Raport privind integrarea testelor de framework privind vizualizare și monitorizare

Raport științific și tehnic 2021

28.05.2021

Istoricul versiunilor

Istoricul versiunilor			
Autor	Commentarii	Versiune	Data
Oliviu Matei	Schiță	0.1	
Daniela Delinschi, Rudolf Erdei	Schiță	0.3	
Oliviu Matei, Daniela Delinschi, Rudolf Erdei	Final	1.0	2021.05.28

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Cuprins

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

1.Introducere

În sfera lumii cloud, apare o nouă paradigmă, și anume calculul serverless, care este un model de execuție bazat pe componente mici care pornesc sau mor în funcție de necesități și utilizarea lor. În acest caz, resursele cloud sunt alocate dinamic. Prețul se bazează mai mult pe cantitatea reală de resurse consumate de o aplicație, decât pe unități de capacitate pre-achiziționate (Miller2015).

În multe aplicații specifice, calculul serverless este soluția optimă care permite foarte ușor scalarea, planificarea capacității și întreținerea aplicației. Nu mai sunt necesare servere complete și resursele nu sunt blocate pentru totdeauna pentru o singură platformă (Raines2010).

Acest lucru nu trebuie confundat cu modelele de calcul sau de rețea care nu necesită un server real pentru a funcționa, cum ar fi peer-to-peer (P2P).

Aproape toți furnizorii serverless oferă ca și servicii platforme funcționale (FaaS), care execută logica aplicației, dar nu stochează date. În 2008, Google a lansat Google App Engine, care conținea facturarea contorizată pentru aplicațiile care foloseau un framework Python personalizat, dar nu puteau executa un cod arbitrar (Zahariev, 2009).

Kubeless și Fission sunt două platforme Open Source FaaS care rulează cu Kubernetes (Brewer, 2015). Primul furnizor public de cloud care oferea facilități serverless a fost Amazon cu AWS Lambda, în 2014 (Villamizar, 2016). Mai multe instrumente suplimentare serverless AWS, cum ar fi AWS Serverless Application Model (AWS SAM) Amazon CloudWatch, și altele însoțesc serviciul serverless. Google Cloud Platform oferă funcții Google Cloud din 2016 (Lynn, 2017). IBM oferă funcții IBM Cloud în public IBM Cloud începând cu 2016 (Cash, 2016). Microsoft Azure oferă funcții Azure, fie în cloud-ul public Azure, fie local prin Azure Stack (Sreeram, 2020).

Scopul principal al proiectului este de a crea o platformă unică care va optimiza și gestiona implementarea aplicațiilor serverless în mediul multi-cloud. Această abordare este rezultatul unei piețe în creștere a aplicațiilor care utilizează intensiv date, care urmăresc o mai bună eficiență a resurselor și a costurilor. Calculul serverless este poziționat pentru a schimba starea de joc pentru aplicațiile cloud.

Cazul de afaceri trebuie să valideze platforma Functionizer (Kritikos, 2019), demonstrând că computerul serverless poate fi încorporat în mod eficient în domeniul multi-cloud și demonstrează modul în care Functionizer face ca implementarea și gestionarea aplicațiilor cu mai multe date în cloud să fie mai rapide, mai simple și mai ieftine. Cazul de afaceri se concentrează pe o anumită soluție software, care preia un flux audio / video de pe dispozitive portabile (și anume ochelari inteligenți) și îl procesează pe un server pentru recunoașterea feței sau a imaginii. Acesta are aplicații în mai multe domenii, cum ar fi:

- **Industrie**. Din punctul de vedere al unei companie, există situații care necesită ca un specialist să fie prezent la diferite intervenții. Astfel puteți livra o pereche de ochelari oriunde aveți nevoie și un angajat care va fi echipat cu ei. Ochelarii vor transmite un flux live la tot ce urmărește angajatul, iar la un centru de asistență, expertul sau specialistul va putea oferi de la distanță asistența necesară.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

- **Medicină și răspunsuri de urgență.** Medicii și paramedicii pot fi coordonați de un specialist din camera de urgență în timpul manevrelor de resuscitare.
- **Training**. Lectorul poate efectua demonstrații live (prezentarea echipamentului, efectuarea intervențiilor chirurgicale sau a sănătății și siguranței), în timp ce studenții pot vedea exact ce face în timp real. De asemenea orele pot fi înregistrate și toate acestea, în timp ce lectorul își poate folosi ambele mâini.

2. Abordarea testării și validării

Acest capitol descrie abordarea de verificare și validare în cadrul platformei software Functionizer. Pentru testarea Functionizer, se aplică următoarele reguli generale:

- Testarea software-ului se face conform ghidului aplicabil descris în secțiunile 3-7;
- Revizuirile se fac în conformitate cu procesul de revizuire aplicabil, și anume evaluarea inter pares de către partenerii individuali în curs de dezvoltare.

2.1 Cartografierea procesului de dezvoltare

Activitățile de dezvoltare și testare ar trebui să se desfășoare în paralel. Activitățile de implementare a testelor ar trebui să înceapă de îndată ce încep activitățile de dezvoltare. În mod clar, testarea reală va începe de îndată ce entitatea de testat este disponibilă.

2.2 Strategia de testare

Atributele de calitate și importanța lor relativă au fost derivate din (Gorton, 2011). Rezultatele sunt raportate în Tabel 1 de mai jos.

Tabel 1 Importanța relativă a atributelor de calitate

Atribut de calitate	Descriere	Importanta relativă (%)
Mentenabilitate	Gradul de eficacitate și eficiență cu care produsul poate fi modificat.	22% (12/53)
Performanță, scalabilitate și capacitate	Performanța în raport cu numărul de resurse utilizate în condițiile menționate.	19% (10/53)
Fiabilitate	Gradul în care un sistem sau o componentă îndeplinește funcții specifice în condiții specificate pentru o perioadă de timp specificată. Include și „Disponibilitate”.	28% (8+7/53)
Securitate	Gradul de protecție a informațiilor și datelor, astfel încât persoanele sau sistemele neautorizate să nu le poată citi sau modifica iar persoanelor sau sistemelor autorizate nu li se refuză accesul.	23% (12/53)
Utilizare	Gradul în care produsul are atribute care îi permit să fie înțeles, învățat, utilizat și atractiv pentru utilizator, atunci când este utilizat în condiții specificate. Include, de asemenea, „Funcționalitate și gestionabilitate”.	8% (4+0/53)

Există o serie de puncte demne de menționat:
(Gorton, 2011) „Disponibilitate” au fost îmbinate sub „Fiabilitate” pentru a se potrivi cu descrierea atributului de calitate menționată de ISO-25010.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Cerințele nefuncționale din secțiunea „Funcționalitate și gestionabilitate” au fost luate în considerare în „Utilizare”, deoarece ISO-25010 nu menționează acest atribut de calitate. În (Gorton, 2011), acest atribut se referă la ușurința utilizării, instalării și gestionării platformei de către utilizatorul final.

Importanța relativă din tabelul de mai sus oferă o indicație a modului de împărțire a efortului de testare peste atributele de calitate.

Importanța relativă a fost determinată pe baza nivelurilor de prioritate atribuite cerințelor nefuncționale. Singurele niveluri luate în considerare sunt Must și Should, întrucât sunt declarate nivelurile care desemnează cerințele care trebuie îndeplinite de platforma implementată. Pentru fiecare atribut de calitate, importanța a fost determinată prin însumarea greutății atribuite (Must = 2, Should = 1, others = 0) pentru nivelul de prioritate atribuit unei cerințe referitoare la acea calitate. Numărul total de puncte din toate categoriile a fost de 53. Acest scor este menit doar ca o valoare pur orientativă.

Exemple ale atributelor de calitate menționate anterior în sistemul prevăzut pot fi găsite în T2.3 în tabelul fiecărei cerințe de la capitolul „Use case”.

Atributele de calitate vor fi măsurate folosind Indicele Calității (TQI) al TIOBE, așa cum este descris în secțiunea 8. Testarea nefuncțională, care se bazează și pe ISO-25010. Această potrivire garantează că toate atributele de calitate menționate mai sus sunt gestionate folosind un singur instrument. Facilitatea de funcționare și gestionabilitatea, care nu face parte din ISO-25010, vor fi evaluate utilizând feedback-ul utilizatorului și testele de utilizare.

Deși menținerea nu este o calitate care poate fi testată prin activitățile obișnuite de testare, ea poate fi măsurată, monitorizată și aplicată în mod static. Prin urmare, prin testarea Mentenabilității ne referim la conformitatea valorilor măsurate detectate pe codul sursă cu cadrul de vizualizare și monitorizare din (D2.4).

Pe lângă atributele de calitate menționate în (Gorton, 2011), activitățile de testare includ și teste pentru funcționalitatea adecvată, și anume îndeplinirea cerințelor funcționale și a cazurilor de utilizare. Deoarece eforturile de implementare vor urma prioritatea atribuită într-un astfel de document, testarea va urma aceeași prioritate a testării cerințelor.

2.2.1 Caracteristici de calitate pentru fiecare nivel de test

Testarea bazată pe atribute de calitate nu trebuie făcută pentru toate atributele de calitate de pe fiecare nivel de testare. În acest paragraf, atributele de calitate sunt atribuite unuia sau mai multor niveluri de testare. Pot exista diferite atribute de calitate pentru diferite subsisteme sau module.

Testarea unității

Securitatea ar trebui testată la acest nivel de testare numai în modulele în care codul gestionează datele sensibile ale utilizatorului.

Mentenabilitatea este verificată la nivel de unitate de către partenerii în curs de dezvoltare care trebuie să respecte, individual, cerințele nefuncționale aferente.

Testarea integrității

Performanța ar trebui testată la acest nivel, deoarece ar putea exista mai multe interacțiuni între diferite componente software implementate de același partener sau de diferiți parteneri. Astfel de componente vor fi identificate în arhitectura software, dar conform definițiilor cazurilor de utilizare, apar următoarele subsisteme: analize extinse bazate pe codul sursă, manipularea și analiza datelor și prognozarea sunt principalul subiect al activităților de testare.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Trebuie testate *funcționalitatea adecvată* la nivel de integrare datorită prezenței mai multor componente arhitecturale care oferă funcționalități cheie prin interacțiunea între ele. Aceste componente pot fi implementate fie de același partener, fie de parteneri diferiți. În ambele cazuri, este necesară testarea la acest nivel.

Testarea sistemului

- *Securitatea* ar trebui să fie acoperită în testele de sistem pentru a evita eventuale scurgeri de date și accesuri neautorizate cauzate de un schimb sensibil de date sensibile între componentele sistemului.
- *Utilizarea* ar trebui acoperită în testele sistemului, deoarece experiența utilizatorului depinde de întregul sistem. Toate interfețele utilizatorului trebuie testate aici.
- *Performanța* ar trebui testată la acest nivel, deoarece performanța generală a sistemelor depinde de mai multe componente care lucrează împreună.
- *Fiabilitatea* trebuie testată la acest nivel de testare, deoarece funcționarea defectuoasă a unei componente poate întrerupe serviciul oferit de întregul sistem.
- *Funcționalitatea adecvată* este testată temeinic la acest nivel pentru a garanta că cerințele cheie (Trebuie să aibă) au fost corect implementate.

Test de admitere

- *Utilizare*, deoarece utilizatorul final trebuie să aprobe ușurința utilizării sistemului final.
- *Funcționalitatea adecvată* este testată în sfârșit și de către utilizatorul final al sistemului, verificând dacă acesta îi îndeplinește așteptările.

Atributele de calitate sunt atribuite nivelului (testelor) de testare în care se potrivesc cel mai bine după cum urmează:

Tabel 2 Atribute de calitate atribuite nivelurilor de testare

Quality Attribute	*Test de unitate*	*Test de integrare*	*Test de sistem*	*Test de acceptare*
Mentenabilitate	+			
Performanţă		+		
Fiabilitate			++	
Securitate	++		+	
Utilizare			+	++
Funcționalitatea adecvată		+	++	+

(Gol) atributul de calitate nu este o problemă la acest nivel;
\+ Acest nivel de testare va acoperi acest atribut de calitate;
++ Atributul de calitate va fi acoperit cu atenție - este un obiectiv major la acest nivel de testare.

3. Testarea principiilor de implementare

Această secțiune descrie principiile de bază de implementare a testelor care stau la baza întregii abordări de testare pentru platforma software Functionizer. Acest lucru este elaborat în continuare la nivelul corespunzător în fiecare secțiune de specificații de testare.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

3.1 Trasabilitate

Trasabilitatea cerințelor testate la fiecare nivel de testare se realizează după cum urmează:

- Trasabilitatea se realizează prin asocierea identificatorilor de caz-test la identificatorii de cerințe folosind matrici dedicate de trasabilitate. Matricea are o coloană pentru ID-ul testului, o coloană pentru ID-ul cerinței funcționale sau nefuncționale și o coloană de descriere dedicată pentru informații suplimentare.
- Matricile vor fi completate după procesul individual de proiectare a testului și fac parte din acest document.

Verificarea dacă cerințele sunt efectiv testate de fiecare test face parte din procesul de revizuire.
Fiecare caz de testare este trasat la cerințele software corespunzătoare, dacă este cazul, și în cele din urmă la cazul de utilizare corespunzător (folosind o coloană suplimentară).
Documentația privind specificațiile testului trebuie să indice ce cerințe software sunt acoperite de fiecare test specificat.

3.2 Activități de testare

Următoarele activități trebuie efectuate:

Planificare și control
Scopul principal al acestei activități este de a oferi îndrumări pentru executarea și testarea activităților de finalizare.

Execuţie
Această activitate constă în principal în executarea articolelor de testare specificate utilizând infrastructura de testare implementată și generarea unui raport asupra rezultatelor.
Înainte de executarea efectivă a testelor, codul va fi compilat automat și verificat pentru controlul calității software-ului. De asemenea, vor fi verificate erorile și avertismentele compilatorului, care nu vor permite avertismentele / erorile L1 și L2.

Executarea testării sistemului și testarea integrării vor face parte din activitatea de integrare continuă. Execuția lor este, prin urmare, complet automatizată.
Cu toate acestea, pentru activitățile de testare unitară, partenerii individuali sunt responsabili de adoptarea propriei strategii de testare atâta timp cât respectă strategia de testare descrisă în secțiunea anterioară.
Prin urmare, partenerii individuali au capacitatea de a specifica individual propria infrastructură de testare și unitățile de testare pe baza arhitecturii propriului instrument. Cu toate acestea, în ceea ce privește raportarea și înregistrarea rezultatelor testării, acestea trebuie să respecte îndrumările menționate mai jos.

3.2.1 Completare

În această activitate, toate articolele de testare, jurnalele de testare și baza de testare sunt arhivate și se generează un raport de evaluare. Următoarele linii directoare se aplică pentru toate nivelurile de testare:

- Toate execuțiile testului trebuiesc urmărite;

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

- Acoperirea testului (cod și posibil calea), atunci când este disponibilă, și rezultatele testelor sunt principalele variabile care trebuiesc urmărite;
- Jurnalele de execuție trebuie să fie în format XML / JSON sau ușor convertibile, pentru a facilita generarea automată a raportului și trebuie să includă, pe lângă celelalte informații, ID-ul lor unic de testare;
- Jurnalele de execuție ale testelor trebuie încărcate pe platforma desemnată;
- Instrumentul care va fi utilizat pentru generarea de rapoarte trebuie să accepte XML ca ieșire.

3.2.2 Criterii de intrare

Înainte de începerea testării, trebuie îndeplinite următoarele criterii generale:

- Baza de testare trebuie să fie disponibilă conform descrierii din Tabelul 3.
- Codul trebuie să poată fi construit fără erori de compilare și trebuie să fie disponibil mediul complet pentru a trece de la cod la executabil.
- Pentru testarea statică a documentelor (revizuire) elementele de testare trebuie să fie sub controlul versiunii și în „Starea propunerii interne";
- Pentru testarea statică a codului, elementele de testare trebuie să fie construibile fără erori de compilare.

Tabel 3 Baza de testare a Functionizer

ID-ul documentului	Descrierea
D2.1	Analiza cerințelor
D2.2	Analiza cerințelor referitoare la studiul de caz
D.2.3	Descrierea metodologiei și a soft-ului
D2.4	Codul sursă al studiului de caz

În plus, pentru fiecare nivel de testare, trebuie îndeplinite și următoarele.
Testarea unității

- Livrabilele tehnice din WP2 trebuie să fie cel puțin într-o stare de proiectare avansată.
- Sunt disponibile coduri și unități testabile.
- Mediul de testare este gata.

Testarea integrării

- Testarea unității a fost finalizată cu succes.
- Bugurile cu prioritate maximă găsite în timpul testării unitare trebuie să fie remediate și închise.
- Planul de testare a integrării și mediul de testare pentru testarea integrării sunt gata.
- Livrabilele tehnice din WP2 trebuie să fie în starea lor de versiune finală.

Testarea sistemului

- Testarea integrării a fost finalizată cu succes.
- Bugurile cu prioritate maximă găsite în timpul testării integrării trebuie să fie remediate și închise.
- Livrabilele tehnice de la WP2 trebuie să fie în starea lor de versiune finală.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

- Sunt definite planuri detaliate de testare a sistemului (folosind piloții WP6 ca bază) și mediul de testare a sistemului este gata.
- Artefactele (adică codul sursă) din testele-pilot definite de sarcinile WP6 sunt disponibile pentru a fi furnizate ca intrare pe platforma Functionizer pentru testarea sistemului.

Testarea de acceptare

- Testarea sistemului a fost finalizată cu succes, iar mediul de testare a acceptării este gata de implementare.
- Bugurile cu prioritate maximă găsite în timpul testării sistemului trebuie să fi fost remediate și închise.
- Cerințele funcționale și nefuncționale prioritare sunt îndeplinite.
- O versiune beta a sistemului este disponibilă pentru a fi implementată partenerilor furnizori de cazuri de testare.

3.2.3 Criteriul de acceptare

Acest paragraf descrie pentru testul static și dinamic obiectivele pentru a decide dacă un test a trecut sau nu.

Test minim de acoperire

Acoperirea minimă a testelor va fi măsurată cu diferite instrumente, în funcție de platforma de dezvoltare utilizată de partenerul în curs de dezvoltare. În general, pentru proiectele bazate pe Java, JUnit trebuie utilizat ca platformă de testare la nivelul unității. Tabelul 4 prezintă procentele minime de acoperire pe nivel de test.

Tabel 4 Obiective de acoperire pentru acceptare:

Nivelul testului	% Acoperirea codului	% Acoperirea căii	% Acoperirea cerințelor	% Acoperirea cazului testului pilot
Test de unitate	50%	50%	-	-
Test de integrare	-	-	20%	-
Test de sistem	-	-	80%	33% (1/3)
Test de admitere	-	-	-	100% (3/3)

Acoperirea cerințelor va fi măsurată folosind urmele și jurnalele de execuție a testului.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Criterii de acceptare / respingere

Tabelul de mai jos prezintă criteriile dacă un test trece.

Tabel 5 Criterii de acceptare / respingere pentru test de executie

Nivelul testului	Criterii de acceptare / respingere
Test de unitate	Partea codului testat respectă comportamentul așteptat implementat de test.
Test de integrare	Cerința este implementată corect și oferă pe deplin funcționalitatea așteptată în cadrul constrângerii definite de cerințele nefuncționale.
Test de sistem	Cerința este implementată corect și oferă pe deplin funcționalitatea așteptată în cadrul constrângerii definite de cerințele nefuncționale.

3.3 Testarea regresiei

Testarea de regresie este activitatea de bază care reduce riscul introducerii de erori în codul sursă existent prin adăugarea de funcționalități, remedierea altor erori sau revizuirea caracteristicilor existente.

Testarea de regresie este de obicei aplicată în etapele avansate de dezvoltare atunci când sistemul a început deja să-și asume o formă și există mai multe funcționalități deja disponibile pentru a fi utilizate. Primele teste de regresie încep în paralel cu activitățile de testare a sistemului.

Strategia de testare a regresiei adoptată în acest proiect este o combinație de testare manuală și automată de regresie. Această alegere permite detectarea tipurilor de bug-uri care nu pot fi detectate doar prin adoptarea unei singure strategii.

3.3.1 Regresia manuală

Strategia de regresie manuală este complet delegată echipelor de dezvoltare, care verifică manual execuția corectă a funcționalităților modificate și a zonelor adiacente. Deoarece aceasta este o activitate care consumă foarte mult timp, este recomandat să fie efectuată numai după efectuarea unor modificări importante care ar putea afecta funcționalitatea de bază a sistemului.

În plus, pentru a verifica codul legat de modificările minore, este bine ca echipele de dezvoltare să pregătească o listă de verificare a funcționalităților minore care trebuie verificate și să le verifice toate împreună o dată.

3.3.2 Regresie automată

Acest tip de testare constă în reexecutarea unui set selectat de teste unitare și de integrare care s-au dovedit a identifica mai multe erori în trecut.

Pentru a selecta un astfel de set, este necesar să se colecteze statistici ale testelor trecute și eșuate în timpul activităților de testare anterioare. Cu toate acestea, dezvoltatorii și testerii pot sugera, de asemenea, teste specifice pe baza experienței lor cu codul și a erorilor anterioare. Testarea de regresie automată este considerată parte a integrării continue, aplicabilă la toate nivelurile de testare.

3.4 Raportarea problemelor

3.4.1 Instrucțiuni

Pentru a menține un flux de lucru eficient pentru remedierea erorilor și pentru a asigura că problemele deschise vor fi rezolvate în timp util, reporterul va urma câteva îndrumări simple.

Înainte de a crea o problemă, se trec prin următoarele instrucțiuni:

- Verificarea Documentației pentru dezvoltatori și Ghidul utilizatorului pentru a asigura că comportamentul pe care se raportează este într-adevăr o eroare, nu o caracteristică;
- Verificarea problemelor existente pentru a asigura că nu se copiază munca cuiva;
- Asigurarea că informațiile pe care urmează să fie raportate sunt o problemă tehnică;
- Dacă sunteți sigur că problema pe care o întâmpinați este cauzată de o eroare, înregistrați o nouă problemă.

3.4.2 Șablon de probleme

Șablonul de raportare a problemelor este un substituent implicit pentru fiecare nouă problemă. Rețineți că un nivel mai ridicat de detaliu din raport crește șansele ca un dezvoltator să poată reproduce problema. Este greu de sfătuit cu privire la orice probleme care nu pot fi replicate.

Titlul problemei

Titlul este o parte vitală a raportului de erori pentru dezvoltator și ajută la identificarea rapidă a unei probleme unice. Un titlu bine scris ar trebui să conțină o explicație clară și scurtă a problemei, punând accent pe cele mai importante puncte.

Descrierea problemei

Condiții prealabile

Descrierea condițiilor prealabile este un început excelent, furnizați informații despre setările de configurare a sistemului pe care le-ați modificat, informații detaliate despre entitățile create (produse, clienți etc.), versiunea Magento. Practic, tot ceea ce ar ajuta dezvoltatorul să creeze același mediu ca și dvs.

Pași pentru a reproduce.

Această parte a raportului de erori este cea mai importantă, deoarece un dezvoltator va folosi aceste informații pentru a reproduce problema. Problema este mai probabil să fie rezolvată dacă poate fi reprodusă. Ar trebui să descrieți cu precizie fiecare pas pe care l-ați făcut pentru a reproduce problema. Trebuie incluse cât mai multe informații, uneori chiar diferențe minore pot fi cruciale.

Rezultatul real și așteptat

Pentru a vă asigura că toți cei implicați în remediere sunt pe aceeași pagină, descrieți cu precizie rezultatul pe care vă așteptați să îl obțineți și rezultatul pe care l-ați observat efectiv după efectuarea pașilor.

Informații suplimentare

Informații suplimentare sunt deseori solicitate atunci când raportul de eroare este procesat, se poate economisi timp oferind jurnale, capturi de ecran, ramură de depozitare și revizuire care a fost verificată pentru a instala Functionizer sau orice alte artefacte legate de problemă, la judecata testatorului.

4. Testarea unitară

4.1 Scop

Testarea unității este un nivel de testare software în care sunt testate unități individuale/componente ale unui software. Scopul este de a valida faptul că fiecare unitate a software-ului funcționează conform proiectării.

4.2 Domeniul de aplicare

Testarea unitară este primul nivel de testare software și se efectuează înainte de testarea integrării și se concentrează pe codul sursă în sine.

4.3 Abordare

O unitate este cea mai mică parte testabilă a oricărui software. De obicei are una sau câteva intrări și de obicei o singură ieșire. În programarea procedurală, o unitate poate fi un program individual, o funcție, o procedură etc. În programarea orientată obiect, cea mai mică unitate este o metodă, care poate aparține unei clase de bază / super, clasă abstractă sau derivată / clasă copil. Cadrele de testare a unității, driverele, butoanele și obiectele simulate / false sunt utilizate pentru a ajuta la testarea unității. Cadrele de testare unitare vor fi utilizate și în scopuri de integrare continuă, pentru a permite testarea automată de regresie.

Deoarece testarea unitară este strâns legată de dezvoltare, va fi adoptată în procesul de dezvoltare în sine.

5. Testarea integrării

5.1 Scop

Acest capitol are ca scop definirea și descrierea procesului global de testare a integrării care va fi adoptat în cadrul Functionizer, pe baza selectării unei abordări de testare a integrării și a utilizării mediilor de colaborare și a instrumentelor de integrare continuă care să o susțină.

5.2 Domeniul de aplicare

Testarea integrării este al doilea nivel de testare efectuat după testarea unitară și înainte de testarea sistemului. În timpul testării integrării, toate unitățile individuale sunt combinate și testate ca un grup pentru a expune defecțiuni în interacțiunea dintre unitățile integrate.

5.3 Abordare

Există mai multe abordări de testare a integrării și cele mai utilizate sunt:

- **Big Bang**: este o abordare a testării integrării în care toate sau majoritatea unităților sunt combinate împreună și testate simultan. Această abordare este urmată atunci când echipa de testare primește întregul software într-un pachet. Testarea integrării Big Bang nu trebuie confundată cu testarea sistemului, deoarece prima testează doar interacțiunile dintre unități, în timp ce cea din urmă testează întregul sistem.
- **De sus în jos**: este o abordare a testării integrării în care unitățile de nivel superior sunt testate primul și unitățile de nivel inferior sunt testate treptat după aceea. Această abordare este urmată atunci când se realizează dezvoltarea de sus în jos. De obicei, unitățile de nivel inferior nu sunt disponibile în fazele inițiale ale dezvoltării, astfel încât Test Stubs sunt folosite pentru a le simula.
- **De jos în sus**: este o abordare a testării integrării în care unitățile de nivel inferior sunt testate mai întâi și unitățile de nivel superior sunt testate treptat după aceea. Această abordare este urmată atunci când se realizează dezvoltarea de jos în sus. De obicei, unitățile de nivel superior nu sunt disponibile în timpul fazelor inițiale ale dezvoltării, astfel încât driverele de testare sunt utilizate pentru a le simula.

Printre abordările de testare a integrării menționate mai sus, abordarea de jos în sus este cea mai potrivită pentru cazul platformei software Functionizer. Platforma generală este formată din componente individuale (de exemplu, cutii de instrumente), care sunt implementate independent de către partenerii relevanți și vor fi disponibile ca microservicii individuale, unificate în cadrul platformei Functionizer. Atât abordările de sus în jos, cât și cele de jos în sus se potrivesc bine în strategia de testare a integrării continue, care va fi adoptată pentru implementarea platformei finale, deoarece acestea permit testarea integrării să înceapă în paralel cu dezvoltarea efectivă a platformei. Acestea oferă o flexibilitate mai mare, deoarece componentele individuale sunt integrate în sistemul mai larg de îndată ce sunt disponibile și funcționale, în timp ce comportamentul componentelor care nu sunt încă pregătite este simulat prin intermediul driverelor de testare și al butoanelor, ducând în acest mod la un timp redus la piață. Între cele două abordări ierarhice, abordarea de jos în sus este mai potrivită, deoarece procesul de dezvoltare de jos în sus va fi adoptat pentru implementarea platformei. De fapt, dezvoltarea va începe de la funcționalitățile individuale de nivel scăzut pe care ar trebui să le ofere platforma generală și va progresa cu integrarea treptată a acestor funcționalități în componente și module mai largi.

Înainte de a începe testarea integrării, este important să se asigure că există cel puțin un document de proiectare adecvat disponibil, în care interacțiunile dintre fiecare unitate sunt clar specificate. În livrabilul D2.3 Descrierea metodologiei și a soft-ului, sunt specificate componentele principale ale sistemului și interfețele dintre ele. În plus, este important ca fiecare unitate separată să fie testată pe unitate înainte de testarea integrării și ca toate testele să fie automatizate în mod corespunzător în cea mai mare măsură, deoarece testarea manuală poate fi ineficientă deoarece dezvoltatorii trebuie să rețină multe artefacte de construcție și să le testeze manual. Acest lucru poate fi realizat prin activarea integrării continue, adică prin procesul de automatizare a construirii și testării codului de fiecare dată când un membru al echipei face modificări într-un mediu colaborativ.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Integrare continuă

Abordarea generală de integrare a Functionizer se va baza pe utilizarea unui mediu de colaborare, instrumente de integrare continuă și un plan de versionare. Strategia de mai sus va permite, pe de o parte, tuturor dezvoltatorilor să progreseze cu dezvoltarea propriului modul care lucrează în procese independente, folosind și propriile instrumente de testare și, pe de altă parte, să își integreze modulele între ele în versiunile majore, respectând planul de eliberări prevăzut. Acest lucru va duce, de asemenea, la detectarea deficiențelor la începutul dezvoltării, în care problemele sunt de obicei mai mici și mai ușor de rezolvat.

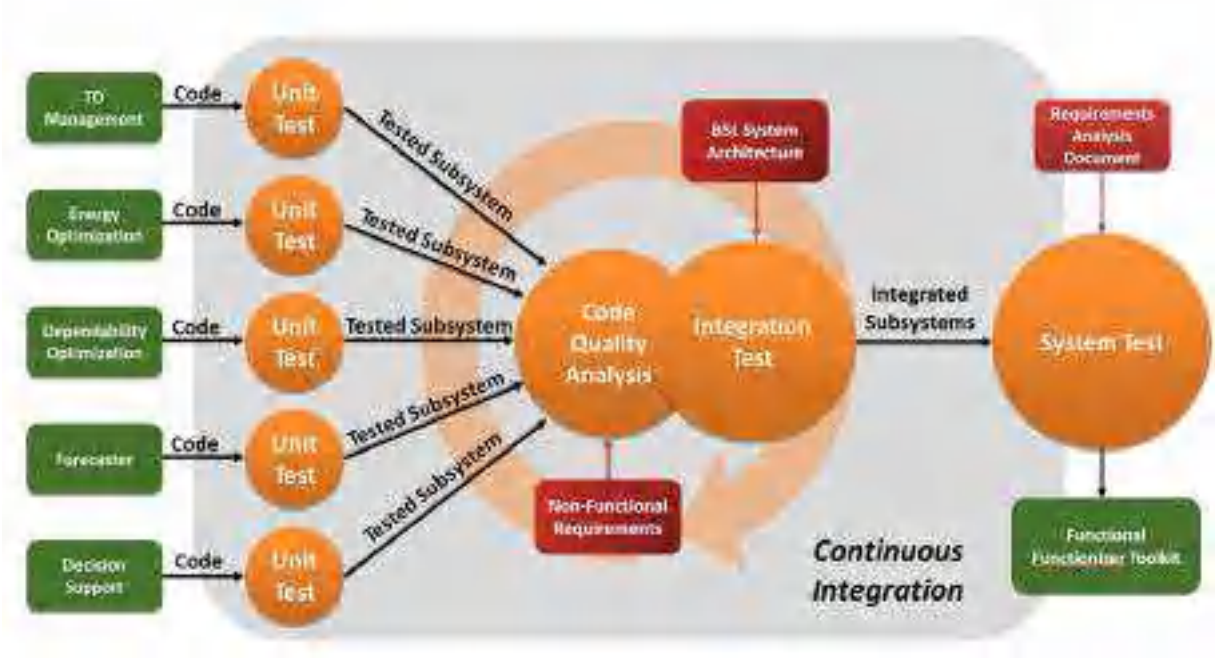

Figura 1 Prezentare generală a procesului de testare Functionizer

O imagine de ansamblu asupra procesului de testare Functionizer este ilustrată în Figura 1. În special, Functionizer va utiliza integrarea continuă pentru a automatiza executarea scripturilor de testare a unității și a integrării incluse ca parte a setului de instrumente iar toate API-urile principale ale modulelor sunt integrate (adică Gestionează TD, Gestionează fiabilitatea, Gestionează consumul de energie, Forecaster și Modulul de asistență pentru decizii). Aceste scripturi efectuează inițial o serie de teste unitare pentru a afirma buna funcționare a fiecărui modul și pentru a se asigura că API-urile funcționează conform așteptărilor. În timpul rulării, ele invocă o serie de componente de testare, fiecare izolată de celelalte, pentru a se asigura că fiecare resursă sau element final funcționează exact așa cum este specificat și documentat. De îndată ce testele unitare au succes, urmează testul de integrare. Toate unitățile individuale (adică module) sunt combinate în conformitate cu abordarea de integrare descrisă mai sus și testate ca un grup pentru a expune defecțiuni în interacțiunea dintre unitățile integrate, reducând în același timp riscul de noi actualizări care provoacă efecte secundare neașteptate.

Unul dintre cele mai utilizate instrumente pentru integrare continuă este Jenkins. Jenkins este utilizat pentru a construi și testa proiecte software în mod continuu, permițând dezvoltatorilor să integreze cu ușurință modificările proiectelor lor, indiferent de platforma pe care lucrează. Poate fi integrat cu o serie de tehnologii de testare și dezvoltare și este complet configurabil prin intermediul interfeței sale web prietenoase. Cazurile de utilizare tipice ale

Jenkins implică crearea unei aplicații dintr-un sistem de control al versiunilor și rularea unei serii de teste automate. Pe de altă parte, prin utilizarea Jenkins se poate realiza testarea imediată a ultimelor modificări, iar dezvoltatorii pot obține feedback imediat cu privire la funcționalitatea codului scris. În cazul în care apare o eroare, codul poate fi readus cu ușurință într-o stare fără erori, fără a pierde prea mult timp pentru depanare.

Activând Jenkins în Functionizer, executarea testelor va fi declanșată automat de fiecare dată când o modificare a codului este împinsă în managerul de depozitare Git bazat pe web (de exemplu, GitHub, GitLab etc.). De îndată ce execuția testelor este finalizată, pot fi afișate câteva informații utile, cum ar fi numărul de teste care au fost executate, cât a durat executarea și detaliile unui eșec al testului. Cu Jenkins, testarea automată a detaliilor unei anumite defecțiuni poate fi accesată cu ușurință doar făcând clic pe linkul corespunzător. Mai mult, membrii echipei care vor trebui să știe când au fost finalizate testele împreună cu rezultatele corespunzătoare ale testelor pot fi anunțați prin intermediul asistenței Jenkins pentru notificări prin e-mail.

6. Testarea sistemului

6.1 Scop

Acest capitol vizează definirea și descrierea procesului general de testare a sistemului care este adoptat în cadrul Functionizer, pe baza selectării unei abordări de testare a sistemului și a utilizării parțiale a mediilor de colaborare și a instrumentelor de integrare continuă care să o susțină.

6.2 Domeniul de aplicare

Testarea sistemului este al treilea nivel de testare efectuat după testarea integrării și înainte de testarea acceptării. În timpul testării sistemului, software-ul complet și integrat este testat pentru a verifica dacă cerințele funcționale sunt implementate corect.

6.3 Abordare

Cea mai utilizată abordare pentru testarea sistemului este testarea cutiei negre, cunoscută și sub numele de testare comportamentală. Testarea cutiei negre este o metodă de testare software în care testatorul nu cunoaște structura internă / proiectarea / implementarea elementului testat. Aceste teste pot fi funcționale sau nefuncționale, deși de obicei funcționale.

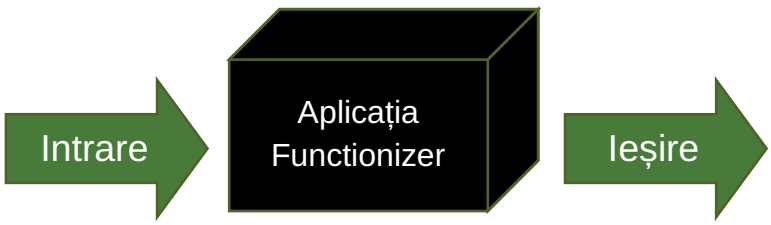

Figura 2 Testarea cutiei negre

Această metodă este denumită astfel deoarece programul software, în ochii testerului, este ca o cutie neagră; în interiorul căruia nu se poate vedea. Această metodă încearcă să găsească erori în următoarele categorii:

- Funcții incorecte sau lipsă
- Erori de interfață
- Erori în structurile de date sau accesul la baza de date externă
- Comportament sau erori de performanță
- Erori de inițializare și de terminare

Următoarele sunt câteva tehnici care pot fi utilizate pentru proiectarea testelor cutiei negre.

- Partiționare echivalentă: este o tehnică de proiectare a testului software care implică împărțirea valorilor de intrare în partiții valide și nevalide și selectarea valorilor reprezentative din fiecare partiție ca date de testare.
- Analiza valorii limită: este o tehnică de proiectare a testului software care implică determinarea limitelor pentru valorile de intrare și selectarea valorilor care se află la limite și chiar în interiorul / în afara limitelor ca date de testare.
- Graficarea cauzei-efect: este o tehnică de proiectare a testului software care implică identificarea cazurilor (condiții de intrare) și a efectelor (condiții de ieșire), producerea unui grafic cauză-efect și generarea cazurilor de testare în consecință.

7. Testare nefuncțională

7.1 Scop

Scopul testării nefuncționale este de a prelua valori din codul sursă vizat, care oferă o măsură pentru a indica mentenabilitatea, fiabilitatea, compatibilitatea, securitatea și, o oarecare, extindere a adecvării funcționale și a eficienței performanței.

7.2 Domeniul de aplicare

Accentul este pus pe calitatea codului spre deosebire de calitatea cerințelor sau arhitectura. De asemenea, după descrierea valorilor, sunt furnizați indicatori pentru efortul de îmbunătățire a software-ului și sunt descrise și relațiile dintre valori.

7.3 Fiabilitate și securitate

7.3.1 Acoperirea codului

Pentru a testa funcționalitatea codului sursă, este important ca dezvoltatorii să scrie teste unitare și să se asigure că aceste teste sunt aplicate prin scripturi automate pentru a detecta regresii cât mai curând posibil. Maturitatea testelor unitare poate fi măsurată cu ajutorul „statement coverage” și „branch coverage”.

Aceste valori indică procentul de linii de cod testate și respectiv procentul de ramuri testate în software. Dacă acoperirea testului este redusă, atunci fie unele părți ale codului nu sunt testate deloc, fie unele părți ale codului nu sunt deloc accesibile. TQI ia media dintre „statement coverage” și „branch coverage”.

7.3.2 Interpretare abstractă

Interpretarea abstractă, cunoscută și sub denumirea de „analiza fluxului profund”, este o tehnologie destul de nouă, capabilă să găsească tot felul de erori fatale în software fără a-l

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

rula efectiv. Acest lucru se face prin inspectarea tuturor căilor de execuție posibile prin cod. În acest fel pot fi găsite probleme precum „dereferențele indicatorului nul”, „matricea în afara limitelor”, „împărțirea la zero”, „scurgeri de memorie” și „scurgeri de resurse” (de exemplu, o conexiune la bază de date este deschisă, dar niciodată închisă pentru o anumită cale de execuție). Prin urmare, interpretarea abstractă va acoperi și unele aspecte legate de securitate.
Încălcările detectate ale acestui tip de erori fatale sunt ponderate în funcție de importanța și cantitatea lor. Rezultatul eventual este mapat pe o scară între 0 și 100 în conformitate cu o metodă descrisă în (Steneker2016) . Acesta se numește „factorul de conformitate” sau pe scurt „conformitatea”.

7.3.3 Avertismente ale compilatorului

Majoritatea programelor software trebuie să fie compilatoare înainte de a putea fi executate. Un compilator emite atât erori de compilare, cât și avertismente ale compilatorului în timpul acestui proces. Dacă există erori de compilare într-un program, acesta nu poate fi executat. Pe de altă parte, avertismentele compilatorului nu sunt fatale, dar sunt o indicație importantă dacă există încă probleme importante în software.

Avertismentele compilatorului sunt evaluate în TQI în același mod ca și interpretarea abstractă. Numărul de apariții este luat în considerare împreună cu importanța unui avertisment al compilatorului. Aceasta este conformitatea de avertizare a compilatorului. Rezultatele sunt mapate pe o scară între 0 și 100 în conformitate cu o metodă descrisă în (Steneker2016).

7.4 Testabilitate

7.4.1 Complexitatea ciclomatică

Complexitatea ciclomatică a unei funcții calculează numărul de căi de execuție liniare-independente ale unei funcții așa cum este definită de McCabe [McCabe94]. Aceste valori sunt utilizate pentru a măsura complexitatea codului și testabilitatea unui sistem software. De obicei, se măsoară complexitatea ciclomatică medie a tuturor funcțiilor. O complexitate medie ciclomatică mai mică de 3 este considerată, în general, ca fiind foarte bună.

7.4.2 Modularitate

Modularitatea unui sistem la nivel de cod este măsurată prin calcularea numărului de dependențe externe per modul, acesta fiind numit și „fan out”. În cazul în care numărul mediu de dependențe pe modul este ridicat, devine greu de înțeles sistemul software și de a-l testa izolat. Mai mult, șansele de a reutiliza părți ale sistemului sunt scăzute într-un astfel de caz.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

7.5 Mentenabilitate

7.5.1 Standarde de codare

TIOBE definește și menține standardele de codare pentru diferite limbaje de programare pentru clienții săi. Aceste standarde constau din reguli general acceptate la care dezvoltatorii ar trebui să adere pentru a preveni erorile și problemele de întreținere.

Valoarea standard de codare TQI este calculată într-un mod similar, așa cum se face pentru metricele „avertismente ale compilatorului” și „interpretarea abstractă”. Pe lângă numărul de încălcări ale standardului, se ia în considerare și gravitatea încălcărilor și dimensiunea sistemului. Rezultatele calculate sunt mapate pe o scară de la 0 la 100 în conformitate cu metoda descrisă în (Steneker2016). Valoarea TQI a acestui factor de conformitate pentru standardele de codare este după cum urmează.

7.5.2 Duplicarea codului

Dacă un sistem software conține o mulțime de coduri similare în diferite locații, atunci acest lucru ar putea influența mentenabilitatea sistemului. Să presupunem că un bug a fost remediat într-o astfel de bucată de cod, atunci există șansa ca bug-ul să nu fie remediat la una dintre locațiile codului duplicat. Codul duplicat are următorul scor TQI. Duplicarea măsurată prin identificarea a 100 de jetoane identice consecutive fără a lua în considerare comentariile și aspectul.

7.5.3 Cod mort

Codul mort într-un sistem software este o risipă inutilă. Costă efort de întreținere. În ciuda faptului că această valoare contează doar pentru o parte foarte mică din calitatea totală a codului, este un bun indiciu al ordonării sistemului.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

7.6 Relații metrice

Pentru a îmbunătăți o anumită valoare, trebuie să depuneți eforturi în activitățile de inginerie software, care vizează această îmbunătățire. Cât de mult efort va costa, nu poate fi descris exact. Ceea ce poate fi descris, totuși, este compararea efortului de a îmbunătăți o anumită valoare. Dacă luăm în considerare influența metricelor unul asupra celuilalt, se poate aplica planificarea strategică.

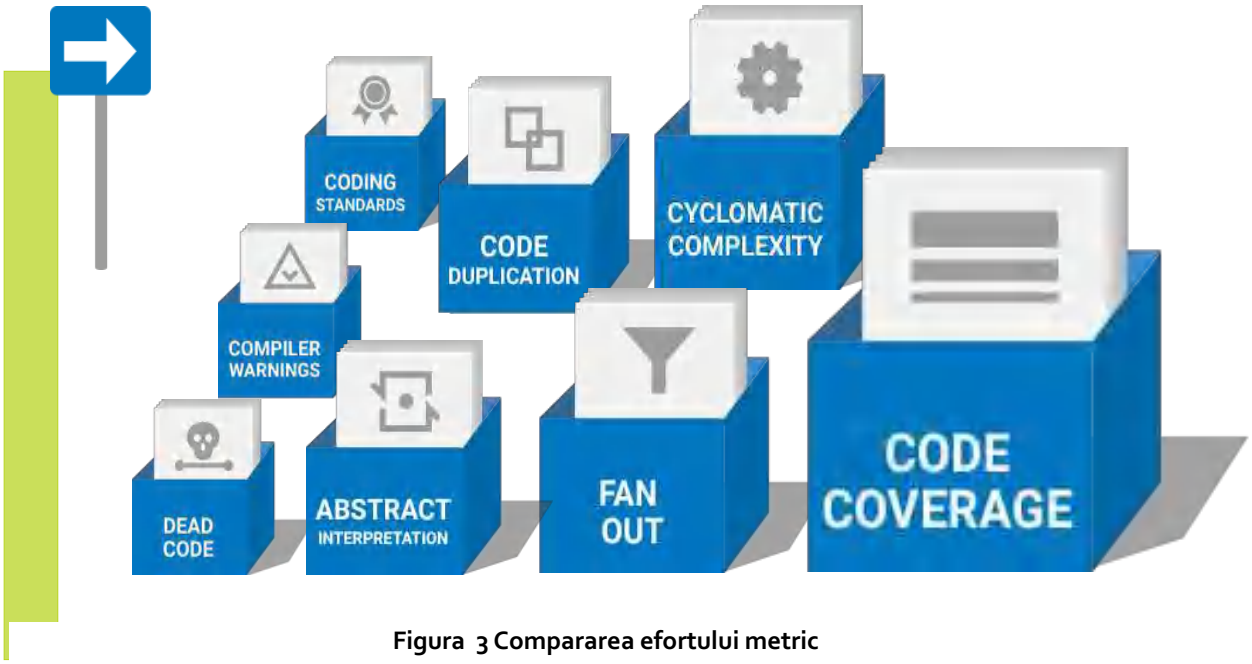

Figura 3 Compararea efortului metric

Imaginea de mai sus indică efortul de a îmbunătăți o valoare. Cu cât este mai mare cutia, cu atât va costa mai mult efort pentru a îmbunătăți acea valoare particulară. Figura 3 arată relația dintre valori. De acolo, schema de prioritizare poate fi recuperată.

8. Integrare continuă

8.1 Scop

Integrarea continuă se reduce la practica în care dezvoltatorii își îmbină sursele într-un depozit de coduri. Un sistem de asamblare construiește apoi sursele și cadrele de testare, și își execută testele disponibile. Efectuarea manuală a acestor pași este laborioasă și greoaie. Cu toate acestea, prin automatizarea acestui proces, devine foarte puternic, deoarece rezultatele de construcție și testare sunt disponibile rapid și sunt create în mod constant.

8.2 Practica obișnuită

Primul pas este menținerea unui depozit comun. Fiecare componentă a Functionizer va avea propriul său substituent în depozit, unde fiecare dezvoltator își poate aloca sursele sau așa-numitele artefacte. Acest lucru este necesar, astfel încât un instrument de integrare continuă (CI) poate prelua aceste surse pentru a le furniza unui sistem de construire.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Figura 4 Prezentare generală a procesului de testare Functionizer

Al doilea pas este de a avea unul sau mai multe sisteme de construire, unul pentru fiecare componentă. Aceste sisteme de construcție vor fi furnizate cu sursele, preluate din depozit de către CI. Construirea va fi invocată și de CI. Apoi, CI poate verifica, analizând eroarea standard sau eroarea standard, dacă versiunea a reușit sau nu.

În cele din urmă, al treilea pas este utilizat pentru a conecta cadre de testare și calitate. CI va invoca cadrele configurate, astfel încât fiecare cadru să își poată îndeplini datoria. CI poate colecta, de asemenea, rezultatele din aceste cadre în scopuri de prezentare și raportare.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

9. Metodologia de validare

Această secțiune prezintă metodologia de validare, care va asigura că modelul cazului de afaceri este adecvat pentru testarea platformei FUNCTIONIZER pe baza cerințelor generale definite de 7bulls.

Fluxul de validare

Validarea modelului software urmează fluxul descris în Figura 5.

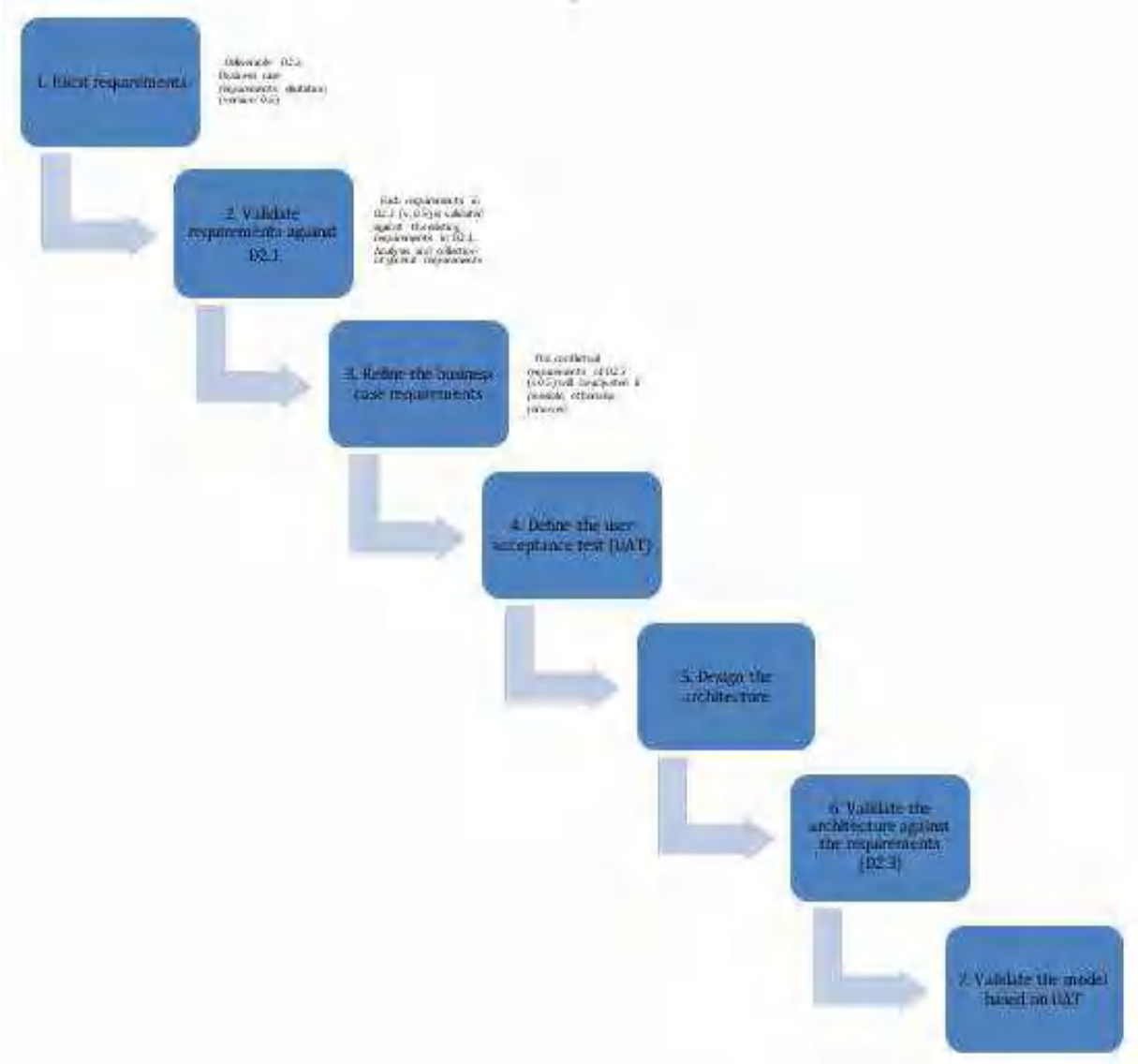

Figura 5 Metodologia de validare

9.1 Definirea cerințelor

Cerințele cazului de afaceri (BC) sunt eliberate de la 7bulls. Versiunile finale ale cerințelor, specificațiilor și cadrului Functionizer fac obiectul sarcinilor WP2 în care sunt specificate definițiile problemei companiei 7bulls.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

9.2. Validarea cerințelor

Cerințele BC sunt validate în funcție de cerințele funcționale și nefuncționale ale platformei Functionizer, subiectul sarcinii *D2.1 Definirea și analiza cerințelor generale*. Pe baza acestei validări, apar trei cazuri:

- Cerințele BC sunt valabile;
- Cerințele BC sunt în afara scopului proiectului;
- Cerințele BC sunt în conflict cu cerințele generale.

9.3. Rafinarea cerințelor BC

Cerințele BC sunt tratate în funcție de tipul lor, așa cum se arată în **Error! Reference source not found.**Tabel 6.

Tabel 6 Rafinarea cerințelor BC

Tipul cerinței BC	Rafinament
Cerință valabilă	-
În afara domeniului de aplicare	Acceptat ca atare
Cerință conflictuală	a) Dacă este posibil, reglați pentru a se potrivi cerințelor generale b) În caz contrar, scoateți-l

Ori de câte ori este descoperită o cerință conflictuală, aceasta trebuie atenuată fie prin adaptarea acesteia la cerințele generale, fie prin eliminarea acesteia. Ambele cazuri, proprietarul acesteia este informat și ea este cea care decide măsurile adecvate de atenuare.

9.4. Definirea testelor de acceptare a utilizatorului (UAT)

Testarea acceptării utilizatorului (UAT) constă într-un proces de verificare a faptului că o soluție funcționează pentru utilizatorul care proiectează arhitectura (Hambling, 2013).

9.5. Validarea arhitecturii în funcție de cerințe

Este disponibilă o suită de trei metode, toate dezvoltate la Institutul de Inginerie Software, și anume:

- Procesul ATAM (Architecture Tradeoff Analysis Method) constă în adunarea părților interesate pentru a analiza factorii de afaceri (funcționalitatea sistemului, obiectivele, constrângerile, proprietățile nefuncționale dorite) și din acești factori extrag atribute de

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

calitate care sunt utilizate pentru a crea scenarii. Aceste scenarii sunt apoi utilizate împreună cu abordările arhitecturale și deciziile arhitecturale pentru a crea o analiză a compromisurilor, a punctelor de sensibilitate și a riscurilor (sau non-riscurilor). Această analiză poate fi convertită în teme de risc și impactul acestora, după care procesul poate fi repetat. Cu fiecare ciclu de analiză, procesul de analiză continuă de la mai general la mai specific, examinând întrebările care au fost descoperite în ciclul anterior, până când arhitectura a fost reglată și temele de risc au fost abordate (Kazman , 1998).

- SAAM (Software Architecture Analysis Method): este o metodă utilizată în arhitectura software pentru a evalua o arhitectură de sistem. A fost prima metodă de analiză a arhitecturii software documentată și a fost dezvoltată la mijlocul anilor 1990 pentru a analiza un sistem de modificabilitate, dar este util pentru testarea oricărui aspect nefuncțional (Dobrica, 2002).
- ARID (Active Reviews for Intermediate Designs) este o metodă de evaluare a arhitecturilor software care combină aspecte din metoda de analiză a arhitecturii (ATAM) și metoda de analiză a arhitecturii software (SAAM) într-un nivel mai tactic (Clements, 2000).

9.6. Validarea modelul pe baza UAT

Criteriile testului de acceptare a utilizatorului (UAT) (în dezvoltarea software-ului agil) sunt de obicei create de clienți de afaceri și exprimate într-un limbaj de domeniu de afaceri (Cimperman, 2006). Acestea sunt teste la nivel înalt pentru a verifica exhaustivitatea unei povești de utilizator sau a unor povești „redate” în timpul oricărui sprint / iterație.

10. Metodologia de testare

10.1. Analiza codului

Metodologia de testare include un pas numit Analiza codului, un pas important pentru a limita creșterea datoriei tehnice. Importanța acestui pas este fundamentală, deoarece inginerii se concentrează de obicei pe optimizările de cod din punct de vedere al eficienței, și nu din cel de întreținere. Aceasta înseamnă că, în viitor, codul tinde să fie dezorganizat, greu de înțeles și de înțeles, greu de depanat și reparat. Platforma Functionizer, dezvoltată în platforma software Functionizer (în care HOLISUN este partener), oferă exact acest tip de analiză și sugestii pentru o bază de cod mai bună. O altă piesă software utilizată în acest domeniu este SonarQube.

În primul rând, am explorat analiza evoluției și caracteristica de evaluare TD a setului de instrumente TD. Evoluția datoriei tehnice de-a lungul versiunilor software-ului este prezentată în Figura 9. Aspectele TD care sunt surprinse și pe care le-am monitorizat sunt: dobânda (EUR), principalul (EUR) punctul de rupere și dobânda cumulată (EUR)). Sumele sunt exprimate în EUR, ca o estimare a **costului de timp * pe unitate de timp** care ar necesita eliminarea completă a TD. Deci, aceasta înseamnă pierderea efectivă a proiectului.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

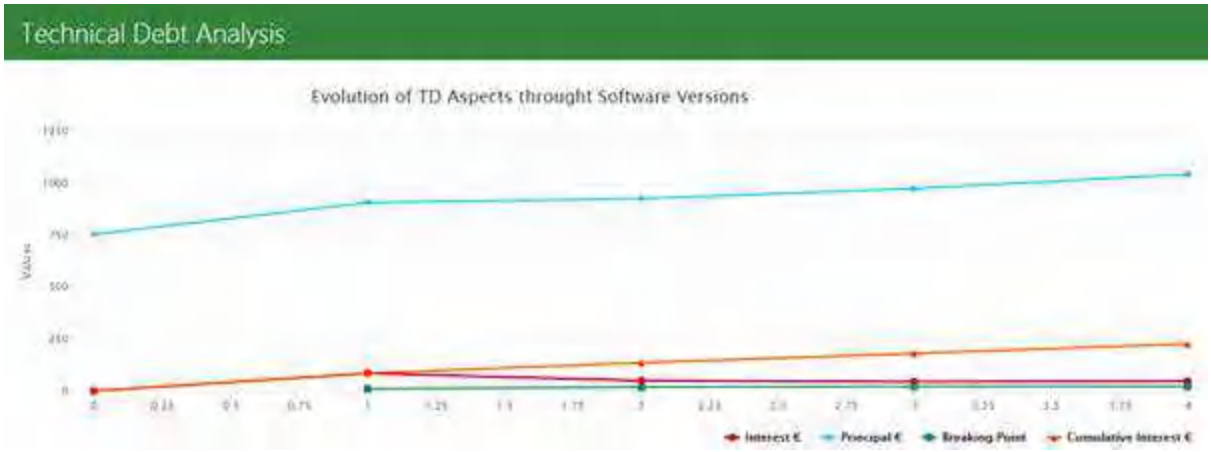

Figura 6 Evoluția TD pe parcursul versiunilor

După cum se poate vedea în Figura 6, TD crește orele suplimentare (atât principalul, cât și dobânda cumulată), cu toate acestea dobânda (linia roșie) merge în jos. Se așteaptă creșterea continuă a principalului TD și dobânda cumulată, deoarece baza de cod a aplicației devine din ce în ce mai mare. Pe partea pozitivă, interesul scăzut sugerează ca echipa de dezvoltare să mențină costurile de întreținere la niveluri bune, asigurând sustenabilitatea sistemului. Rezumatul proiectului în ceea ce privește TD (Figura 7), arată că:

- Principalul TD însumează până la 1364 minute (adică 22,73 ore) sau 909,33 EUR. Acest lucru va crește în timp dacă nu se iau măsuri. TD este foarte evident atunci când trebuie întreprinse acțiuni rapide pentru menținerea software-ului la fața locului, sub presiunea timpului.
- În cod existau 13 vulnerabilități potențiale, au fost identificate 191 mirosuri de cod și 30 de duplicări; cu toate acestea, nu au fost observate erori în timpul analizei.

Figura 7 Rezumatul TD în ceea ce privește platforma Functionizer

Rezumatul proiectului în termeni de interes TD (Figura 8) arată că:

- Punctul de rupere va fi atins la versiunea 22 a software-ului. Aceasta înseamnă că, având în vedere condițiile actuale, în versiunea 22, dobânda cumulată va fi mai mare decât principalul corespunzător. Cu toate acestea, deoarece proiectul se află în prezent în versiunea 4 (pe baza analizei), punctul de rupere se află cu mult în viitor. Cu toate acestea, practicile de monitorizare continuă privind controlul calității trebuie menținute la niveluri ridicate

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

- Dobânda totală este de 46,74 EUR cu o probabilitate de 13,89%. Acest lucru înseamnă că nu se rezumă prea multe dobânzi, iar stabilirea datoriei tehnice nu ar trebui să fie de mare prioritate în companie; cu toate acestea, trebuie luate măsuri înainte ca suma să crească prea mult (de exemplu, un salariu lunar);

Figura 8 Rezumatul proiectului de interes

În cele din urmă, o analiză detaliată a artefactelor, așa cum se arată în Figura 9, sugerează că pot fi evidențiate hotspoturi de proiectare în baza de cod, cum ar fi clasa ConferenceActivity, care concentrează sume mari de dobândă și se modifică destul de frecvent.

Figura 9 Analiza interesului pe clasă

Trecând evaluarea noastră la mecanismele de reducere a TD, am reușit să obținem indicații asupra unor părți ale codului, unde am putea aplica refactorizarea (cum ar fi divizarea metodei

lungi sau mutarea claselor între pachete) sau indicii pentru încălcările obișnuite ale calității, așa cum este prezentat în Figura. 10.

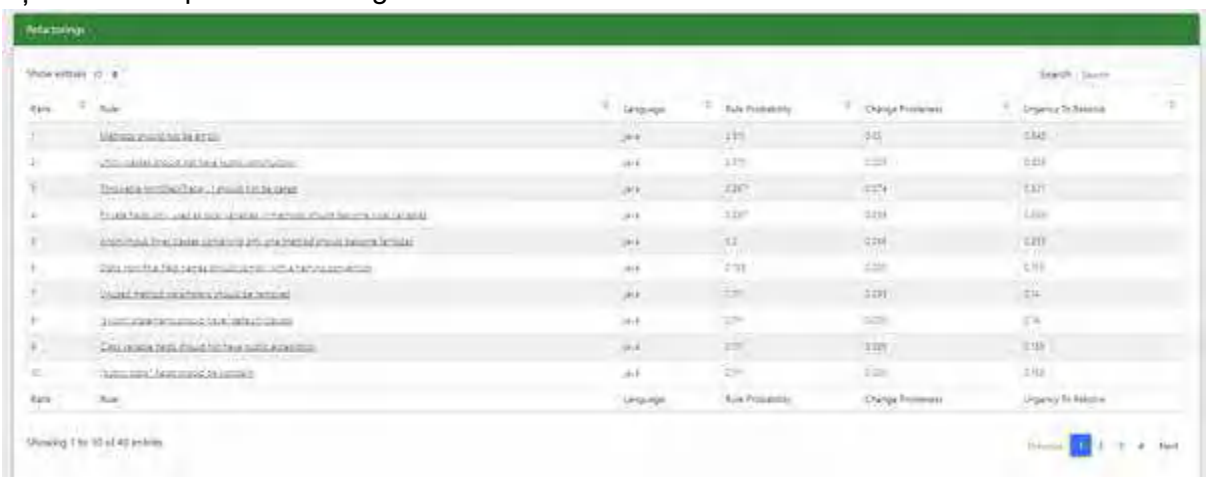

Figura 10 Regulile frecvent încălcate

10.2 Setul de instrumente pentru fiabilitate

Fiabilitatea este evaluată în ceea ce privește securitatea și punctul de control optim.

10.2.1 Securitate

Indicele de securitate al codului sursă al cazului de utilizare auto este de 72% (adică 4 stele din 5). Valoarea se datorează faptului că aplicația este în stadii incipiente, tehnologia nu este încă matură și se schimbă foarte des. Obiectivul nostru este să fie peste 75%, de preferință peste 85%, prin urmare codul este refactorizat având în vedere problemele de securitate raportate de instrument.

Figura 11 Indicele de securitate

Scorurile caracteristicilor, care se referă la confidențialitate, disponibilitate și integritate (Figura 12) sunt:

- **Măsurile de confidențialitate** (0.8) protejează informațiile împotriva accesului neautorizat și a utilizării necorespunzătoare. Majoritatea sistemelor informaționale găzduiesc informații care au un anumit grad de sensibilitate. Ar putea fi informații comerciale proprietare pe care concurenții le-ar putea folosi în avantajul lor sau informații personale cu privire la angajații, clienții sau clienții unei organizații. Acest lucru este peste standardul industriei.

- **Măsurile de disponibilitate** (0.7) protejează accesul la timp și neîntrerupt la sistem. Unele dintre cele mai fundamentale amenințări la adresa disponibilității sunt de natură

non-rău intenționată și includ eșecuri hardware, timp de nefuncționare neprogramat al software-ului și probleme cu lățimea de bandă a rețelei. Atacurile rău intenționate includ diverse forme de sabotaj menite să provoace daune unei organizații prin refuzarea accesului utilizatorilor la sistemul de informații.

- **Măsurile de integritate** (0,7) protejează informațiile împotriva modificărilor neautorizate. Aceste măsuri oferă asigurarea exactității și exhaustivității datelor. Necesitatea protejării informațiilor include atât datele stocate pe sisteme, cât și datele transmise între sisteme, cum ar fi e-mailul. În menținerea integrității, nu este necesar doar să se controleze accesul la nivel de sistem, ci să se asigure în continuare că utilizatorii sistemului pot modifica doar informațiile pe care sunt legitimați să le modifice.

În aplicații similare, confidențialitatea, disponibilitatea și integritatea sunt, în general, acceptate la 75%, ceea ce înseamnă că, în cazul nostru specific, confidențialitatea este bună, dar trebuie să se lucreze la disponibilitate și integritate.

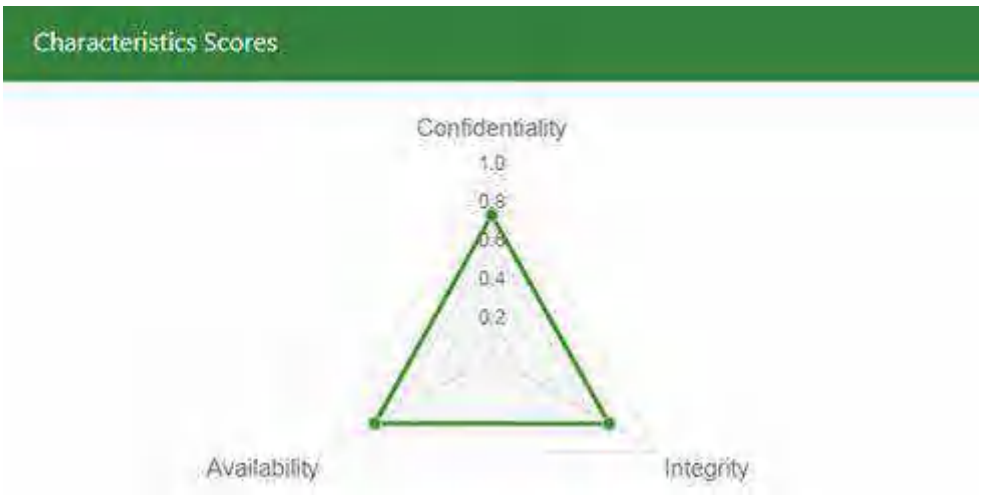

Figura 12 Scoruri caracteristice

Scorurile proprietăților (Figura 13) sunt rezumate în Tabelul 7. Scorurile proprietăților se referă la instrucțiuni sensibile care se ocupă de excepții, memorie sau alte resurse:

Tabel 7 Scorul proprietăților

Proprietate	Scorul	Aparențe
Manipularea resurselor	80%	385
Misiune	85%	447
Manevrarea excepțiilor	80%	14

Funcționalitate utilizată greșit	72%	86
Sincronizare	20%	16
Indicator nul	85%	6
Complexitate	82%	N/A
Coeziune	88%	N/A
Cuplare	50%	N/A
Incapsularea	90%	N/A

Resursele sunt gestionate în 385 de cazuri, există 447 de sarcini și 14 gestionări de excepție. Instrumentul a identificat 86 de funcționalități folosite greșit, 16 sincronizări și 6 posibile pointeri nuli. Coeziunea este o măsură a complexității unei singure unități de program, iar cuplarea este o măsură a complexității relațiilor sau legăturilor dintre unitățile de program. Cifrele arată că lucrările sunt în desfășurare și se îmbunătățesc. Cu toate acestea, toate aceste probleme trebuie tratate cu atenție.

Figura 13 Scorul proprietăților

Harta de căldură de predicție a vulnerabilității (vezi Figura 14) variază clasele de la 0 la 1, cu toate acestea, media este de aproximativ 0,5. Un hotspot de securitate evidențiază o bucată

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

de cod sensibilă la securitate pe care dezvoltatorul trebuie să o revizuiască. După examinare, veți găsi fie că nu există nici o amenințare sau trebuie să aplicați o soluție pentru a securiza codul. Clasele cu nivel zero înseamnă că nu are vulnerabilități de securitate detectate, în timp ce clasele cu nivelul 1 sunt foarte vulnerabile și trebuie reproiectate și rescrise imediat.

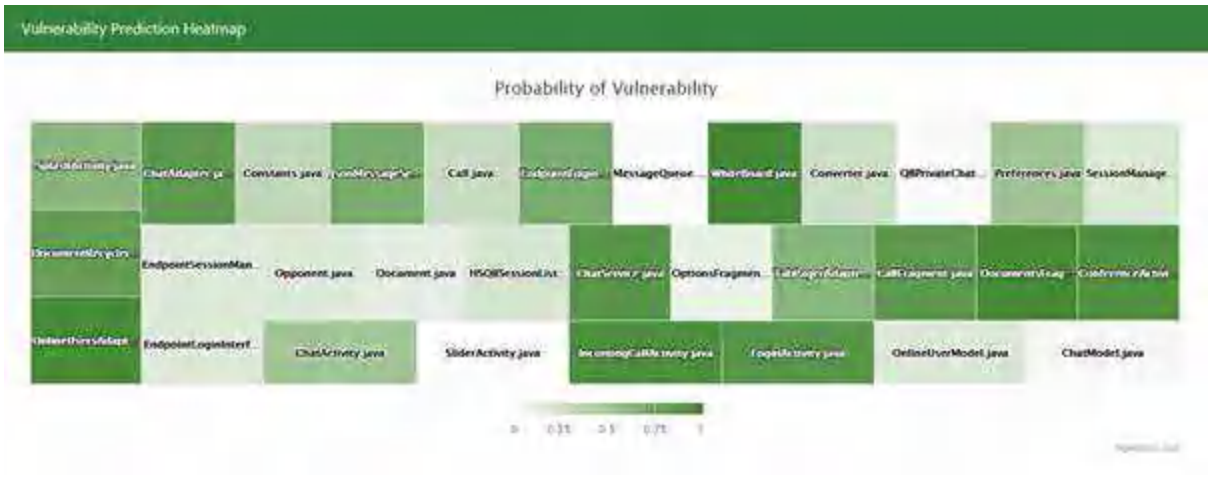

Figura 14 Harta termică de predicție a vulnerabilității

Rezultatele predicției vulnerabilității arată 31 de intrări (a se vedea Figura 15). O vulnerabilitate este un punct din cod care este deschis atacului. Dacă probabilitatea de vulnerabilitate este peste 0,5, clasa este considerată vulnerabilă. Clasele de risc sunt cele care se ocupă de comunicarea între punctele finale, respectiv cele care gestionează interacțiunile utilizatorului. Au fost luate măsuri pentru monitorizarea vulnerabilităților, cum ar fi: validarea datelor și resurselor utilizatorilor, respectiv securizarea comunicării.

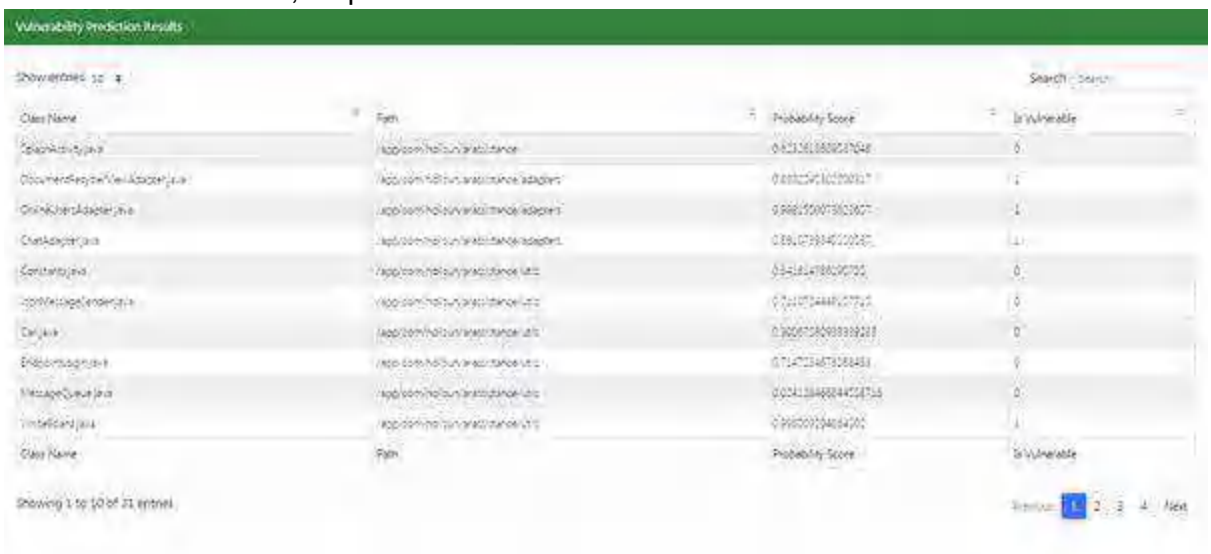

Figura 15 Rezultatul prezicerii vulnerabilității

10.2.2 Punct de control optim

Punctele de control sunt utilizate pentru a asigura fiabilitatea executării programelor. Considerăm consumul de energie pentru execuția programului, în plus față de durata de funcționare a acestuia, drept criterii care trebuie utilizate pentru a minimiza costul general datorat punctelor de control. Sunt derivate expresii noi atât pentru timpul de rulare al programului, cât și pentru consumul de energie corespunzător, care includ probabilitatea de

eșec pe fiecare execuție a instrucțiunilor și cheltuielile generale suportate pentru fiecare punct de control. Figura 16 arată numărul minim de instrucțiuni între punctele de control este 1999. Timpul de execuție crește foarte lent. Aceasta înseamnă că punctele de control pot fi setate la un număr mai mare de instrucțiuni (timpi de execuție).

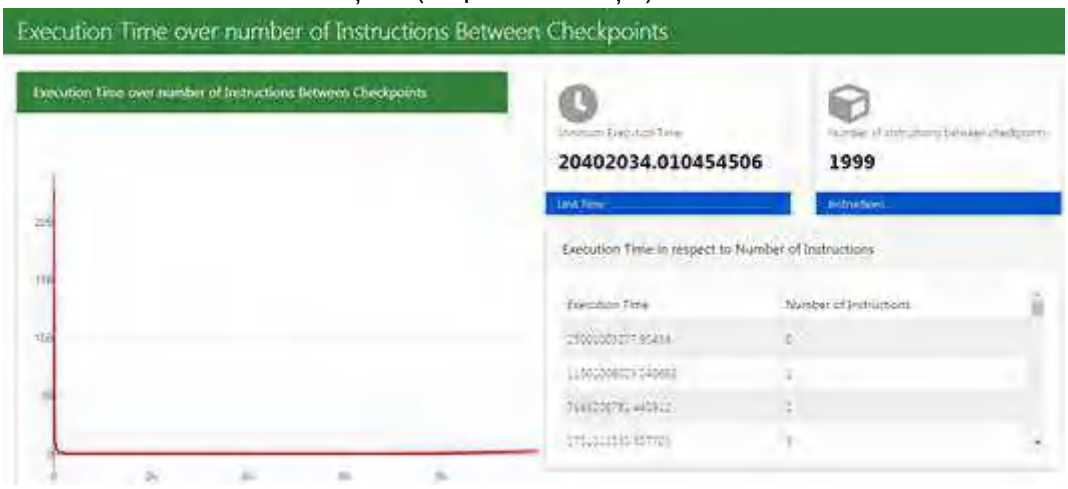

Figura 16 Timpul de execuție peste numărul de instrucțiuni între punctele de control

Figura 17 arată că consumul de energie crește foarte abrupt. Consumul minim este 225200.354, iar numărul de instrucțiuni între punctele de control este de 42. Aceasta înseamnă că fiecare instrucțiune este critică pentru consumul de energie. Am luat decizia de a reduce numărul de instrucțiuni și de a le limita la cele esențiale (de exemplu, eliminați verificările inutile, scrieți un cod de nivel inferior, reduceți utilizarea funcțiilor încorporate și rescrieți-le).

Figura 17 Consumul de energie peste numărul de instrucțiuni între punctele de control

10.2.3 Analiza rezultatelor

Pe baza configurării de mai sus, platforma Functionizer, dezvoltată de Holisun, a fost analizată în Cutia de instrumente Functionizer. Au fost adunate următoarele date:

- Utilizarea memoriei (octeți)
- Încărcare CPU (procent)
- Frecvența procesorului (Hertz)
- Comutatoare de context (număr)
- Durata cazului de testare (secunde)

• Apeluri de sistem (număr)
• Energie totală (Millijoules)

Setul complet al acestor puncte de date este suficient pentru a caracteriza software-ul executat în ceea ce privește eficiența energetică a acestuia. Figura 18 prezintă măsurătorile exacte extrase.

Figura 18 Analiza energetică a platformei Functionizer

De asemenea, prezentăm datele sub formă de tabel, pentru o mai bună lizibilitate Tabelul 8. Unele observații notabile cu privire la rezultatele obținute sunt:

1. Încărcarea CPU este o medie a seriei temporale respective. Rețineți că aplicația nu a fost executată izolat total și, prin urmare, datele sunt supuse aliasării de către restul contextului platformei.
2. Împărțind energia totală cu timpul de execuție al testului, obținem o citire medie a puterii de 12,39 / 5,93 = ~ 2,1 W.
3. Cazul de testare nu a subliniat procesorul cu mai mult de 50% din capacitatea sa.

Tabel 8 Analiza energiei sub formă de tabel

Memorie (octeți)	Încarcare CPU (%)	Frecvența CPU (kHz)	Comutatoare de context (#)	Durata cazului de test (sec)	Apeluri sistem (#)	Energia Totală (Joules)
1733098	49.95	1374600	23604	5.93	278	12.39

După finalizarea cu succes a analizei codului, împreună cu ajustările necesare, am trecut la testarea efectivă a platformei, conform metodologiei.

10.3 Testare funcțională vs. nefuncțională

Scopul utilizării a numeroase metodologii de testare în procesul de dezvoltare este de a vă asigura că software-ul poate funcționa cu succes în medii multiple și pe diferite platforme. Acestea pot fi de obicei împărțite între testarea funcțională și cea nefuncțională. Testarea funcțională implică testarea aplicației în funcție de cerințele afacerii. Incorporează toate tipurile de testare concepute pentru a garanta că fiecare parte a unui software se comportă conform

așteptărilor prin utilizarea cazurilor de utilizare furnizate de echipa de proiectare, de analistul de afaceri sau, în cazul nostru, de furnizorul de cazuri de utilizare care este 7bulls.

Aceste metode de testare sunt de obicei realizate în ordine și includ:

- Testarea unității
- Testarea integrării
- Testarea sistemului
- Testarea acceptării

Metodele de testare nefuncționale încorporează toate tipurile de testare axate pe aspectele operaționale ale unui software. Acestea includ:

- Testarea performanței
- Testarea securității
- Testarea utilizabilității
- Testarea compatibilității

Cheia pentru lansarea unui software de înaltă calitate care poate fi adoptat cu ușurință de către utilizatorii finali este utilizarea unui cadru de testare robust care să implementeze atât metodologii de testare software funcționale, cât și nefuncționale.

➢ Testarea unității

Testarea unitară este primul nivel de testare și este adesea efectuată chiar de dezvoltatori. Este procesul de asigurare a componentelor individuale ale unui software la nivel de cod, funcționale și funcționale așa cum au fost concepute. Dezvoltatorii într-un mediu bazat pe test vor scrie și vor rula testele înainte ca software-ul sau caracteristica să fie transmise echipei de testare. Testarea unității poate fi efectuată manual, dar automatizarea procesului va accelera ciclurile de livrare și va extinde acoperirea testelor. Testarea unității va facilita, de asemenea, depanarea, deoarece găsirea problemelor mai devreme înseamnă că necesită mai puțin timp pentru a remedia decât dacă ar fi descoperite mai târziu în procesul de testare.

➢ Testarea integrării

După ce fiecare unitate este testată temeinic, este integrată cu alte unități pentru a crea module sau componente care sunt proiectate pentru a îndeplini sarcini sau activități specifice. Acestea sunt apoi testate ca grup prin teste de integrare pentru a se asigura că segmente întregi ale unei aplicații se comportă așa cum era de așteptat (de exemplu, interacțiunile dintre unități sunt perfecte). Aceste teste sunt adesea încadrate de scenarii de utilizator, cum ar fi logarea într-o aplicație sau deschiderea fișierelor. Testele integrate pot fi realizate fie de dezvoltatori, fie de testeri independenți și constau de obicei dintr-o combinație de teste funcționale și manuale automatizate.

➢ Testarea sistemului

Testarea sistemului este o metodă de testare a cutiei negre utilizată pentru a evalua sistemul completat și integrat, ca întreg, pentru a se asigura că îndeplinește cerințele specificate. Funcționalitatea software-ului este testată de la capăt la cap și este de obicei condusă de o echipă de testare separată decât echipa de dezvoltare înainte ca produsul să fie introdus în producție.

➢ Testarea acceptării

Testarea acceptării este ultima fază a testării funcționale și este utilizată pentru a evalua dacă platforma finală este sau nu gata pentru livrare. Aceasta implică asigurarea conformității produsului cu toate criteriile comerciale inițiale și cu satisfacerea nevoilor utilizatorului final. Acest lucru necesită ca produsul să fie testat atât intern, cât și extern, ceea ce înseamnă că

va trebui să îl puneți în mâinile utilizatorilor finali pentru testarea beta, împreună cu cei ai echipei dvs. QA. Testarea beta este esențială pentru a obține feedback real de la potențialii clienți și poate rezolva orice problemă finală de utilizare.

➢ Testarea performanței

Testarea performanței este o tehnică de testare nefuncțională utilizată pentru a determina cum se va comporta o aplicație în diferite condiții. Scopul este de a-i testa capacitatea de răspuns și stabilitatea în situații reale ale utilizatorilor. Testarea performanței poate fi împărțită în patru tipuri:

- **Testarea încărcării** este procesul de punere a unei cantități tot mai mari de cereri simulate pe platformă pentru a verifica dacă poate sau nu să facă față a ceea ce este conceput să facă față.
- **Testarea stresului** face acest lucru cu un pas mai departe și este utilizată pentru a evalua modul în care software-ul dvs. va răspunde la sau peste sarcina sa maximă. Scopul testării stresului este de a supraîncărca aplicația în mod intenționat până când se rupe, aplicând atât scenarii de încărcare realiste, cât și nerealiste. Cu testarea la stres, veți putea găsi punctul de eșec al software-ului dvs.
- **Testarea de anduranță**, cunoscută și sub numele de testare prin înmuiere, este utilizată pentru a analiza comportamentul unei aplicații sub o anumită cantitate de sarcină simulată pe perioade mai lungi de timp. Scopul este să înțelegeți cum se va comporta sistemul dvs. în condiții de utilizare susținută, făcându-l un proces mai lung decât testarea sarcinii sau a stresului (care sunt concepute să se încheie după câteva ore). Un test critic de rezistență este că ajută la descoperirea scurgerilor de memorie.
- **Testarea vârfurilor** este un tip de testare a sarcinii utilizat pentru a determina modul în care software-ul dvs. va răspunde la explozii substanțial mai mari de activități simultane ale utilizatorului sau ale sistemului în perioade diferite de timp. În mod ideal, acest lucru vă va ajuta să înțelegeți ce se va întâmpla atunci când sarcina va crește brusc și drastic.

➢ Testarea securității

Odată cu creșterea platformelor de testare bazate pe cloud și a atacurilor cibernetice, există o preocupare și o nevoie crescândă pentru securitatea datelor utilizate și stocate în software. Testarea securității este o tehnică de testare software nefuncțională utilizată pentru a determina dacă informațiile și datele dintr-un sistem sunt protejate. Scopul este de a găsi în mod intenționat lacune și riscuri de securitate în sistem care ar putea duce la accesul neautorizat la sau pierderea informațiilor prin sondarea aplicației pentru puncte slabe. Există mai multe tipuri ale acestei metode de testare, fiecare dintre acestea având ca scop verificarea a șase principii de bază ale securității:

- Integritate
- Confidențialitate
- Autentificare
- Autorizare
- Disponibilitate
- Non-respingere

➢ Testarea utilizabilității

Testarea utilizabilității este o metodă de testare care măsoară ușurința utilizării unei aplicații din perspectiva utilizatorului final și este adesea efectuată în timpul etapelor de testare a sistemului sau de acceptare. Scopul este de a determina dacă designul vizibil și estetica unei aplicații îndeplinesc sau nu fluxul de lucru prevăzut pentru diferite procese, cum ar fi

conectarea la o aplicație. Testarea utilizabilității este o modalitate excelentă pentru echipe de a revizui funcții separate sau sistemul în ansamblu este intuitiv de utilizat.

- Testarea compatibilității

Testarea compatibilității este utilizată pentru a evalua modul în care o aplicație sau o bucată de software va funcționa în diferite medii. Este folosit pentru a verifica dacă platforma și componentele sale sunt compatibile cu mai multe sisteme de operare, platforme, browsere sau configurații de rezoluție. Scopul este de a vă asigura că funcționalitatea software-ului dvs. este acceptată în mod constant în orice mediu pe care vă așteptați să îl utilizeze utilizatorii finali.

- Rezultatele testării
  - Testarea unității

Metoda standard de testare a unității, preferată în cadrul Holisun pentru orice proiect Java, este folosirea jUnit Framework. jUnit este un cadru open-source încorporat în majoritatea cadrelor Java și IDE-urilor (cum ar fi NetBeans). Pentru fiecare clasă a cadrului, există un test definit, cu scopul de a acoperi 100% cod și, dacă nu este posibil, cât mai aproape de 100%. Fiecare ramură este verificată cu atenție, codul este refractat astfel încât metodele de clasă să fie cât mai atomice posibil.

Testele unitare se execută manual la momentul proiectării, pentru a se asigura că atât testele, cât și codul de lucru se comportă conform așteptărilor. Sunt scrise mai multe teste pentru fiecare metodă, verificând cele mai multe valori și combinații posibile pentru parametrii metodei. După efectuarea testelor și dacă toate trec, clasa testată, împreună cu metodele sale, ar trebui să accepte doar tipul / tipurile variabile corecte și numai intervalul valoric corect pentru fiecare dintre ele. Sistemul ar trebui să accepte erori și excepții și ar trebui să trateze oricare dintre ele cu grație și corect.

De asemenea, trebuie înțeles că utilizatorii pot introduce date nevalide (fie din greșeală, fie ca parte a unui atac). În ceea ce privește această situație, toate datele ar trebui să fie validate și evadate corect de fiecare modul, chiar dacă utilizatorul nu introduce date direct în acel modul (lacunele pot apărea în orice modul, deci sistemul ar trebui să aibă mecanisme de siguranță pentru această situație). Acest lucru este acoperit și de testarea unitară.

- Testarea integrării

După finalizarea testării unitare și întregul sistem trece toate testele unitare, este timpul să testați sistemul (sau platforma în cazul nostru) ca întreg. Diferitele părți ale sistemului sunt testate în funcție de scenariile lor de utilizare (API vs acces Browser vs. acces local). O suită de valori este definită pentru toți parametrii necesari și toate funcțiile platformei sunt direcționate prin intermediul software-ului. Pentru această testare am folosit aplicația Open-Source Jenkins.

Jenkins este o platformă software de integrare continuă / implementare continuă (CI / CD), utilizată pentru automatizarea construcției corecte a întregii platforme software și, de asemenea, pentru a rula diferite cazuri de test pe software-ul construit cu succes, cazuri de testare care au fost definite anterior de echipa de testare . Jenkins este, de asemenea, capabil să publice rezultatele pe un server live (un server de stocare). Rezultatele testării sunt raportate înapoi echipei de dezvoltare, astfel încât problemele să poată fi rezolvate.

Similar cu jUnit, Jenkins folosește cazuri de testare definite de echipa de testare. Dar, spre deosebire de jUnit, Jenkins va fi aplicat pe întreaga platformă, concentrându-se pe colaborarea corectă a diferitelor module, schimbul corect de informații și, în cele din urmă, ieșirea corectă pentru diferite intrări.

Setarea implicită pentru Jenkins implică faptul că fluxul de lucru este declanșat de fiecare dată când există modificări ale codului. Jenkins scanează folderul GIT pentru noi confirmări, trasând modificările, construind și testând toate componentele cadrului, trecând astfel întregul cod prin conducta sa.

- Testarea sistemului

Odată ce întregul sistem trece toate testele și integrarea nu produce erori, echipa de testare trece prin unele teste manuale sau semi-automate ale sistemului. Diferite platforme software bazate pe Selenium sunt utilizate dacă partea testată a platformei are o componentă de afișare care necesită interacțiune cu mouse-ul sau tastatura.

Este definit un grafic de sistem și GraphWalker este utilizat, împreună cu cazurile de testare Selenium, pentru a simula toate rutele posibile pe care le-ar putea parcurge un utilizator atunci când folosește GUI, împreună cu stările aplicației. Testarea sistemului va scoate la iveală potențiale probleme ascunse, cum ar fi link-uri moarte, rutare incorectă sau probleme de interfață.

API-urile au fost testate cu o combinație de cod personalizat și aplicația gratuită Postman. Postman a permis echipei de testare să testeze și să depaneze manual funcțiile API. Aceste teste au fost limitate la etapele inițiale de dezvoltare, unde testarea rapidă este importantă, pentru a vedea dacă o funcție se comportă corect. Pentru teste mai aprofundate, jUnit a fost utilizat cu teste care au acoperit o gamă largă de valori posibile, precum și valori greșite, pentru a evalua corectitudinea acestor funcții.

Tabel 9 Verificare de securitate pentru asistență AR

➔ Toate componentele aplicației sunt identificate și cunoscute a fi necesare.	Da
➔ Facilitățile de stocare a credențialelor de sistem sunt utilizate în mod corespunzător pentru a stoca date sensibile, cum ar fi credențiale de utilizator sau chei criptografice.	Da
➔ Nu sunt scrise date sensibile în jurnalele de aplicații.	Da
➔ Nu sunt partajate date sensibile cu terți, cu excepția cazului în care este o parte necesară a arhitecturii.	Da
➔ Clipboard-ul este dezactivat pe câmpurile de text care pot conține date sensibile.	Da
➔ Nu sunt expuse date sensibile prin intermediul mecanismelor IPC.	Da

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

➔ Nu sunt expuse date sensibile, cum ar fi parolele sau pinii, prin interfața cu utilizatorul.	Da
➔ Nu sunt incluse date sensibile în copiile de rezervă generate de sistemul de operare mobil.	Da
➔ Aplicația elimină datele sensibile din vizualizări atunci când este în fundal.	Da
➔ Aplicația nu conține date sensibile în memorie mai mult decât este necesar, iar memoria este ștearsă explicit după utilizare.	Da
➔ Aplicația nu se bazează pe criptografie simetrică cu chei codificate ca o singură metodă de criptare.	Da
➔ Aplicația folosește implementări dovedite ale primitivelor criptografice.	Da
➔ Aplicația nu folosește protocoale criptografice sau algoritmi care sunt considerați pe scară largă depreciați din motive de securitate.	Da
➔ Toate valorile aleatoare sunt generate utilizând un generator de numere aleatorii suficient de sigur.	Da
➔ Datele sunt criptate în rețea folosind TLS (sau echivalente). Canalul securizat este utilizat în mod constant în toată aplicația.	Da
➔ Aplicația verifică certificatul X.509 al punctului final la distanță atunci când este stabilit canalul securizat. Sunt acceptate numai certificatele semnate de un CA de încredere.	Da
➔ Aplicația fie folosește propriul magazin de certificate, fie fixează certificatul de punct final sau cheia publică și ulterior nu stabilește conexiuni cu puncte finale care oferă un certificat sau o cheie diferită, chiar dacă este semnat de o autoritate de încredere	Da
➔ Aplicația solicită doar setul minim de permisiuni necesare.	Da

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

➔ WebViews sunt configurate pentru a permite doar setul minim de manipulare de protocol necesare (în mod ideal, doar https este acceptat). Handlerele potențial periculoase, cum ar fi fișierul, telul și aplicația-id, sunt dezactivate.	Vizualizările web nu sunt utilizate
➔ Codul de depanare a fost eliminat, iar aplicația nu înregistrează erori detaliate sau mesaje de depanare.	Da
➔ Toate componentele de terță parte utilizate de aplicația mobilă, cum ar fi bibliotecile și cadrele, sunt identificate și verificate pentru vulnerabilități cunoscute.	Da
➔ Aplicația prinde și gestionează posibile excepții.	Da
➔ Logica de gestionare a erorilor în controalele de securitate refuză accesul în mod implicit	Da
➔ Funcțiile de securitate gratuite oferite de lanțul de instrumente, cum ar fi minimizarea codurilor de octeți, protecția stivei, suportul PIE și numărarea automată a referințelor, sunt activate.	Da
➔ Aplicația previne depanarea și / sau detectează și răspunde la atașarea unui depanator. Toate protocoalele de depanare disponibile trebuie acoperite.	Da
➔ Toate fișierele și bibliotecile executabile care aparțin aplicației sunt fie criptate la nivel de fișier și / sau segmente importante de cod și date din interiorul executabilelor sunt criptate sau împachetate. Analiza statică banală nu dezvăluie codul sau date importante.	Da

Tabel 10 Verificări de securitate a bazei de date MySQL

➔ Securizați serverul care găzduiește instanța bazei de date MySQL	◆ Multe atacuri cunoscute sunt posibile numai după ce a fost dobândit accesul fizic la o mașină. Din acest motiv, cel mai bine este să aveți serverul de aplicații și serverul de baze de date pe diferite mașini. Dacă acest lucru nu este posibil, trebuie să vă asigurați că executați comenzi la distanță prin intermediul unui server de aplicații, în caz contrar, un atacator poate să vă dăuneze baza de date chiar și fără permisiuni. Din acest motiv, oricărui serviciu care rulează pe aceeași mașină ca baza de date ar trebui să i se acorde cele mai mici privilegii de permisiune care să permită serviciului să funcționeze fără probleme.	Da (pe diferite mașini virtuale)

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

➔ Dezactivați sau restricționați accesul la distanță	◆ Dacă se utilizează accesul la distanță, asigurați-vă că numai gazdele definite pot accesa serverul. Luați în considerare restricționarea MySQL de la deschiderea unui socket de rețea (inițierea unei conexiuni la distanță)	Da
➔ Dezactivați utilizarea LOCAL INFILE	◆ Dezactivați utilizarea comenzii „LOAD DATA LOCAL INFILE”, care va ajuta la prevenirea citirii neautorizate din fișierele locale.	Da
➔ Schimbați numele de utilizator și parola de root	◆ Numele de utilizator implicit al administratorului de pe serverul MySQL este „root”. Hackerii încearcă adesea să obțină acces la permisiunile sale. Pentru a face această sarcină mai dificilă, redenumiți „root” cu altceva și furnizați-i o parolă alfanumerică lungă și complexă.	Da
➔ Eliminați baza de date „test”	◆ MySQL vine cu o bază de date „test” destinată spațiului de testare. Acesta poate fi accesat de utilizatorul anonim și, prin urmare, folosită de numeroase atacuri.	Da
➔ Eliminați conturile anonime și învechite	◆ Baza de date MySQL vine cu unii utilizatori anonimi cu parole goale. Drept urmare, oricine se poate conecta la baza de date	Da
➔ Privilegiile reduse ale sistemului; creșteți securitatea bazei de date cu ajutorul controlului bazat pe roluri	◆ O recomandare foarte comună de securitate a bazei de date este reducerea permisiunilor acordate diferitelor părți. MySQL nu este diferit. De obicei, atunci când dezvoltatorii lucrează, aceștia folosesc permisiunea maximă a sistemului și acordă o atenție mai mică principiilor permisiunii decât ne-am putea aștepta. Această practică poate expune baza de date la riscuri semnificative	Da

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

➔ Privilegiile mai mici ale bazei de date	◆ Doar conturilor de administrator trebuie să li se acorde privilegiile SUPER / PROCESS / FILE și accesul la baza de date MySQL. De obicei, este o idee bună să reduceți permisiunile administratorului pentru accesarea datelor. Examinați privilegiile celorlalți utilizatori și asigurați-vă că acestea sunt setate corespunzător.	Da
➔ Schimbați directorul root	◆ Un chroot pe sistemele de operare Unix este o operație care schimbă directorul aparent al rădăcinii discului pentru procesul curent de rulare și pentru copiii acestuia. Un program reînrădăcinat într-un alt director nu poate accesa sau denumi fișierele din afara acestuia director, iar directorul este numit „închisoare chroot" sau (mai rar) „închisoare chroot". Prin utilizarea mediului chroot, accesul la scriere al proceselor MYSQL (și al proceselor copil) poate fi limitat, sporind securitatea serverului.	Da
➔ Eliminați istoricul	◆ În timpul procedurilor de instalare, există o mulțime de informații sensibile care pot ajuta un intrus să atace o bază de date.	Da

11. Concluzii

Instrumentul de vizualizare a datelor face parte din sistemul cel mare de colectare și analiză a datelor ce țin de proiectul Functionizer, pe baza cazurilor de utilizare furnizate de 7bulls.

12. Artefacte 2021

Artefactele obținute se împart în două categorii mari:

1) produse informatice
2) servicii informatice

Produsele informatice dezvoltate de HOLISUN în cadrul proiectului FUNCTIONIZER sunt sumarizate în Tabel 11.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Tabel 11 Descrierea tipurilor de produse informatice

Denumire produs/serviciu	Tip	Descriere	Dată
Platforma de recunoastere faciala, utilizand calculul fara server	Produs Informatic	Platforma software utilizata pentru recunoastere faciala, utilizand tehnologii cloud fara server. Imaginile vin de la stream-uri video (unele de pe ochelari inteligenti).	mai 2021
Tehnologie de recunoastere faciala	Tehnologie	Algoritmi specializati de recunoastere faciala utilizand tehnologii fara server	mai 2021
Tehnologie de testare a platformelor cloud fara server	Tehnologie	Tehnologie de testare a platformelor cloud fara server, bazata pe o metodologie foarte bine definita, independenta de furnizorul de cloud.	ianuarie 2021

Totodată, HOLISUN a lansat un nou serviciu pe piață, bazat pe rezultatele și know-how-ul obținut în cadrul proiectului:

Tabel 12 Descrierea tipurilor de serivicii IT

Denumire serviciu	Tip	Descriere	Dată
Servicii de testare a platformelor cloud	Serviciu Informatic	Servicii de testare a platformelor cloud. Functiile fara server sunt testate cu tehnologia de testare creata in cadrul acestui proiect	mai 2021

13. Livrabile 2021

Pe parcursul proiectului au fost elaborate următoarele livrabile:

Tabel 13 Livrabile din cadrul proiectului

Nr. Livrabil	Termen	Denumire livrabil	Status
D6.4	M30	Respectarea eticii	Livrat 2021

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

14. Articole publicate 2021

Articolele publicate în cadrul proiectului FUNCTIONIZER sunt enumerate în Tabel 14.

Tabel 14 Lista de articole publicate în cadrul proiectului

Nr	DOI	Tipul publicației	Link către publicație	Titlu	Autori	Publicare	Pagini relevante	ISBN	Editor
1		Conference - to appear		Functionizer - A Cloud Agnostic Platform for Serverless Computing	Oliviu Matei, katerzina Materka, Pawel Skzypek, Rudolf Erdei	Proceedings of the 35th International Conference on Advanced Information Networking and Applications (AINA-2021)			
2	https://doi.org/10.1007/978-3-030-68787-8_46	Conference	https://link.springer.com/chapter/10.1007%2F978-3-030-68787-8_46	A Serverless Architecture for a Wearable Face Recognition Application	Oliviu Matei, Rudolf Erdei, Robert Heb, Alexandru Moga	Pattern Recognition. ICPR International Workshops and Challenges: Virtual Event	642-655	978-3-030-68786-1	Springer, Cham

15. Alte activități de diseminare 2021

Proiectul a fost diseminat:

- pe pagina web: https://holisun.com/proiecte-de-cercetare/FUNCTIONIZER , având un număr de 4500 de vizitatori lunari
- pe contul de LinkedIn: https://www.linkedin.com/company/holisun , cu 340 de adepți
- pe pagina de Facebook: https://www.facebook.com/Holisun.IT/ , având 1830 de urmăritori.

Au fost desfășurate o serie de activități de diseminare în cadrul unor evenimente de afaceri, expoziții și evenimente de brokeraj sau networking, listate în Tabel 15.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Tabel 15 Lista de activități de diseminare

Eveniment	Locație / Organizator	Data	Link	Participanți	Rezultate
International Machines Forum	Zoom / b2match	11-12 Martie 2021	https://machinery2021.b2match.io/	Rudolf Erdei, Daniela Delinschi	Prezentarea scenariilor de utilizare și a progreselor domeniului, în contextul Iot și al optimizărilor
Cluster 3 HE	b2match	5-6 Mai 2021	https://cluster3he.b2match.io	Rudolf Erdei, Daniela Delinschi	Prezentarea proiectului BSL și stabilirea unor posibile colaborări
B2B Software Days	b2match	10-12 Mai 2021	https://2021.b2bsoftwaredays.com/	Rudolf Erdei	Prezentarea proiectului BSL și stabilirea unor posibile colaborări
DIGITAL ENTERPRISE SHOW 2021	b2match	18-19 Mai 2021	https://des2021.b2match.io/	Rudolf Erdei	Prezentarea proiectului BSL și stabilirea unor posibile colaborări
#GIS2021 - Global Innovation Summit 2021	b2match	18-20 Mai 2021	https://gis2021.b2match.io/	Daniela Delinschi	Prezentarea proiectului BSL și stabilirea unor posibile colaborări
Green Opportunities with the EEA and Norway Grants	b2match	19-20 Mai 2021	https://green-opportunities-with-eea.b2match.io/	Oliviu Matei, Rudolf Erdei	Prezentarea proiectului BSL și stabilirea unor posibile colaborări
ITmatch – virtual IT/ICT cooperation day 2021	b2match	25 Mai 2021	https://itmatch-virtual-it-ict-cooperation.b2match.io/	Rudolf Erdei, Daniela Delinschi	Prezentarea proiectului BSL și stabilirea unor posibile colaborări

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Referințe

(Miller, 2015) Miller, Ron. "AWS Lambda makes serverless applications a reality." TechCrunch (2015).

(Raines, 2010) Raines, Geoffrey, and Lawrence Pizette. Platform as a service: A 2010 marketplace analysis. MITRE CORP MCLEAN VA MCLEAN, 2010.

(Zahariev, 2009) Zahariev, Alexander. "Google app engine." Helsinki University of Technology (2009): 1-5.

(Brewer, 2015) Brewer, Eric A. "Kubernetes and the path to cloud native." Proceedings of the sixth ACM symposium on cloud computing. 2015.

(Villamizar, 2016) Villamizar, Mario, et al. "Infrastructure cost comparison of running web applications in the cloud using AWS lambda and monolithic and microservice architectures." 2016 16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid). IEEE, 2016.

(Lynn, 2017) Lynn, Theo, et al. "A preliminary review of enterprise serverless cloud computing (function-as-a-service) platforms." 2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2017.

(Cash, 2016) Cash, S., et al. "Managed infrastructure with IBM cloud OpenStack services." IBM Journal of Research and Development 60.2-3 (2016): 6-1.

(Sreeram, 2020)Sreeram, Praveen Kumar. Azure Serverless Computing Cookbook: Build and monitor Azure applications hosted on serverless architecture using Azure functions. Packt Publishing Ltd, 2020.

(Kritikos, 2019) Kritikos, Kyriakos, et al. "Towards the modelling of hybrid cloud applications." 2019 IEEE 12th International Conference on Cloud Computing (CLOUD). IEEE, 2019.

(Gorton, 2011) Gorton, Ian. "Software quality attributes." Essential Software Architecture. Springer, Berlin, Heidelberg, (2011). 23-38.

(Haklay, 2008) Haklay, Mordechai, and Patrick Weber. "Openstreetmap: User-generated street maps." IEEE Pervasive Computing 7, no. 4 (2008): 12-18.

(Karich, 2014) Karich, Peter, and Stefan Schröder. "Graphhopper." http://www. graphhopper. com, last accessed 4, no. 2 (2014): 15.

(McHugh, 2013) McHugh, Bibiana. "Pioneering open data standards: The GTFS Story." Beyond transparency: open data and the future of civic innovation (2013): 125-135.

(Chen, 2017) Chen, Yiqun, Abbas Rajabifard, and Jennifer Day. "An advanced web API for isochrones calculation using OpenStreetMap data." In International Conference on Computers in Urban Planning and Urban Management, pp. 185-205. Springer, Cham, 2017.

(Noto, 2000) Noto, Masato, and Hiroaki Sato. "A method for the shortest path search by extended Dijkstra algorithm." In *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0*, vol. 3, pp. 2316-2320. IEEE, 2000.

(Nosrati, 2012) Nosrati, Masoud, Ronak Karimi, and Hojat Allah Hasanvand. "Investigation of the*(star) search algorithms: Characteristics, methods and approaches." *World Applied Programming* 2, no. 4 (2012): 251-256.

(Geisberger, 2008) Geisberger, Robert, Peter Sanders, Dominik Schultes, and Daniel Delling. "Contraction hierarchies: Faster and simpler hierarchical routing in road networks." In *International Workshop on Experimental and Efficient Algorithms*, pp. 319-333. Springer, Berlin, Heidelberg, 2008.

(Steneker2016)Steneker, Maikel. Towards an empirical validation of the TIOBE Quality Indicator. Diss. Eindhoven University of Technology, 2016.

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

Telefon: +40262226778
WEB: http://www.holisun.com • E-mail: info@holisun.com

E! 11990 Functionizer

Multi-cloud & serverless deployment optimisation platform
for data-intensive computing

Deliverable D6.6

Ethical compliance

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

Document	
Deliverable title	Ethical compliance
Related Work package	WP6
Responsible editor	Oliviu Matei
Contributors	N/A
Delivery date	2020.11.30

Version history			
Author	Comment	Version	Date
Oliviu Matei	Draft	0.1	
Oliviu Matei	Final version	1.0	30.11.2020

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

Table of Contents

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

1. Introduction

This deliverable presents the requirements regarding the business case application within Functionizer project. The main goal of the project is to create a unique platform that will optimize and manage the deployment of serverless and hybrid applications in multi-cloud environments. This approach is an outcome of a growing market of data-intensive applications that constantly pursue better performance, resource- and cost-efficiency. One advantage of serverless architecture is the easy parallelization for calculation and data (or resource) access. Distributed cloud infrastructure will make use of the network edge in the future. According to [Var2018], serverless computing is expected to have the following impacts:

- Two tier applications will be replaced by new multi-tier cloud architectures;
- Next generation cloud computing impacts both societal and scientific avenues;
- A new marketplace will need to be developed for resources at the network edge;
- Security and sustainability are key to architecting future cloud systems.

Serverless computing could be also handy for other types of applications which might comprise components which are rarely executed due to null costs involved by idle components, comparing with server-based architecture, which run all the time and incumbe continuous costs, independently on actual the usage.

1.1. Structure of the document

The remaining document is structured as follows:

- Chapter 2 describes the context of the ethical issues relevant for the project and its intended output in the form of the Functionizer framework and the reference application based on face recognition.
- Chapter 3 defines the ethical issues prerequisites.
- Chapter 4 presents the overall approach and procedures implemented to ensure the ethical compliance.
- The last chapter summarizes the work presented in the deliverable and draws important conclusions, needed for further development of the project and future exploitation of the reference application.

1.2. Intended audience

The intended audience of this document is internal because it defines the approach, tools and procedures needed for the implementation of the validation phase of the project and potential future commercial exploitation of Holisun's face recognition technology in line with the requirements of the ethical research and the proper protection of personal data.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

2. Context description

The ethical issues which may arise from the use of the technology created in the course of the project are limited to the reference application that acts as a use case validating the Functionizer framework and the validation phase of the project. Holisun's face recognition technology has been selected as a use case application. Since this application collects information of a person's facial features that are classified as biometric, thus sensitive personal data according to the GDPR definition, it may potentially raise ethical concerns that are addressed in this document. This chapter presents the context of the use case application, its technical and functional features and relevant data sources.

2.1 Business case perspective

The business case must validate the Functionizer platform, by demonstrating that serverless computing can be effectively incorporated in the multi-cloud domain and demonstrate how Functionizer makes deployment and management of multi-cloud data-intensive applications faster, simpler and cheaper. The business case focuses on a certain software solution, which takes an audio/video streaming from wearable devices (namely smart glasses) and processes it on a server for face or image recognition. It has applications is several fields, such as:

1. Industry. As a company there are situations that require a specialist to be present at various interventions. You can ship a pair of glasses anywhere you need and have an employee ready to be equipped with them. The glasses will transmit a live feed of whatever the employee is watching, back to a support center where your expert will be able to provide the much needed assistance.
2. Medicine and Emergency response. Doctors and paramedics can be coordinated by a specialist from the Emergency Room during resuscitation maneuvers.
3. Training. The lecturer can perform live demonstrations (presenting equipment, performing surgery or health and safety), while students can see exactly what he is doing in real time, classes can be recorded and all that while the lecturers are using both their hands.

The features employed by the solutions include:

1. Audio/video streaming: The engineer and the technician can talk to each other and see what the other sees. The stream is encoded using H.264 encoder. If the device supports hardware acceleration, this feature is also used for better video quality. The default frame rate is 30 fps, and the default image resolution is 640x480. They resolution may vary between 320x240 and 1028x768, depending on the bandwidth. The unidirectional stream bandwidth is 1 Mb/s at a resolution of 640x480. As the communication is bidirectional, the reasonably needed bandwidth is 2 Mb. If there is a multi-user conference with n users, the bandwidth should be 2xn Mb.
2. Hands free: While the technician has the support of the engineer and streaming back what he sees, he also has his hands free and available for using the tools he needs. Therefore, the efficiency is not affected in any way.
3. Chat: This can be used when the audio stream is bad, or the user needs to send a model or serial number. The technician can send the inventory codes of the assets or their models or

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

serial numbers. Moreover, the chat is the base communication means for drawings and file transfer. Of course, they are not visible in the chat form.

4. Drawings: The engineer can draw simple shapes, such as rectangles, circles, polylines, and lines for spotting points of interest and making himself clearer in designating things. More complex shapes are useless, because if the glasses wearer moves her head, the shapes may not focus on the desired spot.
5. File transfer: The engineer can send maps of the pipelines, maintenance manuals, and designs of the specific equipment or pipes to be repaired directly to the technician. The file can be opened on the glasses if there is a viewer installed. The most often transferred files are AutoCAD, pdf, images, doc, and txt files.
6. Platform independency: We tested on the following OS: Android 5.1+, ReticleOS, iOS, and Windows. The devices used are desktops/notebooks, smart glasses (ODG R7 (HL) and Epson Moverio BT-300), and smart phones with the indicated OS. This means that the engineer can provide his support even when he is mobile (whether using Android or iPhone).
7. Snapshots: These are possible from the support center (desktop/notebook) for documenting interventions. If a solution is not available because of very specific configuration of the pipe or equipment, the engineer can take a snapshot and further research the possible solutions.
8. Recording: This is similar to snapshots. The recordings are stored when they are ended. This means that during a teleconference there can be more recordings (only of the important phases). The engineer can decide which parts of the conversation are worth being recorded and later stored. This improves the quantity of institutional knowledge in the company, which usually is lost when a technician leaves the company.
9. Multi-user video-conferencing: This is an option if they are all available from the beginning. For each user, some basic information (e.g. GPS coordinate and the browser) is available.

2.2 Operating environment

To support multi-cloud application deployment, the business case will be cloud agnostic. The software stack constituting the operating environment for this application is presented in Figure 1.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

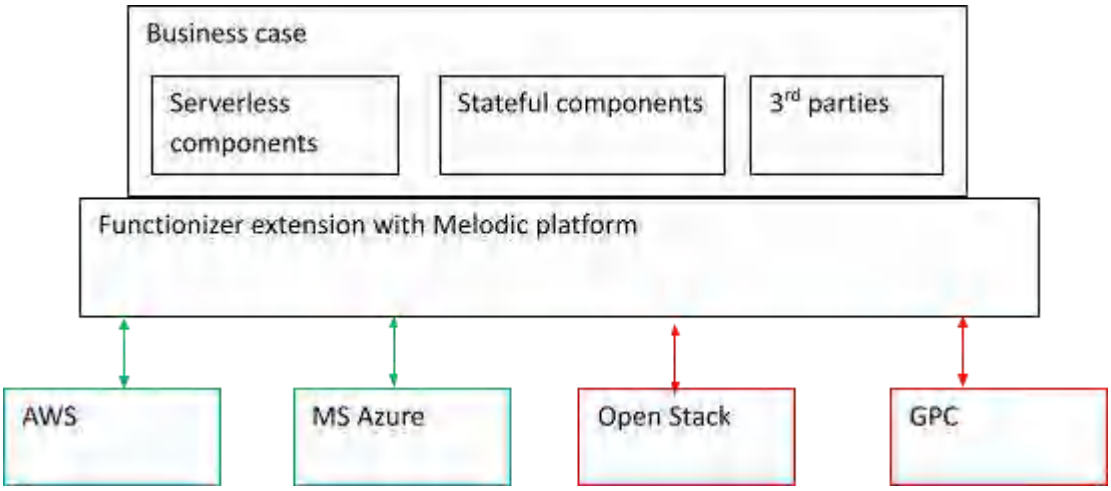

Figure 1. Software stack

2.3 Data sources

We hereby confirm that we will only use publicly available, standard test datasets set up outside of the EU for research purposes. These are:

Labeled Faces in the Wild (LFW): http://vis-www.cs.umass.edu/lfw/

LFW is a public database of face photographs designed for studying the problem of unconstrained face recognition. This database was created and maintained by researchers at the University of Massachusetts Amherst College of Information and Computer Sciences (CICS). The data set contains more than 13,000 images crawled from public web sources, including the news stories.

YouTube Faces Database: https://www.cs.tau.ac.il/~wolf/ytfaces/

YouTube Faces is a database of face videos designed for studying the problem of unconstrained face recognition in videos. It was created by researchers from The Blavatnik School of Computer Science at Tel-Aviv University and the Computer Science Division at the Open University of Israel, The data set contains over 3,400 videos of more then 1,500 different people, all downloaded from the YouTube platform.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

3. Ethical issues pre-requisites

Based on the Ethics Screening Report on the Functionizer project issues in January 2018 and the general rules for the European funded research, all activities included in the project workplan have been investigated for compliance with ethical principles and relevant national, European and international legislation, including the charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its supplementary Protocols.

In result of the ethics screening process, (1) research involving human participants and (2) personal data collection were identified as two areas where ethical concerns may potentially be raises.

In terms of **research involving human participants**, the key requirements include the compliance with the ethical principles as well as applicable international, EU and national law. A general principle of maximising benefits and minimising risks/harm should always be followed. The research carried out must ensure respect for people and for human dignity and fair distribution of the benefits and burden of research, and the protection of the values, rights and interests of the research participants. Participation must be voluntary and clear participants' written informed consent must be obtained. The potential participants must fully understand the information and not feel pressured into giving their consent. Further on, the details of recruitment, inclusion and exclusion criteria and informed consent procedures should be provided. The research sponsor must also ensure that the research methodologies do not result in discriminatory practices or unfair treatment.

In Functionizer, the requirement is relevant only in the validation phase of the project. The main idea is to use Holisun's face recognition application to validate the technical and architectural concepts and developments achieved in the project. The validation has been planned as a part of work package 6 Integration & Testing & Final validation once the different components are integrated into a complete prototype of the Functionizer framework. The validation will be completed with the use of public databases of face images available for research purposes and no human participants as such will be involved. Thus, it will not require procedures for identification and recruitment of research participants.

According to a definition provided in Article 4 of the General Data Protection Regulation (EU) 2016/679, **personal data** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Processing of personal data is by definition any operation, incl. collection, recording, organisation and storage, alteration, retrieval, use, disclosure and destruction, performed on this data manually or automatically. Processing also covers any action that uses data for research purposes.

As the face recognition technology used for the validation of the Functionizer framework collects information of a person's facial features that are classified as biometric, thus sensitive personal data according to the GDPR definition, the requirements related to protection of personal data are relevant for the validation phase of the project.

The validation of the technology is based on public databases of facial images set up outside of the EU and available for research purposes. As such, in general, it will not require compliance with the EU's general Regulation on data protection (679/2016 - GDPR). To avoid potential risks related to GDPR

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

compliance or to mitigate the possible inadequacy of the public databases for the validation of the Functionizer framework, the consortium has nevertheless designated Oliviu Matei of Holisun to act as the Data Protection Officer (DPO). The DPO is responsible for identifying all actions where the GDPR rules apply and, whenever applicable, handling the related requirements.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

4. Ethical compliance

4.1. Relevant EU and international regulations

- Regulation (EC) 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data:
  http://eur-lex.europa. eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF
- Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks:
  http://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
- Directive 2004/23/EC of 31 March 2004 on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells:
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:102:0048:0058:en:PDF
- UNESCO International Declaration on Human Genetic Data 2003:
  http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/human-genetic-data/

As the face recognition technology collects information of a person's facial features that are classified as biometric, thus sensitive personal data according to the GDPR definition, the requirements related to protection of personal data will become relevant at the validation phase of the project that is expected to start around month 30.

There are no specific national rules in Romania applicable and the project does not foresee the collection of personal data as the validation will be completed based on data from public databases set up outside of the EU. Thus, no authorization or a declaration on compliance under national law is required.

4.2. General principles

- Informed consent – Any data researchers generate that could be determined as personal needs to be protected and the release of any information needs to have gone through a strict informed consent process. Informed consent gives the subject a sense of control over their personal information or alleviates the fear that the data, samples or information will be retained or used in any other unintended manner.
- Anonymity/confidentiality – Any data collected should be anonymised so that it is not personally identifiable. Anonymisation keys and cryptographic procedures need to be established with secured access to the keys.
- Data/sample use and destruction – Any research should clearly state how long the samples or data will be retained, who will have access to it, and how it will be destroyed after the research is complete.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

- Respect the principle of proportionality – only collect data necessary and proportionate to the research objectives.
- Use expertise – An expert in data management, encryption and data protection should be consulted or employed on sensitive projects. This person or team should also have experience in other ethical issues and serve on the ethics panel or as an ethics adviser.

4.3. Data used within Functionizer

The data used for the project use case validation are the face photographs and face videos labelled with the name of the person pictured and gathered in public databases designed for studying the problem of unconstrained face recognition.

4.4. Pseudonymization and anonymization

https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection.pdf

One of the best ways to mitigate the ethical concerns arising from the use of personal data is to anonymise them so that they no longer relate to identifiable persons. Data that no longer relate to identifiable persons, such as aggregate and statistical data, or data that have otherwise been rendered anonymous so that the data subject cannot be re-identified, are not personal data and are therefore outside the scope of data protection law. However, even if you plan to use only anonymised datasets, your proposal may still raise significant ethics issues. These could relate to the origins of the data or the manner in which they were obtained. You must therefore specify the source of the datasets you intend to use in your proposal and address any ethics issues that arise. You must also consider the potential for misuse of the research methodology or findings, and the risk of harm to the group or community that the data concern. Where it is necessary to retain a link between the research subjects and their personal data, you should, wherever possible, pseudonymise the data in order to protect the data subject's privacy and minimise the risk to their fundamental rights in the event of unauthorised access. Pseudonymisation and anonymisation are not the same thing and it is important that you are aware of the difference between them, as the GDPR requires you to use them wherever possible or feasible (Article 89 GDPR).

While anonymised data are no longer considered personal data, anonymisation processes are challenging, particularly where large datasets containing a wide range of personal data are concerned. This is because it is very difficult to create fully anonymous datasets that retain the granular information needed for research purposes.4 As far as your research proposal is concerned, if there is a significant prospect of re-identification of persons whose data have been collected, the information should be treated as personal data. It is difficult to assess the risk of re-identification with absolute certainty and you should always err on the side of caution. A growing body of case studies and research publications in which individuals are identified from 'anonymous' datasets has demonstrated the fundamental constraints to anonymisation as a technique to protect the privacy of individuals. If you intend to anonymise the data you collect for use in your research project, the timing of the anonymisation process is paramount. You are collecting 'anonymised' data only if the anonymisation happens at the point and time at which the data are collected from the research subject, so that no personal data are actually processed. If anonymisation takes place at a later stage, e.g. you intend to remove personally identifiable information during the transcription of audio recordings or at the point at which survey data

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

are fed into a database, the raw data are still personal data and your proposal must include provisions for their protection up until the point at which they are deleted or rendered anonymous. In some instances, your host institution, funding body or publisher may require you to keep the raw data for auditing, accountability or research integrity purposes. There may be other scenarios in which a host institution has a raw dataset which it makes available to its researchers and partners in anonymised form. In these instances, while the recipients of the anonymised data may – subject to the mitigation of the risk of re-identification – be exempt from data protection requirements, the host institution is still processing personal data and must therefore ensure appropriate protection for the raw (personal) data. This includes technical and organisational measures to protect the data and the means to identify the data subjects (e.g. the keys, codes or applications used to anonymise the data) against unauthorised access or use. If you are in any doubt as to the adequacy of the technique(s) that you intend to use, you should seek advice from your DPO or a suitably qualified expert. As noted below (see Box 5), for sensitive or complex processing scenarios involving pseudonymisation or anonymisation, it may even be necessary to conduct a DPIA in order to ensure an appropriate level of data protection and minimise risk to the data subjects' rights.

4.5. Data protection by design and default

To innovate ethically and responsibly, researchers and developers have long been encouraged to apply the concept of 'privacy by design', which provides a framework for focusing the design of systems, databases and processes on respect for data subjects' fundamental rights. A wider concept of 'data protection by design', now included in the GDPR, requires data controllers to implement appropriate technical and organisational measures to give effect to the GDPR's core data-protection principles (articles 5 and 25 GDPR). Data protection by design is one of the best ways to address the ethics concerns that arise from your research proposal at the design stage of your project. In a research and development context, measures to achieve data protection by design could include: the pseudonymisation or anonymisation of personal data; data minimisation (see Box 3); applied cryptography (e.g. encryption and hashing); using data-protection focused service providers and storage platforms; and arrangements that enable data subjects to exercise their fundamental rights (e.g. as regards direct access to their personal data and consent to its use or transfer). When considering whether and how to apply the principle of data protection by design, you should take into account: the nature, scope, context and purposes of processing; the severity of the risks to the data subjects' fundamental rights should you fail to protect their information; and the cost and availability of the technologies and applications you may need. You must apply the principle of data protection by design where it could mitigate the ethics risks raised by the data processing in your research project, and explain in your research proposal how this will be achieved. This approach is underscored by the principle of data protection by default. Wherever you have the possibility to enhance the level of data protection afforded to your research subjects, you should apply such measures by default rather than just considering them or making them available as an optional extra. Where your research involves complex, sensitive or large-scale data processing, your proposal should include a description of the measures you will take to apply the principles of data protection by design and default, and/or to enhance security so as to prevent unauthorised access to personal data or equipment.

4.6. Informed consent to data processing

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

Informed consent is the cornerstone of research ethics. It requires you to explain to research participants what your research is about, what their participation in your project will entail and any risks that may be involved. Only after you have conveyed this information to the participants – and they have fully understood it – can you seek and obtain their express permission to include them in your project (Articles 4(11) and 7 GDPR).

The requirements related to participation of humans in research are only relevant in the validation phase of the project that will take place in the frame of work package 6 around month 30 of the project. In the validation phase, we will only use the public databases of facial images and the participation of human research participants as such is not foreseen. Thus, the informed consent procedure is not required.

4.7. Use of previously collected data ('secondary use')

As noted above, some of the most high-profile breaches of ethics standards have concerned the use of data collected for one purpose and then used for other research or targeting processes, without the knowledge or consent of the data subject. If you are processing personal data in your research without the express consent of the data subjects, you must explain how you will obtain the data, justify their use in your project and ensure that the processing is fair to the data subject. If the collection or use of data raises specific ethics issues (e.g. as regards consent and transparency, privacy and the rights and expectations of the data subjects), you must provide a detailed overview of the planned data collection and processing operations and explain how the ethics concerns will be mitigated. If you are using data that are publicly available, you must provide details of the source(s) and confirm that the data are openly and publicly accessible and may be used for research purposes. You must also do this where the data you intend to use have been manifestly made public by the data subject.

If you intend to use personal data that were collected from a previous research project, you must provide details regarding the initial data collection, methodology and informed consent procedure. You must also confirm that you have permission from the owner/manager of the dataset(s) to use the data in your project. Where the planned use of data is predicated on the 'legitimate interests' of the data controller, the nature and purpose of the dataset must be set out in detail, together with the safeguards (e.g. anonymisation or pseudonymisation techniques) that warrant its use in your project. 9 If your intended data processing is based on national legislation or international regulations authorising your research, or a demonstrable overriding public interest (e.g. public health, social protection) allows you to use a particular dataset, your proposal must make reference to the relevant Member State or Union law or policy. In principle, if you are using personal data provided to you by a third party and the data subjects have not expressly consented to its use in research projects, you must, in accordance with the GDPR, inform them that you have acquired the data and what you will be using them for (art.14 GDPR). You must also provide them with the same basic information about the data processing and their rights as data subjects that you are obliged to provide to people you are collecting data from directly (see section V). These requirements do not apply only where it is not possible or would involve a disproportionate effort to contact the data subjects. However, in such cases you must implement appropriate safeguards, including technical and organisational measures to ensure respect for the principle of data minimisation (see Box 3) and protect the subjects' fundamental rights. Crucially, the GDPR requires that pseudonymisation or anonymisation techniques (see above) be implemented wherever viable (article 89 GDPR).

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

4.8. Data security

Whenever and however you collect personal data, you have both ethical and legal obligations to ensure that participants' information is properly protected. This is fundamental to safeguarding their rights and freedoms, and minimising the ethics risks related to the data processing. The GDPR requires all data controllers and processors to implement appropriate technical and organisational measures to ensure a level of data security that is commensurate to the risks faced by the data subjects in the event of unauthorised access to, or disclosure, accidental deletion or destruction of, their data (art.32 GDPR).

Your proposal should provide details of the technical and organisational measures that will be implemented to protect the personal data processed in the course of your research, e.g. with reference to your host institution's and research partners' data protection and information security policies. Such measures may include the pseudonymisation and encryption of personal data, and policies and procedures to ensure the confidentiality, integrity, availability and resilience of processing systems. Where higher-risk processing is envisaged (e.g. involving special categories or large-scale data), you should explain clearly how you will ensure an enhanced level of data security. In these scenarios, it is important that you choose appropriate research methods and data-processing tools (see Box 7). This is vital where your research involves research subjects who are vulnerable or may be rendered vulnerable because of their participation in your research project. This may be the case, e.g. if you are collecting data on sensitive political issues or communicating with people in countries with repressive governments. Almost all communication is vulnerable to surveillance and interception, but some channels are more susceptible than others. Wherever you believe there is a heightened risk to researchers and research participants, you should ensure that your communications are secure from unauthorised access.

4.9. Transfer of personal data to non-EU countries

Sending participants' personal data to partners, collaborators or service providers outside the EU raises ethical and legal issues that can be difficult to address in practice. Researchers based outside the EU may be subject to different ethical rules and their treatment of the data may fall short of EU standards. Few non-EU countries have received an 'adequacy determination' from the European Commission indicating that they have a data protection framework offering a level of protection equivalent to that provided under EU law.13 This means that your research subjects' data may not be adequately protected or may even be used in ways that undermine their fundamental rights. The EU requires that its ethics standards apply to all of the research it funds, regardless of the country in which it takes place. The transfer of personal data from non-EU countries is subject to strict data protection requirements under Chapter V GDPR.

You do not actually have to 'send' the data to a non-EU country for these provisions to apply; if one of your partners or service providers is located outside the EU and is able to access the personal data you have collected, this amounts to a 'data transfer' in the context of the GDPR. You must give details of all envisaged data transfers to non-EU countries in your proposal. You must also ensure that the recipients of the data ensure the same level of data protection as is required under EU law. For data transfers to non-EU countries to be lawful they must be predicated on one of the following grounds: the explicit consent of the data subject (which requires them to be informed in advance of any such transfers); an 'adequacy determination' by the European Commission in respect of the country in question; a

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

data-transfer agreement containing EC standard contractual clauses giving effect to EU data protection law; or binding corporate rules covering both sender and recipient and approved by a national supervisory authority. These requirements apply to all personal data transfers, regardless of the sensitivity of the data. From a research ethics perspective, the transfer of research participants' data to non-EU countries should in principle always be based on their informed consent, which must be sought and obtained in accordance with the guidance set out above. If your research proposal envisages the transfer of participants' data to non-EU countries without their express consent of the data subjects, then your proposal must clarify the legal basis for any such transfer. In such cases, you should seek the advice of your host institution's DPO as to the legality of the data transfer and include their opinion in your proposal. If your host institution does not have a DPO, you should seek the advice of a suitably qualified expert.

4.10. Collection of personal data outside the European Union

Collecting personal data from research subjects in non-EU countries raises similar ethical issues, but these may be amplified by the need to ensure that the participants are:

- Wholly comfortable with being part of a research project conducted by researchers from outside their own country;
- Aware of what will happen to their data; and
- Not subject to any undue pressure to participate.

As noted above, the EU's ethics requirements apply to all EU-funded research, irrespective of where it takes place. Similarly, the GDPR applies to all data-processing operations conducted by data controllers based in the EU, irrespective of where the processing takes place. This means that, even if you are collecting personal data outside the EU, you must still ensure and be able to demonstrate compliance with EU law.

You also have to comply with the laws of the country in which you are conducting your research, including any national data-protection laws. For example, you may be under an obligation to notify or seek permission for your research from national authorities or data protection regulators.

Further authorisations may be required to transfer personal data outside the country in which the research takes place. 'Data sovereignty' provisions may even prohibit the transfer of certain kinds of information, such as health or patient data, out of the country.

It is your responsibility to determine what legal obligations apply to any research you conduct outside the EU and to take whatever action is necessary to comply with them. You must also be able to demonstrate compliance upon request. Again, if you are unsure as to how to handle issues related to international data transfers, you should seek the advice of your host institution's DPO, or a suitably qualified expert, and include their opinion in your proposal.

4.11. Deletion and archiving of data

You may keep the personal data you collect only as long as it necessary for the purposes for which they were collected, or in accordance with the established auditing, archiving or retention provisions for your project. These must be explained to your research participants in accordance with informed consent procedures. Recent high-profile cases involving the misuse of personal data have stemmed from data

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

controllers' failure to delete personal data and ensure that third parties to whom the data were provided had done the same in accordance with the agreed terms of their use. As soon as your research data are no longer needed, or subject to an established retention period, you must securely delete the data in their entirety and make sure that they cannot be recovered. Data retained for auditing processes should be stored securely and further processed for those purposes only. If research data are held in the cloud or by a third-party service provider, you should ensure that it has securely deleted the data together with any back-ups. If data have been shared with partners or transferred to third parties in the course of your project, you should ensure that they have deleted the data, unless they have a legitimate basis for retaining them.

4.12. Data Protection Officer

The validation of the technology will be carried out based on public databases of facial images set up outside of the EU and available for research purposes. As such, in general, it will not require compliance with the EU's general Regulation on data protection (679/2016 - GDPR). To avoid potential risks related to GDPR compliance or to mitigate the possible inadequacy of the public databases for the validation of the Functionizer framework, the consortium has nevertheless designated Oliviu Matei of Holisun to act as the Data Protection Officer (DPO). The DPO will be responsible for identifying all actions where the GDPR rules apply and, whenever applicable, handling the following activities:

- Monitoring compliance of actions and processes with GDPR;
- Informing the data subjects about their data protection rights;
- Informing and training of staff involved in processing operations about their rights, obligations and responsibilities related to the protection of personal data;
- Acting as a contract point between the personnel of the project, partners' management and study participants in all matters related to the protection of personal data;
- Managing the relevant documentation.

The privacy policy is annexed to this deliverable.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

5. Conclusions

The deliverable has presented the requirements for the business case along with an initial architecture of the respective application. We capture both functional and non-functional requirements. The functional requirements refer to audio and video streaming, file transfer and storage, snapshots and recordings, multi-source streaming and user management. The non-functional requirements relate to performance, security, data storage and interoperability.

We also present the inter-relationships between the requirements for a holistic view, respectively the inter-dependencies in terms of priority and prerequisites for their implementation.

The requirements and the architecture have been validated according to the methodology presented in deliverable *D2.3. Methodology and software description*.

As the architecture presented in section 3 is in an initial stage, it is possible the future change will occur. However, it is important to notice that this initial architecture is validated based on the approved methodology.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

Annex 1. Privacy Policy

INTRODUCTION

Thank you for choosing to be part of our community at Functionizer project (“company”, “we”, “us”, or “our”). We are committed to protecting your personal information and your right to privacy. If you have any questions or concerns about our policy, or our practices with regards to your personal information, please contact us at [contact email].

When you visit our website [website] (“Site”) and use our services, you trust us with your personal information. We take your privacy very seriously. In this privacy notice, we describe our privacy policy. We seek to explain to you in the clearest way possible what information we collect, how we use it and what rights you have in relation to it. We hope you take some time to read through it carefully, as it is important. If there are any terms in this privacy policy that you do not agree with, please discontinue use of our site and our services.

This privacy policy applies to all information collected through our websites (such as [INSERT URL]), [our mobile] [or] [our Facebook applications] ("**Apps**"), and/or any related services, sales, marketing or events (we refer to them collectively in this privacy policy as the "**Sites**").

Please read this privacy policy carefully as it will help you make informed decisions about sharing your personal information with us.

Table of contents

This privacy policy was created using Termly.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

What information do we collect?

Personal information you disclose to us

In Short: *We collect personal information that you provide to us such as name, address, contact information, passwords and security data, payment information, and social media login data.*

We collect personal information that you voluntarily provide to us when [registering at the Sites or Apps,] expressing an interest in obtaining information about us or our products and services, when participating in activities on the Sites [(such as posting messages in our online forums or entering competitions, contests or giveaways)] or otherwise contacting us.

The personal information that we collect depends on the context of your interactions with us and the Sites, the choices you make and the products and features you use. The personal information we collect can include the following:

Name and Contact Data. We collect your first and last name, email address, postal address, phone number, and other similar contact data.

Credentials. We collect passwords, password hints, and similar security information used for authentication and account access.

Payment Data. We collect data necessary to process your payment if you make purchases, such as your payment instrument number (such as a credit card number), and the security code associated with your payment instrument. All payment data is stored by our payment processor and you should review its privacy policies and contact the payment processor directly to respond to your questions.

Social Media Login Data. We provide you with the option to register using social media account details, like your Facebook, Twitter or other social media account. If you choose to register in this way, we will collect the Information described in the section called "Social Logins" [LINK] below.

All personal information that you provide to us must be true, complete and accurate, and you must notify us of any changes to such personal information.

Information automatically collected

In Short: *Some information – such as IP address and/or browser and device characteristics – is collected automatically when you visit our websites.*

We automatically collect certain information when you visit, use or navigate the Sites. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you use our Site and other technical information. This information is primarily needed to maintain the security and operation of our Sites, and for our internal analytics and reporting purposes.

Like many businesses, we also collect information through cookies and similar technologies. [You can find out more about this in our Cookies Policy [Hyperlink]].

Information collected through our Apps

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

In Short: *We may collect information regarding your geo-location, mobile device, push notifications, and Facebook permissions when you use our apps.*

If you use our Apps, we may also collect the following information:

- *Geo-Location Information.* We may request access or permission to and track location-based information from your mobile device, either continuously or while you are using our mobile application, to provide location-based services. If you wish to change our access or permissions, you may do so in your device's settings.
- *Mobile Device Access.* We may request access or permission to certain features from your mobile device, including your mobile device's [Bluetooth, calendar, camera, contacts, microphone, reminders, sensors, SMS messages, social media accounts, storage,] and other features. If you wish to change our access or permissions, you may do so in your device's settings.
- *Mobile Device Data.* We may automatically collect device information (such as your mobile device ID, model and manufacturer), operating system, version information and IP address.
- *Push Notifications.* We may request to send you push notifications regarding your account or the mobile application. If you wish to opt-out from receiving these types of communications, you may turn them off in your device's settings.]
- [Facebook Permissions. We by default access your Facebook basic account information, including your name, email, gender, birthday, current city, and profile picture URL, as well as other information that you choose to make public. We may also request access to other permissions related to your account, such as friends, checkins, and likes, and you may choose to grant or deny us access to each individual permission. For more information regarding Facebook permissions, refer to the Facebook Permissions Reference.

Information collected from other Sources

In Short: *We may collect limited data from public databases, marketing partners, social media platforms, and other outside sources.*

We may obtain information about you from other sources, such as public databases, joint marketing partners, social media platforms (such as Facebook), as well as from other third parties. Examples of the information we receive from other sources include: social media profile information (your name, gender, birthday, email, current city, state and country, user identification numbers for your contacts, profile picture URL and any other information that you choose to make public); marketing leads and search results and links, including paid listings (such as sponsored links).

How do we use your information?

In Short: *We process your information for purposes based on legitimate business interests, the fulfillment of our contract with you, compliance with our legal obligations, and/or your consent.*

We use personal information collected via our Sites for a variety of business purposes described below. We process your personal information for these purposes in reliance on our legitimate business interests ("Business Purposes"), in order to enter into or perform a contract with you ("Contractual"), with your consent ("Consent"), and/or for compliance with our legal obligations ("Legal Reasons"). We indicate the specific processing grounds we rely on next to each purpose listed below.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

We use the information we collect or receive:

- **To facilitate account creation and logon process [**with your Consent**]**. If you choose to link your account with us to a third party account *(such as your Google or Facebook account), we use the information you allowed us to collect from those third parties to facilitate account creation and logon process. See the section below headed "Social Logins" for further information.
- **To send you marketing and promotional communications** [for Business Purposes and/or with your Consent]. We and/or our third party marketing partners may use the personal information you send to us for our marketing purposes, if this is in accordance with your marketing preferences. You can opt-out of our marketing emails at any time (see the "Your Privacy Rights" below).
- **To send administrative information to you** [for Business Purposes, Legal Reasons and/or possibly Contractual]. We may use your personal information to send you product, service and new feature information and/or information about changes to our terms, conditions, and policies.
- **Fulfill and manage your orders** [for Contractual reasons]. We may use your information to fulfill and manage your orders, payments, returns, and exchanges made through the Sites.
- **To post testimonials** [with your Consent]. We post testimonials on our Sites that may contain personal information. Prior to posting a testimonial, we will obtain your consent to use your name and testimonial. If you wish to update, or delete your testimonial, please contact us at [INSERT CONTACT] and be sure to include your name, testimonial location, and contact information.
- **Deliver targeted advertising to you** [for our Business Purposes and/or with your Consent]. We may use your information to develop and display content and advertising (and work with third parties who do so) tailored to your interests and/or location and to measure its effectiveness. [For more information, see our Cookie Policy [HYPERLINK]].
- **Administer prize draws and competitions** [for our Business Purposes and/or with your Consent]. We may use your information to administer prize draws and competitions when you elect to participate in competitions.
- **Request Feedback** [for our Business Purposes and/or with your Consent]. We may use your information to request feedback and to contact you about your use of our Sites.
- **To protect our Sites** [for Business Purposes and/or Legal Reasons]. We may use your information as part of our efforts to keep our Sites safe and secure (for example, for fraud monitoring and prevention).
- **To enable user-to-user communications** [with your consent]. We may use your information in order to enable user-to-user communications with each user's consent.
- **To enforce our terms, conditions and policies** [for Business Purposes, Legal Reasons and/or possibly Contractual].
- **To respond to legal requests and prevent harm** [for Legal Reasons]. If we receive a subpoena or other legal request, we may need to inspect the data we hold to determine how to respond.
- **For other Business Purposes**. We may use your information for other Business Purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Sites, products, services, marketing and your experience.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

Will your information be shared with anyone?

In Short: *We only share information with your consent, to comply with laws, to protect your rights, or to fulfill business obligations.*

We only share and disclose your information in the following situations:

- **Compliance with Laws**. We may disclose your information where we are legally required to do so in order to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal process, such as in response to a court order or a subpoena (including in response to public authorities to meet national security or law enforcement requirements).
- **Vital Interests and Legal Rights**. We may disclose your information where we believe it is necessary to investigate, prevent, or take action regarding potential violations of our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved.
- **Vendors, Consultants and Other Third-Party Service Providers**. We may share your data with third party vendors, service providers, contractors or agents who perform services for us or on our behalf and require access to such information to do that work. Examples include: payment processing, data analysis, email delivery, hosting services, customer service and marketing efforts. We may allow selected third parties to use tracking technology on the Sites, which will enable them to collect data about how you interact with the Sites over time. This information may be used to, among other things, analyze and track data, determine the popularity of certain content and better understand online activity. Unless described in this Policy, we do not share, sell, rent or trade any of your information with third parties for their promotional purposes.
- **Business Transfers**. We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.
- **Third-Party Advertisers**. We may use third-party advertising companies to serve ads when you visit the Sites. These companies may use information about your visits to our Website(s) and other websites that are contained in web cookies and other tracking technologies in order to provide advertisements about goods and services of interest to you. [See our Cookie Policy [Hyperlink] for further information].
- **Affiliates.** We may share your information with our affiliates, in which case we will require those affiliates to honor this privacy policy. Affiliates include our parent company and any subsidiaries, joint venture partners or other companies that we control or that are under common control with us.
- **Business Partners.** We may share your information with our business partners to offer you certain products, services or promotions.
- **With your Consent.** We may disclose your personal information for any other purpose with your consent.
- **Other Users.** When you share personal information (for example, by posting comments, contributions or other content to the Sites) or otherwise interact with public areas of the Site [or App], such personal information may be viewed by all users and may be publicly distributed outside the Site [and our App] in perpetuity. [If you interact with other users of our Sites and register through a social network (such as Facebook), your contacts on the social network will see your name, profile photo, and descriptions of your activity.] Similarly, other users will be

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

able to view descriptions of your activity, communicate with you within our Sites, and view your profile.

- **Offer Wall.** Our Apps may display a third-party hosted "offer wall." Such an offer wall allows third-party advertisers to offer virtual currency, gifts, or other items to users in return for acceptance and completion of an advertisement offer. Such an offer wall may appear in our mobile application and be displayed to you based on certain data, such as your geographic area or demographic information. When you click on an offer wall, you will leave our mobile application. A unique identifier, such as your user ID, will be shared with the offer wall provider in order to prevent fraud and properly credit your account.

Do we use cookies and other tracking technologies?

In Short: *We may use cookies and other tracking technologies to collect and store your information.*

We may use cookies and similar tracking technologies (like web beacons and pixels) to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Policy.

Do we use Google Maps?

In Short: *Yes, we use Google Maps for the purpose of providing better service.*

This website, mobile application, or Facebook application uses Google Maps APIs. You may find the Google Maps APIs Terms of Service here. To better understand Google's Privacy Policy, please refer to this link.

By using our Maps API Implementation, you agree to be bound by Google's Terms of Service. [By using our implementation of the Google Maps APIs, you agree to allow us to gain access to information about you including personally identifiable information (such as usernames) and non-personally identifiable information (such as location).

For a full list of what we use information for, please see the previous sections titled "Use of Your Information" and "Disclosure of Your Information." [You agree to allow us to obtain or cache your location. You may revoke your consent at anytime.] [We use information about location in conjunction with data from other data providers.]

[The Maps APIs that we use store and access cookies and other information on your devices. If you are a user currently in the European Union, please take a look at our EU User Consent Policy, which can be found at this link: [link from question].]

How do we handle your social logins?

In Short: *If you choose to register or log in to our websites using a social media account, we may have access to certain information about you.*

Our Sites offers you the ability to register and login using your third party social media account details (like your Facebook or Twitter logins). Where you choose to do this, we will receive certain profile information about you from your social media provider. The profile Information we receive may vary depending on the social media provider concerned, but will often include your name, e-mail address, friends list, profile picture as well as other information you choose to make public. [If you login using

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

Facebook, we may also request access to other permissions related to your account, such as friends, check-ins, and likes, and you may choose to grant or deny us access to each individual permission.]

We will use the information we receive only for the purposes that are described in this privacy policy or that are otherwise made clear to you on the Sites. Please note that we do not control, and are not responsible for, other uses of your personal information by your third party social media provider. We recommend that you review their privacy policy to understand how they collect, use and share your personal information, and how you can set your privacy preferences on their sites and apps.

Is your information transferred internationally?

In Short: *We may transfer, store, and process your information in countries other than your own.*

Our servers are located in [INSERT DETAILS]. If you are accessing our Sites from outside [INSERT LOCATION OF SERVERS], please be aware that your information may be transferred to, stored, and processed by us in our facilities and by those third parties with whom we may share your personal information (see "Disclosure of Your Information" above), in [INSERT DETAILS OF DESTINATION COUNTRIES] and other countries.

If you are a resident in the European Economic Area, then these countries may not have data protection or other laws as comprehensive as those in your country. We will however take all necessary measures to protect your personal information in accordance with this privacy policy and applicable law.

Option 1: European Commission's Standard Contractual Clauses (use this if you choose model clauses as a ground for international transfers): Such measures implementing the European Commission's Standard Contractual Clauses for transfers of personal information between our group companies and between us and our third-party providers, which require all such recipients to protect personal information that they process from the EEA in accordance with European data protection laws. [Our Standard Contractual Clauses can be provided upon request / are available here [link]]. We have implemented similar appropriate safeguards with our third party service providers and partners and further details can be provided upon request.

OR

Option 2: EU-U.S. Privacy Shield Framework (use this if you choose the Privacy shield framework as a ground for international transfers:

In particular [COMPANY] complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States and has certified its compliance with it. As such, [COMPANY] is committed to subjecting all personal information received from European Union (EU) member countries, in reliance on the Privacy Shield Framework, to the Framework's applicable Principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List.

[COMPANY] is responsible for the processing of personal information it receives, under the Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf.

With respect to personal information received or transferred pursuant to the Privacy Shield Framework, [COMPANY] is subject to the regulatory enforcement powers of the U.S. FTC. In certain situations, we

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

OR

Option 3: Binding Corporate Rules (use this if you choose to implement Binding Corporate Rules):

These include, a set of Binding Corporate Rules ("BCRs") established and implemented by [COMPANY]. Our BCRs have been recognized by EEA data protection authorities as providing an adequate level of protection to the personal information we process internationally. You can find a copy of our BCRs here [INSERT LINK].]

What is our stance on third-party websites?

In Short: *We are not responsible for the safety of any information that you share with third-party providers who advertise, but are not affiliated with, our websites.*

The Sites may contain advertisements from third parties that are not affiliated with us and which may link to other websites, online services or mobile applications. We cannot guarantee the safety and privacy of data you provide to any third parties. Any data collected by third parties is not covered by this privacy policy. We are not responsible for the content or privacy and security practices and policies of any third parties, including other websites, services or applications that may be linked to or from the Sites. You should review the policies of such third parties and contact them directly to respond to your questions.

How long do we keep your information?

In Short: *We keep your information for as long as necessary to fulfill the purposes outlined in this privacy policy unless otherwise required by law.*

We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy policy, unless a longer retention period is required or permitted by law (such as tax, accounting or other legal requirements). No purpose in this policy will require us keeping your personal information for longer than [90 days/6 months/1 year/2 years/the period of time in which you have an account with us/90 days past the termination of your account/6 months past the termination of your account/1 year past the termination of your account/2 years past the termination of your account].

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

How do we keep your information safe?

In Short: *We aim to protect your personal information through a system of organizational and technical security measures.*

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

We have implemented appropriate technical and organizational security measures designed to protect the security of any personal information we process. However, please also remember that we cannot guarantee that the Internet itself is 100% secure. Although we will do our best to protect your personal information, transmission of personal information to and from our Sites is at your own risk. You should only access the services within a secure environment.

Do we collect information from minors?

In Short: *We do not knowingly collect data from or market to children under 18 years of age.*

We do not knowingly solicit data from or market to children under 18 years of age. By using the Sites, you represent that you are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Site [and App]. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we have collected from children under age 18, please contact us at [INSERT CONTACT EMAIL].

What are your privacy rights?

In Short: *[In some regions, such as the European Economic Area, you have rights that allow you greater access to and control over your personal information.] You may review, change, or terminate your account at any time.*

[In some regions (like the European Economic Area), you have certain rights under applicable data protection laws. These may include the right (i) to request access and obtain a copy of your personal information, (ii) to request rectification or erasure; (iii) to restrict the processing of your personal information; and (iv) if applicable, to data portability. In certain circumstances, you may also have the right to object to the processing of your personal information. To make such a request, please use the contact details provided below [HYPERLINK]. We will consider and act upon any request in accordance with applicable data protection laws.

If we are relying on your consent to process your personal information, you have the right to withdraw your consent at any time. Please note however that this will not affect the lawfulness of the processing before its withdrawal.

If you are resident in the European Economic Area and you believe we are unlawfully processing your personal information, you also have the right to complain to your local data protection supervisory authority. You can find their contact details here: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

Account Information

You may at any time review or change the information in your account or terminate your account by:

- Logging into your account settings and updating your account
- Contacting us using the contact information provided below
- [Other]

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, some information may be retained in our files to

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme

prevent fraud, troubleshoot problems, assist with any investigations, enforce our Terms of Use and/or comply with legal requirements.

Cookies and similar technologies: Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Sites. To opt-out of interest-based advertising by advertisers on our Site visit http://www.aboutads.info/choices/. [For further information, please see our Cookie Policy [HYPERLINK]].

Opting out of email marketing: You can unsubscribe from our marketing email list at any time by clicking on the unsubscribe link in the emails that we send or by contacting us using the details provided below. You will then be removed from the marketing email list – however, we will still need to send you service-related emails that are necessary for the administration and use of your account. You can also opt-out by:

- Noting your preferences at the time you register your account with the Sites.
- Logging into your account settings and updating your preferences.
- Contacting us using the contact information provided below.

Do we make updates to this policy?

In Short: *Yes, we will update this policy as necessary to stay compliant with relevant laws.*

We may update this privacy policy from time to time. The updated version will be indicated by an updated "Revised" date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy policy, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy policy frequently to be informed of how we are protecting your information.

This project has received funding from the Eurostars-2 joint programme with co-funding from the European Union Horizon 2020 research and innovation programme