Metoda evaluacije pouzdanosti biometrijskih sustava

Ćosić, Zoran

Sveučilište u Zagrebu

Fakultet organizacije i informatike

Zoran Ćosić

METODA EVALUACIJE POUZDANOSTI BIOMETRIJSKIH SUSTAVA

DOKTORSKI RAD

Varaždin, 2015.

Sveučilište u Zagrebu

Fakultet organizacije i informatike

Zoran Ćosić

METODA EVALUACIJE POUZDANOSTI BIOMETRIJSKIH SUSTAVA

DOKTORSKI RAD

Varaždin, 2015.

Sveučilište u Zagrebu

Fakultet organizacije i informatike

ZORAN ĆOSIĆ

METODA EVALUACIJE POUZDANOSTI BIOMETRIJSKIH SUSTAVA

DOKTORSKI RAD

Mentor(i):

Prof.dr.sc. Miroslav Bača
Doc.dr.sc. Markus Schatten

Varaždin, 2015.

University of Zagreb

Faculty of Organization and Informatics

Zoran Ćosić

BIOMETRICS SYSTEM RELIABILITY EVALUATION METHOD

DOCTORAL THESIS

Varaždin, 2015.

PODACI O DOKTORSKOM RADU

I. AUTOR

Ime i prezime	Zoran Ćosić
Datum i mjesto rođenja	12.12.1967.godine, Mostar, Bosna i Hercegovina
Naziv fakulteta i mjesto diplomiranja na VII/I stupnju	Poslijediplomski studij, Pomorski Fakultet u Splitu, Split, 2007
Sadašnje zaposlenje	Statheros d.o.o., Kaštel Stari, Hrvatska

II. DOKTORSKI RAD

Naslov	Metoda evaluacije pouzdanosti biometrijskih sustava
Broj stranica, slika, tabela, priloga, bibliografskih podataka	243 stranice, 78 slika, 23 tablice, 72 koda, 4 priloga, 132 bibliografska podataka
Znanstveno područje i polje iz kojega je postignut doktorat znanosti	Društvene znanosti, informacijske i komunikacijske znanosti
Mentori ili voditelji rada	Prof.dr.sc. Miroslav Bača, mentor Doc.dr.sc. Markus Schatten, sumentor
Fakultet na kojem je obranjen doktorski rad	Fakultet organizacije i informatike
Oznaka i redni broj rada	

III. OCJENA I OBRANA

Datum sjednice Fakultetskog vijeća na kojoj je prihvaćena tema	14.03.2014
Datum predaje rada	02.04.2015
Datum sjednice Fakultetskog vijeća na kojoj je prihvaćena pozitivna ocjena rada	26.05.2015
Sastav povjerenstva koje je rad ocijenilo	1. (predsjednik Povjerenstva) Doc.dr.sc.Sandro Gerić 2. Doc.dr.sc. Markus Schatten 3. Prof.dr.sc. Mirko Čubrilo 4. Prof.dr.sc. Bernardin Ibrahimpašić 5. Prof.dr.sc. Miroslav Bača
Datum obrane doktorskog rada	10.06.2015.
Sastav povjerenstva pred kojim je rad obranjen	1. (predsjednik Povjerenstva) Doc.dr.sc.Sandro Gerić 2. Doc.dr.sc. Markus Schatten 3. Prof.dr.sc. Mirko Čubrilo 4. Prof.dr.sc. Bernardin Ibrahimpašić 5. Prof.dr.sc. Miroslav Bača
Datum promocije	

MOJOJ OBITELJI VILMI, DORIS I MARCU

MOJIM RODITELJIMA VERI I DRAGI

ZAHVALE:

Zahvaljujem se svom mentoru prof.dr.sc. Miroslavu Bači na inicijalnoj ideji, podršci, usmjeravanju te bezuvjetnoj pomoći tijekom pisanja ovog rada.

Zahvaljujem su-mentoru doc.dr.sc. Markus Schatten koji mi je nesebično pomogao u domeni formalizacije koncepata te realizaciji predmetne ontologije.

Zahvaljujem članovima povjerenstva na povjerenju i podršci mom radu : Doc.dr.sc.Sandru Geriću; Prof.dr.sc. Mirku Čubrilu te Prof.dr.sc. Bernardinu Ibrahimpašiću

Posebna zahvala kolegi i prijatelju dr.sc. Jasminu Ćosiću, sa kojim sam napisao i objavio veliki broj znanstvenih radova u domeni digitalne forenzike i biometrije te njegovoj supruzi Edisi koja nas je podržavala u nastojanjima da znanstveni rad privedemo konkluziji.

Posebna zahvala mom prijatelju Ivici Šafranku na podršci te motivaciji.

Hvala mojim roditeljima Veri i Dragi, koji nisu dočekali ovaj događaj ali žive u mom srcu, koji su mi usadili duh svjetonazora prema kojem su znanje i učenje temeljne vrijednosti.

Posljednje ali i najveće zahvale te posveta rada u cijelosti, idu mojoj supruzi Vilmi, kćeri Doris i sinu Marcu.

Hvala na potpori i strpljenju, ohrabrenju, razumijevanju te bezuvjetnoj podršci, koje su imali sve vrijeme dok su trajala moja nastojanja u znanstvenom smislu, za oblikovanje ovoga rada, naročito posljednjih godinu dana intenzivnog pisanja doktorskog rada.

Vrijeme koje sam mogao provesti sa njima, a proveo sam ga pišući ovaj rad svakako nije bilo provedeno uzaludno.

Snagu i inspiraciju za istraživanje i pisanje crpio sam iz njihove ljubavi i podrške koje su imali za mene.

SAŽETAK

Biometrijski sustavi ulaze u sve češću i raširenu uporabu od 2003 godine, kada naputak o primjeni istih, u domeni uporabe u svrhu jačanja nacionalne sigurnosti, biva ugrađen u strategiju nacionalne sigurnosti EU ,SAD te mnogih drugih zemalja. Motivi za primjenu biometrijskih sustava, posebno u domeni mjera nacionalne sigurnosti, često otvaraju niz pitanja iz područja povjerenja u svrhu korištenja prikupljenih podataka čime se u mnogim situacijama zadire u sferu potencijalnog kompromitiranja i narušavanja privatnosti osoba. Procesi standardizacije biometrijskih antropometrijskih sustava, kao preduvjet za povećanje povjerenja korisnika sustava, aktualni posljednjih godina, uglavnom se fokusiraju na definiranje određenih tehničkih značajki sustava bez eksplicitnog definiranja zahtjeva kvalitete funkcioniranja samih biometrijskih sustava. Pouzdanost biometrijskih sustava jedan je od temeljnih parametara za ocjenu kvalitete istih te sukladno tomu prijedlog budućeg znanstvenog istraživanja biti će utemeljen na povezivanju postojećih saznanja glede evaluacije pouzdanosti biometrijskih sustava s aspekta tehnologije sustava, okoline uporabe te korisnika sustava s ciljem definiranja metode za evaluaciju pouzdanosti utemeljenoj na ontologiji.

U radu je dan pregled postojećih modela evaluacije pouzdanosti te razvijen evaluacijski model OOEPBS (otvoreni okvir za evaluaciju pouzdanosti biometrijskih sustava) utemeljen na definiranoj metodi za evaluaciju pouzdanosti biometrijskih sustava.

Na temelju evaluacijskog modela OOEPBS izgrađena je ontologija čija je krovna domena biometrijska znanost sa specijalizacijom koncepata koji pokrivaju problematike evaluacije pouzdanosti biometrijskih sustava. Realizirana je također i provjera valjanosti te vrednovanje izgrađene ontologije, te su kreirane i instance koje su poslužile za testiranje okvira.

Ključne riječi: biometrija, biometrijski sustavi, pouzdanost, hardver, softver, performanse, okolina, korisnik, ontologija, otvoreni okvir, evaluacija pouzdanosti, model, metoda.

EXTENDED ABSTRACT

The widespread usage of biometric systems is gaining momentum after 2003., when their utilization, within enforcement national security process, has been ordered and built into security strategies of the E.U., U.S.A., and many other countries. The motives for the utilization of such systems with emphasis on preserving national security, often raises a number of questions in the domain of privacy concerns regarding the potential misuse of the collected data, thus often penetrating into the sphere of potential compromising of users privacy. On the other hand, biometric system's standardization processes, which should be a prerequisite for increasing the users' confidence into the systems, predominantly focuses on defining certain technical features, without explicitly defining quality requirements. Reliability of biometric system is one of the fundamental parameters for evaluating the quality of the same, followed by the proposal of future scientific research will be based on linking existing knowledge regarding the evaluation of the reliability of biometric systems in terms, customer motivation, motivation of use of technology, the environment , usability and performance evaluation parameters with the aim of defining method for evaluating reliability based on ontology.

An overview of actual evaluation models is presented in this doctoral thesis and also is developed an evaluation model OOEPBS (open framework for reliability evaluation for biometric systems) based on the reliability evaluation method for biometric systems.
OOEPBS evaluation model has served for the development of the ontology with domain in biometrical science and specialization of the concepts within the reliability evaluation area. Ontology is evaluated and tested by using an open framework testing instances.

Keywords: biometrics, biometrical systems, reliability, hardware, software, performance, biometrija, environment, user, ontology, open framework, reliability evaluation, model, method.

SADRŽAJ

POPIS SLIKA

POPIS TABLICA

POPIS KODOVA

POPIS SWRL PRAVILA

POGLAVLJE I

1 UVOD

Biometrija [1] u širem smislu predstavlja statističko proučavanje bioloških fenomena uz primjenu matematike i statistike u procesima razumijevanja živih bića što je naročito evidentno u modernoj medicinskoj znanosti. U užem smislu biometriju [2] može se definirati kao automatizirano prepoznavanje osoba temeljeno na njihovim biološkim/fizičkim ili psihološkim/ponašajnim karakteristikama imitiranjem sposobnosti ljudi da prepoznaju jedni druge[1]. Biometrija može biti definirana također kao "alat" za utvrđivanje razine pouzdanosti ili povjerenja u odluku sustava da je određena osoba poznata ili nepoznata sustavu ili pripada li određenoj grupi osoba kojima pripadaju određena prava ili grupi osoba kojima su određena prava uskraćena. Funkcioniranje i primjena biometrijskih sustava utemeljena je na pretpostavci da je moguće osobe prepoznavati odnosno razlikovati prema njihovim biološkim ili psihološkim karakteristikama. Sve šira primjena biometrijskih sustava ostavlja prostora za širok spektar otvorenih pitanja koja se vezuju uz efektivnost te efikasnost biometrijskih sustava kao nadzornih ili sigurnosnih mehanizama implementiranih u druge sustave [3] , njihovu pristupačnost pri korištenju, faktore upravljivosti, prikladnost biometrijskih sustava, društveni utjecaj, utjecaj na privatnost te pravne i političke implikacije koje mogu imati.

Neka od otvorenih pitanja iz domene pouzdanosti biometrijskih sustava su sljedeća:

-Problematika prepoznavanja osoba je inherentno probabilistička te prema tome inherentno pogriješiva. Vjerojatnost pogreške sustava može biti svedena na minimalnu prihvatljivu vrijednost ali ne može biti eliminirana,

-Problematike znanstvenog dokazivanja distribucije biometrijskih karakteristika osoba unutar ciljane populacije korisnika,

-Problematike proučavanja interakcije osoba sa biometrijskim sustavima naročito u područjima primjene koji uključuju sustave od važnosti za nacionalnu sigurnost.

[1] ISO/IEC JTC1 1/SC37 WG1 Harmonized biometric vocabulary

Biometrijski sustavi inkorporiraju u sebi suštinske, tehnološke te društvene konotacije primjene te istovremeno predstavljaju komponentu šireg tehnološkog te društvenog konteksta primjena i namjena tih sustava otvarajući sve više pitanja na koja je vrlo malo konkretnih odgovora. Jedno od takvih pitanja je i pitanje pouzdanosti biometrijskih sustava koji sukladno gore navedenom ima višestruko stratificirane razine otvorenih problematika.

1.1 Predmet istraživanja

Nadolazeće nove tehnologije poput biometrije [4] susreću se sa često nerealnim očekivanjima glede njihovih operativnih performansi te ih se često nepravedno uspoređuje sa sustavima koji koriste samo zaporke ili neke druge trivijalne alternative. Uzimajući u obzir vjerojatnosni karakter mehanizama donošenja odluke biometrijskog sustava [5] postavlja se pitanje: Mora li biometrijski sustav biti 100% siguran i precizan ili može biti dopustiva određena granica nepovjerenja ili nepouzdanosti u sustav?

Pojam nepouzdanosti ili nepovjerenja u sustav može biti definiran kako to sugerira [6] ISO/IEC GUIDE 98-32 točka 2.2:„u principu mjerna vrijednost ne može biti kompletno opisana bez beskonačne količine podataka. Tako definiran opseg vodi ka otvaranju prostora za interpretacije rezultata pa, nekompletna definicija mjerene vrijednosti nas uvodi u problematike nepouzdanosti rezultata mjerenja gdje komponenta nepouzdanosti može ili ne mora imati značajan utjecaj na zahtijevani razina preciznosti samog rezultata mjerenja“

ili:

„kada se evaluiraju sve poznate komponente greške te apliciraju odgovarajuće korekcije , ostaje još nepouzdanost u izraženi rezultat kao sumnje u to kako dobro taj rezultat mjerenja predstavlja mjerenu vrijednost.“

Pojedina rješenja biometrijskih sustava [7] zahtijevaju visoku razinu pouzdanosti a ne samo zadovoljavajuću pa je zato lakše opravdati potrebu za investiranjem u razvoj takovih sustava. U svakom slučaju dizajneri i projektanti sustava moraju imati alate za dovoljnu razinu spoznaje o primjeni biometrijskih sustava da bi se postigao glavni cilj primjene sustava kroz

[2] ISO/IEC GUIDE 98-3 Uncertainty of measurement Part 3: Guide to the expression of uncertainty in measurement (GUM:1995)

predefinirane razinae performansi. Ipak rješenja problema prepoznavanja osoba, gledajući kroz povijest, bila su često nedostižna a napor koji je potreban da bi se do rješenja došlo bio je isto tako podcijenjen. Problematike prepoznavanja osoba [8], gledajući kroz aspekt ljudske prirođene ,naizgled jednostavne, sposobnosti prepoznavanja i razlikovanja, često su se poistovjećivale sa laganim zadatkom koji ima isto tako lagana rješenja. Uzimajući u obzir da sve veći broj vlada država širom svijeta otvaraju vrata širokom spektru primjene biometrijskih sustava u domeni krucijalnih društvenih funkcija kao što su npr. izdavanje i kontrola identifikacijskih dokumenata, javlja se velika potreba za znanstveno-istraživačkim djelovanjem u ovom području. Tako je 2011. godine formiran i pokrenut projekt Evaluiranja biometrije i testiranja BEAT[3] [9] pod pokroviteljstvom Europske Komisije pod 7. okvirnim programom[4] pod nazivom «Evaluation of identification technologies, including biometric (SEC-2011.5.1-1)» , koji ukazuje na područja otvorena za istraživačke poduhvate. Područja istraživanja sa mnoštvom otvorenih pitanja do danas nedovoljno proučavanih sa manjkom predloženih rješenja mogu se klasificirati preko sljedećih aspekata:

a) Tehnologija biometrijskih sustava,

Iako postoje međunarodni standardi [10] koji reguliraju problematike testiranja performansi biometrijskih sustava kao što je ISO/IEC 19795-15 koji u svojim aneksima definiraju najbolje svjetske prakse konteksta primjene biometrijskih sustava kao što su npr. biometrijski sustavi za prepoznavanje geometrije lica, nedovoljna je količina kvalitativnih zahtjeva koje sustav mora ispuniti da bi se od korisnika dobio optimalan način interakcije sa sustavom ili:Što sustav treba imati inkorporirano da bi se na neinvazivan način dobila optimalna slika lica korisnika?

b) Društvenog konteksta primjene biometrijskih sustava [3],

Društveni i kulturološki problemi primjene biometrijskih sustava mogu biti podijeljeni na dvije razine:

1. razina osobe

   Problematike interakcije osobe sa biometrijskim uređajem ovisno radi li se o aktivnoj ili pasivnoj interakciji, otvorenoj ili prikrivenoj interakciji itd.
2. razina zajednice

[3] Izvorno: Biometric Evaluation and Testing

[4] Izvorno: Seventh Framework Programme

[5] ISO/IEC 19795-1 Information technology — Biometric performance testing and reporting-Part 1:Principles and framework

Problematike utjecaja primjene biometrijskih sustava na zajednicu u smislu trgovine, turizma, sprječavanja ilegalne imigracije, prevencije terorizma itd.

Potrebno je produbiti spoznaje o određivanju neinvazivnih protokola funkcioniranja biometrijskih sustava koji mogu utjecati na razina prihvaćanja biometrijskih sustava od strane osoba odnosno zajednice te analize sklonosti sudionika ciljane skupine ka poštivanju autoriteta, želje za usvajanjem novih tehnologija, njihove privrženosti određenim religioznim i kulturološkim uvjerenjima itd.

c) Politike javne i nacionalne sigurnosti po pitanju motivacije za primjenu biometrijskih sustava,

Uzimajući u obzir trend rasta stupnja uključivanja biometrijskih sustava [11] u servise koje javne ili državne službe stavljaju na raspolaganje, moguć je razvoj razina zabrinutosti od strane korisnika glede namjera moguće uporabe podataka u odnosu na onu deklariranu od strane vlasti. Također nisu zanemarivi činitelji privatnosti i povjerljivosti podataka kojima raspolažu biometrijski sustavi. Problematike koje ostavljaju prostora za daljnje istraživanje mogu se razvrstati na:

- Problematike vezane uz mogućnosti aktualno dostupne tehnologije glede zadovoljavanja potreba primjene biometrijskih sustava,
- Problematike vezane uz upravljanje rizicima prilikom korištenja biometrijskih sustava,
- Problematike vezane uz razmatranje potrebe za ili ne zakonskom prisilom korištenja biometrijskim uređajima za određene svrhe,
- Problematike vezane za stručnost kadra koji radi sa biometrijskim uređajima.

Istraživanje po bilo kojem od navedenih područja može dati značajan doprinos razvoju primjene biometrijskih sustava. Definiranje problematike pouzdanosti sa različitih aspekata navedenih u ovome radu poslužiti će za bolje sagledavanje kroz jedinstvenu perspektivu, opcija za dizajn, razvoj te implementaciju biometrijskih sustava. Tijek znanstvenog istraživanja biti će realiziran na području definiranja Otvorenog okvira za izradu evaluacijskog modela pouzdanosti biometrijskih sustava utemeljenog na ontologiji. Ontologija [12] ima za cilj opsežno i detaljno opisati aspekte pouzdanosti biometrijskih sustava te povezati iste u jednu cjelinu radi definiranja Otvorenog okvira za izradu jedinstvenog evaluacijskog modela pouzdanosti biometrijskih sustava. Otvoreni okvir može biti linija vodilja za definiranje specifičnih modela sačinjenih od primjerenih setova pitanja ili

naredbi, usmjerenih na detalje te modalitete primjene , koja mogu dati korisne informacije kako korisnicima biometrijskih sustava tako dizajnerima i proizvođačima.

1.2 Ciljevi istraživanja

Obzirom da se radi o relativno nepokrivenom znanstvenom području u dostupnoj literaturi je vrlo malo objavljenih radova koji se bave istraživanjima na ovu temu.

Cilj ovog znanstvenog rada je definirati otvoreni metodološki okvir za evaluaciju pouzdanosti biometrijskih sustava uzimajući u obzir aspekte pouzdanosti biometrijskih sustava manifestiranih kroz sljedeće sastavnice: tehnologija sustava, okolina uporabe sustava te korisnik biometrijskog sustava. Metodološki okvir utemeljen je na ontologiji, kao osnovi za izradu specifičnih modela koji će se baviti proučavanjem te detaljnom razradom navedenih aspekata pouzdanosti biometrijskih sustava.

Metodološki okvir za evaluaciju pouzdanosti biometrijskog sustava strukturiran je na način da uzima u obzir pojavnosti biometrijskih sustava kroz trijadu aspekata koje su opisane kako slijedi:

- Tehnologija biometrijskih sustava sa stanovišta pouzdanosti hardvera, softvera te performansi sustava kroz statističke parametre FMR i FNMR, te FTA i FTE a koji su definirani od strane proizvođača sustava,
- Okolina uporabe biometrijskih sustava sa stanovišta okolinskih čimbenika unutar kojih biometrijski sustav funkcionira,
- Korisnik biometrijskih sustava sa stanovišta utjecaja na karakteristike korisnika koje predstavljaju ulaz u proces identifikacije ili verifikacije te osobnih činitelja utjecaja na samog korisnika tijekom interakcije sa biometrijskim sustavom.

Metodološki okvir pretpostavlja serijsku ovisnost navedenih aspekata pouzdanosti biometrijskih sustava u smislu isključivog utjecaja pojedinog aspekta na sposobnost sustava da izvršava svoju operativnu funkciju. Metodološki okvir omogućava rezoniranje o prihvatljivosti riješenja biometrijskih sustava u domeni pouzdanosti te na temelju ulaznih podataka o tehnologiji, okolini uporabe te korisniku sustava, definiciju te analizu razine pouzdanosti biometrijskih sustava, metrički definiranih u samoj ontologiji. Pravila za

rezoniranje implementirana su unutar alata Protege' u jeziku SWRL (Izvorno: Semantic Web Rule Language).

Pojedinačni ciljevi doktorskog rada mogu se sublimirati kao:

- identifikacija sastavnica navedenih aspekata pouzdanosti biometrijskih sustava a koji imaju utjecaj na performanse biometrijskih sustava,

- definicija funkcije međusobne ovisnosti sastavnica aspekata pouzdanosti biometrijskih sustava,

- parametrizacija sastavnica te njihovo metričko definiranje,

- formalna ontološka deskripcija pojmova koji opisuju parametrizirane sastavnice aspekata pouzdanosti odabranih biometrijskih sustava te definiranje međusobne povezanosti i atributa,

- implementacija ontološki opisanih pojmova pomoću alata otvorenog koda Protege',

- implementacija pravila za rezoniranje o razini pouzdanosti biometrijskih sustava na temelju postavljanja upita u jeziku SWRL,

- pomoću izrađene ontologije metodološkog okvira za evaluaciju pouzdanosti biometrijskih sustava, stvaranje temelja za širi pristup problematikama evaluacije pouzdanosti biometrijskih sustava.

1.3 Motivacija za istraživanje

Biometrija ima potencijal [13] postati temelj širokog spektra mogućih uporaba u domeni sigurne identifikacije ili verifikacije osoba u službi nacionalne sigurnosti te prevencije krađa i prijevara biometrijskih identiteta osoba. Korporacijski biometrijski sustavi za identifikaciju zaposlenika, sigurnost bankarskih transakcija, sigurnost investicija i ostalih financijskih transakcija, primjena zakonskih propisa, zdravstvene i socijalne usluge već koriste prednosti ovih tehnologija. Premda biometrija nije nova kao pojam pa tako tehnologija identifikacije putem biometrije nije novina ali događaji vezani uz 11.09.2001 , promijenili su stav ljudi prema uporabi te potrebi za biometrijskim sustavima. Navedeni događaj [11] je dramatično smanjio odbojnost javnog mnijenja prema biometrijskoj tehnologiji isprva viđenoj kao

invazivnoj. Kombinacija iznenađenja, straha te šoka utjecala je na stvaranje kolektivne atmosfere prihvaćanja ideje o efektivnijoj tehnologiji sigurnosti i zaštite. Ispitivanja koja su provedena u USA nakon toga, nadmoćno pokazuju odobravanje amerikanaca nad primjenom biometrijskih tehnologija na aerodromima ili ondje gdje je nasušna potreba za primjenom mjera za identifikaciju potencijalnih terorista. Ovaj val uopćenog odobravanja uporabe biometrijskih tehnologija za identifikaciju i verifikaciju sadrži određene rezerve glede problematika privatnosti i tajnosti prikupljenih podataka sa iznimkom situacija koje se smatraju od značaja za nacionalnu sigurnost. Identifikacija i verifikacija osoba dobila je zeleno svjetlo putem Zakona Patriot[6] iz 2001 ažuriranog 2006 sa mandatom ka definiranju standarda u domeni identifikacije i verifikacije putem korištenja biometrijskih tehnologija. Mandat za kreiranje standarda [6] i sukladno tomu novih tehnologija imalo je za rezultat masovno financijsko ulaganje države kroz razne poticaje. Postoje procjene da je u projekt US-Visit , projekt za kontrolu nad useljeničkim podacima kroz biometrijske sustave, uloženo preko 10 mlrd $. Korištenje biometrije za potvrđivanje identiteta osoba postala je ključna komponenta nacionalne sigurnosti velikog broja zemalja (opp.a. - 60 zemalja,do sada, koriste biometrijske putovnice) pa tako postoji eskalacija potrebe za razvojem pouzdanih biometrijskih sustava [3] koji sa visokom preciznošću i efikasnošću mogu ispuniti svoju zadaću. Nacionalni savjet znanosti i tehnologije[7] SAD izdao je dokument naslovljen Nacionalni biometrijski izazovi [14] gdje se definiraju okviri za stvaranje pretpostavki stvaranja biometrijskih tehnologija kao preduvjeta za identifikaciju osoba u realnom vremenu. Po ugledu na događanja u SAD , Europska unija također je usvojila uporabu biometrijskih tehnologija kao temelj za provedbu Shengenskog sporazuma te implementaciju druge generacije Shengenskog informacijskog sustava[8]. Ustanovljena je također EURODAC[9] baza podataka otisaka prstiju, koja omogućava pretraživanje i verifikaciju tražitelja azila u zemljama EU uključujući Norvešku i Island. Ustanovljen je Informacijski sustav [3] o vizama[10] koji sadrži bazu podataka o preko 70 milijuna kompleta otisaka prstiju zajedno sa demografskim podacima te omogućuje razmjenu podataka među zemljama članicama te podrška projektu US-Visit.

[6] Izvorno: Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

[7] Izvorno: National Science and Technology Council – NSTC

[8] Izvorno: Shengen Information System – SIS II

[9] Izvorno: European dactyloscopy

[10] Izvorno: Visa Information System – VIS

1.4 Istraživačka pitanja i hipoteze

Sukladno postavljenim ciljevima definirana su istraživačka pitanja na koja ovaj rad daje odgovor su:

- Koje su sastavnice aspekata pouzdanosti biometrijskih sustava koje imaju utjecaj na performanse biometrijskih sustava?,
- Koje su funkcije međusobne ovisnosti sastavnica aspekata pouzdanosti biometrijskih sustava?,
- Kako se sastavnice mogu parametrizirati te metrički definirati?,
- Da li je moguća ontološka deskripcija pojmova koji opisuju parametrizirane sastavnice aspekata pouzdanosti odabranih biometrijskih sustava te definiranje međusobne povezanosti i atributa?,
- Da li je moguća implementacija ontološki opisanih pojmova pomoću alata otvorenog koda Protege'?,
- Da li je moguća implementacija pravila za rezoniranje o razini pouzdanosti biometrijskih sustava na temelju postavljanja upita u jeziku SWRL?
- Da li je moguće pomoću definirane ontologije metodološkog okvira za evaluaciju pouzdanosti biometrijskih sustava, stvaranje temelja za širi pristup problematikama evaluacije pouzdanosti biometrijskih sustava?

Aspekti pouzdanosti biometrijskih sustava, za potrebe ovog rada a sukladno iznešenome u poglavlju 1.2 , definiraju se na sljedeći način:

1. Tehnologija biometrijskih sustava sa stanovišta pouzdanosti hardvera, softvera te performansi sustava kroz parametre FMR[11] i FNMR[12], FTE[13] i FTA[14] koji su definirani od strane proizvođača sustava. Ovo stanovište pouzdanosti uzima u obzir tehnički sustav samog biometrijskog uređaja sa komponentama hardver i softver te kvalitativnom ocjenom rada sustava uzimajući u obzir statističke parametre– stopa pogrešnog podudaranja (FMR) , Stopa pogrešnog nepodudaranja (FNMR), greška prilikom uvježbavanja (FTE) te greška prilikom izuzimanja (FTA). U radu je

[11] Izvorno : False Match Rate – FMR

[12] Izvorno: False non match rate – FNMR

[13] Izvorno: Failure to enroll – FTE

[14] Izvorno: Failure to acquire – FTA

razrađena metodologija za ocjenu utjecaja tehnologije na pouzdanost biometrijskog sustava.

2. Okolina uporabe biometrijskih sustava sa stanovišta okolinskih čimbenika unutar kojih biometrijski sustav funkcionira. Okolina uporabe predstavlja kontekst u kojem biometrijski sustav funkcionira a koji uzima u obzir ambijent te eventualno društveno okruženje. U radu je razrađena metodologije za ocjenu utjecaja okoline na pouzdanost biometrijskog sustava,
3. Korisnik biometrijskih sustava sa aspekta utjecaja ergonomije sustava na karakteristike korisnika koje predstavljaju ulaz u proces identifikacije ili verifikacije te osobnih, ponašajnih i fizičkih činitelja utjecaja samog korisnika tijekom interakcije sa biometrijskim sustavom. Korisnik biometrijskog sustava važan je čimbenik utjecaja na funkciju samog sustava. U radu je razrađena metodologija za ocjenu utjecaja korisnika na pouzdanost samog sustava.

Analizom navedenih aspekata pouzdanosti biometrijskih sustava moguće je utvrditi njihovu međusobnu ovisnost sukladno utjecaju koji mogu imati na pouzdanost funkcije biometrijskog sustava. Uzimajući u obzir funkciju međuovisnosti navedenih sastavnica njihovo parametriziranje te metričko definiranje olakšava se definicija okvira za evaluaciju pouzdanosti biometrijskih sustava. Koristeći metodu ontologije, konceptualiziraju se postojeća saznanja iz predmetne domene te definiraju atributi i relacije među definiranim konceptima i instancama domene pouzdanosti biometrijskih sustava. Konceptualizirano domensko znanje implementirano je u okruženje otvorenog koda Protege'. Razvojem pravila za rezoniranje nad predmetnom ontologijom omogućuje se razvoj metode za evaluaciju pouzdanosti biometrijskih sustava na temelju predefiniranih ulaznih parametara.

Hipoteze koje proizlaze iz istraživačkih pitanja su:

H1: Moguće je ontološki opisati činitelje pouzdanosti biometrijskih sustava s aspekta tehnologije, korisnika i okružja uporabe te ih međusobno povezati u otvoreni metodološki okvir za evaluaciju pouzdanosti.

H2: Temeljem otvorenog metodološkog okvira za evaluaciju pouzdanosti biometrijskih sustava, definirati će se pravila pomoću kojih će se moći rezonirati o prihvatljivosti rješenja biometrijskih sustava u smislu razine pouzdanosti biometrijskog sustava u odnosu na predefinirane ulazne parametre.

1.5 Metodološki okvir

U ovome znanstveno-istraživačkom radu dan je pregled recentnih spoznaja u domeni aspekata pouzdanosti biometrijskih sustava spram navedenih sastavnica iz poglavlja 1.4, kroz iznalaženja elemenata za njihovu integraciju te prijedlog novog, šireg, pristupa rješenju problema evaluacije pouzdanosti biometrijskih sustava utemeljenog na ontologiji u vidu otvorenog okvira za uspostavljanje metodologije za evaluaciju pouzdanosti biometrijskih sustava. Kako bi bilo moguće razumjeti problematike pouzdanosti biometrijskih sustava potrebna je određena količina znanja o biometrijskim sustavima te njihovoj primjeni radi identificiranja područja koja sadrže pouzdanost kao ključni intrinzični parametar. Tijekom procesa istraživačkog rada koristila se relevantna literatura iz područja evaluacije pouzdanosti biometrijskih sustava kako slijedi: knjige iz oblasti pouzdanosti biometrijskih sustava, znanstveni članci iz međunarodnih časopisa indeksirani u referentnim bazama podataka (IEEE, ACM, SCOPUS i sl.), zbornici radova s konferencija s međunarodnom recenzijom, dostupni članci s web stranica autora koji se bave temom razrade aspekata pouzdanosti biometrijskih sustava. Ponuđeno rješenje problema i dokazivanje postavljenih hipoteza i podhipoteza zahtijeva korištenje kombinirano - primarno i sekundarno kvalitativne i kvantitativne znanstvene metode [15]. U teorijskom dijelu, prilikom opisa osnovnih koncepata iz domene pouzdanosti biometrijskih sustava, provela se temeljita kvalitativna analiza, za što se koriste opće znanstvene metode [16], deskripcije, generalizacije, kompilacije, analize te komparacije. Svrha kvalitativnog pristupa jest detaljni opis koncepata koji određuju domenu pouzdanosti biometrijskih sustava uzimajući u obzir aspekte tehnologije sustava, okoline te korisnika biometrijskih sustava. U empirijskom dijelu [17] znanstvenog istraživanja koristila se metoda klasifikacije u svrhu razvrstavanja osnovnih koncepata pouzdanosti biometrijskih sustava te njihovog postavljanja u hijerarhijski odnos s predmetnom domenom istraživanja. Kao rezultat ovoga procesa dobila se taksonomija koncepata kao prvi korak u izgradnji ontologije [18] pouzdanosti biometrijskih sustava. Ontologija pouzdanosti biometrijskih sustava je domenska (D) pri čemu je aplikacijska domena područje biometrijske znanosti koje se bavi pouzdanošću biometrijskih sustava za prepoznavanje otiska prsta [19] , dlana te analizu glasa, s aspekta tehnologije sustava, okoline uporabe te korisnika biometrijskih sustava. Aplikacijska domena razrađena je top-down pristupom do razine detaljizacije koja će biti dovoljna za uspostavljanje metodološkog okvira

za evaluaciju pouzdanosti. Dovoljna razina detaljizacije podrazumjeva definiciju funkcije međusobne ovisnosti sastavnica aspekata pouzdanosti, parametrizaciju navedenih sastavnica aspekata pouzdanosti, metrički definiranih, te definiranje pravila za rezoniranje o razinama pouzdanosti biometrijskih sustava. Ontologija je zamišljena je kao otvoreni okvir radi omogućavanja dijeljenja znanja iz domene istraživanja te ponovne uporabe tih znanja uz nadogradnju s eventualnim novim saznanjima.

Metoda modeliranja [20] koristila se za izgradnju otvorenog ontološkog okvira za uspostavu metode za evaluaciju pouzdanosti biometrijskih sustava kroz definiranje potrebnih klasa (koncepata), instanci (osoba), pravila (aksioma) koja vladaju unutar referentnih problematika a koje su unutar domene ovoga istraživanja. Pri tome se razvoj otvorene ontologije ograničava na opisivanje koncepata i pravila na najvišjoj mogućoj razini uz izbjegavanje trivijalnosti, dok se osobe konkretiziraju u testne tipologije obzirom da je tu riječ o konkretnim biometrijskim sustavima pa njihovo sveobuhvatno opisivanje nije izvedivo. Prilikom razvoja otvorene ontologije koristi se metodika METHONTOLOGY [21] koja definira sljedeće faze procesa kreiranja i izgradnje ontologije:

1. Specifikacija – predstavlja fazu u kojoj se ontologija izražava kroz dokument napisan na prirodnom jeziku koji opisuje svrhu te domenu finalnog korištenja ontologije,

2. Konceptualizacija – predstavlja fazu strukturiranja domene ontologije te definiranja taksonomije glavnih pojmova ili koncepata. Definiranje pojmova ontologije te izrada taksonomije realizirana je kroz proces razvoja ontologije za što će se koristiti softverski alat Protege' [22],

3. Integracija – predstavlja fazu povezivanja definiranih koncepata,

4. Implementacija – ova faza zahtijeva korištenje odgovarajućeg okružja koje podržava strukturiranje ontologije, a kao rezultat ima ontologiju kodiranu sukladno jednom od dostupnih formalnih jezika. Programski jezik se koristi za izgradnju ontologije jeste OWL[15], odnosno SWRL[16] za modeliranje pravila za rezoniranje nad ontologijom koja se razvija korištenjem softvera Protége [23] preko specifikacije termina u domeni činitelja pouzdanosti biometrijskih sustava. Softver Protége razvijen je od strane „Centra za biomedicinska istraživanja informatike“ na Sveučilištu Stanford School of Medicine. Softver Protégé je

[15] Izvorno: Ontology Web Language

[16] Izvorno: Semantic Web Rule Language

platforma otvorenog koda koja korisnicima omogućava uporabu alata za izgradnju modela domene te na znanju temeljene aplikacije s ontologijama,

5. Evaluacija - Ova faza predstavlja procese verifikacije, evaluacije korektnosti ontologije u tehničkom smislu te validacije, potvrde da se ontologija odnosi na domenu koja se željela opisati. Realizirana ontologija u navedenom alatu Protege' evaluira se sukladno metodologiji OntoQA [24] za evaluaciju ontologija. Rezultati evaluacijskog modela realiziranoga u SWRL-u testiraju se na temelju definiranih instanci Ontologije te verficiraju na postojećim biometrijskim sustavima za otisak prsta, otisak dlana te analizu glasa, pri čemu se vrši poredba razine pouzdanosti.

1.6 Očekivani doprinos

Društveni doprinos ovoga rada ogleda se u primjeni znanstvenih istraživanja u praksi prilikom projektiranja biometrijskih sustava te korištenja određenog modela evaluacije pouzdanosti u ranoj fazi projektiranja. Rezultati ovoga istraživanja moći će se koristiti, kako za diseminaciju znanja iz referentnog područja, tako i za realizaciju te implementaciju konkretnog sustava utemeljenog na predloženom okviru za evaluaciju pouzdanosti biometrijskih sustava. Budući da se radi o relativno neistraženom području sa mnoštvom nesistematiziranih pojmova koji opisuju određene probleme povezane sa pouzdanošću, te uzimajući u obzir da je biometrija znanost u razvoju, istraživačkim radom se stavlja akcent na povezivanje postojećih dostupnih analiza biometrijske znanosti fokusiranih na problematike evaluacije pouzdanosti biometrijskih sustava sukladno pojavnostima uporabe biometrijskih sustava. Izgrađeni otvoreni evaluacijski okvir omogućio bi sistematizaciju recentnih saznanja te povezivanje u jednu cjelinu postojećih definiranih i prihvaćenih teorija te modela evaluacije pouzdanosti biometrijskih sustava kao važnog segmenta biometrijske znanosti sa naglaskom na stvaranje temelja za definiranje i konsolidaciju pojmova kvalitete performansi biometrijskih sustava kao temelja za standardizaciju istih. Primjenom znanstvenih metoda te realizacijom ontologije identificirati će se, definirati i klasificirati osnovni pojmovi, te nakon toga izraditi otvoreni evaluacijski okvir kao preduvjet za izgradnju evaluacijskog modela, te dati prijedlog rješenja moguće primjene u praksi definirane metode. Razvijena ontologija pouzdanosti biometrijskih sustava je samo prva faza u lancu narednih aktivnosti koje podrazumijevaju definiranje okvira

te u konačnici izgradnju temelja za realizaciju metode za evaluaciju pouzdanosti biometrijskih sustava utemeljene na ontologiji.

Znanstveni doprinos ovoga istraživanja može se odrediti kroz sljedeće sastavnice:

1. Daje se doprinos sistematizaciji znanja iz područja biometrijske znanosti, a koja se odnose na problematike pouzdanosti biometrijskih sustava,
2. Omogućuje se diseminacija znanja iz područja pouzdanosti biometrijskih sustava sistematiziranih kroz otvorenu ontologiju iz predmetne domene,
3. Određuju se ontološki opisani, međusobno povezani, te metrički definirani činitelji aspekata pouzdanosti biometrijskih sustava spram tehnologije, okoline te korisnika biometrijskog sustava,
4. Razvija se otvoreni metodološki okvir za evaluaciju pouzdanosti biometrijskih sustava.

1.7 Struktura disertacije

Disertacija je strukturirana na način, da se sastoji iz deset poglavlja koja predstavljaju logičku cjelinu te se međusobno nadovezuju. U prvom poglavlju dan je prikaz same disertacije, predmeta i ciljeva istraživanja, istraživačka pitanja te hipoteze, metodološki okvir te očekivani društveni i znanstveni doprinos. U drugom poglavlju su, u cilju pojašnjenja same domene, dane definicije osnovnih pojmova iz domene pouzdanosti biometrijskih sustava, koji su relevantni za samu disertaciju. Poglavlje broj tri daje pregled trenutnih spoznaja u domeni istraživanja zakonitosti u ocjenama pouzdanosti biometrijskih sustava, dok je u poglavlju broj četiri obrađena problematika te dan pregled aktualno definiranih modela ocjene pouzdanosti različitih aspekata ili pojavnosti biometrijskih sustava. Nastavak je dan u poglavlju broj pet, u kojem je obrađena tematika postojećih evaluacijskih modela koji se bave ocjenom razina pouzdanosti biometrijskih sustava. Poglavlje broj šest se odnosi na definiranje otvorenog okvira za evaluaciju pouzdanosti biometrijskih sustava te evaluacijska metoda po modelu za evaluaciju dok je u sedmom poglavlju opisan ontološki pristup definiranju evaluacijskog modela. U osmom poglavlju opisano je testiranje funkcionalnosti definirane ontologije te ograničenja samoga otvorenog okvira. U devetom poglavlju opisana je provjera valjanosti definirane ontologije a desetom poglavlju dan je zaključak te otvorena istraživačka pitanja.

POGLAVLJE II

2 DEFINIRANJE POJMOVA RELEVANTNIH ZA DISERTACIJU

U ovom poglavlju su definirani osnovni pojmovi relevantni za disertaciju.

Dana je definicija biometrijskih sustava, pojma pouzdanosti vezanog uz funkciju biometrijskih sustava te pojma evaluacije pouzdanosti biometrijskih sustava.

2.1 Pojam biometrijskih sustava

Općeniti biometrijski sustav, sukladno Waymanu [25] te ISO/IEC 19795-1 Information technology- Biometric performance testing and reporting – Part 1: Principles and framework first edition 2006-04-01, sastoji se sastoji od pet podsustava [26]:

1. Prikupljanje podataka,

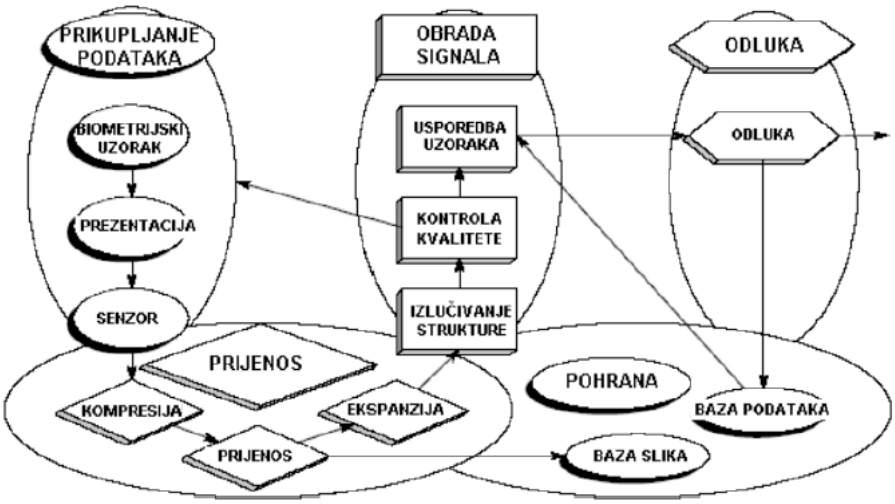
2. Prijenos podataka,

3. Obrada podataka,

4. Pohrana podataka,

5. Donošenje odluke.

Svaki od navedenih podsustava sastoji se također od nekoliko elemenata čija se konfiguracija može prikazati kao na slici 1.



Slika 1 Uopćeni prikaz biometrijskog sustava sa podsustavima [27]

Biometrijski sustavi se danas koriste kroz široku paletu načina prepoznavanja osoba te reguliranja prava pristupa određenim fizičkim prostorima, informacijama, uslugama te ostalim pravima ili prednostima uključujući također modalitete prelaska međunarodnih granica.

Motivi korištenja biometrijskih sustava [11] su različiti te uglavnom podrazumijevaju poboljšanje prikladnosti i efikasnosti pristupnih procedura određenim servisima, redukciju mogućnosti prijevare te poboljšanja percepcije javne te nacionalne sigurnosti.

2.2 Pojam pouzdanosti biometrijskih sustava

Pouzdanost [28], sukladno definiciji standarda ISO/IEC 2382-14:1997[17], jeste sposobnost funkcionalne jedinice sustava za izvršavanje zahtijevane funkcije.

Pouzdanost je navedena kao jedna od komponenti trijade Pouzdanost[18], Dostupnost ili Raspoloživost[19], Održivost[20]

1. Pouzdanost predstavlja vjerojatnost rada sustava bez otkaza,

[17] ISO/IEC 2382-14:1997 Information technology-Vocabulary-Part 14: Reliability, maintainability and availability

[18] Izvorno: Reliability

[19] Izvorno: Availability

[20] Izvorno: Održivost

Činitelji definiranja parametra pouzdanosti:

a) MTFB – (Izvorno: mean time between failure), srednje vrijeme između otkaza je parametar koji uzima u obzir vremenski period u kojem je sustav u funkciji
b) MTTF-(Izvorno: mean time to failure), srednje vrijeme do prvog otkaza je parametar koji uzima u obzir vrijeme funkcioniranja sustava do prvog otkaza

2. Dostupnost ili raspoloživost predstavlja mogućnost korištenja sustava onda kada je to potrebno,

Činitelji [29] definiranja parametra raspoloživosti:

c) Vrijeme neaktivnosti[21] predstavlja vrijeme kada sustav nije u funkciji iz različitih razloga kao što su: održavanje, ažuriranje, pad energetskog sustava itd.
d) Vrijeme aktivnosti[22] predstavlja vrijeme kada je sustav u funkciji,
e) Operativna raspoloživost[23] predstavlja vrijeme u kojem je sustav dostupan korisnicima te se izražava kao odnos:

$$Operativna\_raspolozivost = \frac{Vrijeme\_aktivnosti}{Vrijeme\_aktivnosti + Vrijeme\_neaktivnosti}$$

3. Sposobnost održavanja predstavlja mogućnost efikasnog održavanja sustava u slučaju otkaza (korektivno održavanja) ili tijekom njegovog perioda operativnosti radi smanjenja vjerojatnosti otkaza (preventivno održavanje). Činitelji parametra sposobnost održavanja:

f) Srednje vrijeme uspostavljanja operativnog statusa sustava, MTTR[24],
g) Maksimalno vrijeme uspostavljanja operativnog statusa sustava, MaTTR[25]

Standard ISO 17359:2003[26] definira otkaz kao uvjet u kojemu sustav ili dio istoga prezentira nenormalno ponašanje. Pouzdanost je definirana kao zahtjev br.6 navedenog standarda koji zahtijeva izradu blok-dijagrama pouzdanosti sa definiranjem kritičnosti pojedinih komponenti sustava glede konteksta pouzdanosti cijelog sustava.

Pouzdanost [30] ,kao jedan od ključnih parametara pri razmatranju kvalitete performansi biometrijskih sustava [31] , pojavljuje se u raščlambama parametara kvalitete u skoro svim

[21] Izvorno: Downtime

[22] Izvorno: Uptime

[23] Izvorno: Operational availability

[24] Izvorno: Mean time to recovery

[25] Izvorno: Maximum time to recovery

[26] ISO 17359:2003 – Condition monitoring and diagnostic of machines – General guidelines - First edition 2003-07-01

Činiteljima funkcionalnosti sustava, npr. ISO/IEC FDIS 9126-1[27], definira pouzdanost kao komponentu Modela kvalitete softvera u točki 6.2 koji može biti predstavljen kao niz parametara:

1. Funkcionalnost,
2. Pouzdanost,
3. Mogućnost korištenja,
4. Efikasnost,
5. Mogućnost održavanja,
6. Prenosivost.

2.3 Pojam evaluacije pouzdanosti biometrijskih sustava

Evaluacija pouzdanosti biometrijskih sustava [32] ima višestruke aspekte razmatranja, glede rezultata procesa funkcioniranja biometrijskih sustava kao sustava identifikacije ili verifikacije, posebice uzimajući u obzir vjerojatnosni karakter rezultata primarne funkcije sustava, tj. donošenja odluke koja za ishod ima određeni rezultat podudaranja ili nepodudaranja unešenih biometrijskih uzoraka/karakteristika sa pohranjenim podacima.

Vjerojatnosno svojstvo odluke sustava [33] često nije predmet rasprava ili tvrdnji brojnih znanstvenih radova iz ovog područja iz razloga što donesena odluka je samo određena vjerojatnost podudaranja ili nepodudaranja unesenih podataka, biometrijskih karakteristika osobe, sa onima već pohranjenima u sustav. Takovo svojstvo biometrijske [19] sustave čini posebno osjetljivim na otvorene ili prikrivene pokušaje podrivanja razina povjerenja u njihovu pouzdanost te sama diskusija o vjerojatnosnoj nesigurnosti rezultata može na određeni način sugerirati te ukazivati na nepouzdanost biometrijskih sustava.

Problematike evaluacije pouzdanosti biometrijskih sustava uključuju tehnološki a također i društveni kontekst njihove primjene [34] pa se izazovi koji se postavljaju pred evaluacijske modele mogu sagledati sa dva različita gledišta:

1. Uporabe biometrijskih sustava kao sigurnosnih mehanizama [35] za zaštitu drugih sustava,

[27] ISO/IEC FDIS 9126-1 - Information technology – Software product quality – Part 1: Quality model

2. Njihovih vlastitih slabosti, ograničenja te ranjivosti [5] uzimajući u obzir društveni kontekst razloga njihove primjene.

Napominjući vjerojatnosno svojstvo mehanizama odluke biometrijskog sustava dolazimo do pretpostavke da biometrijski sustavi [36] mogu biti definirani kao skoro-točni ili skoro-pouzdani sustavi. Uzevši u obzir sve navedeno možemo doći do zaključka da je evaluacija pouzdanosti biometrijskih sustava jedna od determinanti percepcije kvalitete performansi biometrijskih sustava koja treba omogućiti daljnju općeprihvaćenu primjenu. Analiza utjecaja na pouzdanost biometrijskih sustava trebala bi uključivati sljedeće sastavnice pojavnosti biometrijskih sustava:

- Tehničkih komponenti sustava od kojih je sačinjen hardver biometrijskog sustava,
- Softverskih komponenti koje podrazumijevaju također algoritme kreiranja, pretvaranja osobnih karakteristika u digitalne modela te poredbe pohranjenih karakteristika sa onima koje osoba prezentira sustavu,
- Okoline u kojoj je biometrijski sustav lociran,
- Dizajna aplikacije za komunikaciju sa korisnikom,
- Dizajna samog biometrijskog sustava opisanog kao ergonomski utjecaj na korisnika,
- Uvjeta koji utječu na interakciju korisnika sa biometrijskim sustavom, itd.

POGLAVLJE III

3 DOSADAŠNJA ISTRAŽIVANJA IZ PREDMETNE DOMENE

Sukladno iznešenome u prethodnim Poglavljima mogu se izlučiti osnovna područja istraživanja pouzdanosti biometrijskih sustava koja obuhvaćaju tehnologiju biometrijskih sustava, okolinu biometrijskih sustava te korisnika biometrijskih sustava.

3.1 Područje pouzdanosti tehnologije biometrijskih sustava

Ovo područje predstavlja pokušaje modeliranja problematika pouzdanosti hardvera te softvera biometrijskih sustava.

I. Modeli pouzdanosti hardvera [37] ,

Uvidom u znanstvene radove objavljene iz ovog područja, ovi modeli se bave problematikama modeliranja stohastičkih procesa koristeći funkcije međuovisnosti: serijske, paralelne, kombinirane te „k“ od „n“ ovisnosti komponenata sustava kroz analizu otkaza preko metoda [38]: Grananja pogrešaka[28] , Petrijevih mreža[29], Markovljevih lanaca[30] [28] te Mreža aktivnosti[31] sa svim prednostima i ograničenjima sukladno sugestijama autora [29] U praksi primijenjen je ,naveden u prethodnom poglavlju, standard ISO/IEC 2382-14:1997 koji definira pouzdanost kao: “sposobnost, funkcionalne jedinice sustava, za izvršavanje zahtijevane funkcije“.

U Poglavlju 2.2 pojašnjeni su detalji predmetne terminologije vezane uz elemente pouzdanosti hardvera.

[28] Izvorno: Fault trees

[29] Izvorno: Petri nets

[30] Izvorno: Markov chains

[31] Izvorno: Activity nets

II. Modeli pouzdanosti softvera [39]

Ovakovi modeli predmet su velikog broja znanstvenih radova koji opisuju modele pouzdanosti utemeljene na stanju [40], na putanjama, aditivne modele [41] te modele propagiranja pogreške kroz sustav.

U praksi je također primijenjen standard ISO/IEC FDIS 9126-1[32], koji definira pouzdanost kao "jedan od ključnih faktora kvalitete softvera kao proizvoda te kao sposobnost softvera za zadržavanje specificiranog razinaa performansi kada se koristi u specificiranim uvjetima".

Podkategorije termina pouzdanosti softvera [42] ,sukladno definicijama navedenog standarda, mogu se definirati kroz sljedeće karakteristike sustava [43]:

-**Zrelost** – Sposobnost izbjegavanja cjelokupnog otkaza kao rezultata otkaza unutar softvera .

-**Tolerancija na otkaz** – Sposobnost zadržavanja specificiranog razinaa performansi u slučajevima otkaza softvera ili kompromitiranja specificiranog sučelja. Specificirani razina performansi može uključivati i tzv. sposobnost sigurnog otkaza.

-**Popravljivost** – Sposobnost ponovnog uspostavljanja specificiranog razinaa performansi te oporavak podataka koji su direktno povezani s otkaznim stanjem.

-**Ispunjavanje zahtjeva po pitanju pouzdanosti** – Sposobnost ispunjavanja zahtjeva standarda, konvencija ili regulative povezane s pitanjima pouzdanosti.

Skupni termin koji objedinjava zahtjeve zrelosti, tolerancije na otkaz te popravljivosti naziva se dostupnost koja može biti definirana kao sposobnost dolaska u stanje funkcionalnosti u određenom vremenskom periodu pod određenim uvjetima korištenja.

3.2 Područje pouzdanosti performansi biometrijskih sustava

Ovo područje također je pokriveno obiljem znanstvenih radova te je analizom dostupne literature moguće izlučiti sljedeće odrednice: Ključne aspekte efikasnosti performansi biometrijskih sustava predstavljaju; stopa pogrešaka prilikom procesa prepoznavanja biometrijskih karakteristika osoba, propusnost sustava, brzina izvršavanja operacija, troškovi

[32] ISO/IEC FDIS 9126-1- Software quality model

funkcioniranja i održavanja sustava, sigurnost podataka i privatnosti, uporabljivost, prihvaćanje od strane korisnika. Uopćeno gledano efikasnim sustavom može se smatrati onaj sustav koji ima ujednačen omjer utjecaja svih navedenih parametara kao što npr. stopa pogreške prepoznavanja uzorka može biti smanjena povećanjem vremena za uzorkovanje što opet može povećati vrijeme korištenja sustava, povećati troškove, a smanjiti razina prihvaćanja korisnika.

Stope pogrešaka [44] biometrijskih sustava pojednostavljeno mogu biti definirane preko sljedećih parametara:

- stopa pogrešnog podudaranja - FMR[33]
  Ovaj parametar predstavlja vjerojatnost da sustav korisnika zamjeni s nekim drugim korisnikom čiji su podaci uneseni u sustav ili da je pogrešan uzorak prepoznat kao validan.

- stopa pogrešnog nepodudaranja - FNMR[34]
  Ovaj parametar predstavlja vjerojatnost da sustav ne prepozna korisnika čiji su podaci uneseni u sustav ili da korektan uzorak nije prepoznat kao validan.

  Ova dva parametra opisuju pogreške koje su vezane uz proces usporedbe i prepoznavanja uzoraka te su usko povezani s parametrima FAR[35] stopa pogrešnog prihvaćanja te FRR[36] stopa pogrešnog neprihvaćanja.

  Sukladno gore navedenome vjerojatnost prepoznavanja pravog uzorka kao validnog jeste (1-FNMR) a vjerojatnost neprepoznavanja pogrešnog uzorka jeste (1-FMR).

- stopa pogrešnog uzimanja uzorka - FTA[37]
  Ova vrsta pogreške javlja se tijekom procesa unošenja biometrijske karakteristike u sustav te predstavlja vjerojatnost da će doći do pogreške tijekom procesa. Razlozi mogu biti različiti : nemogućnost unošenja zbog smetnji iz okoline ili samog korisnika, nedovoljna kvaliteta uzorka itd. FTA može biti korigiran smanjenjem zadanog praga kvalitete unosa uzoraka ili boljom kontrolom uvjeta u okolini sustava.

[33] Izvorno: false match rate

[34] Izvorno: false non match rate

[35] Izvorno: false acceptance rate

[36] Izvorno: false rejection rate

[37] Izvorno: failure to acquire rate

- stopa pogrešnog pohranjivanja uzorka - FTE ili FER[38]

  Slično kao i FTA ova vrsta pogreške predstavlja vjerojatnost da proces uzimanja i pohrane referentnih uzoraka neće biti uspješan zbog razloga sličnih onima iz opisa FTA parametra. Što se tiče pragova za prepoznavanje kvalitete uzoraka FTE posjeduje uobičajeno veću vrijednost praga radi garancije kavalitete referentnog uzorka dok posljedično FTA ima manji prag kvalitete.

Sukladno navedenome smatra se da je vrijednost navedenih parametara od 0,01 (1%) vrijednost pouzdanih sustava [45].

3.3 Područje pouzdanosti korisnika te okoline uporabe sustava

Identifikacija, parametrizacija te integriranje aspekata pouzdanosti biometrijskih sustava s onima koji su povezani s aspektima izvan domene tehnologije [46] te performansi biometrijskih sustava kao što su: Korisničke motivacije, motivacije primjene, okolina primjene te uporabljivost sustava predstavlja jedno od relativno neistraženih područja biometrijske znanosti [47]. Pregledom dostupne literature utvrđeno je da je objavljen relativno ograničen broj znanstvenih radova koji se bave temom sistematizacije i parametrizacije sastavnica pouzdanosti izvan prethodno navedenih područja te da se relativno ograničeni broj autora bavi ovim problemom. Okvir za definiranje metode za evaluaciju pouzdanosti biometrijskih sustava koji bi omogućio širu definiciju utjecaja navedenih parametara na pouzdanost biometrijskih sustava nije do sada definiran te bi bio predmet ovoga znanstvenog istraživanja. Temelj za sistematizaciju postojećih znanja te implementaciju novih znanja bila bi računalna ontologija evaluacija pouzdanosti biometrijskih sustava, kao metoda za sistematičan i znanstveno utemeljen prikaz znanja iz domene pouzdanosti biometrijskih sustava. Ontologija bi omogućila veću razumljivost dijeljenog koncepta kroz detaljnu specifikaciju terminologije putem taksonomije, ponovnu uporabu definiranih saznanja te olakšanu komunikaciju među znanstvenicima, organizacijama i drugim zainteresiranim stranama. Određena ograničenja znanstvenog istraživanja odnose se na činjenicu da se radi o relativno nedovoljno istraženom području, te da je malo specijaliziranih znanstvenih časopisa i konferencija čija domena je pouzdanost biometrijskih sustava. Pretraživanje putem specijaliziranog pretraživača sa ontologijama semantičkog Weba, SWOOGLE [48], ukazuje

[38] Izvorno: failure to enroll rate

na nepostojanje ontologija koje se bave problematikama koje su predmet ovoga znanstvenog istraživanja.

POGLAVLJE IV

4 MODELI POUZDANOSTI PRIMJENJIVI NA BIOMETRIJSKE SUSTAVE

U ovom poglavlju dan je pregled modela pouzdanosti primjenjivih na biometrijske sustave.

4.1 Pojam pouzdanosti primjenjiv na biometrijske sustave

Pojavnosti biometrijskih sustava preko kojih se isti manifestira su:

- tehnologija sustava sačinjena od:
  1. hardvera,
  2. softvera.
- funkcija sustava sačinjena od:
  1. performansi sustava,
  2. rezultata funkcije sustava.

Sukladno iznešenome u Poglavlju 2.2 , definicija pouzdanosti u općem smislu predstavlja sposobnost sustava da izvršava i održava svoju operativnu funkciju u rutiniranim okolnostima, ali i u neprikladnim te neočekivanim okolnostima. Uzimajući u obzir specifičnost biometrijskih sustava kao multidisciplinarnih, tada pouzdanost istih ima višestruke aspekte razmatranja, glede rezultata procesa identifikacije ili verifikacije, posebice uzimajući u obzir vjerojatnosno svojstvo rezultata primarne funkcije sustava, donošenja odluke koja za ishod ima određeni rezultat podudaranja ili nepodudaranja uzoraka s pohranjenim podacima.

Teorija pouzdanosti [49] kao opća teorija otkaza sustava razvijena je od strane matematičara Richarda Barlowa[39] , Borisa Gnedenka[40] te Franka Proschana[41].

Prvotno je razvijena da opiše zakonitosti otkaza i starenja kompleksnih vojnih elektroničkih sustava i zahtjeva sustavni pristup te primjenu teorije vjerojatnosti.

[39] Richard E. Barlow (1931-) professor emeritus, University of California, Berkeley, *Reliability and decision making* 1993.

[40] Boris Vladimirovič Gnedenko (1912-1995), *Mathematics and reliability theory* 1982

[41] Frank Proschan (1921-2003)

Teorija pouzdanosti [28] je znanost koja se bavi proučavanjem zakonitosti pojava otkaza tehničkih sustava i njihovih sastavnih elemenata[42]. Sa praktičnog gledišta, pouzdanost sustava može se shvatiti kao svojstvo sustava da radi bez otkaza u određenim uvjetima[43] u određenom vremenskom periodu.

Pouzdanost kao vjerojatnost (broj između 0 i 1 ili 0% i 100%) može se predstaviti kao odnos između broja uspješnih zadataka i ukupnog broja zadataka u vremenu specificiranom za funkcioniranje sustava tj.

$$\underline{R}(t) = \frac{n_1(t)}{n(t)}, \tag{1}$$

gdje je: $\underline{R}(t)$ - procjena pouzdanosti,

$n_1(t)$ - broj uspješnih zadataka u vremenu *t*,

$n(t)$ - ukupan broj izvedenih zadataka u vremenu *t*,

t - vrijeme specificirano za funkcioniranje sustava.

Vrijednost $\underline{R}(t)$ predstavlja procijenjenu pouzdanost uslijed toga što je broj zadataka *n(t)* konačan. Zato se stvarna pouzdanost *R(t)* dobije kada broj zadataka *n(t)* teži beskonačnosti.

$$R(t) = \lim_{n(t)\to\infty} \underline{R}(t). \tag{2}$$

Nepodudarnost prikazanih veličina *R(t) i* $\underline{R}(t)$ zahtijeva uvođenje pojma razina povjerenja. Statističke procjene se obično predstavljaju u vidu intervala, uz vjerojatnost ili povjerenje da će stvarna vrijednost biti u tom intervalu. Krajnje točke tog intervala zovu se granice povjerenja i mogu se izračunati kada je poznata distribucija danog parametra.

[42] Podsustava, dijela, sklopa itd.

[43] Režimi rada, okolina, uvjeti eksploatacije itd.

1 2 n

4.2 Pregled modela pouzdanosti primjenjivih na biometrijske sustave

Sukladno iznešenome u Poglavlju 3 postoji obilje znanstvenih radova koji se bave matematičkim modelima kvalitativne ocjene pouzdanosti tehnologije biometrijskih sustava koja se manifestira kroz ugrađeni hardver i softver [39].

4.2.1 Modeli pouzdanosti hardvera

Prilikom analize pouzdanosti nekog kompleksnog sustava [50] , možemo taj sustav rastaviti na funkcionalne cjeline koje mogu predstavljati podsustave, uređaje, elemente i slično. Pouzdanost takvog sustava [51] uopćeno uzima u obzir kontinuiranu aktivnost svih komponenti sustava koje mogu imati bilo koju kombinaciju međusobnih veza.

Uopćena jednadžba pouzdanosti jednog takvog sustava može se definirati kao

$$R_s = \prod_{i=1}^{n} R_i \ , \tag{3}$$

gdje je

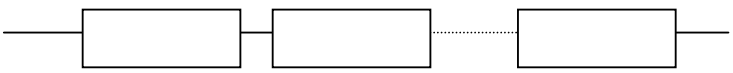
R_s - pouzdanost sustava

R_i - pouzdanost komponenti sustava

n - broj komponenti sustava

4.2.1.1 Serijska konfiguracija komponenti sustava

Serijska konfiguracija [28] komponenti vrlo je česta u analizi pouzdanosti. Blok-dijagram pouzdanosti za ovu konfiguraciju prikazan je na slici 2:



Slika 2 Serijska konfiguracija komponenti biometrijskog sustava

Svaki element prikazan na slici 2 mora uspješno funkcionirati da bi sustav koji se sastoji od n elemenata uspješno funkcionirao.

1

2

Pouzdanost sustava može se dobiti i razmatranjem vjerojatnosti otkaza elemenata tj. kao relacija $R=1-P(\overline{A})$. Sustav će otkazati ako otkaže bilo koji element, te je pouzdanost sustava

i

$$R = 1 - P(\overline{A}_1 \cup \overline{A}_2 \cup \overline{A}_3 \cup ... \cup \overline{A}_n) = 1 - Q, \quad (4)$$

gdje je

$\overline{A}_n$ - otkaz komponente sustava,

P - vjerojatnost,

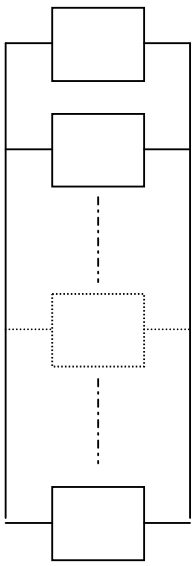
Q - nepouzdanost sustava.

4.2.1.2 Paralelna konfiguracija komponenti sustava

Paralelna konfiguracija komponenti sustava je jedna od mogućih konfiguracija a susreće se u dva slučaja:

- kao rezultat strukture samog sustava
- kao posljedica konstruktivnog rješenja kada se radi o povećavanju pouzdanosti ugrađivanjem rezervnih elemenata koji se uključuju kad neki element otkaže.

Blok-dijagram pouzdanosti paralalne konfiguracije elemenata sustava prikazan je na slici 3.



Slika 3 Paralelna konfiguracija komponenti biometrijskog sustava

A_{11} A_{12} A_{1n}

A_{21} A_{22} A_{2n}

A_{m1} A_{m2} A_{mn}

Sustav će otkazati ako u njemu otkažu svi elementi te se pouzdanost dobije kad od 1 odbijemo nepouzdanost tj. vjerojatnost otkaza sustava u slučaju paralelne konfiguracije (koja je jednaka vjerojatnosti presjeka događaja $\bar{A}_1, \bar{A}_2, ..., \bar{A}_n$). Tako da imamo da je

$$\begin{aligned} R &= 1 - Q = 1 - P(\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap ... \bar{A}_n) \\ &= 1 - P(\bar{A}_1) \cdot P(\bar{A}_2 / \bar{A}_1) \cdot P(\bar{A}_3 / \bar{A}_1 \cap \bar{A}_2) \cdot ... P(\bar{A}_n / \bar{A}_1 \cap \bar{A}_2 \cap ... \cap \bar{A}_{n-1}) \end{aligned} , \tag{5}$$

gdje je *P(B|A)* tzv. uvjetna vjerojatnost, tj. vjerojatnost događaja B uz uvjet da se ostvario događaj A, koja se računa prema formuli

$$P(B / A) = \frac{P(B \cap A)}{P(A)} . \tag{6}$$

Ako su događaji međusobno neovisni tada iz gornje jednadžbe slijedi:

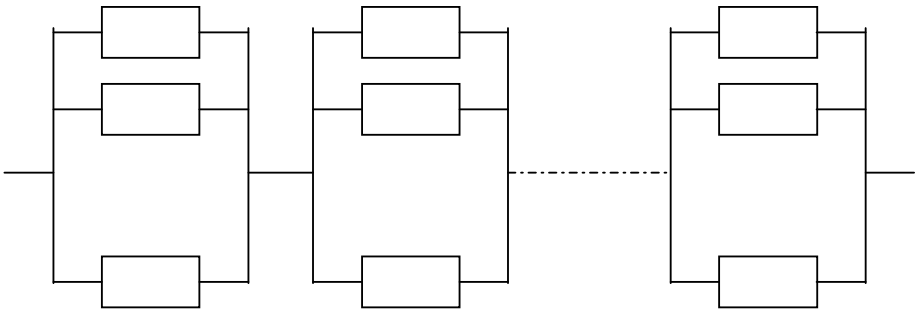
$$R = 1 - P(\bar{A}_1) \cdot P(\bar{A}_2) \cdot ... P(\bar{A}_n) = 1 - \prod_{i=1}^{n} P(\bar{A}_i) , \tag{7}$$

U slučaju da su svi elementi identični pri čemu je pouzdanost svakog od njih možemo označiti sa *p* a nepouzdanost će tada biti označena sa *1-p* tada iz gornje jednadžbe dobivamo:

$$R = 1 - (1 - p)^n . \tag{8}$$

4.2.1.3 Paralelno-serijska konfiguracija komponenti sustava

Na slici 4 prikazan je slučaj kada je serijski vezano *n* grupa koje se sastoje od jednakog broja *m* paralelno vezanih komponenti sustava.



Slika 4 Paralelno-serijska konfiguracija komponenti biometrijskog sustava

Ako su svi otkazi neovosni jedan o drugogome, tada je pouzdanost *j*-te grupe, po analogiji s formulom (6), jednaka:

A_{11} A_{12} A_{1n}

A_{21} A_{22} A_{2n}

$$R_j = 1 - P(\overline{A}_{1j}) \cdot P(\overline{A}_{2j}) \cdot ... P(\overline{A}_{mj}) = 1 - \prod_{i=1}^{m} P(\overline{A}_{ij}) \ , \qquad (9)$$

A_{m1} A_{m2} A_{mn}

gdje je

$\overline{A}_{ij}$ - događaj da je *i*-ti element u *j*-toj grupi neispravan.

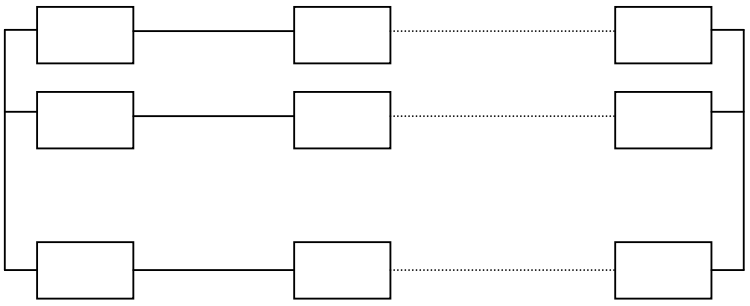
Ako su sve komponente identične, a vjerojatnost uspješnog rada svakog od njih *P* iz (9) se dobije da je:

$$R = \prod_{j=1}^{n} \left[1 - (1-p)^m \right] = \left[1 - (1-p)^m \right]^n \ . \qquad (10)$$

4.2.1.4 Serijsko-paralelna konfiguracija komponenti sustava

Za serijsko-paralelnu konfiguraciju, gdje su sve komponente vezane paralelno a grupe komponenti serijski, najprije se izračuna pouzdanost svake grupe, pa se onda množenjem tih vrijednosti dobije pouzdanost sustava. Procedura izračuna pouzdanosti kada se broj komponenti u grupama razlikuje ista je kao i kad je broj komponenti u grupama isti.

Na slici 5 prikazana je serijsko-paralelna konfiguracija sa po *m* pravaca i sa po *n* elemenata na svakom pravcu.



Slika 5 Serijsko-paralelna konfiguracija komponenti biometrijskog sustava

Da bi odredili pouzdanost ovog sustava najprije ćemo odrediti pouzdanost *i*-tog pravca.

Po analogiji kao u formuli (9) slijedi da je

$$R_i = P(A_{i1}) \cdot P(A_{i2}) \cdot \ldots \cdot P(A_{in}) = \prod_{j=1}^{n} P(A_{ij}) \quad , \tag{11}$$

pri čemu je *Ri* pouzdanost *i*-tog pravca, a broj pravaca je *i=1,2,...,m,* dok je broj komponenti na svakom pravcu *j=1,2,...,n*.

Događaji *Aij* znače da je *j*-ti element na *i*-tom pravcu funkcionirao ispravno.

Ako su svi elementi identični sa vjerojatnošću uspješnog rada p , tada je pouzdanost sustava:

$$R = 1 - \prod_{i=1}^{m} \left(1 - p^n\right) = 1 - \left(1 - p^n\right)^m \ . \tag{12}$$

4.2.2 Modeli pouzdanosti softvera

Uzimajući u obzir autore Goševa et.al. [40],[52] pouzdanost sustava jedna je od najvažnijih metrika za ocjenu kvalitete istoga. Za procjenu pouzdanosti sukladno sa ciljem rada uzeti su u obzir modeli za sustave[44] sačinjene od više komponenti [31], [39]. U modelima sustava sačinjenih od komponenti [41], svaka komponenta promatrana je kao samostalna logička jedinica koja ima vlastiti utjecaj na strukturu sustava. Prilikom proučavanja modela [53] pouzdanosti softvera [54] potrebno je uzeti u obzir arhitekturu samog softvera [55] sustava te istu modelirati kao [56]:

-Diskretni vremenski Markovljev Lanac[45],

-Kontinuirani vremenski Markovljev Lanac[46],

-Semi-Markovljev proces[47].

Modeli pouzdanosti softvera kroz publicirane znanstvene radove se modeliraju također korištenjem Bayesovih mreza [57,61] .

[44] Izvorno: Component-based systems

[45] Izvorno: Discrete Time Markov Chain - DTMC

[46] Izvorno: Continuous Time Markov Chain - CTMC

[47] Izvorno: Semi Markov Process - SMP

4.2.2.1 Modeli temeljeni na stanju sustava

Ovi modeli koriste diskretne, kontinuirane vremenske Markovljeve lance te semi-Markovljeve procese za definiranje karakteristika aplikacijske arhitekture. Pretpostavka modela jeste da gustoća otkaza komponenti i veza među njima ovisi o vremenu te da je promjenjiva s vremenom.

Ovi modeli također se mogu podjeliti na

-kompozitne, koji kombiniraju arhitekturu softvera sa modalitetom[48] događanja otkaza sustava,

-hijerarhijske, koji rješavaju prvo model arhitekture softvera pa se na njega primijeni modalitet događanja otkaza sustava.

Cheung model [52]

Ovaj model može biti opisan kroz dva apsorpcijska stanja *C*-korektan izlaz iz sustava i *F*-otkaz. Matrica vjerojatnosti *P* je predstavljena putem predviđanja vjerojatnosti $\widehat{P}$.

Početna tranzicijska vjerojatnost p_{ij} transformira se u izraz $R_{ij}p_{ij}$ koji predstavlja vjerojatnost da će modul *i* proizvesti korektan rezultat te da će kontrola biti transferirana na modul *j*.

Prijelaz sa izlaznog stanja *n* u stanje *C* kreirano je tranzicijskom vjerojatnošću R_n te predstavlja korektno izvršenje zadatka.

Otkaz komponente *i* razmatran je prijelazom u stanje *F* sa tranzicijskom vjerojatnošću $\left(1-R_i\right)$.

Pouzdanost softvera u ovom slučaju je vjerojatnost dolaska u apsorpcijsko stanje *C* diskretnog Markovljevog lanca DTMC.

[48] Izvorno: Failure Behavior

Gdje je

$Q^k(1,n)$ - vjerojatnost prijelaza u stanje n od 1 preko k tranzicija koje mogu varirati od $(0 \to \infty)$), što se može prikazati izrazom skupa stanja *S*:

$$S = 1 + Q + Q^2 + Q^3 + ... + Q^k = \sum_{k=0}^{n} Q^k = (1-Q)^{-1} \quad . \tag{13}$$

Ukupna pouzdanost sustava može biti prikazana izrazom:

$$R = S(1,n)R_n \quad . \tag{14}$$

Ovaj model je integriran u softver Cleanroom Reliability manager za planiranje postupaka certifikacije pouzdanosti softverskog sustava utemeljenog na komponentama.

Laprie model [37]

Arhitektura ovoga sustava je utemeljena na komponentama koje su međusobno povezane i ovisne. Parametri koji opisuju ovaj model mogu se prikazati kako slijedi:

$\frac{1}{\mu_i}$ - srednje vrijeme izvršenja operacije MET[49],

P_{ij} - vjerojatnost da će se komponenta *j* aktivirati iza komponente *i* bez otkaza.

Pretpostavka sustava je da svaka komponenta otkazuje sa konstantnim intenzitetom otkaza λ_i. Model ovoga sustava je na n+1 stanju Kontinuiranog Markovljevog Lanca - CTMC[50] gdje sustav radi sukladno stanjima: $0 \le i \le n,(n+1)$. Stanje $(n+1)$ je apsorpcijsko stanje uslijed pojave otkaza određene komponente.

Pridružena matrica funkcionalnih stanja $B = \left[b_{ij} \right]$ dana je izrazima:

$$b_{ii} = -(\mu_i + \lambda_i), \tag{15}$$

[49] Izvorno: Mean execution time

[50] Izvorno: Continuous time Markov chain

$$b_{ij} = p_{ij} + \mu_{ij} \text{ za } i \neq j \,. \tag{16}$$

Matrica *B* predstavlja sumu dviju matrica (15) i (16) u kojima je:

- Proces funkcioniranja sustava upravljan stanjem B' čije su dijagonale $-\mu_i$ i $p_{ij}\mu_{ij}$.

- Proces otkaza upravljan stanjem B'' čije su dijagonale $-\lambda_i$ i 0.

Model pouzdanosti može biti opisan izrazom za intenzitet otkaza sustava

$$\lambda_s = \sum_{i=1}^{n} \pi_i \cdot \lambda_i \tag{17}$$

Gdje je:

λ_s - Intenzitet otkaza sustava

$\pi = \left[\pi_i \right]$ Vektor vjerojatnosti pripremnog stanja i rješenje od $\pi B' = 0$.

π_i - vremenski interval proveden u stanju *i* bez otkaza.

Kubat model [62]

Sukladno propozicijama ovoga modela sustav je komponiran od *n* modula koji izvršavaju *K* različitih zadataka.

Arhitektura sustava sukladno ovome modelu temelji se na sljedećim pretpostavkama:

-Tranzicije stanja među komponentama slijede zakonitosti Diskretnog Markovljevog Lanca[51] DTMC,

- Zadatak *k* angažirati će komponentu *i* sa vjerojatnošću $q_i(k)$,

- Zadatak *k* angažirati će komponentu *j* nakon izvršenja zadatka komponente *i* sa vjerojatnošću $p_{ij}(k)$,

- Vrijeme boravka zadatka *k* u modulu *i* , ima funkciju gustoće vjerojatnosti[52] $g_i(k,t)$.

[51] Izvorno: Discrete time Markov chain

Sukladno gore navedenim pretpostavkama arhitektura modela za svaki zadatak postaje semi-Markov proces - SMP. Intenzitet otkaza modula ili komponente sustava je λ_i.

Vjerojatnost da se otkaz neće dogoditi tijekom izvršenja zadatka *k* dok je modul u stanju *i* je

$$R_i(k) = \int_0^\infty e^{-\lambda_i t} g_i(k,t)dt\,, \tag{18}$$

Očekivani broj prolaza zadatka *k* kroz modul *i* označen je sa $V_i(k)$ i može biti prikazan na sljedeći način:

$$V_i(k) = q_i(k) + \sum_{i=1}^{n} V_j(k) p_{ji}(k)\,, \tag{19}$$

Vjerojatnost da se neće dogoditi otkaz tijekom izvršenja zadatka k može biti prikazana izrazom

$$V_i(k) = q_i(k) + \sum_{i=1}^{n} V_j(k) p_{ji}(k)\,, \tag{20}$$

Intenzitet otkaza sustava može biti predstavljen izrazom

$$\lambda_s = \sum_{k=1}^{K} r_k \left[1 - R(k)\right]. \tag{21}$$

Gdje je

r_k - stopa izvršivosti zadatka k.

Gokhale et al. Model [63]

Ovaj model koristi alat Regression Test Suite za određenje pouzdanosti komponenti softvera a pri tome ponašanje komponenti u otkazu slijedi zakonitosti diskretnog Markovljevog lanca DTMC. Za određivanje tranzicijskih vjerojatnosti prijelaza iz jednog stanja u drugo p_{ij} koristi se analitički alat ATAC[53].

[52] Izvorno: Probability density function - pdf

[53] Izvorno: Advanced Test Automation for Complex and Highly-Configurable Software-intensive Systems dostupno na https://itea3.org/project/atac.html (09.01.2015 u 18.00)

Očekivano vrijeme boravka u modulu *i* za prolazak t_i računa se kao proizvod očekivanog vremena izvršenja u svakom bloku te broja blokova unutar modula.

Ponašanje u otkazu svake komponente sustava slijedi zakonitosti nehomogeni Poisonov proces NHPP[54] pri čemu se koristi intenzitet otkaza ovisan o vremenu $\lambda_i(t)$. Intenzitet otkaza je određen mjerenjima otkaza pojedinih blokova unutar modula koristeći pristup gustoće otkaza.

Očekivani broj prolaza kroz modul *i* , označen kao V_i , može biti izračunat sukladno izrazu

$$V_i = q_i + \sum_{j=1}^{n} V_j p_{ji} , \tag{22}$$

Gdje je

q – vektor vjerojatnosti početnog stanja.

Pouzdanost modula *i* , uz poznati intenzitet otkaza $\lambda_i(t)$ i ukupno očekivano vrijeme $V_i t_i$ provedeno u modulu i radi izvršenja aplikacije može biti opisana sljedećim izrazom:

$$R_i = e^{\int_0^{V_i t_i} \lambda_i(t) dt} , \tag{23}$$

Tada pouzdanost cijele aplikacije postaje :

$$R = \prod_{i=1}^{n} R_i . \tag{24}$$

Ledoux model [64]

Ovaj model je recentna ekstenzija modela Littlewood u smislu uključivanja utjecaja otkaza na proces izvršenja zadatka te kašnjenje u procesu povratka u operativno stanje.

Arhitektura sustava pretpostavlja softver sastavljen od kompleta od *C* komponenti modeliran zakonitostima kontinuiranog Markovljevog lanca CTMC sa tranzicijskim stopama q_{ij}. Ponašanje u otkazu uključuje dva tipa otkaza, i to Primarni i Sekundarni otkaz.

Primarni otkaz podrazumijeva pauzu u izvršenju zadatka nakon koje se operativno stanje uspostavlja sa određenim kašnjenjem. Sekundarni otkaz ne utječe na funkcionalnost softvera

[54] Izvorno: Non homogeneous Poisson process

budući da se pretpostavlja uspostava funkcionalnosti putem automatskog restarta nakon pojave otkaza.

Za aktivnu komponentu c_i primarni otkaz se događa sa konstantnim intenzitetom otkaza λ'_i dok se sekundarni otkaz, opisan kao Poisonov proces, događa sa intenzitetom otkaza λ''_i .

Prelazak nadzora izvršenja softvera sa komponente *i* na komponentu *j* može imati za posljedicu događanje primarnog otkaza sa vjerojatnošću v'_{ij} a sekundarnog otkaza sa vjerojatnošću v''_{ij} .

Ako označimo sa R skup ponovnih uspostavljanja operativnog stanja tada polje stanja sustava postaje $C \cup R$ a kontinuirani Markovljev lanac CTMC modelira prelaske iz stanja operativnosti u stanja u otkazu i obratno.

4.2.2.2 Modeli temeljeni na putanjama sustava

Ova klasa modela utemeljena je na istim principima kao i klasa modela prethodno opisana sa izuzetkom pristupa kombiniranju arhitekture sustava sa ponašanjem otkaza koje može biti opisano kao utemeljeno na putanji izvršenja naredbi softvera. Sustav računa pouzdanost u ovisnosti o putanjama softvera tijekom izvršenja.

Shooman model [65]

Ovaj model je jedan od prvih modela koji uzima u obzir pouzdanost modularnih komponenti softvera uvođenjem pristupa ovisnosti o putanjama izvršenja naredbi te učestalosti kojima se pojedine putanje pojavljuju prilikom izvršenja naredbi.

Arhitektura ovoga modela pretpostavlja različite putanje sa frekvencijama f_i sa kojima se određena putanja *i* pojavljuje prilikom izvršenja određenih naredbi sustava.

Vjerojatnost otkaza u putanji *i*, q_i ,za svako izvršenje naredbe opisuje ponašanje sustava u otkazu.

Ukupni broj otkaza n_f u N izvršenja naredbi u *m* putanja *i* dan je sljedećim izrazom

$$n_f = \sum_{i=1}^{m} N \cdot f_i \cdot q_i \,, \tag{25}$$

gdje je

$N \cdot f_i$ - broj ukupnih prolazaka putanjom *i*,

q_i - vjerojatnost otkaza u putanji *i,*

Vjerojatnost otkaza sustava q_s opisana je sljedećim izrazom

$$q_s = \lim_{N \to \infty} \frac{n_f}{N} = \sum\nolimits_{i=1}^{m} f_i \cdot q_i \,. \tag{26}$$

Krishnamurthy and Mathur model [66]

Ovaj model koristi kombinaciju arhitekture i ponašanja otkaza na način da prvo uzima u obzir procjenu vjerojatnosti otkaza utemeljenu na redoslijedu aktiviranja komponenti sustava za svako izvršenje naredbi te računa srednju vrijednost otkaza za sve putanje tijekom izvršenja svih naredbi sustava te tako dolazi do procjene pouzdanosti cijelog sustava.

Arhitektura ovoga modela obilježena je praćenjem redoslijeda izvršavanja komponenti u putanjama tijekom izvršavanja naredbi sustava.

Ponašanje otkaza obilježeno je pretpostavkom da svaka komponenta ima svoju pouzdanost R_m. Ovaj model pretpostavlja serijsku ovisnost redoslijeda izvršenja komponenti tijekom određene putanje izvršenja naredbi softvera.

Pojedine komponente prelaze u stanje otkaza neovisno o drugim komponentama sustava te je ukupna pouzdanost tijekom izvršenja određene putanje proizvod pouzdanosti svih komponenti tijekom putanje.

Praćenje redoslijeda izvršenja komponenti određenog programa *P* za neki test *TC*[55] označen sa skupom vrijednosti *M(P,TC)*, predstavlja redoslijed izvršenja komponenti *m* kada je program *P* aktivan tijekom testa *TC*.

Pouzdanost određene putanje programa *P* kada je u tijeku izvršenje određene naredbe testa $TC \in TS$; a *TS*[56] predstavlja testni komplet ; dana je sljedećim izrazom:

$$R_t = \prod_{\forall m \in M(P,TC)} R_m , \tag{27}$$

Procjena pouzdanosti programa *P* unutar skupa *TS* jeste:

$$R = \frac{\sum_{\forall TC \in TS} R_{TC}}{\left|TS\right|} . \tag{28}$$

Yacoub, Cukic and Ammar model [67]

Ovaj model je podesan za specifične analize temeljene na izvršenju određenih predefiniranih scenarija. Scenario predstavlja set interakcija komponenti iniciranih specifičnim inputima.

Arhitektura ovoga modela predstavlja vjerojatnosni model nazvan Grafikon ovisnosti komponenata CGD[57]. Čvor n_i unutar CDG modelira izvršenje zadatka komponente sa srednjim vremenom izvršenja t_i . Vjerojatnost prijelaza p_{ij} pridružena je svakoj usmjerenoj ivici[58] *e* koja modelira stanje čvora n_i te prijelaz iz čvora n_i na n_j .

CDG ima dva dodatna čvora a to su: *s*-startni čvor i *t*-terminacijski čvor.

Proces otkaza podrazumijeva pouzdanosti pojedinačnih komponenti R_i te prijelazne pouzdanosti $(1-v_{ij})$ pridružene čvoru n_i , sa prijelazom sa čvora n_i na n_j .

[55] Izvorno: Test trace

[56] Izvorno: Test set

[57] Izvorno: Component dependency graph

[58] Izvorno: Edge

Analiza pouzdanosti se temelji na algoritmu prijelaza grananja TTA[59] a rezultat je procjena pouzdanosti softvera kao funkcije pouzdanosti komponenti i veza među njima.

Algortam ekspandira sve grane CDG-a počevši od startnog čvora. Dubina svake putanje prestavlja redoslijed izvršenja komponenti te je predstavljen kao proizvod pojedinačnih pouzdanosti komponenti.

4.2.2.3 Aditivni modeli [28]

Klasa ovih modela ne uzima u obzir eksplicitnu arhitekturu sustava nego je fokusirana na procjenu pouzdanosti cijelog sustava koristeći podatke o otkazima komponenti sustava. Ovi modeli analiziraju procese rasta pouzdanosti softvera.

Ovi modeli se nazivaju aditivni pod pretpostavkom da je pouzdanost komponenti moguće predstaviti nehomogenim Poissonovim procesima NHPP. Sukladno tomu intenzitet otkaza može biti predstavljen kao zbroj intenziteta otkaza komponenti.

Xie and Wohlin model [68]

Ovaj model pretpostavlja da je softver sačinjen od *n* komponenti te sukladno tomu pretpostavlja se serijska ovisnost komponenti koja za rezultat ima otkaz cijelog sustava u slučaju otkaza bilo koje komponente.

Ako je pouzdanost komponenti modelirana sa NHPP sa intenzitetom otkaza $\lambda_i(t)$, tada je intenzitet otkaza cijelog sustava

$$\lambda_s(t) = \lambda_1(t) + \lambda_2(t) + ...\lambda_n(t) = \sum_{i=1}^{n} \lambda_i(t)\,, \tag{29}$$

Rezultat je očekivani kumulativni broj otkaza sustava u vremenu *t*, poznat kao funkcija srednje vrijednosti $\mu_s(t)$, te je dan sljedećim izrazom

$$\mu_s(t) = \sum_{i=1}^{n} \mu_i(t) = \int_0^t \sum_{i=1}^{n} \lambda_i(t)dt\,. \tag{30}$$

[59] Izvorno: Tree traversal algorithm

Everett model [69]

Pristup koji je karakterističan za ovaj model jeste fokusiranost na problematike definiranja pouzdanosti pojedinačnih komponenti sustava. Pouzdanost pojedinačnih komponenti je analizirana korištenjem modela Produženog Vremena Izvršenja[60] EET. Parametri modela EET mogu biti određeni direktno iz svojstava softvera koji se analizira te informacija o testiranju sustava i podataka o stresu komponenti tijekom operativne aktivnosti softvera.

Svojstva koja utječu na pouzdanost komponenti uopćeno se mogu podijeliti na

- Statička svojstva,
- Dinamička svojstva.

Tijekom funkcioniranja softvera faktor stresa za komponente jeste vrijeme provedeno u izvršenju zadatka. Ova vrsta pristupa zahtjeva čuvanje podataka o kumulativnom vremenu aktivnosti komponenti tijekom izvršenja zadataka.

4.2.3 Pouzdanost funkcionalnosti sustava [44]

Operativna uporaba biometrijskog sustava podrazumjeva unos i obradu biometrijskih karakteristika korisnika sustava. Biometrijska karakteristika jedan je od važnijih faktora koji utječu na pouzdan rad biometrijskog sustava. Pod biometrijskom karakteristikom podrazumijeva se fizička ili ponašajna karakteristika osobe na temelju koje se obavlja prepoznavanje ili neprepoznavanje. Fizičke karakteristike su prirođene karakteristike osobe, poput karakteristika lica, otiska prsta, geometrije dlana, šarenice, mrežnice, termograma lica i tijela, uha, mirisa, DNK i sl. Ponašajne karakteristike su karakteristike koje je osoba, tijekom vremena usvojila odnosno naučila, poput potpisa, glasa, dinamike tipkanja, hoda i sl. Bilo koji biometrijski sustav koristi jednu ili više biometrijskih karakteristika za identifikaciju ili verifikaciju , pozitivnu ili negativnu, osobe kao korisnika toga sustava.

[60] Izvorno: Extended execution time

Uopćeno, aktivnost biometrijskog [70] sustava temelji se na usporedbi ekstrapolirane karakteristike i one pohranjenje u sustavu tijekom faze uvježbavanja[61] te rezultata te aktivnosti u vidu podudaranja[62] ili nepodudaranja[63] . Tijekom aktivnosti sustava , (pogledati Poglavlje 3) sukladno politici odlučivanja koja je dio arhitekture, dobiva se rezultat koji je predstavljen serijom grešaka izraženih kroz stupanj pogrešnog podudaranja *FMR* ili „stupanj pogrešnog nepodudaranja“ *FNMR*. Uopćene jednadžbe koje opisuju gore navedene greške mogu biti razvijene za dosta opće prihvaćenih politika odlučivanja biometrijskih sustava. Ako uzmemo u obzir slučaj gdje je *M* neovisnih biometrijskih mjerenja korišteno tijekom funkcioniranja biometrijskog sustava te politiku odlučivanja koja omogućava rezultat „podudaranja“ samo u slučaju potpune podudarnosti uzorka korisnika i pohranjenog uzorka tada će vjerojatnost pogrešnog podudaranja na jednom uzorku, FMR_{SR} biti jednaka izrazu:

$$FMR_{SR} = \prod_{j=1}^{R_j} FMR_j(t_j), \tag{31}$$

gdje je

$FMR_j(t_j)$ - stupanj pogrešnog podudaranja jednog uzorka za *j*-ti biometrijski metod koji može imati drugačije definiran prag podudarnosti t_j.

Pretpostavimo također da su prag podudarnosti t_j i stupanj pogrešnog podudaranja *FMR* jednog uzorka neovisni međusobno. Vjerojatnost da neće postojati ni jedna greška pogrešnog podudaranja može biti prikazana izrazom

$$FMR_{sys} = 1 - (1 - FMR_{SR})^{\mu - N}, \tag{32}$$

gdje je

FMR_{sys} - stupanj pogrešnog podudaranja cijelog sustava,

N – broj zapisa u bazi podataka.

[61] Izvorno: Enrollment

[62] Izvorno : Match

[63] Izvorno : Non Match

μ – srednja vrijednost postotka baze podataka koji je pretražen tijekom procesa usporedbe uzoraka[64]. Sukladno tomu za stupanj pogrešnog nepodudaranja tijekom uzimanja jednog uzorka imamo izraz:

$$FMR_{sys} = 1 - \prod_{i=1}^{N} (1 - FMR_j(t_i)). \tag{33}$$

4.3 Pristupi ocjeni pouzdanosti biometrijskih sustava

Sukladno navedenome u Poglavljima 4.1 i 4.2 modeli ocjene pouzdanosti biometrijskih sustava fragmentirani su na modele za ocjene pojedinih komponenti sustava u ovom slučaju hardvera i softvera kao sastavnica tehnologije biometrijskih sustava. U nastavku biti će opisani neki od pristupa ocjeni pouzdanosti biometrijskih sustava koji uzimaju u obzir cjelovitost istoga.

4.3.1 Ocjena pouzdanosti tehnologije biometrijskih sustava

Biometrijski sustav se može testirati te uspoređivati međusobno prema vrstama biometrijske tehnologije. Jedan od vodećih svjetskih znanstvenika na polju biometrije i dobitnik mnogih nagrada za inovacije, dr. Yau Wei Yun [71] sa Sveučilišta u Singaporeu, navodi obilježja raznih tipova biometrijskih sustava kroz sedam kriterija:

- **Općenitost** – opisuje koliko je česta biometrijska karakteristika kod pojedinca,
- **Jedinstvenos**t – kazuje koliko dobro biometrijska karakteristika razlikuje jednog pojedinca od drugog,
- **Trajnost** – predstavlja mjeru utjecaja procesa starenja na biometrijsku karakteristiku,
- **Dohvatljivost** – kazuje koliko lako je prikupiti biometrijsku karakteristiku za mjerenje,
- **Performanse** – kazuje kolika je preciznost, brzina i robustnost sustava koji mjeri biometrijsku karakteristiku,

[64] Izvorno : Penetration Rate

- **Prihvatljivost** – kazuje stupanj prihvaćanja tehnologije biometrijskih sustava u javnosti,
- **Prevarljivost** – kazuje koliko je lako prevariti sustav za autentikaciju.

Zbog niske [72] učestalosti pogrešaka testiranje biometrijskih sustava iznimno je teško a da bi se dobio uvid u statističke podatke moraju se prekontrolirati tisuće transakcija biometrijskih sustava [73]. Ljudski faktor je pritom nezamjenjiv jer biometrijski sustav zahtjeva ljudsku interakciju i nijedno od biometrijskih stanja se ne može točno kvantificirati samo putem teorijskih proračuna. Vrijednosti pogrešaka biometrijskih predstavljaju statističke veličine izvedene iz niza transakcija krajnjih korisnika sa pretpostavkom da je što je veći broj populacije i transakcija, veća i točnost rezultata procesa odluke biometrijskih sustava. Sukladno navedenome između svih parametara za ocjenu biometrijskog sustava jedino Stopa pogrešnog prihvaćanja[65] *FAR* može biti izračunata s prihvatljivom točnošću putem unakrsne usporedbe predložaka iz velikih baza podataka.

Trenutno mnogi proizvođači vrše svoja testiranja u stvarnim uvjetima koristeći podatke krajnjih korisnika. Međutim, bitno je napomenuti da su terenska testiranja vrlo skupa, te da si ih mogu priuštiti samo vladine službe. Ono što je za biometrijske sustave najvažnije su istraživanja neovisnih laboratorija kao što su National Biometric Test Center (SAD) i National Physical Laboratory (UK)[66].

4.3.2 Ocjena pouzdanosti performansi biometrijskih sustava

Evaluacija performansi biometrijskih sustava [44] se sastoji u ocjeni radnih karakteristika tijekom procesiranja podataka prilikom operativne uporabe sustava. Evaluacija performansi [74] predstavlja jedan od ulaznih parametara za ocjenu kvalitete samog biometrijskog sustava. Performanse sustava pod utjecajem su arhitekture sustava te konteksta uporabe odnosno njegove osnovne namjene. Jedan od čestih pokazatelja kod evaluacije performansi je i proučavanje stope pogrešaka sustava u prihvaćanju ili neprihvaćanju unešenog podatka u proces. Trenutno dostupne tehnologije imaju različite vrijednosti greške jednakosti koje variraju od niskih 60% do visokih 99,9%. Sposobnosti [72] i mogućnosti biometrijskog

[65] Izvorno: False accept rate

[66] Poput američkog NTSB-a u slučaju istraživanja uzroka zrakoplovnih nesreća. Istraživanja se vrše nezavisno od pojedinaca i institucija i bez pristranosti.

mjerenja se obično ogledaju kroz mjeru pogrešno prihvaćenih rezultata *FAR* , omjer pogrešnih nepoklapajućih ili odbačenih rezultata *FRR*[67], te omjeru grešaka pri uzorkovanju *FTE* ili *FER*. Sukladno dosadažnjim istraživanjima najčešće se javljaju dvije vrste pogrešaka prilikom operativne uporabe biometrijskih sustava

1. Pogrešno prihvaćanje *FAR*, pogreška I. tipa – sustav pogrešno prihvaća osobu kao legitimna korisnika jer je u bazi pronašao predložak dovoljno sličan unesenom. Dovoljnu sličnost definira politika prihvaćanja ili odbijanja predefinirana sustavom u formi praga prihvatljivosti sličnosti unešenog uzorka sa onime već pohranjenom u sustavu.

2. Pogrešno odbijanje *FRR*, pogreška II. tipa – legitimni korisnik se odbija jer sustav nije pronašao dovoljnu sličnost očitanih podataka s predloškom iz baze. Pogrešno odbijanje predstavlja neugodnost za korisnika, ali smatra se prihvatljivijim od I. tipa jer korisnik može ponovno pokušati s autentifikacijom u sustav. Sposobnosti i mogućnosti biometrijskog mjerenja najčešće se ogledaju kroz tri ključne pogreške biometrijskog sustava:

- stupanj pogrešnog podudaranja[68]
- stupanj pogrešnog nepodudaranja[69]
- neuspješno registriranje/zaprimanje uzorka[70]

Pogrešno podudaranje se događa kada sustav netočno odredi identitet, a *FMR* predstavlja postotak nedopuštenih korisnika koji su prihvaćeni kao legitimni korisnici. Kod verifikacije i pozitivnih identifikacijskih sustava osobama bez dozvole može biti dopušten pristup kao rezultat netočne identifikacije, dok kod negativnih sustava rezultat krive identifikacije može biti zabrana pristupa određenim sadržajima ili servisima. U vezu s pogrešnim podudaranjem dovodi se i pojam *stupanj pogrešnog prihvaćanja*[71] koji je po definiciji jednak *FMR*, s tom razlikom da je *FMR* vjerojatnost pogrešnog podudaranja s jednim predloškom, dok je *FAR* vjerojatnost pogrešnog podudaranja prilikom uspoređivanja sa svim predlošcima u bazi podataka[72]. *FAR* mora biti dovoljno nizak da bi odvratio nelegitimnog korisnika od pokušaja neovlaštenog pristupa. Za današnje biometrijske sustave *FAR* varira u rasponu od 0.0001% do 0.1%. [44]. Također je bitno za napomenuti da *FAR* mora biti pomnožen s brojem pokušaja

[67] Izvorno: FRR - False non match or reject rate

[68] Izvorno: FMR - *false match rate*.

[69] Izvorno: FNMR - *false non-match rate*.

[70] Izvorno: FTE(R) – *failure to enroll rate*.

[71] Izvorno: FAR – *false accept rate*.

[72] U specifikacijama proizvođača najčešće nalazimo statistike FAR i FRR pogrešaka, a manje FMR i FNMR.

neovlaštenog pristupa da bi se utvrdio broj mogućih prilika za eventualni neovlašteni pristup. Pogrešno nepodudaranje se događa kada sustav odbije valjani identitet legitimnog korisnika, a *FNMR* je postotak legitimnih korisnika koji su odbačeni kao nelegitimni. Kod verifikacije i pozitivnih identifikacijskih sustava osobama može biti odbijen pristup kao rezultat neuspjelog pronalaženja podudarnosti, dok kod negativnih identifikacijskih sustava rezultat pogrešnog nepodudaranja može biti dopuštanje pristupa osobi tamo gdje joj pristup ne bi smjeo biti dopušten. Za *stupanj pogrešnog odbijanja*[73] vrijedi ista analogija kao i za *FAR*. Za današnje biometrijske sustave *FRR* varira u rasponu od 0.00066% do 1.0%. [74] Pogrešna podudaranja događaju se u slučaju sličnosti dviju osoba, dok se pogrešna nepodudaranja javljaju kada nema dovoljno jake sličnosti između referentnog i probnog predloška, što se može desiti zbog više razloga npr. starenje, ozljede, itd. Za biometrijske sustave u realnim uvjetima *FAR* i *FRR* karakteristika obično su u različitim odnosima, ovisno o postavkama parametara sustava. Proizvođači često koriste pojam *stupanj jednakosti pogrešaka*[74], koji se još naziva i *prijelazni odnos pogreške*[75], kao dodatni indikator performanse sustava izveden pomoću *FMR* i *FNMR* (*FAR* i *FRR*), a koji opisuje preciznost njihovog sustava. Tu se misli na točku gdje je *FMR* = *FNMR* (*FAR* = *FRR*), tj. odnos pri kojem oba parametra podjednako prihvaćaju i odbijaju pogreške. Ako se sustav podesi tako da je prag odluke u točki *EER* rezultat će biti jednakost vjerojatnosti pogrešnog prihvaćanja i obijanja. Preciznost sustava je veća što je niža vrijednost *EER*, a balans *FMR* i *FNMR* (*FAR* i *FRR*) je ključ uspjeha sustava jer je u stvarnim uvjetima korištenja aplikacije potreba za sigurnošću podjednaka potrebi za praktičnošću uporabe[76].

[73] Izvorno: FRR – *false reject rate*.

[74] Izvorno: EER – *equal error rate*.

[75] Izvorno: CER – *cross-over error rate*.

[76] Manji FAR – manje uspješnih napada nelegitimnih korisnika, ali i manja tolerancija prema legitimnim korisnicima; manji FRR – sustav prepoznaje legitimnog korisnika isprve, ali više tolerira lošija podudaranja i napade.

POGLAVLJE V

5 EVALUACIJSKI MODELI BIOMETRIJSKIH SUSTAVA

Evaluacija biometrijskih sustava [9] predstavlja kompleksnu problematiku [75] uzimajući u obzir sve širu njihovu uporabu u svakodnevnom životu. Biometrijski sustavi ovisno o njihovoj namjeni odnosno kontekstu njihove uporabe imaju različite zahtjeve glede pouzdanosti tako da neki konteksti u odnosu na druge stavljaju akcent na pojedine aspekte biometrijskih sustava koji isključivo utječu na percepciju njihove pouzdanosti. Uzimajući u obzir specifičnosti biometrijskih sustava kao informacijski intenzivnih sustava koji zahtijevaju sudjelovanje ,svjesno ili nesvjesno, korisnika sustava preko unosa biometrijskih karakteristika koji jasno i nedvojbeno identificiraju osobu omogućavajući ili ne pristup istoj određenim servisima ili mogućnostima, biometrijski sustav [76] se u određenim kontekstima može pojaviti i kao diskriminacijski faktor što može utjecati na percepciju i prihvaćanje biometrijskih sustava koji služe npr. u svrhu povećanja razina nacionalne sigurnosti u domeni akcija protiv širenja terorizma.

5.1 Definicija evaluacije biometrijskih sustava

Uopćeno evaluacija biometrijskih sustava predstavlja skup postupaka analize biometrijskih algoritama ,komponenata , biometrijskih karakteristika ili cijelih aplikacija sa svrhom testiranja njihove sposobnosti da ispunjavaju svoju ulogu proizvodeći prema tome empirijski opipljive dokaze [77].

Proces evaluacije bi trebao ,svim zainteresiranim stranama za funkcioniranje biometrijskih sustava, dati informacije o

- Ponašanju biometrijskog sustava tijekom operativne uporabe sa mogućnostima poboljšanja njegove funkcije,
- Određivanju prednosti i nedostataka uporabe biometrijskih sustava u određenim kontekstima,

- Metodama za detekciju vjerojatnosti operativnih otkaza tijekom rada u određenim uvjetima,
- Metodama odlučivanja o primjerenosti određenih rješenja biometrijskih sustava u idnosu na neke druge,
- Metodama poredbe rješenja biometrijskih sustava za određenu funkciju radi određivanja one optimalne.

Cjelovita i sveobuhvatna metodologija evaluacije biometrijskih sustava do danas nije formalizirana. Postoje formalne procedure sadržane u nekolicini međunarodnih standarda koje definiraju detaljno metodologije za : testiranje performansi biometrijskih sustava (Poglavlje 4.2.2) , testiranje pouzdanosti tehnologije sustava (Poglavlje 4.2.1) te testiranje sigurnosti biometrijskih sustava. Navedeno znači da postoji niz aspekata evaluacije biometrijskih sustava koji nisu predmet evaluacija te mogu biti uzrok nepouzdanosti sustava u smislu otkaza ili nefunkcionalnosti sustava.

Upravo zbog toga glavni cilj ove disertacije je definiranje temelja metodologije za ocjenu pouzdanosti biometrijskih sustava koja izlazi izvan navedenih područja te uzima u obzir kontekst uporabe biometrijskih sustava u vidu okruženja te korisnika sustava kao faktora koji sigurno utječu na pouzdano funkcioniranje biometrijskih sustava, koja do danas nije definirana u tom obliku. Definiranje ciljane metodologije biti će utemeljeno na postojećim metodologijama koje ocjenjuju pojedine aspekte pouzdanosti biometrijskih sustava.

5.2 Pristupi problematikama evaluacije biometrijskih sustava

Sukladno već navedenome u poglavlju 4. pristupi problematikama razmatranja pouzdanosti biometrijskih sustava različiti su te uzimaju u obzir pojedine aspekte biometrijskih sustava a zanemaruju neke druge ovisno o kontekstu uporabe.

Sukladno navedenome, u nastavku ovoga rada, biti će prikazani i ukratko opisani pristupi problematikama evaluacije biometrijskih sustava.

5.2.1 Evaluacija performansi biometrijskih sustava

Ovaj pristup evaluaciji biometrijskih sustava sastoji se od mjerenja performansi biometrijskih sustava te njihove poredbe sa referentnim vrijednostima sukladno zahtjevima standarda :International Organization for Standardization, ISO/IEC 19795-1, Information technology -- Biometric performance testing and reporting -- Part 1: Principles and framework ISO/IEC 19795-1:2006, 2006b., te standarda International Organization for Standardization, ISO/IEC TR 24741, Information technology -- Biometrics tutorial, ISO/IEC TR 24741:2007, 2007b. [10]. Oba navedena standarda uvode pojam performansi sustava a koji se mogu se izraziti preko parametara preciznosti sustava te brzini obrade podataka itd.

Navedena metodologija definira postupke evaluacije biometrijskih sustava koristeći metode za:

- Testiranje pouzdanosti koje analizira učestalost ponavljanja grešaka te sposobnost biometrijskog sustava za nastavak funkcioniranja nakon nastanka greške u funkcioniranju,
- Testiranje izdržljivosti koje analizira sposobnost sustava za funkciniranje sustava u uvjetima učestalih ometanja iz okoline ili korisnika, namjernih ili nenamjernih,
- Testiranje raspoloživosti koje analizira vremenski period u kojem je sustav ponovo raspoloživ za uporabu nakon nastanka greške u operativnoj funkciji,
- Testiranje vremena odziva koje analizira vremenski period čekanja korisnika na odluku sustava,
- Testiranje mogućnosti održavanja koje analizira troškove te isplativnost zahtijevanog održavanja biometrijskog sustava.

5.2.2 Evaluacija sukladnosti biometrijskih sustava

Evaluacija ovoga tipa predstavlja postupke ocjene usklađenosti određenih aspekata biometrijskih sustava sa precizno definiranim zahtjevima. Takovi zahtjevi najčešće su dio

paketa međunarodnih standarda od kojih su dosta važni sljedeći:

a.)International Organization for Standardization, ISO/IEC 29109-1, Information technology -- Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 -- Part 1: Generalized conformance testing methodology, ISO/IEC 29109-1:2009, 2009c,

Ovaj standard, definira formate podataka biometrijskih sustava da bi isti bili interoperabilni i uporabljivi od strane drugih biometrijskih sustava neovisno o proizvođaču ili modalitetu uporabe.

b.)International Organization for Standardization, ISO/IEC 19794-1, Information technology -- Biometric data interchange formats -- Part 1: Framework, 2011a,

Ovaj standard defnira opća obilježja te zahtjeve za definiranje međusobno razmjenjivih i uporabljivih biometrijskih podataka. Formatiranje međusobno razmjenjivih podataka neovisno je o platformi izvedbe te sadržajnoj definiciji podataka. Također se definira ono što je zajedničko za formate biometrijskih podataka kao što je : standardizacija zajedničkog sadržaja, značenja te prikaza biometrijskih podataka.

c.)International Organization for Standardization, ISO/IEC 19784-1, Information technology -- Biometric application programming interface -- Part 1: BioAPI specification, ISO/IEC 19784-1:2006, 2006a,

Ovaj standard definira zajedničke zahtjeve za biometrijsko sučelje za programiranje – BioAPI[77] kako bi se omogućila neometana komunikacija između softverskih rješenja te različitih tipova hardvera koji se koriste za izradu biometrijskih sustava.

d.)International Organization for Standardization, ISO/IEC 24709-1, Information technology -- Conformance testing for the biometric application programming interface (BioAPI) -- Part 1: Methods and procedures, ISO/IEC 24709-1:2007, 2007d.

Ovaj standard definira neophodne metodologije za provedbu testova sukladnosti sa zahtjevima standarda ISO/IEC 19784-1.

[77] Izvorno:Biometric programming interface

e.)International Organization for Standardization, ISO/IEC 19785-1, Information technology -- Common Biometric Exchange Formats Framework -- Part 1: Data element specification, ISO/IEC 19785-1:2006, 2006c.

Ovaj standard definira okvir za testiranje Zajedničkih biometrijskih formata – CBEFF[78] te sukladno navedenome definira zajednički strukturu formata podataka radi omogućavanja zajedničkog korištenja od strane više biometrijskih sustava.

Može se zaključiti da proces ocjene sukladnosti zahtjevima navedenih standarda predstavlja garanciju korisniku odnosno vlasniku da je proizvod , u ovom slučaju biometrijski sustav, sukladan propozicijama međunarodnih standarda te kao takav pogodan za uporabu.

5.2.3 Evaluacija sigurnosti biometrijskih sustava

Biometrijski sustavi [78] u svakodnevnoj uporabi pojavljuju se često u ulozi sustava koji nadziru ili garantiraju sigurnost drugih sustava pa je kao posljedica neophodno poznavati razinae sigurnosti biometrijskih sustava [79] a sukladno tomu i njihove eventualne ranjivosti. Cilj evaluacije sigurnosti biometrijskih sustava je upravo dokazivanje određenih razinaa sigurnosti biometrijskih sustava. Uopćeno , evaluacija sigurnosti biometrijskih sustava [75] sastoji se od provjere stupnja zadovoljavanja određenih sigurnosnih zahtjeva te provjere otpornosti biometrijskih sustava na eventualne napade. Određeni setovi sigurnosnih provjera koji danas postoje uključuju sljedeće evaluacije:

- ocjena sukladnosti te zadovoljavanja sigurnosnih zahtjeva biometrijskih sustava određene namjene [35],

- procjena ranjivosti biometrijskih sustava [80] koja može uključivati i testove prodora u sustav[79],

Procjena ranjivosti biometrijskih sustava [5] mora uključivati popis potencijalnih prijetnji [81] te vjerojatnosti da se ranjivost iskoristi a prijetnje ostvare kroz potencijalne napade na sustav [46].

[78] Izvorno: Common Biometric Exchange Formats Framework

[79] Izvorno: Penetration test

Scenarij napada se testira putem metodologije testova prodora. Svaki neuspješan napad zatvara ranjivost prema kojoj se izvodio i obratno.

5.2.4 Evaluacija zaštite privatnosti biometrijskih sustava

Evaluacija zaštite privatnosti biometrijskih [5] sustava predstavlja derivat ocjene usklađenosti ali ovaj put sa regulativnom koja definira problematike zaštite privatnosti podataka korisnika biometrijskih sustava [82]. Cilj usklađenja sa navedenom regulativom jeste osiguranje ispravnog korištenja i raspolaganja osobnim podacima koji se pohranjuju te procesiraju kroz biometrijski sustav. Provedba evaluacije zaštite privatnosti [83] implementiranih biometrijskih sustava podrazumjeva provjeru zaštite privatnosti tijekom operativne funkcije te provjere sukladnosti dokumentacije koja opisuje sustav i administrativnih procedura sa problematikama zaštite privatnosti. Metodologije za ovu vrstu evaluacije propisane su sljedećim standardima:

- National Science and Technology Council (NSTC), Privacy & Biometrics. Building a Conceptual Foundation, 2006a,
- IEEE Certified Biometrics Professional (CBP), Module 3 Biometric System Design and Evaluation, 2009d.

5.2.5 Evaluacija mogućnosti korištenja biometrijskih sustava

Evaluacija mogućnosti korištenja biometrijskih sustava [47] fokusirana je na korisnika biometrijskih sustava te na sposobnost sustava da bude korištena na odgovarajući način. Temelj ove evaluacije je proces interakcije korisnika i biometrijskog sustava. Sukladno međunarodnom standardu : International Organization for Standardization, ISO 9241: Ergonomic requirements of human system interaction for office work with visual display terminals (VDTs) – Part 11: Guidance on usability, ISO 9241-11:1998, 1998. , termin mogućnost korištenja sustava[80] definiran je kroz tri parametra: efektivnost sustava, efikasnost

[80] Izvorno: Usability

sustava te zadovoljstvo korisnika. Svaki od parametara je metrički definiran serijom pitanja na koja je potrebno dati precizan odgovor. Proučavanjem dostupne literature [32] moguće je proširiti zahtjeve evaluacije mogućnosti korištenja biometrijskih sustava sa sljedećim parametrima koji utječu na interakciju korisnika sa sustavom:

- ergonomija biometrijskog sustava ,
- prihvatljivost biometrijskih sustava od strane korisnika.

5.3 Postojeći modeli evaluacije biometrijskih sustava

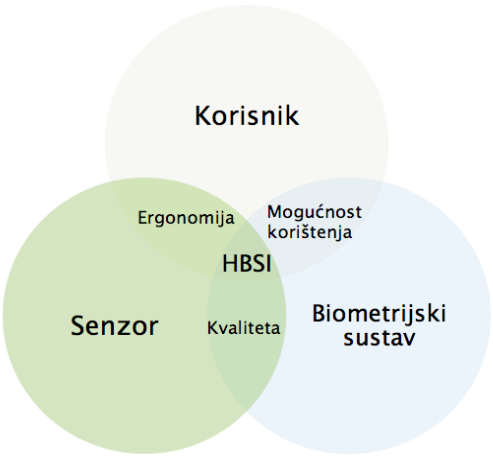
Metodologije opisane u prethodnim poglavljima uzimaju u obzir prevalentno tehničke Činitelje biometrijskih sustava premda utjecaj korisnika na funkcioniranje samog sustava, bez dubljih ulaženja u problematiku, nameće se kako jako bitan. Utjecaj korisnika manifestira se kroz sami stav korisnika prema biometrijskom sustavu glede njegove namjene te prezentiranja biometrijske kakakteristike sustava u procesu unošenja preko senzora. Proučavajući literaturu iz referentnog područja [84] mogu se izdvojiti koncepti kao što su: prihvatljivost, razina priviknutosti na sustav itd. koji se mogu smatrati činiteljima utjecaja na biometrijski sustav.

5.3.1 HBSI model

Određeni pokušaj povezivanja navedenih faktora u metodologiju evaluacije sadržan je u radovima znanstvenika S. Elliott and E. Kukula koji su između 2006. i 2010. Godine razvili model nazvan– Interakcija osobe i senzora biometrijskog sustava - HBSI[81] [84]. Model se bavi proučavanjem utjecaja korisnika na performanse biometrijskih sustava te ih metrički definira koristeći pretpostavke prethodno navedenih specifičnih modela evaluacije. Konceptualni model [85] prikazuje trijadu : biometrijski sustav, korisnik te senzor sa područjima preklapanja a to su: *Ergonomija* kao prostor preklapanja područja *Korisnik* te *Senzor*, *Mogućnost korištenja* kao prostor preklapanja područja *Korisnik* te *Biometrijski sustav* i *Kvaliteta* kao prostor preklapanja područja *Biometrijski sustav* i *Senzor*.

[81] Izvorno: Human-Biometric Sensor Interaction

Konceptualni model sa područjima te preklapanjima prikazan je na slici 6.



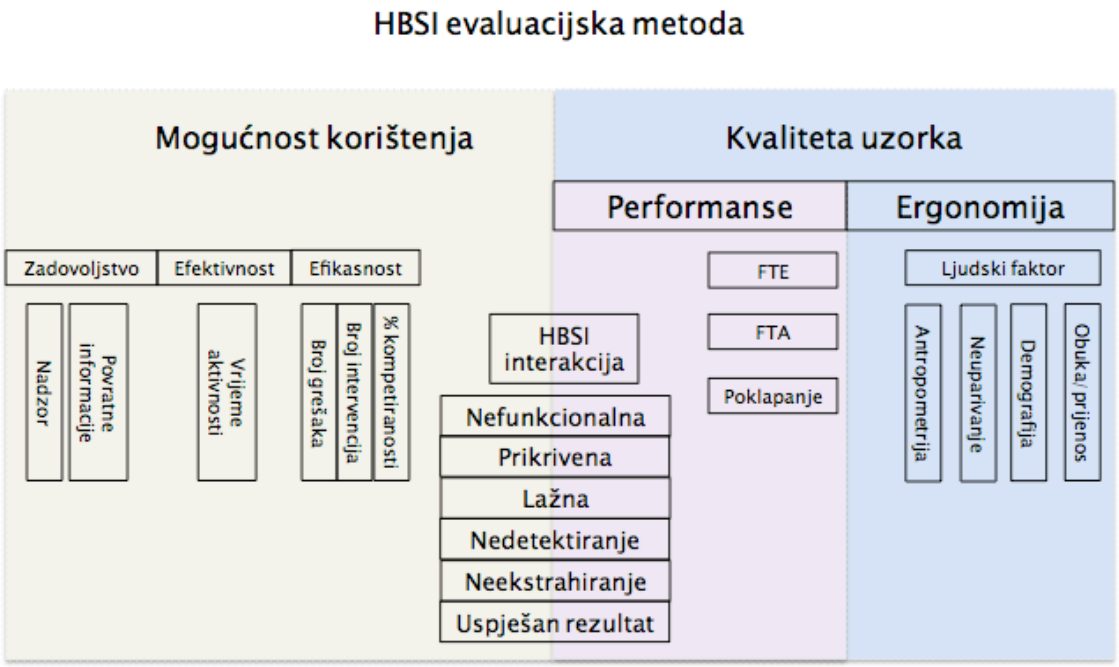
Slika 6 Konceptualni model HBSI

Sukladno konceptualnom modelu autori su razvili metodu za evaluaciju HSBI koja za cilj ima uzimanje u obzir faktora koji utječu na funkcioniranje biometrijskih sustava ,podijeljenih u tri grupe, a to su:

1. Mogućnosti korištenja biometrijskog sustava,
    I. Zadovoljstvo
        i. Nadzor
        ii. Povratne informacije
    II. Efektivnost
        i. Vrijeme aktivnosti
    III. Efikasnost
        i. Broj grešaka
        ii. Broj intervencija
        iii. % izvršenja zadatka
2. Performanse
    I. FTA
    II. FTE
    III. Podudaranje
3. Ergonomija
    I. Ljudski faktor
        i. Antropometrija

ii. Neuparivanje
iii. Demografija
iv. Obuka/Prijenos

HBSI [86] evaluacijska metoda prikazana je na slici 7.



Slika 7 Evaluacijska metoda sukladno HBSI metodelu

Autori su definirali metrike parametara kojima se služi evaluacijska metoda radi evaluacije biometrijskih sustava. Metrike su rezultati podudaranja područja utjecaja konceptualnog modela te ekstencija postojeće FTA metrike za ocjenu biometrijskih sustava.

Metrike su definirane na sljedeći način:

1. Nefunkcionalna interakcija – DI[82], prestavlja situaciju nefunkcionalnog prezentiranja biometrijske karakteristike u sustav te kao rezultat ima neprihvaćanje sustava.
2. Prikrivena interakcija – CI[83], predstavlja situaciju kada je verificirana pogrešna prezentacija biometrijske karakteristike u sustav koji ju nije prepoznao te niti tretirao kao pogrešnu.

[82] Izvorno: defective interaction

[83] Izvorno: concealed interaction

3. Lažna interakcija – FI[84], predstavlja situaciju kada je sustav prepoznao pogrešnu prezentaciju biometrijske karakteristike te ju kao takvu i tretirao.
4. Nedetektiranje – FTD[85], predstavlja odnos prezentiranih karakteristika zabilježenih od strane testnog tima a nezabilježenih od strane biometrijskog sustava.
5. Neekstrahiranje, neprocesiranje – FTE/FTP[86], predstavlja situaciju nemogućnosti procesiranja predstavljene biometrijske karakteristike.
6. Uspješan rezultat – SAS[87], predstavlja situaciju korektnog predstavljanja biometrijske karakteristike koju sustav prepoznaje te adekvatno procesira.

Model je ažuriran radom autora [85].

5.3.2 H-B Interakcijski model

H-B Interakcijski model skraćeni je naziv za Evaluacijsku metodu za H-B interakcijski test biometrijskih sustava autora Belén Fernández Saavedra [86] , koja je dio doktorske disertacije pod nazivom: Evaluation Methodologies for Security Testing of Biometric Systems beyond Technological Evaluation, obranjene u ožujku 2013. godine na UNIVERSIDAD CARLOS III DE MADRID. Ovaj model predstavlja ekstenziju opisanog HBSI modela uvođenjem parametra Okoline koji utječe na funkcionalnost biometrijskog sustava. H-B interakcijski model opisuje seriju funkcionalnih testova tijekom kojih skup korisnika interagira sa biometrijskim sustavom s ciljem izračuna stupnja preciznosti i brzine algoritama prepoznavanja biometrijskih karakteristika kada se jedna ili više okolnosti realiziraju:

a. Određena biometrijska karakteristika vezana uz senzor biometrijskog sustava se promijenila,
b. Osoba i pridružena biometrijska karakteristika ima određene specifične, ili
c. Bilo koji faktor koji ima utjecaj na H-B interakcijski proces je promijenjen.

Drugim riječima H-B iterakcijski model je «end-to-end» evaluacija biometrijskih sustava uzimajući u obzir određene faktore okoline, ergonomije te mogućnosti korištenja

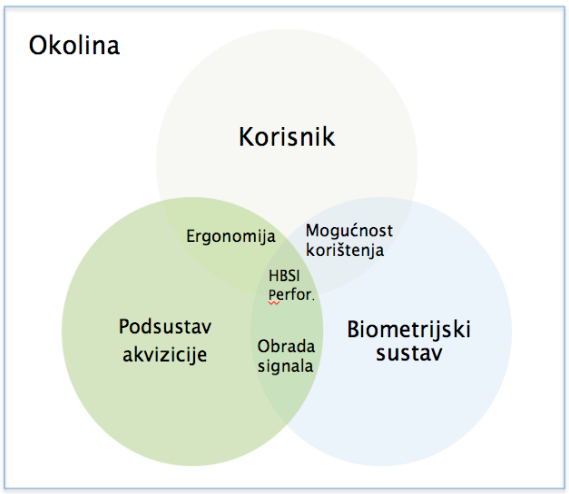
[84] Izvorno: false interaction

[85] Izvorno: failure to detect

[86] Izvorno: failure to extract/failure to process

[87] Izvorno: Successfull acqusition sample

biometrijskih sustava. Model se bavi proučavanjem utjecaja korisnika na performanse biometrijskih sustava te ih metrički definira koristeći pretpostavke HBSI modela. Konceptualni model prikazuje trijadu : *biometrijski sustav*, *korisnik* te *senzor* sa područjima preklapanja a to su: *Ergonomija* kao prostor preklapanja područja *Korisnik* te *Podsustav unosa*, *Mogućnost korištenja* kao prostor preklapanja područja *Korisnik* te *Biometrijski sustav* i *Obrada signala* kao prostor preklapanja područja *Biometrijski sustav* i *Podsustav akvizicije*. Konceptualni model sa područjima te preklapanjima prikazan je na slici 8.



Slika 8 Konceptualni model H-B Interakcijska metoda

Sukladno konceptualnom modelu autori su razvili metodu za evaluaciju H-B Interakcijski model koja za cilj ima uzimanje u obzir faktora koji utječu na funkcioniranje biometrijskih sustava ,podijeljenih u dvije grupe te tri podgrupe. Metrike organizirane u podgrupe prve grupe su sljedeće:

1. Mogućnosti korištenja biometrijskog sustava,
    I. Zadovoljstvo korisnika
        i. % zadovoljnih korisnika
2. Ergonomija
    I. Kognitivna
        i. % korisnika koji znaju koristiti sustav
        ii. % korisnika koji se sjećaju kako se koristi sustav
        iii. % korisnika koji su naučili kako se koristi sustav
    II. Fizička
        i. % korisnika koji mogu koristiti sustav

III. Uzorak

i. Metrika kvalitete

ii. Vrijeme trajanja akvizicije

3. Kvaliteta uzorka

I. Procesiranje

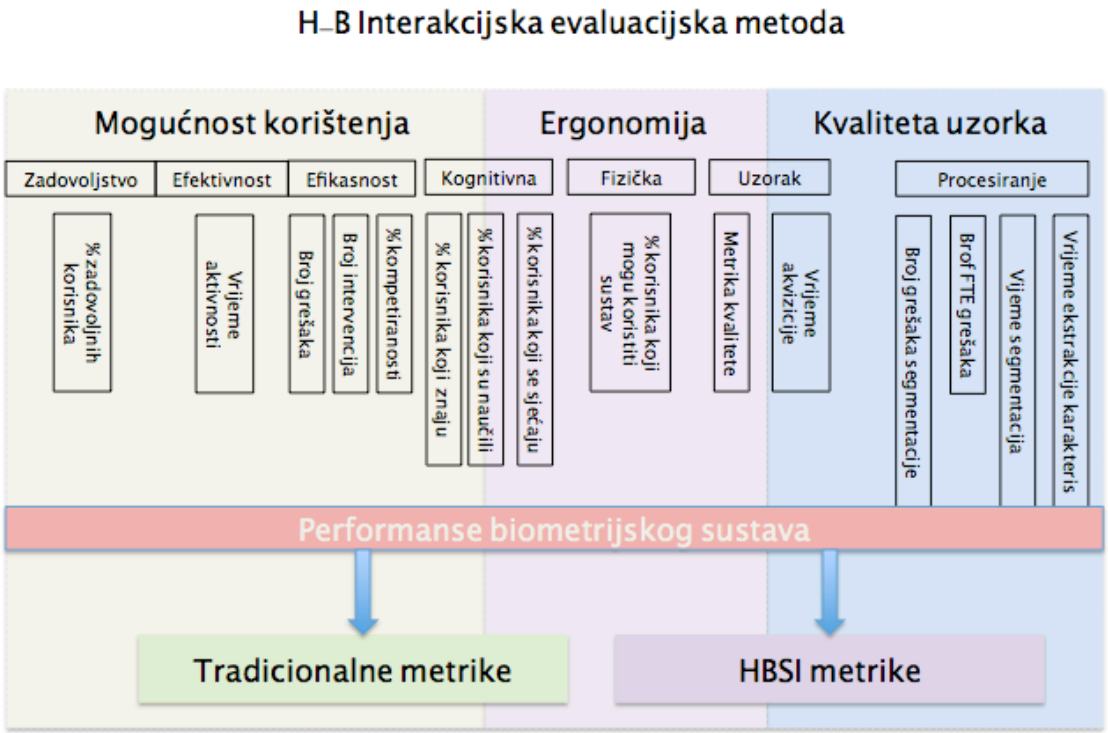
i. Broj grešaka segmentacija

ii. Broj FTE grešaka

iii. Vrijeme segmentacije

iv. Vrijeme ekstrakcije karakteristika

Druga grupa parametara [87] fokusira se na ocjenu ukupnog utjecaja uključivo sa svim komponentama biometrijskog sustava. Metrike ove grupe parametara predstavljaju tradicionalne metrike za ocjenu performansi biometrijskog sustava [88] sukladno propozicijama standarda te stopama pogrešaka HBSI evaluacijskog modela. Sukladno gore navedenome H-B Interakcijska evaluacijska metoda prikazana je na slici 9.



Slika 9 Evaluacijska metoda sukladno H-B Interakcijskom metodelu

POGLAVLJE VI

6 OTVORENI OKVIR ZA EVALUACIJU POUZDANOSTI BIOMETRIJSKIH SUSTAVA

U prethodnim Poglavljima predstavljene su metodologije za ocjenu pojedinačnih aspekata biometrijskih sustava sukladno tradicionalnim te standardiziranim protokolima ta zatim i evaluacijski modeli koji uključuju određene specifične metode evaluacije biometrijskih sustava uvođenjem pojmova utjecaja korisnika putem parametra mogućnost korištenja te okoline biometrijskih sustava. Sukladno navedenome s jedne strane imamo više specifičnih modela za ocjenu biometrijskih sustava [89] u smislu utjecaja na njihove performanse npr: položaj senzora [90], dob korisnika [91], spol korisnika, priviknutost korisnika , uvježbanost korisnika, dostupnost uputa za korištenje te povratne informacije od strane korisnika. Sa druge strane imamo evaluacijske modele koji su usmjereni na ocjenu utjecaja na sigurnost biometrijskih sustava [3] određenih činitelja njihovog funkcioniranja. Uglavnom svaki navedeni pristup evaluaciji koristi vlastitu metodologiju.

Zaključak prethodno navedenih analiza jeste da ne postoji jedinstvena, opće prihvaćena metodologija za evaluaciju biometrijskih sustava koja objedinjuje dosadašnje napore i domenska istraživanja.

Cilj ovog doktorskog rada jeste razrada činitelja pouzdanosti biometrijskih sustava koji se manifestiraju kao trijada aspekata:

1- Tehnologija od koje je sačinjen biometrijski sustav, uzimajući u obzir hardver i softver te njihove performanse tijekom funkcioniranja biometrijskog sustava,

2- Okolina unutar koje je smješten te funkcionira biometrijski sustav,

3- Korisnik biometrijskog sustava koji interagira sa sustavom te je ishodište svrhe postojanja biometrijskog sustava.

Ova trijada aspekata te njihovih činitelja biti će definirana te razrađena kao otvoreni okvir u smislu otvorenosti za nedogradnju i poboljšanja te dostupnosti eventualnim zainteresiranim stranama.

U ovom poglavlju nadalje biti će predstavljeni te definirani:

a.)Otvoreni Okvir Za Evaluaciju Pouzdanosti Biometrijskih Sustava (nadalje OOEPBS) kao temelj za definiranje metode za evaluaciju pouzdanosti biometrijskih sustava,

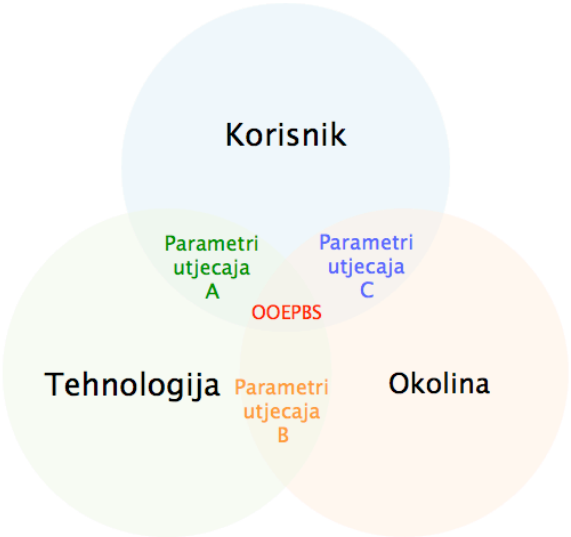
b.)Metoda za evaluaciju pouzdanosti biometrijskih sustava

6.1 Konceptualni model OOEPBS

Otvoreni okvir za evaluaciju pouzdanosti biometrijskih sustava podrazumijeva definiciju aspekata te pripadajućih činitelja pouzdanosti biometrijskih sustava sukladno definicijama iz poglavlja 4 gdje se pouzdanost definira kao: « sposobnost sustava da izvršava i održava svoju operativnu funkciju u rutiniranim okolnostima, ali i u neprikladnim i neočekivanim okolnostima».

Sposobnost sustava da izvršava svoju operativnu funkciju, odnosno pouzdanost, podložna je utjecajima aspekata konteksta uporabe samog sustava. Kontekst uporabe biometrijskog sustava može se definirati kao trijada aspekata (pojavnosti) već opisana u uvodu ovoga poglavlja.

Konceptualni model OOEPBS prikazan je na slici 10.



Slika 10 Konceptualni model OOEPBS

Trijada aspekata, Korisnik, Okolina te Tehnologija predstavljaju domenu ovoga otvorenog evaluacijskog okvira. Pojedini aspekti trijade biti će parametrizirani putem činitelja koji će opisivati utjecaje aspekata na pouzdanost biometrijskog sustava. Područja preklapanja aspekata su definirani kao činitelji utjecaja *A*, *B* i *C* koji će biti definirani kroz evaluacijski model OOEPBS, evaluacijsku metodu te kasnije ontološki definirani.

6.2 Aspekti pouzdanosti biometrijskih sustava

Na temelju definiranog konceptualnog modela trijade aspekata pouzdanosti biometrijskih sustava u ovom poglavlju biti će predstavljena parametrizacija pojedinih aspekata pouzdanosti putem definiranja metrika za svaki specifični parametar koje će biti u funkciji sklapanja modela evaluacije pouzdanosti biometrijskih sustava te poslužiti kao temelj za definiranje metode za evaluaciju biometrijskih sustava.

6.2.1 Aspekt tehnologije biometrijskog sustava

Kako je navedeno u poglavlju 2.1 , slika 1, uopćeni biometrijski sustav sastoji se sastoji od pet podsustava:

1. Prikupljanje podataka,

2. Prijenos podataka,

3. Obrada podataka,

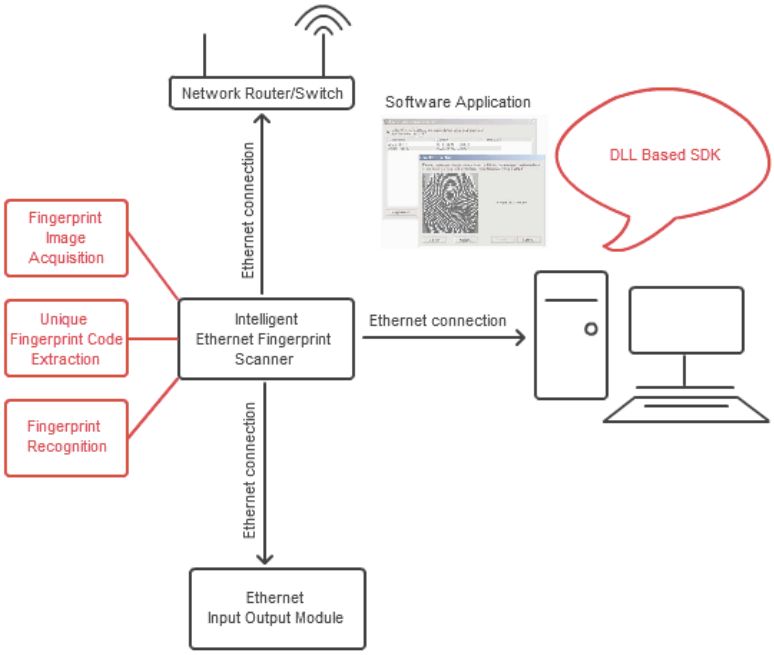
4. Pohrana podataka,

5. Donošenje odluke.

Svaki podsustav ima specifičnu ulogu tijekom izvršavanja operativne funkcije biometrijskog sustava ovisno o kontekstu uporabe.

Sa aspekta tehnologije izvedbe biometrijskog sustava , isti se može prikazati kao spoj softvera i hardvera koji su povezani funkcijom samog sustava koja njihovim zajedničkim

funkcioniranjem ima određene performanse kao što je prikazano na slici 11:



Slika 11 Prikaz tehnologije izvedbe biometrijskog sustava [88]

Softver i hardver [43] imaju zajedničku osobinu limitiranog vijeka trajanja zbog zastarijevanja, deterioracije te degradacije pa stoga obje komponente zahtijevaju intervencije nadzora te preventivnog odnosno korektivnog održavanja tijekom životnog ciklusa biometrijskog sustava.

Tehnologija izvedbe biometrijskih sustava je definirana odredbama mnogobrojnih međunarodnih standarda od kojih ćemo navesti samo neke [10]

- ISO/IEC 25062:2006- Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Common Industry Format (CIF) for usability test reports,

- ISO/IEC 2382-14:1997 Information technology-Vocabulary-Part 14: Reliability, maintainability and availability,

- ISO 17359:2003 – Condition monitoring and diagnostic of machines – General guidelines - First edition 2003-07-01,

- ISO 9241-210:2010 – Ergonomic of human system interaction – Part 210: Human centered

[88] preuzeto sa http://www.biometricsys.de/Intelligent-fingerprint-scanner-ifis131.html 21.03.2015 u 20:30

design for interactive systems, itd.

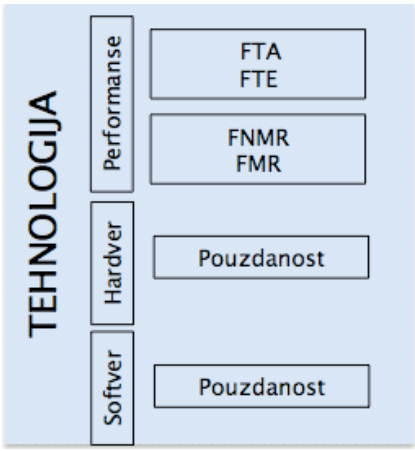
Performanse biometrijskih sustava predstavljaju zadane karakteristike metrički definirane putem kojih se ocjenjuje kvaliteta funkcioniranja biometrijskih sustava kako je detaljnije opisano u poglavlju 4.2.2. gdje su izdvojeni parametri koji imaju najrašireniju uporabu u praksi a koje proizvođači biometrijskih sustava ističu na svojim deklaracijama o kvaliteti biometrijskih sustava.

Za potrebe ovoga doktorskog rada aspekt tehnologija biometrijskih sustava kao sastavni dio konceptualnog modela, biti će opisan kroz parametre svojih činitelja pouzdanosti. Činitelji koji opisuju aspekt tehnologije su:

- softver,
- hardver,
- performanse biometrijskih sustava.

Činitelj softver, aspekta tehnologije biti će opisan putem parametra pouzdanost čija će metrika nadalje biti definirana (vidjeti poglavlje 4.1.2). Činitelj hardver, aspekta tehnologije biti će opisan putem parametra pouzdanost čija će metrika nadalje biti definirana (vidjeti poglavlje 4.1.1). Činitelj performanse, aspekta tehnologije biti će opisan putem parametara: statistike FMR i FNMR te statistike FTA i FTE (vidjeti poglavlje 4.2.2).

Slika 12 prikazuje razradu činitelja pouzdanosti aspekta tehnologije biometrijskih sustava koji utječu na njihovu pouzdanost :



Slika 12 Aspekt tehnologije biometrijskog sustava sa pripadajućim činiteljima te parametrima

Parametrizacija činitelja pouzdanosti te njihovo metričko definiranje neophodan je korak ka definiranju evaluacijskog okvira a samo definiranje područja pouzdanosti omogućava stvaranje temelja za ustanovljavanje metode za evaluaciju biometrijskih sustava.

Činitelji hardver i softver mogu se definirati putem parametra pouzdanost kojeg proizvođači naznačuju sukladno tehničkoj dokumentaciji odnosno na deklaracijama kvalitete proizvoda. Parametar pouzdanost opisan je u poglavljima 4.1.1 i 4.1.2, sukladno važećim modelima za ocjenu pouzdanosti koji su dani u navedenim poglavljima. Metrika navedenog parametra je postotak (%) a područje pouzdanosti je područje koje pokriva vrijednosti parametra jeste područje : pouzdanost (*P*) veća od 90 posto (> 90%).

Činitelj performanse biometrijskog sustava može se definirati skupom Statističkih parametara (S): *FMR, FNMR, FTA, FTE* a metrika navedenih parametara je postotak (%) a područje pouzdanosti je područje koje pokriva vrijednosti parametra jeste: područje manje ili jednako 1 posto (< = 1%) kako je opisano u poglavlju 4.2.2.

Pregled parametrizacije činitelja aspekta tehnologije sa referentnim metrikama te područjima pouzdanosti dan je u Tablici 1:

Tablica 1 Pregled činitelja aspekta Tehnologije

Aspekt	**Činitelj**	**Parametar**	**Metrika**	**Područje pouzdanosti**
Tehnologija	Softver	Pouzdanost (P)	%	> 90
	Hardver	Pouzdanost (P)	%	> 90
	Performanse	Statistike (S): FTA, FTE, FMR,FNMR	%	< = 1

6.2.2 Aspekt okoline biometrijskog sustava

Okolina biometrijskog sustava može se definirati kao okruženje ili skup uvjeta u kojima sustav postoji te funkcionira [45] te je moguće zaključiti da se biometrijski sustavi određene namjene ponašaju različito u odnosu na određene okolinske uvjete te da uvjeti koji vladaju u okolini utječu na funkcioniranje biometrijskih sustava. Promjena okolinskih uvjeta u kojima je smješten i funkcionira biometrijski sustav utječe na interakciju korisnika i biometrijskih

sustava te tako i na promjenu performansi biometrijskih sustava. Sukladno navedenome okolina biometrijskog sustava predstavlja važan aspekt koji utječe na performanse a samim tim i na pouzdanost biometrijskog sustava.

Pregledom radova autora A. Jain, R. Bolle and S. Pankanti [92] razvidan je utjecaj konteksta primjene biometrijskih sustava na performanse tehnologije biometrijskih sustava. Autori su zaključili da kontekst primjene u vidu okoline biometrijskih sustava utječe na broj ponavljanja uzimanja biometrijskog uzorka pa tako i na mogućnost distinkcije biometrijskih karakteristika korisnika. Autori također definiraju nekoliko kategorija uvjeta primjene biometrijskih sustava, ovisno o njihovoj primarnoj namjeni a koje su: kooperativni-nekooperativni, prikriveni-otkriveni, prilagođeni-neprilagođeni, očekivani-neočekivani, standardni uvjeti-nestandardni uvjeti, javni-privatni, zatvoreni-otvoreni. Radovi autora A.J. Mansfield and J.L. Wayman [93] and J. Wayman, A. Jain, D. Maltoni and D. Maio [94] zaključuju da su krivulje performansi biometrijskih sustava ovisne o utjecajima okoline te populacije korisnika. Također sadrže dodatak koji detaljizira okolišne faktore koji imaju utjecaja na određene biometrijske modalitete. Autori T. Dunstone and N. Yager [95] te Stan Li and A. Jain [45] zaključuju da svaka promjena u okolinskim uvjetima nedvojbeno utječe na performanse biometrijskih sustava uglavnom negativno.

Sukladno prethodno navedenome okolina je jedan od faktora od presudnog utjecaja na funkcioniranja biometrijskog sustava sukladno njegovoj primarnoj namjeni. Glavni utjecaj očituje se na interakciju korisnika odnosno na korisnikovu biometrijsku karakteristiku te na podsustav unosa biometrijskog sustava. Budući da je to ulaz u proces identifikacije ili verifikacije razvidno je da je, sukladno navedenome, i taj sami proces kompromitiran u svojoj primarnoj funkciji donošenja odluke o prihvaćanju ili neprihvaćanju biometrijske karakteristike korisnika.

Trenutno nije formulirana općeprihvaćena metodologija za ocjenu takovog utjecaja na pouzdano funkcioniranje biometrijskih sustava pa će u ovom poglavlju biti opisana metodologija za ocjenu ovoga aspekta biometrijskog sustava te njegovo uključivanje u metodu za evaluaciju pouzdanosti biometrijskih sustava. U nastavku opisana je metoda evaluacije utjecaja okoline na temelju zahtjeva međunarodnog standarda ISO/IEC TR 19795-3 Information technology -- Biometric performance testing and reporting -- Part 3: Modality specific testing

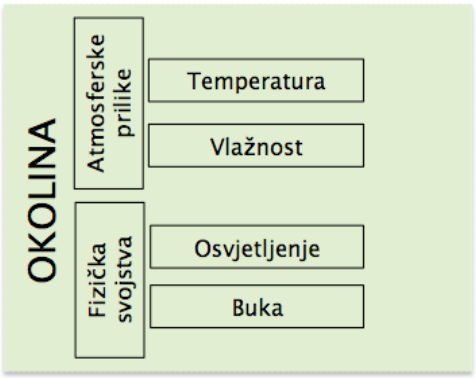
Sukladno navedenome standardu postoji više parametara okoline koji mogu biti uzeti u obzir radi ocjene utjecaja na biometrijski sustav ali svi ne utječu na biometrijski sustav na isti način. U ovom poglavlju fokusirati ćemo se na one parametre koji imaju utjecaj na korisnika sustava i njegovu biometrijsku karakteristiku te podsustav unosa biometrijskog sustava.

Evaluacijski model ne obuhvaća sve parametre (npr. utjecaj eventualnih vibracija, prašine, magle itd.) što ostavlja prostora za buduću nadogradnju otvorenog okvira za evaluaciju pouzdanosti biometrijskih sustava..

Činitelji aspekta okoline mogu se specificirati se kako slijedi:

- atmosferske prilike,
- fizička svojstva.

Činitelji aspekta okoline prikazani su na slici 13:



Slika 13 Aspekt okoline biometrijskog sustava sa pripadajućim činiteljima te parametrima

Atmosferske prilike su oni činitelji koji predstavljaju atmosferski utjecaj na biometrijski sustav putem manifestacija toga utjecaja na korisnika te interakciju korisnika sa biometrijskim sustavom.

Parametri putem kojih se može definirati utjecaj atmosferskih činitelja su sljedeći:

- Temperatura okoline (T).

Ovaj parametar kvantificira stupanj intenziteta topline koja vlada u okolini biometrijskog sustava, koji može utjecati na funkcioniranje biometrijskog sustava direktno ili indirektno preko utjecaja na korisnika. Definira se preko mjernih jedinica Kelvin [K] ili Celsius [°C].

Područje pouzdanosti ovoga parametra je temperatura od 10 °C do 40 °C ukoliko u tehničkoj dokumentaciji sustava nije navedeno drugačije.

- relativna Vlažnost (V).

Ovaj parametar kvantificira količinu vodene pare u zraku u okolini biometrijskog sustava, koji može utjecati na funkcioniranje biometrijskog sustava direktno ili indirektno preko utjecaja na korisnika biometrijskog sustava. Najraširenij način izražavanja ovoga parametra je korištenje stope vlažnosti koja predstavlja omjer količine vodene pare pri određenoj temperaturi i tlaku naspram maksimalne količine vodene pare koju može imati na istoj temperaturi i tlaku. Relativna vlažnost se može izraziti kroz postotak relativne vlažnosti[89] [%rh]. Područje pouzdanosti navedenog parametra je područje od 40%rh do 60%rh relativne vlažnosti ukoliko u tehničkoj dokumentaciji sustava nije navedeno drugačije.

Fizički činitelji su oni činitelji koji predstavljaju mikroklimatski utjecaj specifične lokacije na kojoj se biometrijski sustav nalazi.

Parametri putem kojih se može definirati utjecaj afizičkih činitelja su sljedeći:

- Osvjetljenje (O),

Ovaj parametar kvantificira količinu elektromagnetnog zračenja različitih valnih duljina elektromagnetskog spektra. Za funkcioniranje biometrijskog sustava a također i za korisnika biometrijskog sustava bitne su dvije metrike ovoga parametra: vidljivo područje osvjetljenja te nevidljivo područje zračenja. Osvjetljenje kvantificira vidljivi dio spektra elektromagnetnog zračenja kroz količinu svjetlosti koja udara u površinu sustava a koja je izražena putem mjerne jedinice lux [lx].

Slično osvjetljenju , zračenje kvantificira količinu elektromagnetskog zračenja koje udara u površinu sustava a koje pokriva cijeli elektromagnetni spektar a koje je izraženo putem mjerne jedinice, watt po metru kvadratnom [W/m2]. Područje pouzdanosti navedenog parametra je 1500-2000 lx ukoliko u tehničkoj dokumentaciji sustava nije navedeno drugačije.

- Buka (B),

[89] Izvorno: Relative humidity

Ovaj parametar kvantificira prisutnost zvuka određene jačine koja može utjecati na biometrijski sustav ili na korisnika tijekom uporabe sustava. Smetnja se naročito može očitovati utjecajima na biometrijske sustave koji se koriste analizom glasa te audio uputama korisnicima o tijeku procesa.

Najraširenija metrika ovoga parametra je razina buke izražen u decibelima [dB] . Područje pouzadnosti navedenog parametra je < 80 dB ukoliko u tehničkoj dokumentaciji sustava nije navedeno drugačije.

U tablici 2 dan je pregled činitelja pouzdanosti aspekta Okoline biometrijskih sustava sa definiranim područjima pouzdanosti biometrijskih sustava.

Tablica 2 Pregled činitelja aspekta okolina biometrijskog sustava

Aspekt	**Činitelj**	**Parametar**	**Metrike**	**Područje pouzdanosti**
Okolina	Fizička svojstva	Osvjetljenje (O)	lx	1500-2000
	Fizička svojstva	Buka (B)	dB	< 80
	Atmosferske prilike	Temperatura (T)	°C	10-40
	Atmosferske prilike	Vlažnost (V)	%rh	40-60

6.2.3 Aspekt korisnika biometrijskog sustava

Od samoga početka uporabe biometrijskih sustava postoje razmišljanja o utjecaju korisnika [96] na samo funkcioniranje sustava uzimajući u obzir npr. ponašanje korisnika tijekom faze unosa biometrijske karakteristike u sustav što ima direktan utjecaj na performanse biometrijskog sustava. Tijekom godina razvoja i uporabe biometrijskih sustava razvili su se različiti koncepti koji opisuju ovaj utjecaj a neki od njih su sljedeći: razina naviknutosti korisnika na sustav, razina očekivanosti biometrijskog sustava koji definira evaluaciju u smislu da li je sustav očekivan od strane korisnika ili ne , a koji se tradicionalno kroz literaturu nazivaju činitelji koji utječu na proces akvizicije biometrijske karakteristike korisnika. Recentna istraživanja opisuju različite specifične pristupe ocjeni navedenih utjecaja korisnika na funkcioniranje biometrijskih sustava kao što su: položaj senzora [90], dob

korisnika [91], spol korisnika, priviknutost korisnika , uvježbanost korisnika, dostupnost uputa za korištenje te povratne informacije od strane korisnika., pristupačnost biometrijskog sustava korisnicima sa hendikepom [47]. Svako od navedenih istraživanja koristi vlastitu metodologiju tako da opće prihvaćena metodologija ocjene utjecaja ovoga faktora na funkcioniranje biometrijskog sustava do sada nije formulirana.

Nedvojbeno iz do sada navedenog mogu se izlučiti dva pristupa analizi utjecaja korisnika na biometrijski sustav i to:

1. Činitelji koji ovise o podsustavu unosa biometrijske karakteristike u sustav,

   Ova grupa faktora podrazumjeva analizu činitelja koji se odnose na dizajn, poziciju ili stanje podsustava unosa biometrijske karakteristike, imaju značajan utjecaj na interakciju korisnika sa sustavom te na sami ishod procesa unosa biometrijske karakteristike u sustav pa tako i na performanse sustava.

2. Činitelji koji ovise o korisniku biometrijskog sustava,

   Ova grupa faktora obuhvaća biometrijske karakteristike putem kojih korisnik interagira sa sustavom. Biometrijske karakteristike zbog velikog broja faktora značajno utječu na performanse biometrijskog sustava.

Za potrebe ovoga doktorskog rada definirati će se činitelji aspekta Korisnika biometrijskog sustava na sljedeći način:

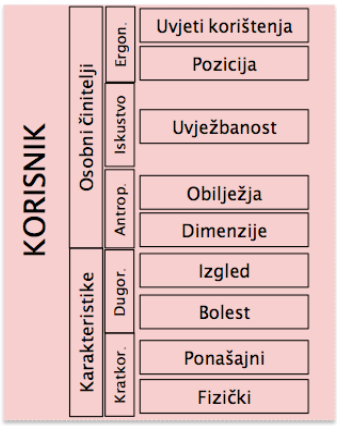
- činitelj biometrijske karakteristike,
  - kratkoročni utjecaj – predstavlja utjecaj na funkcioniranje sustava koji se može korigirati tijekom interakcije korisnik-sustav,
    - Ponašajni utjecaj predstavlja utjecaj korisnikovog ponašanja tijekom interakcije sa biometrijskim sustavom kao što može biti ekspresija emocija , sreće, tuge , zabrinutosti itd.,
    - Fizički utjecaj predstavlja utjecaj korisnika na senzor ili senzora na korisnika koji se manifestira fizičkim djelovanjem kemikalija ili supstanci koje su prisutne na korisniku ili na samom senzoru (npr. kreme ili druge supstance) koje mogu djelomično ili potpuno prekriti senzor,
  - dugoročni utjecaj – predstavlja utjecaj na funkcioniranje sustava koji se ne

može korigirati tijekom interakcije korisnik-sustav,

- Bolest predstavlja utjecaj kada se određena biometrijska karakteristika mijenja te je nemoguća identifikacija korisnika (npr. prehlada u modalitetu prepoznavanja glasa),
- Izgled predstavlja utjecaj vanjskih obilježja korisnika biometrijskih sustava (npr. kosa, brkovi itd.),

- osobni činitelji korisnika,
  - antropometrija – predstavlja utjecaj antropometrijskih karakteristika korisnika biometrijskog sustava,
    - tjelesna obilježja predstavljaju obilježja koja su prirođena korisniku (npr. boja kose ili očiju, položaj tijela itd.),
    - tjelesne dimenzije predstavljaju obilježja koja su stečena od strane korisnika (npr. debljina, mršavost),
  - iskustvo – predstavlja utjecaj iskustva korisnika prilikom korištenja biometrijskog sustava , na funkcioniranje biometrijskog sustava,
    - uvježbanost predstavlja razina utjecaja uvježbanosti korisnika za korištenje funkcionalnosti biometrijskog sustava,
  - osjetljivost na ergonomiju – predstavlja utjecaj fizičke izvedbe implementiranog biometrijskog sustava na interakciju sa korisnikom tijekom funkcioniranja biometrijskog sustava,
    - uvjeti korištenja – predstavljaju utjecaj eventualnih nečistoća ili oštećenja prisutnih na senzoru biometrijskog sustava na interakciju sa korisnikom pa sukladno tomu i na funkcioniranje biometrijskog sustava,
    - pozicija – predstavlja utjecaj putem visine senzora, orjentacije te nagiba senzora na korisnika i njegovu interakciju sa biometrijskim sustavom.

Slika 14 prikazuje definiciju činitelja aspekta korisnika biometrijskih sustava.



Slika 14 Aspekt korisnika biometrijskog sustava sa pripadajućim činiteljima te parametrima

Metrike parametara činitelja aspekta korisnika biometrijskih sustava predstavljaju procjenu utjecaja svakoga parametra na interakciju korisnika sa sustavom te na funkcioniranje samog sustava putem utjecaja na inherentnu pouzdanost biometrijskog sustava.

Metrike se definiraju kao procjena razine utjecaja:

- Mali – vrijednost 1, kada se interakcija korisnika sa sustavom odvija bez smetnji,

- Srednji – vrijednost 2, kada se interakcija korisnika sa sustavom odvija sa malim otklonjivim smetnjama, te

- Veliki - vrijednost 3, kada je interakcija korisnika sa sustavom onemogućena.

Procjena utjecaja predstavlja arbitrarnu vrijednost koju dodjeljuje evaluator u trenutku evaluacije sukladno predefiniranim parametrima.

Područje pouzdanosti se definira kao procjena ustjecaja koja predstavlja vrijednosti <=2.

Tablica 3 predstavlja sistematizaciju činitelja aspekta korisnik sa pripadajućim parametrima utjecaja , metrikama parametara te područjem pouzdanosti za svaki parametar.

Tablica 3 Pregled činitelja aspekta Korisnik

Aspekt	**Činitelj**	**Parametar**	**Metrike**	**Područje pouzdanosti**
Korisnik	Karakteristike	Kratkoročni utjecaj: - ponašajni (PON) - fizički (FIZ)	Mali -1 Srednji-2 Veliki-3	<=2
Korisnik	Karakteristike	Dugoročni utjecaj: - Izgled (IZG) - Bolest (BOL)	Mali -1 Srednji-2 Veliki-3	<= 2
Korisnik	Osobni činitelji	Antropometrija: - Obilježja (OBI) - Dimenzije (DIM)	Mali -1 Srednji-2 Veliki-3	<= 2
Korisnik	Osobni činitelji	Iskustvo: - Uvježbanost (UVJ)	Mali -1 Srednji-2 Veliki-3	<= 2
Korisnik	Osobni činitelji	Ergonomija: - Uvjeti korištenja (UV.KOR) - Pozicija (POZ)	Mali -1 Srednji-2 Veliki-3	<= 2

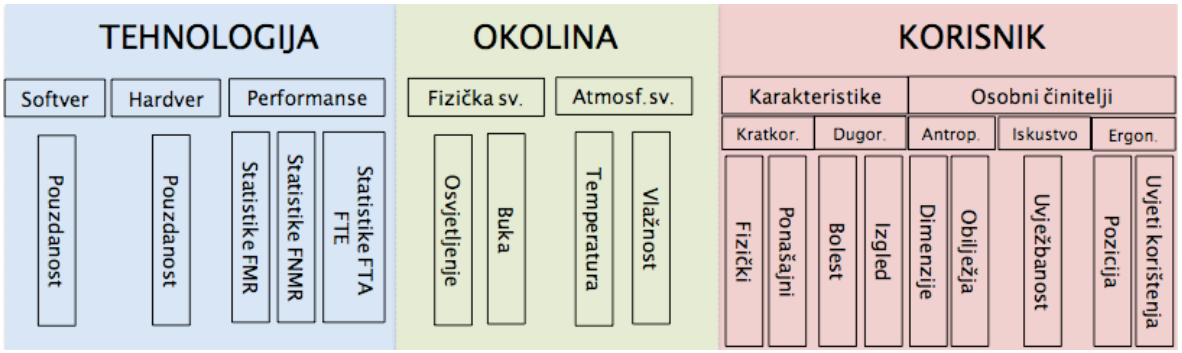
6.3 Evaluacijski model OOEPBS

Na temelju definiranog konceptualnog modela trijade aspekata biometrijskih sustava u ovom poglavlju biti će predstavljena parametrizacija pojedinih činitelja pouzdanosti biometrijskog sustava putem definiranja metrika za svaki specifični parametar, koje će biti u funkciji definicije modela za evaluaciju pouzdanosti biometrijskih sustava te poslužiti kao temelj za definiranje metode za evaluaciju biometrijskih sustava.

U prethodnim poglavljima predstavljen je opis aspekata pouzdanosti biometrijskih sustava sa pripadajućim činiteljima, koji utječu na funkcioniranje sustava a samim time i na njegovu pouzdanost glede izvršavanja operativne funkcije u okviru određenog konteksta uporabe. Glavna ideja ove disertacije je objedinjavanje trijade aspekata biometrijskih sustava i njihovih činitelja u metodu za evaluaciju pouzdanosti biometrijskih sustava po modelu Otvorenog okvira za evaluaciju pouzdanosti biometrijskih sustava - OOEPBS. Model je zamišljen kao otvoreni okvir, predisponiran za daljnju nadogradnju te poboljšavanja.

Otvoreni okvir za evaluaciju pouzdanosti biometrijskih sustava OOEPBS podrazumijeva definiciju činitelja koji utječu na pouzdanost biometrijskih sustava sukladno pretpostavkama konceptualnog modela poglavlja 6.2 slika 10.

Konceptualni model se može prikazati uzimajući u obzir strukturu pojedinih aspekata tijekom funkcioniranja biometrijskih sustava kao što je prikazano na slici 15:



Slika 15 Trijada aspekata biometrijskog sustava

Pretpostavka ovoga modela jeste da svi aspekti međusobno imaju podjednak i presudan utjecaj na pouzdan rad i funkcioniranje biometrijskog sustava tada se može definirati funkcija međusobnog utjecaja sukladno onome definiranom u Poglavlju 4.2.1.1 pretpostavljajući serijsku ovisnost trijade aspekata biometrijskog sustava prikazane na slici 15.

Objedinjavajući činitelje aspekata biometrijskog sustava funkcijom međusobnog utjecaja te utjecaja na pouzdano funkcioniranje biometrijskog sustava možemo oblikovati model na način da se pretpostavi serijska ovisnost parametara evaluacijskog modela sukladno izrazu (4) kao funkcija koja međusobno povezuje parametre pouzdanosti.

Pretpostavljajući serijsku ovisnost parametara pouzdanosti biometrijskog sustava može se preliminarno definirati model OOEPBS kako slijedi:

OOEPBS= { **f**(Aspekt_korisnika

Karakteristike

Kratkoročni_utjecaj (fizički,ponašajni)

Dugoročni_utjecaj (bolest,izgled)

Osobni činitelji

Antropometrija (tjelesna_obilježja, tjelesne_dimenzije)

Iskustvo (uvježbanost_korisnika)

Ergonomija (pozicija, uvjeti_korištenja)

Aspekt_okoline

Fizička_svojstva

Osvjetljenje

Buka

Atmosferska_svojstva

Temperatura

Vlažnost

Aspekt_tehnologije

Softver

Pouzdanost

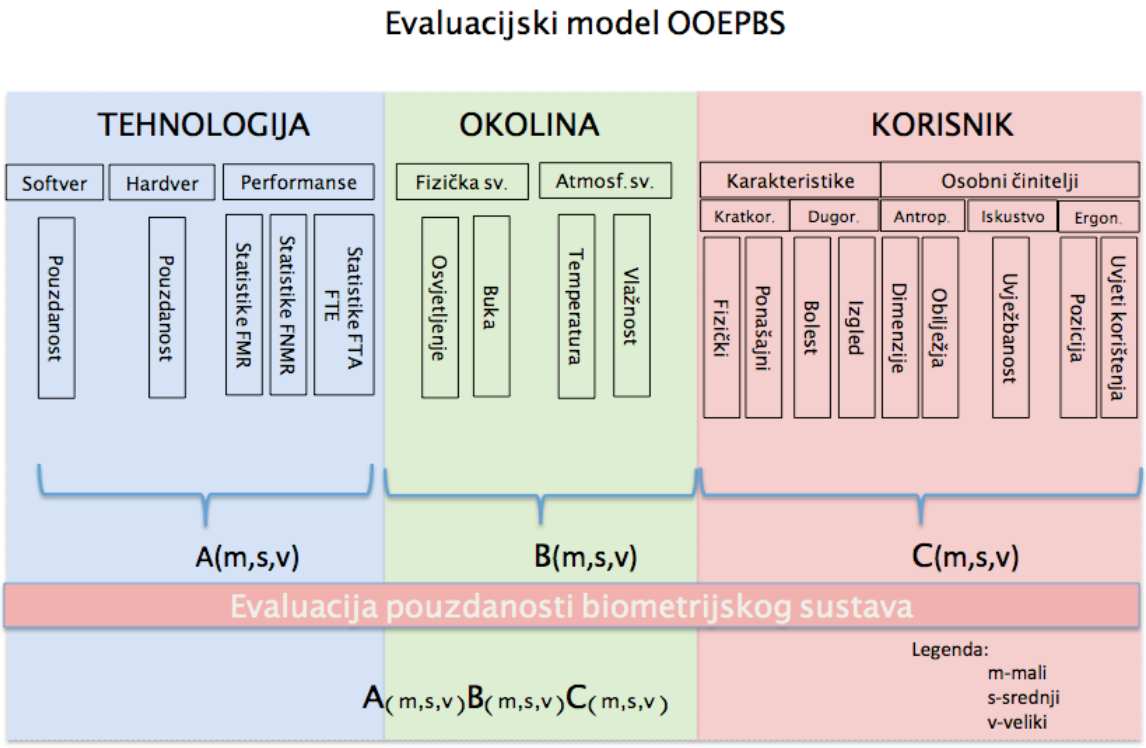
Hardver

Pouzdanost

Performanse

Statistike (FMR,FNMR,FTE;FTA)}

Slika 16 prikazuje evaluacijski model OOEPBS objedinjavajući aspekte pouzanosti te pripadajuće činitelje definirane u prethodnim poglavljima sa definiranim parametrima utjecaja na pouzdanost cijelovitog sustava:



Slika 16 Evaluacijski model OOEPBS

Model uzima u obzir aspekte biometrijskog sustava sukladno definiranim činiteljima te pripadajućim parametrima. Svaki činitelj pouzdanosti predstavlja jedan segment čiji rezultat evaluacije čini jednu od komponenata ocjene pouzdanosti biometrijskog sustava. Radi lakšeg shvaćanja modela rezultati evaluacije sukladno činiteljima pouzdanosti te pripadajućim parametrima označeni su na sljedeći način: *A*- rezultat evaluacije utjecaja aspekta tehnologije, *B* – rezultat evaluacije utjecaja aspekta okoline te *C* – rezultat evaluacije utjecaja aspekta korisnika biometrijskog sustava. Rezultat je izražen gradacijom utjecaja kako je prikazano na slici 16, *m*- mali, *s*-srednji i *v*-veliki. Rezultat evaluacije jeste parametar *A(vrijednost)B(vrijednost)C(vrijednost)* putem kojega se može rezonirati o razini pouzdanosti biometrijskog sustava te indikacija o utjecaju pojedinih činitelja na pouzdano funkcioniranje biometrijskog sustava.

Objedinjavanjem sadržaja tablica 1, 2 te 3 dobivamo pregled svih definiranih činitelja pouzdanosti biometrijskog sustava sa pregledom metrika te područja pouzdanosti odnosno nepouzdanosti funkcioniranja biometrijskog sustava (PRILOG A).

Definirani model, u sljedećem poglavlju, biti će detaljno opisan u obliku Metode za evaluaciju pouzdanosti biometrijskih sustava.

6.4 Evaluacijska metoda sukladno modelu OOEPBS

Evaluacija [95] odnosno vrijednovanje predstavlja sistematičnu akviziciju i procjenu informacija radi dobivanja zaključka o promatranom objektu ili problematici.

6.4.1 Tipologije evaluacijskih metoda

Glavni cilj koji proizilazi iz definicije jeste da evaluacija mora proizvesti koristan zaključak ili povratnu informaciju zainteresiranim stranama. Zaključak se može smatrati korisnim ako je od pomoći u procesu odlučivanja o danom problemu ili objektu evaluacije. Usprkos važnosti veza između rezultata evaluacije i utjecaja na proces donošenja odluka je kompleksna jer podrazumijeva predviđanje modela zakonitosti utjecaja na odluke kratkoga te dugoga roka. Bez obzira na kompleksnost važno je istaknuti da je neophodno postaviti za cilj evaluacije utjecaj na donošenje odluka ili definiranje politika za buduće pristupe problematici.

Tipologije evaluacija [44] se uopćeno mogu podijeliti na sljedeće dvije grupe:

- Kvalitativne

  Kvalitativne evaluacije koriste radije opisne podatke negoli brojčane.Ova tipologija evaluacija se uglavnom koristi u formativnim procesima prenošenja znanja na zainteresirane strane.

- Kvantitativne

  Kvantitativne evaluacije koriste brojčane vrijednosti te također kao rezultat imaju brojčani rezultat ili kombinaciju znakova.Ova metoda evaluacije najčešća je kada se procjenjuje postizanje određene namjere ili namjene od strane promatranog objekta ili problematike

Kao rezultat ove evaluacijske metode može se koristiti tzv. matrica predefiniranih vrijednosti (scenarija). Matrica predefiniranih vrijednosti predstavlja skup vrijednosti koje mogu postići dobivene vrijednosti evaluacijskog modela a koje se klasificiraju po predefiniranim razinama. Ovaj način predstavljanja vrijednosti zastupljen je u metodologijama za procjenu rizika. Model OOEPBS biti će razvijen sukladno opisanoj metodologiji.

Model OOEPBS predstavlja okvir na temelju kojega se može razviti metoda za evaluaciju pouzdanosti biometrijskih sustava uzimajući u obzir poznate vrijednosti definiranih činitelja pouzdanosti te ocjene utjecaja pojedinih činitelja na aspekte pouzdanosti biometrijskog sustava pa tako i na sami biometrijski sustav. Opisani aspekti pouzdanosti biometrijskog sustava predstavljaju komponente utjecaja na pouzdanost samog sustava tijekom izvršenja operativne funkcije sustava u interakciji sa korisnikom sustava a sve pod utjecajem okoline u kojoj se interakcija odvija. Evaluacija pouzdanosti biometrijskih sustava predstavlja neizostavan proces u svim fazama životnog ciklusa biometrijskog sustava kao proizvoda koji ima svoj pročetak, tijek uporabe te kraj. Prije stavljanja u uporabu cilj evaluacije jeste ukazivanje na ranjivosti ili kritične točke biometrijskih sustava tijekom uporabe unutar određenog konteksta. Identifikacija slabosti te njihovo poboljšanje može dovesti do bolje implementacije sustava u zadani kontekst te bolju prihvaćenost biometrijskog sustava od strane korisnika sustava. Kontinuirana evaluacija tijekom uporabe sustava neophodna je radi održavanja operativne funkcije sustava na odgovarajućem predefiniranom razinau uzimajući u obzir povratne informacije koje dolaze iz samog sustava ,npr. statističke analize performansi, te one koje dolaze od strane korisnika sustava glede uporabljivosti sustava i njegove primjerenosti kontekstu uporabe. U ovom poglavlju biti će opisani ciljevi, standardni uvjeti, postupak te rezultat evaluacije kroz proces rezoniranja o rezultatu evaluacijskog postupka. Definiranje ove evaluacijske metode poslužiti će se ispitivanje hipoteze H1 te njeno prihvaćanje ili odbijanje.

6.4.2 Definiranje ciljeva evaluacije

Metoda evaluacije sukladno modelu OOEPBS potpada pod kategoriju metoda matrice predefiniranih vrijednosti ili evaluacije scenarija i kao takova ima sljedeće ciljeve:

• Detaljan opis biometrijskog sustava koji se evaluira uključno sa tehničkim podacima o sustavu: Naziv, serijski broj, modalitet, lokacija uporabe,

• Detaljan opis konteksta uporabe: verifikacija jedan na jedan ili identifikacija jedan na više,

• Detaljan opis konteksta okoline sustava unutar koje sustav funkcionira uključno sa opisom atmosferskih i fizičkih značajki okoline sustava te otvorenosti i nadzora okoline sustava,

• Detaljan opis konteksta korisnika biometrijskog sustava uključno sa procjenama grupa korisnika koji će koristiti sustav,

• Detaljan opis standardnih operativnih uvjeta funkcioniranja biometrijskog sustava koji utječu na pouzdanost sustava kako je opisano u prethodnim poglavljima,

• Detaljan opis rezultata evaluacije biometrijskog sustava.

6.4.3 Definiranje evaluacijskih parametara

6.4.3.1 Tehnologija biometrijskog sustava

Vodič za uporabu biometrijskog sustava važan je segment za evaluaciju ovoga činitelja pouzdanosti. Ovaj dokument mora uključivati detaljne opise biometrijskih funkcija koje su implementirane unutar sustava te kako iste funkcije djeluju te kakovi su njihovi očekivani izlazni parametri. Vodič mora uključivati izjavu proizvođača sustava o procjeni pouzdanosti hardvera i softvera te testiranih performansi sustava (npr. FMR, FNMR, FTA, FTE) .

Detalji podaci koji su od važnosti su također oni o rezultatima testiranja biometrijskog sustava u smislu hardvera, softvera te performansi sustava sukladno opisanome u Poglavlju 6.2.1.

Izjava o sukladnosti sa zahtjevima kvalitete softvera i hardvera te pripadajući certifikati kvalitete predstavljaju osnovu za proces evaluacije. Ukoliko navedena dokumentacija nije isporučena sa biometrijskim sustavom istu je potrebno zatražiti od proizvođača ili prodavača sustava.

Parametri koji su predmet evaluacije predstavljaju:

- vrijednosti pouzdanosti (*P*) hardvera biometrijskog sustava koji su izraženi u postotku (%) te koji su sadržani u tehničkoj dokumentaciji biometrijskog sustava.
- vrijednosti pouzdanosti (*P*) softvera biometrijskog sustava koji su izraženi u postotku (%) te koji su sadržani u tehničkoj dokumentaciji biometrijskog sustava.
- vrijednosti statistika performansi (*S*) putem parametara FMR te FNMR odnosno FTE,

FTA a koji su izraženi u postotku (%) te koji su sadržani u tehničkoj dokumentaciji biometrijskog sustava.

Vrijednosti navedenih parametara se kroz proces evaluacije porede sa definiranim područjem pouzdanosti kako je prikazano u Tablici 1.

6.4.3.2 Okolina biometrijskog sustava

Okolina biometrijskog sustava sukladno Poglavlju 6.2.2. predstavlja operativno okruženje unutar kojega biometrijski sustav funkcionira. Okolina predstavlja skup utjecaja kako na korinika tako i na sami biometrijski sustava tako da je evaluacija ovoga aspekta bitan dio evaluacijskog procesa radi definiranja područja od značaja za pouzdanost biometrijskog sustava.

Parametri koji su predmet evaluacije su sljedeći:

- vrijednosti temperature (T) koja vlada u okolini biometrijskog sustava a koja je izražena u stupnjevima Celzijusa (°C)
- vrijednosti vlažnosti (V) koja vlada u okolini biometrijskog sustava a koja je izražena u postotku relativne vlažnosti [%rh]
- vrijednosti osvjetljenja (O) koje vlada u okolini biometrijskog sustava a koja je izražena u jačini osvjetljenja lux [lx]
- vrijednosti buke (B) koja koja je prisutna u okolini biometrijskog sustava a koja je izražena u jačini buke (dB)

Vrijednosti navedenih parametara se kroz proces evaluacije porede sa definiranim područjem pouzdanosti kako je prikazano u Tablici 2. Područje pouzdanosti definirano u tablici vrijedi ukoliko u tehničkoj dokumentaciji biometrijskog sustava nije navedeno drugačije.

Evaluacija biometrijskog sustava po scenariju može biti provedena u laboratorijskim kontroliranim uvjetima prije implementacije u realno operativno okruženje. Prije takovoga postupka važno je definirati : okolišne uvjete te evaluacijske uvjete u kojima će sustav biti evaluiran te koji će se uspoređivati za zadanim vrijednostima parametara.

6.4.3.3 Korisnik biometrijskog sustava

Korisnik biometrijskog sustava predstavlja svrhu postojanja biometrijskog sustava te ispunjenje osnovne namjene operativne funkcije biometrijskog sustava. Sukladno iznešenome u poglavlju 6.2.3. korisnik predstavlja jednu od komponenti procesa evaluacije pouzdanosti biometrijskih sustava zbog mogućnosti utjecaja na sami biometrijski sustav te na njegove performanse a sukladno tomu i na rezultat procesa biometrijske identifikacije ili verifikacije.

Parametri koji su predmet evaluacijskog procesa su sljedeći:

- vrijednosti procjene utjecaja fizičkih (FIZ) te ponašajnih (PON) obilježja korisnika na performanse sustava,
- vrijednosti procjene utjecaja eventualne bolesti (BOL) te izgleda (IZG) korisnika na performanse sustava,
- vrijednosti procjene utjecaja antropometrije izražene kroz tjelesna obilježja (OBI) te dimenzije (DIM) korisnika na performanse sustava,
- vrijednosti procjene utjecaja iskustva korisnika na performanse sustava preko procjene utjecaja uvježbanosti (UVJ) korisnika,
- vrijednosti procjene utjecaja ergonomije biometrijskog sustava izražene kroz uvjete korištenja (UV.KOR) te poziciju (POZ) sustava na korisnika biometrijskog sustava pa tako i na performanse biometrijskog sustava.

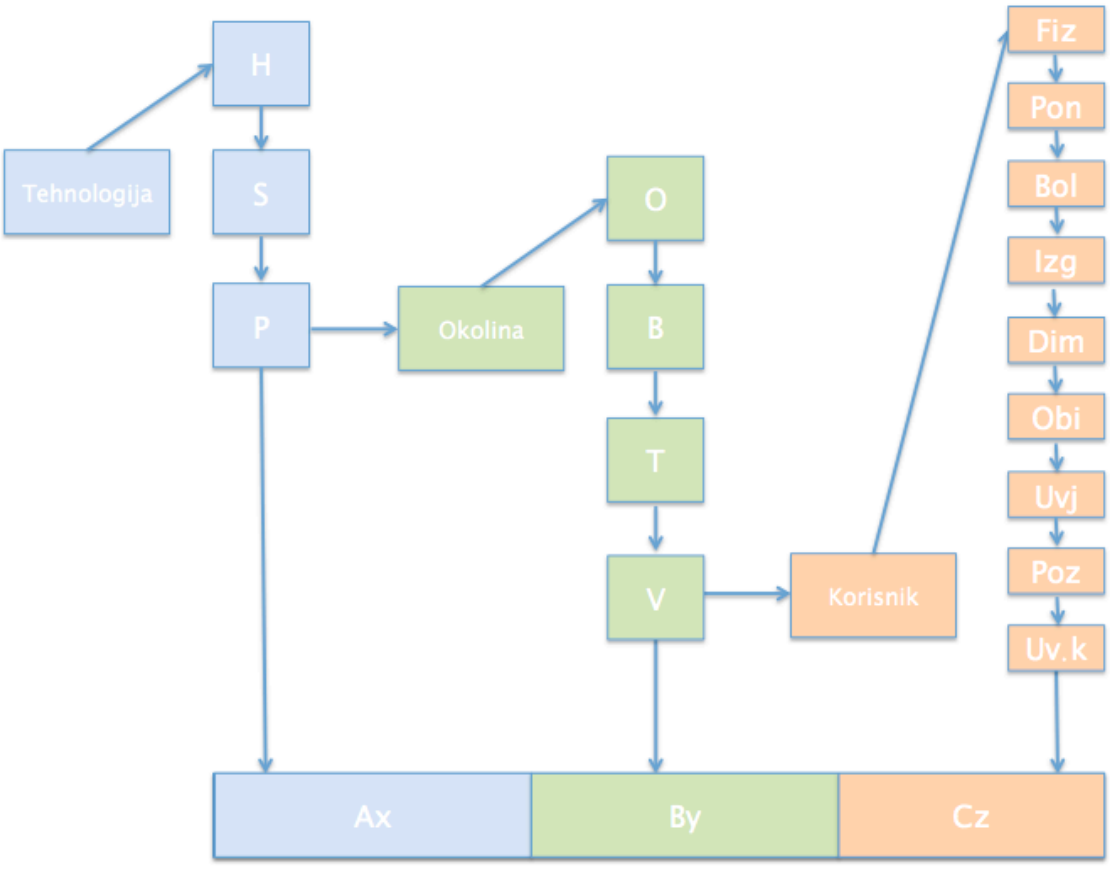
Vrijednosti navedenih parametara se kroz proces evaluacije porede sa definiranim područjem pouzdanosti kako je prikazano u Tablici 3. Područje pouzdanosti definirano u tablici vrijedi sukladno procjeni evaluatora koji uzima u obzir kontekst primjene specifičnog biometrijskog sustava. Utjecaj na inherentnu pouzdanost biometrijskog sustava mora biti što manji da bi činitelj doprinosio pouzdanosti cijelog sustava te da bi se utjecaji koji su inherentni korisniku bili svedeni na minimum.

6.4.4 Definiranje postupka evaluacije

Sukladno navedenome u prethodnom poglavlju može se definirati postupak evaluacije pouzdanosti biometrijskog sustava kao slijed pojedinačnih evaluacija aspekata sa pripadajućim činiteljima te parametrima.

Slijed evaluacijskog postupka predstavlja niz evaluacijskih operacija koje mogu biti grafički predstavljene kao na slici 17. na kojoj je opisan tijek pojedinačnih evaluacijskih postupaka a koji uzimaju u obzir sve definirane parametre aspekata pouzdanosti biometrijskih sustava.

Tijek evaluacije se provodi na temelju postojeće dokumentacije sustava, ocjene konteksta uporabe uzimajući u obzir uvjete okoline biometrijskog sustava te grupe korisnika kojoj je namjenjen, putem procjene utjecaja pojednih aspekata na inherentnu pouzdanost biometrijskog sustava.



Slika 17 Tijek evaluacije po modelu OOEPBS

Gdje je:

Tehnologija : *H*-Hardver, *S*- softver, *P*- performanse

Okolina : *O*- Osvjetljenje, *B*- Buka, *T*- Temperatura, *V*- Vlažnost

Korisnik: *Fiz* – Fizički utjecaji, *Pon* – Ponašajni utjecaji, *Bol* – Bolest, *Izg* – Izgled, *Dim* – Dimenzije , *Obi* – Obilježja, *Uvj* – Uvježbanost, *Poz* – Pozicija, *Uv.k* – Uvjeti korištenja

Opis postupka evaluacije:

a. Parametri skupine Tehnologija evaluiraju se poredbom sa definiranim standardnim vrijednostima. Rezultat usporedbe predstavlja evaluacijsku vrijednost iz skupine *A* (vidjeti sliku 16.).

- vrijednosti pouzdanosti hardvera biometrijskog sustava koji su izraženi u postotku (%) te se porede sa standardnim vrijednostima (vidjeti tablicu 1),
- vrijednosti pouzdanosti softvera biometrijskog sustava koji su izraženi u postotku (%) te se porede sa standardnim vrijednostima (vidjeti tablicu 1),
- vrijednosti parametara FMR te FNMR, FTE te FTA, koji su izraženi u postotku (%) te se porede sa standardnim vrijednostima (vidjeti tablicu 1).

Evaluacijska vrijednosti može zaprimiti sljedeće veličine *A1*, *A2* ili *A3* ovisno o vrijednosti dobivene nakon usporedbe.

b. Parametri skupine Okolina evaluiraju se usporedbom sa definiranim standardnim vrijednostima. Rezultat usporedbe predstavlja evaluacijsku vrijednost iz skupine *B* (vidjeti sliku 16.).

- vrijednosti temperature koja vlada u okolini biometrijskog sustava a koja je izražena u stupnjevima Celzijusa (°C) te se porede sa standardnim vrijednostima sukladno Tablici 2,
- vrijednosti vlažnosti koja vlada u okolini biometrijskog sustava a koja je izražena u postotku relativne vlažnosti [%] te se porede sa standardnim vrijednostima sukladno Tablici 2,
- vrijednosti osvjetljenja koje vlada u okolini biometrijskog sustava a koja je izražena u jačini osvjetljenja lux [lx], te se porede sa standardnim vrijednostima sukladno Tablici 2,

- vrijednosti buke koja koja je prisutna u okolini biometrijskog sustava a koja je izražena u jačini buke (dB) te se porede sa standardnim vrijednostima sukladno Tablici 2.

Evaluacijska vrijednosti može zaprimiti sljedeće veličine: *B1*, *B2* ili *B3* ovisno o vrijednosti dobivene nakon usporedbe.

c. Parametri skupine Korisnik evaluiraju se usporedbom sa definiranim standardnim vrijednostima. Rezultat usporedbe predstavlja evaluacijsku vrijednost iz skupine *C* (vidjeti sliku 16.).

- vrijednosti procjene utjecaja fizičkih te ponašajnih obilježja korisnika na performanse sustava koji se porede sa definiranim standardnim vrijednostima sukladno Tablici 3,
- vrijednosti procjene utjecaja eventualne bolesti te izgleda korisnika na performanse sustava koji se porede sa definiranim standardnim vrijednostima sukladno Tablici 3,
- vrijednosti procjene utjecaja antropometrije izražene kroz tjelesna obilježja te dimenzije korisnika na performanse sustava koji se porede sa definiranim standardnim vrijednostima sukladno Tablici 3,
- vrijednosti procjene utjecaja iskustva korisnika na performanse sustava, putem procjene uvježbanosti, koji se porede sa definiranim standardnim vrijednostima sukladno Tablici 3,
- vrijednosti procjene utjecaja antropometrije izražene kroz izražena obilježja te dimenzije korisnika na performanse sustava koji se porede sa definiranim standardnim vrijednostima sukladno Tablici 3,
- vrijednosti procjene utjecaja osjetljivosti na ergonomiju biometrijskog sustava izražene kroz uvjete korištenja te poziciju sustava na korisnika biometrijskog sustava pa onda i na performanse biometrijskog sustava koji se porede sa definiranim standardnim vrijednostima sukladno Tablici 3.

Evaluacijska vrijednosti može zaprimiti sljedeće veličine *C1*, *C2* ili *C3* ovisno o vrijednosti dobivene nakon usporedbe.

Evaluacija se može vršiti putem evaluacijskog obrasca (PRILOG B).

6.4.5 Definiranje rezultata evaluacije

Nakon završenog postupka evaluacije sukladno definicijama iz prethodnog poglavlja dobiti će se evaluacijske vrijednosti za svaki evaluirani aspekt pouzdanosti biometrijskog sustava. Rezultati evaluacije proizišli iz evaluacijskog postupka , sukladno evaluacijskom modelu OOEPBS, mogu biti definirani te prezentirani kako slijedi:

Aspekt Tehnologije:

Rezultati evaluacije aspekta tehnologije prikazani su u tablici 4:

Tablica 4 Rezultati evaluacije aspekta korisnik

		Softver	Hardver	Performanse	
Tehnologija	A1	P>90	P>90	S<0,01	PO
	A2	80<P<90	80<P<90	0,01<S<0,02	DP
	A3	P<90	P<90	S>0,02	NP

Gdje se rezultati mogu interpretirati na sljedeći način:

Evaluacijska vrijednost *A1* predstavlja područje pouzdanosti činitelja softver $P>90\%$, činitelja hardver $P>90\%$ te činitelja Performanse $S<0{,}01\%$ što se može identificirati kao područje pouzdanosti (*PO*) što znači područje malog utjecaja na inherentnu pouzdanost biometrijskog sustava.

Evaluacijska vrijednost *A2* predstavlja područje pouzdanosti činitelja softver $80\%<P<90\%$, činitelja hardver $80\%<P<90\%$ te činitelja Performanse $0{,}01\%<S<0{,}02\%$ što se može identificirati kao područje djelomične pouzdanosti (*DP*) što znači područje srednjeg utjecaja na inherentnu pouzdanost biometrijskog sustava.

Evaluacijska vrijednost *A3* predstavlja područje pouzdanosti činitelja softver $P<90\%$, činitelja hardver $P<90\%$ te činitelja Performanse $S>0{,}02\%$ što se može identificirati kao područje nepouzdanosti (*NP*) što znači područje velikog utjecaja na inherentnu pouzdanost biometrijskog sustava.

Aspekt Okoline:

Rezultati evaluacije aspekta tehnologije prikazani su u tablici 5:

Tablica 5 Rezultati evaluacije aspekta okoline

		Temperatura	Vlažnost	Osvjetljenje	Buka	
Okolina	B1	10<T<40	40<H<60	1500<Lx<2000	dB<80	PO
	B2	10>T	40>H	1500>Lx	80<db<90	DP
	B3	40<T	60<H	2000<Lx	dB>90	NP

Evaluacijska vrijednost *B1* predstavlja područje pouzdanosti parametra temperatura 10°C <*T*<40°C, parametra vlažnost 40%<*H*<60% , parametra osvjetljenje 1500lx<Jačina<2000lx , parametra buka jačina<80dB što se može identificirati kao područje pouzdanosti (*PO*) što znači područje malog utjecaja na inherentnu pouzdanost biometrijskog sustava.

Evaluacijska vrijednost *B2* predstavlja područje pouzdanosti parametra temperatura 10°C >*T*, parametra vlažnost 40%>*H* , parametra osvjetljenje 1500lx>Jačina , parametra buka 80dB<jačina<90dB što se može identificirati kao područje djelomične pouzdanosti (*DP*) što znači područje srednjeg utjecaja na inherentnu pouzdanost biometrijskog sustava.

Evaluacijska vrijednost *B3* predstavlja područje pouzdanosti parametra temperatura 40°C <*T*, parametra vlažnost 60%<*H* , parametra osvjetljenje 2000lx<Jačina , parametra buka 90dB<jačina što se može identificirati kao područje nepouzdanosti (*NP*) što znači područje velikog utjecaja na inherentnu pouzdanost biometrijskog sustava.

Aspekt korisnika:

Rezultati evaluacije aspekta korisnika prikazani su u tablici 6:

Tablica 6 Rezultati evaluacije aspekta okoline

		Ponaš.	Fizički	Bolest	Izgled	Obilj.	Dim.	Poz.	Uvj.	
Korisnik	C1	1	1	1	1	1	1	1	1	PO
	C2	2	2	2	2	2	2	2	2	DP
	C3	3	3	3	3	3	3	3	3	NP

Evaluacijska vrijednost *C1* predstavlja područje pouzdanosti parametra ponašajni utjecaj 1 (mali), parametra fizički utjecaj 1 (mali) , parametra utjecaj bolesti 1 (mali), parametra utjecaj izgleda 1 (mali), parametra utjecaj obilježja 1 (mali), parametra utjecaj dimenzija 1 (mali),

parametra utjecaj pozicije 1 (mali), parametra utjecaj uvjeta korištenja 1 (mali), što se može identificirati kao područje pouzdanosti (*PO*) što znači područje malog utjecaja na inherentnu pouzdanost biometrijskog sustava.

Evaluacijska vrijednost *C2* predstavlja područje pouzdanosti parametra ponašajni utjecaj 2 (srednji), parametra fizički utjecaj 2 (srednji), parametra utjecaj bolesti 2 (srednji), parametra utjecaj izgleda 2 (srednji), parametra utjecaj obilježja 2 (srednji), parametra utjecaj dimenzija 2 (srednji), parametra utjecaj pozicije 2 (srednji), parametra utjecaj uvjeta korištenja 2 (srednji) što se može identificirati kao područje djelomične pouzdanosti (*DP*) što znači područje srednjeg utjecaja na inherentnu pouzdanost biometrijskog sustava. Evaluacijska vrijednost *C* zaprima vrijednost *C2* ako bilo koji parametar ima vrijednost 2 a ostali imaju vrijednost 1.

Evaluacijska vrijednost *C3* predstavlja područje pouzdanosti parametra ponašajni utjecaj 3 (veliki), parametra fizički utjecaj 3 (veliki), parametra utjecaj bolesti 3 (veliki), parametra utjecaj izgleda 3 (veliki), parametra utjecaj obilježja 3 (veliki), parametra utjecaj dimenzija 3 (veliki), parametra utjecaj pozicije 3 (veliki), parametra utjecaj uvjeta korištenja 3 (veliki) što se može identificirati kao područje nepouzdanosti (*NP*) što znači područje velikog utjecaja na inherentnu pouzdanost biometrijskog sustava. Evaluacijska vrijednost *C* zaprima vrijednost *C3* ako bilo koji parametar ima vrijednost 3 a ostali imaju vrijednost 1 ili 2.

Pregled stanja ovoga evaluacijskog modela može biti prikazan Tablicom 7:

Tablica 7 Pregled stanja evaluacijskog modela

		Aspekt tehnologije								
Aspekt okoline		A1	A1	A1	A2	A2	A2	A3	A3	A3
	B1	A1B1C1	A1B1C2	A1B1C3	A2B1C1	A2B1C2	A2B1C3	A3B1C1	A3B1C2	A3B1C3
	B2	A1B2C1	A1B2C2	A1B2C3	A2B2C1	A2B2C2	A2B2C3	A3B2C1	A3B2C2	A3B2C3
	B3	A1B3C1	A1B3C2	A1B3C3	A2B3C1	A2B3C2	A2B3C3	A3B3C1	A3B3C2	A3B3C3
		C1	C2	C3	C1	C2	C3	C1	C2	C3
		Aspekt korisnika								

Pregledom stanja evaluacijskog modela definirana su sva stanja evaluacijskih vrijednosti koje proizilaze iz evaluacijskog procesa sukladno metodi za evaluaciju pouzdanosti biometrijskog sustava.

Područja označena zelenom bojom predstavljaju područja pouzdanosti biometrijskog sustava.

Područja označena žutom bojom predstavljaju područja djelomične pouzdanosti biometrijskog sustava.

Područja označena crvenom bojom predstavljaju područja nepouzdanosti biometrijskog sustava.

Razrada stanja evaluacijskog modela sukladno matrici prikazanoj tablicom 7 predstavlja interpretaciju značenja svake pojedinačne kombinacije parametara ocjene aspekata tehnologije *A*, okoline *B* te korisnika *C* sa pripadajućim parametrarskim vrijednostima 1,2 ili 3.

Tablica 8 predstavlja razradu stanja evaluacijskog modela, sukladno definiranim područjima pouzdanosti, uzimajući u obzir rezultate evaluacija pojedinih aspekata biometrijskog sustava.

Tablica 8 Razrada stanja evaluacijskog modela

	TEH	OK	KOR
A1B1C1	PO	PO	PO
A1B2C1	PO	DP	PO
A1B3C1	PO	NP	PO
A1B1C2	PO	PO	DP
A1B2C2	PO	DP	DP
A1B3C2	PO	NP	DP
A1B1C3	PO	PO	NP
A1B2C3	PO	DP	NP
A1B3C3	PO	NP	NP
A2B1C1	DP	PO	PO
A2B2C1	DP	DP	PO
A2B3C1	DP	NP	PO
A2B1C2	DP	PO	DP
A2B2C2	DP	DP	DP
A2B3C2	DP	NP	DP
A2B1C3	DP	PO	NP
A2B2C3	DP	DP	NP
A2B3C3	DP	NP	NP
A3B1C1	NP	PO	PO
A3B2C1	NP	DP	PO
A3B3C1	NP	NP	PO
A3B1C2	NP	PO	DP
A3B2C2	NP	DP	DP
A3B3C2	NP	NP	DP
A3B1C3	NP	PO	NP
A3B2C3	NP	DP	NP
A3B3C3	NP	NP	NP

Razrada stanja podrazumijeva pojašnjenje kombinacije evaluacijskih vrijednosti područja pouzdanosti sa pojedinačnim aspektima pouzdanosti biometrijskog sustava.

Detaljna razrada stanja evaluacijskih vrijednosti definirana je Tablicom interpretacije evaluacijskih vrijednosti (PRILOG C).

Definirana metoda za evaluaciju pouzdanosti biometrijskog sustava u sljedećem poglavlju biti će ontološki definirana te implementirana u alatu Protege' . Implementirana metoda poslužiti će kao alat za rezoniranje o razinaima pouzdanosti određenih riješenja biometrijskih sustava primjenjenih u određenim kontekstima uporabe.

POGLAVLJE VII

7 ONTOLOŠKI PRISTUP DEFINIRANJU EVALUACIJSKOG MODELA OOEPBS

Biometrijska znanost kao znanost novijeg doba te kao takva još u razvoju raspolaže niskom sistematizacijom znanja [97] iz referentnog područja što je razvidno iz literature. Sukladno tomu tako i domena koja se bavi proučavanjem pouzdanosti u visokom je stupnju fragmentiranosti a specifična područja pokrivaju međunarodni standardi sa svojim specifikacijama kao što je navedeno u prethodnim poglavljima. Razlog za to leži u činjenici da se suvremene tehnologije koje koriste biometrijske sustave ili se koriste biometrijskim sustavima kontinuirano razvijaju te nadograđuju, a znanje koje se pohranjuje u sustave znanja omogućava lakše shvaćanje problematika, razvijanje modela, referentnih standarda ili procedura. Da bi se stekao uvid u pravce razvoja referentne domene [98] često je potrebno stvoriti nove koncepte ili ideje iz postojećih informacija koje su pohranjene u tzv. sustavima znanja gdje je omogućeno dijeljenje te uporaba domenskog znanja. Ovdje značajnu ulogu igraju ontologije, koje nam pomažu u procesu kreiranja novog znanja i definicija u ciljanoj domeni.

7.1 Ontologije i metode izgradnje

Pojam ontologije u kontekstu filozofije predstavlja dio metafizike koji se bavi fenomenom bivanja odnosno postojanja. Pojam ontologija je grčkog porijekla i predstavlja spoj dvije riječi "*onto*" što znači "biće, stvarnost, postojanje", i "*logos*" što znači „znanost"[90]. Dakle, ontologija predstavlja znanost o biću - znanost o postojanju [18].

Ontologije [99] danas imaju veoma veliku primjenu u informatici , umjetnoj inteligenciji, sustavima za upravljanje, sustavima za potporu odlučivanju, bazama znanja, semantičkom webu, bioinformatici te softverskom inženjerstvu. Ontologije [100] u kontekstu informacijsko-komunikacijskih tehnologija predstavljaju proces formalizacije domenskog

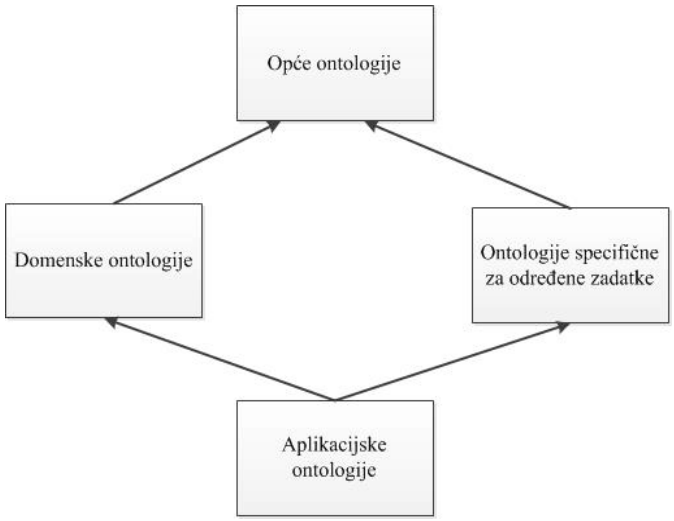
znanja, odnosno formalno definiranje sustava znanja uz pomoć pojmova (koncepata) i odnosa između tih koncepata. Postoji nekoliko aktualnih definicija pojma ontologije koje se koriste u informacijsko-komunikacijskim tehnologijama:

- Tom Grubor [101] - Ontologija je eksplicitna specifikacija konceptualizacije,
- Nicola Guarino [102] postoji distinkcija između ontologije sa velikim „O“ i malim „o“. Ontologija sa „O“ je povezana sa filozofijom i pojmom „bivanja postojanja“ i Aristotelovim teorijama postojanja. Ontologija sa malim “o“ je i dalje vezana za filozofiju i sustavni prikaz postojanja, te opisuje situaciju u kojoj je znanje stečeno u svrhu organiziranja i klasifikacije,
- Borst [103]: „Ontologija je formalna, eksplicitna specifikacija zajedničke konceptualizacije“,
- Guarino i Giaretta [104]: „Ontologija je logička teorija koja daje eksplicitni, nepotpuni prikaz konceptualizacije...“,
- Jasper i Uschold daju definiciju koja popularizira ontologije u korištenju unutar drugih znanstvenih disciplina [100]: „Ontologije mogu pružiti različite forme, ali će nužno uključivati rječnik pojmova i neke specifikacije njihovog značenja; to uključuje i definiciju koncepta i njihovog međusobnog odnosa što u cijelosti nameće strukturu domene i ograničava moguće prikaze pojmova“.

Na temelju prikupljenih informacija određene domene ontologijama se stvaraju rječnici (taksonomije) ciljane domene opisujući koncepte, atribute i relacije među tim konceptima unutar domene. Ontologije [105] također igraju veoma veliku ulogu te prihvaćene su u mnogim poslovnim i znanstvenim sustavima, kao metode za ponovno korištenje, dijeljenje i obradu znanja u ciljanoj domeni, te interoperabilnosti sustava.

U kontekstu ove doktorske disertacije koristit će se izraz *otvorena ontologija* [27] u cilju omogućavanja dijeljenja te nadogradnje izrađene ontologije, kao i u kontekstu pojma otvorenog koda u softverskom inženjerstvu. Problematika evaluacije pouzdanosti je , sukladno navedenome u prethodnim poglavljima, kompleksna je te zahtijeva multidisiplinarni pristup a postojeća saznanja putem znanstvenih istraživanja i definiranih modela predstavljaju visoki stupanj fragmentiranosti te nepovezanosti. Stoga je cilj ove doktorske disertacije izraditi funkcionalnu ontologiju koje će se vremenom, pojavom novih metoda, alata ili novih koncepata veoma lako moći dijeliti, nadograditi te promijeniti (u smislu dodavanja novih

spoznaja u vidu komponenata te funkcionalnosti). Slika 17 prikazuje podjelu tipologija ontologija [106] sukladno ciljanim domenama.



Slika 18 Tipologije ONTOLOGIJA

Ontologija koja će se izgraditi u ovoj doktorskoj disertaciji predstavlja domensku ontologiju[91] jer opisuje koncepte, instance, atribute i relacije unutar jednog užeg područja evaluacije pouzdanosti biometrijskih sustava sa ciljem definiranja evaluacijskog modela te metode za evaluaciju. Sukladno tomu biti će definirana Ontologija modela evaluacije (OOEPBS) koja predstavlja specijalizaciju odnosno specijaliziranu ontologiju sa definicijom koncepata koji se mogu javiti, a vezani su za pojam pouzdanosti biometrijskih sustava te evaluacijski okvir odnosno metodu za evaluaciju biometrijskih sustava u kojoj su definirani koncepti koji karakteriziraju proces evaluacije pouzdanosti određenog biometrijskog sustava. Ova ontologija će poslužiti provjeri te prihvaćanju ili neprihvaćanju hipoteze H2.

Prilikom razvoja otvorene ontologije koristit će se metodika METHONTOLOGY [107] koja definira sljedeće faze procesa kreiranja i izgradnje ontologije:

1. Specifikacija – predstavlja fazu u kojoj se ontologija izražava kroz dokument napisan na prirodnom jeziku koji opisuje svrhu te domenu finalnog korištenja ontologije. Ova faza opisana je u prethodnom poglavlju koje definira specifikaciju Činitelja pouzdanosti biometrijskih sustava te pripadajućih činitelja, parametara te njihovih metrika,

2. Konceptualizacija – predstavlja fazu strukturiranja domene ontologije te definiranja taksonomije glavnih pojmova ili koncepata.Definiranje pojmova ontologije te izrada

[91] Izvorno: Domain ontology

taksonomije biti će realizirana kroz proces razvoja ontologije za što će se koristiti softverski alat Protege' [108],

3. Integracija – predstavlja fazu povezivanja definiranih koncepata,

4. Implementacija – ova faza zahtijeva korištenje odgovarajućeg okružja koje podržava strukturiranje ontologije, a kao rezultat ima ontologiju kodiranu sukladno jednom od formalnih jezika. Programski jezik koji će se koristiti za izgradnju ontologije biti će OWL (Izvorno: Web Ontology Language), odnosno SWRL (Izvorno: Semantic Web Rule Language) za modeliranje pravila za rezoniranje nad ontologijom koja će biti razvijena korištenjem softvera Protége [108] preko specifikacije termina u domeni činitelja pouzdanosti biometrijskih sustava. Softver Protége razvijen je od strane „Centra za biomedicinska istraživanja informatike“ na Sveučilištu Stanford School of Medicine. Softver Protégé je platforma otvorenog koda koja korisnicima omogućava uporabu alata za izgradnju modela domene te na znanju temeljene aplikacije s ontologijama,

5. Evaluacija [109] - Ova faza predstavlja procese verifikacije [110], evaluacije korektnosti ontologije u tehničkom smislu te validacije, potvrde da se ontologija odnosi na domenu koja se željela opisati [111]. Realizirana ontologija u navedenom alatu Protege' biti će evaluirana sukladno metodologiji OntoQA [24] za evaluaciju ontologija [112]. Rezultati evaluacijskog modela [113] realiziranoga u SWRL-u biti će testirani od strane biometrijskih eksperata na postojećim biometrijskim sustavima za otisak prsta, otisak dlana te analizu glasa, pri čemu će se uspoređivati dobivene razine pouzdanosti.

7.2 Definiranje domene i obuhvat ontologije

Krovna domena [114] za koju se razvija ontologija je biometrijska znanost sa specijalizacijom koncepata koji pokrivaju problematike evaluacije pouzdanosti biometrijskih sustava. Cilj je razviti ontologiju evaluacijskog modela biometrijskih sustava, metode za evaluaciju pouzdanosti biometrijskih sustava koja će biti osnova za izgradnju otvorenog evaluacijskog okvira.

Osnovu za razvoj ontologije čini evaluacijski model opisan u Poglavlju 6.

Izgrađena ontologija omogućuje korištenje znanja pohranjenog u vidu rječnika podataka predmetne domene, omogućiti će ponovnu upotrebljivost[92] domenskog znanja, te se, obzirom da će ontologija biti formalizirana u OWL-u i SWRL-u, omogućuje korištenje iste od strane računalnih programa ili drugih agenata. Ontologija je otvorena, te ima veze na sve slične i kompatibilne ontologije koje su već ranije izgrađene a mogu se upotrijebiti. Pored diseminacije znanja o nužnosti evaluacije pouzdanosti biometrijskih sustava, ontologiju će osim znanstvenika moći koristiti i proizvođači pri projektiranju i kreiranju biometrijskih sustava sukladno određenim kontekstima primjene.

7.3. Ponovno korištenje postojećih ontologija

Pretraživanje putem specijaliziranog pretraživača sa ontologijama semantičkog Weba, SWOOGLE [48], te pretraživanje putem alata *Ontoligua* biblioteka ontologija (http://www.ksl.stanford.edu/software/ontolingua/) ili *DAML* biblioteka ontologija (http://www.daml.org/ontologies/) ukazuje na nepostojanje ontologija koje se bave problematikama koje su predmet ovoga znanstvenog istraživanja.Ontologije koje su dostupne uglavnom pokrivaju područja koja se vežu uz pojmove pouzdanosti vezane uz medicinu te statistike preživljavanja pacijenata. Implementirana ontologija biti će javno objavljena u nekom od postojećih relevantnih repozitorija, te će tako biti javno dostupna za korištenje te za eventualnu nadogradnju.

7.4 Definiranje koncepata te hijerarhije koncepata u domeni evaluacijskog modela OOEPBS

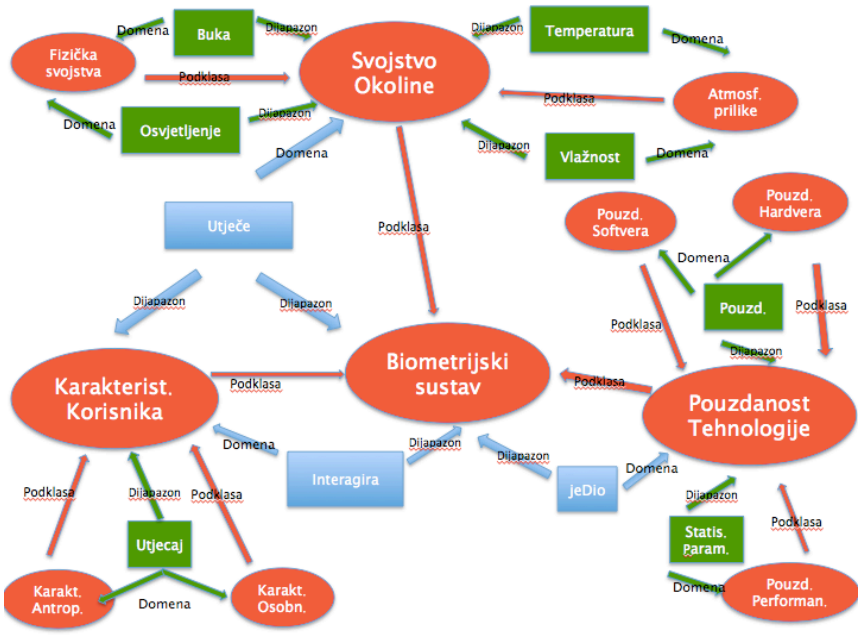
Postoji više mogućih pristupa u razvoju hijerarhije koncepata (klasa) [115] , odozgo prema dolje (Izvorno: *top-down*), odozdo prema gore (Izvorno: *bottom-up*) ili kombinirani pristup (Izvorno: *combination*) [20]. Pristup koji će se koristiti u razvoju ontologije u disertaciji je odozgo prema dolje. Ključni koncepti su: Biometrijski sustav te Pouzdanost Biometrijskog Sustava. Koncepti koji su temelj za definiranje evaluacijskog modela su: Pouzdanost

[92] Izvorno: Reusability

Tehnologije Biometrijskog sustava, Svojstvo Okoline Biometrijskog Sustava, Karakteristika Korisnika Biometrijskog Sustava.

Evaluacijski model se temelji na konceptu Parametar Evaluacije sa konceptom Rezultat Evaluacije koji razrađuje pojedinačne rezultate evaluacijskog procesa sa dobivenim vrijednostima.

Domena Ontologije evaluacijskog modela OOEPBS može biti prikazana sljedećim konceptualnim modelom prikazanim na slici 19.



Slika 19 Konceptualni model Ontologije po modelu OOEPBS

Na slici 19 prikazana je, na konceptualnom nivou, razina odnos Klasa (koncepata) pojedinih aspekata pouzdanosti biometrijskog sustava sa međusobnim vezama, podatkovnim te objektnim svojstvima klasa (koncepata) sukladno definiranom modelu OOEPBS. Implementacijom konceptualnog modela OOEPBS u programsko okruženje alata Protege' dobivaju se taksonomije pojedinačnih koncepata te njihovih podklasa te će isto biti tema razrade ovoga poglavlja.

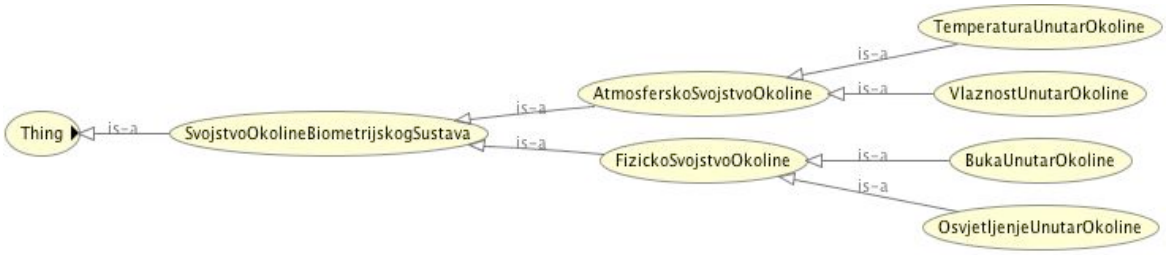
Dijagram taksonomije koncepata modela OOEPBS sukladno iznešenome u prethodnom poglavlju definiran je kako slijedi:

Koncept *PouzdanostTehnologijeBiometrijskogSustava* prikazan je na slici 20.

Slika 20 Taksonomija koncepta *PouzdanostTehnologijeBiometrijskogSustava*

Koncept *PouzdanostTehnologijeBiometrijskogSustava* predstavlja dio trijade aspekata pouzdanosti biometrijskog sustava. Podklase su: *PouzdanostHardvera, PouzdanostSoftvera* te *PouzdanostPerformansiTehnologijeBiometrijskogSustava.* Podklasa *StatusCertifikacijeBiometrijskogSustava* predstavlja opciju za poboljšanje modela OOEPBS koja će biti predmet razrade u sljedećem poglavlju. Podklase koncepta *PouzdanostHardvera* su: *HardverPouzdan, HardverDjelomicnoPouzdan, HardverNepouzdan.* Podklase koncepta *PouzdanostSoftvera* su: *SoftverPouzdan, SoftverDjelomicnoPouzdan, SoftverNepouzdan.* Podklase koncepta *PouzdanostPerformansiTehnologijeBiometrijskogSustava* su: *PerformanseTehnologijePouzdane, PerformanseTehnologijeNepouzdane* te *PerformanseTehnologijeDjelomicnoPouzdane.*

Koncept *SvojstvoOkolineBiometrijskogSustava* prikazan je na slici 21.

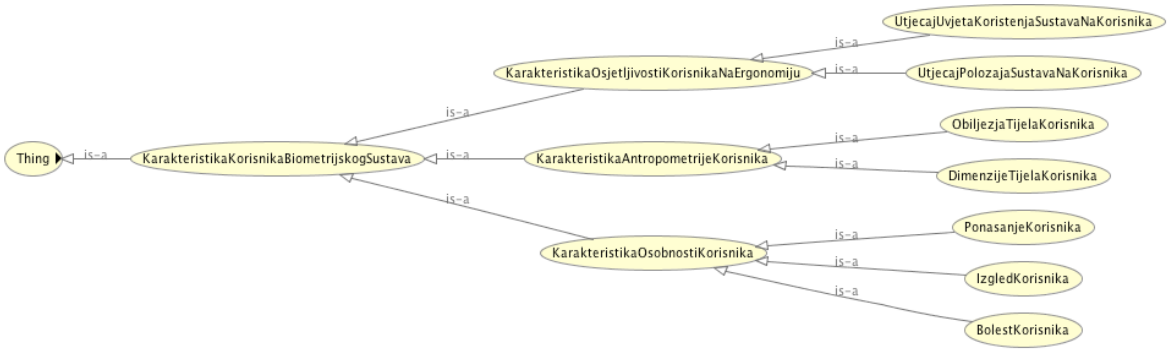


Slika 21 Taksonomija koncepta SvojstvoOkolineBiometrijskogSustava

Koncept *SvojstvoOkolineBiometrijskogSustava* također predstavlja dio trijade aspekata pouzdanosti biometrijskog sustava. Podklase su: *FizickoSvojstvoOkoline te AtmosferskoSvojstvoOkoline* . Podklase koncepta *FizickoSvojstvoOkoline* su : *JacinaBuke* te *JacinaOsvjetljenja.* Podklase koncepta *AtmosferskoSvojstvoOkoline* su : *Vlaznost* te

Temperatura. Podklase koncepta *FizickoSvojstvoOkoline* su : *JacinaBuke* te *JacinaOsvjetljenja.* Koncept *NadzorNadOkolinom* predstavlja mogućnost za poboljšanje ovoga modela Podklase koncepta *NadzorNadOkolinom* su : *OkolinaPodNadzorom* te *OkolinaBezNadzora..*

Koncept *KarakteristikaKorisnikaBiometrijskogSustava* prikazan je na slici 22.



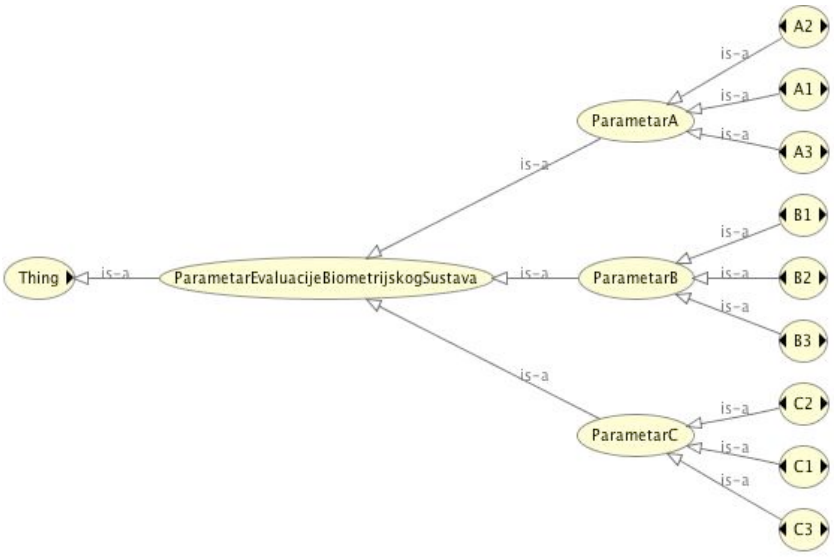
Slika 22 Taksonomija koncepta *KarakteristikaKorisnikaBiometrijskogSustava*

Koncept *KarakteristikaKorisnikaBiometrijskogSustava* također predstavlja dio trijade aspekata pouzdanosti biometrijskog sustava. Podklase su: *KarakteristikaOsjetljivostiKorisnikaNaErgonomiju, KarakteristikaOsobnostiKorisnika* te *KarakteristikaAntropometrijeKorisnika.* Podklase koncepta *KarakteristikaOsjetljivostiKorisnikaNaErgonomiju* su: *UtjecajPozicijeSustava* te *UtjecajUvjetaKorištenjaSustava.* Podklase koncepta *KarakteristikaOsobnostiKorisnika* su: *IzgledKorisnika, PonašanjeKorisnika* te *BolestKorisnika.* Podklase koncepta *KarakteristikaAntropometrijeKorisnika* su: *DimenzijeTijelaKorisnika* te *ObiljezjaTijelaKorisnika.* Koncept *UvjezbanostKorisnika* predstavlja mogućnost za poboljšanje ovoga modela. Podklasa koncepta *UvjezbanostKorisnika* je : *IskustvoKorisnika.*

Taksonomije prethodno opisanih koncepata implementiranih u softveru Protege' na temelju modela OOEPBS predstavljaju okosnicu za rezoniranje unutar evaluacijskog modela putem pravila koja će nadalje biti implementirana.

Evaluacijski model utemeljen na modelu OOEPBS definiran je putem implementacije sljedećih koncepata:

Koncept *ParametarEvaluacijeBiometrijskogSustava* prikazan je na slici 23.

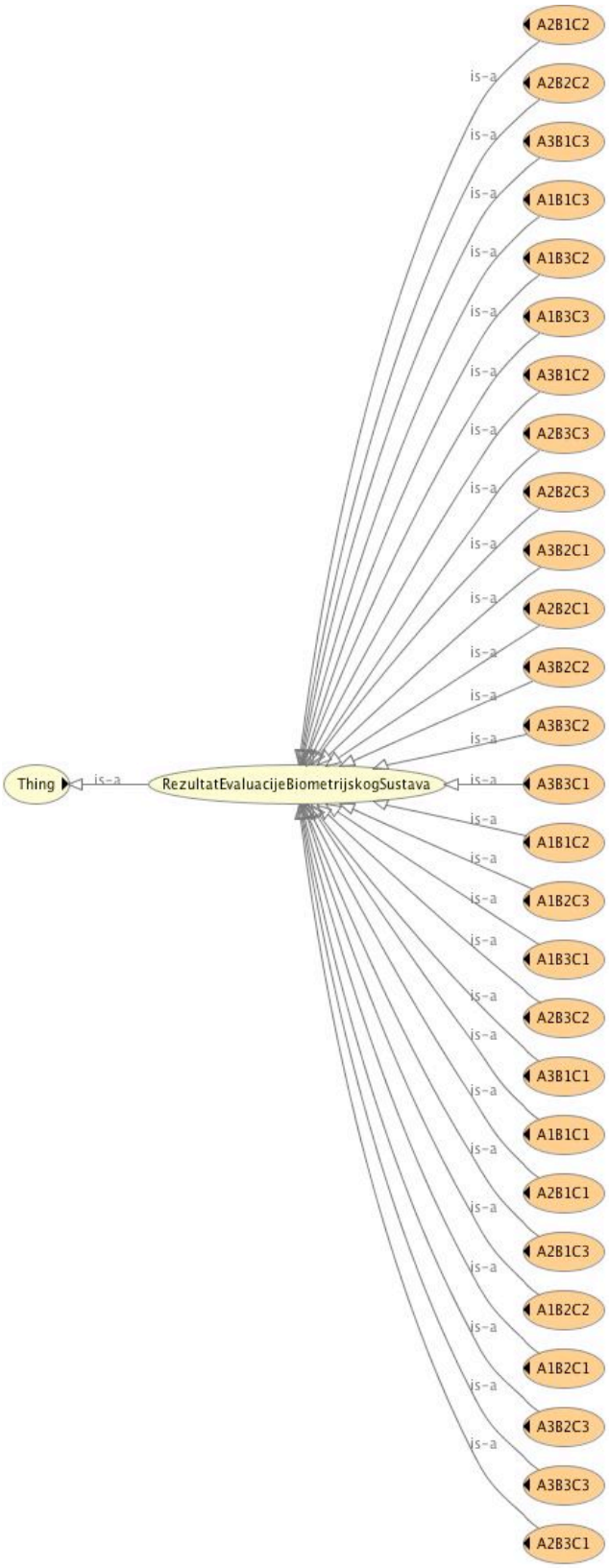


Slika 23 Taksonomija koncepta *ParametarEvaluacijeBiometrijskogSustava*

Ovaj koncept je početni koncept evaluacijskog modela jer definira evaluacijski okvir slijedom definiranja parametara evaluacije prethodno definiranih aspekata pouzdanosti biometrijskog sustava te je sastavljen od sljedećih podklasa: *ParametarA, ParametarB* te *ParametarC.* Koncept *ParametarA* sastavljen je od podklasa: *A1,A2* te *A3* koje predstavljaju evaluacijski okvir za aspekt Tehnologije biometrijskog sustava. Koncept *ParametarB* sastavljen je od podklasa: *B1,B2* te *B3* koje predstavljaju evaluacijski okvir za aspekt Okoline biometrijskog sustava. Koncept *ParametarC* sastavljen je od podklasa: *C1,C2* te *C3* koje predstavljaju evaluacijski okvir za aspekt Korisnika biometrijskog sustava.

Koncept *RezultatEvaluacijeBiometrijskogSustava* predstavlja implementaciju modela predstavljenoga Tablicom 7 i Tablicom 8 prethodnog Poglavlja.

Koncept *RezultatEvaluacijeBiometrijskogSustava* prikazan je na slici 24.



Slika 24 Taksonomija koncepta *RezultatEvaluacijeBiometrijskogSustava*

Ovaj koncept je završni koncept evaluacijskog modela jer definira prostor mogućih rezultata evaluacije pouzdanosti biometrijskog sustava sukladno modelu OOEPBS. Podklase ovoga koncepta dane su u Tablici 8.

7.5 Definiranje koncepata pouzdanosti aspekata biometrijskog sustava

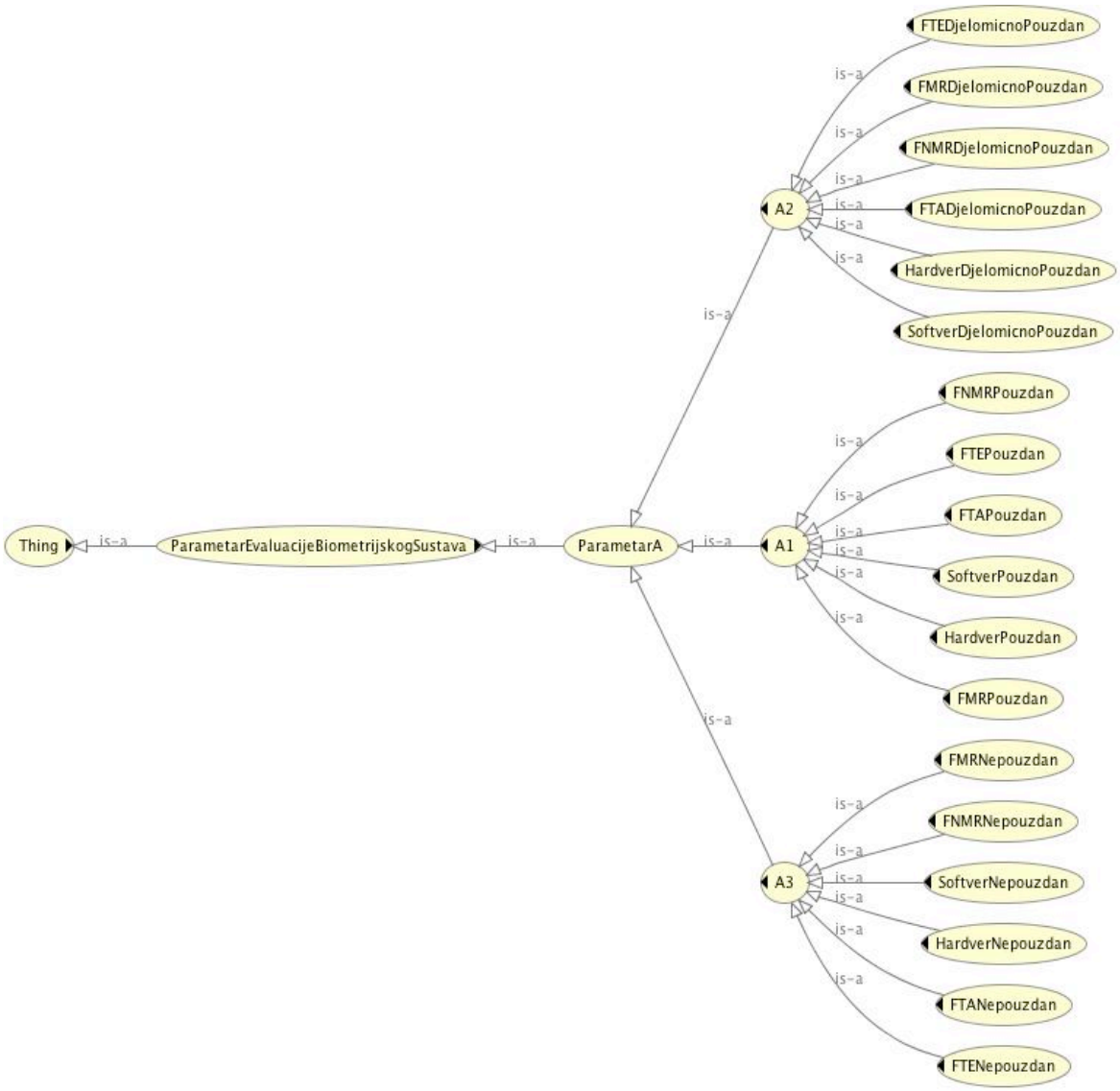
7.5.1 Koncepti parametara evaluacije sukladno modelu OOEPBS

Okvir za evaluacijski model pouzdanosti biometrijskih sustava postavljen je definiranjem koncepata : *ParametarEvaluacijeBiometrijskogSustava* te *RezultatEvaluacijeBiometrijskogSustava* kako je predstavljeno na slikama 23 i 24 prethodnog poglavlja gdje je definirana taksonomija spomenutih koncepata na prvoj razini.

Koncept *ParametarEvaluacijeBiometrijskogSustava* prikazan je na slici 23 te prikazuje detalje parametrizacije pouzdanosti aspekata biometrijskog sustava.

Koncepti pojedinačnih parametara su prikazani kako slijedi:

Koncept *ParametarA* prikazan je na slici 25.



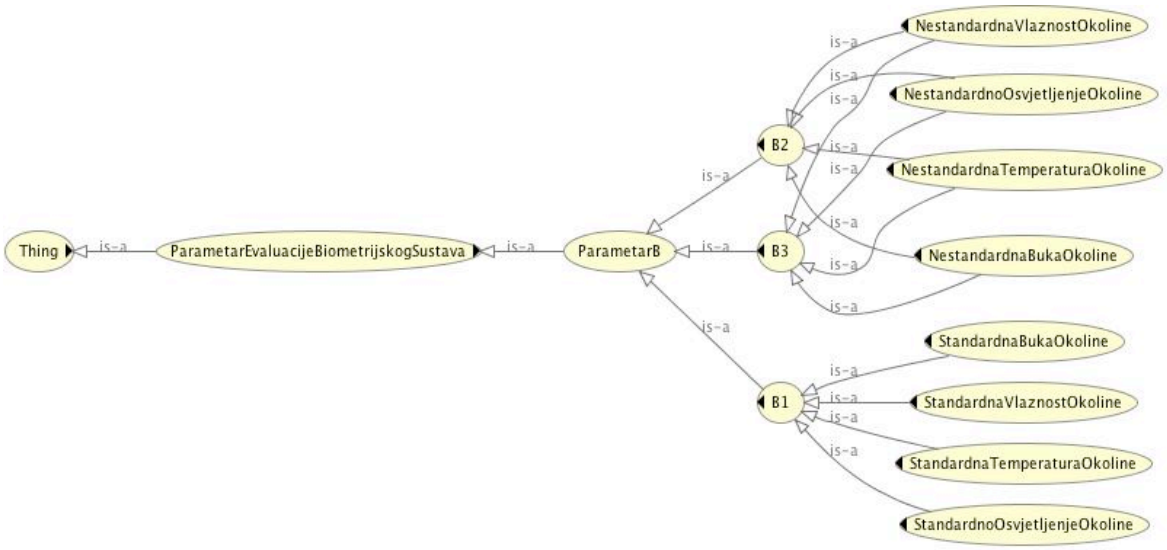
Slika 25 Taksonomija koncepta *ParametarA*

Koncept *A1* sastoji se od podklasa: *SoftverPouzdan, HardverPouzdan, FTAPouzdan, FTEPouzdan, FMRPouzdan* te *FNMRPouzdan.*

Koncept *A2* sastoji se od podklasa: *SoftverDjelomicnoPouzdan, HardverDjelomicnoPouzdan, FTADjelomicnoPouzdan, FTEDjelomicnoPouzdan, FMRDjelomicnoPouzdan* te *FNMRDjelomicnoPouzdan.*

Koncept *A3* sastoji se od podklasa: *SoftverNepouzdan, HardverNepouzdan, FTANepouzdan, FTENepouzdan, FMRNepouzdan* te *FNMRNepouzdan.*

Koncept *ParametarB* prikazan je na slici 26.

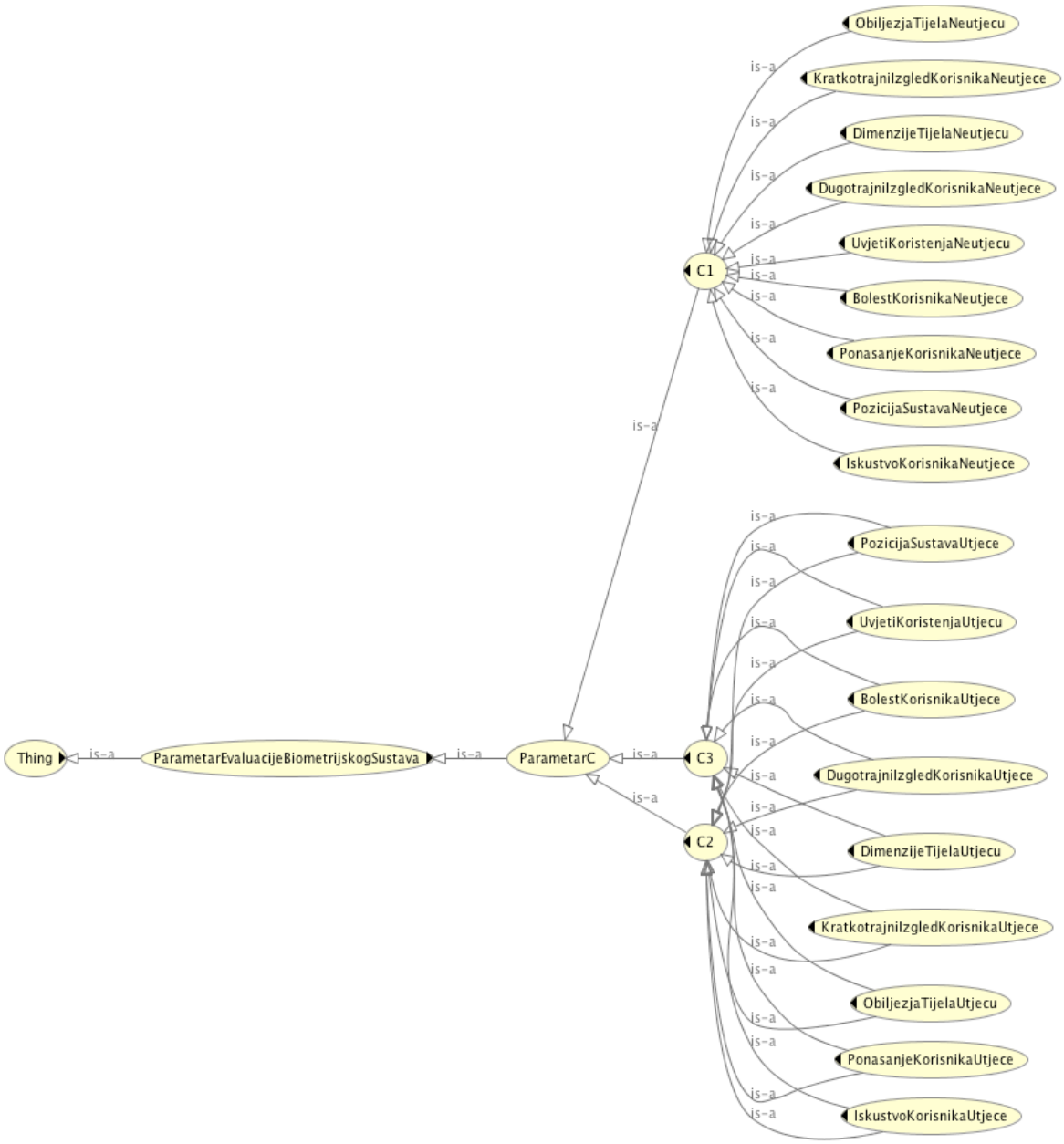


Slika 26 Taksonomija koncepta *ParametarB*

Koncept *B1* sastoji se od podklasa: *StandardnaTemperaturaOkoline, StandardnaVlaznostOkoline, StandardnaBukaOkoline te StandardnoOsvjetljenjeOkoline.*

Koncept *B2 i B3* sastoji se od podklasa: *NestandardnaTemperaturaOkoline, NestandardnaVlaznostOkoline, NestandardnaBukaOkoline te NestandardnoOsvjetljenjeOkoline.*

Koncept *Parametar C* prikazan je na slici 26.



Slika 27 Taksonomija koncepta *ParametarC*

Koncept *C1* sastoji se od podklasa: *DugotrajniIzgledNeUtjece, ObiljezjaTijelaNeutjecu, KratkotrajniIzgledKorisnikaNeutjece, UtjecajPozicijeSustavaNeutjece, BolestKorisnikaNeutjece, IskustvoKorisnikaNeutjece, UvjetiKoristenjaNeutjecu, PonasanjeKorisnikaNeutjece te DimenzijeTijelaNeutjecu.*

Koncept *C2 i C3* sastoji se od podklasa: *DugotrajniIzgledUtjece, ObiljezjaTijelaUtjecu, KratkotrajniIzgledKorisnikaUtjece, UtjecajPozicijeSustavaUtjece, BolestKorisnikaUtjece, IskustvoKorisnikaUtjece, UvjetiKoristenjaUtjecu, PonasanjeKorisnikaUtjece te DimenzijeTijelaUtjecu.*

7.5.2 Koncepti pouzdanosti sukladno modelu OOEPBS

Koncepti pouzdanosti predstavljaju rezultate evaluacijskog modela utemeljenog na modelu OOEPBS koji evaluira pouzdanost svakoga aspekta pouzdanosti pojedinačno.

Koncepti koji se referiraju na razmatranja aspekata pouzdanosti biometrijskog sustava opisani su kako slijedi:

Pouzdanost Tehnologije biometrijskog sustava

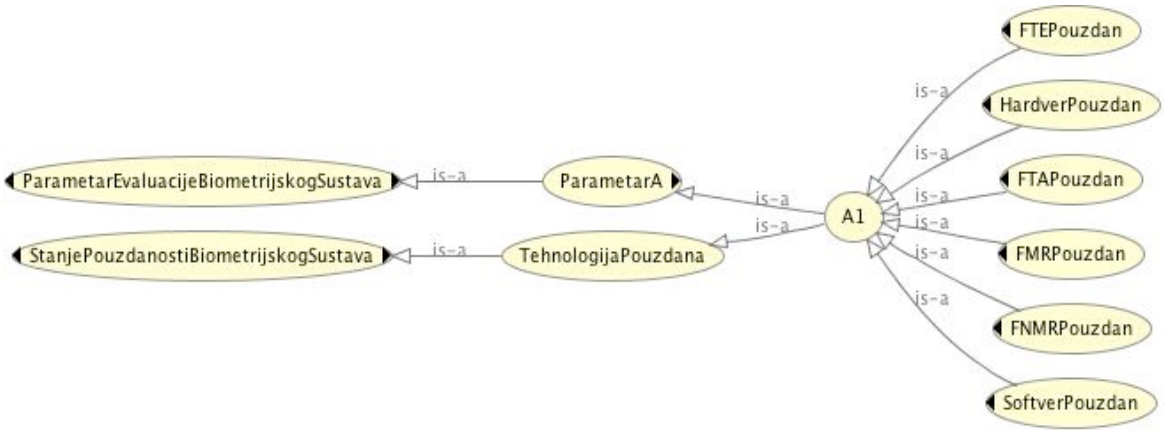
Koncept *TehnologijaPouzdana* prikazana je na slici 28.

Slika 28 Taksonomija koncepta *TehnologijaPouzdana*

Ovaj koncept definiran je evaluacijskim parametrom *A1* čija je taksonomija predstavljena na slici 25 također.

Koncept *TehnologijaPouzdana* sastoji se od podklase *A1* a koja se sastoji se od podklasa: *SoftverPouzdan, HardverPouzdan, FTAPouzdan, FTEPouzdan, FMRPouzdan* te *FNMRPouzdan.*

Evaluacijski parametar *A1* predstavljen je slikom 29:



Slika 29 Taksonomija koncepta *A1*

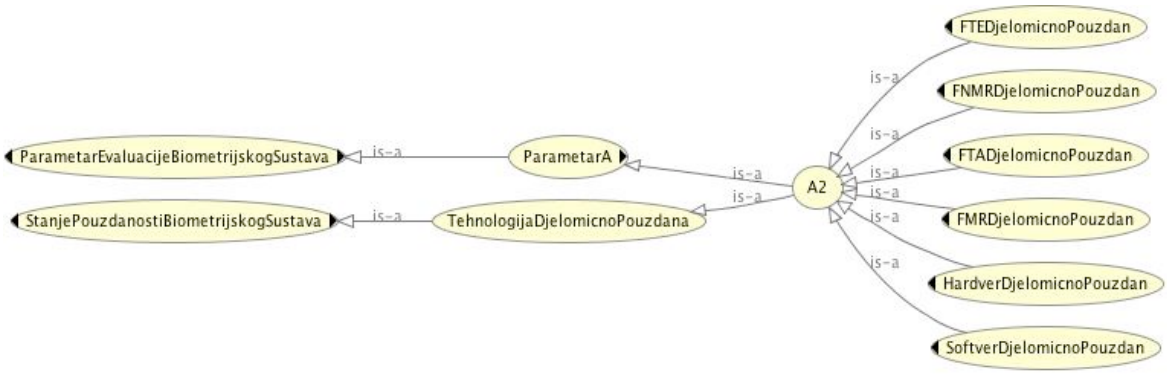
Koncept *TehnologijaDjelomičnoPouzdana* prikazana je na slici 30.

Slika 30 Taksonomija koncepta *TehnologijaDjelomicnoPouzdana*

Ovaj koncept definiran je evaluacijskim parametrom *A2* čija je taksonomija predstavljena na slici 25 također.

Koncept *TehnologijaDjelomicnoPouzdana* sastoji se od podklase *A2* a koja se sastoji se od podklasa: *SoftverDjelomicnoPouzdan, HardverDjelomicnoPouzdan, FTADjelomicnoPouzdan, FTEDjelomicnoPouzdan, FMRDjelomicnoPouzdan* te *FNMRDjelomicnoPouzdan.*

Evaluacijski parametar *A2* predstavljen je slikom 31:



Slika 31 Taksonomija koncepta *Parametar A2*

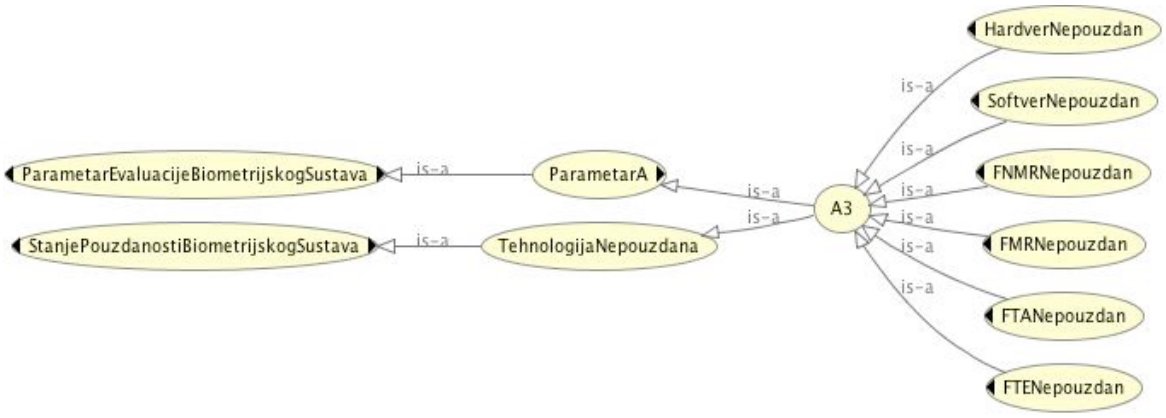
Koncept *TehnologijaNepouzdana* prikazana je na slici 32.

Slika 32 Taksonomija koncepta *TehnologijaNepouzdana*

Ovaj koncept definiran je evaluacijskim parametrom *A3* čija je taksonomija predstavljena na slici 25 također.

Koncept *TehnologijaNepouzdana* sastoji se od podklase *A3* a koja se sastoji se od podklasa: *SoftverNepouzdan, HardverNepouzdan, FTANepouzdan, FTENepouzdan, FMRNepouzdan* te *FNMRNepouzdan.*

Evaluacijski parametar *A3* predstavljen je slikom 33:



Slika 33 Taksonomija koncepta Parametar *A3*

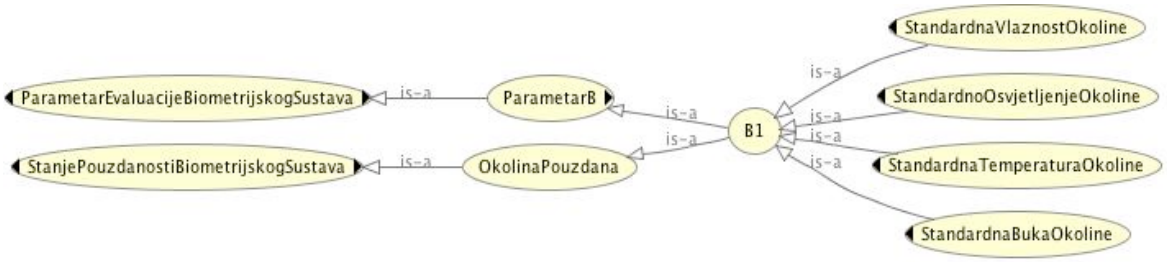
Svojstvo Okoline biometrijskog sustava

Koncept *OkolinaPouzdana* prikazana je na slici 34.

Slika 34 Taksonomija koncepta *OkolinaPouzdana*

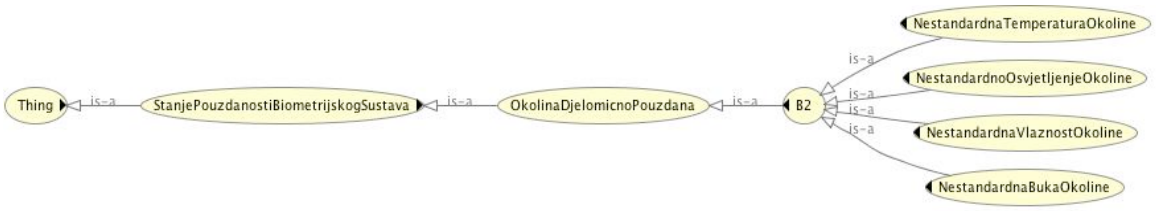
Ovaj koncept definiran je evaluacijskim parametrom *B1* čija je taksonomija predstavljena na slici 26. Koncept *OkolinaPouzdana* sastoji se od podklase *B1* a koja se sastoji se od podklasa: *StandardnaTemperaturaOkoline, StandardnaVlaznostOkoline, StandardnaBukaOkoline te StandardnoOsvjetljenjeOkoline.*

Evaluacijski parametar *B1* predstavljen je slikom 35:



Slika 35 Taksonomija koncepta Parametar *B1*

Koncept *OkolinaDjelomičnoPouzdana* prikazana je na slici 36.

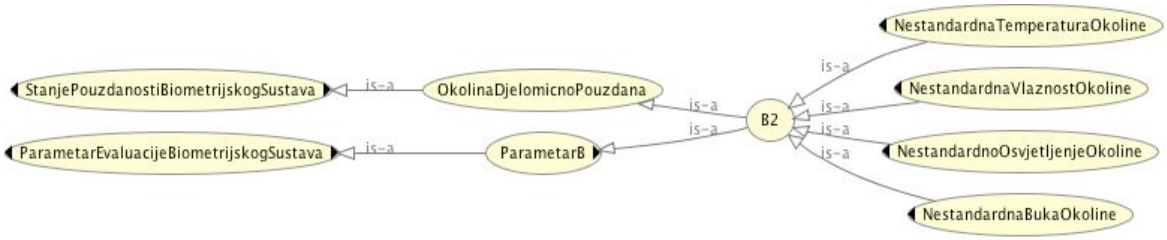


Slika 36 Taksonomija koncepta *OkolinaDjelomičnoPouzdana*

Ovaj koncept definiran je evaluacijskim parametrom *B2* čija je taksonomija predstavljena na slici 26 također.

Koncept *OkolinaDjelomicnoPouzdana* sastoji se od podklase *B2* a koja se sastoji se od podklasa: *NestandardnaTemperaturaOkoline, NestandardnaVlaznostOkoline, NestandardnaBukaOkoline te NestandardnoOsvjetljenjeOkoline.*

Evaluacijski parametar *B2* predstavljen je slikom 37:



Slika 37 Taksonomija koncepta Parametar *B2*

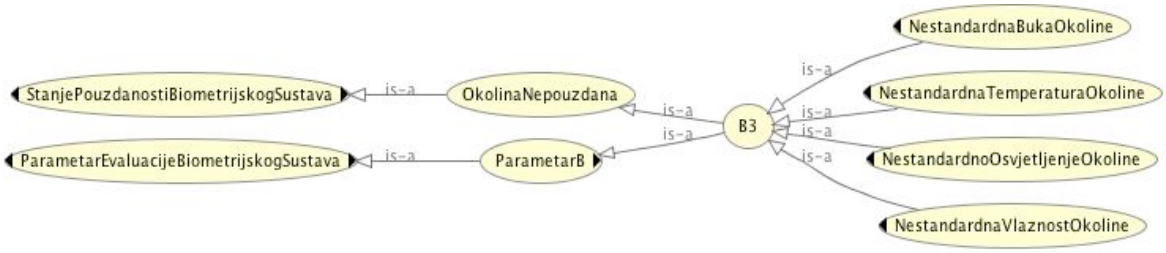
Koncept *OkolinaNepouzdana* prikazana je na slici 38.

Slika 38 Taksonomija koncepta *OkolinaNepouzdana*

Ovaj koncept definiran je evaluacijskim parametrom *B3* čija je taksonomija predstavljena na slici 26 također.

Koncept *OkolinaNepouzdana* sastoji se od podklase *B3* a koja se sastoji se od podklasa: *NestandardnaTemperaturaOkoline, NestandardnaVlaznostOkoline, NestandardnaBukaOkoline te NestandardnoOsvjetljenjeOkoline.*

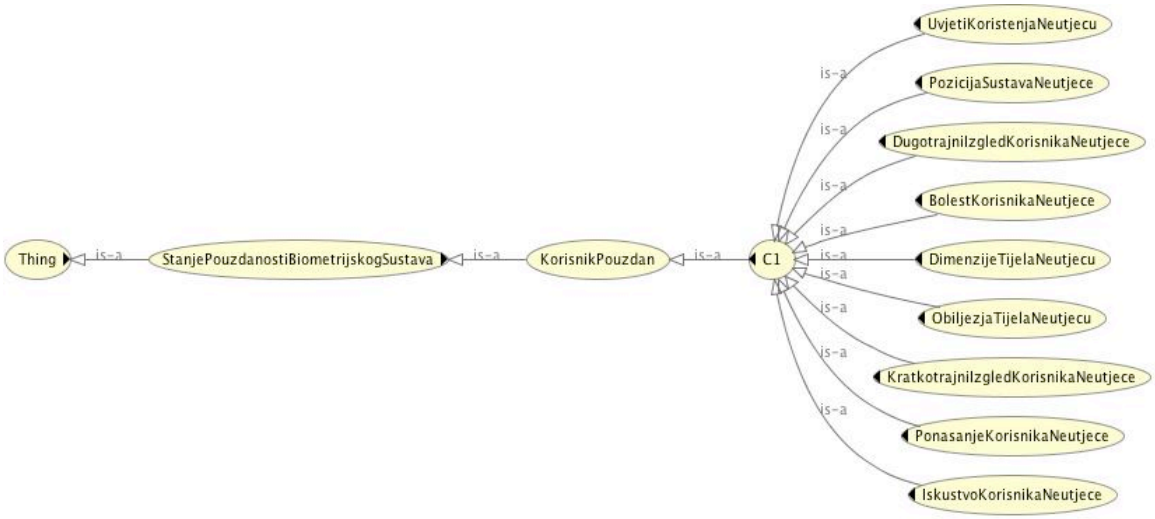
Evaluacijski parametar *B3* predstavljen je slikom 39:



Slika 39 Taksonomija koncepta Parametar *B3*

Karakteristika korisnika biometrijskog sustava

Koncept *KorisnikPouzdan* prikazan je na slici 40.



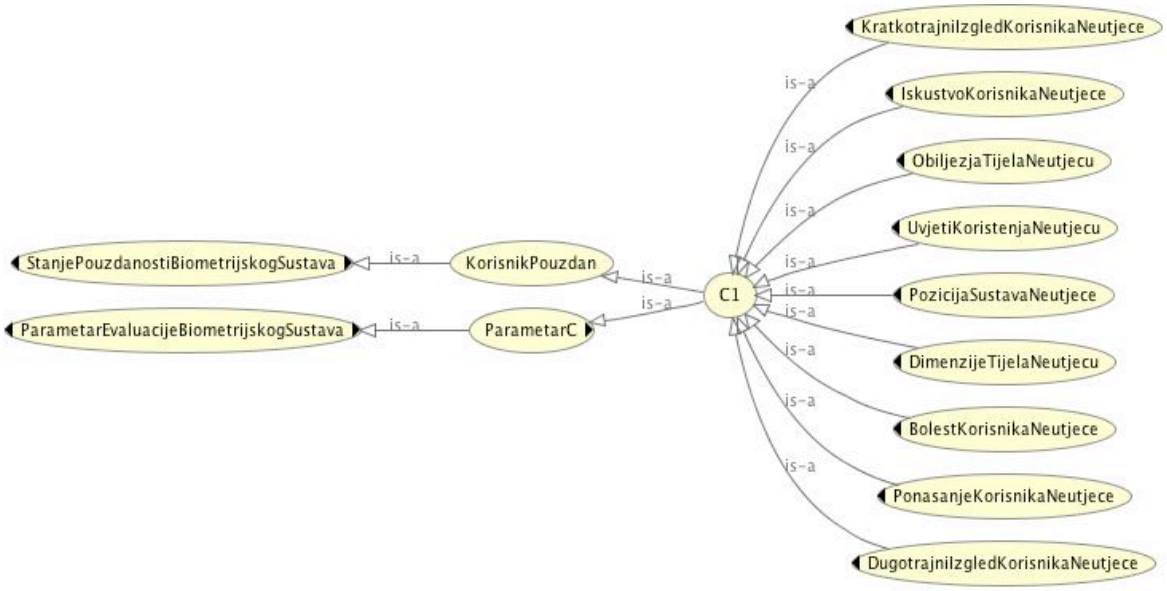
Slika 40 Taksonomija koncepta *KorisnikPouzdan*

Ovaj koncept definiran je evaluacijskim parametrom *C1* čija je taksonomija predstavljena na slici 27.

Koncept *KorisnikPouzdan* sastoji se od podklase *C1* a koja se sastoji se od podklasa: *DugotrajniIzgledNeUtjece, ObiljezjaTijelaNeutjecu, KratkotrajniIzgledKorisnikaNeutjece,*

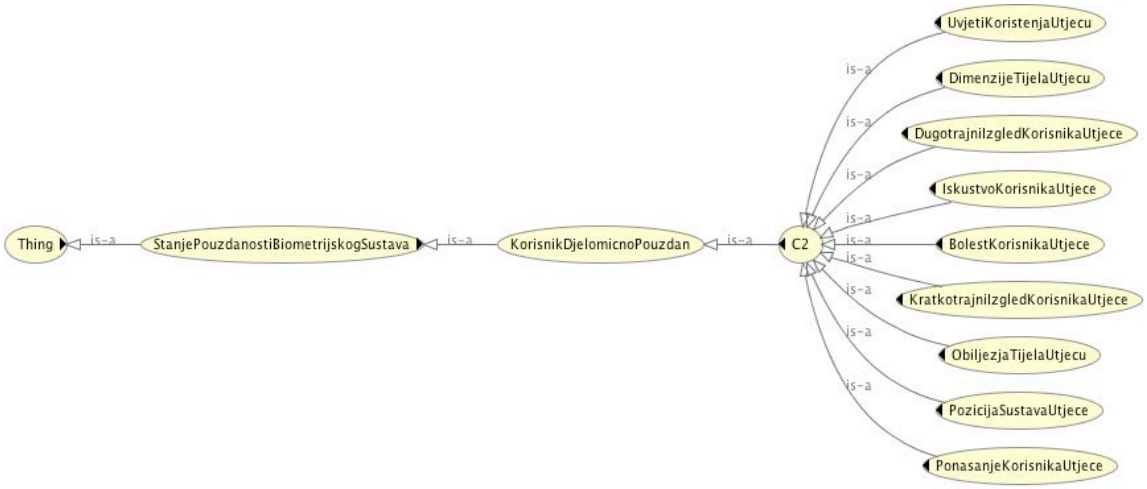
UtjecajPozicijeSustavaNeutjece, BolestKorisnikaNeutjece, IskustvoKorisnikaNeutjece, UvjetiKoristenjaNeutjecu, PonasanjeKorisnikaNeutjece te DimenzijeTijelaNeutjecu.

Evaluacijski parametar *C1* predstavljen je slikom 41:



Slika 41 Taksonomija koncepta Parametar *C1*

Koncept *KorisnikDjelomicnoPouzdan*» prikazan je na slici 42.

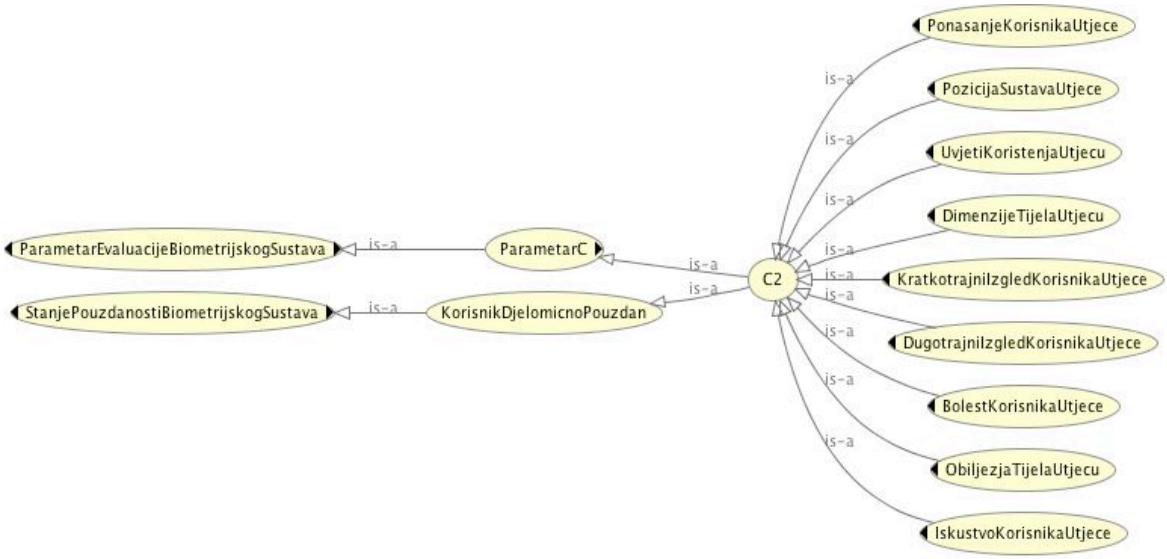


Slika 42 Taksonomija koncepta *KorisnikDjelomičnoPouzdan*

Ovaj koncept definiran je evaluacijskim parametrom *C2* čija je taksonomija predstavljena na slici 27 također.

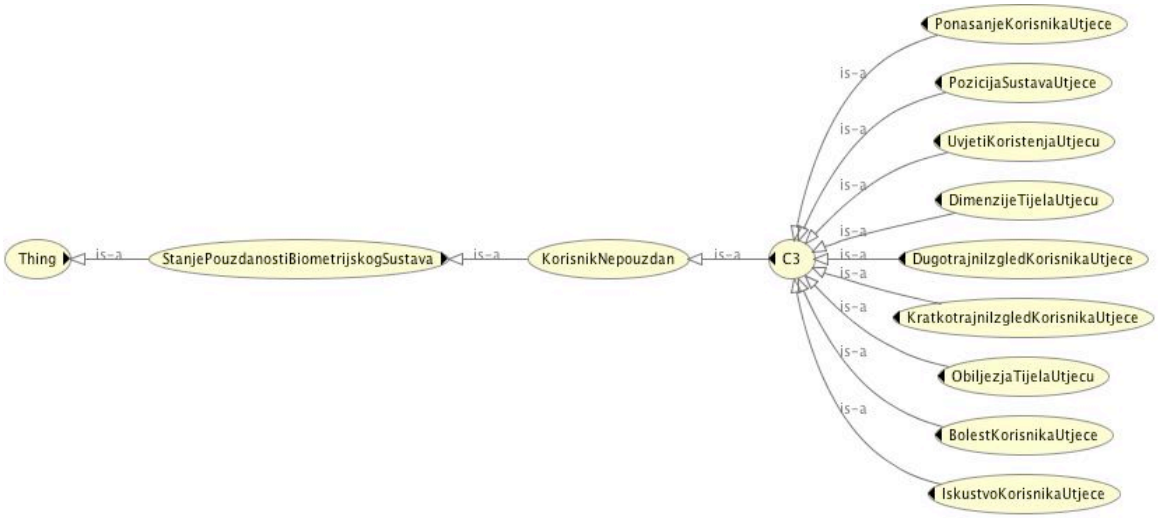
Koncept *KorisnikDjelomicnoPouzdan* sastoji se od podklase *C2* a koja se sastoji se od podklasa: *DugotrajniIzgledUtjece, ObiljezjaTijelaUtjecu, KratkotrajniIzgledKorisnikaUtjece, UtjecajPozicijeSustavaUtjece, BolestKorisnikaUtjece, IskustvoKorisnikaUtjece, UvjetiKoristenjaUtjecu, PonasanjeKorisnikaUtjece te DimenzijeTijelaUtjecu.*

Evaluacijski parametar *C2* predstavljen je slikom 43:



Slika 43 Taksonomija koncepta Parametar *C2*

Koncept *KorisnikNepouzdan* prikazan je na slici 44.

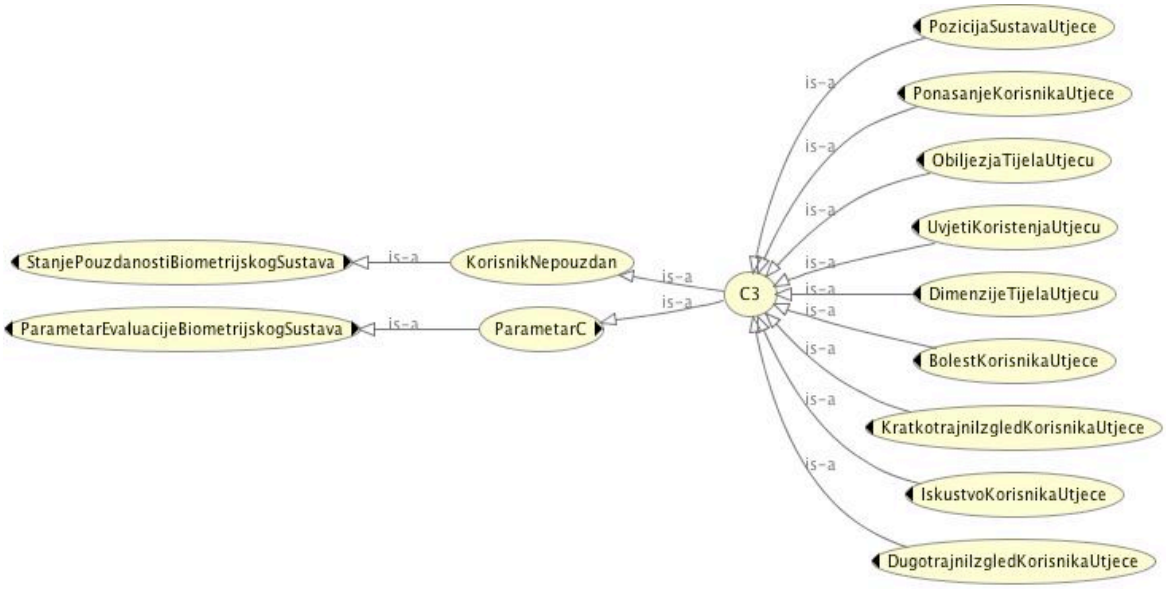


Slika 44 Taksonomija koncepta *KorisnikNepouzdan*

Ovaj koncept definiran je evaluacijskim parametrom *C3* čija je taksonomija predstavljena na slici 27 također.

Koncept *KorisnikDjelomicnoPouzdan* sastoji se od podklase *C3* a koja se sastoji se od podklasa: *DugotrajniIzgledUtjece, ObiljezjaTijelaUtjecu, KratkotrajniIzgledKorisnikaUtjece, UtjecajPozicijeSustavaUtjece, BolestKorisnikaUtjece, IskustvoKorisnikaUtjece, UvjetiKoristenjaUtjecu, PonasanjeKorisnikaUtjece te DimenzijeTijelaUtjecu.*

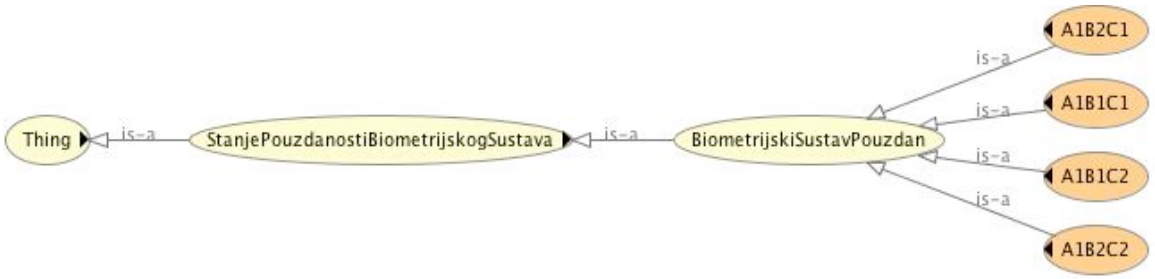
Evaluacijski parametar *C3* predstavljen je slikom 45:



Slika 45 Taksonomija koncepta Parametar *C3*

Stanje pouzdanosti koje se odnosi na biometrijski sustav

Koncept *BiometrijskiSustavPouzdan* prikazan je na slici 46.

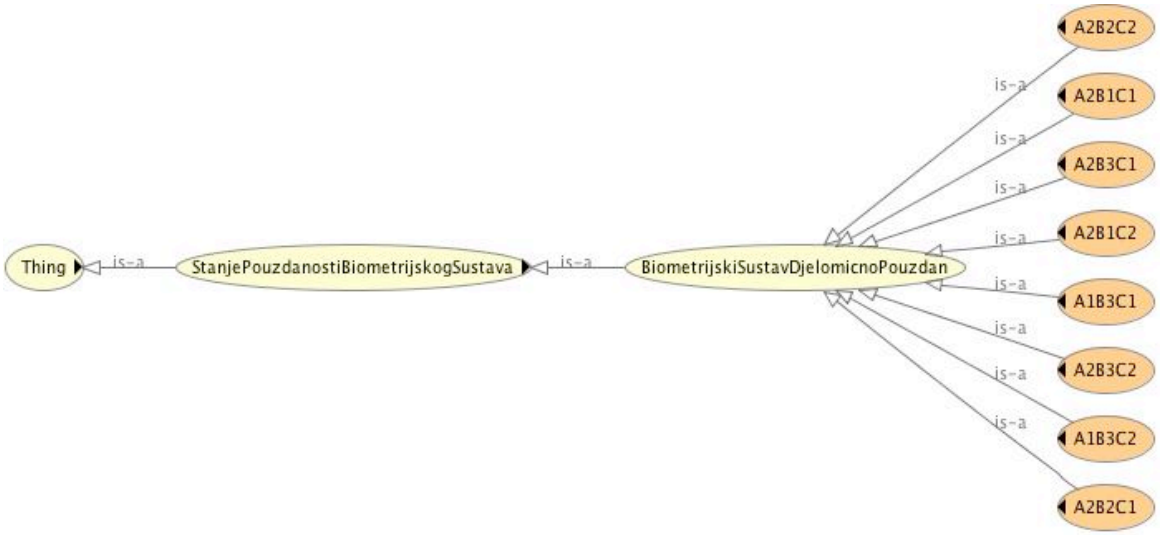


Slika 46 Taksonomija koncepta *BiometrijskiSustavPouzdan*

Ovaj koncept definiran je skupom vrijednosti koje su definirane kroz pregled stanja rezultata evaluacije modela OOEPBS. Vrijednosti koje pripadaju ovome skupu dane su u tablici 7 i 8. te su označene zelenom bojom.

Koncept *BiometrijskiSustavPouzdan* sastoji se od podklasa: *A1B2C1, A1B1C1, A1B1C2* te *A1B2C2.*

Koncept *BiometrijskiSustavDjelomičnoPouzdan* prikazan je na slici 47.

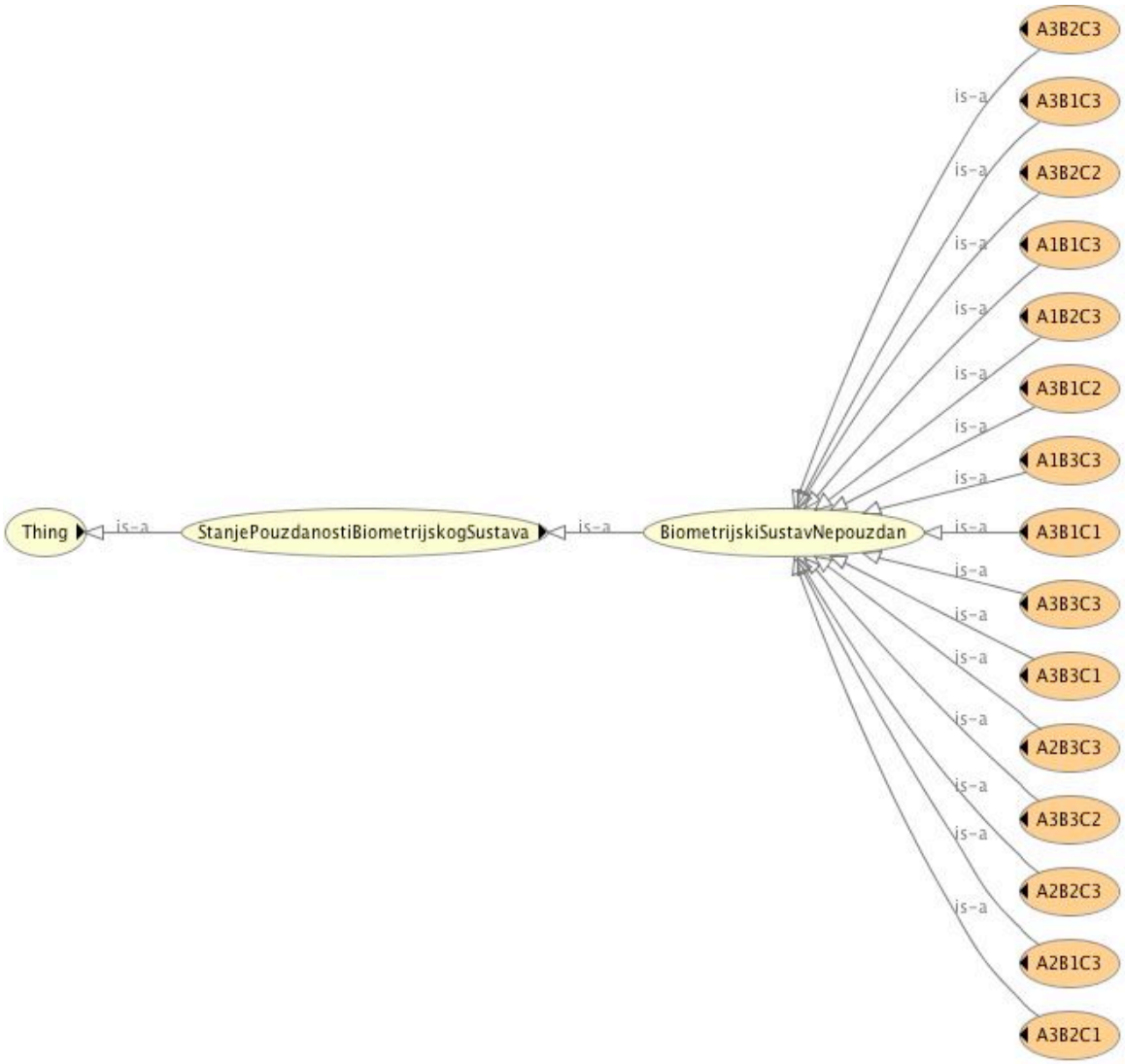


Slika 47 Taksonomija koncepta Biometrijski sustav djelomično pouzdan

Ovaj koncept definiran je također skupom vrijednosti koje su definirane kroz pregled stanja rezultata evaluacije modela OOEPBS. Vrijednosti koje pripadaju ovome skupu dane su u tablici 7 i 8. te su označene žutom bojom.

Koncept *BiometrijskiSustavDjelomicnoPouzdan* sastoji se od podklasa: *A2B2C2, A2B1C1, A2B3C1*, *A2B1C2, A1B3C1, A2B3C2, A1B3C2* te *A2B2C1.*

Koncept *BiometrijskiSustavNepouzdan* prikazan je na slici 48.



Slika 48 Taksonomija koncepta Biometrijski sustav nepouzdan

Ovaj koncept definiran je također skupom vrijednosti koje su definirane kroz pregled stanja rezultata evaluacije modela OOEPBS. Vrijednosti koje pripadaju ovome skupu dane su u tablici 7 i 8. te su označene crvenom bojom.

Koncept *BiometrijskiSustavNepouzdan* sastoji se od podklasa: *A3B2C3, A3B1C3, A3B2C2*, *A1B1C3, A1B2C3, A3B1C2, A1B3C3, A3B1C1, A3B3C3, A3B3C, A2B3C3, A3B3C2, A2B2C3, A2B1C3* te *A3B2C1*.

7.6 Definiranje svojstava-atributa koncepata te relacija među konceptima

Taksonomije klasa ,definirane i postavljene u dijagram , ne nude mnogo informacija o samim konceptima i promatranoj domeni. Nakon što su definirane klase potrebno ih je detaljno obraditi, odnosno opisati njihovu strukturu. Kao što je ranije spomenuto biti će korišteni samo koncepti koji su neophodni za definiranje otvorenog okvira i pravila koji će omogućiti zaključivanje o formalnoj prihvatljivosti digitalnih dokaza.

Svojstva [22] mogu biti: a.) objektna – svojstva koja entitete povezuju sa entitetima (osobe, klase svojstva ili tip podataka), te b.) podatkovna – svojstva koja entitetu pridružuju podatkovnu vrijednost.

Pri opisu se koristi Manchester notacija [116] , jer je ista čitljivija za ljude od OWL[93] ili RDF[94] notacije koja se najčešće koristi za zapisivanje ontologija za računala.

a.) Opis svojstava objekata (relacija):

Za potrebe implementacije pravila modela OOEPBS definiran je skup objektnih svojstava koja povezuju koncepte definirane u prethodnom poglavlju te omogućuju rezoniranje kroz Ontologiju sukladno postavljenim pretpostavkama te pravilima.

Objektna svojstva modela OOEPBS su predstavljena slikom 49:

Slika 49 Objektna svojstva modela OOEPBS

Definirana objektna svojstva su opisana sukladno zapisima Manchester notacije na sljedeći način:

[93] Izvorno: Ontology web language

[94] Izvorno: Resource definition framework

```
ObjectProperty: Ima

    Annotations:
        TV_sg "Imas",
        TV_pl "Ima",
        TV_vbg "Imaed"

    Characteristics:
        Functional

    Domain:
        Ima some SvojstvoOkolineBiometrijskogSustava,
        Ima some KarakteristikaKorisnikaBiometrijskogSustava,
        Ima some PouzdanostTehnologijeBiometrijskogSustava

    Range:
        Ima some BiometrijskiSustav
```

Kôd 7.1 Zapis u manchester notaciji svojstva "Ima"

Kôd prikazan u 7.1 opisuje svojstvo `Ima` koje subjektu koji je osoba klase *BiometrijskiSustav* te kojoj pridružuje osobe klase *SvojstvoOkolineBiometrijskogSustava*, *KarakteristikaKorisnikaBiometrijskogSustava* te *PouzdanostTehnologijeBiometrijskogSustava*. Ovaj kod definira domenu predmetnog modela OOEPBS.

```
ObjectProperty: Interagira

    Annotations:
        TV_pl "Interagira",
        TV_vbg "Interagiraed",
        TV_sg "Interagiras"

    Characteristics:
        Functional

    Domain:
        Interagira some BiometrijskiSustav

    Range:
        Interagira some KarakteristikaKorisnikaBiometrijskogSustava
```

Kôd 7.2 Zapis u manchester notaciji svojstva "Interagira"

Kôd prikazan u 7.2 opisuje svojstvo `Interagira` koje subjektu koji je osoba klase BiometrijskiSustav te kojoj pridružuje individuu klase *KarakteristikaKorisnikaBiometrijskogSustava*. Ovaj kod definira ulogu korisnika unutar

predmetnog modela OOEPBS definirajući odnos biometrijskog sustava prema aspektima vlastite pouzdanosti.

```
ObjectProperty: jeDio

    Annotations:
        TV_sg "jeDioes",
        TV_vbg "jeDioed",
        TV_pl "jeDio"

    Characteristics:
        Functional

    Domain:
        jeDio some BiometrijskiSustav

    Range:
        jeDio some KarakteristikaKorisnikaBiometrijskogSustava,
        jeDio some SvojstvoOkolineBiometrijskogSustava,
        jeDio some PouzdanostTehnologijeBiometrijskogSustava
```

Kôd 7.3 Zapis u manchester notaciji svojstva "jeDio"

Kôd prikazan u 7.2 opisuje svojstvo `jeDio` koje subjektu koji je osoba klase BiometrijskiSustav te kojoj pridržuje pridružuje osobe klase *SvojstvoOkolineBiometrijskogSustava*, *KarakteristikaKorisnikaBiometrijskogSustava* te *PouzdanostTehnologijeBiometrijskogSustava*. Ovaj kod definira također domenu predmetnog modela OOEPBS razmatrajući relaciju aspekata pouzdanosti biometrijskog sustava prema samom biometrijskom sustavu.

```
ObjectProperty: Nema

    Annotations:
        TV_vbg "Nemaed",
        TV_sg "Nemas",
        TV_pl "Nema"

    Characteristics:
        Functional

    Domain:
        Nema some SvojstvoOkolineBiometrijskogSustava,
        Nema some KarakteristikaKorisnikaBiometrijskogSustava,
        Nema some PouzdanostTehnologijeBiometrijskogSustava

    Inverse property of:
        Ima
```

Kôd 7.4 Zapis u manchester notaciji svojstva "Nema"

Kôd prikazan u 7.4 opisuje inverznu funkciju of funkcije opisane u 7.1 , `Ima`.

```
ObjectProperty: NijeDio

    Annotations:
        TV_pl "NijeDio",
        TV_vbg "NijeDioed",
        TV_sg "NijeDioes"

Characteristics:
        Functional

    Range:
        NijeDio some KarakteristikaKorisnikaBiometrijskogSustava,
        NijeDio some SvojstvoOkolineBiometrijskogSustava,
        NijeDio some PouzdanostTehnologijeBiometrijskogSustava

    Inverse property of:
        jeDio
```

Kôd 7.5 Zapis u manchester notaciji svojstva "NijeDio"

Kôd prikazan u 7.4 opisuje inverznu funkciju of funkcije opisane u 7.3 , `JeDio`.

```
ObjectProperty: Utjece

    Annotations:
        TV_sg "Utjeces",
        TV_vbg "Utjeced",
        TV_pl "Utjece"

    Characteristics:
        Functional

    Domain:
        Utjece some PouzdanostTehnologijeBiometrijskogSustava,
        Utjece some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        Utjece some SvojstvoOkolineBiometrijskogSustava
```

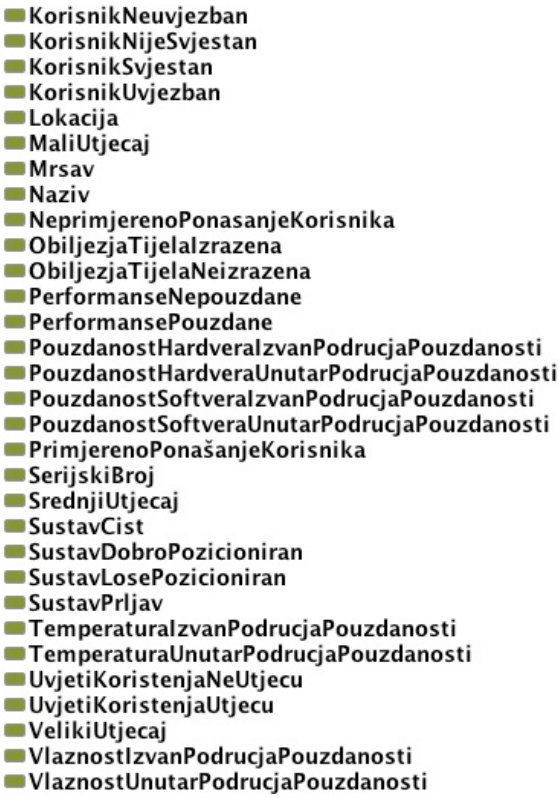
Kôd 7.6 Zapis u manchester notaciji svojstva "Utjece"

Kôd prikazan u 7.6 opisuje svojstvo `Utječe` koje subjektu koji je osoba klase BiometrijskiSustav te kojoj pridružuje osobe klase, *KarakteristikaKorisnikaBiometrijskogSustava* te *PouzdanostTehnologijeBiometrijskogSustava*.

b.) Opis svojstava podataka

Podatkovna svojstva modela OOEPBS su predstavljena slikama 50 i 51:

Slika 50 Podatkovna svojstva modela OOEPBS



Slika 51 Podatkovna svojstva modela OOEPBS

Definirana podatkovna svojstva su opisana sukladno zapisima Manchester notacije na sljedeći način:

```
DataProperty: DimenzijeTijelaIzrazene

    Annotations:
        TV_sg "TjelesneDImenzijeUtjecus",
        TV_pl "TjelesneDImenzijeUtjecu",
        TV_vbg "TjelesneDImenzijeUtjecued"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string
```

Kôd 7.7 Zapis u manchester notaciji svojstva "DimenzijeTijelaIzrazene"

Kôd prikazan u 7.7 opisuje svojstvo `DimenzijeTijelaIzrazene` koje subjektu koji je osoba klase *KarakteristikaKorisnikaBiometrijskogSustava* pridružuje individuu klase *TjelesneDimenzijeUtjecu*.

```
DataProperty: DimenzijeTijelaNeizrazene

    Annotations:
        TV_vbg "TjelesneDimenzijeNeUtjecued",
        TV_sg "TjelesneDimenzijeNeUtjecus",
        TV_pl "TjelesneDimenzijeNeUtjecu"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string
```

Kôd 7.8 Zapis svojstva "DimenzijeTijelaNeizrazene"

Kôd prikazan u 7.8 opisuje svojstvo `DimenzijeTijelaNeizrazene` koje subjektu koji je osoba klase *KarakteristikaKorisnikaBiometrijskogSustava* pridružuje individuu klase *TjelesneDimenzijeNeutjecu*.

```
DataProperty: FizickiVanjskiIzgledBezUtjecaja

    Annotations:
        TV_vbg "FizickiIzgledPrikladaned",
        TV_pl "FizickiIzgledPrikladan",
        TV_sg "FizickiIzgledPrikladans"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string
```

Kôd 7.9 Zapis svojstva "FizickiVanjskiIzgledBezUtjecaja"

Kôd prikazan u 7.9 opisuje svojstvo `FizickiVanjskiIzgledBezUtjecaja` koje subjektu koji je osoba klase *KarakteristikaKorisnikaBiometrijskogSustava* pridružuje individuu klase *FizickiIzgledPrikladan*.

```
DataProperty: FizickiVanjskiIzgledSaUtjecajem

    Annotations:
        TV_vbg "FizickiIzgledNeprikladaned",
        TV_pl "FizickiIzgledNeprikladan",
        TV_sg "FizickiIzgledNeprikladans"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string
```

Kôd 7.10 Zapis svojstva "FizickiVanjskiIzgledSaUtjecajem"

Kôd prikazan u 7.10 opisuje svojstvo `FizickiVanjskiIzgledSaUtjecajem` koje subjektu koji je osoba klase *KarakteristikaKorisnikaBiometrijskogSustava* pridružuje individuu klase *FizickiIzgledNeprikladan*.

```
DataProperty: FMRIzvanPodrucjaPouzdanosti

    Annotations:
        TV_sg "FMRNestandardnis",
        TV_vbg "FMRNestandardnied",
        TV_pl "FMRNestandardni"
```

```
    Characteristics:
        Functional

    Domain:
         Ima some PouzdanostTehnologijeBiometrijskogSustava
         FMRDjelomicnoPouzdan
         and (Ima some FMRNepouzdan)

    Range:
        string
```

Kôd 7.11 Zapis svojstva "FMRIzvanPodrucjaPouzdanosti"

Kôd prikazan u 7.11 opisuje svojstvo `FMRIzvanPodrucjaPouzdanosti` koje subjektu koji je osoba klase PouzdanostTehnologijeBiometrijskogSustava te *FMRDjelomicnoPouzdan and (Ima some FMRNepouzdan)* pridružuje individuu klase *FMRNestandardni*.

```
DataProperty: FMRUnutarPodrucjaPouzdanosti

    Annotations:
        TV_sg "FMRStandardnis",
        TV_vbg "FMRNStandardnied",
        TV_pl "FMRStandardni"

    Characteristics:
        Functional

    Domain:
        Ima some PouzdanostTehnologijeBiometrijskogSustava
        Ima some FMRPouzdan

    Range:
        string
```

Kôd 7.12 Zapis svojstva "FMRUnutarPodrucjaPouzdanosti"

Kôd prikazan u 7.12 opisuje svojstvo `FMRUnutarPodrucjaPouzdanosti` koje subjektu koji je osoba klase *PouzdanostTehnologijeBiometrijskogSustava* te *Ima some FMRPouzdan* pridružuje individuu klase *FMRStandardni*.

```
DataProperty: FNMRIzvanPodrucjaPouzdanosti

    Annotations:
        TV_sg "FNMRNestandardnis",
        TV_vbg "FNMRNestandardnied",
        TV_pl "FNMRNestandardni"
```

```
    Characteristics:
        Functional

    Domain:
         Ima some PouzdanostTehnologijeBiometrijskogSustava
         FNMRNepouzdan
         and (Ima some FNMRDjelomicnoPouzdan)

    Range:
        string
```

Kôd 7.13 Zapis svojstva "FNMRIzvanPodrucjaPouzdanosti"

Kôd prikazan u 7.13 opisuje svojstvo `FNMRIzvanPodrucjaPouzdanosti` koje subjektu koji je osoba klase *PouzdanostTehnologijeBiometrijskogSustava* te *Ima some FNMRNepouzdan* pridružuje individuu klase *FNMRNestandardni*.

```
DataProperty: FNMRUnutarPodrucjaPouzdanosti

    Annotations:
        TV_sg "FNMRStandardnis",
        TV_vbg "FNMRStandardnied",
        TV_pl "FNMRStandardni"

    Characteristics:
        Functional

    Domain:
        Ima some PouzdanostTehnologijeBiometrijskogSustava
        Ima some FNMRPouzdan

    Range:
        string
```

Kôd 7.14 Zapis svojstva "FNMRUnutarPodrucjaPouzdanosti"

Kôd prikazan u 7.14 opisuje svojstvo `FNMRUnutarPodrucjaPouzdanosti` koje subjektu koji je osoba klase *PouzdanostTehnologijeBiometrijskogSustava* te *Ima some FNMRPouzdan* pridružuje individuu klase *FNMRStandardni*.

```
DataProperty: FTAIzvanPodrucjaPouzdanosti

    Annotations:
        TV_sg "FTANestandardnis",
        TV_pl "FTANestandardni",
        TV_vbg "FTANestandardnied"

    Characteristics:
        Functional
```

```
    Domain:
        Ima some PouzdanostTehnologijeBiometrijskogSustava
        Ima some FTANepouzdan,
        Ima some FTADjelomicnoPouzdan

    Range:
        string
```

Kôd 7.15 Zapis svojstva "FTAIzvanPodrucjaPouzdanosti"

Kôd prikazan u 7.15 opisuje svojstvo `FTAIzvanPodrucjaPouzdanosti` koje subjektu koji je osoba klase *PouzdanostTehnologijeBiometrijskogSustava* , *Ima some FTADjelomicnopouzdan* te *Ima some FTANepouzdan*, pridružuje individuu klase *FTANestandardni*.

```
DataProperty: FTAUnutarPodrucjaPouzdanosti

    Annotations:
        TV_vbg "FTAStandardnied",
        TV_pl "FTAStandardni",
        TV_sg "FTAStandardnis"

    Characteristics:
        Functional

    Domain:
        Ima some PouzdanostTehnologijeBiometrijskogSustava
        Ima some FTAPouzdan

    Range:
        string
```

Kôd 7.16 Zapis svojstva "FTAUnutarPodrucjaPouzdanosti"

Kôd prikazan u 7.16 opisuje svojstvo `FTAUNutarPodrucjaPouzdanosti` koje subjektu koji je osoba klase *PouzdanostTehnologijeBiometrijskogSustava* te *Ima some FTAPouzdan*, pridružuje individuu klase *FTAStandardni*.

```
DataProperty: FTEIzvanPodrucjaPouzdanosti

    Annotations:
        TV_vbg "FTENestandardnied",
        TV_pl "FTENestandardni",
        TV_sg "FTENestandardnis"

    Characteristics:
        Functional
```

```
    Domain:
        Ima some PouzdanostTehnologijeBiometrijskogSustava
        Ima some FTEDjelomicnoPouzdan,
        Ima some FTENepouzdan

    Range:
        string
```

Kôd 7.17 Zapis svojstva "FTEIzvanPodrucjaPouzdanosti"

Kôd prikazan u 7.17 opisuje svojstvo `FTEIzvanPodrucjaPouzdanosti` koje subjektu koji je osoba klase *PouzdanostTehnologijeBiometrijskogSustava* , *Ima some FTEDjelomicnopouzdan* te *Ima some FTANepouzdan*, pridružuje individuu klase *FTANestandardni*.

```
DataProperty: FTEUnutarPodrucjaPouzdanosti

    Annotations:
        TV_vbg "FTEStandardnied",
        TV_pl "FTEStandardni",
        TV_sg "FTEStandardnis"

    Characteristics:
        Functional

    Domain:
        Ima some PouzdanostTehnologijeBiometrijskogSustava
        Ima some FTEPouzdan

    Range:
        string
```

Kôd 7.18 Zapis svojstva "FTEUnutarPodrucjaPouzdanosti"

Kôd prikazan u 7.18 opisuje svojstvo `FTEUNutarPodrucjaPouzdanosti` koje subjektu koji je osoba klase *PouzdanostTehnologijeBiometrijskogSustava* te *Ima some FTEPouzdan*, pridružuje individuu klase *FTEStandardni*.

```
DataProperty: ImaKorisnikPouzdan

    Annotations:
        CN_pl "KorisnikPouzdans",
        TV_sg "KorisnikPouzdans",
        TV_pl "KorisnikPouzdan",
```

```
        CN_sg "KorisnikPouzdan",
        TV_vbg "KorisnikPouzdaned"

    Characteristics:
        Functional

    Domain:
        BiometrijskiSustav
        KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string
```

Kôd 7.19 Zapis svojstva "ImaKorisnikPouzdan"

Kôd prikazan u 7.19 opisuje svojstvo `ImaKorisnikPouzdan` koje subjektu koji je osoba klase *BiometrijskiSustav* te *KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *KorisnikPouzdan*.

```
DataProperty: ImaOkolinaPouzdana

    Annotations:
        TV_sg "OkolinaPouzdanas",
        CN_sg "OkolinaPouzdana",
        CN_pl "OkolinaPouzdanas",
        TV_vbg "OkolinaPouzdanaed",
        TV_pl "OkolinaPouzdana"

    Characteristics:
        Functional

    Domain:
        BiometrijskiSustav
        SvojstvoOkolineBiometrijskogSustava

    Range:
        string
```

Kôd 7.20 Zapis svojstva "ImaOkolinaPouzdana"

Kôd prikazan u 7.20 opisuje svojstvo `ImaOkolinaPouzdana` koje subjektu koji je osoba klase *BiometrijskiSustav* te *SvojstvoOkolineBiometrijskogSustava*, pridružuje individuu klase *OkolinaPouzdana*.

```
DataProperty: ImaTehnologijaPouzdana

    Annotations:
        TV_pl "TehnologijaPouzdana",
```

```
        TV_vbg "TehnologijaPouzdanaed",
        TV_sg "TehnologijaPouzdanas",
        CN_pl "TehnologijaPouzdanas",
        CN_sg "TehnologijaPouzdana"

    Characteristics:
        Functional

    Domain:
        BiometrijskiSustav
        PouzdanostTehnologijeBiometrijskogSustava

    Range:
        string
```

Kôd 7.21 Zapis svojstva "ImaTehnologijaPouzdana"

Kôd prikazan u 7.21 opisuje svojstvo `ImaTehnologijaPouzdana` koje subjektu koji je osoba klase *BiometrijskiSustav* te *PouzdanostTehnologijeBiometrijskogSustava*, pridružuje individuu klase *TehnologijaPouzdana*.

```
    DataProperty: IzgledKorisnikaNeprimjeren

    Annotations:
        TV_sg "TjelesniIzgledSaUtjecajems",
        comment "Kosa Brada itd"^^string,
        TV_pl "TjelesniIzgledSaUtjecajem",
        TV_vbg "TjelesniIzgledSaUtjecajemed"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string
```

Kôd 7.22 Zapis svojstva "IzgledKorisnikaNeprimjeren"

Kôd prikazan u 7.22 opisuje svojstvo `IzgledKorisnikaNeprimjeren` koje subjektu koji je osoba klase *KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *TjelesniIzgledSaUtjecajem*.

```
DataProperty: IzgledKorisnikaPrimjeren

    Annotations:
```

```
        TV_vbg "TjelesniIzgledBezUtjecajaed",
        TV_sg "TjelesniIzgledBezUtjecajas",
        comment "Kosa Brada itd"^^string,
        TV_pl "TjelesniIzgledBezUtjecaja"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string
```

Kôd 7.23 Zapis svojstva "IzgledKorisnikaPrimjeren"

Kôd prikazan u 7.23 opisuje svojstvo `IzgledKorisnikaPrimjeren` koje subjektu koji je osoba klase *KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *TjelesniIzgledBezutjecaja*.

```
DataProperty: JacinaBukeIzvanPodrucjaPouzdanosti

    Annotations:
        TV_pl "NestandardnaBuka",
        TV_vbg "NestandardnaBukaed",
        TV_sg "NestandardnaBukas"

    Characteristics:
        Functional

    Domain:
        SvojstvoOkolineBiometrijskogSustava
        Ima some FizickoSvojstvoOkoline

    Range:
        string

    DisjointWith:
        JacinaBukeUnutarPodrucjaPouzdanosti
```

Kôd 7.24 Zapis svojstva "JacinaBukeIzvanPodrucjaPouzdanosti"

Kôd prikazan u 7.24 opisuje svojstvo `JacinaBukeIzvanPodrucjaPouzdanosti` koje subjektu koji je osoba klase *SvojstvoOkolineBiometrijskogSustava* te *Ima some FizickoSvojstvoOkoline*, pridružuje individuu klase *NestandardnaBuka*.

```
DataProperty: JacinaBukeUnutarPodrucjaPouzdanosti

    Annotations:
```

```
        TV_sg "StandardnaBukas",
        TV_pl "StandardnaBuka",
        TV_vbg "StandardnaBukaed"

    Characteristics:
        Functional

    Domain:
        SvojstvoOkolineBiometrijskogSustava
        Ima some FizickoSvojstvoOkoline

    Range:
        string

    DisjointWith:
        JacinaBukeIzvanPodrucjaPouzdanosti
```

Kôd 7.25 Zapis svojstva "JacinaBukeUnutarPodrucjaPouzdanosti"

Kôd prikazan u 7.25 opisuje svojstvo `JacinaBukeUnutarPodrucjaPouzdanosti` koje subjektu koji je osoba klase *SvojstvoOkolineBiometrijskogSustava* te *Ima some FizickoSvojstvoOkoline*, pridružuje individuu klase *StandardnaBuka*.

```
DataProperty: JacinaOsvjetljenjaIzvanPodrucjaPouzdanosti

    Annotations:
        TV_pl "NestandardnoOsvjetljenje",
        TV_sg "NestandardnoOsvjetljenjes",
        TV_vbg "NestandardnoOsvjetljenjed"

    Characteristics:
        Functional

    Domain:
        SvojstvoOkolineBiometrijskogSustava
        Ima some FizickoSvojstvoOkoline

    Range:
        string

    DisjointWith:
        JacinaOsvjetljenjaUnutarPodrucjaPouzdanosti
```

Kôd 7.26 Zapis svojstva "JacinaOsvjetljenjaIzvanPodrucjaPouzdanosti"

Kôd prikazan u 7.26 opisuje svojstvo `JacinaOsvjetljenjaIzvanPodrucjaPouzdanosti` koje subjektu koji je osoba klase *SvojstvoOkolineBiometrijskogSustava* te *Ima some FizickoSvojstvoOkoline*, pridružuje individuu klase *NestandardnoOsvjetljenje*.

```
DataProperty: JacinaOsvjetljenjaUnutarPodrucjaPouzdanosti

    Annotations:
        TV_sg "StandardnoOsvjetljenjes",
        TV_vbg "StandardnoOsvjetljenjed",
        TV_pl "StandardnoOsvjetljenje"

    Characteristics:
        Functional

    Domain:
        Ima some SvojstvoOkolineBiometrijskogSustava

    Range:
        string

    DisjointWith:
        JacinaOsvjetljenjaIzvanPodrucjaPouzdanosti
```

Kôd 7.27 Zapis svojstva "JacinaOsvjetljenjaUnutarPodrucjaPouzdanosti"

Kôd prikazan u 7.27 opisuje svojstvo `JacinaOsvjetljenjaUnutarPodrucjaPouzdanosti` koje subjektu koji je osoba klase *SvojstvoOkolineBiometrijskogSustava* te *Ima some FizickoSvojstvoOkoline*, pridružuje individuu klase *StandardnoOsvjetljenje*.

```
DataProperty: KorisnikImaBolest

    Annotations:
        TV_vbg "ImaBolested",
        TV_pl "ImaBolest",
        TV_sg "ImaBolests"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string

    DisjointWith:
        KorisnikNemaBolest
```

Kôd 7.28 Zapis svojstva "KorisnikImaBolest"

Kôd prikazan u 7.28 opisuje svojstvo `KorisnikImaBolest` koje subjektu koji je osoba klase *Ima some KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *ImaBolest*.

```
DataProperty: KorisnikNemaBolest

    Annotations:
        TV_sg "NemaBolests",
        TV_vbg "NemaBolested",
        TV_pl "NemaBolest"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string

    DisjointWith:
        KorisnikImaBolest
```

Kôd 7.29 Zapis svojstva "KorisnikNemaBolest"

Kôd prikazan u 7.29 opisuje svojstvo `KorisnikNemaBolest` koje subjektu koji je osoba klase *Ima some KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *NemaBolest*.

```
DataProperty: KorisnikNeuvjezban

    Annotations:
        TV_sg "KorisnikNeuvjezbans",
        TV_vbg "KorisnikNeuvjezbaned",
        TV_pl "KorisnikNeuvjezban"

    Characteristics:
        Functional

    Domain:
        KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string

    DisjointWith:
        KorisnikUvjezban
```

Kôd 7.30 Zapis svojstva "KorisnikNeuvjezban"

Kôd prikazan u 7.30 opisuje svojstvo `KorisnikNeuvjezban` koje subjektu koji je osoba klase *KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *KorisnikNeuvjezban*.

```
DataProperty: KorisnikNijeSvjestan

    Annotations:
        TV_sg "KorisnikNijeSvjestans",
        TV_vbg "KorisnikNijeSvjestaned",
        TV_pl "KorisnikNijeSvjestan"

    Characteristics:
        Functional

    Domain:
        KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string

    DisjointWith:
        KorisnikSvjestan
```

Kôd 7.31 Zapis svojstva "KorisnikNijeSvjestan"

Kôd prikazan u 7.31 opisuje svojstvo `KorisnikNijeSvjestan` koje subjektu koji je osoba klase *KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *KorisnikNijeSvjestan*.

```
DataProperty: KorisnikSvjestan

    Annotations:
        TV_pl "KorisnikSvjestan",
        TV_sg "KorisnikSvjestans",
        TV_vbg "KorisnikSvjestaned"

    Characteristics:
        Functional

    Domain:
        KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string

    DisjointWith:
```

```
        KorisnikNijeSvjestan
```

Kôd 7.32 Zapis svojstva "KorisnikSvjestan"

Kôd prikazan u 7.32 opisuje svojstvo `KorisnikSvjestan` koje subjektu koji je osoba klase *KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *KorisnikSvjestan*.

```
DataProperty: KorisnikUvjezban

    Annotations:
        TV_pl "KorisnikUvjezban",
        TV_vbg "KorisnikUvjezbaned",
        TV_sg "KorisnikUvjezbans"

    Characteristics:
        Functional

    Domain:
        KarakteristikaKorisnikaBiometrijskogSustava

    DisjointWith:
        KorisnikNeuvjezban
```

Kôd 7.33 Zapis svojstva "KorisnikUvjezban"

Kôd prikazan u 7.33 opisuje svojstvo `KorisnikUvjezban` koje subjektu koji je osoba klase *KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *KorisnikUvjezban*.

```
DataProperty: Lokacija

    Annotations:
        CN_pl "Lokacijas",
        TV_sg "Lokacijas",
        TV_pl "Lokacija",
        TV_vbg "Lokacijaed",
        CN_sg "Lokacija"

    Characteristics:
        Functional

    Domain:
        BiometrijskiSustav

    Range:
        string
```

Kôd 7.34 Zapis svojstva "Lokacija"

Kôd prikazan u 7.34 opisuje svojstvo `Lokacija` koje subjektu koji je osoba klase *BiometrijskiSustav*, pridružuje individuu klase *Lokacija*.

```
DataProperty: MaliUtjecaj

    Annotations:
        TV_vbg "MaliUtjecajed",
        comment "1",
        TV_sg "MaliUtjecajs",
        TV_pl "MaliUtjecaj"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava
        Ima some MaliUtjecajNaKorisnika

    Range:
        string

    SubPropertyOf:
        topDataProperty
```

Kôd 7.35 Zapis svojstva "MaliUtjecaj"

Kôd prikazan u 7.35 opisuje svojstvo `MaliUtjecaj` koje subjektu koji je osoba klase *Ima some KarakteristikaKorisnikaBiometrijskogSustava;Ima some MaliUtjecajNaKorisnika*, pridružuje individuu klase *MaliUtjecaj*.

```
DataProperty: Mrsav

    Annotations:
        TV_pl "Mrsav",
        TV_vbg "Mrsaved",
        TV_sg "Mrsavs"

    Characteristics:
        Functional

    Domain:
        KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string
```

Kôd 7.36 Zapis svojstva "Mrsav"

Kôd prikazan u 7.36 opisuje svojstvo `Mrsav` koje subjektu koji je osoba klase *Ima some KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *KarakteristikaKorisnikaBiometrijskogSustava*.

```
DataProperty: Naziv

    Annotations:
        CN_sg "Naziv",
        TV_sg "Nazivs",
        TV_pl "Naziv",
        TV_vbg "Nazived",
        CN_pl "Nazivs"

    Characteristics:
        Functional

    Domain:
        BiometrijskiSustav

    Range:
        string
```

Kôd 7.37 Zapis svojstva "Naziv"

Kôd prikazan u 7.37 opisuje svojstvo `Naziv` koje subjektu koji je osoba klase *Ima some BiometrijskiSustav*, pridružuje individuu klase *Naziv*.

```
DataProperty: NeprimjerenoPonasanjeKorisnika

    Annotations:
        TV_sg "NeprimjerenoPonasanjes",
        TV_vbg "NeprimjerenoPonasanjed",
        TV_pl "NeprimjerenoPonasanje"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string

    DisjointWith:
        PrimjerenoPonašanjeKorisnika
```

Kôd 7.38 Zapis svojstva "NeprimjerenoPonasanjeKorisnika"

Kôd prikazan u 7.38 opisuje svojstvo `NeprimjerenoPonasanjeKorisnika` koje subjektu koji je osoba klase *Ima some KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *NeprimjerenoPonasanje*.

```
DataProperty: ObiljezjaTijelaIzrazena

    Annotations:
        TV_vbg "ImaObiljezjaed",
        TV_sg "ImaObiljezjas",
        TV_pl "ImaObiljezja"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string

    DisjointWith:
        ObiljezjaTijelaNeizrazena
```

Kôd 7.39 Zapis svojstva "ObiljezjaTijelaIzrazena"

Kôd prikazan u 7.39 opisuje svojstvo `ObiljezjaTijelaIzrazena` koje subjektu koji je osoba klase *Ima some KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *ImaObiljezja*.

```
DataProperty: ObiljezjaTijelaNeizrazena

    Annotations:
        TV_vbg "NemaObiljezjaed",
        TV_sg "NemaObiljezjas",
        TV_pl "NemaObiljezja"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string

    DisjointWith:
        ObiljezjaTijelaIzrazena
```

Kôd 7.40 Zapis svojstva "ObiljezjaTijelaNeizrazena"

Kôd prikazan u 7.40 opisuje svojstvo `ObiljezjaTijelaNeizrazena` koje subjektu koji je osoba klase *Ima some KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *NemaObiljezja*.

```
DataProperty: PerformanseNepouzdane

    Annotations:
        TV_pl "PerformanseNepouzdane",
        TV_vbg "PerformanseNepouzdaned",
        TV_sg "PerformanseNepouzdanes"

    Characteristics:
        Functional

    Domain:
        Ima some PouzdanostTehnologijeBiometrijskogSustava

    Range:
        string

    DisjointWith:
        PerformansePouzdane
```

Kôd 7.41 Zapis svojstva "PerformanseNepouzdane"

Kôd prikazan u 7.41 opisuje svojstvo `PerformanseNepouzdane` koje subjektu koji je osoba klase *Ima some PouzdanostTehnologijeBiometrijskogSustava*, pridružuje individuu klase *PerformanseNepouzdane*.

```
DataProperty: PerformansePouzdane

    Annotations:
        TV_sg "PerformansePouzdanes",
        TV_vbg "PerformansePouzdaned",
        TV_pl "PerformansePouzdane"

    Characteristics:
        Functional

    Domain:
        Ima some PouzdanostTehnologijeBiometrijskogSustava

    Range:
        string

    DisjointWith:
        PerformanseNepouzdane
```

Kôd 7.42 Zapis svojstva "PerformansePouzdane"

Kôd prikazan u 7.42 opisuje svojstvo `PerformanseNepouzdane` koje subjektu koji je osoba klase *Ima some PouzdanostTehnologijeBiometrijskogSustava*, pridružuje individuu klase *PerformanseNepouzdane*.

```
DataProperty: PouzdanostHardveraIzvanPodrucjaPouzdanosti

    Annotations:
        CN_sg "HardverNepouzdan",
        TV_pl "HardverNepouzdan",
        TV_vbg "HardverNepouzdaned",
        TV_sg "HardverNepouzdans",
        CN_pl "HardverNepouzdans"

    Characteristics:
        Functional

    Domain:
        HardverDjelomicnoPouzdan
         and (Ima some HardverNepouzdan)

    Range:
        string

    DisjointWith:
        PouzdanostHardveraUnutarPodrucjaPouzdanosti
```

Kôd 7.43 Zapis svojstva "PouzdanostHardveraIzvanPodrucjaPouzdanosti"

Kôd prikazan u 7.43 opisuje svojstvo `PouzdanostHardveraIzvanPodrucjaPouzdanosti` koje subjektu koji je osoba klase *HardverDjelomicnoPouzdan and (Ima some HardverNepouzdan)*, pridružuje individuu klase *HardverNepouzdan&HardverDjelomicnoPouzdan*.

```
DataProperty: PouzdanostHardveraUnutarPodrucjaPouzdanosti

    Annotations:
        TV_pl "HardverPouzdan",
        CN_sg "HardverPouzdan",
        TV_sg "HardverPouzdans",
        TV_vbg "HardverPouzdaned",
        CN_pl "HardverPouzdans"
```

```
    Characteristics:
        Functional

    Domain:
        Ima some HardverPouzdan

    Range:
        string

    DisjointWith:
        PouzdanostHardveraIzvanPodrucjaPouzdanosti
```

Kôd 7.44 Zapis svojstva "PouzdanostHardveraUnutarPodrucjaPouzdanosti"

Kôd prikazan u 7.44 opisuje svojstvo `PouzdanostHardveraUnutarPodrucjaPouzdanosti` koje subjektu koji je osoba klase *Ima some HardverPouzdan*, pridružuje individuu klase *HardverPouzdan*.

```
DataProperty: PouzdanostSoftveraIzvanPodrucjaPouzdanosti

    Annotations:
        TV_sg "softverNepouzdans",
        CN_sg "SoftverNepouzdan",
        TV_pl "softverNepouzdan",
        CN_pl "SoftverNepouzdans",
        TV_vbg "softverNepouzdaned"

    Characteristics:
        Functional

    Domain:
        SoftverNepouzdan
         and (Ima some SoftverDjelomicnoPouzdan)

    Range:
        string

    DisjointWith:
        PouzdanostSoftveraUnutarPodrucjaPouzdanosti
```

Kôd 7.45 Zapis svojstva "PouzdanostSoftveraIzvanPodrucjaPouzdanosti"

Kôd prikazan u 7.45 opisuje svojstvo `PouzdanostSoftveraIzvanPodrucjaPouzdanosti` koje subjektu koji je osoba klase *SoftverNepouzdan and (Ima some SoftverDjelomicnoPouzdan)*, pridružuje individuu klase *SoftverNepouzdan&SoftverDjelomicnoPouzdan*.

```
DataProperty: PouzdanostSoftveraUnutarPodrucjaPouzdanosti

    Annotations:
        TV_sg "SoftverPouzdans",
        TV_vbg "SoftverPouzdaned",
        TV_pl "SoftverPouzdan",
        CN_sg "SoftverPouzdan",
        CN_pl "SoftverPouzdans"

    Characteristics:
        Functional

    Domain:
        Ima some SoftverPouzdan

    Range:
        string

    DisjointWith:
        PouzdanostSoftveraIzvanPodrucjaPouzdanosti
```

Kôd 7.46 Zapis svojstva "PouzdanostSoftveraUnutarPodrucjaPouzdanosti"

Kôd prikazan u 7.46 opisuje svojstvo `PouzdanostSoftveraUnutarPodrucjaPouzdanosti` koje subjektu koji je osoba klase *Ima some SoftverPouzdan* , pridružuje individuu klase *SoftverPouzdan*.

```
DataProperty: PrimjerenoPonašanjeKorisnika

    Annotations:
        TV_pl "PrimjerenoPonašanje",
        TV_sg "PrimjerenoPonašanje",
        TV_vbg "PrimjerenoPonašanje"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string

    DisjointWith:
        NeprimjerenoPonasanjeKorisnika
```

Kôd 7.47 Zapis svojstva "PrimjerenoPonasanjeKorisnika"

Kôd prikazan u 7.47 opisuje svojstvo `PrimjerenoPonašanjeKorisnika` koje subjektu koji je osoba klase *Ima some KarakteristikaKorisnikaBiometrijskogSustava* , pridružuje individuu klase *PrimjerenoPonašanje*.

```
DataProperty: SerijskiBroj

    Annotations:
        TV_sg "SerijskiBrojs",
        TV_pl "SerijskiBroj",
        CN_sg "SerijskiBroj",
        CN_pl "SerijskiBrojs",
        TV_vbg "SerijskiBrojed"

    Characteristics:
        Functional

    Domain:
        BiometrijskiSustav

    Range:
        string
```

Kôd 7.48 Zapis svojstva "SerijskiBroj"

Kôd prikazan u 7.48 opisuje svojstvo `SerijskiBroj` koje subjektu koji je osoba klase *BiometrijskiSustav* , pridružuje individuu klase *SerijskiBroj*.

```
DataProperty: SrednjiUtjecaj

    Annotations:
        comment "2",
        TV_sg "SrednjiUtjecajs",
        TV_pl "SrednjiUtjecaj",
        TV_vbg "SrednjiUtjecajed"

    Characteristics:
        Functional

    Domain:
        Ima some SrednjiUtjecajNaKorisnika

    Range:
        string
```

Kôd 7.49 Zapis svojstva "SrednjiUtjecaj"

Kôd prikazan u 7.49 opisuje svojstvo `SrednjiUtjecaj` koje subjektu koji je osoba klase *Ima some SrednjiUtjecajNaKorisnika* , pridružuje individuu klase *SrednjiUtjecaj*.

```
DataProperty: SustavCist

    Annotations:
        TV_vbg "Cisted",
        TV_pl "Cist",
        TV_sg "Cists"

    Characteristics:
        Functional

    Domain:
        Ima some UvjetiKoristenjaSustava

    Range:
        string

    DisjointWith:
        SustavPrljav
```

Kôd 7.50 Zapis svojstva "SustavCist"

Kôd prikazan u 7.50 opisuje svojstvo `SustavCist` koje subjektu koji je osoba klase *Ima some UvjetiKoristenjaSustava* , pridružuje individuu klase *Cist*.

```
DataProperty: SustavDobroPozicioniran

    Annotations:
        TV_vbg "DobroPozicioniraned",
        TV_sg "DobroPozicionirans",
        TV_pl "DobroPozicioniran"

    Characteristics:
        Functional

    Domain:
        Ima some UtjecajPozicijeSustava

    Range:
        string

    DisjointWith:
        SustavLosePozicioniran
```

Kôd 7.51 Zapis svojstva "SustavDobroPozicioniran"

Kôd prikazan u 7.51 opisuje svojstvo `SustavDobroPozicioniran` koje subjektu koji je osoba klase *Ima some UtjecajPozicijeSustava* , pridružuje individuu klase *DobroPozicioniran*.

```
DataProperty: SustavLosePozicioniran

    Annotations:
        TV_pl "LosePozicioniran",
        TV_vbg "LosePozicioniraned",
        TV_sg "LosePozicionirans"

    Characteristics:
        Functional

    Domain:
        Ima some UtjecajPozicijeSustava

    Range:
        string

    DisjointWith:
        SustavDobroPozicioniran
```

Kôd 7.52 Zapis svojstva "SustavLosePozicioniran"

Kôd prikazan u 7.52 opisuje svojstvo `SustavLosePozicioniran` koje subjektu koji je osoba klase *Ima some UtjecajPozicijeSustava* , pridružuje individuu klase *LosePozicioniran*.

```
DataProperty: SustavPrljav

    Annotations:
        TV_pl "Prljav",
        TV_vbg "Prljaved",
        TV_sg "Prljavs"

    Characteristics:
        Functional

    Domain:
        Ima some UvjetiKoristenjaSustava

    Range:
        string

    DisjointWith:
        SustavCist
```

Kôd 7.53 Zapis svojstva "SustavCist"

Kôd prikazan u 7.53 opisuje svojstvo `SustavPrljav` koje subjektu koji je osoba klase *Ima some UvjetiKoristenjaSustava*, pridružuje individuu klase *Prljav*.

```
DataProperty: TemperaturaIzvanPodrucjaPouzdanosti

    Annotations:
        TV_sg "NestandardnaTemperaturas",
        TV_pl "NestandardnaTemperatura",
        TV_vbg "NestandardnaTemperaturaed"

    Characteristics:
        Functional

    Domain:
        Ima some NestandardnaTemperaturaOkoline

    Range:
        string

    DisjointWith:
        TemperaturaUnutarPodrucjaPouzdanosti
```

Kôd 7.54 Zapis svojstva "TemperaturaIzvanPodrucjaPouzdanosti"

Kôd prikazan u 7.54 opisuje svojstvo `TemperaturaIzvanPodrucjaPouzdanosti` koje subjektu koji je osoba klase *Ima some NestandardnaTemperaturaOkoline*, pridružuje individuu klase *NestandardnaTemperatura*.

```
DataProperty: TemperaturaUnutarPodrucjaPouzdanosti

    Annotations:
        TV_vbg "StandardnaTemperaturaed",
        TV_sg "StandardnaTemperaturas",
        TV_pl "StandardnaTemperatura"

    Characteristics:
        Functional

    Domain:
        Ima some StandardnaTemperaturaOkoline


    Range:
        string

    DisjointWith:
        TemperaturaIzvanPodrucjaPouzdanosti
```

Kôd 7.55 Zapis svojstva "TemperaturaUnutarPodrucjaPouzdanosti"

Kôd prikazan u 7.55 opisuje svojstvo `TemperaturaUnutarPodrucjaPouzdanosti` koje subjektu koji je osoba klase *Ima some StandardnaTemperaturaOkoline*, pridružuje individuu klase *StandardnaTemperatura*.

```
DataProperty: UvjetiKoristenjaNeUtjecu

    Annotations:
        TV_sg "UvjetiKoristenjaNeUtjecus",
        TV_pl "UvjetiKoristenjaNeUtjecu",
        TV_vbg "UvjetiKoristenjaNeUtjecued"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string
```

Kôd 7.56 Zapis svojstva "UvjetiKoristenjaNeUtjecu"

Kôd prikazan u 7.56 opisuje svojstvo `UvjetiKoristenjaNeUtjecu` koje subjektu koji je osoba klase *Ima some KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *UvjetiKoristenjaNeUtjecu*.

```
DataProperty: UvjetiKoristenjaUtjecu

    Annotations:
        TV_vbg "UvjetiKoristenjaUtjecued",
        CN_pl "UvjetiKoristenjaUtjecus",
        CN_sg "UvjetiKoristenjaUtjecu",
        TV_pl "UvjetiKoristenjaUtjecu",
        TV_sg "UvjetiKoristenjaUtjecus"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        string
```

Kôd 7.57 Zapis svojstva "UvjetiKoristenjaUtjecu"

Kôd prikazan u 7.57 opisuje svojstvo `UvjetiKoristenjaUtjecu` koje subjektu koji je osoba klase *Ima some KarakteristikaKorisnikaBiometrijskogSustava*, pridružuje individuu klase *UvjetiKoristenjaUtjecu*.

```
DataProperty: VelikiUtjecaj

    Annotations:
        TV_vbg "VelikiUtjecajed",
        comment "1",
        TV_sg "VelikiUtjecajs",
        TV_pl "VelikiUtjecaj"

    Characteristics:
        Functional

    Domain:
        Ima some VelikiUtjecajNaKorisnika

    Range:
        string
```

Kôd 7.58 Zapis svojstva "VelikiUtjecaj"

Kôd prikazan u 7.58 opisuje svojstvo `VelikiUtjecaj` koje subjektu koji je osoba klase *Ima some VelikiUtjecajNaKorisnika*, pridružuje individuu klase *VelikiUtjecaj*.

```
DataProperty: VlaznostIzvanPodrucjaPouzdanosti

    Annotations:
        TV_pl "NestandardnaVlaznost",
        TV_sg "NestandardnaVlaznosts",
        TV_vbg "NestandardnaVlaznosted"

    Characteristics:
        Functional


    Domain:
        Ima some SvojstvoOkolineBiometrijskogSustava

    Range:
        string

    DisjointWith:
        VlaznostUnutarPodrucjaPouzdanosti
```

Kôd 7.59 Zapis svojstva "VlaznostIzvanPodrucjaPouzdanosti"

Kôd prikazan u 7.59 opisuje svojstvo `VlaznostIzvanPodrucjaPouzdanosti` koje subjektu koji je osoba klase *Ima some SvojstvoOkolineBiometrijskogSustava*, pridružuje individuu klase *NestandardnaVlaznost*.

```
DataProperty: VlaznostUnutarPodrucjaPouzdanosti

    Annotations:
        TV_sg "StandardnaVlaznosts",
        TV_pl "StandardnaVlaznost",
        TV_vbg "StandardnaVlaznosted"

    Characteristics:
        Functional

    Domain:
        Ima some SvojstvoOkolineBiometrijskogSustava

    Range:
        string

    DisjointWith:
        VlaznostIzvanPodrucjaPouzdanosti
```

Kôd 7.60 Zapis svojstva "VlaznostUnutarPodrucjaPouzdanosti"

Kôd prikazan u 7.60 opisuje svojstvo `VlaznostUnutarPodrucjaPouzdanosti` koje subjektu koji je osoba klase *Ima some SvojstvoOkolineBiometrijskogSustava*, pridružuje individuu klase *StandardnaVlaznost*.

7.7 Kreiranje instanci modela OOEPBS

Instanca odnosno osoba [113] u ontologijama predstavlja konkretizaciju klasa odnosno entiteta. Konkretizacija entiteta predstavlja podlogu za proces testiranja definiranog modela utemeljen na postavkama testnih modela putem instanci ontologije. Instance ontologije u slučaju modela OOEPBS predstavljaju sljedeće entitete:

- Biometrijski sustav 1 (*BS1*),
- Biometrijski sustav 2 (*BS2*)
- Biometrijski sustav 3 (*BS3*)
- Aspekti pouzdanosti predstavljenih biometrijskih sustava:
    - Okolina Biometrijskog sustava

        - Okolina 1 (*OK1*),
        - Okolina 2 (*OK2*),
        - Okolina 3 (*OK3*),
    - Tehnologija biometrijskog sustava
        - Tehnologija1 (*TE1*),
        - Tehnologija 2 (*TE2*),
        - Tehnologija 3 (*TE3*),
    - Korisnik biometrijskog sustava
        - Korisnik 1 (*KO1*),
        - Korisnik 2 (*KO2*)
        - Korisnik 3 (*KO3*).

Navedene instance modela OOEPBS prikazane su na slici 52.

Slika 52 Instance modela OOEPBS

Svaka od navedenih instanci ima definirane karakteristike sukladno propozicijama modela OOEPBS te ih se može predstaviti putem Manchester zapisa kako slijedi:

```
Osobal: BiometrijskiSustav1
    Annotations:
        comment "Biometrijski sustav za prepoznavanje otiska
dlana"^^string,
        PN_sg "BS1"
    Types:
        BiometrijskiSustavPouzdan,
        BiometrijskiSustavTemeljenNaOtiskuDlana,
        A1B1C2
    Facts:
```

```
    VlaznostUnutarPodrucjaPouzdanosti  "50"^^string,
    JacinaBukeUnutarPodrucjaPouzdanosti  "80"^^string,
    Lokacija  "Biometrijski laboratorij FOI"^^string,
    FNMRUnutarPodrucjaPouzdanosti  "1"^^string,
    KorisnikUvjezban  "1"^^string,
    Naziv  "Biometrijski sustav za prepoznavanje otiska
dlana"^^string,
    FizickiVanjskiIzgledBezUtjecaja  "1"^^string,
    IzgledKorisnikaPrimjeren  "1"^^string,
    UvjetiKoristenjaNeUtjecu  "1"^^string,
    FTAUnutarPodrucjaPouzdanosti  "1"^^string,
    ObiljezjaTijelaIzrazena  "2"^^string,
    TemperaturaUnutarPodrucjaPouzdanosti  "22"^^string,
    KorisnikImaBolest  "2"^^string,
    PrimjerenoPonašanjeKorisnika  "1"^^string,
    PouzdanostSoftveraUnutarPodrucjaPouzdanosti  "96"^^string,
    SerijskiBroj  "SN001435B23456984XXZ"^^string,
    SustavDobroPozicioniran  "1"^^string,
    DimenzijeTijelaNeizrazene  "1"^^string,
    FMRUnutarPodrucjaPouzdanosti  "1"^^string,
    FTEUnutarPodrucjaPouzdanosti  "1"^^string,
    PouzdanostHardveraUnutarPodrucjaPouzdanosti  "96"^^string,
    JacinaOsvjetljenjaUnutarPodrucjaPouzdanosti  "1600"^^string
```

Kôd 7.61 Zapis instance “BiometrijskiSustav1"

Kôd prikazan u 7.61 opisuje instancu `BiometrijskiSustav1` koja ima oznaku `PN_sg "BS1"` te predstavlja model «`Biometrijski sustav za prepoznavanje otiska dlana"^^string`». Ova instanca uključuje aspekte pouzdanosti u obliku `Okolina1`, `Tehnologija1` te `Korisnik1`.

```
Osobal: BiometrijskiSustav2
    Annotations:
        PN_sg "BS2",
        comment  "Biometrijski  sustav  za  prepoznavanje  otiska
prsta"^^string
    Types:
```

```
        A1B3C2,
        BiometrijskiSustavTemeljenNaOtiskuPrsta,
        BiometrijskiSustavDjelomicnoPouzdan
    Facts:
     FMRUnutarPodrucjaPouzdanosti  "1"^^string,
     SustavDobroPozicioniran  "1"^^string,
     UvjetiKoristenjaUtjecu  "2"^^string,
     KorisnikUvjezban  "1"^^string,
     PouzdanostSoftveraUnutarPodrucjaPouzdanosti  "96"^^string,
     Naziv      "Biometrijski   sustav   za   prepoznavanje   otiska
prsta"^^string,
     FTAUnutarPodrucjaPouzdanosti  "1"^^string,
     TemperaturaUnutarPodrucjaPouzdanosti  "22"^^string,
     ObiljezjaTijelaIzrazena  "2"^^string,
     IzgledKorisnikaPrimjeren  "1"^^string,
     NeprimjerenoPonasanjeKorisnika  "2"^^string,
     JacinaBukeIzvanPodrucjaPouzdanosti  "85"^^string,
     FNMRUnutarPodrucjaPouzdanosti  "1"^^string,
     PouzdanostHardveraUnutarPodrucjaPouzdanosti  "96"^^string,
     Lokacija  "Biometrijski laboratorij FOI"^^string,
     DimenzijeTijelaIzrazene  "2"^^string,
     VlaznostIzvanPodrucjaPouzdanosti  "90"^^string,
     SerijskiBroj  "SN008876456334324ZKP"^^string,
     JacinaOsvjetljenjaUnutarPodrucjaPouzdanosti  "2000"^^string,
     FizickiVanjskiIzgledBezUtjecaja  "1"^^string,
     FTEUnutarPodrucjaPouzdanosti  "1"^^string,
     KorisnikImaBolest  "2"^^string
```

Kôd 7.62 Zapis instance “BiometrijskiSustav2"

Kôd prikazan u 7.62 opisuje instancu `BiometrijskiSustav2` koja ima oznaku `PN_sg "BS2"` te predstavlja model «`Biometrijski sustav za prepoznavanje otiska prsta"^^string`». Ova instanca uključuje aspekte pouzdanosti u obliku `Okolina2`, `Tehnologija2` te `Korisnik2`.

```
Osobal: BiometrijskiSustav3
    Annotations:
```

```
        comment     "Biometrijski     sustav     za     prepoznavanje
glasa"^^string,
        PN_sg "BS3"
    Types:
        BiometrijskiSustavTemeljenNaOtiskuGlasa,
        A1B2C3,
        BiometrijskiSustavNepouzdan
    Facts:
     FTAUnutarPodrucjaPouzdanosti  "1"^^string,
     ObiljezjaTijelaIzrazena  "3"^^string,
     PouzdanostHardveraUnutarPodrucjaPouzdanosti  "96"^^string,
     PouzdanostSoftveraUnutarPodrucjaPouzdanosti  "96"^^string,
     FizickiVanjskiIzgledBezUtjecaja  "1"^^string,
     SerijskiBroj  "SNXCV5B23456983344KLM"^^string,
     Lokacija  "Biometrijski laboratorij FOI"^^string,
     IzgledKorisnikaPrimjeren  "1"^^string,
     FNMRUnutarPodrucjaPouzdanosti  "1"^^string,
     FMRUnutarPodrucjaPouzdanosti  "1"^^string,
     TemperaturaUnutarPodrucjaPouzdanosti  "22"^^string,
     NeprimjerenoPonasanjeKorisnika  "3"^^string,
     UvjetiKoristenjaNeUtjecu  "1"^^string,
     JacinaBukeIzvanPodrucjaPouzdanosti  "85"^^string,
     KorisnikUvjezban  "1"^^string,
     VlaznostUnutarPodrucjaPouzdanosti  "50"^^string,
     SustavDobroPozicioniran  "1"^^string,
     FTEUnutarPodrucjaPouzdanosti  "1"^^string,
     DimenzijeTijelaNeizrazene  "1"^^string,
     KorisnikImaBolest  "3"^^string,
     Naziv  "Biometrijski sustav za prepoznavanje glasa"^^string
```

Kôd 7.63 Zapis instance “BiometrijskiSustav3"

Kôd prikazan u 7.63 opisuje instancu `BiometrijskiSustav3` koja ima oznaku `PN_sg "BS3"` te predstavlja model «`Biometrijski sustav za prepoznavanje otiska glasa"^^string`». Ova instanca uključuje aspekte pouzdanosti u obliku `Okolina3`, `Tehnologija3` te `Korisnik3`.

`Osobal: Tehnologija1`

```
    Annotations:
        PN_sg "TE1"
    Types:
        TehnologijaPouzdana,
        A1
    Facts:
     jeDio  BiometrijskiSustav1,
     PouzdanostHardveraUnutarPodrucjaPouzdanosti  "96"^^string,
     PouzdanostSoftveraUnutarPodrucjaPouzdanosti  "96"^^string,
     FTAUnutarPodrucjaPouzdanosti  "1"^^string,
     FMRUnutarPodrucjaPouzdanosti  "1"^^string,
     FNMRUnutarPodrucjaPouzdanosti  "1"^^string,
     FTEUnutarPodrucjaPouzdanosti  "1"^^string
```

Kôd 7.64 Zapis instance "Tehnologija1"

Kôd prikazan u 7.64 opisuje instancu `Tehnologija1` koja ima oznaku `PN_sg "TE1"` te predstavlja aspekt `Tehnologija` instance `BiometrijskiSustav1`. Ova instanca ima sljedeće pretpostavke: Pouzdanost Hardvera postavljena je kao `PouzdanostHardveraUnutarPodrucjaPouzdanosti "96"^^string`, Pouzdanost Softvera postavljena je kao `PouzdanostSoftveraUnutarPodrucjaPouzdanosti "96"^^string`, Pouzdanost FTA postavljena je kao `FTAUnutarPodrucjaPouzdanosti "1"^^string`, Pouzdanost FTE postavljena je kao `FTEUnutarPodrucjaPouzdanosti "1"^^string`, Pouzdanost FMR postavljena je kao `FMRUnutarPodrucjaPouzdanosti "1"^^string`, Pouzdanost FNMR postavljena je kao `FNMRUnutarPodrucjaPouzdanosti "1"^^string`.

```
Osobal: Tehnologija2
    Annotations:
        PN_sg "TE2"
    Types:
        TehnologijaPouzdana,
        A1

    Facts:
     jeDio  BiometrijskiSustav2,
```

```
    PouzdanostHardveraUnutarPodrucjaPouzdanosti  "96"^^string,
    FTAUnutarPodrucjaPouzdanosti  "1"^^string,
    FTEUnutarPodrucjaPouzdanosti  "1"^^string,
    FNMRUnutarPodrucjaPouzdanosti  "1"^^string,
    PouzdanostSoftveraUnutarPodrucjaPouzdanosti  "96"^^string,
    FMRUnutarPodrucjaPouzdanosti  "1"^^string
```

Kôd 7.65 Zapis instance "Tehnologija2"

Kôd prikazan u 7.65 opisuje instancu `Tehnologija2` koja ima oznaku `PN_sg "TE2"` te predstavlja aspekt `Tehnologija` instance `BiometrijskiSustav2`. Ova instanca ima sljedeće pretpostavke: Pouzdanost Hardvera postavljena je kao `PouzdanostHardveraUnutarPodrucjaPouzdanosti "96"^^string`, Pouzdanost Softvera postavljena je kao `PouzdanostSoftveraUnutarPodrucjaPouzdanosti "96"^^string`, Pouzdanost FTA postavljena je kao `FTAUnutarPodrucjaPouzdanosti "1"^^string`, Pouzdanost FTE postavljena je kao `FTEUnutarPodrucjaPouzdanosti "1"^^string`, Pouzdanost FMR postavljena je kao `FMRUnutarPodrucjaPouzdanosti "1"^^string`, Pouzdanost FNMR postavljena je kao `FNMRUnutarPodrucjaPouzdanosti "1"^^string`.

```
Osobal: Tehnologija3
    Annotations:
        PN_sg "TE3"
    Types:
        TehnologijaPouzdana,
        A1
    Facts:
     jeDio  BiometrijskiSustav3,
     FNMRUnutarPodrucjaPouzdanosti  "1"^^string,
     PouzdanostSoftveraUnutarPodrucjaPouzdanosti  "96"^^string,
     FTEUnutarPodrucjaPouzdanosti  "1"^^string,
     PouzdanostHardveraUnutarPodrucjaPouzdanosti  "96"^^string,
     FTAUnutarPodrucjaPouzdanosti  "1"^^string,
     FMRUnutarPodrucjaPouzdanosti  "1"^^string
```

Kôd 7.66 Zapis instance "Tehnologija3"

Kôd prikazan u 7.66 opisuje instancu `Tehnologija3` koja ima oznaku `PN_sg "TE2"` te predstavlja aspekt `Tehnologija` instance `BiometrijskiSustav3`. Ova instanca ima sljedeće pretpostavke: Pouzdanost Hardvera postavljena je kao `PouzdanostHardveraUnutarPodrucjaPouzdanosti "96"^^string`, Pouzdanost Softvera postavljena je kao `PouzdanostSoftveraUnutarPodrucjaPouzdanosti "96"^^string`, Pouzdanost FTA postavljena je kao `FTAUnutarPodrucjaPouzdanosti "1"^^string`, Pouzdanost FTE postavljena je kao `FTEUnutarPodrucjaPouzdanosti "1"^^string`, Pouzdanost FMR postavljena je kao `FMRUnutarPodrucjaPouzdanosti "1"^^string`, Pouzdanost FNMR postavljena je kao `FNMRUnutarPodrucjaPouzdanosti "1"^^string`.

```
Osobal: Okolina1
    Annotations:
        PN_sg "OK1"
    Types:
        OkolinaPouzdana,
        B1
    Facts:
     jeDio  BiometrijskiSustav1,
     JacinaBukeUnutarPodrucjaPouzdanosti  "80"^^string,
     TemperaturaUnutarPodrucjaPouzdanosti  "22"^^string,
     JacinaOsvjetljenjaUnutarPodrucjaPouzdanosti  "1600"^^string,
     VlaznostUnutarPodrucjaPouzdanosti  "50"^^string
```

Kôd 7.67 Zapis instance “Okolina1"

Kôd prikazan u 7.67 opisuje instancu `Okolina1` koja ima oznaku `PN_sg "OK1"` te predstavlja aspekt `Okolina` instance `BiometrijskiSustav1`. Ova instanca ima sljedeće pretpostavke: Jačina buke okoline postavljena je kao `JacinaBukeUnutarPodrucjaPouzdanosti "80"^^string`, Temperatura okoline postavljena je kao `TemperaturaUnutarPodrucjaPouzdanosti "22"^^string`, Jačina osvjetljenje okoline postavljena je kao `JacinaOsvjetljenjaUnutarPodrucjaPouzdanosti "1600"^^string`, Vlažnosti okoline postavljena je kao `VlaznostUnutarPodrucjaPouzdanosti "50"^^string`.

```
Osobal: Okolina2
    Annotations:
        PN_sg "OK2"
   Types:
        B3
    Facts:
     jeDio  BiometrijskiSustav2,
     VlaznostIzvanPodrucjaPouzdanosti  "90"^^string,
     TemperaturaUnutarPodrucjaPouzdanosti  "22"^^string,
     JacinaBukeIzvanPodrucjaPouzdanosti  "85"^^string,
     JacinaOsvjetljenjaIzvanPodrucjaPouzdanosti  "2000"^^string
```

Kôd 7.68 Zapis instance “Okolina2"

Kôd prikazan u 7.68 opisuje instancu `Okolina2` koja ima oznaku `PN_sg "OK2"` te predstavlja aspekt `Okolina` instance `BiometrijskiSustav2`. Ova instanca ima sljedeće pretpostavke: Jačina buke okoline postavljena je kao `JacinaBukeIzvanPodrucjaPouzdanosti "85"^^string`, Temperatura okoline postavljena je kao `TemperaturaUnutarPodrucjaPouzdanosti "22"^^string`, Jačina osvjetljenje okoline postavljena je kao `JacinaOsvjetljenjaIzvanPodrucjaPouzdanosti "2000"^^string`, Vlažnosti okoline postavljena je kao `VlaznostIzvanPodrucjaPouzdanosti "90"^^string`.

```
Osobal: Okolina3
    Annotations:
        PN_sg "OK3"
    Types:
        B2
    Facts:
     jeDio  BiometrijskiSustav3,
     JacinaOsvjetljenjaIzvanPodrucjaPouzdanosti  "2000"^^string,
     JacinaBukeIzvanPodrucjaPouzdanosti  "85"^^string,
     VlaznostUnutarPodrucjaPouzdanosti  "50"^^string,
     TemperaturaUnutarPodrucjaPouzdanosti  "22"^^string
```

Kôd 7.69 Zapis instance “Okolina3"

Kôd prikazan u 7.69 opisuje instancu `Okolina3` koja ima oznaku `PN_sg "OK3"` te predstavlja aspekt `Okolina` instance `BiometrijskiSustav3`. Ova instanca ima sljedeće pretpostavke: Jačina buke okoline postavljena je kao `JacinaBukeIzvanPodrucjaPouzdanosti "85"^^string`, Temperatura okoline postavljena je kao `TemperaturaUnutarPodrucjaPouzdanosti "22"^^string`, Jačina osvjetljenje okoline postavljena je kao `JacinaOsvjetljenjaIzvanPodrucjaPouzdanosti "2000"^^string`, Vlažnosti okoline postavljena je kao `VlaznostIzvanPodrucjaPouzdanosti "90"^^string`.

```
Osobal: Korisnik1

    Annotations:
        PN_sg "KO1"
    Types:
        C2
    Facts:
     Interagira  BiometrijskiSustav1,
     KorisnikImaBolest  "2"^^string,
     KorisnikUvjezban  "1"^^string,
     SustavDobroPozicioniran  "1"^^string,
     IzgledKorisnikaPrimjeren  "1"^^string,
     FizickiVanjskiIzgledBezUtjecaja  "1"^^string,
     DimenzijeTijelaNeizrazene  "1"^^string,
     UvjetiKoristenjaNeUtjecu  "1"^^string,
     PrimjerenoPonašanjeKorisnika  "1"^^string,
     ObiljezjaTijelaIzrazena  "2"^^string
```

Kôd 7.70 Zapis instance “BiometrijskiSustav1"

Kôd prikazan u 7.70 opisuje instancu `Korisnik1` koja ima oznaku `PN_sg "KO1"` te predstavlja aspekt `Korisnik` instance `BiometrijskiSustav1`. Ova instanca ima sljedeće pretpostavke: Bolest korisnika postavljena je kao `KorisnikImaBolest "2"^^string`, Uvježbanost korisnika postavljena je kao `KorisnikUvjezban "1"^^string`, Pozicija

biometrijskog sustava postavljena je kao `SustavDobroPozicioniran "1"^^string,` Izgled korisnika postavljen je kao `IzgledKorisnikaPrimjeren "1"^^string,` Fizički vanjski izgled postavljen je kao `FizickiVanjskiIzgledBezUtjecaja "1"^^string, ,` Dimenzije tijela korisnika postavljene su kao `DimenzijeTijelaNeizrazene "1"^^string,` Uvjeti koristenja biometrijskog sustava postavljeni su kao `UvjetiKoristenjaNeUtjecu "1"^^string, ,` Ponašanje korisnika biometrijskog sustava postavljeno je kao `PrimjerenoPonašanjeKorisnika "1"^^string,` Obilježja tijela korisnika postavljena su kao `ObiljezjaTijelaIzrazena "2"^^string,`

```
Osobal: Korisnik2

    Annotations:
        PN_sg "KO2"

    Types:
        C2

    Facts:
     Interagira  BiometrijskiSustav2,
     UvjetiKoristenjaUtjecu  "2"^^string,
     DimenzijeTijelaIzrazene  "2"^^string,
     ObiljezjaTijelaIzrazena  "2"^^string,
     IzgledKorisnikaPrimjeren  "1"^^string,
     FizickiVanjskiIzgledBezUtjecaja  "1"^^string,
     NeprimjerenoPonasanjeKorisnika  "2"^^string,
     SustavDobroPozicioniran  "1"^^string,
     KorisnikUvjezban  "1"^^string,
     KorisnikImaBolest  "2"^^string
```

Kôd 7.71 Zapis instance “BiometrijskiSustav1"

Kôd prikazan u 7.71 opisuje instancu `Korisnik2` koja ima oznaku `PN_sg "KO2"` te predstavlja aspekt `Korisnik` instance `BiometrijskiSustav2.` Ova instanca ima sljedeće pretpostavke: Bolest korisnika postavljena je kao `KorisnikImaBolest "2"^^string,` Uvježbanost korisnika postavljena je kao `KorisnikUvjezban "1"^^string,` Pozicija biometrijskog sustava postavljena je kao `SustavDobroPozicioniran "1"^^string,`

Izgled korisnika postavljen je kao IzgledKorisnikaPrimjeren "1"^^string, Fizički vanjski izgled postavljen je kao FizickiVanjskiIzgledBezUtjecaja "1"^^string, , Dimenzije tijela korisnika postavljene su kao DimenzijeTijelaIzrazene "2"^^string, Uvjeti koristenja biometrijskog sustava postavljeni su kao UvjetiKoristenjaUtjecu "2"^^string, , Ponašenje korisnika biometrijskog sustava postavljeno je kao NeprimjerenoPonasanjeKorisnika "2"^^string, Obilježja tijela korisnika postavljena su kao ObiljezjaTijelaIzrazena "2"^^string,

```
Osobal: Korisnik3

    Annotations:
        PN_sg "KO3"

    Types:
        C3

    Facts:
     Interagira  BiometrijskiSustav3,
     KorisnikUvjezban  "1"^^string,
     ObiljezjaTijelaIzrazena  "3"^^string,
     DimenzijeTijelaNeizrazene  "1"^^string,
     UvjetiKoristenjaNeUtjecu  "1"^^string,
     FizickiVanjskiIzgledBezUtjecaja  "1"^^string,
     NeprimjerenoPonasanjeKorisnika  "3"^^string,
     IzgledKorisnikaPrimjeren  "1"^^string,
     SustavDobroPozicioniran  "1"^^string,
     KorisnikImaBolest  "3"^^string
```

Kôd 7.72 Zapis instance “BiometrijskiSustav1"

Kôd prikazan u 7.72 opisuje instancu Korisnik3 koja ima oznaku PN_sg "KO3" te predstavlja aspekt Korisnik instance BiometrijskiSustav3. Ova instanca ima sljedeće pretpostavke: Bolest korisnika postavljena je kao KorisnikImaBolest "3"^^string, Uvježbanost korisnika postavljena je kao KorisnikUvjezban "1"^^string, Pozicija biometrijskog sustava postavljena je kao SustavDobroPozicioniran "1"^^string,

Izgled korisnika postavljen je kao `IzgledKorisnikaPrimjeren "1"^^string`, Fizički vanjski izgled postavljen je kao `FizickiVanjskiIzgledBezUtjecaja "1"^^string`, , Dimenzije tijela korisnika postavljene su kao `DimenzijeTijelaNeizrazene "1"^^string`, Uvjeti koristenja biometrijskog sustava postavljeni su kao `UvjetiKoristenjaNeUtjecu "1"^^string`, , Ponašenje korisnika biometrijskog sustava postavljeno je kao `NeprimjerenoPonasanjeKorisnika "3"^^string`, Obilježja tijela korisnika postavljena su kao `ObiljezjaTijelaIzrazena "3"^^string`,

POGLAVLJE VIII

8 TESTIRANJE FUNKCIONALNOSTI EVALUACIJSKOG MODELA OOEPBS

U prethodnom poglavlju opisana je ontologija modela OOEPBS, sa detaljnim opisom implementacije metode evalucije pouzdanosti biometrijskog sustava. Pobrojani su temeljni koncepti, njihove karakteristike i svojstva, te su kreirane i instance s temeljnim svojstvima (atributima), a koje se javljaju u modelu OOEPBS, te determiniraju evaluacijsku metodu pouzdanosti biometrijskog sustava.

U nastavku rada, u ovom poglavlju, definirati će se formalna pravila za rezoniranje o pouzdanosti biometrijskog sustava sukladno definiranom evaluacijskom modelu. Pravila će se formalizirati kroz jezik SWRL te integrirati u ontologiju, što će u konačnici predstavljati evaluacijski okvir uz pomoć kojeg će se moći rezonirati o pouzdanosti biometrijskog sustava sukladno modelu OOEPBS.

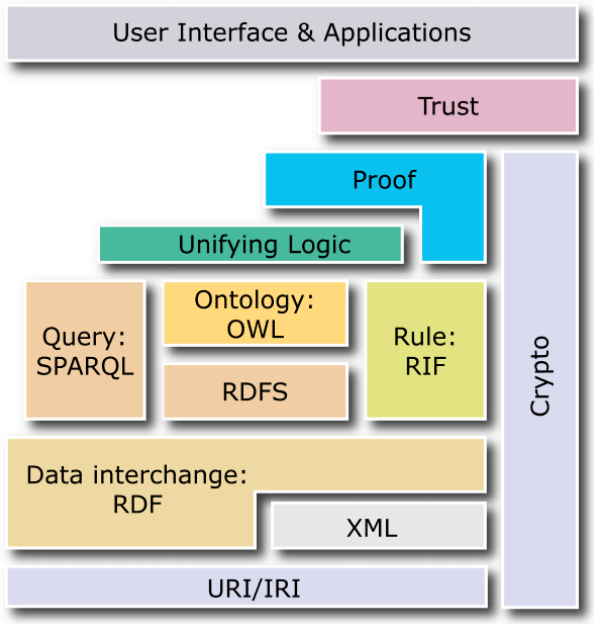
8.1 Semantičko modeliranje pravila za evaluaciju pouzdanosti po modelu OOEPBS uz pomoć jezika SWRL

Pravila za semantički web razvijaju se u okruženju SWRL[95] [117]. Jezik SWRL razvio se iz RuleML jezika koji je prvenstveno namijenjen modeliranju poslovnih pravila za rezoniranje unutar definirane domene. Jezik SWRL objedinjuje grupu XML specijaliziranih jezika za definiranje pravila, koja obuhvaća široki spektar industrijski standardiziranih oblika web pravila [118]. SWRL omogućava višu razinu konceptualizacije te razvoja modela OWL-a zbog izražajnosti koju nudi RuleML [118] u kombinaciji sa OWL-om. SWRL je predstavljen od strane W3C 2004. godine kao jezik koji sadrži punu snagu OWL DL jezika [116], kompleksniju i stratificiranu odlučivost te lakšu implementaciju u praksi. SWRL je osmišljen kao jezik za izražavanje pravila temeljenih na konceptima OWL-a. U svojim pravilima, SWRL omogućava potpuno korištenje koncepata iz OWL-a kako bi osigurao naprednije

[95] Izvorno: *Semantic Web Rule Language*

mogućnosti zaključivanja od onih koje ima sam OWL. SWRL također je semantički strukturiran korištenjem deskriptivne logike (Izvorno: *Description Logic,DL*), iste osnove kakvu ima OWL DL [108]. Iz navedenog može se zaključiti da je osnovna namjena SWRL-a postavljanje poslovnih pravila u cilju zaključivanja odnosno donošenja određenih zaključaka na osnovu ranije formaliziranih pravila [119].

Na slici 53 prikazan je dijagram konfiguracije semantičkog web-a u obliku «layer cake» [120] kako je prezentiran na www.w3.org/2007/03/layerCake.png.

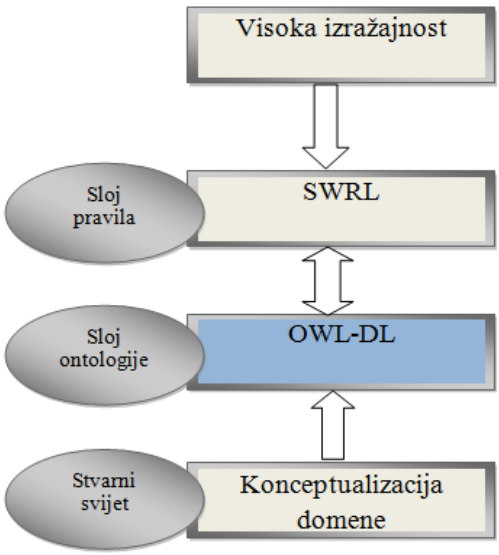


Slika 53 Posljednja inačica W3C Sematic Web "Layer Cake" [96][120]

Na početku projekta semantičkog web-a , W3C je definirao stog tehnologije prikazan naslici 53.Vremenom ste stog mijenjao, evaluirao, a posljednja inačica je prikazana u izvornom obliku na slici br.53. Ova specifikacija je prerasla u 4 glavne grupe jezika: RDF (modeliranje podataka), OWL/RDFS (ontologije), SPARQ (upiti) i SWRL (uloge) . SWRL je postao *de-facto* standard za pravila u semantičkom web-u. Obzirom da kombiniranje OWL-a i SWRL-a ne nudi dovoljno funkcionalnosti definiranih u specifikaciji jezika , upotreba u definiranju poslovnih pravila bi bila nemoguća bez tzv. pogona (Izvorno: „*engine*“) u kojima su integrirane tražene funkcionalnosti [117]. Najpoznatiji su iz obitelji KAON2 (http://kaon2.semanticweb.org/), FaCT++ (http://owl.man.ac.uk/factplusplus/), HermiT

[96] U izvornom obliku (http://www.w3.org/2007/03/layerCake.png)

(http://hermit-reasoner.com/), RacerPro (http://semanticweb.org/wiki/RacerPro) i Pellet (http://clarkparsia.com/pellet/). Za potrebe ovog rada upotrjebljavat će se Pellet reasoner [121]. Slika br.54 strukturni položaj SWRL-a u slojevima ontologije.



Slika 54 Slojevi ontologije

Pravila definirana u SWRL-u sastoje se od dva dijela: premisa (Izvorno: *antecedent*) i zaključak (Izvorno: *consequent*). Premisa predstavlja tijelo SWRL pravila, dok zaključak predstavlja tzv. glavu SWRL pravila [108]. Svako pravilo u svojoj suštini sastoji se od atoma, pa tako i premisa i zaključak, kako slijedi:

$$atom \wedge atom \wedge atom \rightarrow atom \wedge atom$$

$$premisa \rightarrow zakljucak$$

pri čemu se zaključak ispunjava u slučaju kad su svi atomi premise zadovoljeni.

Svaki atom je sljedećeg oblika:

$$p(\arg_1, \arg_2, ... \arg_n)$$

gdje je p simbol predikata iz OWL-a, dok su $(\arg_1, \arg_2, ... \arg_n)$ argumenti tog predikata. Pri tome simbol predikata može predstavljati OWL klasu, svojstvo ili tip podatka. Argumenti mogu biti OWL osobe, podatkovne vrijednosti ili varijable koje se na njih odnose [116].

U nastavku je dan kôd u kom je prikazano korištenje atoma za prikaz jedne OWL osobe iz ontologije pouzdanosti biometrijskih sustava.

```
BiometrijskiSustavPouzdan(?x)
```

SWRL 8.1 Varijabla ?x postaje osoba OWL klase "BiometrijskiSustavPouzdan"

BiometrijskiSustavPouzdan je OWL klasa, dok je ?x varijabla koja predstavlja individuu klase *BiometrijskiSustavPouzdan*. Umjesto varijable ?x moguće je umetnuti i konkretnu OWL individuu, a što je prikazano u sljedećem kôdu:

```
BiometrijskiSustavPouzdan(?x,?BS1)
```

SWRL 8.2 pravilo koje definira članstvo individue *BS1* u klasi *BiometrijskiSustavPouzdan*

8.2 Implementcija pravila za evaluaciju po modelu OOEPBS

Da bi evaluacijski model mogao ispuniti svoju svrhu moraju biti ispunjeni sljedeći preduvjeti koji će biti definirani kao pravila u jeziku SWRL a koja će omogućiti rezoniranje o pouzdanosti biometrijskog sustava po modelu OOEPBS:

8.1 Biometrijski sustav je pouzdan ukoliko su aspekti pouzdanosti ocjenjeni kao: Tehnologija Pouzdana, Okolina Pouzdana te Korisnik Pouzdan (vidjeti Tablice 7. i 8.),

8.2 Biometrijski sustav je djelomicno pouzdan ukoliko su aspekti pouzdanosti ocjenjeni kao :Tehnologija Djelomično Pouzdana, Okolina Djelomično Pouzdana te Korisnik Djelomično Pouzdan (vidjeti Tablice 7. i 8.),

8.3 Biometrijski sustav je nepouzdan ukoliko su aspekti pouzdanosti ocjenjeni kao: Tehnologija Nepouzdana, Okolina Nepouzdana te Korisnik Nepouzdan (vidjeti Tablice 7. i 8.),

8.4 Tehnologija biometrijskog sustava je pouzdana ukoliko ima parametre pouzdanosti : Pouzdanost Softvera Unutar područja pouzdanosti, Pouzdanost Hardvera Unutar područja pouzdanosti te Pouzdanost Statistika (FTA,FTE,FMR,FNMR) Unutar područja pouzdanosti (vidjeti Tablicu 4.),

8.5 Tehnologija biometrijskog sustava je djelomicno pouzdana ukoliko ima parametre pouzdanosti : Pouzdanost Softvera Unutar izvan područja pouzdanosti, Pouzdanost Hardvera izvan područja pouzdanosti te Pouzdanost Statistika (FTA,FTE,FMR,FNMR) izvan područja pouzdanosti (vidjeti Tablicu 4.),

8.6 Tehnologija biometrijskog sustava je nepouzdana ukoliko ima parametre pouzdanosti : Pouzdanost Softvera Unutar izvan područja pouzdanosti, Pouzdanost Hardvera izvan područja pouzdanosti te Pouzdanost Statistika (FTA,FTE,FMR,FNMR) izvan područja pouzdanosti (vidjeti Tablicu 4.),

8.7 SvojstvoOkolineBiometrijskogSustava je pouzdana ukoliko ima ima parametre pouzdanosti: Temperatura unutar područja pouzdanosti, Vlažnost unutar područja pouzdanosti, Buka unutar područja pouzdanosti, Osvjetljenje unutar područja pouzdanosti (vidjeti Tablicu 5.),

8.8 SvojstvoOkolineBiometrijskogSustava je djelomicno pouzdana ukoliko ima parametre pouzdanosti: Temperatura ispod područja pouzdanosti, Vlažnost ispod područja pouzdanosti, Buka ispod područja pouzdanosti, Osvjetljenje ispod područja pouzdanosti (vidjeti Tablicu 5.),

8.9 SvojstvoOkolineBiometrijskogSustava je nepouzdana ukoliko ima parametre pouzdanosti: Temperatura iznad područja pouzdanosti, Vlažnost iznad područja pouzdanosti, Buka iznad područja pouzdanosti, Osvjetljenje iznad područja pouzdanosti (vidjeti Tablicu 5.),

8.10 Korisnik biometrijskog sustava je pouzdan ukoliko ima parametre pouzdanosti: Ponašanje Korisnika sa malim utjecajem, Vanjski Fizički Izgled Korisnika sa malim utjecajem, Bolest Korisnika sa malim utjecajem, Izgled Korisnika sa malim utjecajem, Obilježja Korisnika sa malim utjecajem, Dimenzije Korisnika sa malim utjecajem, Pozicija Sustava sa malim utjecajem na korisnika, Uvjeti Korištenja sa malim utjecajem na korisnika. (vidjeti Tablicu 6.),

8.11 Korisnik biometrijskog sustava je djelomicno pouzdan ukoliko ima parametre pouzdanosti: Ponašanje Korisnika sa srednjim utjecajem, Vanjski Fizički Izgled Korisnika sa srednjim utjecajem, Bolest Korisnika sa srednjim utjecajem, Izgled Korisnika sa srednjim utjecajem, Obilježja Korisnika sa srednjim utjecajem, Dimenzije Korisnika sa srednjim utjecajem, Pozicija Sustava sa srednjim utjecajem na korisnika, Uvjeti Korištenja sa srednjim utjecajem na korisnika. (vidjeti Tablicu 6.),

8.12 Korisnik biometrijskog sustava je nepouzdan ukoliko ima parametre pouzdanosti: Ponašanje Korisnika sa velikim utjecajem, Vanjski Fizički Izgled Korisnika sa velikim utjecajem, Bolest Korisnika sa velikim utjecajem, Izgled Korisnika sa velikim utjecajem,

Obilježja Korisnika sa velikim utjecajem, Dimenzije Korisnika sa velikim utjecajem, Pozicija Sustava sa velikim utjecajem na korisnika, Uvjeti Korištenja sa velikim utjecajem na korisnika. (vidjeti Tablicu 6.).

Navedeni uvjeti mogu se formalizirati u jeziku SWRL kako slijedi:

Definicija 8.1 *Biometrijski sustav je pouzdan ukoliko su aspekti pouzdanosti ocjenjeni kao: Tehnologija Pouzdana, Okolina Pouzdana te Korisnik Pouzdan (vidjeti Tablice 7. i 8.).*

$$\text{BIOMETRIJSKISUSTAVPOUZDAN} \equiv \text{BIOMETRIJSKISUSTAV} \sqcap$$

$$\exists\text{TEHNOLOGIJAPOUZDANA} \sqcap \exists\text{OKOLINAPOUZDANA} \sqcap \exists\text{OKORISNIKPOUZDAN}$$

```
BiometrijskiSustav(?x),
TehnologijaBiometrijskogSustavaPouzdana(?x,?tp),
OkolinaBiometrijskogSustavaPouzdana(?x,?op),
KorisnikBiometrijskogSustavaPouzdan(?x,?kp),) ->
BiometrijskiSustavPouzdan(?x)
```

SWRL 8.3 pravilo koje definira kada je Biometrijski Sustav Pouzdan

U SWRL pravilu br. 8.3 definirano je sljedeće: Osoba (?x) koja pripada klasi *Biometrijski Sustav*, i koja ima parametar Tehnologija Pouzdana, Okolina Pouzdana te Korisnik Pouzdan, jeste Osoba koja pripada klasi Biometrijski Sustav Pouzdan. Znači Biometrijski Sustav je Pouzdan samo ako su zadovoljeni ovi uvjeti.

Definicija 8.2 *Biometrijski sustav je djelomicno pouzdan ukoliko su aspekti pouzdanosti ocjenjeni kao :Tehnologija Djelomično Pouzdana, Okolina Djelomično Pouzdana te Korisnik Djelomično Pouzdan (vidjeti Tablice 7. i 8.)*

$$\text{BIOMETRIJSKISUSTAVDJELOMICNOPOUZDAN} \equiv \text{BIOMETRIJSKISUSTAV} \sqcap$$

$$\exists\text{TEHNOLOGIJADJELOMICNOPOUZDANA} \sqcap \exists\text{OKOLINADJELOMICNOPOUZDANA} \sqcap$$

$$\exists\text{OKORISNIKDJELOMICNOPOUZDAN}$$

```
BiometrijskiSustav(?x),
TehnologijaBiometrijskogSustavaDjelomicnoPouzdana(?x,?td),
OkolinaBiometrijskogSustavaDjelomicnoPouzdana(?x,?od),
KorisnikkBiometrijskogSustavaDjelomicnoPouzdan  (?x,?kd),) ->
BiometrijskiSustavDjelomicnoPouzdan(?x)
```

SWRL 8.4 pravilo koje definira kada je Biometrijski Sustav Djelomično Pouzdan

U SWRL pravilu br. 8.4 definirano je sljedeće: Osoba (?x) koja pripada klasi *Biometrijski Sustav*, i koja ima parametar Tehnologija Djelomično Pouzdana, Okolina Djelomično Pouzdana te Korisnik Djelomično Pouzdan, jeste Osoba koja pripada klasi Biometrijski Sustav Djelomično Pouzdan. Znači Biometrijski Sustav je Djelomično Pouzdan samo ako su zadovoljeni ovi uvjeti.

Definicija 8.3 *Biometrijski sustav je nepouzdan ukoliko su aspekti pouzdanosti ocjenjeni kao: Tehnologija Nepouzdana, Okolina Nepouzdana te Korisnik Nepouzdan (vidjeti Tablice 7. i 8.)*

$$\text{BIOMETRIJSKISUSTAVNEPOUZDAN} \equiv \text{BIOMETRIJSKISUSTAV} \sqcap \exists\text{TEHNOLOGIJANEPOUZDANA} \sqcap \exists\text{OKOLINANEPOUZDANA} \sqcap \exists\text{OKORISNIKNEPOUZDAN}$$

```
BiometrijskiSustav(?x),
TehnologijaBiometrijskogSustavaNepouzdana(?x,?tn),
OkolinaBiometrijskogSustavaNepouzdana (?x,?on),
KorisnikBiometrijskogSustavaNepouzdan  (?x,?kn),) ->
BiometrijskiSustavNepouzdan (?x)
```

SWRL 8.5 pravilo koje definira kada je Biometrijski Sustav Nepouzdan

U SWRL pravilu br. 8.5 definirano je sljedeće: Osoba (?x) koja pripada klasi *Biometrijski Sustav*, i koja ima parametar Tehnologija Nepouzdana, Okolina Nepouzdana te Korisnik Nepouzdan, jeste Osoba koja pripada klasi Biometrijski Sustav Nepouzdan. Znači Biometrijski Sustav je Nepouzdan samo ako su zadovoljeni ovi uvjeti.

Definicija 8.4 *Tehnologija biometrijskog sustava je pouzdana ukoliko ima parametre pouzdanosti : Pouzdanost Softvera iznad područja pouzdanosti, Pouzdanost Hardvera iznad*

područja pouzdanosti te Pouzdanost Statistika (FTA,FTE,FMR,FNMR) iznad područja pouzdanosti.

$$\text{TEHNOLOGIJAPOUZDANA} \equiv \text{TEHNOLOGIJA} \sqcap$$

$$\exists \text{SOFTVERIZNADPODRUCJAPOUZDANOSTI} \sqcap$$

$$\exists \text{HARDVERIZNADPODRUCJAPOUZDANOSTI} \sqcap$$

$$\exists \text{PERFORMANSEIZNADPODRUCJAPOUZDANOSTI}$$

```
PouzdanostTehnologijeBiometrijskogSustava(?x),
PerformanseIznadPodrucjaPouzdanosti(?x, ?pp),
PouzdanostHardveraIznadPodrucjaPouzdanosti(?x, ?hp),
PouzdanostSoftveraIznadPodrucjaPouzdanosti(?x, ?sp) ->
TehnologijaPouzdana(?x)
```

SWRL 8.6 pravilo koje definira kada je Tehnologija Pouzdana

```
PouzdanostTehnologijeBiometrijskogSustava(?x),
TehnologijaPouzdana(?x) -> A1(?x)
```

SWRL 8.6a SWRL pravilo koje dodjeljuje parameter A1 kada je Tehnologija Pouzdana

SWRL pravilom br. 8.6 i 8.6a definirano je sljedeće: Osoba (?x) koja pripada klasi *PouzdanostTehnologijeBiometrijskogSustava*, i koja ima parametar HardverIznadPodrucjaPouzdanosti, SoftverIznadPodrucjaPouzdanosti te PerformanseIznadPodrucjaPouzdanosti, jeste Osoba koja pripada klasi TehnologijaPouzdana. Znači Tehnologija Biometrijskog Sustava je pouzdana samo ako su zadovoljeni ovi uvjeti te joj se dodjeljuje oznaka evaluacijskog parametra *A1*.

Definicija 8.5 *Tehnologija biometrijskog sustava je djelomicno pouzdana ukoliko ima parametre pouzdanosti : Pouzdanost Softvera unutar područja pouzdanosti, Pouzdanost Hardvera unutar područja pouzdanosti te Pouzdanost Statistika (FTA,FTE,FMR,FNMR) unutar područja pouzdanosti*

$$\text{TEHNOLOGIJADJELOMICNOPOUZDANA} \equiv \text{TEHNOLOGIJA} \sqcap$$
$$\exists \text{SOFTVERUNUTARPODRUCJAPOUZDANOSTI} \sqcap$$
$$\exists \text{HARDVERUNUTARPODRUCJAPOUZDANOSTI} \sqcap$$
$$\exists \text{PERFORMANSEUNUTARPODRUCJAPOUZDANOSTI}$$

```
PouzdanostTehnologijeBiometrijskogSustava(?x),
PerformanseUnutarPodrucjaPouzdanosti(?x, ?pn),
PouzdanostHardveraUnutarPodrucjaPouzdanosti(?x, ?hp),
PouzdanostSoftveraUnutarPodrucjaPouzdanosti(?x, ?sp) ->
TehnologijaDjelomicnoPouzdana(?x)
```

SWRL 8.7 pravilo koje definira kada je Tehnologija Djelomicno Pouzdana

```
PouzdanostTehnologijeBiometrijskogSustava(?x),
TehnologijaDjelomicnoPouzdana(?x) -> A2(?x)
```

SWRL 8.7a pravilo koje dodjeljuje parameter A2 kada je Tehnologija Djelomicno Pouzdana

SWRL pravilom br. 8.7 i 8.7a definirano je sljedeće: Osoba (?x) koja pripada klasi *PouzdanostTehnologijeBiometrijskogSustava*, i koja ima parametar HardverUnutarPodrucjaPouzdanosti, SoftverUnutarPodrucjaPouzdanosti te PerformanseUnutarPodrucjaPouzdanosti, jeste Osoba koja pripada klasi TehnologijaDjelomicnoPouzdana. Znači Tehnologija Biometrijskog Sustava je djelomično pouzdana samo ako su zadovoljeni ovi uvjeti te joj se dodjeljuje oznaka evaluacijskog parametra *A2*.

Definicija 8.6 *Tehnologija biometrijskog sustava je nepouzdana ukoliko ima parametre pouzdanosti : Pouzdanost Softvera Unutar ispod područja pouzdanosti, Pouzdanost Hardvera ispod područja pouzdanosti te Pouzdanost Statistika (FTA,FTE,FMR,FNMR) ispod područja pouzdanosti.*

$$\text{TEHNOLOGIJANEPOUZDANA} \equiv \text{TEHNOLOGIJA} \sqcap$$
$$\exists \text{SOFTVERISPODPODRUCJAPOUZDANOSTI} \sqcap$$
$$\exists \text{HARDVERISPODPODRUCJAPOUZDANOSTI} \sqcap$$
$$\exists \text{PERFORMANSEISPODPODRUCJAPOUZDANOSTI}$$

```
PouzdanostTehnologijeBiometrijskogSustava(?x),
PerformanseIspodPodrucjaPouzdanosti(?x, ?pn),
PouzdanostHardveraIspodPodrucjaPouzdanosti(?x, ?hp),
PouzdanostSoftveraIspodPodrucjaPouzdanosti(?x, ?sp) ->
TehnologijaNepouzdana(?x)
```

SWRL 8.8 pravilo koje definira kada je Tehnologija Nepouzdana

```
PouzdanostTehnologijeBiometrijskogSustava(?x),
TehnologijaNepouzdana(?x) -> A3(?x)
```

SWRL 8.8a pravilo koje dodjeljuje parametar A3 kada je Tehnologija Nepouzdana

SWRL pravilom br. 8.8 i 8.8a definirano je sljedeće: Osoba (?x) koja pripada klasi *PouzdanostTehnologijeBiometrijskogSustava*, i koja ima parametar HardverIspodPodrucjaPouzdanosti, SoftverIspodPodrucjaPouzdanosti te PerformanseIspodPodrucjaPouzdanosti, jeste Osoba koja pripada klasi TehnologijaNepouzdana. Znači Tehnologija Biometrijskog Sustava je nepouzdana samo ako su zadovoljeni ovi uvjeti te joj se dodjeljuje evaluacijski parametar A3.

Definicija 8.7 *SvojstvoOkolineBiometrijskogSustava je pouzdano ukoliko ima ima parametre pouzdanosti: Temperatura unutar područja pouzdanosti, Vlažnost unutar područja pouzdanosti, Buka unutar područja pouzdanosti, Osvjetljenje unutar područja pouzdanosti*

$$\text{OKOLINAPOUZDANA} \equiv \text{OKOLINA} \sqcap$$

$$\exists \text{TEMPERATURAUNUTARPODRUCJAPOUZDANOSTI} \sqcap \exists$$

$$\text{VLAZNOSTUNUTARPODRUCJAPOUZDANOSTI} \sqcap \exists$$

$$\text{BUKAUNUTARPODRUCJAPOUZDANOSTI} \sqcap$$

$$\exists \text{OSVJETLJENJEUNUTARPODRUCJAPOUZDANOSTI}$$

```
SvojstvoOkolineBiometrijskogSustava(?x),
JacinaOsvjetljenjaUnutarPodrucjaPouzdanosti(?x, ?so),
TemperaturaUnutarPodrucjaPouzdanosti(?x, ?st),
JacinaBukeUnutarPodrucjaPouzdanosti(?x,?bu),
VlaznostUnutarPodrucjaPouzdanosti(?x,?vu) -> OkolinaPouzdana(?x)
```

SWRL 8.9 pravilo koje definira kada je Okolina Pouzdana

```
SvojstvoOkolineBiometrijskogSustava(?x), OkolinaPouzdana(?x) ->
B1(?x)
```

SWRL 8.9a pravilo koje dodjeljuje parametar B1 kada je Okolina Pouzdana

SWRL pravilom br. 8.9 i 8.9a definirano je sljedeće: Osoba (?x) koja pripada klasi *SvojstvoOkolineBiometrijskogSustava*, i koja ima parametar JacinaOsvjetljenjaUnutarPodrucjaPouzdanosti, TemperaturaUnutarPodrucjaPouzdanosti, JacinaBukeUnutarPodrucjaPouzdanosti te VlaznostUnutarPodrucjaPouzdanosti, jeste Osoba koja pripada klasi OkolinaPouzdana. Znači SvojstvoOkolineBiometrijskogSustava je pouzdano samo ako su zadovoljeni ovi uvjeti te joj se dodjeljuje evaluacijski parametar *B1*.

Definicija 8.8 *SvojstvoOkolineBiometrijskogSustava je djelomično pouzdano ukoliko ima ima parametre pouzdanosti: Temperatura ispod područja pouzdanosti, Vlažnost ispod područja pouzdanosti, Buka ispod područja pouzdanosti, Osvjetljenje ispod područja pouzdanosti*

$$\text{OKOLINADJELOMICNOPOUZDANA} \equiv \text{OKOLINA} \sqcap \exists \text{TEMPERATURAISPODPODRUCJAPOUZDANOSTI} \sqcap \exists \text{VLAZNOSTISPODPODRUCJAPOUZDANOSTI} \sqcap \exists \text{BUKAISPODPODRUCJAPOUZDANOSTI} \sqcap \exists \text{OSVJETLJENJEISPODPODRUCJAPOUZDANOSTI}$$

```
SvojstvoOkolineBiometrijskogSustava(?x),
JacinaOsvjetljenjaIspodPodrucjaPouzdanosti(?x, ?so),
TemperaturaIspodPodrucjaPouzdanosti(?x, ?st),
JacinaBukeIspodPodrucjaPouzdanosti(?x,?bu),
VlaznostIspodPodrucjaPouzdanosti(?x,?vu) ->
OkolinaDjelomicnoPouzdana(?x)
```

SWRL 8.10 pravilo koje definira kada je Tehnologija Djelomično Pouzdana

```
SvojstvoOkolineBiometrijskogSustava(?x), OkolinaPouzdana(?x) ->
B1(?x)
```

SWRL 8.10a pravilo koje dodjeljuje parametar B2 kada je Okolina Djelomično Pouzdana

SWRL pravilom br. 8.10 i 8.10a definirano je sljedeće: Osoba (?x) koja pripada klasi *SvojstvoOkolineBiometrijskogSustava*, i koja ima parametar JacinaOsvjetljenjaIspodPodrucjaPouzdanosti, TemperaturaIspodPodrucjaPouzdanosti, JacinaBukeIspodPodrucjaPouzdanosti te VlaznostIspodPodrucjaPouzdanosti, jeste Osoba koja pripada klasi OkolinaDjelomicnoPouzdana. Znači SvojstvoOkolineBiometrijskogSustava

je djelomično pouzdano samo ako su zadovoljeni ovi uvjeti te joj se dodjeljuje evaluacijski parametar *B2*.

Definicija 8.9 *SvojstvoOkolineBiometrijskogSustava je nepouzdano ukoliko ima ima parametre pouzdanosti: Temperatura iznad područja pouzdanosti, Vlažnost iznad područja pouzdanosti, Buka iznad područja pouzdanosti, Osvjetljenje iznad područja pouzdanosti*

$$\text{OKOLINANEPOUZDANA} \equiv \text{OKOLINA} \sqcap$$
$$\exists \text{TEMPERATURAIZNADPODRUCJAPOUZDANOSTI} \sqcap \exists$$
$$\text{VLAZNOSTIZNADPODRUCJAPOUZDANOSTI} \sqcap \exists \text{BUKAIZNADPODRUCJAPOUZDANOSTI}$$
$$\sqcap \exists \text{OSVJETLJENJEIZNADPODRUCJAPOUZDANOSTI}$$

```
SvojstvoOkolineBiometrijskogSustava(?x),
JacinaOsvjetljenjaIznadPodrucjaPouzdanosti(?x, ?so),
TemperaturaIznadPodrucjaPouzdanosti(?x, ?st),
JacinaBukeIznadPodrucjaPouzdanosti(?x,?bu),
VlaznostIznadPodrucjaPouzdanosti(?x,?vu) -> OkolinaNepouzdana(?x)
```

SWRL 8.11 pravilo koje definira kada je Okolina Nepouzdana

```
SvojstvoOkolineBiometrijskogSustava(?x), OkolinaPouzdana(?x) ->
B1(?x)
```

SWRL 8.11a pravilo koje dodjeljuje parametar B3 kada je Okolina Nepouzdana

SWRL pravilom br. 8.11 i 8.11a definirano je sljedeće: Osoba (?x) koja pripada klasi *SvojstvoOkolineBiometrijskogSustava*, i koja ima parametar JacinaOsvjetljenjaIznadPodrucjaPouzdanosti, TemperaturaIznadPodrucjaPouzdanosti, JacinaBukeIznadPodrucjaPouzdanosti te VlaznostIznadPodrucjaPouzdanosti, jeste Osoba koja pripada klasi OkolinaNepouzdana. Znači SvojstvoOkolineBiometrijskogSustava je nepouzdano samo ako su zadovoljeni ovi uvjeti te joj se dodjeljuje evaluacijski parametar *B3*.

Definicija 8.10 *Korisnik biometrijskog sustava je pouzdan ukoliko ima parametre pouzdanosti: Ponašanje Korisnika sa malim utjecajem, Vanjski Fizički Izgled Korisnika sa malim utjecajem, Bolest Korisnika sa malim utjecajem, Izgled Korisnika sa malim utjecajem, Obilježja Korisnika sa malim utjecajem, Dimenzije Korisnika sa malim utjecajem, Pozicija Sustava sa malim utjecajem na korisnika, Uvjeti Korištenja sa malim utjecajem na korisnika.*

$$\text{KORISNIKPOUZDAN} \equiv \text{KORISNIK} \sqcap \exists \text{FIZICKIVANJSKIIZGLEDBEZUTJECAJA} \sqcap \exists \text{KORISNIKNEMABOLEST} \sqcap \exists \text{OBILJEZJATIJELANEIZRAZENA} \sqcap \exists \text{PRIMJERENOPONASANJEKORISNIKA} \sqcap \exists \text{UVJETIKORISTENJENEUTJECU} \sqcap \exists \text{IZGLEDBEZUTJECAJA} \sqcap \exists \text{DIMENZIJENEUTJECU} \sqcap \exists \text{SUSTAVDOBROPOZICIONIRAN}$$

```
KarakteristikaKorisnikaBiometrijskogSustava(?x),
FizickiVanjskiIzgledBezUtjecaja(?x, ?fv), KorisnikNemaBolest(?x,
?nb), ObiljezjaTijelaNeizrazena(?x, ?ot),
IzgledKorisnikaNeUtjece(?x,ik), ObiljezjaKorisnikaNeUtjecu(?x,?ok),
DimenzijeKorisnikaNeUtjecu(?x,?dk) PrimjerenoPonašanjeKorisnika(?x,
?pp), UvjetiKoristenjaNeUtjecu(?x, ?uu),
SustavDobroPozicioniran(?x,?dp) -> KorisnikPouzdan(?x)
```

SWRL 8.12 pravilo koje definira kada je Korisnik Pouzdan

```
KarakteristikaKorisnikaBiometrijskogSustava(?x), KorisnikPouzdan(?x)
-> C1(?x)
```

SWRL 8.12a pravilo koje dodjeljuje parametar C1 kada je Korisnik Pouzdan

SWRL pravilom br. 8.12 i 8.12a definirano je sljedeće: Osoba (?x) koja pripada klasi *KarakteristikaKorisnikaBiometrijskogSustava*, i koja ima parametar FizickiVanjskiIzgledBezUtjecaja, KorisnikNemaBolest, ObiljezjaTijelaNeizrazena, IzgledKorisnikaNeUtjece, ObiljezjaKorisnikaNeUtjecu, DimenzijeKorisnikaNeUtjecu PrimjerenoPonašanjeKorisnika, UvjetiKoristenjaNeUtjecu, SustavDobroPozicioniran, znači

da je Korisnik Biometrijskog Sustava pouzdan samo ako su zadovoljeni ovi uvjeti te joj se dodjeljuje evaluacijski parametar C1.

Definicija 8.11 *Korisnik biometrijskog sustava je djelomično pouzdan ukoliko ima parametre pouzdanosti: Ponašanje Korisnika sa srednjim utjecajem, Vanjski Fizički Izgled Korisnika sa srednjim utjecajem, Bolest Korisnika sa srednjim utjecajem, Izgled Korisnika sa srednjim utjecajem, Obilježja Korisnika sa srednjim utjecajem, Dimenzije Korisnika sa srednjim utjecajem, Pozicija Sustava sa srednjim utjecajem na korisnika, Uvjeti Korištenja sa srednjim utjecajem na korisnika.*

$$\text{KORISNIKDJELOMICNOPOUZDAN} \equiv \text{KORISNIK} \sqcap \exists \text{FIZICKIVANJSKIIZGLEDSAUTJECAJEM} \sqcap \exists \text{KORISNIKIMABOLEST} \sqcap \exists \text{OBILJEZJATIJELAIZRAZENA} \sqcap \exists \text{NEPRIMJERENOPONASANJEKORISNIKA} \sqcap \exists \text{UVJETIKORISTENJEUTJECU} \sqcap \exists \text{IZGLEDSAUTJECAJEM} \sqcap \exists \text{DIMENZIJEUTJECU} \sqcap \exists \text{SUSTAVLOSEPOZICIONIRAN}$$

```
KarakteristikaKorisnikaBiometrijskogSustava(?x),
FizickiVanjskiIzgledSaUtjecajem(?x, ?fv), KorisnikImaBolest(?x,
?nb), ObiljezjaTijelaIzrazena(?x, ?ot),
IzgledKorisnikaUtjece(?x,ik), ObiljezjaKorisnikaUtjecu(?x,?ok),
DimenzijeKorisnikaUtjecu(?x,?dk) NeprimjerenoPonašanjeKorisnika(?x,
?np), UvjetiKoristenjaUtjecu(?x, ?uu),
SustavLosePozicioniran(?x,?lp) -> KorisnikDjelomicnoPouzdan(?x)
```

SWRL 8.13 pravilo koje definira kada je Korisnik Djelomično Pouzdan

```
KarakteristikaKorisnikaBiometrijskogSustava(?x),
KorisnikDjelomicnoPouzdan(?x) -> C2(?x)
```

SWRL 8.13a pravilo koje dodjeljuje parametar C2 kada je Korisnik Djelomično Pouzdan

SWRL pravilom br. 8.13 i 8.13a definirano je sljedeće: Osoba (?x) koja pripada klasi *KarakteristikaKorisnikaBiometrijskogSustava*, i koja ima parametar FizickiVanjskiIzgledSaUtjecajem sa srednjim utjecajem, KorisnikImaBolest sa srednjim utjecajem, ObiljezjaTijelaIzrazena sa srednjim utjecajem, IzgledKorisnikaUtjece sa srednjim utjecajem, ObiljezjaKorisnikaUtjecu sa srednjim utjecajem, DimenzijeKorisnikaUtjecu sa srednjim utjecajem, NeprimjerenoPonašanjeKorisnika sa srednjim utjecajem, UvjetiKoristenjaUtjecu sa srednjim utjecajem, SustavLosePozicioniran sa srednjim utjecajem, znači da je Korisnik Biometrijskog Sustava djelomicno pouzdan samo ako su zadovoljeni ovi uvjeti te joj se dodjeljuje evaluacijski parametar *C2*.

Definicija 8.12 *Korisnik biometrijskog sustava je nepouzdan ukoliko ima parametre pouzdanosti: Ponašanje Korisnika sa velikim utjecajem, Vanjski Fizički Izgled Korisnika sa velikim utjecajem, Bolest Korisnika sa velikim utjecajem, Izgled Korisnika sa velikim utjecajem, Obilježja Korisnika sa velikim utjecajem, Dimenzije Korisnika sa velikim utjecajem, Pozicija Sustava sa velikim utjecajem na korisnika, Uvjeti Korištenja sa velikim utjecajem na korisnika.*

$$\text{KORISNIKNEPOUZDAN} \equiv \text{KORISNIK} \sqcap \exists \text{FIZICKIVANJSKIIZGLEDSAUTJECAJEM} \sqcap \exists \text{KORISNIKIMABOLEST} \sqcap \exists \text{OBILJEZJATIJELAIZRAZENA} \sqcap \exists \text{NEPRIMJERENOPONASANJEKORISNIKA} \sqcap \exists \text{UVJETIKORISTENJEUTJECU} \sqcap \exists \text{IZGLEDSAUTJECAJEM} \sqcap \exists \text{DIMENZIJEUTJECU} \sqcap \exists \text{SUSTAVLOSEPOZICIONIRAN}$$

```
KarakteristikaKorisnikaBiometrijskogSustava(?x),
FizickiVanjskiIzgledSaUtjecajem(?x, ?fv), KorisnikImaBolest(?x,
?nb), ObiljezjaTijelaIzrazena(?x, ?ot),
IzgledKorisnikaUtjece(?x,ik), ObiljezjaKorisnikaUtjecu(?x,?ok),
DimenzijeKorisnikaUtjecu(?x,?dk) NeprimjerenoPonašanjeKorisnika(?x,
?np), UvjetiKoristenjaUtjecu(?x, ?uu),
SustavLosePozicioniran(?x,?lp) -> KorisnikNepouzdan(?x)
```

SWRL 8.14 pravilo koje definira kada je Korisnik Nepouzdan

```
KarakteristikaKorisnikaBiometrijskogSustava(?x),
KorisnikNepouzdan(?x) -> C3(?x)
```

SWRL 8.14a pravilo koje dodjeljuje parametar C3 kada je Korisnik Nepouzdan

SWRL pravilom br. 8.14 i 8.14a definirano je sljedeće: Osoba (?x) koja pripada klasi *KarakteristikaKorisnikaBiometrijskogSustava*, i koja ima parametar FizickiVanjskiIzgledSaUtjecajem sa velikim utjecajem, KorisnikImaBolest sa velikim utjecajem, ObiljezjaTijelaIzrazena sa velikim utjecajem, IzgledKorisnikaUtjece sa velikim utjecajem, ObiljezjaKorisnikaUtjecu sa velikim utjecajem, DimenzijeKorisnikaUtjecu sa velikim utjecajem, NeprimjerenoPonašanjeKorisnika sa velikim utjecajem, UvjetiKoristenjaUtjecu sa velikim utjecajem, SustavLosePozicioniran sa velikim utjecajem, znači da je Korisnik Biometrijskog Sustava nepouzdan samo ako su zadovoljeni ovi uvjeti te joj se dodjeljuje evaluacijski parametar *C3*.

Na slici 55. Prikazan je popis pravila modela OOEPBS u SWRL-u.

Slika 55 Popis pravila u SWRL-u

8.2 Testiranje funkcionalnosti evaluacijskog modela

8.2.1 Uvod

Za potrebe testiranja funkcionalnosti prethodno opisanog evaluacijskog modela kreirane su konkretne osobe klasa ontologije OOEPBS sa konkretnim atributima. Poštivana su pravila definirana u jeziku SWRL. Cilj je bio testiranje modela u smislu prepoznavanja razinaa pouzdanosti biometrijskog sustava na temelju unešenih parametara predviđenih evaluacijskim modelom kako je opisano u poglavlju 7.7 temeljem definiranih Instanci modela. Tablice broj 9 i 10 prikazuju interpretaciju osnovnih koncepata i svojstava iz studije slučaja koja opisuje tri biometrijska sustava:

- Biometrijski sustav za prepoznavanje otiska dlana – BS1 kojemu pripadaju
    - Tehnologija 1 –TE1, Okolina 1- OK1, te sa njim interagira Korisnik 1-KO1
- Biometrijski sustav za prepoznavanje otiska prsta – BS2
    - Tehnologija 2 –TE2, Okolina 2- OK2, te sa njim interagira Korisnik 2-KO2
- Biometrijski sustav za prepoznavanje glasa – BS3
    - Tehnologija 3 –TE3, Okolina 3- OK3, te sa njim interagira Korisnik 3-KO3

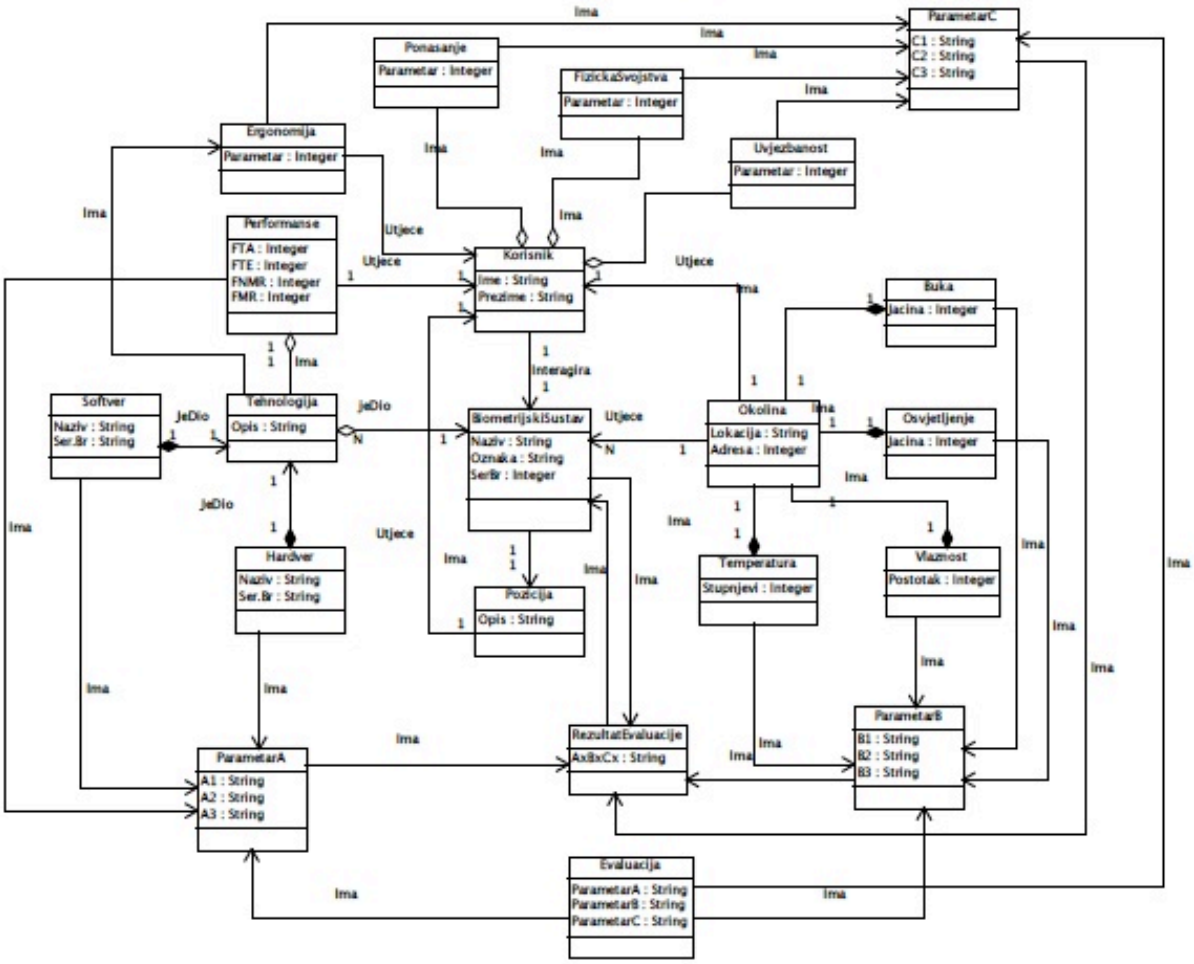
Tablica 9 Interpretacija koncepata iz studije slučaja

Koncept (A)	**Skup u kojeg se koncept preslikava u interpretaciji I (A`)**
BiometrijskiSustav	{Biometrijski_Sustav_za_prepoznavanje_otiska_dlana, Biometrijski_Sustav_za_prepoznavanje_otiska_prsta, Biometrijski_Sustav_za_prepoznavanje_glasa }
Tehnologija	{Softver,Hardver}
Okolina	{Temperatura, Vlažnost, Buka, Osvjetljenje}
Korisnik	{Ponašanje, Fizički_vanjski_Izgled, Bolest, Izgled, Obiljezja_Tijela, Dimenzije_Tijela, Uvjeti_Koristenja, Pozicija_Sustava }
Pouzdanost	{BiometrijskiSustavPouzdan, BiometrijskiSustavDjelomicnoPouzdan, BiometrijskiSustavNepouzdan}

Tablica 10 Interpretacija svojstava iz studije slučaja

Relacija (R)	**Skup u kojeg se relacija preslikava u intepretaciji I (R`)**
Ima	{(BiometrijskiSustav);(Tehnologija);(Okolina);(Korisnik)}{(Tehnologija);(Softver);(Hardver);(Performanse)};{(Okolina);(Temperatura);(Vlaznost);(Buka);(Osvjetljenje)};{(Korisnik);(Ponašajna svojstva);(Fizička Svojstva);(Uvježbanost);(Ergonomija)}
Interagira	{(BiometrijskiSustav);(Korisnik)}
jeDio	{(Softver);(Hardver)}
Utjece	{(BiometrijskiSustav);(Okolina);(Tehnologija)}

Uopćeno UML [122] dijagram klasa sa atributima i relacijama modeliran za DBMS (Izvorno: *Database Management System*) je prikazan kako slijedi na slici 56.:



Slika 56 UML dijagram procesa evaluacije po modelu OOEPBS

Opisani su osnovni koncepti, njihovi osnovni atributi, te relacije između koncepata koji se pojavljuju u procesu evaluacije pouzdanosti biometrijskog sustava.

8.2.2 Implementacija evaluacijske metode

Implementacija evaluacijskog modela realizirana je definiranjem instanci koje su opisane u poglavlju 7.7 a koje predstavlju tri tipologije biometrijskih sustava koji funkcioniraju u predefiniranim uvjetima:

a.) Prvi slučaj predstavlja biometrijski sustav opisan tablicom 11:

Tablica 11 Biometrijski sustav za prepoznavanje otiska dlana

Biometrijski sustav:	Biometrijski sustav za prepoznavanje otiska dlana
Naziv:	BS1
Serijski broj:	SN001435B23456984XXZ
Tip:	N/A
Modalitet:	Prepoznavanje otiska dlana
Namjena:	Verifikacija
Lokacija:	Biometrijski laboratorij

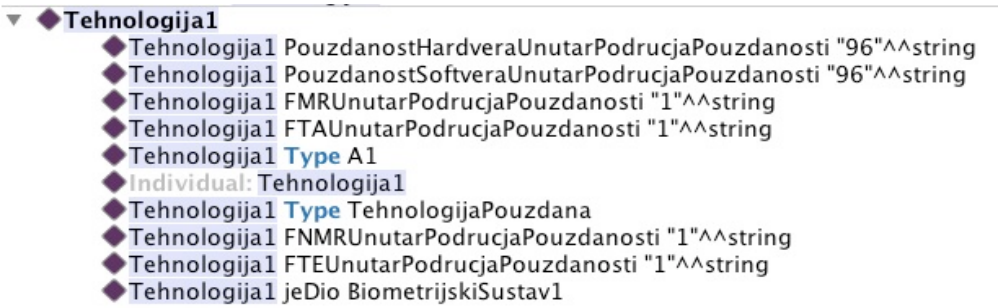
Evaluacijski model:	Parametar	Vrijednost	Područje pouzdanosti	Rezultat	Rezultat grupe	Rezultat modela
Tehnologija: softver	Pouzdanost	96	>95	1		
Tehnologija: hardver	Pouzdanost	96	>95	1		
Tehnologija: Performanse	FMR	1	<2	1		
Tehnologija: Performanse	FNMR	1	<2	1		
Tehnologija: Performanse	FTE	1	<2	1		
Tehnologija: Performanse	FTA	1	<2	1		
GRUPA A				1	A1	
Okolina: Fizička svojstva	Osvjetljenje	1600	1500 do 2000	1		
Okolina: Fizička svojstva	Buka	80	80 do 90	1		
Okolina: Atmosferske prilike	Temperatura	22	10 do 40	1		
Okolina: Atmosferske prilike	Vlažnost	50	40 do 60	1		
GRUPA B				1	B1	
Korisnik:Karakteristike	KU: Ponašajni	1	<2	1		
Korisnik:Karakteristike	KU: Fizički	1	<2	1		
Korisnik:Karakteristike	DU: Izgled	1	<2	1		
Korisnik:Karakteristike	DU: Bolest	2	<2	2		
Korisnik:Osobni činitelji	AN: Obilježja	2	<2	2		
Korisnik:Osobni činitelji	AN: Dimenzije	1	<2	1		
Korisnik:Osobni činitelji	IS: Uvježbanost	1	<2	1		
Korisnik:Osobni činitelji	ER: Uvjeti	1	<2	1		
Korisnik:Osobni činitelji	ER: Pozicija	1	<2	1		
GRUPA C				2	C2	
REZULTAT MODELA						A1B1C2

Implementacija ovoga slučaja realizirana je definiranjem instance Biometrijski Sustav 1 (BS1) kako slijedi:

Na slici 57 prikazana je implementacija Instance BS1.

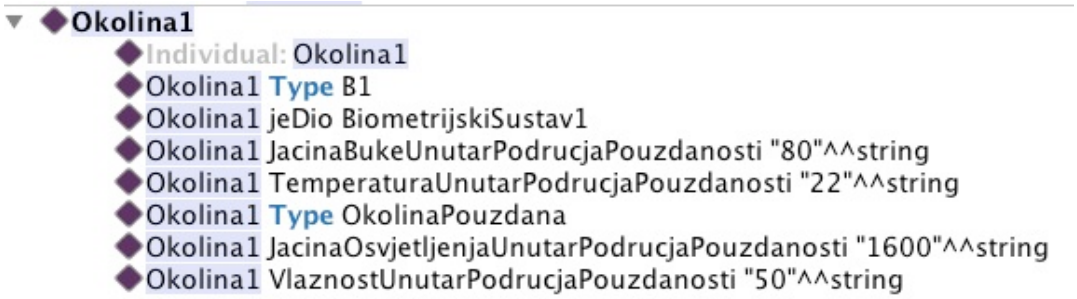
Slika 57 Implementacija instance Biometrijski sustav 1 (BS1)

Slika br.58 prikazuje implementaciju instance Tehnologija 1.



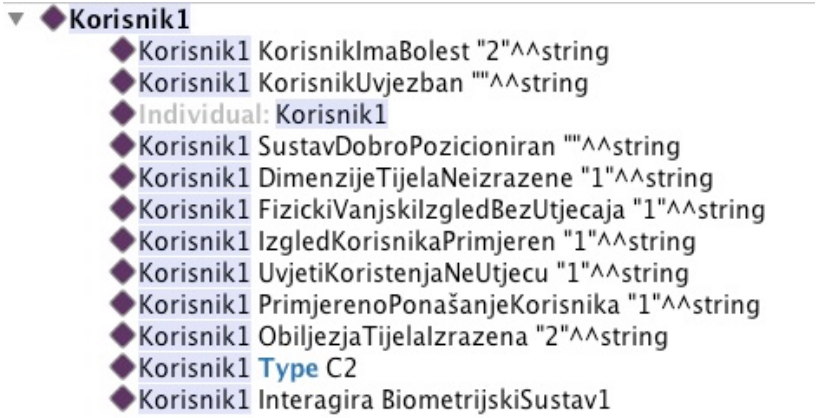
Slika 58 Implementacija instance Tehnologija 1

Slika br.59 prikazuje implementaciju instance Okolina 1.



Slika 59 Implementacija instance Okolina 1

Na slici br. 60 je prikazana implementacija instance Korisnik 1 koji interagira sa Biometrijskim sustavom 1.



Slika 60 Implementacija instance Korisnik 1

Dobivena evaluacijska vrijednost za Biometrijski sustav 1 , nakon evaluacije po modelu OOEPBS jeste *A1B1C2* što znači, sukladno definicijama iz poglavlja 6.4.5. te tablicama 7. i 8. da je ova biometrijski sustav ocjenjen pouzdanim.

b.) Drugi slučaj predstavlja biometrijski sustav opisan tablicom 12:

Tablica 12 Biometrijski sustav za prepoznavanje otiska prsta

Biometrijski sustav:	Biometrijski sustav za prepoznavanje otiska prsta
Naziv:	BS2
Serijski broj:	SN0088764563343 24ZKP
Tip:	N/A
Modalitet:	Prepoznavanje otiska prsta
Namjena:	Verifikacija
Lokacija:	Biometrijski laboratorij

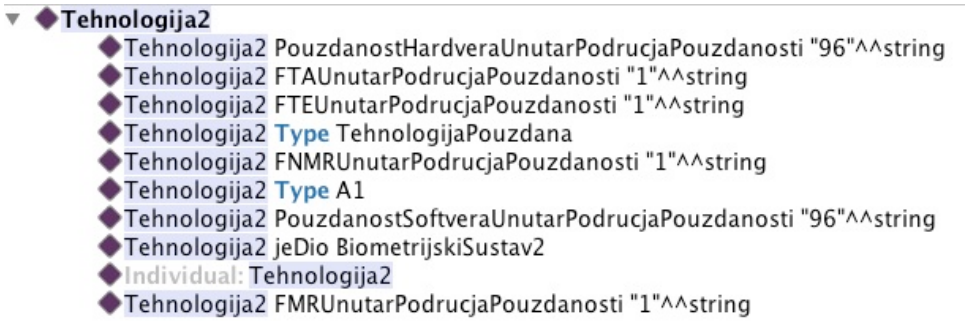
Evaluacijski model:	Parametar	Vrijednost	Područje pouzdanosti	Rezultat	Rezultat grupe	Rezultat modela
Tehnologija: softver	Pouzdanost	96	>95	1		
Tehnologija: hardver	Pouzdanost	96	>95	1		
Tehnologija: Performanse	FMR	1	<2	1		
Tehnologija: Performanse	FNMR	1	<2	1		
Tehnologija: Performanse	FTE	1	<2	1		
Tehnologija: Performanse	FTA	1	<2	1		
GRUPA A				1	A1	
Okolina: Fizička svojstva	Osvjetljenje	2000	1500 do 2000	1		
Okolina: Fizička svojstva	Buka	85	80 do 90	2		
Okolina: Atmosferske prilike	Temperatura	22	10 do 40	1		
Okolina: Atmosferske prilike	Vlažnost	90	40 do 60	3		
GRUPA B				3	B3	
Korisnik:Karakteristike	KU: Ponašajni	2	<2	2		
Korisnik:Karakteristike	KU: Fizički	1	<2	1		
Korisnik:Karakteristike	DU: Izgled	1	<2	1		
Korisnik:Karakteristike	DU: Bolest	2	<2	2		
Korisnik:Osobni činitelji	AN: Obilježja	2	<2	2		
Korisnik:Osobni činitelji	AN: Dimenzije	2	<2	2		
Korisnik:Osobni činitelji	IS: Uvježbanost	1	<2	1		
Korisnik:Osobni činitelji	ER: Uvjeti	2	<2	2		
Korisnik:Osobni činitelji	ER: Pozicija	1	<2	1		
GRUPA C				2	C2	
REZULTAT MODELA						A1B3C2

Implementacija ovoga slučaja realizirana je definiranjem instance Biometrijski Sustav 2 (BS2) kako slijedi:

Na slici 61 prikazana je implementacija Instance BS2.

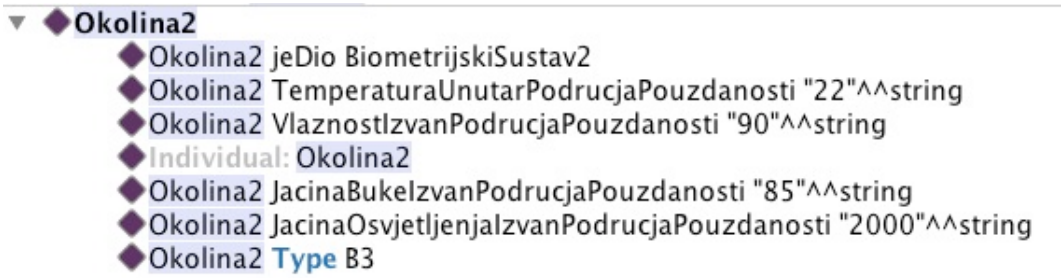
Slika 61 Implementacija instance Biometrijski sustav 2 (BS2)

Slika br.62 prikazuje implementaciju instance Tehnologija 2.



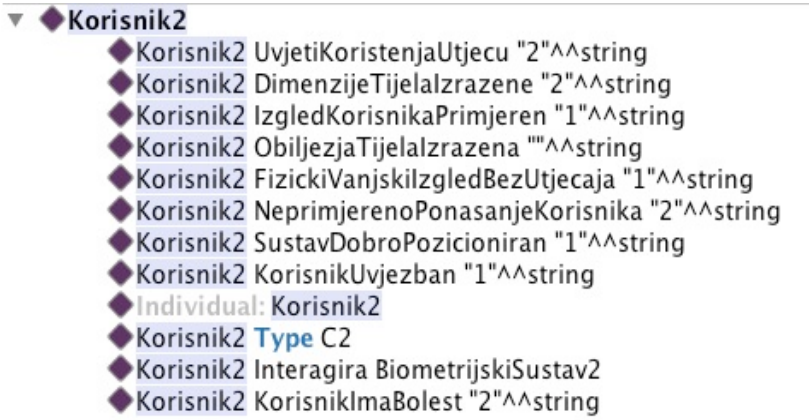
Slika 62 Implementacija instance Tehnologija 2

Slika br.63 prikazuje implementaciju instance Okolina 2.



Slika 63 Implementacija instance Okolina 2

Na slici br. 64 je prikazana implementacija instance Korisnik 2 koji interagira sa Biometrijskim sustavom 2.



Slika 64 Implementacija instance Korisnik 2

Dobivena evaluacijska vrijednost za Biometrijski sustav 2 , nakon evaluacije po modelu OOEPBS jeste *A1B3C2* što znači, sukladno definicijama iz poglavlja 6.4.5. te tablicama 7. i 8. da je ovaj biometrijski sustav ocjenjen djelomično pouzdanim.

c.) Treći slučaj predstavlja biometrijski sustav opisan tablicom 13:

Tablica 13 Biometrijski sustav za prepoznavanje glasa

Biometrijski sustav:	Biometrijski sustav za prepoznavanje glasa
Naziv:	BS3
Serijski broj:	SNXCV5B23456983344KLM
Tip:	N/A
Modalitet:	Prepoznavanje glasa
Namjena:	Verifikacija
Lokacija:	Biometrijski laboratorij

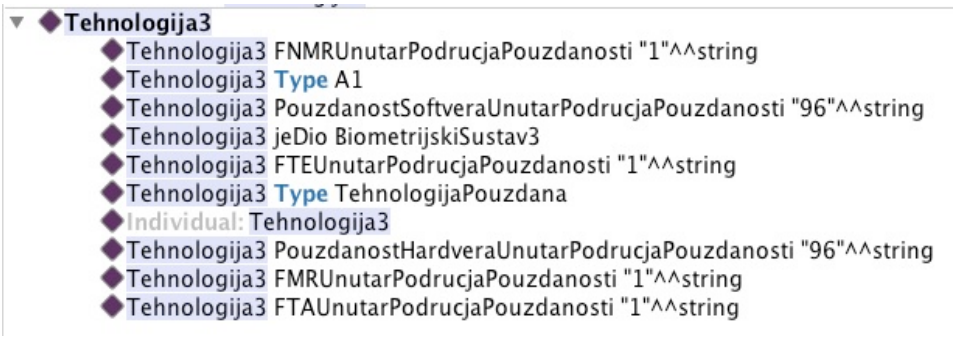
Evaluacijski model:	Parametar	Vrijednost	Područje pouzdanosti	Rezultat	Rezultat grupe	Rezultat modela
Tehnologija: softver	Pouzdanost	96	>95	1		
Tehnologija: hardver	Pouzdanost	96	>95	1		
Tehnologija: Performanse	FMR	1	<2	1		
Tehnologija: Performanse	FNMR	1	<2	1		
Tehnologija: Performanse	FTE	1	<2	1		
Tehnologija: Performanse	FTA	1	<2	1		
GRUPA A				1	A1	
Okolina: Fizička svojstva	Osvjetljenje	2000	1500 do 2000	1		
Okolina: Fizička svojstva	Buka	85	80 do 90	2		
Okolina: Atmosferske prilike	Temperatura	22	10 do 40	1		
Okolina: Atmosferske prilike	Vlažnost	90	40 do 60	1		
GRUPA B				2	B2	
Korisnik:Karakteristike	KU: Ponašajni	3	<2	3		
Korisnik:Karakteristike	KU: Fizički	1	<2	1		
Korisnik:Karakteristike	DU: Izgled	1	<2	1		
Korisnik:Karakteristike	DU: Bolest	3	<2	3		
Korisnik:Osobni činitelji	AN: Obilježja	3	<2	3		
Korisnik:Osobni činitelji	AN: Dimenzije	1	<2	1		
Korisnik:Osobni činitelji	IS: Uvježbanost	1	<2	1		
Korisnik:Osobni činitelji	ER: Uvjeti	1	<2	1		
Korisnik:Osobni činitelji	ER: Pozicija	1	<2	1		
GRUPA C				3	C3	
REZULTAT MODELA						A1B2C3

Implementacija ovoga slučaja realizirana je definiranjem instance Biometrijski Sustav 3 (BS3) kako slijedi:

Na slici 65 prikazana je implementacija Instance BS3.

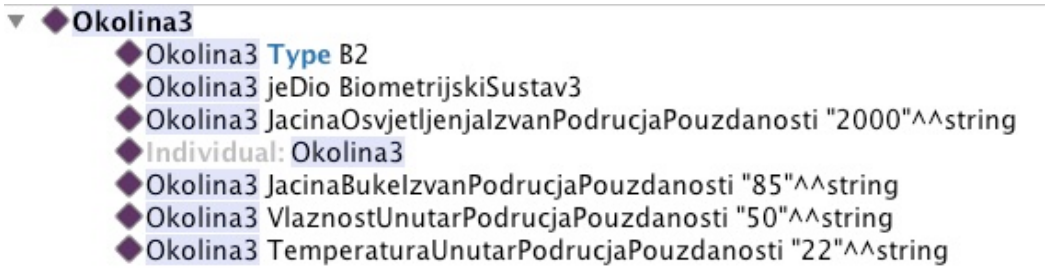
Slika 65 Implementacija instance Biometrijski sustav 3 (BS3)

Slika br.66 prikazuje implementaciju instance Tehnologija 3.



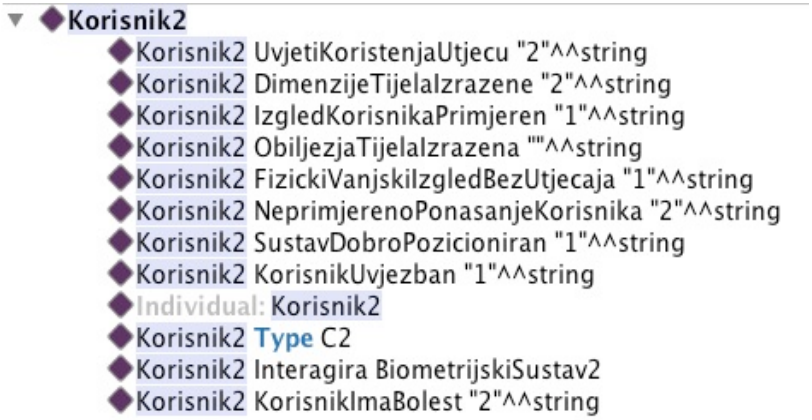
Slika 66 Implementacija instance Tehnologija 3

Slika br.67 prikazuje implementaciju instance Okolina 3.



Slika 67 Implementacija instance Okolina 3

Na slici br. 68 je prikazana implementacija instance Korisnik 3 koji interagira sa Biometrijskim sustavom 3.

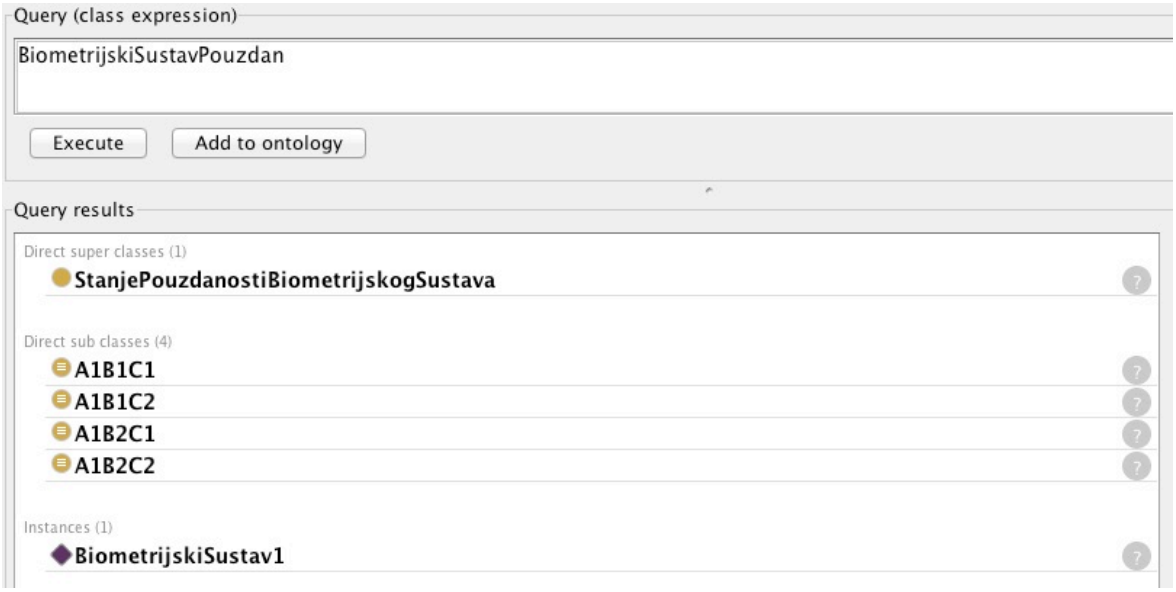


Slika 68 Implementacija instance Korisnik 3

Dobivena evaluacijska vrijednost za Biometrijski sustav 3 , nakon evaluacije po modelu OOEPBS jeste *A1B2C3* što znači, sukladno definicijama iz poglavlja 6.4.5. te tablicama 7. i 8. da je ovaj biometrijski sustav ocjenjen nepouzdanim.

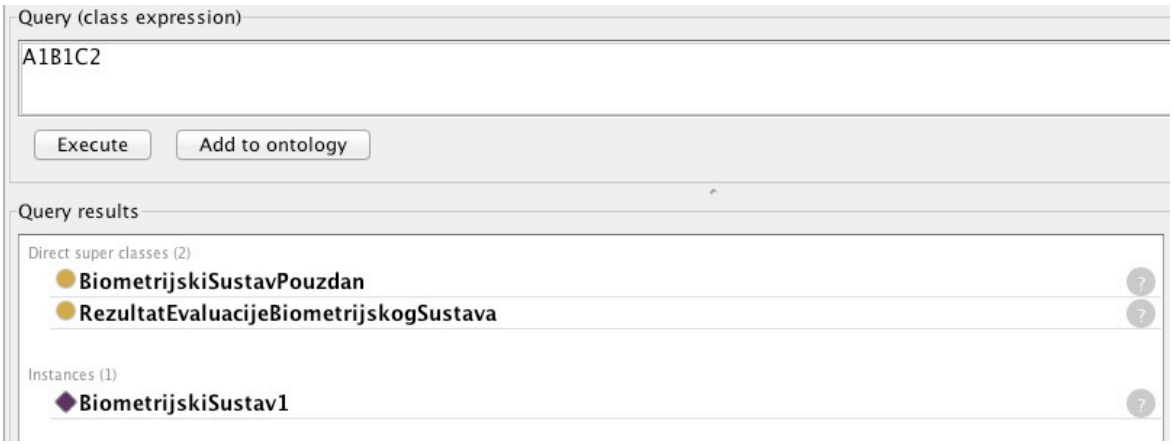
8.2.3 Testiranje evaluacijskog okvira

Testiranje funkcionalnosti evaluacijskog okvira vrši se putem dodatka DL query softvera Protege'. Obzirom da je osoba *BiometrijskiSustav* koncipirana tako da ima sve atribute koji omogućuju rezoniranje o pouzdanosti, kada smo pokrenuli upit u „DL query TAB“, ***BiometrijskiSustavPouzdan***, alata Protege', Pellet reasoner je kao rezultat dao ***BiometrijskiSustav1*** kao što je prikazano na slici 69.



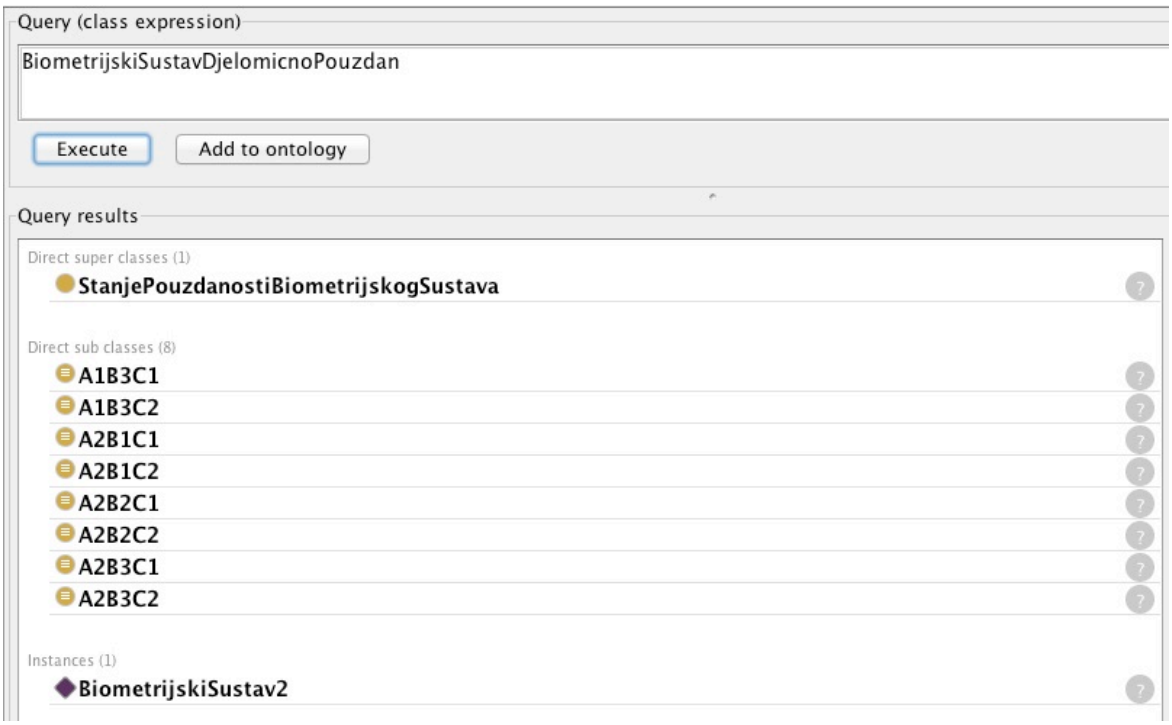
Slika 69 DL upit koji daje odgovor na pitanje koji je BiometrijskiSustavPouzdan

Također postavljajući kao upit dobivenu evaluacijsku vrijednost «***A1B1C2***» dobiva se sljedeći rezultat kao na slici 70.:



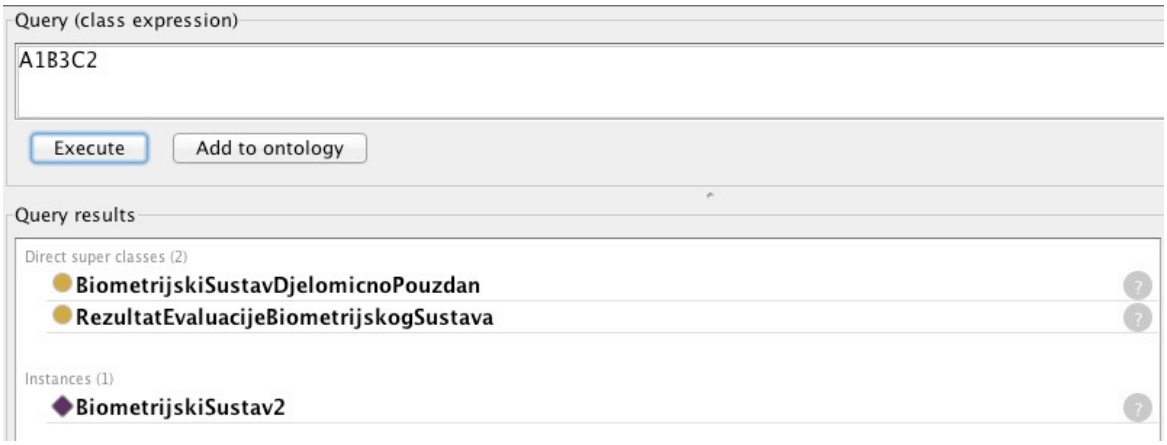
Slika 70 DL upit koji daje odgovor na pitanje značenja evaluacijske vrijednosti A1B1C2

Nadalje postavljajući upit ***BiometrijskiSustavDjelomicnoPouzdan***, Pellet reasoner je kao rezultat dao ***BiometrijskiSustav2*** kao što je prikazano na slici 71.



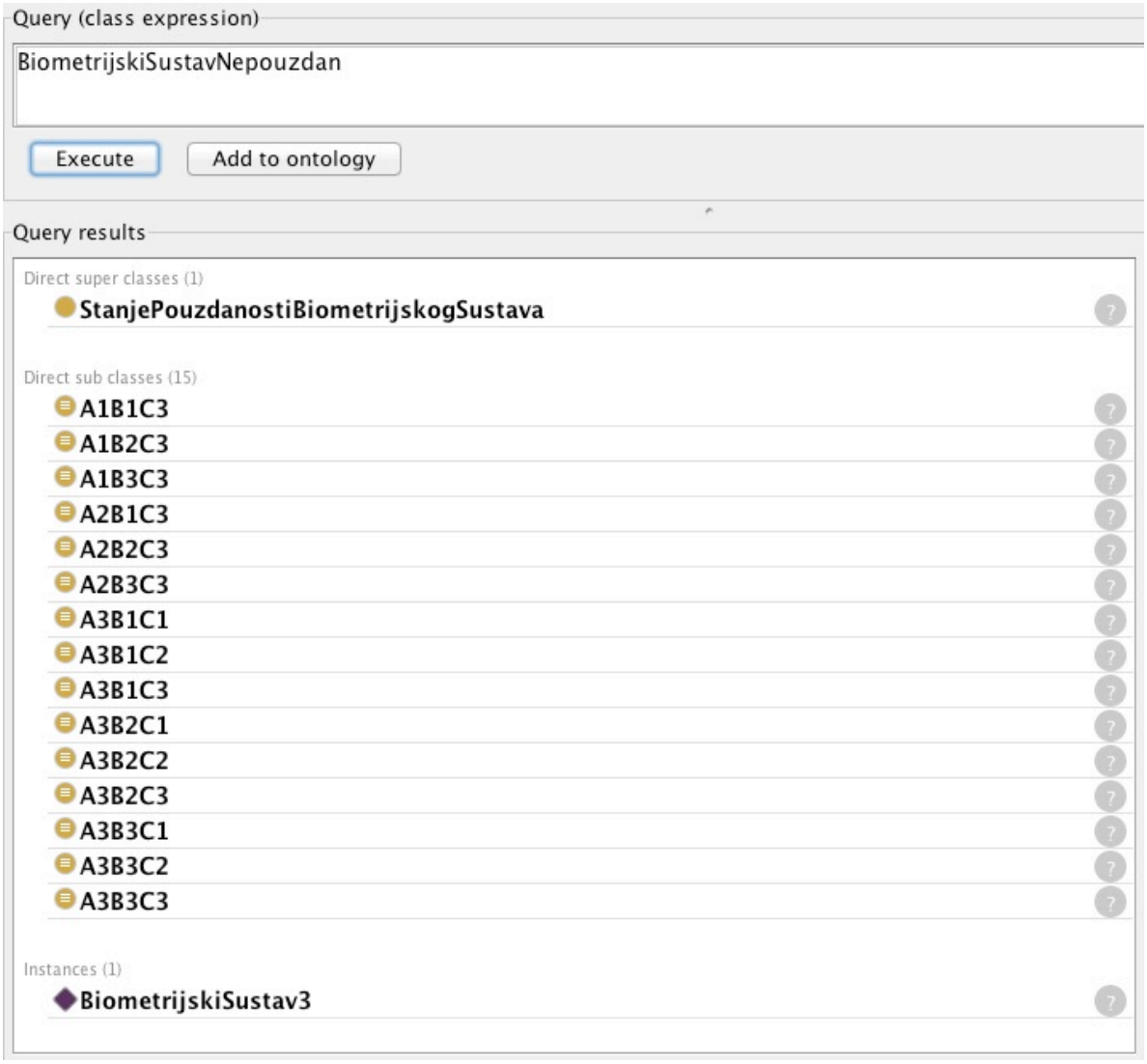
Slika 71 DL upit koji daje odgovor na pitanje koji je BiometrijskiSustavDjelomicnoPouzdan

Također postavljajući kao upit dobivenu evaluacijsku vrijednost «***A1B3C2***» dobiva se sljedeći rezultat kao na slici 72.:



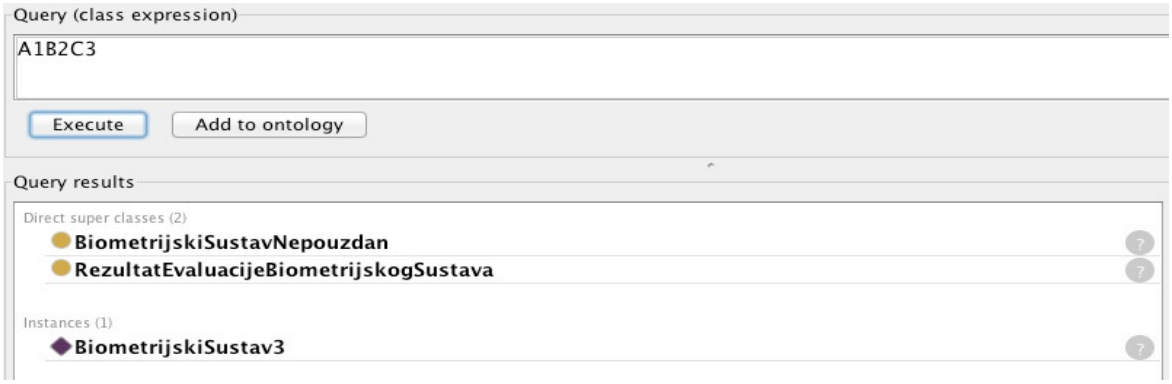
Slika 72 DL upit koji daje odgovor na pitanje značenja evaluacijske vrijednosti A1B3C2

Na kraju postavljajući upit ***BiometrijskiSustavNepouzdan***, Pellet reasoner je kao rezultat dao ***BiometrijskiSustav3*** kao što je prikazano na slici 73.



Slika 73 DL upit koji daje odgovor na pitanje koji je BiometrijskiSustavNepouzdan

Također postavljajući kao upit dobivenu evaluacijsku vrijednost «***A1B2C3***» dobiva se sljedeći rezultat kao na slici 74.:

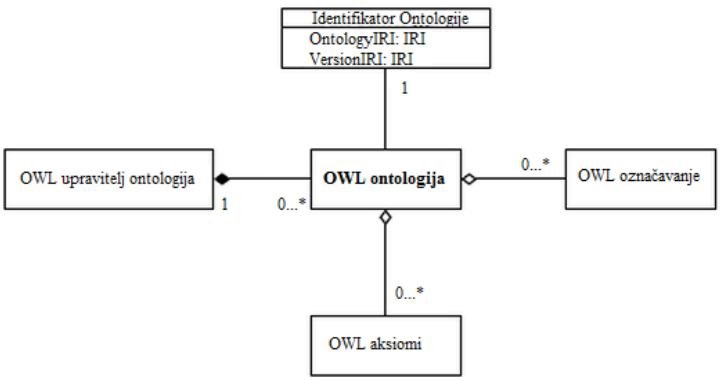


Slika 74 DL upit koji daje odgovor na pitanje značenja evaluacijske vrijednosti A1B3C2

8.3 Mogućnosti ponovnog korištenja evaluacijskog okvira

Evaluacijski okvir definiran kao ontologija predstavlja mogućnost ponovnog korištenje putem stavljanja na raspolaganje istraživačima ili profesionalcima koji se bave sličnim područjem sa mogućnošću inkorporiranja u nove Ontologije. Ontologija formalizirana u OWL-u s pravilima postavljenim u SWRL-u biti će postavljena on-line na neki od javno dostupnih i korištenih repozitorija ontologija. Evaluacijski okvir će biti moguće uvesti u druge ontologije putem dostupnih alata ili jednostavno putem korištenja URI-a[97] koji identificira i referencira domensku ontologiju. Za navedenu svrhu postoji niz alata razvijenih od strane Akademske zajednice na nekoliko Sveučilišta u svijetu a koji omogućuju razvoj aplikacija u nekom programskom jeziku (npr. Java) koji se oslanjaju na znanje pohranjeno u ontologiji. Jedno od vodećih na polju ontologija je i Sveučilište Stanford, USA. Razvijeno je nekoliko različitih sučelja u formi API[98] [116] i java aplikacija koje omogućavaju izradu aplikacija i manipulaciju ontologijama [123] (pozivanje ontologije, importiranje, dodavanje, brisanja klasa, svojstava, osoba, postavljanje pravila nad istom te rezoniranje na osnovu tih pravila. Neki od njih su OWL API, HP Jena Toolkit, i sl. [124].

Na slici br. 75. je prikazana arhitektura OWL API sučelja, gdje je OWL ontologija u centru repozitorija te na koju se cijela struktura naslanja [120].



Slika 75 Položaj ontologije i upravljanje u OWLAPI [120]

[97] URI (Izvorno: Uniform Resource Identifier) predstavlja set karaktera koji identificiraju neki resurs na web-u

[98] Izvorno: *Application Programming Interface*

U nastavku je dano nekoliko primjera kôda za manipuliranje ontologijama uz pomoć OWL API[99] [116]:

```
OWLOntologyManager m = create();
OWLOntology o =
m.createOntology(http://www.semanticweb.org/zoran/OOEPBS);
assertNotNull(o);
```

Kôd 8.1 Implementacija kreiranja ontologije u Java-i

```
OWLOntologyManager m = create();
OWLOntology                              o                              =
m.loadOntologyFromOntologyDocument(http://www.semanticweb.org/zoran/
OOEPBS);
assertNotNull(o);
StringDocumentTarget target = new StringDocumentTarget();
m.saveOntology(o, target);
m.removeOntology(o);
OWLOntology o2 = m
.loadOntologyFromOntologyDocument(
new StringDocumentSource(target.toString()));
assertNotNull(o2);
```

Kôd 8.2 Učitavanja ontologije iz IRI iz String Source

```
OWLOntologyManager m = OWLManager.createOWLOntologyManager();
// map the ontology IRI to a physical IRI (files for example)
File output = File.createTempFile("OOEPBS", "owl");
IRI documentIRI = IRI.create(output);
// Set up a mapping, which maps the ontology to the document IRI
SimpleIRIMapper mapper =
new SimpleIRIMapper(example_save_iri, documentIRI);
m.addIRIMapper(mapper);
// set up a mapper to read local copies of ontologies
File localFolder = new File("materializedOntologies");
// the manager will look up an ontology IRI by checking
// localFolder first for a local copy
```

[99] http://stackoverflow.com/questions/17357836/using-swrl-with-jena-and-pellet 22.03.2015 u 21:30

```
m.addIRIMapper(new AutoIRIMapper(localFolder, true));
// Now create the ontology using the ontology IRI (not the
physical URI)
OWLOntology o = m.createOntology(example_save_iri);
// save the ontology to its physical location - documentIRI
m.saveOntology(o);
```

Kôd 8.3 Učitavanja ontologije iz IRI uz pomoć IRIMAPPER

```
OWLOntologyManager m = create();
OWLOntology o =
m.createOntology(http://www.semanticweb.org/zoran/OOEPBS);
// class A and class B
OWLClass clsA = df.getOWLClass(IRI.create(OOEPBS + "#A"));
OWLClass clsB = df.getOWLClass(IRI.create(OOEPBS + "#B"));
// Now create the axiom
OWLAxiom axiom = df.getOWLSubClassOfAxiom(clsA, clsB);
// add the axiom to the ontology.
AddAxiom addAxiom = new AddAxiom(o, axiom);
// We now use the manager to apply the change
m.applyChange(addAxiom);
// remove the axiom from the ontology
RemoveAxiom removeAxiom = new RemoveAxiom(o,axiom);
m.applyChange(removeAxiom);
```

Kôd 8.4 Dodavanje aksioma u učitanu Ontologiju

```
OWLOntologyManager m = create();
OWLOntology o = m.createOntology(example_iri);
// Get hold of references to class A and class B.
OWLClass clsA = df.getOWLClass(
IRI.create(example_iri + "#A"));
OWLClass clsB = df.getOWLClass(
IRI.create(example_iri + "#B"));
SWRLVariable var = df.getSWRLVariable(
IRI.create(example_iri + "#x"));
SWRLClassAtom body = df.getSWRLClassAtom(clsA, var);
SWRLClassAtom head = df.getSWRLClassAtom(clsB, var);
```

```
SWRLRule rule = df.getSWRLRule(Collections.singleton(body),
Collections.singleton(head));
m.applyChange(new AddAxiom(o, rule));
```

Kôd 8.5 Dodavanje SWRL pravila u učitanu Ontologiju

Na ovaj način je moguće kreirati učinkovite aplikacije u java ili nekom drugom programskom jeziku, a koje će se oslanjati na izrađenu ontologiju te znanje pohranjeno u istoj.

8.4 Ograničenja evaluacijskog okvira

Ograničenje okvira proizlazi iz činjenice da ,sukladno iznešenome u poglavlju 5.2, ne postoji općenito prihvaćena evaluacijska metoda pouzdanosti biometrijskih sustava koja će omogućiti evaluaciju aspekata pouzdanosti biometrijskih sustava prije njihova stavljanja u operativnu funkciju te usporedbe sa podacima tijekom operativne uporabe.

Nije dostupna općeprihvaćena metodologija ocjene međusobnog utjecaja pojedinih aspekata pouzdanosti te refleksije na određene kontekste primjene u domeni interakcije sa korisnikom te ispunjavanja svrhe vlasnika biometrijskog sustava.

Također ne postoji znanstveno utemeljena analiza usmjerena na proučavanje zakonitosti distribucije pojedinih biometrijskih karakteristika koja ukazuje na parametre jedinstvenosti te eventualnih anomalija.

Model OOEPBS obuhvaća aspekte Tehnologije, Okoline te Korisnika biometrijskog sustava a unutar istih postoji mogućnost proširenja sa činiteljima koji nisu obuhvaćeni ovim evaluacijskim modelom. Model OOEPBS stvara pretpostavku za daljnju nadogradnju te razmjenu iskustava iz znanstvenih istraživanja i prakse.

Utjecaj raširene uporabe biometrijskih sustava u domeni omogućavanja ili negiranja pristupa određenim pravima osoba zadire u sferu socio-političkih odnosa te u ovom segmentu također postoji širok spektar mogućnosti istraživanja zakonitosti unutar utjecaja primjene biometrijskih sustava.

Mogućnosti za proširenje evaluacijskog modela biti će iznešene u posljednjem poglavlju ovoga rada.

POGLAVLJE IX

9 PROVJERA VALJANOSTI ONTOLOGIJE MODELA OOEPBS

Evaluacijski model OOEPBS, implementiran kao ontologija, definira najčešće korišteni riječnik podataka za istraživače domenskog područja koji žele dijeliti informacije, omogućava ponovnu upotrebljivost domenskog znanja, čini pretpostavke domene jasnijim, sublimira te omogućava analizu domenskog znanja nasuprot onome uopćenome [22].

Sukladno iznešenome u prethodnim poglavljima temelj za ontologiju predstavlja model OOEPBS razvijen kao otvoreni okvir u ranijim fazama ovoga znanstvenog istraživanja. Ontologija je otvorena što znači da se naknadno mogu nadodavati nove klase, atributi, relacije ili instance klasa, te je bitno napomenuti da ima poveznice na sve slične i kompatibilne ontologije koje su već ranije realizirane a upotrebljive. Na slici br. 76 su prikazane ključne komponente sustava uporabe ontologija te njihov međusobni odnos. Razvidno je da su pravila (aksiomi) pokretač ontologije te da od njihove implementacije ovisi i sama funkcionalnost definirane ontologije kroz mogućnost ponovne upotrebljivosti.

Slika 76 Pravila kao pogon te ključni element ontologije

Uzimajući u obzir sve veći interes za razvoj sadržaja za tzv. semantički web, te sukladno tomu razvoj sve većeg broja ontologija iz različitih područja, pojavila se potreba za razvoj metodologija [125] i alata za evaluaciju [111] istih. Glavni pravci u procesima razvoja evaluacijskih metoda [126] ontologija su sljedeći:

1. Vrijednovanje ontologije pomoću alata za kreiranje ontologije Protege',
2. Vrijednovanje ontologije unutar nekog programa-aplikacije,
   To se još naziva i aplikacijski bazirano vrijednovanje ontologije[100],
3. Vrijednovanje u kontekstu njene primjene i zadataka koje treba obaviti.
   To se još naziva i vrijednovanje temeljeno na zadacima[101] [127],
4. Evaluacija utemeljena na razvoju ontologije[102] [24] ,
   Ova vrsta evaluacija temelji se na praćenju promjena već razvijenih ontologija kroz vrijeme korištenja iste. Ontologija evoluira i mijenja se kroz vrijeme uglavnom iz tri sljedeća razloga:
   - promjene unutar domene Ontologije koje se ogledaju u nadodavanju sadržaja u vidu novih znanja iz predmetne domene
   - promjene u konceptualizaciji koje se ogledaju u promjeni načina ili pogleda na opis određenih koncepata u funkciji domenskih promjena.
   - promjene u eksplicitnim specifikacijama koje se ogledaju u eventualnoj promjeni implementacijskog alata ili jezika implementacije Ontologije
5. Logička evaluacija[103] [128],
   Ova vrsta evaluacija temelji se na validacije logičke strukture Ontologije na temelju ugrađenih (*built-in*) alata ili pravila (npr. *Reasoner*)
6. Evaluacija utemeljena [129] na metrikama performansi[104].
   Ova vrsta evaluacija temelji se na parametrima performansi Ontologije sukladno domeni i namjeni same Ontologije [126]. Većina tehnika kojima se koriste metodologije za ocjenu ovoga tipa temelje se na objedinjavanju određenih statističkih ovisnosti parametara koji su definirani unutar same ontologije te koji opisuju znanje predmetne domene.

[100] Izvorno: *Application based ontology evaluation*

[101] Izvorno: *Task based evaluation*

[102] Izvorno: *Evolution based evaluation*

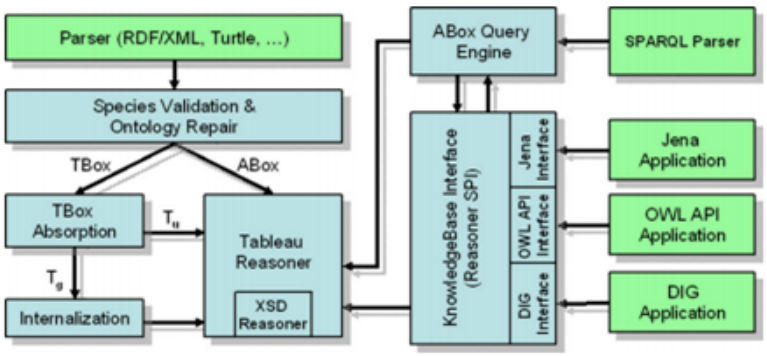
[103] Izvorno: *Logical rule-based evaluation*

[104] Izvorno: *Metric feature based*

Za potrebe provjere konzistentnosti i evaluacije [130] implementirane ontologije koristit će se dodatci koji se integriraju u sam softver Protége (*Pellet, OntoClean, OntoCheck, EvaluationTab*), te metoda OntoQA [23] koja će biti opisana u nastavku, a koja će se provjeravati sa aplikacijom koju su autori [131] napisali u java programskom jeziku i koja se distribuira pod licencom otvorenog koda[105].

9.1 Logička provjera konzistentnosti reasonerom PELLET

Tijekom izgradnje ontologije uključivanjem funkcije Reasoner aktivira se kontinuirana evaluacija ontologije. Reasoner je deduktivni dodatak Protége-u koji omogućava rezoniranje nad definiranom ontologijom u ovom slučaju modela OOEPBS. Za potrebe ovoga doktorskog rada korišten je Pellet reasoner [121]. Pellet reasoner namijenjen je za aplikacije u kojima je potrebno predstaviti informacije i omogućiti rezoniranje nad njima korištenjem jezika OWL. Postao je neizostavan alat [119] koji se koristi sa OWL-om, a koji ima punu potporu za OWL-DL. Implementiran u Java-i, distribuira se pod licencom otvorenog koda [119]. Na slici br. 77 vidimo njegove glavne komponente.



Slika 77 Izvorni grafikon primjene Pellet-a [119]

Tijekom izgradnje ontologije reasoner je stalno aktivan tako da upućuje na nekonzistentnosti klasa te pravila ontologije. Nakon završnog testiranja reasoner nije ukazao na niti jednu nekonzistentnost predmetne ontologije.

Analiza metričke strukture ontologije pokazuje sljedeće iznešeno u tablici 14:

[105] http://tartir-ontoqa.googlecode.com/files/OntoQA.zip

Tablica 14 Metrička struktura Ontologije OOEPBS

Broj aksioma:	1438
Logički broj aksioma:	668
Broj klasa:	156
Objektna svojstva:	6
Podatkovna svojstva	15
Broj instanci:	12
DL izražajnost:	ALCHF(D)

Tablica 15 Aksiomi klasa Ontologije OOEPBS

Broj SubClassOf aksioma:	233
Broj EquivalentClass aksioma:	31
Broj DisjointClass aksioma:	28
Sakriveni CGI:	29

Tablica 16 Aksiomi objektnih svojstava Ontologije OOEPBS

Broj FunctionalObjectProperty aksioma:	5
Broj ObjectPropertyDomain aksioma:	7
Broj ObjectPropertyRange aksioma:	7

Tablica 17 Aksiomi svojstava podataka Ontologije OOEPBS

Broj SubDataPropertyOf aksioma:	1
Broj DisjointDataProperty aksioma:	14
Broj FunctionalDataProperty aksioma:	54
Broj DataPropertyDomain aksioma:	51
Broj DataPropertyRange aksioma:	53

Tablica 18 Aksiomi instanci Ontologije OOEPBS

Broj ClassAssertion aksioma:	22
Broj ObjectPropertyAssertion aksioma:	9
Broj DataPropertyAssertion aksioma:	122
Broj AnnotationAssertion aksioma:	542

Podaci iznešeni u gore navedenim tablicama izvedenica su iz softvera Protege' , Active Ontology tab te pregleda Ontology metrics.

Metrike ontologije sukladno modelu OOEPBS predstavljaju sublimaciju podataka sadržanih u modelu koju predstavlja tablica 14 a koji su detaljno izloženi u poglavlju 8.

Ukupan broj pravila koja reguliraju odnose među klasama jeste 1438 među kojima je 668 kompleksnih logičkih pravila.

Temeljne metrike koje prikazane su u tablici 19:

Tablica 19 Temeljne karakteristike ontologije OOEPBS

Broj Aksioma /Broj klasa	9,2
Broj Logičkih aksioma / Broj klasa	4,3
Broj Aksioma /Broj Logičkih aksioma	2,2
Broj Klasa / Broj Objektnih Svojstava	26
Broj Klasa / Broj Podatkovnih Svojstava	10,4

Metrika omjera Broja aksioma / Broja klasa iznosi 9,2 što se može interpretirati kao visok omjer broja pravila po pojedinoj definiranoj klasi ontologije. Metrika omjera Broja logičkih aksioma / Broja klasa iznosi 4,3 što se može interpretirati kao visok omjer broja kompleksnih pravila po pojedinoj definiranoj klasi ontologije.Logički aksiom predstavlja pravilo koje koristi kompleksne logičke funkcije u odnosu na one jednostavnije definirane aksiomima. Omjer broja aksioma / broja logičkih aksioma iznosi 2,2 što se može interpretirati kao odnos 2,2 jednostavna pravila na jedno kompleksno pravilo primjenjeno na klase ontologije. Ontologija također posjeduje 26 svojstava od kojih su 6 objektna a 25 podatkovna a koja definiraju međusobne odnose klasa te instanci ontologije. Omjer broja klasa / broj podatkovnih svojstava jeste 10,4 što znači svako podatkovno svojstvo regulira međusobne odnose 10,4 klasa. Omjer broja klasa / broj objektnih svojstava jeste 26 što znači svako podatkovno svojstvo regulira međusobne odnose 26 klasa.

Osim kontinuirane provjere logičke konzistentnosti ontologije te pravila koja su definirana u jeziku SWRL analiza pokazuje da je klasa DL Izražajnosti (Izvorno: Digital Logic) ocijenjena kao ALCHF(D) što može biti pojašnjeno na sljedeći način (Izvor: softver Protege', opcija DL Metrics):

AL- Korišten je atributivni jezik koji omogućava :

- atomičku negaciju tvrdnji
- intersekciju definiranih koncepata
- definiciju univerzalnih restrikcija

- egzistencijalnih kvantifikacija

C- korišten je kompleksni opis konceptualnih negacija,

H- opisana je hijerarhija uloga unutar koncepata,

F- definirana su funkcionalna svojstva koncepata,

(D)- korištena su podatkovna svojstva koncepata sa brojčanim vrijednostima.

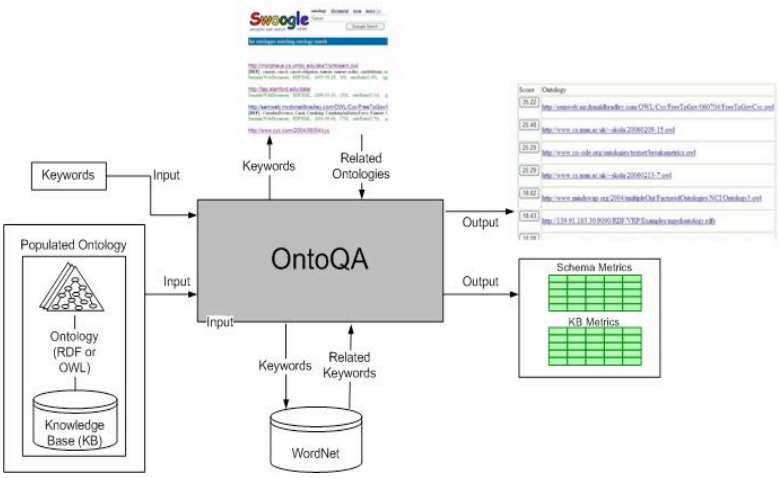
Može se zaključiti da je domenska ontologija OOEPBS logički konzistentna te visoko definirana ontologija sa visokim omjerom pravila na pojedinu klasu ontologije te spada u takozvane Vertikalne specijalizirane ontologije koje sadrže specifična domenska znanja.

9.2 Metoda ONTOQA

Prema OntoQA [24] evaluacijskoj metodi, metrika analize ontologije [112] je podijeljena u sljedeće kategorije:

- metrika sheme (strukture) te,
- metrika baze znanja (instanci) što je prikazano na slici 78.

Metrika sheme ontologije bavi se evaluacijom strukture ontologije, te potencijalom ontologije u predstavljanju specifičnih znanja dok se metrika baze znanja bavi evaluacijom dispozicije instanci podataka unutar ontologije te efektivnog korištenja znanja modeliranog kroz strukturu ontologije.



Slika 78 Arhitektura OntoQA metode[132]

U nastavku biti će dani rezultati analize ontologije modela OOEPBS po metodi OntoQA [112].

9.2.1 Metrika sheme (strukture)

Metrika sheme (strukture) evaluira strukturu podataka unutar same ontologije. Nepostojanje standardne opće prihvaćene analize strukture ontologije onemogućava procjenu «korektnosti» strukture ontologije. Ova metrika postavlja temelje za evaluaciju bogatstva podacima, širine, dužine te dosljednost same strukture ontologije.

9.2.1.1 Bogatstvo vezama[106] RR

Metrika RR reflektira različitost tipova relacija među podacima unutar ontologije. Ontologija koja ima samo vlastite ili strukturne relacije siromašnija je od one koja ima više različitih setova relacija. Parametar se računa uz pomoć indeksa koji nam pokazuje koliko je blizu ili je daleko shema strukture od dijagrama taksonomije, te predstavlja raznolikost tipova relacija unutar ontologije te predstavlja dobar indikator bogatstva sheme ontologije. Ovaj indeks se izražava u postotku.

$$RR = \frac{|P|}{|SC| + |P|} \quad (\%), \qquad [34]$$

Gdje je:

$|P|$- broj relacija, a

$|SC|$- broj pod klasa

Kada u formulu unesemo podatke iz ontologije dobit će se vrijednost RR=25,79 % .

[106] Izvorno: Relationship Richness

Ovo indicira da je kod ontologije OOEPBS većina relacija u domeni pod klasa (IS-A veza) što označava veću razgranatost podataka ontologije te veću detaljiziranost u opisu podataka.

9.2.1.2 Bogatstvo atributa[107] AR

Broj atributa (*slots*) koji je definiran za svaku klasu može indicirati i kvalitetu dizajna ontologije i količinu informacija koje se odnose na instance podataka. Ovaj indeks pokazuje koliko informacija sadrže klase. Općenito se može reći da ontologija koja sadrži više atributa koji su definirani, izražava više znanja.

$$AR = \frac{|att|}{|C|} \ , \qquad [35]$$

Gdje je $|att|$: broj atributa literal-a , a $|C|$: broj klasa

Kada u formulu unesemo podatke iz ontologije dobit će se vrijednost AR=1.40 što ukazuje na relativno visoku definiranost klasa atributima te pravilima jer indeks prelazi odnos 1 klasa / 1 atribut.

9.2.1.3 Bogatstvo prirođenosti[108] *IR*

Metrika bogatstva prirođene strukture ontologije opisuje distribuciju informacija među različitim razinama stabla strukture ontologije. Ona je dobar pokazatelj koliko je dobro znanje grupirano u različite kategorije i podkategorije unutar ontologije. Ova metrika razlikuje vodoravnu ontologiju u kojoj klase imaju veliki broj direktnih pod klasa, te vertikalnu u kojoj klase imaju mali broj direktnih podklasa. Ontologija sa malim indeksom bogatstva nasljeđivanja pokazuje da se radi o dubokoj ili vertikalnoj ontologiji koja pokriva specifičnu domenu, dok ontologija sa visokim indeksom pokazuje da se radi o površnoj ili horizontalnoj ontologiji koja indicira da se radi o uopćenoj ontologiji sa širokim spektrom općenitog znanja s niskom razinom detalja.

Uopćeno znanje (*spanning various domains*) vs. specifično

[107] Izvorno: Attribute Richness

[108] Izvorno: Inheritance Richness

$$IR_S = \frac{\sum_{C_i \in C} \left| H^C \left(C_j, C_i \right) \right|}{|C|} \quad . \qquad [36]$$

Gdje je |*Hc(cj, ci)|:* broj pod-klasa klase *Ci* , a |*C*|: broj klasa.

Kada u formulu unesemo podatke iz ontologije dobit će se vrijednost $IR_S = 2,96$.

Sukladno dobivenoj vrijednosti može se zaključiti da je unutar ontologije vertikalnost podataka izraženija, ontologija je specifičnija, te izražava više specifičnog znanje.

9.2.2. Metrika baze znanja

Način na koji su podaci pozicionirani i distribuirani unutar ontologije također je važno mjerilo kvalitete ontologije, jer to može ukazivati na učinkovitost dizajna ontologije, te količine znanja iz stvarnog svijeta koje je pohranjeno u ontologiji. Metrika obuhvaća podatke koji opisuju bazu znanja kao cjelinu, i podatke koji opisuju način na koji se svaka shema klasa koristi u bazi znanja koja je temelj ontologije.

9.2.2.1 Bogatstvo klasa[109] *CR*

Ova metrika je povezana relacijom kako su instance distribuirane kroz klase definirane unutar ontologije. Broj klasa koje imaju instance u bazi znanja se poredi s ukupnim brojem klasa, dajući opću predodžbu o tome koliko se dobro baza znanja koristi znanjem modeliranim ontološkom shemom klasa. Dakle, ako baza znanja ima mali indeks bogatstva klasa, tada baza znanja nema podatke koji pokazuju sve znanje klasa koje postoji u shemi. S druge strane baza znanja koja ima velik indeks bogatstva klasa (CR) indicira da podaci pohranjeni u bazi znanja predstavljaju većinu znanja u shemi.

$$CR = \frac{|C'|}{|C|} \qquad [37]$$

[109] Izvorno: Class Richness

Gdje je $|C'|$:broj klasa koje koriste a $|C|$: broj definiranih klasa

Kada u formulu unesemo podatke iz izrađene ontologije dobit će se vrijednost *CR*=63,27 što ukazuje na visok indeks bogatstva klasa te sukladno tome visoku razinu pohranjenog domenskog znanja.

9.2.2.2 Prosječna populacija[110] *AP*

Prosječna populacija ili prosječna distribucija instanci kroz sve klase pokazuje broj instanci naspram broja klasa.

$$P = \frac{|I|}{|C|} \qquad [38]$$

Gdje je $|I|$: broj instanci, a $|C|$: broj definiranih klasa

Kada u formulu unesemo podatke iz ontologije dobit će se vrijednosti *P*=0.13 što ukazuje da instance predstavljaju 13% ukupnog broja entiteta definiranih u ontologiji što reflektira osnovnu namjenu definiranih instanci koje su posužile za testiranje funkcionalnosti ontologije.

9.3 Analiza rezultata dobivenih ONTOQA metodom

Rezultati dobiveni uz pomoć alata OntoQA predstavljeni su u nastavku u tablicama 20 i 21 i slikama 47 i 48.

Tablica broj 21 prikazuje metrike sheme ontologije OOEPBS. Kratica RR predstavlja bogatstvo vezama, IRbogatstvo nasljeđivanjem i AR bogatstvo atributa.

[110] Izvorno: Average Population

Tablica 20 Metrika sheme ontologije

Metrika sheme	OOEPBS
Ukupan broj klasa	156
Ukupan broj veza	65
RR (bogatstvo vezama)	25,79
IR (bogatstvo nasljeđivanja)	2,96
Tree balance	2,07
AR (bogatstvo atributima)	1.40

Tablica broj 21 prikazuje metrike baze znanja ontologije OOEPBS. Kratica CR (engl. *Class Richness*) predstavlja bogatstvo klasa, AP (engl. *Average Population*) je prosječna populacija i IC (engl. *Inheritance Richness*) pokrivenost instanci ili osoba.

Tablica 21 Metrika baze znanja ontologije

Metrika baze znanja	OOEPBS
Ukupan broj instanci	21
CR (bogatstvo klasama)	63,27
AP (prosječna populacija)	0.13
IC (pokrivenost instanci)	0.53

Sukladno evaluaciji po metodi OntoQA može se zaključiti da je domenska ontologija OOEPBS visoko definirana ontologija sa visokim omjerom pravila na pojedinu klasu ontologije te spada u takozvane Vertikalne specijalizirane ontologije koje sadrže specifična domenska znanja.

9.4 Poredba sa dostupnim ontologijama

U nastavku je iznešena poredba sa nekoliko referentnih ontologija prezentirana kroz Tablicu 22

Tablica 22 Poredba sa primjerom ontologija [120]

Ontologija	Klase	Relacije	Instance	Bogatstvo klasama
SWETO[111]	44	101	813,217	59.100
TAP[112]	6.969	25	85.637	0.240
GlycO[113]	361	56	660	48.100
KAOntology[114]	96	0	0	71.420
CameraOntology[115]	10	15	2	25
CoC Ontologija	85	47	22	46.280
DD Ontologija	187	50	24	38.28
OOEPBS Ontologija	156	65	21	63,27

Poredba je izvršena sa nekoliko ontologija:

1. SWETO je generalna ontologija opće namjene. Pokriva nekoliko domena, publikacije, zemljopis, terorizam, udruženja,
2. TAP je ontologija izrađena na Stanford Sveučilištu , te je također ontologija opće namjene podijeljena u 43 pod-domene – sport, zemljopis, publikacije i sl.,
3. GlycO je ontologija razvijena na Sveučilištu Georgija (Laboratorij za glikan),
4. KAOntology je Ontologija definira koncepte akademskih istraživanja. Autor je Ian Horrocks,
5. CameraOntology je ontologija koja pokriva domenu digitalnih kamera,
6. CoC je ontologija lanca očuvanosti digitalnog dokaza,
7. DD je ontologija Digitalnog dokaza.

[111] LSDIS' ontologija opće namjene – pokriva domenu publikacija, udruženja, zemljopisa i terorizam.

[112] Stanford's ontologija opće namjene. Podjeljena u 43 domene. Neke od domona su publikacije, sport i zemljopis.

[113] LSDIS' ontologija koncepta „Glycan Expression"

[114] Ontologija definira koncepte akademskih istraživanja. Autor je Ian Horrocks (http://protegewiki.stanford.edu/wiki/Protege_Ontology_Library)

[115] OWL ontologija o dijelovima foto kamere (http://protegewiki.stanford.edu/wiki/Protege_Ontology_Library)

Prema rezultatima prikazanim u tablici br. 23 *CR* je najveći kod KAOntology ontologije što znači da podaci u bazi znanja ove ontologije predstavljaju najviše znanja u shemi. Ontologija OOEPBS je prema rezultatima pri vrhu među analiziranim ontologijama.

Tablica 23 Poredba ostale metrike

Ontologija	Broj klasa	Broj instanci	Bogatstvo nasljeđivanja	Bogatstvo klasama	Prosječna populacija
SWETO	44	1,003,021	0.9	56.8%	22,795.9
TAP	3,230	71,487	1.2	9.4%	22.1
GlycO	356	387	1.3	18.0%	1.1
KAOntology	96	0	4.0	71.42%	0.0
CameraOntology	10	2	2.5	25.0%	0.2
DD Ontologija	187	24	3.35	38.28%	0.12
CoC Ontologija	85	22	3.29	46.28%	0.25
OOEPBS Ontologija	165	56	2,96	63,27%	0.13

Prema rezultatima prikazanim u tablici 23 najgeneralnija ontologija je KAOntologija, dok su najspecifičnije, vertikalne SWETO, TAP i GlycO ontologije. DD Ontologija i CoC Ontologija također su relativno generalne. OOEPBS pripada grupi ontologija sa visokim parametrom bogatstva klasa te srednje visokim parametrom bogatstva nasljeđivanja koji govori o distribuciji znanja unutar ontologije. Sve vrijednosti izrađenih ontologija su u prihvatljivim granicama. U odnosu na ostale objavljene ontologije , OOEPBS je vertikalna te predstavlja specifično znanje.

POGLAVLJE X

10 ZAKLJUČAK I OTVORENA PITANJA

10.1 Zaključak

Predmet ovoga doktorskog rada bio je istraživanje postojećih saznanja u domeni pouzdanosti biometrijskih sustava te razmatranja definiranih modela koji su obrađeni u poglavljima 3 i 4.

Motivacija te okosnica ovoga doktorskog rada bila je činjenica da se nadolazeće nove tehnologije poput biometrije susreću sa često nerealnim očekivanjima glede njihovih operativnih performansi te ih se često nepravedno uspoređuje sa sustavima koji koriste samo zaporke ili neke druge trivijalne alternative. Uzimajući u obzir vjerojatnosni karakter mehanizama donošenja odluke biometrijskog sustava nužan je i odgovor na pitanje: Mora li biometrijski sustav biti 100% siguran i precizan ili može biti dopustiva određena granica nepovjerenja ili nepouzdanosti u sustav?

Osnovna svrha rada je bila znanstveno istraživanje koje će dati uvid u specifikaciju pojma pouzdanosti u širem smislu te pojma pouzdanosti biometrijskog sustava u užem smislu uzimajući u obzir recentna istraživanja iz domene pouzdanosti biometrijskih sustava te određivanje pravca za definiranje metode za evaluaciju pouzdanosti biometrijskih sustava koja će omogućiti rezoniranje o pouzdanosti istih tijekom projektiranja i osmišljavanja a prije same uporabe.

Cilj ovog znanstvenog rada bio je definirati otvoreni metodološki okvir za evaluaciju pouzdanosti biometrijskih sustava uzimajući u obzir činitelje pouzdanosti biometrijskih sustava manifestiranih kroz sljedeće sastavnice: tehnologija sustava, okolina uporabe sustava te korisnik sustava. Metodološki okvir trebao je biti utemeljen na ontologiji, kao osnovi za izradu specifičnih modela koji će se baviti proučavanjem te detaljnom razradom navedenih aspekata pouzdanosti sa pripadajućim činiteljima opisanima u poglavlju 6.

Metodološki okvir za evaluaciju pouzdanosti biometrijskog sustava je strukturiran na način da uzima u obzir pojavnosti biometrijskih sustava kroz trijadu sastavnica koje su opisane kako slijedi:

- Tehnologija biometrijskih sustava sa aspekta pouzdanosti hardvera, softvera te performansi sustava kroz parametre FMR i FNMR, te FTA i FTE a koji su definirani od strane proizvođača sustava,
- Okolina uporabe biometrijskih sustava sa aspekta otvorenosti pristupa sustavu, nadzora nad sustavom te okolinskih čimbenika unutar kojih biometrijski sustav funkcionira,
- Korisnik biometrijskih sustava sa aspekta utjecaja na karakteristike korisnika koje predstavljaju ulaz u proces identifikacije ili verifikacije [32] te osobnih činitelja utjecaja na samog korisnika tijekom interakcije sa biometrijskim sustavom.

Metodološki okvir pretpostavlja serijsku ovisnost navedenih sastavnica pouzdanosti biometrijskih sustava u smislu isključivog utjecaja pojedine sastavnice na sposobnost sustava da izvršava svoju operativnu funkciju. Metodološki okvir je definiran na način da može omogućiti rezoniranje o prihvatljivosti riješenja biometrijskih sustava u domeni pouzdanosti te na temelju ulaznih podataka o tehnologiji, okolini uporabe te korisniku sustava, analizirati razine pouzdanosti, biometrijskih sustava, koje su metrički definirane te implementirane u samoj ontologiji. Pravila za rezoniranje su implementirana unutar alata Protege' u jeziku SWRL (Izvorno: Semantic Web Rule Language).

Sukladno postavljenim ciljevima istraživačka pitanja na koja je rad pokušao dati odgovor su:

1. Koje su sastavnice aspekata pouzdanosti biometrijskih sustava koje imaju utjecaj na performanse biometrijskih sustava?,
2. Koje su funkcije međusobne ovisnosti sastavnica aspekata pouzdanosti biometrijskih sustava?,
3. Kako se sastavnice mogu parametarski te metrički definirati?,
4. Da li je moguća ontološka deskripcija pojmova koji opisuju parametrizirane sastavnice aspekata pouzdanosti odabranih biometrijskih sustava te definiranje međusobne povezanosti i atributa?,
5. Da li je moguća implementacija ontološki opisanih pojmova pomoću alata otvorenog koda Protege'?,
6. Da li je moguća implementacija pravila za rezoniranje o razini pouzdanosti biometrijskih sustava na temelju postavljanja upita u jeziku SWRL?
7. Da li je moguće pomoću izrađene ontologije metodološkog okvira za evaluaciju pouzdanosti biometrijskih sustava, stvaranje temelja za širi pristup problematikama evaluacije pouzdanosti biometrijskih sustava?

Odgovor na pitanje broj jedan dan je u Poglavlju broj 6.3 gdje su opisani činitelji pojedinih aspekata pouzdanosti u vidu sastavnica pouzdanosti. Odgovor na drugo pitanje dan je u poglavlju 6.4 gdje je definiran model OOEPBS (Otvoreni okvir za evaluaciju pouzdanosti biometrijskih sustava) sa funkcijama međuovisnosti pojedinih činitelja. Na pitanje broj tri odgovor je dan u Poglavlju 6. a detaljnije u Poglavljima 6.3, 6.4 i 6.5 gdje su opisani koncepti modela OOEPBS sa razlaganjem aspekata na činitelje sa njihovim metrički definiranim parametrima te je definirana evaluacijska metoda sukladno modelu OOEPBS. Na pitanje broj četiri i pet odgovor je dan kroz Poglavlje 7 gdje je detaljno izložen postupak stvaranja ontologije modela OOEPBS po metodi Methontology te njegove implementacije u softverskom alatu Protege'. Odgovor na pitanje broj šest dan je izlaganjem u Poglavlju 8 koje se bavi testiranjem funkcionalnosti implementiranog evaluacijskog modela putem definiranja pravila za rezoniranje u jeziku SWRL koji je integralni dio softverskog alata Protege'. Odgovor na pitanje broj 7 dan je u Poglavlju 9 u kojemu su iznešeni zaključci provjera valjanosti definirane ontologije i poredbe sa dostupnim ontologijama, te u Poglavlju 10.2 koje se bavi otvorenim pitanjima koje ostavlja ovaj rad te mogućnostima za nadogradnju ovoga evaluacijskog okvira.

Hipoteze koje su proizašle iz definiranih istraživačkih pitanja bile su sljedeće:

H1: Moguće je ontološki opisati činitelje pouzdanosti biometrijskih sustava s aspekta tehnologije, korisnika i okružja uporabe te ih međusobno povezati u otvoreni metodološki okvir za evaluaciju pouzdanosti.

H2: Temeljem otvorenog metodološkog okvira za evaluaciju pouzdanosti biometrijskih sustava, definirati će se pravila pomoću kojih će se moći rezonirati o prihvatljivosti rješenja biometrijskih sustava u smislu razine pouzdanosti biometrijskog sustava u odnosu na predefinirane ulazne parametre.

Provjera hipoteze H1 izvršena je kroz Poglavlje 6 i 7 gdje je detaljno opisan postupak razlaganja aspekata pouzdanosti na činitelje te pripadajuće parametre koji su međusobno povezani u evaluacijsku metodu te metrički definirani unutar ontologije po modelu OOEPBS tako da je hipoteza H1 prihvaćena realizacijom samog evaluacijskog modela kroz definiranje metode za evaluaciju.

Provjera hipoteze H2 izvršena je kroz Poglavlja 8 i 9 gdje je detaljno opisan postupak implementacije modela OOEPBS u ontologiju uz korištenje softverskog alata Protege' sa

opisanim konceptima, atributima, pravilima za rezoniranje implementiranih u jeziku SWRL te je izvršeno testiranje ontologije putem definiranih instanci nad kojima su definirana pravila testirana uporabom DL opcije softvera Protege'. Također je izvršena te dokumentirana analiza valjanosti ontologije korištenjem reasonera Pellet te uz pomoć metode OntoQA gdje su iznešeni zaključci a kao nadopuna validaciji također je izvršena poredba sa dostupnim ontologijama slične strukture. Iz izloženog može se zaključiti da je hipoteza H2 prihvaćena realizacijom ontologije , njenom provjerom valjanosti te poredbom sa ostalim sličnim ontologijama.

Društveni doprinos rada se ogleda u primjeni znanstvenih istraživanja u praksi prilikom projektiranja biometrijskih sustava te korištenja određenog modela evaluacije pouzdanosti u ranoj fazi projektiranja. Rezultati istraživanja moći će se koristiti , kako za diseminaciju znanja iz referentnog područja, tako i za realizaciju te implementaciju konkretnog sustava utemeljenog na predloženom okviru za evaluaciju pouzdanosti biometrijskih sustava. Budući da se radi o relativno neistraženom području sa mnoštvom nesistematiziranih pojmova koji opisuju određene probleme povezane sa pouzdanošću, te uzimajući u obzir da je biometrija znanost u razvoju, istraživačkim radom se stavio akcent na povezivanje postojećih partikularnih analiza biometrijske znanosti fokusiranih na problematike evaluacije pouzdanosti biometrijskih sustava sukladno pojavnostima uporabe biometrijskih sustava.

Znanstveni doprinos istraživanja se može odrediti kroz doprinos sistematizaciji znanja iz područja biometrijske znanosti, a koja se odnose na problematike pouzdanosti biometrijskih sustava, omogućavanje diseminacija znanja iz područja pouzdanosti biometrijskih sustava sistematiziranih kroz definiranu otvorenu ontologiju iz predmetne domene kroz koju su određeni, ontološki opisani, međusobno povezani, te metrički definirani činitelji aspekata pouzdanosti biometrijskih sustava spram korisničke interakcije, tehnologije, okruženja/lokacije primjene. Razvoj i definicija otvorenog metodološkog okvira za evaluaciju pouzdanosti biometrijskih sustava koji može biti primjenjen na biometrijske sustave u fazi njihove izrade a prije uporabe te nadograđen na temelju iskustava tijekom operativne funkcije predstavlja također znanstveni doprinos ovoga rada.

10.2 Otvorena pitanja

Sukladno iznešenome u Poglavlju 8.4 model OOEPBS obuhvaća aspekte Tehnologije, Okoline te Korisnika biometrijskog sustava a unutar istih postoji mogućnost proširenja sa činiteljima koji nisu obuhvaćeni ovim evaluacijskim modelom. Model OOEPBS stvara pretpostavku za daljnju nadogradnju te razmjenu iskustava iz znanstvenih istraživanja i prakse.

Mogućnosti proširenja otvorenog okvira su raznolike te omogućuju istraživačima proširenje ovoga modela drugim činiteljima koji mogu utjecati na funkcionalnost biometrijskog sustava tijekom interakcije sa korisnikom. Iako su već u poglavlju 6.3 , tijekom definiranja pojedinačnih činitelja pouzdanosti te parametriziranja istih, iznešeni konkretni primjeri mogućnosti nadogradnje postojećeg modela moguće je istraživanje nastaviti u sljedećim pravcima:

1. Nadogradnja aspekta korisnik biometrijskog sustava uzimajući u obzir mogućnost korištenja biometrijskog sustava[116],

Definicija mogućnosti korištenja ,sukladno međunarodnoj normi ISO 13407:1999, jeste : " Razina do kojega proizvod može biti korišten od strane specifičnih korisnika radi postizanja specifičnih ciljeva kroz efektivnost, efikasnost i zadovoljstvo u određenom kontekstu uporabe". Mogućnost korištenja predstavlja važan parametar u ocjeni funkcionalnosti prije stavljanja u operativnu funkciju biometrijskog sustava jer ima značajan utjecaj na korisnika te isto tako i na pouzdanost operativne funkcije sustava.

Metrike kojima se može definirati ovaj parametar su sljedeće:

- Efektivnost
  - ✓ Broj grešaka sustava
  - ✓ Broj asistencija
  - ✓ Postotak kompletiranih zadaća
- Efikasnost
  - ✓ Vrijeme obavljanja zadatka

[116] Izvorno: Usability

- Zadovoljstvo korisnika
  - ✓ Postotak zadovoljnih korisnika

2. Prihvatljivost biometrijskog sustava predstavlja također nadogradnju aspekta korisnik

Prihvatljivost se može opisati kao razina prihvaćanja uloge biometrijskog sustava od strane korisnika te se može konkretizirati formuliranjem upitnika koji trebaju biti strukturirani na način da daju odgovor na pitanje razinaa prihvatljivosti određenih rješenja kategorijama korisnika kojima je namijenjen biometrijski sustav.

Metrike prihvatljivosti biometrijskog sustava mogu biti definirane kako slijedi:

- Komfort tijekom uporabe
- rizik po zdravlje korisnika
- Očuvanje privatnosti tijekom korištenja sustava

3. Nadzor nad okolinom biometrijskog sustava predstavlja mogućnost za nadogradnju aspekta okolina

Nadzor nad okolinom može se definirati kao razina kontrole nad uvjetima koji vladaju u okolini u kojoj djeluje biometrijski sustav te se isti može parametrizirati na način da se opišu činitelji koji su od utjecaja na pouzdanost funkcije biometrijskog sustava.

4. Certificiranost tehnologije biometrijskog sustava predstavlja mogućnost za nadogradnju aspekta tehnologija

Posjedovanje komponenti tehnologije koje su certificirane u velikoj mjeri može značiti utjecaj na pouzdanosti operativne funkcije biometrijskih sustava tako da parametrizacija zahtjeva po tom pitanju može biti uključena u evaluacijski model.

PRILOZI

PRILOG A – Pregled činitelja aspekata pouzdanosti

Aspekt	Činitelj	Parametar	M.J.	Područje pouzdanosti
Tehnologija	Softver	Pouzdanost (P)	%	> 90
	Hardver	Pouzdanost (P)	%	> 90
	Performanse	Statistike (S): FTA, FTE, FMR,FNMR	%	< 1
Okolina	Fizička svojstva	Osvjetljenje (O)	lx	1500-2000
	Fizička svojstva	Buka (B)	dB	< 80
	Atmosferske prilike	Temperatura (T)	°C	10-40
	Atmosferske prilike	Vlažnost (V)	%	40-60
Korisnik	Karakteristike	Kratkoročni utjecaj: - ponašajni (PON) - fizički (FIZ)	Mali -1 Srednji-2 Veliki-3	< 2
Korisnik	Karakteristike	Dugoročni utjecaj: - Izgled (IZG) - Bolest (BOL)	Mali -1 Srednji-2 Veliki-3	< 2
Korisnik	Osobni činitelji	Antropometrija: - Obilježja (OBI) - Dimenzije (DIM)	Mali -1 Srednji-2 Veliki-3	< 2
Korisnik	Osobni činitelji	Iskustvo: - Uvježbanost (UVJ)	Mali -1 Srednji-2 Veliki-3	< 2
Korisnik	Osobni činitelji	Ergonomija: - Uvjeti korištenja (UV.KOR) - Pozicija (POZ)	Mali -1 Srednji-2 Veliki-3	< 2

PRILOG B – Evaluacijski obrazac

Biometrijski sustav:	
Naziv:	
Serijski broj:	
Tip:	
Modalitet:	
Namjena:	
Lokacija:	

Evaluacijski model:	Parametar	Vrijednost	Područje pouzdanosti	Rezultat	Rezultat grupe	Rezultat modela
Tehnologija: softver	Pouzdanost		>95			
Tehnologija: hardver	Pouzdanost		>95			
Tehnologija: Performanse	FMR		<2			
Tehnologija: Performanse	FNMR		<2			
Tehnologija: Performanse	FTE		<2			
Tehnologija: Performanse	FTA		<2			
GRUPA A						
Okolina: Fizička svojstva	Osvjetljenje		1500 do 2000			
Okolina: Fizička svojstva	Buka		80 do 90			
Okolina: Atmosferske prilike	Temperatura		10 do 40			
Okolina: Atmosferske prilike	Vlažnost		40 do 60			
GRUPA B					B2	
Korisnik:Karakteristike	KU: Ponašajni		<2			
Korisnik:Karakteristike	KU: Fizički		<2			
Korisnik:Karakteristike	DU: Izgled		<2			
Korisnik:Karakteristike	DU: Bolest		<2			
Korisnik:Osobni činitelji	AN: Obilježja		<2			
Korisnik:Osobni činitelji	AN: Dimenzije		<2			
Korisnik:Osobni činitelji	IS: Uvježbanost		<2			
Korisnik:Osobni činitelji	ER: Uvjeti		<2			
Korisnik:Osobni činitelji	ER: Pozicija		<2			
GRUPA C						
REZULTAT MODELA						

PRILOG C – Tablica interpretacije vrijednosti evaluacijskog modela

	A			B			C								
	Softver	Hardver	Performanse	Temperatura	Vlažnost	Osvjetljenje	Buka	Ponašajni	Fizički	Bolest	Izgled	Obilježja	Dimenzije	Uvježbanost	Uvjeti kor.	Pozicija
A1B1C1	P>90	P>90	S<0,01	10<T<40	40<H<60	1500<Lx<2000	dB<80	1	1	1	1	1	1	1	1	1
A1B2C1	P>90	P>90	S<0,01	10>T	40>H	1500>Lx	80<dB<90	1	1	1	1	1	1	1	1	1
A1B3C1	P>90	P>90	S<0,01	10<T	60<H	2000<Lx	dB>80	1	1	1	1	1	1	1	1	1
A1B1C2	P>90	P>90	S<0,01	10<T<40	40<H<60	1500<Lx<2000	dB<80	2	2	2	2	2	2	2	2	2
A1B2C2	P>90	P>90	S<0,01	10>T	40>H	1500>Lx	80<dB<90	2	2	2	2	2	2	2	2	2
A1B3C2	P>90	P>90	S<0,01	10<T	60<H	2000<Lx	dB>80	2	2	2	2	2	2	2	2	2
A1B1C3	P>90	P>90	S<0,01	10<T<40	40<H<60	1500<Lx<2000	dB<80	3	3	3	3	3	3	3	3	3
A1B2C3	P>90	P>90	S<0,01	10>T	40>H	1500>Lx	80<dB<90	3	3	3	3	3	3	3	3	3
A1B3C3	P>90	P>90	S<0,01	10<T	60<H	2000<Lx	dB>80	3	3	3	3	3	3	3	3	3
A2B1C1	80<P<90	80<P<90	0,01<S<0,02	10<T<40	40<H<60	1500<Lx<2000	dB<80	1	1	1	1	1	1	1	1	1
A2B2C1	80<P<90	80<P<90	0,01<S<0,02	10>T	40>H	1500>Lx	80<dB<90	1	1	1	1	1	1	1	1	1
A2B3C1	80<P<90	80<P<90	0,01<S<0,02	10<T	60<H	2000<Lx	dB>80	1	1	1	1	1	1	1	1	1
A2B1C2	80<P<90	80<P<90	0,01<S<0,02	10<T<40	40<H<60	1500<Lx<2000	dB<80	2	2	2	2	2	2	2	2	2
A2B2C2	80<P<90	80<P<90	0,01<S<0,02	10>T	40>H	1500>Lx	80<dB<90	2	2	2	2	2	2	2	2	2
A2B3C2	80<P<90	80<P<90	0,01<S<0,02	10<T	60<H	2000<Lx	dB>80	2	2	2	2	2	2	2	2	2
A2B1C3	80<P<90	80<P<90	0,01<S<0,02	10<T<40	40<H<60	1500<Lx<2000	dB<80	3	3	3	3	3	3	3	3	3
A2B2C3	80<P<90	80<P<90	0,01<S<0,02	10>T	40>H	1500>Lx	80<dB<90	3	3	3	3	3	3	3	3	3
A2B3C3	80<P<90	80<P<90	0,01<S<0,02	10<T	60<H	2000<Lx	dB>80	3	3	3	3	3	3	3	3	3
A3B1C1	P<90	P<90	S>0,02	10<T<40	40<H<60	1500<Lx<2000	dB<80	1	1	1	1	1	1	1	1	1
A3B2C1	P<90	P<90	S>0,02	10>T	40>H	1500>Lx	80<dB<90	1	1	1	1	1	1	1	1	1
A3B3C1	P<90	P<90	S>0,02	10<T	60<H	2000<Lx	dB>80	1	1	1	1	1	1	1	1	1
A3B1C2	P<90	P<90	S>0,02	10<T<40	40<H<60	1500<Lx<2000	dB<80	2	2	2	2	2	2	2	2	2
A3B2C2	P<90	P<90	S>0,02	10>T	40>H	1500>Lx	80<dB<90	2	2	2	2	2	2	2	2	2
A3B3C2	P<90	P<90	S>0,02	10<T	60<H	2000<Lx	dB>80	2	2	2	2	2	2	2	2	2
A3B1C3	P<90	P<90	S>0,02	10<T<40	40<H<60	1500<Lx<2000	dB<80	3	3	3	3	3	3	3	3	3
A3B2C3	P<90	P<90	S>0,02	10>T	40>H	1500>Lx	80<dB<90	3	3	3	3	3	3	3	3	3
A3B3C3	P<90	P<90	S>0,02	10<T	60<H	2000<Lx	dB>80	3	3	3	3	3	3	3	3	3

PRILOG D – dio izvornog kôda ontologije prikazan u manchester notaciji

```
################################################
#ONTOLOGIJA OOEPBS V.1.2 (C) 2014
#ZAPIS GLAVNIH KARAKTERISTIKA ONTOLOGIJE
#JE DAN U MANCHESTER NOTACIJI
#CJELOKUPAN SOURCE CODE CE BITI JAVNO OBJAVLJEN
#U NEKOM OD JAVNO DOSTUPNIH REPOZITORIJA
################################################

Ontology: <http://www.semanticweb.org/OOEPBS>

Datatype: rdf:PlainLiteral

Datatype: xsd:string

Datatype: xsd:dateTime

Prefix: :
<http://www.semanticweb.org/zorancosic/ontologies/2014/8/untitled-
ontology-39#>
Prefix: owl: <http://www.w3.org/2002/07/owl#>
Prefix: rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
Prefix: xml: <http://www.w3.org/XML/1998/namespace>
Prefix: xsd: <http://www.w3.org/2001/XMLSchema#>
Prefix: rdfs: <http://www.w3.org/2000/01/rdf-schema#>
Prefix: swrl: <http://www.w3.org/2003/11/swrl#>
Prefix: swrlb: <http://www.w3.org/2003/11/swrlb#>
Prefix: ace_lexicon: <http://attempto.ifi.uzh.ch/ace_lexicon#>
Prefix: untitled-ontology-39:
<http://www.semanticweb.org/zorancosic/ontologies/2014/8/untitled-
ontology-39#>

Ontology:
<http://www.semanticweb.org/zorancosic/ontologies/2014/8/untitled-
ontology-39>

AnnotationProperty: ace_lexicon:TV_pl


AnnotationProperty: ace_lexicon:PN_sg


AnnotationProperty: ace_lexicon:TV_sg


AnnotationProperty: ace_lexicon:CN_sg


AnnotationProperty: ace_lexicon:CN_pl


AnnotationProperty: rdfs:comment


AnnotationProperty: ace_lexicon:TV_vbg
```

```
Datatype: rdf:PlainLiteral


Datatype: xsd:string


ObjectProperty: Nema

    Annotations:
        ace_lexicon:TV_vbg "Nemaed",
        ace_lexicon:TV_sg "Nemas",
        ace_lexicon:TV_pl "Nema"

    Characteristics:
        Functional

    Range:
        KarakteristikaKorisnikaBiometrijskogSustava


ObjectProperty: Ima

    Annotations:
        ace_lexicon:TV_sg "Imas",
        ace_lexicon:TV_pl "Ima",
        ace_lexicon:TV_vbg "Imaed"

    Characteristics:
        Functional

    Domain:
        Ima some SvojstvoOkolineBiometrijskogSustava,
        Ima some KarakteristikaKorisnikaBiometrijskogSustava,
        Ima some PouzdanostTehnologijeBiometrijskogSustava

    Range:
        Ima some BiometrijskiSustav


ObjectProperty: jeDio

    Annotations:
        ace_lexicon:TV_sg "jeDioes",
        ace_lexicon:TV_vbg "jeDioed",
        ace_lexicon:TV_pl "jeDio"

    Characteristics:
        Functional

    Domain:
        jeDio some BiometrijskiSustav

    Range:
        jeDio some KarakteristikaKorisnikaBiometrijskogSustava,
        jeDio some SvojstvoOkolineBiometrijskogSustava,
        jeDio some PouzdanostTehnologijeBiometrijskogSustava
```

```
ObjectProperty: Interagira

    Annotations:
        ace_lexicon:TV_pl "Interagira",
        ace_lexicon:TV_vbg "Interagiraed",
        ace_lexicon:TV_sg "Interagiras"

    Characteristics:
        Functional

    Domain:
        Interagira some BiometrijskiSustav

    Range:
        Interagira some KarakteristikaKorisnikaBiometrijskogSustava


ObjectProperty: Utjece

    Annotations:
        ace_lexicon:TV_sg "Utjeces",
        ace_lexicon:TV_vbg "Utjeced",
        ace_lexicon:TV_pl "Utjece"

    Characteristics:
        Functional

    Domain:
        Utjece some PouzdanostTehnologijeBiometrijskogSustava,
        Utjece some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        Utjece some SvojstvoOkolineBiometrijskogSustava


ObjectProperty: NijeDio

    Annotations:
        ace_lexicon:TV_pl "NijeDio",
        ace_lexicon:TV_vbg "NijeDioed",
        ace_lexicon:TV_sg "NijeDioes"


DataProperty: JacinaBukeUnutarPodrucjaPouzdanosti

    Annotations:
        ace_lexicon:TV_sg "StandardnaBukas",
        ace_lexicon:TV_pl "StandardnaBuka",
        ace_lexicon:TV_vbg "StandardnaBukaed"

    Characteristics:
        Functional

    Domain:
        Ima some FizickoSvojstvoOkoline

    Range:
```

```
        xsd:string

    DisjointWith:
        JacinaBukeIzvanPodrucjaPouzdanosti


DataProperty: FMRUnutarPodrucjaPouzdanosti

    Annotations:
        ace_lexicon:CN_sg "FMR",
        ace_lexicon:TV_pl "FMRDjelomicnoPouzdan",
        ace_lexicon:CN_pl "FMRs",
        ace_lexicon:TV_sg "FMRDjelomicnoPouzdans",
        ace_lexicon:TV_vbg "FMRDjelomicnoPouzdaned"

    Characteristics:
        Functional

    Domain:
        Ima some FMRPouzdan

    Range:
        xsd:string


DataProperty: SrednjiUtjecaj

    Annotations:
        rdfs:comment "2",
        ace_lexicon:TV_sg "SrednjiUtjecajs",
        ace_lexicon:TV_pl "SrednjiUtjecaj",
        ace_lexicon:TV_vbg "SrednjiUtjecajed"


    Characteristics:
        Functional

    Domain:
        Ima some SrednjiUtjecajNaKorisnika

    Range:
        xsd:string


DataProperty: KorisnikNeuvjezban

    Annotations:
        ace_lexicon:TV_sg "KorisnikNeuvjezbans",
        ace_lexicon:TV_vbg "KorisnikNeuvjezbaned",
        ace_lexicon:TV_pl "KorisnikNeuvjezban"

    Characteristics:
        Functional

    Domain:
        KarakteristikaKorisnikaBiometrijskogSustava

    Range:
```

```
        xsd:string

    DisjointWith:
        KorisnikUvjezban


DataProperty: DimenzijeTijelaNeizrazene

    Annotations:
        ace_lexicon:TV_vbg "TjelesneDimenzijeNeUtjecued",
        ace_lexicon:TV_sg "TjelesneDimenzijeNeUtjecus",
        ace_lexicon:TV_pl "TjelesneDimenzijeNeUtjecu"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        xsd:string


DataProperty: PrimjerenoPonašanjeKorisnika

    Annotations:
        ace_lexicon:TV_pl "PrimjerenoPonašanje",
        ace_lexicon:TV_sg "PrimjerenoPonašanje",
        ace_lexicon:TV_vbg "PrimjerenoPonašanje"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        xsd:string

    DisjointWith:
        NeprimjerenoPonasanjeKorisnika


DataProperty: PerformansePouzdane

    Annotations:
        ace_lexicon:TV_sg "PerformansePouzdanes",
        ace_lexicon:TV_vbg "PerformansePouzdaned",
        ace_lexicon:TV_pl "PerformansePouzdane"

    Characteristics:
        Functional

    Domain:
        Ima some PouzdanostTehnologijeBiometrijskogSustava

    Range:
        xsd:string
```

```
    DisjointWith:
        PerformanseNepouzdane


DataProperty: PouzdanostHardveraUnutarPodrucjaPouzdanosti

    Annotations:
        ace_lexicon:TV_pl "HardverPouzdan",
        ace_lexicon:CN_sg "HardverPouzdan",
        ace_lexicon:TV_sg "HardverPouzdans",
        ace_lexicon:TV_vbg "HardverPouzdaned",
        ace_lexicon:CN_pl "HardverPouzdans"

    Characteristics:
        Functional

    Domain:
        Ima some HardverPouzdan

    Range:
        xsd:string

    DisjointWith:
        PouzdanostHardveraIzvanPodrucjaPouzdanosti


DataProperty: VlaznostUnutarPodrucjaPouzdanosti

    Annotations:
        ace_lexicon:TV_sg "StandardnaVlaznosts",
        ace_lexicon:TV_pl "StandardnaVlaznost",
        ace_lexicon:TV_vbg "StandardnaVlaznosted"

    Characteristics:
        Functional

    Range:
        xsd:string

    DisjointWith:
        VlaznostIzvanPodrucjaPouzdanosti


DataProperty: Lokacija

    Annotations:
        ace_lexicon:CN_pl "Lokacijas",
        ace_lexicon:TV_sg "Lokacijas",
        ace_lexicon:TV_pl "Lokacija",
        ace_lexicon:TV_vbg "Lokacijaed",
        ace_lexicon:CN_sg "Lokacija"

    Characteristics:
        Functional

    Domain:
        BiometrijskiSustav
```

```
    Range:
        xsd:string


DataProperty: owl:topDataProperty


DataProperty: ObiljezjaTijelaNeizrazena

    Annotations:
        ace_lexicon:TV_vbg "NemaObiljezjaed",
        ace_lexicon:TV_sg "NemaObiljezjas",
        ace_lexicon:TV_pl "NemaObiljezja"

    Characteristics:
        Functional

    Domain:
        KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        xsd:string

    DisjointWith:
        ObiljezjaTijelaIzrazena


DataProperty: KorisnikImaBolest

    Annotations:
        ace_lexicon:TV_vbg "ImaBolested",
        ace_lexicon:TV_pl "ImaBolest",
        ace_lexicon:TV_sg "ImaBolests"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        xsd:string

    DisjointWith:
        KorisnikNemaBolest


DataProperty: ObiljezjaTijelaIzrazena

    Annotations:
        ace_lexicon:TV_vbg "ImaObiljezjaed",
        ace_lexicon:TV_sg "ImaObiljezjas",
        ace_lexicon:TV_pl "ImaObiljezja"

    Characteristics:
        Functional
```

```
    Domain:
        KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        xsd:string

    DisjointWith:
        ObiljezjaTijelaNeizrazena


DataProperty: FizickiVanjskiIzgledBezUtjecaja

    Annotations:
        ace_lexicon:TV_vbg "FizickiIzgledPrikladaned",
        ace_lexicon:TV_pl "FizickiIzgledPrikladan",
        ace_lexicon:TV_sg "FizickiIzgledPrikladans"

    Characteristics:
        Functional

    Domain:
        Ima some IzgledKorisnika

    Range:
        xsd:string


DataProperty: MaliUtjecaj

    Annotations:
        ace_lexicon:TV_vbg "MaliUtjecajed",
        rdfs:comment "1",
        ace_lexicon:TV_sg "MaliUtjecajs",
        ace_lexicon:TV_pl "MaliUtjecaj"

    Characteristics:
        Functional

    Domain:
        Ima some MaliUtjecajNaKorisnika

    Range:
        xsd:string

    SubPropertyOf:
        owl:topDataProperty


DataProperty: FTAUnutarPodrucjaPouzdanosti

    Annotations:
        ace_lexicon:TV_vbg "FTAStandardnied",
        ace_lexicon:TV_pl "FTAStandardni",
        ace_lexicon:TV_sg "FTAStandardnis"

    Characteristics:
        Functional
```

```
    Domain:
        Ima some FTAPouzdan

    Range:
        xsd:string


DataProperty: KorisnikSvjestan

    Annotations:
        ace_lexicon:TV_pl "KorisnikSvjestan",
        ace_lexicon:TV_sg "KorisnikSvjestans",
        ace_lexicon:TV_vbg "KorisnikSvjestaned"

    Characteristics:
        Functional

    Range:
        xsd:string

    DisjointWith:
        KorisnikNijeSvjestan


DataProperty: NeprimjerenoPonasanjeKorisnika

    Annotations:
        ace_lexicon:TV_sg "NeprimjerenoPonasanjes",
        ace_lexicon:TV_vbg "NeprimjerenoPonasanjed",
        ace_lexicon:TV_pl "NeprimjerenoPonasanje"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        xsd:string

    DisjointWith:
        PrimjerenoPonašanjeKorisnika


DataProperty: IzgledKorisnikaPrimjeren

    Annotations:
        ace_lexicon:TV_vbg "TjelesniIzgledBezUtjecajaed",
        ace_lexicon:TV_sg "TjelesniIzgledBezUtjecajas",
        rdfs:comment "Kosa Brada itd"^^xsd:string,
        ace_lexicon:TV_pl "TjelesniIzgledBezUtjecaja"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava
```

```
    Range:
        xsd:string


DataProperty: DimenzijeTijelaIzrazene

    Annotations:
        ace_lexicon:TV_sg "TjelesneDImenzijeUtjecus",
        ace_lexicon:TV_pl "TjelesneDImenzijeUtjecu",
        ace_lexicon:TV_vbg "TjelesneDImenzijeUtjecued"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        xsd:string


DataProperty: UvjetiKoristenjaNeUtjecu

    Annotations:
        ace_lexicon:TV_sg "UvjetiKoristenjaNeUtjecus",
        ace_lexicon:TV_pl "UvjetiKoristenjaNeUtjecu",
        ace_lexicon:TV_vbg "UvjetiKoristenjaNeUtjecued"

    Characteristics:
        Functional

    Domain:
        Ima some KarakteristikaKorisnikaBiometrijskogSustava

    Range:
        xsd:string


DataProperty: PouzdanostSoftveraUnutarPodrucjaPouzdanosti

    Annotations:
        ace_lexicon:TV_sg "SoftverPouzdans",
        ace_lexicon:TV_vbg "SoftverPouzdaned",
        ace_lexicon:TV_pl "SoftverPouzdan",
        ace_lexicon:CN_sg "SoftverPouzdan",
        ace_lexicon:CN_pl "SoftverPouzdans"

    Characteristics:
        Functional

    Domain:
        Ima some SoftverPouzdan

    Range:
        xsd:string

    DisjointWith:
        PouzdanostSoftveraIzvanPodrucjaPouzdanosti
```

REFERENCE

[1] A.-M. Moore, “Biometric technologies -- an introduction,” *Biometric Technol. Today*, vol. 15, no. 1, pp. 6–7, 2007.

[2] M. Schatten, M. Bača, and M. Čubrilo, “Towards a General Definition of Biometric Systems,” *IJCSI Int. J. Comput. Sci. Issues*, vol. 7, no. 4, p. 1, 2010.

[3] K. L. Jacobsen, “Biometric as security technology : Expansion amidst fallibility,” Vesterkopi AS, Strandgade 56, DK-1401 Copenhagen, Denmark, 2012.

[4] B. M. P. Down and R. J. Sands, “Biometrics: An Overview of the Technology, Challenges and Control Considerations,” *Inf. Syst. Control J.*, vol. 4, 2004.

[5] Z. Ćosić, J. Ćosić, and M. Bača, “Biometric System Vulnerability as a Compromising Factor for Integrity of Chain of Custody and Admissibility of Digital Evidence in Court of Justice: Analysis and Improvement Proposal,” *J. Inf. Organ. Sci. - JIOS*, vol. 38, no. 1, pp. 11–33, 2014.

[6] F. Deravi, “Biometric Standards,” in *Biometric Technology Today*, vol. 14, no. 1, Springer, 2007, pp. 165–175.

[7] “Biometrics and Standards ITU-T Technology watch report,” 2009.

[8] M. D. Femila and A. A. Irudhayaraj, “Biometric system,” *Retina*, vol. 1, no. 43, pp. 152–156, 2011.

[9] J. (UAM. Galbally, J. (UAM) Fierrez, A. (IDIAP) Anjos, S. (IDIAP) Marcel, N. (UNIS) Poh, C. C. (UNIS) HO, and J. (MORPHO) Bringer, “Biometrics Evaluation and Testing,” Bruxelles, 2012.

[10] F. Podio, “Published Biometric International Standards,” 2010.

[11] J. N. Pato, L. I. Millett, and F. Street, “Biometric Recognition Challenges and opportunities,” The National Academies Press; 500 Fifth Street, N.W. Washington D.C. 20001, Washington D.C., 2010.

[12] M. Ushold and M. Gruninger, “Ontologies: Principles, Methods and Applications,” *Knowl. Eng. Rev.*, vol. 11, no. 2, 1996.

[13] R. Ryan, “The importance of biometric standards,” *Biometric Technol. Today*, vol. 2009, no. 7, pp. 7–10, 2009.

[14] National Science and Technology Council Subcommittee on Biometrics and Identity Management, “The National Biometrics Challenge,” 2011.

[15] V. Žugaj, M., Dumičić, K., Dušak, *Temelji znanstvenoistraživačkog rada, metodologija i metodika*. Varaždin: TIVA i FOI, 2006, p. 323.

[16] J. W. Creswell, *Research Design - Qualitative, Quantitative and Mixed Methods Approaches*, Third Edit. Lincoln: SAGE Publications, Inc, 2009, p. 296.

[17] R. Zelenika and S. Zelenika, “Klasifikacija znanosti u fokusu metodologije I tehnologije znanstvenoga istraživanja,” in *Pomorski zbornik vol. 44*, 2007, pp. 11–39.

[18] T. Lawson, “A conception of ontology,” *Mimeogr. Univ. Cambridge*, pp. 1–24, 2004.

[19] W. Approach, R. Brumnik, I. Podbregar, and T. Ivanuša, “Reliability of Fingerprint Biometry,” in *Biometric Systems,Design and Applications*, 2011.

[20] U. Mike and M. Gruninger, “Ontologies:Principles,Methods and Application,” *Knowl. Eng. Rev.*, vol. 11, no. 2, 2006.

[21] O. Corcho, M. Fernández-lópez, A. Gómez-pérez, and A. López-, “Building legal ontologies with METHONTOLOGY and WebODE,” *Law Semant. Web Lect. Notes Comput. Sci.*, vol. 3369, pp. 142–157, 2005.

[22] N. F. Noy and D. L. Mcguinness, “Ontology Development 101 : A Guide to Creating Your First Ontology,” 2001.

[23] N. F. Noy, A. Chugh, W. Liu, and M. A. Musen, “A Framework for Ontology Evolution in Collaborative Environments,” in *ISWC’06 Proceedings of the 5th international conference on The Semantic Web*, 2006, pp. 544–558.

[24] S. Tartir, B. I. Arpinar, and P. A. Sheth, “Ontological evaluation and validation,” in *Theory and applications of Ontology: Computer applications*, R. Poli, Ed. Springer, 2010, pp. 115–130.

[25] J. L. Wayman, “A generalized biometric identification system model,” in *Conference Record of the ThirtyFirst Asilomar Conference on Signals Systems and Computers Cat No97CB36136*, 1997, vol. 1, pp. 291–295.

[26] C. Tilton, “Biometric Standards – An Overview,” 2006.

[27] M. Schatten, “Zasnivanje otvorene ontologije odabranih segmenata biometrijske znanosti,” FOI (Varaždin), 2007.

[28] Z. Cosic, J. Cosic, and M. Baca, “Additive model of reliability of biometric systems with exponential distribution of failure probability,” *IJCSI Int. J. Comput. Sci. Issues*, vol. 9, no. 6, pp. 1–4, 2011.

[29] Z. Cosic, J. Cosic, and M. Baca, “Recovery function of Components of Additive Model of Biometric System Reliability in UML,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 9 No.7, no. ISSN 1947–5500, pp. 1–4, 2011.

[30] a. Rattani, N. Poh, and F. Roli, “Critical analysis of adaptive biometric systems,” *IET Biometrics*, vol. 1, no. 4, pp. 179–187, Dec. 2012.

[31] W.-L. Wang, D. Pan, and M.-H. Chen, “Architecture-based software reliability modeling,” *J. Syst. Softw.*, vol. 79, no. 1, pp. 132–146, 2006.

[32] D. Bhattacharyya, R. Ranjan, F. A. A, and M. Choi, “Biometric Authentication : A Review,” *Int. J. Serv. Sci. Technol.*, vol. 2, no. 3, pp. 13–28, 2009.

[33] N. Poh, J. Kittler, and A. Motivation, "A Unified Framework for Biometric Expert Fusion Incorporating Quality Measures," *Pattern Anal. Mach. Intell. IEE Trans. Biometric Compend. IEEE*, vol. 34, no. 1, pp. 1–14, 2012.

[34] V. De Rada, "Measure and control of non-response in a mail survey," *Eur. J. Mark.*, vol. 39, no. 1, pp. 16–32, 2005.

[35] M. Gomez-Barrero, J. Galbally, A. Morales, M. a. Ferrer, J. Fierrez, and J. Ortega-Garcia, "A novel hand reconstruction approach and its application to vulnerability assessment," *Inf. Sci. (Ny).*, vol. 268, pp. 103–121, Jun. 2014.

[36] J. Richter, N. Kuntze, and C. Rudolph, "Security digital evidence," *... Approaches to Digit. ...*, pp. 119–130, 2010.

[37] J. C. Laprie and K. Kanoun, "X-ware reliability and availability modeling," in *IEEE Transactions on Software Engineering*, 1992, vol. 18, no. 2, pp. 130–147.

[38] D. Hamlet, D. Mason, and D. Woit, "Theory of Reliability Based on Components," in *Reflection in Practice 3rd International Workshop on ComponentBased Software Engineering*, 2000, pp. 361–370.

[39] W. Wang and M. Chen, "An Architecture-Based Software Reliability Model Component-Based Reliability Modeling Style-based Reliability Modeling," *J. Syst. Softw.*, vol. 79, no. 1, pp. 132–146, 2006.

[40] P. Popic, "The Impact of Error Propagation on Software Reliability Analysis of Component-based Systems," College of Engineering at West Virginia University, 2005.

[41] D. Hong, T. Gu, and J. Baik, "A UML Model Based White Box Reliability Prediction to Identify Unreliable Components," *2011 Fifth International Conference on Secure Software Integration and Reliability Improvement Companion*. IEEE, pp. 152–159, 2011.

[42] M. Gomez-Barrero, J. Galbally, and J. Fierrez, "Efficient software attack to multimodal biometric systems and its application to face and iris fusion," *Pattern Recognit. Lett.*, vol. 36, pp. 243–253, Jan. 2014.

[43] A. Taweel and G. Tyson, "Prediction of Non- Functional Properties of Service-Based Systems: A Software Reliability Model," in *Engineering Reliable Service Oriented Architecture Managing Complexity and Service Level Agreements*, N. Milanovic, K. Klinger, J. Gamon, K. Glazewski, and N. Pronio, Eds. 2011.

[44] P. Grother and E. Tabassi, "Performance of biometric quality measures.," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 531–43, Apr. 2007.

[45] L. Stan Z, *Encyclopedia of Biometrcs*, Chinese ac. Springer-Verlag, NewYork, 2009, p. 778.

[46] T. D. F. Pereira and M. De Martino, "Can face anti-spoofing countermeasures work in a real world scenario ?," in *Biometrics (ICB), 2013 International Conference on Biometrics Compendium, IEEE*, 2013, pp. 1–8.

[47] M. Theofanos, B. Stanton, and C. A. Wolfson, "Usability & Biometrics: Ensuring Successful Biometric Systems," National Institute of Standards & Technology Information Access Division Information Technology Lab, Gaithersburg, MD 20899, 2008.

[48] T. Finin, P. Reddivari, R. S. Cost, and J. Sachs, “Swoogle : A Search and Metadata Engine for the Semantic Web,” in *ACM conference on Information and knowledge management*, 2004, pp. 652–659.

[49] Z. Ćosić, “Sustav dinamičko modeliranje tehničkog sustava brodskog kompresora,” 2007.

[50] L. S. Musolino and T. R. Conrad, *Simplified Weibull modeling of component early life reliability*. 1988.

[51] A. Schottl, *A reliability model of a system with dependent components*, vol. 45, no. 2. 1996, pp. 267–271.

[52] K. Goseva-Popstojanova and K. S. Trivedi, “Arhitecture based approach to reliability assessment of software systems,” *Perform. Eval.*, vol. 45, pp. 2–3, 2001.

[53] C.-H. Hu, X.-S. Si, and J.-B. Yang, “System reliability prediction model based on evidential reasoning algorithm with nonlinear optimization,” *Expert Syst. Appl.*, vol. 37, no. 3, pp. 2550–2562, 2010.

[54] L.-N. Qin, *Software reliability prediction model based on PSO and SVM*. IEEE, 2011, pp. 5236–5239.

[55] I. N. Reliability, “Toward an effective software reliability evaluation,” *Proc. 3rd Int. Conf. Softw. Eng.*, p. 46{\textendash}55, 1978.

[56] Z. Lai-shun, H. Yan, and L. Zhong-wen, *Building Markov chain-based software reliability usage model with UML*. IEEE, 2011, pp. 548–551.

[57] D. Marquez, M. Neil, and N. Fenton, “A new Bayesian Network approach to Reliability modelling,” 2006.

[58] H. Langseth, “Bayesian Networks in Reliability : Some Recent Developments,” *Reliab. Eng. Syst. Saf.*, vol. 92, no. 1, pp. 92–108, 2007.

[59] E. Chiodo and G. Mazzanti, *Bayesian reliability estimation based on a Weibull stress-strength model for aged power system components subjected to voltage surges*, vol. 13, no. 1. 2006, pp. 935–937.

[60] A. W. Moore, “Bayes Nets for representing and reasoning about uncertainty What we ’ ll discuss,” 2001.

[61] H. Ý. Singh, V. Þ. Cortellessa, B. Þ. Cukic, E. Ý. Gunel, and V. Þ. Bharadwaj, “A Bayesian Approach to Reliability Prediction and Assessment of Component Based Systems £ Ý Department of Statistics,” in *Proceedings of the 12th International Symposium on Software Reliability Engineering (ISSRE’ 01)*, 2001.

[62] Q. Zheng, *Software Reliability Prediction Model Based on Relevance Vector Machine*, vol. 1. IEEE, 2010, pp. 317–320.

[63] S. S. Gokhale and V. B. Mendiratta, “Architecture-Based Assessment of Software Reliability,” *2008 The Eighth International Conference on Quality Software*. Ieee, pp. 444–444, 2008.

[64] J. L. Horowitz and E. Mammen, “Nonparametric Estimation of an Additive Model With a Link Function,” *Ann. Stat.*, vol. 32, no. 6, pp. 2412–2443, 2005.

[65] M. L. Shooman and A. K. Trivedi, *A Many-State Markov Model for Computer Software Performance Parameters*, vol. R-25, no. 2. 1976.

[66] K. Krishna Mohan, A. K. Verma, A. Srividya, and L. Papic, “Integration of black-box and white-box modeling approaches for software reliability estimation,” *Int. J. Reliab. Qual. Saf. Eng.*, vol. 17, no. 3, pp. 261–273, 2010.

[67] S. Yacoub, B. Cukic, and H. H. Ammar, “A scenario-based reliability analysis approach for component-based software,” in *Ieee Transactions On Reliability*, 2004, vol. 53, no. 4, pp. 465–480.

[68] M. Xie and C. Wohlin, “An additive reliability model for the analysis of modular software failure data,” in *Proceedings of Sixth International Symposium on Software Reliability Engineering ISSRE95*, 1995, pp. 188–194.

[69] Optimum Biometric Labs, “Reliability , Availability and Maintainability in Biometric Applications Delivering Quality of Service that customer wants,” 2008.

[70] K. Kryszczuk, J. Richiardi, P. Prodanov, and A. Drygajlo, “Reliability-Based Decision Fusion in Multimodal Biometric Verification Systems,” *EURASIP J. Adv. Signal Process.*, vol. 2007, no. 1, p. 086572, 2007.

[71] M. Lil, Y. Wei, D. Desovski, H. Nejad, S. Ghose, B. Cukic, and C. Smidts, “Validation of a methodology for assessing software reliability,” in *15th International Symposium on Software Reliability Engineering*, 2004, pp. 66–76.

[72] S. Stoic, “Primjena biometrijskih metoda u sigurnosnom menadžmentu zračnog prometa,” 2007.

[73] B. Garbinato, “An Open Framework for Reliable Distributed Computing,” *J. ACM Comput. Surv.*, vol. 32, no. 1es, p. Art.nr.22, 2003.

[74] G. C. C. J, “Performance Analysis of Multimodal Biometric System Authentication,” *Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 3, pp. 290–296, 2009.

[75] U. D. C. Basse-normandie, “Evaluation of biometric systems : a study of users ’ acceptance and satisfaction Mohamad El-Abed *, Romain Giot , Baptiste Hemery and Christophe Rosenberger,” *Inderscience Int. J. Biometrics*, vol. 1, no. 1, pp. 1–26, 2012.

[76] B. Vukelić, “Evaluacija biometrijskih karakteristika pomoću AHP metode,” FOI Varaždin, 2009.

[77] IEEE, *Certified Biometrics Professional (CBP) Program*, vol. 3. 2013, p. 54.

[78] M. El-abed, C. Charrier, and C. Rosenberger, “Evaluation of Biometric Systems Evaluation of Biometric Systems,” *Inderscience Int. J. Biometrics*, vol. 1, no. 1, pp. 1–27, 2012.

[79] W. Lawrence and S. Sankaranarayanan, “Application of Biometric Security in Agent based Hotel Booking System - Android Environment,” *Int. J. Inf. Eng. Electron. Bus.*, vol. 4, no. 3, pp. 64–75, Jul. 2012.

[80] H. Chu, L. Wu, H. Yu, and J. Park, “Digital Trails Discovering of a GPS Embedded Smart Phone-Take Nokia N78 Running Symbian S60 Ver 3.2 for Example,” *Secur. Trust Comput. Data …*, vol. 187, pp. 41–49, 2011.

[81] A. Rattani and N. Poh, “Biometric System Design Under Zero and Non-Zero Effort Attacks,” in *Biometrics (ICB), 2013 International Conference on Biometrics Compendium, IEEE*, 2013, pp. 1–8.

[82] N. Y. Liu, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*. Routledge, 2013, p. 296.

[83] U. Ani, G. Epiphaniou, and T. French, “A Novel Evidence Integrity Preservation Framework (EIPF) for Virtualised Environments: A Digital Forensic Approach,” *Second Int. Conf. …*, 2013.

[84] S. E. and E. Kukula, “A Definitional Framework for the Human-Biometric Sensor Interaction Model,” in *Proceedings of SPIE - The International Society for Optical Engineering ed, Society of Photo-Optical Instrumentation Engineers*, 2010, pp. 67–76.

[85] S. Elliott, “Evolution of the Human Biometric Sensor Interaction,” in *International Biometric Performance Testing Conference (ICBP 2012),* 2012.

[86] M[a] Belén Fernández Saavedra, “Evaluation Methodologies for Security Testing of Biometric Systems beyond Technological Evaluation,” UNIVERSIDAD CARLOS III DE MADRID, 2013.

[87] et al. Belen Fernandez-Saavedra, Raul Sanchez-Reillo, Judith Liu-Jimenez, “Common Criteria and Biometric Performance Testing,” in *International Biometric Performance Testing Conference (ICBP 2012)*, 2012.

[88] et al. Belen Fernandez-Saavedra, Raul Sanchez-Reillo, Judith Liu-Jimenez, “Guidelines for Applying AGD and ATE Testing Activities to Biometric Systems,” in *International Common Criteria Conference (ICCC),* 2012.

[89] and S. J. E. E. P. Kukula, M. J. Sutton, “The Human Biometric-Sensor Interaction Evaluation Method: Biometric Performance and Usability Measurements,” in *IEEE Transactions on Instrumentation and Measurement*, 2010, pp. 784–791.

[90] M. E. and M. Fairhurst, “A methodological framework for investigating age factors on the performance of biometric systems,” in *Proceedings of the on Multimedia and security, ACM*, 2012.

[91] M. Erbilek and M. Fairhurst, “Framework for managing ageing effects in signature biometrics, Biometrics,” in *IET, 1(2),* 2012, pp. 136–147.

[92] R. B. and S. P. A. Jain, *Biometrics: Personal Identification in Networked Society*. 2002, p. 419.

[93] A. J. M. and J. L. Wayman, *Best Practices in Testing and Reporting Performance of Biometric Devices Version 2.01*, vol. National P. 2002.

[94] et al. J. L. Wayman, A. K. Jain, D. Maltoni, *Biometric Systems: Technology, Design and Performance Evaluation*. Springer-Verlag, NewYork, 2004, p. 300.

[95] T. D. and Y. Neil, *Biometric Systems and Data Analysis. Design, Evaluation, and Data Mining*. Springer-Verlag, NewYork, 2009, p. 158.

[96] M. Madonna, G. Martella, L. Monica, E. P. Maini, and L. Tomassini, "THE HUMAN FACTOR IN RISK ASSESSMENT : METHODOLOGICAL COMPARISON BETWEEN HUMAN RELIABILITY ANALYSIS TECHNIQUES," *Prev. today*, vol. 5, no. 1, pp. 67–83, 2009.

[97] M. Pollit and A. Whiteledge, "Exploring big Haystack,Data Mining and Knowledge ManagementNo Title," *Adv. Digit. forensic II IFIP*, 2006.

[98] H. Chawla and H. Xu, "A Real-Time Reliability Model for Ontology-Based Dynamic Web Service Composition," in *A Real-time Reliability Model for Ontology-based Dynamic Web Service Composition: A Thesis in Computer Science*, 2011, pp. 153–158.

[99] M. Bača, M. Schatten, and K. Rabuzin, "Towards an open biometric ontology," *J. Inf. Organ. Sci.*, vol. Volume 31, no. 1, pp. 1–11, 2007.

[100] R. Jasper and M. Uschold, "A framework for understanding and classifying ontology applications," *Twelfth Work. Knowl. Acquis. Model. Manag. KAW'99*, 1999.

[101] T. R. Gruber, "A Translation Approach to Portable Ontology Specifications," *Knowl. Creat. Diffus. Util.*, vol. 5, pp. 199–220, 1993.

[102] N. Guarino, "Formal Ontology and Information Systems," in *Proceedings of FOIS'98*, 1998, no. June, pp. 3–15.

[103] W. N. Borst, "Construction of Engineering Ontologies for Knowledge Sharing and Reuse," *Cent. Telemat. Inf. Technol.*, no. University of Twenty, Enschede, The Netherlands, 1997.

[104] N. Guarino and P. Giaretta, "Ontologies and Knowledge Bases: Towards a Terminological Clarification," no. IOS Press, Amsterdam, 1995.

[105] A. Lozano-tello and U. De Extremadura, "ONTOMETRIC : A Method to Choose the Appropriate Ontology," *J. Database Manag.*, vol. 15, no. June, pp. 1–18, 2004.

[106] M. Swimmer, "Towards An Ontology of Malware Classes," *Online] January*, pp. 1–16, 2008.

[107] M. Fernandez, A. Gomez-p, and N. Juristo, "METHONTOLOGY : From Ontological Art Towards Ontological Engineering," *AAAI Tech. Rep. SS-97-06*, vol. 06, pp. 33–40, 1997.

[108] O. M, "SWRL Language FAQ," *ProtegeWiki*, 2013. .

[109] A. Gangemi, C. Catenacci, M. Ciaramita, and J. Lehmann, "A theoretical framework for ontology evaluation and validation," in *Proceedings of Semantic Web Workshop SWAP*, 2005.

[110] D. Vrandecic, "Ontology Evaluation," 2010.

[111] M. Silva, E. Elias, E. Costa, I. I. Bittencourt, H. Barros, L. Dias, A. Pedro, and D. Véras, "Combining Methontology and Ontology Driven Approach to Build an Educational Ontology," *IEEE Multidiscip. Eng. Educ. Mag.*, vol. 6, no. 3, 2011.

[112] S. Tartir, “Ontology-Driven Question Answering And Ontology Quality Evaluation,” Universitiy of Georgia, 2009.

[113] A. Gangemi, C. Catenacci, M. Ciaramita, and J. Lehmann, “Modelling Ontology Evaluation and Validation,” in *3rd European Semantic Web Conference (ESWC2006)*, 2006.

[114] Ó. Corcho, A. Gómez-pérez, D. J. Guerrero-rodríguez, A. Ruiz-cristina, T. Sastre-toral, and M. C. Suárez-figueroa, “Evaluation experiment of ontology tools ’ interoperability with the WebODE ontology engineering workbench,” in *Proceedings of the 2nd International Workshop on Evaluation of Ontology-based Tools held at the 2nd International Semantic Web Conference ISWC 2003*, 2003.

[115] N. K.NANDHAKUMAR, U. AGARWAL, and F. H., “Use of AFF4 ‘ Chain of Custody ’ - Methodology for Foolproof Computer Forensics Operation,” in *International Journal of Communication and Networking System Volume*, 2012, no. June, pp. 49–57.

[116] I. Palmisano and O. A. Team, “The Rough Guide to the OWL API,” in *OWLED 2011*, 2011.

[117] A. Meech, “Business Rules Using OWL and SWRL,” *Adv. Semant. Comput.*, vol. 2, pp. 23–31, 2010.

[118] W. M. Submission, “SWRL: A Semantic Web Rule Language Combining OWL and RuleML.” .

[119] E. Sirin, B. Parsia, B. C. Grau, A. Kalyanpur, and Y. Katz, “Pellet: A practical OWL-DL reasoner,” *Web Semant. Sci. Serv. Agents World Wide Web*, vol. 5, no. 2, pp. 51–53, Jun. 2007.

[120] J. Ćosić, “Izgradnja otvorenog okvira za uspostavu i očuvanje lanca dokaza u forenzičkoj analizi digitalnih dokaza,” University of Zagreb, 2014.

[121] K. Clark, B. Parsia, M. Grove, E. Sirin, and M. Smith, “Pellet: Owl 2 reasoner for java,” ... *http//clarkparsia. com/pellet*, 2011.

[122] P. S. Kaliappan and H. Koenig, “An Approach to Synchronize UML-Based Design Components for Model-Driven Protocol Development,” *2011 IEEE 34th Software Engineering Workshop*. IEEE, pp. 27–35, 2011.

[123] E. Gonz and C. Garc, “An Open Source Java Framework for Biometric Web Authentication based on BioAPI,” *Knowledge-Based Intell. Inf. Eng. Syst. Lect. Notes Comput. Sci.*, vol. 4693, pp. 809–815, 2007.

[124] M. Horridge and S. Bechhofer, “The owl api: A java api for owl ontologies,” *Semant. Web*, vol. 4, no. 1, pp. 1–11, 2011.

[125] V. Cross and A. Pal, “OntoCAT: An Ontology Consumer Analysis Tool and Its Use on Product Services Categorization Standards,” in *5th International semantic web conference ISWC, Athens*, 2006.

[126] C. Brewster, H. Alani, S. Dasmahapatra, P. Street, and C. B. Y. Wilks, “Data Driven Ontology Evaluation,” in *International conference on language resources and evaluation (LREC 2004)*, 2004.

[127] D. Vrandečić, “Ontology Evaluation,” Fakultaet fuer Wirtschaftswissenschaften des Karlsruher Instituts fuer Technologie (KIT), 2010.

[128] N. Fanizzi, C. D’Amato, and F. Esposito, “DL-FOIL concept learning in description logics,” *Inductive Log. Program.*, vol. 5194, pp. 107–121, 2008.

[129] I. Palmisano, V. Tamma, L. Iannone, T. Payne, and P. Doran, “Dynamic ontology evolution in open environments,” *Comput. Sci.*, vol. 6423, pp. 122–132, 2010.

[130] J. Pak and L. Zhou, “A Framework for Ontology Evaluation,” *Explor. Gd. Challenges Next Gener. E-bus.*, vol. 52, pp. 10–18, 2011.

[131] S. Tartir and I. B. Arpinar, “Ontology Evaluation and Ranking using OntoQA,” *Int. Conf. Semant. Comput. (ICSC 2007)*, pp. 185–192, Sep. 2007.

[132] S. Tartir, I. B. Arpinar, M. Moore, A. P. Sheth, and B. Aleman-Meza, “OntoQA: Metric-Based Ontology Quality Analysis,” in *IEEE Workshop on Knowledge Acquisition from Distributed, Autonomous, Semantically Heterogeneous Data and Knowledge Sources*, 2005.

ŽIVOTOPIS

Zoran Ćosić rođen je 1967. godine u Mostaru u Bosni i Hercegovini, gdje je završio osnovnu školu. Srednju pomorsku školu završava 1986. te iste godine upisuje Vojnu pomorsku akademiju koju završava 1990 godine. Iste godine u počinje raditi za kompaniju OPI s.r.l. Pesaro, Italija u kojoj na različitim funkcijama ostaje do 2004. kada obnaša funkciju izvršnog direktora.

Iste godine pokreće u Splitu tvrtku Statheros d.o.o. za poslovno savjetovanje čiji je djelatnik i direktor do danas.

2005. godine upisuje poslijediplomski stručni studij na Pomorskom Fakultetu u Splitu i isti dovršava 2007. godine.

Od 2008. godine polaznik je Poslijediplomskog doktorskog studija na Fakultetu organizacije i informatike u Varaždinu.

Uposlen je u tvrtci Statheros d.o.o. te direktor te voditelj preko 200 projekata standardizacije poslovnih procesa na teritoriji RH, BiH i Republike Italije.

Od 2008. godine postaje vanjski suradnik certifikacijskog tijela Bureau Veritas kao Lead Auditor za standarde ISO 9001, ISO 14001, OHSAS 18001, ISO 27001 i ISO 50001 sa kojima realizira preko 300 audit dana na teritoriju RH, BIH i CG.

Područja interesa su mu biometrijski sustavi u domeni proučavanja pouzdanosti operativne funkcije te sustavi upravljanja u domeni informacijske sigurnosti .

Suradnik je „Centra za biometriju“ FOI-a u Varaždinu .

Sretno je oženjen i otac je kćeri Doris i sina Marca.

POPIS RADOVA

1. Ćosić, Z., Ćosić, J., Bača, M.: Biometric system reliability as important factor of influence on Chain of custody of digital evidence , CECIIS-Varaždin, 2014
2. Ćosić, Z., Ćosić, J., Bača, M.: Biometric System Vulnerability as a Compromising Factor for Admissibility of Digital Evidence: Analysis and Improvement Proposal, JIOS-Journal of Information and Organization Science, VOL38-NO1, Croatia, 2014
3. Ćosić, Z., Ćosić, J., Bača, M. (2013): Towards on modelling prediction of biometric system reliability, CECIIS-Varaždin, 2013
4. Bača, M., Ćosić, J., Ćosić, Z.: Forensic analysis of Social Networks (case study), ITI - Cavtat, 2013
5. Ćosić, J., Ćosić, Z.: Chain of Custody and Life Cycle of Digital Evidence, JCTA - Journal of Computer Technology and Application 3, p.p. 126-129, USA, 2012
6. Ćosić, Jasmin; Ćosić, Zoran; Bača, Miroslav Knowledge Sharing and Reuse in Digital Forensic Domain a Review // Proceeding of ITIS 2012, Novo Mesto
7. Ćosić, J., Ćosić, Z. (2012): Business impact analysis & methodology of risk analysis as the most important aspects within operational continuity process defining, TELFOR – Beograd, 2012
8. Ćosić, J., Ćosić, Z., Bača, M.: Chain of digital evidence based model of digital forensic investigation process, IJCSIS- International Journal of Computer Science & Information Security 2011, VOL9-NO7, USA, 2011 (best paper award).
9. Ćosić, J., Ćosić, Z., Bača, M.: Modeling Digital Evidence Management and Dynamics Using Petri Nets, JCTA - Journal of Computer Technology and Application, USA, 2011
10. Ćosić, J., Ćosić, Z., Bača, M.: Ćosić, J., Ćosić, Z., Bača, M.: An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence, JIOS-Journal of Information and Organization Science, VOL35-NO1,Croatia, 2011
11. Ćosić, Z., Ćosić, J., Bača, M.: Additive Model of Reliability of Biometric Systems with Exponential Distribution of Failure Probability, IJCSIS- International Journal of Computer Science & Information Security 2011, VOL9-NO6, USA, 2011 (best paper award).

12. Ćosić, Z., Ćosić, J., Bača, M.: Recovery function of Components of Additive model of Biometrics System Reliability in UML , IJCSIS- International Journal of Computer Science & Information Security 2011, VOL9-NO7, USA, 2011
13. Ćosić, J., Ćosić, Z., Bača, M.: (Il)legal aspects of digital antiforensics , CECIIS 2011, Varaždin, Croatia, 2011
14. Ćosić, Z., Ćosić, J., Bača, M. (2011): Implementation as Integration Factor Of Business Consulting And Knowledge Management , INFOTEH, Jahorina, B&H, Vol.10, 2011
15. Ćosić, J., Ćosić, Z. : The Necessity of Developing an Digital Evidence Ontology, CECIIS 2012 - Central European Conference on Information and Intelligent Systems - University of Zagreb – Croatia, 2010
16. Ćosić, J., Ćosić, Z., Bača, M. (2010): Digital antiforensic – manipulation with digital forensic, TELFOR – Beograd, Serbia, 2010
17. Ćosić, Jasmin; Ćosić, Zoran: "Druga strana" socijalnih mreža // Korisnička konferencija - CUC 2010. Split, 2010.