specifice pentru gestionarea atentă a bugetului pe care dorim să-l investim în dezvoltarea proiectului.

6.1 Rezultate obținute

Din punct de vedere al rezultatelor obținute putem spune că ne-am atins majoritatea obiectivelor definite la începutul activităților de cercetare, atât din punct de vedere fundamental, cât și aplicativ. Pentru o urmărire mai ușoară vom prezenta rezultatele concrete împărțite în funcție de capitolele unde au fost elaborate. După cel introductiv în care s-au prezentat direcțiile pe care dorim să le abordăm, următorul capitol s-a ocupat de definirea zonelor majore de risc și metoda de calcul pe care am ales-o pentru notarea factorilor de risc specifici ce afectează proiectele IoT.

Deci, principalele contribuții ce s-au evidențiat în urma activităților de cercetare se pot împărți astfel:

Începând cu capitolul 2 din teză am definit zone majore de risc ce afectează proiectele IoT și le-am împărțit în categorii și factori specifici de risc. Fiecare zonă a fost prezentată în cadrul unei secțiuni alături de un studiu de caz pentru a înțelege mai bine cum beneficiarii metodei noastre de calcul își aleg factorii de risc. În cadrul aceluiași capitol am documentat ecuațiile folosite în metoda noastră de calcul. Acestea sunt formate din ponderile zonelor majore de risc pentru un proiect în funcție de domeniu și de media aritmetică a factorilor de risc din cadrul unei categorii. Astfel, am identificat, pe lângă zona de securitate informatică, alte zone majore de risc importante precum soluția de alimentare, mediul de instalare, siguranța și protecția muncii, zona echipamentelor fizice și zona riscurilor de livrare software. Acestea au un tabel de ponderi specific în funcție de frecvența apariției în cadrul unui domeniu. Am creat acest tabel de ponderi printr-un studiu aplicat unei audiențe de specialiști și generalisți IoT. Pe baza acestui studiu am stabilit care zonă are o relevanță mai mare în cadrul unui domeniu anume – amintim că lista noastră include un număr de douăsprezece domenii de actualitate (eHealth, militar, case inteligente, orașe inteligente, agricultură inteligentă, farmare inteligentă, măsurare inteligentă, logistică și retail, control industrial, monitorizarea mediului, securitate și urgențe). Tot în cadrul aceluiași capitol am arătat cum putem obține nota pentru fiecare factor de risc în sine. Acest aspect se realizează tot printr-un chestionar îndreptat asupra unui beneficiar al metodei noastre de calcul (project manager, technical lead, arhitect, dezvoltator individual etc.). Prin intermediul acestui chestionar, el își notează fiecare factor de risc în funcție de nevoile, obiectivele și constrângerile specifice. Atunci când nu reușește să ofere o valoare relevantă am apelat la statistici deja existente, furnizate în urma altor studii conduse de Eurostat și Project Management Academy. Ca un mic exemplu, dacă ne gândim la factorul de risc ‘Gestionarea conflictelor în echipă’ ce face parte din categoria ‘Resurse umane’ din zona majoră de risc ‘SDLC’ este puțin mai dificil să cuantificăm riscul înainte de a cunoaște și de a lucra cu echipa de dezvoltare. În consecință, vom alege o valoare de referință de 0.09 pentru metoda noastră de calcul (după cum am văzut în această secțiune, 9% dintre proiectele care eșuează au conflictul între membrii echipei ca motiv). Pe baza literaturii parcurse suntem primii care vin cu o metodă de calcul pentru a cuantifica și a analiza riscul din cadrul mai multor zone de interes în ceea ce privește proiectele IoT. De aceea, pe baza datelor concrete în urma studiului am reușit să sporim gradul de conștientizare a

riscului în rândul celor care au participat. Metoda noastră de calcul va fi din ce în ce mai precisă cu cât primim mai multe răspunsuri la chestionarele pe care le-am construit.

Capitolul 3 din teză vine cu o soluție de mitigare a riscului prin adoptarea unei metode de livrare ce se aseamănă foarte mult cu trendul IoT și evoluția acestuia în dinamicul context al dezvoltării tehnologice. Această metodă de livrare este reprezentată de Agile, iar în cadrul acestui capitol am explicat avantajele și cum abordarea acesteia în livrarea IoT duce la o scădere considerabilă a riscului din cadrul SDLC. Acest lucru s-a făcut cu ajutorul unui studiu de caz ale cărui etape au fost mapate pe principalele etape de livrare și repere din metodologia Agile. Datorită flexibilității și posibilității de a adresa majoritatea factorilor de risc din capitolul 2 recomandăm această metodologie pentru dezvoltarea și livrarea proiectelor IoT, acolo unde se poate.

De asemenea, capitolul 4 vine cu o rezolvare de mitigare a riscului prin folosirea unei soluții de procesare și monitorizare a proiectelor reprezentată de Tableau. Aici am evidențiat faptul că multe dintre cerințele unui proiect IoT pot fi acoperite de funcționalitățile acestei aplicații. Pentru a demonstra acest lucru ne-am ales un studiu de caz bazat pe o nevoie reală (un proiect de parcare inteligentă). Implementarea soluției de procesare și monitorizare s-a realizat cu zero costuri, folosind versiunea gratuită a acestei aplicații. Recomandăm folosirea acestei aplicații pentru monitorizare și afișare, deoarece adresează în mod indirect o bună parte din factorii de risc prezentați în capitolul 2, în special din zona echipamentelor fizice. Tableau este o soluție foarte bună pentru lucrul cu pachete foarte mari de date, oferind posibilitatea de a susține o parte majoră din logica de procesare în timp real, eliberând astfel resursele plăcuțelor de procesare ce sunt integrate cu elementele de achiziție, respectiv de execuție.

În capitolul 5, ultimul înainte de concluzii, am avut ca scop validarea ponderilor prin metoda chestionarului și procesarea răspunsurilor folosind Tableau. Am început prin a defini audiența de care avem nevoie atunci când dorim să începem o campanie/un studiu care intră sub umbrela proiectelor IoT. Deoarece ne-am așteptat la răspunsuri numeroase, o provocare a fost reprezentată de alegerea și gestionarea datelor pe care le-am primit. Pe parcursul capitolului am prezentat formulele la care ne-am gândit pentru a defini ponderile fiecărei categorii de risc în metoda noastră de calcul. Totodată, am evidențiat și soluția tehnică pe care o propunem pentru a face trecerea de la o întrebare la o valoare concretă în metoda de calcul folosită. Cum ne-am obișnuit deja, am folosit Tableau chiar și pentru aplicația noastră de risc și am aplicat funcționalitățile necesare pentru a oferi utilizatorilor o interfață intuitivă unde pot vedea toate informațiile actualizate. Mai mult, pe baza acestor informații care se actualizează pe măsură ce primim cât mai multe pachete cu răspunsuri de la entitățile interesate am creat variabile cu ajutorul cărora vom calcula nota finală a unui proiect din punct de vedere al riscului. Acestea vor fi aplicate pe răspunsurile specifice pe care le primim de la client. Chiar dacă această notă finală este un reper important, vom oferi posibilitatea utilizatorului de a vedea și o analiză detaliată a zonelor ce au contribuit la aceasta notă. Avantajele folosirii unei astfel de metode ce nu este prezentă în literatura de specialitate va ajuta procesele decizionale pe baza cărora se alege, se dezvoltă, respectiv se livrează proiectele IoT. Acest ultim capitol ne demonstrează că discuția în ceea ce privește riscul poate fi dusă și în alte zone decât cea legată de securitate și vulnerabilități software. În plus, reprezintă un pas important pe drumul cuantificării riscurilor ce pot părea inabordabile/neprevăzute.

6.2 Contribuții originale

Vom dedica acest capitol pentru documentarea contribuțiilor originale prezentate în detaliu pe parcursul tezei de doctorat. Începem, așadar, din punct de vedere business cu partea de nevoi și constrângeri ce țin de domeniul IoT, parte ce a determinat redactarea acestei teze. Deci, avem următoarele contribuții originale:

- 1) Conștientizarea și documentarea nevoii de a avea o metodă de calcul care să cuantifice riscul prezent în alte domenii decât cel de securitate informatică. Nevoia și stadiul actual au fost prezentate în detaliu în cadrul primului raport de cercetare prezentat în secțiunea următoare la punctul [25]. Pentru o mai bună înțelegere a acestui subiect am ales exemple din experiența mea profesională, fiind astfel mai ușor să evidențiez zone neacoperite de risc. Un exemplu potrivit este reprezentat de modulul de predicție al avalanșelor, proiect ce este afectat de o mulțime de factori de risc, mai ales cei prezenți în mediul de instalare. Studiul de caz a fost publicat și prezentat pe îndelete în articolul publicat și notat cu [20]. Pe parcursul lucrării, putem găsi aceste noțiuni în capitolul introductiv, dar și în capitolul 2.
- 2) Prezentarea unor factori de risc din zone neanalizate până acum ce pot afecta proiectele de tip Internet of Things și construirea unei metode de clasificare și reprezentare. Acestea au fost documentate pe parcursul articolului și raportului din [21, 27]. Pe parcursul lucrării, aceștia sunt detaliați în capitolul 2.
- 3) Elaborarea unei metode de calcul pentru a reprezenta greutatea fiecărui factor de risc prezentat la punctul anterior în funcție de cele mai noi domenii în care se implementează proiectele IoT. Aceasta a fost prezentată în raportul de cercetare de la [26]. Pentru o categorie concretă de risc axată pe un studiu de caz sugestiv am publicat metoda de calcul pe care am conceput-o în cadrul articolului de la [24]. În cadrul tezei, metoda este prezentată punctual în funcție de fiecare categorie majoră de risc în cadrul capitolelor 2 și 5.
- 4) Dezvoltarea unor chestionare orientate către specialiștii și generaliștii din domeniul IoT pentru a stabili ponderea factorilor de risc în funcție de domeniul ales de aceștia pentru a implementa proiectul. Mai mult, unul dintre chestionare este orientat către beneficiarii metodei noastre de calcul ce își pot realiza procesul de analiză a riscului pentru a aduce un plus de valoare business-ului în care sunt implicați. Acestea sunt prezentate în detaliu, alături de beneficiile și indicii de performanță măsurabili, în cadrul raportului de cercetare de la [28]. Pe parcursul lucrării, chestionarele, audiența și metodele de procesare a răspunsurilor sunt prezentate în capitolul 5.
- 5) Metode de mitigare a riscului SDLC prin alegerea unei metode de livrare software potrivite în funcție de cerințele proiectului. Prezentarea acestora și a factorilor de risc specifici ce contribuie la metoda de livrare se găsesc în cadrul articolului publicat de la [23]. Acestea sunt prezentate în capitolul 3 al acestei lucrări.

- 6) Metode de mitigare a riscului din zonele SDLC și 'Hardware' prin alegerea unei aplicații corecte de procesare și afișare. Acestea se regăsesc în articolul publicat menționat în secțiunea următoare la [22]. În cadrul tezei, metodele și avantajele tehnologiei de afișare sunt prezentate în capitolul 4.
- 7) Construirea funcționalităților principale pentru o interfață intuitivă care să acopere funcționalitățile principale ale metodei noastre de calcul, de la răspunsurile primite în chestionare până la reprezentarea grafică a ponderilor de risc. Aceste funcționalități au fost documentate în cadrul raportului de cercetare de la [29], iar tehnologiile folosite în articolul publicat de la [22]. Interfața și metoda de prelucrare a datelor achiziționate de la specialiștii IoT se regăsesc în cadrul capitolului 4.

6.3 Lista lucrărilor originale

Structurarea metodei de calcul în contextul prezentat, procesarea și notarea factorilor de risc, dar și rezultatele obținute pe parcursul acestei teze au fost publicate atât la conferințe specializate, cât și în reviste relevante în domeniul ingineriei. Pe lângă rapoartele științifice prezentate în fiecare semestru al pregătirii, lista de publicații conține un număr de cinci articole unde am contribuit ca autor principal.

Înainte de prezentarea listei, țin să mulțumesc specialiștilor care au contribuit atât cu timpul, cât și cu expertiza la notarea și analiza articolelor.

Avem așadar următoarea listă de lucrări originale, clasificate în funcție de natura lor și ordonate cronologic:

Publicații:

[20] *Vlad-Valentin Firețeanu, Andreea Tudor-Șerban, Ioan Ștefan Sacala, Mihnea Alexandru Moisescu*, Avalanche Prediction Based on Snow Level Monitoring using Wireless Sensor Networks, Applied Mechanics and Materials, (ICMERA), vol 656, pp 369-377, Octombrie 2014

[21] *Vlad-Valentin Firețeanu*, Risk Assesment parameters for Internet of Things projects, 15th International Conference on Engineering of Modern Electric Systems (EMES) IEEE, pp 41-44, Iunie 2019

[22] *Vlad-Valentin Firețeanu*, Integrating Tableau with Internet of Things Acquiring Projects, 12th Internatioanl Conference on Electronics, computers and Artificial Intelligence (ECAI) IEEE, Iunie 2020

[23] *Vlad-Valentin Firețeanu*, Agile Methodology Advantages when delivering Internet of Things projects, 12th Internatioanl Conference on Electronics, computers and Artificial Intelligence (ECAI) IEEE, Iunie 2020

[24] *Vlad-Valentin Firețeanu, Mihai Ciuc Ph. D.* Designing Risk Assesment Applications for Internet of Things projects, Buletin Universitatea Politehnica București, vol Inginerie Electrică și Știința Calculatoarelor, Iunie 2021

[25] *Vlad-Valentin Fireșteanu*, Quantifying Work Safety Risk Factors for Internet of Things Projects, International Conference on Electrical, Computer and Energy Technologies, ICECET2021, Decembrie 2021

Rapoarte de cercetare:

[26] *Vlad-Valentin Fireșteanu*, Nevoi și constrângeri în contextul proiectelor Internet of Things, Iunie 2016

[27] *Vlad-Valentin Fireșteanu*, Metode de calculare a riscului în contextul proiectelor Internet of Things, Decembrie 2016

[28] *Vlad-Valentin Fireșteanu*, Prezentarea factorilor de risc pentru proiectele Internet of Things, Iunie 2017

[29] *Vlad-Valentin Fireșteanu*, Analiza, notarea și procesarea factorilor de risc în cadrul proiectelor Internet of Things, Decembrie 2017

[30] *Vlad-Valentin Fireșteanu*, Funcționalitățile principale ale aplicației de gestionare a riscului pentru proiectele Internet of Things, Iunie 2018

6.4 Perspective de dezvoltare ulterioară

Eficiența acestui framework este determinată de eforturile de cercetare necesare pentru mentenanța și actualizarea sa. În funcție de stadiul actual al proiectelor, de eficiența lor, dar și de actualizările ce apar constant într-un asemenea mediu dinamic, ponderile factorilor de risc vor suferi schimbări. Chiar dacă majoritatea aplicațiilor sunt construite în jurul părții de securitate software, pe parcursul lucrării s-a demonstrat nevoia de acoperire, respectiv de îmbunătățire și a altor zone majore, precum siguranța fizică a echipamentelor, managementul autonomiei etc.

Legat de aceste zone noi, una dintre cele mai importante perspective de dezvoltare ulterioară este studiul constant al pieței pentru a adăuga sau actualiza zone noi de risc. De asemenea, putem adăuga și domenii noi în metoda noastră de calcul, fiind ajutați de scalabilitatea acesteia. Totodată, în paralel cu aceste activități de cercetare în piață este necesară abordarea cât mai multor specialiști și generaliști IoT pentru a stabili ponderi cât mai exacte. Așadar, cu cât metoda noastră de calcul este folosită mai mult, iar chestionarul circulă mai des în cadrul comunității profesionale IoT, cu atât răspunsurile pe care le oferim beneficiarilor sunt mai aproape de contextul actual IoT. Un alt avantaj al abordării specialiștilor este reprezentat de statisticile interesante pe care le putem genera folosind un pachet așa mare de date. Deci, când trebuie să parsăm și să interpretăm din ce în ce mai multe date putem alege diferite formule de parcurgere inteligentă a arborelui generat de răspunsurile la chestionarele noastre. Putem observa anumite trenduri, iar pe baza lor să oferim consultanță sau sfaturi înainte de demararea unui proiect. Am observat, de exemplu, că o bună parte din proiectele de casa inteligentă au fost realizate în cadrul unui proiect individual, fără ca dezvoltatorul să fie parte dintr-o echipă dedicată de dezvoltare care lucrează după anumite metodologii de livrare. Așadar, astfel de proiecte au fost mai predispuse la riscuri legate de estimarea costurilor, și în general a resurselor, lipsa unor activități de testare software dedicate, gradul foarte mic de acoperire în ceea ce privește vulnerabilitățile de securitate etc. Scopul metodei este generarea de metrice care să

vină în ajutorul tuturor resurselor implicate în crearea unui proiect, orientat în funcție de rolul și nevoile fiecăruia.

Prin urmare, un alt pas indicat pentru metoda noastră este legat de mentenanța și actualizarea interfeței cu utilizatorul, orientată mai ales către partea cu datele demografice. În funcție de parcurgerea inteligentă prezentată mai sus, se pot adăuga numeroase funcționalități și acțiuni la nivel de interfață. Printr-o abordare interactivă cu diagramele ne dorim să filtrăm ponderile doar pentru domeniul care ne interesează printr-un simplu click pe pictograma acestuia. În consecință, în funcție de câmpul pe care dorim să-l acționăm, un singur tabel de ponderi va fi generat. Acesta va include toate zonele majore de risc și procentele de relevanță specifice. Ne dorim așadar o fragmentare inteligentă a datelor, în prezent acestea fiind afișate în totalitate. Tot din punct de vedere al ușurinței cu care ne dorim să parcurgem informațiile avem în vedere și implementarea unei funcționalități de gradient al culorilor. Astfel, ne va fi mai ușor să urmărim, atât nouă cât și beneficiarilor direcți, dacă o categorie de risc are o pondere mai ridicată în cadrul unui domeniu. Acest aspect va contribui notabil la gradul de conștientizare a riscului. Plecând de la același exemplu, un dezvoltator amator care dorește să cocheteze cu proiectul IoT va fi conștient încă de la început de riscurile ce pot apărea atât pe parcursul dezvoltării, cât și după ce proiectul a fost instalat și este considerat funcțional. Crește astfel posibilitatea ca dezvoltatorul să realizeze o analiză mai detaliată a proiectului înainte de a-l aborda. Va reuși, în acest fel, să se orienteze către componente ce nu sunt identificate ca fiind vulnerabile, se va gândi la protecțiile adiționale pe care trebuie să le achiziționeze, la soluții alternative de alimentare ș.a.m.d. Trecerea sa la acest domeniu va fi una echilibrată, fiind conștient de mai multe aspecte pe care trebuie să le ia în calcul sau pe baza cărora trebuie să se documenteze.

La un nivel superior, în ceea ce privește livrarea unui proiect în cadrul unei companii dezvoltate, un manager de proiect va avea o resursă suplimentară înainte de a gestiona o echipă de dezvoltare, respectiv înainte de accepta un proiect dintr-un anumit domeniu de interes. Ca un exemplu, atunci când ia contact cu riscurile unui anumit domeniu și ponderea acestora, se poate hotărî să investească mai multe resurse în testarea non-funcțională atunci când are de-a face cu un proiect militar, contribuind activ la succesul proiectului. Totodată, după cum am mai specificat pe parcursul lucrării, atunci când se licitează pentru un proiect nou, folosirea metodei noastre de calcul poate fi prezentată ca un avantaj în fața clientului. Faptul că avem la dispoziție o aplicație care ne ajută în gestionarea optimă a resurselor se va răsfrânge indirect și asupra clientului.

În concluzie, odată cu evoluția continuă a acestui domeniu, trebuie să fim pregătiți de apariția anumitor standarde de livrare sau de funcționare. Ne dorim ca această metodă de calcul a riscului să fie printre primii pași care se fac în această direcție de standardizare. Odată cu timpul și cu implicarea resurselor relevante vom reuși să înțelegem în ce măsură practicile deja existente pentru livrarea proiectelor software se aplică sau suferă modificări în contextul IoT, cu ce provocări noi vine acest domeniu și ce putem face noi, de la tehnicieni entuziaști până la ingineri cu experiență pentru a contribui la o dezvoltare echilibrată, sănătoasă și sigură.

Bibliografie

- [1] Mohammad Ammad-Udidin, Imran Baig, El-Hadi M. Aggoune, Muhammad Ayaz, *Wireless Sensor's Civil Applications, Prototypes, and Future Integration Possibilities: A Review*, IEEE Sensors Journal, vol.18, 2017, pp 4-30
- [2] H.P. Enterprise, *Internet of Things research study*, Hewlett Packard Enterprise Release, 2015
- [3] Y. Qing, L. Jun, *Take unauthorized control of Zigbee devices*, Publicat online în 2015, disponibil la <https://media.defcon.org/defcon23/defcon23presentations/> accesat pe data de 9 Septembrie 2018
- [4] S. Ranger, *What is IoT? Everything you need to know about the Internet of Things right now*, Zdnet, 2020
- [5] Bruce Potter, *Microsoft SDL Threat Modelling Tool*, Network Security, vol. 2009, numărul 1, January 2009, pp 15-18
- [6] David Levitsky, *Assessing Security Risk in IoT Devices*, 2018, disponibilă online la următoarea adresă <https://digitalcommons.calpoly.edu/theses/1954>, accesată pe data de 15 Noiembrie 2020
- [7] Colin Tankard, *The security issues of the Internet of Things*, Computer Fraud and Security, vol 2015, pp 11-14
- [8] Hanny F. Atlam, Ezz El-Din Hemdan, Ahmed Alenezi, *Security Development Lifecycle, Internet of Things Forensics: A review*, Internet of Things, vol 11, 2020, pp 1-41
- [9] Arne Bröring; Stefan Schmid; Corina-Kim Schindhelm; Abdelmajid Khelil; Sebastian Käbis; Denis Kramer, *Enabling IoT Ecosystems through Platform Interoperability*, IEEE Software , Volume: 34, Issue: 1, Jan.-Feb. 2017, pp 54 – 61
- [10] Montbel Thibaud, Huihui Chi, Wei Zhou, Selwyn Piramuthu, *Internet of Things (IoT) in high- risk Environment, Health and Safety (EHS) industries*, vol 108, 2018, pp 79-95
- [11] G.G. Gable, *Integrating case study and survey research methods: an example in information systems*, European Journal of Information Systems, Volume 3, Decembrie 2017, pp 112-126
- [12] Jim Chase, *The Evolution of the Internet of Things*, White Paper, Texas instruments USA 2013
- [13] Kent Beck, Mike Beedle, Arie van Bennekum, Alistair Cockburn, Ward Cunningham, Martin Fowler, James Grenning, Jim Highsmith, Andrew Hunt, Ron Jeffries, Jon

Kern,Brian Marick,Robert C. Martin,Steve Mellor,Ken Schwaber,Jeff Sutherland,Dave Thomas, *Manifesto for Agile Software Development*, Februarie 2021

[14] Mordor Intelligence Report, *Internet of things Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021-2026)*, disponibil online la <https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry> accesat pe data de 21 Iunie 2021

[15] Mike McCormick, *Waterfall vs. Agile Methodology*, Editura MPCS.Inc, 2012

[16] Data Flair Trainings, *Types of Tableau Data Sources with Connection Establishment Process*, Technical Training, Data Flair disponibil la <https://data-flair.training/blogs/tableau-data-sources/> accesat pe data de 16 August 2020

[17] Sugimiyanto Suma Rashid Mehmood Aiiad Albeshri, *Automatic Event Detection in Smart Cities Using Big Data Analytics*, International Conference on Smart Cities, Infrastructure, Technologies and Applications SCITA 2017: Smart Societies, Infrastructure, Technologies and Applications ,2017, pp 111-122

[18] Tableau Community, *Create Dashboard Layouts for Different Device Types*, informație de pe site-ul oficial Tableau disponibil la https://help.tableau.com/current/pro/desktop/en-us/dashboards_dsd_create.htm , accesat pe data de 12 Februarie 2020

[19] Dorothy Graham, *Foundation of Software Testing*, Editura Cengage, USA, 2006

[20] Vlad-Valentin Fireșteanu, Andreea Tudor-Șerban, Ioan Ștefan Sacala, Mihnea Alexandru Moisescu, *Avalanche Prediction Based on Snow Level Monitoring using Wireless Sensor Networks*, Applied Mechanics and Materials, (ICMERA), vol 656, pp 369-377, Octombrie 2014

[21] Vlad-Valentin Fireșteanu, *Risk Assesment parameters for Internet of Things projects*, 15th International Conference on Engineering of Modern Electric Systems (EMES) IEEE, pp 41-44, Iunie 2019

[22] Vlad-Valentin Fireșteanu, *Integrating Tableau with Internet of Things Acquiring Projects*, 12th Internatioanal Conference on Electronics, computers and Artificial Inteligence (ECAI) IEEE, Iunie 2020

[23] Vlad-Valentin Fireșteanu, *Agile Methodology Advantages when delivering Internet of Things projects*, 12th International Conference on Electronics, computers and Artificial Inteligence (ECAI) IEEE, Iunie 2020

[24] Vlad-Valentin Fireșteanu, Mihai Ciuc Ph. D. *Designing Risk Assesment Applications for Internet of Things projects*, Buletin Universitatea Politehnica București, vol. Inginerie Electrică și Știința Calculatoarelor, Iunie 2021

[25] Vlad-Valentin Fireșteanu, *Quantifying Work Safety Risk Factors for Internet of Things Projects*, International Conference on Electrical, Computer and Energy Technologies, ICECET2021, Decembrie 2021

[26] Vlad-Valentin Fireșteanu, *Raport de cercetare: Nevoi și constrângeri în contextul proiectelor Internet of Things*, Iunie 2016

[27] Vlad-Valentin Fireșteanu, *Raport de cercetare: Metode de calculare a riscului în contextul proiectelor Internet of Things*, Decembrie 2016

[28] Vlad-Valentin Fireșteanu, *Raport de cercetare: Prezentarea factorilor de risc pentru proiectele Internet of Things*, Iunie 2017

[29] Vlad-Valentin Fireșteanu, *Raport de cercetare: Analiza, notarea și procesarea factorilor de risc în cadrul proiectelor Internet of Things*, Decembrie 2017

[30] Vlad-Valentin Fireșteanu, *Raport de cercetare: Funcționalitățile principale ale aplicației de gestionare a riscului pentru proiectele Internet of Things*, Iunie 2018