Univerza v Mariboru

Fakulteta za organizacijske vede

Doktorska disertacija

UČINKOVITOST IN ZANESLJIVOST BIOMETRIČNEGA SISTEMA PRI OSEBNI IDENTIFIKACIJI

Kranj, Maj 2011

Kandidat: Robert BRUMNIK
Mentor: red. prof. dr. Zvone BALANTIČ

Kar zapuščaš za seboj, ni vklesano v kamnu, temveč je vtkano v življenja drugih.

PERIKLEJ

POSEBNA ZAHVALA

Zahvaljujem se dr. Vojanu Rozmanu za nesebično pomoč, strokovne in konstruktivne usmeritve in nasvete pri procesu nastajanja tega dela.

Še posebej se zahvaljujem za prijazno podporo, dobro voljo in pozitivno energijo, ki mi je pomagala na poti do cilja.

ZAHVALA

Zahvaljujem se mentorju red. prof. dr. Zvonku Balantiču za vso strokovno pomoč, spodbudo in koristne nasvete pri izdelavi disertacije.

Zahvala gre tudi vsem profesorjem Fakultete za organizacijske vede, ki so mi kakorkoli pomagali v vseh letih, ko sem se kot raziskovalec uvajal v akademske in raziskovalne sfere.

Zahvala vsem, ki so kakorkoli prispevali k nastajanju tega dela.

POVZETEK

Biometrija se nanaša na identifikacijo osebe, na osnovi fizikalnih in vedenjskih značilnosti. Danes poznamo veliko biometričnih sistemov, ki temeljijo na prepoznavi teh, za vsakogar edinstvenih značilnosti. Nekateri od biometričnih sistemov vključujejo značilnosti: prstni odtisi, geometrija roke, glas, šarenica itd., ki se lahko uporabijo za osebno identifikacijo. Večina biometričnih sistemov temelji na odvzemu in primerjavi biometričnih značilnosti na osnovi katerih se izvede identifikacija. Študijo začnemo z zgodovinskim pregledom biometričnih in radiofrekvenčih identifikacijskih (RFID) metod ter raziskovalnega področja. Študijo nadaljujemo v smeri biometričnih metod na osnovi prstnih odtisov. Vsak biometrični sistem vključuje naslednje tri postopke: registracija, priprava odčitanega vzorca, in preverba ujemanja odčitanega vzorca s shranjenim digitaliziranim vzorcem v bazi podatkov. Optimizacija biometričnega sistema z nevronskimi mrežami rezultira v multi–biometričnih ali multimodalnih biometričnih sistemih. S tem postopkom združimo dve ali več biometričnih metod v obliki učinkovitejšega ter varnejšega biometričnega sistema.

Z raziskavo parametrov zanesljivosti in razpoložljivosti, ki vplivajo na učinkovitost identifikacijskega sistema v uporabi, preverjamo predpostavljene hipoteze. Povzetek dobljenih ocen parametrov zanesljivosti in razpoložljivosti biometričnega sistema, primerjamo s kartičnim sistemom. Izsledki raziskave kažejo, da je ocena časa do odpovedi (zanesljivost) biometričnega sistema z izračunom karakteristike $MTTF_S$=88,8 dneva in $MTTF_S$=76,5 dneva, za kartični sistem. Ocena časa popravila za biometrični sistem, z izračunom karakteristike $MTTR_S$=1,2 dneva in $MTTR_S$=2,1 dneva, za kartični identifikacijski sistem. Ocena razpoložljivosti biometričnega sistema z izračunom karakteristike A_S=0,987 in A_S=0,973 za kartični identifikacijski sistem.

Hipoteze, ki smo jih v doktorski nalogi predpostavili, z raziskavo v celoti potrdimo. V raziskavi obravnavan biometrični sistem, je glede na parametre in pogoje raziskave zanesljivejši in učinkovitejši, od kartičnega sistema in hkrati omogoča večjo pretočnost oseb.

V raziskavi smo razvili matematični model na osnovi »markovskih verig« za določevanje zanesljivosti in razpoložljivosti predstavljenega identifikacijskega sistema. Z aktualnimi razvojno raziskovalnimi projekti na tem področju, pa to študijo še empirično potrjujemo. Učinkovitost in zanesljivost sta pomembna dejavnika pri obravnavi in delovanju vseh biometričnih sistemov. Z raziskavo se osredotočamo na meritve v procesu delovanja biometričnih in RFID sistemov ter pojasnimo, kaj pomenijo dobljeni rezultati. V okviru raziskave navajamo pregled relevantnih standardov, ki služijo za določitev politike biometričnih ukrepov, varnostnih mehanizmov in uspešno ter kakovostno izvedbo identifikacije.

KLJUČNE BESEDE

pristopna kontrola, biometrija, RFID, učinkovitost, zanesljivost

EFFICIACY AND RELIABILITY OF BIOMETRIC SYSTEM FOR PERSONAL IDENTIFICATION

ABSTRACT

Biometrics refers to the identification of a person on the basis of physical and behavioural characteristics. Today we know a lot of biometric systems based on the identification of everyone's unique characteristics. Some biometric systems include the characteristics of: fingerprints, hand geometry, voice, iris, etc., and can be used for identification. Most biometric systems are based on the collection and comparison of biometric characteristics, which can provide identification. The study begins with a historical review of biometric and radio frequency identification (RFID) methods and research area. The study continues in the direction of biometric methods based on fingerprints. Each biometric system includes the following three processes: registration, preparation of sample, and readings of the sample. Finally, the system provides comparison of the measured sample with digitized samples stored in the database. The optimization of a biometric system with neural networks results in multi-biometric or multimodal biometric systems. This procedure combines two or more biometric methods in the form of more efficient and more secure biometric system.

With research on the parameters of reliability and availability, which affect the results of the biometric system in use, we test the hypothesis. The summary of the obtained results discusses the measured parameters of reliability and availability of the biometric system in comparison with the card identification system. The survey's findings for the estimated time to failure (reliability) of biometric system obtained by calculating the characteristics were $MTTF_S$=88,8 days and $MTTF_S$=76,5 days for the card identification system. The estimated time of repair for the calculation of biometric characteristics was $MTTR_S$=1,2 days and $MTTR_S$=2,1 days for the card identification system. The assessment of the availability of biometric system calculated the characteristics of A_S= 0,987 and A_S= 0,973 for the card identification system.

The survey fully confirmed the hypothesis. Biometric methods based on research parameters are both, more reliable and effective than card identification systems while enabling a greater flow of people.

During research, we carried out the »Markov chains« mathematical model for determining of the effectiveness of the identification system. With actual ongoing research and development projects in this area, this study has to be confirmed empirically. Efficiency and reliability are important factors in reading and operation of biometric systems. The research focuses on the measurement of activity in the process of biometric and RFID systems, and explains what the obtained result mean. The research gives a review of relevant standards, which are necessary to determine the policy of biometric measures, security mechanisms and successful implementation of quality identification process.

KEYWORDS

access control, biometry, RFID, efficiency, reliability

UDK: 005.336.3:004.89(043.3)

1 UVOD

Biometrija temelji na uporabi telesnih značilnosti, kot načinu identifikacije in nadzorovanja oseb (Fitzpatrick, 2002). Gre za proces zbiranja, procesiranja in shranjevanja podatkov o posameznikovih fizičnih in bioloških (vedenjskih) lastnostih z namenom identifikacije (Kovačič, 2006). Raziskovanje teh človeških lastnosti pa je pot k medsebojnemu ločevanju oseb (Trapečar in Robek, 2003). Beseda biometrija (biometry) izhaja iz dveh grških besed bios (življenje) in metrikos (meriti) (Prabhakar in drugi, 2003). Glede na Slovenski medicinski slovar (2009) je biometrija veda, ki uporablja merjenje in statistično analizo na vseh področjih biologije in kot sinonim uporablja izraz »biometrika«.

Prvi prstni odtisi so bili najdeni med izkopaninami starodavnih mest Jericho in Paphos iz 7000 l. pr. n. št. (Maier in Karageorghis, 1984). Za časa vladavine Hamurabija Babilonu v 19. st.pr.n.št., so prstne odtise uporabljali za pečate pogodb. Antični Egipt in Kitajska sta odigrala pomembno vlogo v razvoju biometrije (Ashbaugh, 1991). Izvor biometričnih podatkov lahko zasledimo že v 12. stoletju na Kitajskem. Angleški raziskovalec Barrow je v 18. stoletju zapisal, da so kitajski trgovci z odtisi stopal na papirju razlikovali otroke (Galton, 2003). Zanimivo je, da to prakso še danes uporabljajo v nekaterih delih sveta. Kasneje, v 19. stoletju, je antropolog Bertillon poskušal najti način za identifikacijo zločincev. Razvil je sistem imenovan »Bertillonage«, ki uporablja fizikalne značilnosti (telesne dimenzije), kot sredstvo za identifikacijo zločincev (Bhattacharyya in drugi, 2009). Ta sistem je lahko napačno identificiral zločinca, saj ima več oseb enake lastnosti, ki jih je Bertillon uporabljal za identifikacijo. Pomanjkljivosti Bertillonage sistema so v začetku 20. stoletja spodbudile Henrya, da razvije bolj zanesljive metode za odkrivanje kaznivih dejanj. Henry je temeljil na desetprstni klasifikaciji odtisov, kot najbolj natančnemu načinu identifikacije. Sprejet je tudi s strani policije v Scotland Yardu, kot glavni način identifikacije v kazenskih zadevah. Battley l. 1930 razvije prvi enoprstni sistem prstnih odtisov (Maver, 2004). Leta 1985, je postala aktualna ideja identifikacijskega sistema na osnovi prepoznave šarenice. Razvoj sega v leto 1993, leta 1994 je bil patentiran algoritem prepoznave šarenice in leto kasneje so postali dostopni prvi komercialni identifikacijski sistemi.

Definicije biometričnih izrazov v znanstveni literaturi se ne razlikujejo, so le izpeljanke osnovno oblikovanih definicij. V večini zapisov je terminologija standardizirana v skladu s harmoniziranim biometričnim slovarjem ISO/IEC JTC1/SC 37 N 2777 kjer je biometrični element (biometric element) merljiva fizična ali vedenjska značilnost, ki je uporabljena za prepoznavo posameznika. Značilke so elementi, na osnovi katerih lahko enolično identificiramo človeka (prstni odtis, roženica, šarenica, DNK). Biometrični vzorec (biometric sample) je neobdelan podatek, ki predstavlja biometrično značilnost končnega uporabnika, kot je zajet s strani biometričnega sistema. Biometrični podatek (biometric data) je informacija, ki je vzeta iz biometričnega vzorca in uporabljena ali za kreiranje šablone ali za primerjavo z že prej narejeno šablono (Bolle in drugi, 2004). Registracija ali vpis (enrollment) je proces zbiranja (odvzema) biometričnih vzorcev osebe, nadaljnje priprave in shranjevanje biometričnih reference predlog, ki predstavlja identiteto te osebo. Za biometrični vzorec, nad katerim se vrši proces identifikacije ali verifikacije,

so primerni le deli telesa, katerih karakteristike so specifične za vsakega posameznika, so s časom nespremenljive oz. stabilne in so merljive (Fefer, 2004).

Šablona (template) je podatek, ki predstavlja biometrično meritev posameznika in je tvorjena s pomočjo algoritma ter jo uporablja biometrični sistem za primerjavo z na novo vzetim biometričnim vzorcem (Woodward in drugi, 2003).

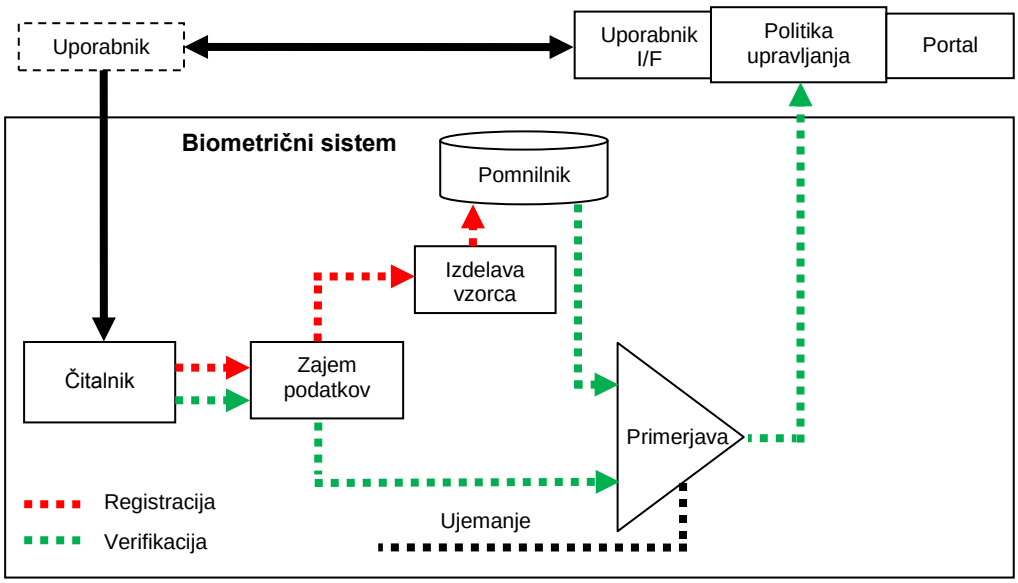
Biometrične metode so avtomatizirane metode prepoznave ljudi, temelječe na njihovih fizioloških ali/in vedenjskih značilnosti (Woodward in drugi, 2003). Beseda »avtomatizirane« je nujna za definicijo, ker bi brez nje opisovali tudi celo množico zelo običajnih, toda bistveno manj zanesljivih identifikacijskih tehnik kot je npr. fotografija ali črnilni prstni odtis na identifikacijski znački itd. Biometrične metode so avtomatizirane do stopnje, kot je avtomatiziran proces zajema vzorca, vzorčenja, primerjave zajetega vzorca s poprej pridobljenim vzorcem in algoritemske primerjave, ki omogoči rezultat (Jain in drugi, 2004).

Z biometrijo smo lahko identificirani skozi fizične značilnosti (obraz, oči, prstni odtis, DNK itd.) in biološke lastnosti (glas, podpis, hoja, dinamika tipkanja itd.). Biometrijo lahko uporabimo v dveh primerih: za identifikacijo ali prepoznavanje posameznika na osnovi primerjave z vsemi shranjenimi v bazi podatkov ter za verifikacijo (avtentikacijo) oz. potrditev, kjer v procesu identifikacije ugotovimo ali res gre za tisto osebo, za katero se izdaja. Poznamo različne načine ali modalnosti biometrične identifikacije in verifikacije oseb (Jain in drugi, 2002):

- Prstni odtisi so vzorci, prisotni na človeškem prstu in so edinstveni za vsakega človeka (razlikujejo se tudi glede na vsak prst).
- Prepoznavanje geometrije obraza je najbolj sprejemljiv biometrični podatek in je najbolj splošna metoda identifikacije, ki jo uporabljamo pri vizualni komunikaciji. Kljub temu pa se tudi ta tehnologija spopada z različnimi težavami, kot so procesi staranja, obrazno izražanje itd.
- Geometrija rok temelji na identifikaciji človeka glede na obliko roke, npr. velikost in širino prstov.
- Vsak posameznik ima edinstveno strukturo šarenice. Natančnost in hitrost sistemov, ki temeljijo na šarenici, sta obetavni, izvedljiv pa je tudi identifikacijski sistem velikega obsega. Vsaka šarenica je unikatna, podobno kot pri prstnem odtisu pa se tudi šarenici dvojčkov razlikujeta. Šarenico je zelo težko ponarediti, ugotavljanje umetnih dodatkov pa je dokaj enostavno. S spreminjanjem osvetlitve lahko še dodatno ugotovimo, ali se oko pravilno odziva, s tem pa, ali gre za živ objekt. Zajemanje slike šarenice je manj vsiljivo kot pri mrežnici, ker se šarenica lepo vidi tudi z razdalje nekaj metrov.
- Žilna sistema mrežnice levega in desnega očesa se močno razlikujeta, enak pojav zaznamo tudi pri levem in desnem prstnem odtisu.
- Preverjanje podpisa temelji na načinu pisanja, ki pa je velikokrat odvisen od trenutnega čustvenega in fizičnega stanja posameznika. Poznamo statično (le geometrijska oblika podpisa, npr. velikost in oblika črk) in dinamično (ne samo oblika podpisa, ampak tudi hitrost, način pisanja) verifikacijo podpisa.
- Prepoznavanje glasu je odvisno predvsem od kvalitete mikrofona in komunikacijskega kanala, prav tako pa tudi od posameznikovega zdravja (prehlad itd.), stresnih in emocionalnih situacij.

- Infrardeča toplotna identifikacija obraza in ostalih delov telesa – termogram: človeško telo oddaja toploto in ta vzorec toplotnih žarkov predstavlja značilnosti vsakega posameznika.
- Dinamika tipkanja: vsak posameznik na tipkovnico tipka na svojevrsten način. Ta dinamika temelji na časovnih presledkih med tipkanjem (Hocquet in drugi, 2005).
- Prepoznavanje hoje: svojevrstne način hoje, ki pa ni edinstvena za vsakega posameznika, vendar je zadostna značilnost za identificiranje. Seveda pa se skozi obdobja spreminja (pridobitev telesne teže, ob alkoholiziranosti itd.).
- Vonj: vsak posameznik izloča vonj, torej posebne značilnosti kemične sestave vonja.
- Biometrija ušesa je ločevanje glede na obliko in strukturo, vendar pa vsak posameznik nima edinstvenega ušesa (Rahman, 2007).
- DNK je zares edinstvena koda vsakega posameznika (razen enojajčnih dvojčkov, ki imata isti DNK vzorec).

Biometrični sistemi (slika 1.1) so v bistvu primerjalniki vzorcev in se zelo razlikujejo glede na princip delovanja (ne glede na tip karakteristike, ki jo pregledujemo) (BEM WG, 2002). Prepoznava osebe temelji na primerjanju binarne kode neke fiziološke lastnosti, s tisto kodo, ki je v napravi že shranjena (Mraović, 2003). Najprej je potrebno zajeti žive podatke z osebe. S pomočjo kompleksnih algoritmov sistem zajete podatke pretvori v binarno kodo, ki jo nato primerja s tisto v svojem spominu.



Slika 1.1: Poenostavljen biometrični sistem (BEM WG, 2002)

Danes se za primerjavo in analizo biometričnih vzorcev uporabljajo zelo izpopolnjene matematične metode z nevronskimi mrežami (LFA, AFP itd.). LFA je najbolj uporabljena metoda pri prepoznavi obraza, ki je v nekaj pogledih zelo podobna eigenface metodi, le da se je ta metoda bolj sposobna prilagajati spremebi videza osebe, spremebi svetlobe, spremembi pričeske, barvi kože in modnih dodatkov. AFP je najbolj okrnjena metoda, ki temelji na analizi enostavno določljivih razdalj in razmerij razdalj obraza (razdalja med očmi, ušesi, dolžino ustnic itd.).

Metodi sta uporabni za 1:N in 1-1 prepoznave (Mraović, 2003). Očitno je, da so fizične in vedenjske lastnosti bolj ali manj primerne za preverjanje identifikacije. Fizični identifikatorji so relativno stabilni, splošno nespremenljivi brez vpliva psiholoških dejavnikov, medtem ko so vedenjske lastnosti zelo odvisne od psiholoških dejavnikov oziroma psihičnega stanja opazovalca. Različne fizične ali vedenjske karakteristike rangiramo glede na osnovne lastnosti, ki naj bi jih imela dobra biometrična lastnost:

- univerzalnost (karakteristika določene osebe se nujno razlikuje od vseh ostalih, je edinstvena),
- stalnost (karakteristika se s časom ne spreminja),
- zbirnost (karakteristika se zbira na uporabniku prijazen način).

Najbolj pogosto so fizične karakteristike (biometrični vzorci) zajeti preko optičnega senzorja. V večini primerov so optični biometrični sistemi enostavni, saj vsebujejo izvor svetlobe, napravo za pozicioniranje biometrike in kamero. Optični filtri absorbirajo svetlobo določenih valovnih dolžin in prepuščajo potrebno, da prehaja na vzorec. V primeru, ko gre za odčitavanje prstnih odtisov in mrežnice je optika veliko bolj zahtevna, sistem šablon in algoritmov primerjave pa veliko bolj kompleksen. Sama tehnika zajema biometričnih lastnosti poteka preko čitalca, ki zajame karakteristično sliko osebka, ki naj bi bil identificiran (Prabhakar in drugi, 2003). To sliko pretvori v digitalni signal, ki jo nato sprocesiran v zapis ekvivalenten biometričnemu vzorcu. Nato sledi postopek primerjave med odčitano sliko in predhodno registriranim vzorcem. Primerjava med biometričnim vzorcem in dejanskim odčitkom pokaže, da ta dva nista nikoli popolnoma enaka. Vzrok temu je lahko različna postavitev senzorjev, spremembe okolja ali deformacije identificiranega osebka.

Vsaka izmed biometričnih metod ima svoje prednosti in slabosti, zato moramo pri izbiri sistema biti pozorni na parametre kakovosti od katerih je odvisno, ali bo identifikacijski sistem izpolnjeval zahteve pristopne kontrole. Biometrija dlani se sicer uporablja že vrsto za let, vendar je za splošno rabo neprimerna, saj se dlani med sabo ne razlikujejo dovolj. Prav tako okoli 5% ljudi nima čitljivega prstnega odtisa, bodisi zaradi genskih napak, zaradi obrabe, staranja ali nesreč. Prepoznavanje obraza temelji na 30 obraznih točkah, vendar tudi ta sistem ne deluje brezhibno. Modalnosti torej lahko imajo probleme omejene uporabnosti oziroma aplikativnosti, katerih rešitve iščemo v kombiniranju in optimiranju modalnosti v večmodalni biometrični sistem. Multibiometrični sistemi oziroma sistemi, ki uporabljajo multibiometrične metode, omogočajo dokaj veliko zanesljivost (Črnčec, 2004). Za ugotavljanje identifikacije, je tako najbolj primerno analiziranje DNK, šarenice in mrežnice. Ravno odčitavanje šarenice je dovolj zanesljiva metoda, kjer hkrati tudi ni potreben fizični stik kot npr. pri oddajanju prstnih odtisov. Za večjo verodostojnost identifikacije se raziskovalci nagibajo k multibiometričnim sistemom, torej kombinaciji različnih biometričnih metod. ZDA so za večino sistemov pristopne kontrole in identifikacije izbrale skeniranje prstnih odtisov in prepoznavanje obraza, temu sledi Evropa, tudi Slovenija z novimi potnimi listi zaradi zahtev ZDA. S preverjanjem več biometričnih podatkov hkrati (multimodalnost) se tako poveča zanesljivost preverjanja ljudi (Dorizzi, 2005).

Biometrični proces omogoča: kontrolo dostopa, identifikacijo, verifikacijo, pregledovanje, kontrolo časa prihoda in odhoda, kontrolo časa dostopa in uporabe določenega vira. Ne glede na dejavnik prepoznave je biometrični proces sestavljen

iz dveh delov. V prvem delu, ki ga imenujemo registracija, je oseba vpisana v biometrični sistem. V tem primeru biometrični identifikator prebere podatek s pomočjo senzorja. Ta pošlje signal v analogno digitalni pretvornik, kjer se oblikuje digitalna koda s pomočjo primernega algoritma. Koda za potrebno informacijo je po velikosti minimalna, sistem pa vsebuje celotno zajeto informacijo. Postopek se ponovi večkrat, da dobimo določeno povprečje, ki je neodvisno od naključnih variacij biometričnega vzorca. Biometrični vzorec ne dovoljuje rekonstrukcije originalnega signala s strani senzorja, ki lahko prostorsko zasedejo manj od 10 bajtov do nekaj kilobajtov. V bazo podatkov se zapiše določen biometrični vzorec identificiranega osebka in pripadajoč algoritem ali geslo. Drugi del biometričnega procesa je verifikacija ali identifikacija. Pri biometrični pregledni točki je biometrični senzor povezava za dostopanje baze podatkov (Chirillo in Blaul, 2003). Pride do odčitavanja biometričnih lastnosti (značilk) pregledovane osebe, katere biometrični sistem primerja z vpisanimi podatki v bazi. Lahko se izvaja postopek verifikacije ali identifikacije. V večini primerov korelacija med obema shranjenim in odčitanim vzorcem ni 100%, saj pride do določenih odstopanj. Oseba nikoli ne položi roke pod istim kotom, poleg tega lahko pride do različnih šumov in motenj v času odčitavanja vzorca. Lahko se zgodi, da že registriran osebek naprava zavrne, zato se primerjava registriranega in odčitanega vzorca opravi algoritemsko. Kljub že doseženim izboljšavam je gotovo, da bo v prihodnosti prišlo do nadaljnjega tehnološkega napredka in dviga standardov točnosti, hitrosti in zanesljivosti biometričnih sistemov.

V ZDA je bilo izvedenih veliko poskusov za izboljšanje slabe zanesljivosti tovrstnih sistemov z izboljšavo kakovosti posameznih komponent. Zahtevana je bila uporaba kakovostnejšega materiala in izboljšana zasnova samih proizvodov. Na začetku 20. stoletja so Shewhart, Dodge in Roming postavili teoretične osnove uporabe statističnih metod pri nadzoru kakovosti industrijskih proizvodov, vendar do druge svetovne vojne niso bili v širši uporabi (Chase in drugi, 1998). Koncept zanesljivosti tehničnih sistemov in njegova uporaba sta se pojavila neposredno po prvi svetovni vojni, ko je matematik Lusser[1] izpeljal zakone verjetnosti zaporedno vezanih komponent (Krehl, 2008). Teorem trdi, da je zanesljivost takega sistema enaka zmnožku zanesljivosti posameznih komponent sistema. Po drugi svetovni vojni se je z naraščanjem kompleksnosti proizvodov (televizijskih aparatov, elektronskih računalnikov itd.) povečeval tudi problem njihove zanesljivosti. Konec petdesetih in na začetku šestdesetih let so v ZDA ustanovili združenje inženirjev, ki so se ukvarjali z vprašanjem zanesljivosti. Tako je bila leta 1963 objavljena prva revija na temo zanesljivosti (IEEE Transaction on Reliability). Leta 1965 je bil s strani mednarodne elektrotehniške komisije (IEC) ustanovljen odbor TC56 za obravnavo področij zanesljivosti, razpoložljivosti in vzdrževalnosti. V letih 1989 in 1990 je bilo dogovorjeno, da področja niso več omejena samo na področje elektrotehnike, ampak obravnavajo splošna vprašanja zanesljivosti v vseh disciplinah. Do sedaj je bilo razvitih že več kot 40 različnih dinamičnih modelov v zveznem času za računanje zanesljivosti računalniških programov (Hudoklin in Rozman, 2004). Za večino teh je možno dokazati, da temeljijo na markovski procesih (Musa in drugi, 1987). Navzkrižno članstvo odbora TC56 v organizacijah IEEE in ASQ je poskus, da se zmanjša podvajanje standardov.

[1] *Lusser (1899–1969) je bil med 2. svetovno vojno inženir v nemški letalski industriji. Znan je po inženirskem in konstruktorskem delu pri projektu Messercshmitt.*

Weibull (1972) prejme medaljo ameriškega združenja inženirjev (ASME) na področju statistične obravnave zanesljivosti (slika 1.2). Podrobnejši zgodovinski pregled tehnologije zagotavljanja zanesljivosti opišejo Ansell in Phillips (1994) ter Rausand in Hoyland (2004). Po Shoomanovem[2] modelu zanesljivost ocenjujemo na osnovi že odstranjenih napak po določenem času odstranjevanja. V ZDA se je resni analizi zanesljivosti kompleksnih sistemov posvetila vojaška industrija (TM5-698-1, 2003). Zanesljivost je definirana s časom do prve odpovedi in je ne moremo nadomestiti z intenzivnejšim vzdrževanjem naprav.

Slika 1.2: Weibull (na levi) ob prejemu priznanja združenja ameriških inženirjev (ASME) l.1972 skupaj s Folsom (v sredini) in človekom, ki je naredil prvi korak na luno (na desni)– astronavt Armstrong (Abernethy, 2005)

Poleg naštetih zahtev pa moramo pri implementaciji biometričnega sistema v praksi upoštevati tudi: učinkovitost (točnost, hitrost in izrabo virov sistema), sprejemljivost (za uporabnika mora biti neškodljiv in sprejemljiv za namenjeno populacijo uporabnikov) in varnost (biti mora dovolj robusten za različne možnosti prevar in vdorov). V okviru sistema TQM kazalnik zanesljivost poznamo tudi s stališča proizvodnje, ki poleg relacij proizvajalec-kupec vsebuje tudi kazalnik OEE (skupna učinkovitost naprav) (Ahmad in Dhafr, 2002). V preteklosti učinkovitosti biometričnih sistemov, ni bilo mogoče zanesljivo oceniti zaradi zelo pogosto nasprotujočih si informacij, največkrat komercialne narave (Petermann in Sauter, 2002). Nejasnost meja zmogljivosti med obstoječo identifikacijsko tehnologijo in tehnologijo

[2] *Shooman je profesor na Hunter College, City University of New York, dobitnik nagrad za 5 najboljših člankov na temo zanesljivosti in razpoložljivosti računalniških sistemov. Je konzultant pri NASA, US Army, Lockheed Martin, IBM, AT&T in SAIC.*

prihodnosti, je bil vir zmede pri določanju parametrov učinkovitosti in zanesljivosti. Najbolj splošna je definicija uporabnosti programske opreme, ki je opredeljena v standardu ISO 9241–11, »Uporabnost sistema je merilo uspešnosti, učinkovitosti in zadovoljstva, s katerim lahko tipičen uporabnik z uporabo tega sistema, v določenih pogojih in okolju, doseže zastavljeni cilj« (UsabilityNet, 2007). Standard ISO 9241–11 je eden od 17 delov standarda ISO 9241 (1997): Ergonomske potrebe pri pisarniškem poslovanju z uporabo slikovnih zaslonov, ki velja za osrednji standard s področja uporabnosti, saj natančno opredeljuje, kateri podatki so relevantni za ocenjevanje uporabnosti opazovanega sistema. Nielsen (1993) je uporabnost opredelil kot večdimenzionalno lastnost uporabniškega vmesnika, ki je povezana s petimi atributi (učljivost, zapomnljivost, učinkovitost, zadovoljstvo in napake). Učinkovitost sistema nam pove, kako hitro lahko uporabnik opravi zadano nalogo. Za učinkovit sistem se predpostavlja, da uporabnik z njim potem, ko se ga nauči uporabljati, svoje delo opravlja z visoko stopnjo produktivnosti. To produktivnost lahko merimo po času ali številu opravljenih nalog.

Na nacionalni in mednarodni ravni veliko število odborov dela na opredelitvi meril za oceno prihodnje generacije biometričnih sistemov, in obstoječe tehnike (pogosto prototipov). Opravljajo se primerjalna praktična testiranja različnih pilotnih projektov, vendar pa še ni splošno priznane metodologije za primerjavo prednosti in slabosti različnih biometričnih sistemov. Poleg tega različne stopnje zrelosti različnih biometričnih sistemov onemogočajo primerjalno oceno. Takšna ocena bi morala vključevati logične in informativne podatke o zanesljivosti, natančnosti, občutljivosti, sprejetju, stabilnosti, skladnosti, preprostosti, stroških itd. (Petermann in Sauter, 2002).

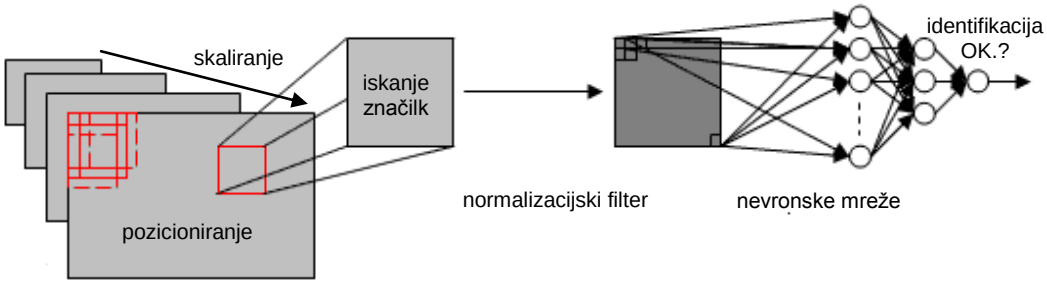
Učinkovitost biometričnega sistema lahko povečamo tudi z nevronskimi mrežami[3] (Rowley in drugi, 1998). Za razliko od drugih avtorjev, ki so za učenje uporabili eno ali dve nevronski mreži, je Rowley učinkovitost povečal z uporabo več nevronskih mrež in z različnimi metodami za izbiro med izhodi teh nevronskih mrež. Nevronske mreže se uporabljajo že na veliko področjih človekovega delovanja, kjer so z njimi realizirane odločitvene funkcije. Omenimo nekaj tistih, kjer so najbolj razširjene:

a) Ekonomija: tu se uporabljajo za ocene tveganja poslovanja (npr. dajanje posojil), simuliranje obnašanja trga (napovedovanje cen), raziskovanje trga, kupcev, preverjanje podatkov itd.
b) Politika: uporaba za strateško napovedovanje in odločanje, določanje indikatorjev politične nestabilnosti (Andreou in drugi, 2005).
c) Medicina: vedno bolj se uporabljajo predvsem za postavljanje diagnoz (npr. hepatitis, obolenja srca) ali njihovo potrjevanje.
d) Komunikacije: popravljanje napak telekomunikacijskih omrežij zaradi napak programske opreme, prepoznavanje govorcev. Pri optimizaciji biometrije v segmentu prepoznave glasu so že znani primeri uporabe nevronske mreže (Oglesby in Mason, 1991).
e) Prepoznavanje vzorcev: interpretacija večpomenskih kitajskih besed, prepoznavanje pisave, 3D objektov, obrazov, odkrivanje podmorskih min. Pri

[3] *Nevronska mreža, tudi umetna nevronska mreža, (angl. neural network, nem. neuronales netz) je način za obdelavo informacij, ki deluje po vzoru človeških oz. živalskih možganov.*

optimizaciji biometrije v segmentu prepoznave obrazov prav tako najdemo uporabo nevronskih mrež (Navarrete in Solar, 2002).

f) Filtriranje: določanje pomembnih podatkov je proces, ko na osnovi podatkovnega rudarjenja (data mining), s programskimi orodji (IBM DB2, Inteligent Miner, XpertRuleMiner, Clementine SPSS, SQL Server Analysis, SAS Enterprise Miner itd.) pride do odkrivanja znanja (Bohanec, 2001). Odkrivanje znanja iz podatkov je proces odkrivanja doslej neznanega in potencialno uporabnega znanja iz podatkov (Groth, 2000).
g) Igranje inteligentih iger: šah.
h) Načrtovanje zanesljivosti programske opreme (Karunanithi in Malaiya, 1996).
i) Sistemi identifikacije (slika 1.3): na tem področju nevronske mreže veliko obetajo v prihodnosti (Garcia in Delakis, 2004). Pri nastavljanju (učenju) mreži predstavimo sliko, ki jo ta primerja s sliko v svojem spominu. Mreža nato nastavlja uteži, dokler ne dobimo želenega rezultata.



Slika 1.3: Nevronske mreže v biometriji (Rowley, 1998)

V obravnavi povezave modela nevronskih mrež in biometričnega sistema želimo doseči optimizacijo in s tem učinkovitejši in hitrejši postopek osebne identifikacije. Modeli so lahko še bolj učinkoviti, če se povežejo še z nekaterimi metodami umetne inteligence (npr. genetskimi algoritmi[4], iskanjem s tabuji itd.). Iskanje s tabuji (tabu search) je hevristično postopek, ki uporablja dinamično generirane omejitve ali tabuje, ki vodijo iskanje k optimalni rešitvi (Pham in Karaboga, 2000). Obstaja več vrst prenosnih (aktivacijskih) funkcij glede na probleme, ki naj bi jih nevronska mreža reševala. Ponavadi se uporablja ista aktivacijska funkcija za vse nevrone v določenem nivoju nevronske mreže, čeprav to ni nujno. Med pogosto uporabljene prenosne funkcije sodita (Kononenko in Hong, 1997):

a) stopničasta deterministična funkcija (skočna funkcija) in
b) zvezna determinističa funkcija, ki je ponavadi sigmoidna pragovna funkcija.

Vsaka inteligentna tehnika ima svojo računalniško lastnost (npr. sposobnost učenja, razlaganja, sprejemanja odločitev), zaradi katere je primerna za določeno rešitev, medtem ko za druge takšna specifična uporabnost ni ustrezna. Nevronske mreže so na primer dobre v prepoznavanju vzorcev, niso pa dobre v razlaganju, kako so prišle do rešitev (Fausett, 1994).

[4] *Genetski algoritmi iščejo optimum s pomočjo procesov, ki so podobni procesom naravne selekcije in genetike. Znan je večpopulacijski samoprilagodljiv genetski algoritem za gradnjo odločitvenih dreves, ki s širjenjem informacije med populacijami nadzira prilagajanje adaptivne cenitvene funkcije pri gradnji optimalnih odločitvenih dreves.*

Fuzzy[5] logični sistemi so dobri v razlaganju svojih rešitev, toda po drugi strani ne morejo avtomatično pridobiti pravil, ki jih uporabljamo pri konstruiranju teh odločitev (Klir in drugi, 1997). Za fuzzy logiko zasledimo izraz »mehka logika« ali »mehka množica« (Virant in Zimic, 1996). Takšno poimenovanje tudi prikaže, da je mehka logika nasprotje klasične dvovrednostne, ki bi jo lahko poimenovali tudi trda logika. Navedene lastnosti so bile glavno vodilo za ustvarjanje hibridnih inteligentnih sistemov, v katerih sta kombinirani dve ali več tehnik z namenom, da se presežejo pomanjkljivosti posameznih tehnik (Huvanandana, 2002). Hibridni sistemi so zato pomembni pri različni naravi aplikacijskih domen (Hagan in drugi, 1996). Še pred nekaj leti so se z mehko logiko ukvarjali le znanstveno v nekaterih krogih. Njen razvoj in uveljavljanje je zavrlo tudi spoznanje, da ni uporabna za modeliranje odločitvenih procesov v ekspertnih sistemih, ker se z razvejitvijo na več odločitvenih nivojev, izgublja informacija. Zadeh je leta 1965 postavil temelje mehke logike in leta 1973 objavil članek, v katerem je izpostavil uporabno vrednost mehke logike. Članek je eno temeljnih del na področju mehke logike. V kombinaciji z nevronskimi mrežami, se mehka logika uporablja kot aplikativna evolucijska metoda za optimizacijo multimodalne biometrije (Hidalgo in drugi, 2008).

Spiralni razvoj in implementacijo inteligentnega multimodalnega biometričnega sistema izvedemo s pomočjo programskega orodja EasyNN, ki rabi za modeliranje in implementacijo modelov nevronskih mrež in sistemske dinamike. Prvi modeli razvoja programske opreme so bili linearni sekvenčni modeli, ki so temeljili na tradicionalni paradigmi programskega inženiringa (Boehm, 1989). Zaradi sekvenčne narave se pri omenjenem modelu pojavljajo težave. Za stalno razvijanje programske opreme je primernejši razvoj spiralnega modela. Tak model združuje ponavljalno naravo prototipa s kontrolo in sistemskim pogledom linearnega sekvenčnega modela (Balantič, 2006) in ga bomo uporabili pri našem razvoju inteligentnega multimodalnega biometričnega sistema.

Možnosti avtomatičnega odkrivanja deviantnosti so v zadnjem času pritegnile veliko zanimanja med raziskovalci inteligentnih biometričnih sistemov. Dosedanje raziskave kažejo, da je integracija različnih biometričnih identifikatorjev z inteligentnim sklepanjem pomembna izboljšava pri zagotavljanju optimalne varnosti. Aplikativni del projekta je v sklepni fazi razvoja (testiranje in validacija) ter temelji na prstnem odtisu. Raziskavo lahko razširimo na preostale biometrične metode: skeniranje šarenice, geometrija obraza, kamera, prepoznava glasu, podpis itd. Tako združimo[6] znanstvene komponente, ki bodo biometrijo, nevronske mreže (mikroučenje, makroučenje) in ekspertni sistem povezale v inteligentni multimodalni biometrični sistem. Z integracijo več različnih identifikacijskih metod in posebno z inteligentnim prilagajanjem glede na kriterije[7] preverbe se tako bistveno zmanjša možnost zlorabe sistema. V sodobnih procesih se stopnjujejo zahteve po uvedbi varnih osebnih identifikacijskih sistemov za povečanje zaupanja pri verifikaciji posameznikove identitete v fizičnem ali virtualnem prostoru logističnega procesa

[5] *Angleški izraz »fuzzy« [izg.: fázi] je uvedel Zadeh in s tem povzročil veliko dilem glede ustreznosti izraza. Težava je, da ga je težko prevesti, saj ima v angleščini za različne situacije različen pomen: vlaknat, puhast, razcefran; zabrisan, nerazločen, meglen.*

[6] *Združevanje biometrije (konkretno glasu) in nevronskih mrež z namenom optimiranja (enomodalno).*

[7] *Kriteriji preverbe v tej raziskavi nastopajo kot varnostni dejavniki, na osnovi katerih se odločitveni model odloča za izbiro koombinacije modulov varnostnega sistema.*

(Dorizzi in drugi, 2004). Zanesljiv identifikacijski sistem mora biti zgrajen v skladu z zakonodajo in politiko organizacije ter upoštevajoč varovanje posameznikovih osebnih podatkov. Identifikacijski sistemi morajo zagotavljati varnost podatkov in učinkovito verifikacijo identitete posameznika, hkrati pa zanesljivo varovati njegove osebne podatke.

Prstni odtis, očesna šarenica, mrežnica, obraz ipd. so biometrični podatki in kot taki nedvomno tudi osebni podatki, saj gre za značilnosti, ki so edinstvene in stalne za vsakega posameznika in na podlagi katerih je oseba določena oziroma vsaj določljiva. Zato se vsakršno zbiranje, shranjevanje, pošiljanje ali uničevanje teh podatkov šteje za obdelavo osebnih podatkov in posledično zanje veljajo določbe zakona, ki ureja varstvo osebnih podatkov (ZVOP–1, 2004). Zasebnost in družbeno sprejemljivost nadzornih tehnologij raziskujejo številni raziskovalci in strokovnjaki. Zaradi soodvisnosti je nujno interdisciplinarno in hkratno obravnavanje obeh vprašanj. Gre namreč za problematiko, ki ima družboslovne, pravne, filozofske in tehnološke razsežnosti in se močno dotika pravic posameznikov oziroma uporabnikov interneta. Poleg tega imamo opraviti s tehnologijo, ki se hitro razvija. Vsi ti razlogi narekujejo, da je poglobljeno raziskovanje tega področja še kako relevantno in aktualno.

Problemi, s katerimi se ukvarjajo tako rekoč vsi raziskovalci tega področja, zadevajo predvsem odsotnost nedvoumne in jasne definicije, kaj sploh je zasebnost. Ta nedorečenost je delno tudi posledica tega, da sta pojem in obseg pravice do zasebnosti podvržena nenehnim vplivom družbenih in tehnoloških sprememb. V Bruslju so sprejeli nekaj novih ukrepov za izboljšanje dostopnosti do evropskih podatkovnih baz, tako da bi članice EU in Europol imeli dostop do vizumskega informacijskega sistema (VIS) ter do baze prstnih odtisov prosilcev za azil in nezakonitih priseljencev EURODAC. S tem naj bi državljani EU dobili pomemben branik pred največjo grožnjo 21. stoletja–terorizmom.

Hustinx (2006) meni, da se pri oblikovanju omenjenih podatkovnih baz žal ni dovolj upoštevala zaščita osebnih podatkov. Interoperativnost teh podatkovnih zbirk povečuje nevarnost za državljane, saj omogoča nov dostop do osebnih podatkov. Zato je po njegovem nujno, da se zadeva pozorneje preuči. Evropska unija je na ukaz ZDA vse državljane obvezala k lastništvu biometričnih potnih listov, če želijo potovati v ZDA. Evropa si je za jemanje prstnih odtisov in odčitavanje črtnih kod očesnih šarenic od ZDA skušala izprositi še nekaj časa. Evropska unija oziroma njena uprava se je odločila, da malce upočasni projekt implementacije biometrije. Rezultati v zvezi z napredovanjem Lizbonske strategije, po kateri naj bi EU do leta 2010 implementirala biometrijo na vstopnih točkah v države, tako še ne dosegajo začrtanih ciljev. Evropske oblasti napovedujejo, da se bodo biometrični elementi široko uporabljali v gospodarstvu, zdravstvu, pri mejnih in drugih kontrolah, pa tudi pri povsem banalnih zadevah, kot so vstop v šolsko jedilnico, vžigu avtomobila, vožnji z avtobusom. Za uporabo štedilnika bi se na primer lahko uporabljala geometrija roke. Ljudje bodo svojo skenirano šarenico lahko uporabljali namesto gesla za dostop do podatkov in shranjenih dragocenosti, otroci pa se bodo igrali z biometričnimi igračami, ki bodo prepoznale registrirane uporabnike.

Raziskava v okviru doktorskega dela obravnava problematiko razvoja ter integracije biometričnih identifikacijskih sistemov za avtentikacijo in potrjevanje identitete oseb. Predstavljene so nadzorne tehnologije, pripadajoča zakonodaja ter družbena

sprejemljivost nadzornih in inteligentnih sistemov ter principov, na katerih temeljijo: arhitektura, pravilo učenja, aktivacijska funkcija in optimiranje. Tovrstni sistemi kontrole pristopa so namenjeni za uporabo kot varnostni mehanizem pri vstopu v določen realen ali virtualen prostor, lahko pa tudi pri vstopu na ozemlje neke države, ko je treba potrditi avtentičnost ali identificirati osebo. Sistem preprečuje nepooblaščenim osebam vstop v varovane prostore, hkrati pa omogoča natančno evidenco gibanja posameznikov po varovanem objektu oziroma kompleksu. Osrednji del podrobneje opisuje teoretični model samoorganizirajoče se nevronske mreže, ki rešuje problem optimalne konfiguracije identifikacijskih sistemov na osnovi prepoznave vzorcev tveganja. Ob uvedbi novih tehnologij na področju identifikacije bomo raziskali parametre zanesljivosti in učinkovitosti biometričnega sistema v identifikacijskem procesu.

Teorijo stohastičnih procesov so v letih 1905-1918 začeli razvijati Einstein in Smoluchowsky ob raziskavah Brownovega gibanja, Shottky pri opazovanju šuma v elektronkah in Erlang pri študiju telefonskega prometa. Matematične osnove teorije stohastičnih procesov je izdelal Kolmogorov (1931). V zadnjih desetletjih so doživeli stohastični procesi velik razmah tako v teoriji kot v različnih aplikacijah (Hudoklin, 1986). Teorijo stohastičnih procesov bomo v raziskavi uporabili za izvedbo matematičnega modela strežbe identifikacijskega sistema, s katerim bomo v praksi lahko ugotovili ekonomsko upravičenost izbire identifikacijskega sistema, modelirali njegovo optimalno konfiguracijo ter racionalno planirali vzdrževanje.

Namen raziskave je v praksi zagotoviti optimalno raven varnosti sistema glede na različne varnostne stopnje ali zahteve po identifikaciji in predvsem v zvezi z varnostnimi tveganji. V primerjalni študiji učinkovitosti in zanesljivosti identifikaijskih sistemov bomo relevantne parametre raziskali pri biometričnih sistemih, ki se poleg kartičnih v tem času največ uporabljajo. Z Weibullovo analizo zagotovimo dovolj dobre rezultate raziskovalnih parametrov z majhnim številom vzorcev, ki omogočajo tudi stroškovno ugodno raziskovanje zanesljivosti (Chi–Chao, 1997). Model nevronskih mrež in ekspertnih sistemov bomo glede na specifične zahteve uporabili v funkciji inteligentnega biometričnega sistema. Sistemska simulacija v povezavi z ekspertnimi sistemi je pomembna metoda za celovito proučevanje in razumevanje organizacijskih procesov (Pograjc in drugi, 2003). Zamisel o avtomatizaciji identifikacijskih sistemov se v zadnjih desetih letih z razvojem mikroelektronike izredno hitro razvija in obeta velik porast znanstvenih in aplikativnih raziskav v inženirski stroki na tem področju.

1.1 NAMEN RAZISKOVALNEGA DELA

Po svetu se biometrija vse bolj uveljavlja kot znanstvena disciplina. V Združenih državah Amerike so se z aktivnostmi na tem področju začeli ukvarjati v šestdesetih letih prejšnjega stoletja, najprej sicer v povezavi s forenzičnimi vedami. Danes se pomena biometrije čedalje bolj zavedamo tudi na območju EU, na kar med drugim kaže tehnični dokument EUR 21585 EN, ki ga je pripravil IPTS (2005) za Evropski parlament. Gre za težnjo po zagotovitvi varnosti s kar najmanjšim vplivom na svoboščine evropskih državljanov. Pri vsem tem pa je nujno zavedanje, da se že dotikamo tudi vprašanja družbene sprejemljivosti tako razvite tehnologije (Maghiros in drugi, 2005).

Problematika sistemov za avtentikacijo (potrjevanje identitete) oseb zadnja leta pridobiva pomen tako v Sloveniji kot v Evropski uniji ter drugod po svetu. Po eni strani gre za strateško vprašanje tako Republike Slovenije kot geopolitičnih povezav, v katere je vključena (EU in NATO), saj je vprašanje varnosti in potencialnih terorističnih napadov čedalje bolj v ospredju. Hkrati pa je za Republiko Slovenijo pomembna tudi uskladitev standardov, ki jih uporablja, s tistimi, ki jih na tem področju prevzema zaradi vključitve v NATO.

O biometriji je opravljenih in objavljenih precej raziskav. Slovenija na tem področju ne prednjači, saj se biometrija zaenkrat večinoma uporablja v zasebnem sektorju, za vstop v zgradbe. Na nacionalni ravni je edini znan projekt uvedba biometričnih potnih listin. Iz strateških razlogov je zelo pomembno, da sami razvijemo in vpeljemo sistem za avtentikacijo. Nujno je ohraniti nadzor nad ključnimi tehnologijami, povezanimi z zagotavljanjem varnosti in gibanjem državljanov. Strateški interes pa ni samo v varnostnih vidikih uporabe biometričnih sistemov. Glede na to, da gre za svetovno težnjo, se pričakuje silovit razmah trga na tem področju in s tem možnost za prispevek h gospodarski rasti s komercializacijo tovrstnih sistemov.

Vse pogostejši vdori v varovane objekte (banke, poslovne prostore) in teroristični napadi so v družbi okrepili zavest o pomenu zagotavljanja varnosti oseb in varovanih prostorov. Zato je bistveno zagotoviti učinkovit nadzor vstopa in gibanja v varovanih prostorih. Zahteve po nadzornih sistemih postajajo vse pogostejše in se uveljavljajo tudi na drugih krajih, kot so mejni prehodi, letališča ter pomembni turistični in poslovni objekti. Na področju identifikacije in avtentikacije ljudi so čedalje bolj pomembne in razširjene biometrične identifikacijske metode, ki omogočajo višjo raven varnosti pri nadzoru vstopa (Dorizzi, 2006). Takšni prijemi lahko zagotovijo večjo stopnjo osebne varnosti, učinkovitejše izvajanje osebnih pravic ter varnejšo državno in evropsko mejo. »Teroristu je mogoče slediti edino s pomočjo biometrije,« je mnenje enega od direktorjev FBI, Kirkpatricka (2001). Pri tem moramo upoštevati, da vse varnostne situacije niso enake, tudi znotraj istega sistema ne. Možen odgovor na potrebo po prilagajanju posameznim varnostnim situacijam je kombiniranje različnih identifikacijskih metod. Izbira, usklajevanje in uravnoteženje varnostnih prijemov, vključno z metodo identifikacije, so ključni, saj omogočajo ustrezno prilagajanje varnostnim potrebam. Kombinirane metode identifikacije je bistveno težje zaobiti kot eno samo, ne glede na to, da so nekateri identifikacijski sistemi izredno zanesljivi že sami po sebi (Maghiros in drugi, 2005). Posebno po terorističnih napadih v ZDA in drugod po svetu je poskočilo vlaganje v raziskave in razvoj na področju biometričnih sistemov za nadzor oseb. Danes v razvitem svetu velja, da je najučinkovitejše sredstvo v boju proti terorizmu inteligenca. ZDA so zato sprejele vrsto zakonov, ki omogočajo obširnejše zbiranje (osebnih) podatkov in elektronski nadzor. Z več podatki tako postaja eden ključnih mehanizmov v boju proti terorizmu uporaba inteligentnih metod za nadzor oseb (Gams, 2001). Inteligentni identifikacijski sistemi lahko z novimi tehnikami opazijo sumljivo ali deviantno obnašanje posameznika, ki ima lažno identiteto ali pa celo pravo, vendar se njegovo vedenje iz kakršnihkoli razlogov razlikuje od običajnega. Odstopanje se kaže v odklonskosti od običajnega vedenja (npr. oseba je pod vplivom opojnih substanc ali ima porušeno duševno ravnotežje) ali pa od posameznikovih lastnih biometričnih značilk (npr. glede na starost, videz itd.).

1.2 CILJI RAZISKOVALNEGA DELA

Aplikativni model identifikacijskega sistema mora zagotavljati nemoten proces obdelave osebnih informacij v ključnih trenutkih, ko je treba iz takšnih ali drugačnih razlogov ugotoviti istovetnost človeka ali ga identificirati. Metode biometrične identifikacije omogočajo zbiranje podatkov o osebah, ki jih nato obdelamo z inteligentnimi sistemi, kar omogoča višji in poglobljen nivo ugotavljanja morebitnih varnostnih anomalij. Za določitev optimalne konfiguracije pristopne kontrole je treba izbrati strežna mesta, ki bodo zagotovila nemoten pretok ljudi z upoštevanjem odpovedi ali vzdrževalnih posegov na identifikacijskih sistemih. V odvisnosti od varnostnih dejavnikov bomo s pomočjo nevronskih mrež določili biometrične metode oz. sisteme biometričnih kombinacij pristopne kontrole, ki bi ustrezale optimalni ravni varnosti (cena/parametri varnosti/ergonomija/družbena sprejemljivost) varovanega objekta ali subjekta. Učinkoviti sistemi za podporo odločanju pa nam bodo omogočili integracijo simulacijskih metod in umetne inteligence pri razvoju zanesljivih biometričnih (nadzornih) sistemov pristopne kontrole.

1.2.1 POJASNILA V ZVEZI S CILJI DOKTORSKE NALOGE

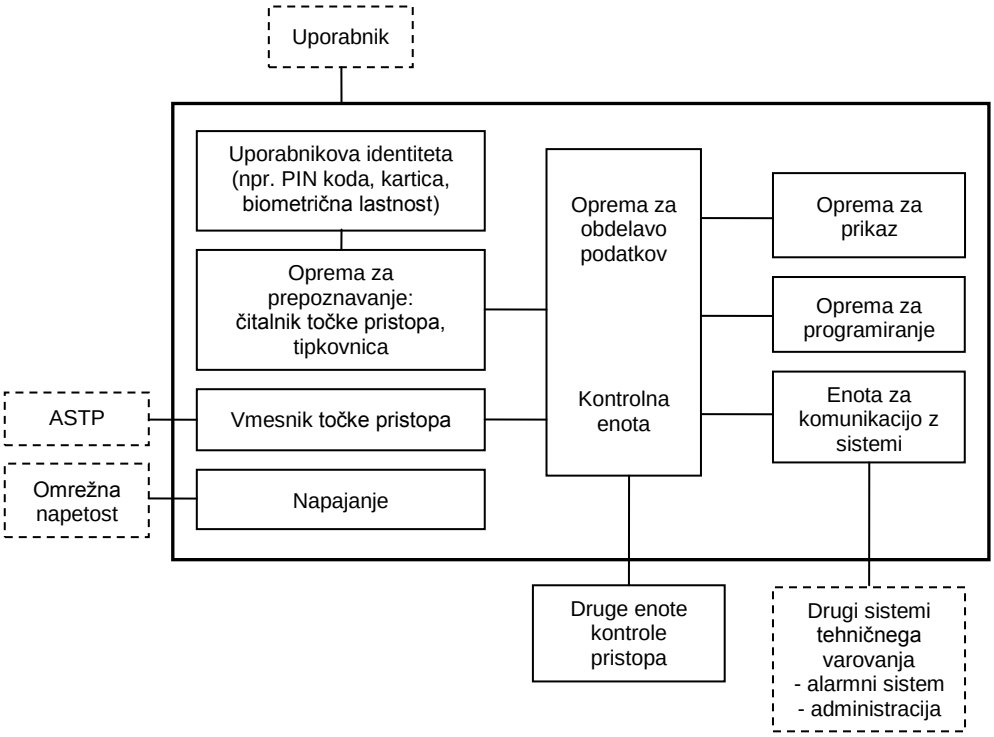
Študija zanesljivosti in razpoložljivosti v zvezi z zagotavljanjem kontinuiranega delovanja identifikacijskega sistema omogoča pravočasno zamenjavo komponent v predvidenih intervalih, ko še ne nastopi odpoved. Za ugotovitev optimalnega časa potrebnega za vzdrževanje, moramo določiti:

- parameter, ki ga bomo merili,
- s čim ga bomo merili in
- meje (Kje so meje, ko je že potrebno popravilo?).

Pri kompleksnih napravah s konstantno trenutno pogostostjo odpovedi λ se cela naprava obnaša, kot da je v dobi normalnega delovanja. Opravimo lahko manjša popravila ali vzdrževalna dela, ne zamenjujemo delov in upamo, da smo neko odpoved preprečili. S stohastičnimi procesi lahko določimo najustreznejšo konfiguracijo pristopne kontrole s kar najmanjšim posegom v človekovo zasebnost. Pri tem določimo:

a. optimalno število identifikacijskih elementov, če so parametri FAR in FRR enaki,
b. optimalno število identifikacijskih elementov, če parametri FAR in FRR niso enaki,
c. zaporedje identifikacijskega procesa, da bo celoten čas identifikacije najkrajši (Zaporedja obdelave si sledijo v določenem zaporedju, lahko pa tudi čakajo.) in
d. koliko zaposlenih (domačih in zunanjih vzdrževalcev, kooperantov itd.) je treba imeti, da bodo stroški vzdrževanja kar najmanjši.

Za dosego optimalnega varnostnega nivoja bomo glede na varnostno tveganje z nevronskimi mrežami določili teoretični odločitveni model izbire konfiguracije identifikacijskega sistema pristopne kontrole. Sistem pristopne kontrole je definiran v skladu s standardom SIST EN 50133 in v svojih sistemskih zahtevah vključuje področja, prikazana na sliki 1.4.



Slika 1.4: Konfiguracija sistema pristopne kontrole po SIST EN 50133

1.2.2 IZVIRNI PRISPEVEK K ZNANOSTI

Doktorska disertacija temelji na znanstvenoraziskovalnem delu na področju inženiringa zanesljivosti in statističnem vrednotenju aplikativno razvitega biometričnega sistema pristopne kontrole v smislu razpoložljivosti. Raziskovalno delo dosega večplasten pozitivni učinek metodologije organiziranja procesov, ki ga v osnovi lahko nakažemo v praktičnem in teoretičnem prispevku k znanosti.

1. Biometrični modul za avtentifikacijo in potrjevanje identitete oseb na podlagi več značilk bomo integrirali z elektronskim sistemom zaklepanja (ELS), kar naj bi nazadnje pripomoglo k izboljšanemu sistemu za avtentikacijo oseb in preprostejšemu omejevanju dostopa do prostora (realen ali virtualen prostor, zgradbe, lahko tudi države) ali varnostno zaščitenih informacij. Z raziskavo želimo potrditi domneve o biometriji kot preprostem, a zanesljivem in učinkovitem načinu prepoznavanja identitete posameznika v širši javni uporabi. Izvedli in predstavili bomo raziskavo parametrov FAR in FRR ter v okviru tega pripravili statistično oceno kvantitativnih parametrov zanesljivosti in razpoložljivosti sistema identifikacije. Predstavljen bo njun medsebojni vpliv v sistemu biometrične identifikacije pristopne kontrole. Z optimizacijo na osnovi nevronskih mrež in markovskih verig bomo raziskali možnosti za izboljšanje učinkovitosti identifikacije.
2. Kot rezultat uporabnosti bo sledila optimizacija obstoječih postopkov osebne identifikacije in obstoječih identifikacijskih sistemov (brezkontaktne čipne kartice,

kontaktne čipne kartice, čipi in ostali RFID identifikatorji) z biometričnim načinom identifikacije (prstni odtis). Pričakovani rezultat aplikativnega dela raziskave bo optimirani »multimodalni sistem za biometrično prepoznavanje oseb« v sistemu pristopne kontrole. Tak sistem bodo lahko uporabljale tako državne ustanove kot tudi druge organizacije (zavarovalnice, banke, podjetja itd.), ki želijo nadzorovati dostop do določenih realnih ali virtualnih prostorov, v katerih so kakršnekoli zaščitene varnostne informacije. Z uporabo rezultata v praksi bo mogoče na zanesljiv način omejiti dostop do tovrstnih informacij ali prostorov. Rezultat raziskave bo tudi patentno zaščiten, kar bo omogočalo njegovo gospodarsko izkoriščanje.

3. V literaturi lahko zasledimo množico raziskav, ki se ukvarjajo z učinkovitostjo najrazličnejših postopkov prepoznavanja prstnih odtisov. Večina teh raziskav temelji na predpostavki, da je digitaliziran vzorec že lociran. Izrezi prstnih odtisov, uporabljeni za avtentikacijo, se torej po velikosti, orientaciji in položaju značilnih delov prsta (papilarne linije petlja, lok, spirala, središčna točka, delta, karakteristične linije in papilarno število) med seboj bistveno ne razlikujejo. Ta predpostavka je upravičena pri proučevanju učinkovitosti algoritmov prepoznavanja prstnih odtisov, v realnih sistemih pa moramo upoštevati še problem »avtomatske registracije«. V tem primeru je treba prst pred postopkom istovetenja še lokalizirati in ustrezno normalizirati. Postopek biometrične registracije vnaša v identifikacijski sistem dodatne napake, ki jih je treba pri vrednotenju sistema prav tako upoštevati. Tako se pojavi neskladje med doslednim upoštevanjem standardov ter natančnostjo in hitrostjo, ko gre za standardizacijo avtomatizacije procesa. Ker je vpliv nekaterih od omenjenih dejavnikov na učinkovitost identifikacije tako rekoč neraziskan, se bomo posvetili ovrednotenju napak, ki jih naštete spremembe v kakovosti vzorca vnašajo v biometrični sistem, ter njihovemu vplivu na učinkovitost in zanesljivost sistema (FAR, FRR).

   Poleg problema lokalizacije se lahko v praksi srečamo še z drugimi težavami, ki prav tako vplivajo na učinkovitost algoritmov prepoznavanja in so bile v dosedanjih raziskavah zanemarjene. V primeru, da sta biometrični čitalnik in sistem za prepoznavo krajevno ločena, se lahko del informacije, ki jo vsebuje vzorec, na poti izgubi, vzorec je zamegljen, del vzorca je zaradi ovir med čitalnikom in identificirano osebo prekrit (vlaga, nikotin, obrabljeni grebeni prstne blazine – vpliv staranja, vzorci so nepopolni zaradi deformacije strukture kože, ki je bila dlje časa izpostavljena vplivu vlage, zajeti vzorci so lahko neustrezni zaradi neustrezne namestitve čitalnika, rotiranega za določen kot). Na osnovi raziskanega bomo z uporabo nevronskih mrež optimirali biometrični sistem za osebno identifikacijo v realnem času v velikih podatkovnih bazah, ki temelji na odvzemu značilk prstnega odtisa.

1.2.3 PRIČAKOVANE IZBOLJŠAVE GLEDE NA OBSTOJEČE SISTEME IDENTIFIKACIJE

Identifikacijski sistem na osnovi prstnega odtisa, ki smo ga v okviru doktorske naloge razvili in uporabili kot primerjalni model za določitev in raziskavo učinkovitosti ter občutljivosti, se od RFID sistema razlikuje po naslednjih lastnostih:

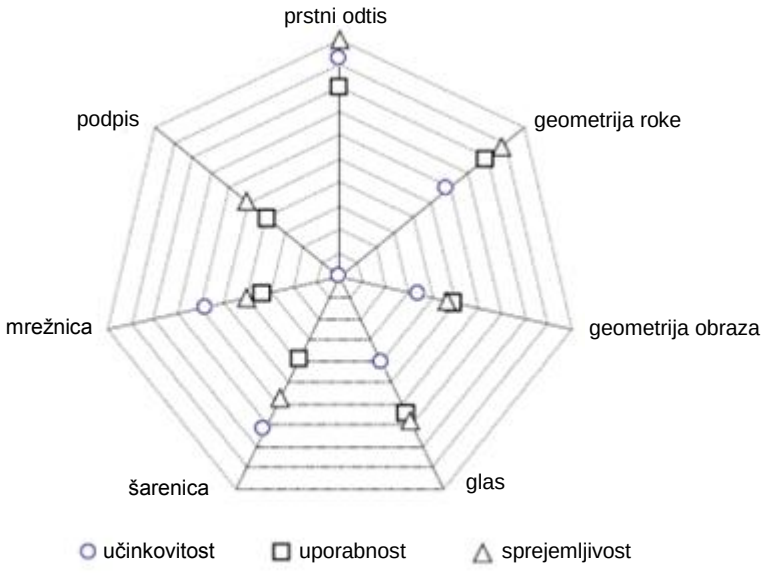
- večja hitrost odčitavanja prstnih odtisov in distribucije podatkov,

- neobčutljivost za vlago, umazanijo in položaj prstnega odtisa,
- možnost integracije s čipnimi karticami, kar poveča stopnjo varnosti in posledično prilagodljivost sistema,
- integracija z drugimi biometričnimi metodami (multimodalnost) na osnovi optimizacije z nevronskimi mrežami,
- večja robustnost in razpoložljivost sistema (višji $MTTF$, manjši $MTTR$ in višji $MTBF$),
- večja varnost osebnih podatkov in
- manjši poseg v zasebnost in večja sprejemljivost.

Prvi rezultati aplikativnega dela raziskave so že bili predstavljeni zainteresirani javnosti na mednarodnih konferencah ter v strokovnih in znanstvenih člankih, objavljenih v mednarodnih revijah.

1.2.4 KAKŠNO PRIHODNOST IN POMEN IMA NAŠE PODROČJE DELA

Pomen raziskovalnega in razvojnega dela na tem področju je izdelati biometrični identifikacijski sistem, ki bo tako varnostno kot cenovno optimalen. Tehnologija s strani odobravanja uporabnika mora biti prijazna in ne sme posegati v človekove pravice (Jain in drugi, 2002). Na sliki 1.5 vidimo posamezne tipe biometričnih sistemov glede na oceno parametrov učinkovitosti, uporabnosti in sprejemljivosti. Razvidno je, da biometrija na osnovi prepoznave prstnega odtisa v primerjavi z ostalimi metodami prednjači, glede na podane parametre (učinkovitost, uporabnost in sprejemljivost).



Slika 1.5: Lastnosti posameznih tipov biometrij (Kapczyński, 2006)

1.3 ZNANSTVENORAZISKOVALNO PODROČJE

Spremembe na znanstvenoraziskovalnem področju nadzornih tehnologij so opazne v mnogih vejah znanosti, nanje kažejo strokovne knjige, pomembne konference, k določeni temi usmerjene strokovne revije in nastanek novih raziskovalnih združenj. Podobno se dogaja tudi z nevroznanostjo na področju biometrije.

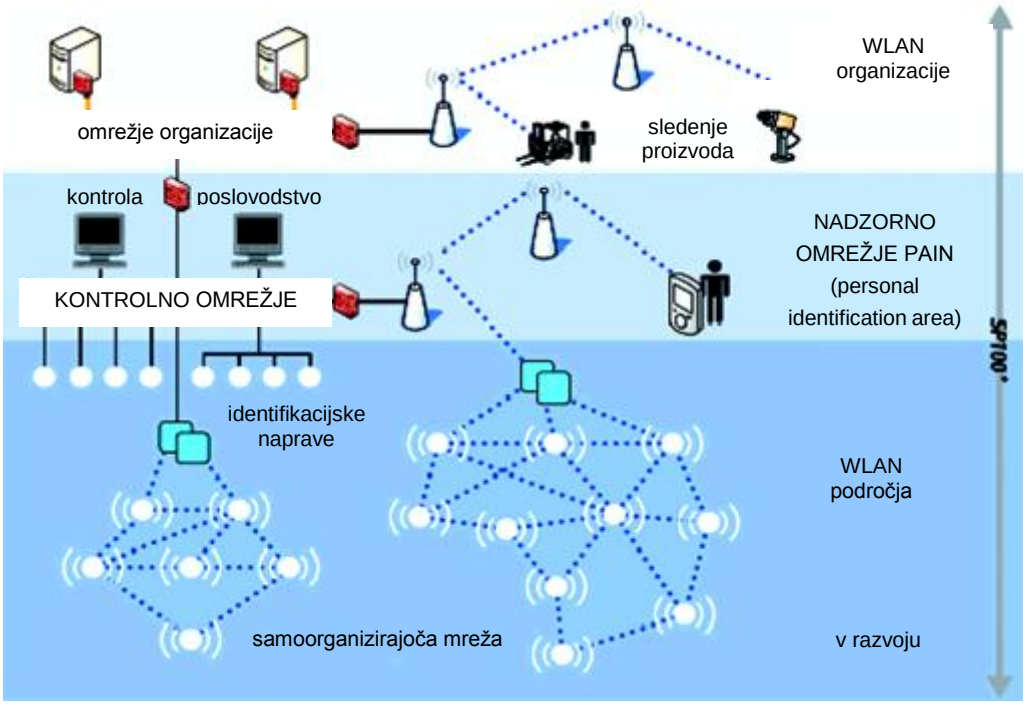
Biometrični identifikaciji je namenjenih kar nekaj mednarodnih konferenc, in sicer IAPR, BCC itd. Prav tako so na področju nevroznanosti in ekspertnih sistemov znane svetovne konference ICONIP, ICIC, IASTED idr. Število znanstvenih člankov o omenjenih tematikah je v zadnjem času zelo naraslo, kar kaže na vse pomembnejšo vlogo tega področja v raziskovalni dejavnosti. Aplikacije biometrične tehnologije so v velikem razmahu in se čedalje bolj širijo tudi na nova področja uporabe, kot so finančni posli, boj proti kriminaliteti, trgovske verige, elektronsko bančništvo, dostop do podatkov, pravosodje, obmejni vstopi, varnostni sistemi, letališča, zapori itd. Kjer sta potrebni največji varnost in zanesljivost, se uporabljajo t. i. večslojni[8] sistemi za preverjanje identifikacije in avtentikacijo (Maghiros in drugi, 2005). Pregled znanstvenih baz kaže, da je ugotavljanje zanesljivosti identifikacijskih sistemov z vidika ugotavljanja odpovedi modulov razmeroma neraziskano področje. Prednjači ugotavljanje zanesljivosti na osnovi študij FAR in FRR (Dorizzi, 2006). Preden se posameznik ali družba odločita za uporabo biometričnega preverjanja, je vsekakor nujno spoznati prednosti in slabosti različnih biometričnih tehnik (tabela 1.1).

[8] *Večslojni (layered) aplikacijski sistemi; združujejo več tehnologij nadzora in tako še bistveno povečajo zanesljivost sistema.*

Tabela 1.1: Značilnosti različnih tipov biometrične identifikacije (Vir: Biometric practical guide, 2007)

	Prstni odtis	Oblika dlani	Očesna mrežnica	Očesna šarenica	Obraz	Lastnoročni podpis	Glas
Težavnost uporabe	velika	velika	majhna	srednja	srednja	velika	velika
Možnost napake	suha, umazana ali postarana koža	poškodba dlani, staranje	očala, leče	slaba osvetlitev	slaba osvetlitev, staranje, očala	sprememba podpisovanja	hrup, prehlad
Natančnost	velika	velika	zelo velika	zelo velika	velika	velika	velika
Uporabnikovo odobravanje	srednje	srednje	srednje	srednje	srednje	srednje	visoko
Zahtevan varnostni nivo	visok	srednji	visok	zelo visok	srednji	srednji	srednji
Uporabnost na daljši rok	velika	srednja	velika	velika	srednja	srednja	srednja

V sodobnih proizvodnih procesih strojegradnje (avtomobilska, letalska in vesoljska industrija, farmacija, forenzika itd.) je nujno hitro in zanesljivo obvladovanje logistike materiala in ljudi (slika 1.6). Podjetja, kot so dobavitelji vojaške opreme in avtomobilov, lahko preverijo uporabnost kvalificiranih delov. TWIC sistem z uporabo programa DaonENGINE omogoča nadzor logistike zaposlenih na osnovi biometrije (OASIS–INCITS M1, 2006). S sledenjem edinstvenim serijskim številkam poslovnih dogodkov in transakcij, povezanih s posameznimi deli, preprečimo uporabo kopij ali konstrukcijskih delov brez garancije.



Slika 1.6: Samoorganizirana brezžična mreža z integrirano identifikacijsko tehnologijo v logistiki industrijskega procesa (Kohonen, 2007)

Že iz uvodnega dela je razvidno, da raziskovalno delo vsebuje raznolika znanstvena področja, zato v nadaljevanju naštejmo nekaj osnovnih.

1.3.1 INFORMACIJSKA TEHNOLOGIJA

Računalništvo je znanstvena veda o delovanju računalnikov in njihovi uporabi, kar vključuje strojno in programsko opremo. V praksi je računalništvo povezano z mnogimi drugimi vedami, od abstraktne analize algoritmov do bolj stvarnih tem, kot so programski jeziki, programska in strojna oprema. Kot znanstvena veda se računalništvo razlikuje od matematike, programiranja, programskega in računskega inženirstva, čeprav se ta področja pogosto zamenjujejo.

1.3.2 ERGONOMIJA IDENTIFIKACIJSKIH SISTEMOV

Ergonomija je beseda grškega izvora, sestavljena iz dveh besed: ergon (ergon) – delo in nomos (nomox) – zakon. Na splošno lahko rečemo, da ima izraz ergonomija mnogo definicij, vendar je v osnovi bistvo pri vseh enako, in sicer prilagoditev sistema človek–stroj v korist človeka kot glavnega udeleženca v tem sistemu, s pogojem, da ne porušimo njegovega ravnovesja in ravnovesja okolice (Balantič, 2001). Ergonomija pomeni skupno uporabo ustreznih bioloških in inženirskih znanosti, da se zavaruje skupna optimalna adaptacija. Cilj je povečati učinek človeka in mu zagotavljati čim lažje delo. Nove metode in tehnologije s področja ergonomije nam ponujajo dobro možnost uresničitve naštetih ciljev pri implementaciji nadzorne in identifikacijske tehnologije. Veda, ki proučuje vprašanja pravilne in ustrezne interakcije[9] človeka z računalnikom, se imenuje ergonomija programske in strojne opreme. Ukvarja se s prilagoditvijo tehniških sistemov človeku, z analizo, oblikovanjem in ocenjevanjem povezav in medsebojnih vplivov med napravami, uporabniki in računalniki. Cilj ergonomije programske opreme je zagotoviti zadovoljivo in učinkovito povezavo med uporabnikom in informacijsko tehnologijo.

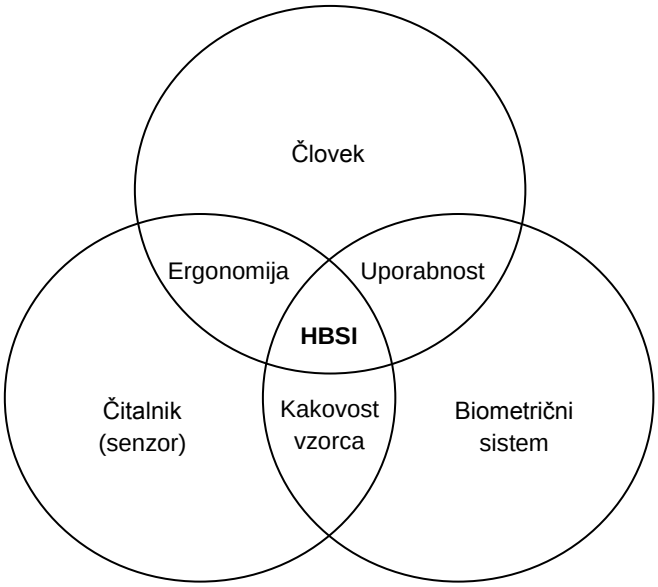
Vsak načrtovalec mora pri svojem delu precej upoštevati človekove zmogljivosti in sposobnosti. V preteklosti so se razmerja znotraj sistema človek–stroj pogosto menjavala glede na kakovost in zahteve. Upoštevajoč človeške zmožnosti in meje moramo procesne in sistemske komponente med človekom in nadzornim sistemom izdelati tako, da dosežemo:

- gospodarnost,
- prijaznost do okolja,
- zanesljivost celotnega sistema kakor tudi,
- delovno in socialno zadovoljstvo glavnega udeleženca v tem sistemu – človeka, uporabnika.

Večja zanesljivost je potrebna povsod tam, kjer so izvedeni kompleksni nadzorni sistemi, ki so lahko nevarni tako za človeka kot za okolje, na primer v jedrskih elektrarnah, kemijskih obratih in na letališčih (Karimi in Hüllermeier, 2005). Če želimo, da bo neki sistem prijazen do okolja, ni dovolj, da ga naredimo izredno zanesljivega, ampak je treba tudi določiti ustrezne postopke, ki jih morajo upoštevati uporabniki. Pri tem pa je socialno in družbeno zadovoljstvo višji cilj, saj gre za pomen vključevanja nadzornih sistemov v širše socialno in družbeno okolje. Med vsemi omenjenimi cilji obstajajo najrazličnejša razmerja. Vsak cilj po svoje vpliva na druge in nasprotno. Vsi po vrsti pa neposredno ali posredno vplivajo na nadzorovano okolje, na razmerja med ljudmi, ki uporabljajo nadzorne sisteme, in ljudi, ki so nadzorovani. Povezava mora biti čim manj občutljiva za uporabnikove napake. V zadnjem času se vse večja pozornost namenja razmerju do oblikovanja uporabniško prijaznih vmesnikov in ustrezne funkcionalnosti. Pri tem moramo upoštevati, da rešitve teh problemov neposredno vplivajo na oblikovanje nadzorovanega prostora, kar pomeni, da se pri analizi in oblikovanju ne smemo omejiti samo na vmesnike, ampak moramo zajeti tudi oblikovanje uporabnikovih

[9] *Dialog ali interakcija omogoča izvajanje komunikacije med človekom in sistemom v vseh primerih z namenom identifikacije ali avtentifikacije človeka.*

delovnih nalog. Za naše raziskovalno in praktično delo se ergonomija uporablja v smislu najmanjšega posega nadzornih tehnologij v človekovo zasebnost ob optimalni zagotovitvi kakovosti in kar najbolj olajšanem postopku identifikacije za človeka. Ergonomija v biometričnem sistemu nastopa v interakciji kakovosti in uporabnosti (HBSI) (slika 1.7).



Slika 1.7: Interaktivni HBSI model človek–biometrični sistem–čitalnik (Kukula in Proctor,2009)

1.3.3 KOGNITIVNA PSIHOLOGIJA

Na teoretične zasnove kognitivne znanosti, tudi računalništva, je vplival koncept »nevronskih mrež«, ki naj bi v nasprotju s sukcesivnimi modeli vpeljal vzporedno procesiranje in s tem poudaril hkratnost odvijanja dogodkov. Vsaka mreža je sestavljena iz nevronov, ki predstavljajo enoto, te enote pa so povezane (prepletene) med seboj in komunicirajo po načinih ekscitacije in inhibicije. Če vsota dražljajev vseh vhodnih povezav do enote presega njeno mejno sprejemljivo vrednost, potem ta enota odda presežek signala naslednjim enotam, s katerimi je povezana. Način povezave določa lastnosti posamezne enote, tako imamo lahko različne strukture in ravni (npr. vhodne in izhodne) (Clark, 2001). Reprezentacija koncepta se shranjuje razporejeno po vzorcu aktivacije nevronske mreže. Ista mreža lahko sprejme več vzorcev, ki med seboj ne interferirajo, če so dovolj različni. Koncept nevronskih mrež je nov model za proučevanje možganov, ki presega anatomske predstave o lokalizaciji (npr. spomina) ter omogoča natančno proučevanje in razumevanje mentalnih funkcionalnih primanjkljajev.

1.3.4 UMETNA INTELIGENCA[10]

Na obliko in način razvoja programske opreme bodo v prihodnosti močno vplivali postopki, ki jih razvija umetna inteligenca. Umetna inteligenca (angl. artificial intelligence) je področje informatike z interdisciplinarnim značajem. Njen cilj je razvoj naprav, ki se vedejo, kot da bi razpolagale z inteligenco (Laeeq in Adeel, 2007). Umetna inteligenca se prepleta s psihologijo, nevrologijo, matematiko, logiko, filozofijo in drugimi vedami. Temeljni cilj umetne inteligence je izdelati stroj, ki posnema človeško razmišljanje. Za uporabniške vmesnike bodo pomembni računalniško razumevanje naravnega jezika in prepoznavanje govora ter samodejna interpretacija slik (Rich in Knight, 1991). Raziskovalci umetne inteligence se ukvarjajo tudi z dokazovanjem pravilnosti programov, razvojem jezikov na zelo visoki ravni (angl. very high level languages), posebnostmi v naravnem jeziku, programiranjem na osnovi primerov in z inteligentnimi asistenti.

1.3.5 ANTROPOLOGIJA

Antropologija izhaja iz grških besed ἄνθρωπος : anthropos – človek + λογος : logos – beseda, govor. Antropologija je znanstvena veda, ki obravnava človeštvo (rod homo – hominoid) kot člen narave in proučuje njegovo biološko naravo (Monaghan in Just, 2000). Raziskuje njegov položaj med drugimi živimi bitji, lastnosti telesne zgradbe, izvor, starodavne in sodobne fizične tipe. V raziskavi bo veda obravnavana s stališča raziskave fizičnih značilk človeka za namene osebne identifikacije.

1.3.6 INŽENIRSTVO IN NAČRTOVANJE

Programsko inženirstvo je uporaba sistematičnega, discipliniranega in določljivega pristopa k razvoju, uporabi in vzdrževanju programske opreme. Termin je bil vpeljan leta 1968 na konferenci pod okriljem Nata. Inženirstvo se je na področju programske opreme začelo uporabljati v 60. letih s študijem pristopov (Solina, 1997). Danes metodologijo progamskega inženirstva ureja standard IEEE 610.12. Upoštevanje principov programskega (informacijskega) inženirstva nujno pomeni projektno delo pri načrtovanju in razvoju informacijskih sistemov.

1.4 METODOLOGIJA RAZISKOVALNEGA DELA

V raziskavi je uporabljena naslednja metodologija:
- eksplorativni pristop, zaradi interdisciplinarnosti tudi multimetodski,
- pregled znanstvene in strokovne literature, analiz in obstoječih raziskav na področju (biometričnih) nadzornih tehnologij in nevronskih mrež,
- analitično raziskovanje povezanosti dejavnikov zanesljivosti in njihovega vpliva na uspešnost procesa razvoja ter implementacije biometričnega sistema,

[10] *Obstajajo najmanj štiri področja: vizualna inteligenca (prepoznavanje oblik, obrazov, prstnih odtisov itd.), govorna inteligenca (prepoznavanje govora, sinteza govora itd.), manipulativna inteligenca (nadzor gibanja robotske roke, nadzor nožnih mehanizmov itd.), racionalna inteligenca (ekspertni sistemi, podatkovne baze itd.).*

- eksperimentalni pristop primerjalnega testiranja identifikacijskih sistemov in statistično ugotavljanje zanesljivosti, razpoložljivosti in učinkovitosti aplikativnega modela biometričnega identifikacijskega sistema,
- empirično preverjanje hipotez v realnih aplikacijah,
- validacija prototipiranja nevronske mreže za optimizacijo biometričnega sistema,
- odločitveno in podatkovno modeliranje,
- analiza vgrajenosti dejavnikov zanesljivosti in njihove povezanosti s tržno uspešnostjo biometričnega sistema.

1.4.1 HIPOTEZE

Hipoteza 1
Predpostavljamo, da v procesu osebne identifikacije biometrični sistemi omogočajo večjo pretočnost oseb (razpoložljivost) kot zdaj aktualni kartični sistemi (pametne kartice).

Hipoteza 2
Predpostavljamo, da so biometrični sistemi identifikacije bolj zanesljivi kot kartični identifikacijski sistemi.

1.4.2 OMEJITVE

Rezultati določanja in računanja zanesljivosti so statistične ocene karakteristik zanesljivosti in so boljši ali slabši približek dejanskega stanja. Za boljše ocene bi bilo potrebno izvajati obsežne in dolgotrajne preskuse velikega števila enot, kar je drago in večkrat tudi neizvedljivo. Zanesljivosti posameznega izdelka ni mogoče določati, zato je treba med obratovanjem opazovati večje število enakih primerkov in zapisovati njihove odpovedi (čase do odpovedi). Tako lahko zberemo zadostno število podatkov, ki jih uporabimo za izračun točkaste ocene karakteristik zanesljivosti gradnikov sistema. Med načrtovanjem lahko torej vnaprej določimo ocene zanesljivosti posameznih gradnikov sistema, sistemu pa nato oceno zanesljivosti lahko izračunamo z uporabo ene od znanih analitičnih metod.

V aplikativnem delu raziskave zanesljivosti smo uporabili model, ki sloni na Weibullovi[28] porazdelitvi. Obravnavali smo vzorec 10 čitalnih modulov (kartičnega in biometričnega identifikacijskega sistema), ki smo jih na osnovi serijske številke spremljali v obdobju enega leta. Pri tem velja poudariti, da pri aplikativnih raziskavah običajno ni na voljo mnogo dragih in velikih sistemov. V raziskavi smo se omejili na zajem podatkov o odpovedih iz uporabe sistema, saj je njegovo delovanje v obratovalnem okolju pogoj, pod katerim mora izdelek zanesljivo delovati. Potrebujemo torej nekaj delujočih sistemov, ki jih v začetnih fazah razvoja še ni. Vpliv dejavnikov na uspešnost in pravilnost implementacije identifikacijskega sistema v realno okolje je bil kontroliran.

V raziskavi bomo upoštevali zakonodajo in predpisane mednarodne standarde na obravnavanem področju identifikacijskih sistemov, ki so natančneje opisani v petem poglavju.

1.5 ORODJA, UPORABLJENA V RAZISKOVANJU

Raziskava se loteva sistematičnih odnosov znotraj identifikacijskih sistemov. Pri statistični obdelavi in oblikovanju zaključkov smo uporabili orodja programskega paketa Weibull++7[11] za statistično obdelavo in določanje ocen karakteristik zanesljivosti in učinkovitosti (Mettas in Zhao, 2004). Glede na cilj raziskave, to je izboljšava teoretičnega modela identifikacijskega sistema s čim bolj stabilno identifikacijo v realnih dinamičnih sistemih, sledi optimizacija z vključevanjem dinamičnih sprememb, do katerih lahko pride v procesu identifikacije. Optimiranje v funkciji avtomatizacije identifikacije bo potekalo z modeliranjem nevronskih mrež s ciljem minimiranja stroškov in posega v zasebnost uporabnikov. Sočasno bomo empirično obdelovali podatke in razvijali računski model za določanje zanesljivosti in razpoložljivosti identifikacijskih sistemov na osnovi markovskih verig. Predvidena orodja empiričnega in aplikativnega raziskovanja so:

- programski paket Weibull++7 za analizo in za določanje ocen karakteristik zanesljivosti,
- markovske verige za razvoj matematičnega modela za določanje zanesljivosti in razpoložljivosti identifikacijskih sistemov na podlagi strukturiranega procesa, ki sloni na teoriji stohastičnih procesov,
- teorija stohastičnih procesov za razvoj modela za določitev konfiguracije pristopne kontrole,
- identifikacijski sistem (na prstni odtis) pristopne kontrole kot temeljni aplikativni model eksperimentalnega raziskovanja in primerjalnega testiranja,
- teorija nevronskih mrež za razvoj optimizacijskega modela pri raziskavi možnosti implementacije multimodalnosti v nadzorno-identifikacijske sisteme,
- odločitvene tabele identifikacijskih in verifikacijskih metod z uporabo odločitvenih parametrov in postavitvijo njihovih uteži in
- prototip inteligentnega multimodalnega biometričnega sistema s podatki že znanih realiziranih identifikacijskih sistemov.

1.6 STRUKTURA DOKTORSKE DISERTACIJE

Kot smo uvodoma (prvo poglavje) že omenili, bomo v doktorskem delu interdisciplinarno obravnavali biometrijo skozi prizmo:

- proučevanja učinkovitosti, zanesljivosti, razpoložljivosti in varnosti identifikacijskih sistemov v primerjavi z alternativnimi metodami identifikacije,
- njene uporabe v poslovnem procesu in procesu varovanja,
- optimizacije z nevronskimi mrežami in
- podajanja ocene zanesljivosti identifikacijskih sistemov (kartičnega in biometričnega) na podlagi relevantnih parametrov zanesljivosti.

Proizvajalec biometričnega sistema (drugo poglavje) za svoj izdelek odgovarja kazensko in materialno. Če izdelki pogosto odpovedujejo, potrošniki izgubijo

[11] *Namenska programska oprema Weibull++7 se uporablja za raziskave zanesljivosti in preračunavanje življenjske dobe pri inženiringu zanesljivosti sistemov z Weibullovo distribucijo.*

zaupanje vanje, morebitni kupci jih odklanjajo, ker jih štejejo za nekakovostne, poleg tega uporabniki izdelke vračajo že ob najmanjših nepravilnostih v delovanju, medtem ko bi te v normalnih okoliščinah brez težav sprejeli. Odpoved biometričnega sistema (tretje poglavje) vsekakor škoduje potrošniku in proizvajalcu. Potrebni so prijemi za zmanjševanje verjetnosti nastopa odpovedi. Večina elektronskih naprav ne opravlja kritičnih nalog, vendar pa se od njih pričakuje nemoteno delovanje. Odpornost proti odpovedi proizvoda opisuje veličina, ki se imenuje zanesljivost. Pomen zanesljivosti in njeno zagotavljanje sta sestavni del inženirskega načrtovanja; to se v sodobnem času izvaja prek projektnega vodenja, ki ga obravnavamo v četrtem poglavju. Naprave, ki so odpovedale, ne opravljajo svoje naloge, zato za potrošnika pomenijo izgubo. Izguba je manjša, če naprava odpove le za kratek čas, zato je pomembna tudi organizacija popravil in vzdrževanja ter standardizacija (peto poglavje). Nove zahteve silijo v razvoj in uporabo biometričnih tehnologij, ki ob najmanjšem posegu v zasebnost zagotavljajo optimalno raven varnosti in kakovosti (šesto poglavje). Učinkovitost zagotavljamo z optimizacijo hierarhičnih modelov za podporo odločanju. Za kompleksne sisteme je treba razviti diagnostiko delovanja, vzdrževanje in servis na daljavo (Polajnar, 2003). V sedmem poglavju obravnavamo matematični model zanesljivosti, razpoložljivosti in učinkovitosti, ki bo osnova za aplikativni del določanja parametrov prototipa nevronske mreže biometričnega sistema (osmo in deveto poglavje). Aplikativni del raziskave na osnovi parametrov učinkovitosti osebnih identifikacijskih sistemov je opisan v desetem poglavju. Zanesljivost in razpoložljivost gradnikov identifikacijskega sistema bomo določili z uporabo markovskega modela v enajstem poglavju. Hibridni inteligentni sistemi kot osnova za optimizacijo multimodalnosti na podlagi vstopnih parametrov so teoretično obravnavani v dvanajstem poglavju. Opisan je pristop k razvoju programskega modela za optimiranje biometričnega sistema z nevronskimi mrežami. Podrobneje je prikazana struktura baze znanja, statistično opisani kazalci oz. spremenljivke in agregatne funkcije, ki nastopajo v bazi znanja. Sledi predstavitev dinamičnih operacij, ki so mogoče v modelu, pri čemer opišemo potrebne postopke, ki se morajo v modelu sprožiti pri določenih zahtevah uporabnika, kot so dodajanje ali odstranjevanje spremenljivke iz modela ali vrednosti v njeni zalogi vrednosti. Uporabljena so orodja za večkriterijsko odločanje, nevronske mreže in »neurofuzzy« sistemi kot optimizacijski modeli multimodalnih biometričnih sistemov, kjer opišemo tudi proces vrednotenja variant in možnosti ter analize. Tak pristop je uspešnejši od klasičnega pri reševanju kompleksnih problemov, za katere ni mogoče zgraditi klasičnih matematičnih modelov, kjer so vhodne vrednosti bodisi nenatančne ali nepopolne ali pa po svoji naravi mehko določene (upravljanje fizikalnih in kemijskih sistemov, ekspertni sistemi itd.) (Negnevitsky in drugi, 2007). V nadaljevanju, v trinajstem poglavju, so predstavljeni ter interpretirani rezultati raziskave, ki so temelj za teoretično zasnovo optimizacije sistema. Od organizacije procesa in njegove zmogljivosti je odvisna končna učinkovitost identifikacijskega sistema. Nadalje v zaključku (štirinajsto poglavje) povzamemo rezultate in bistvene ugotovitve raziskave ter v štirinajstem poglavju razpravljamo o predvidenih nadaljnih aktivnostih in možnih smereh razvoja na področju osebne identifikacije. V petnajstem poglavju podamo seznam kratic, ki smo jih uporabili v doktorski nalogi. Šestnajsto poglavje vsebuje literaturo, na katero smo se navezovali oz. jo citirali. Navedbo elektronskih virov, zakonov in standardov, seznam slik in tabel ter dodatek (matrike in pojasnila) pa smo strnili v sedemnajstem poglavju.

2 PREDSTAVITEV RAZVOJNO RAZISKOVALNEGA DELOVANJA PODJETJA

2.1 PREDSTAVITEV IN ZGODOVINA PODJETJA

Podjetje Metra inženiring, d. o. o., je bilo ustanovljeno leta 1990 in je registriralo svoje poslovanje s primarno dejavnostjo proizvodnje merilnih, preizkuševalnih in navigacijskih instrumentov in naprav (DL33.200).

Kasneje, leta 2000, je primarno proizvodno dejavnost dopolnilo z raziskovalno dejavnostjo po ustanovitvi raziskovalne skupine Metra. Raziskovalna skupina (operativno sestavlja razvojni oddelek) omogoča lasten razvoj produktov, ki jih podjetje tudi samo proizvaja in trži. Skupina je nastala na podlagi sodelovanja s Fakulteto za elektrotehniko v Ljubljani in danes pokriva naslednja raziskovalna področja po klasifikaciji agencije za raziskovalno dejavnost republike Slovenije (ARRS1685):

2.07.05 tehniške vede / računalništvo in informatika / informacijski sistemi – programska oprema,
2.07.07 tehniške vede / računalništvo in informatika / inteligentni sistemi – programska oprema,
2.07.08 tehniške vede / računalništvo in informatika / inteligentni sistemi – strojna oprema,
2.10.05 tehniške vede / proizvodne tehnologije in sistemi / industrijski inženiring,
2.11.04 tehniške vede / konstruiranje / strojni deli, stroji in naprave in
2.18.02 tehniške vede / arhitektura in oblikovanje / oblikovanje (industrijsko, vizualno).

Po klasifikaciji CERIF podjetje v okviru raziskovalne skupine pokriva naslednje panoge:

P170 računalništvo, numerična analiza, sistemi, kontrola,
T120 sistemsko inženirstvo, računalniška tehnologija,
T121 obdelava signalov in
T240 arhitektura, oblikovanje notranjosti.

2.2 NAJPOMEMBNEJŠA RAZVOJNA OBDOBJA PODJETJA

Proizvodni program temelji na lastnem razvoju, proizvodnji, trženju ter vzdrževanju izdelkov in rešitev. Storitve vključujejo svetovanje, proizvodnjo sistemov, izvedbo inštalacije, šolanje strank, postavitev opreme in vzdrževanje sistemov. Metra inženiring na področju varnostno-identifikacijskih sistemov sodeluje s številnimi slovenskimi podjetji in ustanovami (Darsom, Mercatorjem, Zavodom za zdravstveno zavarovanje RS, Gasilsko opremo Ljubljana, kopališči, pravno fakulteto Ljubljana in mnogimi drugimi). Od leta 1993 je distributer za največjega svetovnega proizvajalca čipnih kartic, francosko družbo Gemplus (zdaj Gemalto). Leta 1996 je sodelovalo z irskim podjetjem CSI, eno nosilnih družb na področju elektronskega denarja.

Revija Byte magazine je podjetju Metra inženiring na mednarodni razstavi System 96 v Münchnu podelila nagrado za drugi najboljši industrijski izdelek, in sicer za

SAC BCV – varnostni sistem, ki prepozna biometrične lastnosti (geometrijo) prstov. Poleg tega je Metra inženiring d.o.o. leta 1999 zmagal na tekmovanju RFID 99 v okviru sejma Scantech, ki ga je v Kölnu organizirala družba Automatic ID News Europe. Prvo mesto v kategoriji »Security« je osvojil z izdelkom sistem LCC (Leisure Centre Card) – kartični sistem za identifikacijo in kontrolo. Na podlagi izkušenj, pridobljenih na različnih področjih, ki zajemajo uporabo čipnih kartic in biometrije, podjetje izdelke uspešno prodaja v tujini (v Avstriji, Islandiji, Franciji, Rusiji, Hrvaški, Italiji, Nemčiji itd.). V Sloveniji se udeležuje razvojnih nacionalnih projektov v okviru Ministrstva za gospodarstvo, Ministrstva za visoko šolstvo, znanost in tehnologijo ter programa Eureka.

Ključne poglede strategij prihodnosti pri identifikacijskih sistemih moramo vzeti pod drobnogled ob sprejemanju nove poslovne strategije o konkurenčnem poslovnem okolju. Potrebna je nova vizija upravljanja znanja s stališča obdelave informacij in zakonitosti, ki so veljale v okolju industrijskega poslovanja.

Nov koncept upravljanja znanja temelji na sinergiji med možnostmi, ki jih dajejo nove informacijske tehnologije, ter kreativnostjo in inovativnostjo posameznikov, kar omogoča spretno in hitro prilagajanje zahtevam nastajajočega poslovnega okolja. Če želimo ostati v poslu in zagotavljati dobro podporo svojim strankam, moramo biti hitri, delovati s čim manjšimi fiksnimi in skupnimi stroški, skrajšati razvojni čas izdelka, izboljšati storitve, usposobiti zaposlene za opravljanje nalog, biti inovativni in ponujati visokokakovostne izdelke, biti moramo prilagodljivi, zaznati informacije, oblikovati znanje, ga deliti in se učiti. Vse to ni mogoče brez stalnega razmišljanja o izdelavi, posodobitvi, dostopnosti, kakovosti in uporabi znanja vseh zaposlenih in delovnih skupin v podjetju.

3 IDENTIFIKACIJSKI SISTEMI

Identifikacijske sisteme uporabljamo za prepoznavanje oseb, izdelkov v procesu proizvodnje in prodaje, knjig v knjižnici, živali, avtomobilov v prometu itd. Identifikacijo lahko opravljamo ročno ali pa se izvaja avtomatično, pri čemer se identifikacijski elementi v sistemu samodejno identificirajo prek medija.

Skupna značilnost identifikacijskih sistemov je tako medij, ki z različnimi posredovalci ali nosilci informacij (magnetni trak, črtna koda, proximity[12], RF, MW, biometrične značilke itd.) omogoča zanesljivo elektronsko prepoznavo elementa identifikacije in razlikovanje med pooblaščenimi in nepooblaščenimi uporabniki (Trast International, 2010).

3.1 IDENTIFIKACIJA IN VERIFIKACIJA (AVTENTIKACIJA)

Pogosto se zgodi, da pojem avtentikacija uporabljamo pri verifikaciji in nasprotno (NSCT, 2006). Avtentikacija pomeni določanje osebe na podlagi njenih biometričnih podatkov. Največkrat imamo bazo biometričnih podatkov, s katero primerjamo trenutno zajete podatke, dokler ne najdemo najbolj sovpadajočih. Iščemo med N osebami v bazi, zato tudi pogosto rečemo, da je to 1:N (one-to-many comparison). Pri identifikaciji iščemo identiteto osebe (npr. ime). Pri verifikaciji pa preverjamo, ali je oseba res tista, za katero se predstavlja (Mraović, 2003). V tem primeru imamo samo eno primerjavo 1:1 (one-to-one comparison). Ker vemo, kdo naj bi ta oseba bila (poznamo ime), primerjamo s senzorjem odčitane podatke s podatki te osebe, shranjenimi v bazi.

3.1.1 PREGLED TIPOV KARTIC, KI SO SE IN SE UPORABLJAJO V SISTEMIH KONTROLE PRISTOPA

Čipne kartice (pametne kartice, brezkontaktne kartice ICC ali RFID kartice) so plastične kartice žepne velikosti z vgrajeno anteno in čipom za obdelavo podatkov. ICC kartice na splošno delimo v dve skupini: spominske kartice imajo lahko vgrajena breznapetostni pomnilnik in varnostno logiko, mikroprocesorske pa vsebujejo spominsko in mikroprocesorsko enoto (Četrta pot, 2009).

Osnovne izvedbe kartic so:
- reliefno izbočene kartice (embossed cards),
- kartice s črtno kodo,
- magnetne kartice (magnetic strip cards),
- inteligentne kartice (smart cards),
- pomnilne kartice,
- mikroprocesorske kartice – pametne kartice,
- brezkontaktne inteligentne kartice (contactless smart cards),
- optične pomnilne kartice (optical memory cards),
- Wiegand kartice,

[12] *Proximity cards (ISO, Mifare, Wiegand, MT–Multi Technology itd.) so bralne kartice, ki jih je v 80. letih razvilo podjetje HID.*

- brezkontaktne kartice (proximity cards ali hands-free cards/tags) (slika 3.1). Osnovni radijsko-frekvenčni tokokrog je v kartici in ga sestavljata mikročip in antena. Antena oddaja zakodirane informacije z radijskimi valovi (signalom). Čitalnik kartic ima zmožnost branja ca. od 5 cm do 50 cm (odvisno od modela), sprejema signal in omogoči ali zavrne dostop. Brezkontaktne kartice delujejo na frekvenci 13,56 MHz.) (Hidglobal, 2009).

Slika 3.1: Struktura kombinirane »proximity« ali »hands-free« kartice (Fargo, 2010)

V namene identifikacije so največkrat v uporabi bralne, bralno-pisalne, kombinirane in MiFare kartice.

Bralne kartice so izdelane v skladu s standardom ISO 7816. Vsebujejo integrirano vezje z vpisano 64-bitno serijsko kodo in anteno, v kateri se inducira električni tok in rabi za napajanje. Z njo integrirano vezje na razdalji do 10 cm okrog sebe odda 64-bitno informacijo.

Bralno-pisalne kartice (RW) po merah ustrezajo standardu ISO 7816 in so tudi na pogled enake kot bralne kartice). Poleg 64-bitne serijske kode imajo 256 bitov spomina (EEPROM), v katerega lahko zapišemo osnovne podatke o imetniku kartice (osebno številko, ime in priimek ipd.). Uporabljajo se predvsem v podjetjih za registracijo delovnega časa in pristopno kontrolo. Njihove poglavitne prednosti so varnost pred ponarejanjem, večja odpornost proti odpovedi in možnost zapisa podatkov za različne namene.

Kombinirana RW duel kartica je rezultat razvoja zadnje generacije pametnih kartic in pomeni enostavno rešitev za identifikacijo zaposlenih na vseh ravneh uporabe. V eni kartici sta združena brezkontaktni in kontaktni vmesnik, kar omogoča fizično in logično pristopno kontrolo. Zaposleni se s to kartico identificira prav na vseh korakih od parkirišča do digitalnega podpisa na svojem računalniku. Kartica uporablja najzahtevnejše varnostne metode za uporabo digitalnega podpisa in javnih ključev. Hkrati je ena redkih kartic na svetu, ki jo brez dodatnih gonilnikov prepoznavajo vsi najnovejši Microsoftovi operacijski sistemi in aplikacije.

MiFare pametne kartice ustrezajo standardu ISO 7816, električne signale in prenose pa določa standard ISO 14443-1. Transakcije so opravljene v zelo kratkem času, od 10 do 100 ms. Kartica vsebuje 8192 bitov bralno-pisalnega pomnilnika, 64 bitov je rezerviranih za serijsko kodo. Pomnilnik na kartici je razdeljen na 16 neodvisnih sektorjev, od katerih je vsak zaščiten z dvema ključema, ki omogočata samo bralni ali bralno-pisalni dostop. Kodirana je tudi komunikacija med čitalnikom in kartico. Sistem podpira več kartic v polju enega čitalnika (antikolizija), zato lahko hkrati prepoznava, bere in zapisuje, vendar pa v nekem trenutku komunicira le z eno kartico. Zapis v napačno kartico tako ni mogoč. Pametno kartico uporabljamo pri elektronskem cestninjenju, v avtobusnem javnem potniškem prometu, kot smučarsko vozovnico na nekaterih slovenskih smučiščih in podobno (Četrta pot, 2009).

3.1.2 PODROČJA UPORABE BREZKONTAKTNE RFID TEHNOLOGIJE

RFID tehnologija se uveljavlja na različnih področjih. Naj jih nekaj navedemo:

- kontrola pristopa,
- identifikacija opreme,
- obvladovanje terenskega dela v elektrogospodarstvu,
- brezgotovinsko plačevanje vozovnic in cestnine (Dars–ABC),
- obvladovanje nevarnih snovi,
- identifikacija izdelkov,
- sledenje in identifikacija živali,
- identifikacija in sledenje ljudi (zaporniki, vojaška industrija),
- gostinstvo (plačevanje gostinskih storitev v rekreacijskih objektih; smučišča, bazeni, savne itd.),
- evidenca delovnega časa,
- sledenje izposoje orodja in delovne obleke,
- identifikacija in sledenje vozil (cestni, železniški, pomorski in letalski promet),
- upravljanje izdelkov za zdravstvo in farmacijo in
- sledenje zabojev in prtljage.

Skupina EPC Global želi komercializirati tehnologije EPC in piše svoje lastne standarde. Ta skupina je določila tudi standarde za črtne kode. Prizadeva si, da bi bili EPC protokoli združljivi z ISO standardi. EPC Global je trenutno vodilni razvijalec EPC standardov za podporo RFID in tako podpira pravzaprav vse obstoječe kode GS1[13] (Hunt in drugi, 2007):

- GTIN se uporablja za označevanje izdelkov, embalaže, palet,
- SSCC se uporablja za označevanje in sledenje logističnih enot,
- GLN se uporablja za identifikacijo fizičnih, pravnih ali funkcijskih osebkov,
- GRAI se uporablja za označevanje povratne embalaže,
- GIAI se uporablja za označevanje in sledenje individualnih predmetov (navadno so to predmeti velike vrednosti).

[13] *GS1 je mednarodna neprofitna organizacija. Ustanovljena je bila leta 1977 v Bruslju kot EAN International. Od leta 1987 tesno sodeluje z organizacijo Uniform Code Council (UCC), ki pokriva ozemlje ZDA in Kanade.*

3.1.3 PODROČJA UPORABE KONTAKTNE TEHNOLOGIJE KARTIC

Kontaktna tehnologija kartic (t. i. pametna kartica ali smartcard) je trenutno najbolj razširjena na javnih področjih uporabe (banke, zavarovalnice itd.). Kartico pri uporabi vložimo v čitalnik, ki dostopa do njenega mikroprocesorja in pomnilnika prek pozlačenih kontaktov. Zmogljivosti kontaktnih kartic (procesorska moč, pomnilnik in operacijski sistem) so običajno boljše kot pri brezkontaktnih. Identifikacija je sicer nekoliko počasnejša, vendar zahtevnejša in s tem varnejša. V tabeli 3.1 so navedena osnovna področja uporabe brezkontaktne in kontaktne tehnologije.

Tabela 3.1: Primerjava in dopolnjevanje brezkontaktne in kontaktne tehnologije (Gemalto, 2010; ISO/IEC 14443; ISO/IEC 15693)

	Brezkontaktna tehnologija	Kontaktna tehnologija
Področja uporabe	• pristopna kontrola • registracija delovnega časa • vstop na parkirišče • plačilo malice • plačilo na samopostrežnih avtomatih • elektronska denarnica • identifikacija obiskovalcev • identifikacija v proizvodnji	• pristopna kontrola • vstop v računalnik (log on) • prijava v lokalno omrežje • prijava na internetne strani • digitalni podpis za e-pošto • zapisovanje podatkov na pomnilniški medij • hotelske sobe • bančne aplikacije
Način identifikacije	približanje na 10 do 15 cm	po vstavitvi v režo prek kontaktov
Napajanje kartic in pretok podatkov	RF polje; 125 kHz 13,56 MHz 15,56 MHz	kontakti po ISO 7816-3

Obe kartični tehnologiji na splošno ne tekmujeta med seboj, temveč se dopolnjujeta. Idealna kombinacija je združitev obeh v skupno kartico, ki omogoča večino potrebnih aplikacij ID, od kontrole pristopa skozi vrata do prijave v informacijsko omrežje. Takšni kartici pravimo kombinirana kartica in postaja vse bolj razširjen medij za prepoznavanje oseb. Njeno vsestransko uporabnost in varnost dokazuje tudi odločitev ameriškega ministrstva za obrambo, ki uvaja kombinirano kartico za vse svoje zaposlene.

3.1.4 PODROČJA UPORABE BIOMETRIČNE TEHNOLOGIJE

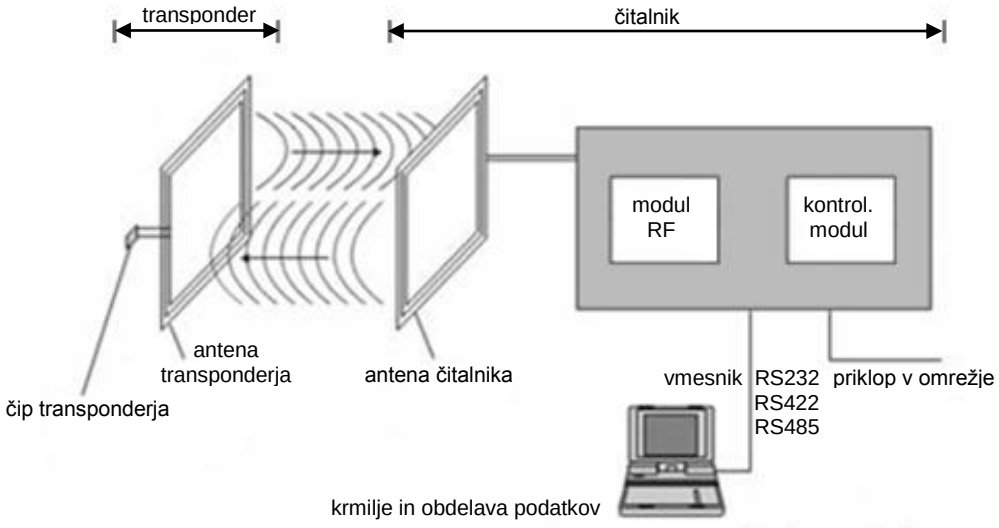
V širšem pogledu uporabo biometrije lahko razdelimo na tri področja:
- sodna medicina (preiskave, identifikacija trupel, določanje starševstva),
- civilna družba (identiteta državljana, distribuiranje socialnega prispevka, prečkanje mej, vozniški izpit) in
- komercialni nameni (bankomati, kreditne kartice, omejevanje dostopa).

Biometrijo pa lahko uporabljamo kot element verifikacije ali identifikacije uporabnika v naslednjih primerih:

- dostop do računalnika,
- dostop do baz podatkov (prepustne kartice, novinarske kartice, izmenljive kartice, identifikacijske kartice),
- prehod čez mejo,
- telefonija (telefonski žetoni),
- odklepanje avtomobila, hiše,
- dostop do zavarovanih območij (laboratoriji, vojaški objekti, tajne obveščevalne službe, tiskarne denarja, potnih listov),
- verifikacija na potovanjih (letališča, potovalni čeki, vavčerji),
- verifikacija pri poslovanju (bančne kartice, čeki, internetno poslovanje, pogodbe, obrazci) in za
- sledenje ter identifikacijo ljudi (Carič in Ajdašik, 2003).

3.2 RFID SISTEMI

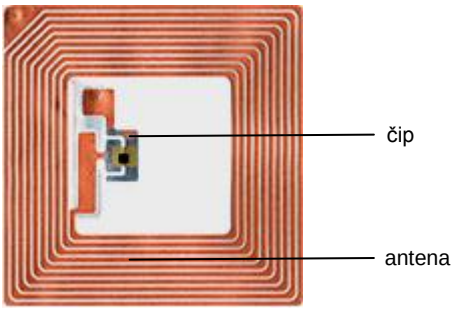
Tipičen RFID sistem sestavljajo štirje glavni deli: tag, enkoder (zapisovalnik podatkov na tag), čitalnik podatkov s taga in računalnik, kot prikazuje slika 3.2. Kar zadeva same čitalnike, so po večini povezani v lokalno internetno omrežje (LAN) ali v brezžično internetno omrežje (WAN), velikokrat pa je treba zagotoviti ločeno infrastrukturo, da ne obremenimo primarnega omrežja.



Slika 3.2: Shema RFID sistema (Emmett in Kern, 2005)

RFID tag (slika 3.3) je narejen iz mikročipa (miniaturnega integriranega vezja) in gibljive antene. Ko je RFID oznaka aktivirana, dekodira prihajajočo poizvedbo (zaporedje ukazov). Vse skupaj je spravljeno v plastično oz. plastificirano ohišje. Enkoder se uporablja za zapisovanje informacij na tag. V uporabo pa prihajajo tudi RFID tagi, ki so že vgrajeni v proizvod ali integrirani v pametne kartice. Radijskofrekvenčna oznaka (RFID) je trenutno zadnja razvojna stopnja v miniaturizaciji mikroračunalnikov. Prenosne oznake RFID so miniaturni, zelo omejeni računalniki, ki za delovanje ne potrebujejo nujno baterijskega napajanja.

Induktivno se lahko napajajo prek zunanje bralne naprave. Energijo za njihovo delovanje pridobimo iz radijskih valov, ki se hkrati uporabljajo tudi za prenos informacij. RFID oznake zmorejo obdelati le majhno količino informacij, običajno imajo manj kot 1024 bitov delovnega spomina. Radiofrekvenčna identifikacija je gotovo obetavna tehnologija za avtomatično identifikacijo.



Slika 3.3: RFID tag (RVB Group, 2010)

RFID tehnologija je po svojem bistvu podobna tehnologiji črtne kode (slika 3.4), nedvomno najbolj znani in uveljavljeni tehnologiji avtomatične identifikacije, a jo v marsičem presega. Sistem črtne kode je sestavljen iz čitalnika in etikete s črtno kodo, ki je na objektu, medtem ko RFID sistem sestavljata čitalnik in RFID priponka, ki je na objektu ali je celo njegov sestavni del. Branje črtne kode temelji na principu odboja čitalnikove izsevane svetlobe od črtne kode. Prenosni medij med čitalnikom in etiketo s črtno kodo je torej svetloba. Pri identifikaciji z RFID tehnologijo gre za izmenjavo radijskih signalov nizke moči med čitalnikom in priponko, prenosni medij pa so radijski valovi.

Slika 3.4: Črtna koda (GS1, 2009)

3.2.1 VRSTE RFID SISTEMOV

Odzivniki RFID se na osnovi oddajanja sporočil delijo na aktivne, pasivne, induktivne in elektromagnetne (Brown, 2007).

3.2.1.1 Aktivni RFID sistem

Oddajniki poleg antene in čipa vsebujejo tudi baterijo, ki napaja njihovo vezje. Zato so bistveno dražji in večji, imajo pa precej prednosti, kot so večja moč oddajanja,

daljši domet in zanesljivejše delovanje v neprijaznem okolju (bližina kovine ali tekočine).

3.2.1.2 Pasivni RFID sistem

Pasivni sistemi v nasprotju z aktivnimi nimajo svojega napajanja, temveč energijo, potrebno za delovanje, dobijo neposredno od signala, ki se inducira v anteni. Sprejeti izmenični signal se usmeri ter dovede do čipa, ki se zbudi in prične delovati. Ker pasivni oddajniki ne vsebujejo baterije, so precej cenejši in manjši od aktivnih, vendar imajo veliko krajši domet in so manj zanesljivi, kar zadeva napake.

3.2.1.3 Induktivni RFID sistem

Induktivni RFID sistem za prenos informacije uporablja princip magnetne indukcije. Dve bližnji tuljavi sta induktivno sklopljeni, ko magnetni pretok, ki ga povzroča tok prve tuljave, doseže drugo in na njenih priključnih sponkah inducira napetost. Komunikacija deluje v bližnjem polju (približno 0,16 valovne dolžine), zato je domet induktivnih sistemov razreda nekaj deset centimetrov in pada z naraščanjem frekvence (krajšanje valovne dolžine). Oddajnik informacijo prenese čitalniku z uporabo bremenske modulacije (load modulation), ki v praksi pomeni spreminjanje sklopnega faktorja med tuljavama v ritmu podatkov.

3.2.1.4 Elektromagnetni RFID sistem

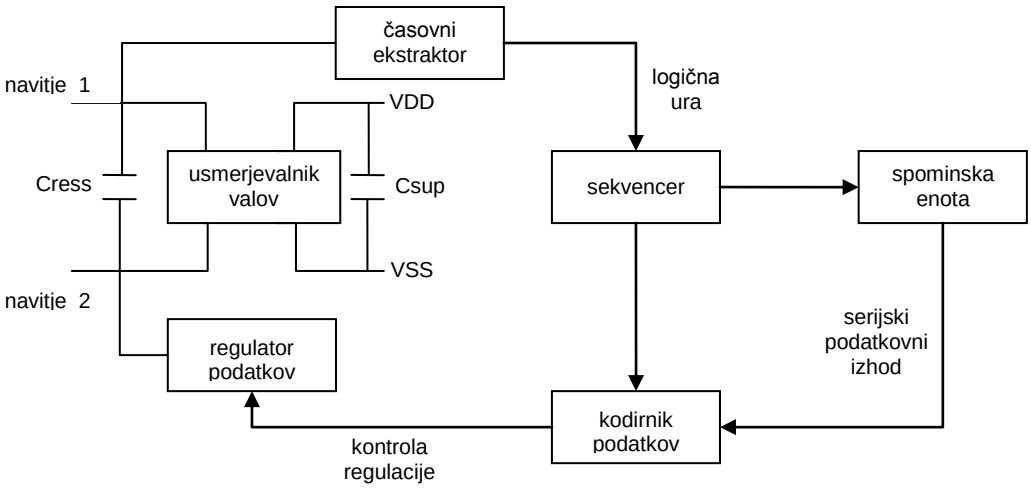
Sistem komunicira z uporabo elektromagnetnih (EM) valov. Čitalnik oddaja EM valove, ki dosežejo oddajnik in se od njega odbijejo. Ta odboj lahko izkoristimo za prenos informacije od oddajnika do čitalnika. V trenutku, ko se oddajnik zbudi, začne svojo lastno impedanco spreminjati v ritmu podatkov in tako spreminja svojo oscilacijsko frekvenco. Signal, ki se odbije, je zato moduliran, celoten pojav pa imenujemo modulacijski odboj (modulation backscatter).

Glede na način funkcionalnosti razlikujemo naslednje RF kartice (Brown, 2007):
- bralne kartice (RO),
- bralno-pisalne kartice (RW HITAG1),
- pametne bralno-pisalne kartice (MF),
- kombinirane brezkontaktne in kontaktne kartice (RW DUEL) in
- plastične kartice standardnih dimenzij kot službene izkaznice.

3.2.2 PRINCIP DELOVANJA

Premikanje elektronov povzroči EM valovanje, ki se razširja po zraku. Na svoji poti se lahko razširja tudi skozi nekatere vrste fizičnih objektov oz. ovir, celo skozi vakuum. Število nihajev EM valovanja na sekundo imenujemo frekvenca, katere merska enota je hertz (Hz), razdalji med dvema vrhovoma (peak) valovanja pa rečemo valovna dolžina. S priključitvijo ustrezno velike antene v električni krog lahko uspešno oddajamo in sprejemamo EM valovanje, pri čemer mora biti seveda na ustrezni razdalji nameščen tudi sprejemnik. Na tem principu temeljijo vse brezžične komunikacije.

Pri RFID komunikaciji se moramo osredotočiti na značilnosti prenosa radijskih valov na razmeroma kratkih razdaljah. Elektromagnetni valovi se skozi vakuum razširjajo s svetlobno hitrostjo. Pri bakreni žici se ta hitrost zmanjša na približno dve tretjini in postane na neki način odvisna od frekvence. Čitalnik ustvarja v svoji okolici šibko radiofrekvenčno magnetno polje. Ko se RFID element približa čitalniku in vstopi v njegovo polje, se »vzbudi« elektronsko vezje v priponki in odda svoj podatek (lastno identifikacijsko kodo, podatke) v obliki radijskega signala. Čitalnik ta signal sprejme in ga v ustrezni obliki sporoči računalniku. Če gre za bralno-vpisovalne priponke, lahko čitalnik tudi »zapiše« nove podatke v notranji pomnilnik priponke (slika 3.5) (Finkezzeller, 2002).



Slika 3.5: Shematski prikaz RFID konfiguracije vezja (Finkezzeller, 2002)

Pri RFID kartičnih sistemih poznamo naslednja frekvenčna območja (Čeh-Ambruš, 2006):

- LF (low frequency): nizkofrekvenčni sistem za katerega je značilno, da imajo nalepke veliko ovojev žice na anteni in zelo kratek domet,
- HF (high frequency): visokofrekvenčni sistem deluje na območju 13,56 MHz in ima na anteni manj ovojev kot LF ter daljši domet in
- UHF (ultra high frequency): ultravisokofrekvenčni sistem je najsodobnejši in se dandanes tudi največ uporablja. Omogoča hiter prenos podatkov (možno je prebrati več RFID nalepk hkrati). Prav tako so nalepke veliko cenejše, saj so antene močno poenostavljene (imajo zelo malo ovojev).

Radijski, infrardeči, mikrovalovi in del valov vidnega spektra se lahko uporabljajo za prenos informacij prek amplitudne, frekvenčne ali fazne modulacije. Poznamo dve vrsti brezkontaktnih kartic:

- pasivne kartice: aktivirajo se, ko pridejo v območje magnetnega polja čitalnika in
- aktivne kartice: vsebujejo baterije z dolgo življenjsko dobo (long-life battery) in neprestano pošiljajo signal v enakih časovnih zamikih.

Cenovno gledano so aktivne kartice štirikrat dražje od pasivnih. Razdalja med aktivno kartico in čitalnikom pa je do dveh metrov. Prednost tega je možnost, da so

čitalniki skriti in tako lahko spremljamo gibanje zaposlenih ali obiskovalcev po objektu, ne da bi se ti tega zavedali. V tabeli 3.2 sta podana pregled različnih frekvenčnih območij in razdalja branja za posamezne brezkontaktne kartice.

Tabela 3.2: Pregled različnih frekvenčnih območij in razdalj branja proximity kartice (Elatec, 2011; ISO/IEC 14443; ISO/IEC15693)

frekvence	LF (30–300) KHZ	HF (3–30) MHZ	UHF (300–1000) KHZ	mikrovalovi od 1 GHZ naprej
razdalja branja	pod 2 m 1 cm–1,5 m	pod 1 m 1 cm–0,7 m	1–100 m 1–3 m	1–300 m 1–10 m
hitrost komunikacije	1–10 kb/s	10–200 kb/s	1 kb/s–10 Mb/s	1 kb/s–10 Mb/s
občutljivost	velika	povprečna	povprečna/ majhna	majhna

3.2.3 PREDNOSTI RFID TEHNOLOGIJE

Naštejmo nekaj osnovnih prednosti RFID tehnologije:

- Ni potrebe po vidnem polju. Tehnologija ne zahteva, da je priponka v vidnem polju čitalnika (kot pri črtni kodi).
- Prilagojenost zahtevnim okoljem. Zaradi principa delovanja je RFID idealna rešitev za okolja, v katerih sta nečistoča in vlaga. RFID priponke je mogoče prilagoditi najzahtevnejšemu industrijskemu okolju (ekstremne temperature, vlaga, jedke tekočine, velika mehanska odpornost).
- Dolga uporabna doba. Ker RFID čitalniki in priponke ne vsebujejo nobenih premikajočih se delov, redko potrebujejo vzdrževanje, njihova uporabna doba pa je zelo dolga. Zato lahko trdimo, da je RFID najcenejši način avtomatične identifikacije.
- Zaščita podatkov. Drugače kot pri črtni kodi je kopiranje RFID priponk tako rekoč nemogoče, zato je ta tehnologija idealna za aplikacije, pri katerih je identifikacija oseb ali predmetov zaupnejše narave.
- Hitrost zajema. Čitalnik zajame podatek iz RFID priponke v nekaj milisekundah. Dejanski čas zajema je sicer odvisen še od izvedbe komunikacije z računalnikom, vendar velja, da celoten proces traja največ nekaj deset milisekund.

3.2.4 TEŽAVE PRI IMPLEMENTACIJI RFID TEHNOLOGIJE

Ovira pri implementaciji RFID tehnologije so po mnenju nekaterih avtorjev tudi različna frekvenčna območja za njeno uporabo. Frekvenčno območje namreč ni enotno za vse celine[14], zato potrebujemo na svetovni ravni več različnih RFID bralnikov. Prav tako težave povzročajo elektromagnetne motnje pri branju ter interferenca med bralnikom in oznakami (Marić, 2005). V letu 2006 so raziskovalci

[14] *Težava za omenjeno področje so neenotni standardi po svetu. Izhodiščni standard, ki pokriva radiofrekvenčno območje sistema RFID, je ISO 18000.*

Fakultete za znanost pri Univerzi v Amsterdamu pokazali dve možnosti za spremembo informacij na RFID oznakah, kar z vidika varnosti pomeni potencialno veliko teroristično grožnjo. Problem z branjem nalepk pa se pojavlja pri sistemu UHF RFID na kovini in v vodi, vendar ga že intenzivno rešujejo. Tako lahko že danes z ustrezno izbiro nalepk zmanjšamo ali celo odpravimo to pomanjkljivost.

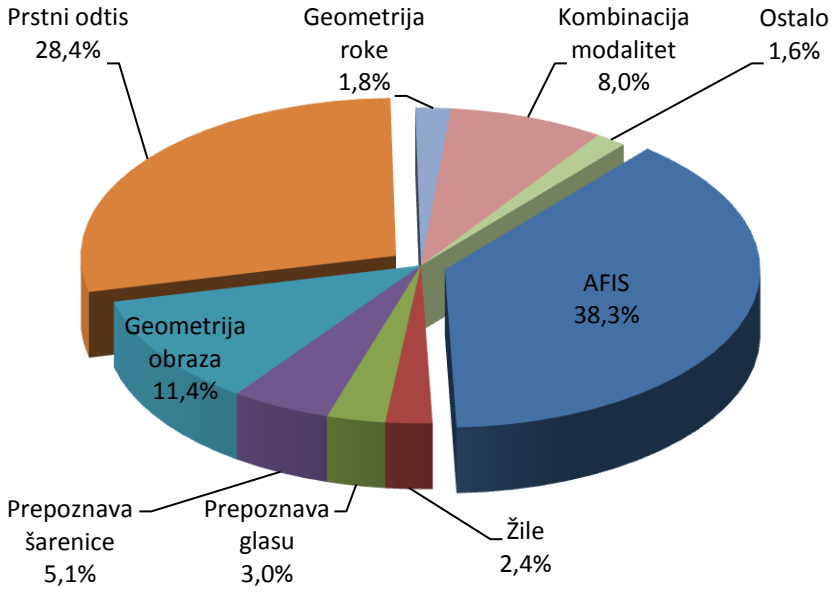
3.3 BIOMETRIČNI SISTEMI

Biometrija je veda o prepoznavanju identitete posameznika glede na njegove edinstvene lastnosti. Je proces zbiranja, proučevanja in shranjevanja podatkov o posameznikovih fizičnih lastnostih in vedenjskih značilnostih z namenom identifikacije in avtentikacije. Biometrične fizične značilnosti so prstni odtis, oblika obraza, geometrija roke, geometrija prsta, žilni sistem roke, žilni sistem obraza, žilni sistem mrežnice, telesni vonj, vzorec šarenice, oblika linij prsta in linija gub na dlani. K vedenjskim značilnostim pa lahko štejemo strukturo glasu, statični podpis, dinamični podpis, značilno tipkanje itd.

Glavna domena biometrije pri osebni identifikaciji in avtentikaciji je priskrbeti verodostojna in kakovostna dokazila pri odgovorih na vprašanji (Chirillo in Blaul, 2003):

- Kdo sem (si)? Biometrična identifikacija.
- Ali sem (si) res to, za kar se izdajam (izdajaš)? Biometrična avtentikacija, verifikacija ali overjanje.

Tehnologija prepoznavanja prstnega odtisa (slika 3.6) v svetovnem merilu dosega 49-odstotni tržni delež, in se vsako leto povečuje. Sledijo obraz s 15 odstotki, geometrija roke s 10 odstotki, šarenica s 6 odstotki itd.



Slika 3.6: Tržni delež modalitet biometrične tehnologije (International Biometric Group, 2009)

Odčitavanje biometričnih značilnosti je proces preverjanja ali dodeljevanja identitete in ravno v tem se identifikacija in verifikacija razlikujeta. Osebna identifikacija je proces, pri katerem naprava poveže določeno osebo z njeno identiteto. Pomeni, da osebi dodelimo identiteto glede na prej odvzete biometrične značilnosti iz baz podatkov. Verifikacija (avtentikacija) pa pomeni preverjanje, ali je oseba, za katero se predstavlja, res ta oseba.
Biometrični sistemi se sami po sebi zelo razlikujejo, če ne gledamo na tip značilnosti, ki jo pregledujemo. Pozorni moramo biti na naslednje dejavnike (Carič in Ajdašik, 2003):

- delovanje: natančnost, hitrost, velikost, vpliv zunanjih dejavnikov,
- sprejemljivost: ali so ljudje, vključeni v takšen način preverjanja identitete, pripravljeni delovati s takšnim sistemom in
- ukanljivost: kako hitro lahko sistem prevaramo.

Razlog, da tržni delež tehnologije prepoznavanja prstnega odtisa zelo narašča, je tudi ugodna cena čitalnikov prstnega odtisa, ki je primerljiva s sedanjimi čitalniki »pametnih kartic«, hkrati pa zagotavljajo bistveno višjo stopnjo varnosti. Zaradi vse večje odvisnosti od informacijskih sistemov in globalizacije poslovanja je nujnost razpoložljivosti informacij vedno večja. Zagotoviti moramo verodostojne in hitro dosegljive informacije ter upoštevati njihovo morebitno zaupnost. Zavedati se je treba, da razvoj ter implementacija biometričnih sistemov v procesu identifikacije ni cilj, pač pa pot. Neprestano se spreminjajo okolje, ranljivost informacijskih sistemov ter grožnje. Prav tako se spreminjata strojna in programska oprema, pa tudi zaposleni, ki jo upravljajo. Pomemben dejavnik pri zagotavljanju varnosti je identifikacija osebe oz. preverjanje, ali je oseba res ta, za katero se izdaja. Preverjanje mora biti zanesljivo, hitro, ne sme posegati v telo in na voljo mora biti za primerno ceno. V preteklosti je tovrstno preverjanje temeljilo na identifikacijski kartici, obesku, geslu, PIN kodi, podpisu ali celo na prepoznavanju osebe s strani varnostnika ali vratarja in večinoma je tako še danes. Toda vsi ti načini so glede na zahteve v sodobnem svetu postali nezanesljivi in zelo omejeni. Biometrija ponuja enostavno, zanesljivo in cenovno ugodno rešitev pri preverjanju identitete uporabnikov, ki jo lahko uporabimo tudi na nenadzorovanih in oddaljenih območjih. Prihodnost identifikacije je torej na strani biometrije.

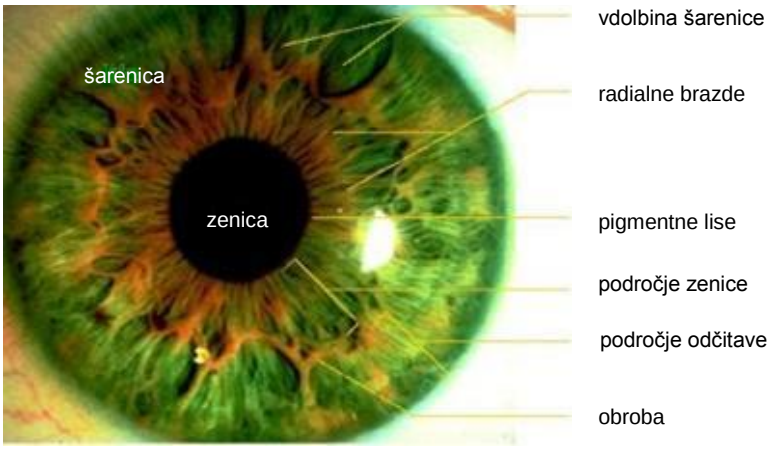
3.3.1 RAZLIČNI POSTOPKI BIOMETRIČNE IDENTIFIKACIJE

V podpoglavjih so opisani nekateri najpogosteje uporabljeni postopki biometrične identifikacije.

3.3.1.1 Identifikacija na osnovi prepoznavanja šarenice

Za šarenico je značilno, da niti levi in desni vzorec istega človeka nista enaka, kaj šele, da bi bila enaka pri več ljudeh. Naprava deluje tako, da kamera zajame oko (slika 3.7) in signal spremeni v digitalno obliko. Zanimivo je, da postopka ne motijo niti kontaktne leče. Za uspešno identifikacijo zadostuje 20 % šarenice. Naprednejše metode nam dajo 3,4 bita/mm^2 podatkov pri 19 - mm premeru šarenice. Pri takšni gostoti podatkov lahko rečemo, da ima vsaka šarenica 266 DOF. Druge biometrične metode dosegajo od 13 do 60 DOF (Wayman, 1999). Seveda se tu pojavljajo omejitve. Največja je omejitev samega korelacijskega algoritma, poleg tega se prirojene lastnosti šarenice razlikujejo od posameznika do posameznika. Realno

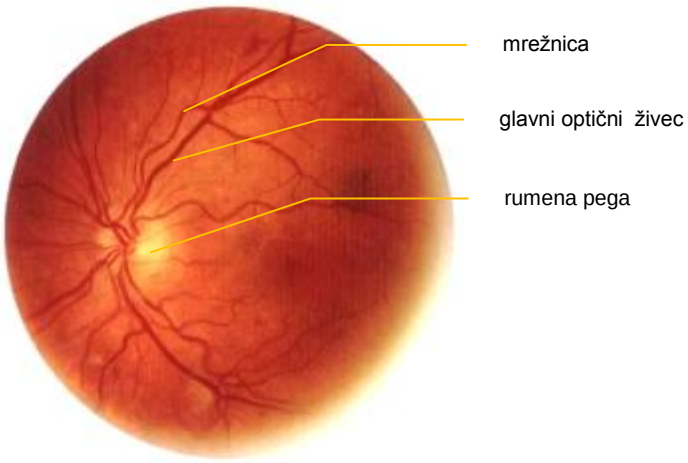
lahko pričakujemo do 170 DOF. Podatki se shranijo v 512 - bajtne šablone (angl. templates). To omogoča zelo hitro primerjanje (500.000 primerjav na sekundo). Boljši algoritmi vse zaznane lastnosti hranijo v obliki vektorjev in z njim tvorijo fazorski diagram. To jim omogoča zelo veliko točnost in hitrost primerjanja. Algoritem, ki primerja dve šarenici med seboj, ne primerja njunih slik, ampak le fazorske diagrame.



Slika 3.7: Struktura šarenice pri biometrični identifikaciji (Mainguet, 2010)

3.3.1.2 Identifikacija na osnovi prepoznavanja mrežnice

Očesna mrežnica (slika 3.8) je sloj krvnih žilic na zadnji strani očesa in tvori značilen vzorec, ki prične razpadati kmalu po smrti. Pri postopku prepoznave mora oseba gledati v določeno točko, sproži se bliskavica in tako naprava prepozna sloj krvnih žilic na zadnjem delu očesa (Marin˜o, 2006). Slabost te oblike je ravno svetloba, ki se pojavi pri postopku, zaradi katere se ljudje pogosto pritožujejo. Uporablja se pri visokih stopnjah varnosti, kjer je varnost na prvem mestu.

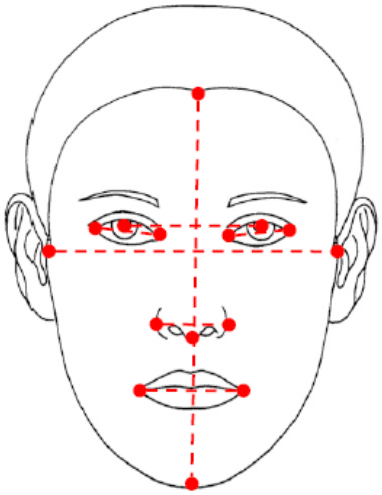


Slika 3.8: Struktura krvnih žil mrežnice pri biometrični identifikaciji (Mainguet, 2010)

3.3.1.3 Identifikacija na osnovi prepoznave obraza

V preteklosti so se sistemi zanašali na enostavne geometrijske lastnosti obraza. Osnovni korak pri sistemih prepoznave obraza je zajem ustrezne slike obraza, in ker gre za dinamičen sistem, potrebujemo najmanj 3 do 5 slik na sekundo pri minimalni ločljivosti 320 x 200 točk (pikslov). Algoritem nato analizira sliko z različnimi metodami oziroma s kombinacijo metod. Po opravljeni analizi se podatki primerjajo z bazo podatkov. Algoritmi za izvajanje analize slonijo na kompleksnih matematičnih metodah, kar zahteva veliko procesorsko moč.

Povsem drugačen problem je prepoznavanje posameznika v množici, saj moramo iz celotne okolice identificirati le obraze. Takšni sistemi so prvi korak k popolni avtomatiziranosti sistemov za prepoznavanje obraza (Mraović, 2003). Pri obrazu prav tako razlikujemo dva tipa prepoznave. Najpogostejši način uporabe je video identifikacija, medtem ko drugi uporablja termično obdelavo. Pri prvem načinu (slika 3.9) osebo zajame kamera, ki si zapomni nekaj značilnih točk na obrazu (npr. položaj oči, ust, nosnic in razdalje med točkami).

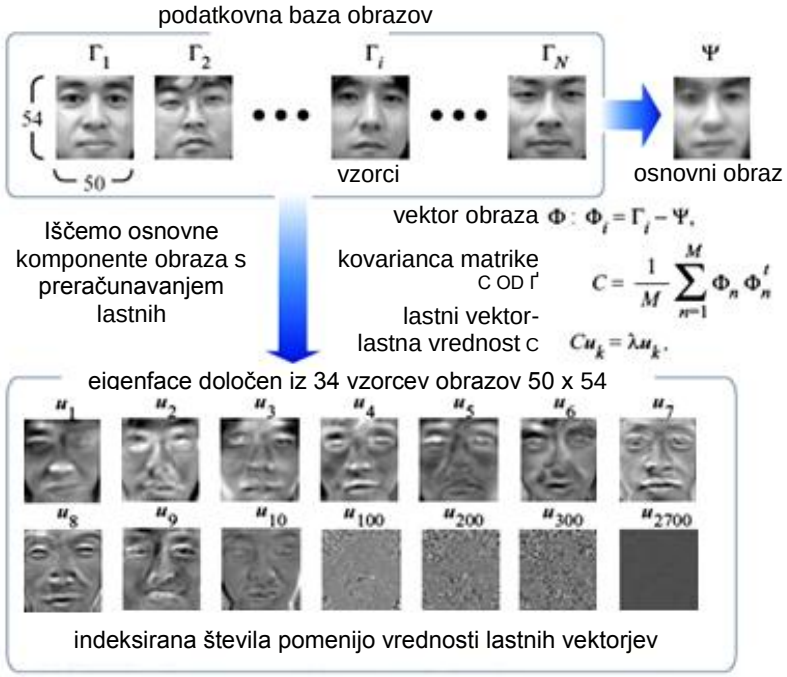


Slika 3.9: Prepoznava obraza na osnovi dvajsetih obraznih značilk (Jain, 2010)

Prepoznave ne zmotijo niti obrazna mimika, očala, klobuk ali brada. Pri termični obdelavi (slika 3.10) obraz zajame infrardeča kamera, prepoznava se izvede na podlagi cepitve krvnih žilic v obrazu. Prednost tega postopka je, da se lahko opravi brez uporabe rok, pri čemer enostavno pogledamo v nameščen zaslon. Oseba tako ne ve, kdaj se njen obraz analizira. Največkrat se uporablja v igralnicah in na letališčih.

Slika 3.10: Termična slika obraza (Mainguet, 2010)

Eigenface postopek je patentirana tehnologija, razvita na inštitutu MIT. Temelji na 2D sivinskih slikah, ki vsebujejo podatke o različnih obraznih lastnostih (eigenvector) vektorskega prostora, ki omogočajo identifikacijo ljudi. Te lastnosti se uporabljajo pri prepoznavi obraza na osnovi računalniškega vida (Turk in Pentland, 1991). Na sliki 3.11 vidimo eigenface več ljudi, pridobljenih z aproksimacijo različnih slik posameznika.

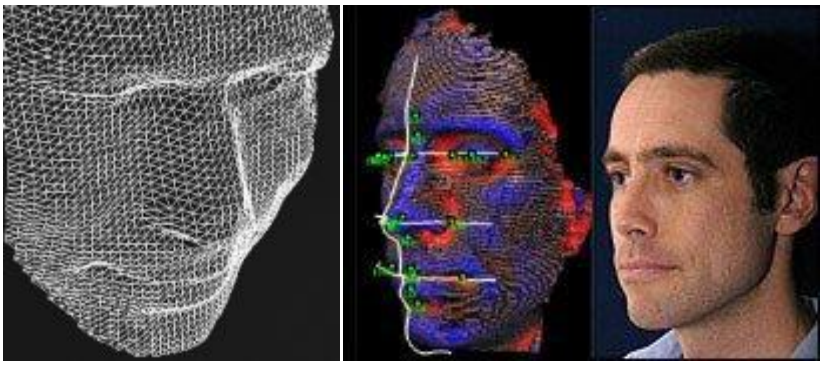


Slika 3.11: Metodologija eigenface (Ando in drugi, 2004)

Eigenface aproksimiramo iz nekaj slik, na katerih z algoritmom poiščemo določene lastnosti (PCA metoda). Ponavadi se za aproksimacijo uporabijo slike več obraznih izrazov iste osebe, slike z očali in brez njih, z brado oz. brki in brez njih ter z različnimi pričeskami (čop, kitke itd.). Vsakemu eigenfaceu je treba določiti še spol,

raso, ime, starost in druge potrebne lastnosti (Huang in drugi, 2005). Metoda je uporabna tako za prepoznave 1:N kot za 1:1. Zanjo je treba zagotoviti dobro osvetljen prostor in kakovostne slike sprednje strani obraza.

Metoda LFA (slika 3.12) se pri prepoznavi obraza največkrat uporablja. Zelo je podobna metodi eigenface, le da se je bolj sposobna prilagajati spremembi videza osebe, spremembi svetlobe, spremembi pričeske, barvi kože in različnim modnim dodatkom. LFA analizira veliko lastnosti na različnih delih obraza, pri tem pa upošteva tudi relativne razdalje (npr. med očmi, od ust do nosu itd.). Izbrane lastnosti se uporabijo kot gradniki obraza. Pri identifikaciji oz. verifikaciji se upošteva tip gradnika (značilnosti okoli ust, oči itd.) kot tudi postavitev na obrazu. Metoda zna predpostavljati, da se majhni odmiki določene lastnosti (npr. ust) kažejo kot majhni odmiki različnih lastnosti v njeni bližini. Najboljše rezultate dobimo s slikami sprednje strani obraza, čeprav metoda pravilno prepoznava tudi pri odmikih do 25°. Težave se pojavijo, ko imamo kompleksno ozadje (Mraović, 2003).



Slika 3.12: Metoda prepoznave obraza LFA (Mainguet, 2010)

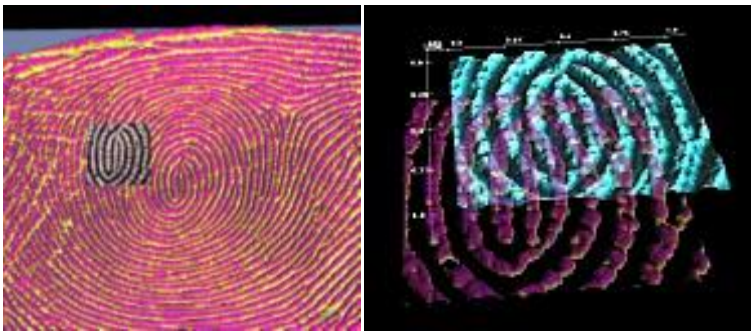
Identifikacijska metoda z uporabo nevronske mreže temelji na »učenju« nevronske mreže. Mreža ima npr. v spominu neki obraz, in ko zajamemo sliko nekega drugega obraza, začne obraz v spominu prilagajati temu obrazu. Nastavljati začne razne »uteži«, ki vplivajo na identifikacijo obraza. Teoretično se lahko nauči prepoznati obraze tudi pri zelo slabih pogojih zajemanja slike. Metoda analizira celotno sliko, na kateri išče kontrastne elemente (oči, obrvi, usta, ličnice itd.). V praksi se postopek uporablja tako za identifikacijo kot za verifikacijo (Bunney, 1997).

Kljub vse cenejši strojni opremi pa je še vedno razmeroma velik strošek ustrezna programska oprema, ki opravi meritve in primerjanje. Cene kakovostnih programov se gibljejo okoli nekaj tisoč evrov.

3.3.1.4 Tehnologija prstnih odtisov

Tehnologijo prstnih odtisov (slika 3.13) so najprej uporabljali v vojski in policiji, vendar je vse bolj razširjena tudi na komercialnih trgih. Na voljo je več sistemov tovrstne prepoznave. Analizirajo se jasna znamenja na prstu ali razlika med grebeni prsta (Khanna, 2004). V praksi je ta vrsta priznana kot zelo zrel način preverjanja identitete, zato se tudi uporablja pri finančnih transakcijah, varovanju omrežja,

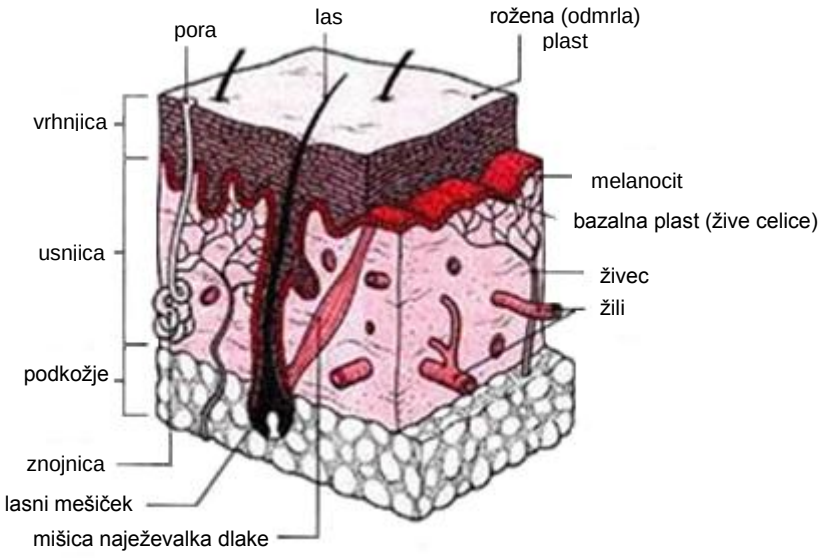
nadzorovanju gibanja posameznikov in forenziki. V raziskavi doktorske naloge se bomo osredotočili predvsem na identifikacijo na osnovi prstnega odtisa.



Slika 3.13: Vzorec prstnega odtisa (ScienceGL, 2008)

3.3.1.5 Poroskopija

Poroskopija (Maver, 2004) je metoda ugotavljanja identifikacije s primerjavo znojnih por na papilarnih linijah. Začetnik poroskopije je Locard, ki je s preiskavami ugotovil, da je velikost por med 88 in 220 ym. Leta 1912 sta s poizkusom predstavila vrednost poroskopije Boudet in Simonin. Označila sta 901 prstno znojno poro in več kot 2000 znojnih por na odtisu dlani. Predlagal je metodo identifikacije, ki temelji na velikosti, obliki, lokaciji in pogostosti znojnih por – menil je, da za pozitivno prepoznavo zadostuje od 20 do 40 skladnih por (slika 3.14).



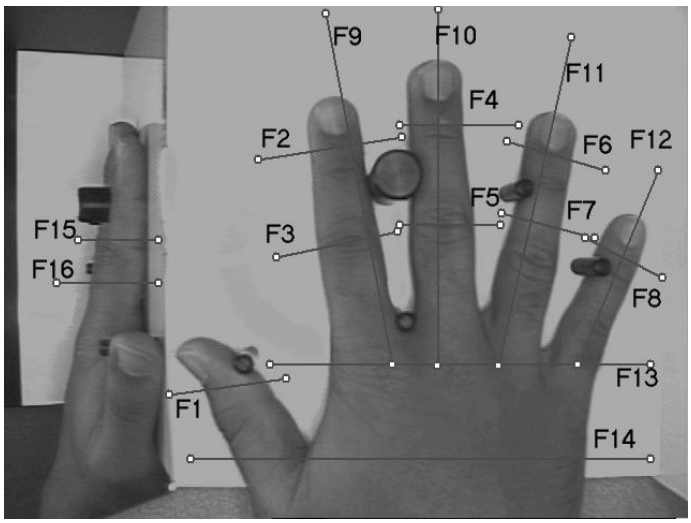
Slika 3.14: Zgradba kože (Standring, 2004)

Na ta način so se izognili težavam, ki nastanejo pri identifikaciji otrok in ostarelih, saj imajo ti precej plitek odtis, ter ljudi z začasno ali trajno poškodovanimi blazinicami prstov.

3.3.1.6 Geometrija rok oz. dlani in prsta

Leta 1971 so strokovnjaki z raziskovalnega inštituta Stanford dokazali različnost človeških dlani. Zaradi majhne ponovljivosti (verjetnost ponovljivosti je 1/10.000) je metodo mogoče uvrstiti med identifikacijske postopke. Z meritvami ugotovimo dolžino in debelino prstov, širino dlani pri različnih točkah, radij dlani, prosojnost kože ter obliko in debelino dlani. Metoda z geometrijo roke (slika 3.15) je ena najhitrejših biometričnih metod, vendar pa je zaradi neunikatnosti roke uporabna le za hitro verifikacijo 1:1 (Jain in drugi, 1999). Njena izboljšava poteka v smeri povečanja točnosti takega merjenja. Ena od izboljšav je dodatna kamera, ki meri tudi debelino roke s strani.

Tehnologija uporablja tridimenzionalno sliko dlani in izmeri ostrino, širino in dolžino prstov in členkov. Je ena najbolj uporabljanih vrst biometrije v današnjem svetu. Njeni prednosti sta velika prilagodljivost različnim uporabnikom in dolga uporabna doba, saj se dobro obnese tudi v zunanjih pogojih.



Slika 3.15: Geometrija dlani (Jain in drugi, 1999)

Sistem za zajemanje geometrije roke je sestavljen iz izvora svetlobe (običajno IR), CCD kamere, ogledala za bočno projekcijo in ravne površine z več (običajno petimi) zatiči, ki rabijo za točno namestitev dlani ter prstov. Mogoče je spreminjati jakost svetlobnega vira in ostrenje objektiva kamere. V praksi se najpogosteje zajema geometrija desne dlani. Oseba pri verifikaciji položi dlan na ravno površino s prsti med zatiči, ogledalo pa v objektiv kamere projicira tudi bočno sliko dlani, ki je pomembna za določanje debeline prstov. Sistem za zajemanje geometrije dlani se priključi neposredno na PC, kar omogoča enostavno metodo verifikacije uporabnika, predvsem pri računalniških omrežjih, kjer uporabniška gesla zaradi prenosljivosti pomenijo razmeroma slabo zaščito podatkov.

Pri verifikaciji geometrije roke poznamo dva načina preverjanja identitete:

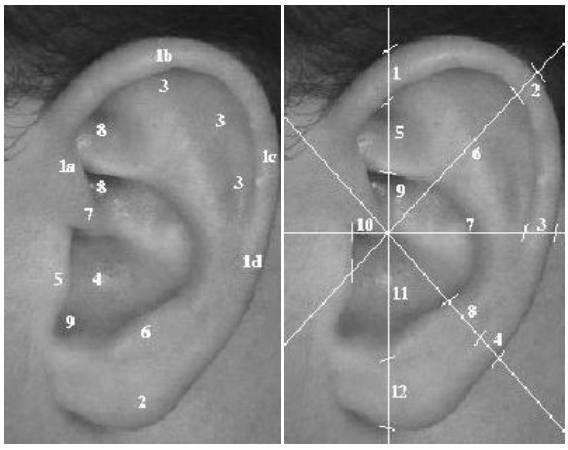
- uporabnik uporablja PIN kodo ali kartico s svojo ID kodo,
- uporabnik ima svojo predlogo shranjeno na pametni (smart) kartici.

V prvem primeru se pri uporabi PIN kode ali kartice s strežnika s podatkovno bazo (na varovani strani objekta) izvede prenos ustrezne predloge do verifikacijske naprave, nato se opravi primerjava in na koncu sledi rezultat: vzorec se bodisi ujema ali ne. V drugem primeru je predloga shranjena že na pametni kartici (ne v verifikacijski napravi), kar pomeni, da se po predložitvi kartice v sistem neposredno izvede primerjava 1:1 s predlogo na kartici, na podatkovni strežnik pa se zapiše le »transakcija«.

V samostojnem režimu delovanja (stand alone) naprava prevzame vlogo lokalnega sistema kontrole pristopa, ker lahko neposredno krmili npr. električno ključavnico vrat ter prejema sporočila (pogoje) in jih predaja drugim sistemom tehničnega varovanja (npr. sistemu za javljanje vloma ali javljanje požara), kar je v praksi velikokrat zelo uporabna rešitev. Velikost zapisa, shranjenega v bazi računalnika, je navadno od 9 do 100 bajtov.

3.3.1.7 Geometrija ušesa

Osebna identifikacija se lahko izvede tudi na osnovi geometrije ušesa. Presečiščno točko določimo iz dveh navzkrižnih diagonal pravokotnika. S prilagajanjem določimo oddaljenosti točke presečiščne točke do vrhnje točke, desne točke, najnižje točke in skrajno leve točke ušesa. Dobimo razdalje *1*, *2*, *3* itd. (slika 3.16a in b), katerih razmerja so potrebna za identifikacijo človeka (Rahman, 2007).



Slika 3.16 a in b: Geometrija ušesa (Burge in Burger, 1998)

3.3.1.8 Dinamika tipkanja

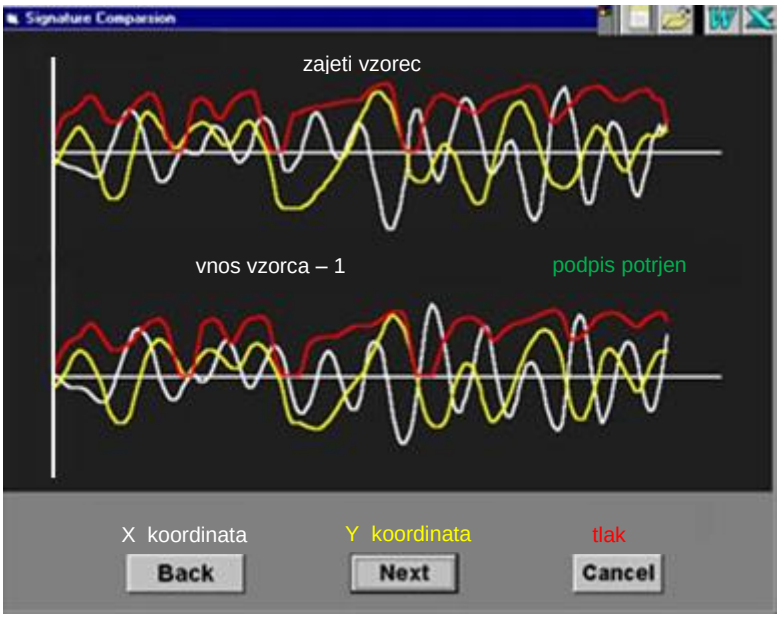
Vsak posameznik na tipkovnico tipka na svojevrsten način. Ta biometrična identifikacija temelji na časovnih presledkih med tipkanjem. Za identifikacijo se

opravlja meritev časovne manipulacije tipke in med tipkami (Ilonen, 2003) (slika 3.17).

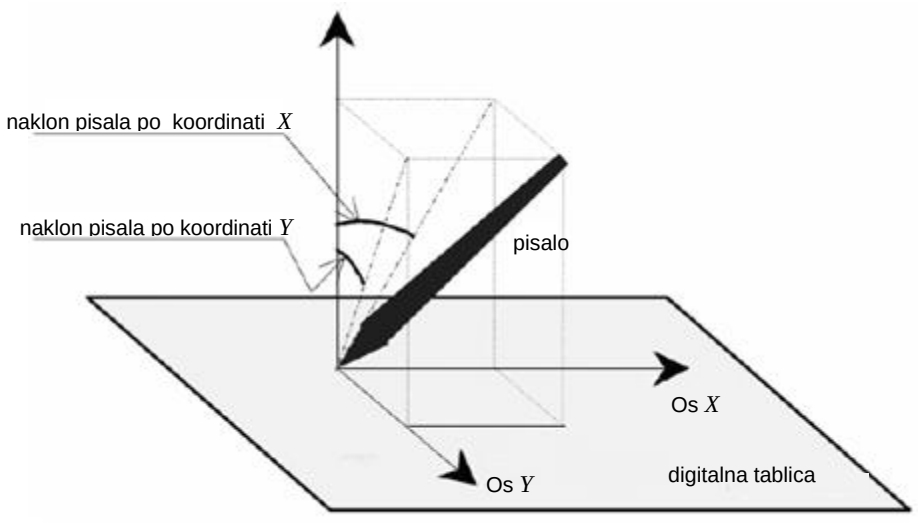
Slika 3.17: Dinamika tipkanja (Olzak, 2007)

3.3.1.9 Preverjanje podpisa

H geometriji spada tudi preverjanje podpisa (slika 3.18a). Tu se opazuje kot, pod katerim oseba drži pisalo, čas, potreben za podpis, kakšen je bil pritisk na podlago in kolikokrat je oseba pisalo dvignila s papirja (Janbandhu in Siyal, 2001) (slika 3.18b).



Slika 3.18a: Potrjevanje istovetnosti podpisa (NSTC, 2009)



Slika 3.18b: Naklon pisala pri potrjevanju istovetnosti podpisa (Drygajlo, 2005a)

3.3.1.10 Prepoznava glasu

Pri prepoznavi glasu (slika 3.19) se ugotavljajo njegov ritem, uglašenost in ton. Govorni signal je vhod v procesor, ki opravlja nalogo vhodnega filtra. Zaznava začetek, konec signala, nastavlja ojačenje in ga nato analizira. Poiščejo se določene lastnosti v signalu, tako se tvori vhodni vektor podatkov (Reynolds in Campbell, 2007).

Slika 3.19: Analiza signala govora (Drygajlo, 2005b)

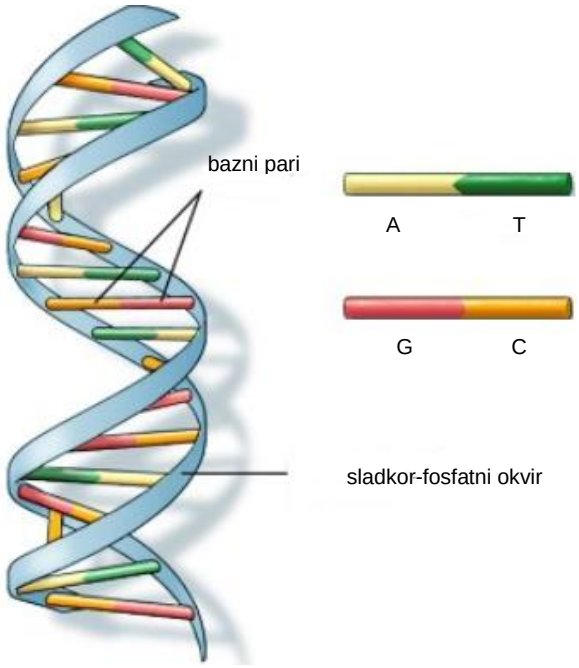
Za vsakega uporabnika sistema je potrebno predhodno posneti vzorec glasu, ga analizirati ter shraniti vektor. Sledi primerjava, vhodni vektor se primerja z izhodnim. Alogritmi za prepoznavo glasu so zelo raznovrstni. Skoraj vsak sistem ima svojega. Eden izmed pristopov je takšen, da se najprej določi diskretna prenosna funkcija vokalnega trakta (Mraović, 2003). Težave se pojavijo, ker se telo spreminja, s tem pa tudi lastnosti vokalnega trakta. V zadnjem času je vse večji trend analiza fonemov. Metoda ni odvisna od vnaprej pripravljenih besednih nizov, kar ji daje določene prednosti. Sposobna je prepoznati osebo med deseterico ljudi, tak sistem je težko prevarati s posnetkom. Metoda ima enako težavo kot prejšnje, da se

parametri človeškega telesa precej spreminjajo s časom. Kljub vsemu so takšne naprave zelo zanesljive, pravilno prepoznavajo tudi prehlajena grla in so zelo enostavna za uporabo, za upravljanje ne potrebujemo veliko izkušenj. Za kakovost delovanja sistema pa je pomemben tudi morebiten hrup v ozadju.

3.3.1.11 Prepoznava na osnovi DNK

Obstajajo še druge vrste, med katerimi naj kot zanimivost omenimo obliko ušesa, človekov telesni vonj in DNK, ki pa je velikokrat nimajo za tehnologijo na podlagi biometrije.
Biometrija na osnovi prepoznave DNK (slika 3.20) temelji na dušikovih bazah, ki se vežejo na štiri t. i. kratke baze:

- adenin (A),
- citozin (C),
- gvanin (G) in
- timin (T).



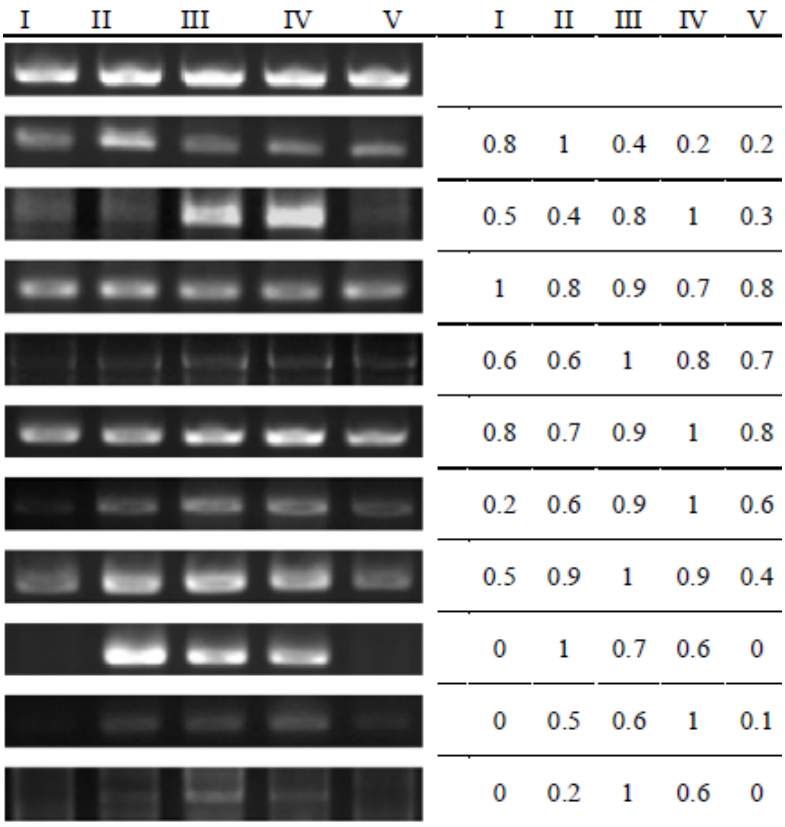
Slika 3.20: Identifikacija DNK (U.S. National Library of Medicine, 2008)

Vsaka baza se kombinira s svojim nasprotnim delom ter tvori osnovni par: adeninske baze kombinirajo pare s timini in citozinske baze kombinirajo gvanine. DNK je merljiva z enoto nt (nukleotidi).

Iskanje značilk DNA (genetic fingerprinting ali DNA testing) je tehnika za identificiranje posameznikov in ugotavljanje sorodstvenih vezi med njimi izključno na podlagi zaporedja njihove DNA (Groleau, 2004). Sodobna različica tehnike temelji na ugotavljanju zaporedja zelo variabilne regije DNA (slika 3.21) s kratkimi

tandemskimi ponovitvami (VTNR)[15], dolžine zaporedij, ki so unikatne pri vsakem posamezniku.

Odkritelj testiranja DNA je Jeffreys, genetik z Univerze v Leicestru. Leta 1985 je razvil in objavil metodo ugotavljanja DNA, še istega leta pa so jo prvič uporabili na civilnem sodišču v Veliki Britaniji pri reševanju imigracijskega primera.



I	II	III	IV	V
0.8	1	0.4	0.2	0.2
0.5	0.4	0.8	1	0.3
1	0.8	0.9	0.7	0.8
0.6	0.6	1	0.8	0.7
0.8	0.7	0.9	1	0.8
0.2	0.6	0.9	1	0.6
0.5	0.9	1	0.9	0.4
0	1	0.7	0.6	0
0	0.5	0.6	1	0.1
0	0.2	1	0.6	0

Slika 3.21: Regije DNA (razlike med dolžinami zaporedij VTNR pri petih osebah) (Heinemann in drugi , 2011)

3.3.2 PREDNOSTI BIOMETRIČNE TEHNOLOGIJE

Motivov za raziskovalno in razvojno dejavnost na področju biometričnih sistemov je več kot dovolj. Med njimi velja poudariti nekaj najpomembnejših:

1. Enostavnost in varnost uporabe tovrstnih sistemov pri postopkih identifikacije.
2. Stroškovni vidik biometričnih sistemov (razpoložljivost, vzdrževanje):

[15] *VNTR so regije DNA oz. kratka zaporedja baznih parov (med 2 in 5) na več mestih v genomu, s spremenljivim številom kratkih tandemskih ponovitev (angl. short tandem repeats, STR). Število ponovitev se lahko razlikuje od posameznika do posameznika, vendar so zaporedja, kjer se ponavljata samo dva bazna para, nezanesljiva, saj se lahko število razlikuje od tkiva do tkiva pri istem človeku. S to metodo ciljajo zaporedja, kjer se ponavlja 3 do 5 baznih parov (največkrat 4).*

- večja razpoložljivost biometričnih identifikacijskih sistemov,
- manj odpovedi,
- cenejša vzdrževanje in oprema.

3. Uporabnost izsledkov raziskave v mnogih znanstvenih disciplinah: medicini, informatiki itd.
4. Prilagojenost raziskovalnega in razvojnega procesa potrebam aktualnih EU projektov:
   - SIS II,
   - schengenski informacijski sistem.
5. Trend globalizacije:
   - standardizacija,
   - študija Evropske komisije JRC (2005) o vpeljavi biometrije v evropski »način življenja« in njenem vplivu na družbo kot celoto.
6. Tržno-ekonomski vidik, kjer izhajamo iz dejstva, da trenutno predstavlja:
   - Evropa 80 % trga pametnih kartic,
   - Azija 15 %,
   - Severna Amerika pa samo 5 %.

Vsi našteti dejavniki vodijo k uporabi sistemov osebne identifikacije, ki morajo biti varni, zanesljivi in enostavni za uporabo. V sistemu varovanja podatkov morajo biti natančno določene vloge in odgovornost udeleženih v postopku identificiranja. V fazi upravljanja tveganja je treba izvesti vse potrebne kontrolne postopke, ki bodo morebitno tveganje kar najbolj zmanjšali ali ga odpravili.

3.3.3 TEŽAVE PRI VPELJAVI BIOMETRIČNE TEHNOLOGIJE V PRAKSO

Poleg vseh prednosti, ki jih prinaša biometrična tehnologija, pa je znanih tudi kar nekaj slabosti oz. težav pri njeni implementaciji v realno okolje:

- hitrost prepoznavanja, ki traja največ nekaj sekund, je ob slabo optimizirani nastavitvi FAR in FRR lahko precej manjša kot pri uporabi kartice, kar upočasnjuje pretok ljudi pri identifikaciji,
- zanesljivost prepoznavanja ni popolna, saj je v vsakem okolju nekaj odstotkov oseb, katerih prstnega odtisa ni mogoče zanesljivo prebrati.
- prstni odtis je dokaj preprosto ponarediti, razen pri uporabi izpopolnjenih in temu primerno dragih biometričnih čitalnikov,
- nekateri ljudje imajo pomisleke iz higienskih razlogov in se ne želijo dotikati čitalnika skupaj s stotinami svojih sodelavcev, čeprav to vsak dan počnemo na kljukah vrat, pipah in raznih drugih predmetih (Četrta pot, 2009).

3.4 IDENTIFIKACIJA NA OSNOVI PRSTNEGA ODTISA

Prstni odtis je odtis, ki ga naredi koža na blazinici človeškega prsta. Nikoli še niso našli dveh ljudi, niti enojajčnih dvojčkov, ki bi imela identičen prstni odtis, zato se prstni odtisi uporabljajo za dokazovanje istovetnosti osebe. Fiziološko je prstni odtis konfiguracija grebenov s porami, ki jih delijo doline. Ležijo na ožilju, tik pod kožo. Morfologija (oblika) prstnega odtisa je povezana s specifičnimi električnimi in toplotnimi značilnostmi kože. To pomeni, da svetlobo, toploto ali električno napetost (ali kombinacijo vseh) lahko uporabimo za zajem podobe prstnega odtisa. Prstni

odtis nastane že med razvojem zarodka in se s starostjo osebe ne spremeni, temveč raste v svoji prvotni obliki in po končani rasti osebe ostane v svoji velikosti nespremenjen. Prav tako se po poškodbi obnovi v prvotno obliko.

Med vsemi biometričnimi metodami je metoda prepoznavanja prstnih odtisov najstarejša. Odtisi so zavarovani pred mutacijami. Sestavljajo jih kožne gubice in brazde ter različni detajli, katerih značilnosti lahko enostavno odčitamo z biometričnim modulom. Detajli so vzorci na koncu ali pregibu gubic. Globalni vzorci, ki jih naredijo gubice, brazde in detajli na konici prstov, so na vsakem prstu drugačni in zelo prikladni za prepoznavanje. Za prepoznavanje enega prstnega odtisa lahko zadostuje že informacija s količino od nekaj sto bajtov (iskanje detajlov) do nekaj megabajtov (visoka varnost). Nikoli se ne hrani dejanska slika odtisa. Iz shranjenih podatkov ni mogoče rekonstruirati slike prstnega odtisa. Pri korelacijskih metodah je količina podatkov večja (Trepečar, 2007).

Pojem prstni odtisi vključuje t. i. odvzete odtise prstov in dlani, npr. pri daktiloskopiranju osumljenih kaznivih dejanj, oseb za preverjanje identitete, mrtvih oseb za identifikacijske potrebe, domačih oseb pri kaznivih dejanjih zaradi izločitvenih postopkov itd. Veda, ki se ukvarja s kožnimi reliefi prstov, dlani in stopal, se imenuje daktiloskopija[16]. Identifikacijska vrednost daktiloskopije je zasnovana na dveh znanstveno in mednarodno priznanih dejstvih, in sicer:

- da ni dveh oseb s popolnoma enakimi prstnimi odtisi in
- da se ti ne spremenijo (razen po velikosti) od rojstva do razpada trupla.

V te namene se uporablja že več kot 120 let. Naloge daktiloskopije so predvsem:

- registracija storilcev kaznivih dejanj po prstnih odtisih, ugotavljanje istovetnosti storilcev kaznivih dejanj brez dokumentov, ko o sebi nočejo oziroma ne morejo dati podatkov ali so ti lažni, ugotavljanje istovetnosti mrtvih oseb po prstnih odtisih,
- potrjevanje identitete osebe pri navajanju njenih podatkov, ugotavljanje storilcev kaznivih dejanj po prstnih sledovih, puščenih na krajih kaznivih dejanj, in dokazovanje navzočnosti storilcev na kraju kaznivih dejanj, razvrščanje prstnih odtisov v skupine in klasificiranje (tako kartotečno kot računalniško).

Prstni odtisi imajo vsaj tri temeljne značilnosti (Hace in Škrabar, 2008):

- edinstvenost – vsak je edinstven, niti dva človeka nimata enakega, prav tako je odtis drugačen na vsakem prstu,
- trajnost – prstni odtisi se ne spremenijo od tri mesece starega zarodka do razkroja trupla. Brazgotine so ena od izjem tega pravila, pa še to le, če so trajne (v primeru, ko se poškodujejo bazalne celice v usnjici) in
- vzorčnost – vse prstne odtise lahko razvrstimo v vzorčne tipe.

Zgodovinski mejnik je v letih 1911 in 1912 postavil Locard[17] (Maver, 2004). Določil je najmanjše število individualnih značilnosti, potrebnih za prstno identifikacijo, in predstavil naslednje tridelno pravilo:

- če je na prstni sledi in prstnem odtisu več kot dvanajst skladnih individualnih značilnosti, identifikacijska gotovost ni dvomljiva in

[16] *Termin daktiloskopija je sestavljen iz dveh grških besed, prva, daktylos, pomeni prst in druga, skopein, pomeni gledati oziroma videti.*

[17] *Locard (1877–1966) je bil ustanovitelj in direktor Inštituta za kriminalistiko pri univerzi Lyons v Franciji.*

- če je skladnih individualnih značilnosti med osem in dvanajst, potem je primer mejni. V tem primeru je identifikacijska gotovost dosežena, ko jo potrdita vsaj dva kompetentna in izkušena daktiloskopska strokovnjaka, odvisna pa je od jasnosti prstne sledi in prstnega odtisa, redkosti tipa vzorca, prisotnosti vzorčnega centra in delte v preiskovanem delu prstne sledi in odtisa, prisotnosti por, točne oziroma očitne skladnosti širine in pozicije papilarnih linij ter viličenj.

Nekatere države, med njimi Francija, Finska, Belgija, Nizozemska, Izrael, Španija, ZDA in Slovenija, so se držale Locardovega pravila o skladnosti dvanajstih individualnih značilnosti, medtem ko so Nemčija, Švedska in Švica opravljale identifikacije z osmimi do dvanajstimi značilnostmi. Skrajni numerični standard pa so postavili v Italiji in Veliki Britaniji s šestnajstimi ter Rusiji s sedmimi značilnostmi. Leta 1970 je komisija strokovnjakov IAI zasnovala študijo vprašanj o ustreznosti numeričnega standarda za potrebe daktiloskopskih identifikacij. Ugotovili so, da princip identifikacije ne more biti zaključen samo s štetjem individualnih značilnosti. Dejstvo je, da vsaka identifikacija predstavlja edinstveno število okoliščin in da je identifikacijska vrednost skladnih točk dveh prstnih odtisov odvisna tudi od raznolikosti okoliščin, ki samodejno izključujejo katerikoli minimalni standard. Ko daktiloskop opravi identifikacijo, doseže t. i. odločitveni prag. Ta prag vključuje število skladnih točk v seštevku tega kvantitativnega elementa pa tudi oceno kvalitativnih dejavnikov, kot so redkost oziroma izvirnost osnovnega vzorca, tipi individualnih značilnosti in relativna pogostost teh točk. V tej smeri je torej proces identifikacije univerzalna ocena, ki uravnoteža tako kvantitativni kot tudi kvalitativni pristop. Biometrični način identifikacije posameznika pomeni individualno obravnavanje človekovih fizičnih lastnosti ali značilnosti obnašanja ter zajem in shranjevanje tega vzorca (imenovanega tudi živi vzorec) v standardni podatkovni obliki. Vzorec se v postopku identifikacije primerja z vzorcem (imenovanim tudi shranjeni vzorec ali podpis), ki temelji na istih značilnostih in je shranjen v varnostnem sistemu. Primerjava obeh vzorcev potrdi ali zavrže identiteto posameznika (Trapečar, 2007).

3.4.1 RAZLIČNE METODE BIOMETRIČNE IDENTIFIKACIJE S PRSTNIM ODTISOM

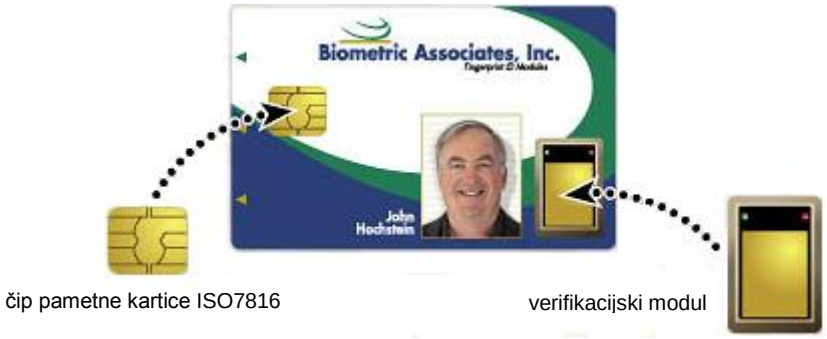
Metode za prepoznavanje prstnih odtisov se v glavnem delijo na dve področji. Prve so takšne, ki iščejo detajle prstnih odtisov. S temi postopki se najprej poiščejo vsi detajli, nato pa natančno določita njihova lega (2D koordinate) in medsebojna razdalja. Težave se pojavijo pri slabi kakovosti zajetih odtisov. Pri teh metodah je zanemarjena informacija o globalni razporeditvi brazd in gubic na prstu. Druge, bolj uporabne, so korelacijske metode. So bolj celostne, v tem smislu, da upoštevajo usmerjenost, debelino in gostoto gubic na določenem mestu. Bolj izpopolnjeni algoritmi analizirajo vse značilnosti prstnega odtisa: gubice, brazde in detajle, usmerjenost, gostoto oz. frekvenco, zapomnijo si tudi razne nepravilnosti. Ti podatki se nato shranijo v spomin. Velikost podatkov je sorazmerna s kompleksnostjo analize. Za en prstni odtis lahko zadostuje že nekaj sto bajtov (pri metodah, ki iščejo detajle), medtem ko ima lahko sistem za zagotavljanje visoke varnosti podatke shranjene v več megabajtih za en odtis. Nikoli se ne hrani dejanska slika odtisa. Iz shranjenih podatkov tako ni mogoče rekonstruirati slike prstnega odtisa. Pri korelacijskih metodah je količina podatkov večja (Mraovič, 2006).

Danes imamo že zelo velike baze prstnih odtisov, samo FBI jih ima okoli 70 milijonov. Razviti so algoritmi za hitro pregledovanje tako obsežnih baz. Prstni odtisi se najprej razdelijo v več skupin. Vsi s podobnimi lastnostmi gredo v eno skupino (npr. desno ukrivljeni, velik lok ipd.). Na skupini odtisov nato uporabimo eno od zgoraj opisanih metod. V vsakdanji rabi ima prepoznava prstnih odtisov kar nekaj prednosti pred prepoznavo obraza. Manjše so zahteve po strojni opremi. Tu ni treba obdelovati digitalnega videa v realnem času. Vse sisteme za prepoznavanje prstnih odtisov odlikujejo enostavna postavitev, nastavitev in vzdrževanje. Takšni sistemi se bodo v velikem številu pojavili na naših tipkovnicah, bančnih karticah, dlančnikih in še marsikje.

Za zajem značilnosti vzorca prstnega odtisa je znanih več algoritemskih metod. Najbolj razširjene so zasnovane na prepoznavanju vzorca ali izvlečku minucij. Pri algoritmih, ki temeljijo na minucijah, je prstni odtis sestavljen iz grobih značilnosti, kot so loki, zanke in zasuki, ter drobnih značilnosti (minucij), kot so predvsem bifurkacije (razdelitve), delte (združevanja v obliki črke Y) in zaključki grebenov. Prstni odtis ima med 30 in 40 minucij (slika 3.22). Za vsako so značilni položaj (koordinate), tip (bifurkacija, delta ali zaključek) in usmerjenost (orientacija). Skupek značilnosti minucij lahko da predlogo za prstni odtis. Če so natančno zajete, je možnost, da bi imela dva prstna odtisa enake značilnosti, izjemno majhna (Ratha in drugi, 2001a).

Slika 3.22: Značilke prstnega odtisa (NSTC, 2009)

Površina kože na dlaneh, prstih in stopalih je prekrita z drobnimi brazdami, ki se imenujejo papilarne linije. Vloga papilarnih linij nam olajša identifikacijo. Ker obstaja veliko število možnih kombinacij papilarnih linij, je tako rekoč nemogoče, da imata dve osebi popolnoma enako teksturo kože. Identifikacija na temelju prepoznavanja prstnih odtisov se izvede tako, da se primerja nepoznan prstni odtis z nizom poznanih odtisov oz. prototipov. Prepoznavanje prstnih odtisov temelji na prepoznavanju karakterističnih značilk, dobljenih iz slike odtisa. Eden od razlogov za takšen pristop namesto prepoznavanja celotne slike je varčevanje pri mediju (slika 3.23) za hranjenje znanih odtisov Ta proces neizpodbitno potrdi osebo, ki predloži kartico s primerjavo kriptografskega ključa uporabnika in kriptografskega ključa, ki je shranjen v podatkovni datoteki (Corcoran in drugi, 1999).



Slika 3.23: Kartica z vgrajenim modulom za prepoznavanje prstnih odtisov (Biometric Associates, 2010)

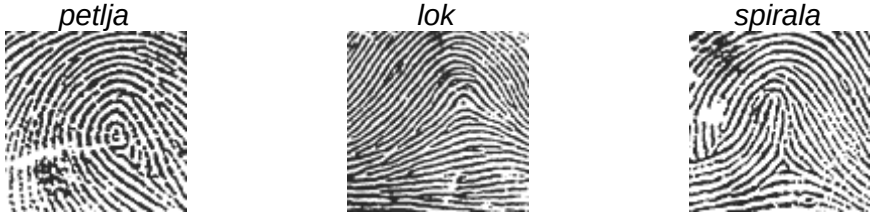
Drugi razlog je, da pogosto nimamo na voljo popolne slike odtisa, ampak samo njen del oz. sled.
Značilke, dobljene iz slike odtisa prsta, lahko razdelimo v dve skupini:
- globalne značilke (grobi vzorci, vidni na prvi pogled) in
- lokalne značilke.

Izvedba identifikacije temelji na primerjavi lokalnih značilk s prototipom.

3.4.1.1 Globalne značilke prstnega odtisa

Globalne značilke (slika 3.24) ne zadostujejo za identifikacijo, zadostujejo pa za razvrstitev prstnih odtisov v skupine (Šafaržik in Višnjić, 2009):
a. osnovni vzorci papilarnih linij
   - petlja (loop),
   - lok (arch),
   - spirala (whorl),
b. središčna točka (core point),
c. delta,
d. karakteristične linije (type lines),
e. papilarno število (ridge count).

Zastopanost osnovnih oblik:
- petljasta oblika – 60 %,
- spiralna oblika – 30 %,
- ločna oblika – 5 %,
- druge oblike – 5 %.



a) papilarne linije (osnovni vzorci)

b) središčna točka c) karakteristične linije d) delta e) papilarno število

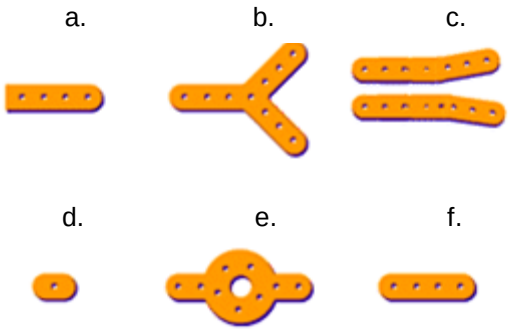
Slika 3.24: Globalne značilke (Šafaržik in Višnjić, 2009)

Središčna točka (core point) je približno na sredini odtisa in rabi kot referenčna točka pri obdelavi odtisa. Karakteristični liniji (type lines) sta papilarni liniji v notranjosti odtisa z vzporednim začetkom, ki divergirata ter obkrožita tako imenovano območje vzorca. Delta je točka prve mejitve v območju vzorca oziroma katerakoli točka tik pred centrom divergence karakterističnih papilarnih linij. Papilarno število (ridge count) je število papilarnih linij v območju vzorca. Določi se s štetjem papilarnih linij, ki sekajo zamišljeno dolžino, povlečeno med delto in središčno točko.

3.4.1.2 Lokalne značilke

Lokalne značilke se imenujejo minucijske točke. Minucijske točke ali minucije so prekinitve tokov papilarnih linij (nepredvidena prekinitev, mejišča itd.) in hkrati nosilci univerzalnih informacij, na katerih temelji izvedba biometrične identifikacije. Obstaja pet različnih značilk minucijskih točk:

1. minucije (šest tipov) (slika 3.25):
   a. papilarni zaključek (hitra prekinitev papilarne linije),
   b. papilarno mejišče (bifurkacija, točka mejišča linije v več novih),
   c. papilarno širjenje (divergenca, razdvajanje paralelnih linij),
   d. papilarna točka/otok (zelo kratka linija),
   e. papilarni ogib (linija, ki se razdeli v dve, ti pa se zatem ponovno spojita v zaprto območje),
   f. kratka papilarna linija (kratka linija, daljša od otoka),
2. orientacija minucije je smer, v katero je usmerjena minucijska točka,
3. splošna frekvenca minucije označuje, koliko so oddaljene papilarne linije v okolju minucije,
4. ukrivljenost minucije, ki označuje kako hitro se spremeni smer minucije in
5. minucijske koordinate, ki označujejo relativno ali absolutno oddaljenost minucije od središčne točke ali delte.

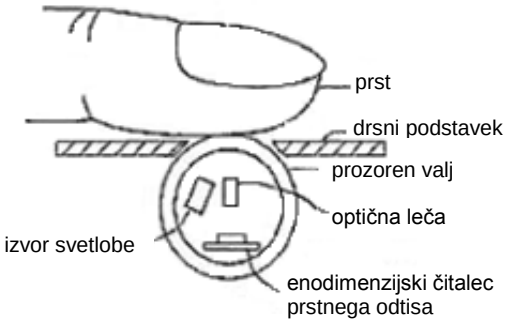


Slika 3.25: Lokalne značilke (Šafaržik in Višnjić, 2009)

3.4.2 TEHNOLOGIJE ČITALNIKOV PRSTNIH ODTISOV

3.4.2.1 Optična

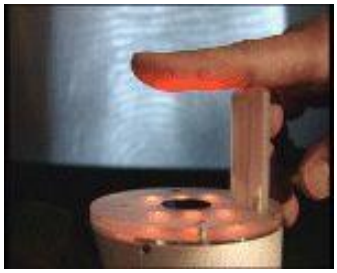
Podoba prstnega odtisa se odčitava z digitalno kamero. Prst položimo na ustrezno osvetljeno stekleno ploščo (slika 3.26). Za približanje objekta snemanja se uporabljajo posebne leče. Slika se zajame z množico točk CMOS[18] ali CCD ustrezne ločljivosti in spremeni v sive odtenke (od 2 do 16 tonov). Pomanjkljivost te tehnike je, da prstni odtis ostane na stekleni plošči in ga lahko ponovno uporabimo (zlorabimo), poleg tega je izredno težko razlikovati med živim prstom in dobro oblikovano imitacijo (Matjaš in Riha, 2004).



Slika 3.26: Optično odčitavanje prstnega odtisa (Mainguet, 2010)

Optično odčitavanje prstnega odtisa pa je možno tudi brez dotika (slika 3.27).

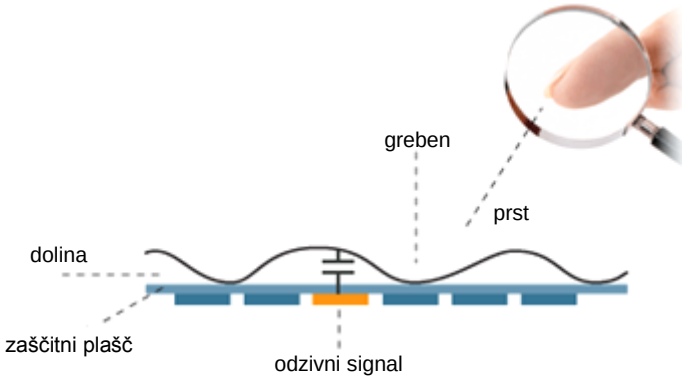
[18] *Tipala CMOS/CCD in drugi elektronski deli zajema in digitalnega procesiranja so od leta 1968 znani iz vesoljske in vojaške tehnike ter od začetka 70. let iz grafične tehnike skenerjev.*



Slika 3.27: Optično odčitavanje prstnega odtisa brez dotika (Mainguet, 2010)

3.4.2.2 Kapacitivna

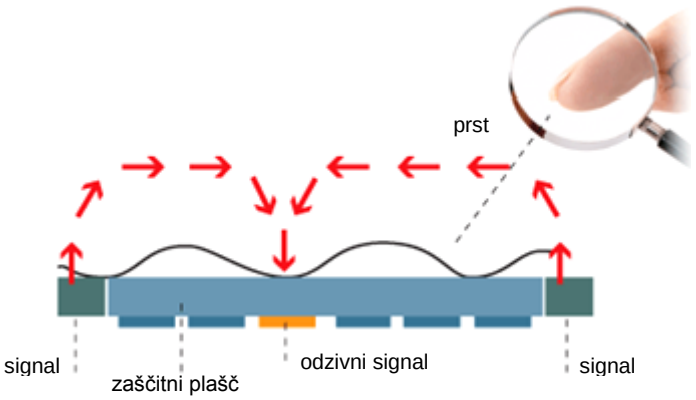
Ko položimo prst na množico točk, občutljivih za spremembe električne napetosti, se razlike v napetosti med grebeni (pretežno voda) in dolinami (pretežno zrak) zapišejo kot slika (slika 3.28). Kljub občutljivosti tega načina za elektrostatične motnje v okolju in druga električna polja je tehnika ena najbolj razširjenih (Chikkerur, 2005). Prav tako jo je dokaj enostavno obiti z imitacijami prstov in latentnimi odtisi.



Slika 3.28: Kapacitivni čitalnik prstnega odtisa (Mainguet, 2010)

3.4.2.3 Radijska

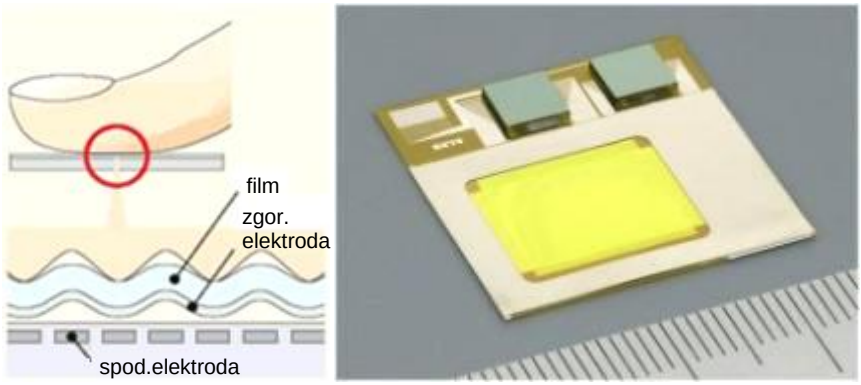
Če prst obsevamo z radijskimi valovi nizke intenzitete, deluje kot oddajnik, razlike v oddaljenosti med grebeni in dolinami pa so prepoznavne kot množica ustrezno usmerjenih točkovnih anten. Prst mora biti v stiku z oddajno površino senzorja (slika 3.29). Ker ta način temelji na fizioloških značilnostih kože, je radijski senzor težko prevarati z umetnim prstom. Slabost te tehnike je stik med prstom in oddajnim obročem, ki lahko postane neprijetno vroč.



Slika 3.29: Radijski čitalnik prstnega odtisa (Mainguet, 2010)

3.4.2.4 Tlačna

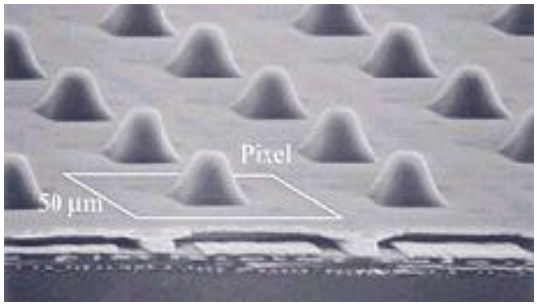
Točkovna množica, občutljiva za tlak, je sestavljena iz piezoelektričnih elementov, ki zajemajo vzorec grebenov, ko nanjo položimo prstni odtis (slika 3.30). Kljub številnim pomanjkljivostim te tehnike (slaba občutljivost, nezmožnost razlikovanja med pravim in umetnim prstom, občutljivost za premočan pritisk) kar nekaj proizvajalcev razvija prototipe.



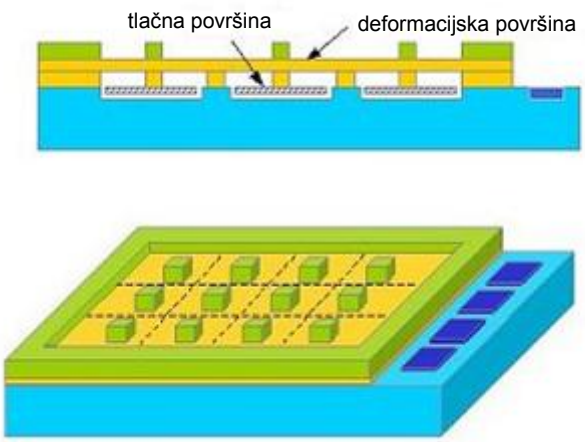
Slika 3.30: Tlačni čitalnik prstnega odtisa (Mainguet, 2010)

3.4.2.5 Mikroelektromehanična

Mikroelektromehanična metoda je ostala na stopnji med raziskavo in razvojem ter uporabo v različnih aplikacijah. V laboratorijih so naredili množico mikromehaničnih tipal, ki zaznavajo grebene in doline prstnega odtisa, vendar ne morejo zagotoviti robustnosti in široke uporabnosti (slika 3.31a in 3.31b). Prav tako ni mogoče ločevati med živim prstom in imitacijo.



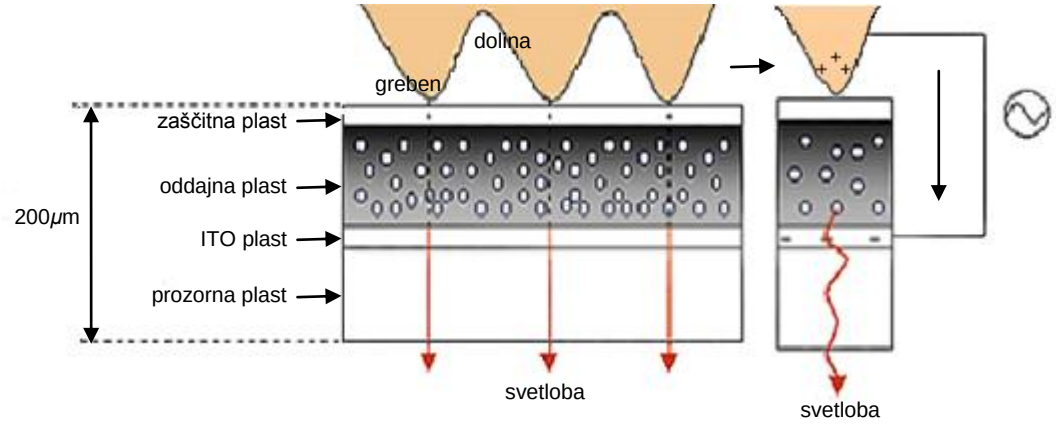
Slika 3.31a: Mikroelektromehanično tipalo (Mainguet, 2010)



Slika 3.31b: Mikroelektromehanično tipalo (Mainguet, 2010)

3.4.2.6 Elektrooptična

Elektrooptično odčitavanje prstnih odtisov (slika 3.32) temelji na skeniranju neposredno iz prsta. Iz tega izhajajoč vzorec se shrani na čip, ki pretvori vzorec v digitalno obliko, ki se lahko obdeluje, shranjuje, in primerja z drugimi vzorci prstnih odtisov. Digitalne slike so predstavljene z visoko resolucijo in omogočajo hitro primerjavo slik prstnih odtisov v velikih podatkovnih bazah.

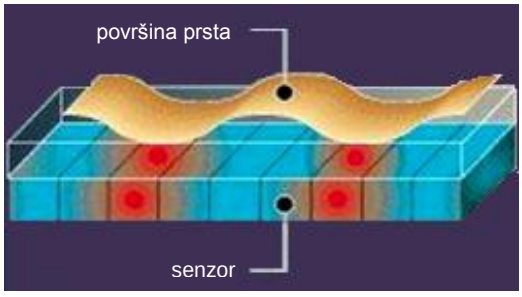


Slika 3.32: Elektrooptični čitalnik prstnega odtisa (Mainguet, 2010)

3.4.2.7 Termična

Piroelektrični material lahko razliko v temperaturi spremeni v določeno napetost. Ta način je zelo razširjen in se uporablja tudi v infrardečih kamerah. Termični čitalnik prstnega odtisa (slika 3.33), ki temelji na uporabi tega materiala, meri temperaturno razliko med točkami, ki so v stiku (grebeni), in tistimi, ki niso (doline). Termični pristop ima številne prednosti, npr. neobčutljivost za statično elektriko in odsotnost signala, poslanega iz čitalnika na prst, deluje tako v skrajnih kot v običajnih temperaturnih razmerah. Prav tako je tako rekoč nemogoča zamenjava živega prsta z imitacijo (Lemme, 2005).

Slabost termičnega načina pa je, da slika hitro izgine. Ko prst položimo na senzor, je na začetku velika razlika v temperaturi, vendar že po kratkem času (prej kot v sekundi) slika izgine, ker se temperatura izenači. To je med drugim razlog, da se uporablja način zajema slike, opisan v naslednjem podpoglavju.



Slika 3.33: Termični čitalnik prstnega odtisa (Mainguet, 2010)

3.4.2.8 Statična ali odčitavana slika

Statično sliko zajemamo na okencu enake velikosti, kot je velik prstni odtis, tako da prst pritisnemo na površino za toliko časa, kolikor je potrebno za zajem slike.

Prednost te tehnike je, da zajame celotno sliko v enem koraku. Precejšnji pomanjkljivosti pa sta velikost čitalnika in dejstvo, da odtis prsta ostane na njegovi površini. Drugi način je uporaba pravokotnega okenca enake širine kot slika in z le nekaj točkami višine, po katerem navpično potegnemo s prstom. Ta način zahteva, da sliko zajemamo sekcijsko, programska oprema pa jo rekonstruira v celoto. Prednosti so gotovo majhnost, stabilnost slike zaradi termičnega odčitavanja in dejstvo, da je čitalnik samočistilen. Na njem ne ostanejo latentni odtisi. Zaradi kratke obstojnosti termične razlike je to tudi edina metoda, ki jo lahko uporabimo pri termičnih čitalnikih.

4 PROJEKTNO VODENJE RAZVOJA IN OPTIMIZACIJE BIOMETRIČNEGA SISTEMA

Projekt raziskave zanesljivosti, učinkovitosti in razpoložljivosti biometričnega identifikacijskega sistema je enovit proces, ki ga sestavljajo koordinirane in obvladovane aktivnosti z določenim rokom začetka in konca. Opravljamo jih zaradi doseganja zastavljenih ciljev in zahtev, skupaj z omejitvami glede časa, stroškov in virov. Za naš primer raziskave v okviru izdelave doktorske disertacije smo uporabili teoretični Balantičev (2006) model za razvoj programske opreme, prirejen po Boehmu (1988). Zaradi izkustvene narave razvoja programske in elektronske opreme ter razmeroma mlade dejavnosti še ni enotne in splošne metodologije, ki bi bila primerna za tovrstne tipe projektov. V praksi mora tako razvojno-raziskovalna skupina svoje razvojne in raziskovalne postopke nadgrajevati z lastnimi izkušnjami. V operativnem smislu so znana mnoga orodja za vodenje stroškov in virov pri izvedbi projekta. Za naš primer bo uporabljeno programsko orodje MS Project proizvajalca Microsoft.

Večjo standardizacijo razvoja programske opreme sicer postopoma prinašajo integrirana orodja za razvoj programske opreme CASE, ki bodo razvijalcem določila način dela, vendar za naš primer teh orodij nismo uporabili.

4.1 PROCESNA ORGANIZACIJA RAZISKOVALNEGA OKOLJA

Poslovni sistem ter posledično razvojni oddelek v organizacijski strukturi je organiziran procesno. Razvoj, raziskave in testiranja identifikacijkih sistemov potekajo interaktivno v dinamičnem okolju.

Potreben pogoj za takšno dinamično prilagajanje struktur poslovnih objektov spreminjajočim procesom, torej za obstoj procesne organizacije, je ustrezna računalniška podpora meta-procesa. Procesna organizacija je mogoča le pod pogojem, da se izvaja tudi razporejanje in terminiranje potrebnih poslovnih objektov, ki je enotno za celoten poslovni sistem. V tem primeru postanejo modeli, ki so skupaj s podatki shranjeni v repositoriju »gonilniki poslovnih procesov«, torej nadomeščajo klasično zasnovane informacijske sisteme (Kern, 1998).

4.2 METODOLOGIJE PROJEKTNEGA VODENJA

Temeljni delitvi, ki odločilno vplivata na način vodenja in organiziranja projektov, sta delitev na deterministične in stohastične projekte ter na enkratne projekte in projektne procese (Solina, 1997).

4.2.1 DETERMINISTIČNI IN STOHASTIČNI PROJEKTI

Deterministični projekti so tisti, kjer lahko končne cilje povsem določimo ali determiniramo. S končnimi cilji posredno določimo tudi delne cilje oziroma celotno strukturo izvedbe projekta (Hauc, 2002). Za deterministične projekte je torej značilno ciljno retrogradno oblikovanje projektov. To pomeni, da se na osnovi jasno

določenega končnega cilja postopoma določi vse aktivnosti, potrebne za njegovo dosego. Večina projektov, katerih cilji so uresničljivi s precejšnjo verjetnostjo, sodi v to skupino.

Stohastični projekti so tisti, pri katerih končnih ciljev ni mogoče natančno definirati. To so največkrat raziskovalni in razvojni projekti, kjer šele delni rezultati začetnih aktivnosti omogočajo definicijo nadaljnjih ciljev. Tak postopni način oblikovanja projektov imenujemo ciljno progresivni (Solina, 1997).

4.2.2 ENKRATNI PROJEKTI IN PROJEKTNI PROCESI

Enkratni projekti se pojavljajo le enkrat. Vodenje takega projekta zato zahteva posebej zasnovano projektno organizacijo. Projektni procesi pa so projekti, ki se v podobnih okoliščinah večkrat ponovijo. To so tipski projekti z enakimi ekonomskimi ali tehnološkimi značilnostmi, ki zahtevajo neki ustaljen način izvedbe in vodenja. Njihovo vodenje je zasnovano na stalni projektni organizaciji.

Oblikovanju organizacije poslovnega sistema na osnovi modela strukturiranih organizacijskih procesov (Kern, 1998) in projektnemu organiziranju razvoja identifikacijskih sistemov je namenjeno naslednje podpoglavje.

4.2.3 APLIKATIVNI DEL PROJEKTA

Plan projekta vsebuje seznam dejavnosti oziroma aktivnosti v okviru ugotavljanja zanesljivosti, učinkovitosti in razpoložljivosti ter njihovo trajanje. Za preračun plana in realističen prikaz modela projekta, ki ga vodimo, smo uporabili programsko orodje MS Project, ki vsebuje in analizira podatke o dejavnostih, njihovem trajanju in druge podatke, kot so fiksni datumi in vmesni roki.

Za aplikativni del doktorske disertacije, v katerem raziskujemo zanesljivost, učinkovitost in razpoložljivost identifikacijskega sistema, smo definirali (Lientz in Rea, 1999):

1. Okvirni časovni načrt, v katerem smo določili časovni okvir za izdelavo projekta. Okvir se razdeli na mejnike za dosego glavnih ciljev in podciljev projekta.
2. Operacije dela s spiskom dejavnosti, ki so zaokrožene delovne aktivnosti z jasnimi cilji. Med metodami za določanje aktivnosti prevladuje metoda, ki določa delovno strukturo WBS, kjer MS Project samodejno določi hierarhično številko vsaki dejavnosti. Ta števila se uporabljajo kot privzeta WBS koda in se avtomatično korigirajo, ko se spreminja struktura plana. Seveda pa jih lahko popravimo in ustvarimo svojo WBS kodo.
3. Odgovornost za posamezne projektne aktivnosti in podaktivnosti.
4. Okvirne stroške projekta. Kljub temu da gre za projekt v okviru izdelave doktorske naloge, se mora po ekonomskem izračunu izplačati. Stroški projekta naj bi se kasneje povrnili, na primer v obliki novih, boljših ali hitrejših storitev identifikacijskega sistema.
5. Mrežni načrt, glede na okvirni časovni načrt. S pomočjo spiska aktivnosti in časovnega diagrama glavnih podciljev se začne izdelava mrežnega načrta. Za vsako aktivnost se mora oceniti potreben čas, nato pa določiti vrstni red izvajanja aktivnosti. Za mrežno načrtovanje poznamo več različnih metod in celo več različnih vrst mrežnih diagramov. Eden od rezultatov mrežnega načrtovanja pa je določitev aktivnosti, odločilnih za pravočasno izpeljavo projekta. Zaporedju

takih aktivnosti pravimo kritična pot. Na tej poti so samo aktivnosti, ki nimajo časovne rezerve.

6. Potrebne vire glede na spisek aktivnosti. Za vsako aktivnost posebej določimo potrebne kadre, opremo, storitve, skratka vse vire, potrebne za dosego ciljev posamezne aktivnosti.

5 STANDARDIZACIJA IDENTIFIKACIJSKIH SISTEMOV

Standardizacija je usklajenost z dogovorjenimi predpisi (standardi), ki proizvajalcem in kupcem prinese vrsto prednosti, kot so:
a. zagotavljanje in kontrola kakovosti in
b. v fazi načrtovanja omogoča lažjo primerjavo, povezavo in selekcijo proizvodov različnih proizvajalcev.

Pri obravnavi identifikacijskih sistemov in pristopne kontrole standardizacija pokriva različna področja, npr. področje proizvodov, procesov, testov, kvalitete izdelkov itd. V nadaljevanju navajamo relevantne standarde, ki se uporabljajo pri razvoju in izvedbi identifikacijskih sistemov pristopne kontrole. Pri načrtovanju, razvoj in implementaciji sistemov pristopne kontrole za uporabo in varnostnih aplikacij (alarmni sistemi) upoštevamo standarde SIST EN 50133.

5.1 RFID STANDARDI

Standardi, ki jih na področju RFID pristopne kontrole najpogosteje zasledimo:
- JTC1/SC17: Cards & Personal ID ISO14443 – SmartCard (13,56 MHz),
- ISO15693 – Nadzor dostopa z RFID (13,56 MHz),
- ISO18000-3 – Uporaba RFID za dobavno verigo (13,56 MHz),
- ISO18000-6 – Sistem UHF RFID.

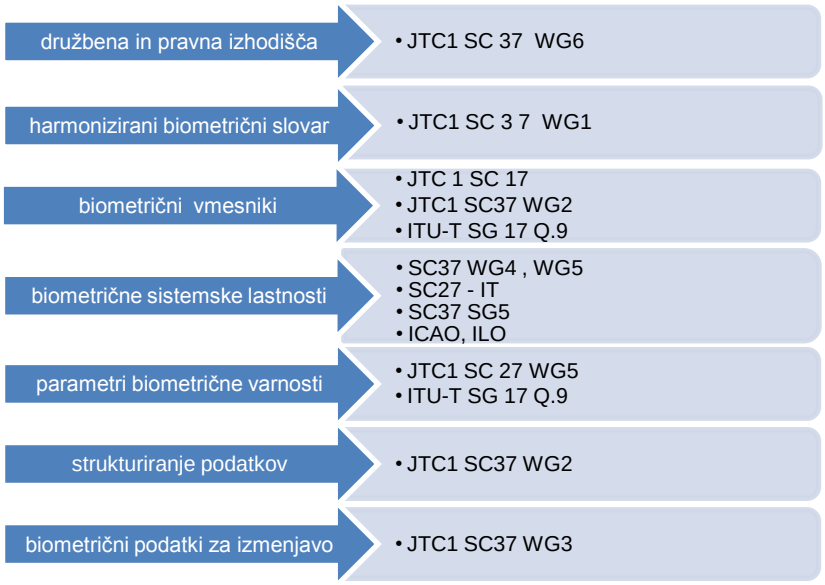
Trenutno se največ dela na standardizaciji področja UHF in celotne infrastrukture (protokol EPC – UHF za brezžični vmesnik, standardizacija podatkov na odzivniku RFID, protokol za izmenjavo podatkov, standardi za povezovanje v omrežje itd.). Znotraj EPC Global delujejo različne delovne skupine, ki pokrivajo področja strojne opreme, programske opreme in celotnih poslovnih sistemov. EPC Global (Electronic Product Code) je trenutno vodilni razvijalec standardov za podporo RFID, ki deluje pod okriljem GS1. S članstvom v EPC Global pa se pridobita možnost sodelovanja pri oblikovanju novih standardov ter seveda tudi dostop do obstoječih standardov.

5.2 STANDARDI BIOMETRIČNE PROGRAMSKE IN STROJNE OPREME

V zvezi z biometričnimi podatki je najpomembnejši organ za standarde ISO / IEC JTC1 SC37, ki je usmerjevalni odbor v katerega spada skupni tehnični odbor za ISO in IEC (JTC1). SC37 je področje standardizacije generičnih biometričnih tehnologij, ki se nanašajo na človeka in podpira interoperabilnost ter izmenjavo podatkov med aplikacijami in sistemi.

5.2.1 ISO/IEC JTC1 SC37

Aktivnosti v okviru standarda ISO/IEC JTC1 SC37 so opisane v šestih različnih delovnih skupinah (WG) (slika 5.1).



Slika 5.1: Dejavnosti JTC1 biometričnih standardov (ITU-T Technology Watch Reports, 2009)

- Glavna ideja za WG1 (harmonizirani biometrični slovar) je dokumentirati in standardizirati izraze in definicije, ki se uporabljajo v celotnem mednarodnem standardu SC 37. Rezultat je usklajen biometrični besednjak.
- WG2 (biometrični vmesniki) se osredotoča na standardizacijo vseh potrebnih biometričnih vmesnikov in interakcij biometričnih elementov in podsistemov. Rezultati iz te skupine so BioAPI biometrični standardi krovni standard biometričnih interakcij (CBEFF).
- Poudarek WG3 (biometrični podatki za izmenjavo) je standardizacija vsebine, pomena in zastopanosti biometričnih podatkov in formatov, ki so značilne za posamezno biometrično tehnologijo. Rezultat te skupine je standard ISO/IEC 19794 (Data Interchange Formats), ki trenutno vključuje standardni format izmenjave podatkov za prst, vzorec spektralnih podatkov, podatkovne slike prsta, podatkov podobe obraza, slikovni podatki šarenice itd.
- Cilj WG4 (strukturiranje podatkov) je razviti funkcionalno arhitekturo biometričnih in sorodnih profilov, ki povezujejo različne biometrične standarde, povezane na način, ki je skladen s funkcionalnimi bloki delovanja biometričnih sistemov. Glavni rezultat te delovne skupine je standard ISO/IEC 24713, ki definira biometrični profil za interoperabilnost ter izmenjavo podatkov, vključuje BRA kot prvi del in biometrični način preverjanja identifikacije v visoko varovanem okolju kot drugi del.
- WG5 (biometrične sistemske lastnosti) pokriva standardizacijo metodologije preskušanja in poročanja o meritvah, ki pokrivajo biometrične tehnologije, sisteme in komponente. Rezultat te skupine je standard ISO/IEC 19795, ki ima štiri podpoglavja, in sicer: 1. del - načela in okvir, del 2 – metodologije testiranja, 3. del - posebne metodologije testiranja in 4. del – posebni testni programi.

- WG6 (družbena in pravna izhodišča) se osredotoča na standardizacijo na področju pravosodnega in družbenih vidikov pri uporabi ISO/IEC biometričnih standardov. V tem smislu, in naloge vključujejo podporo oblikovanju in izvajanju biometričnih tehnologij v zvezi z dostopnostjo, zdravja in varnosti ter podpori zakonskih zahtev in potrditev medpravosodnega in družbenih vidikov, ki se nanašajo na osebne podatke. Rezultat te skupine je tehnično poročilo o pristojnostih in družbenih vidikih izvajanja biometričnih tehnologij.

5.2.2 STANDARDI NA PODROČJU BIOMETRIČNIH PROIZVODOV

ISO je skupaj z IEC ustanovil JTC1 za pripravo standardov informacijske tehnologije. JTC1 pa ima v strukturi tudi podskupino, za pripravo standardov biometrične tehnologije.

Mednarodna organizacija za civilno letalstvo (ICAO) si prizadeva za oblikovanje standardov potnih dokumentov. Ti standardi določajo fotografijo, zahteve digitalnega zapisa obraza in podobe prstnih odtisov, oblike shranjevanja slik in njihovih funkcij v namen izmenjave. Standardi ICAO temeljijo na CBEFF normah biometričnih podatkov.

Ameriški državni inšitut za standarde ANSI, je vladna ustanova, ki skrbi za standardizacijo in določa standarde na področju komunikacij in računalništva ter s tem omogoča združljivost izdelkov različnih proizvajalcev.

Za vmesno programsko opremo, zlasti tisto, ki izpostavlja dokumentarno gradivo za uporabo prek spletnih storitev (Web Services), pride v poštev standard OASIS.
Elektronski zajem slik in algoritmi za razpoznavanje vzorcev, so danes dovolj razviti, da vzorec prstnega odtisa avtomatsko obdelajo in shranijo. V več primerih za ta postopek obstojajo tudi standardi. Ti standardi obstojajo za vzorce, ki temeljijo na minucijah. Najbolj uporabljan je standard, ki ga v ZDA predpisuje NIST.

Pri prenosu zahtev standardov v prakso se izkaže, da biometrični sistemi kontrole pristopa popolnoma sledijo podanim zahtevam in da zaradi najvišjega razreda prepoznavanja dvigujejo varnost na najvišjo možno raven. Biometrični sistemi so tako primerni tudi za najzahtevnejše aplikacije sistemov kontrole pristopa (npr. dostop do trezorjev, strogo varovanih vojaških prostorov, strežniških oziroma računalniških centrov itd.).

5.3 STANDARDI DRUŽINE ISO/IEC 27000 V OKVIRU INFORMACIJSKE VARNOSTI

Biometrični sistem je del informacijskega sistema, zato je pri njegovi implementaciji nujno upoštevati tudi standarde informacijske varnosti (BEM WG, 2002).

Dobra osnova za upravljanje varovanja informacij v postopkih identifikacije, kjer upravljamo osebne podatke, je standard BS7799. Zaradi zahtev po varnosti osebnih

informacij v državni upravi in bančnem sektorju (II. Baselski sporazum[19]) ga je leta 2000 povzel tudi ISO in ga poimenoval ISO17799. Izpeljava projekta je bila nujna, saj so se zahteve po varovanju informacij vse pogosteje pojavljale tudi v gospodarstvu in zasebnem sektorju. Pravnih aktov, ki bi zahtevali upoštevanje priporočil standarda ali vsaj postavili nekatere zahteve za varovanje informacij ob začetkih njegovega uvajanja, v Sloveniji ni bilo. Slovenski inštitut za standardizacijo je leta 2000 prevedel in sprejel britanski standard BS7799 (1995). Ta določa zahteve za oblikovanje, vpeljevanje, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje dokumentacije sistema za upravljanje varovanja informacij v okviru celotnega tveganja organizacije (Ključevšek in Vodopivec, 2002). Z uveljavitvijo ZVOP-1 in zakona o varstvu dokumentarnega in arhivskega gradiva ter povezanih podzakonskih predpisov in normativov so zahteve po varovanju informacij in podatkov postale tako rekoč univerzalne. Veljajo za veliko večino pravnih oseb v gospodarstvu in negospodarstvu. Standard BS7799 se je tako razvil v družino mednarodnih standardov ISO/IEC 27000.

[19] *II. Baselski sporazum, sprejet 29. 06. 2004, je poleg tržnega in kapitalskega tveganja za banke uvedel tudi operativno tveganje in s tem kapitalske zahteve zanj. Operativno tveganje je po definiciji tega sporazuma tveganje izgube kot posledice neprimernega ali neuspešnega izvajanja notranjih procesov, ravnanj ljudi, delovanja sistemov ali zunanjih dejavnikov.*

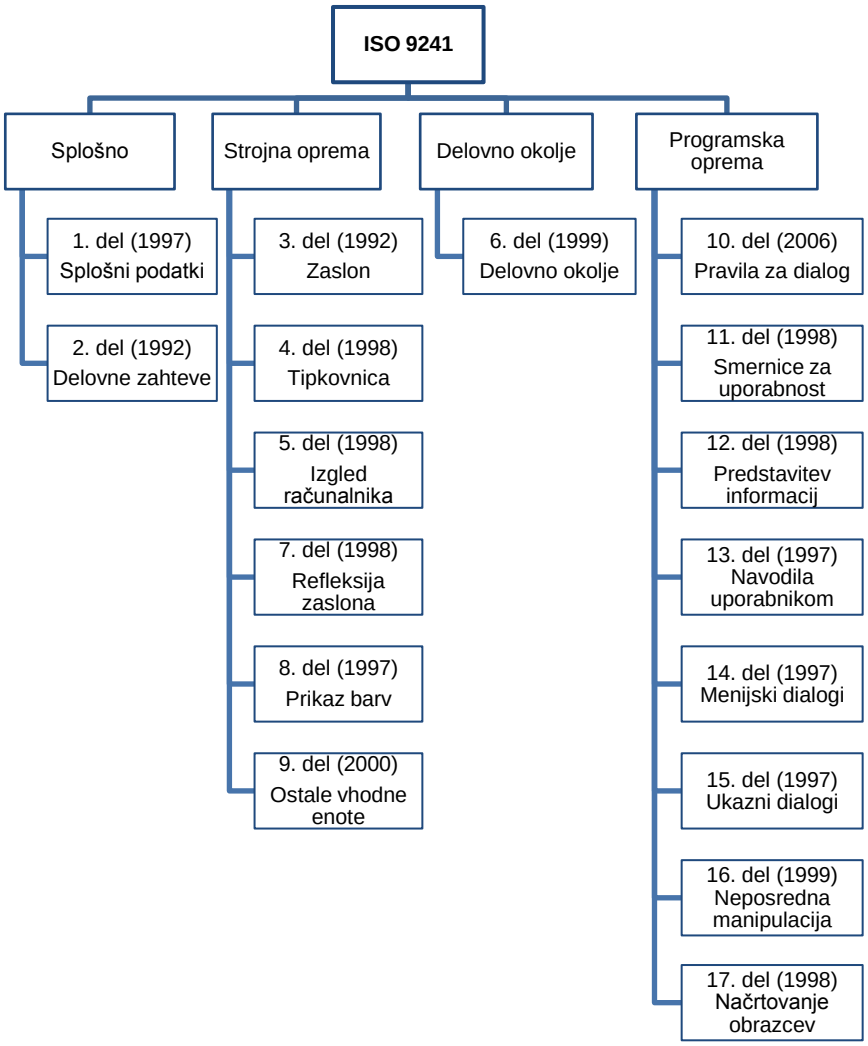
6 KAKOVOST BIOMETRIČNIH SISTEMOV ZA IDENTIFIKACIJO

Kakovost je določena s stopnjo, do katere skupek pripadajočih karakteristik izpolnjuje zahteve (Marolt in Gomišček, 2005), se glasi ena od opredelitev kakovosti, ki se razlikuje od nekaterih drugih definicij, saj je stopnja izpolnjevanja merljiva in jo lahko matematično zapišemo na naslednji način:

$$Q = \sum_{i=1}^{n} W_i C_i \qquad (1)$$

pri čemer je:
Q – stopnja izpolnjevanja,
W_i – pomembnost posamezne lastnosti,
C_i – ocena lastnosti in
i– število lastnosti predmeta trgovanja.

Zagotavljanje kakovosti je del managementa kakovosti, osredotočenega na pridobitev zaupanja, da bodo zahteve kakovosti izpolnjene (Marolt in Gomišček, 2005). Ta definicija jasno pove, da ni smiselno ločevati politike kakovosti od poslovne politike podjetja, saj sta obe usmerjeni k povsem enakemu cilju, ki je predvsem izpolniti pričakovanja kupca. Kupec je namreč tisti, čigar mnenje šteje več od mnenja kateregakoli organa, ki bo presojal skladnost sistema managementa kakovosti v podjetju z zahtevami različnih standardov. Kadar govorimo o kakovosti biometričnih sistemov moramo upoštevati napotke, ki jasno in nedvoumno opišejo namen uporabe izdelka (strojna oprema, programska oprema ali storitev) ter navesti merila uporabnosti (ISO 9241) (slika 6.1). Standard ISO 9241 (1997): Ergonomske potrebe pri pisarniškem poslovanju z uporabo slikovnih zaslonov velja za osrednji standard s področja uporabnosti, saj natančno opredeljuje, kateri podatki so relevantni za ocenjevanje uporabnosti opazovanega sistema. V okviru standarda je natančno opredeljena definicija uporabnosti (glej stran 6 standarda). Takšna oblika standarda od uporabnika zahteva zelo dobro poznavanje izdelka v kontekstu uporabe, zahtev in pričakovanj uporabnikov ter značilnosti končnih uporabnikov itd.



Slika 6.1: Shematični prikaz standarda ISO 9241 (1997)

6.1 KAKOVOST INFORMACIJSKIH SISTEMOV

V zadnjih nekaj letih je vse več govora o kakovosti informacijskih sistemov. Podjetja ugotavljajo, da se izplača visoka kakovost, tako izdelkov kot storitev pravi Solina (1997). Kakovostno programsko opremo je tudi lažje prodajati, saj imajo kupci z njo manj težav in dodatnih stroškov. Kakovost pri razvoju programske opreme je nujna tudi zato, da se sploh lahko izdelajo posamezni kompleksni sistemi. Brez skrbi za kakovost določenih velikih in kompleksnih sistemov ne bi bilo mogoče zgraditi.

Ker igra programska oprema vedno večjo vlogo v človeški družbi, je kakovost potrebna tudi za preprečevanje škode in celo izgube življenj. Dokumentiranih je precej primerov, ko je bila napaka v programski opremi neposredni krivec za smrt. Kot posledica vse večje zavesti o potrebi po kakovosti se v svetu pojavljajo novi standardi in predpisi. Nekaj je precej splošnih, drugi so namenjeni posebej

programski opremi. Vsekakor je v zvezi s kakovostjo programske opreme še veliko nejasnosti (Solina, 1997).

6.1.1 KAKOVOST PROGRAMSKE OPREME

Težko je našteti, kaj vse vpliva na kakovost programske opreme, še težje jo je izmeriti (Solina, 1997). Zagotovo pa je kakovost zelo lahko prepoznati. Pri tem razlikujemo notranje in zunanje vidike, nižje in višje, merljive in le subjektivno določljive.

McCall (1977) predlaga obširno shemo za opredeljevanje kakovosti (Côté in Georgiadou, 2006). Na visokem nivoju je določil tri dejavnike kakovosti programske opreme:

1. Delovanje sistema
   - pravilnost – Ali dela, kar zahtevam?
   - zanesljivost – Ali deluje ves čas pravilno?
   - učinkovitost – Ali dela na mojem računalniku kar se da hitro?
   - varnost – Ali je varen?
   - uporabnost – Ali ga znam uporabljati?
2. Revizija sistema
   - možnost vzdrževanja – Ali ga lahko popravim?
   - možnost testiranja – Ali ga lahko preizkusim?
   - fleksibilnost – Ali ga lahko spreminjam?
3. Tranzicija sistema
   - prenosljivost – Ali ga lahko uporabljam na drugih računalnikih?
   - ponovna uporabljivost – Ali lahko ponovno uporabim del programske opreme?
   - združljivost – Ali ga lahko povežem z drugimi sistemi?

Na nižjem pa McCall (1977) predlaga 23 meril kakovosti (npr. popolnost, sledljivost, modularnost, samodokumentiranje, splošnost, preprostost itd.) (BTH, 2009). Dejavniki in merila so med seboj povezani tako, da je treba za doseganje vsakega dejavnika izpolnjevati določena merila. Za zanesljivost, na primer, so potrebne popolnost, konsistentnost in sledljivost. Težava tega in podobnih sistemov je, da so dejavniki med seboj odvisni, nekateri celo v negativnem smislu (npr. če želimo visoko učinkovitost, to slabo vpliva na možnost vzdrževanja, možnost testiranja, fleksibilnost in prenosljivost). Kakovost programske opreme opredeljujejo številni modeli[20] in pristopi[21].

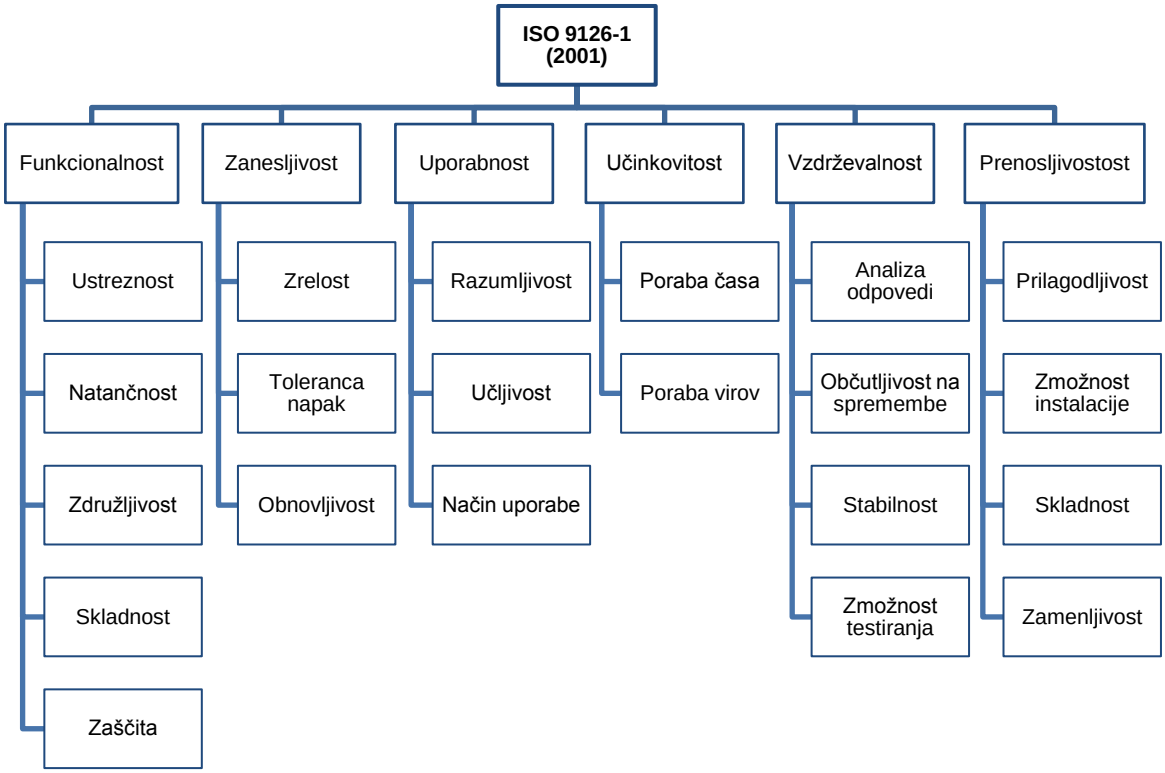
Kakovost programske opreme po IEEE 1061 je stopnja, s katero programska oprema izpolnjuje želeno kombinacijo atributov kakovosti. Namen metrike programske opreme je, da v celotnem življenjskem ciklu oceni ali je programska oprema izpolnjevala zahteve glede kakovosti.

Standard ISO/IEC 9126-1 (2001) danes predstavlja okvir za ocenjevanje kakovosti izdelkov programske opreme (slika 6.2). Standard ne predpisuje zahtev za

[20] *Nekateri modeli kakovosti: McCall, Boehm, Grady FURPS/FURPS+, Dromey, ISO9126, ISO/IEC 15504 SPICE, IEEE, CMM, Six Sigma.*

[21] *Nekateri pristopi k obravnavi kakovosti: Crosby, Deming, Feigenbaum, Ishikawa, Juran, Shewart.*

programsko opremo, temveč definira model kakovosti, ki je uporaben in primeren za vse vrste programskih rešitev. Vključuje vseh šest glavnih kategorij kakovosti programske opreme, ki so pomembne tudi pri njenem razvoju: funkcionalnost, zanesljivost, uporabnost, učinkovitost, vzdrževalnost in prenosljivost. Vsaka izmed kategorij je kasneje razdeljena še na podkategorije.



Slika 6.2: Programsko inženirstvo - kakovost proizvoda - 1. del: Model Kakovosti (ISO 9126-1, 2001)

6.1.2 STANDARDIZACIJA KAKOVOSTI PROGRAMSKE OPREME

Pri zagotavljanju kvalitete sistemskega produkta je mogoče izbrati dve poti (Solina, 1997):

1. preveriti (testirati) kakovost gotovega izdelka ali
2. organizirati tak razvojni oziroma produkcijski proces, da bo sistem zagotovo ustrezal določenim merilom kakovosti.

Najprej je prevladoval prvi način, zdaj pa vse bolj drugi, saj je potratno izdelati neki sistem in ga potem zavreči, če ni ustrezen. To še toliko bolj velja pri maloserijskih ali unikatnih produktih.

ISO je izdal številne standarde, ki govorijo o kakovosti programske opreme. Standard ISO/IEC 90003 (2004) podaja smernice, namenjene razvoju, prodaji, nakupu, vzdrževanju in uporabi (ergonomiji) programske opreme. Standard ISO/IEC 9126 vsebuje napotke za evalvacijo kakovosti programske opreme in ga lahko

uporabljamo skupaj s standardom ISO/IEC 14598, ki opredeljuje presojo kakovosti informacijskega sistema. V letu 2001 je standard ISO/IEC 9126 (1991) zamenjal nov štiridelni standard, ki obravnava model kakovosti, zunanje in notranje metrike ter kakovost uporabe metrike.

6.1.3 FMEA in SWFMEA

Metoda FMEA je ena izmed mnogih metod analize tveganja, ki jih priporočajo mednarodni standardi. Omogoča sistematični iterativni postopek za odkrivanje vrste možnih tveganj, ki lahko vodijo v odpoved sistema. Prav tako FMEA analiza omogoča odkrivanje vzrokov, ki predpostavljajo tveganja in nenazadnje omogoča ovrednotenje in zmanjšanje posledic ob odpovedi sistema. Izvajamo jo tako, da iščemo povezavo med možnimi načini odpovedi in posledicami ter odpovedi poskušamo preprečiti. V procesu izvedbe FMEA smo osredotočeni na tri glavne cilje:

1. Prepoznava in ocena možnih tveganj, odpovedi in njihovih posledic.
2. Oblikovanje seznama prednostnih ukrepov, ki odpravijo tveganja, možne odpovedi ali zmanjšajo njihovo verjetnost pojavljanja.
3. Izdelava dokumentacije za ovrednotenje podanih izboljšav.

Razloge in vzroke za odpovedi posameznih strojnih komponent poznamo. Odpovedi nastopijo zaradi obrabe, staranja ali nepričakovane obremenitve. Lahko pa pride tudi do slučajne odpovedi, ki je posledica skritih napak v materialu (Jerman, 2008).

Pri programski opremi je situacija nekoliko drugačna. Odpovedi programske opreme so ponavadi vnaprej neznane. Programski moduli ne odpovejo s stališča obrabe, temveč zgolj izkažejo nepravilno obnašanje (Pentti in Atte, 2002). Zato uporabimo v različnih fazah življenjskega cikla različne vrste metode SWFMEA. Standard IEC 60812 opisuje metodologijo FMEA in FMECA z napotki in postopki.

Standarda MIL-STD-1629A in IEC 60812 opredeljujeta dva vidika kritičnosti – frekvenco pojavljanja odpovedi (likelihood of occurrence, F) in resnost odpovedi (severity of failure, S), medtem ko SAE J-1739 vpeljuje še tretji vidik – verjetnost zaznave odpovedi (detection probability, D) (Mäckel,2006). Produkt dveh oziroma vseh treh števil imenujemo prioriteta tveganj RPN (Risk Priority Number).

6.1.4 ZBIRANJE PODATKOV O ODPOVEDIH INFORMACIJSKEGA SISTEMA

Standard ISO 9241-11 vključuje navodila o načinu ocenjevanja in specifikaciji uporabnosti izdelka, ki so skladna s sistemom kakovosti v okviru standarda ISO 9001 (2000).

Za določitev karakteristik zanesljivosti moramo opraviti testiranja, s katerimi dobimo podatke o uporabni dobi proizvoda, frekvenci odpovedi itd. Vse te informacije so nujne za določitev karakteristik zanesljivosti, ki jih raziskujemo. Da bi lahko definirali testne parametre za določanje zanesljivosti identifikacijskega sistema, ki je predmet raziskave, si bomo v naslednjih podpoglavjih pogledali nekatere relevantne izvedbene karakteristike.

Podatke o odpovedih identifikacijskega sistema, ki jih potrebujemo za oceno zanesljivosti, dobimo iz:

- laboratorijskih preskusov. Pri zanesljivih sistemih je pogosto težko oziroma nemogoče oceniti zanesljivost izdelkov, ker je čas do odpovedi predolg. Zato v laboratoriju skrajšamo čas preskusa tako, da izvajamo pospešene preskuse,
- eksploatacije. Najbolj realne podatke o zanesljivosti izdelka dobimo, če imamo podatke o njegovem delovanju iz uporabe (izkoriščanja, eksploatacije).

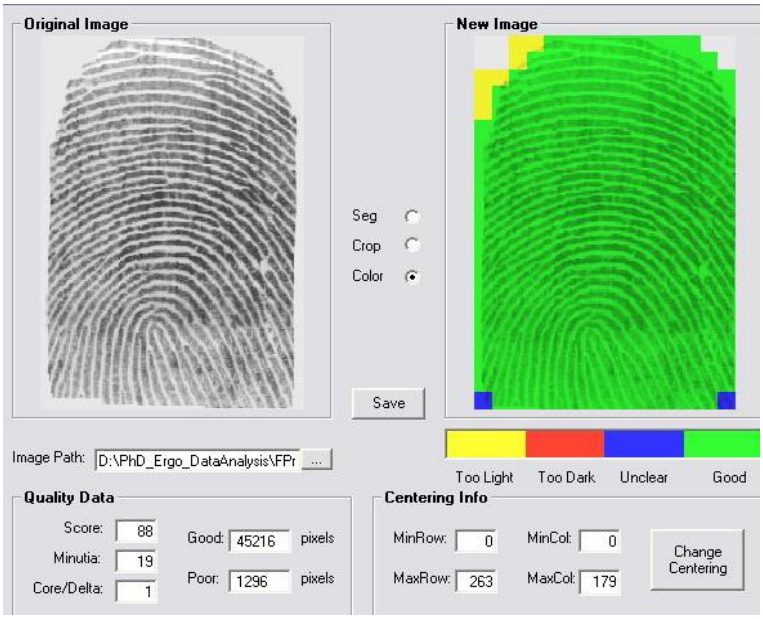
6.2 KAKOVOST BIOMETRIČNIH SISTEMOV NA OSNOVI PRSTNEGA ODTISA

Kakovost v biometriji igra ključno vlogo v procesu zajemanja vzorca, vzdrževanju baze podatkov (sprememba vzorca) in v fazi obdelave vzorcev. Izboljševanje kakovosti vodi v izboljšanje biometrične sistemske natančnosti in učinkovitosti v procesu identifikacije. V primeru opustitve kakovosti bi bil dosežen negativen vpliv na pravilnost in učinkovitost delovanja biometričnih sistemov. Kakovost je mogoče izboljšati, bodisi z izbiro, nastavitvami in konstrukcijo senzorja, (ki služi kot vmesnik za identifikacijo posameznika) bodisi s standardi, ki zagotavljajo skladnost postopka identifikacije. Za tiste vidike kakovosti v biometriji, ki jih ni mogoče načrtovani (nezmožnost zajema vzorca), je potrebno predvideti možnost za analizo kakovosti in selektivno sklicevanje na alternativne načine obdelave vzorca (Gamassi in drugi, 2005).

V primeru biometrične identifikacije s prstnim odtisom so področje kakovosti med drugimi definirali (Tabassi in drugi, 2004) v dokumentu NISTIR 7151. Prav tako so pomembne raziskave kakovosti prstnih odtisov, za različne starostne skupine ljudi (Sickler in Elliot, 2005). Dokazano je, da sta ustreznost in uporabnost prstnih odtisov obratno sorazmerna s staranjem ljudi, zlasti pomembni pa so ergonomski vidiki in uporabnost. ENVP[22], podobno kot pri določanju starostne omejitve za otroke, priporoča, da se kot dodatna izjema uvede starostna meja za starejše osebe, pri določitvi pa naj se upoštevajo obstoječe izkušnje (v programu US visit je določena meja 79 let). V literaturi je podan pregled kakovosti biometričnih postopkov (Fernandez in drugi, 2005).

Zavedajoč se pomembnosti kakovosti prstnega odtisa je podjetje Avare's razvilo programsko opremo za merjenje kakovosti slike odčitanega vzorca. Programska oprema tako glede na število zajetih značilk (0-99) poda oceno kakovosti vzorca (slika 6.3).

[22] *ENVP (evropski nadzornik za varstvo podatkov) deluje v skladu z Uredbo (ES) št. 45/2001. Uredba (ES) št. 45/2001 z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov UL L 8, 12. 01. 2001, str. 1.*



Slika 6.3: Aware's (WSQ) programska oprema za določanje kakovosti prstnega odtisa– VBQuality software v2.42E

6.3 NAPAKE PRI IDENTIFIKACIJI IN VERIFIKACIJI

Zahteve avtomatičnega prepoznavanja pri identifikaciji 1:N, kjer se po zajemu vzorca izvede iskanje enakega vzorca – predloge v podatkovni bazi, so veliko strožje kot pri verifikaciji 1:1, kjer se izkaže identiteta na kartici in potem na podlagi primerjave zajetega vzorca s samo eno predlogo na kartici ali v podatkovni bazi izvede verifikacija z rezultatom DA/NE. Če je P_1 verjetnost napake napačne primerjave pri enkratnem poskusu verifikacije, potem je verjetnost P_N vsaj enkratne napačne primerjave v podatkovni bazi z N neodvisnimi vzorci enaka:

$$P_N = 1-(1-P_1)^N, \qquad (2)$$

pri čemer je $(1–P_1)$ verjetnost, da se napaka napačne primerjave ne zgodi; v podatkovni bazi z N neodvisnimi vzorci je treba izvesti N neodvisnih poskusov, torej je $(1–P_1)^N$ verjetnost, da se napačna primerjava nikoli ne zgodi.

Ne glede na velika vlaganja v razvoj biometrije in najsodobnejšo opremo pa ne moremo zagotoviti popolne natančnosti. Vedno namreč obstajajo razlike med trenutno izmerjenimi biometričnimi parametri in podatki, shranjenimi v računalniški bazi (Hicklin in drugi, 2005). V sistemih, ki opravljajo funkcijo verifikacije oseb, imamo navadno opravka z dvema vrstama uporabnikov (klienti in vsiljivci). Za vse biometrične postopke identifikacije sta značilni dve napaki: v prvem primeru govorimo o napaki potrditve lažne osebe FAR, v drugem pa o napaki zavrnitve

prave osebe FRR (Dorizzi, 2006). V biometričnih sistemih sta FAR in FRR soodvisna vhodna parametra.

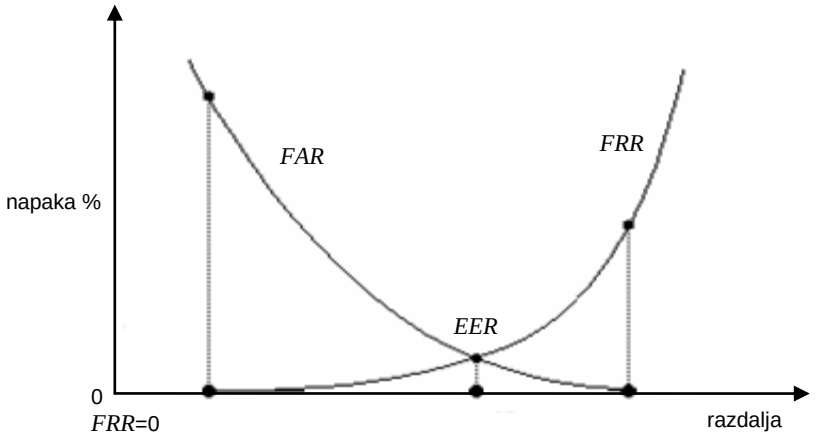
Pri identifikaciji se običajno uporabljata enotestni in tritestni protokol. V enotestnem protokolu ima posameznik pri biometrični preverbi samo eno možnost. V primeru neuspelega poskusa ta oseba biometrične identifikacije ne more opraviti ponovno. Tritestni protokol se uporablja pri bankomatih, telefonih itd. Posameznik ima tri poskuse za identifikacijo, kar zviša FRR in hkrati ne zviša FAR, ker je razlika med različnimi šablonami zelo majhna. Napaki matematično lahko opišemo z enačbama:

$$FAR = \frac{EI}{I} 100\,\% \tag{3}$$

$$FRR = \frac{EC}{C} 100\,\%. \tag{4}$$

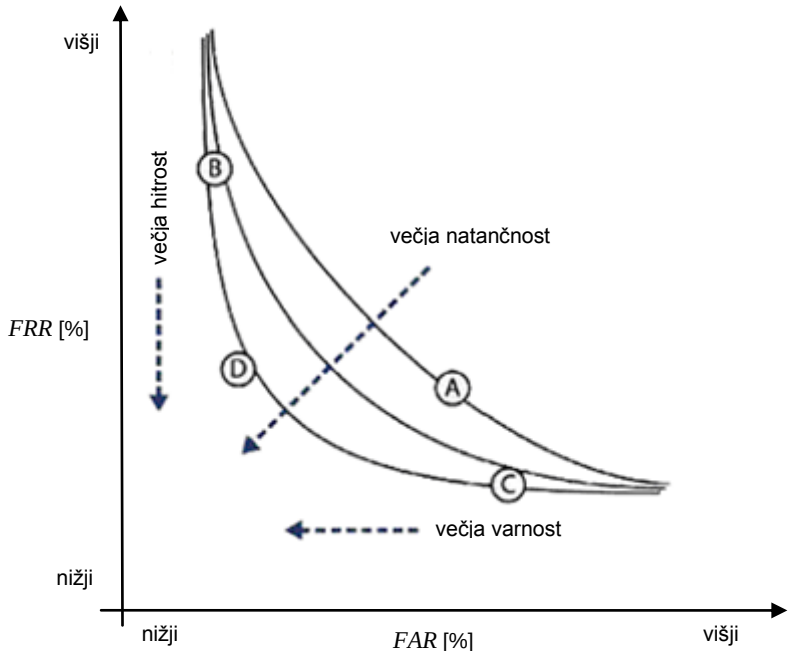
V enačbah pomeni EI število sprejetih vsiljivcev, EC število zavrnjenih klientov, I število vseh prijav vsiljivcev in C število vseh prijav klientov.

Grafični prikaz obeh napak v odvisnosti od velikosti praga sistema si lahko ogledamo na sliki 6.3. Opazimo, da ni mogoče določiti praga tako, da bi bili vrednosti FAR in FRR hkrati enaki nič, saj zmanjšanje napake FRR vodi do povečanja FAR in nasprotno. Zaradi tega izberemo vrednost praga tako, da sta vrednosti obeh napak čim manjši, kar ustreza pragu v točki EER. EER je razmerje, pri katerem sta napaki FAR in FRR enaki. Nižji je EER, za natančnejšega velja biometrični sistem (Carič in Ajdašik, 2003).



Slika 6.3: Odvisnost napak FAR in FRR od vrednosti praga (Dorizzi,2006)

Napaki FAR in FRR pogosto prikazujemo tudi v obliki funkcije $FRR(FAR)$. To krivuljo imenujemo ROC in je prikazana na sliki 6.4. Skupna variacija DET je pridobljena z uporabo normalnega odstopanja lestvic na obeh oseh. Bolj linearna oblika krivulje omogoča večjo natančnost (osvetljuje redke napake).



Slika 6.4: Krivulja ROC (Drygajlo, 2005c)

Za določanje krivulje ROC na osnovi meritev FAR in FRR v namen raziskave smo uporabili programski paket PRESS. PRESS je programska oprema proizvajalca CITeR za statistično modeliranje parametrov. Z njo določamo minimalno velikost populacije, ki jo moramo identificirati za dosego nekaterih parametrov zanesljivosti biometričnega sistema.

Poleg omenjenih napak pri vrednotenju rezultatov verifikacije večkrat uporabimo še napako $HTER$, ki predstavlja srednjo vrednost napak FAR in FRR. $HTER$ definiramo kot:

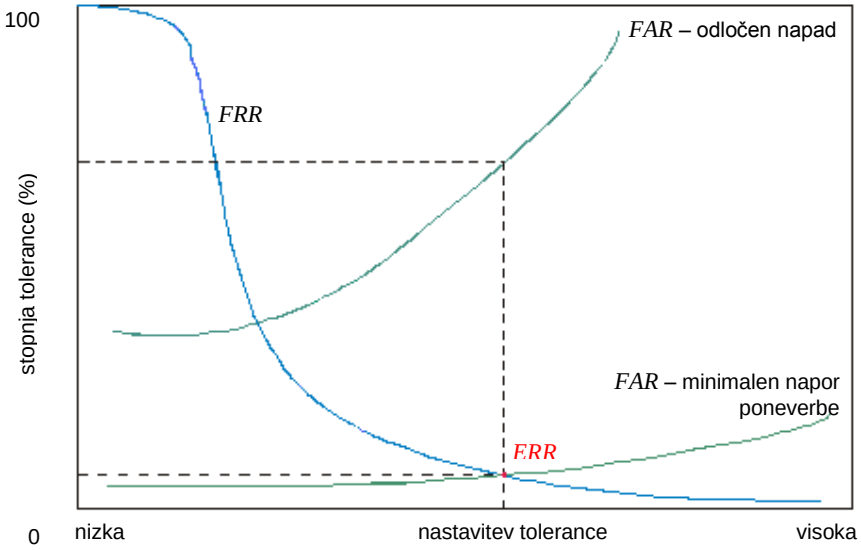
$$HTER = \frac{FRR + FAR}{2}. \qquad (5)$$

Ugotovimo lahko, da v primeru, ko za vrednost praga izberemo vrednost, ki ustreza točki EER (slika 6.4), minimiziramo napako $HTER$.

Kot je razvidno, sta stopnji FAR in FRR zelo odvisni od tolerance. To lahko nastavimo v območju, kjer sta FAR in FRR enaka oziroma se njuni krivulji sekata, in tako dobimo enako stopnjo napake (EER), vendar takšnega načina pri zahtevani visoki varnosti ne uporabljamo, saj v tem primeru želimo, da je FAR čim bližje nič, FRR pa nas ne zanima (Dorizzi, 2006). Napaka registracije (FTE ali FER) je delež vnesenih podatkov, ki se štejejo kot neveljavni ali neuspešni pri vnosu v identifikacijski sistem (podatkovno bazo). Napaka registracije se zgodi v primeru, ko se identifikacija ne izvede zaradi slabe kakovosti vzorca (Hicklin in Khanna, 2006).

Količina vzorcev je največja možna količina podatkov, ki jih lahko vnesemo v bazo identifikacijskega sistema. Nizka stopnja napak je pogoj za zadovoljivo delovanje

biometričnih naprav. V praksi se lahko nepravilna prepoznava pojavi tudi v 10 odstotkih primerov. Pri primerjanju pregledov pri biometričnih napravah pa je treba biti pozoren tudi na to, da lahko registracijo predpišemo napačnemu objektu kot funkcijo previsoke tolerance – minimalen napor poneverbe (slika 6.5). V primeru, ko se pregledovana oseba zaveda, kaj vpliva na način identifikacije, pa govorimo o »odločnem napadu«.

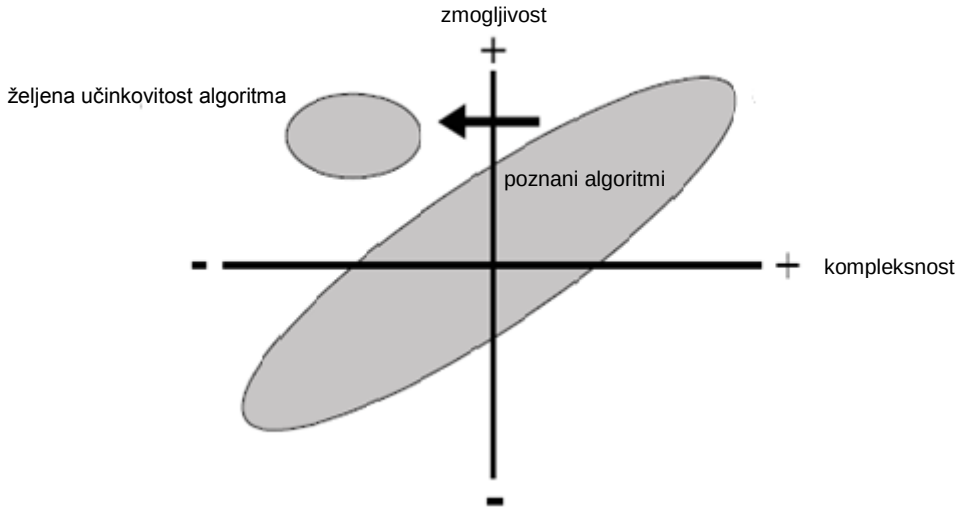


Slika 6.5: Stopnja napake kot funkcija nastavitve tolerančnega območja biometrične opreme (Carič in Ajdašik, 2003)

7 UČINKOVITOST, ZANESLJIVOST IN RAZPOLOŽLJIVOST IDENTIFIKACIJSKEGA SISTEMA

Strategija »zanesljivost, razpoložljivost in vzdrževalnost« (RAM) opisuje organizacijski pristop k načrtovanju zanesljivosti za vse sisteme, ki jih dobavitelj razvija in dobavlja svojim strankam. Strategija se lahko šteje kot osnovna formula za uspeh in se uporablja za vse vrste sistemov in storitev. Strategija načrtovanja zanesljivosti se je izkazala kot uspešna v različnih industrijskih panogah in ponekod v javnem sektorju (Drstvenšek, 2006).

Učinkovitost v kontekstu raziskave, obravnavane v doktorski nalogi, je v skladu s standardom ISO 9241–11 parameter uporabnosti biometričnega sistema, ki predvideva identifikacijo v realnem času brez nepotrebnih zapletov in intervencij administratorja sistema, kar povzroča dodatne stroške. Učinkovit sistem z razmeroma nizko kompleksnostjo in sodobnimi algoritmi dosega visoko hitrost identifikacije t. j. visoko zmogljivost. Merilo za oceno učinkovitosti je primerjava identifikacijskega sistema pred izvedeno optimizacijo in po izvedeni optimizaciji. Ta koncept učinkovitosti, je grafično prikazan na sliki 7.1.



Slika 7.1: Grafični prikaz pojma učinkovitosti identifikacijskega sistema (Donkelaar, 2000)

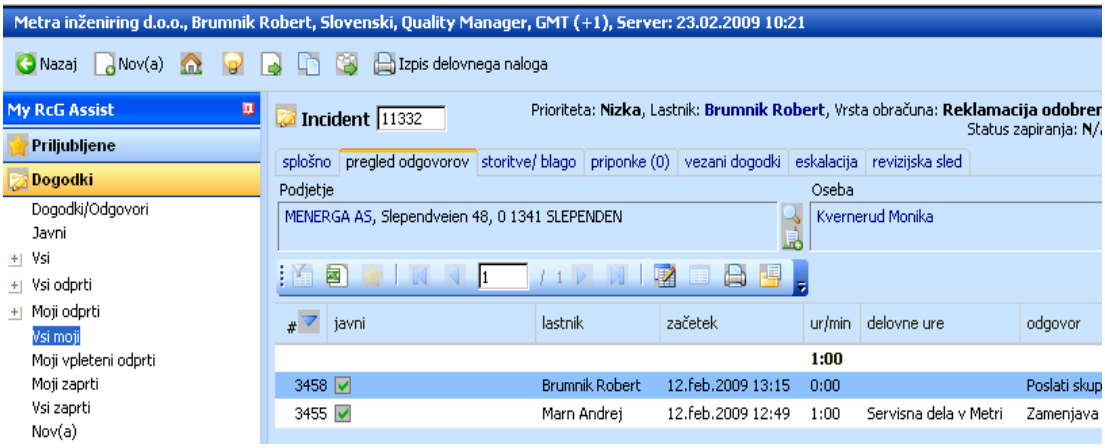
7.1 INFORMACIJSKI SISTEM ZA ZAJEMANJE PODATKOV O IZREDNIH DOGODKIH

Informacijska tehnologija je prodrla v vse dele tekočega poslovanja, tako da skoraj ni več področja, ki bi lahko operativno delovalo brez nje. Vse bolj pa postaja tudi ključnega strateškega pomena pri inženiringu zanesljivosti. Informacijska tehnologija mora zato delovati načrtno, urejeno in v skladu s strateškimi cilji podjetja. Svojo vlogo lahko ustrezno odigra skozi uspešno izvedene projekte. Vendar pri tem ne gre

le za informacijske projekte, saj so tudi razvojni projekti in projekti rasti v podjetju lahko učinkovito načrtovani, izpeljani in nadzirani le s pomočjo ustreznega informacijskega okolja. Tega pa ni mogoče vzpostaviti brez ustrezno usposobljenih kadrov.

7.1.1 RcG INFORMACIJSKI SISTEM ZA VNOS PODATKOV O IZREDNIH DOGODKIH

Informacijski sistem za vnos podatkov o izrednih dogodkih je ena od komponent integriranega poslovnega sistema. Na sliki 7.2 je ekranska maska programskega modula RcG za vnos podatkov o izrednih dogodkih, ki je bil uporabljen za zajem podatkov v namen raziskave. Tehnologije, ki dopolnjujejo integriran model sistema, so tehnologije skupinskega dela, poteka posla, sodelovanja v skupini. Tako informacijska tehnologija poda relevantne informacije o stanju implementiranih identifikacijskih sistemov pristopne kontrole v realnem času.



Slika 7.2: Grafični vmesnik – ekranska maska RcG za vnos podatkov o izrednih dogodkih

Taki poslovni sistemi pomenijo premik na omrežno usmeritev, ki jo ponujata intranet in svetovni splet. Ti sistemi temeljijo na modelu fleksibilnosti informacijske strategije in omogočajo medorganizacijske informacijske tokove z dobavitelji, distributerji in kupci. Evolucijo modelov obdelave informacij v zadnjem desetletju lahko prikažemo v treh stopnjah (Gorenšček, 2001):

1. avtomatizacija ali povečanje učinkovitosti operacij,
2. racionalizacija postopkov ali usmeritev postopkov in odpravljanje očitnih ozkih grl in
3. reinženiring ali radikalna prenova poslovnih procesov, ki temeljijo na intenzivni prenovi informacijske tehnologije delovnih tokov in procesov.

V vseh teh fazah je informacijska tehnologija temeljila na razmeroma predvidljivih sistemih in storitvah ter ustreznih organizacijskih in industrijskih strukturah. Z vse večjo vlogo kupcev, dobaviteljev in posrednikov v dinamičnih cenovnih modelih zunanji trg vpliva na določitev interne logistike poslovanja. Nov poudarek na vrednosti informacije, pravzaprav znanja, na neoprijemljivi vrednosti in intelektualnem kapitalu je dvignil virtualna podjetja nad »standardna«. Tako imenovana net podjetja so redefinirala svojo vrednost v odnosu do dobaviteljevih,

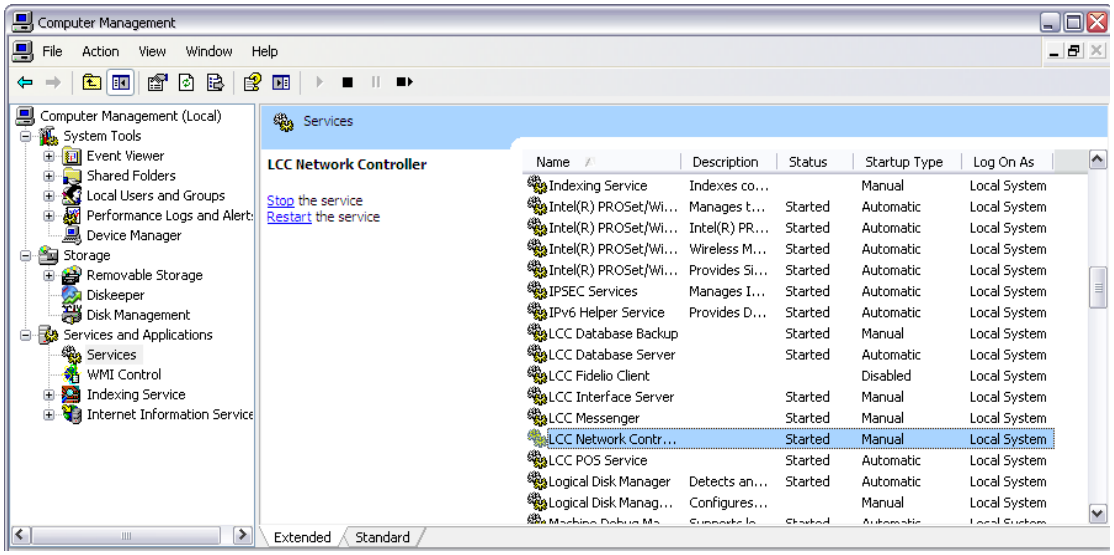
internih in distributorskih verig. Poslovni strateg Hamel za Harvard Business Review (2006) trdi, da inovativna strategija za premik tradicionalnega poslovnega sveta v e–poslovni svet pomeni tudi 70 % tako tveganja na eni strani kot dobička na drugi, le 30 % pa je odvisnih od informacijske tehnologije za poslovni reinženiring, racionalizacijo delovnih procesov in avtomatizacijo.

7.1.2 SISTEMSKI DNEVNIK PROGRAMSKE OPREME ELS PRISTOPNE KONTROLE

Sistemski dnevnik (system log) avtorizacijskega računalnika je datoteka, v katero se zapisujejo različna sporočila, ki jih generira identifikacijski sistem ELS. S tem omogočimo transparentnost (vpogledljivost) in sledljivost dogajanju v sistemu in njegovem okolju. Kako »daleč« v okolje vidimo, je odvisno od tega, katera sporočila zapisujemo v sistemski dnevnik.

Ponavadi sporočila delimo na sistemska in aplikativna. V našem primeru bomo pod sistemskimi sporočili razumeli vse vrste komunikacijskih sporočil, ukazna sporočila napravam v sistemu, ukaze za prenos parametrov, sporočila za izmenjavo varnostnih ključev, sporočila za administracijo sistema, sporočila za vzpostavitev in preverjanje seje ter tudi sporočila o stanju posameznih procesov sistema.

Pod aplikativna sporočila pa štejemo sporočila, ki izhajajo iz uporabniške aplikacije: stanje uspešnih in neuspešnih identifikacijskih postopkov, podatki o identifikacijski kartici, stanje na računu identifikacijskega elementa, podatki iz aplikativnih podatkovnih baz, avtorizacijski zahtevki itd. Sporočila se v sistemski dnevnik zapisujejo v prihajajočem časovnem zaporedju, ki je vezano na nastavitev centralnega sistemskega časa (slika 7.3). Vsako sporočilo je enolično določeno s pripadajočo številko, vrsta sporočila pa z njegovo kodo. Tako lahko s krmilnimi ukazi pridemo do tistega sporočila, ki nas v danem trenutku zanima.



Slika 7.3: Sistemski dnevnik mrežnega sistema LCC

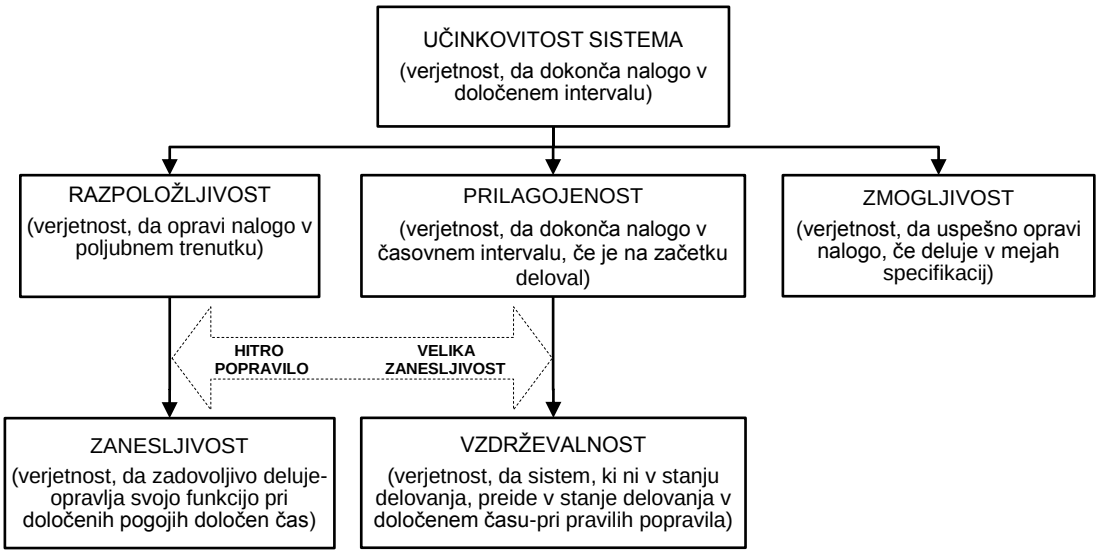
7.2 KLASIFIKACIJA ODPOVEDI IN DEFINICIJE ZAGOTOVITVENIH ZNANOSTI

Zanesljivost je ena najpomembnejših karakteristik učinkovitosti informacijskega sistema. Vpliva tako na njegovo varnost kot na učinkovitost. Zanesljivost ni časovno konstantna vrednost. Povečanje zanesljivosti sistema pomeni manj zastojev in s tem manjše stroške poslovanja. S konstrukcijskimi posegi v razvojni fazi, se slabosti odpravi. Tudi sestavne dele proizvajalci nenehno izboljšujejo, tako da zanesljivost vseh gradnikov raste. Analiza odpovedi in odpravljanje napak povečujeta zanesljivost. Z ekstrapolacijo ocenimo zanesljivost in uporabno dobo izdelka. Ta podatek pomaga pri načrtovanju proizvodnje rezervnih delov.

V vezi z inženiringom zanesljivosti sta Hoyland in Rausand (1994) podala definicije:

- Učinkovitost sistema je verjetnost, da sistem uspešno opravi (izpolni) zahtevano nalogo v določenem času in pod določenimi pogoji. Odvisna je od razpoložljivosti, prilagojenosti in zmogljivosti. Komponente učinkovitosti so shematsko prikazane na sliki 7.4.
- Razpoložljivost je verjetnost, da sistem v poljubnem trenutku zadovoljivo deluje, če deluje v določenih pogojih. Odvisna je od zanesljivosti in vzdrževanosti sistema, ki morata biti opredeljeni in vgrajeni že v razvojni fazi.
- Prilagojenost je verjetnost, da sistem v določenih pogojih konča nalogo v določenem intervalu, če je na začetku tega intervala deloval zadovoljivo. Odvisna je od zanesljivosti in vzdrževanosti sistema.
- Zmogljivost je verjetnost, da sistem uspešno opravi (izpolni) dano nalogo v mejah določenih specifikacij.
- Zanesljivost je verjetnost, da sistem v določenih pogojih zadovoljivo deluje določen čas.
- Vzdrževanost je verjetnost, da se sistem, ki je odpovedal, v določenem času povrne v stanje zadovoljivega delovanja, če so vzdrževalni pogoji skladni s predpisanimi postopki.
- Odpoved sistema (sestavnega dela) je prenehanje njegove sposobnosti, da zadovoljivo opravlja zahtevano funkcijo.

Programe zanesljivosti, pripadajočo terminologijo in matematične metode, ki so v uporabi za zagotavljanje, predvsem pa za povečanje zanesljivosti in razpoložljivosti opisujejo nekateri mednarodni standardi (IEC 60812, IEC 61014, IEC 61078, IEC 61164, IEC 61165, IEC 61703 itd.)



Slika 7.4: Shema gradnikov učinkovitosti sistema (Hudoklin in Rozman, 2004)

Odpovedi sistema klasificiramo glede na različne kriterije (Hudoklin in Rozman, 2004).

Glede na stopnjo jih delimo na delne in popolne. Delna odpoved povzroči poslabšanje delovanja, ne prepreči pa povsem opravljanja zahtevane funkcije. Popolna odpoved povzroči, da zahtevane funkcije ni mogoče opravljati.

Po hitrosti nastajanja delimo odpovedi na postopne in nenadne. Postopno odpoved je možno predvideti na osnovi predhodne preiskave (poznan fizikalno–kemijski model), nenadne odpovedi pa ne. Delne in postopne so degradacijske, nenadne in popolne odpovedi pa so katastrofalne.

Glede na vzrok delimo odpovedi na odpovedi zaradi pomanjkljivosti projekta, proizvodnje, transporta in instalacije sistema/elementa/gradnika sistema, odpovedi zaradi njegove napačne rabe in odpovedi zaradi staranja ali obrabe materiala. Pri analizi zanesljivosti sistemov se je v zadnjem obdobju pojavil tudi pojem odpoved s skupnim vzrokom. Taka odpoved izniči koristi vzporednih vezav gradnikov sistema s stališča zanesljivosti.

Odpovedi klasificiramo tudi glede na njihov učinek. Nekatere odpovedi sestavnih delov ne vplivajo neposredno na funkcijo sistema in zahtevajo le občasne korektivne dejavnosti, druge pa vplivajo neposredno na funkcijo sistema. Običajno delimo odpovedi po učinku na štiri razrede: manj pomembne, pomembne, zelo pomembne in kritične. Manj pomembna odpoved povzroči degradacijo funkcije sistema, katere posledica je zanemarljiva škoda na sistemu ali njegovi okolici. Človeka ne ogroža. Pomembna odpoved poslabša funkcijo sistema, ne da bi znatno poškodovala sistem, njegovo okolico ali človeka. Zelo pomembna odpoved povzroči prenehanje primarne funkcije sistema. Posledica take odpovedi je znatna škoda na sistemu ali v njegovi okolici in zanemarljiva ogroženost človeka. Kritična odpoved povzroči prenehanje primarne funkcije sistema. Posledica je znatna škoda na sistemu ali v njegovi okolici in/ali poškodba ali smrt človeka.

7.3 ZANESLJIVOST ČLOVEKA

Za kvantitativno ocenjevanje zanesljivosti človeka v sistemu človek – stroj je bilo razvitih več različnih metod in matematičnih modelov. Večina jih je prilagojena pogojem delovanja človeka v kompleksnih sistemih določenega tipa (Hudoklin in Rozman, 2004).

Pri določanju ocene za verjetnost človekove odpovedi HEP moramo upoštevati vrsto dejavnikov, med katerimi so najpogostejši naslednji (Villemeur, 1992):

- kompleksnost naloge,
- čas, ki je na razpolago,
- vrst vmesnika preko katerega deluje človek,
- obremenjenost človeka in
- obremenljivost človeka.

V literaturi srečamo vrsto metod, ki jih označujejo kar kratice njihovih angleških imen in so razvrščene po načinu zbiranja podatkov. Metode TESEO, THERP, ASEP in OAT so zasnovane na principu razčlenjevanja človekovih opravil na enostavnejša opravila. Za ta opravila potem na osnovi empiričnih podatkov ali podatkov iz preskusov in simulacij določimo oceno za kvantitativno karakteristiko zanesljivosti HEP. Ostale metode omogočajo določitev HEP za kompleksna opravila in v glavnem uporabljajo podatke, pridobljene na osnovi ekspertnih mnenj (Hudoklin in Rozman, 2004).

7.4 ZANESLJIVOST IN PRESKUSI ZANESLJIVOSTI STROJNE OPREME

Odvisnost karakteristik zanesljivosti gradnikov strojne opreme od delovnih pogojev (način delovanja ter nivoji notranjih in okoliških obremenitev) moramo poznati, da lahko vrednosti karakteristik zanesljivosti, ki jih določimo na osnovi laboratorijskih preskusov, prilagodimo pogojem dejanske uporabe gradnikov (Hudoklin in Rozman, 2004). Rezultati izračunavanja zanesljivosti so povprečja, ocene in predvidevanja in so boljši ali slabši približek dejanskega stanja (Lyu, 1996). Potrebni so obsežni in dolgotrajni preskusi velikega števila enot. Med obratovanjem je treba opazovati večje število enakih primerkov in zapisovati čase njihovih odpovedi. Lahko pa beležimo število odpovedi v posameznih časovnih intervalih. Če to število izpadlih naprav še normiramo s številom vseh opazovanih, dobimo gostoto verjetnosti za čas do odpovedi. Ob določitvi pogostosti odpovedi pa lahko izračunamo skoraj vse druge mere, ki opisujejo zanesljivost izdelka.

Preskuse zanesljivosti lahko razvrstimo glede na različne kriterije. Najpogosteje jih delimo glede na cilj, način obremenjevanja in stopnjo razvoja oziroma osvajanja proizvodnje (Hudoklin in Rozman, 1985). Pri načrtovanju in izvajanju preizkusov zanesljivosti lahko uporabimo različne vrste preizkusov, ki jih planiramo in izvajamo v odvisnosti od narave preizkušanca in zmožnosti testnega okolja (laboratorij, delovno okolje itd.).

Vrste preizkusov zanesljivosti so:

- pospešeni preizkus. Podatke o odpovedih dobimo v razmeroma kratkih obdobjih, obremenitve so večje od običajnih, skrajšamo čas do odpovedi,
- popolni preizkus. Čakamo, da odpovedo vsi preizkušanci v vzorcu,
- primerjalni preizkus. Primerjamo npr. pogostosti odpovedi λ istovrstnih izdelov različnih proizvajalcev,
- okrnjeni preizkus. Preizkus prekinemo glede na čas, porabljen za preizkušanje, ali glede na število odpovedanih primerkov.

Pri načrtovanju preizkusov moramo upoštevati:
- način izbire vzorcev (naključni vzorec),
- tip preizkusa,
- obseg preizkušanja,
- odpovedi, ki jih bomo opazovali in
- karakteristike zanesljivosti in učinkovitosti, ki jih bomo določili.

Pri izvajanju preizkusov:
a. izpostavljamo vzorce preskušancev določenim obremenitvam
b. preskus prekinemo v določenih intervalih zaradi meritev in registriramo čase do odpovedi oziroma število preskušancev, ki so odpovedali v posameznem časovnem intervalu.

Izvajamo tudi izločilne preskuse na celotni populaciji v obdobju zgodnjih odpovedi. S tem izločimo potencialno nezanesljive primerke in zagotovimo dobro kakovost izdelave, ki je predpogoj za izkoriščanje vgrajene zanesljivosti. Najbolj značilen preskus je staranje ali vtekanje (Hudoklin in Rozman, 2004).

Za izvedbo preizkušanja biometričnih sistemov v namen raziskave zasledujemo standarde ISO/IEC19795-1 (2006), ISO IEC 29109 in INCITS M1.

7.5 ZANESLJIVOST IN PRESKUSI ZANESLJIVOSTI PROGRAMSKE OPREME

Napake v programski opremi v času uporabe lahko povzročijo odpovedi in stroške, ki precej presegajo stroške dodatnega iskanja napak pri preskušanju v fazi razvoja pred dokončno uporabo programske opreme. Zanesljivost programske opreme empirično določimo kot normirano število programskih napak, t.j. število napak na časovno enoto, deljeno s številom vseh strojnih instrukcij programske opreme. Zanesljivost programske opreme lahko definiramo tudi kot verjetnost, da programska oprema deluje brez napake v času opazovanja na matični aparaturni opremi v mejah, ki so bile postavljene predhodno v okviru specifikacij opreme (Solina, 1997). Na kompatibilni opremi je zanesljivost lahko že manjša (neobvezujoča za razvijalca).

V praksi je znanih več orodij in metodologij[23] za določanje zanesljivosti programske opreme. Večina modelov za določanje zanesljivosti programske opreme vsebuje naslednje sestavne dele: predpostavke, dejavnike in matematično funkcijo, ki se nanaša na zanesljivost. Matematična funkcija je običajno eksponentna (višje stopnje) ali logaritemska (Pan, 1999). Tehnike modeliranja zanesljivosti programske opreme lahko razdelimo v dve podkategoriji: napovedovanje in ocenjevanje. Obe

[23] *CMMI, FMEA itd.*

tehniki temeljita na opazovanju in zbiranju podatkov ter analiziranju napak s statističnim sklepanjem. Glavna razlika modelov je prikazana v tabeli 7.1.

Tabela 7.1: Razlika modelov napovedovanja in ocenjevanja zanesljivosti programske opreme (Pan, 1999)

	Model napovedovanja	Model ocenjevanja
Uporabljeni podatki	podatki preteklih projektov	uporaba podatkov trenutnega razvoja programske opreme
Kdaj je uporabljen v razvojnem ciklu	običajno se uporabijo pred razvojem ali preskusnih fazah v zgodnji fazi koncipiranja	ponavadi kasneje v življenjskem ciklu (po tem ko so bili podatki zbrani), običajno se ne uporablja v konceptni ali razvojni fazi
Časovni okvir	napovedovanje zanesljivosti za prihodnost	ocena zanesljivosti za sedanjost in delno tudi za prihodnost

Predstavniki modelov napovedovanja zanesljivosti so modeli Musa, Putnam, TR-92-51, TR-92-15 itd. Z uporabo modelov za predvidevanje lahko zanesljivost programske opreme napovemo zgodaj v razvojni fazi in tako sprejmemo korektivne ukrepe za izboljšanje zanesljivosti. Predstavniki ocenjevalnih modelov pa so modeli eksponentnih porazdelitev in Weibullov, Thompsonov, Chelsonov model itd.

Računanje zanesljivosti programske opreme z orodjem CASRE omogoča določanje zanesljivosti programske opreme na osnovi skoraj vseh obstoječih modelov, kot vhodne podatke pa lahko sprejme intervalne in časovne podatke (Open Channel Foundation, 2000). S programi SRE (Williams, 2007):

- v fazi »razhroščevanja« programske opreme zapisujemo čase odkritja napak,
- z uporabo modelov lahko napovemo intenzivnost pojavljanja še neodkritih napak,
- zanesljivost programske opreme lahko napovedujemo le, če se hkrati z odkrivanjem in odpravljanjem napak v razvojni fazi, ko program preskušamo, povečuje zanesljivost (časi med odkritimi napakami se povečujejo),
- vhodni podatki modelov so časi med odkritimi napakami.

Zahteve metrike zanesljivosti v izogib različnim interpretacijam med kupcem in stranko ali soudeleženim v projektu določajo med drugimi standardi IEEE 982.2 (1987), MIL-STD-498 (1994), ISO/IEC 2382-14 (1997) idr. V nadaljevanju si bomo pogledali dve tipični metodi izvajanja testiranja programske opreme.

7.5.1 INTERVALNO TESTIRANJE – INTERVALNI PODATKI

Programsko opremo testiramo v časovnih intervalih (failure counts), pri čemer:

- zapisujemo število odkritih napak v vsakem testnem intervalu ter delež programske opreme, testirane v tem intervalu (pokritost),
- dolžina intervalov je lahko spremenljiva,
- hkrati lahko določamo tudi resnost vsake od odkritih napak (npr. od 1 – manj huda do 9 – zelo huda napaka).

Prednost tega načina je enostavno testiranje, saj evidentiramo število odkritih napak le ob koncu vsakega testnega intervala (npr. ob koncu 8 urnega delavnika).

7.5.2 NEPREKINJENO TESTIRANJE – PODATKI ZA ČASE DO ODPOVEDI

V času testiranja evidentiramo čas, ki preteče od odkritja predhodne do trenutne napake (George, 2001). Hkrati pa določamo tudi resnost vsake od odkritih napak (npr. z ocenami od 1 do 9). Slabost tega pristopa je potreba po sprotnem zapisovanju časa nastopa odpovedi.

Omenjeni model testiranja bomo uporabili v naši raziskavi, vsekakor pa je pomembno določiti osnovne parametre (npr. število vzorcev, matematično zaupanje itd.), da bo testiranje dalo kar najbolj verodostojne rezultate ob določenih pogojih.

Za intervalno testiranje, kot tudi neprekinjeno testiranje programske opreme lahko uporabimo programska orodja[24], s katerimi lahko glede na statistični model in vhodne parametre določamo zanesljivost programske opreme.

7.6 KVANTITATIVNE KARAKTERISTIKE ZANESLJIVOSTI IN RAZPOLOŽLJIVOSTI

Kot mero zanesljivosti sistemov in njihovih sestavnih delov uporabljamo različne kvantitativne karakteristike. Nekatere so funkcije časa, druge pa so časovna povprečja. Katere karakteristike so primerne, je odvisno od postavljenih ciljev, izbrane metode analize in dosegljivosti podatkov (Abernethy, 2004). Karakteristike zanesljivosti temeljijo na časih do odpovedi. Čas do odpovedi je naključna spremenljivka. Definicije kvantitativnih karakteristik zanesljivosti so povzete po Hoylandu in Rausandu (1994).

Funkcija nezanesljivosti $F(t)$ je verjetnost, da sistem (sestavni del) odpove v časovnem intervalu med 0 in t:

$$F(t) = P(X \le t)\,. \tag{6}$$

$F(t)$ je torej verjetnost, da sistem ali kritični sestavni del odpove v časovnem intervalu med 0 in t.

Če opazujemo množico primerkov določenega sistema ali njegovega sestavnega dela, lahko izračunamo točkasto oceno za funkcijo nezanesljivosti po formuli:

$$\widehat{F}(t) = \frac{N_0 - N(t)}{N_0}, \tag{7}$$

pri čemer je:
$N(t)$ – število primerkov, ki so zadovoljivo delovali v intervalu (0, t),
N_0 – število primerkov na začetku opazovanja pri t = 0.

[24] *SMERFS, SoftRel idr.*

Funkcija zanesljivosti $R(t)$ je verjetnost, da sistem (sestavni del) odpove po času t:

$$R(t) = 1 - F(t) = P(X > t). \tag{8}$$

Statistično oceno za funkcijo zanesljivosti določimo po formuli:

$$\hat{R}(t) = \frac{N(t)}{N_0}. \tag{9}$$

Funkcija gostote verjetnosti za čas do odpovedi $f(t)$, pomnožena z dt, je verjetnost, da sistem ali sestavni del odpove v intervalu $(t, t+\Delta t)$. Funkcijo $f(t)$ izračunamo s časovnim odvodom funkcije nezanesljivosti:

$$f(t) = \frac{dF(t)}{dt}. \tag{10}$$

Statistično oceno za $f(t)$ izračunamo iz enačbe:

$$\hat{f}(t) = \frac{N(t) - N(t+\Delta t)}{N_0 \, \Delta t} \tag{11}$$

pri čemer je Δt interval $(t, t+\Delta t)$.

Trenutna pogostost odpovedi $\lambda(t)$, pomnožena z dt, je pogojna verjetnost, da sistem (sestavni del) odpove v intervalu $(t, t+\Delta t)$ pri pogoju, da je zadovoljivo deloval v intervalu $(0, t)$:

$$\lambda(t) = \frac{f(t)}{R(t)}. \tag{12}$$

Statistična ocena za $\lambda(t)$ je podana z izrazom:

$$\hat{\lambda}(t) = \frac{N(t) - N(t+\Delta t)}{N(t) \, \Delta t}. \tag{13}$$

Povprečen čas do odpovedi sistema $MTTF$ je karakteristika zanesljivosti, ki ni funkcija časa, temveč je povprečna vrednost funkcije gostote verjetnosti za čase do odpovedi (Hudoklin in Rozman, 2004):

$$MTTF = \int_0^\infty t f(t) dt = \int_0^\infty R(t) dt \tag{14}$$

Točkasto oceno za povprečni čas do odpovedi $MTTF$ izračunamo za n časov do odpovedi s cenilko:

$$\hat{MTTF} = \frac{1}{n}\sum_{i=1}^{n} t_i \ . \tag{15}$$

V obdobju normalnega delovanja je $MTTF$ enak:

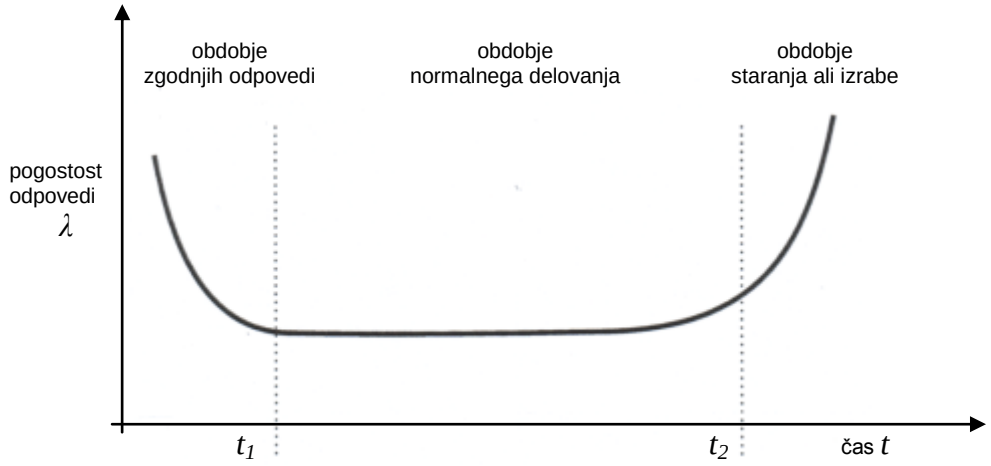
$$MTTF = \frac{1}{\lambda}. \tag{16}$$

Funkcija $\lambda(t)$ ima za veliko število sistemov oziroma njihovih sestavnih delov značilno obliko kopalne kadi (slika 7.5). Življensko dobo sistema lahko glede na potek $\lambda(t)$ razdelimo na tri obdobja:

1. obdobje zgodnjih odpovedi,
2. obdobje normalnega delovanja in
3. obdobje staranja oziroma izrabe.

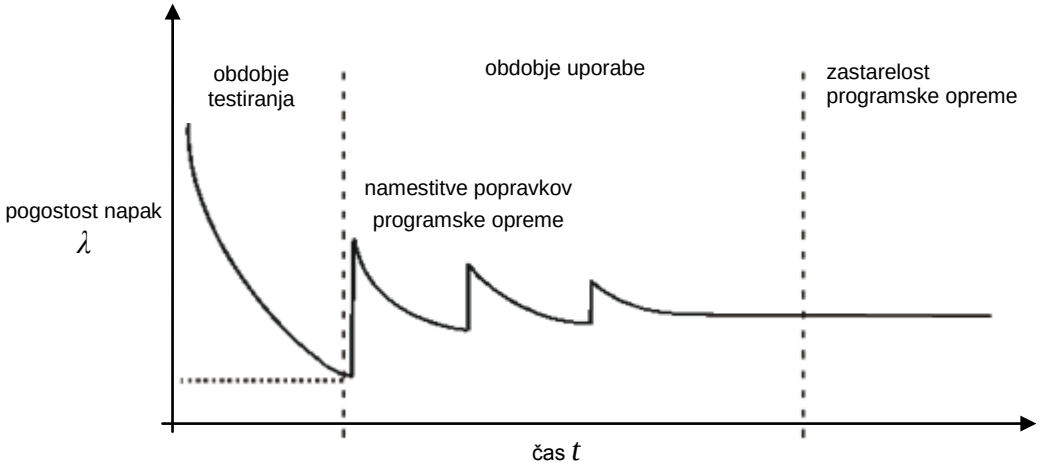
V prvem obdobju krivulja za $\lambda(t)$ pada, v drugem je konstantna, v tretjem pa narašča (Hudoklin in Rozman, 2004). Odpovedi v prvem obdobju se pojavljajo zaradi grobih odpovedi v proizvodnji (napak v konstrukciji, sestavi ali transportu itd.) ter zaradi človeškega dejavnika (uporabnik še ne zna ravnati s sistemom). Odpovedi v drugem obdobju nastanejo iz različnih nepovezanih vzrokov, ki so tudi posledica skritih napak v postopku razvoja in izdelave hardvera, ali napak človeka pri zaznavanju dražljajev in odzivu nanje. Imenujemo jih nenadne odpovedi. V tretjem obdobju začne trenutna pogostost odpovedi naraščati, ker postane poglaviten mehanizem odpovedi staranje ali obraba materialov ali utrujenost človeka. Staranje povzročijo različne ireverzibilne fizikalno-kemične spremembe, ki nastajajo tudi, če sistem ni normalno obremenjen.

V obdobju zgodnjih odpovedi in obdobju izrabe se pojavljajo katastrofalne in degradacijske odpovedi, v obdobju normalnega delovanja pa predvsem katastrofalne (Hoyland, 1994). Trenutna pogostost odpovedi v obdobju normalnega delovanja je neodvisna od časa. Imenujemo jo pogostost odpovedi, označujemo pa s simbolom λ. Trenutna pogostost zaključkov popravil $\mu(t)$, pomnožena z dt, je pogojna verjetnost, da popravimo komponento v intervalu (t, $t+\Delta t$) pri pogoju, da v intervalu (0,t) še ni bila popravljena (delovala ni zaradi odpovedi).



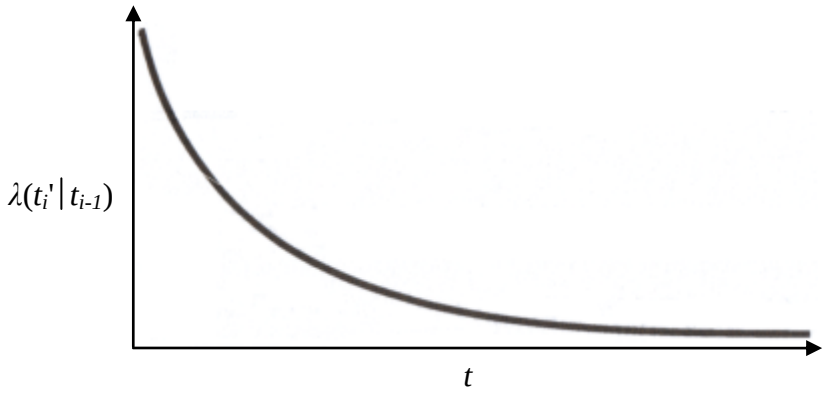
Slika 7.5: Krivulja »kopalne kadi« za strojno opremo (Hudoklin in Rozman, 2004)

V primeru določanja zanesljivosti programske opreme dobimo za pogostost odpovedi značilno žagasto krivuljo, ki nakazuje padanje pogostosti odpovedi v odvisnosti od časa. Krivulja kopalne kadi, se z odpravljanjem napak v programski opremi modificira v krivuljo, prikazano na sliki 7.6. Pogostost napak se v odvisnosti od časa manjša v razvojni fazi, prav tako v obdobju uporabe ni obrabe programske opreme (RAC, 1996).



Slika 7.6: Krivulja pogostosti napak programske opreme (RAC, 1996)

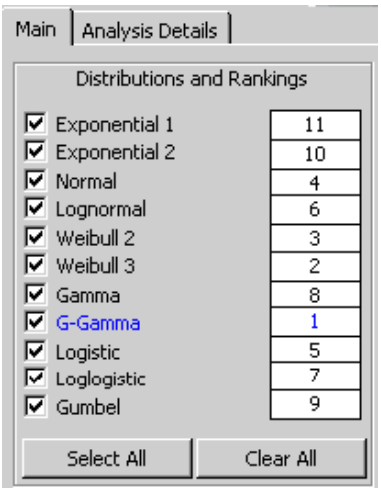
Poissonov model predpostavlja, da lahko z izvajanjem odkrijemo vse napake in z njihovo odstranitvijo pridemo do absolutno zanesljivega programa (Hudoklin in Rozman, 2004). S slike 7.7 je razvidno, da se trenutna pogostost odpovedi programa z odpravljanjem napak zvezno zmanjšuje.



Slika 7.7: Trenutna pogostost odpovedi programske opreme po modelu Poissonovega tipa za $\lambda_a(t)$ = konstanta (Hudoklin in Rouman, 2004)

7.6.1 WEIBULLOV MODEL

Pri statistični obravnavi izmerjenih podatkov se velikokrat zadovoljimo z izračunom povprečne vrednosti in standardne deviacije opazovane veličine, ki pa nam ne povesta vseh informacij o njeni statistični porazdelitvi. Zato je priporočljivo najprej ugotoviti, za katero statistično porazdelitveno funkcijo v danem primeru sploh gre (slika 7.8), potem pa najti parametre te funkcije. Čeprav se pri statistični obravnavi za večje količine podatkov za obdobje normalnega delovanja uporablja eksponentna porazdelitev, za obdobje izrabe pa Gaussova porazdelitev, je za določitev nekaterih lastnosti zanesljivosti sistemov ustreznejša Weibullova porazdelitev. S slednjo namreč lahko popišemo vsa tri življenska obdobja opazovanih vzorcev.



Slika 7.8: Določitev porazdelitvene funkcije s programsko opremo Weibull++7

Za določitev ocen karakteristik zanesljivosti torej lahko uporabimo Weibullov porazdelitveni zakon (Abernethy, 2004):

$$f(t)=\frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1}\exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right], \tag{17}$$

$$\lambda(t)=\frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1}. \tag{18}$$

Pri tem sta parameter oblike β (shape parameter) in umeritveni parameter η (scale parameter) parametra porazdelitve. S stališča zanesljivosti je parameter η karakteristična življenska doba. Triparametrično Weibullovo statistiko dobimo iz dvoparametrične tako, da dodamo še parameter premika γ (location parameter) in v gornjih enačbah naredimo transformacijo $t \rightarrow t-\gamma$, kar pomeni, da je teoretično najmanjša možna vrednost veličine t enaka γ namesto 0. V praksi bi to pomenilo, da pride do odpovedi že pred regularno uporabo, npr. v skladišču.

7.6.1.1 Vhodni podatki za grafično Weibullovo metodo

Avtorji O'Connor (2002) in Kneževič (1997) ugotavljajo, da kljub dejstvu, da obstaja več različnih papirjev za distribucijo verjetnosti odpovedi, vsi temeljijo na istem načelu.

Obravnavali bomo Weibullovo verjetnostno mrežo in kratko razpravljali o uporabi grafične metode. Gre za ročno določitev parametrov, ki je dobra tudi v primerih, ko imamo na razpolago malo podatkov. V primeru določanja zanesljivosti z uporabo grafične Weibullove metode je osnova verjetnostni papir, na katerem je funkcija $F(t)$ linearizirana. Nomogrami na verjetnostnem papirju omogočajo odčitavanje ocen parametrov porazdelitve (β, η ter γ), ki nato služijo za računanje ocen karakteristik zanesljivosti. Vhodni podatki za analizo so časi do odpovedi t_i, razvrščeni po velikosti, in ocene funkcije nezanesljivosti, ki jih izračunamo po formuli:

$$\hat{F}(t_i)=\frac{i-0{,}3}{N+0{,}4} \tag{19}$$

N – velikost vzorca (sample size)
i – zaporedna številka odpovedi (opazovanja)

Raziskavo podkrepimo s konstrukcijo Weibullove krivulje na verjetnostnemu papirju, kjer določimo parametre porazdelitve (β, η, μ ter γ). Na Weibullov verjetnostni papir (slika 7.9) vnesemo točke (t_i, $F(t)$). Povleči moramo krivuljo (običajno je to premica), ki se najbolj prilega množici vrisanih točk.

Postopek ročne metode določanja parametrov zanesljivosti iz Chartwellovega modela Weibullovega verjetnostnega papirja, smo podrobneje pokazali v dodatku 3. Metoda je uporabna tudi za primere, ko imamo na razpolago manjše število merjenih podatkov.

Varianco porazdelitve časov do odpovedi izračunamo po formuli:

$$\sigma^2 = \eta^2 \left[\Gamma\left(1+\frac{2}{\beta}\right) - \Gamma^2\left(1+\frac{1}{\beta}\right) \right] \quad (20)$$

Dvoparametrični Weibullov model lahko opišemo s funkcijami za določanje zanesljivosti (Hudoklin in Rozman, 2004):

$$\hat{R}(t) = \exp\left(-\left(\frac{t}{\eta}\right)^{\beta} \right). \quad (21)$$

σ – standardni odmik od povprečne življenjske dobe
β – parameter oblike
η – karakteristična življenjska doba (characteristic life), ki pri β = 1 postane povprečna življenska doba
Γ – funkcija Gamma
γ – parameter lokacije

Zaradi boljšega ujemanja ekperimentalnih točk s krivuljo na mreži, lahko vpeljemo še tretji parameter ter uporabimo tri parametrično Weibullovo porazdelitveno funkcijo. Čas γ ustreza začetnemu času oz. obdobju, ki so ga elementi preživeli pred začetkom delovanja v napravi, npr. med procesom izdelave, ob začetnem pospešenem staranju ali testiranju (pred začetkom opazovanja).

7.6.1.2 Parameter β (shape parameter)

Parameter oblike beta spreminja obliko funkcije porazdelitve časov do odpovedi, hkrati pa je značilen tudi za obliko funkcije $\lambda(t)$.

β – parameter oblike

1. $\beta < 1$ – trenutna pogostost odpovedi $\lambda(t)$ pada (zgodnje obdobje, uvajanje sistema v uporabo),
2. $\beta = 1$ – trenutna pogostost odpovedi $\lambda(t)$ je konstantna (obdobje normalnega delovanja sistema),
3. $\beta > 1$ – trenutna pogostost odpovedi $\lambda(t)$ raste (izraba, staranje).

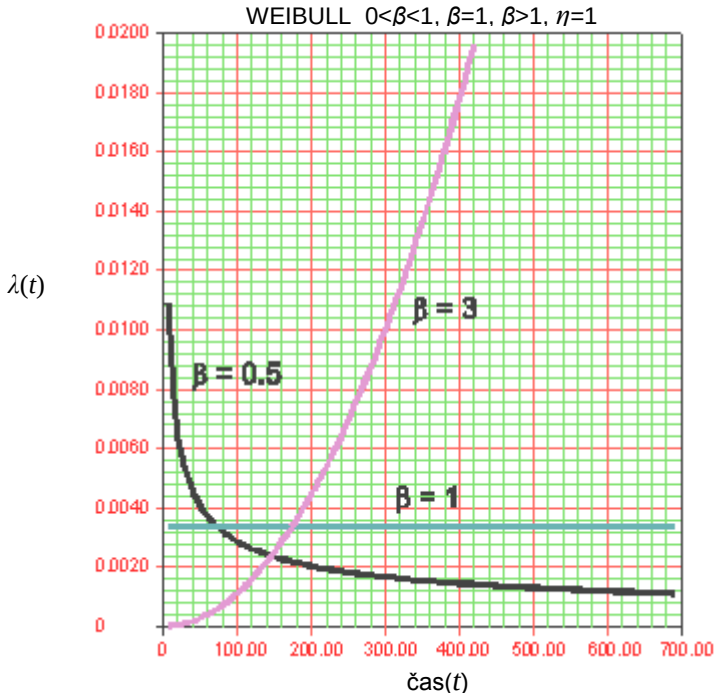
Parameter β pri zanesljivosti človeka pomeni:

a. $\beta < 1$ – človek se uči nekega opravila, zato povzroči veliko napak, katerih število s časom upada;
b. $\beta > 1$ – človek je utrujen, število napak pri delu s časom narašča.

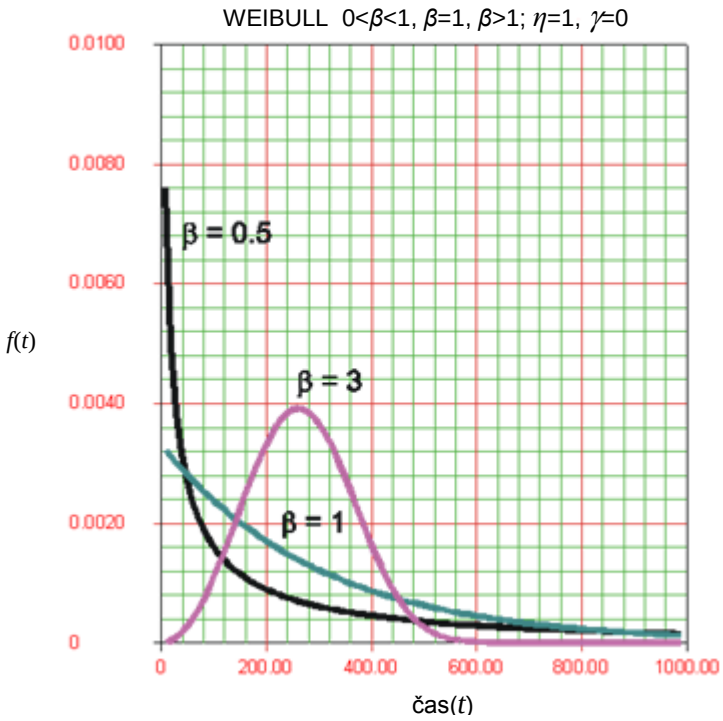
Weibullova analiza verjetnostne porazdelitve vključuje številne specifične vrednosti za β. Za vrednost β=1 je oblika porazdelitvene funkcije eksponentna, za β=2 oblika posnema Rayleigh distribucijo, za β=2,5 opisuje log–normal krivuljo, za β=3,6 je distribucija normalna in pri β = 5 normalna distribucija doseže svojo zgornjo mejo.

Poglejmo si časovni potek funkcij $\lambda(t)$ (slika 7.9), $f(t)$ (slika 7.10), $R(t)$ (slika 7.11) in $F(t)$ (slika 7.12) za Weibullov porazdelitveni zakon pri različnih vrednostih

parametrov. S slike 7.9 je razvidno, da s krivuljami lahko sestavimo krivuljo v obliki kopalne kadi. To je tudi dobrota Weibullove metode, saj z različnimi vrednostmi parametra β lahko popišemo vsa tri obdobja življenja istovrstnih gradnikov ali sistemov.

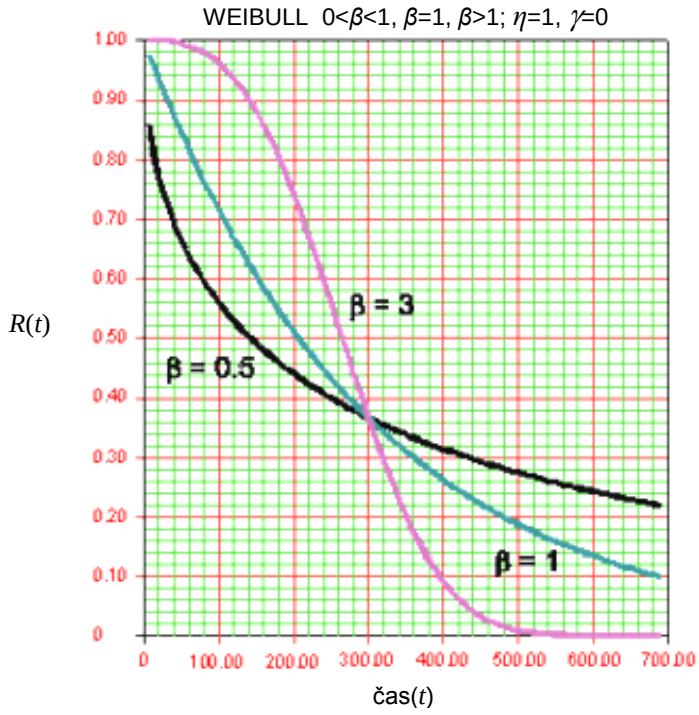


Slika 7.9: Graf funkcije $\lambda(t)$ za tipične vrednosti parametra β (Weibull, 2006)

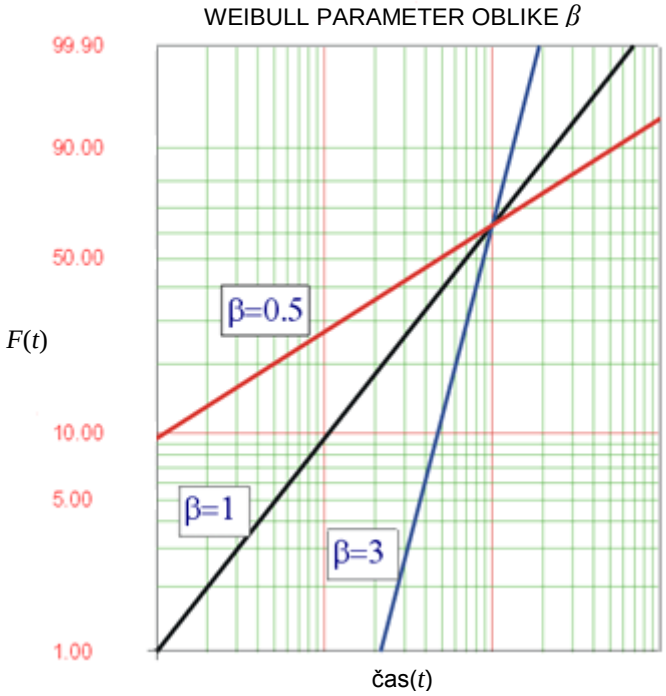


Slika 7.10: Graf porazdelitve $f(t)$ za različne vrednosti parametra β (Weibull, 2006)

Krivulja zanesljivosti $R(t)=1-F(t)$ za $0<\beta<1$ je padajoča (slika 7.11). Za $\beta=1$ je krivulja $R(t)$ eksponentna funkcija. Za $\beta>1$ krivulja $R(t)$ pada in ima prevoj pri določeni vrednosti t. V presečiščni točki krivulja $R(t)$ preide iz konveksne v konkavno obliko.



Slika 7.11: Graf porazdelitve $R(t)$ v odvisnosti od parametra β (Weibull, 2006)

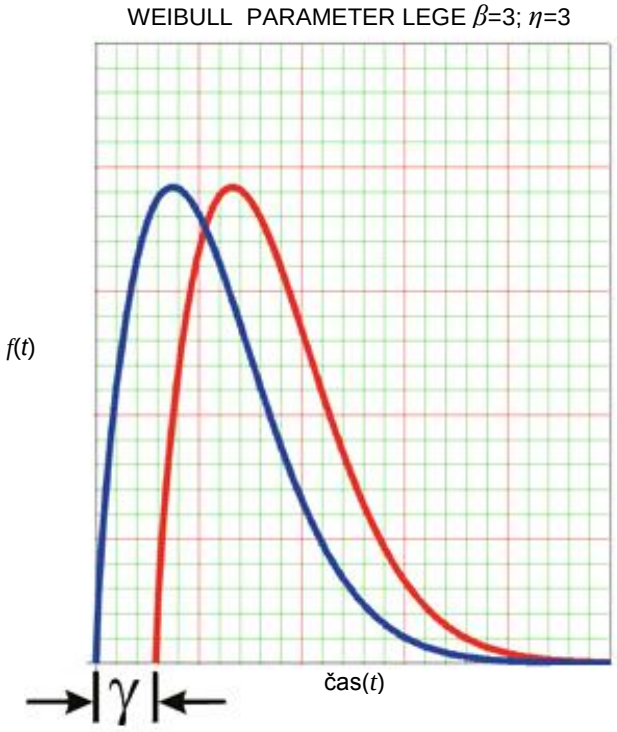


Slika 7.12: Graf funkcije $F(t)$ za različne vrednosti parametra oblike β na Weibullvem verjetnostnem papirju (Weibull, 2006)

7.6.1.3 Parameter γ (location parameter)

γ – najkrajša življenjska doba (minimum life), je parameter lege (slika 7.13).

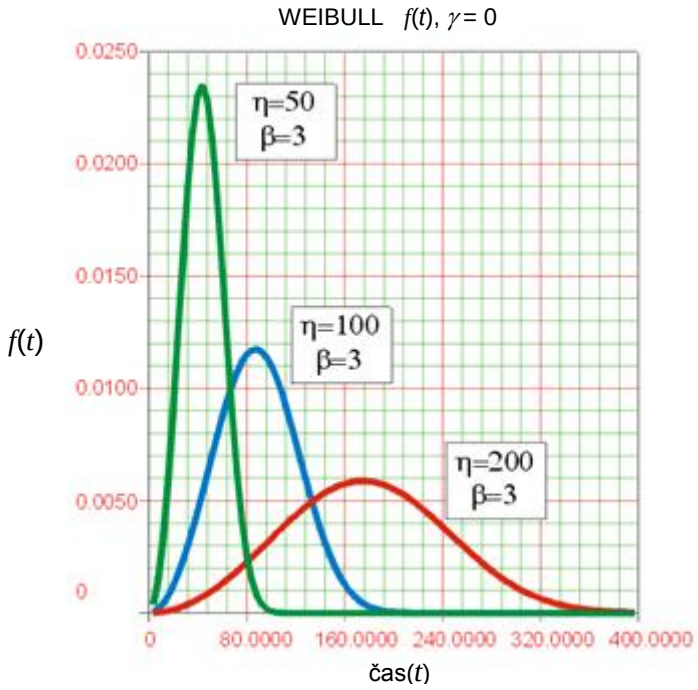
1. $\gamma > 0$ pomeni, da se začno odpovedi pojavljati šele po določenem času uporabe izdelka,
2. $\gamma < 0$ pomeni, da se začno odpovedi pojavljati že v času skladiščenja izdelka,
3. običajno postavimo $\gamma = 0$ in s tem predpostavimo, da se odpovedi začno pojavljati v trenutku, ko začnemo izdelek uporabljati.



Slika 7.13: Graf funkcije $f(t)$ glede na parameter γ (Weibull, 2006)

7.6.1.4 Parameter η (scale parameter)

Weibullov umeritveni parameter (karakteristična življenska doba) η (angleško scale parameter) nastopa kot merjena veličina npr.: ura, milja, sila, cikel itd. Sprememba parametra η ima na distribucijo enak učinek kot sprememba merila abscise. Če se η poveča, medtem ko se β in γ ohranijo enaki, se krivulja raztegne na desno in zmanjša višina, hkrati pa krivulja ohranja obliko in lokacijo. Če se η zmanjša, medtem ko se β in γ ohranita enaki, se krivulja raztegne proti levi njena višina pa se povečuje (slika 7.14).



Slika 7.14: Graf funkcije $f(t)$ glede na parameter η (Weibull, 2006)

7.6.2 INDUKTIVNA METODA IZRAČUNA ZANESLJIVOSTI SISTEMA BREZ UPOŠTEVANJA POPRAVIL

Karakteristike zanesljivosti sistemov lahko izračunamo, če poznamo karakteristike zanesljivosti in način vezave njihovih sestavnih delov (gradnikov). Vezava je z vidika zanesljivosti serijska, če odpoved posameznega sestavnega dela povzroči odpoved celotnega sistema. Čim več zaporedno vezanih sestavnih delov vsebuje sistem, tem bolj je nezanesljiv. Če je sistem sestavljen iz velikega števila gradnikov, je zanesljivost njegovega delovanja lahko zelo majhna, kljub temu, da je zanesljivost posameznih gradnikov velika (Hoyland in Rausand, 1994).

Vezava je s stališča zanesljivosti paralelna, če več gradnikov sistema opravlja isto funkcijo. Sistem odpove, kadar odpovedo vsi ekvivalentni gradniki (popolna paralelna vezava) ali pa le nekateri od njih (delna paralelna vezava). Pri paralelni vezavi razlikujemo še aktivno in pasivno (čakalno). V prvem primeru sočasno delujejo vsi ekvivalentni gradniki, v drugem pa deluje ves čas le neko število gradnikov, preostali pa se vključujejo šele, ko prvi odpovedo. Zanesljivost paralelne vezave gradnikov je večja od zanesljivosti enega samega gradnika, zato uporabljamo tako vezavo takrat, kadar želimo povečati zanesljivost sistema. Pasivna paralelna vezava je teoretično bolj zanesljiva kot aktivna paralelna. Nezanesljivost mehanizma zaznavanja odpovedi in mehanizma vključevanja čakajočih gradnikov v sistem ter možnost odpovedi gradnikov v času čakanja pa lahko močno zmanjšajo prednosti pasivne paralelne vezave pred aktivno.

Serijska ali paralelna vezava z vidika zanesljivosti pa ne pomeni vedno, da so gradniki tudi dejansko (fizično) vezani v seriji ali vzporedno. Če obravnavamo kot sestavni del sistema gradnik, ki vsebuje več komponent, računamo zanesljivost gradnika iz zanesljivosti komponent na enak način kot zanesljivost sistema računamo iz zanesljivosti gradnikov.

7.6.2.1 Serijska vezava gradnikov

Če imamo n neodvisnih gradnikov, ki so s stališča zanesljivosti vezani serijsko, na osnovi pravil verjetnostnega računa funkcijo zanesljivosti sistema $R_S(t)$ izračunamo po enačbi (Hoyland in Rausand, 1994):

$$R_S(t) = R_1(t)R_2(t)...R_n(t) = \prod_{i=1}^{n} R_i(t)\,, \tag{22}$$

pri čemer $R_i(t)$ pomeni funkcijo zanesljivosti i–te enote, ki je $R_i(t)=\exp(-\lambda_i\, t)$. Če v enačbi (22) izrazimo funkcijo zanesljivosti sistema s trenutno pogostostjo odpovedi $\lambda(t)dt$, lahko zapišemo:

$$\begin{aligned} R_S(t) &= \exp\left\{-\int_0^t \lambda_S(t)dt\right\} \\ &= \exp\left\{-\int_0^t \lambda_1(t)dt\right\}\exp\left\{-\int_0^t \lambda_2(t)dt\right\}\cdots\exp\left\{-\int_0^t \lambda_n(t)dt\right\}. \end{aligned} \tag{23}$$

Trenutno pogostost odpovedi sistema lahko zapišemo:

$$\lambda_S(t) = \lambda_1(t) + \lambda_2(t) + ... + \lambda_n(t) = \sum_{i=1}^{n} \lambda_i(t)\,, \tag{24}$$

Funkcija nezanesljivosti, ki je komplementarna funkciji zanesljivosti, je potem enaka:

$$F_S(t) = 1 - \exp\left\{-\int_0^t \lambda_S(t)dt\right\}. \tag{25}$$

Povprečen čas do odpovedi sistema $MTTF_S$ izračunamo po enačbi:

$$MTTF_S = \int_0^{\infty} R_S(t)dt\,. \tag{26}$$

V primeru, da je pogostost odpovedi posameznih enot konstantna $\lambda_i(t)=\lambda_i$, se izraza za $R_S(t)$ in $F_S(t)$ zreducirata na obliko:

$$R_S(t) = \exp(-\lambda_S\ t) \tag{27}$$

$$F_S(t) = 1-\exp(-\lambda_S\ t)\,, \tag{28}$$

pri čemer je λ_S konstantna pogostost odpovedi sistema in jo določimo kot vsoto:

$$\lambda_S = \lambda_1 + \lambda_2 + ... + \lambda_n = \sum_{i=1}^{n} \lambda_i\,. \tag{29}$$

Povprečni čas do odpovedi sistema je v tem primeru enak:

$$MTTF_S = \frac{1}{\lambda_S} = \frac{1}{\sum_{i=1}^{n} \lambda_i}. \tag{30}$$

7.6.2.2 Aktivna paralelna vezava gradnikov

Če je sistem sestavljen iz *n* neodvisnih gradnikov, ki so s stališča zanesljivosti vezane aktivno paralelno, funkcijo nezanesljivosti sistema izračunamo po enačbi (Hoyland in Rausand, 1994):

$$F_S(t) = F_1(t)F_2(t)...F_n(t) = \prod_{i=1}^{n} F_i(t)\,, \tag{31}$$

pri čemer funkcija $F_i(t)$ pomeni nezanesljivost *i*-tega gradnika.
Funkcija zanesljivosti sistema je enaka:

$$R_S(t) = 1-\left[1-R_1(t)\right]\ \left[1-R_2(t)\right]...\left[1-R_n(t)\right]. \tag{32}$$

Povprečni čas do odpovedi sistema izračunamo po enačbi:

$$MTTF_S = \int_0^{\infty} R_S(t)dt\,. \tag{33}$$

V primeru konstantne pogostosti odpovedi λ_i posameznih gradnikov lahko zapišemo $R_S(t)$ sistema v naslednji obliki:

$$R_S(t) = 1-\left(1-\exp\left(-\lambda_1 t\right)\right)\left(1-\exp\left(-\lambda_2 t\right)\right)...\left(1-\exp\left(-\lambda_n t\right)\right)\cdot \tag{34}$$

Trenutna pogostost odpovedi sistema, ki vsebuje paralelno vezane gradnike s konstantno pogostostjo odpovedi, ni več časovna konstanta. Za poljuben t jo izračunamo s splošno enačbo:

$$\lambda_S(t) = \frac{f(t)}{R_S(t)}. \tag{35}$$

Povprečni čas do odpovedi sistema je podan z enačbo:

$$MTTF_S = \left[\frac{1}{\lambda_1} + \frac{1}{\lambda_2} + ... + \frac{1}{\lambda_n}\right] - \left[\frac{1}{\lambda_1+\lambda_2} + \frac{1}{\lambda_1+\lambda_3} + ... + \frac{1}{\lambda_i+\lambda_j}\right] + \left[\frac{1}{\lambda_1+\lambda_2+\lambda_3} + \frac{1}{\lambda_1+\lambda_2+\lambda_4} + \frac{1}{\lambda_i+\lambda_j+\lambda_k}\right] - .... + (-1)^{n+1}\frac{1}{\sum_{i=1}^{n}\lambda_i}. \tag{36}$$

Če so vsi gradniki identični s pogostostjo odpovedi $\lambda_i(t) = \lambda$ za i =1,2,...,n se zgornji izraz poenostavi v:

$$MTTF_S = \frac{1}{\lambda}\sum_{i=1}^{n}\frac{1}{i}. \tag{37}$$

Funkcijo zanesljivosti sistema lahko v primeru identičnih gradnikov tako pri popolni kot pri delni paralelni vezavi, izračunamo tudi po binomski formuli. Če npr. sistem deluje, dokler deluje r izmed n identičnih gradnikov s pogostostjo odpovedi λ, določimo $R_S(t)$ kot vsoto verjetnosti za realizacijo tistih kombinacij i izmed n delujočih gradnikov, kjer je i=r, r+1, r+2,...,n po formuli (Hudoklin in Rozman, 2004):

$$R_S(t) = \sum_{i=r}^{n}\binom{n}{i}\exp(-i\lambda t)\left[1-\exp(\lambda t)\right]^{n-i}. \tag{38}$$

7.6.3 INDUKTIVNA METODA IZRAČUNA ZANESLJIVOSTI IN RAZPOLOŽLJIVOSTI SISTEMA Z UPOŠTEVANJEM TAKOJŠNJIH POPRAVIL – MARKOVSKI MODELI

Induktivne metode računanja zanesljivosti, ki smo jih obravnavali v prejšnjem poglavju, odpovedo, kadar moramo upoštevati popravila sistema. Prav tako niso primerne pri izračunu zanesljivosti sistemov, pri katerih so odpovedi gradnikov med seboj odvisne, in sistemov z gradniki v pasivni paralelni vezavi. V vseh navedenih primerih si lahko pomagamo z modeli stohastičnih procesov, natančneje z markovskimi modeli (Hoyland in Rausand, 1994). Ti modeli so primerni za izračunavanje zanesljivosti sistemov, kadar so pogostosti odpovedi komponent in

pogostosti zaključkov njihovih popravil konstantne. Standard IEC 61165 opisuje metodologijo Markovskega modeliranja strategije vzdrževanja in definira tudi grafični način izvedbe modela.

Stohastični (naključni) procesi so družine naključnih spremenljivk. Karakteristike, ki označujejo zanesljivost sistema, npr. čas do prve odpovedi, čas med zaporednima odpovedma, število odpovedi v nekem časovnem intervalu, so naključne spremenljivke. Zato lahko vedenje sistema v času obravnavamo kot stohastični proces. Tak proces opišemo, če opredelimo vsa možna stanja, v katerih se sistem lahko nahaja, ter določimo verjetnosti za zasedbo teh stanj v poljubnem času. Verjetnosti za zasedbo stanj v času ($t+\Delta t$) lahko določimo, če poznamo verjetnosti za zasedbo stanj v času t in verjetnost prehoda iz enega stanja v drugo v majhnem časovnem intervalu ($t,t+\Delta t$). Prehodne verjetnosti so po svoji naravi pogojne verjetnosti, ker so odvisne od tega, v katerih stanjih je bil sistem pred časom ($t+\Delta t$). Kadar je pogojna verjetnost prehoda iz enega stanja v drugo odvisna le od tega, v katerem stanju se je nahajal sistem v trenutku t neposredno pred prehodom, ne pa od tega, v katerih stanjih je bil v prejšnjih obdobjih, imenujemo tak stohastični proces markovski proces. Drugače povedano, markovski proces nima spomina; za napoved vedenja sistema v prihodnosti je torej treba poznati sedanjost, ne pa tudi preteklosti.

Za izračunavanje karakteristik zanesljivosti sistema po teoriji markovskih procesov moramo najprej opredeliti stanja procesa oziroma sistema. Sistemu, ki ga sestavlja določeno število enot (podsklopov ali komponent) določimo stanja glede na to, ali posamezne enote delujejo ali so odpovedale in kako se to odraža na delovanje sistema.
Za lažje razumevanje si poglejmo sistem, ki je sestavljen npr. iz dveh enot v aktivni vzporedni vezavi. Tak sistem ima tako naslednja stanja:
1. oba gradnika delujeta, sistem deluje
2. prvi gradnik deluje, drug odpove, sistem deluje
3. prvi gradnik odpove, drug gradnik deluje, sistem deluje
4. oba gradnika odpovesta, sistem ne deluje.

Pri aktivni vzporedni vezavi dobimo za n gradnikov 2^n stanj, kar je pri realnih sistemih lahko zelo veliko. Dostikrat pa imamo v sistemu z gradniki v aktivni vzporedni vezavi vgrajeno določeno število ekvivalentnih gradnikov, ki opravljajo isto funkcijo. V takih primerih se zadovoljimo s tem, da povemo, koliko gradnikov je odpovedalo, ne specificiramo pa, kateri. S tem bistveno zmanjšamo število stanj: pri n ekvivalentnih gradnikih dobimo le $n+1$ stanj. V primeru dveh ekvivalentnih gradnikov v aktivni vzporedni vezavi imamo tri stanja:
1. oba gradnika delujeta, sistem deluje
2. eden izmed gradnikov odpove, sistem deluje
3. oba gradnika odpovesta, sistem ne deluje.

Opredelili smo tudi, v katerih stanjih sistem kot celota zadovoljivo deluje ali ne – je odpovedal. Stanja sistema torej razdelimo na delujoča in nedelujoča, pred tem pa smo morali seveda natančno definirati odpovedi sistema. Nedelujoča stanja so lahko tudi absobcijska ali ponorna, če sistem ne more več iz njih. S stališča zanesljivosti so takšna vsa nedelujoča stanja sistema.

S pomočjo teorije markovskih procesov izračunamo verjetnosti za zasedbo posameznih stanj v poljubnem času. Vsota verjetnosti za zasedbo delujočih stanj predstavlja funkcijo zanesljivosti sistema $R_s(t)$.

S $p_j(t)$ označimo verjetnost, da je v času t zasedeno stanje j sistema, s $p_{ij}(t)$ pa verjetnost prehoda iz stanja i v stanje j v kratkem časovnem intervalu Δt. Pri tem indeksa i in j tečeta od 1 do n. Predpostavimo, da se verjetnosti prehodov s krajšanjem časovnega intervala približujejo konstantnim vrednostim, zato jih lahko zapišemo v obliki (Hoyland in Rausand, 1994):

$$p_{ij}(\Delta t) = q_{ij}\Delta t, \quad j \neq i \tag{39}$$

$$p_{ii}(\Delta t) = 1 + q_{ii}\Delta t\,. \tag{40}$$

Veljata tudi relaciji:

$$\sum_j p_{ij}(\Delta t) = 1 \text{ in } \sum_j q_{ij} = 0\,. \tag{41}$$

Verjetnost, da je v času $(t+\Delta t)$ zasedeno stanje j, izračunamo iz naslednjega sistema diferenčnih enačb:

$$p_j(t+\Delta t) = p_j(t)(1+q_{jj}\Delta t) + \sum_{k\neq j} p_k q_{kj}\Delta t\,. \tag{42}$$

Posebej moramo še navesti, katero stanje je bilo zasedeno na začetku opazovanja ($t=0$). Iz zgornjega sistema diferenčnih enačb s preureditvijo in limitiranjem, ko gre Δt proti 0, dobimo sistem diferencialnih enačb za $p_j(t)$:

$$p_j'(t) = \sum_k p_k(t) q_{kj}\ ; \tag{43}$$

Upoštevati moramo še začetni pogoj. Če je na začetku opazovanja sistem v stanju, ko vse njegove enote delujejo, in če to stanje označimo z 1, se začetni pogoj glasi:

$$p_1(0) = 1,\ p_j(0) = 0,\ j \neq 1\,. \tag{44}$$

Koeficienti q_{ij} v navedenem sistemu diferencialnih enačb za $p_j(t)$ so konstante in pri obravnavanju zanesljivosti sistema pomenijo pogostost odpovedi ali pogostost zaključkov popravil posameznega gradnika sistema.

Sistem diferencialnih enačb (43) pa lahko zapišemo v matrični obliki:

$$\mathbf{p}'(t) = \mathbf{p}(t)\mathbf{Q}\,. \tag{45}$$

Vrednosti q_{ij} za konkretne primere lahko določimo s preskusi v obdobju uporabe. Najprej opredelimo prostor stanj, ki ga predstavljajo vsa stanja, v katerih se sistem lahko znajde. Prehajanje med N stanji markovskega procesa, s katerim opišemo zanesljivost in razpoložljivost sistema, lahko prikažemo tudi grafično. V verjetnostnem grafu posamezna stanja sistema narišemo kot vozlišča, prehode med stanji v kratkem časovnem intervalu Δt označimo z usmerjenimi vezmi, ob njih pa zapišemo še verjetnost prehoda. Vrednosti q_{ij}, ki so elementi matrike **Q**, razberemo iz verjetnostnega grafa tako, da pri posameznih verjetnostih prehoda izpustimo Δt in odštejemo še 1 pri verjetnostih prehoda stanja samega vase (diagonalni elementi matrike). Dobljene sisteme diferencialnih enačb prvega reda s konstantnimi koeficienti najlaže rešimo s pomočjo Laplaceovih integralskih transformacij, ki funkcijo iz časovnega prostora preslika v frekvenčni prostor kompleksne spremenljivke (Hudoklin, 2003). Sistem diferencialnih enačb pretvorimo v sistem navadnih enačb, rešitve pa z inverzno Laplaceovo transformacijo nato preslikamo nazaj v časovni prostor. Vsota verjetnosti za zasedbo delujočih stanj pa je funkcija zanesljivosti:

$$R_S(t) = \sum_{\substack{i-delujoče \\ \text{stanje}}} p_i(t)\,. \tag{46}$$

Določanje $R_S(t)$ je lahko zamudno in tudi nerešljivo, zato se v praksi za določanje zanesljivosti zadovoljimo z določitvijo ocene za $MTTF_S$. Za določitev zanesljivosti identifikacijskih sistemov uporabljenih v raziskavi bomo nastavili računski model za $MTTF_S$, kar nam zadostuje s stališča zanesljivosti.

7.6.4 BINOMSKI IN POISSONOV MODEL DOLOČANJA POGOSTOSTI ODPOVEDI PROGRAMSKE OPREME

Analitične modele določanja zanesljivosti računalniških programov razvrščamo v statične in dinamične. V raziskavi se bomo omejili na dinamične binomske in Poissonove modele, ker bomo v primeru odpovedi programa med njegovim izvajanjem vzrok napake locirali in ga odpravili. Primeri uporabe dinamičnih modelov so prikazani v tabeli 7.2.

Tabela 7.2: Primerjava Binomskega in Poissonovega modela zanesljivosti računalniškega programa (Hudoklin in Rozman, 2004)

Binomski	Poissonov
Trenutna pogostost odpovedi programa zaradi napake a, $\lambda_a(t)$, za vse napake enaka	Trenutna pogostost odpovedi programa zaradi napake a, $\lambda_a(t)$, za vse napake enaka
Predpostavlja fiksno število napak μ_0 na začetku izvajanja programa	Začetno število napak ni natančno znano; poznamo le poprečno št. napak na začetku izvajanja ω_0; število začetnih napak obravnavamo kot slučajno sprejemljivko
Ne upošteva nepopolnega odstranjevanja napak in vnašanja novih napak pri popravljanju programa	Upošteva tudi nepopolno odstranjevanje napak in vnašanje novih napak pri popravljanju programa

Odprava napak se pokaže kot diskontinuiteta pri časovnem poteku trenutne pogostosti odpovedi programa	Odprava napake zahteva določen čas, zato je trenutna pogostost odpovedi programa zvezna časovna funkcija
Število odpovedi v neskončnem času je končno	Število odpovedi v neskončnem času je končno ali neskončno

Pri obeh modelih je trenutna pogostost odpovedi $\lambda_a(t)$ enaka za vse napake a. V raziskavi bomo upoštevali napake, ki jih bomo lahko locirali in niso bile vnešene s popravljanjem, kar ustreza modelu binomskega tipa.

7.6.5 FUNKCIJA RAZPOLOŽLJIVOSTI IN RAZPOLOŽLJIVOST SISTEMA

Pri izračunu karakteristik razpoložljivosti upoštevamo tudi popravila gradnikov sistema, ker to vpliva na njegovo razpoložljivost. Nedelujoča stanja sistema niso več ponorna, zato je treba konstruirati nov verjetnostni graf in določiti novo matriko, ki jo označimo s simbolom $\mathbf{Q}_A$. Funkcija razpoložljivosti sistema $A_S(t)$ je določena kot vsota verjetnosti za zasedbo delujočih stanj (Hudoklin in Rozman, 2004):

$$A_S(t) = \sum_{\substack{i-delujoče \\ \text{stanje}}} p_i(t) \tag{47}$$

Verjetnosti za zasedbo posameznih stanj sistema $p_i(t)$ za $i=1,2,...,N$ določimo z rešitvijo sistema diferencialnih enačb, ki ga v matrični obliki zapišemo:

$$\mathbf{p}'(t)=\mathbf{p}(t)\mathbf{Q}_A \text{ pri pogoju } \mathbf{p}(0)=[0,\ldots,0,1,0,\ldots,0] \tag{48}$$

kjer uporabimo matriko $\mathbf{Q}_A$, elemente q_{ij}, za $i,j=1,2,...,N$ pa določimo iz verjetnostnega grafa za razpoložljivost podobno kot pri zanesljivosti (Hudoklin in Rozman, 2004).

Funkcija razpoložljivosti $A(t)$ je definirana kot verjetnost, da gradnik ali sistem zadovoljivo deluje. Če sistem uporabljamo dalj časa, funkcija razpoložljivosti doseže neko stacionarno razpoložljivost. Ob predpostavki, da sta trenutna pogostost odpovedi in trenutna pogostost zaključkov popravil časovni konstanti, lahko asimptotično vrednost funkcije razpoložljivosti imenujemo kar asimptotična razpoložljivost, stacionarna razpoložljivost ali kar razpoložljivost. Največjo stacionano razpololožljivost sistema bi v praksi lahko dosegli le, če bi bil čas zastoja zaradi odpovedi enak času aktivnega popravila. Ker $MTTR$ pomeni povprečni čas aktivnega popravila lahko lastno razpoložljivost izračunamo po enačbi (Hudoklin in Rozman, 2004):

$$A = \frac{MTTF}{MTTF + MTTR}. \tag{49}$$

Razpoložljivost pa lahko interpretiramo tudi kot delež časa, ko sistem deluje znotraj intervala opazovanja. Za oceno razpoložljivosti enega samega sistema lahko zapišemo:

$$A = \frac{t_d}{t_d + t_n}, \tag{50}$$

kjer pomeni:
t_d – kumulativni čas delovanja v intervalu opazovanja,
t_n – kumulativni čas nedelovanja zaradi popravil v intervalu opazovanja.
Če za t_n vstavimo čas aktivnega popravila, dobimo izraz za lastno razpoložljivost, če pa je t_n celotni čas zastoja, izračunamo obratovalno razpoložljivost. Izraz velja, če je t_n izračunan za sistem, ki ga vzdržujemo samo korektivno ali pa tudi preventivno (Hudoklin in Rozman, 2004).

7.7 STOHASTIČNI PROCESI

Stohastični proces je proces, v katerem sta dinamika oz. del dinamike pogojena z zakonom verjetnostni (Hudoklin, 1986).
Stohastični proces opredelimo na podlagi treh zakonitosti:
1. prostor stanj; če je množica stanj končna, pomeni, da so stanja diskretna (stohastične verige), sicer pa so stanja na intervalih na zvezni osi (proces z zveznimi stanji),
2. indeksni parameter (uporaba zveznega časa - proces v zveznem času, uporaba diskretnega časa - stohastično zaporedje),
3. statistična odvisnost (vsaj del dinamike mora biti verjetnostno pogojen).

V raziskavi bomo predstavili matematični model stohastičnega procesa, ki bo dobra aproksimacija za realni proces identifikacije. Ta model nam bo v nadaljnih raziskavah osnova za izračun stanj strežnih mest pristopne kontrole in dejansko primerjavo strežbe v praktičnem primeru kartične in biometrične pristopne kontrole. Meritve časa strežbe za oba primera identifikacije so v praksi dolgotrajne in presegajo okvire te raziskave, zato se bomo za ta namen omejili na matematični model ter pripadajoče formulacije. Modeliranje in preračunavanje nam pokaže ekonomsko upravičenost izvedenih optimizacij pristopne kontrole ter predvideva učinkovit ter racionalen sistem vzdrževanja identifikacijskega sistema.

7.7.1 MARKOVSKE[25] VERIGE

Markovske verige so markovski procesi z diskretnimi stanji v diskretnem času (Hudoklin, 2003). Število stanj je lahko končno ali številno neskončno. Opraviti imamo s stohastično naravo sistema, z diskretnim časom in brez pomnjenja ob prehajanju iz stanja v stanje. Verjetnosti prehoda so lahko odvisne od časa ali neodvisne od časa. Če so vse verjetnosti prehoda stacionarne, govorimo o homogeni markovski verigi.

[25] *Markov (1856–1922), ruski matematik, ki se je ukvarjal s stohastičnimi (randomiziranimi) procesi.*

Lastnosti diskretnih časovnih markovskih verig:

1. Stacionarnost: obstajajo limitne vrednosti verjetnosti za zasedbo stanj, ki niso odvisne od začetne verjetnostne porazdelitve za zasedbo stanj.
2. Reducibilnost: veriga je nereducibilna, če je vsako stanje dosegljivo iz vseh drugih stanj v končnem št. korakov, in reducibilna, če vsebuje več kot eno izolirano podmnožico stanj.
3. Periodičnost: sistem markovskih verig je periodičen s periodo t, če se po $t \cdot n$ korakih vrača v isto stanje verige.
4. Povrnljivost (rekurenčnost): povrnljivo stanje j je tisto, pri katerem je verjetnost nahajanja v stanju j pri zelo velikem številu korakov večja od 0:

$$\lim_{k\to\infty} \pi_j^{(k)} > 0 \,. \tag{51}$$

Markovska veriga je definirana z množico diskretnih slučajnih spremenljivk $\{X_n\}$; $n = 0,1,2 \ldots$ Če poznamo vrednost X_m v poljubnem trenutku m, je v nekem poznejšem trenutku $m+n$ verjetnostna porazdelitev X_{m+n} popolnoma določena. Poznavanje vrednosti v časih, manjših od m, ni potrebna in zapišemo lahko (Hudoklin, 2003):

$$P(X_{m+n} = j \mid X_m = i,\ X_{m-1} = h,\ X_{m-2} = g, \ldots) = P(X_{m+n} = j \mid X_m = i) \tag{52}$$

Markovske verige s končnim številom stanj imenujemo končne, s številno neskončnim številom stanj pa neskončne markovske verige. Markovska veriga je časovno homogena, ali kratko homogena, če je pogojna verjetnost odvisna le od širine časovnega intervala n, ne pa od časa opazovanja m.

Velja:

$$P(X_{m+n} = j \mid X_m = i) = P(X_n = j \mid X_0 = i);\ m = 1, 2, \ldots;\ n = 1, 2, \ldots \tag{53}$$

Pogojno verjetnost, da je bilo na začetku opazovanja zasedeno stanje i, v času n pa stanje j, imenujemo verjetnost prehoda iz stanja i v stanje j v času n (v n korakih). Označimo jo s simbolom :

$$p_{ij}^{(n)} = P(X_{m+n} = j \mid X_m = i) \tag{54}$$

Verjetnost prehoda v enem koraku $p_{ij}^{(1)}$ označim s p_{ij} .

Pri končni markovski verigi s prostorom stanj $S = \{0, 1, 2, \ldots, N\}$ je $(N+1)^2$ verjetnosti prehodov iz enega stanja verige v drugo. Vrednosti zapišemo s prehodno matriko **P**:

$$\mathbf{P} = \{p_{ij}\} = \begin{bmatrix} p_{00} & p_{01} & . & p_{0N} \\ p_{10} & p_{11} & . & p_{1N} \\ . & . & . & . \\ p_{N0} & p_{N1} & . & p_{NN} \end{bmatrix}. \quad (55)$$

Začetna stanja v t se spreminjajo po vrsticah, končna v $t+\Delta t$ pa po stolpcih. Vsaka prehodna matrika je stohastična matrika z naslednjimi lastnostmi:
a) elementi matrike so nenegativni,
b) vsota členov v posamezni vrstici matrike je enaka 1 in
c) matrika je kvadratna.

Za izračun verjetnosti, da bodo zasedena posamezna stanja homogene markovske verige v poljubnem času, moramo poleg prehodne matrike poznati še verjetnostno porazdelitev za zasedbo stanj na začetku opazovanja. Začetno verjetnostno porazdelitev zapišemo z vrstičnim vektorjem:

$$\mathbf{p}^{(0)} = [p_0{}^{(0)}, p_1{}^{(0)}, p_2{}^{(0)}, \ldots] \quad (56)$$

katerega komponente predstavljajo verjetnosti, da je na začetku opazovanja (t=0) zasedeno stanje i:

$$P(X_0 = i) = p_i(0)\,;\; i = 0, 1, 2, \ldots \quad (57)$$

Verjetnosti za zasedbo posameznih stanj sistema v času t = 1 z dano prehodno matriko $\mathbf{P}$ in začetno verjetnostno porazdelitvijo $\mathbf{p}^{(0)}$ izračunamo tako, da upoštevamo vsa možna stanja pred prehodom v novo stanje in vse verjetnosti prehoda iz kateregakoli stanja v novo stanje

$$p_{ij}{}^{(n)} = P(X_i = j) = \sum_{i=0}^{\infty} p_i^{(1)} p_{ij}. \quad (58)$$

Veriga je v času n v stanju j, če je bila že v času n-1 v stanju j in v naslednjem koraku ni prišlo do spremembe stanja ali pa je bila v času n-1 v nekem drugem stanju i in se je v naslednjem koraku zgodil prehod iz i v j:

$$p_j{}^{(n)} = \sum_{i=0}^{\infty} p_i^{(n-1)} p_{ij}; n = 1, 2, \ldots \quad (59)$$

Vrsta na desni strani izraza konvergira, ker tvori množica verjetnostno porazdelitev in je tako vsota vseh elementov enaka 1, elementi prehodne matrike pa so nenegativni in omejeni z vrednostjo 1 za vse i, j.

Enačbo lahko zapišemo v matrični obliki:

$$\mathbf{p}^{(n)} = \mathbf{p}^{(n-1)} \mathbf{P}. \quad (60)$$

Verjetnost za zasedbo stanj procesa v času lahko torej določimo, če poznamo začetno verjetnostno porazdelitev za zasedbo stanj in prehodno matriko.

7.7.1.1 Klasifikacija stanj markovske verige

S klasifikacijo stanj v markovski verigi lahko stanja razdelimo na različne tipe. Verjetnost, da se veriga, ki je bila na začetku v stanju i prvič povrne v to stanje v času n (po n korakih), v časih $1,2,...,n\text{-}1$ pa se stanju i izogiba, naj bo enaka f_{ii}. Verjetnost, da se veriga sploh kdaj povrne v stanje i, je enaka .

$$f_i = \sum_{n=1}^{\infty} f_{ii}^{(n)}. \tag{61}$$

Povprečni čas prve vrnitve v stanje i je

$$\mu_i = \sum_{n=1}^{\infty} n f_{ii}^{(n)}. \tag{62}$$

Stanje je povratno, če je verjetnost, da se veriga kdaj povrne v to stanje, enaka 1. Če je povprečni čas vrnitve v stanje i končen $\mu_i<\propto$, je stanje pozitivno povratno. Kadar je povprečni čas vrnitve v stanje i neskončen, imenujemo stanje ničelno. Stanje i je minljivo, če je verjetnost, da se veriga kdaj povrne v to stanje, manjša od 1. Stanje, ki ni minljivo, je povrnljivo stanje. Stanje j je dosegljivo iz stanja , kadar je možen prehod iz stanja v stanje v koncnem številu korakov. Stanji i in j sta povezani, če je stanje j dosegljivo iz stanja i in stanje i dosegljivo iz stanja j. Stanja, ki se v prvem koraku povrnejo sama vase z verjetnostjo 1, imenujemo ponorna ali absorbirajoča stanja. Vsa taka stanja so pozitivno povratna. Povratno stanje je periodično, če se veriga vrača vanj le v časih, ki so mnogokratniki nekega celega števila, večjega od 1, imenovanega perioda. Če je perioda enaka 1, je stanje neperiodično. Pozitivno povratno neperiodično stanje imenujemo ergodijsko stanje. Markovsko verigo, v kateri so vsa stanja povrnljiva, neperiodična in dosegljiva iz kateregakoli stanja, imenujemo ergodijska veriga.

7.7.1.2 Ravnovesne porazdelitve

V nekaterih primerih se verjetnostna porazdelitev za zasedbo stanj po daljšem času ustali pri neki limitni porazdelitvi, verjetnosti za zasedbo posameznih stanj pa postanejo neodvisne od začetnih pogojev. Tako verjetnostno porazdelitev za zasedbo stanj imenujemo ravnovesna porazdelitev. Če je prehodna matrika ergodijske markovske verige s stanji, potem obstaja taka ravnotežna porazdelitev, da velja:

$$\lim_{n\to\infty} \mathbf{P}^n = \begin{bmatrix} \pi_1 & \pi_2 & . & \pi_s \\ \pi_1 & \pi_2 & . & \pi_s \\ . & . & . & . \\ \pi_1 & \pi_2 & . & \pi_s \end{bmatrix}. \quad (63)$$

ij–ti element matrike $\mathbf{P}^n$ je enak verjetnosti prehoda iz stanja *i* v stanje *j* v *n* korakih $p_{ij}^{(n)}$. Za ravnotežno porazdelitev velja, da je ena sama in da k njej konvergira vrsta neodvisno od začetne verjetnostne porazdelitve:

$$\lim_{n\to\infty} p_{ij}^{(n)} = \pi_j . \quad (64)$$

Po določenem času (številu prehodov v različna stanja) se nahajamo v stanju *j* z verjetnostjo π_j. Ergodijska markovska veriga se torej po nekem času stabilizira. V ravnotežnem stanju velja, da je verjetnost izhoda iz določenega stanja enaka verjetnosti vstopa v to stanje:

$$\pi_j (1 - p_{jj}) = \sum_{k\neq j} \pi_k p_{kj} . \quad (65)$$

$$\pi_j = \sum_{k=1}^{k=s} \pi_k p_{kj} . \quad (66)$$

Označimo z μ_i povprečni čas prvega prehoda iz stanja *i* v stanje *j*. Za ergodijske markovske verige velja :

$$\mu_i = 1 + \sum_{k\neq j} \pi_{ik} q_{kj} . \quad (67)$$

Povprečni čas povrnitve v stanje *i* je enak μ_{ii} in za ravnotežno porazdelitev velja:

$$\pi_j = \frac{1}{\mu_{jj}}; j = 1,2,..s. \quad (68)$$

Mnogo zanimivih primerov uporabe markovskih verig vključuje verige, ki poleg minljivih stanj vsebujejo tudi nekaj absorbirajočih stanj. Takim verigam pravimo absorbirajoče verige, pri katerih nas zanima:

- kolikšen je povprečni čas bivanja v posameznih minljivih stanjih?
- kolikšna je verjetnost, da bo veriga prišla v posamezno absorbirajoče stanje?

Da bi lahko odgovorili na vprašanji, je potrebno prehodno matriko zapisati v obliki:

$$\mathbf{P} = \begin{bmatrix} \mathbf{Q} & \mathbf{R} \\ \mathbf{0} & \mathbf{I} \end{bmatrix}, \quad (69)$$

pri čemer matrika **Q** predstavlja prehode med minljivimi stanji, matrika **R** prehode iz minljivih v absorbirajoče stanje in matrika **I** (enotska matrika) absorbirajoča stanja. Matrika **0** (sestavljena iz samih ničel) izkazuje dejstvo, da je nemogoč prehod iz absorbirajočega stanja v minljivo (Winston, 1991). Povprečne čase bivanja v posameznih minljivih stanjih izračunamo s fundamentalno matriko, katere elementi f_{ij} so kar povprečni časi bivanja v minljivem stanju j, če je bila veriga na začetku v stanju i:

$$F = [\, f_{ij} \,] = (\mathbf{I}-\mathbf{Q})^{-1}. \tag{70}$$

Vsota elementov (f_{ij}), sešteta po minljivih stanjih j, predstavlja skupni povprečni čas bivanja v minljivem stanju j. Verjetnost za zasedbo posameznih absorbirajočih stanj nam povejo elementi matrike:

$$[\mathbf{Q}]^{-1} = (\mathbf{I}-\mathbf{Q})^{-1}, \tag{71}$$

kjer ij–ti element pove verjetnost absorbcije v absorbirajoče stanje j.

Poprečni čas do odpovedi $MTTF$ je poprečni čas do absorpcije iz začetnega stanja in ga določimo kot vsoto elementov prve vrstice inverzne matrike $[\mathbf{Q}]^{-1}$.

V poglavju 7.7.1 navedena teorija markovskih verig nam bo kasneje v raziskavi služila kot orodje za preračunavanje zanesljivosti in razpoložljivosti identifikacijskih sistemov ter določanja vzdrževalnih pogojev. V okviru stohastičnih procesov bomo nadalje v poglavju 7.7.2 na kratko obravnavali še druga področja, vezana na optimiranje identifikacijskih sistemov. Tematika sicer presega okvire te doktorske disertacije, vendar bo v nadaljnih aplikativnih raziskavah identifikacijskih sistemov nujno prisotna za dosego optimalnega strežnega mesta. S tem bi v praksi omogočili časovno optimalen prehod strank skozi identifikacijski sistem, stroške in minimalno bivanje stranke v prostoru za čakanje (sistemu identifikacije).

7.7.2 MNOŽIČNA STREŽBA

Običajno povzroča kopičenje strank v vrsti omejeno število strežnih mest. V nekaterih primerih pa obstajajo tudi časovne omejitve: Strežba je dosegljiva le v določenih časovnih intervalih (Hudoklin, 2003). Z analizo sistemov množične strežbe dobimo podatke, ki omogočajo uvajanje izboljšav v obstoječe sisteme (zaposlimo lahko več ali manj strežnikov, povečamo število strežnih mest, avtomatiziramo strežbo ipd.), medsebojno primerjavo različnih sistemov ter projektiranje novih sistemov strežbe.

Množično strežbo sestavljajo (Hudoklin, 2003):
- eno ali več strežnih mest,
- proces prihajanja strank in
- proces strežbe.

Enostavni sistemi strežbe določajo naslednje karakteristike (Hudoklin, 2003):

1. Vhodni tok strank obravnava prihode strank, kjer lahko stranke prihajajo v sistem posamič ali v skupinah. Pogostost prihodov je bodisi konstantna ali se s časom spreminja. Prihodi so lahko razporejeni različno:
   - neprava porazdelitev (enakomerni intervali, D),
   - eksponentna porazdelitev (prihodi tvorijo Poissonov proces, M),
   - splošna porazdelitev (G).

V literaturi so najpogosteje obravnavani sistemi množične strežbe kjer stranke prihajajo posamič, časi med dvema zaporednima prihodoma pa so med seboj neodvisni in enako porazdeljeni. Osnovni model porazdelitve teh časov so naslednji:
   - neprava porazdelitev (stranke prihajajo v nepravih presledkih),
   - eksponentna porazdelitev (zaporedni prihodi strank tvorijo Poissonov proces),
   - splošna porazdelitev.

2. Mehanizem strežbe opredeljujejo zmogljivost in razpoložljivost sistema ter porazdelitev časov strežbe. Zmogljivost določa število strežnih mest, razpoložljivost je ponavadi polna, porazdelitev pa je lahko konstantna (avtomatizirana strežba), eksponentna ali Erlangova.
3. Disciplina strežbe je pravilo po katerm določamo vrstni red strežbe. Lahko je FIFO, LIFO, naključna izbira ali prednostna izbira.

Modele sistemov množične strežbe, v katere prihajajo stranke posamič, označujemo z zapisom oblike: vhodna porazdelitev/porazdelitev časov strežbe/ število strežnih mest, ki mu dodamo tekstualni opis ostalih pomembnih lastnosti.

Nadalje bomo obravnavali lastnosti strežnih mrež in sistemov ter njihove numerične značilnosti.

7.7.2.1 Strežna mreža

Poljubno vezavo poljubnega števila strežnih enot definirata μ in λ, pri čemer je:
μ– intenzivnost strežbe [št. zahtev/sek.] in
λ– intenzivnost prihajanja zahtev [št. zahtev/sek.].

Povprečen strežni čas določimo s formulo:

$$\overline{x}=\frac{1}{\mu}\,. \tag{72}$$

Uporabnostni faktor strežne mreže je:

$$\rho=\frac{\lambda}{\mu} \quad \text{pri} \quad \left[0\le\rho\le 1\right]. \tag{73}$$

Pogoj $\mu>\lambda$ ne sme biti izpolnjen, saj bi to pomenilo, da sistem ni zmožen sprocesirati potrebnih zahtev.

7.7.2.2 Strežni sistem

Kendalova notacija je standardni zapis strežnih sistemov, ki definira *A/B/m/K/M/***Q**, pri čemer velja, da je:
A– porazdelitev medprihodnih časov zahtev
B– porazdelitev strežnih časov zahtev
m– število strežnikov
K– zmogljivost sistema *K* = št. strežnikov + vsota čakalnih vrst,
M– velikost populacije zahtev: končna, neskončna
Q– čakalna disciplina.

Čakalna disciplina v sistemu strežbe je pravilo, po katerem določamo vrstni red strežbe. Najobičajnejše pravilo je: »Kdor prvi pride, je prvi postrežen (FIFO)«. V industrijskih aplikacijah pa pogosto nastopa tudi pravilo: »Kdor zadnji pride, je prvi postrežen (LIFO)«. Disciplina v sistemu je lahko tudi povsem neodvisna od prihodov strank (RND) ali pa izbira, ki upošteva določene proritete (priority). Time sharing disciplina predvideva dodeljevanje časovnih intervalov strežbe. V primeru, da je obdelava predolga se vrne nazaj na začetek vrste. Pri tem za A in B veljajo naslednje porazdelitve:
D– deterministična porazdelitev,
M– eksponentna porazdelitev,
E– Erlangova porazdelitev in
G– splošna porazdelitev.

7.7.2.3 Numerične značilnosti strežnih sistemov

Osnovni numerični atributi strežnega sistema so:
N – povprečno št. zahtev v sistemu v nekem trenutku je enako vsoti števila zahtev, ki se v danem trenutku nahajajo po vrstah strežnega sistema + število zahtev ki se nahajajo v strežnikih tega sistema.

T_k – povprečen čas bivanja k-te zahteve v sistemu je enak vsoti čakalnega časa k-te zahteve in strežnega časa k-te zahteve.

$$T_k = W_k + \overline{x_k}\,. \tag{74}$$

W_k – povprečni čas čakanja zahteve, pri čemer lahko imamo več strežb oz. več čakalnih vrst.

$\bar{x}_k$ – povprečni čas strežbe.

$P_k(t)$ – verjetnost, da je v sistemu v času t k zahtev.

Littlov teorem velja za strežne enote za katere velja, da je povprečno število zahtev v strežni enoti produkt med povprečnim časom zadrževanja zahteve v sistemu in intenzivnostjo prihajanja zahtev.

$$N = T \cdot \lambda \tag{75}$$

Povprečno št. zahtev v vrsti je:

$$N_q = W \cdot \lambda. \tag{76}$$

Povprečno število zahtev v strežnikih je:

$$N_s = \bar{x} \cdot \lambda = \frac{\lambda}{\mu} = \rho. \tag{77}$$

Zakon o ohranitvi pretoka predvideva, da mora na dolgi rok biti $A=B$, pri čemer je:
A– število prispelih zahtev in
B– število postreženih zahtev.

Enakost na dolgi rok mora biti zagotovljena, saj bi v primeru $A>B$, prišlo do eksplozije v sistemu $\rho>1$ oz. v primeru $A<B$, sistem ne bi generiral zahtev.

7.8 IDENTIFIKACIJSKI SISTEMI V PROIZVODNO-LOGISTIČNEM PROCESU

V proizvodno-logističnih procesih se pogosto pojavijo zahteve po identifikaciji nosilcev procesov operativnih aktivnosti (reklamacije, presoje procesov, izvedeni preventivno–korektivni ukrepi zaradi neskladnosti). Odgovorni nosilci teh aktivnosti so običajno ljudje, ki lahko svojo identiteto dokazujejo na različne načine (lastnoročni podpis, PIN kode, čipne kartice, biometrična identifikacija, kamere itd.). Ob tem pa se moramo v procesu omejiti na postopke zbiranja informacij, ki niso sporni s stališča človekove integritete in zaupnosti.

Zaradi nenehne optimizacije in avtomatizacije procesov se implementacija »enostavnih identifikacijskih sistemov« v proizvodno–logistične procese vedno bolj uveljavlja. Biometrija omogoča hitro in enostavno izvedbo osebne identifikacije v logističnem procesu na osnovi značilk, brez potrebnih dodatnih identifikacijskih elementov. Seveda pa je treba raziskati parametre zanesljivosti in učinkovitosti, da bi preprečili nepredvidene učinke pri uvedbi obravnavanih tehnologij.

V raziskavi smo za kartične sisteme uporabili pomnilniške in mikroprocesorske identifikatorje (čipe), ki jih lahko namestimo na konstrukcijske elemente v proizvodno–logističnem procesu. S kartičnimi identifikatorji se v vsakem delu procesa lahko identificira tudi človek.

Pomnilniški RFID identifikatorji nimajo lastnega procesorja in zato ne morejo dinamično obdelovati podatkov. Mikroprocesorski identifikatorji so v nasprotju s pomnilniškimi RFID sposobni dinamičnega obdelovanja podatkov. Mikroprocesorski identifikatorji vsebujejo procesor, vhodno–izhodno enoto ter več vrst pomnilnika. Trenutno se uporabljajo 8–, 16– in 32–bitni procesorji, ki imajo v povprečju 64 Kb ROM–a, 16 do 32 Kb EEPROM–a in 3 Kb RAM–a, vhodno-izhodna enota pa dosega prenose 9,6–115 Kbit/s (pri čemer je možen samo polovični-dupleksni način). Po računski moči so primerljivi s prvotnim računalnikom IBM–XT, s kriptosoprocesorjem pa v nekaterih opravilih prekašajo celo 50–MHz računalnik 486.

Z ustrezno zasnovo lahko večino računanja in vodenja dnevnikov prenesemo s pametne kartice v osebni računalnik, ki ima večje računske in pomnilniške zmogljivosti. Varnost podatkov zagotovimo z različnimi kriptosistemi kot so DES, 3DES, RSA itd. RSA je algoritem, ki spada v družino algoritmov za šifriranje z javnim ključem. Je prvi algoritem, v praksi primeren za podpisovanje in šifriranje, in ena prvih prednosti šifriranja z javnim ključem. RSA se na široko uporablja v protokolih, namenjenih komercialnim komunikacijam, in velja za varnega, če je le dolžina ključev dovolj velika. Za kriptosistem RSA z javnimi ključi so priporočene dolžine ključev tudi do 2000 bitov. Dodajanje komponent (npr. soprocesorja) kartice podraži, hkrati pa se utegne zmanjšati njihova zanesljivost in s tem varnost. Pri pomanjkanju pomnilnika in procesorske moči si danes že lahko pomagamo z novimi tehnologijami kriptosistemov z eliptičnimi krivuljami ECC, ki omogočajo krajše šifrirne ključe in hitrejše računanje (z obstoječim procesorjem), pri tem pa ohranijo enako stopnjo varnosti. ECC računajo število točk na krivulji in to informacijo uporabljajo za generiranje ključev, pri čemer zagotavljajo enako stopnjo zaščite kot RSA ali DSA s 1024–bitnim modulusom ob bistveno krajših ključih (lažje kodiranje in dekodiranje ob prenosu podatkov).

V nasprotju s klasičnimi postopki identifikacije moramo pri biometričnih upoštevati tudi verjetnost. Vsi senzorji, ki jih uporabljamo, so podvrženi šumom in napakam. Še večja težava pa sta razvoj in implementacija varnega kriptoalgoritma (Ratha in drugi, 2001b). Na koncu se vse omejitve stekajo k dvema pojmoma: FRR in FAR (tabela 7.3).

Tabela 7.3: *FAR*, *FRR* in *EER* karakteristike različnih biometričnih sistemov

Biometrika	Glas	Hitrost tipkanja	Očesna šarenica	Očesna šarenica ITIRT	Oblika dlani	Prstni odtis FVC	Prstni odtis FpVTE	Obraz FRTV
EER%	6	1,8	0,01	<1	1	2	ni podatka	ni podatka
FAR%	2	7	0,0001	0,94	2	2	1	1
FRR%	10	0,1	0,2	0,99	0,1	2	0,1	10
Število čitanj	310	15	132	1224	129	100	25000	37437
Opomba	odvisno od besedila večjezikovno	6-mesečno obdobje	najboljši pogoji	notranjost	s prstanom neprimerno okolje	rotacija prsta povečana obraba kože	operativni podatki ameriške vlade	spremenljiva svetloba
Vir	(NIST, 2005b)	(Hocquet in drugi , 2005)	(NIST, 2005a)	(International Biometric Group, 2005)	(Kukula in Elliott, 2006)	(Cappelli in drugi, 2006)	(Wilson in drugi, 2004)	(Philips, Grother, Micheals, Blackburn, Tabassi in Bone, 2002)

Pri občutljivosti sistema je treba narediti kompromis. Če je sistem zelo občutljiv, dobimo majhne vrednosti FAR, zato pa toliko večje FRR (npr. veliki sistemi farmacevtskih korporacij, kjer je treba zagotavljati popolno sledljivost zdravil in ljudi v procesu). Pri manj občutljivem sistemu pa je slika ravno obratna. Takšen sistem sprejme skoraj vsakogar ($FAR>FRR$). Občutljivost lahko izberemo tudi tako, da sta vrednosti FAR in FRR enaki. Tej skupni vrednosti pravimo EER. Manjša kot je vrednost EER, večja je točnost sistema. Pri aplikacijah, kjer dajemo prednost hitrosti identifikacije pred varnostjo (npr. manjši sistemi, z malo soudeleženimi v procesu), pa lahko dopustimo visoko vrednost FAR.

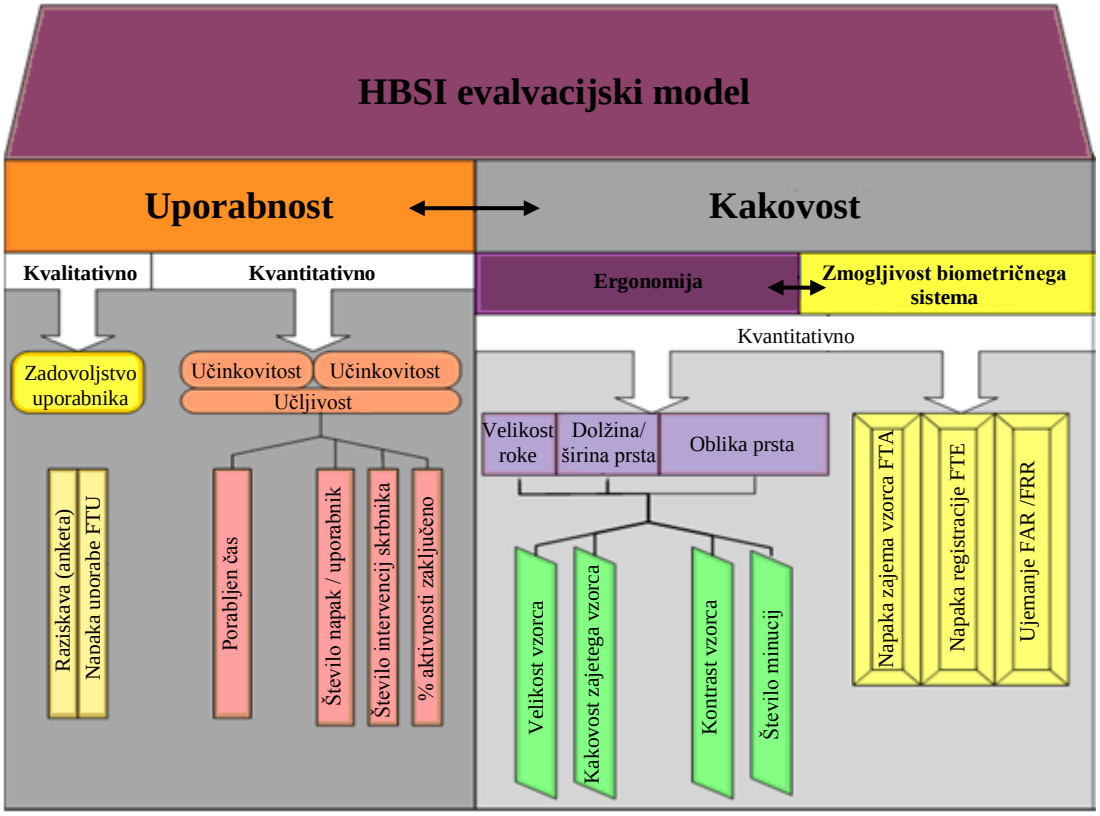
7.9 UČINKOVITOST BIOMETRIČNIH SISTEMOV (HBSI)

Učinkovitost se v kontekstu raziskave doktorske naloge nanaša tudi na lastnosti sistema, ki z razmeroma nizko kompleksnostjo dosega visoko hitrost identifikacije. Merilo za oceno učinkovitosti je primerjava funkcioniranja identifikacijskega sistema pred izvedeno optimizacijo in po njej. Na razmerje med delovno uspešnostjo in kompleksnostjo biometričnega sistema vplivajo dejavniki (procesorska moč, izbira kriptoalgoritma, izbira tipa biometričnega senzorja, določitev FAR in FRR itd.), ki v končni fazi določajo tudi ceno sistema. Učinkovitost biometričnih sistemov delimo na učinkovitost programske in strojne opreme in je parameter kakovosti.

7.9.1 UČINKOVITOST NA NIVOJU PRODUKTA

Merilo učinkovitosti biometričnega sistema je njegova uporabnost, ki se meri v času, ki ga identificirana oseba porabi za dokončanje vseh postopkov v procesu identifikacije. Ta evalvacijski koncept učinkovitosti (HBSI), je prikazan na sliki 7.15 (Kukula in Proctor, 2009). V interakciji človek-računalnik pa je učinkovitost opredeljena tudi kot »točnost in popolnost« izvajanja nalog uporabnikov pri uporabi sistema. Od tega je odvisno število napak, ki jih naredi uporabnik in posledično tudi intervencij skrbnika sistema ter v končni fazi kolikšen delež operacij identifikacije je uspešno izvedenih.

Zajem podatkov prstnega odtisa preko senzorja, registracija ter shranjevanje in iskanje v bazi shranjenih vzorcev, je merjena v sekundah. Izbira biometričnega čitalca je ključnega pomena za učinkovitost sistema kot celote, saj tip (zasnova) biometričnega senzorja vpliva na hitrost interakcij za dokončanje identifikacijskih postopkov. Kvantitativna metrika uporabnosti za evalvacijo vrednotenja modela HBSI je učljivost. Učljivost sestavljajo trije parametri: število storjenih napak glede na uporabnika, dokončanje postopka identifikacije in številko intervencij skrbnika, pri uvajanju biometričnega sistema.

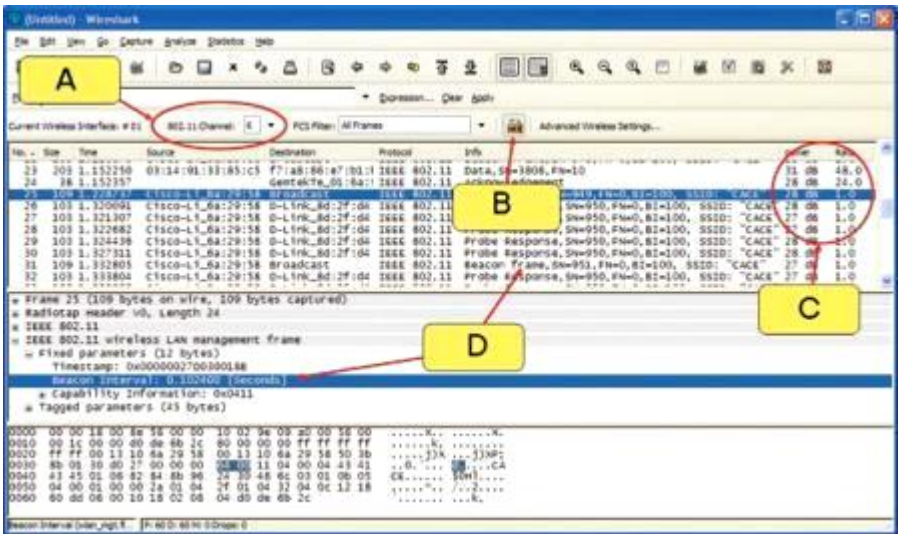


Slika 7.15: HBSI evalvacijski model biometričnega sistema (Kukula in Proctor, 2009)

7.10 VARNOST IN ZASEBNOST OSEBNIH PODATKOV PRI UPORABI BIOMETRIJE

Zasebnost je definirana kot: »Zahteva posameznika, da se sam odloči, kdaj, kako in v kakšni obliki bodo njegovi osebni podatki posredovani drugim« (Electronic Privacy Information Center, 2004). Da bi to dosegli, je treba razvijati dinamično in globalno strategijo, ki mora temeljiti na kulturi varnosti. Razpoložljivost, zanesljivost in varnost omrežij in informacijskih sistemov postajajo vse pomembnejši dejavniki za naše gospodarstvo in družbo kot celoto. Spoprijemanje z varnostnimi izzivi informacijske družbe zahteva tridelni pristop: posebne ukrepe za zagotavljanje varnosti omrežij in informacij, ustrezno zakonodajo o elektronskih komunikacijah (ki mora ustrezno obravnavati tudi vprašanja zasebnosti in varstva podatkov) in boj proti kibernetičnemu kriminalu. Te tri vidike bi bilo sicer do neke mere mogoče razvijati ločeno, vendar številne oblike medsebojne odvisnosti in prepletenosti govorijo v prid oblikovanja usklajene strategije in enotnega okvira za izvedbo in izboljšanje skladnega pristopa k varnosti omrežij in informacij (VOI). Čeprav sta zagotavljanje VOI in varovanje zasebnosti nedvomno izjemno pomembna, pa je obenem treba vsaj ohraniti že doseženo raven svobode izražanja oz. ta nikakor ne sme biti prizadeta. Zakonodajni okvir, ki obravnava področje elektronskih komunikacij, je treba dopolniti z določbami, povezanimi z varnostjo, v tistih delih, v katerih je

trenutno veljavna zakonodaja šibka. Pri tem se je mogoče nasloniti na direktivo o zasebnosti in elektronskih komunikacijah (2002/58/ES), po kateri so ponudniki javno dostopnih komunikacijskih storitev dolžni zagotavljati varnost storitev, ki jih ponujajo. Direktiva prav tako določa ukrepe zoper nezaželeno elektronsko pošto (spam) in vohunsko programsko opremo (spyware). Slika 7.16 prikazuje kako omrežje vidi Wireshark. A: Trenutno izbrani kanal. B: Dešifriranje WEP na ravni gonilnikov. C: Podatki o jakosti signala. D: Prikaz podatkov v podatkovnih okvirih.



Slika 7.16: Wireshark orodje za analizo in zajemanje brezžičnega prometa (Wireshark, 2011)

Zasebnost osebnih podatkov ali informacijska zasebnost je zahteva posameznika, da podatki o njem samem (osebni podatki) niso avtomatično na razpolago drugim osebam in organizacijam. Kadar pa so posredovani drugim, mora imeti možnost kontrole podatkov in nadzora uporabe (Clarke, 2006).

Informacijska zasebnost so pravila za upravljanje zbirk osebnih podatkov, kot so finančne informacije, medicinske kartoteke in zapisi, ki jih upravljajo vladne agencije. Informacijska zasebnost je znana tudi kot »varovanje podatkov«.
S filozofskega vidika obravnavanja zasebnosti naj bi bilo sodobno razumevanje zasebnosti tako imenovana Moorova[26] teorija nadzora in omejenega dostopa (kombinacija teorij filozofov Frieda[27] in Gavisona[28]), ki zagovarja stališče, da ohranja posameznik zasebnost v odnosu do drugih samo, če je situacija takšna, da je zaščiten pred motenjem, vmešavanjem in dostopom do informacij.

Uporabnost ID kartic za pristopno kontrolo in evidentiranje delovnega časa zaposlenih je dobro raziskana. Manj znane so možnosti, ki jih kombinirana ID kartica

[26] *Moor (1997) se ne strinja s Friedovo teorijo nadzora. Pravi, da danes, v dobi računalništva, ni mogoče imeti popolnega nadzora nad lastnimi osebnimi podatki.*

[27] *Po teoriji nadzora Frieda (1970) je posameznikova zasebnost odvisna od nadzora nad njegovimi lastnimi informacijami.*

[28] *Teorija omejenega dostopa filozofinje Gavison (restricted access theory) definira zasebnost kot omejitev dostopa drugim do posameznikovih podatkov. Pri tem upošteva tajnost, anonimnost in samoto.*

ponuja za zaščito podatkov in identifikacijskih sistemov, za kar pa je potrebnega nekaj osnovnega znanja o kriptografiji.

7.10.1 SISTEM ZA UPRAVLJANJE INFORMACIJSKE VARNOSTI – SUIV

SUIV (angl. information security management system) je upravljavski sistem ali sistem vodenja, podoben sistemu vodenja kakovosti (quality management system), pri katerem pa temeljni cilj ni optimizacija poslovanja, temveč obvladovanje informacijskih tveganj in usklajenost z zahtevami za varovanje informacij.

Implementacija sistema upravljanja informacijske varnosti v organizacijo zahteva dobro poznavanje lastnih dobrin, njihove vrednosti za organizacijo kakor tudi njihove ranljivosti. Prevzemanje odgovornosti za zagotavljanje varnosti informacijskih dobrin pomeni zmanjševanje tveganj za uresničitev različnih groženj, ki tem dobrinam pretijo. Zato je treba v organizaciji vzpostaviti ustrezen sistem za upravljanje. SUIV organizaciji zagotavlja ogrodje za učinkovitejše obvladovanje varnostnih tveganj. Za načrtovanje in izvedbo SUIV so priporočeni naslednji procesni koraki (Gaberšček, 2007):

1. faza Načrtuj (angl. plan)
   - določitev obsega SUIV in pristopa k oceni tveganj
   - analiza tveganj
     - identifikacija tveganj:
       - opredelitev ključnih aktivnosti
       - opredelitev virov ključnih aktivnosti
       - identifikacija groženj
     - ocenjevanje tveganj:
       - ocena verjetnosti uresničitve grožnje
       - izdelava profila tveganj
   - obravnava tveganj
       - ovrednotenje oziroma opredelitev sprejemljivosti tveganj
       - identifikacija predlogov obravnave tveganj in njihova analiza
   - izbor ukrepov obravnave tveganj
   - pridobitev odobritve ostanka tveganj in odobritve implementacije SUIV
2. faza Izvedi (angl. do)
   - načrt implementacije in implementacija kontrol
   - merjenje učinkovitosti kontrol
   - programi izobraževanja in zavedanja
   - upravljanje izvajanja SUIV in potrebnih virov
   - upravljanje informacijskih izrednih dogodkov
3. faza Preveri (angl. check)
   - nadzor in pregled vseh komponent SUIV
4. faza Ukrepaj (angl. act)
       - vzdrževanje in izboljšave SUIV

Predstavljen primer temelji na razviti metodologiji PDCA[29], ki je osnova za izvajanje svetovanja pri načrtovanju in implementaciji modelov upravljanja informacijske varnosti v javni upravi in gospodarskem sektorju.

7.10.2 METODOLOGIJA ISM^3

ISM^3 (information security management maturity model) je eden novejših pristopov k upravljanju varnosti informacij. Model opisuje zrelost upravljanja varnosti informacij in temelji na standardu za management kakovosti ISO 9001 z razširitvami za upravljanje varnosti informacij. Temelj informacijske varnosti ISM^3 je opredeljen s petimi nivoji zrelosti pri upravljanju in omogoča organizaciji dolgoročno načrtovanje in prilagajanje stopnje varnosti poslovnim potrebam. ISM^3 je usmerjen k procesom za zagotavljanje informacijske varnosti in ne k nadzoru. Procesi so formalno opisani ter vsebujejo matrike in ciljne nivoje uspešnosti. Pomembno je, da že v izhodišču dobimo merljivo informacijsko varnost. Organizacije, ki upravljajo IT storitve v skladu z ITIL oz. ISO/IEC 20000, lahko z ISM^3 okrepijo proces varnosti.

7.11 TEHNOLOGIJE ZA IZBOLJŠANJE ZASEBNOSTI

Biometrija ima z vidika posameznika nedvomno določene praktične prednosti. Kot vsaka druga tehnologija se lahko uporabi na način, ki je prijazen do posameznikove zasebnosti, lahko pa gre za občutne posege v zasebnost in učinek »velikega brata«. Praktične prednosti biometrije so praviloma vidne na prvi pogled, to pa ne velja za nekatere vidike, ki dokazujejo, da tudi biometrija ni vsemogočna in popolna. Biometrični ukrepi so po naravi stvari takšni, da pomenijo velik poseg v zasebnost in dostojanstvo posameznika, zato je treba vse pogoje za njihovo uporabo razlagati v luči njune zaščite in izhajati iz ZVOP-1-UPB1[30], ki določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov.

Potreba po varni izmenjavi podatkov je stara že tisočletja in se je skozi čas prilagajala metodam šifriranja v posameznem obdobju. Če je bilo šifriranje podatkov nekdaj predvsem potreba vojske in bank, se je krog uporabnikov danes močno povečal. Glavni razlog je razširjenost svetovnega spleta in vsega, kar ta omogoča. S tem se na eni strani pojavlja širok krog uporabnikov, ki želijo varno izmenjevati podatke, na drugi pa odprto javno omrežje s številnimi možnostmi zlorab. Rešitev je uporaba kriptografske opreme, ki se zaradi velikega povpraševanja uporabnikov vse bolj izpopolnjuje in standardizira.

---

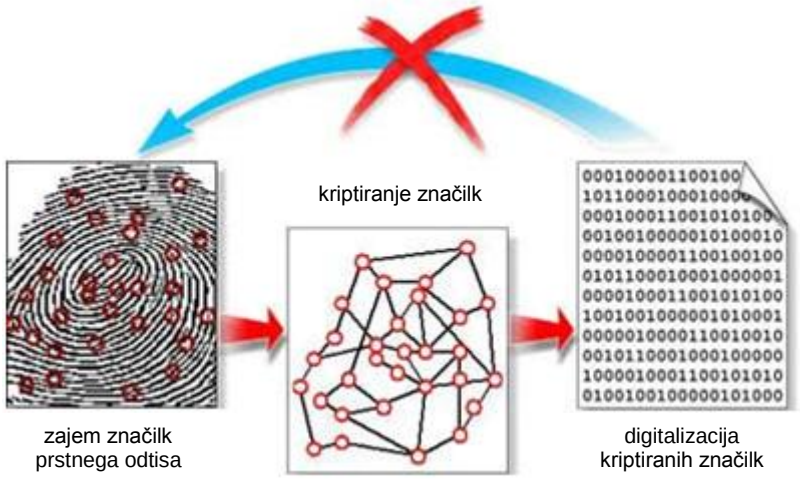
[29] *PDCA krog po Demingu (1900–1993). Deming je bil ameriški fizik in statistik, ki je med 2. svetovno vojno izboljšal proizvodne procese v ZDA, čeprav je najbolj znan po svojem delu na Japonskem.*

[30] *Na podlagi 153. člena Poslovnika državnega zbora je Državni zbor Republike Slovenije na seji 27. septembra 2007 potrdil uradno prečiščeno besedilo Zakona o varstvu osebnih podatkov, ki obsega: a) Zakon o varstvu osebnih podatkov – ZVOP-1 (Uradni list RS, št. 86/04 z dne 5. 8. 2004), b) Zakon o informacijskem pooblaščencu – ZInfP (Uradni list RS, št. 113/05 z dne 16. 12. 2005), c) Zakon o spremembah in dopolnitvah Zakona o ustavnem sodišču – ZUstS-A (Uradni list RS, št. 51/07 z dne 8. 6. 2007) in d) Zakon o spremembah in dopolnitvah Zakona o varstvu osebnih podatkov – ZVOP-1A (Uradni list RS, št. 67/07 z dne 27. 7. 2007).*

7.11.1 KRIPTOLOGIJA

Kriptologija je veda o tajnosti, šifriranju, zakrivanju sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza). Uporabljata se še pojma enkripcija (šifriranje) in dekripcija (dešifriranje). Beseda kriptologija izvira iz grškega izraza »kryptos logos«, ki pomeni skrita beseda, prvi pa jo je v angleščini uporabil Browne leta 1658 (Kovačič, 2006). Sporočilo po nekem postopku (algoritmu, metodi) spremenimo v kriptirano sporočilo, pri čemer uporabimo določene vrednosti za parametre v algoritmu, ki jim rečemo ključ (slika 7.17). Sogovornika se morata torej dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila. Šifriranje podatkov je ključnega pomena za ohranitev tajnosti njihove vsebine. Osnovno sporočilo ponavadi imenujemo čistopis (cleartext, plaintext), zašifrirano pa šifropis ali tajnopis (kriptogram, ciphertext). Bolj kot so podatki tajni, močnejši mora biti šifrirni algoritem.

Biometrična aplikacija mora glede varnosti (Uludag in Jain, 2003) zagotoviti:
- zaupnost (confidentiality),
- celovitost (integrity),
- overjanje (authentication),
- preprečevanje tajenja (nonrepudiation) in
- kontrolo dostopa (access control).



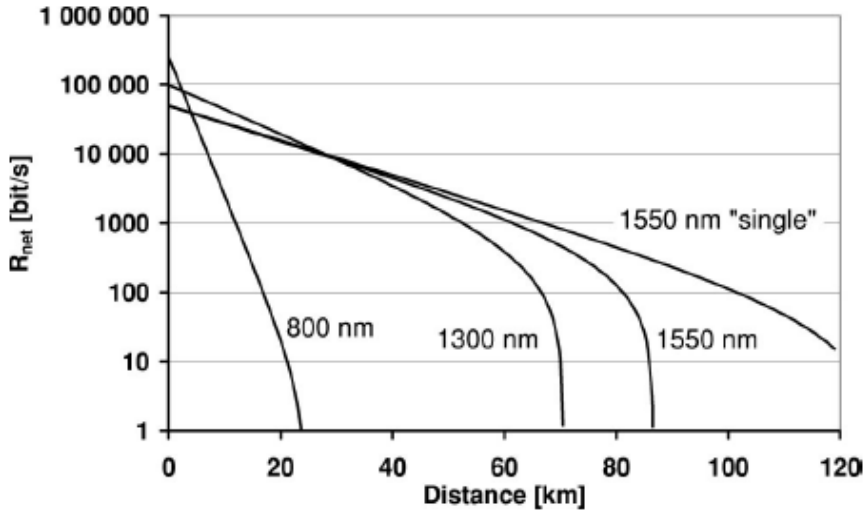
Slika 7.17: Kriptografija značilk prstnega odtisa (Biometric Visions, 2008)

Najnovejše raziskave na tem področju potekajo v smeri kvantne kriptografije[31] (Knil, 2010). Kvantna kriptografija je novejše temeljno znanstveno področje, ki uporablja principe kvantne fizike za doseganje absolutne varnosti pri prenosu informacije v telekomunikacijah. Raziskovalci michiganske fakultete so oblikovali poseben kvantni procesor, namenjen hitremu šifriranju in dešifriranju podatkov. Procesor deluje tako, da s pomočjo svetlobnega žarka opravi uspešen prenos kvantnih lastnosti enega

[31] *Začetki kvantne kriptografije segajo v leto 1984, ko sta Bennet in Brassard razvila protokol varne distribucije ključev BB84.*

atomskega para na svoj nasprotni par, ki tako dobi enake lastnosti kot izvorni par. Matematične algoritme, na katerih sloni varnost prenosa v klasični kriptografiji, nadomesti s fizikalnimi zakonitostmi, ki zagotavljajo absolutno tajnost prenosa. Možnost pošiljanja je do 100 km po zraku ali optiki (slika 7.18) pri čemer pride do različnih vrednosti pojemanj glede na različne izvedbe sprejemnikov. NIST omogoča pošiljanje s hitrostjo do 1 Mbps.

Ključ, ki je povsem naključen in ga je nemogoče odkriti, je vzpostavljen z nizom fotonov. Posredovati in sprejemati ga je mogoče na različnih lokacijah, pri čemer je zagotovljen način, kako lahko dekodirajo morebitne vdiralce. Vsakdo, ki bi prekinil ali poskušal odčitati tok fotonov, bi na samem toku pustil sled, ki bi jo na pravem ponoru lahko zaznali in ustrezno ukrepali.



Slika 7.18: Graf hitrosti bita pri kvantni kriptografiji, v odvisnosti od razdalje med oddajnikom in sprejemnikom (Gisin in drugi, 2002)

7.11.2 VARNOST ŠIFRIRNIH ALGORITMOV

Za varovanje podatkov uporabljamo simetrične, asimetrične in zgoščevalne kriptografske algoritme. Simetrični algoritmi so zaradi hitrosti namenjeni šifriranju podatkov. Uporabljajo tajni ključ, ki ga je treba izmenjati, in ta poskrbi za dešifriranje sporočila. Za varno izmenjavo tajnega ključa se uporabljajo asimetrični algoritmi. Dolžina simetričnega ključa se giblje od 40 do 128 bitov. Daljši kot je ključ, manjša je verjetnost razkritja vsebine šifriranega sporočila. Asimetrični algoritmi temeljijo na konceptu javnega in zasebnega ključa. Uporabljajo se predvsem za digitalno podpisovanje ključev. Najbolj razširjen algoritem je RSA, ki temelji na faktoriranju velikih števil (dolžina ključa od 512 do 2048 bitov).

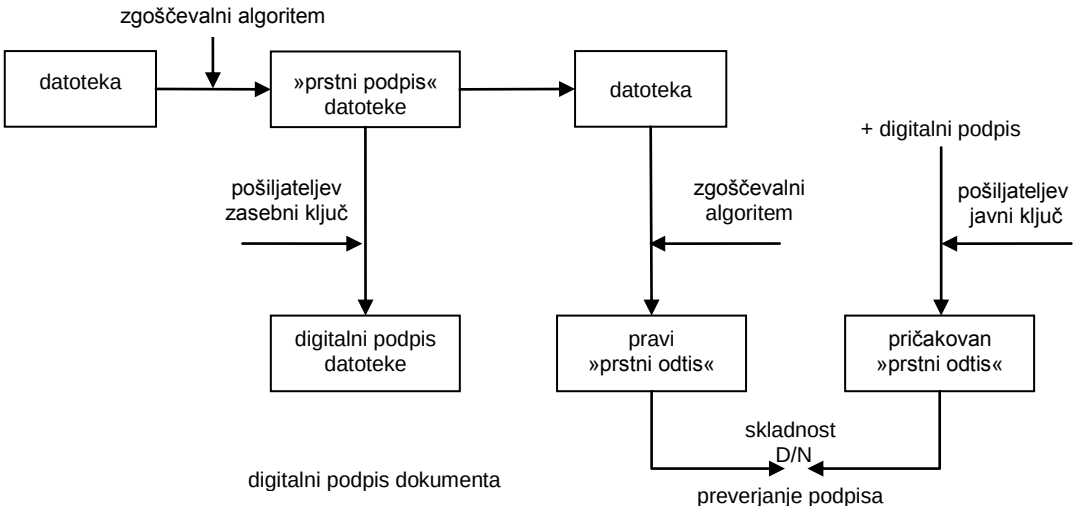
Zgoščevalni algoritmi preslikajo poljuben niz znakov v blok predpisane dolžine, ki predstavlja povzetek vhodnih podatkov. Isti blok podatkov se vedno preslika v isti izhodni blok. Reverzibilnost transformacije ni mogoča. Zaradi tega zgoščevalne algoritme uporabljamo za ugotavljanje nespremenjenosti prejetih podatkov. Za

digitalni podpis dokumentov povzetek (rezultat zgoščevalnega algoritma) dodatno šifriramo z enim od asimetričnih algoritmov.

7.11.3 DIGITALNI PODPIS IN DIGITALNI CERTIFIKAT

Za varno izmenjavo podatkov v informacijskih omrežjih je pomemben digitalni podpis, ki rabi kot nadomestilo klasičnega. Zagotavljati mora avtentičnost podpisnika, hkrati pa ga ne sme biti mogoče ponarediti, kopirati in zanikati. Za izvedbo podpisa uporabljamo različne kombinacije kriptografskih metod, največkrat zgoščevalnega in asimetričnega algoritma. Povzetek dokumenta pošiljatelj izračuna z zgoščevalnim algoritmom, nato ga zašifrira s svojim zasebnim ključem in dobi t. i. digitalni podpis, ki se priloži osnovnemu dokumentu. Prejemnik z javnim ključem pošiljatelja dešifrira podpis in dobi povzetek. Ponovno izračuna povzetek pisma z istim zgoščevalnim algoritmom kot pošiljatelj. Če se ujemata, je dobil enak dokument, kot ga je pošiljatelj podpisal (slika 7.19).

Da bi lahko zaupali avtentičnosti javnega ključa pošiljatelja (da ga ni morda kdo zlorabil), uporabljamo digitalna potrdila javnih ključev (digitalni certifikat).
Certifikate izdajajo overitelji (certification authority – CA). Če želita stranki varno izmenjevati podatke, si izbereta skupnega overitelja, ki mu zaupata, in na podlagi izdanih certifikatov pričneta izmenjavo podatkov.



Slika 7.19: Fingerprint avtentikacija s prenosom javnega ključa (Sotomajor, 2005)

Za avtomatizirano in pregledno izdajanje, objavljanje in uporabo javnih ključev nastajajo baze javnih ključev (PKI – public key infrastructure). Za overjanje javnih ključev skrbijo CA. Vsak overitelj objavi svoj javni ključ in dokument »certification policy«, ki opisuje postopek, kako in komu podeljuje potrdila ter na kakšen način varuje svoj zasebni ključ. Na podlagi tega dokumenta uporabnik oceni, ali lahko zaupa overitelju in posledično vsem uporabnikom izdanih certifikatov overitelja.

Na trgu se pojavljajo različne organizacije, ki podeljujejo certifikate podjetjem in posameznikom ter seveda storitve tudi zaračunavajo. V poplavi različnih ponudnikov

pa je lahko modra odločitev gradnja lastne infrastrukture PKI znotraj podjetja, s katero celoten sistem prilagodimo svojim potrebam in ga vgradimo v obstoječe informacijske rešitve.

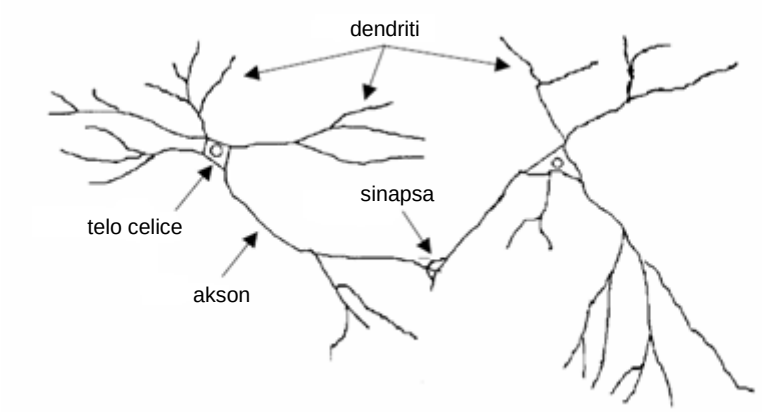
8 MODELI ODLOČANJA

Formalen pristop k načrtovanju in gradnji odločitvenih modelov naj bi zmanjšal število napak in težo njihovih posledic, zagotovil integriteto podatkov, podprl vzdrževanje ter postavil realne temelje za izpolnjevanje značilnosti kakovostnega identifikacijskega sistema, kot so zanesljivost, popolnost, spremenljivost, vpogledljivost, pravilna zasnova in zadovoljstvo uporabnika (Kreie in drugi, 2000).

8.1 NEVRONSKE MREŽE

Pri nastavljanju (učenju) mreži predstavimo sliko, podpis ali prstni odtis, ki jo ta primerja s sliko v svojem spominu. Mreža nato nastavlja uteži, dokler ne dobimo želenega rezultata. Teoretično se lahko mreže naučijo prepoznavati vse obraze na tem planetu tudi pri zelo slabih pogojih zajemanja slike. Mreža analizira celotno sliko, na kateri išče kontrastne elemente (oči, obrvi, eno stran nosu, usta, ličnice itd.). Metoda se uporablja pri obeh načinih iskanja, 1:N in 1:1 (Rowley in drugi, 1998).

Računalniško simulirana nevronska mreža deluje na podobnem principu kot biološka (slika 8.1) nevronska mreža (možgani). Prav tako vsebuje nevrone in povezave med njimi.



Slika 8.1: Zgradba živčne celice ali nevrona (Dobnikar, 1990)

Poznamo več tipov umetnih nevronskih mrež, vendar se bomo v tem poglavju omejili le na večplastno nevronsko mrežo, učeno z vzvratnim razširjanjem, ki smo jo tudi uporabili v našem programu. Lastnosti, ki opisujejo nevronske mreže (Kokol in drugi, 2001):

a. Vrsta topologije:
- večnivojska – organizirana po nivojih (vhodni nivo, skriti nivoji, izhodni nivo),
- breznivojska (enonivojska) – dovoljene povezave med vsemi nevroni.

b. Usmerjenost povezav:
- nevronske mreže brez povezav nazaj – nerekurentne (feedforward) nevronske mreže,

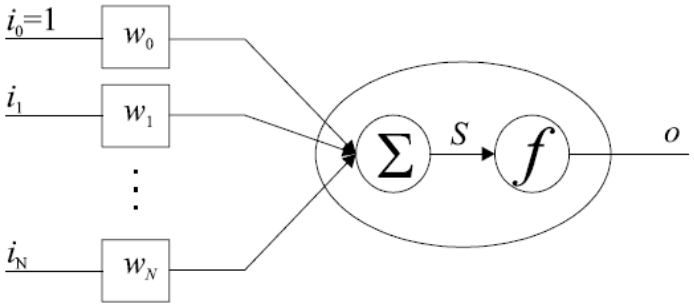
- nevronske mreže s povezavami nazaj – rekurentne nevronske mreže.

c. Način učenja:
- nadzorovano učenje (supervised learning) – učitelj poda mreži pravilen odgovor,
- nenadzorovano učenje (unsupervised learning) – ni primerjave med odgovorom in pričakovanim odgovorom, mreža se organizira glede na vnaprej podano funkcijo.

d. Tipi vhodnih spremenljivk:
- binarni (0,1),
- bipolarni (-1,1),
- realna števila.

e. Vrste aktivacijskih funkcij:
- linearna,
- stopničasta,
- sigmoidna.

(Večnivojsko) mrežo največkrat poimenujemo po številu skritih nivojev, saj se tako izognemo nepravilnostim pri (ne)upoštevanju vhodnega nivoja (slika 8.2).



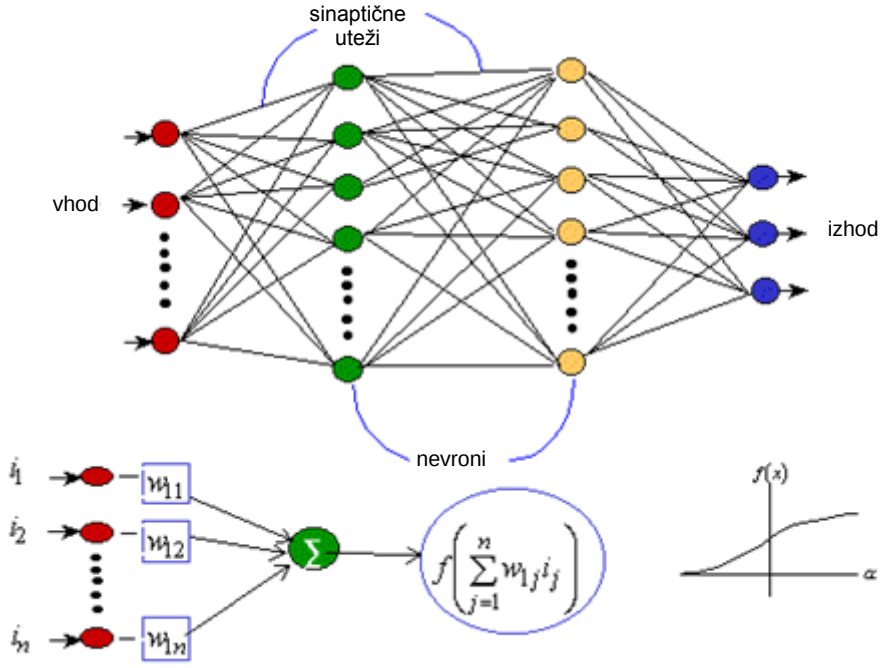
Slika 8.2: Zgradba umetnega nevrona (Dobnikar, 1990)

Prva in najpomembnejša naloga pri uporabi nevronskih mrež je določitev topologije oz. števila nivojev in števila nevronov na posameznem nivoju. Kadar je nevronska mreža premajhna, ne bo zmožna predstaviti želene funkcije. Če je mreža prevelika, pride do čezmernega prileganja[32], ne da bi se akumuliralo splošno znanje (Tetko in drugi, 1995). Do ustrezne topologije najlažje pridemo s poskušanjem.
Nevronska mreža je masovni paralelni porazdeljeni procesor, ki shranjuje eksperimentalno znanje in omogoča njegovo uporabo. Možganom je podobna v dveh pogledih:
- znanje se zbira z mrežo skozi proces učenja in
- mednevronske povezave, znane kot sinaptične uteži, se uporabljajo za shranjevanje tega znanja (Guid in Strnad, 2007).

Učenje nevronske mreže se izvaja z algoritmom učenja, ki spreminja uteži v povezavah med nevroni in s tem »oblikuje« znanje, ki bo shranjeno (slika 8.3). En sam nevron ima zelo omejene zmožnosti. Povezovanje nevronov v mreže nam da

[32] *Čezmerno prilagajanje (angl. overfitting); termin »overfitting« pri učenju nevronskih mrež je znan tudi kot »overtraining«.*

veliko močnejše orodje. Načinu in številu povezav nevronov pravimo topologija nevronske mreže. Poznamo veliko načinov povezovanja, vsak ima drugačne lastnosti ter s tem prednosti in slabosti (Guid in Strnad, 2007).



Slika 8.3: Nivoji nevronske mreže (Spanner, 2000)

8.1.1 OSNOVNE OBLIKE NEVRONSKIH MREŽ

8.1.1.1 Feed-Forwardove nevronske mreže (FF)

FF nevronske mreže so večnivojske, brez povezav nazaj in se učijo nadzorovano. Tipičen primer uporabe FF nevronske mreže je klasifikacija vzorcev. So brez skritih nivojev in lahko razdelijo hiperprostor na dva hiperpodprostora. FF nevronske mreže z enim skritim nivojem lahko omeji poljubno konveksno območje, medtem ko tiste z dvema skritima nivojema lahko omeji kakršnokoli območje. V primeru klasifikacije se izhode lahko kodira v obliki t. i. navideznih (dummy) spremenljivk, pri čemer imamo toliko izhodov, kot je razredov, izhod razreda, ki mu pripada vhodni vzorec, se postavi na 1, preostali pa na 0. Tipična metoda za učenje teh mrež je metoda padajočih gradientov (backpropagation). Včasih FF nevronske mreže imenujemo kar backpropagation nevronske mreže, po metodi učenja. Posplošeno pravilo delta, ki ga je razvil Rumelhart s sodelavci, zahteva, da so aktivacijske funkcije, ki opisujejo umetni nevron, diferenciabilne (Kokol in drugi, 2001).

8.1.1.2 Hopfieldove[33] nevronske mreže

Te nevronske mreže shranijo učne vzorce kot množico stabilnih stanj. Ko damo na vhod nov (testni) vzorec nevronske mreže, konvergira k tistemu stabilnemu (naučenemu) stanju, ki leži najbližje vhodu. Vsak nevron lahko zavzame samo dve bipolarni stanji (1, -1), pri čemer stanje 1 pomeni prisotnost, stanje -1 pa odsotnost neke lastnosti. Število nevronov in s tem »stanj« nevronske mreže je tolikšno, kolikor je lastnosti (lastnosti imajo lahko samo dve vrednosti). Nevronska mreža ima le en nevron, ki je polno povratno povezan (izhodi vsakega nevrona so prek uteži W_{ij} povezani z vhodi vseh nevronov). Vsak nevron ima prav tako vhodno povezavo s svojo lastnostjo n. Vsak učni objekt Hopfieldove nevronske mreže je predstavljen z vektorjem dolžine n, ki opisuje njegove lastnosti. Po končanem učenju »stanje« vsakega nevrona predstavlja tudi izhod n. Pri učenju Hopfieldovih nevronskih mrež samo enkrat nastavimo uteži povezavam, kasneje jih ne spreminjamo več (Kokol in drugi 2001). Osnovni pravili sta $W_{ij} = W_{ji}$ in $W_{ii} = 0$. Vrednosti $W_{ij(i\neq j)}$ so določene z izrazom:

$$W_{ij} = \Sigma(vseh\ učnih\ vzorcev)\ X_i(učni\ vzorec) \cdot X_j(učni\ vzorec). \quad (78)$$

Povedano drugače; če imata X_i (učni vzorec) in X_j (učni vzorec) enake vrednosti, se utež ojači, sicer pa oslabi. Učenje je kljub temu nadzorovano, saj učitelj priskrbi prave učne vzorce.

Začetne vrednosti vhodov v nevrone dobimo iz neznanega vzorca, ki ga želimo prepoznati. Če opazujemo nevron i, izračunamo novo (začasno) vrednost

$$TEMP_i = \Sigma(j, vsi\ nevroni)\ W_{ij} \cdot X_j. \quad (79)$$

Novo vrednost postavimo na 1, če je $TEMP_i > prag$, na -1, če je $TEMP_i < prag$, in na 0, če je $TEMP_i = prag$. Prag je običajno enak 0. Vrednosti vhodov/izhodov nevronov osvežujemo posamično, najpogosteje z naključno funkcijo. Vsak nevron naj bi bil namreč izbran enakokrat, da obstaja možnost, da se bo vhod približal najbližjemu vzorcu. Za opazovanje napredka pri iskanju uporabljamo energijsko funkcijo (funkcijo Ljapunova[34]). Ko se vrednost energijske funkcije neha zmanjševati, je to znak, da so tudi nevroni nehali spreminjati svoje stanje in da lahko zaključimo iskanje najbližjega vzorca.

---

[33] *Prepoznavanje znakov v ekspertnem sistemu ESSOD (Expert System for Salvation of Old Documents) ali ekspertnem sistemu za optično prepoznavanje znakov temelji na Hopfieldovih nevronskih mrežah. Tako prisotni »šumi« (stari dokumenti, katerih vsebino rešujemo, so večkrat nečitljivi) ne vplivajo toliko na prepoznavanje, saj Hopfieldove nevronske mreže prepoznavajo tudi pošumljene in delno uničene (manjkajoče) vhode. Namen: obdelava in shranjevanje (starih) dokumentov v elektronski obliki ter reševanje vsebine starih dokumentov pred uničenjem.*

[34] *Ljapunov (1857–1918); ruski matematik. url: http://www.slovarji.com/slovarji/slovarji-08/8l.html (14.07.2009)*

8.1.1.3 Kohonenove[35] nevronske mreže

So predstavnice samoorganiziranega kompetitivnega nenadzorovanega učenja. To pomeni, da se nevronska mreža sama organizira tako, da je sposobna dati koristne informacije (je samoorganizirana). Povezave nevronov tekmujejo[36] med seboj, pri čemer zmagovalci ojačajo povezave, poraženci pa jih oslabijo (mreža je kompetitivna). Nevronski mreži nihče ne pove, ali deluje v pravilni smeri ali ne (je nenadzorovana). Kohonenova nevronska mreža je dvonivojska z vhodnim nivojem (n nevronov) in Kohonenovim nivojem (m nevronov) s povezavami (W_{ij}) samo naprej. Vhodi v nevronske mreže so zvezna števila. Kohonenov nivo je lahko urejen večdimenzionalno. V postopku inicializacije definiramo radij R, ki nam določa soseščino nekega nevrona, in hitrost učenja $alpha$. Pri tem je ($0<alpha<1$), uteži pa nastavimo na majhne naključne vrednosti. Sledi iterativni del, ki se ponavlja za vsak vhodni vektor x iz učne množice (učne vektorje izbiramo po naključnem vrstnem redu). Izberemo zmagovalni Kohonenov nevron, t. j. nevron z najmanjšo razdaljo do vhoda D (Kokol in drugi, 2001):

$$D = D_{(Wj,X)};\ W_j = \left(W_{1j}, W_{2j}, ..., W_{nj}\right). \tag{80}$$

Vsem nevronom znotraj radija R popravimo uteži na novo vrednost:

$$W_{j(t+1)} = W_{j(t)} + alpha\left[X_{(t)} - W_{j(t)}\right]. \tag{81}$$

Hitrost in radij se s številom iteracij manjšata. Po dovolj velikem številu iteracij in dovoj velikem številu učnih vzorcev se vektorji uteži združujejo v skupke tam, kjer so učni vektorji pogostejši. Zaradi tega so podobni vhodni vektorji klasificirani v podobne ali iste skupke (clusters[37]).

8.1.1.4 Druge oblike nevronskih mrež

Kot smo že omenili, je struktura nevronske mreže odvisna od namena uporabe. Zgoraj smo opisali le tri najbolj uporabljane oblike, da bi predstavili raznoliko uporabo nevronskih mrež. Njihova uporaba pa seveda ni omejena na te tri osnovne oblike, temveč je arhitektura odvisna predvsem od namena uporabe in pa občutka in znanja oblikovalca.

---

[35] *Finski profesor Kohonenov je, predsednik evropskega združenja za raziskovanje nevronskih mrež.*

[36] *Tekmovalno pravilo zahteva, da je v določeni skupini nevronov aktiven vedno natanko eden. To se doseže z ustrezno topologijo, pri čemer je v skupini vsak nevron povezan z vsakim z zaviralnimi vezmi. Ko en nevron postane aktiven, z zaviralnimi vezmi »zatre« preostale, da ne morejo postati aktivni. Po tem pravilu se uči samo zmagovalni nevron, in sicer tako, da poveča uteži vezem, ki so mu pomagale, da je »zmagal«, vsem drugim pa jih zmanjša.*

[37] *Razvrščanje (angl. clustering); od naučene nevronske mreže pričakujemo, da bo niz vhodnih podatkov razvrstila v ustrezno skupino. url: http://www.gimvic.org/predmeti/informatika/gradiva/html-ji/nevronske.html (12.07.2007)*

8.1.2 UČENJE NEVRONSKE MREŽE

Računalniško simulirana nevronska mreža deluje po podobnem principu kot biološka nevronska mreža (možgani). Prav tako vsebuje nevrone in povezave med njimi.

Učenje je proces, v katerem se prosti parametri nevronske mreže prilagodijo skozi kontinuiran proces simulacije od okolja, v katero je vložena mreža. Tip učenja določa način, po katerem se spreminjajo parametri. Nevronsko mrežo naučimo znanja s pomočjo učnih vzorcev, ki predstavljajo zgled (klasifikacija[38]). Priučitev nevronske mreže v grobem poteka tako, da mreža na vhodu prejme signale, ki označujejo karakteristiko učnega objekta, nato pa na vsakem nivoju spreminjamo uteži, dokler vhodi ne ustrezajo želenim izhodom. To spreminjanje se izvaja v ciklih (epochs), pri čemer en cikel predstavlja izračun napake in prilagoditev uteži za vse nevrone na vseh nivojih mreže (Guid in Strnad, 2007).

Poznamo več tipov umetnih nevronskih mrež, vendar se bomo za našo raziskavo omejili na samoučečo se mrežo, uporabljeno v programu EasyNN. Učenje nevronske mreže se izvaja z algoritmom učenja, ki spreminja uteži v povezavah med nevroni in s tem oblikuje (generalizira[39]) znanje, ki bo shranjeno.
Naj omenimo le nekaj učnih pravil (Kononenko, 2005):

- Hebbovo pravilo,
- pravilo delta,
- posplošeno pravilo delta,
- tekmovalno pravilo,
- nenadzorovano učenje,
- nadzorovano učenje.

8.2 EKSPERTNI SISTEMI

Z razvojem »vede o pojasnjevanju«, kot so strokovnjaki poimenovali umetno inteligenco[40] (Kodratoff in Tecuci, 1988), se je razširila tudi uporabnost ekspertnih sistemov, računalniških programov, ki posnemajo delo izvedencev in na podlagi vanje vnesenih podatkov in pravil sklepanja podajo končno oceno, ki jo glede na namen uporabe lahko razumemo kot kazalec stanja, napoved, koristnost ali drugo lastnost predmetov obravnave. Ekspertni sistemi se veliko uporabljajo na nekaterih, navadno zelo specializiranih znanstvenih področjih, še posebno v medicini. Zanje velja, da so bili razviti izključno za uporabo na zelo ozkem področju. Širšo uporabo so omogočile lupine ekspertnih sistemov, v katerih so že zapisana pravila sklepanja,

[38] *Pri klasifikacijskih problemih se mreža uči iz parov primerov vhodni podatki-rešitev, od nje pričakujemo, da bo med delovanjem naučene vhodne podatke prepoznala, čeprav bodo vsebovali šum.*

[39] *Pri generalizaciji od naučene nevronske mreže pričakujemo, da bo napovedala rezultat za vhodne podatke, ki so drugačni od tistih v času učenja. url: http://www.gimvic.org/predmeti/informatika/gradiva/html-ji/nevronske.html (12.07.2007)*

[40] *Turing (1912–1954), britanski matematik, logik, filozof, biolog in tajnopisec, ki velja za pionirja na področjih računalniške znanosti, kognitivne znanosti, umetne inteligence in umetnega življenja. Je eden od očetov moderne računalniške znanosti.*

naloga uporabnikov je le, da v sistem na ustrezen način zapišejo svoje znanje. Sodobne lupine ekspertnih sistemov, npr. Dex[41], to delo precej poenostavijo.

8.3 HIBRIDNI INTELIGENTNI SISTEMI

Uporaba hibridnih inteligentnih sistemov hitro narašča z uspešnimi aplikacijami na številnih področjih, kot so procesna kontrola, industrijsko načrtovanje, finančno trgovanje, ocenjevanje kreditov, medicinske kontrole in poznavalne simulacije. V hibridnih inteligentnih sistemih združujemo različne tehnologije (Subašić, 1997):

- fuzzy logiko,
- nevronske mreže,
- genetske algoritme in
- odločitvena drevesa.

8.4 NEUROFUZZY SISTEMI

Fuzzy logika se uporablja na mnogih področjih, kjer so pristopi, temelječi na konvencionalnih modelih, težki ali pa njihova implementacija ne upraviči stroškov glede na učinkovitost. Uporabnost sega tudi na področje biometrije (Melin in Castillo, 2005). Pri večanju kompleksnost sistema, je bilo težko določiti zanesljiva fuzzy pravila in članske funkcije, uporabljene za opisovanje obnašanja sistema. Kakorkoli, omejeni ali nečisti podatki se lahko kažejo v nekonsistentnih, nepomembnih izhodih. To je znano kot velika težava nevronskih mrež.

8.4.1 PREDNOSTI MEHKE LOGIKE

Osnovna prednost mehke logike je, da zelo enostavno matematično (Gill, 2004) popiše človekovo sklepanje in način njegovega razmišljanja. Pri regulaciji z mehko logiko ne potrebujemo matematičnega modela procesa. Ker je po svoji naravi nelinearna, je zelo uporabna za reševanje nelinearnih regulacijskih problemov. Mehka logika omogoča večjo robustnost regulatorjev in do neke mere tudi adaptivno delovanje. V regulacijski tehniki so rešitve problemov enostavnejše, cenejše, hitrejše in bolj tolerantne glede motenj (McNeill in Thro, 1994).

8.4.2 POMANJKLJIVOSTI IN TEŽAVE PRI UPORABI MEHKE LOGIKE

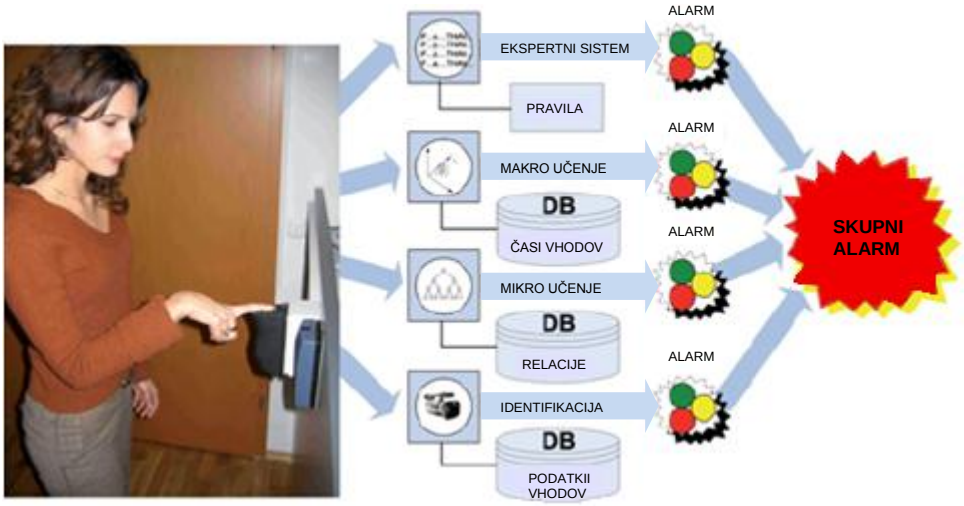
Mehka logika se dolgo ni množično uveljavila, ker kljub njeni enostavnosti potrebujemo precejšnje računalniške zmogljivosti za izvajanje mehkih pravil v realnem času (McNeill in Thro, 1994). Pri tem mislimo na računsko moč in pomnilniške zahteve. Z običajnimi mikroprocesorji in mikrokrmilniki lahko dosegamo nekaj sto do nekaj tisoč regulacijskih akcij v sekundi. Posebna strojna oprema pa omogoča za enak sistem tudi milijon in več regulacijskih akcij v sekundi. Zaradi hitrega razvoja mehke logike in pripadajoče strojne opreme bodo navedene pomanjkljivosti in težave sčasoma zagotovo odpravljene.

[41] *Dex je lupina ekspertnega sistema za večparametrsko odločanje, razvita na Institutu Jožef Stefan v Ljubljani. Uporablja se za podporo odločevalcem pri reševanju zapletenih problemov odločanja tako v poslovni kot individualni rabi.*

9 UPORABA NEVRONSKE MREŽE ZA DOLOČITEV MULTIMODALNEGA BIOMETRIČNEGA SISTEMA

9.1 RAZVOJ INTELIGENTNIH MULTIMODALNIH BIOMETRIČNIH SISTEMOV

Davis opisuje inteligentne sisteme kot »pripomočke za razmišljanje«, pri čemer navaja analogijo z mehanskimi sistemi, ki omogočajo povečanje naših fizičnih zmogljivosti (dvigala lahko dvigajo veliko težo, s teleskopom vidimo dlje itd.) (Podgorelec, 2001). Inteligentni sistemi so njihov ekvivalent na področju podpore razmišljanja, reševanja problemov in obdelave velikih količin podatkov. Njihova prednost pred običajnimi ekspertnimi sistemi je to, da znajo inteligentni sistemi (slika 9.1) izkoristiti dodatna orodja in tehnologije, zaradi česar so lažji za uporabo, lažje jih je graditi, vzdrževati in integrirati v konvencionalne informacijske sisteme.



Slika 9.1: Struktura inteligentnega biometričnega sistema (Gams in Tušar, 2007)

V preteklih 50 letih raziskovanje umetne inteligence ni izpolnilo mnogih pričakovanj in je tako pustilo mnogo izzivov. Eden od aktualnejših projektov je poiskati način za izvedbo avtomatskega učenja in sklepanja nad realnimi podatki, pri čemer je treba upoštevati specifične omejitve posameznih aplikacijskih področij (tabela 9.1). Dosedanje raziskave (Snelick in drugi, 2000) o uporabi avtomatičnega določanja inteligentnih multimodalnih biometričnih sistemov so specifično namenske (Baker in Maurer, 2008), prav tako ni teoretičnih dognanj ali obsežnejših empiričnih preizkusov, ki bi omogočali ovrednotenje uporabnosti takšnega pristopa.

Tabela 9.1: Metodologija inteligentnih sistemov (Podgorelec, 2001)

	Mikroskopski, primarno numeričen vhod	Mikroskopski, deskriptiven in numeričen vhod
Deduktiven	kaos	mehke množice
Induktiven	• nevronske mreže • genetski algoritmi • evolucijsko programiranje	• grobe množice • odločitvena drevesa

9.2 NAČRTOVANJE, ANALIZA, SIMULACIJA IN OPTIMIZACIJA

Obstaja veliko različnih tehnik za modeliranje poslovnih procesov. Diagrami poteka, diagrami toka podatkov, eEPC in EPC diagrami, razne oblike tabelaričnih zapisov (v metodologiji TAD), Petrijeve mreže itd. Za preslikavo realnosti v model uporablja metodologija TAD niz različnih tabel, v katerih se opisuje delovanje sistema. Izdelava simulacijskega modela in izvajanje poskusov so potrebni podatki o zgradbi identifikacijskega sistema, izdelkih, naročilih in napakah. Sistem opisuje tloris prostorske razmestitve v točkovni ali vektorski grafiki (2D in 3D) (Čufer, 2003).

Simulacija poteka v treh osnovnih korakih: izdelava modela, izvajanje poskusov ter razlaga rezultatov in ukrepanje. Podatki o obstoječem procesu oziroma načrt novega sistema so osnova za gradnjo simulacijskega modela, s katerim se nato izvajajo poskusi, njihovi rezultati se analizirajo in so podlaga za sprejemanje odločitev o ukrepih za spremembo obstoječega procesa ali dopolnitev načrta (Chung, 2004).

9.3 ZAHTEVAN VARNOSTNI NIVO

Posameznik ali družba, ki želita uporabljati biometrično tehnologijo, morata določiti zahtevan varnostni nivo delovanja takšnega sistema. Obstajajo nizek, srednji in visok varnostni nivo. Če zadostuje nizek ali srednji nivo, imamo na voljo vse vrste identifikacijskih tehnik, če pa je zahtevan visok nivo, smo omejeni na tiste tehnike, ki delujejo na osnovi unikatne telesne značilnosti (Liu in Silverman, 2001).

9.4 NEURAL NETWORK TOOLBOX™ 7.0

Program je namenjen za konstrukcijo, implementacijo, vizualizacijo in simulacijo nevronskih mrež na področjih, kjer so konvencionalne analize otežene ali celo nemogoče (npr. prepoznava vzorcev in nelinearni sistemi identifikacije in kontrole). Vsebuje GUI (uporabniške grafične vmesnike) za konstrukcijo in upravljanje mreže (Beale, Hagan in Demuth, 2010).

9.5 EASYNN (RAZVOJNO ORODJE ZA IZDELAVO VEČNIVOJSKE NEVRONSKE MREŽE)

S programom EasyNN[42] (Neural Planner Software) lahko sestavljamo večnivojske nevronske mreže iz podatkov v tabeli. Vhodi in izhodi iz nevronskih celic ustrezajo vhodnim in izhodnim stolpcem v tabeli. Skriti nivoji, ki povezujejo vhodni in izhodni nivo, vzdržujejo optimalno število nevronskih celic in povezav med njimi. Vsaka celica vsebuje nevron in njegove povezovalne naslove. Celoten proces pa je samodejen.

9.6 VNOS PODATKOV

Samo mrežo oblikujemo z uvozom podatkov iz tabelnih in tekstovnih datotek, v katerih so besede ločene s tabulatorji ali vejicami, iz bitmap slikovnih ali binarnih datotek. Mrežo je mogoče sestaviti tudi ročno z vpisom podatkov v posebnem podprogramu EasyNN. Za gradnjo nevronske mreže se lahko uporabijo numerični, tekstovni, slikovni ali kombinirani podatkovni tipi.

9.7 OMEJITVE NEVRONSKIH MREŽ

Največje omejitve, ki zadevajo nevronske mreže danes, so problem skaliranja[43], testiranje in verifikacija. Na nekaterih področjih so ti postopki nedopustni (jedrska tehnologija, vesoljski programi, obrambni sistemi). Matematične teorije, ki bi zagotavljale stabilnost delovanja, se še razvijajo (Kononenko, 2002). Trenutna rešitev bi lahko bila učenje in verifikacija trenutnih inteligentnih sistemov kot v primeru človeka. Obstajajo tudi drugi praktični problemi (Kokol in drugi, 2005):

- Simulacija paralelnosti nevronskih mrež; kljub temu da so nevronske mreže paralelne, so trenutno simulirane na sekvenčnih računalnikih, posledica tega pa je hitro naraščajoča časovna potratnost. Možna rešitev je implementacija nevronskih mrež neposredno s strojno opremo (hardware), kar se še vedno razvija.
- Nevronske mreže podajo samo odgovor in ne odgovorijo na vprašanje, zakaj je ta odgovor pravi (svojih sklepov ne pojasnijo).

[42] *Programska oprema je dosegljiva na: http://www.easynn.com/ (12.1.2011).*
[43] *Problem skaliranja (scalability problem); v velikih sistemih nevronske mreže včasih delujejo nestabilno.*

10 RAZISKAVA

V raziskavi je potrebno za definirano obdobje opredeliti ocene karakteristik zanesljivosti kartičnih in biometričnih identifikacijskih sistemov. Ocene karakteristik zanesljivosti sestavnih delov sistema (komponent) določimo na podlagi spremljanja delovanja primerno velikega vzorca izdelkov v eksploataciji.

S spremljanjem kartičnega ter biometričnega sistema v uporabi opazujemo proces odpovedovanja izbranih primerkov (gradnikov sistema). Odpovedi primerkov v vzorcu so med seboj neodvisne, z beleženjem časov do odpovedi oziroma časov aktivnih popravil pa bomo z izbranimi metodami ocenili vrednosti karakteristik zanesljivosti in razpoložljivosti čitalnih modulov kartičnega ter biometričnega sistema.

10.1 RAZISKOVALNO OKOLJE ZA APLIKATIVNI DEL RAZISKAVE

Raziskovalno okolje predstavljata sistem za kontrolo vstopa v športno - rekreacijske centre in sistem elektronskih ključavnic. Rešitev je poimenovana LCC & ELS (Leisure Center Card & Electronic Locking System). Sistem LCC & ELS podpira dva načina konfiguracije pristopne kontrole.

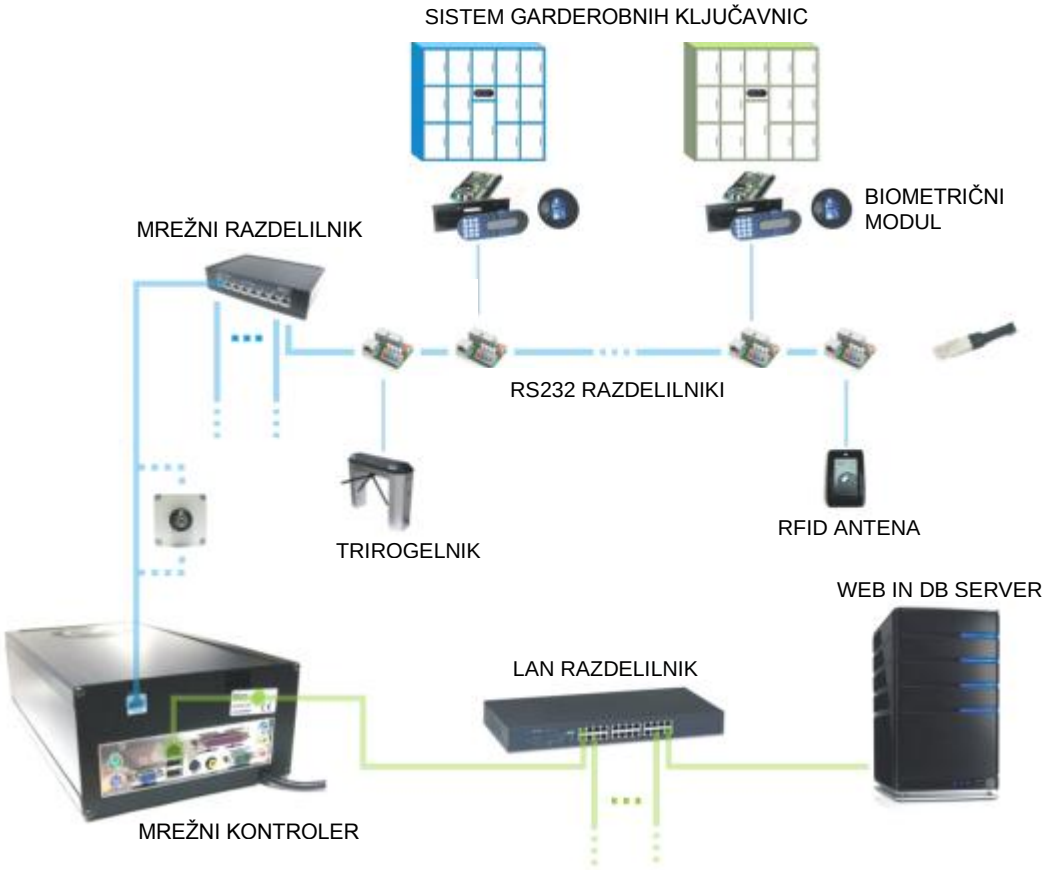
10.1.1 NAČINI KONFIGURACIJE PRISTOPNE KONTROLE

1. V načinu LCC so vsi podatki dejansko zapisani na mediju. Ta način delovanja je statičen oziroma nepriključen (off-line), saj deluje s skoraj polno funkcionalnostjo tudi v primeru izpada strežnika.
2. Način ELS je dinamičen oziroma priključen (on-line) način delovanja. To pomeni, da nosilec informacije ni več prenosni medij, temveč so vse informacije zapisane na strežniku. V primeru izpada strežnika naprave preidejo v tako imenovani varni način obratovanja (podobno kot varni način (safe mode) pri operacijskem sistemu na računalniku). V tovrstnih sistemih je vedno bolj uveljavljeno biometrično preverjanje (prstnega odtisa) uporabnika.

V obeh načinih je prenosni medij (čip, RFID ali biometrični zapis) uporabljen kot:
- dostop do bazena in drugih športnih objektov,
- zaklepanje garderobne omarice,
- vstop v hotelsko sobo,
- plačilo v restavraciji, baru ali pri lokalnih partnerjih stranke in
- uporaba parkirišča.

10.1.2 ARHITEKTURA SISTEMA PRISTOPNE KONTROLE ELS

Nove smernice nam narekujejo razvoj aplikacij v smeri čim lažje uporabe programskih proizvodov in programskih vmesnikov (slika 10.1), ki so že na trgu, ter tako omogočiti kar se da visok nivo ergonomije storitev teh proizvodov v javni in zasebni uporabi.



Slika 10.1: Metra ELS NET identifikacijski sistem

10.1.2.1 Programska oprema

Programsko okolje za obračunavanje storitev (LCC & ELS) je integriran informacijski sistem za administracijo podatkov o kupcih, povezan s sistemom obračunavanja storitev. Programsko okolje odlikuje več izvrstnih lastnosti:

- je aplikacija, narejena na ključ, sestavljena tako iz strojne kot programske opreme,
- sistem obsega zajem podatkov, obračun storitev in skrb za kupca,
- razpoložljivost in podpora sistema sta stalna: 24 ur na dan, 7 dni v tednu, 365 dni v letu.

LCC & ELS je izdelek, primeren za različno velike sisteme. Združuje več tipov storitev, ki jih ponuja organizacija na podlagi informacij, shranjenih v podatkovni bazi SQL. Glavno uporabljeno programsko orodje je Borland JBuilder – hitro razvojno orodje za delo v javanskih okoljih.

10.1.2.2 Kontrolna enota

Kontrolna enota (slika 10.2) je osrednji del strojne opreme. Zaradi modularne zasnove jo lahko po potrebi nadgrajujemo za različne tipe identifikacijskih sistemov (kontaktni, RFID in biometrični). Na matični plošči ima vgrajen mikroračunalnik, ki ji omogoča avtonomno delovanje tudi v primeru, da centralni računalnik, s katerim komunicira in na katerem je nameščena nadzorna programska oprema, ne deluje. Komunikacijski modul omogoča kontrolniku komunikacijo s sosednjim kontrolnikom s pomočjo programabilnih vhodno-izhodnih modulov in s tem posredno delovanje zunanjih naprav, kot so senzorji, električne ključavnice, detektorji, zapornice, trikrake prepreke, dvigala, razsvetljava itd. Za povezavo kontrolnih enot med seboj in naprej s centralnim nadzornim računalnikom (strežnikom) je za obravnavani model identifikacijskega sistema uporabljena komunikacija RS232, RS485 in CAN bus. V asinhronem serijskem komunikacijskem sistemu pa se lahko pojavi tudi tokovna zanka in v zadnjem času še povezave Ethernet TCP/IP.

Kontrolna enota pošilja v računalnik sporočila, ki jih program interpretira kot alarmna ali nealarmna. Nekatera sporočila so samo alarmna, nekatera pa samo nealarmna. Sporočila o neodobrenih prehodih lahko individualno definiramo kot alarmna ali nealarmna.

Slika 10.2: Kontrolna enota ELS

Nadzorni program obdela alarmna in nealarmna sporočila na različne načine. Alarmno sporočilo običajno spremlja zvočni signal ali pa se v primeru tihega alarma samo izpiše v oknu za nadzor sistema. Nealarmna sporočila o odobrenem ali neodobrenem prehodu se sproti shranjujejo v dnevniške datoteke na trdem disku računalnika. Te datoteke sistem uporablja za izdelavo različnih poročil in jih moramo ustrezno arhivirati. Tudi alarmna sporočila se sproti shranjujejo v posebno datoteko na trdem disku. Namen alarmnih sporočil je alarmiranje osebe, odgovorne za nadzor sistema. Tipična alarmna sporočila so: napačna koda objekta, uporabnik ni v bazi podatkov, prepovedana dostopna pravica, prepovedano časovno obdobje, preklicana (blokirana) kartica, kartica ima napačno številko izdaje, vnos napačne kode (PIN), predolgo odprta vrata, nasilno odpiranje vrat itd.

10.1.2.3 RFID brezkontaktna (antenska) enota za identifikacijo

Kot smo že omenili, nam čitalnik kartic omogoča postopek prepoznavanja identitete osebe, ki želi vstopiti v varovan prostor. V nadaljevanju si bomo podrobneje ogledali tako imenovano radiofrekvenčno identifikacijo (RFID) ter enega od njenih principov, tako imenovano proximity tehnologijo, ki je značilna predvsem za sisteme kontrole pristopa. Čitalniki (slika 10.3) so odvisni od identifikacijskih elementov (kontaktni ali brezkontaktni) in lahko omogočajo delovanje na nekaj centimetrov (brezkontaktne kartice na frekvencah 125 KHz in 13,56 MHz) ali več deset metrov (daljinski upravljalniki na frekvenci 433 MHz).

Slika 10.3: Modula za RFID identifikacijo MiFare in TagSys

Pomembno je, da so dovolj robustni zaradi sabotaže in da morebitno poškodovanje čitalnika ne omogoči odprtja vrat. To dosežemo z ločeno krmilno enoto, ki vsebuje krmilno logiko in lokalno podatkovno bazo uporabnikov kartic. Kadar je čitalnik nameščen v okolju z močnim RF šumom oziroma motnjami, se bralno območje močno zmanjša in je še manjše od najmanjših vrednosti, navedenih v tabeli 10.1.

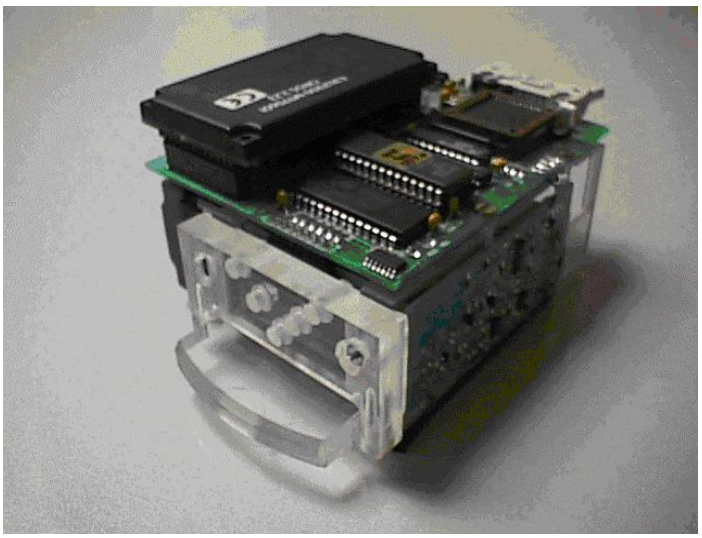
Tabela 10.1: Bralna območja čitalnikov kartic proximity (Elatec, 2011)

	PROXIMITY ČITALNIKI KARTIC – BRALNO OBMOČJE				
Proximity kartice	ProxPoint čitalnik (cm)	MiniProx čitalnik (cm)	ProxPro (cm)	ProxPro Plus (cm)	NT MaxiProx (cm)
Prox	5–7,5	10–14	14–20	20–25,5	40–71
ISO Prox	2,5–5	5–10	10–15	12,5–18	25–45
Duo Prox	2,5–5	5–10	10–15	12,5–18	25–45
Smart Prox	1,2–3,7	3,7–6,2	7,5–12,5	10–15	25–35

Prox Plus	1,2–2,5	2,5–5	5–7,5	7,5–10	20–25
Prox Key	2,5–3,7	2,5–5	2,5–7,5	10–15	15–28

10.1.2.4 MMR kontaktna enota za identifikacijo s čipnimi karticami

Kontaktna tehnologija (slika 10.4) kartične identifikacije (t. i. pametna kartica ali smartcard) je trenutno najbolj razširjena na javnih področjih uporabe (banke, zavarovalnice itd.). Kartico pri uporabi vložimo v čitalno mesto, ki dostopa do njenega mikroprocesorja in pomnilnika prek pozlačenih kontaktov. Zmogljivosti kontaktnih kartic (procesorska moč, pomnilnik, operacijski sistem) so običajno boljše od brezkontaktnih. Identifikacija je sicer počasnejša, vendar bolj zahtevna in s tem varnejša.

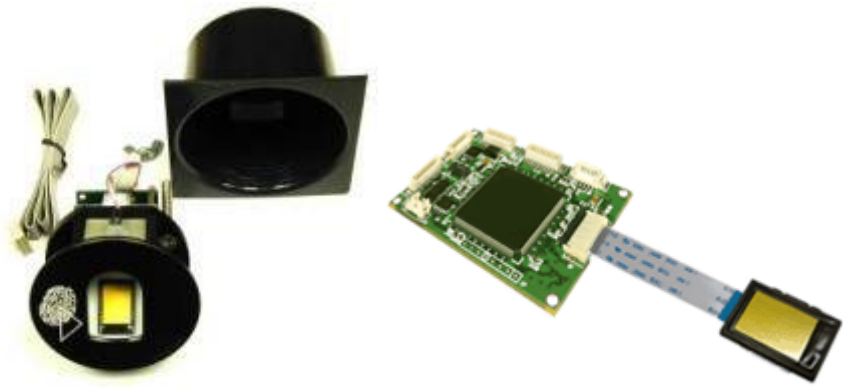


Slika 10.4: Kontaktna tehnologija–MMR kartični čitalec

10.1.2.5 Biometrična enota za identifikacijo na osnovi prstnega odtisa

Za nemene raziskave smo uporabili komercialni biometrični čitalec Suprema (slika 10.5) z mikrokrmilniškim sistemom razvitim v podjetju Metra d.o.o (Krejan, 2002). Algoritem verifikacije temelji na preizkušeni minutiae tehnologiji, ki po podatkih FVC2004 in FVC2006[44] velja za naboljši komercialni algoritem na svetu.

[44] *FVC (Fingerprint Verification Competition). url: http://bias.csr.unibo.it/fvc2006/ (5. 5. 2009)*



Slika 10.5: Suprema biometrični modul za identifikacijo na osnovi prstnega odtisa

10.2 ZAJEM PODATKOV ZA IZRAČUN ZANESLJIVOSTI IN RAZPOLOŽLJIVOSTI

Podatke za izračun pogostosti odpovedi λ in pogostosti zaključkov popravil μ zagotavljata v poglavju 7.1. predstavljen informacijski sistem RCg in programski incident modul. Na voljo sta dva načina zajemanja podatkov: eden se napaja s pomočjo t. i. ročnega vnosa, ki ga prek grafičnega uporabniškega vmesnika informacijskega sistema izvajajo zaposleni v oddelku za nadzor (kakovost) in podporo (servis, inženiring, distributerji), drugi pa je sistemski dnevnik programske opreme, v katerega se sporočila o dogajanju na sistemu ELS zapisujejo avtomatično. Za nadzor in podporo informacijskega sistema družbe je organizirana posebna (dežurna) služba, ki je obenem tudi centralna točka za sprejemanje sporočil o motnjah in zastojih na sistemu ter za obveščanje o njih ter njihovo reševanje. Delovanje službe za nadzor in podporo je tehnično podprto z ustrezno strojno in programsko opremo: vstopne telefonske klice sprejema posebna telefonska centrala, ki omogoča razporejanje dohodnih klicev po strežniških mestih glede na dano postavitev. Dodatna programska oprema omogoča vodenje statistike obnašanja sistema in njegovih najpomembnejših parametrov (število dohodnih in odhodnih klicev v različnih časovnih intervalih, čakalni časi, zavrnjeni klici, statistična poročila za različna pretekla obdobja itd.). Nadzor nad posameznimi deli identifikacijskega sistema avtomatično opravljajo posebni programski moduli in o stanju sistema pošiljajo ustrezna sporočila ali pa posamezne ukaze ročno izvaja operater. Postopki, kako delovati v primeru motenj, zastojev in drugih izrednih situacij, ki se pojavijo v sistemu, so opisani v protokolu službe za nadzor in podporo. V primeru klica o napaki (motnji) mora oseba, ki kliče, podati čim več verodostojnih, nedvoumnih informacij o zaznani motnji, kot so čas pojavitve, čas zaznave, lokacija, oseba, ki je motnjo zaznala, stanje sistema in izvedeni postopki pred pojavitvijo motnje, ob pojavitvi in po njej, vplivi (posledice) na delovanje drugih delov sistema ipd.

Glede na zbrane informacije prevzemnik klica obvesti skrbnika izbranega področja (ki naj bi motnjo tudi odpravil), navedenega v posebni »intervencijski tabeli«. Če odgovorni skrbnik področja ni dosegljiv, prevzemnik klica pokliče njegovega namestnika (glede na intervencijsko tabelo). Glede na kompleksnost motnje oziroma

po naročilu že klicanih dežurnih delavcev obvesti tudi druge dežurne, ki so odgovorni za odpravo motnje. Sodelujoči v odpravljanju motnje obveščajo operaterja o poteku oz. odpravi motnje. V primeru, da motnja ni odpravljena v času izmene operaterja, ta preda potrebne informacije svojemu nasledniku. Potek dogodkov se zapisuje v aplikaciji za vodenje evidence motenj in izpadov identifikacijskega sistema (RCg–QM). Aplikacija je bila zasnovana in razvita v podjetju in je prilagojena posebnostim lastnega informacijskega sistema. Njeno jedro je zgrajeno kot nabor elementov oz. sklopov identifikacijskega sistema, ki so med seboj v značilnih relacijah. Relacije tako opisujejo soodvisnost posameznih programskih in strojnih podsistemov ter njihov medsebojni vpliv v primeru nedelovanja posameznega modula.

Definirani so naslednji moduli (gradniki identifikacijskega sistema):
1. HW (diski, fizične linije),
2. SISTEM (IBM, Tandem, Bkfserver),
3. SISTEMSKI SERVIS (Exchange),
4. APLIKATIVNI SW (vnos podatkov, obdelave, poročila),
5. APLIKACIJA (aplikacija ELS),
6. IDENTIFIKACIJSKO PODROČJE (biometrični čitalnik, kartični čitalnik, kartice).

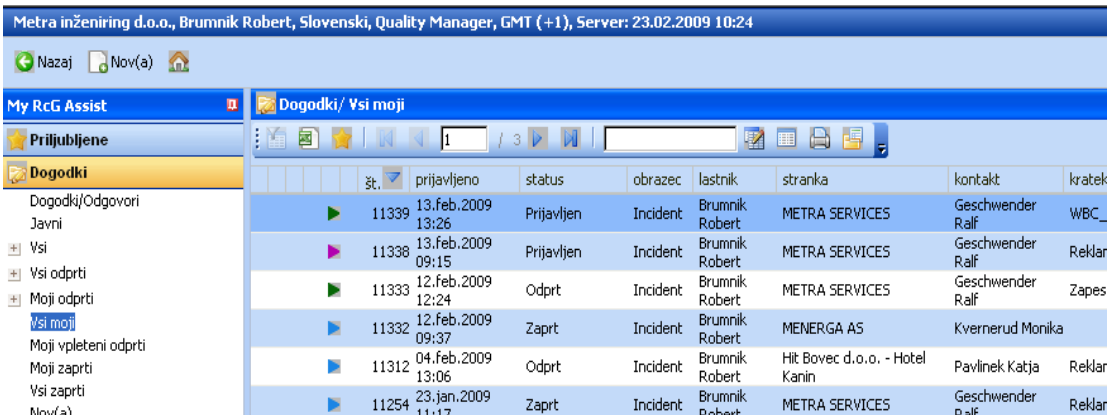
Med elementi so določeni tipi (vrste) odvisnosti:
1. popolna (nedelovanje enega pomeni tudi nedelovanje drugega (odvisnega) elementa),
2. delna (nedelovanje enega pomeni moteno delovanje drugega (odvisnega) elementa),
3. začasna popolna (nedelovanje enega elementa v določenem časovnem intervalu pomeni nedelovanje drugega (odvisnega) elementa) in
4. začasna delna (nedelovanje enega elementa v določenem časovnem intervalu pomeni moteno delovanje drugega (odvisnega) elementa).

Aplikacija za vodenje evidence je namenjena vnosu osnovnih (temeljnih) parametrov, ki določajo motnjo oziroma odpoved sistema (na kateri element se veže odpoved, vrsta odpovedi, čas pojavitve, vzrok odpovedi, čas odprave napake, čas ponovnega delovanja elementa itd.). Iz zajetih podatkov se mesečno pripravljajo poročila o (ne)delovanju sistema, namenjena ravnateljstvu in ukrepom družbe. Prav tako aplikacija omogoča trenutne vpoglede v evidentirane izpade, ki so lahko že odpravljeni oziroma se še vedno vodijo kot aktivni (napaka še ni odpravljena) in bodo kot zaključeni označeni pozneje.

10.2.1 APLIKACIJA ZA VODENJE EVIDENCE MOTENJ IN IZPADOV IDENTIFIKACIJSKEGA SISTEMA

Aplikacija, prikazana na sliki 11.1, se za kratke časovne intervale opazovanja odpovedi sistema ne izkazuje kot najbolj ustrezna za zajem in analizo podatkov, potrebnih za izračune v modelu, ki ga obravnava doktorsko delo. Razlog je predvsem v precej velikem tolerančnem območju zapisanih časov odpovedi in njihove odprave, saj se ti zapisujejo ročno, pri čemer je zaradi »človeškega dejavnika« mogoča nenatančnost. Aplikacija je bila namreč prvotno zasnovana kot morebitna bodoča baza znanja, s katero bi z ustreznim dodatnim razvojem omogočali kakovostnejšo, lažjo in hitrejšo analizo napake ter s tem njeno hitrejšo odpravo. Hkrati bi znatno zmanjšali število potrebnih klicev skrbnikov posameznih

področij, saj bi se operaterji o ustreznih akcijah lažje in večkrat odločali sami. V nadaljevanju bi z ustreznim razvojem programskih vmesnikov lahko omogočili avtomatični zajem verodostojnih podatkov iz sistemskega dnevnika centralnega računalnika (sistemski dnevnik je prikazan v poglavju 11.1.2).



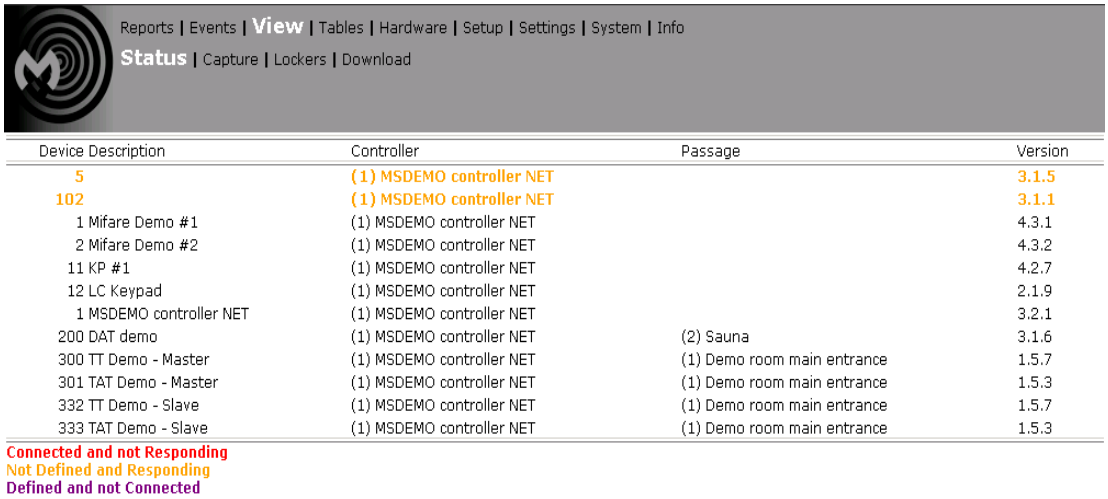
Slika 10.6: Ekranska maska za vnos podatkov o izrednih dogodkov

Kljub temu so podatki iz te baze uporabljeni pri izračunu karakteristik odpovedi, saj za daljše preteklo obdobje ni na voljo podatkov, zajetih s sistemskim dnevnikom. S pomočjo prikazane zaslonske maske uporabnik določi nov izpad in poda ustrezne parametre. Glavni parametri so naslednji:

- Posredovanje na identifikacijskemu sistemu – tip elementa (sklopa identifikacijskega sistema), na katerem je prišlo do motnje oziroma izpada delovanja.
- Vzrok posredovanja – uporabnik navede vzrok posredovanja.
- Tipska vrsta napake – uporabnik navede preddefinirano vrsto napake (SW, HW).
- Začetek – čas začetka odpovedi.
- Vzpostavitev – čas pričetka ponovnega delovanja.
- Vir prijave – kdo je skrbniku prijavil napako.

10.2.2 SISTEMSKI DNEVNIK IDENTIFIKACIJSKEGA SISTEMA

Za naše potrebe (izračun pogostosti odpovedi in pogostosti zaključkov popravil) bomo iz sistemskega dnevnika izbrali del sistemskih sporočil, ki govorijo o prenehanju delovanja posameznih procesov in njihovi ponovni oživitvi. Na sliki 11.2 je prikazan izsek sistemskega dnevnika identifikacijskega sistema.



Slika 10.7: Sistemski dnevnik identifikacijskega sistema pristopne kontrole

10.3 WEIBULLOV MODEL ZA DOLOČANJE OCEN KARAKTERISTIK ZANESLJIVOSTI

Razpoložljivost identifikacijskega sistema je ena najpomembnejših karakteristik učinkovitosti identifikacijskega sistema, ki vpliva tako na njegovo varnost kot učinkovitost. Povečanje zanesljivosti sistema pomeni manj popravil, krajši čas identifikacije in s tem večjo razpoložljivost. Vgrajevanje zanesljivosti med razvojem in njeno zagotavljanje med uporabo sistema zahtevata poznavanje metod, tehnik in teorije zanesljivosti ter njihovega medsebojnega vpliva.

Za mero zanesljivosti identifikacijskih sistemov in njihovih sestavnih delov se uporablja cela vrsta karakteristik. Nekatere so časovne funkcije, druge pa predstavljajo časovna povprečja. Od postavljenih ciljev, izbrane metode analize in dosegljivosti podatkov je odvisno, katere karakteristike so uporabimo v posameznih primerih.

Karakteristike zanesljivosti temeljijo na časih do odpovedi in časih do zaključka popravil. Oba časa sta naključni veličini, ki ju bomo označili s simbolom t_i. Uporabili bomo cenilke osnovnih karakteristik zanesljivosti na osnovi definicij podanih v teoretičnem delu:

- $MTTF$– povprečni čas do odpovedi,
- $MTTR$– povprečni čas do zaključka popravil,
- $R(t)$ – funkcija zanesljivosti,
- $\lambda(t)$ – trenutna pogostost odpovedi.

10.4 KARAKTERISTIKE ZANESLJIVOSTI ČITALNIKA KARTIČNEGA SISTEMA ZA IDENTIFIKACIJO

Odpovedi, ki smo jih upoštevali pri določitvi karakteristik $MTTF$, $MTTR$ (tabela 10.2) kartičnega/RFID čitalnika:

- napake v delovanju programske opreme (nezmožnost branja RFID identifikatorja) in
- napake v delovanju strojne opreme (odpoved kartičnega/RFID čitalnika, nezmožnost programiranja kartičnega/RFID identifikatorja ali mikročipov).

Tabela 10.2: Podatki za določitev ocene $MTTF–MTTR$ za kartični sistem

Ser. št.	Čas do prve odpovedi (dni)	Čas do druge odpovedi (dni)	Čas do tretje odpovedi (dni)	Povprečna vrednost (dni)
22345	13	139	48	76,5
22359	27	106	42	
22346	54	106	58	
22347	54	110	83	
22348	72	96	73	
22349	90	82	88	
22360	116	28	93	
22375	87	29	115	
22381	51	40	145	
22387	60	36	155	
Ser. št.	Trajanje (dni) prvega servisa	Trajanje (dni) drugega servisa	Trajanje (dni) tretjega servisa	Povprečna vrednost (dni)
22345	1	1	1	2,1
22359	1	1	1	
22346	2	3	2	
22347	2	0	3	
22348	5	3	7	
22349	1	1	1	
22360	4	1	2	
22375	4	2	1	
22381	4	3	4	
22387	1	0	1	
Ser. št.	Čas do ponovnega zagona (dni)	Čas do ponovnega zagona (dni)	Čas do ponovnega zagona (dni)	Povprečna vrednost (dni)
22345	14	140	49	78,6
22359	28	107	43	
22346	56	109	60	
22347	56	110	86	
22348	77	99	80	
22349	91	83	89	
22360	120	29	95	
22375	91	31	116	
22381	55	43	149	
22387	61	36	156	

Rangirane vrednosti (tabela 10.3) časov do odpovedi kartičnega sistema $(t_i; i = 1,2,3)$:

Tabela 10.3: Rangirani časi do odpovedi za kartični sistem

Serijska številka kartičnega modula	Čas do odpovedi (dni)
22345	13
22359	27
22360	28
22375	29
22387	36
22381	40
22359	42
22345	48
22381	51
22346	54
22347	54
22346	58
22387	60
22348	72
22348	73
22349	82
22347	83
22375	87
22349	88
22349	90
22360	93
22348	96
22359	106
22346	106
22347	110
22375	115
22360	116
22345	139
22381	145
22387	155

10.5 KARAKTERISTIKE ZANESLJIVOSTI ČITALNIKA BIOMETRIČNEGA SISTEMA

Odpovedi, ki smo jih upoštevali pri določitvi karakteristik *MTTF*, *MTTR* biometričnega sistema (tabela 10.4):

- napake v delovanju programske opreme (nezmožnost branja vzorca),
- napake v delovanju strojne opreme (biometrični čitalnik, PCBs[45]) in

[45] *PCB (printed circuit board); ELS matična plošča*

- napake zaradi nastavitev odčitavanja senzorjev: *FAR*, *FRR*.

Tabela 10.4: Podatki za določitev ocene *MTTF–MTTR* za biometrični sistem

Ser. št.	Čas do prve odpovedi (dni)	Čas do druge odpovedi (dni)	Čas do tretje odpovedi (dni)	Povprečna vrednost (dni)
36365	53	89	88	88,8
36359	60	106	73	
36366	87	106	88	
36364	86	161	88	
36368	102	130	13	
36369	99	102	98	
36360	56	150	93	
36345	57	90	126	
36381	81	52	117	
36384	90	65	105	
Ser. št.	Trajanje (dni) prvega servisa	Trajanje (dni) drugega servisa	Trajanje (dni) tretjega servisa	Povprečna vrednost (dni)
36365	1	1	1	1,2
36359	0	1	0	
36366	1	3	2	
36364	1	0	1	
36368	1	3	1	
36369	2	1	1	
36360	2	1	1	
36345	3	1	1	
36381	2	1	1	
36384	2	0	1	
Ser. št.	Čas do ponovnega zagona (dni)	Čas do ponovnega zagona (dni)	Čas do ponovnega zagona (dni)	Povprečna vrednost (dni)
36365	56	90	89	90,1
36359	60	105	73	
36366	88	107	90	
36364	85	161	89	
36368	103	133	16	
36369	101	103	99	
36360	58	151	96	
36345	60	91	127	
36381	83	53	118	
36384	92	65	106	

Rangirane vrednosti (tabela 10.5) časov do odpovedi biometričnega sistema $(t_i; i = 1,2,3)$:

Tabela 10.5: Rangirani časi do odpovedi za biometrični sistem

Serijska številka biometričnega modula	Čas do odpovedi (dni)
36368	13
36381	52
36365	53
36360	56
36345	57
36359	60
36384	65
36359	73
36381	81
36364	86
36366	87
36365	88
36366	88
36364	88
36365	89
36384	90
36345	90
36360	93
36369	98
36369	99
36368	102
36369	102
36384	105
36359	106
36366	106
36381	117
36345	126
36368	130
36360	150
36364	161

10.6 DOLOČITEV POGOSTOSTI ODPOVEDI PRI KARTIČNEM IN BIOMETRIČNEM ČITALNEM MODULU IDENTIFIKACIJSKEGA SISTEMA

Zanesljivost bralnega modula kartičnega sistema popišemo s trenutno pogostostjo odpovedi $\lambda(t)$, ki jo obravnavamo v celotnem življenjskem obdobju:

- obdobju zgodnjih odpovedi,
- obdobju normalnega delovanja in v
- obdobju staranja in izrabe.

Čase do odpovedi vzorcev kartičnega identifikacijskega sistema in pripadajoče točkaste ocene preračunamo s porazdelitvenim zakonom beta:

$$\hat{F}(t_i) = \frac{i - 0,3}{N_0 + 0,4} \quad za \quad i = 1, 2, \ldots, N_0$$

in jih podamo v tabeli 10.6.

Tabela 10.6: Časi do odpovedi in pripadajoče točkaste ocene funkcije $F(t)$ za kartični sistem

ČASI DO PRVE ODPOVEDI										
i	1	2	3	4	5	6	7	8	9	10
t_i (dni)	13	27	51	54	54	60	72	87	90	116
F_i	7	16	26	36	45	55	64	74	84	93
ČASI DO DRUGE ODPOVEDI										
i	1	2	3	4	5	6	7	8	9	10
t_i (dni)	28	29	36	40	82	96	106	106	110	139
F_i	7	16	26	36	45	55	64	74	84	93
ČASI DO TRETJE ODPOVEDI										
i	1	2	3	4	5	6	7	8	9	10
t_i (dni)	42	48	58	73	83	88	93	115	145	155
F_i	7	16	26	36	45	55	64	74	84	93

Za čase do prve odpovedi je β=1,8 in η=72, medtem, ko sta za čase do druge odpovedi parametra β=1.9 in η=86,8. Za čase do tretje odpovedi sta vrednosti parametrov β=2,6 in η=101,17. Časi do odpovedi primerkov vzorca biometričnega identifikacijskega sistema in pripadajoče točkaste ocene za $F(t)$ (tabela 10.7):

Tabela 10.7: Časi do odpovedi in pripadajoče točkaste ocene funkcije $F(t)$ za biometrični sistem

ČASI DO PRVE ODPOVEDI										
i	1	2	3	4	5	6	7	8	9	10
t_i (dni)	53	56	57	60	81	86	87	90	99	102
F_i	7	16	26	36	45	55	64	74	84	93
ČASI DO DRUGE ODPOVEDI										
i	1	2	3	4	5	6	7	8	9	10
t_i (dni)	52	65	89	90	102	106	106	130	150	161
F_i	7	16	26	36	45	55	64	74	84	93
ČASI DO TRETJE ODPOVEDI										
i	1	2	3	4	5	6	7	8	9	10
t_i (dni)	13	73	88	88	88	93	98	105	117	126
F_i	7	16	26	36	45	55	64	74	84	93

Za čase do prve odpovedi je β=4,6 in η=72, medtem, ko sta za čase do druge odpovedi parametra β=3,23 in η=117,2. Za čase do tretje odpovedi sta vrednosti parametrov β=2 in η=101.

Ob predpostavki, da so časi do odpovedi eksponentno porazdeljeni, pare (t_i, F_i) iz tabel 10.6 in 10.7 združimo v tabeli 10.8 ter s pomočjo programske opreme Weibull++7 določimo oceni parametrov β in η za oba sistema.

Tabela 10.8: Časi do odpovedi in pripadajoče ocene funkcije F_i za kartični in biometrični modul

kartični modul		
i	t_i (dni)	F_i
1	13	2,3
2	27	5,6
3	28	8,9
4	29	12,2
5	36	15,5
6	40	18,8
7	42	22,0
8	48	25,3
9	51	28,6
10	54	31,9
11	54	35,2
12	58	38,5
13	60	41,8
14	72	45,1
15	73	48,4
16	82	51,6
17	83	54,9
18	87	58,2
19	88	61,5
20	90	64,8
21	93	68,1
22	96	71,4
23	106	74,7
24	106	78,0
25	110	81,3
26	115	84,5
27	116	87,8
28	139	91,1
29	145	94,4
30	155	97,7

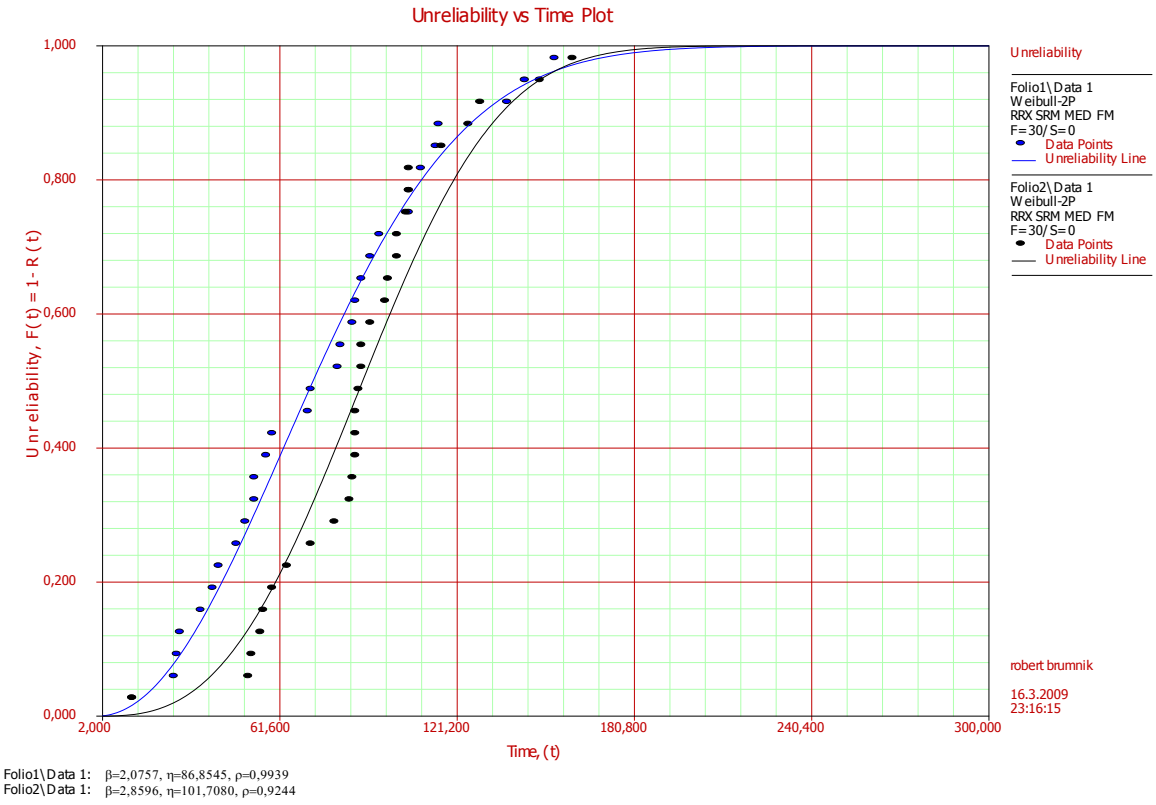
biometrični modul		
i	t_i (dni)	F_i
1	13	2,3
2	52	5,6
3	53	8,9
4	56	12,2
5	57	15,5
6	60	18,8
7	65	22,0
8	73	25,3
9	81	28,6
10	86	31,9
11	87	35,2
12	88	38,5
13	88	41,8
14	88	45,1
15	89	48,4
16	90	51,6
17	90	54,9
18	93	58,2
19	98	61,5
20	99	64,8
21	102	68,1
22	102	71,4
23	105	74,7
24	106	78,0
25	106	81,3
26	117	84,5
27	126	87,8
28	130	91,1
29	150	94,4
30	161	97,7

Ob upoštevanju vseh časov do odpovedi za kartični sistem dobimo oceni β=2,08 in η=86,85 medtem, ko sta za biometrični sistem oceni parametrov β=2,86 in η=101,71. Izračunana parametra β in η sta le točkasti oceni in ne natančni teoretični vrednosti, saj imamo opravka le z omejenim vzorcem. Zato navadno

podajamo intervalno oceno z 90 % zaupanjem (na kratko 90 % IZ); npr. če za parameter določimo spodnjo in zgonjo mejo, to pomeni, da lahko pričakujemo z verjetnostjo 90 %, da je prava vrednost parametra res med obema mejama.
Točkaste ocene parametra β (slika 10.8 in 10.9) nakazujejo na obdobje staranja oz. izrabljenost kartičnega identifikacijskega sistema (β=2,08) in prav tako biometričnega sistema (β=2,86).

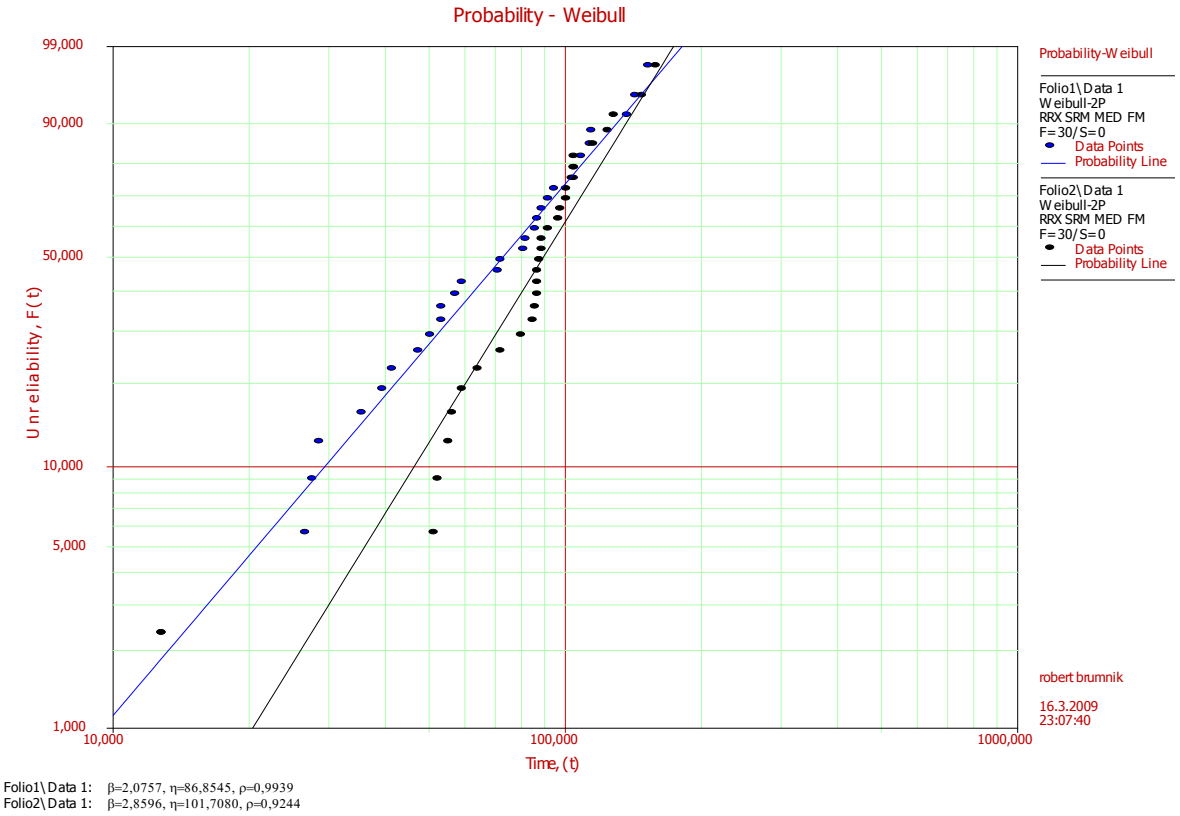
Za določanje karakteristik zanesljivosti smo uporabili Weibullov model, ki je uporaben tudi za primere, ko $\lambda(t)$ ne moremo ponazoriti s konstanto funkcijo. Za dobljene meritve bomo izkoristili prednost Weibullove analize ki, zagotavlja preprosto grafično metodo. Z analizo bomo zagotovili (z razumno napako analize) dovolj dobre ocene parametrov porazdelitve kljub majhnim vzorcem (v našem primeru trideset kosov biometričnih in kartičnih modulov). Dobljene rešitve nam omogočijo zgodnjo identifikacijo znakov možnih problemov, s čimer lahko preprečimo resnejše sistemske odpovedi in predvidimo vzdrževalni cikel (povečamo razpoložljivost sistema). V raziskavi smo z relativno majhnim vzorcem omogočili tudi stroškovno učinkovit preskus karakteristik delovanja. Preskušanje je končano, ko opazovani sistem odpove (nenadna odpoved) v vsaki od treh skupin (prvi modul vsake serije) sestavnih delov (kartični, biometrični) in pričnemo z Weibullovo analizo.

Graf na sliki 10.8 predstavlja časovni funkciji nezanesljivoti za kartični (modra linija) in biometrični sistem (črna linija), ki predstavljata verjetnost, da sistem odpove v časovnem intervalu med 0 in 180 dni. Opazujemo množico primerkov biometričnega in kartičnega sistema/modula in določimo ocene za funkcijo nezanesljivosti. Iz grafa je razvidno, da za 40% nezanesljivost nastopi obdobje odpovedi kartičnega sistema v šesdesetih dneh medtem, ko za biometrični sistem pri enakem odstotku nezanesljivosti to obdobje nastopi v osemdesetih dneh. Za 80% nezanesljivost nastopi obdobje odpovedi za kartični sistem v stodesetih dneh. Za enako stopnjo nezanesljivosti pa se obdobje odpovedi za biometrični sistem pojavi v stodvajsetih dneh. Sklepamo, da v celotnem obdobju življenskega cikla za različne stopnje nezanesljivosti obdobje odpovedi in izraba biometričnega sistema, nastopi v kasnejšem obdobju.



Slika 10.8: Primerjalna grafika funkcije nezanesljivosti $F(t)$ v odvisnosti od časa za kartični in biometrični sistem

Na sliki 10.9 pokažemo grafiko funkcije nezanesljivosti, ki predstavlja linearizacijo krivulj iz slike 10.8. Abscisna os diagrama podaja čase do odpovedi biometričnega sistema. Parameter staranja v našem primeru je čas delovanja. Ordinatna os diagrama predstavlja oceno nezanesljivosti. Za opredelitev Weibull linije sta značilna parameter oblike β in karakteristična življenska dobe η. Merjenje časov do odpovedi gradnikov kartičnega in biometričnega sistema, da karakteristične linije iz katerih je razvidno, da so časi do odpovedi biometričnega sistema daljši.

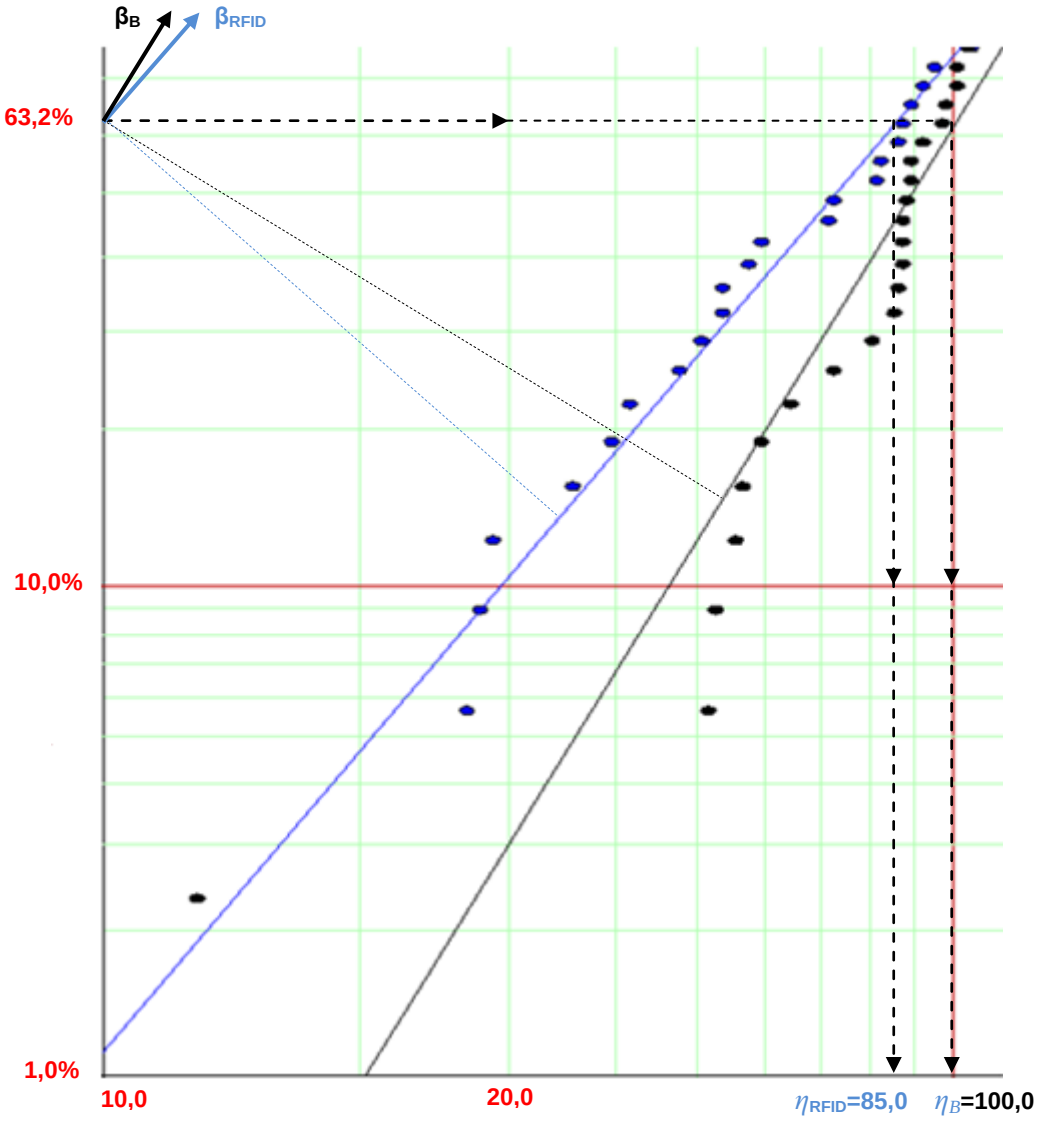


Slika 10.9: Primerjalna grafika funkcije nezanesljivosti $F(t)$ kartičnega in biometričnega sistema

Pri grafičnem določanju (slika 10.10) karakteristične življenske dobe (η) izhajamo iz ordinatene točke $F(t)$=63,2%, vlečemo ravno vodoravno črto, dokler ne sekamo eksperimentalne premice. Parameter η določimo kot projekcijo presečišča na abscisno os in izhaja iz formulacije:

$$Q(T) = 1 - e^{-(\frac{\eta}{\eta})} = 1 - e^{-(-1)} = 0{,}632 = 63{,}2\%.$$

V primeru, da je β=1, je vrednost na abscisi ocena poprečnega časa do odpovedi. Za naš primer je ta ocena $\hat{\eta}$=85 dni za kartični sistem in $\hat{\eta}$=100 dni za biometrični sistem. Ob določitvi parametra β lahko nadalje izračunavamo oceno funkcije znesljivosti za poljuben čas.



Slika 10.10: Grafično določanje karakteristične življenske dobe η

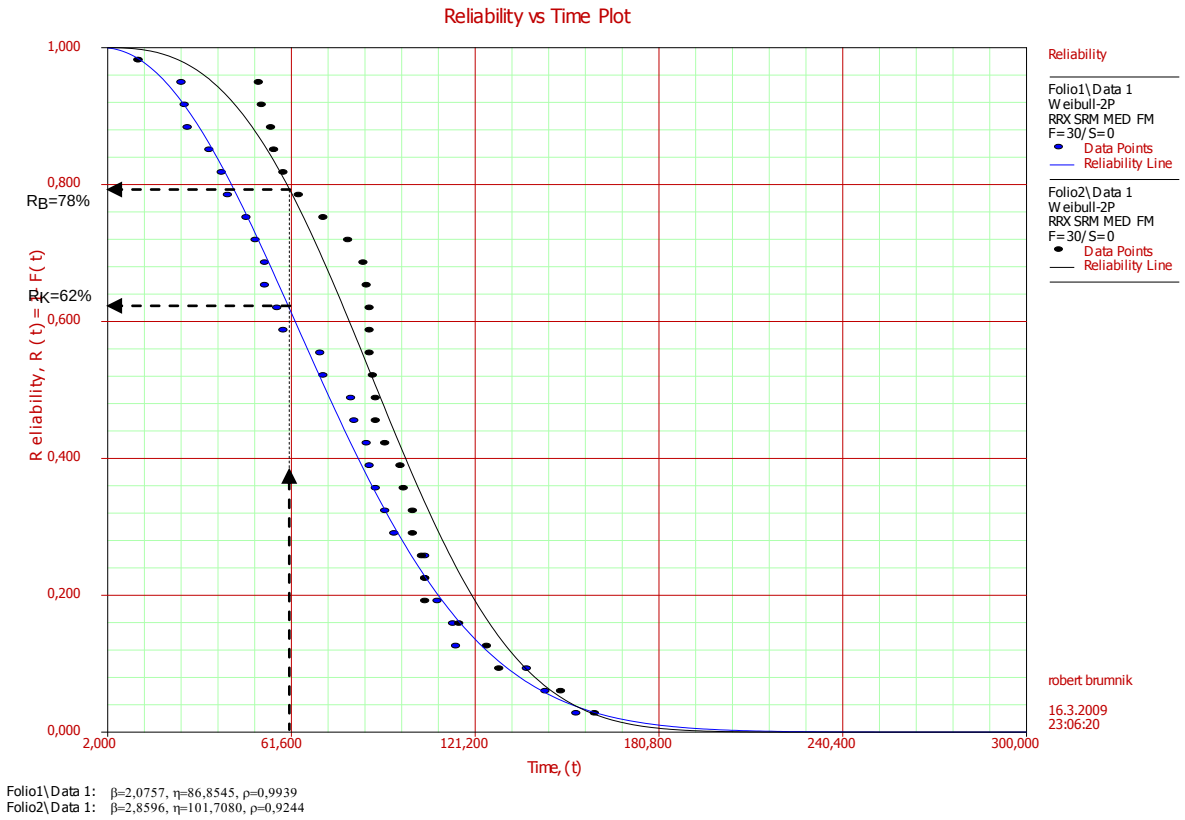
Funkcijo zanesljivosti za identifikacijski sistem lahko določimo grafično s preračunavanjem na osnovi ocen parametrov β in $\hat{\eta}$ po formuli:

$$R(t) = 1 - e^{-(\frac{t}{\eta})^{\beta}},$$

ali s programsko opremo Weibull++7, kjer na osnovi vnosa časov do odpovedi rezultate podamo grafično (slika 10.11):

- funkcija zanesljivosti $R(t)$ za kartični sistem pri β=2,08 in η=86,85 (modra krivulja) ter
- funkcija zanesljivosti $R(t)$ za biometrični sistem pri β=2,86 in η=101,70 (črna krivulja).

Iz grafike lahko povzamemo, da je za isti časovni presek (npr.: t=61,6 dni) karakteristika zanesljivosti $R(t)$=0,78 (78%) za biometrični sistem, medtem, ko je karakteristika zanesljivosti kartičnega sistema $R(t)$=0,62 (62%) za isti časovni presek. Zaključimo lahko, da so biometrični sistemi v opazovanem intervalu zaneslivejši od kartičnega identifikacijskega sistema.

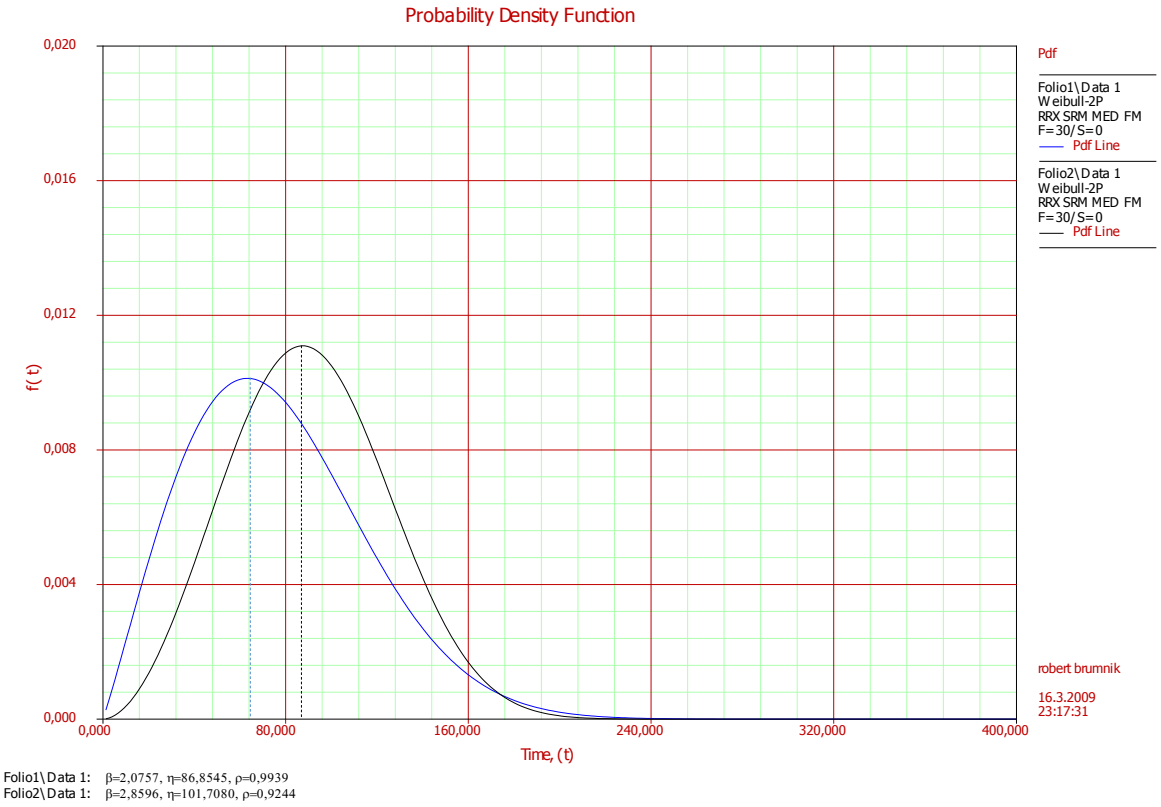


Slika 10.11: Primerjalna grafika funkcije zanesljivosti $R(t)$ kartičnega in biometričnega sistema

Pri praktični izvedbi preskusa zanesljivosti, je funkcija verjetnostne porazdelitve, redko pravilne zvončaste oblike. Za podatke raziskave sta prikazani krivulji (slika 10.12) rahlo nagnjeni:

- funkcija gostote verjetnosti za čase do odpovedi $f(t)$ za kartični sistem pri β=2,08 in
- funkcija gostote verjetnosti za čase do odpovedi $f(t)$ za biometrični sistem pri β=2,86.

Funkcija gostote verjetnosti za čas do odpovedi kartičnega sistema doseže ekstrem pri η_K=70 dneh. Pri istih pogojih preskušanja je gostota verjetnost za biometrični sistem dosežena pri η_B=88 dneh.

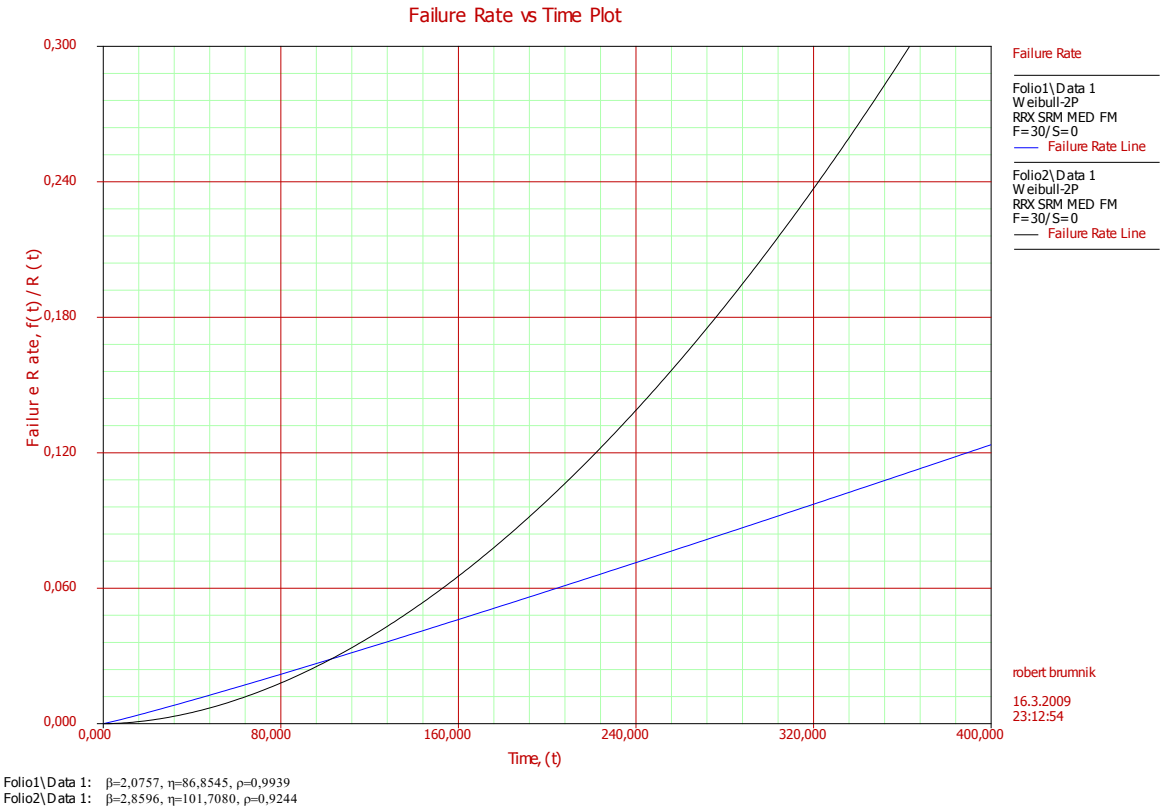


Slika 10.12: Primerjalna grafika funkcije gostote verjetnosti za čas do odpoved $f(t)$ kartičnega in biometričnega sistema

Krivulji trenutne pogostosti odpovedi primerjanih sistemov (biometrični in kartični) nam pokažeta pričakovano število odpovedi v časovni enoti (slika 10.13):

- trenutna pogostost odpovedi $\lambda(t)$ za kartični sistem pri β=2,08 in
- trenutna pogostost $\lambda(t)$ za biometrični sistem pri β=2,86.

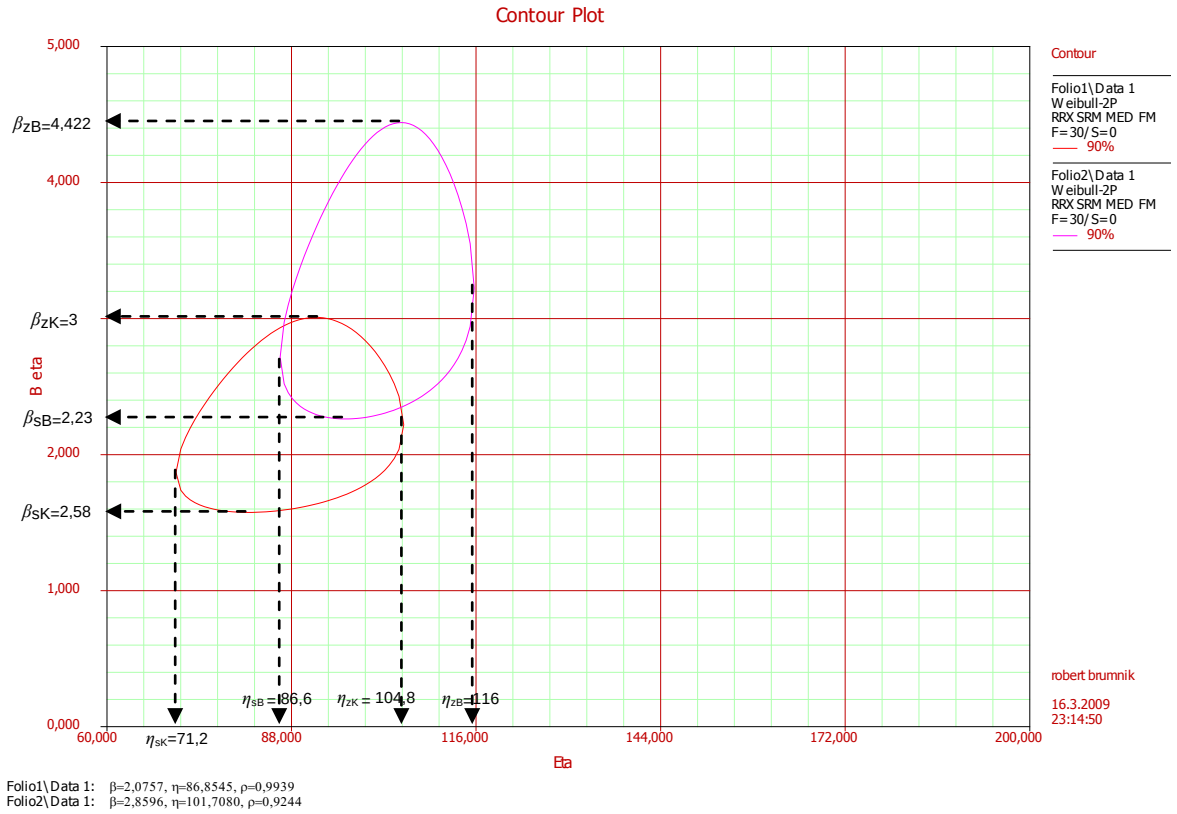
Na osnovi grafike ugotavljamo, da trnutna pogostosti odpovedi za biometrični sistem v obdobju staranja narašča hitreje od kartičnega sistema.



Slika 10.13: Primerjalna grafika trenutne pogostosti odpovedi $\lambda(t)$ kartičnega in biometričnega sistema

Razliko v karakteristikah zanesljivosti opazovanih sistemov ugotovljamo na osnovi analize naborov podatkov o odpovedih s statističnim orodjem Weibull++. Metodologija nam koristi tudi za primer izboljševanja zanesljivosti sistema, ko želimo ugotoviti ali smo z določeno spremembo (ukrepom), ki jo implementiramo v sistem, dosegli izboljšavo zanesljivosti.

Na osnovi naborov podatkov kartičnega in biometričnega sistema ugotavljamo, da se dva podatkovna nabora za β in η bistveno razlikujeta pri 90% stopnji zaupanja (slika 10.14). Za naš primer raziskave je to pričakovano, saj testiramo zanesljivost dveh različnih modulov sistema in je posledično narava odpovedi različna. Zgornja in spodnja meja parametra oblike za biometični sistem sta β_{zB}=4,42, β_{sB}=2,23 in η_{zB}=116, η_{sB}=86,6 ter za kartični sistem β_{zK}=3,0, β_{sK}=2,58 in η_{zK}=104,8, η_{sK}=71,2. Grafika kaže, da je uporaba biometrije bolj zanesljiva.

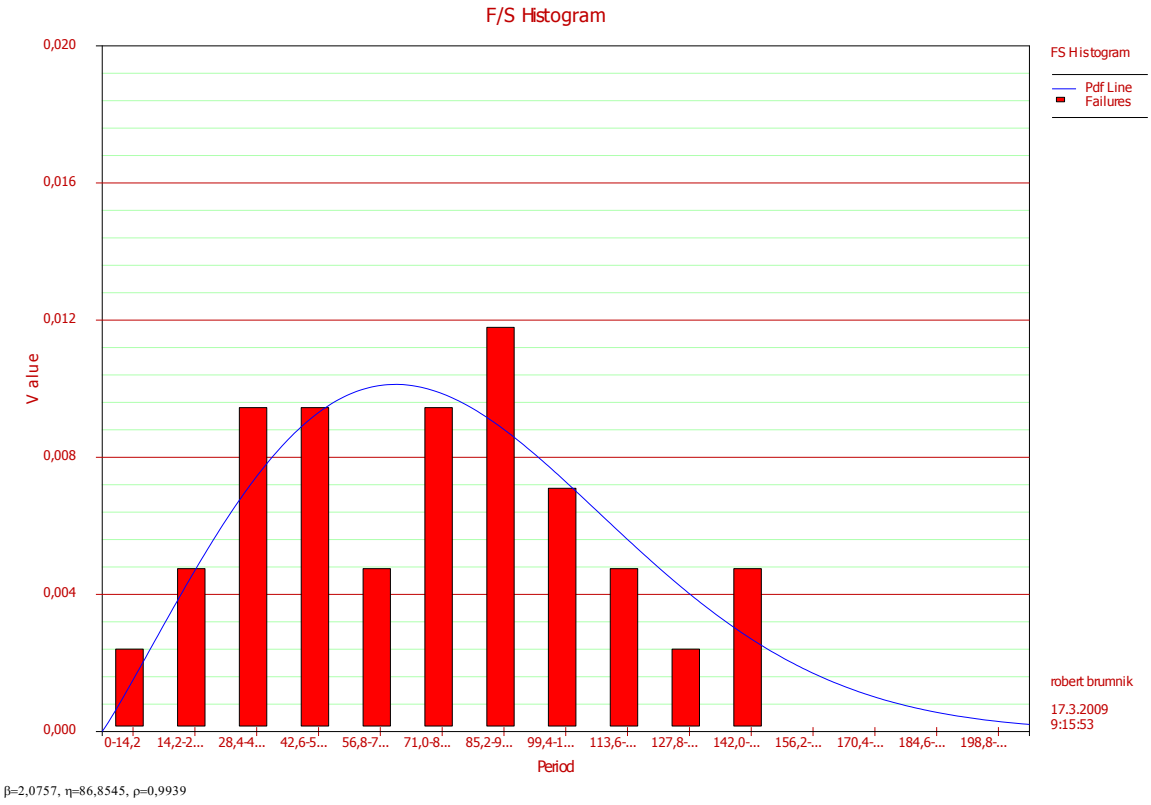


Slika 10.14: Primerjalna grafika obsega parametrov β in η kartičnega in biometričnega sistema

Histogram na sliki 10.15 prikazuje frekvenco odpovedi za enajst štirinajstdnevnih intervalov kartičnega sistema. Frekvence odpovedi so podane za celotno obdobje opazovanja sistema pri čemer je največja frekvenca odpovedi dosežena v sedmem intervalu. Modra linija prikazuje Weibullovo porazdelitveno funkcijo za β=2,08 in η=86,85.

Po določenem obdobju izvajanja poizkusa nastopi staranje oz.obraba preskušanega kartičnega sistema. V tem obdobju je $\lambda(t)$ naraščajoča, funkcija $f(t)$ pa dobi značilno kopasto obliko.

Relavantni karakteristiki v tem obdobju sta povprečna življenska doba Θ in standardni odmik od življenske dobe σ.



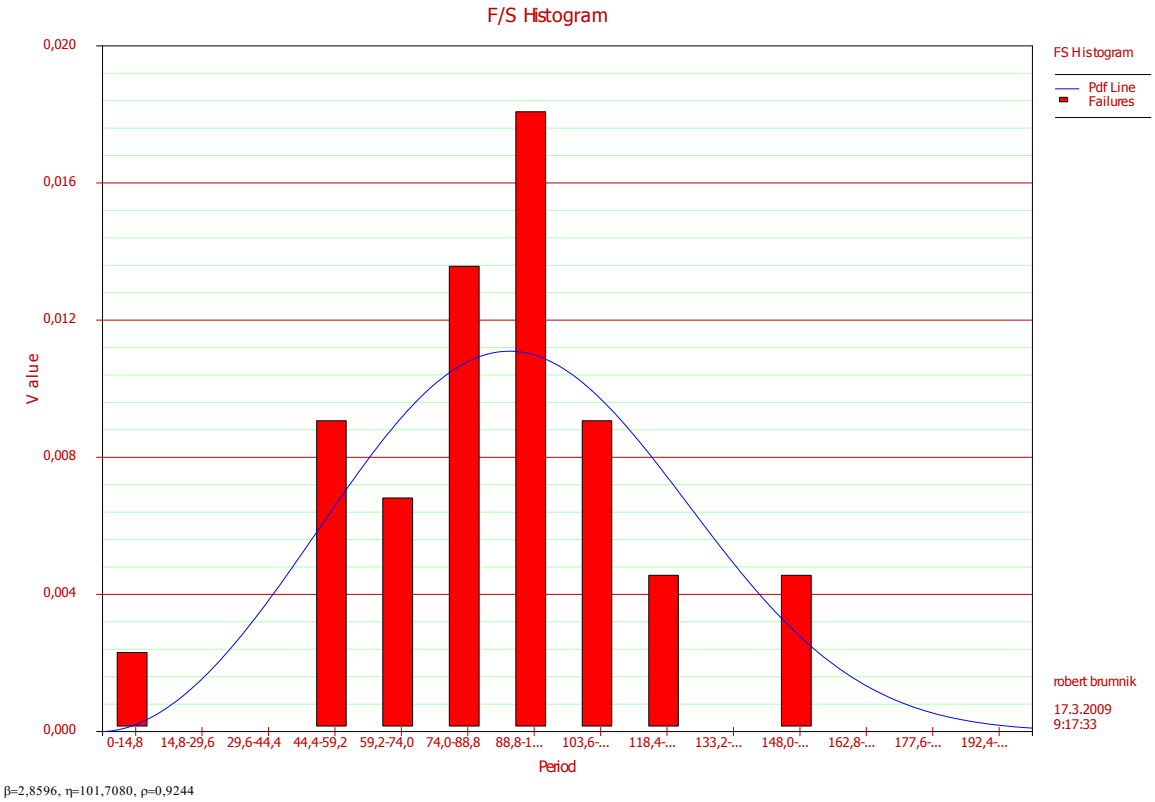
Slika 10.15: Histogram za kartični identifikacijski sistem pri β= 2,0757

Histogram na sliki 10.16 prikazuje frekvenco odpovedi za enajst štirinajstdnevnih intervalov biometričnega sistema. Frekvence odpovedi so porazdeljene za celotno obdobje delovanja sistema pri čemer je največja frekvenca odpovedi dosežena v sedmem intervalu. Modra linija prikazuje Weibullovo funkcijo za β=2,86 in η=101,71.

Po določenem obdobju izvajanja poizkusa nastopi obdobje staranja/obrabe. V tem obdobju je $\lambda(t)$ naraščajoča, funkcija $f(t)$ pa dobi značilno kopasto obliko.

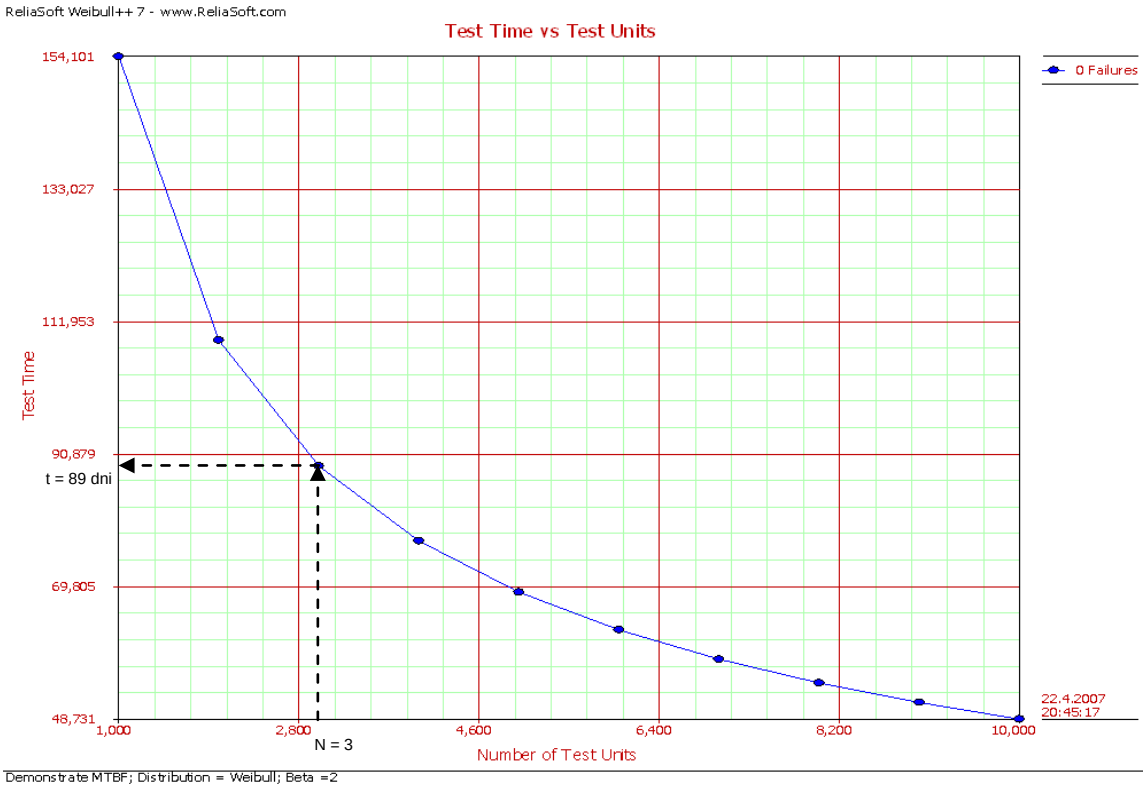
Relavantni karakteristiki v tem obdobju sta povprečna življenska doba Θ in standardni odmik od življenske dobe σ.

S primerjavo histogramov za kartični in biometrični sistem ugotavljamo, da najvišja frekvenca verjetnostne gostote odpovedi za biometrični sistem nastopi kasneje kot za kartični sistem. Pri preskušanju sistemov moramo upoštevati tudi dejstvo, da gre pri biometriji za relativno novo tehnologijo in je nekaj odpovedi nastalo zaradi nepravilnih nastavitev parametrov, ki niso neposredna posledica staranja sistema.



Slika 10.16: Histogram za biometrični identifikacijski sistem pri β= 2,8596

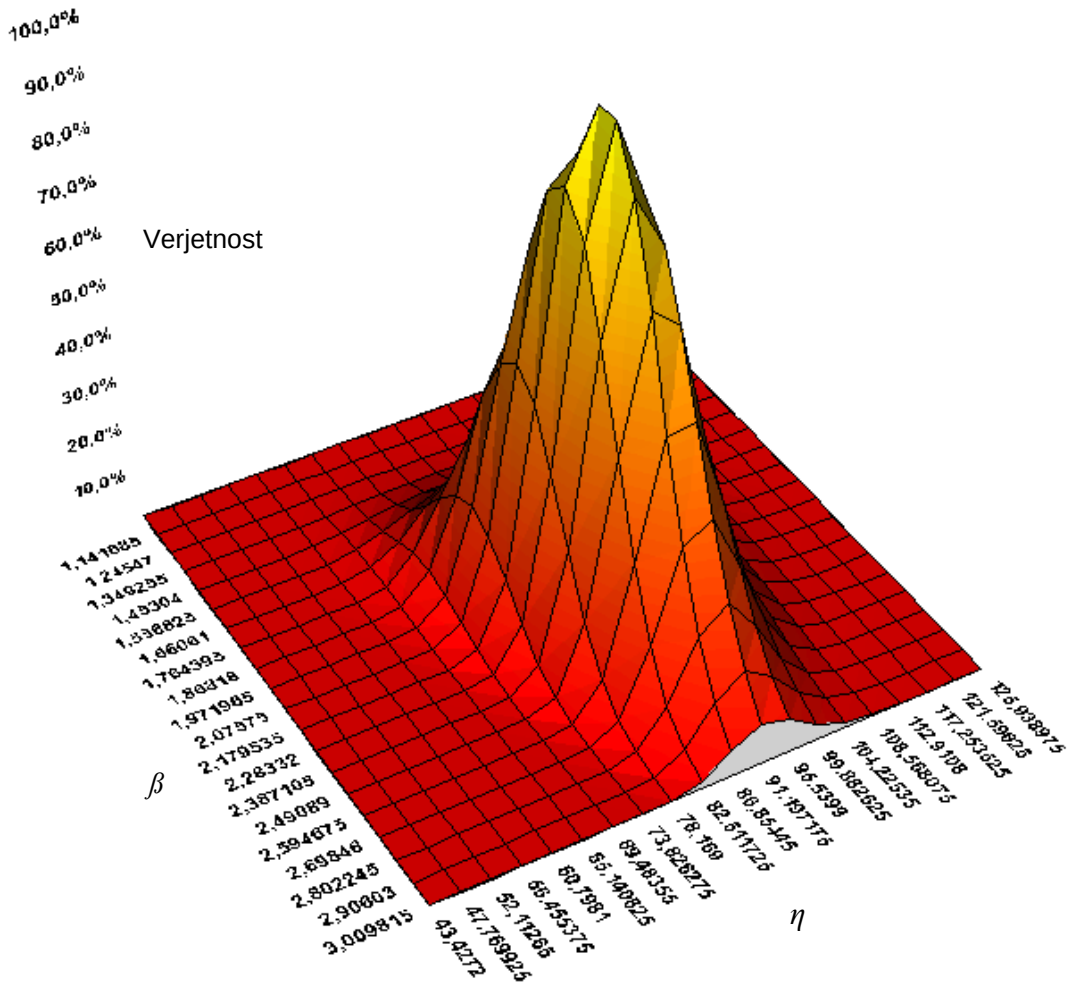
Grafika na sliki 10.17 prikazuje testni plan za opazovani sistem za strategijo 0 napak pri parametru β=2. Potreben čas testiranja sistema, v kolikor v testni plan vključimo tri testne enote, je 89 dni. Z večanjem nabora testnih enot se potrebna dolžina testiranja ustrezno zmanjšuje in obratno, če vključimo v testni plan manjše število modulov namenjenih za preverjanje zanesljivosti, se čas testiranja ustrezno podaljša. V kolikor bi testirali 1 modul se čas testiranja podaljša na 154 dni.



Slika 10.17: Potreben čas testiranja v odvisnosti od števila testnih enot za strategijo 0 napak pri β = 2

Bolj pregledno sliko časovnega spreminjanja jakosti odpovedi pa dobimo, če podatke prikažemo v 3D grafiki, kjer modeliramo parametre β, η in verjetnost odpovedi preskušanih sistemov.

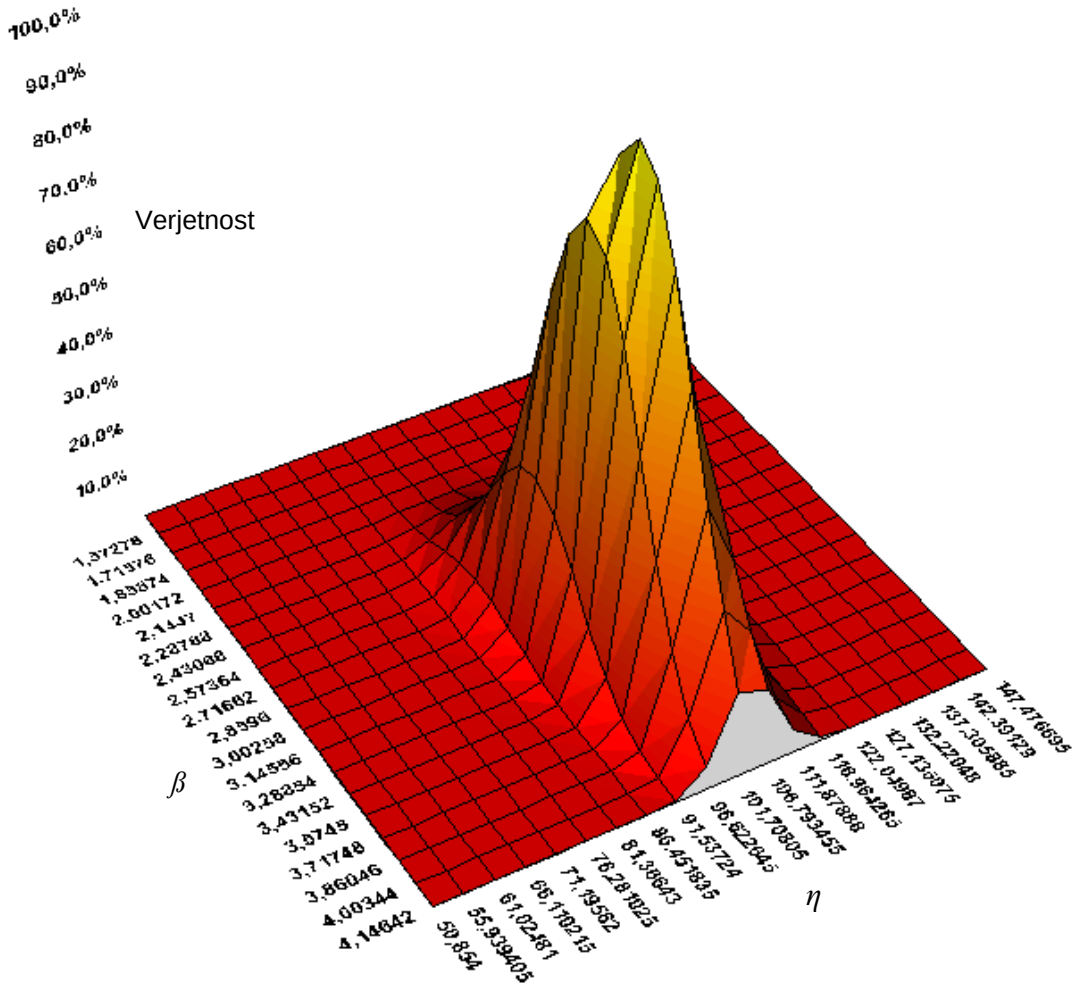
Z Weibull++7 modelirajmo verjetnostno gostoto za čas do odpovedi za kartični sistem z Weibullovim porazdelitvenim zakonom s parametri β in η (slika 10.18). Ob 100% verjetnosti nastopi odpoved za kartični sistem pri β=2,1 in η=86,8.



Slika 10.18: Verjetnostna gostota za čas do odpovedi kartičnega sistema

Z Weibull++7 modeliramo verjetnostno gostoto za čas do odpovedi za biometrični sistem z Weibullovim porazdelitvenim zakonom s parametri β in η (slika 10.19). Ob 100% verjetnosti nastopi odpoved za biometrični sistem pri β=2,8 in η=101,7.

Primerjava grafik preskušanih sistemov za verjetnostno gostoto odpovedi rezultira v ugotovitvi, da ob 100% verjetnosti nastopijo odpovedi za biometrični sistem za 14,9% kasneje kot za kartični sistem.



Slika 10.19: Verjetnostna gostota za čas do odpovedi biometričnega sistema

10.6.1 REZULTATI OCEN ZANESLJIVOSTI KARTIČNEGA SISTEMA

Karakteristike zanesljivosti za Weibullovo porazdelitev časov do odpovedi kartičnega identifikacijskega sistema so naslednji:

$$\hat{MTTF} = \frac{1}{n}\sum_{i=1}^{n} t_i = 76{,}5\ dneva$$

$$f(t) = \frac{\beta}{\eta}\left(\frac{t-\gamma}{\eta}\right)^{\beta-1}\exp\left[-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right] = \frac{2.0757}{86.8545}\left(\frac{t}{86.8545}\right)^{2.0757-1}\exp\left[-\left(\frac{t}{86.8545}\right)\right]^{2.0757}$$

$$\lambda(t)=\frac{\beta}{\eta}\left(\frac{t-\gamma}{\eta}\right)^{\beta-1}=\frac{2.0757}{86.8545}\left(\frac{t}{86.8545}\right)^{2.0757-1}$$

$$R(t)=\exp\left(-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right)=\exp\left(-\left(\frac{t}{86.8545}\right)^{2.0757}\right)$$

$$F(t)=1-\exp\left(-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right)=1-\exp\left(-\left(\frac{t}{86.8545}\right)^{2.0757}\right).$$

10.6.2 REZULTATI OCEN ZANESLJIVOSTI BIOMETRIČNEGA SISTEMA

Karakteristike zanesljivosti za Weibullovo porazdelitev časov do odpovedi biometričnega identifikacijskega sistema so:

$$\hat{MTTF}=\frac{1}{n}\sum_{i=1}^{n}t_i=88{,}8\ dneva$$

$$f(t)=\frac{\beta}{\eta}\left(\frac{t-\gamma}{\eta}\right)^{\beta-1}\exp\left[-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right]=\frac{2.8596}{101.7080}\left(\frac{t}{101.7080}\right)^{2{,}8596-1}\exp\left[-\left(\frac{t}{101.7080}\right)\right]^{2.8596}$$

$$\lambda(t)=\frac{\beta}{\eta}\left(\frac{t-\gamma}{\eta}\right)^{\beta-1}=\frac{2.8596}{101.7080}\left(\frac{t}{101.7080}\right)^{2.8596-1}$$

$$R(t)=\exp\left(-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right)=\exp\left(-\left(\frac{t}{101.7080}\right)^{2.8596}\right)$$

$$F(t)=1-\exp\left(-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right)=1-\exp\left(-\left(\frac{t}{101.7080}\right)^{2.8596}\right).$$

Rezultati izračunanih ocen zanesljivosti (časov do odpovedi $MTTF_S$), preskušanih identifikacijskih sistemov so za 13,1% boljši za biometrični sistem. Ostali parametri so podani kot funkcije in grafično prikazani ter komentirani skozi deseto poglavje.

10.7 DOLOČITEV TOČKASTIH OCEN RAZPOLOŽLJIVOSTI KARTIČNEGA IN BIOMETRIČNEGA SISTEMA

Kartični modul za identifikacijo je v obdobju enoletnega opazovanja odpovedal desetkrat. Po vsaki odpovedi smo izvedli popravilo, modul povrnili v stanje delovanja ter ob tem merili čas aktivnih popravil. Časi aktivnih popravil kartičnih modulov so podani v tabeli 10.8. Iz dobljenih podatkov celotnega časa zastojev t_i bomo analitično določili obratovalno razpoložljivost sistema, ki ga v našem primeru vzdržujemo korektivno.

Tabela 10.9: Časi aktivnih popravil za kartični modul

ČASI PRVEGA AKTIVNEGA POPRAVILA(dni)										
i	1	2	3	4	5	6	7	8	9	10
t_i	1	1	2	2	5	1	4	4	4	1
ČASI DRUGEGA AKTIVNEGA POPRAVILA(dni)										
i	1	2	3	4	5	6	7	8	9	10
t_i	1	1	3	0	3	1	1	2	3	0
ČASI TRETJEGA AKTIVNEGA POPRAVILA(dni)										
i	1	2	3	4	5	6	7	8	9	10
t_i	1	1	2	3	7	1	2	1	4	1

Točkasto oceno za povprečno vrednost časa do zaključka popravil kartičnega modula izračunamo po formuli:

$$\hat{MTTR} = \frac{1}{r}\sum_{i=1}^{r} t_i = \frac{1}{30}\left(25+15+23\right) = 2{,}1\ dneva$$

Točkasta ocena za razpoložljivost kartičnega modula v obdobju opazovanja je po formuli (47):

$$\hat{A} = \frac{MTTF}{MTTF + MTTR} = \frac{76{,}5}{76{,}5 + 2{,}1} = 0{,}973$$

Biometrični modul za identifikacijo je v enoletnem obdobju opazovanja odpovedal desetkrat. Po vsaki odpovedi smo izvedli popravilo, modul povrnili v stanje delovanja ter ob tem merili čas aktivnih popravil. Časi aktivnih popravil biometričnih modulov so podani v tabeli 10.9. Tudi v tem primeru bomo iz podatkov preračunali obratovalno razpoložljivost biometričnega sistema ob predpostavki, da smo sistem vzdrževali korektivno.

Tabela 10.10: Časi aktivnih popravil za biometrični modul

ČASI PRVEGA AKTIVNEGA POPRAVILA(dni)										
i	1	2	3	4	5	6	7	8	9	10
t_i	1	0	1	1	1	2	2	3	2	2
ČASI DRUGEGA AKTIVNEGA POPRAVILA(dni)										
i	1	2	3	4	5	6	7	8	9	10
t_i	1	1	3	0	3	1	1	1	1	0
ČASI TRETJEGA AKTIVNEGA POPRAVILA(dni)										
i	1	2	3	4	5	6	7	8	9	10
t_i	1	0	2	1	1	1	1	1	1	1

Za biometrični modul določimo točkasto oceno za povprečno vrednost zaključkov popravil:

$$\hat{MTTR} = \frac{1}{r}\sum_{i=1}^{r} t_i = \frac{1}{30}(15+12+10) = 1,2 \; dneva$$

Točkasta ocena za razpoložljivost biometričnega modula v obdobju opazovanja je:

$$\hat{A} = \frac{MTTF}{MTTF + MTTR} = \frac{88,8}{88,8+1,2} = 0,987$$

10.8 PREGLED HITROSTI ODČITAVANJA PRSTNEGA ODTISA V REALNEM ČASU

Aplikativnih primerjav, ki bi ob upoštevanju naraščanja hitrosti registracije obravnavale padanje natančnosti identifikacijskega sistema, je razmeroma malo. Tabela 7.4 prikazuje povprečne vrednosti za različne hitrosti identifikacije. FAR se ne spreminja in je v testu odvisen samo od zahtevane varnostne stopnje, ki je za omenjeni primer 1/1.000.000.

Tabela 10.11: Gibanje FRR (%) v odvisnosti od spremembe hitrosti algoritma

	Normalni način	Hitri način 1	Hitri način 2	Hitri način 3	Hitri način 4	Hitri način 5
FRR	1,31	1,44	1,45	1,57	1,77	1,95

Iz tabele lahko povzamemo naslednje:

- Pri večanju hitrosti iskalnega algoritma v načinu 1 ali 2 FRR naraste za 10 %.
- Pri večanju hitrosti iskalnega algoritma v načinu 3 FRR naraste za 17 %, v načinu 4 pa za 25 %.

- FRR se poslabša za 32 % v hitrem načinu 5 in je celo sprejemljiv za nekatere baze, kjer je hitrost identifikacije pomembna.

Čeprav se učinkovitost sistema poveča, hitrega načina ni smiselno uporabljati za identifikacijo v majhnih podatkovnih bazah, recimo z manj kot 100 vzorci (Huvanandana in drugi, 2000). V tem primeru je razlika v času identifikacije in ujemanju vzorcev med normalnim in hitrim načinom zanemarljiva.

11 MARKOVSKE VERIGE ZA IZPELJAVO KVANTITATIVNEGA MODELA ZA OCENO ZANESLJIVOSTI IN RAZPOLOŽLJIVOSTI BIOMETRIČNEGA SISTEMA

Obravnavana identifikacijska sistema (kartični in biometrični) se nahajata v obdobju staranja, to je v obdobju, ko se pojavljajo odpovedi, so posledice daljšega časa delovanja in nepovratnih fizikalno-kemijskih procesov.

Odpovedi, ki se pojavljajo v obdobju normalnega delovnaja, so slučajne narave. Pogostost odpovedi je konstantna, saj zgodnjih odpovedi ni več, odpovedi zaradi izrabe pa še niso nastopile. Čas do odpovedi je tako porazdeljen po eksponentni porazdelitvi, ki je posebna oblika Weibullovega zakona s parametrom β=1. Za predpostavko, da je pogostost zaključkov popravil neodvisna od časa in s tem čas popravila porazdeljen skladno z eksponentno porazdelitveno funkcijo, pa ni kake posebne utemeljitve. V praksi se velikokrat pokaže, da je čas popravila porazdeljen po log-normalnem. V takih primerih za konstantno vrednost μ vzamemo povprečje trenutne pogostosti zaključkov popravil v opazovanem časovnem intervalu (Hudoklin in Rozman, 1989).

Osnovne predpostavke, na katerih temelji izpeljani model, so torej:
1. Odpovedi gradnikov sistema so statistično neodvisne.
2. Pogostosti gradnikov sistema so neodvisne od časa.
3. Pogostosti zaključkov popravil gradnikov ali sistema so neodvisne od časa.
4. Izračunane so točkaste ocene za pogostosti odpovedi in pogostosti zaključkov popravil.

Verjetnost prehoda sistema iz stanja v drugo stanje zaradi odpovedi i–tega gradnika v časovnem intervalu $(t+\Delta t)$ je $\lambda_i \Delta t$, verjetnost prehoda zaradi popravila i–tega gradnika pa $\mu_i \Delta t$. Pogostosti odpovedi λ_i in pogostosti zaključkov popravil μ_i posameznih gradnikov sistema predstavljajo elemente matrike **Q**.

Pri določanju zanesljivosti upoštevamo, da so vsa nedelujoča stanja sistema absorbirajoča stanja, ker popravilo sistema po odpovedi ne izboljša njegove zanesljivosti. Pri izračunu razpoložljivosti pa upoštevamo, da sistem po odpovedih popravljamo, nedelujoča stanja sistema pa niso več absorbirajoča, ker so iz njih možni prehodi v druga stanja.

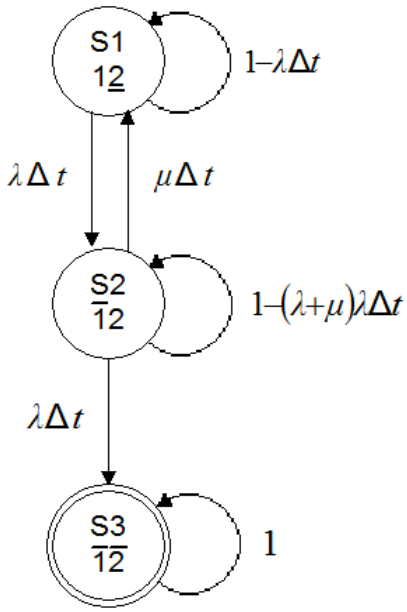
V praksi je podana zahteva za nemoteno delovanje identifikacijskega sistema kljub verjetnosti odpovedi biometričnega ali kartičnega čitalca (letališča, upravne enote, policija itd.). Zagotoviti je potrebno vzporedni gradnik ali sistem, ki prevzame funkcijo v primeru odpovedi prvega.

11.1 MODEL IZRAČUNA $MTTF$ IN A SISTEMA Z DVEMA EKVIVALENTNIMA GRADNIKOMA V VZPOREDNI VEZAVI

V praksi je podana zahteva za nemoteno delovanje identifikacijskega sistema kljub verjetnosti odpovedi biometričnega ali kartičnega čitalca (letališča, upravne enote,

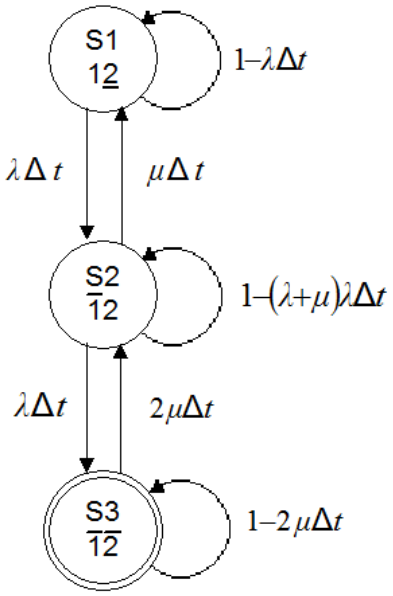
policijske postaje itd.). Za povečanje zanesljivosti biometričnega sistema in zagotovitev nemotenega delovanja, pasivno vežemo dve ekvivalentni enoti biometričnega čitalnega modula, da v primeru odpovedi prvega čitalca funkcijo prevzame drugi čitalec. Prikazali bomo verjetnostni graf za čitalne enote biometričnega sistema, ki jih bomo paralelno vezali za dosego boljših parametrov zanesljivosti identifikacijskega sistema.

Vzemimo sistem, ki sestoji iz dveh ekvivalentnih enot. Naj bo pogostost odpovedi posameznega čitalnega modula λ, pogostost zaključkov popravil pa μ. Konstruirajmo ustrezni verjetnostni graf za zanesljivost (slika 11.1) v pasivni vzporedni vezavi z absolutno zanesljivim stikalom:



Slika 11.1: Verjetnostni graf zanesljivosti biometričnega sistema z dvema ekvivalentnima čitalcema

Verjetnostni graf za razpoložljivost dveh vzporedno vezanih biometričnih gradnikov je prikazan na sliki 11.4. Stanje S_3 ni več ponorno, verjetnost prehoda iz stanja S_3 v stanje S_2 pa je $2\mu\Delta t$ pri predpostavki, da en vzdrževalec popravi en gradnik.



Slika 11.2: Verjetnostni graf razpoložljivosti biometričnega sistema z dvema ekvivalentnima čitalcema

11.2 IZRAČUN λ IN μ ZA MODEL Z DVEMA EKVIVALENTNIMA GRADNIKOMA V VZPOREDNI VEZAVI

Iz zajetih podatkov so bile po formulah (Hudoklin, 2003) izračunane ustrezne točkaste ocene za pogostosti odpovedi in zaključkov popravil (λ in μ), ki nastopajo v matriki **Q**:

$$\hat{\lambda} = \frac{r}{nt_0}$$

r – število odpovedi v obdobju opazovanja (koledarski čas)
n – število istovrstnih gradnikov
t_0 – čas obratovanja posameznega gradnika: razlika med koledarskim časom in časom planiranega (nadgradnja posameznih gradnikov zaradi razvoja novih funkcionalnosti) in neplaniranega zastoja posameznega gradnika.

$$\hat{\mu} = \frac{r}{\sum_{i=1}^{n} T_i} = \frac{r}{T_S}$$

T_i – skupni čas zastoja i–tega gradnika v obdobju opazovanja (čas dejanskega popravila)
T_s – skupno trajanje odpovedi n istovrstnih gradnikov.

Kadar sta enoti vezani paralelno je λ_1=2λ, v primeru pasivne paralelne vezave pa je $\lambda_1 = \lambda_2 = \lambda$ in $\mu_1 = \mu_2 = \mu$. Iz verjetnostnega grafa odčitamo naslednje vrednosti q_{ij}:

$$\begin{array}{lll} q_{11} = -\lambda & q_{21} = \lambda & q_{31} = 0 \\ q_{12} = \mu & q_{22} = -(\lambda + \mu) & q_{32} = \lambda \\ q_{13} = 0 & q_{23} = 0 & q_{33} = 0 \end{array}$$

Vrednosti za vsa možna stanja sistema z dvema ekvivalentnima gradnikoma zapišemo v obliki matrike:

$$\mathbf{Q} = \begin{array}{c} \\ S_1 \\ S_2 \\ S_3 \end{array} \begin{array}{c} \begin{array}{ccc} S_1 & S_2 & S_3 \end{array} \\ \begin{bmatrix} -\lambda & \lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & 0 & 0 \end{bmatrix} \end{array}.$$

Povprečni čas do odpovedi sistema $MTTF$ določimo z inverzijo matrike **Q***, ki jo dobimo, če matriki **Q** zamenjamo predznak in izpustimo vrstice in stolpce, ki pripadajo absorbirajočim stanjem (v taki vrstici so same ničle). $MTTF$ je potem enak vsoti elementov prve vrstice invertirane matrike. V našem primeru je matrika **Q*** enaka:

$$\mathbf{Q}^* = \begin{bmatrix} \lambda & -\lambda \\ -\mu & (\lambda+\mu) \end{bmatrix}.$$

Inverzna matrika ima obliko:

$$[\mathbf{Q}^*]^{-1} = \begin{bmatrix} \frac{\lambda+\mu}{\lambda^2} & \frac{1}{\lambda} \\ \frac{\mu}{\lambda^2} & \frac{1}{\lambda} \end{bmatrix}.$$

Povprečni čas do odpovedi sistema je enak :

$$MTTF = \frac{2\lambda+\mu}{\lambda^2}.$$

Iz verjetnostnega grafa s slike 11.2 odčitamo elemente matrike $\mathbf{Q}_A$, ki se glasi:

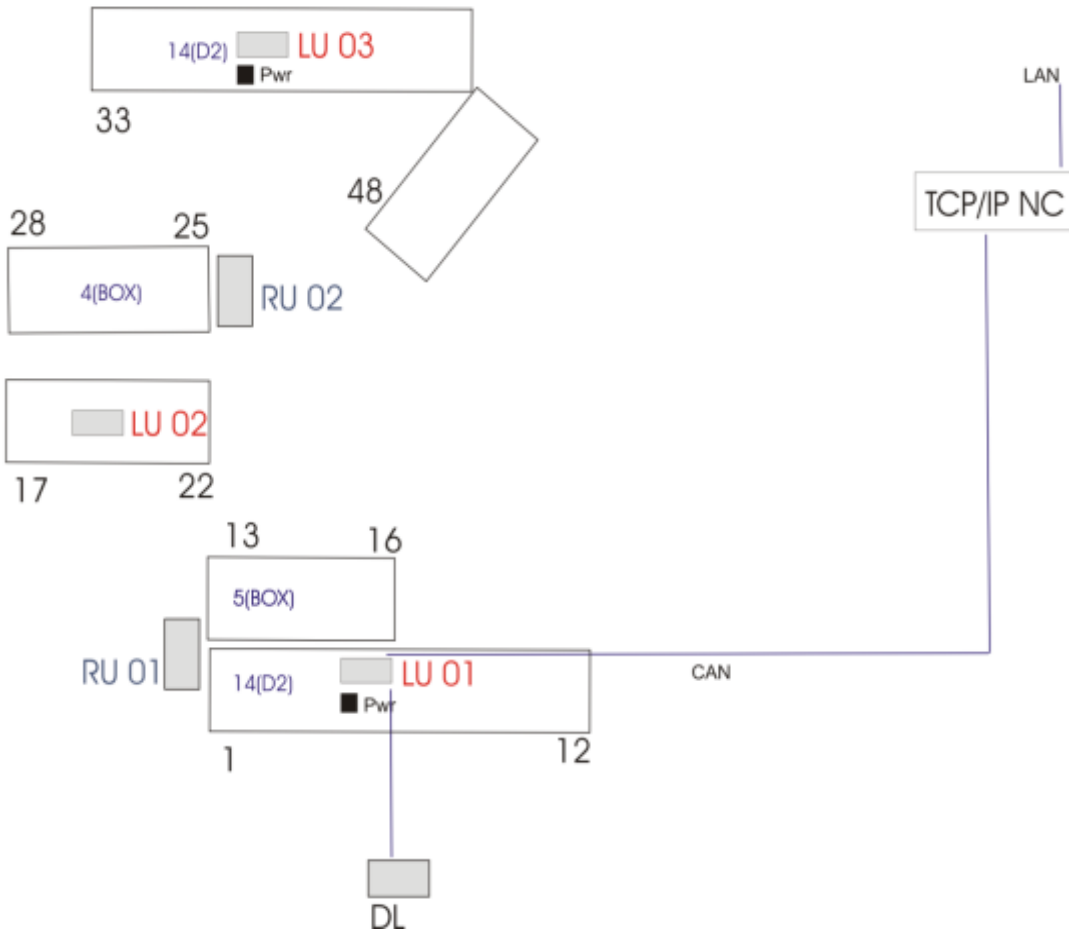
$$\mathbf{Q_A} = \begin{array}{c} \\ S_1 \\ S_2 \\ S_3 \end{array} \begin{array}{c} \begin{array}{ccc} S_1 & S_2 & S_3 \end{array} \\ \begin{bmatrix} -\lambda & \lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & 2\mu & -2\mu \end{bmatrix} \end{array}.$$

Za izračun razpoložljivost najprej določimo matriko $[\mathbf{Q}_A]^{-1}$ in razpoložljivost pa nato določimo po enačbi:

$$A_S = \frac{2\lambda\mu + 2\mu^2}{\lambda^2 + 2\lambda\mu + 2\mu^2}.$$

11.3 PRIKAZ DEJANSKE POSTAVITVE IDENTIFIKACIJSKEGA SISTEMA ZA PRIMER RAZISKAVE

Slika 11.3 predstavlja konfiguracijo identifikacijskega sistema za izpeljavo matematičnega modela zanesljivosti. Konfiguracijo identifikacijskega sistema sestavljajo:
RU– Prikazovalna enota - displej
LU– Elektronika za krmiljenje elektronskih ključavnic
Pwr– Izvor napetosti
Lck– Elektronske ključavnice
NTWC – TCP/IP NC mrežni kontroler
BL– biometrični terminal NET terminal
ELSSW – Programski del identifikacijskega sistema



Slika 11.3: Konfiguracija ELS003 – strežna mesta identifikacijskega sistema

11.4 BLOKOVNA SHEMA MODELA IDENTIFIKACIJSKEGA SISTEMA IN OPIS STANJ

Iz obstoječe dejanske postavitve modulov identifikacijskega sistema izpeljemo ustrezno blokovno shemo z vidika zanesljivosti. Le-ta je prikazana na sliki 11.4. Sistem sestavlja pet funkcionalnih enot A, B, C, D in E. Sistem opravlja zahtevano funkcijo, če zadovoljivo deluje vseh pet celot.

Funkciona celota A je sestavljena iz dveh identičnih biometričnih čitalcev, ki sta v obdobju staranja. Eden izmed obeh čitalcev iz funkcionalne enote A stalno deluje, drugi pa je neaktiven in se vklopi, ko prvi čitalec odpove. Predpostavljamo, da neaktiven čitalec med čakanjem ne odpove. Ocena za pogostost odpovedi teh gradnikov je $2{,}4.10^{-2}$.

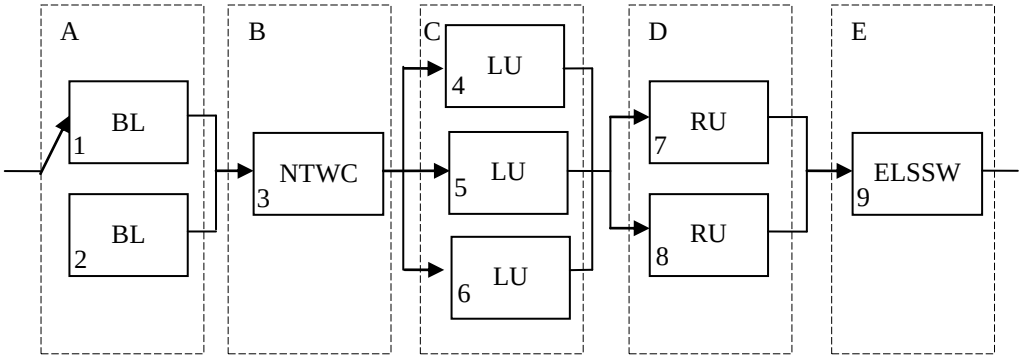
Funkcionalno celoto B predstavlja gradnik NTWC (mrežni kontroler), ki je v obdobju normalnega delovanja in je njegova ocena za povprečni čas do odpovedi 244 dni.

Funkcionalna celota C je sestavljena iz treh identičnih gradnikov LU (elektronika za krmiljenje elektronskih ključavnic), ki so v obdobju normalnega delovanja. Ocena za pogostost odpovedi je $2{,}1.10^{-4}$ odpovedi na uro (čas do odpovedi je 88 dni). Funkcionalna enota C normalno deluje kadar zadovoljivo delujeta vsaj dva gradnika.

Funkcionalna celota D je sestavljena iz dveh identičnih gradnikov RU (prikazovalnik), ki so v obdobju normalnega delovanja. Ocena za pogostost odpovedi je $1{,}6.10^{-4}$ odpovedi na uro.

Funkcionalno celoto E predstavlja gradnik ELSSW programska oprema, ki je v obdobju normalnega delovanja in je njegova ocena za povprečni čas do odpovedi 167 dni.

Na sliki 11.4 smo prikazali blokovno shemo biometričnega identifikacijskega sistema.



Slika 11.4: Blokovna shema identifikacijskega sistema s stališča zanesljivosti

Proces delovanja naprave aproksimiramo s homogeno markovsko verigo, katere stanja definiramo takole (tabela 11.1):

Tabela 11.1: Opis stanj sistema s slike 11.5

št. stanja	oznaka stanja	opis stanja	
1	S_1	$1\underline{2}3456789$	D
2	S_2	$\overline{1}23456789$	D
3	S_3	$12\overline{3}456789$	N
4	S_4	$123\overline{4}56789 \cup 1234\overline{5}6789 \cup 12345\overline{6}789$	D
5	S_5	$12345\overline{6}789 \cup 123456\overline{7}89$	D
6	S_6	$123456789\overline{}$	N
7	S_7	$\overline{12}3456789$	N
8	S_8	$\overline{1}2\overline{3}456789$	N
9	S_9	$\overline{1}23\overline{4}56789 \cup \overline{1}234\overline{5}6789 \cup \overline{1}2345\overline{6}789$	D
10	S_{10}	$\overline{1}23456\overline{7}89 \cup \overline{1}23456\overline{8}9$	D
11	S_{11}	$\overline{1}23456789\overline{}$	N
12	S_{12}	$12\overline{34}56789 \cup 12\overline{3}4\overline{5}6789 \cup 12\overline{3}45\overline{6}789$	N
13	S_{13}	$123\overline{45}6789 \cup 1234\overline{56}789 \cup 123\overline{4}5\overline{6}789$	N
14	S_{14}	$123\overline{4}56\overline{7}89 \cup 1234\overline{5}6\overline{7}89 \cup 12345\overline{6}\overline{7}89 \cup$ $123\overline{4}56\overline{8}9 \cup 1234\overline{5}6\overline{8}9 \cup 12345\overline{6}\overline{8}9$	D
15	S_{15}	$123\overline{4}5678\overline{9} \cup 1234\overline{5}678\overline{9} \cup 12345\overline{6}78\overline{9}$	N
16	S_{16}	$12\overline{3}456\overline{7}89 \cup 12\overline{3}456\overline{8}9$	N
17	S_{17}	$123456\overline{78}9$	N
18	S_{18}	$12345\overline{6}78\overline{9} \cup 12345\overline{67}89$	N
19	S_{19}	$\overline{12}\overline{3}\overline{4}56789 \cup \overline{12}\overline{3}4\overline{5}6789 \cup \overline{12}\overline{3}45\overline{6}789$	N
20	S_{20}	$\overline{1}2\overline{3}\overline{4}56789 \cup \overline{1}2\overline{3}4\overline{5}6789 \cup \overline{1}2\overline{3}45\overline{6}789$	N
21	S_{21}	$\overline{1}23\overline{4}\overline{5}6789 \cup \overline{1}23\overline{4}5\overline{6}789 \cup \overline{1}23\overline{4}5\overline{6}789$	N
22	S_{22}	$\overline{1}23\overline{4}56\overline{7}89 \cup \overline{1}23\overline{4}5\overline{6}\overline{7}89 \cup \overline{1}23\overline{4}5\overline{67}89 \cup$ $\overline{1}23\overline{4}56\overline{8}9 \cup \overline{1}23\overline{4}5\overline{6}\overline{8}9 \cup \overline{1}23\overline{4}5\overline{6}\overline{8}9$	D
23	S_{23}	$\overline{1}23\overline{4}5678\overline{9} \cup \overline{1}234\overline{5}678\overline{9} \cup \overline{1}23\overline{4}5\overline{6}78\overline{9}$	N
24	S_{24}	$\overline{12}3456\overline{7}89 \cup \overline{12}3456\overline{8}9$	N
25	S_{25}	$\overline{1}2\overline{3}456\overline{7}89 \cup \overline{1}2\overline{3}456\overline{8}9$	N
26	S_{26}	$\overline{1}23456\overline{78}9$	N
27	S_{27}	$\overline{1}23456\overline{7}8\overline{9} \cup \overline{1}23456\overline{89}$	N
28	S_{28}	$12\overline{34}56\overline{7}89 \cup 12\overline{3}4\overline{5}6\overline{7}89 \cup 12\overline{3}45\overline{6}\overline{7}89 \cup$ $12\overline{3}4\overline{5}6\overline{8}9 \cup 12\overline{3}4\overline{5}6\overline{7}\overline{8}9 \cup 12\overline{3}4\overline{5}6\overline{7}\overline{8}9$	N
29	S_{29}	$123\overline{45}6\overline{7}89 \cup 1234\overline{56}\overline{7}89 \cup 123\overline{4}5\overline{6}\overline{7}89 \cup$ $123\overline{4}5\overline{6}\overline{8}9 \cup 1234\overline{5}6\overline{7}\overline{8}9 \cup 123\overline{4}5\overline{6}\overline{7}\overline{8}9$	N
30	S_{30}	$123\overline{4}56\overline{78}9 \cup 1234\overline{5}6\overline{78}9 \cup 12345\overline{6}\overline{78}9$	N
31	S_{31}	$123\overline{4}56\overline{7}8\overline{9} \cup 1234\overline{5}6\overline{7}8\overline{9} \cup 12345\overline{6}\overline{7}8\overline{9} \cup$ $123\overline{4}56\overline{89} \cup 1234\overline{5}6\overline{89} \cup 12345\overline{6}\overline{89}$	N
32	S_{32}	$\overline{12}\overline{3}\overline{4}56\overline{7}89 \cup \overline{12}\overline{3}4\overline{5}6\overline{7}89 \cup \overline{12}\overline{3}45\overline{6}\overline{7}89 \cup$	N

		$\overline{12}3\overline{456}\overline{789} \cup \overline{12}34\overline{5}6\overline{78}9 \cup \overline{12}345\overline{689}$	
33	S_{33}	$\overline{1}2\overline{3}\overline{456}\overline{789} \cup \overline{1}2\overline{3}4\overline{5}6\overline{789} \cup \overline{1}2\overline{3}45\overline{6}\overline{789} \cup \overline{12}\overline{3}\overline{456}\overline{789} \cup \overline{12}34\overline{5}6\overline{789} \cup \overline{12}345\overline{6}\overline{789}$	N
34	S_{34}	$\overline{1}23\overline{45}\overline{6}\overline{789} \cup \overline{1}234\overline{5}\overline{6}\overline{789} \cup \overline{1}23\overline{4}5\overline{6}\overline{789} \cup \overline{123}\overline{4}\overline{56}\overline{789} \cup \overline{12}34\overline{5}\overline{6}\overline{789} \cup \overline{12}345\overline{6}\overline{789}$	N
35	S_{35}	$\overline{1}23\overline{456}\overline{789} \cup \overline{1}234\overline{5}\overline{6}\overline{789} \cup \overline{1}23\overline{45}\overline{6}\overline{789}$	N
36	S_{36}	$\overline{1}23\overline{456}\overline{789} \cup \overline{1}234\overline{5}\overline{6}\overline{789} \cup \overline{1}23\overline{45}\overline{6}\overline{789} \cup \overline{12}3\overline{456}\overline{789} \cup \overline{1}23\overline{4}5\overline{6}\overline{789} \cup \overline{1}2345\overline{6}\overline{789}$	N

Verjetnostni graf za zanesljivost biometričnega identifikacijskega sistema je prikazan na sliki 11.4. Pri konstrukciji grafa za zanesljivost smo predpostavili, da gradnik označen s številko 1, po popravilu tudi priklopimo.

Oznake za λ in μ posameznih modulov biometričnega sistema:
λ_1, λ_2 – pogostost odpovedi BL
λ_3 – pogostost odpovedi modula NTWC
$\lambda_4, \lambda_5, \lambda_6$ – pogostost odpovedi modula LU
λ_7, λ_8 – pogostost odpovedi modula RU
λ_9 – pogostost odpovedi modula ELSSW
μ_1, μ_2 – pogostost zaključkov popravil BL
μ_3 – pogostost zaključkov popravil NTWC
μ_4, μ_5, μ_6 – pogostost zaključkov popravil LU
μ_7, μ_8 – pogostost zaključkov popravil RU
μ_9 – pogostost zaključkov popravil ELSSW

11.5 VERJETNOSTNI GRAF ZA ZANESLJIVOST IN RAZPOLOŽLJIVOST IDENTIFIKACIJSKEGA SISTEMA IN PRERAČUN $MTTF_S$, A

V nadaljevanju bomo za blokovno shemo razvitega biometričnega sistema izračunali oceno za povprečni čas do odpovedi sistema $MTTF_S$. Izračun nam podaja oceno za povprečni čas do odpovedi biometričnega sistema, kjer smo razpoložljivost povečali z dodatnim biometričnim čitalcem, ki zagotavlja nemoteno delovanje tudi v primeru odpovedi prvega modula.

Za izačun[46] povprečnega časa do odpovedi in stacionarne razpoložljivosti identifikacijskega sistema, je najprej potrebno konstruirati matriko **Q**. Za izračun povprečnega časa do odpovedi $MTTF_S$ izpeljemo matriko **Q*** in izračunamo njen

[46] *Mathematica je komercialna programska oprema podjetja Wolfram Reserch in predstavlja enega od nabolj priljubljenih matematičnih orodij, ki ga lahko uporabimo tudi za izračun povprečnega časa do odpovedi in stacionarne razpoložljivosti obravnavanih identifikacijskih sistemov. Dosegljivo na: http://www.wolfram.com/products/mathematica/index.html (12.05.2009).*

inverz $[\mathbf{Q^*}]^{-1}$. Matriko **Q*** dobimo tako, da v prehodni matriki **Q** črtamo vse vrstice in stolpce, ki pripadajo nedelujočim stanjem, preostalo matriko pa odštejemo od enotske matrike **I**. Povprečni čas do odpovedi dobimo iz enačbe:

$$MTTF = m_{11} + m_{12} + ...m_{1k}\,[h].$$

Stanje sistema, ko delujejo vsi moduli, je označeno s številko 1, indeks k pa pomeni število delujočih stanj sistema. Členi enačbe predstavljajo kar elemente prve vrstice matrike $[\mathbf{Q^*}]^{-1}$. Za izračun stacionarne rapoložljivosti biometričnega sistema A najprej formiramo matriko $\mathbf{Q_A}$, v kateri zadnji stolpec nadomestimo z enojkami in tako dobimo matriko $\mathbf{Q^*_A}$. Po izračunu inverzne matrike $[\mathbf{Q^*_A}]^{-1}$ izračunamo stacionarno razpoložljivost kot vsoto elementov zadnje vrstice, ki pripadajo delujočim stanjem.

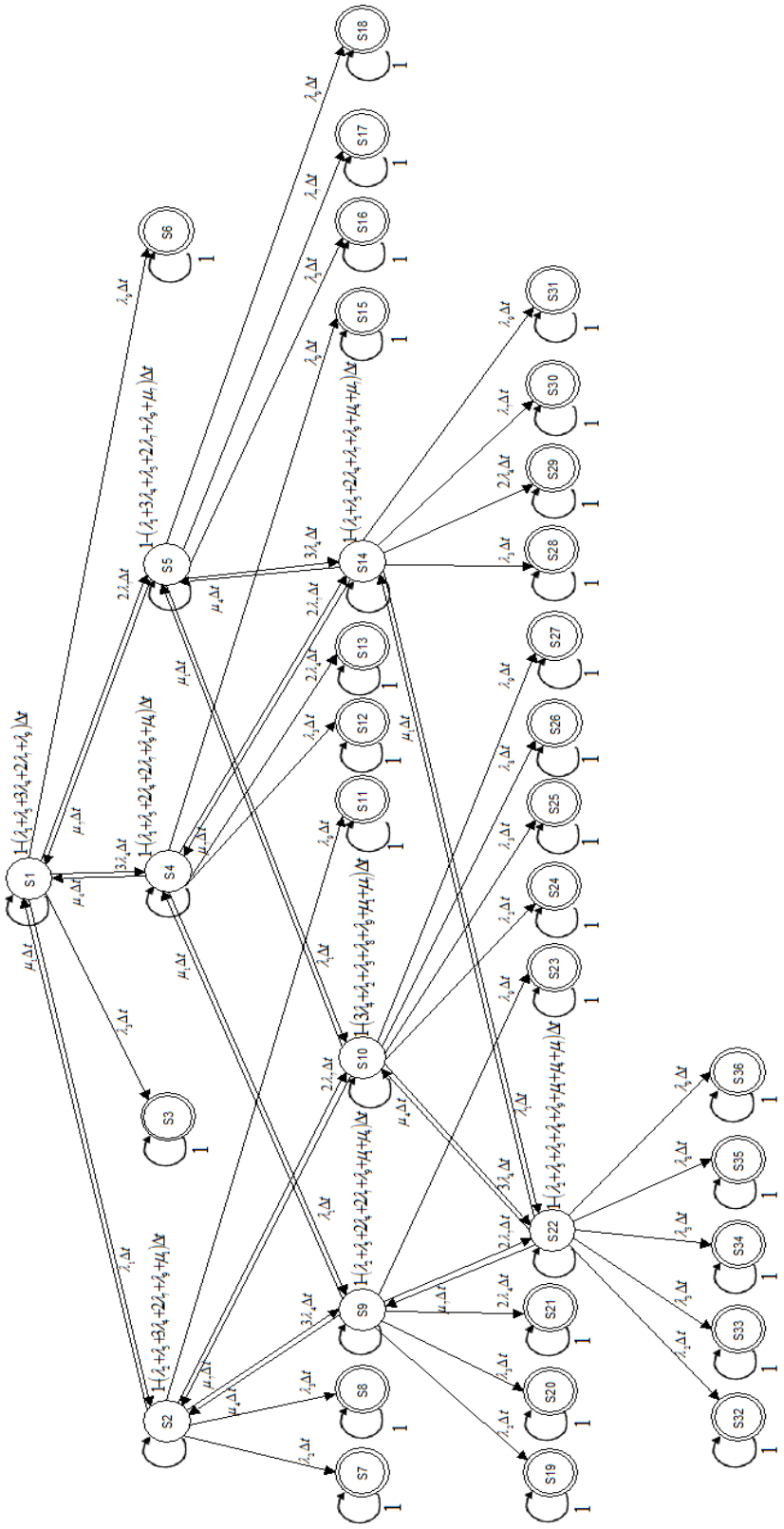
V poglavju 17.5. (dodatek 3) smo konstruirali matrike **Q**, **Q***, $\mathbf{Q_A}$ in $\mathbf{Q^*_A}$ na osnovi verjetnostnih grafov na slikah 11.4 in 11.5.

Izračun smo izvedli za oceno zanesljivosti $MTTF_S$ glede na podake v poglavju 13.1.2 (dodatek 3), s čimer potrjujemo pravilnost ocene raziskave v poglavju 10.6. Na podoben način se izvede preračunavanje za oceno razpoložljivosti po zgoraj opisanem postopku.

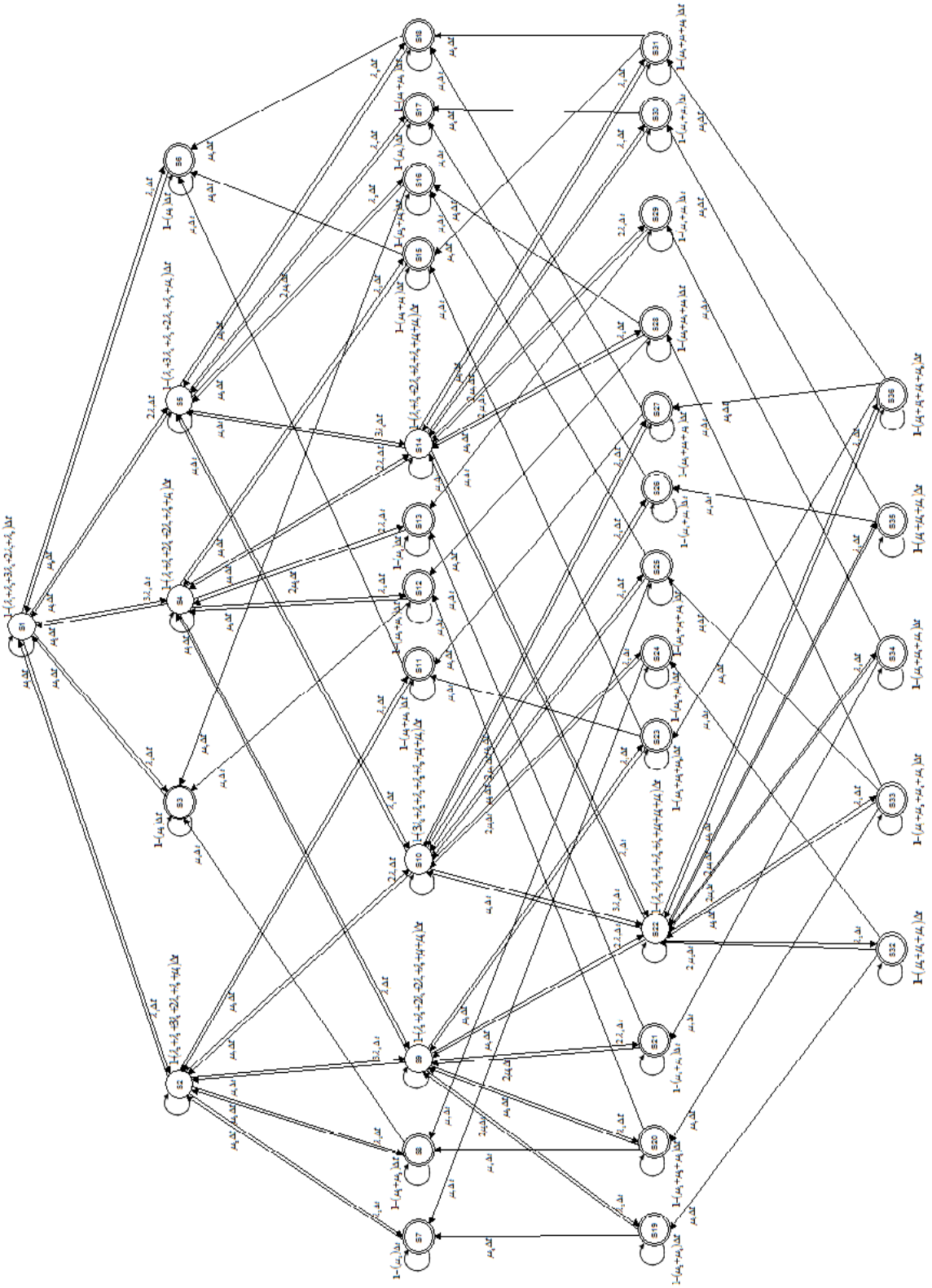
Zaradi obsežnih matrik in posledično preračunavanja smo modeliranje izvedli samo za biometrični sistem ter tako preverili pravilnost rezultatov za zanesljivost, dobljenih po Weibullovi metodi v poglavju 10.6. Na enak način bi preračun ter ocenjevanje zanesljivosti in razpoložljivosti izvedli za kartični sistem.

Za blokovno shemo na sliki 11.4 ter opis stanj iz tabele 11.1 bomo nadalje prikazali verjetnostni graf za zasedbo delujočih in nedelujočih stanj (slika 11.5).

Za blokovno shemo na sliki 11.4 ter opis stanj iz tabele 11.1 bomo na sliki 11.6 prikazali verjetnostni graf za razpoložljivost biometričnega identifikacijskega sistema.



Slika 11.5: Verjetnostni graf za zanesljivost biometričnega identifikacijskega sistema



Slika 11.6: Verjetnostni graf za razpoložljivost biometričnega identifikacijskega sistema

12 IZDELAVA PROTOTIPA SAMOUČEČE NEVRONSKE MREŽE MULTIMODALNEGA BIOMETRIČNEGA SISTEMA

Izdelava prototipa nevronske mreže v smislu povečanja učinkovitosti ter optimizacije za multimodalni biometrični sistem, temelji na zahtevanih parametrih uporabnika za izbiro modalitete. Na osnovi teh zahtev definiramo relavantne vhodne parametre za konstrukcijo nevronske mreže in jih po vnosu obdelamo s programsko opremo. Nevronska mreža je samoučeča in na osnovi vhodnih parametrov kreira lasten odločitveni model za izbiro optimalne modalitete.

Rezultat tega dela raziskave je multimodalni biometrični sistem, katerega učinkovitost lahko prilagajamo (optimiramo) glede na zahtevan nivo varnosti, hitrosti identifikacije, natančnosti in ostalih zahtev.

12.1 VHODNE VREDNOSTI

Glede na lastnosti sistema, ki ga stranka potrebuje, bomo določili vhodne vrednosti v nevronsko mrežo in njihove uteži. Po dosedanjih izkušnjah na odločitev o vrsti sistema aplikacije (ID oz. biometrični metodi) vplivajo naslednje bistvene lastnosti:

- težavnost uporabe (nizka, srednja, velika),
- možnost napake oz. zahtevnost okolja (nizka, srednja, visoka),
- natančnost (nizka, srednja, visoka, zelo visoka),
- odobravanje uporabnikov (nizko, srednje, visoko),
- zahtevana stopnja varnosti (nizka, srednja, visoka),
- potreba po spremembi obratovalnega režima naprav (da ali ne),
- vlažnost in izpostavljenost vremenskim vplivom (nizka, srednja, visoka).

Z razvojem aplikacij se je pojavila tudi potreba po razvoju t. i. povezanih (angl. on-line[47]) aplikacij, ki so veliko bolj prilagodljive in hitreje odgovorijo na želje uporabnika. Ker pred leti strežniki in mrežne povezave še niso bili tako hitri in zanesljivi kot danes, je razvoj logičen (večina Metra[48] aplikacij pred letom 2000 je bila razvitih po »off-line«[49] metodi).

Primer: Odločitev o vrsti aplikacije je odvisna od zahtev po sprotnih spremembah delovanja naprav in od števila različnih režimov obratovanja objekta (večinoma športni objekti). Tako želijo uporabniki ločen režim, kot je nočno kopanje, dan odprtih vrat, drugačno obnašanje naprave ob različnih urah dneva itd. Za takšno delovanje sistema je vsekakor primernejša povezana ali on-line aplikacija. V

[47] *On-line; v računalniški in telekomunikacijski tehnologiji imata termina specifičen pomen komunikacije računalniških modulov. Termina opredeljuje ameriški zvezni standard Federal Standard 1037C.*

[48] *Metra aplikacije so informacijsko-identifikacijski sistemi LCC (Leisure Centre Card) in ELS (Electronic Locking Systems), razviti v podjetju Metra inženiring, d. o. o. Aplikacije so namenjene kontroli vstopa v poslovne objekte in rekreativne centre (hoteli, bazeni, smučišča itd.) dostopno na: http://www.metra.si (13.07.2009).*

[49] *Off-line; glej ([36]).*

podjetju Metra d.o.o so določene naprave samo za tip sistema off-line, nekatere pa samo za on-line. Glede na to značilnost je v primeru zahteve po on-line načinu vedno najbolj univerzalen RFID medij, ki je tudi najbolj podprt. To značilnost smo uporabili tudi v nevronski mreži, kar je razvidno v nadaljevanju.

12.2 SKRITI NIVO

Po sliki 60 se vhodi in uteži vhodnega nivoja navezujejo na nevrone skritega nivoja nevronske mreže, ki bo na izhodu podala tip sistema oziroma primernost ali neprimernost določene biometrične metode identifikacije za določen tip sistemskega okolja. Najpogostejše metode biometrične identifikacije predstavljajo nevrone drugega skritega nivoja:

- glas,
- obraz,
- mrežnica,
- šarenica,
- podpis,
- dlan in
- preverjanje prstnega odtisa (fingerprint).

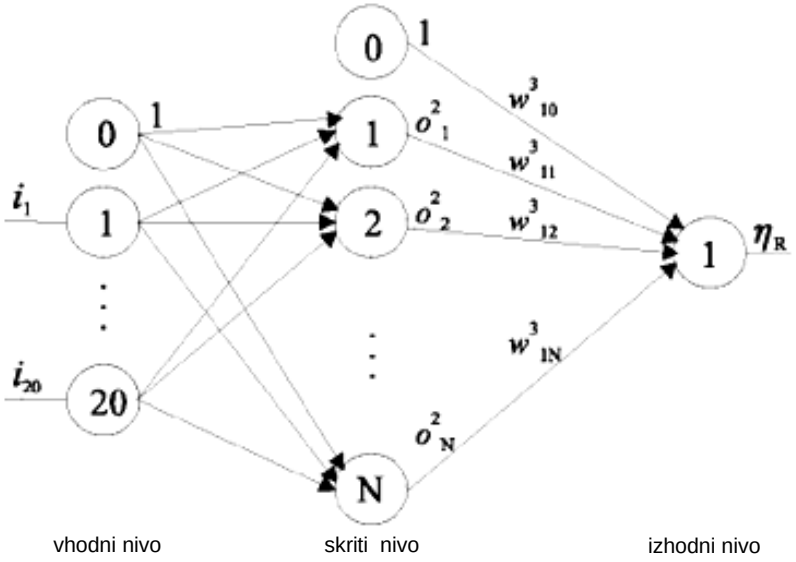
Njihove lastnosti so obenem tudi lastnosti bodočega sistema oziroma vhodov v nevronsko mrežo. S tem smo mrežo poenostavili na samo en skriti nivo.

12.3 IZHODNE VREDNOSTI

Sam izhod iz nevronske mreže smo si zamislili kot tekstovni zapis (glas, obraz, mrežnica, šarenica, podpis, dlan in prstni odtis (FP)). Tako je tudi najbolj razvidno, kateri sistem ustreza danim vhodom.

Na ta način smo dobili topologijo trinivojsko usmerjene nevronske mreže (slika 12.1), ki je primerna za vnos v program EasyNN. Nevronska mreža za naš raziskovalni primer ima tako:

- 7 vhodnih nevronov,
- 2 nevrona skritega nivoja in
- 1 izhodni nevron.



Slika 12.1: Trinivojsko usmerjena nevronska mreža

12.4 VNOS PODATKOV

Na osnovi dosedanjih spoznanj in podatkov smo sestavili preglednico značilnosti različnih biometričnih metod, ki so v širši uporabi (vsaka metoda predstavlja posamezen nevron). Njihove lastnosti (prednosti in slabosti) nam bodo rabile kot vhodi v nevrone. Primernost uporabe glede na določeno lastnost pa bo odvisna od uteži posameznih vhodov v nevronske celice.

Samo mrežo oblikujemo z uvozom podatkov iz tabelnih datotek, tekstovnih datotek, kjer so besede ločene s tabulatorji in vejicami, iz bitmap slikovnih datotek ali binarnih datotek. Mrežo lahko sestavimo tudi ročno z vpisom podatkov v poseben editorski podprogram v sklopu programa EasyNN. Za gradnjo nevronske mreže lahko uporabimo numerične, tekstovne, slikovne ali kombinirane podatkovne tipe. Za naš primer je vnos podatkov tekstovni. Tabelo 1.1 prenesemo v vnosno tabelo programa (tabela 12.1). V tabeli smo uporabili okrajšave in jih tudi čim bolj poenostavili. Tako je vnos hitrejši in enostavnejši. Nevronsko mrežo je najlažje zgraditi iz tabelaričnega zapisa. V tabeli določimo vhodne in izhodne stolpce. Določimo tudi tip vnosne vrstice, to je lahko vrstica, iz katere se mreža uči, ali pa vrstica za poizvedovanje (angl. query). Dodali smo vrstice za učenje, ki za primer potrebe on-line načina pri napravah PIN in FP (prstni odtis, angl. fingerprint) predvidevajo nadomestno RFID napravo. Tako smo se izognili napačnim odgovorom, saj za on-line način ni naprav PIN in FP.

Z vnosom vhodnih parametrov dobimo tabelo v kateri prvih šest vrstic (od T:0 do T:6) vsebuje podatke za učenje nevronske mreže (training), zadnje tri vrstice (od Q:7 do Q:9) pa so poizvedovalni primeri (query). Da bi lahko dobili vpogled v proces identifikacije, bomo simulacijski model gradili z upoštevanjem naslednjih elementov (kratice v tabeli pomenijo dejavnike glede na preglednico 1.1):

- TEZ_UPORABE – težavnost uporabe,
- NATANČNOST – natančnost,
- UPORAB_ODO – uporabnikovo odobravanje,
- ZAH_VAR.NI – zahtevani varnostni nivo,
- UPOR_DA – uporabnost na daljši rok,
- BIOMETRIJA1 – biometrija (izbrana biometrija glede na podane dejavnike),
- MULTI – za primer multimodalne biometrije (višji varnostni nivo) in
- BIOMETRIJA2 – alternative BIOMETRIJI1 za primer multimodalnosti.

Vsi tipi tabelaričnih polj so tekstovni, kar olajša vnos in tolmačenje odgovora.

Tabela 12.1: Dejavniki multimodalne biometrije

Day 6	TEZ_UPORABE	NATANCNOST	UPORAB_ODO	ZAH_VAR.NI	UPOR_DA	BIOMETRIJA1	MULTI	BIOMETRIJA2
T:0	velika	visoka	visoko	srednji	srednja	GLAS	da	ŠARENICA
T:1	velika	visoka	srednje	srednji	srednja	PODPIS	da	MREŽNICA
T:2	srednja	visoka	srednje	srednji	srednja	OBRAZ	da	PODPIS
T:3	srednja	zelo visoka	srednje	zelo velik	velika	ŠARENICA	da	MREŽNICA
T:4	nizka	zelo visoka	srednje	velik	velika	MREŽNICA	da	MREŽNICA
T:5	velika	visoka	srednje	srednji	srednja	DLAN	da	DLAN
T:6	velika	velika	srednje	velik	velika	PRST. ODTIS	da	MREŽNICA
Q:7	srednja	visoka	visoko	velik	velika	~~~~PRST. O	?	~MREŽNICA
Q:8	velika	visoka	srednje	velik	srednja	~~~ŠARENICA	?	~~~~ŠARENIC
Q:9	nizka	visoka	srednje	srednji	srednja	~~~~PODPIS	da	~~~~DLAN

Takoj ko zaženemo program, ta ne prepozna nobenega podatka, saj je njegov »spomin« popolnoma prazen; zato je program ob zagonu v fazi snemanja (recording). Ko vnesemo tri biometrične vzorce in se z vsakim seveda strinjamo, program preide v fazo učenja (training). To se zgodi tudi vsakič naslednjič, ko vnesemo nov podatek.

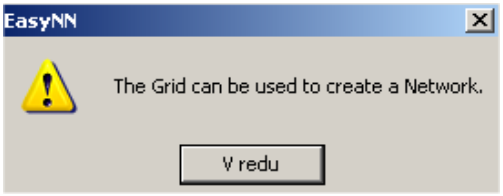
12.4.1 FAZE PROGRAMA

Nevronske mreže v programu se naučijo podatkov, ki so vneseni v mrežo (učni vzorci), in obenem primerjajo preverjalne podatke, sočasno pa izvajajo samokontrolo. Ko je učenje mreže končano, lahko takšno nevronsko mrežo uporabljamo za preverjanje izhodov glede na dana vprašanja na vhodu, uporabimo interaktivna povpraševanja prek orodij ali uporabimo vhodne podatke iz ločene datoteke. Koraki, potrebni za gradnjo nevronske mreže, so avtomatizirani. Sam program izdela najenostavnejšo možno nevronsko mrežo, ki se bo učila iz podatkov. Uporabimo lahko tudi grafični editor za gradnjo kompleksnejših mrež.

12.4.2 FAZE UČENJA NEVRONSKE MREŽE

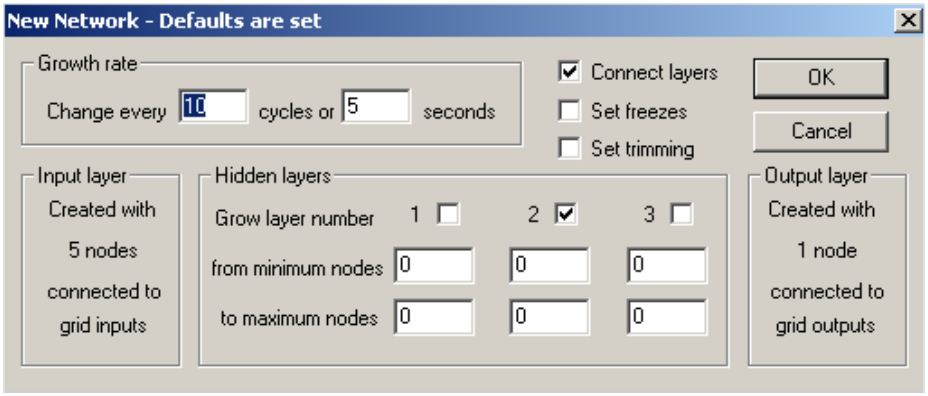
Učenje nevronske mreže poteka z naključnim spreminjanjem uteži na sinapsah (pomnilniških celicah). Ena sinapsa predstavlja vez med aktivnostmi dveh nevronov. Nevronska mreža izkazuje svoje svoje znanje s tem, da za vhodne varnostne parametre vrača pravilne ali vsaj dovolj približne izhodne vrednosti za izbor biometrične modalitete. Za tabelo z vnešenimi vhodnimi parametri, lahko preverimo njeno primernost za gradnjo nevronske mreže. Tukaj bi se lahko pojavil problem

končne rešitve, saj je ob naključnem spreminjanju uteži čisto mogoče, da rešitve sploh ne dobimo. Kliknemo na gumb (Check Grid), in če je vse v redu, dobimo odgovor (slika 12.2):



Slika 12.2: Ekranska maska za pričetek gradnje nevronske mreže

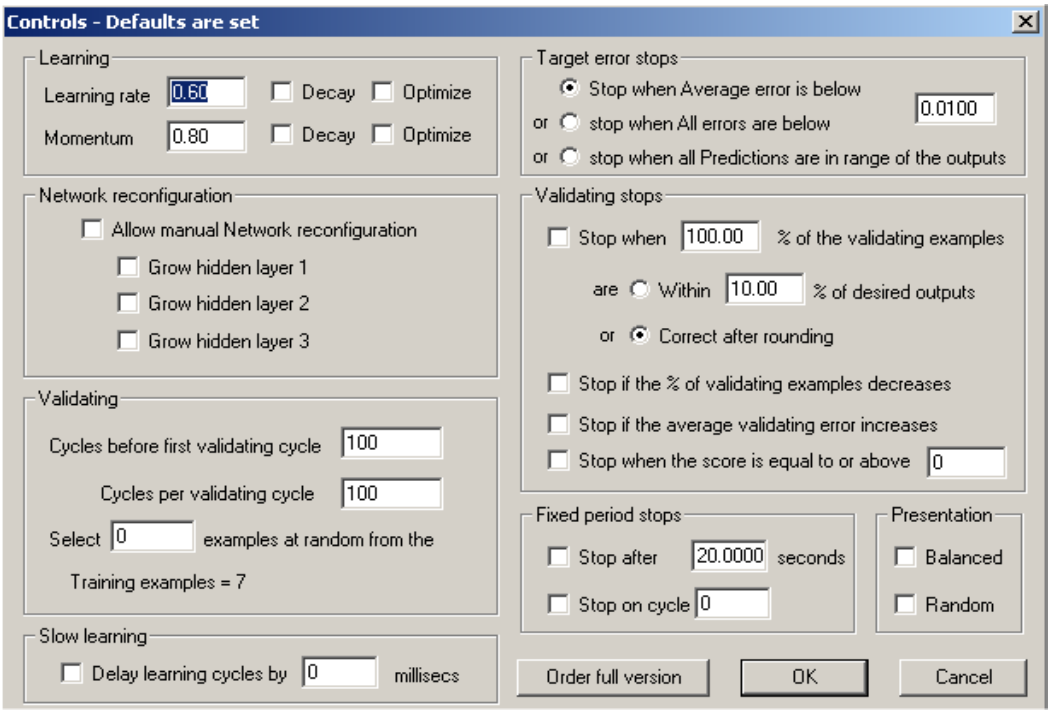
To je zelena luč za pričetek gradnje nevronske mreže. Kliknemo na gumb (Growth Network) in prikaže se pogovorno okno, v katerem določimo parametre (slika 12.3) nove nevronske mreže:



Slika 12.3: Ekranska maska nastavitev parametrov

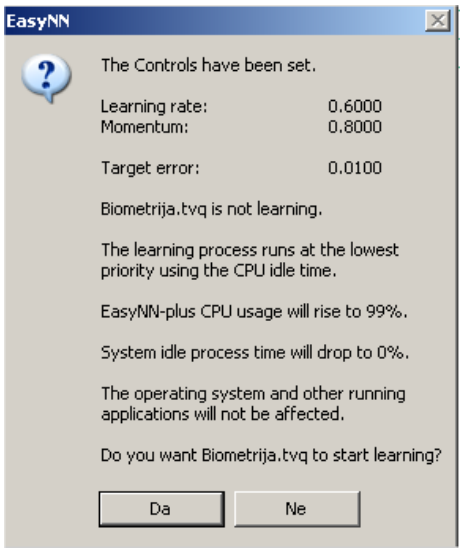
Za dosego optimalnega rezultata v doglednem času mora rešitev konvergirati k najboljši možni rešitvi. Izpolnitev pogoja konvergiranja pa dosežemo z algoritmom učenja z vzratnm razširjanjem. Spreminjamo lahko število nevronov in povezav med njimi. Za naš primer prednastavljene vrednosti niso problematične. Kliknemo OK in prikaže se pogovorno okno za nastavitev parametrov učenja. Bistvena parametra sta learning rate (tempo učenja) in momentum[50] (moment) (slika 12.4). Klik na gumb OK prične z učenjem po prednastavljenih parametrih. Nastavimo še stopnjo shranjevanja in kliknemo OK.

[50] *Z nastavitvami momenta se poskušamo izogniti napakam pri gradnji nevronske mreže.*

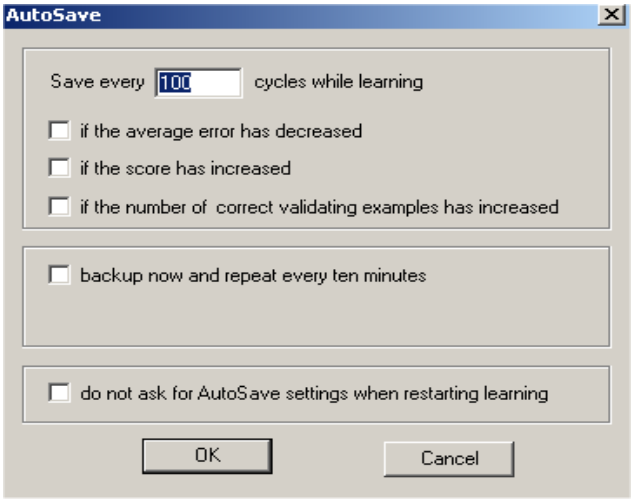


Slika 12.4: Nastavitev parametrov učenja in momenta

Za pričetek učenja dobimo obvestilo (slika 12.5) in po potrditvi nastavimo frekvenco shranjevanja (slika 12.6):



Slika 12.5: Začetek učenja



Slika 12.6: Frekvenca shranjevanja

V desnem spodnjem kotu je prikazan potek učenja. Ko je učenje končano, dobimo obvestilo »Stopped Learning« in zadostno število korakov; za našo mrežo je bilo potrebnih 21 korakov (slika 12.7):

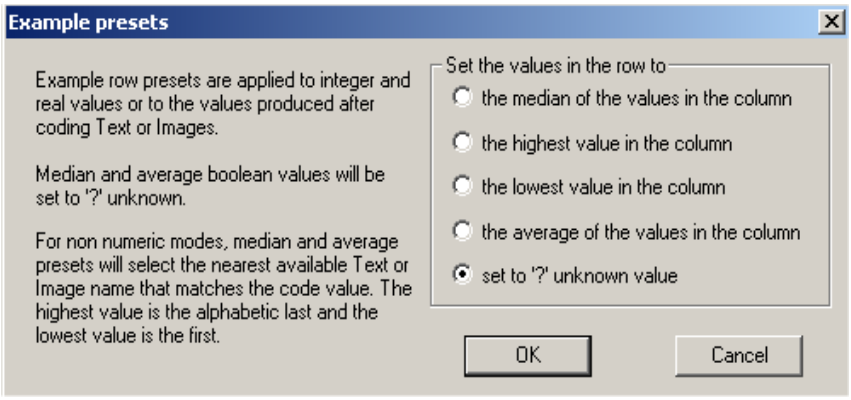
Slika 12.7: Število ciklov učenja nevronske mreže

Ko smo končali z gradnjo in učenjem nevronske mreže, lahko preizkusimo njeno delovanje. V vrsticah poizvedovanja Q:7 in Q:8 (angl. query) vpišemo naključne poizvedovalne dejavnike, ki so prisotni v sistemu, ki ga želimo opremiti z biometrično opremo. Ti dejavniki v končni fazi vplivajo na izbiro biometrične identifikacije (slika 12.9). V izhodnem stolpcu dobimo odgovor glede na podane dejavnike (~~~~PRST.O in ~~~PODPIS):

Q:7	srednja	visoka	visoko	velik	velika	~~~~PRST. O
Q:8	velika	visoka	srednje	velik	srednja	~~~PODPIS

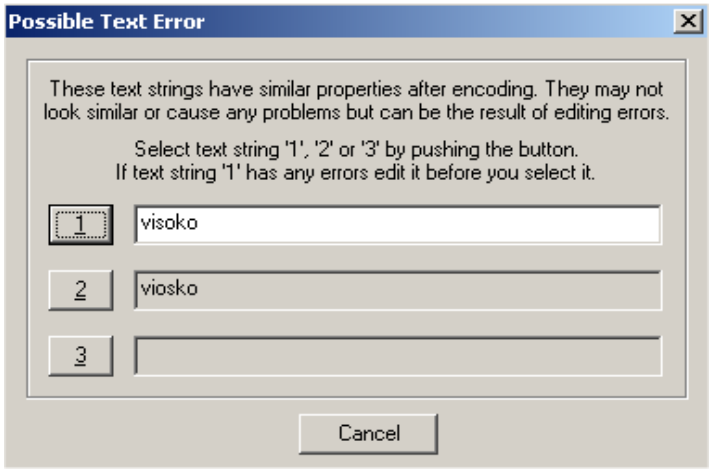
Slika 12.9: Rezultati glede na poizvedovalne vrednosti

Za nove poizvedbe lahko dejavnike izbiramo v okviru preliminarnih vrednosti (dejavnikov) nevronske mreže ali pa določimo popolnoma nove (slika 12.10):



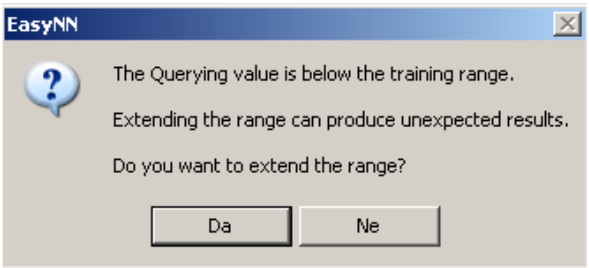
Slika 12.10: Izbor kriterijev glede na preliminarne dejavnike

V primeru, da vhodna vrednost (dejavnik) ni vsebovana v fazi učenja, dobimo opozorilo (slika 12.11).



Slika 12.11: Vrednost zunaj dosega mreže

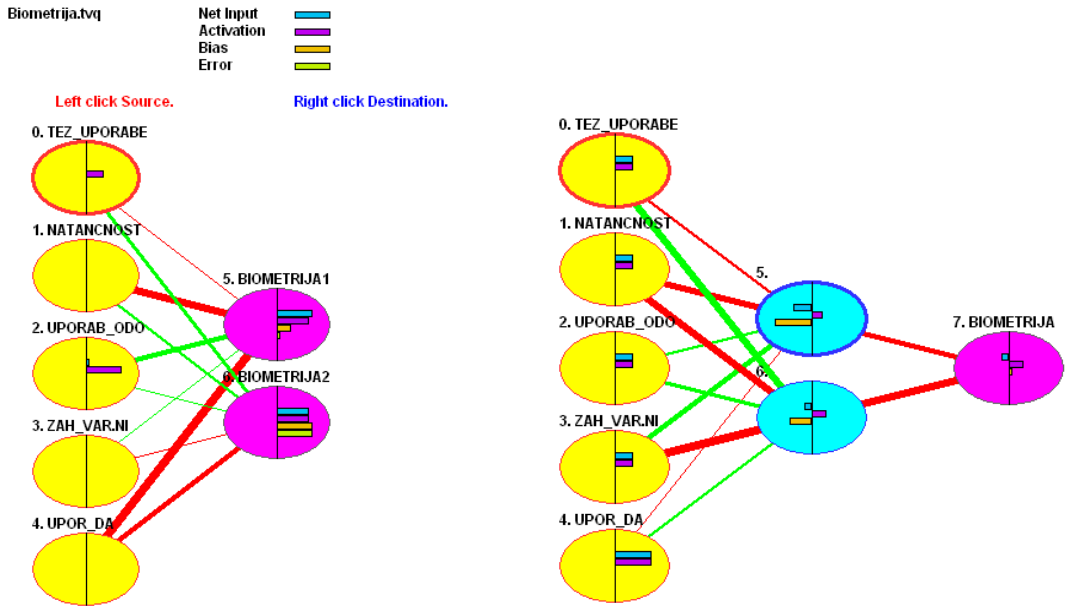
V primeru, da vztrajamo pri vrednosti zunaj dosega, program samodejno nastavi vrednost na najvišjo (slika 12.12).



Slika 12.12: Samodejna nastavitev

Za naš problem moramo določiti takšno politiko kombiniranja biometrij, ki bo minimizirala varnostna tveganja, glede na pomembnost vhodnih dejavnikov.

Nadalje si lahko ogledamo nevronsko mrežo multimodalnega biometričnega sistema (slika 12.8).



Slika 12.8: Nevroni in nivoji nevronske mreže ter povezave (s skritim nivojem in brez njega)

13 REZULTATI IN UGOTOVITVE RAZISKAVE

Ocenjevanje zanesljivosti in razpoložljivosti identifikacijskih sistemov je področje, ki je lahko pri izbiri sistema pristopne kontrole ključnega pomena. Statistične metode za ocenjevanje učinkovitosti pristopajo k tej nalogi z ocenjevanjem zanesljivosti in razpoložljivosti vseh gradnikov identifikacijskega sistema z Weibullovim modelom. Dvoparametrična Weibullova funkcija dobro opisuje karakteristike zanesljivosti primerjanih identifikacijskih sistemov. Vizualizacija podatkov z grafi daje nazoren prikaz ujemanja med meritvami in Weibullovo porazdelitvijo. Čim večja je strmina premice, kar pomeni večji Weibullov parameter β, tem večja je zanesljivost izdelkov, t. j. manjša je verjetnost (pri istem parametru η), da bo identifikacijski sistem odpovedal v krajšem času. To je posledica dejstva, da pomeni večja vrednost Weibullovega parametra daljše čase do odpovedi. Ugotovitev ponazorimo z nekaj številkami. Pri oceni statističnih parametrov se moramo zavedati, da se lahko ta ocena zelo odmika od dejanske vrednosti parametrov. Razvidno je, da je za 30 podatkov pričakovani interval (z 90–odstotnim zaupanjem) za resnično vrednost Weibullovega parametra širok okrog 10 odstotkov izračunane vrednosti tega parametra, medtem ko je izračun drugega parametra Weibullove porazdelitve zanesljivejši.

Z izračunom ocen časov do odpovedi in med odpovedmi primerjanih identifikacijskih sistemov po Weibullovi metodologiji, dobimo naslednje rezultate za oceno zanesljivosti in razpoložljivosti:

1. Ocena časa do odpovedi (zanesljivosti) biometričnega sistema z izračunom karakteristike $MTTF_S$=88,8 dneva.
2. Ocena časa popravila biometričnega sistema z izračunom karakteristike $MTTR_S$=1,2 dneva.
3. Ocena razpoložljivosti biometričnega sistema z izračunom karakteristike A_S=0,987.
4. Ocena časa do odpovedi (zanesljivosti) kartičnega sistema z izračunom karakteristike $MTTF_S$=76,5 dneva.
5. Ocena časa popravila kartičnega sistema z izračunom karakteristike $MTTR_S$=2,1 dneva.
6. Ocena razpoložljivosti kartičnega sistema z izračunom karakteristike A_S=0,973.

V okviru raiskave smo izvedli različne modele za oceno zanesljivosti in razpoložljivosti, ki so zasnovane z uporabo različnih pristopov. Kot novost na področju zasnove ocen zanesljivosti identifikacijskega sistema, smo zasnovali in uporabili markovski model, ki je postopek, neodvisen od Weibullove metode in nam v nalogi služi kot preverba za izračune po Weibull modelu. Pri aplikaciji modela na področju biometrije smo obravnavali uporabnost metode v realni domeni.

Za izračun ocene $MTTF_S$ in za oceno razpoložljivosti biometričnega sistema (A_S) upoštevamo izračunane pogostosti odpovedi in pogostosti zaključkov popravil gradnikov identifikacijskega sistema (tabela 13.1):

Tabela 13.1: Pogostosti odpovedi in pogostosti zaključkov popravil biometričnega sistema

λ_1	=	0,00022	odpovedi/uro
λ_2	=	0,00017	odpovedi/uro
λ_3	=	0,00017	odpovedi/uro
λ_4	=	0,00021	odpovedi/uro
λ_5	=	0,00025	odpovedi/uro
λ_7	=	0,0002	odpovedi/uro
λ_8	=	0,0002	odpovedi/uro
λ_9	=	0,00025	odpovedi/uro
μ_1	=	0,02	popravil/uro
μ_2	=	0,02	popravil/uro
μ_3	=	0,02	popravil/uro
μ_4	=	0,02	popravil/uro
μ_5	=	0,02	popravil/uro
μ_6	=	0,02	popravil/uro
μ_7	=	0,02	popravil/uro
μ_8	=	0,02	popravil/uro

Z invertiranjem matrike **Q*** , ki je zaradi velikosti podana v tabeli 17.4 v Dodatku 3, določimo $[\mathbf{Q}^*]^{-1}$. Elementi invertirane tabele so podani v tabeli 13.2.

Tabela 13.2: Izračunani elementi matrike $[\mathbf{Q}^*]^{-1}$ biometričnega sistema

$-q_{1,1}$	=	2006,531837	$q_{1,2}$	=	-21,37113771	$q_{1,4}$	=	-60,36358244
$q_{2,1}$	=	-1939,010654	$-q_{2,2}$	=	67,92235644	$q_{2,4}$	=	-59,02393874
$q_{4,1}$	=	-1917,185336	$q_{4,2}$	=	-20,68300648	$-q_{4,4}$	=	104,8374398
$q_{5,1}$	=	-1925,53897	$q_{5,2}$	=	-20,77509561	$q_{5,4}$	=	-58,61296869
$q_{9,1}$	=	-1880,377778	$q_{9,2}$	=	-43,14795496	$q_{9,4}$	=	-79,84551328
$q_{10,1}$	=	-1894,173757	$q_{10,2}$	=	-43,36056379	$q_{10,4}$	=	-57,88510448
$q_{14,1}$	=	-1872,542549	$q_{14,2}$	=	-20,28973672	$q_{14,4}$	=	-79,60510633
$q_{22,1}$	=	-1850,29295	$q_{22,2}$	=	-34,99287532	$q_{22,4}$	=	-71,21091877
$q_{1,5}$	=	-30,79435865	$q_{1,9}$	=	-0,681555882	$q_{1,10}$	=	-0,348793776
$q_{2,5}$	=	-30,11356781	$q_{2,9}$	=	-1,386915449	$q_{2,10}$	=	-0,708034669
$q_{4,5}$	=	-29,771566	$q_{4,9}$	=	-0,93053278	$q_{4,10}$	=	-0,338758525
$-q_{5,5}$	=	76,58059224	$q_{5,9}$	=	-0,664885872	$q_{5,10}$	=	-0,612063812
$q_{9,5}$	=	-29,31713175	$-q_{9,9}$	=	25,38629004	$q_{9,10}$	=	-0,572493717
$q_{10,5}$	=	-52,18240608	$q_{10,9}$	=	-1,126973851	$-q_{10,10}$	=	24,90988428
$q_{14,5}$	=	-51,78110342	$q_{14,9}$	=	-0,825052692	$q_{14,10}$	=	-0,510184662
$q_{22,5}$	=	-43,66993488	$q_{22,9}$	=	-8,95750871	$q_{22,10}$	=	-8,516567057

$q_{1,14}$	=	-0,943178789	$q_{1,22}$	=	-0,010881404		
$q_{2,14}$	=	-0,925959151	$q_{2,22}$	=	-0,018219282		
$q_{4,14}$	=	-1,273539425	$q_{4,22}$	=	-0,013382009		
$q_{5,14}$	=	-1,630964958	$q_{5,22}$	=	-0,016215519		
$q_{9,14}$	=	-1,135891226	$q_{9,22}$	=	-0,143461628		
$q_{10,14}$	=	-1,375154997	$q_{10,22}$	=	-0,26841245		
$-q_{14,14}$	=	25,68574121	$q_{14,22}$	=	-0,110583406		
$q_{22,14}$	=	-9,238790117	$-q_{22,22}$	=	16,55388515		

Vsota elementov prve vrstice matrike, da rezulatat za oceno $MTTF_S$ biomeričnega sistema, ki je v našem primeru 2121,04 ur (88,37 dni), kar potrjuje izračun po Weibullu za merjene vrednosti v raziskavi $MTTF_S$=88,8 dni (poglavje 10.6.2).

Matriko $\mathbf{Q}_A^*$, ki je zaradi velikosti podana v tabeli 17.5, preračunamo s podatki in jo invertiramo v $[\mathbf{Q}_A^*]^{-1}$ ter seštejemo elemente, ki pripadajo delujočim stanjem (S_1, S_2, S_4, S_5, S_9, S_{10}, S_{14} in S_{22}) v zadnji vrstici. Zaradi razsežnosti invertirane matrike bomo zapisali samo zadnjo vrstico, ki je relavantna za izračun ocene razpoložljivosti (tabela 13.3).

Tabela 13.3: Izračunane vrednosti zadnje vrstice elementov matrike $[\mathbf{Q}_A^*]^{-1}$ biometričnega sistema

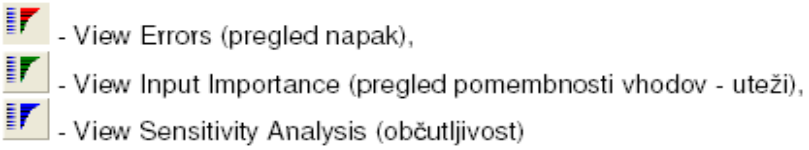
$q_{36,1}$	=	**0,91577**	$q_{36,2}$	=	**0,01143**	$q_{36,3}$	=	0,008032	$q_{36,4}$	=	**0,02994**
$q_{36,5}$	=	**0,01557**	$q_{36,6}$	=	0,012419	$q_{36,7}$	=	0,000467	$q_{36,8}$	=	5,06E-05
$q_{36,9}$	=	**0,00064**	$q_{36,10}$	=	**0,0008**	$q_{36,11}$	=	0,000317	$q_{36,12}$	=	0,000129
$q_{36,13}$	=	0,000644	$q_{36,14}$	=	**0,00078**	$q_{36,15}$	=	0,000433	$q_{36,16}$	=	6,84E-05
$q_{36,17}$	=	0,000168	$q_{36,18}$	=	0,000222	$q_{36,19}$	=	2,73E-06	$q_{36,20}$	=	1,82E-06
$q_{36,21}$	=	6,75E-06	$q_{36,22}$	=	**0,00026**	$q_{36,23}$	=	0,000245	$q_{36,24}$	=	0,000367
$q_{36,25}$	=	2,27E-06	$q_{36,26}$	=	4,01E-06	$q_{36,27}$	=	0,000246	$q_{36,28}$	=	2,22E-06
$q_{36,29}$	=	8,23E-06	$q_{36,30}$	=	3,92E-06	$q_{36,31}$	=	0,000246	$q_{36,32}$	=	0
$q_{36,33}$	=	0	$q_{36,34}$	=	3,93E-18	$q_{36,35}$	=	0	$q_{36,36}$	=	0,000728

Ob upoštevanju ocen za pogostost odpovedi gradnikov in ocen pogostosti zaključkov popravil je ocena za A_S=0,9751, kar potrjuje izračunano vrednost v raziskavi A_S=0,987 (poglavje 10.7). S primerjavo povratnih informacij z Weibullovo oceno zanesljivosti in razpoložljivosti smo ugotovili, da se le-ti značilno ne razlikujeta, kar kaže na potencial uporabe metodologije markovskih sistemov v praksi. Na področju aplikativnega raziskovanja učinkovitosti biometričnih sistemov razviti matematični model pomeni novost v uporabi stohastičnega pristopa pri celoviti obravnavi razpoložljivosti tovrstnih identifikacijskih sistemov. Uporaba markovskega modela za oceno parametrov zanesljivosti in razpoložljivosti je primerna za hitro in točno načrtovanje in spremljanje zanesljivosti in razpoložljivosti biometričnega sistema za osebno identifikacijo. Izračunane karakteristike zanesljivosti in razpoložljivosti za dana identifikacijska sistema (kartični in biometrični) pomenijo prvo kvantitativno ovrednotenje le–teh in tako postavljajo

izhodišče za nadaljnje analize in spremljanje delovanja identifikacijskega sistema. Neposredni rezultat doktorskega dela je markovski model za spremljanje zanesljivosti in razpoložljivosti konkretnega identifikacijskega sistema, pričakovani dolgoročni rezultat pa je njegova nadgradnja in implementacija, ki bo omogočila analizo in stalno spremljanje izboljševanja razpoložljivosti in zanesljivosti identifikacijskega sistema in njegovih elementov. Iz časovnih zahtevnosti in dejanskih časov izvajanj matrik vidimo, da lahko posamezne ocene zanesljivosti in razpoložljivosti izračunamo v realnem času. Kljub večji časovni zahtevnosti konstrukcije verjetnostnega grafa pa lahko najbolj zahtevne časovne operacije izvedemo kot predpripravo izvajalnega algoritma za izračun ocene zanesljivosti in razpoložljivosti posameznega testnega primera. Na ta način lahko oceno zanesljivosti za testni primer tudi pri kompleksnih sistemih matrik izračunamo v realnem času, kar daje praktično uporabnost markovskega modeliranja. Tako se bo povečala kakovost storitev in s tem učinkovitost celotnega identifikacijskega sistema. Razvoj stohastičnega modela za analizo in spremljanje razpoložljivosti biometričnih identifikacijskih sistemov tako pomeni prispevek k poglabljanju znanja na področju uporabe teorije zanesljivosti in razpoložljivosti kompleksnih sistemov.

Optimizacijo identifikacijskeha sistema smo izvedli z modeliranjem nevronskih mrež. Rezultati optimizacije identifikacijskih sistemov z nevronskimi mrežami v smislu multimodalnosti v podpoglavju 12.1.3, v procesu identifikacije ponovno pokažejo prednost biometrije v pretočnosti oseb (hipoteza 1), ko lahko reguliramo FAR in FRR za različne varnostne nivoje (pri kartičnem sistemu regulacija ni možna) in hkrati optimiramo konfiguracijo identifikacijskega sistema glede na parametre (velikost baze, mali ali veliki sistemi, varnostni nivo itd.). Za samo analizo podatkov oziroma poteka učenja imamo na voljo grafična orodja, kjer hitro opazimo morebitno napako v gradnji nevronske mreže. Nevronsko mrežo smo implementirali z orodjem EasyNN, ki v procesu učenja omogoča okrog 5000 posnetkov točk, kar zadošča za 200 milijonov ciklov učenja mreže. Na voljo je tudi pregledovalnik napak v primerih za učenje nevronske mreže. Kot smo videli, je bilo za učenje naše mreže potrebnih zgolj 21 korakov, saj je precej enostavna in vsebuje le en skrit nivo. Kompleksnejše mreže za učenje porabijo precej več korakov, prav tako je veliko pomembnejša nastavitev parametrov učenja.

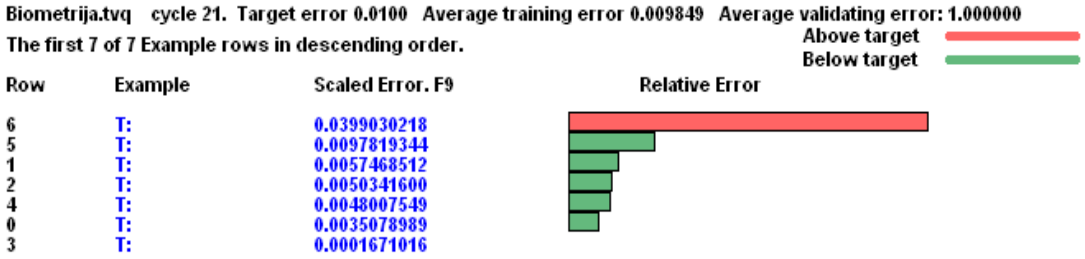
Za izveden prototip nevronske mreže poglejmo rezultate analize (slika 13.1):



Slika 13.1: Ikone za pregled vrednosti in rezultatov prototipa nevronske mreže

Poglejmo:

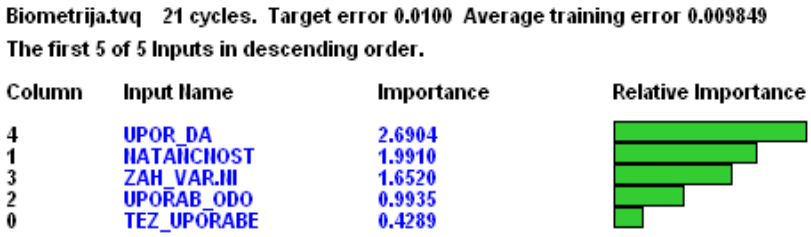
a. absolutne in relativne napake (example errors) (slika 13.2):



Slika 13.2: Graf porazdelitve napak glede na cikle učenja mreže (training row)

Po 21 ciklih učenja nevronske mreže, program določi največjo relativno napako odločitvenega modela, ki je 0,0399. Povprečna vrednost napake s katero bo program sprejemal nadaljne odločitve je 0,009849 in je nižja kot mejna vrednost napake, ki smo jo določili (0,01).

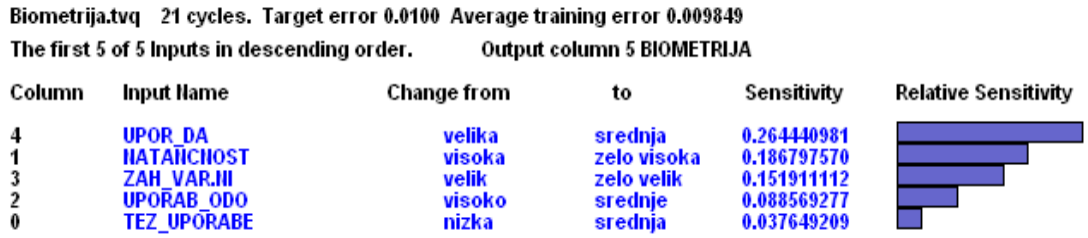
b. kako je program porazdelil uteži vhodnih dejavnikov (input importance) (slika 13.3):



Slika 13.3: Graf porazdelitve uteži glede na vhodne parametre mreže (dejavnike)

Z izračunano povprečno napako odločitvenega modela (0,009849) s programom nadalje določimo pomembnost vhodnih parametrov, na osnovi katerih se bo odločal glede izbire biometrične modalitete ali kombinacije biometrij. Po 21 ciklih učenja program z največjo pomembnostjo ovrednoti vhodni parameter - uporabnost (2,6904) in z najnižjo vrednostjo ovrednoti vhodni parameter - težavnost uporabe (0,4289).

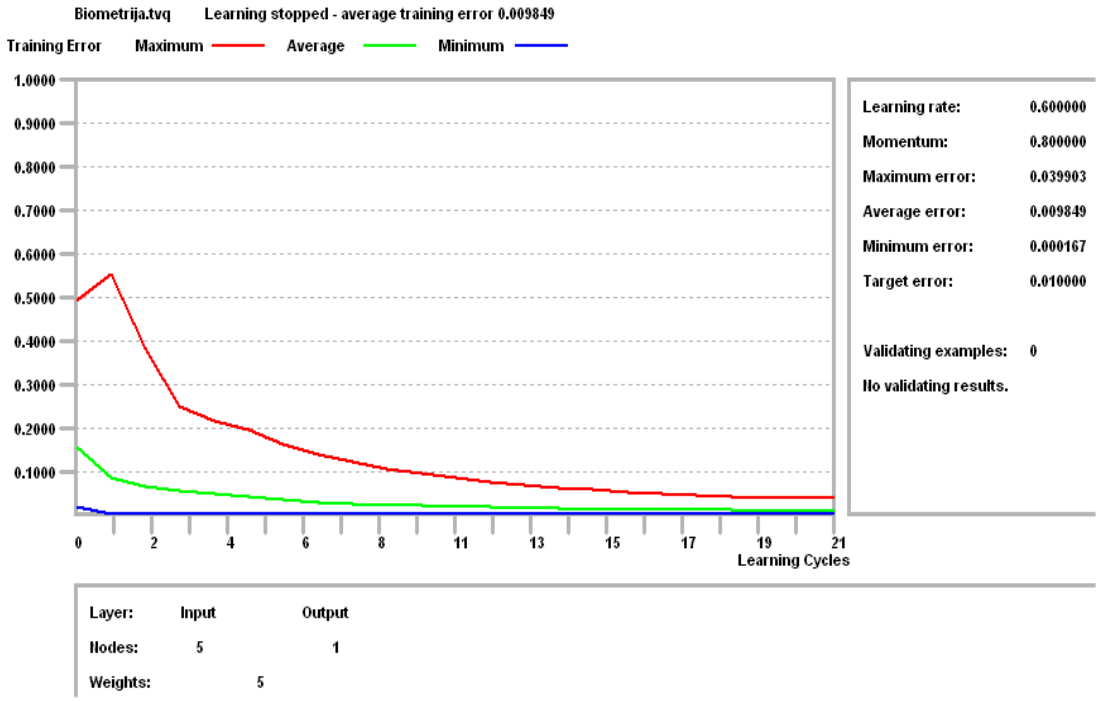
c. in analizo občutljivosti (sensitivity) (slika 13.4):



Slika 13.4: Graf občutljivosti glede na vhodne parametre mreže (dejavnike)

Analiza občutljivosti podaja možne spremembe varnostnih kriterijev vhodnih parametrov pri optimiranju odločitvenega modela. Pri optimizaciji je razvidno, da glede na pomembnost vhodnega parametra program (s povprečno napako 0,009849) predlaga spremembo varnostnih kriterijev. Za naš konkreten odločitveni model, program optimira vhodni parameter – težavnost uporabe, s spremembo varnostnega kriterija »nizko«, v kriterij »srednje«.

d. potek in število ciklov učenja (slika 13.5):



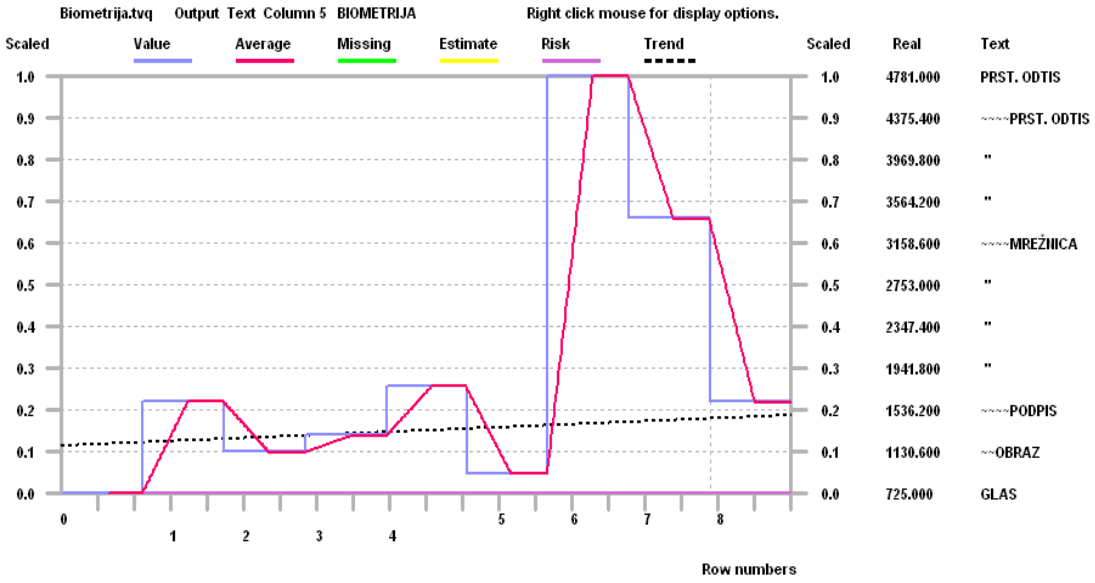
Slika 13.5: Graf poteka in števila ciklov učenja

Grafika podaja potek učenja nevronske mreže in dolžino ciklov, ki so potrebni, da vrednost napake učenja pade pod podano vrednost (0,1). Grafika nam podaja največjo, najmanjšo in srednjo vrednost napake učenja. Iz grafa je razvidno, da največja vrednost napake učenja nevronske mreže pade pod mejno vrednost (0,1) že pri 10 ciklu, vendar program za odločitveni model glede na ostale parametre (hitrost učenja, moment itd.) izvede še preostale cikle.

e. vrednosti za različne biometrične modalitete (slika 13.6):

Vse vrednosti vhodnih in izhodnih stolpcev nevronske mreže so prikazane grafično. Modra linija pomeni dejansko vrednost, rdeča je povprečje in vijolična označuje negotovost (risk number) (EasyNN–User interface manual, 2008). Rdeča linija pomeni maksimalno napako učenja (learning error), modra minimalno napako učenja, oranžna linija pa je povprečna validacijska napaka in je prikazana, če je vsebovan postopek validacije. Iz rezultatov je razvidno, da za podane parametre in

vhodne podatke najbolj ustreza biometrija prstnega odtisa, ki je sicer glede na obstoječe raziskave v praksi tudi najbolj razširjena.



Slika 13.6: Graf vrednosti stolpcev nevronske mreže

Modeli nevronskih mrež v povezavi z biometričnimi sistemi se izkazujejo kot učinkovito orodje za optimiranje identifikacijskih procesov. Tako nastanejo hibridni modeli, ki imajo to lastnost, da so kombinacija vseh prednosti, ki jih ima neka metoda umetne inteligence. Tako se optimalni rešitvi problema lahko še bolj približamo in omogočimo še boljšo optimizacijo, kajti vsak prihranek časa in drugih virov je dragocen. Preizkus metode v doktorskem delu je pokazal, da se pristop s samoučečo se nevronsko mrežo lahko uporabi za optimiranje izbora biometričnih identifikacijskih metod v novi aplikaciji.

13.1 INTERPRETACIJA REZULTATOV GLEDE NA HIPOTEZE

V izvedeni raziskavi smo s preskušanjem dveh neodvisnih hipotez poskušali ugotoviti kakšna je učinkovitost uporabe identifikacijskih postopkov (biometričnih metod in identifikacije s pomočjo kartice) na nivoju uporabnika. Posebej smo ugotavljali ali se je zaradi izvajanja servisnih storitev biometričnih sistemov na daljavo povečala stopnja razpoložljivosti sistema.

V skladu z modelom učinkovitosti, zanesljivosti in razpoložljivosti po Hudoklin in Rozman (2004) lahko glede na dobljene rezultate ocen karakteristik zanesljivosti in razpoložljivosti v desetem poglavju, obe hipotezi potrdimo v njenem celotnem besedilu, kar utemeljujemo z naslednjimi ugotovitvami:

1. Učnkovitost (zanesljivost in razpoložljivost) biometričnih sistemov je glede na izračunane karakteristike $MTTF$, A_S, $\lambda_S(t)$ in $MTTR_S$ (po Weibullovi metodologiji);
   - Ocena zanesljivosti ($MTTF_S$) se z uporabo biometričnega modula izboljša za 12,3 dneva.

Na podlagi navedenih ugotovitev hipotezo 2 SPREJMEMO.

Hipoteza 2
Predpostavljamo, da so biometrični sistemi identifikacije bolj zanesljivi kot kartični identifikacijski sistemi.

- Ocena za $MTTR_S$ je za biometrični modul je s stališča razpoložljivosti boljša za 0,9 dni.
- $\lambda_S(t)$ za SL_CARD, ki je v kartičnemu sistemu najbolj kritičen, pri biometričnemu sistemu odpade, saj pri biometrični identifikaciji ne potrebujemo RFID identifikatorja ali kartice.
- Ocena razpoložljivosti biometričnega sistema A_S je za 2% boljša kot pri uporabi kartičnega sistema, vendar je nujno poudariti, da gre pri biometriji za razmeroma novo tehnologijo, ki je zahtevnejša s stališča uporabe in smo servisne postopke šele vzpostavljali.

2. Pri identifikaciji z biometričnim sistemom odpade modul SL_CARD, ki je šibki člen s stališča učinkovitosti (raziskava pokaže znaten del odpovedi modula SL_CARD že v času enega leta).
3. Čas popravila biometričnih čitalnikov SL_BIOMETRIC je krajši od časa servisiranja kartičnih čitalnikov SL_MMR, povprečno za en dan, kar je za približno 10 % bolje.

Na podlagi navedenih ugotovitev hipotezo 1 SPREJMEMO.

Hipoteza 1
Predpostavljamo, da v procesu osebne identifikacije biometrični sistemi omogočajo večjo pretočnost oseb (razpoložljivost) kot zdaj aktualni kartični sistemi (pametne kartice).

Ugotovljeno smo nadalje potrdili še z markovskim modelom določanja zanesljivosti in razpoložljivosti. Iz raziskave je razvidno, da obdobje staranja oz. izrabljenosti biometričnega sistema nastopi pozneje kot pri kartičnih identifikacijskih sistemih. Očitna je večja razpoložljivost biometričnega sistema identifikacije, stroški vzdrževanja takšnega sistema, pa so s tem manjši. Z matematičnim modelom biometričnega identifikacijskega sistema smo nakazali izvedbo optimizacije, ki zadovoljuje zahteve po razpoložljivosti.

V praksi se glede na ta matematični model, izboljšajo vrednosti parametrov zanesljivosti in razpoložljivosti, kar potrjuje predpostavljeni hipotezi 1 in 2.

Ta del rezultatov pojasnjuje naše predpostavke o višji zanesljivosti, razpoložljivosti in s tem tudi učinkovitosti tudi biometričnih sistemov v primerjavi s kartičnimi sistemi.

Prav tako lahko hipotezi potrdimo glede na interpretacijo učinkovitosti, zanesljivosti in razpoložljivosti po ISO 9126-1 in HBSI modelu, saj so ergonomski parametri za biometrični sistem ugodnejši.

13.2 KRITIČNA INTERPRETACIJA REZULTATOV RAZISKAVE

Raziskava je pokazala, da se obdobje staranja ali izrabe pri biometričnih sistemih prične kasneje kot pri RFID (kartičnih identifikacijskih) sistemih. Zaradi tega je iz raziskave vidna tudi večja razpoložljivost biometričnih sistemov in posledično manjši stroški vzdrževanja. V funkcionalnem in ergonomskem smislu se prednost uporabe biometričnih sistemov kaže v dejstvu, da pri identifikaciji v proizvodno-logističnem procesu ne rabimo dodatnih identifikacijskih elementov.

Pri samem preskušanju in določanju ocen za čase do odpovedi je nujno potrebno poudariti dejstvo, da je biometrija za uporabnika še vedno razmeroma nova tehnologija in je kar nekaj prijav glede nedelovanja biometričnega sistema, rezultiralo v nepravilni uporabi ali celo v nepravilnih nastavitvah sistema. Ker hitrost učenja nekega novega sistema neposredno vpliva na učinkovitost sistema (HBSI) je zaradi tega dejstva, uporaba kartičnega sistema v rahli prednosti, saj je uporabnik z njim že kar dobro seznanjen.

Predstavljena metoda ugotavljanja karakteristik zanesljivosti in razpoložljivosti identifikacijskega sistema s pomočjo Weibullove analize in teorije markovskih verig je bila na danem sistemu uporabljena prvič, zato izračunanih rezultatov za oceno časa do odpovedi in stacionarne razpoložljivosti biometričnega identifikacijskega sistema zaenkrat še ne moremo primerjati s predhodnimi meritvami. Izpeljani model je prvi poskus kvantitativnega modeliranja in analize zanesljivosti in razpoložljivosti predstavljenega identifikacijskega sistema in je namenjen spremljanju parametrov zanesljivosti in razpoložljivosti v prihodnosti; z nadaljnjim evidentiranjem izrednih dogodkov v sistemskem dnevniku bodo izračuni pogostosti odpovedi in zaključkov popravil statistično natančnejši, saj se bo interval opazovanja ustrezno podaljševal. Pri izdelavi in pri uporabi proizvoda lahko na zanesljivost znatno vpliva tudi človeški faktor in se tako uporaba matematičnih in statističnih metod pri modeliranju zanesljivosti spopada z veliko mero negotovosti. Ob izvedbi raziskave je potrebno poudariti tudi dejstvo, da raziskava temelji na desetih določenih vzorcih biometričnega in kartičnega čitalnega modula. To dejstvo nam ob zelo široki ponudbi čitalnih modulov, predstavlja relativno nizek nabor populacije za statistično modeliranje ter splošno podajo ocene zanesljivosti in učinkovitosti.

V nalogi smo razvili nevronsko mrežo, ki jo lahko naučimo izbire biometrične modalitete glede na vhodne varnostne parametre. Omejili smo se na večplastno strukturo z enim skritim nivojem nevronov ter jo učili z znano metodo vzvratnega učenja. Izkazalo se je, da bi bilo za izvedbo računanj izhodov in učenja smiselno narediti logično enoto, ki se nato uporabi za računske operacije pri odločitvenem modeliranju. Praktično uporabnost razvite nevronske mreže smo potrdili na realnih aplikacijah identifikacijskih sistemov. Vzpostavili smo biometrično modaliteto testnega okolja (prstni odtis) in preverjali odločitve nevronske mreže. Sledila so uspešna testiranja nevronske mreže, s katerimi smo potrdili pravilnost odločitve in uporabnost v realnem okolju. V nalogi smo se omejili na testiranje biometrije prstnega odtisa, pa smo zato preverili odločitve nevronske mreže za omenjeno modaliteto, vendar bi za širšo uporabnost bilo smiselno v realnem okolju, testirati še druge biometrične modalitete (šarenica, roženica itd.). V primeru, da se varnostne razmere spreminjajo s časom, ne moremo več predpostavljati, da lahko uporabljamo

vedno isto strategijo učenja nevronske mreže. Izvedba podrobnejše analize postane težavnejša, saj tabela dejavnikov ni značilen ponavljajoč vzorec, kot je to pri konstantnem varnostnem tveganju. Namesto tega moramo upoštevati informacije o varnostnih tveganjih v okviru nekega končnega časovnega intervala, ki prične takrat, ko želimo določiti neko varnostno politiko. Ta časovni načrt se imenuje varnostna ocena tveganja, katerega dolžina ima bistven vpliv na skupne stroške izbrane biometrične tehnologije. Program za gradnjo nevronskih mrež podpira mnogo več, kot smo prikazali za potrebe doktorske naloge. V zaključku naj še enkrat poudarimo, da namen tega dela raziskave ni bil podrobneje analizirati nevronske mreže in izdelati delujočo aplikacijo, ampak raziskati probleme, ki se pojavljajo na tem področju. Rezultate tega dela raziskave smo uporabili v potrditev metodološkega postopka za uspešno klasificiranje biometrije v procesu odločanja s pomočjo nevronskih mrež. Pomembno je spoznanje, da je uporabnost rezultatov simulacije, odvisna od trajanja simulacije. Za boljše simulacijske rezultate, bi morali izvesti vsaj še pet iteracij modeliranja nevronske mreže.

14 RAZPRAVA

Razprava o pomenu zanesljivosti in razpoložljivosti v okviru identifikacijskih sistemov ter prihodnje vloge in pomembnosti za razvoj v svetovnem merilu je razmeroma zahtevna analiza, ki jo otežuje dejstvo, da problem temelji na določenih predvidevanjih in napovedih, kar pa je neizpodbitno povezano z nekaterimi tveganji. Osnovno tveganje je »predvidevanje (ugibanje) zanesljivosti in učinkovitosti človeka«, zato je za analizo pomembno določiti med drugimi tudi sociološki okvir, ki se bo rabil za temeljno ozadje pri razreševanju problema omenjene razprave. Neizbežno dejstvo ob bok zanesljivosti sistema ali gradnika, je zanesljivost in učinkovitost človeka. Človek je kot razvijalec in v končni fazi uporabnik sistema namreč različno zanesljiv in tudi učinkovit (učljiv) glede na različne sociološke dejavnike (starost, izobrazba, okolje v katerem živimo itd). Izpostaviti je potrebno tudi dejstvo, da je v našem okolju dosti ljudi, ki (še) ni nikoli niso uporabili biometrije za identifikacijski postopek. Pri mnogih celo ni opaziti velikega interesa za uporabo tovrstne tehnologije. Vendar pa tuje raziskave razbijajo stereotip, da so ljudje tovrstni tehnofobi, oziroma da jih ne zanima uporaba novih biometričnih tehnologij. Res je, da mnogi ljudje niso zgodnji osvajalci tovrstnih tehnologij, vendar se s splošno prepoznavnostjo, enostavno uporabnostjo, cenovno dostopnostjo ter z uporabnimi aplikacijami počasi veča število tega segmenta uporabnikov. V tem kontekstu je nujno potrebno razmišljati, na kakšen način bi se pospešil proces informatizacije širše družbene skupine za tovrstno tehnologijo. Ob tem je nujno upoštevati ergonomski vidik tako strojne kot programske opreme, ki je vsekakor odločilen pri uvajanju biometričnih sistemov. Učinkovitost biometrične tehnologije v veliki meri zavisi od zanesljivosti in primernosti uporabniškega vmesnika. Če namreč oblikovalec sistema človek-stroj želi razviti uspešen in zanesljiv sistem, mora v zadnjem času vse bolj upoštevati uporabniške vidike in jih tudi ustrezno implementirati v smislu enostavne uporabnosti. Številne študije primerov dokazujejo, da so sistemi, ki so bili že v razvojnih fazah podvrženi ocenjevanju uporabnosti, kasneje veliko bolj uspešni. Poudarek v tem delu je na vgrajevanju zanesljivosti ter uporabnosti v zgodnje faze razvoja in usmerjanje metod in postopkov identifikacije. Za ocenjevanje uporabnosti programske kot strojne opreme imamo na voljo kar nekaj mednarodnih standardov in smernic kot številne metodologije in tehnike. V ta namen smo v prvem delu naloge opravili pregled nekaterih standardov, ki so namenjeni ocenjevanju uporabnosti identifikacijskega sistema. Različne metode so v različnih situacijah različno uspešne, zato v veliki meri od ocenjevalca in njegove izkušenosti zavisi pravilna izbira metodologije ocenjevanja uspešnosti.

Preden spregovorimo o umestitvi dosežkov našega dela v svetovni okvir znanosti, naj povemo nekaj misli glede našega raziskovalnega dela. Splošno znano in tudi sprejeto merilo znanstvenega dela je, da so avtorjeve trditve preverljive in avtentične. Abstraktno raziskovalno delo po navadi začnemo z natančno izraženimi predpostavkami, na podlagi katerih razvijamo teoreme. Znanstveno delo pa lahko izvedemo tudi tako, da skušamo analizirati določena dejstva iz preteklih raziskav ter iz njih izpeljati določene sklepe. Slednji način je bil glede na problematiko raziskave in cilje tega znanstvenega dela primernejši in smo ga pri delu tudi uporabili. Naj poudarimo, da ima ta doktorska naloga značaj razvojno-raziskovalnega dela, ki je na podlagi predhodnih znanstvenih dosežkov usmerjeno predvsem na prenos

rezultatov in ugotovitev v prakso pri upoštevanju določenih specifičnih pogojev. Konkretno gre za raziskavo zanesljivosti in razpoložljivosti novih proizvodov in storitev, ki bodo lahko dolgoročno ključne tudi za uspešnost gospodarstva.

V okviru doktorske naloge smo se osredotočili na problematiko zanesljivosti in razpoložljivosti identifikacijskih sistemov, ki je najprej obravnavana oz. analizirana splošno in teoretično, nato pa konkretno in praktično, kar pomeni izdelavo matematičnega modela in preskušanje realnih sistemov. Za umestitev raziskave v svetovni raziskovalni okvir smo opravli poizvedbe v štirih primarnih podatkovnih bazah ProQuest Digital Dissertations, Inspec&Compendex, ISI Web of Science in Emerald. Pregled baz je pokazal, da podobne raziskave, kot smo jo opravili še ni bila opravljena. V naši raziskavi predstavimo preskuse biometričnih identifikacijskih sistemov in statistično analizo rezultatov po Weibull metodologiji ter matematični markovski model. Takšen način obravnave identifikacijskih sistemov s stališča zanesljivosti in razpoložljivosti je bil uporabljen prvič, zato direktno primerljivi znanstvenih zapisi ali raziskave v pregledanih znanstvenih bazah ne obstajajo. Vsekakor naše delo pomeni doprinos znanosti v delu aplikativnih raziskav, kjer moramo zagotoviti stabilne procese in delujoče proizvode.

Odgovor na vprašanje, kako zagotovljati zanesljivost in razpoložljivost smo iskali v teoretičnih izhodiščih raziskave literature in z izvedbo preskušanj gradnikov obravnavanih sistemov. S proučevanjem raziskovalne problematike smo se soočili z določanjem zanesljivosti in razpoložljivosti, kjer želimo izbrati takšne preskuse gradnikov in sistemov, da bomo z njihovo izvedbo dosegli in potrdili zahtevane kriterije. Na podlagi raziskave literature ter rezultatov preskusov smo zaključili, da so temeljne značilnosti obravnavanih identifikacijskih sistemov naslednje:

- Izvedba takšnih preskušanj in modeliranje zanesljivosti nam omogoča doseči visoko stopnjo zaupanja v zanesljivost identifikacijskih sistemov v fazi razvoja, torej še preden sistem lansiramo na tržišče. Preskušanje zanesljivosti je le del v vrsti preskusov, kamor sodijo tudi preskušanje funkcionalnosti v skladu s kontrolnim planom produkta ali procesa in preskušanje skladnosti in varnosti identifikacijskega sistema pri neodvisnim certifikacijskem organu, v skladu z mednarodnimi standardi. Preskus zanesljivosti in razpoložljivosti tako opravimo v razvojni fazi projekta, kjer je sistem izpostavljen skrajnim vplivom okolice, skladiščenja, transporta in uporabe. Izzvati želimo čim več odpovedi, da odkrijemo šibke točke delovanja in lahko z ustreznimi korektivnimi ukrepi preprečimo ponovitev teh odpovedi. S spremljanjem časov do odpovedi sistema, lahko pri vseh preskusih napovemo, kdaj je konstrukcija sistema dovolj zrela za lansiranje na tržišče. Ugotovitve raziskave sovpadajo s teoretičnimi ugotovitvami številnih avtorjev (Monwar in Gavrilova, 2010; Tronci, Giacinto in Roli, 2009; Kumar in Zhang, 2009), ki pripisujejo velik pomen modeliranju zanesljivosti proizvoda pred vstopom proizvoda na tržišče.
- Spremljanje časa do ponovne vzpostavitve delovanja sistema nam pripomore pri odločitvi glede števila vzdrževalcev za obravnavani sistem in pri določevanju razpoložljivosti. Na podlagi tega in z določitvijo zanesljivosti in razpoložljivosti gradnika pri določeni stopnji zaupanja oblikujemo zahtevane preskuse za gradnike v obliki zahtevanega števila preskušancev, števila opravljenih ciklov, dovoljenega števila odpovedi in števila vzdrževalcev sistema. Dobljene podatke vnesemo v tehnično specifikacijo (tehnično mapo) sistema, kjer navedemo vse

zahteve in definicije za identifikacijske sisteme, med drugimi tudi glede podatke glede njihove zanesljivosti in razpoložljivosti. Takšna specifikacija ponuja preglednost zahtev in je obvezujoča za konstrukterje, razvijalce, tehnologe in v končni fazi tudi za uporabnika v kolikor želi, da mu sistem čimbolje deluje. Izvajanje modeliranja zanesljivosti je del aktivnosti projektnega tima razvojnega projekta, ki ga sestavljajo strokovnjaki razvoja, tehnologije in kakovosti. Odgovornost članov projektnega tima delimo na štiri področja in sicer konstrukcijo, proizvodnjo, kakovost in servisiranje. Ugotovitve raziskave sovpadajo s teoretičnimi ugotovitvami številnih avtorjev (Shunji in Toshihiko, 1979; Kuo, 1985; George, 2001; Hudoklin, Rozman in Brezavšček, 2006; Hudoklin in Rozman, 2004; Liu, 2011), ki pripisujejo velik pomen modeliranju razpoložljivosti proizvoda, pred vstopom proizvoda na tržišče.

- Trenutno je izziv pri razvoju novih izdelkov, ocena zanesljivosti v kratkem časovnem obdobju z namenom izboljšanja kakovosti. Izboljšanje zanesljivosti gradnikov, je nedvomno pomemben vidik kakovosti. To pomeni, da je podatke o zanesljivosti gradnika potrebno pridobiti v kratkem obdobju in rezultate te analize uporabiti v novi razvojni iteraciji ter pri izboljšanju obstoječih gradnikov. Zelo uporabljena metodologija za oceno zanesljivosti je analiza podatkov časov do odpovedi ($MTTF$). Takšna analiza je sestavljena iz modeliranja podatkov življenjske dobe gradnika (časov do odpovedi) s pomočjo regresijskega modela ob upoštevanju nekaj osnovnih statističnih porazdelitev (Weibull, Log-Normal, Gamma itd.) (Ho in Silva, 2006). Usher (1996) predstavi spremenjeni model tehnike iterativnega reševanja, za oceno Weibullovega parametra. Temelji na iterativnemu reševanju v primeru serije sistemov z dvema gradnikoma, ob predpostavki, da je življenjska doba gradnikov opisana z Weibullovo porazdelitvijo. Sarhan (2003) predpostavlja življensko dobo gradnikov s konstantno in eksponentno porazdelitvijo ocen odpovedi. Po Bayesu izračuna največjo verjetnost ocene zanesljivosti gradnikov v primeru serije z n-gradniki. Sarhan (2004) nadgradi svojo teorijo na določanju ocen zanesljivosti za n neodvisnih različnih gradnikov v serijski vezavi. Življenska doba gradnikov je v tem primeru opisana z Weibullovo porazdelitvijo. Chen in Yan (2006) predlagata optimiranje preskusov zanesljivosti in analize življenske dobe kvantalnih verednosti gradnikov z uporabo Monte Carlo simulacije za različne načine in pogoje vzorčenja in čase preskusov, da bi raziskali optimalne pogoje preskusov pri ocenjevanju zanesljivosti na osnovi kvantalnih verednosti. Weibullova porazdelitev merjenih kvantalnih verednosti služi za oceno življenske dobe gradnika (Pan in Chu, 2010). Za primer naše raziskave je uporabljena metoda analize časov do odpovedi ($MTTF$) katere smo lahko opisali z Weibullovo porazdelitvijo. Weibull metodo smo podprli z markovskim modelom, ki je bil v namen določanja zanesljivosti specifičnega biometričnega identifikacijskega sistema uporabljen prvič.
- Skrb za izvedbo modeliranja zanesljivosti mora imeti odgovorna oseba, ki je vključena v projektni tim in sodeluje pri vseh razvojnih odločitvah, tehničnih pregledih konstrukcije in preskušanjih, ki se tičejo zanesljivosti in razpoložljivosti. Od odgovorne osebe se pričakuje poznavanje modeliranja zanesljivosti, vodenja projektov upoštevajoč zahtev in smernic in uporabo različnih metod in tehnik (ISO, APQP, FMEA, SWFMEA itd.) s katerimi lahko vplivamo na zanesljivost ter razpoložljivost. Sodobni pristopi k spodbujanju kakovosti so v ospredje postavili

celovit pristop, ki obsega vzročno posledični princip celotne organizacije vprocesu trženja, prodaje in poprodajnih aktivnosti proizvoda. Te aktivnosti potekajo vzporedno z razvojnimi fazami in se odražajo v izboljševanju konstrukcije. Uporabo naštetih metodologij in alktivnosti prilagajamo glede na posamezen projekt, poskrbimo za sprotno obravnavanje kritičnih točk in v čimkrajšem času poiščemo ter analiziramo rešitve z namenom izboljšanja zanesljivosti in razpoložljivosti (FRACAS). K višji stopnji zaupanja v napovedano zanesljivost in razpoložljivost identifikacijskih sistemov prispeva tudi dovolj dolgo preskušanje pri končnih uporabnikih, kar smo v nalogi tudi izvedli. Izsledke takšnega spremljanja v smislu poprodajnih aktivnosti naknadno upoštevamo pri konstruiraju izdelkov v smislu APQP zanke. Naše ugotovitve v raziskavi sovpadajo z ugotovitvami različnih avtorjev (Kern-Pipan, 2010; Madu,1999; Hudoklin in Rozman, 2004).

- Nevronske mreže so uporabne na mnogih področjih zaradi potrebe po specifikaciji odločitvene funkcije in samodejne aproksimacije te funkcije na osnovi nabora učnih primerov. Njihova uporabnost za potrebe biometričnih sistemov je znana predvsem pri problemih z nejasnimi, nekonsistentnimi in tudi delno nepoznanimi matematičnimi zapisi biometričnih vzorcev ter tudi pri obravnavi nepopolnih vhodnih podatkov (manjka del vzorca prstnega odtisa, vzorec prstnega odtisa je slabo viden itd.). Njihova velika vrednost v biometričnih aplikacijah se pokaže pri analiziranju velike količine podatkov, iskanju vzorcev, relacij in lastnosti objektov v slabo definiranih problemskih situacijah, kjer pravila niso poznana. Optimizacija z nevronskimi mrežami odpira nova poglavja v tematiki učinkovitosti biometričnega sistema, kar dokazujejo raziskave in teoretična dognanja mnogih avtorjev (Malcangi, 2007; Garcia in Delakis, 2004; Hidalgo, Melin in Licea, 2008; Melin in Castillo, 2005). Te ugotovitve prav tako potrjujejo tudi zaključke naše raziskave.

Tabela 14.1 v nadeljevanju opisuje pregled ugotovitev iz raziskav in literature kjer smo razvrstili dejavnike, katerih izsledki so bili za neše raziskovalno delo zelo pomembni. Raziskave obravnavajo različne dejavnike, in njihov vpliv na izboljšanje kakovosti proizvoda in storitev ter so s stališča obravnave problematike blizu naši raziskavi.

Tabela 14.1: Vpliv dejavnikov na kakovost proizvoda ter storitev

	Dejavniki	Avtor	Sklepna ugotovitev
1	Modeliranje zanesljivosti sistemov.	Monwar, 2010; Tronci, Giacinto in Roli, 2009; Kumar in Zhang, 2009; Karimi in Hüllermeier, 2005; Rausand in Hoyland, 2004	Izsledki raziskav kažejo na to, da je za določanje zanesljivosti možno uporabiti več pristopov, vendar je modeliranje zanesljivosti z oceno časa do odpovedi (*MTTF*) primerno, ko moramo hitro podati oceno zanesljivosti.

2	Modeliranje razpoložljivosti sistemov.	Shunji in Toshihiko, 1979; Kuo, 1985; George, 2001; Hudoklin, Rozman in Brezavšček, 2006; Hudoklin in Rozman, 2004	Izsledki raziskav in pregled relavantne literature kažejo na to, da statistično modeliranje razpoložljivosti (*A*), igra pomembno vlogo pri planiranju vzdrževalnih storitev ter vzdrževalcev.
3	Uporaba statistične metodologija pri modeliranju zanesljivosti in razpoložljivosti.	Ho in Silva, 2006 ; Pan in Chu, 2010; Chen in Yan, 2006; Sarhan, 2001; Usher, 1996; Monwar, 2010; Mettas in Zhao, 2004, Chase in drugi, 1998; Sarhan, 2003; Sarhan, 2004; Chi-Chao, 1997	Izsledki raziskav kažejo, da je statistično vrednotenje po Weibull metodologiji primerno za serije, kjer imamo malo vzorcev in daje tudi v teh primerih natančne rezultate pri ocenjevanju zanesljivosti.
4	Metode in tehnike kakovosti za povečanje zanesljivosti.	Kern-Pipan, 2010; Côté in Georgiadou, 2006; McCall, 1977; Marolt in Gomišček, 2005; Solina, 1997; Madu, 1999	Rezultati raziskav in pregled relavantne literature dokazuje pozitiven učinek metod in tehnik ter s tem tudi vpliv na izboljševanje zanesljivosti in razpoložljivosti, tako programske kot strojne opreme biometričnih sistemov.
5.	Optimiranje biometričnih sistemov s pomočjo nevronskih mrež.	Malcangi, 2007; Garcia in Delakis, 2004; Hidalgo, Melin in Licea, 2008, Melin in Castillo, 2005	Pregled relavantne literature ter rezultati raziskav postavlja nevronske mreže v ospredje, ko je potrebno optimirati biometrični sistem. Optimizacija biometričnih sistemov z nevronskimi mrežami ima pozitiven učinek na varnost, hitrost ter ergonomijo v procesu identifikacije.

Na področju proučevanega ugotavljamo večplastni prispevek k znanosti naše raziskave, ki temelji predvsem na modeliranju zanesljivosti, razpoložljivosti, statističnemu vrednotenju rezultatov preskusov in s tem tudi zagotavljanju kakovosti v vseh fazah obravnave proizvoda. Za doseganje predpisane kakovosti proizvoda je nujno upoštevati naštete dejavnike, če želimo ustvariti takšen proces, kjer stalne izboljšave zanesljivosti in razpoložljivosti postanejo del učinkovitega procesa. Zavest zaposlenih in tudi njihova zanesljivost, pa je ob tem neizogibna, da bi lahko zagotavili proces stalnih izboljšav. Seveda ob tem ne smemo pozabiti na vrsto postopkov s katerimi neposredno in posredno vplivamo na dvig kakovosti procesa in proizvoda, kot so npr. certificiranje proizvoda pri neodvisnemu akridetacijskemu organu, notranje presoje, neodvisne procesne ISO presoje, izobraževanje zaposlenih, vzpodbujanje inovacij, EFQM, TQM itd.

Naše zaključke o načrtovanju stalnih izboljšav, notranjih in zunanjih presojah ter programu zanesljivosti, ki pripomorejo k dvigu zavesti in tudi zanesljivosti zaposlenih na vseh nivojih procesa, so potrdila mnoga teoretična dognanja avtorjev, (Kern-Pipan, 2010; Marolt in Gomišček, 2005; Côté in Georgiadou, 2006).

V nadaljevanju bomo podali pregled izsledkov raziskav dejavnikov, ki so bili za nas med pomembnejšimi v raziskovanju. Raziskave obravnavajo različne dejavnike in njihov vpliv na zanesljivost, razpoložljivost in učinkovitost biometričnih sistemov, ki izvirajo bodisi iz vidika uporabe metodologij ali z vidika tehnologije. V tabeli 14.2 podajamo temeljne ugotovitve, ki smo jih pridobili s primerjavo izsledkov rezultatov izbranih raziskav, ki so po raziskovalni problematiki najbližje naši raziskavi:

Tabela 14.2: Primerjava temeljnih izsledkov izbranih primerov raziskav z našo raziskavo

Komponente primerjave	Avtor			
	Monwar (2010)	Kuo, (1985)	Ho in Silva (2006)	ta raziskava
1.modeliranje zanesljivosti	Obravnava zanesljivosti multimodalnega biometričnega sistema.	*MTTF*, Obravnava zanesljivosti za male velikosti vzorcev, ko so časi do odpovedi in čas popravila eksponentno porazdeljeni.	*MTTF*, Weibull	*MTTF*, Weibull, Markovski model (opis stanj, verjetn ostni graf), za biometrični sistem.
2. modeliranje razpoložljivosti	-	*MTTR*, Obravnava razpoložljivosti na osnovi Bayesove cenilke.	-	*MTTR*, Weibull, *A*,Markovski model (opis stanj, verjetn ostni graf), za biometrični sistem.
3.vzdrževanje	-	-	-	Določeno št. vzdrževalcev za obravnavani sistem.
4.statistično modeliranje	-	Bayesian	Weibull	Weibull (ročno in *Weibull++7*)
5.orodja kakovosti	-	-	-	Obravnavana orodja kakovosti za identifikacijski (biometrični)

				sistem.
6. optimiranje	Optimiranje biometričnih podatkov večih podatkovnih baz s pomočjo markovskih verig.	-	Optimiranje s porazdelitvijo vzorcev »bootstrap«.	Multimodalnost biometrije na osnovi optimiranja z nevronsko mrežo.

Ugotovitve iz primerjave raziskav različnih avtorjev kažejo na to, da so področja primerjanih raziskav delno zastopana v naši raziskavi, vendar se razlikujejo bodisi po namenu raziskave, kakor tudi po obsegu in vrsti obravnavanih dejavnikov. Kuo (1985) tako izvede preračun ocene razpoložljivosti na osnovi Bayesove cenilke. Liu (2011) obravnava dejavnike tveganja pri uporabi biometrične tehnologije v EU in ZDA, za obravnavane varnostne programe VIS in US-VISIT. Nobena raziskava, ki smo jo primerjali z našim delom, ne obravnava celovitega modela razpoložljivosti biometričnega sistema z Weibullovim pristopom in markovskim modelom. Ugotovitve ob pregledu znanstvenih baz kažejo na to, da je področje razpoložljivosti biometričnih sistemov slabo pokrito in, da naše delo predstavlja prvi tovrsten pristop k obravnavi biometričnega identifikacijskega sistema, z vsporedno vezavo čitalnih enot (pasivna redundanca).

Na področju zanesljivosti smo pri pregledu znanstvenih baz ter raziskav sicer našli več zadetkov in tudi raziskav, vendar zelo malo teh, se nanaša na modeliranje zanesljivosti za primere biometričnih sistemov. Ugotovitve po pregledu in primerjavi raziskav potrjujejo pravilno izbiro Weibullove statistične metodologije pri obravnavi majhnega števila preskušancev, kar je dognalo tudi vrsto avtorjev (Monwar, 2010; Tronci, Giacinto in Roli, 2009; Kumar in Zhang, 2009; Karimi in Hüllermeier, 2005; Rausand in Hoyland, 2004). Vendar pa na drugi strani, nobena raziskava ne predvideva matematičnega modeliranja, z uporabo stohastičnih procesov in markovskega modela (str.199), kar smo opravili v naši raziskavi. Ta pristop daje iste rezultate pri določanju zanesljivosti in razpoložljivosti, kot smo jih dobili z Weibull metodo (str.197). Oba pristopa tako dajeta iste rezultate pri merjenih časih do odpovedi in med odpovedmi na eni strani ter izračunanimi vrednostmi pogostosti odpovedi na drugi. Ta del raziskave potrjuje smiselnost uporabe stohastičnih procesov in markovskih verig, pri modeliranju zanesljivosti biometričnih sistemov ter je tudi prvi takšen pristop pri modeliranju zanesljivosti biometričnih sistemov.

Področje obravnave nevronskih mrež našega raziskovalnega dela nas je privedlo do zaključkov:

- nevronske mreže so sposobne reševati probleme, ki jih matematično težko izrazimo in hkrati oblikujejo predstavitve informacij,
- nevronske mreže se prilagajajo zahtevam okolja,
- nevronske mreže zgradijo odločitveni model, na osnovi katerega sprejemajo odločitve in
- nevronske mreže z učenjem izboljšujejo učinkovitost.

Ugotovitve v naši raziskavi se bistveno ne razlikujejo od ugotovitev v raziskavah drugih avtorjev, vendar smo v našem primeru nevronske mreže uporabili za izbiro

pri načrtovanju in optimiranju biometrične modalitete, kar je prvi takšen poizkus odločitvenega modeliranja pri optimizaciji identifikacijskega sistema na osnovi variabilniega modela zahtevanih varnostnih parametrov.

S tem ugotovljamo, da je naše raziskovalno delo doprineslo več znanstvenih prispevkov na različnih področjih obravnave biometričnega sistema in tako daje doprinos k znanosti na področju obravnave biometrične identifikacije s stališča zanesljivosti, razpoložljivosti in učinkovitosti.

15 ZAKLJUČKI IN IZHODIŠČA ZA NADALJNJE RAZISKOVANJE

V zadnjih dveh desetletjih smo doživeli precejšen preobrat v razmišljanju in tudi življenju, ki ga zaznamuje čedalje večja liberizacija gospodarstva in mobilnost kapitala ter ljudi. V sedanjem okolju so spremembe zelo hitre in dostopen je skoraj vsak košček na Zemlji. Za čim manj ovirano mobilnost rabimo identifikacijske sisteme, ki omogočajo zanesljivo identifikacijo kadarkoli in kjerkoli. Bistven dejavnik je biometrična identifikacijsko komunikacijska tehnologija, ki s svojim razvojem pripomore, da uporaba fizičnih identifikatorjev ni več nujna za potrditev naše istovetnosti. Seveda nove biometrične identifikacijske tehnologije prinašajo nove organizacijske paradigme in vplivajo na sociološke spremembe. Vedno več identifikacije namreč poteka tako, da zanjo sploh ne vemo, s čimer se v identifikacijski postopek vnašajo elementi virtualnosti. Računalnik se je že skrčil na velikost čipa in ga lahko vstavimo v človeško telo z namenom identifikacije. V prihodnosti bomo imeli kvantni računalnik, ki bo sposoben ohranjati in analizirati velikanske količine podatkov ter se na njihovi podlagi odločati kot človek (Reddy, 2006). Razlaga[51] bionskega človeka se pojavlja v povezavi z eksperimentalnim delom glede na napredek naše vrste kot napredek s pomočjo kombiniranja človeškega telesa s strojno opremo. Gre za zelo preprosto tehnologijo, ki se uporablja pri živalih in se bo zelo verjetno lahko uporabila tudi pri ljudeh. Dosedanje raziskave celičnih avtomatov (Šemrov in drugi, 1996) lahko uporabimo kot modele za kompleksne biokibernetske sisteme in za modeliranje kemičnih reakcij pri vgrajevanju identifikacijskih elementov v človeško telo, kar bi lahko prineslo velike prednosti.

Globalizacija je torej družbeni pojav, ki ima poleg ekonomskih še politične, socialne, tehnološke in varnostne razsežnosti. Sodobne biometrične tehnologije in sodobne identifikacijske storitve, njihove čedalje nižje cene ter odprava ovir vsled različne zakonodaje so prispevali k temu, da se je mobilnost ljudi in izdelkov izjemno povečala. Da bi lahko zadostili strogim varnostnim standardom in čim manj posegali v človekovo avtonomijo moramo poskrbeti za optimalno zanesljivost in razpoložljivost identifikacijskih sistemov.

Primerjalna raziskava zanesljivosti in razpoložljivosti identifikacijskih sistemov je jasno pokazala prednosti biometrije tako v praktični uporabi kot v varnosti podatkov pri avtomatizaciji osebne identifikacije. Osebna odgovornost in natančnost na področjih, kot so zakonodaja, usklajenost s predpisi, proizvodnja in menedžment dobavne verige na nivoju globalnih tehničnih operacij, sta ob avtomatizaciji identifikacije obvladovani. Eden od razvojno raziskovalnih projektov, ki bo zagotovo naredil korak v smer širše uporabe biometrije, je implementacija biometričnih čitalnikov v sisteme javne uporabe, ki bodo delno nadomestili zdaj znane čipne kartice in identifikacijske elemente z integriranimi čipi.

Za učinkovito upravljanje biometrične tehnologije ni dovolj le popolno razumevanje tehničnih karakteristik, operacijskih sistemov in programske opreme, temveč moramo dobro poznati tudi odnose med posameznimi gradniki sistema; samo tako

[51] *Cochrane je prvi človek, ki si je dal implementirati identifikacijski čip v telo.*

bomo namreč lahko razvili ustrezne modele, ki odražajo dejanski (konkretni) identifikacijski sistem. Obstaja področje matematične teorije, na podlagi katerega je moč razviti ustrezne matematične modele realnih identifikacijskih sistemov, s katerimi si lahko tudi v praksi pomagamo pri ocenjevanju razpoložljivosti in zanesljivosti njihovega delovanja. Seveda ni dovolj, da model postavimo enkrat za vselej. Gre namreč za proces, ki se pravzaprav nikoli ne konča (APQP), saj je okolje, v katerem deluje identifikacijski sistem, spremenljivo in zahteva nenehno spremljanje in prilagajanje. Zato ima izreden pomen planiranje in upravljanje zanesljivosti in razpoložljivosti skozi celoten življenjski cikel informacijskega sistema, od začetne faze načrtovanja, implementacije, do samega delovanja sistema. Skozi spremljanje sistema pa ugotavljamo spremembe in potencialno potrebo po obnavljanju in dopolnjevanju procesa zagotavljanja zanesljivosti in razpoložljivosti.

Druga možnost izboljšave učinkovitosti prepoznave pa leži v kombinaciji različnih biometričnih in varnostnih metod. Optimizacijo identifikacijskega procesa smo izvedli s pomočjo metode simulacije nevronske mreže. Tako smo v kombinacijah s sistemi za prepoznavo obrazov uporabili tudi prepoznavo zvoka, prstnih odtisov ali očesne šarenice. Najuspešnejše aplikacije so še vedno tiste, ki uporabljajo majhno ali srednje veliko podatkovno bazo oseb. Takšne sisteme največkrat uporabljamo za kontrolo dostopa ali vstopa v računalniški sistem. Sistemi za kontrolo na letališčih ali za nadzor v javnih prostorih ostajajo izziv za raziskovalce. Takšni sistemi so pri velikem številu oseb, ki jih morajo pregledati, ter zaradi zelo različnih pogojev zajemanja še vedno nezanesljivi. S povezovanjem nevronskih mrež in odločitvenih sistemov v postopkih identifikacije lahko tudi takšni sistemi postanejo bolj zanesljivi. S pomočjo sistemske dinamike smo razvili model nevronske mreže za izbiro identifikacijskega sistema. Na podlagi zgodovinskih podatkov smo v raziskavi pokazali, da se je učljiva nevronska mreža sposobna prilagajati različnim zahtevam varnostnega okolja, ki je po naravi stohastične narave.

Samo preverjanje zanesljivosti in razpoložljivosti pa ne zadostuje za uspeh na tržišču, potreben je aktiven pristop k dvigovanju učinkovitosti (zanesljivosti in razpoložljivosti), da blagovna znamka ali proizvod, ki ga ponudimo tržišču ne postane sinonim za nezanesljivost. Zaradi nezanesljivosti in slabe razpoložljivosti pride do pomanjkanje zaupanja in se poruši sodelovanje med uporabnikom in proizvajalcem. Poslovni odnos kupec – dobavitelj vsebuje veliko osebne note, ki zadovoljuje obe vpleteni strani. Iz tega nastane medsebojno zaupanje, ki temelji tudi na vestnosti in zanesljivosti človeka. Osebe, ki so vključene v ta odnos, morajo imeti nekatere značilne osebnostne lastnosti. Prav tako morajo osebe, ki vodijo program zanesljivosti izkazovati zanesljivost v največji meri, saj je prav od njih odvisno zaupanje na relaciji uporabnik – proizvajalec in s tem preživetje podjetja na trgu. Zaupanje med dobaviteljem in kupcem je temelj poslovanja in lahko vodi do povečanega obsega sodelovanja. S tem je zagotovljeno zadovoljstvo vseh strani in ugled v družbi. Ključne osebnostne lastnosti posameznika pri vodenju projektov, lahko na ta način krojijo politiko celotnega podjetja. Ravno zaradi teh lastnosti so lahko nekateri posamezniki v poslovnem svetu uspešni in znajo spletene poslovne vezi vzdrževati ter jih tudi obdržati.

Znanost, ki razvija sodobne tehnične rešitve, je temeljni vzvod povečanja produktivnosti in konkurenčnosti gospodarstva. Gospodarski osebki imamo pomembno nalogo, da sočasno razvijamo lastno tehnologijo na podlagi dosežkov

sodobne znanosti in jo tudi razumno vključujemo kot znanje v razvoj, proizvodnjo in storitve.

15.1 KAKO POVEČATI ZANESLJIVOST PROGRAMSKE OPREME IDENTIFIKACIJSKIH SISTEMOV

Modeli, ki omogočajo izboljšanje zanesljivosti programske opreme identifikacijskih sistemov (zmanjšati trenutno pogostost odpovedi λ), so analitični modeli. Spoznali smo dva, binomskega in Poissonovega. Osnovne predpostavke binomskega modela so:

a. Ko se odpoved pojavi, napako takoj odpravimo.
b. V programu je fiksno število napak μ_0.
c. Posamezne odpovedi se pojavljajo naključno, neodvisno druga od druge. To pomeni, da so $\lambda a(t)$ za posamezne napake enake.

Model ne dovoljuje obravnave napak, ki se ne dajo locirati, napak, ki jih najdemo s preverjanjem kode, in napak, uvedenih s popravljanjem.

Tudi pri Poissonovem modelu se odpovedi pojavljajo neodvisno in naključno v času. Tukaj je število napak, v programu v času t=0 (začetku preskušanja, uporabe, izvajanja), naključna spremenljivka, porazdeljena po Poissonovem zakonu s povprečjem ω_0. Pri določevanju zanesljivosti si tako pomagamo s specifičnimi modeli:

- Jelinski-Moranda model (binomski),
- bazični Musa model (Poissonov),
- logaritmični Musa model (Poissonov).

Načrtovanje in izboljšanje zanesljivosti programske opreme je nujno upoštevati že v fazi razvoja. Našteli smo nekaj modelov, ki jih glede na posamezen primer in značilnosti projekta uporabimo pri modeliranju zanesljivosti programske opreme. V pomoč pri računanju zanesljivosti pa so tudi programska orodja (SHARPE, SREPT itd.), katera nam delo olajšajo, predvsem pa časovno skrajšajo v primeru kompleksnih programov.

Poleg modelov in programskih orodij pa lahko zanesljivost povečamo tudi s tehnikami, ki neposredno vplivajo na kakovost, na nivoju podjetja (APQP, FMEA, TQM, 6σ itd.) ter načrtovanjem testnh postopkov, v fazi razvoja. Na osnovi izkušenj, pa v postopke naslednjih razvojnih projektov integriramo metodologije, ki preprečijo ponovitve napak.

15.2 PRIHODNOST IN SMERNICE ZA NADALJNJE DELO PRI RAZVOJU BIOMETRIČNIH SISTEMOV

Pričakovati je, da bo biometrična tehnologija kljub pomislekom nekaterih inštitucij (urad za varstvo osebnih podatkov) v polnem razmahu dosegla tudi Slovenijo. Z razvojem biometrične tehnologije se namreč pojavlja mnogo etičnih vprašanj, ki zadevajo človekovo osebnost, zasebnost in nadzor (Nadel, 2006). Identifikacijski sistemi namreč družbi žal ne prinašajo le koristi. Njihova uporaba lahko povzroča tehnične probleme in načenja moralna vprašanja (Gates, 2004), ki se jih moramo

zavedati tudi razvijalci in uporabniki te tehnologije. Celotna človeška družba je zaradi odvisnosti od informacijskih sistemov vedno bolj ranljiva. Med novimi družbenimi problemi, povezanimi z avtomatizacijo identifikacije, so najbolj pereči: računalniški kriminal, varnost računalniških sistemov, kraja programske opreme, varstvo intelektualne lastnine, računalniški virusi, nezanesljivost programske opreme in škoda, ki jo napaka v njej lahko povzroči, podatkovne zbirke in varstvo zasebnosti in druge družbene posledice ekspertnih sistemov.

Sodeč po napovedih bo v novem tisočletju področje identifikacije doseglo nesluten razvoj. Dober kazalec zrelosti tehnologije so investicije in vložki v panogo. Leta 2002 je ameriška vlada vložila v biometrično industrijo 16,63 milijona dolarjev. Pričakovani dohodek te industrije v letu 2014 je 9000 milijonov dolarjev (International Biometric Group, 2008).

Glede na zahteve ZVOP-1 je ključna pridobitev dovoljenja (IP-RS, 2011) pri informacijskem pooblaščencu[52], pri čemer je treba utemeljiti, zakaj je uvedba biometričnih ukrepov v vašem primeru nujna za enega ali več taksativno naštetih namenov: opravljanje dejavnosti, varnost ljudi ali premoženja, varovanje tajnih podatkov ali varovanje poslovne skrivnosti.

Biometrične metode postajajo zelo popularna alternativa tradicionalnim pristopom k identifikaciji. Uporaba biometričnih metod poenostavlja identifikacijo in povečuje zanesljivost, saj so elementi identifikacije (prstni odtis) neprenosljivi in preprečujejo zlorabo in nepooblaščeno uporabo. Prednosti biometrije so jasne, saj ni potrebna uporaba kartice ali drugih identifikacijskih elementov. Z avtomatizacijo identifikacije bosta omogočena združevanje in primerjava trenutnih procesnih podatkov s podatki iz integralnega informacijskega sistema ali drugih poslovnih aplikacij. Vse to pa zagotavlja večjo preglednost ter boljše načrtovanje in izkoristek procesov identifikacije.

Nadaljne raziskave identifikacijskih sistemov lahko usmerimo v proučevanje ekonomskega vpliva modeliranja zanesljivosti, razpoložljivosti in učinkovitosti ter jih povežemo s finančnimi rezultati.

Predvidevamo, da bomo pri nadaljnih raziskavah lahko uporabili testno okolje, kjer bodo v veliki meri že odpravljene odpovedi zaradi uvajanja nove tehnološke rešitve pri uporabniku, za primer biometričnega sistema.

Nadaljne raziskave bomo posvetili tudi iskanju optimalnih modalnosti identifikacijskega sistema s pomočjo nevronskih mrež. Med drugim predvidevamo, da bomo še izboljšali natančnost nastavitev parametrov FAR in FRR za podane varnostne kriterije. Obstaja več možnih smeri razvoja nevronskih mrež, in sicer:

- nevronske mreže za nadzor in vodenje uporabniško specifičnih sistemov za učenje, obdelavo podatkov in zabavo. Nevronska mreža bi prek senzorjev zaznavala vpliv vsebine na človeka (srčni utrip, krvni pritisk, ionizacija kože itd.) in tako dobila zahtevane povratnozančne parametre;

[52] *Informacijski pooblaščenec, Vošnjakova 1, PP 78, 1000 Ljubljana. Obrazec za prijavo biometričnih ukrepov ni predpisan, lahko pa je v pomoč pri oblikovanju zahteve za izdajo dovoljenja pred uvedbo biometričnih ukrepov.*

- nevronske mreže bi nam skupaj z drugimi tehnologijami umetne inteligence, nevrologije in genetike pomagale ustvariti umetno življenje v kakršnikoli obliki (človek, stroj, hibrid itd.);
- nevronske mreže bi nam lahko pomagale pri odkrivanju miselnih procesov ter posledično človekovih sposobnosti. V povezavi z nevropsihologijo bi bila mogoča komunikacija med človekom in strojem.

Nadaljevanje raziskovalnega dela vidimo v podrobnejši razdelitvi biometričnih značilnostih. Sledi postavitev kompleksnejše nevronske mreže (več skritih nivojev, več vhodov, tudi več izhodov). Tip vrednosti na vhodu in izhodu bi lahko bil številski (namesto tekstovni). Tudi pri nastavitvi korakov učenja bi veljalo narediti različne poskuse, spreminjati moment uteži itd. Možnosti za nadaljnje raziskovanje začete teme je tako več kot dovolj. Nekoliko izpopolnjena umetna nevronska mreža bi zagotovo našla prostor kot pripomoček pri optimizaciji procesa odločitve o konfiguraciji nove aplikacije glede na potrebe naročnika. Uporaba umetne nevronske mreže nedvomno pomeni izziv na področju biometričnih identifikacijskih sistemov.

Veliko je še možnosti izboljšanja kriptoalgoritmov za bometrični sistem, kjer bomo povečali varnost in hitrost digitaliziranih informacij biometričnih podatkov.

Eden od pomembnih ciljev nadaljnega dela je nadgradnja matematičnega modela na osnovi markovskih verig, ki je bil narejen med izdelavo doktorske naloge s sistemom množične strežbe, v polno zmogljiv sistem. Z analizo identifikacijskih sistemov smo dobili podatke, ki nam omogočajo uvajanje izboljšav v obstoječe matematične modele in realne sisteme. Sisteme bomo medsebojno primerjali ter projektirali in razvili nove identifikacijske strežne sisteme. S tem bomo mehanizem strežbe optimirali z maksimalno zmogljivostjo in razpoložljivostjo.

16 KRATICE IN AKRONIMI

2D: Two Dimensions (dvo-dimenzijski)

3D: Three Dimensions (tri-dimenzijski)

A

AFP: Automatic Face Processing (avtomatska obdelava značilk obraza)

ANSI: American National Standards Institute (ameriški nacionalni inštitut za standardizacijo)

ARRS: Javna agencija za raziskovalno dejavnost Republike Slovenije

ASEP: Accident Sequence Evaluation Programme (program za sekvenčno ocenjevanje nesreč)

ASME: American Society of Mechanical Engineers (ameriško združenje strojnih inženirjev)

AT&T: American Telephone & Telegraph (AT&T je ameriška družba za telekomunikacije)

B

BS: British Standard (angleški standard)

BCC: The Biometric Consortium Conference (konferenca konzorcija za biometrijo)

BEM WG: Biometric Evaluation Methodology Working Group (združenje za ocenjevanje biometrične tehnologije)

BRA: Biometric Reference Architecture (referenčna arhitektura za biometrijo)

C

CASE: Computer Aided System Engineering (računalniško podprto načrtovanje sistemov)

CAD: Computer Aided Design (računalniško podprto načrtovanje in razvoj)

CAGR: Computed Annual Growth Rate (skupna letna stopnja rasti)

CAM: Computer Aided Manufacturing (računalniško podprta proizvodnja)

CBEFF: Common Biometric Exchange Formats Framework (standard za izmenjavo biometričnih podatkov)

CCTV: Closed Circuit Television cameras

CERIF: Common European Research Information Format (podatkovni model)

CER: Crossover Error Rate; CER = EER

CITeR: Center for Identification Techology Research (center za raziskave identifikacijske tehnologije)

CMMI: Capability Maturity Model Integration (združen zmožnostni zrelostni model)

CODIS: Combined DNA Index System

CSI: Card Services International

D

DOF: Degrees Of Freedom (prostostne stopnje)

DET: Detection Error Trade off Curve (krivulja izmerjenih napak; FNMR glede na FMR ali FRR glede na FAR)

DNA: Deoxyribonucleic Acid, DNA = DNK

DNK: Deoksiribonukleinska Kislina; DNK = DNA (Deoxyribonucleic Acid)

DES: Data Encryption Standard (standard za kriptiranje podatkov)

E

EER: Equal Error Rate (stopnja enake napake); EER = CER

EEPROM: Electrically Erasable Programmable Read–Only Memory (Električno zbrisljiv in programirljiv bralni pomnilnik)

ECC: Elliptic–Curve Cryptography (eliptične krivulje za uporabo v kriptografiji)

EPC: Electronic Product Code (elektronska koda za identifikacijo proizvoda)

Eepc: extended Event–Driven Process Chain (Razširjena dogodkovno vodena veriga procesov, kjer na enem diagramu združimo prikaz organizacijskega, procesnega in podatkovnega pogleda na poslovni proces.)

EFQM European Foundation for Quality Management (Evropska fundacija za kakovost)

ELS: Electronic Locking Systems (ELS je elektronski sistem pristopne kontrole, razvit v podjetju Metra inženiring d. o. o.)

EPC: Electronic Product Code (EPC Global je trenutno vodilni razvijalec standardov za podporo RFID, ki deluje pod okriljem GS1.)

EU: European Union (Evropska unija)

F

FAR: False Acceptance Rate (delež napačnih odobritev; lahko definiramo tudi z verjetnostjo. Primer: FAR 0,1 % pomeni uspešno registracijo 1 neavtoriziranega oz. neobstoječega uporabnika v sistemu 1000 uporabnikov); FAR = FMR

FBI: Federal Bureau of Investigation (zvezna varnostno–policijska organizacija, v ZDA)

FER: Failure to Enrol Rate (delež nezmožnosti registracije); FER = FTE.

FMR: False Match Rate (delež napačnega ujemanja); FMR = FAR

FNMR: False Non–Match Rate (delež napačnega neujemanja); FNMR = FRR

FERET: FacE REcognition Technology (biometrična tehnologija na osnovi prepoznave obraza)

FMEA: Failure Mode and Effects Analysis (Analiza možnih napak in njihovih posledic, je v praksi ena najbolj preizkušenih metod, namenjenih preprečevanju napak v zgodnjih fazah nastajanja proizvoda.)

FRACAS: Failure Reporting Analysis & Corrective Actions System (sistem poročanja, analiziranja odpovedi in korektivnih aktivnosti)

FRR: False Rejection Rate (delež napačnih zavrnitev; primer: FRR 0,05 % pomeni neuspešno registracijo 1 uporabnika z obstoječo avtorizacijo v sistemu 2000 uporabnikov); FRR = FNMR

FRVT: Face Recognition Vendor Test (test za biometrijo prepoznave obraza)

FTE: Failure to Enrol Rate (napaka registracije); FTE = FER

FTA: Failure to Acquire Rate (delež nezmožnosti zajemanja biometričnega podatka)

FTC: Failure to Capture Rate (napaka obravnave vzorca)

S

SAIC: Science Applications International Corporation (mednarodno združenje za aplikativno znanost)

SBD: Slovensko Biokemijsko Društvo (terminološka komisija SBD)

SREPT: Software Reliability Estimation and Prediction Tool (orodje za ocenjevanje in napovedovanje zanesljivosti programske opreme)

SSCC: Serial Shipping Container Code (zaporedna številka ladijskega zabojnika)

SUIV: sistem upravljanja informacijske varnosti (Information Security Management System)

G

GIAI: Global Individual Asset Identifier (globalni identifikator posameznega sredstva)

GLN: Global Location Number (globalna lokacijska številka)

GRAI: Global Returnable Asset Identifier (globalni identifikator za vračilo sredstva)

GTIN: Global Trade Item Number (globalna trgovinska številka)

H

Human ID: Human Identification at a Distance (prepoznava človeške identitete na daljavo)

HBSI: Human-Biometric Sensor Interaction (interakcija človek-biometrični senzor)

HEP: Human Error Probability (verjetnost človeške napake)

HTER: Half Total Error Rate (srednja vrednost napak FAR in FRR)

HDP: High Definition Printing

I

IASTED: International Conference on Artificial Intelligence and Soft Computing (mednarodna konferenca za umetno inteligenco in programiranje)

IAI: International Association for Identification (mednarodno združenje za identifikacijo)

IAFIS: Integrated Automoated Fingerprint Identification System (avtomatiziran sistem za avtomatsko obdelavo prstnih odtisov)

IBM: International Business Machines Corporation

ICAO: International Civil Aviation Organization (mednarodna organizacija za civilno letalstvo)

ICC: Integrated Chip Card (integrirane čipne kartice)

IAPR: International Conference on Biometrics (mednarodna biometrična konferenca)

ICONIP: International Conference on Neural Information Processing

ICIC: International Conference on Intelligent Computing (mednarodna konferenca o inteligentnem računalništvu)

IEEE: Institute of Electrical and Electronics Engineers (inštitut za elektro in elektronsko inženirstvo)

INCITS: International Committee for Information Technology Standards (mednarodni komite za standardizacijo informacijske tehnologije)

INSPASS: INS-Passenger Accelerated Service System (avtomatiziran sistem za hitrejši prehod meje registriranih potnikov)

IR: Infra–Red (infra rdeče)

IEC: International Electrotechnical Commission (mednarodna elektrotehniška komisija)

IPTS: Institute for Prospective Technological Studies (inštitut za napredne tehnološke študije)

ISO: International Standardization Organization (mednarodna organizacija za standardizacijo)

ITO: Indium Thin Oxide (tanka plast indijevega oksida)

ITU: Information Telecommunication Union (zveza za informatiko in telekomunikacije)

ITIL: Information Technology Infrastructure Library (dobra praksa na področju upravljanja IT storitev; tudi Application Management)

J

JRC: Joint Research Centre (Generalni direktorat JRC je znanstveni in tehnični raziskovalni laboratorij, ki spada pod Evropsko komisijo, ji svetuje in posreduje tehnični »know-how« kot podporo znanstveni politiki EU.)

L

LAN: Lockal Area Network (lokalno internetno omrežje)

PCA: Principal Component Analysis (analiza glavnih komponent-značilk)

LFA: Local Feature Analysis (analiza lokalnih značilk)

LIBE: Committee on Civil Liberties, Justice and Home Affairs (odbor za državljanske svoboščine in pravice, sodstvo in notranje zadeve EU)

M

MS: Microsoft

MTTF: Mean Time To Failure (povprečni čas do odpovedi) je povprečni čas od začetka delovanja do odpovedi naprave. Je karakteristika zanesljivosti, ki ni funkcija časa, temveč podaja časovno povprečje.

MTTR: Mean Time To Repair (povprečni čas od pojava odpovedi do ponovnega delovanja naprave).

MTBF: Mean Time Between Failure (povprečni čas med odpovedmi) je povprečni čas od enega začetka (ponovnega) delovanja do naslednjega začetka (ponovnega) delovanja naprave.

MF: MiFare (bralno-pisalne pametne brezkontaktne kartice - RW smart)

MW: Medium Wave (srednji radijski valovi; npr. MWIR 3–5 μm)

N

NATO: North Atlantic Treaty Organization (sevrno atlantska zveza)

NIST: National Institute of Standards and Technology (inštitut za standarde in tehnologijo)

NIST IR: National Institute of Standards and Technology Interagency Reports (nacionalni inštitut za standardizacijo in medresorsko tehnološko usklajevanje)

O

OASIS: Organization for the Advancement of Structured Information Standards (organizacija za napredno strukturiranje informacijskih sistemov)

OAT: Operator Action Tree (plan ukrepov operaterja)

OEE: Overall Equipment Effectiveness (skupna učinkovitost naprav)

P

PCB: Printed Circuit Board (matična plošča ELS)

PDCA: Plan-Do-Check-Act (Demingov krog; planiraj-izvedi-preveri-ukrepaj)

PIN: Personal Identification Number (osebna identifikacijska številka)

PRESS: Program for Rate Estimation and Statistical Summaries (program za statistično ocenjevanje)

R

RAM: Random Access Memory

RAM: Reliability, Availability and Maintability Strategy (strategija za zanesljivost, razpoložljivost in vzdrževalnost)

RFID: Radio Frequency Identification (RFID je avtomatična identifikacijska metoda, ki temelji na daljinski nobdelavi podatkov, shranjenih na RFID identifikatorju.)

ROC: Receiver Operating Characteristic (karakteristika delovanja sprejemnika)

ROM: Read Only Memory

RSA: Rivest, Shamir, Adleman (začetnice imen avtorjev, ki so leta 1977 opisali algoritem na MIT)

RO: Read Only (bralne kartice)

RW: Read-Write (bralno-pisalne kartice)

RW DUEL: kombinirana brezkontaktna in kontaktna kartica

S

SHARPE: Symbolic Hierarchical Automated Reliability and Performance Evaluator

SQL: Standard Query Language (strukturirani povpraševalni jezik za delo s podatkovnimi bazami)

SMERFS: Statistical Modeling and Estimation of Reliability Functions for Systems (Programska oprema za modeliranje in ocenjevanje zanesljivosti)

SRE: Software Reliability Estimation–Engineering (ocenjevanje zanesljivost programske opreme)

T

TAD: Tabelar Aplication Development (tabelarni razvoj aplikacij)

TAB: Technology Assessment at the German Parliament

TESEO: Tecnica empirica stima errori operatori (The Empirical technique for estimating operator errors)

THERP: The Technique for Human Error Rate Prediction (tehnike za predvidevanje človeških napak)

TR: Technical Report (tehnično poročilo)

TQM: Total Quality Management (celovito upravljanje kakovosti)

TWIC: Transportation Worker Identification Credential (identifikacijska poverilnica za delavce na področju transporta)

U

US-VISIT: United States Visitor and Immigrant Status Indicator Technology (vstopno–izstopni program na mejah ZDA)

UHF: Ultra High Frequency (ultra visoke frekvence)

V

VIS: Visa Information System (informacijski sistem za izmenjavo podatkov prebivalcev držav EU)

VNTR: Variable Number of Tandem Repeats (spremenljivo število tandemskih ponovitev)

VOI: varnost omrežij in informacij

VWP: Visa Waiver Program (program v katerega je vključenih 27 držav, ki za vstop v ZDA ne potrebujejo vizuma.)

Z

ZDA: Združene države Amerike

W

WAN: Wireless Area Network (brezžično internetno omrežje)

WBS: Work Breakdown Structure (strukturirana členitev dela)

WSQ: Wavelet Scalar Quantization (kompresijski algoritem prstnih odtisov)

17 LITERATURA

Abernethy, R. (2004). *The New Weibull Handbook Fifth Edition, Reliability and Statistical Analysis for Predicting Life, Safety, Supportability, Risk, Cost and Warranty Claims,* Robert Abernethy, Florida.

Ahmad, M. M., Dhafr, N. (2002). Establishing and improving manufacturing performance measures, *Robotics and Computer Integrated Manufacturing*, 18(3), strani 171-176.

Ansell, J. I., Phillips, M. J. (1994). *Practical Methods for Reliability Data Analysis*, Oxford University Press, New York.

Andreou, A., Mateou N., Zombanakis, G. (2005). Soft Computing for Crisis Management and Political Decision Making: the use of Genetically evolved Fuzzy Cognitive Maps, *Soft Computing–A Fusion of Foundations, Methodologies and Applications,* 9(3), strani 194-210.

Baker, J. P., Maurer, D. E. (2008). Fusing Multimodal Biometrics with Quality Estimates via a Bayesian Belief Network, *Patern Recognition*, 41(3), strani 821–832.

Balantič, Z. (2006). Multimedia spiral architecture development for effective medical education, *WSEAS Transactions on Computers*, 5(10), strani 2293–2300, Athens, Greece.

Boehm, B. V. (1988). A Spiral Model of Software Development an Enhancement, *IEEE Computer*, 21(5), strani 61–72.

Boehm, B. (1989). *Software Risk Management*. IEEE Computer Society Press, Piscataway, New York.

Bolle, M. R., Connell, H. J., Pankanti, S., Ratha, K. N., Senior, W. A. (2004). *Guide to Biometrics.* Springer–Verlag, New York.

Brown, D. (2007). Radio Frequency Identification implementation, *IEEE International Conference on Radio Frequency Identification 2007*, strani 175–182.

Bunney, C. (1997). Survey: face recognition system, *Biometric Technology Today*, 5(4), strani 8–12.

Cappelli, R., Maio, D., Maltoni, D., Wayman, J. L., Jain A. K. (2006). Performance evaluation of fingerprint verification systems, *IEEE Transactions Pattern Analysing & Machine Intelligence*, 28(1), strani 3–18.

Chase, R. B., Aquilano, N. J., Jacobs, F. R. (1998). *Operation Management*. 9th Edition, McGraw–Hill, New York.

Chen, J., Yan, W. (2006). Design of a zero-failure reliability test plan based on customer usage and bench life test data, *Journal of the IEST,* 49(2), strani 93–103.

Chirillo, J., Blaul, S. (2003). *Implementing Biometric Security*. John Wiley & Sons, New York.

Chi-Chao, L. (1997). *A Comparison between the (Weibull and Lognormal Models used to Analyze Reliability Data*, P.hd thesis, University of Nottingham, Nottingham.

Chung, C. C. (2004). *Simulation Modeling Handbook–Aprctical approach.*CRC Press, USA.

Clark, A. (2001). *Mindware: An Introduction to the Philosophy of Cognitive science*. Oxford University Press, New York.

Črnčec, D. (2004). Biometrija: Sodoben način zagotavljanja varnosti!?, *Revija Obramba*, 35(2), strani 19–21.

Čufer, M. (2003). *Uporaba metode TAD*. CIP, Ljubljana.

Dobnikar, A. (1990). *Nevronske mreže: teorije in aplikacije*. Didakta, Radovljica.
Dorizzi, B., Lamadeleine, P., Guerrier, C. (2004). Les Jardins Biométrie: Techniques et usages, *Revue des sciences et techniques de l'ingenieur*.
Emmett, E., Kern, C. (2004). Radio-Frequency-Identification for Security and Media Circulation in Libraries, *Library & Archival Security*,18(2), strani 23–38.
Fausett, L. V. (1994). *Fundamentals of neural networks. Architectures, Algorithms and Applications*. Prentice–Hall, New Jersey.
Fernandez, F., Aguilar, J., Garcia, J. (2005). *A review of schemes for fingerprint image quality computation*, COST275–Biometrics Based Recognition of People over the Internet, strani 3–6, Hatfield, UK.
Fefer, D. (2004). Uporaba biometričnih tehnologij v sistemih pristopne kontrole, *Varstvoslovje*, 6(2), strani 148-156.
Finkezzeller, K. (2003). RFID Handbook. *Fundamentals and Applications in Contactless Smart Cards and Identification (2nd Edition).* John Wiley & Sons, New York.
Fitzpatrick, T. (2002). Critical theory, information society and surveillance tehnologies, *Information, Communication & Society*, 5(3), strani 357–378.
Gates, K. A. (2004). *Our biometric future: The social construction of an emerging information technology*. University of Illinois at Urbana–Champaign, United States.
Gams, M. (2001). Weak Intelligence: Through the principle and paradox of multiple knowledge. Nova Science Publishers, New York.
Gams, M., Tušar, T. (2007). Intelligent high-security access control, *Informatica*, 31(4), strani 469–477.
Gamassi, M. Lazzaroni, M. Misino, M. Piuri, V. Sana, D. Scotti, F. (2005). Quality assessment of biometric systems: a comprehensive perspective based on accuracy and performance measurement, *Instrumentation and Measurement*, 54(4), strani 1489–1496.
Garcia, C., Delakis, M. (2004). Convolutional face finder: a neural architecture for fast and robust face detection, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 26(11), strani 1408–1423.
Garvin, D. (1988). *Managing Quality: The Strategic and Competitive Edge*. Free Press, New York.
Gill, M. A. (2004). Fuzzy random variables: Development and State of the Art, *Mathematics of Fuzzy Systems*, Seminar on Fuzzy Set Theory, Linz, Austria, strani 11–15.
George, L. L. (2001). MTBF Versus Age–Specific Reliability Prediction. *ASQ Reliability Review*, 21(2), strani 13–15.
Groth, R. (2000). *Data Mining–Building Competitive Advantage*. Prentice–Hall, Englewood Cliffs, New York.
Guid, N., Strnad, D. (2007). *Umetna inteligenca*. Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor.
Hauc, A. (2002). *Projektni management*, GV Založba, Ljubljana.
Hagan, M., Demuth, H. B., Beale, M. (1996). *Neural Network Design*, PWS Publishing Company, Boston.
Hamel, G. (2006). Why, What, and How of Management Innovation, *Harvard Business Review,* Harvard Business School Publishing Corporation.
Hidalgo, D., Melin, P., Licea, G. (2008). Optimization of Modular Neural Networks with Interval Type–2 Fuzzy Logic Integration Using an Evolutionary Method with

Application to Multimodal Biometry, *International Journal of Biometrics*, 1(1), strani 111–121.
Hicklin, R. A., Watson, C., Ulery, B. (2005). The Myth of Goats: How many people have fingerprints that are hard to match?, *NIST Interagency Report* 7271.
Heinemann, C., S., Worch H., Hanke T. (2011). Development of an osteoblast/osteoclast co-culture derived by human bone marrow stromal cells and human monocytes for biomaterials testing, *European Cells and Materials,* 21, strani 80-93.
Ho, L. L., Silva, A. F. (2006). Unbiased estimators for mean time to failure and percentiles in a Weibull regression model, *International Journal of Quality & Reliability Management*, 23(3), strani 323–339.
Hoyland, A., Rausand, M. (1994). *System Reliability Theory: Models and Statistical Methods*. John Wiley & Sons, New York.
Hocquet, S., Ramel, J., Cardot, H. (2005). Fusion of Methods for Keystroke Dynamic Authentication, *4th IEEE Workshop on Automatic Identification Advanced Technologies*, USA, strani 224–229.
Hudoklin, A. (2003). *Stohastični procesi (skripta)*. Moderna organizacija, Kranj.
Hudoklin, A., Rozman, V. (1985). *Preskusi zanesljivsoti sestavnih delov*, Elektrotehniški vestnik, 52(3), strani 103–106.
Hudoklin, A., Rozman, V. (1989). Varnost in zanesljivost v železniškem prometu, *XI. jugoslovanski simpozij o elektroniki v prometu*, Elektrotehniška zveza Slovenije, Ljubljana.
Hudoklin, A., Rozman, V. (2004). *Zanesljivost in razpoložljivost sistemov človek-stroj*. Založba Moderna organizacija, Kranj.
Hudoklin, A., Rozman, V. Brezavšček, A. (2006). *Ocenjevanje zanesljivosti in razpoložljivosti sistemov*. Založba Moderna organizacija, Kranj.
Hunt, V., Puglia, A., Puglia, M. (2007). *RFID–A guide to radio frequency identification*, John Wiley and Sons, New Yersy.
Huvanandana, S. (2002). *A framework for a fast fingerprint identification using a hybrid system*, University of Washington, Washington.
Huvanandana, S., Changick, K., Hwang, J. N. (2000). *Reliable and Fast Fingerprint Identification for Security Applications*, Proceedings of the 2000 International Conference on Image Processing (ICIP 2000), Canada, September 10-13.
Huang, T., Xiong, Z., Zhang, Z. (2005). Face Recognition Applications. *Handbook of Face* Recognition (Li, S. Z., Jain, A. K., uredniki), 16, strani 371-390, Springer, New York.
Jain, A. K., Bolle, R., Pankanti, S. (2002). Introduction to biometrics. *Biometrics: Personal Identification in Networked Society* (Jain, A., Bolle, R., Pankanti, S.), strani 1–41, Kluwer Academic Publishers, Massachusetts.
Janbandhu, P. K., Siyal, M. Y. (2001). Novel biometric digital signatures for Internet–based applications, *Information Management and Computer Security*, 9(1).
Jones, J., Hayes, J. (1999). A Comparison of electronics-Reliability prediction models, *IEEE Transactions on Reliability*, 48(2), strani 127-134.
Karimi, I., Hüllermeier, E. (2005). A Fuzzy–Probabilistic Risk Assessment, *System for Natural Disasters*, Proceedings of the IFSA2005 World Congress, Tsinghua University, Beijing, China, strani 1147-1153.
Kern, T. (1998). *Procesna organizacija: oblikovanje organizacije poslovnih sistemov na osnovi modela strukturiranih organizacijskih procesov*, Doktorska disertacija, Fakulteta za organizacijske vede, Kranj.

Kern-Pipan, K. (2010). *Vpliv stalnih izboljšav in človeškega kapitala na poslovno odličnost organizacije*, Doktorska disertacija, Fakulteta za organizacijske vede, Kranj.

Khanna, R. (2004). Systems Engineering for Large–Scale Fingerprint Systems. *Automatic Fingerprint Recognition Systems* (Ratha, N., Bolle, R., Editors), strani 283-303, Springer Verlag, New York.

Klir, G. J., St Clair, U.H., Yuan, B. (1997). *Fuzzy set theory: Foundations and Applications*, Prentice Hall, Englewood Cliffs.

Kodratoff, Y., Tecuci, G. (1988). Learning Based on Conceptual Distance, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 10(6), strani 897–909.

Kohonen, T. (2007). *Self–Organization and Associative Memory*, Springer, Berlin.

Kovačič, M. (2006). *Nadzor in zasebnost v informacijski družbi.* Znanstvena knjižnica, Fakulteta za družbene vede, Ljubljana.

Ključevšek, R., Vodopivec, T. (2002). Gradivo za delavnice: *Obvladovanje informacij po BS7799 in ocena tveganj*, Ljubljana.

Knezevic, J. (1997). Systems Maintainability: *Analysis, Engineering, and Management*, Chapman and Hall.

Kokol, P., Hleb-Babič, Š, Podgorelec, V., Zorman, M. (2001). *Inteligentni sistemi*. Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor.

Kononenko, I. (2005). *Umetne nevronske mreže: strojno učenje*. Fakulteta za računalništvo in informatiko, Ljubljana.

Krehl, P. (2008). *History Of Shock Waves, Explosions And Impact: A Chronological And Biographical Reference*, Springer, Berlin.

Kreie, J., Cronan, T., Pendley, J., Renwick, J. (2000). Application development by End-users: Can Quality be Improved?, *Decision Support systems*, 29(2), strani 143–152.

Krejan, A. (2002). *Mikrokrmilniški sistem za preverjanje identitete uporabnikov z zajemanjem in obdelavo biometričnih podatkov*, Magistrska naloga, Fakulteta za elektrotehniko, računalništvo in informatiko, Ljubljana.

Kukula, E., Proctor, R. (2009). Human–Biometric Sensor Interaction: Impact of Training on Biometric System and User Performance. *Human Interface and the Management of Information* (Smith, M., Salvendy, G., Editors), strani 168–177, Springer Berlin / Heidelberg.

Kukula, E.P, & Elliott, S.J. (2006). Implementation of hand geometry: an analysis of user perspectives and system performance, *IEEE Aerospace and Electronic Systems Magazine,* 21(3), strani 3–9.

Kumar, Zhang (2010). Improving biometric authentication performance from the user quality, *IEEE Transactions on Instrumentation and Measurement*, 59(3), strani 730–735.

Kuo, W. (1985). Bayesian Availability Using Gamma Distributed Priors, *IIE Transactions*, 17(2), strani 132 –141.

Laeeq, A. S., Adeel, S. (2007). Neuro–Fuzzy Hybrid Intelligent System Using Grid Computing, *International Conference on Emerging Technologies*, strani 145–147.

Lemme, H. (2005). Fingerprint as Password, *Elektor Electronics*, 31(347), strani 20–24.

Lientz, B. P., Rea, K. P. (1999). Project manegment. *Planning and implementation*, Harcourt Professional Publishing, San Diego.

Liu, Y. (2011). Scenario study of biometric systems at borders, *Computer Law & Security Review*, 27(1), strani 36–44 .
Madu, C. N. (1999). Reliability and Quality interface, *International Journal of Quality & Reliability Management*, 16(7), strani 691–698.
Maier, F., Karageorghis, V. (1984). *Paphos: History and archaeology*. A.G. Leventis Foundation, Switzerland.
Malcangi, M. (2007). Fuzzy Logic and Artificial Neural Networks for Advanced Authentication Using Soft Biometric Data, *Engineering Applications of Neural Networks*, (Brown, D. in drugi, recenzenti), strani 67–78, Springer, Berlin.
Maltoni, D., Maio, D., Jain, A. K., Prabhakar. S. (2003). *Handbook of Fingerprint Recognition*. Springer Verlag, New York.
Marić, D. (2005). RFID tehnologija v praksi in njena prihodnost. 9. mednarodno posvetovanje o prometni znanosti, *Promet v znanosti in praksi*, Zbornik referatov konference, Fakulteta za pomorstvo in promet, Portorož, Slovenija.
Marin˜o, C., Penedo, G., Penas, J., Carreira F. (2006). Personal authentication using digital retinal images. *Journal of Pattern Analysis and Application*, Springer, 9(1), strani 21–33.
Maver, D. (2004). *Kriminalistika: uvod, taktika in tehnika*. Uradni list republike Slovenije, Ljubljana.
Marolt, J., Gomišček, B. (2005). *Management kakovosti*, Moderna organizacija, Kranj.
Matjaš, V., Riha, Z. (2004). On usability (and security) of Biometric Authentication Systems. *Security in Advanced Networking Technology* (Jerman, B., Schneider, W., Klobučar, T., Editors), strani 178–188, IOS Press, Amsterdam.
McNeill, F. M., Thro, E. (1994). *Fuzzy Logic: A practical approach*. AP–Proffesional, Boston.
Melin, M., Castillo, O. (2005). *Hybrid Intelligent Systems for Pattern Recognition Using Soft Computing: An Evolutionary Approach for Neural Networks and Fuzzy Systems (Studies in Fuzziness and Soft Computing).* Springer–Verlag, New York.
Mettas, A., Zhao, W. (2004). Modeling and Analysis of Complex Repairable Systems, *Technique Report*, ReliaSoft Corporation.
Monaghan, J., Just, P. (2000). *Social & Cultural Anthropology: A Very Short Introduction*. Oxford University Press, Oxford.
Monwar, M., Gavrilova, M. (2010). Robust multimodal biometric system using Markov chain based rank level fusion, *Computer Vision Theory and Applications,* strani 458-463.
Mraović, M. (2003). *Biometrične metode v sistemu pristopne kontrole*. Univerza v Ljubljani, Fakulteta za elektrotehniko, Ljubljana, Slovenija.
Musa, J. D., Iannino, A., Okomuto, K. (1987). *Software reliability: Measurement, Prediction, Application.* McGrawHill, Singapore.
Nadel, L. (2006). *On the Future of Biometrics–Research, Applications, and Social Challenges*, IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2006).
Navarrete, P., Solar, J. (2002). Interactive face retrieval using self-organizing maps, In *Proceedings, 2002 International Joint Conference On Neural Networks (IJCNN2002).*
Nielsen, J. (1993). *Usability Engineering*. Morgan Kaufmann, San Francisco.

Negnevitsky, M., Johnson, P., Santoso, S. (2007). Short term wind power forcasting using hybrid intelligent systems. *IEEE Power Engineering Society General Meeting*, Florida, USA.

Oglesby, J., Mason, J. (1991). Radial basis function networks for speaker recognition, *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 1, strani 393–396.

O'Connor, P. D. T. (2002). *Practical Reliability Engineering*. John Wiley & Sons, New York.

Pan, C. -C, Chu, L. (2010). Reliability assessment for one-shot product with Weibull lifetime components, *International Journal of Quality & Reliability Management,* 27(5), strani 596–610.

Pentti, H., Atte, H. (2002). *Failure mode and effects analysis of software-based automation systems,* STUK, Helsinki.

Polajnar, A. (2003). Presežimo meje na nov način, *Orodjarstvo 2003*, Portorož.

Pham, D. T., Karaboga, D. (2000). *Intelligent Optimisation Techniques: Genetic Algorithms, Tabu Search, Simulated Annealing and Neural Networks*, Springer – Verlag, London.

Podgorelec, V. (2001). *Oblikovanje inteligentnih sistemov in odkrivanje znanja z avtomatskim programiranjem*, Doktorska disertacija, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor.

Pograjc, M., Kljajić, M., Rajkovič, V. (2003). Simulacija procesa učenja ob uporabi baze znanja ekspertnega sistema. *Organizacija*, 36(8), strani 545-551.

Rausand, M., Hoyland, A. (2004). *System reliability theory: models, statistical methods, and applications,* John Wiley & Sons, New York.

Ratha, N. K., Connell, J.H., Bolle R. M. (2001a). An analysis of minutiae matching strength, In *Proceeding 3rd International Conference on Audio and Video–Based Person Authentication (AVBPA)*, Halmstad, Sweden.

Ratha, N. K., Connell, J.H., Bolle R. M. (2001b). Enhancing security and privacy in biometrics-based authentication systems, *IBM Systems Journal*, 40(3), strani 614–634.

Reddy, R. (2006). Robotics and Intelligent Systems in Support of Society, *Intelligent Systems*, 21(3), strani 24–31.

Rich, E., Knight, K. (1991). *Artificial Intelligence*. McGraw-Hill, New York.

Rowley, H., Baluja, S., Kanade T. (1998). Neural Network–Based Face Detection, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(1), strani 23–38.

Sickler, N., Elliott, S. (2005). An evaluation of fingerprint image quality across an elderly population Vis–a–Vis an 18–25 year old population, *the 39th Annual International Carnahan Conference on Security Technology (ICCST)*, Las Palmas de Gran Canaria, Spain.

Sarhan, A. M. (2003). Nonparametric empirical Bayes procedure, *Reliability Engineering & System Safety*, 80(2), strani 115–122.

Sarhan, A. M. (2004). Parameter estimations in a general hazard rate model using masked data, *Applied Mathematics and Computation*, 153(2), strani 513–536.

Shooman, M. L. (2002). *Reliability of Computer Systems and Networks*. Polytechnic University New York, John Wiley&Sons, USA.

Shunji, O., Toshihiko, N. (1979). Availability Evaluation of Redundant Computer Systems, *Computers & Operations Research*, 6(2), strani 87–97.

Snelick, R., Indovina, M., Yen, J. and Mink, A. (2000). Multimodal Biometrics: Issues in Design and Testing, *Fifth International Conference on Multimodal Interfaces*, Vancouver, Canada.

Solina, F. (1997). *Projektno vodenje razvoja programske opreme*, Fakulteta za računalništvo in Informatiko, Ljubljana.

Subašić, P. (1997). *Fuzzy logika i neuronske mreže*. Tehnička knjiga, Beograd.

Standring, S. (2004). *Gray's Anatomy: The Anatomical Basis of Clinical Practice*. Elsevier Churchill Livingstone, Edinburgh.

Galton, F. (2003). Pioneer of Heredity and Biometry. *Literature of travel and exploration* (Speake, J., Editor), stran 352, Taylor and Francis group, London.

Trapečar, M. (2007). *Prstni odtisi–preiskava, primerjava in postopek potrditve identifikacije.* Center za forenzične preiskave, Ljubljana.

Trapečar, M., Robek, A. (2003). Sodobne biometrične metode pri verifikaciji identitet posameznikov ter njihova uporabnost v letalskem prometnem sistemu, *Varstvoslovje,* 5(1), strani 49–56.

Turk, M., Pentland, A. (1991). Eigenfaces for Recognition, *Journal of Cognitive Neuroscience*, 3(1), strani 71–86.

Tronci, R., Giacinto, G., Roli, F. (2009). Designing multiple biometric systems: measures of ensemble effectiveness, *Engineering Applications of Artificial Intelligence,* 22(1), strani 66–78.

Uludag, U., Jain, A. K. (2003). Multimedia Content Protection Via Biometrics–Based Encryption, *International Conference on Multimedia and Expo*, Baltimore, strani 237–240.

Virant, J., Zimic, N. (1996). Attention to time in fuzzy logic, *Fuzzy Sets and Systems,* 82(1), strani 39–49.

Villemeur, A. (1992). *Reliability, Availability, Maintainability and Safety Assessment,* John Wiley & Sons, New York.

Winston, W. L. (1991). *Operations Research: Applications and Algorithms*, Duxbury Press, Belmont.

Woodward, J. D., Orlans, N. M., Higgins, P. T. (2003). *Biometrics*. McGraw–Hill, New York.

Tong, Xiaojun, Ma, Qun (1995). General Regression Analysis Method for Estmating The Weibull Three Parameters, *Journal of Tangshan institute of technology*, 17(2), stran 78.

18 VIRI

18.1 ELEKTRONSKI VIRI

Abernethy, R. B. (2005). *Biography of Dr. E. H. Wallodi Weibull,* dosegljivo na: http://www.bobabernethy.com/bios_weibull.htm (1.2.2011).

Ando, H., Fuchigami, N., Sasaki, M., Iwata A. (2004). *Human Face Detection and Recognition using Principal Component Analysis*, dosegljivo na: http://www.rcns.hiroshima-u.ac.jp/21coe/pdf/2nd_WS/Poster.2-P.80.pdf (10.2.2011).

Beale, M. H., Hagan, M. T., Demuth, H. B. (2010). *Neural Network Toolbox™ 7*: Users Guide, dosegljivo na: http://www.mathworks.com/help/pdf_doc/nnet/nnet.pdf (10.2.2011).

BEM WG (2002). *Biometric Evaluation Methodology*, dosegljivo na: http://www.cesg.gov.uk/policy_technologies/biometrics/media/bem_10.pdf (10.11.2010).

Bhattacharyya, D., Ranjan, R., Alisherov, F., Choi, M. (2009). Biometric Authentication: A Review. *International Journal of u– and e– Service, Science and Technology*, 3(2), dosegljivo na: http://www.sersc.org/journals/IJUNESST/vol2_no3/2.pdf (9.10.2010).

Biometric Vision (2008). *Principles of fingerprint biometrics,* dosegljivo na: http://www.biometricvisions.com/technology/technology.htm (7.11.2010).

Biometric Associates (2010). *The BAL Authenticator™ Smart Card,* dosegljivo na: http://www.biometricassociates.com/products-bai/authenticator-smart-card.html (7.1.2011).

Bohanec, M. (2001). Metode umetne inteligence. *Učno gradivo za podiplomce FOV*, dosegljivo na: http://www-ai.ijs.si/MarkoBohanec/ai/ai.html (12.07.2009).

BTH–Blekinge Tekniska Högskola (2010). *Software Quality Models and Philosophies,* dosegljivo na: http://www.bth.se/tek/besq.nsf/(WebFiles)/CF1C3230DB425EDCC125706900317C44/$FILE/chapter_1.pdf (10.03.2010).

Burge, M., Burger, W. (1998). *Ear Biometrics,* dosegljivo na: http://docs.google.com (10.03.2010).

Carič, T., Ajdašik, I. (2003). *Biometrika*, dosegljivo na: http://www2.arnes.si/~pkuzma/faks/SIPP-biometrika.doc (12.9.2010).

Chikkerur, S. S. (2005). *Online fingerprint verification system*, Master of Science *thesis*, State University of New York at Buffalo, dosegljivo na: http://web.mit.edu/sharat/www/research/thesis.pdf (12.9.2010).

Clarke, R. (2006). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, dosegljivo na: http://www.rogerclarke.com/DV/Intro.html (12.1.2010).

Corcoran, D., Sims, D., Hillhouse, B. (1999). Smart cards and biometrics: Your key to PKI. *Linux Journal.* dosegljivo na: http://www.linuxjournal.com/article.php?sid=3013 (12.2.2010).

Côté, M. A., Georgiadou, E. (2006). Software Quality Model Requirements for Software Quality Engineering. *Software Quality Management & INSPIRE Conference (BSI),* dosegljivo na:

http://profs.logti.etsmtl.ca/wsuryn/research/SQE-Publ/Quality%20model_requirements.%20SQM2006.pdf (9.12.2010).
Čeh-Ambruš, D. (2006). *Konferenca RFID journal live! Europe 2006,* dosegljivo na: http://home.izum.si/COBISS/OZ/2007_1/html/clanek_07.html (15.12.2010).
Četrta pot (2009). *Identifikacijske kartice in obeski,* dosegljivo na: *http://www.cetrtapot.si/izdelki/identifikacijske_kartice_in_obeski/* (06.1.2011).
Donkelaar, E. (2000). *Improvement of efficiency in identification and model predictive control of industrial processes*, dosegljivo na: http://www.dcsc.tudelft.nl/Research/PublicationFiles/publication-5739.pdf (12.01.2011).
Dorizzi, B. (2006). New Trends in Biometrics. *Telecommunications: Advances and Trends in Transmission, Networking and Applications*, strani 173–183, dosegljivo na:http://www.gtel.ufc.br/~charles/PDF/book_telecommunications.pdf (10.01.2011).
IPTS (2005). Biometrics at the Frontiers: Assessing the Impact on Society, *Technical Report Series*, strani 78–86, dosegljivo na: http://ftp.jrc.es/EURdoc/eur21585en.pdf (12.1.2011).
Drstvenšek, I. (2006). *Vzdrževanje v poindustrijski dobi v luči standarda SISI EN 13306*, dosegljivo na: http://www2.arnes.si/~sspvjeme/CPIvzdrzevanje13306.pdf (2.11.2010).
Drygajlo, A. (2005a).*Biometrics*, dosegljivo na: http://scgwww.epfl.ch/courses/Biometrics-Lectures-2005-2006-pdf/04-Biometrics-Lecture-4-2005/04-Biometrics-Lecture-4-Part1-2005.pdf (2.2.2011).
Drygajlo, A. (2005b).*Biometrics*, dosegljivo na: http://scgwww.epfl.ch/courses/Biometrics-Lectures-2005-2006-pdf/02-Biometrics-Lecture-2-2005/02-Biometrics-Lecture-2-Part1-2005.pdf (2.2.2011).
Drygajlo, A. (2005c). *Biometrics*, dosegljivo na: http://scgwww.epfl.ch/courses/Biometrics-Lectures-2005-2006-pdf/03-Biometrics-Lecture-3-2005/03-Biometrics-Lecture-3-Part2-2005.pdf (2.2.2011).
Elatec (2011). *RFID*, dosegljivo na: http://www.elatecworld.com/rfid/downloads.html?no_cache=1 (2.2.2011).
Electronic Privacy Information Center (2004). *Privacy and Human Rights Report*, dosegljivo na: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82589&als[theme]=Privacy%20and%20Human%20Rights&headline=PHR2004 (12.9.2009).
Fargo (2010). *Challenges of Printing on Proximity Cards,* dosegljivo na: http://www.colorid.com/idblog/blogmanager/?post=colorid-white-paper (7.12.2010).
Gemalto (2010). *Security solutions for Enterprises,* dosegljivo na: http://www.gemalto.com/products/classic_tpc/ (3.12.2010)
Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. (2002). *Quantum cryptography,* dosegljivo na: http://prl.aps.org/files/RevModPhys.74.145.pdf (9.2.2011).
Gorenšček, N. (2001). *Upravljanje znanja v okolju omrežnega gospodarstva*, dosegljivo na: http://www.drustvo-informatika.si/fileadmin/dsi2001/sekcija_b/gorenscek.doc (12.12.2010).
Groleau, R. (2004). *Create a DNA Fingerprint*, dosegljivo na: http://www.pbs.org/wgbh/nova/sheppard/analyze.html (12.12.2010).
Hace, B., Škrabar, B. (2008). *Poroskopija*, dosegljivo na: http://www.fvv.uni-mb.si/dv2008/zbornik/clanki/Hace-Skrabar.pdf (12.12.2010).

Hicklin, R. A., Khanna, R. (2006). *The Role of Data Quality in Biometric Systems,* dosegljivo na: http://www.noblis.org/MissionAreas/nsi/ThoughtLeadership/IdentityDiscovery_Management/Documents/Role_of_Data_Quality_Final.pdf (17.7.2010).

Hidglobal (2009). *HID Proximity - 125 kHz - Brochures and Documentation,* dosegljivo na: http://www.hidglobal.com/technology.php?tech_cat=1&subcat_id=9 (12.1.2011).

Hustinx, P. (2006). *Comments on the Communication of the Commission on interoperability of European databases,* dosegljivo na: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf (19.1.2010).

Ilonen, J. (2003). Keystroke dynamics. *Advanced Topics in Information Processing*, dosegljivo na: http://researchweb.iiit.ac.in/~vandana/PAPERS/KS/Ilonen.pdf (12.12.2010).

International Biometric Group (2005). *Independent Testing of Iris Recognition Technology*, dosegljivo na: http://www.biometricscatalog.org/itirt/itirt-FinalReport.pdf (2.1.2010).

International Biometric Group (2008). *Biometrics Market and Industry Report 2009–2014*, dosegljivo na: http://www.biometricgroup.com/reports/public/market_report.php (12.08.2010).

International Biometric Group (2009). Biometric Revenues by Technology. *Biometrics Market and Industry Report 2009–2014*, dosegljivo na: http://www.biometricgroup.com/reports/public/market_report.php (12.1.2010).

IP-RS Informacijski Pooblaščenec Republike Slovenije (2010). *Prijava biometrijskih ukrepov informacijskemu pooblaščencu.* dosegljivo na: http://www.ip-rs.si/fileadmin/user_upload/doc/obrazci (21.12.2010).

ITU-T Technology Watch Reports (2009). *Biometrics and Standards*, dosegljivo na: www.itu.int/dms_pub/itu-t/oth/23/01/T230100000D0002MSWE.doc (12.09.2010).

Jain, A. K., Roos, A., Pankanti, S. (1999). A Prototype Hand Geometry–based Verifiation System. *International Conference on Audio and Video–based Biometric Person Authentication*, strani 166–171, dosegljivo na: http://researchweb.iiit.ac.in/~vandana/PAPERS/HG/Prototype_HG2.pdf (9.8. 2010).

Jain, A. K., Ross, A., Prabhakar, S. (2004). *An Introduction to Biometric Recognition*, dosegljivo na: http://www.csee.wvu.edu/~ross/pubs/RossBioIntro_CSVT2004.pdf. (9.8.2009).

Jain, A. K. (2010). *Avtomatic Face Recognition: State of the Art*, dosegljivo na: http://biometrics.cse.msu.edu/Presentations/AnilJain_FaceRecognition_KU10.pdf (21.2.2011).

Jerman, U. (2008). *Varna in zanesljiva programska oprema elektronskega števca električne energije MT372-SMART,* dosegljivo na: http://lie.fe.uni-lj.si/diplome/PDF/2008/Diploma_UrosJerman.pdf (19.2.2011).

Kapczyński, A. (2006). *Relationship between IT Security and users' needs,* dosegljivo na: http://www.proceedings2006.imcsit.org/pliks/166.pdf (20.2.2010).

Karunanithi, N., Malaiya, Y. K. (1996). Neural Networks for Software Reliability Engineering. *Handbook of Software Reliability Engineering,* dosegljivo na: http://www.cse.cuhk.edu.hk/~lyu/book/reliability/pdf/Chap_17.pdf (12.10.2010).

Kirkpatrick, M. (2001). How New Technologies (Biometrics) Can Be Used To Prevent Terrorism. *Congressional Testimony*, October 2009, dosegljivo na: http://www.fbi.gov/congress/congress01/kp111401.htm (9.12.2009).

Knil, E. (2010). Quantum computing. *Nature, 463(28)*, strani 441–443, dostopno na: http://www.nist.gov/cgi-bin//get_pdf.cgi?pub_id=902941 (9.2.2010).

Kononenko, I., Hong, S. J. (1997*). Attribute Selection for Modeling, Future Generation Computer Systems*, dosegljivo na: http://www.research.ibm.com/dar/papers/pdf/fgcshong_with_cover.pdf (4.10. 2010).

Kononenko, I. (2002). *Nekateri vidiki strojnega učenja, umetne inteligence in zavesti*, dosegljivo na: Nekateri vidiki strojnega učenja, umetne inteligence in zavesti (12.01.2011).

Victoria University of Technology (2010). *Determination of the parameters using Weibull Paper Distribution, dosegljivo* na: http://www.kokoaye.com/WEIBULLPAPER/WeibullPaper.html (12.09.2010).

Liu, S., Silverman, M. (2001). *A practical guide to Biometric Security Technology*, dosegljivo na: http://www.lfca.net/Reference%20Documents/A%20Practical%20Guide%20To%20Biometric%20Security%20Technology.pdf (12.12.2010).

Lyu, M. R. (ed.) (1996). *Handbook of Software Reliability Engineering.* IEEE Computer Society Press and McGraw–Hill Book Company, dosegljivo na: http://www.cse.cuhk.edu.hk/~lyu/book/reliability/ (12.12.2010).

Mäckel, O. (2006). *Software FMEA Opportunities and benefits of FMEA in the development process of software-intensive technical systems*, dosegljivo na: http://www.fmeainfocentre.com/papers/mackel1.pdf (24.12.2010).

Mainguet, J. F. (2010). *Iris*, dosegljivo na: http://fingerchip.pagesperso-orange.fr/biometrics/types/iris.htm (4.2.2011).

McCall, J. A., Richards, P. K., Walters, G. F. (1977). *Factors in software quality*. Griffiths Air Force Base, New York: Rome Air Development Center Air Force Systems Command, dosegljivo na: http://profs.logti.etsmtl.ca/wsuryn/research/SQE-Publ/Quality%20model_requirements.%20SQM2006.pdf (10.6.2010).

Maghiros, I., Punie, Y., Delaitre, S., Lignos, E., Rodríguez, C., Ulbrich, M., Cabrera, M. (2005). *Biometrics at the Frontiers: Assessing the Impact on Society*, dosegljivo na: http://ftp.jrc.es/EURdoc/eur21585en.pdf (12.1.2010).

Mahbubur, R., Rashedul, I., Nazmul, I. B., Bulbul, A., Aminul, I. (2007). Person Identification Using Ear Biometrics. *International Journal of The Computer, the Internet and Management*, 15(2), strani 1–8, dosegljivo na: http://www.ijcim.th.org/past_editions/2007V15N2/p1-IJCIM_EAR_Biometrics-pp-1-8.pdf (10.1.2010).

NIST (2005a). *Iris Challenge Evaluation*, dosegljivo na: http://www.biometricscatalog.org/itirt/ITIRT-FinalReport.pdf (14.1.2010).

NIST (2005b). *Voice Evaluation*, dosegljivo na: http://www.biometricscatalog.org/itirt/ITIRT-FinalReport.pdf (19.1.2010).

NIST (2007). *Biometric Quality Homepage*, dosegljivo na: http://www.itl.nist.gov/iad/894.03/quality/index.html (12.1.2010).

NSCT–National Science and Technology Council (2009). *Biometrics*, dosegljivo na: http://www.biometrics.gov/Documents/biofoundationdocs.pdf (14.7.2010).

NSCT–National Science and Technology Council (2006). *Biometrics*, dosegljivo na:

http://www.biometrics.gov/Documents/glossary.pdf (14.7.2010).
Olteanu, D., Freeman, L. (2008). *Technical Report on the Evaluation of Median Rank Regression and Maximum Likelihood Estimation Techniques for a Two–Parameter Weibull Distribution*, dosegljivo na: http://www.web-e.stat.vt.edu/dept/web-e/tech_reports/Technical_Report-08-4.pdf (12.8.2010).
Olzak, T. (2007). *Reduce multi–factor authentication costs with behavioral biometrics,* dosegljivo na: http://www.zdnetasia.com/reduce-multi-factor-authentication-costs-with-behavioral-biometrics-61984879.htm (16.1.2010).
Open Channel Foundation (2000). *CASRE 3.0*, dosegljivo na: http://www.openchannelsoftware.com/projects/CASRE_3.0 (12.1.2010).
Pan, J. (1999). *Software Reliability*, dosegljivo na: http://www.ece.cmu.edu/~koopman/des_s99/sw_reliability/#reference (10.09.2009).
Petermann,T., Sauter, A. (2002). *Biometrische Identifikationssysteme,* dosegljivo na: http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf (12.1.2010).
Philips, P. Grother, P. Micheals, R. Blackburn, M. Tabassi, E. in Bone J. (2003). Face Recognition Vendor Test 2002: Overview and Summary. *Evaluation Report IR 6965*, National Institute of Standards and Technology, dosegljivo na: ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_6965/FRVT_2002_Overview_and_Summary.pdf (12.10.2009).
Prabhakar, S., Pankanti, S., Anil, K. J. (2003). *Biometric Recognition: Security and Privacy Concerns*, dosegljivo na: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (5.2.2010).
RAC–Reliability Analysis Center (1996). *Introduction to Software Reliability: A state of the Art Review*, dosegljivo na: http://www.ece.cmu.edu/~koopman/des_s99/sw_reliability/ (7. 2. 2010).
Reynolds, D. A., Campbell, W. (2007). Text–Independent Speaker Recognition. *Springer Handbook of Speech Processing and Communication*, Springer–Verlag GMBH, strani 763–779, dosegljivo na: http://www.ll.mit.edu/mission/communications/ist/publications/07-05_Reynolds_sid_ch_Text_JA-GEN-2362.pdf (12.10.2010).
RVB Group (2010). *RFID*, dosegljivo na: http://www.barcode-solutions.com/rfid.shtml (7.9.2010).
ScienceGL (2008). *Fingerprint 3D Comparator: Scientific Visualization in Criminal Biometrics and Forensics*, dosegljivo na: http://www.sciencegl.com/fingerprint_3d/3D_AFIS.htm (2.10.2010).
Slovenski medicinski slovar (2009). Univerza v Ljubljani, Medicinska fakulteta, Lek d. d., dosegljivo na: http://lsm1.amebis.si/lsmeds/lokvir.aspx?pPogoj=biometrija (5.2.2010).
Sotomajor, B. (2005). *Fundamental Security Concepts*, dosegljivo na: http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html (21.1.2011).
Spanner, J. (2000). *Neural networks for ultrasonic detection of intergranular stress corrosion cracking,* dosegljivo na: http://www.ndt.net/article/v05n07/spanner2/spanner2.htm (21.1.2011).
Šafaržik, Z., Višnjić, V. (1999). *Komercijalni sustavi prepoznavanja otisaka prstiju,* dosegljivo na: http://dosl.zesoi.fer.hr/seminari/1998_1999/visnjic-safarzik/index2.html#21T (2.1.2011).

Šemrov, D., Kotnik, T., Miklavčič, D. (1996). Modeliranje bioloških in kemijskih sistemov s celičnimi avtomati. *Elektrotehniški Vestnik*, 63(4/5), strani 241–248, dosegljivo na: http://lbk.fe.uni-lj.si/pdfs/ev1996ds.pdf (14.8.2009).
Tabassi, E., Wilson, C.L., Watson, C. (2004). *Fingerprint Image Quality–NISTIR 7151*, dosegljivo na: http://fingerprint.nist.gov/NFIS/ir_7151.pdf (12.7.2010).
Tetko, I. V., Livingstone, D. J., Luik, A. I. (1995). Neural network studies, 1. Comparison of overfitting and overtraining, *Journal of Chemical Information and Computer Sciences*, 35(5), strani 826-833, dosegljivo na: http://www.vcclab.org/articles/tetko.html#overtraining (7.7.2010).
TM5–698–1 (2003). *Reliability/Availability of Electrical & Mechanical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, And Reconnaissance (C4ISR) Facilities*. Department of the United States Army, dosegljivo na: http://www.wbdg.org/ccb/ARMYCOE/COETM/tm_5_698_1.pdf (7.10.2009).
Trast International (2010). *Identifikacijski sistemi,* dosegljivo na: http://www.trast-int.si/IDS.html (12.6.2010).
U.S. National Library of Medicine (2008). *What is DNA?*, dosegljivo na: http://ghr.nlm.nih.gov/handbook/basics/dna (12.6.2010).
Zadeh, A. L. (1973). Outline of a New Approach to the Analysis of Complex Systems and Decision Processes, *IEEE Transactions on Systems, Man and Cybernetics*, dosegljivo na: http://www-bisc.cs.berkeley.edu/Zadeh-1973.pdf (12.6.2009)
Zadeh, A. L. (1965). Fuzzy Sets. *Information and Control*. Department of Electrical Engineering and Electronics Research Laboratory, University of California, Barkeley, dosegljivo na: http://www-bisc.cs.berkeley.edu/Zadeh-1965.pdf (12.9.2009).
Wayman, J. L. (1999). *Degrees of Freedom as Related to Biometric Device Performance*, dosegljivo na: http://www.engr.sjsu.edu/biometrics/publications_degrees.html (12.1.2011).
Weibull (2006). The Weibull Distribution. *Characteristics of the Weibull Distribution*, dosegljivo na: http://www.weibull.com/LifeDataWeb/characteristics_of_the_weibull_distribution.htm (15.2.2011).
Williams, L. (2007). *Software Reliability Engineering*, dosegljivo na: http://openseminar.org/se/courses/41/modules/206/index/screen.do (10.1.2010).
Wilson, C., Hicklin, A. R., Korves, H., Ulery, B., Zoepfl, M., Bone, M., Grother, P., Micheals, R. J., Otto, S., Watson, C. (2004). *Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report*, NIST Internal Report 7123, dosegljivo na: http://fpvte.nist.gov/report/ir_7123_summary.pdf (9.9.2010).
Wireshark (2011). *Wireshark*, dosegljivo na: http://www.wireshark.org/ (9.9.2010).

18.2 ZAKONI IN STANDARDI

ANSI INCITS 409.3 (2005) Information Technology - Biometric Performance Testing and Reporting–Part 3: Scenario Testing and Reporting.
ANSI X9.84 (2003) Biometric Information Management and Security for the Financial Services Industry.
ANSI/INCITS 358 (2002) The BioAPI Specification.
ANSI/INCITS 377 (2004) Finger Pattern-Based Format for Data Interchange.
ANSI/INCITS 378 (2004) Finger Minutiae Format for Data Interchange.

ANSI/INCITS 381 (2004) Finger Image Format for Data Interchange.
ANSI/INCITS 394 (2004) Application Profile for Interoperability, Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management.
ANSI/INCITS 398 (2005) Common Biometric Exchange Formats Framework (CBEFF).
Bellcore TR–332 (1997) Reliability Prediction Procedure for Electronic Equipment, Issue 6, dosegljivo na: http://www.frontis.co.kr/board/system/db/prediction/upload/82/1034596414/BR-TR-332.pdf (16.8.2009).
BS7799 (1995) Code of practice for Information Security Management.
BS IEC 60605–4 (2001) Equipment reliability testing. Statistical procedures for exponential distribution. Point estimates, confidence intervals, prediction intervals and tolerance intervals.
BS ISO/IEC 29794-1 (2009) Information technology – Biometric sample quality – Framework.
Direktiva 2002/58/ES (2002) Direktiva o zasebnosti in elektronskih komunikacijah, dosegljivo na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:SL:NOT (12.11.2010).
GS1 (2009). GS1 Global Traceability Standard, dosegljivo na: http://www.gs1.org/docs/gsmp/traceability/GS1_Global_Traceability_Standard_i1.pdf (12.11.2009).
IAFIS–DOC–01078–7 (2005) Electronic Fingerprint Transmission Specification (EFTS), Version 7.1, Federal Bureau of Investigation, Criminal Justice Information Services Division
IAFIS–IC–0010 (1997) Wavelet Scalar Quantization (WSQ), Grayscale Fingerprint Image Compression Specification, Version 3, Federal Bureau of Investigation.
IEC 60319 (1999–09) Presentation and specification of reliability data for electronic components.
IEC 61649–8 (2008) Weibull Analysis Standard, 2nd. Edition.
IEC 60812 (1985–07) Analysis techniques for system reliability–Procedure for failure mode and effects analysis (FMEA).
IEC 61014–2 (2003) Programmes for reliability growth.
IEC 61078–2 (2008) Analysis techniques for dependability - Reliability block diagram and boolean methods.
IEC 61164–2 (2003) Reliability growth - Statistical test and estimation methods.
IEC 61165 (1995–01) Application of Markov techniques.
IEC 61703–1 (2001) Mathematical expressions for reliability, availability, maintainability and maintenance support terms.
IEEE 1061 (1998) IEEE Standard for a Software. Quality Metrics Methodology.
IEEE 982.2 (1987) Guide for the Use of Standard Dictionary of Measures to Produce Reliable Software.
INCIST M1 (2007) Study Report on Biometrics in E-Authentication, dosegljivo na: http://www.incits.org/tc_home/m1htm/m1070185rev.pdf (6.7.2009)
ISO/IEC JTC 1/SC 37, Infomation Technology Standards–Biometrics, dosegljivo na: http://isotc.iso.org/livelink/livelink?func=ll&objAction=runReport&objId=3894169&inputLabel1=313770&customview=3922008&const_sort=-

s_nnumber&const_and1=&authenticate=&inputLabel2=&inputLabel3=&inputLabel4=19795&imageField.x=7&imageField.y=6 (17.12.2009).
ISO/IEC JTC 1/SC 37 N 2777 (2008) Biometric Vocabulary, dosegljivo na: http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-2777_SD2_July_2008.pdf?nodeid=7525726&vernum=0 (5. 2. 2010).
ISO/IEC 2382-14 (1997) Information technology–Vocabulary : Reliability, Maintainability, Availability.
ISO/IEC 9126 (2001) Information technology–Software Product Evaluation–Quality characteristics and guidelines for their use, dosegljivo na: http://www.cse.dcu.ie/essiscope/sm2/9126ref.html (8.2.2010).
ISO/IEC 9126-2 (2003) Information technology–Software quality characteristics and metrics–External metrics.
ISO/IEC TR 9126-3 (2003). Information technology–Software quality characteristics and metrics–Internal metrics, dosegljivo na: http://webstore.iec.ch/preview/info_isoiec9126-3%7Bed1.0%7Den.pdf (8.2.2010).
ISO/IEC 9126-4 (2004). Quality in Use Metrics.
ISO 9241 (1997) ISO Ergonomics Standards and Guidelines, dostopno na: http://www.ergoweb.com/resources/reference/guidelines/iso9241.cfm (8.2.2010).
ISO/IEC 90003 (2004). Software engineering–Guidelines for the application of ISO 9001:2000 to computer software, dosegljivo na: http://www.praxiom.com/iso-90003.htm (9.2.2010).
ISO 19092 (2008) Financial services – Biometrics – Security framework.
ISO/IEC 19794-2 (2005) Information Technology – Biometric Data Interchange Format – Part 2: Finger Minutiae Data.
ISO/IEC 19794-4 (2005) Information Technology – Biometric Data Interchange Format – Part 4: Finger Image Data.
ISO/IEC 29109-1 (2009) Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Generalized conformance testing methodology.
ISO/IEC 7816-11 (2004) Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods.
ISO/IEC 14443 (2010) Identification cards – Contactless integrated circuit(s) cards – Proximity cards.
ISO/IEC 14598 (2000) Information Technology – Evaluation of Software Products.
ISO/IEC 15693 (2010) Identification cards – Contactless integrated circuit(s) cards – Vicinity Cards.
ISO/IEC 27001 (2005) Information technology – Security techniques – Information security management systems – Requirements.
ISO/IEC 27002 (2005) Information technology – Security techniques – Code of practice for information security management.
ISO/IEC 27006 (2007) Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.
MIL–HDBK–217 (2001) Reliability Prediction of Electronic Equipment, United States Department of Defense, dosegljivo na: http://snebulos.mit.edu/projects/reference/MIL-STD/MIL-HDBK-217F-Notice2.pdf (12.1.2010).

MIL–STD–498 (1994) Software Development and Documentation, United States Department of Defense, dosegljivo na: http://wwwedms.redstone.army.mil/edrd/ref498/498std.pdf (23.07.2010).
NISTIR 6529–A (2004) Common Biometric Exchange Formats Framework (CBEFF), dosegljivo na: http://csrc.nist.gov/publications/nistir/NISTIR6529A.pdf (12.1.2010).
NISTIR 7298 (2006) Glossary of Key Information Security Terms.
NIST/NFIS2 (2006) dosegljivo na: http://www.itl.nist.gov/iad/894.03/nigos/nigos.html (09.02.2009).
OASIS-INCITS M1 (2006) Use Case Specification: Transportation Worker Identification, dosegljivo na: http://www.oasis-open.org/committees/download.php/20952/TWIC%20Use%20Case%20v1-0.pdf (5. 2. 2010).
SIST EN 50133–1 (1999) Access Control Systems for use in Security Aplications–System Requirements.
UsabilityNet (2007) International Standards for HCI and usability, dosegljivo na: http://www.usabilitynet.org/tools/r_international.htm (12.06.2009).
ZVOP–1 (2004) Zakon o varstvu osebnih podatkov, dosegljivo na : http://www.uradni-list.si/1/objava.jsp?urlid=200794&stevilka=4690 (5.8.2009).
ZVOP–1–UPB1 (2007) Zakon o varstvu osebnih podatkov (uradno prečiščeno besedilo), Ur. l. RS, št. 94/2007.

18.3 DODATEK 1: TABELE

18.4 DODATEK 2: SLIKE

18.5 DODATEK 3: MATRIKE Q, Q*, Q_A, Q_A*

18.5.1 MATRIKA Q BIOMETRIČNEGA SISTEMA

Iz verjetnostnega grafa za zanesljivost biometričnega sistema s slike 11.4 določimo elemente matrike **Q** (tabela 17.1).

V nadaljevanju so zaradi razsežnosti matrike, delne tabele večkrat zapisane na večih zaporednih straneh. Celotno matriko dobimo, če elemente matrike v teh delnih tabelah, zaporedoma horizontalno zložimo.

Tabela 17.1: Matrika **Q** biometričnega sistema

$$\mathbf{Q} = \begin{array}{c|cccccccccccc}
 & S1 & S2 & S3 & S4 & S5 & S6 & S7 & S8 & S9 & S10 & S11 & S12 \\
\hline
S1 & q_{1,1} & q_{1,2} & q_{1,3} & q_{1,4} & q_{1,5} & q_{1,6} & q_{17} & q_{1,8} & q_{1,9} & q_{1,10} & q_{1,11} & q_{1,12} \\
S2 & q_{2,1} & q_{2,2} & q_{2,3} & q_{2,4} & q_{2,5} & q_{2,6} & q_{2,7} & q_{2,8} & q_{2,9} & q_{2,10} & q_{2,11} & q_{2,12} \\
S3 & q_{3,1} & q_{3,2} & q_{3,3} & q_{3,4} & q_{3,5} & q_{3,6} & q_{3,7} & q_{3,8} & q_{3,9} & q_{3,10} & q_{3,11} & q_{3,12} \\
S4 & q_{4,1} & q_{4,2} & q_{4,3} & q_{4,4} & q_{4,5} & q_{4,6} & q_{4,7} & q_{4,8} & q_{4,9} & q_{4,10} & q_{4,11} & q_{4,12} \\
S5 & q_{5,1} & q_{5,2} & q_{5,3} & q_{5,4} & q_{5,5} & q_{5,6} & q_{5,7} & q_{5,8} & q_{5,9} & q_{5,10} & q_{5,11} & q_{5,12} \\
S6 & q_{6,1} & q_{6,2} & q_{6,3} & q_{6,4} & q_{6,5} & q_{66} & q_{6,7} & q_{6,8} & q_{6,9} & q_{6,10} & q_{6,11} & q_{6,12} \\
S7 & q_{7,1} & q_{7,2} & q_{7,3} & q_{7,4} & q_{7,5} & q_{7,6} & q_{7,7} & q_{7,8} & q_{7,9} & q_{7,10} & q_{7,11} & q_{7,12} \\
S8 & q_{8,1} & q_{8,2} & q_{8,3} & q_{8,4} & q_{8,5} & q_{8,6} & q_{8,7} & q_{8,8} & q_{8,9} & q_{8,10} & q_{8,11} & q_{8,12} \\
S9 & q_{9,1} & q_{9,2} & q_{9,3} & q_{9,4} & q_{9,5} & q_{9,6} & q_{9,7} & q_{9,8} & q_{9,9} & q_{9,10} & q_{9,11} & q_{9,12} \\
S10 & q_{10,1} & q_{10,2} & q_{10,3} & q_{10,4} & q_{10,5} & q_{10,6} & q_{10,7} & q_{10,8} & q_{10,9} & q_{10,10} & q_{10,11} & q_{10,12} \\
S11 & q_{11,1} & q_{11,2} & q_{11,3} & q_{11,4} & q_{11,5} & q_{11,6} & q_{11,7} & q_{11,8} & q_{11,9} & q_{11,10} & q_{11,11} & q_{11,12} \\
S12 & q_{12,1} & q_{12,2} & q_{12,3} & q_{12,4} & q_{12,5} & q_{12,6} & q_{12,7} & q_{12,8} & q_{12,9} & q_{12,10} & q_{12,11} & q_{12,12} \\
S13 & q_{13,1} & q_{13,2} & q_{13,3} & q_{13,4} & q_{13,5} & q_{13,6} & q_{13,7} & q_{13,8} & q_{13,9} & q_{13,10} & q_{13,11} & q_{13,12} \\
S14 & q_{14,1} & q_{14,2} & q_{14,3} & q_{14,4} & q_{14,5} & q_{14,6} & q_{14,7} & q_{14,8} & q_{14,9} & q_{14,10} & q_{14,11} & q_{14,12} \\
S15 & q_{15,1} & q_{15,2} & q_{15,3} & q_{15,4} & q_{15,5} & q_{15,6} & q_{15,7} & q_{15,8} & q_{15,9} & q_{15,10} & q_{15,11} & q_{15,12} \\
S16 & q_{16,1} & q_{16,2} & q_{16,3} & q_{16,4} & q_{16,5} & q_{16,6} & q_{16,7} & q_{16,8} & q_{16,9} & q_{16,10} & q_{16,11} & q_{16,12} \\
S17 & q_{17,1} & q_{17,2} & q_{17,3} & q_{17,4} & q_{17,5} & q_{17,6} & q_{17,7} & q_{17,8} & q_{17,9} & q_{17,10} & q_{17,11} & q_{17,12} \\
S18 & q_{18,1} & q_{18,2} & q_{18,3} & q_{18,4} & q_{18,5} & q_{18,6} & q_{18,7} & q_{18,8} & q_{18,9} & q_{18,10} & q_{18,11} & q_{18,12} \\
S19 & q_{19,1} & q_{19,2} & q_{19,3} & q_{19,4} & q_{19,5} & q_{19,6} & q_{19,7} & q_{19,8} & q_{19,9} & q_{19,10} & q_{19,11} & q_{19,12} \\
S20 & q_{20,1} & q_{20,2} & q_{20,3} & q_{20,4} & q_{20,5} & q_{20,6} & q_{20,7} & q_{20,8} & q_{20,9} & q_{20,10} & q_{20,11} & q_{20,12} \\
S21 & q_{21,1} & q_{21,2} & q_{21,3} & q_{21,4} & q_{21,5} & q_{21,6} & q_{21,7} & q_{21,8} & q_{21,9} & q_{21,10} & q_{21,11} & q_{21,12} \\
S22 & q_{22,1} & q_{22,2} & q_{22,3} & q_{22,4} & q_{22,5} & q_{22,6} & q_{22,7} & q_{22,8} & q_{22,9} & q_{22,10} & q_{22,11} & q_{22,12} \\
S23 & q_{23,1} & q_{23,2} & q_{23,3} & q_{23,4} & q_{23,5} & q_{23,6} & q_{23,7} & q_{23,8} & q_{23,9} & q_{23,10} & q_{23,11} & q_{23,12} \\
S24 & q_{24,1} & q_{24,2} & q_{24,3} & q_{24,4} & q_{24,5} & q_{24,6} & q_{24,7} & q_{24,8} & q_{24,9} & q_{24,10} & q_{24,11} & q_{24,12} \\
S25 & q_{25,1} & q_{25,2} & q_{25,3} & q_{25,4} & q_{25,5} & q_{25,6} & q_{25,7} & q_{25,8} & q_{25,9} & q_{25,10} & q_{25,11} & q_{25,12} \\
S26 & q_{26,1} & q_{26,2} & q_{26,3} & q_{26,4} & q_{26,5} & q_{26,6} & q_{26,7} & q_{26,8} & q_{26,9} & q_{26,10} & q_{26,11} & q_{26,12} \\
S27 & q_{27,1} & q_{27,2} & q_{27,3} & q_{27,4} & q_{27,5} & q_{27,6} & q_{27,7} & q_{27,8} & q_{27,9} & q_{27,10} & q_{27,11} & q_{27,12} \\
S28 & q_{28,1} & q_{28,2} & q_{28,3} & q_{28,4} & q_{28,5} & q_{28,6} & q_{28,7} & q_{28,8} & q_{28,9} & q_{28,10} & q_{28,11} & q_{28,12} \\
S29 & q_{29,1} & q_{29,2} & q_{29,3} & q_{29,4} & q_{29,5} & q_{29,6} & q_{29,7} & q_{29,8} & q_{29,9} & q_{29,10} & q_{29,11} & q_{29,12} \\
S30 & q_{30,1} & q_{30,2} & q_{30,3} & q_{30,4} & q_{30,5} & q_{30,6} & q_{30,7} & q_{30,8} & q_{30,9} & q_{30,10} & q_{30,11} & q_{30,12} \\
S31 & q_{31,1} & q_{31,2} & q_{31,3} & q_{31,4} & q_{31,5} & q_{31,6} & q_{31,7} & q_{31,8} & q_{31,9} & q_{31,10} & q_{31,11} & q_{31,12} \\
S32 & q_{32,1} & q_{32,2} & q_{32,3} & q_{32,4} & q_{32,5} & q_{32,6} & q_{32,7} & q_{32,8} & q_{32,9} & q_{32,10} & q_{32,11} & q_{32,12} \\
S33 & q_{33,1} & q_{33,2} & q_{33,3} & q_{33,4} & q_{33,5} & q_{33,6} & q_{33,7} & q_{33,8} & q_{33,9} & q_{33,10} & q_{33,11} & q_{33,12} \\
S34 & q_{34,1} & q_{34,2} & q_{34,3} & q_{34,4} & q_{34,5} & q_{34,6} & q_{34,7} & q_{34,8} & q_{34,9} & q_{34,10} & q_{34,11} & q_{34,12} \\
S35 & q_{35,1} & q_{35,2} & q_{35,3} & q_{35,4} & q_{35,5} & q_{35,6} & q_{35,7} & q_{35,8} & q_{35,9} & q_{35,10} & q_{35,11} & q_{35,12} \\
S36 & q_{36,1} & q_{36,2} & q_{36,3} & q_{36,4} & q_{36,5} & q_{36,6} & q_{36,7} & q_{36,8} & q_{36,9} & q_{36,10} & q_{36,11} & q_{36,12}
\end{array}$$

S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
$q_{1,13}$	$q_{1,14}$	$q_{1,15}$	$q_{1,16}$	$q_{1,17}$	$q_{1,18}$	$q_{1,19}$	$q_{1,20}$	$q_{1,21}$	$q_{1,22}$	$q_{1,23}$	$q_{1,24}$
$q_{2,13}$	$q_{2,14}$	$q_{2,15}$	$q_{2,16}$	$q_{2,17}$	$q_{2,18}$	$q_{2,19}$	$q_{2,20}$	$q_{2,21}$	$q_{2,22}$	$q_{2,23}$	$q_{2,24}$
$q_{3,13}$	$q_{3,14}$	$q_{3,15}$	$q_{3,16}$	$q_{3,17}$	$q_{3,18}$	$q_{3,19}$	$q_{3,20}$	$q_{3,21}$	$q_{3,22}$	$q_{3,23}$	$q_{3,24}$
$q_{4,13}$	$q_{4,14}$	$q_{4,15}$	$q_{4,16}$	$q_{4,17}$	$q_{4,18}$	$q_{4,19}$	$q_{4,20}$	$q_{4,21}$	$q_{4,22}$	$q_{4,23}$	$q_{4,24}$
$q_{5,13}$	$q_{5,14}$	$q_{5,15}$	$q_{5,16}$	$q_{5,17}$	$q_{5,18}$	$q_{5,19}$	$q_{5,20}$	$q_{5,21}$	$q_{5,22}$	$q_{5,23}$	$q_{5,24}$
$q_{6,13}$	$q_{6,14}$	$q_{6,15}$	$q_{6,16}$	$q_{6,17}$	$q_{6,18}$	$q_{6,19}$	$q_{6,20}$	$q_{6,21}$	$q_{6,22}$	$q_{6,23}$	$q_{6,24}$
$q_{7,13}$	$q_{7,14}$	$q_{7,15}$	$q_{7,16}$	$q_{7,17}$	$q_{7,18}$	$q_{7,19}$	q_{720}	q_{721}	q_{722}	q_{723}	q_{724}
$q_{8,13}$	$q_{8,14}$	$q_{8,15}$	$q_{8,16}$	$q_{8,17}$	$q_{8,18}$	$q_{8,19}$	$q_{8,20}$	$q_{8,21}$	$q_{8,22}$	$q_{8,23}$	$q_{8,24}$
$q_{9,13}$	$q_{9,14}$	$q_{9,15}$	$q_{9,16}$	$q_{9,17}$	$q_{9,18}$	$q_{9,19}$	$q_{9,20}$	$q_{9,21}$	$q_{9,22}$	$q_{9,23}$	$q_{9,24}$
$q_{10,13}$	$q_{10,14}$	$q_{10,15}$	$q_{10,16}$	$q_{10,17}$	$q_{10,18}$	$q_{10,19}$	$q_{10,20}$	$q_{10,21}$	$q_{10,22}$	$q_{10,23}$	$q_{10,24}$
$q_{11,13}$	$q_{11,14}$	$q_{11,15}$	$q_{11,16}$	$q_{11,17}$	$q_{11,18}$	$q_{11,19}$	$q_{11,20}$	$q_{11,21}$	$q_{11,22}$	$q_{11,23}$	$q_{11,24}$
$q_{12,13}$	$q_{12,14}$	$q_{12,15}$	$q_{12,16}$	$q_{12,17}$	$q_{12,18}$	$q_{12,19}$	$q_{12,20}$	$q_{12,21}$	$q_{12,22}$	$q_{12,23}$	$q_{12,24}$
$q_{13,13}$	$q_{13,14}$	$q_{13,15}$	$q_{13,16}$	$q_{13,17}$	$q_{13,18}$	$q_{13,19}$	$q_{13,20}$	$q_{13,21}$	$q_{13,22}$	$q_{13,23}$	$q_{13,24}$
$q_{14,13}$	$q_{14,14}$	$q_{14,15}$	$q_{14,16}$	$q_{14,17}$	$q_{14,18}$	$q_{14,19}$	$q_{14,20}$	$q_{14,21}$	$q_{14,22}$	$q_{14,23}$	$q_{14,24}$
$q_{15,13}$	$q_{15,14}$	$q_{15,15}$	$q_{15,16}$	$q_{15,17}$	$q_{15,18}$	$q_{15,19}$	$q_{15,20}$	$q_{15,21}$	$q_{15,22}$	$q_{15,23}$	$q_{15,24}$
$q_{16,13}$	$q_{16,14}$	$q_{16,15}$	$q_{16,16}$	$q_{16,17}$	$q_{16,18}$	$q_{16,19}$	$q_{16,20}$	$q_{16,21}$	$q_{16,22}$	$q_{16,23}$	$q_{16,24}$
$q_{17,13}$	$q_{17,14}$	$q_{17,15}$	$q_{17,16}$	$q_{17,17}$	$q_{17,18}$	$q_{17,19}$	$q_{17,20}$	$q_{17,21}$	$q_{17,22}$	$q_{17,23}$	$q_{17,24}$
$q_{18,13}$	$q_{18,14}$	$q_{18,15}$	$q_{18,16}$	$q_{18,17}$	$q_{18,18}$	$q_{18,19}$	$q_{18,20}$	$q_{18,21}$	$q_{18,22}$	$q_{18,23}$	$q_{18,24}$
$q_{19,13}$	$q_{19,14}$	$q_{19,15}$	$q_{19,16}$	$q_{19,17}$	$q_{19,18}$	$q_{19,19}$	$q_{19,20}$	$q_{19,21}$	$q_{19,22}$	$q_{19,23}$	$q_{19,24}$
$q_{20,13}$	$q_{20,14}$	$q_{20,15}$	$q_{20,16}$	$q_{20,17}$	$q_{20,18}$	$q_{20,19}$	$q_{20,20}$	$q_{20,21}$	$q_{20,22}$	$q_{20,23}$	$q_{20,24}$
$q_{21,13}$	$q_{21,14}$	$q_{21,15}$	$q_{21,16}$	$q_{21,17}$	$q_{21,18}$	$q_{21,19}$	$q_{21,20}$	$q_{21,21}$	$q_{21,22}$	$q_{21,23}$	$q_{21,24}$
$q_{22,13}$	$q_{22,14}$	$q_{22,15}$	$q_{22,16}$	$q_{22,17}$	$q_{22,18}$	$q_{22,19}$	$q_{22,20}$	$q_{22,21}$	$q_{22,22}$	$q_{22,23}$	$q_{22,24}$
$q_{23,13}$	$q_{23,14}$	$q_{23,15}$	$q_{23,16}$	$q_{23,17}$	$q_{23,18}$	$q_{23,19}$	$q_{23,20}$	$q_{23,21}$	$q_{23,22}$	$q_{23,23}$	$q_{23,24}$
$q_{24,13}$	$q_{24,14}$	$q_{24,15}$	$q_{24,16}$	$q_{24,17}$	$q_{24,18}$	$q_{24,19}$	$q_{24,20}$	$q_{24,21}$	$q_{24,22}$	$q_{24,23}$	$q_{24,24}$
$q_{25,13}$	$q_{25,14}$	$q_{25,15}$	$q_{25,16}$	$q_{25,17}$	$q_{25,18}$	$q_{25,19}$	$q_{25,20}$	$q_{25,21}$	$q_{25,22}$	$q_{25,23}$	$q_{25,24}$
$q_{26,13}$	$q_{26,14}$	$q_{26,15}$	$q_{26,16}$	$q_{26,17}$	$q_{26,18}$	$q_{26,19}$	$q_{26,20}$	$q_{26,21}$	$q_{26,22}$	$q_{26,23}$	$q_{26,24}$
$q_{27,13}$	$q_{27,14}$	$q_{27,15}$	$q_{27,16}$	$q_{27,17}$	$q_{27,18}$	$q_{27,19}$	$q_{27,20}$	$q_{27,21}$	$q_{27,22}$	$q_{27,23}$	$q_{27,24}$
$q_{28,13}$	$q_{28,14}$	$q_{28,15}$	$q_{28,16}$	$q_{28,17}$	$q_{28,18}$	$q_{28,19}$	$q_{28,20}$	$q_{28,21}$	$q_{28,22}$	$q_{28,23}$	$q_{28,24}$
$q_{29,13}$	$q_{29,14}$	$q_{29,15}$	$q_{29,16}$	$q_{29,17}$	$q_{29,18}$	$q_{29,19}$	$q_{29,20}$	$q_{29,21}$	$q_{29,22}$	$q_{29,23}$	$q_{29,24}$
$q_{30,13}$	$q_{30,14}$	$q_{30,15}$	$q_{30,16}$	$q_{30,17}$	$q_{30,18}$	$q_{30,19}$	$q_{30,20}$	$q_{30,21}$	$q_{30,22}$	$q_{30,23}$	$q_{30,24}$
$q_{31,13}$	$q_{31,14}$	$q_{31,15}$	$q_{31,16}$	$q_{31,17}$	$q_{31,18}$	$q_{31,19}$	$q_{31,20}$	$q_{31,21}$	$q_{31,22}$	$q_{31,23}$	$q_{31,24}$
$q_{32,13}$	$q_{32,14}$	$q_{32,15}$	$q_{32,16}$	$q_{32,17}$	$q_{32,18}$	$q_{32,19}$	$q_{32,20}$	$q_{32,21}$	$q_{32,22}$	$q_{32,23}$	$q_{32,24}$
$q_{33,13}$	$q_{33,14}$	$q_{33,15}$	$q_{33,16}$	$q_{33,17}$	$q_{33,18}$	$q_{33,19}$	$q_{33,20}$	$q_{33,21}$	$q_{33,22}$	$q_{33,23}$	$q_{33,24}$
$q_{34,13}$	$q_{34,14}$	$q_{34,15}$	$q_{34,16}$	$q_{34,17}$	$q_{34,18}$	$q_{34,19}$	$q_{34,20}$	$q_{34,21}$	$q_{34,22}$	$q_{34,23}$	$q_{34,24}$
$q_{35,13}$	$q_{35,14}$	$q_{35,15}$	$q_{35,16}$	$q_{35,17}$	$q_{35,18}$	$q_{35,19}$	$q_{35,20}$	$q_{35,21}$	$q_{35,22}$	$q_{35,23}$	$q_{35,24}$
$q_{36,13}$	$q_{36,14}$	$q_{36,15}$	$q_{36,16}$	$q_{36,17}$	$q_{36,18}$	$q_{36,19}$	$q_{36,20}$	$q_{36,21}$	$q_{36,22}$	$q_{36,23}$	$q_{36,24}$

S25	S26	S27	S28	S29	S30	S31	S32	S33	S34	S35	S36
$q_{1,25}$	$q_{1,26}$	$q_{1,27}$	$q_{1,28}$	$q_{1,29}$	$q_{1,30}$	$q_{1,31}$	$q_{1,32}$	$q_{1,33}$	$q_{1,34}$	$q_{1,35}$	$q_{1,36}$
$q_{2,25}$	$q_{2,26}$	$q_{2,27}$	$q_{2,28}$	$q_{2,29}$	$q_{2,30}$	$q_{2,31}$	$q_{2,32}$	$q_{2,33}$	$q_{2,34}$	$q_{2,35}$	$q_{2,36}$
$q_{3,25}$	$q_{3,26}$	$q_{3,27}$	$q_{3,28}$	$q_{3,29}$	$q_{3,30}$	$q_{3,31}$	$q_{3,32}$	$q_{3,33}$	$q_{3,34}$	$q_{3,35}$	$q_{3,36}$
$q_{4,25}$	$q_{4,26}$	$q_{4,27}$	$q_{4,28}$	$q_{4,29}$	$q_{4,30}$	$q_{4,31}$	$q_{4,32}$	$q_{4,33}$	$q_{4,34}$	$q_{4,35}$	$q_{4,36}$
$q_{5,25}$	$q_{5,26}$	$q_{5,27}$	$q_{5,28}$	$q_{5,29}$	$q_{5,30}$	$q_{5,31}$	$q_{5,32}$	$q_{5,33}$	$q_{5,34}$	$q_{5,35}$	$q_{5,36}$
$q_{6,25}$	$q_{6,26}$	$q_{6,27}$	$q_{6,28}$	$q_{6,29}$	$q_{6,30}$	$q_{6,31}$	$q_{6,32}$	$q_{6,33}$	$q_{6,34}$	$q_{6,35}$	$q_{6,36}$
q_{725}	q_{726}	q_{727}	q_{728}	q_{729}	q_{730}	q_{731}	q_{732}	q_{733}	q_{734}	q_{735}	q_{736}
$q_{8,25}$	$q_{8,26}$	$q_{8,27}$	$q_{8,28}$	$q_{8,29}$	$q_{8,30}$	$q_{8,31}$	$q_{8,32}$	$q_{8,33}$	$q_{8,34}$	$q_{8,35}$	$q_{8,36}$
$q_{9,25}$	$q_{9,26}$	$q_{9,27}$	$q_{9,28}$	$q_{9,29}$	$q_{9,30}$	$q_{9,31}$	$q_{9,32}$	$q_{9,33}$	$q_{9,34}$	$q_{9,35}$	$q_{9,36}$
$q_{10,25}$	$q_{10,26}$	$q_{10,27}$	$q_{10,28}$	$q_{10,29}$	$q_{10,30}$	$q_{10,31}$	$q_{10,32}$	$q_{10,33}$	$q_{10,34}$	$q_{10,35}$	$q_{10,36}$
$q_{11,25}$	$q_{11,26}$	$q_{11,27}$	$q_{11,28}$	$q_{11,29}$	$q_{11,30}$	$q_{11,31}$	$q_{11,32}$	$q_{11,33}$	$q_{11,34}$	$q_{11,35}$	$q_{11,36}$
$q_{12,25}$	$q_{12,26}$	$q_{12,27}$	$q_{12,28}$	$q_{12,29}$	$q_{12,30}$	$q_{12,31}$	$q_{12,32}$	$q_{12,33}$	$q_{12,34}$	$q_{12,35}$	$q_{12,36}$
$q_{13,25}$	$q_{13,26}$	$q_{13,27}$	$q_{13,28}$	$q_{13,29}$	$q_{13,30}$	$q_{13,31}$	$q_{13,32}$	$q_{13,33}$	$q_{13,34}$	$q_{13,35}$	$q_{13,36}$
$q_{14,25}$	$q_{14,26}$	$q_{14,27}$	$q_{14,28}$	$q_{14,29}$	$q_{14,30}$	$q_{14,31}$	$q_{14,32}$	$q_{14,33}$	$q_{14,34}$	$q_{14,35}$	$q_{14,36}$
$q_{15,25}$	$q_{15,26}$	$q_{15,27}$	$q_{15,28}$	$q_{15,29}$	$q_{15,30}$	$q_{15,31}$	$q_{15,32}$	$q_{15,33}$	$q_{15,34}$	$q_{15,35}$	$q_{15,36}$
$q_{16,25}$	$q_{16,26}$	$q_{16,27}$	$q_{16,28}$	$q_{16,29}$	$q_{16,30}$	$q_{16,31}$	$q_{16,32}$	$q_{16,33}$	$q_{16,34}$	$q_{16,35}$	$q_{16,36}$
$q_{17,25}$	$q_{17,26}$	$q_{17,27}$	$q_{17,28}$	$q_{17,29}$	$q_{17,30}$	$q_{17,31}$	$q_{17,32}$	$q_{17,33}$	$q_{17,34}$	$q_{17,35}$	$q_{17,36}$
$q_{18,25}$	$q_{18,26}$	$q_{18,27}$	$q_{18,28}$	$q_{18,29}$	$q_{18,30}$	$q_{18,31}$	$q_{18,32}$	$q_{18,33}$	$q_{18,34}$	$q_{18,35}$	$q_{18,36}$
$q_{19,25}$	$q_{19,26}$	$q_{19,27}$	$q_{19,28}$	$q_{19,29}$	$q_{19,30}$	$q_{19,31}$	$q_{19,32}$	$q_{19,33}$	$q_{19,34}$	$q_{19,35}$	$q_{19,36}$
$q_{20,25}$	$q_{20,26}$	$q_{20,27}$	$q_{20,28}$	$q_{20,29}$	$q_{20,30}$	$q_{20,31}$	$q_{20,32}$	$q_{20,33}$	$q_{20,34}$	$q_{20,35}$	$q_{20,36}$
$q_{21,25}$	$q_{21,26}$	$q_{21,27}$	$q_{21,28}$	$q_{21,29}$	$q_{21,30}$	$q_{21,31}$	$q_{21,32}$	$q_{21,33}$	$q_{21,34}$	$q_{21,35}$	$q_{21,36}$
$q_{22,25}$	$q_{22,26}$	$q_{22,27}$	$q_{22,28}$	$q_{22,29}$	$q_{22,30}$	$q_{22,31}$	$q_{22,32}$	$q_{22,33}$	$q_{22,34}$	$q_{22,35}$	$q_{22,36}$
$q_{23,25}$	$q_{23,26}$	$q_{23,27}$	$q_{23,28}$	$q_{23,29}$	$q_{23,30}$	$q_{23,31}$	$q_{23,32}$	$q_{23,33}$	$q_{23,34}$	$q_{23,35}$	$q_{23,36}$
$q_{24,25}$	$q_{24,26}$	$q_{24,27}$	$q_{24,28}$	$q_{24,29}$	$q_{24,30}$	$q_{24,31}$	$q_{24,32}$	$q_{24,33}$	$q_{24,34}$	$q_{24,35}$	$q_{24,36}$
$q_{25,25}$	$q_{25,26}$	$q_{25,27}$	$q_{25,28}$	$q_{25,29}$	$q_{25,30}$	$q_{25,31}$	$q_{25,32}$	$q_{25,33}$	$q_{25,34}$	$q_{25,35}$	$q_{25,36}$
$q_{26,25}$	$q_{26,26}$	$q_{26,27}$	$q_{26,28}$	$q_{26,29}$	$q_{26,30}$	$q_{26,31}$	$q_{26,32}$	$q_{26,33}$	$q_{26,34}$	$q_{26,35}$	$q_{26,36}$
$q_{27,25}$	$q_{27,26}$	$q_{27,27}$	$q_{27,28}$	$q_{27,29}$	$q_{27,30}$	$q_{27,31}$	$q_{27,32}$	$q_{27,33}$	$q_{27,34}$	$q_{27,35}$	$q_{27,36}$
$q_{28,25}$	$q_{28,26}$	$q_{28,27}$	$q_{28,28}$	$q_{28,29}$	$q_{28,30}$	$q_{28,31}$	$q_{28,32}$	$q_{28,33}$	$q_{28,34}$	$q_{28,35}$	$q_{28,36}$
$q_{29,25}$	$q_{29,26}$	$q_{29,27}$	$q_{29,28}$	$q_{29,29}$	$q_{29,30}$	$q_{29,31}$	$q_{29,32}$	$q_{29,33}$	$q_{29,34}$	$q_{29,35}$	$q_{29,36}$
$q_{30,25}$	$q_{30,26}$	$q_{30,27}$	$q_{30,28}$	$q_{30,29}$	$q_{30,30}$	$q_{30,31}$	$q_{30,32}$	$q_{30,33}$	$q_{30,34}$	$q_{30,35}$	$q_{30,36}$
$q_{31,25}$	$q_{31,26}$	$q_{31,27}$	$q_{31,28}$	$q_{31,29}$	$q_{31,30}$	$q_{31,31}$	$q_{31,32}$	$q_{31,33}$	$q_{31,34}$	$q_{31,35}$	$q_{31,36}$
$q_{32,25}$	$q_{32,26}$	$q_{32,27}$	$q_{32,28}$	$q_{32,29}$	$q_{32,30}$	$q_{32,31}$	$q_{32,32}$	$q_{32,33}$	$q_{32,34}$	$q_{32,35}$	$q_{32,36}$
$q_{33,25}$	$q_{33,26}$	$q_{33,27}$	$q_{33,28}$	$q_{33,29}$	$q_{33,30}$	$q_{33,31}$	$q_{33,32}$	$q_{33,33}$	$q_{33,34}$	$q_{33,35}$	$q_{33,36}$
$q_{34,25}$	$q_{34,26}$	$q_{34,27}$	$q_{34,28}$	$q_{34,29}$	$q_{34,30}$	$q_{34,31}$	$q_{34,32}$	$q_{34,33}$	$q_{34,34}$	$q_{34,35}$	$q_{34,36}$
$q_{35,25}$	$q_{35,26}$	$q_{35,27}$	$q_{35,28}$	$q_{35,29}$	$q_{35,30}$	$q_{35,31}$	$q_{35,32}$	$q_{35,33}$	$q_{35,34}$	$q_{35,35}$	$q_{35,36}$
$q_{36,25}$	$q_{36,26}$	$q_{36,27}$	$q_{36,28}$	$q_{36,29}$	$q_{36,30}$	$q_{36,31}$	$q_{36,32}$	$q_{36,33}$	$q_{36,34}$	$q_{36,35}$	$q_{36,36}$

Tabela 17.2: Elementi matrike **Q** biometričnega sistema

$q_{1,1} = -(\lambda_1+\lambda_3+3\lambda_4+2\lambda_7+\lambda_9)$	$q_{1,2} = \lambda_1$	$q_{1,3} = \lambda_3$
$q_{2,1} = \mu_1$	$q_{2,2} = -(\lambda_2+\lambda_3+3\lambda_4+2\lambda_7+\lambda_9+\mu_1)$	$q_{2,3} = 0$
$q_{3,1} = 0$	$q_{3,2} = 0$	$q_{3,3} = 0$
$q_{4,1} = \mu_4$	$q_{4,2} = 0$	$q_{4,3} = 0$
$q_{5,1} = \mu_7$	$q_{5,2} = 0$	$q_{5,3} = 0$
$q_{6,1} = 0$	$q_{6,2} = 0$	$q_{6,3} = 0$
$q_{7,1} = 0$	$q_{7,2} = 0$	$q_{7,3} = 0$
$q_{8,1} = 0$	$q_{8,2} = 0$	$q_{8,3} = 0$
$q_{9,1} = 0$	$q_{9,2} = \mu_4$	$q_{9,3} = 0$
$q_{10,1} = 0$	$q_{10,2} = \mu_7$	$q_{10,3} = 0$
$q_{11,1} = 0$	$q_{11,2} = 0$	$q_{11,3} = 0$
$q_{12,1} = 0$	$q_{12,2} = 0$	$q_{12,3} = 0$
$q_{13,1} = 0$	$q_{13,2} = 0$	$q_{13,3} = 0$
$q_{14,1} = 0$	$q_{14,2} = 0$	$q_{14,3} = 0$
$q_{15,1} = 0$	$q_{15,2} = 0$	$q_{15,3} = 0$
$q_{16,1} = 0$	$q_{16,2} = 0$	$q_{16,3} = 0$
$q_{17,1} = 0$	$q_{17,2} = 0$	$q_{17,3} = 0$
$q_{18,1} = 0$	$q_{18,2} = 0$	$q_{18,3} = 0$
$q_{19,1} = 0$	$q_{19,2} = 0$	$q_{19,3} = 0$
$q_{20,1} = 0$	$q_{20,2} = 0$	$q_{20,3} = 0$
$q_{21,1} = 0$	$q_{21,2} = 0$	$q_{21,3} = 0$
$q_{22,1} = 0$	$q_{22,2} = 0$	$q_{22,3} = 0$
$q_{23,1} = 0$	$q_{23,2} = 0$	$q_{233} = 0$
$q_{24,1} = 0$	$q_{24,2} = 0$	$q_{243} = 0$
$q_{25,1} = 0$	$q_{25,2} = 0$	$q_{253} = 0$
$q_{26,1} = 0$	$q_{26,2} = 0$	$q_{263} = 0$
$q_{27,1} = 0$	$q_{27,2} = 0$	$q_{273} = 0$
$q_{28,1} = 0$	$q_{28,2} = 0$	$q_{283} = 0$
$q_{29,1} = 0$	$q_{29,2} = 0$	$q_{293} = 0$
$q_{30,1} = 0$	$q_{30,2} = 0$	$q_{303} = 0$
$q_{31,1} = 0$	$q_{31,2} = 0$	$q_{313} = 0$
$q_{32,1} = 0$	$q_{32,2} = 0$	$q_{323} = 0$
$q_{33,1} = 0$	$q_{33,2} = 0$	$q_{333} = 0$
$q_{34,1} = 0$	$q_{34,2} = 0$	$q_{343} = 0$
$q_{35,1} = 0$	$q_{35,2} = 0$	$q_{353} = 0$
$q_{36,1} = 0$	$q_{36,2} = 0$	$q_{363} = 0$

$q_{1,4} = 3\lambda_4$
$q_{2,4} = 0$
$q_{3,4} = 0$
$q_{4,4} = -(\lambda_1+\lambda_3+2\lambda_4+2\lambda_7+\lambda_9+\mu_4)$
$q_{5,4} = 0$
$q_{6,4} = 0$
$q_{7,4} = 0$
$q_{8,4} = 0$
$q_{9,4} = \mu_1$
$q_{10,4} = 0$
$q_{11,4} = 0$
$q_{12,4} = 0$
$q_{13,4} = 0$
$q_{14,4} = \mu_7$
$q_{15,4} = 0$
$q_{16,4} = 0$
$q_{17,4} = 0$
$q_{18,4} = 0$
$q_{19,4} = 0$
$q_{20,4} = 0$
$q_{21,4} = 0$
$q_{22,4} = 0$
$q_{23,4} = 0$
$q_{24,4} = 0$
$q_{25,4} = 0$
$q_{26,4} = 0$
$q_{27,4} = 0$
$q_{28,4} = 0$
$q_{29,4} = 0$
$q_{30,4} = 0$
$q_{31,4} = 0$
$q_{32,4} = 0$
$q_{33,4} = 0$
$q_{34,4} = 0$
$q_{35,4} = 0$
$q_{36,4} = 0$

$q_{1,5} = 2\lambda_7$
$q_{2,5} = 0$
$q_{3,5} = 0$
$q_{4,5} = 0$
$q_{5,5} = -(\lambda_1+3\lambda_4+\lambda_3+2\lambda_7+\lambda_9+\mu_7)$
$q_{6,5} = 0$
$q_{7,5} = 0$
$q_{8,5} = 0$
$q_{9,5} = 0$
$q_{10,5} = \mu_1$
$q_{11,5} = 0$
$q_{12,5} = 0$
$q_{13,5} = 0$
$q_{14,5} = \mu_4$
$q_{15,5} = 0$
$q_{16,5} = 0$
$q_{17,5} = 0$
$q_{18,5} = 0$
$q_{19,5} = 0$
$q_{20,5} = 0$
$q_{21,5} = 0$
$q_{22,5} = 0$
$q_{23,5} = 0$
$q_{24,5} = 0$
$q_{25,5} = 0$
$q_{26,5} = 0$
$q_{27,5} = 0$
$q_{28,5} = 0$
$q_{29,5} = 0$
$q_{30,5} = 0$
$q_{31,5} = 0$
$q_{32,5} = 0$
$q_{33,5} = 0$
$q_{34,5} = 0$
$q_{35,5} = 0$
$q_{36,5} = 0$

$q_{1,6} = \lambda_9$
$q_{2,6} = 0$
$q_{3,6} = 0$
$q_{4,6} = 0$
$q_{5,6} = 0$
$q_{6,6} = 0$
$q_{7,6} = 0$
$q_{8,6} = 0$
$q_{9,6} = 0$
$q_{10,6} = 0$
$q_{11,6} = 0$
$q_{12,6} = 0$
$q_{13,6} = 0$
$q_{14,6} = 0$
$q_{15,6} = 0$
$q_{16,6} = 0$
$q_{17,6} = 0$
$q_{18,6} = 0$
$q_{19,6} = 0$
$q_{20,6} = 0$
$q_{21,6} = 0$
$q_{22,6} = 0$
$q_{23,6} = 0$
$q_{24,6} = 0$
$q_{25,6} = 0$
$q_{26,6} = 0$
$q_{27,6} = 0$
$q_{28,6} = 0$
$q_{29,6} = 0$
$q_{30,6} = 0$
$q_{31,6} = 0$
$q_{32,6} = 0$
$q_{33,6} = 0$
$q_{34,6} = 0$
$q_{35,6} = 0$
$q_{36,6} = 0$

$q_{1,7} = 0$ $q_{1,8} = 0$ $q_{1,9} = 0$
$q_{2,7} = \lambda_2$ $q_{2,8} = \lambda_3$ $q_{2,9} = 3\lambda_4$
$q_{3,7} = 0$ $q_{3,8} = 0$ $q_{3,9} = 0$
$q_{4,7} = 0$ $q_{4,8} = 0$ $q_{4,9} = \lambda_1$
$q_{5,7} = 0$ $q_{5,8} = 0$ $q_{5,9} = 0$
$q_{6,7} = 0$ $q_{6,8} = 0$ $q_{6,9} = 0$
$q_{7,7} = 0$ $q_{7,8} = 0$ $q_{7,9} = 0$
$q_{8,7} = 0$ $q_{8,8} = 0$ $q_{8,9} = 0$
$q_{9,7} = 0$ $q_{9,8} = 0$ $q_{9,9} = -(\lambda_2+\lambda_3+2\lambda_4+2\lambda_7+\lambda_9+\mu_1+\mu_4)$
$q_{10,7} = 0$ $q_{10,8} = 0$ $q_{10,9} = 0$
$q_{11,7} = 0$ $q_{11,8} = 0$ $q_{11,9} = 0$
$q_{12,7} = 0$ $q_{12,8} = 0$ $q_{12,9} = 0$
$q_{13,7} = 0$ $q_{13,8} = 0$ $q_{13,9} = 0$
$q_{14,7} = 0$ $q_{14,8} = 0$ $q_{14,9} = 0$
$q_{15,7} = 0$ $q_{15,8} = 0$ $q_{15,9} = 0$
$q_{16,7} = 0$ $q_{16,8} = 0$ $q_{16,9} = 0$
$q_{17,7} = 0$ $q_{17,8} = 0$ $q_{17,9} = 0$
$q_{18,7} = 0$ $q_{18,8} = 0$ $q_{18,9} = 0$
$q_{19,7} = 0$ $q_{19,8} = 0$ $q_{19,9} = 0$
$q_{20,7} = 0$ $q_{20,8} = 0$ $q_{20,9} = 0$
$q_{21,7} = 0$ $q_{21,8} = 0$ $q_{21,9} = 0$
$q_{22,7} = 0$ $q_{22,8} = 0$ $q_{22,9} = \mu 7$
$q_{23,7} = 0$ $q_{23,8} = 0$ $q_{23,9} = 0$
$q_{24,7} = 0$ $q_{24,8} = 0$ $q_{24,9} = 0$
$q_{25,7} = 0$ $q_{25,8} = 0$ $q_{25,9} = 0$
$q_{26,7} = 0$ $q_{26,8} = 0$ $q_{26,9} = 0$
$q_{27,7} = 0$ $q_{27,8} = 0$ $q_{27,9} = 0$
$q_{28,7} = 0$ $q_{28,8} = 0$ $q_{28,9} = 0$
$q_{29,7} = 0$ $q_{29,8} = 0$ $q_{29,9} = 0$
$q_{30,7} = 0$ $q_{30,8} = 0$ $q_{30,9} = 0$
$q_{31,7} = 0$ $q_{31,8} = 0$ $q_{31,9} = 0$
$q_{32,7} = 0$ $q_{32,8} = 0$ $q_{32,9} = 0$
$q_{33,7} = 0$ $q_{33,8} = 0$ $q_{33,9} = 0$
$q_{34,7} = 0$ $q_{34,8} = 0$ $q_{34,9} = 0$
$q_{35,7} = 0$ $q_{35,8} = 0$ $q_{35,9} = 0$
$q_{36,7} = 0$ $q_{36,8} = 0$ $q_{36,9} = 0$

$q_{1,10} = 0$ $q_{1,11} = 0$ $q_{1,12} = 0$ $q_{1,13} = 0$
$q_{2,10} = 2\lambda_7$ $q_{2,11} = \lambda_9$ $q_{2,12} = 0$ $q_{2,13} = 0$
$q_{3,10} = 0$ $q_{3,11} = 0$ $q_{3,12} = 0$ $q_{3,13} = 0$
$q_{4,10} = 0$ $q_{4,11} = 0$ $q_{4,12} = \lambda_3$ $q_{4,13} = 2\lambda_4$
$q_{5,10} = \lambda_1$ $q_{5,11} = 0$ $q_{5,12} = 0$ $q_{5,13} = 0$
$q_{6,10} = 0$ $q_{6,11} = 0$ $q_{6,12} = 0$ $q_{6,13} = 0$
$q_{7,10} = 0$ $q_{7,11} = 0$ $q_{7,12} = 0$ $q_{7,13} = 0$
$q_{8,10} = 0$ $q_{8,11} = 0$ $q_{8,12} = 0$ $q_{8,13} = 0$
$q_{9,10} = 0$ $q_{9,11} = 0$ $q_{9,12} = 0$ $q_{9,13} = 0$
$q_{10,10} = -(3\lambda_4+\lambda_2+\lambda_3+\lambda_8+\lambda_9+\mu_1+\mu_7)$ $q_{10,11} = 0$ $q_{10,12} = 0$ $q_{10,13} = 0$
$q_{11,10} = 0$ $q_{11,11} = 0$ $q_{11,12} = 0$ $q_{11,13} = 0$
$q_{12,10} = 0$ $q_{12,11} = 0$ $q_{12,12} = 0$ $q_{12,13} = 0$
$q_{13,10} = 0$ $q_{13,11} = 0$ $q_{13,12} = 0$ $q_{13,13} = 0$
$q_{14,10} = 0$ $q_{14,11} = 0$ $q_{14,12} = 0$ $q_{14,13} = 0$
$q_{15,10} = 0$ $q_{15,11} = 0$ $q_{15,12} = 0$ $q_{15,13} = 0$
$q_{16,10} = 0$ $q_{16,11} = 0$ $q_{16,12} = 0$ $q_{16,13} = 0$
$q_{17,10} = 0$ $q_{17,11} = 0$ $q_{17,12} = 0$ $q_{17,13} = 0$
$q_{18,10} = 0$ $q_{18,11} = 0$ $q_{18,12} = 0$ $q_{18,13} = 0$
$q_{19,10} = 0$ $q_{19,11} = 0$ $q_{19,12} = 0$ $q_{19,13} = 0$
$q_{20,10} = 0$ $q_{20,11} = 0$ $q_{20,12} = 0$ $q_{20,13} = 0$
$q_{21,10} = 0$ $q_{21,11} = 0$ $q_{21,12} = 0$ $q_{21,13} = 0$
$q_{22,10} = \mu_4$ $q_{22,11} = 0$ $q_{22,12} = 0$ $q_{22,13} = 0$
$q_{23,10} = 0$ $q_{23,11} = 0$ $q_{23,12} = 0$ $q_{23,13} = 0$
$q_{24,10} = 0$ $q_{24,11} = 0$ $q_{24,12} = 0$ $q_{24,13} = 0$
$q_{25,10} = 0$ $q_{25,11} = 0$ $q_{25,12} = 0$ $q_{25,13} = 0$
$q_{26,10} = 0$ $q_{26,11} = 0$ $q_{26,12} = 0$ $q_{26,13} = 0$
$q_{27,10} = 0$ $q_{27,11} = 0$ $q_{27,12} = 0$ $q_{27,13} = 0$
$q_{28,10} = 0$ $q_{28,11} = 0$ $q_{28,12} = 0$ $q_{28,13} = 0$
$q_{29,10} = 0$ $q_{29,11} = 0$ $q_{29,12} = 0$ $q_{29,13} = 0$
$q_{30,10} = 0$ $q_{30,11} = 0$ $q_{30,12} = 0$ $q_{30,13} = 0$
$q_{31,10} = 0$ $q_{31,11} = 0$ $q_{31,12} = 0$ $q_{31,13} = 0$
$q_{32,10} = 0$ $q_{32,11} = 0$ $q_{32,12} = 0$ $q_{32,13} = 0$
$q_{33,10} = 0$ $q_{33,11} = 0$ $q_{33,12} = 0$ $q_{33,13} = 0$
$q_{34,10} = 0$ $q_{34,11} = 0$ $q_{34,12} = 0$ $q_{34,13} = 0$
$q_{35,10} = 0$ $q_{35,11} = 0$ $q_{35,12} = 0$ $q_{3513} = 0$
$q_{36,10} = 0$ $q_{36,11} = 0$ $q_{36,12} = 0$ $q_{36,13} = 0$

$q_{1,14} = 0$	$q_{1,15} = 0$	$q_{1,16} = 0$	$q_{1,17} = 0$
$q_{2,14} = 0$	$q_{2,15} = 0$	$q_{2,16} = 0$	$q_{2,17} = 0$
$q_{3,14} = 0$	$q_{3,15} = 0$	$q_{3,16} = 0$	$q_{3,17} = 0$
$q_{4,14} = 2\lambda_7$	$q_{4,15} = \lambda_9$	$q_{4,16} = 0$	$q_{4,17} = 0$
$q_{5,14} = 3\lambda_4$	$q_{5,15} = 0$	$q_{5,16} = \lambda_3$	$q_{517} = \lambda_7$
$q_{6,14} = 0$	$q_{6,15} = 0$	$q_{6,16} = 0$	$q_{6,17} = 0$
$q_{7,14} = 0$	$q_{7,15} = 0$	$q_{7,16} = 0$	$q_{7,17} = 0$
$q_{8,14} = 0$	$q_{8,15} = 0$	$q_{8,16} = 0$	$q_{8,17} = 0$
$q_{9,14} = 0$	$q_{9,15} = 0$	$q_{9,16} = 0$	$q_{9,17} = 0$
$q_{10,14} = 0$	$q_{10,15} = 0$	$q_{10,16} = 0$	$q_{10,17} = 0$
$q_{11,14} = 0$	$q_{11,15} = 0$	$q_{11,16} = 0$	$q_{11,17} = 0$
$q_{12,14} = 0$	$q_{12,15} = 0$	$q_{12,16} = 0$	$q_{12,17} = 0$
$q_{13,14} = 0$	$q_{13,15} = 0$	$q_{13,16} = 0$	$q_{13,17} = 0$
$q_{14,14} = -(\lambda_1+\lambda_3+2\lambda_4+\lambda_7+\lambda_9+\mu_4+\mu_7)$	$q_{14,15} = 0$	$q_{14,16} = 0$	$q_{14,17} = 0$
$q_{15,14} = 0$	$q_{15,15} = 0$	$q_{15,16} = 0$	$q_{15,17} = 0$
$q_{16,14} = 0$	$q_{16,15} = 0$	$q_{16,16} = 0$	$q_{16,17} = 0$
$q_{17,14} = 0$	$q_{17,15} = 0$	$q_{17,16} = 0$	$q_{17,17} = 0$
$q_{18,14} = 0$	$q_{18,15} = 0$	$q_{18,16} = 0$	$q_{18,17} = 0$
$q_{19,14} = 0$	$q_{19,15} = 0$	$q_{19,16} = 0$	$q_{19,17} = 0$
$q_{20,14} = 0$	$q_{20,15} = 0$	$q_{20,16} = 0$	$q_{20,17} = 0$
$q_{21,14} = 0$	$q_{21,15} = 0$	$q_{21,16} = 0$	$q_{21,17} = 0$
$q_{22,14} = \mu_1$	$q_{22,15} = 0$	$q_{22,16} = 0$	$q_{22,17} = 0$
$q_{23,14} = 0$	$q_{23,15} = 0$	$q_{23,16} = 0$	$q_{23,17} = 0$
$q_{24,14} = 0$	$q_{24,15} = 0$	$q_{2416} = 0$	$q_{24,17} = 0$
$q_{25,14} = 0$	$q_{25,15} = 0$	$q_{25,16} = 0$	$q_{25,17} = 0$
$q_{26,14} = 0$	$q_{26,15} = 0$	$q_{2616} = 0$	$q_{26,17} = 0$
$q_{27,14} = 0$	$q_{27,15} = 0$	$q_{27,16} = 0$	$q_{27,17} = 0$
$q_{28,14} = 0$	$q_{28,15} = 0$	$q_{28,16} = 0$	$q_{28,17} = 0$
$q_{29,14} = 0$	$q_{29,15} = 0$	$q_{29,16} = 0$	$q_{29,17} = 0$
$q_{30,14} = 0$	$q_{30,15} = 0$	$q_{30,16} = 0$	$q_{30,17} = 0$
$q_{31,14} = 0$	$q_{31,15} = 0$	$q_{31,16} = 0$	$q_{31,17} = 0$
$q_{32,14} = 0$	$q_{32,15} = 0$	$q_{32,16} = 0$	$q_{32,17} = 0$
$q_{33,14} = 0$	$q_{33,15} = 0$	$q_{33,16} = 0$	$q_{33,17} = 0$
$q_{34,14} = 0$	$q_{34,15} = 0$	$q_{34,16} = 0$	$q_{34,17} = 0$
$q_{35,14} = 0$	$q_{35,15} = 0$	$q_{35,16} = 0$	$q_{35,17} = 0$
$q_{36,14} = 0$	$q_{36,15} = 0$	$q_{36,16} = 0$	$q_{36,17} = 0$

$$
\begin{array}{llllllll}
q_{1,18} = 0 & q_{1,19} = 0 & q_{1,20} = 0 & q_{1,21} = 0 \\
q_{2,18} = 0 & q_{2,19} = 0 & q_{2,20} = 0 & q_{2,21} = 0 \\
q_{3,18} = 0 & q_{3,19} = 0 & q_{3,20} = 0 & q_{3,21} = 0 \\
q_{4,18} = 0 & q_{4,19} = 0 & q_{4,20} = 0 & q_{4,21} = 0 \\
q_{5,18} = \lambda_9 & q_{5,19} = 0 & q_{5,20} = 0 & q_{5,21} = 0 \\
q_{6,18} = 0 & q_{6,19} = 0 & q_{6,20} = 0 & q_{6,21} = 0 \\
q_{7,18} = 0 & q_{7,19} = 0 & q_{7,20} = 0 & q_{7,21} = 0 \\
q_{8,18} = 0 & q_{8,19} = 0 & q_{8,20} = 0 & q_{8,21} = 0 \\
q_{9,18} = 0 & q_{9,19} = \lambda_2 & q_{9,20} = \lambda_3 & q_{9,21} = 2\lambda_4 \\
q_{10,18} = 0 & q_{10,19} = 0 & q_{10,20} = 0 & q_{10,21} = 0 \\
q_{11,18} = 0 & q_{11,19} = 0 & q_{11,20} = 0 & q_{11,21} = 0 \\
q_{12,18} = 0 & q_{12,19} = 0 & q_{12,20} = 0 & q_{12,21} = 0 \\
q_{13,18} = 0 & q_{13,19} = 0 & q_{13,20} = 0 & q_{13,21} = 0 \\
q_{14,18} = 0 & q_{14,19} = 0 & q_{14,20} = 0 & q_{14,21} = 0 \\
q_{15,18} = 0 & q_{15,19} = 0 & q_{15,20} = 0 & q_{15,21} = 0 \\
q_{16,18} = 0 & q_{16,19} = 0 & q_{16,20} = 0 & q_{16,21} = 0 \\
q_{17,18} = 0 & q_{17,19} = 0 & q_{17,20} = 0 & q_{17,21} = 0 \\
q_{18,18} = 0 & q_{18,19} = 0 & q_{18,20} = 0 & q_{18,21} = 0 \\
q_{19,18} = 0 & q_{19,19} = 0 & q_{19,20} = 0 & q_{19,21} = 0 \\
q_{20,18} = 0 & q_{20,19} = 0 & q_{20,20} = 0 & q_{20,21} = 0 \\
q_{21,18} = 0 & q_{21,19} = 0 & q_{21,20} = 0 & q_{21,21} = 0 \\
q_{22,18} = 0 & q_{22,19} = 0 & q_{22,20} = 0 & q_{22,21} = 0 \\
q_{23,18} = 0 & q_{23,19} = 0 & q_{23,20} = 0 & q_{23,21} = 0 \\
q_{24,18} = 0 & q_{24,19} = 0 & q_{24,20} = 0 & q_{24,21} = 0 \\
q_{25,18} = 0 & q_{25,19} = 0 & q_{25,20} = 0 & q_{25,21} = 0 \\
q_{26,18} = 0 & q_{26,19} = 0 & q_{26,20} = 0 & q_{26,21} = 0 \\
q_{27,18} = 0 & q_{27,19} = 0 & q_{27,20} = 0 & q_{27,21} = 0 \\
q_{28,18} = 0 & q_{28,19} = 0 & q_{28,20} = 0 & q_{28,21} = 0 \\
q_{29,18} = 0 & q_{29,19} = 0 & q_{29,20} = 0 & q_{29,21} = 0 \\
q_{30,18} = 0 & q_{30,19} = 0 & q_{30,20} = 0 & q_{30,21} = 0 \\
q_{31,18} = 0 & q_{31,19} = 0 & q_{31,20} = 0 & q_{31,21} = 0 \\
q_{32,18} = 0 & q_{32,19} = 0 & q_{32,20} = 0 & q_{32,21} = 0 \\
q_{33,18} = 0 & q_{33,19} = 0 & q_{33,20} = 0 & q_{33,21} = 0 \\
q_{34,18} = 0 & q_{34,19} = 0 & q_{34,20} = 0 & q_{34,21} = 0 \\
q_{35,18} = 0 & q_{35,19} = 0 & q_{35,20} = 0 & q_{35,21} = 0 \\
q_{36,18} = 0 & q_{36,19} = 0 & q_{36,20} = 0 & q_{36,21} = 0
\end{array}
$$

$q_{1,22} = 0$ $q_{1,23} = 0$ $q_{1,24} = 0$ $q_{1,25} = 0$
$q_{2,22} = 0$ $q_{2,23} = 0$ $q_{2,24} = 0$ $q_{2,25} = 0$
$q_{3,22} = 0$ $q_{3,23} = 0$ $q_{3,24} = 0$ $q_{3,25} = 0$
$q_{4,22} = 0$ $q_{4,23} = 0$ $q_{4,24} = 0$ $q_{4,25} = 0$
$q_{5,22} = 0$ $q_{5,23} = 0$ $q_{5,24} = 0$ $q_{5,25} = 0$
$q_{6,22} = 0$ $q_{6,23} = 0$ $q_{6,24} = 0$ $q_{6,25} = 0$
$q_{7,22} = 0$ $q_{7,23} = 0$ $q_{7,24} = 0$ $q_{7,25} = 0$
$q_{8,22} = 0$ $q_{8,23} = 0$ $q_{8,24} = 0$ $q_{8,25} = 0$
$q_{9,22} = 2\lambda_7$ $q_{9,23} = \lambda_9$ $q_{9,24} = 0$ $q_{9,25} = 0$
$q_{10,22} = 3\lambda_4$ $q_{10,23} = 0$ $q_{10,24} = \lambda_2$ $q_{10,25} = \lambda_3$
$q_{11,22} = 0$ $q_{11,23} = 0$ $q_{11,24} = 0$ $q_{11,25} = 0$
$q_{12,22} = 0$ $q_{12,23} = 0$ $q_{12,24} = 0$ $q_{12,25} = 0$
$q_{13,22} = 0$ $q_{13,23} = 0$ $q_{13,24} = 0$ $q_{13,25} = 0$
$q_{14,22} = \lambda_1$ $q_{14,23} = 0$ $q_{14,24} = 0$ $q_{14,25} = 0$
$q_{15,22} = 0$ $q_{15,23} = 0$ $q_{15,24} = 0$ $q_{15,25} = 0$
$q_{16,22} = 0$ $q_{16,23} = 0$ $q_{16,24} = 0$ $q_{16,25} = 0$
$q_{17,22} = 0$ $q_{17,23} = 0$ $q_{17,24} = 0$ $q_{17,25} = 0$
$q_{18,22} = 0$ $q_{18,23} = 0$ $q_{18,24} = 0$ $q_{18,25} = 0$
$q_{19,22} = 0$ $q_{19,23} = 0$ $q_{19,24} = 0$ $q_{19,25} = 0$
$q_{20,22} = 0$ $q_{20,23} = 0$ $q_{20,24} = 0$ $q_{20,25} = 0$
$q_{21,22} = 0$ $q_{21,23} = 0$ $q_{21,24} = 0$ $q_{21,25} = 0$
$q_{22,22} = -(\lambda_2+\lambda_3+\lambda_5+\lambda_8+\lambda_9+\mu_1+\mu_4+\mu_7)$ $q_{22,23} = 0$ $q_{22,24} = 0$ $q_{22,25} = 0$
$q_{23,22} = 0$ $q_{23,23} = 0$ $q_{23,24} = 0$ $q_{23,25} = 0$
$q_{24,22} = 0$ $q_{24,23} = 0$ $q_{24,24} = 0$ $q_{24,25} = 0$
$q_{25,22} = 0$ $q_{25,23} = 0$ $q_{25,24} = 0$ $q_{25,25} = 0$
$q_{26,22} = 0$ $q_{26,23} = 0$ $q_{26,24} = 0$ $q_{26,25} = 0$
$q_{27,22} = 0$ $q_{27,23} = 0$ $q_{27,24} = 0$ $q_{27,25} = 0$
$q_{28,22} = 0$ $q_{28,23} = 0$ $q_{28,24} = 0$ $q_{28,25} = 0$
$q_{29,22} = 0$ $q_{29,23} = 0$ $q_{29,24} = 0$ $q_{29,25} = 0$
$q_{30,22} = 0$ $q_{30,23} = 0$ $q_{30,24} = 0$ $q_{30,25} = 0$
$q_{31,22} = 0$ $q_{31,23} = 0$ $q_{31,24} = 0$ $q_{31,25} = 0$
$q_{32,22} = 0$ $q_{32,23} = 0$ $q_{32,24} = 0$ $q_{32,25} = 0$
$q_{33,22} = 0$ $q_{33,23} = 0$ $q_{33,24} = 0$ $q_{33,25} = 0$
$q_{34,22} = 0$ $q_{34,23} = 0$ $q_{34,24} = 0$ $q_{34,25} = 0$
$q_{35,22} = 0$ $q_{35,23} = 0$ $q_{35,24} = 0$ $q_{35,25} = 0$
$q_{36,22} = 0$ $q_{36,23} = 0$ $q_{36,24} = 0$ $q_{36,25} = 0$

$q_{1,26}$	=	0	$q_{1,27}$	=	0	$q_{1,28}$	=	0	$q_{1,29}$	=	0
$q_{2,26}$	=	0	$q_{2,27}$	=	0	$q_{2,28}$	=	0	$q_{2,29}$	=	0
$q_{3,26}$	=	0	$q_{3,27}$	=	0	$q_{3,28}$	=	0	$q_{3,29}$	=	0
$q_{4,26}$	=	0	$q_{4,27}$	=	0	$q_{4,28}$	=	0	$q_{4,29}$	=	0
$q_{5,26}$	=	0	$q_{5,27}$	=	0	$q_{5,28}$	=	0	$q_{5,29}$	=	0
$q_{6,26}$	=	0	$q_{6,27}$	=	0	$q_{6,28}$	=	0	$q_{6,29}$	=	0
$q_{7,26}$	=	0	$q_{7,27}$	=	0	$q_{7,28}$	=	0	$q_{7,29}$	=	0
$q_{8,26}$	=	0	$q_{8,27}$	=	0	$q_{8,28}$	=	0	$q_{8,29}$	=	0
$q_{9,26}$	=	0	$q_{9,27}$	=	0	$q_{9,28}$	=	0	$q_{9,29}$	=	0
$q_{10,26}$	=	λ_8	$q_{10,27}$	=	λ_9	$q_{10,28}$	=	0	$q_{10,29}$	=	0
$q_{11,26}$	=	0	$q_{11,27}$	=	0	$q_{11,28}$	=	0	$q_{11,29}$	=	0
$q_{12,26}$	=	0	$q_{12,27}$	=	0	$q_{12,28}$	=	0	$q_{12,29}$	=	0
$q_{13,26}$	=	0	$q_{13,27}$	=	0	$q_{13,28}$	=	0	$q_{13,29}$	=	0
$q_{14,26}$	=	0	$q_{14,27}$	=	0	$q_{14,28}$	=	λ_3	$q_{14,29}$	=	$2\lambda_4$
$q_{15,26}$	=	0	$q_{15,27}$	=	0	$q_{15,28}$	=	0	$q_{15,29}$	=	0
$q_{16,26}$	=	0	$q_{16,27}$	=	0	$q_{16,28}$	=	0	$q_{16,29}$	=	0
$q_{17,26}$	=	0	$q_{17,27}$	=	0	$q_{17,28}$	=	0	$q_{17,29}$	=	0
$q_{18,26}$	=	0	$q_{18,27}$	=	0	$q_{18,28}$	=	0	$q_{18,29}$	=	0
$q_{19,26}$	=	0	$q_{19,27}$	=	0	$q_{19,28}$	=	0	$q_{19,29}$	=	0
$q_{20,26}$	=	0	$q_{20,27}$	=	0	$q_{20,28}$	=	0	$q_{20,29}$	=	0
$q_{21,26}$	=	0	$q_{21,27}$	=	0	$q_{21,28}$	=	0	$q_{21,29}$	=	0
$q_{22,26}$	=	0	$q_{22,27}$	=	0	$q_{22,28}$	=	0	$q_{22,29}$	=	0
$q_{23,26}$	=	0	$q_{23,27}$	=	0	$q_{23,28}$	=	0	$q_{23,29}$	=	0
$q_{24,26}$	=	0	$q_{24,27}$	=	0	$q_{24,28}$	=	0	$q_{24,29}$	=	0
$q_{25,26}$	=	0	$q_{25,27}$	=	0	$q_{25,28}$	=	0	$q_{25,29}$	=	0
$q_{26,26}$	=	0	$q_{26,27}$	=	0	$q_{26,28}$	=	0	$q_{26,29}$	=	0
$q_{27,26}$	=	0	$q_{27,27}$	=	0	$q_{27,28}$	=	0	$q_{27,29}$	=	0
$q_{28,26}$	=	0	$q_{28,27}$	=	0	$q_{28,28}$	=	0	$q_{28,29}$	=	0
$q_{29,26}$	=	0	$q_{29,27}$	=	0	$q_{29,28}$	=	0	$q_{29,29}$	=	0
$q_{30,26}$	=	0	$q_{30,27}$	=	0	$q_{30,28}$	=	0	$q_{30,29}$	=	0
$q_{31,26}$	=	0	$q_{31,27}$	=	0	$q_{31,28}$	=	0	$q_{31,29}$	=	0
$q_{32,26}$	=	0	$q_{32,27}$	=	0	$q_{32,28}$	=	0	$q_{32,29}$	=	0
$q_{33,26}$	=	0	$q_{33,27}$	=	0	$q_{33,28}$	=	0	$q_{33,29}$	=	0
$q_{34,26}$	=	0	$q_{34,27}$	=	0	$q_{34,28}$	=	0	$q_{34,29}$	=	0
$q_{35,26}$	=	0	$q_{35,27}$	=	0	$q_{35,28}$	=	0	$q_{35,29}$	=	0
$q_{36,26}$	=	0	$q_{36,27}$	=	0	$q_{36,28}$	=	0	$q_{36,29}$	=	0

$$
\begin{array}{llllllll}
q_{1,30}=0 & q_{1,31}=0 & q_{1,32}=0 & q_{1,33}=0 & q_{1,34}=0 & q_{1,35}=0 & q_{1,36}=0 \\
q_{2,30}=0 & q_{2,31}=0 & q_{2,32}=0 & q_{2,33}=0 & q_{2,34}=0 & q_{2,35}=0 & q_{2,36}=0 \\
q_{3,30}=0 & q_{3,31}=0 & q_{3,32}=0 & q_{3,33}=0 & q_{3,34}=0 & q_{3,35}=0 & q_{3,36}=0 \\
q_{4,30}=0 & q_{4,31}=0 & q_{4,32}=0 & q_{4,33}=0 & q_{4,34}=0 & q_{4,35}=0 & q_{4,36}=0 \\
q_{5,30}=0 & q_{5,31}=0 & q_{5,32}=0 & q_{5,33}=0 & q_{5,34}=0 & q_{5,35}=0 & q_{5,36}=0 \\
q_{6,30}=0 & q_{6,31}=0 & q_{6,32}=0 & q_{6,33}=0 & q_{6,34}=0 & q_{6,35}=0 & q_{6,36}=0 \\
q_{7,30}=0 & q_{7,31}=0 & q_{7,32}=0 & q_{7,33}=0 & q_{7,34}=0 & q_{7,35}=0 & q_{7,36}=0 \\
q_{8,30}=0 & q_{8,31}=0 & q_{8,32}=0 & q_{8,33}=0 & q_{8,34}=0 & q_{8,35}=0 & q_{8,36}=0 \\
q_{9,30}=0 & q_{9,31}=0 & q_{9,32}=0 & q_{9,33}=0 & q_{9,34}=0 & q_{9,35}=0 & q_{9,36}=0 \\
q_{10,30}=0 & q_{10,31}=0 & q_{10,32}=0 & q_{10,33}=0 & q_{10,34}=0 & q_{10,35}=0 & q_{10,36}=0 \\
q_{11,30}=0 & q_{11,31}=0 & q_{11,32}=0 & q_{11,33}=0 & q_{11,34}=0 & q_{11,35}=0 & q_{11,36}=0 \\
q_{12,30}=0 & q_{12,31}=0 & q_{12,32}=0 & q_{12,33}=0 & q_{12,34}=0 & q_{12,35}=0 & q_{12,36}=0 \\
q_{13,30}=0 & q_{13,31}=0 & q_{13,32}=0 & q_{13,33}=0 & q_{13,34}=0 & q_{13,35}=0 & q_{13,36}=0 \\
q_{14,30}=\lambda_7 & q_{14,31}=\lambda_9 & q_{14,32}=0 & q_{14,33}=0 & q_{14,34}=0 & q_{14,35}=0 & q_{14,36}=0 \\
q_{15,30}=0 & q_{15,31}=0 & q_{15,32}=0 & q_{15,33}=0 & q_{15,34}=0 & q_{15,35}=0 & q_{15,36}=0 \\
q_{16,30}=0 & q_{16,31}=0 & q_{16,32}=0 & q_{16,33}=0 & q_{16,34}=0 & q_{16,35}=0 & q_{16,36}=0 \\
q_{17,30}=0 & q_{17,31}=0 & q_{17,32}=0 & q_{17,33}=0 & q_{17,34}=0 & q_{17,35}=0 & q_{17,36}=0 \\
q_{18,30}=0 & q_{18,31}=0 & q_{18,32}=0 & q_{18,33}=0 & q_{18,34}=0 & q_{18,35}=0 & q_{18,36}=0 \\
q_{19,30}=0 & q_{19,31}=0 & q_{19,32}=0 & q_{19,33}=0 & q_{19,34}=0 & q_{19,35}=0 & q_{19,36}=0 \\
q_{20,30}=0 & q_{20,31}=0 & q_{20,32}=0 & q_{20,33}=0 & q_{20,34}=0 & q_{20,35}=0 & q_{20,36}=0 \\
q_{21,30}=0 & q_{21,31}=0 & q_{21,32}=0 & q_{21,33}=0 & q_{21,34}=0 & q_{21,35}=0 & q_{21,36}=0 \\
q_{22,30}=0 & q_{22,31}=0 & q_{22,32}=0 & q_{22,33}=0 & q_{22,34}=0 & q_{22,35}=0 & q_{22,36}=0 \\
q_{23,30}=0 & q_{23,31}=0 & q_{23,32}=0 & q_{23,33}=0 & q_{23,34}=0 & q_{23,35}=0 & q_{23,36}=0 \\
q_{24,30}=0 & q_{24,31}=0 & q_{24,32}=0 & q_{24,33}=0 & q_{24,34}=0 & q_{24,35}=0 & q_{24,36}=0 \\
q_{25,30}=0 & q_{25,31}=0 & q_{25,32}=0 & q_{25,33}=0 & q_{25,34}=0 & q_{25,35}=0 & q_{25,36}=0 \\
q_{26,30}=0 & q_{26,31}=0 & q_{26,32}=0 & q_{26,33}=0 & q_{26,34}=0 & q_{26,35}=0 & q_{26,36}=0 \\
q_{27,30}=0 & q_{27,31}=0 & q_{27,32}=0 & q_{27,33}=0 & q_{27,34}=0 & q_{27,35}=0 & q_{27,36}=0 \\
q_{28,30}=0 & q_{28,31}=0 & q_{28,32}=0 & q_{28,33}=0 & q_{28,34}=0 & q_{28,35}=0 & q_{28,36}=0 \\
q_{29,30}=0 & q_{29,31}=0 & q_{29,32}=0 & q_{29,33}=0 & q_{29,34}=0 & q_{29,35}=0 & q_{29,36}=0 \\
q_{30,30}=0 & q_{30,31}=0 & q_{30,32}=0 & q_{30,33}=0 & q_{30,34}=0 & q_{30,35}=0 & q_{30,36}=0 \\
q_{31,30}=0 & q_{31,31}=0 & q_{31,32}=0 & q_{31,33}=0 & q_{31,34}=0 & q_{31,35}=0 & q_{31,36}=0 \\
q_{32,30}=0 & q_{32,31}=0 & q_{32,32}=0 & q_{32,33}=0 & q_{32,34}=0 & q_{32,35}=0 & q_{32,36}=0 \\
q_{33,30}=0 & q_{33,31}=0 & q_{33,32}=0 & q_{33,33}=0 & q_{33,34}=0 & q_{33,35}=0 & q_{33,36}=0 \\
q_{34,30}=0 & q_{34,31}=0 & q_{34,32}=0 & q_{34,33}=0 & q_{34,34}=0 & q_{34,35}=0 & q_{34,36}=0 \\
q_{35,30}=0 & q_{35,31}=0 & q_{35,32}=0 & q_{35,33}=0 & q_{35,34}=0 & q_{35,35}=0 & q_{35,36}=0 \\
q_{36,30}=0 & q_{36,31}=0 & q_{36,32}=0 & q_{36,33}=0 & q_{36,34}=0 & q_{36,35}=0 & q_{36,36}=0
\end{array}
$$

18.5.2 MATRIKA Q* BIOMETRIČNEGA SISTEMA

Iz matrike **Q** v poglavju 17.5.1 določimo matriko **Q*** (tabela 17.3) in pripadajoče elemente matrike.

Tabela 17.3: Matrika **Q*** biometričnega sistema

Q* =

	S1	S2	S4	S5	S9	S10	S14	S22
S1	$-q_{1,1}$	$q_{1,2}$	$q_{1,4}$	$q_{1,5}$	$q_{1,9}$	$q_{1,10}$	$q_{1,14}$	$q_{1,22}$
S2	$q_{2,1}$	$-q_{2,2}$	$q_{2,4}$	$q_{2,5}$	$q_{2,9}$	$q_{2,10}$	$q_{2,14}$	$q_{2,22}$
S4	$q_{4,1}$	$q_{4,2}$	$-q_{4,4}$	$q_{4,5}$	$q_{4,9}$	$q_{4,10}$	$q_{4,14}$	$q_{4,22}$
S5	$q_{5,1}$	$q_{5,2}$	$q_{5,4}$	$-q_{5,5}$	$q_{5,9}$	$q_{5,10}$	$q_{5,14}$	$q_{5,22}$
S9	$q_{9,1}$	$q_{9,2}$	$q_{9,4}$	$q_{9,5}$	$-q_{9,9}$	$q_{9,10}$	$q_{9,14}$	$q_{9,22}$
S10	$q_{10,1}$	$q_{10,2}$	$q_{10,4}$	$q_{10,5}$	$q_{10,9}$	$-q_{10,10}$	$q_{10,14}$	$q_{10,22}$
S14	$q_{14,1}$	$q_{14,2}$	$q_{14,4}$	$q_{14,5}$	$q_{14,9}$	$q_{14,10}$	$-q_{14,14}$	$q_{14,22}$
S22	$q_{22,1}$	$q_{22,2}$	$q_{22,4}$	$q_{22,5}$	$q_{22,9}$	$q_{22,10}$	$q_{22,14}$	$-q_{22,22}$

Tabela 17.4: Elementi matrike **Q*** biometričnega sistema

$-q_{1,1} = (\lambda_1+\lambda_3+3\lambda_4+2\lambda_7+\lambda_9)$ $\quad q_{1,2} = -\lambda_1$

$q_{2,1} = -\mu_1$ $\quad -q_{2,2} = (\lambda_2+\lambda_3+3\lambda_4+2\lambda_7+\lambda_9+\mu_1)$

$q_{4,1} = -\mu_4$ $\quad q_{4,2} = 0$

$q_{5,1} = -\mu_7$ $\quad q_{5,2} = 0$

$q_{9,1} = 0$ $\quad q_{9,2} = -\mu_4$

$q_{10,1} = 0$ $\quad q_{10,2} = -\mu_7$

$q_{14,1} = 0$ $\quad q_{14,2} = 0$

$q_{22,1} = 0$ $\quad q_{22,2} = 0$

$q_{1,4} = -3\lambda_4$ $\quad q_{1,5} = -2\lambda_7$

$q_{2,4} = 0$ $\quad q_{2,5} = 0$

$-q_{4,4} = (\lambda 1+\lambda 3+2\lambda 4+2\lambda 7+\lambda 9+\mu 4)$ $\quad q_{4,5} = 0$

$q_{5,4} = 0$ $\quad -q_{5,5} = (\lambda_1+3\lambda_4+\lambda_3+2\lambda_7+\lambda_9+\mu_7)$

$q_{9,4} = -\mu_1$ $\quad q_{9,5} = 0$

$q_{10,4} = 0$ $\quad q_{10,5} = -\mu_1$

$q_{14,4} = -\mu_7$ $\quad q_{14,5} = -\mu_4$

$q_{22,4} = 0$ $\quad q_{22,5} = 0$

$q_{1,9} = 0$ $\quad q_{1,10} = 0$

$q_{2,9} = -3\lambda_4$ $\quad q_{2,10} = -2\lambda_7$

$q_{4,9} = -\lambda_1$ $\quad q_{4,10} = 0$

$q_{5,9} = 0$ $\quad q_{5,10} = -\lambda_1$

$-q_{9,9} = (\lambda_2+\lambda_3+2\lambda_4+2\lambda_7+\lambda_9+\mu_1+\mu_4)$ $q_{9,10} = 0$

$q_{10,9} = 0$ $-q_{10,10} = (3\lambda_4+\lambda_2+\lambda_3+\lambda_8+\lambda_9+\mu_1+\mu_7)$

$q_{14,9} = 0$ $q_{14,10} = 0$

$q_{22,9} = -\mu_7$ $q_{22,10} = -\mu_4$

$q_{1,14} = 0$ $q_{1,22} = 0$

$q_{2,14} = 0$ $q_{2,22} = 0$

$q_{4,14} = -2\lambda_7$ $q_{4,22} = 0$

$q_{5,14} = -3\lambda_4$ $q_{5,22} = 0$

$q_{9,14} = 0$ $q_{9,22} = -2\lambda_7$

$q_{10,14} = 0$ $q_{10,22} = -3\lambda_4$

$-q_{14,14} = (\lambda_1+\lambda_3+2\lambda_4+\lambda_7+\lambda_9+\mu_4+\mu_7)$ $q_{14,22} = -\lambda_1$

$q_{22,14} = -\mu_1$ $-q_{22,22} = (\lambda_2+\lambda_3+\lambda_5+\lambda_8+\lambda_9+\mu_1+\mu_4+\mu_7)$

18.5.3 DOLOČITEV MATRIKE Q_A , Q_A* BIOMETRIČNEGA SISTEMA

Na osnovi verjetnostnega grafa za razpoložljivost biometričnega sistema določimo matriko $\mathbf{Q_A}$ in pripadajoče elemente matrike (tabela 17.5). Matrika $\mathbf{Q_A}$* je matrika $\mathbf{Q_A}$, ki ima v zadnjem stolpcu enke.

Tabela 17.5: Elementi matrike $\mathbf{Q_A^*}$ biometričnega sistema

$-q_{1,1} = -(\lambda_1+\lambda_3+3\lambda_4+2\lambda_7+\lambda_9)$	$q_{1,2} = \lambda_1$	$q_{1,3} = \lambda_3$
$q_{2,1} = \mu_1$	$-q_{2,2} = -(\lambda_2+\lambda_3+3\lambda_4+2\lambda_7+\lambda_9+\mu_1)$	$q_{2,3} = 0$
$q_{3,1} = \mu_3$	$q_{3,2} = 0$	$-q_{3,3} = -\mu_3$
$q_{4,1} = \mu_4$	$q_{4,2} = 0$	$q_{4,3} = 0$
$q_{5,1} = \mu_7$	$q_{5,2} = 0$	$q_{5,3} = 0$
$q_{6,1} = \mu_9$	$q_{6,2} = 0$	$q_{6,3} = 0$
$q_{7,1} = 0$	$q_{7,2} = \mu_2$	$q_{7,3} = 0$
$q_{8,1} = 0$	$q_{82} = \mu_3$	$q_{8,3} = \mu_1$
$q_{9,1} = 0$	$q_{9,2} = \mu_4$	$q_{9,3} = 0$
$q_{10,1} = 0$	$q_{10,2} = \mu_7$	$q_{10,3} = 0$
$q_{11,1} = 0$	$q_{11,2} = \mu_9$	$q_{11,3} = 0$
$q_{12,1} = 0$	$q_{12,2} = 0$	$q_{12,3} = \mu_4$
$q_{13,1} = 0$	$q_{13,2} = 0$	$q_{13,3} = 0$
$q_{14,1} = 0$	$q_{14,2} = 0$	$q_{14,3} = 0$
$q_{15,1} = 0$	$q_{15,2} = 0$	$q_{15,3} = 0$
$q_{16,1} = 0$	$q_{16,2} = 0$	$q_{16,3} = \mu_7$
$q_{17,1} = 0$	$q_{17,2} = 0$	$q_{17,3} = 0$
$q_{18,1} = 0$	$q_{18,2} = 0$	$q_{18,3} = 0$
$q_{19,1} = 0$	$q_{19,2} = 0$	$q_{19,3} = 0$
$q_{20,1} = 0$	$q_{20,2} = 0$	$q_{20,3} = 0$
$q_{21,1} = 0$	$q_{21,2} = 0$	$q_{21,3} = 0$
$q_{22,1} = 0$	$q_{22,2} = 0$	$q_{22,3} = 0$
$q_{23,1} = 0$	$q_{23,2} = 0$	$q_{23,3} = 0$
$q_{24,1} = 0$	$q_{24,2} = 0$	$q_{24,3} = 0$
$q_{25,1} = 0$	$q_{25,2} = 0$	$q_{25,3} = 0$
$q_{26,1} = 0$	$q_{26,2} = 0$	$q_{26,3} = 0$
$q_{27,1} = 0$	$q_{27,2} = 0$	$q_{27,3} = 0$
$q_{28,1} = 0$	$q_{28,2} = 0$	$q_{28,3} = 0$
$q_{29,1} = 0$	$q_{29,2} = 0$	$q_{29,3} = 0$
$q_{30,1} = 0$	$q_{30,2} = 0$	$q_{30,3} = 0$
$q_{31,1} = 0$	$q_{31,2} = 0$	$q_{31,3} = 0$
$q_{32,1} = 0$	$q_{32,2} = 0$	$q_{32,3} = 0$
$q_{33,1} = 0$	$q_{33,2} = 0$	$q_{33,3} = 0$
$q_{34,1} = 0$	$q_{34,2} = 0$	$q_{34,3} = 0$
$q_{35,1} = 0$	$q_{35,2} = 0$	$q_{35,3} = 0$
$q_{36,1} = 0$	$q_{36,2} = 0$	$q_{36,3} = 0$

$q_{1,4} = 3\lambda_4$
$q_{2,4} = 0$
$q_{3,4} = 0$
$-q_{4,4} = -(\lambda_1+\lambda_3+2\lambda_4+2\lambda_7+\lambda_9+\mu_4)$
$q_{5,4} = 0$
$q_{6,4} = 0$
$q_{7,4} = 0$
$q_{8,4} = 0$
$q_{9,4} = \mu_1$
$q_{10,4} = 0$
$q_{11,4} = 0$
$q_{12,4} = \mu_3$
$q_{13,4} = \mu_4$
$q_{14,4} = \mu_7$
$q_{15,4} = \mu_9$
$q_{16,4} = 0$
$q_{17,4} = 0$
$q_{18,4} = 0$
$q_{19,4} = 0$
$q_{20,4} = 0$
$q_{21,4} = 0$
$q_{22,4} = 0$
$q_{23,4} = 0$
$q_{24,4} = 0$
$q_{25,4} = 0$
$q_{26,4} = 0$
$q_{27,4} = 0$
$q_{28,4} = 0$
$q_{29,4} = 0$
$q_{30,4} = 0$
$q_{31,4} = 0$
$q_{32,4} = 0$
$q_{33,4} = 0$
$q_{34,4} = 0$
$q_{35,4} = 0$
$q_{36,4} = 0$

$q_{1,5} = 2\lambda_7$
$q_{2,5} = 0$
$q_{3,5} = 0$
$q_{4,5} = 0$
$-q_{5,5} = -(\lambda_1+3\lambda_4+\lambda_3+2\lambda_7+\lambda_9+\mu_7)$
$q_{6,5} = 0$
$q_{7,5} = 0$
$q_{8,5} = 0$
$q_{9,5} = 0$
$q_{10,5} = \mu_1$
$q_{11,5} = 0$
$q_{12,5} = 0$
$q_{13,5} = 0$
$q_{14,5} = \mu_4$
$q_{15,5} = 0$
$q_{16,5} = \mu_3$
$q_{17,5} = \mu_7$
$q_{18,5} = \mu_9$
$q_{19,5} = 0$
$q_{20,5} = 0$
$q_{21,5} = 0$
$q_{22,5} = 0$
$q_{23,5} = 0$
$q_{24,5} = 0$
$q_{25,5} = 0$
$q_{26,5} = 0$
$q_{27,5} = 0$
$q_{28,5} = 0$
$q_{29,5} = 0$
$q_{30,5} = 0$
$q_{31,5} = 0$
$q_{32,5} = 0$
$q_{33,5} = 0$
$q_{34,5} = 0$
$q_{35,5} = 0$
$q_{36,5} = 0$

$q_{1,6} = \lambda_9$
$q_{2,6} = 0$
$q_{3,6} = 0$
$q_{4,6} = 0$
$q_{5,6} = 0$
$-q_{6,6} = -\mu_9$
$q_{7,6} = 0$
$q_{8,6} = 0$
$q_{9,6} = 0$
$q_{10,6} = 0$
$q_{11,6} = \mu_1$
$q_{12,6} = 0$
$q_{13,6} = 0$
$q_{14,6} = 0$
$q_{15,6} = \mu_4$
$q_{16,6} = 0$
$q_{17,6} = 0$
$q_{18,6} = \mu_7$
$q_{19,6} = 0$
$q_{20,6} = 0$
$q_{21,6} = 0$
$q_{22,6} = 0$
$q_{23,6} = 0$
$q_{24,6} = 0$
$q_{25,6} = 0$
$q_{26,6} = 0$
$q_{27,6} = 0$
$q_{28,6} = 0$
$q_{29,6} = 0$
$q_{30,6} = 0$
$q_{31,6} = 0$
$q_{32,6} = 0$
$q_{33,6} = 0$
$q_{34,6} = 0$
$q_{35,6} = 0$
$q_{36,6} = 0$

$q_{1,7} = 0$ $q_{1,8} = 0$ $q_{1,9} = 0$
$q_{2,7} = \lambda_2$ $q_{2,8} = \lambda_3$ $q_{2,9} = 3\lambda_4$
$q_{3,7} = 0$ $q_{3,8} = 0$ $q_{3,9} = 0$
$q_{4,7} = 0$ $q_{4,8} = 0$ $q_{4,9} = \lambda_1$
$q_{5,7} = 0$ $q_{5,8} = 0$ $q_{5,9} = 0$
$q_{6,7} = 0$ $q_{6,8} = 0$ $q_{6,9} = 0$
$-q_{7,7} = -\mu_2$ $q_{7,8} = 0$ $q_{7,9} = 0$
$q_{8,7} = 0$ $-q_{8,8} = -(\mu_1+\mu_3)$ $q_{8,9} = 0$
$q_{9,7} = 0$ $q_{9,8} = 0$ $-q_{9,9} = -(\lambda_2+\lambda_3+2\lambda_4+2\lambda_7+\lambda_9+\mu_1+\mu_4)$
$q_{10,7} = 0$ $q_{10,8} = 0$ $q_{10,9} = 0$
$q_{11,7} = 0$ $q_{11,8} = 0$ $q_{11,9} = 0$
$q_{12,7} = 0$ $q_{12,8} = 0$ $q_{12,9} = 0$
$q_{13,7} = 0$ $q_{13,8} = 0$ $q_{13,9} = 0$
$q_{14,7} = 0$ $q_{14,8} = 0$ $q_{14,9} = 0$
$q_{15,7} = 0$ $q_{15,8} = 0$ $q_{15,9} = 0$
$q_{16,7} = 0$ $q_{16,8} = 0$ $q_{16,9} = 0$
$q_{17,7} = 0$ $q_{17,8} = 0$ $q_{17,9} = 0$
$q_{18,7} = 0$ $q_{18,8} = 0$ $q_{18,9} = 0$
$q_{19,7} = \mu_4$ $q_{19,8} = 0$ $q_{19,9} = \mu_2$
$q_{20,7} = 0$ $q_{20,8} = \mu_4$ $q_{20,9} = \mu_3$
$q_{21,7} = 0$ $q_{21,8} = 0$ $q_{21,9} = \mu_4$
$q_{22,7} = 0$ $q_{22,8} = 0$ $q_{22,9} = \mu_7$
$q_{23,7} = 0$ $q_{23,8} = 0$ $q_{23,9} = \mu_9$
$q_{24,7} = \mu_7$ $q_{24,8} = 0$ $q_{24,9} = 0$
$q_{25,7} = 0$ $q_{25,8} = \mu_7$ $q_{25,9} = 0$
$q_{26,7} = 0$ $q_{26,8} = 0$ $q_{26,9} = 0$
$q_{27,7} = 0$ $q_{27,8} = 0$ $q_{27,9} = 0$
$q_{28,7} = 0$ $q_{28,8} = 0$ $q_{28,9} = 0$
$q_{29,7} = 0$ $q_{29,8} = 0$ $q_{29,9} = 0$
$q_{30,7} = 0$ $q_{30,8} = 0$ $q_{30,9} = 0$
$q_{31,7} = 0$ $q_{31,8} = 0$ $q_{31,9} = 0$
$q_{32,7} = 0$ $q_{32,8} = 0$ $q_{32,9} = 0$
$q_{33,7} = 0$ $q_{33,8} = 0$ $q_{33,9} = 0$
$q_{34,7} = 0$ $q_{34,8} = 0$ $q_{34,9} = 0$
$q_{35,7} = 0$ $q_{35,8} = 0$ $q_{35,9} = 0$
$q_{36,7} = 0$ $q_{36,8} = 0$ $q_{36,9} = 0$

$q_{1,10}$	=	0	$q_{1,11}$	=	0	$q_{1,12}$	= 0
$q_{2,10}$	=	$2\lambda_7$	$q_{2,11}$	=	λ_9	$q_{2,12}$	= 0
$q_{3,10}$	=	0	$q_{3,11}$	=	0	$q_{3,12}$	= 0
$q_{4,10}$	=	0	$q_{4,11}$	=	0	$q_{4,12}$	= λ_3
$q_{5,10}$	=	λ_1	$q_{5,11}$	=	0	$q_{5,12}$	= 0
$q_{6,10}$	=	0	$q_{6,11}$	=	0	$q_{6,12}$	= 0
$q_{7,10}$	=	0	$q_{7,11}$	=	0	$q_{7,12}$	= 0
$q_{8,10}$	=	0	$q_{8,11}$	=	0	$q_{8,12}$	= 0
$q_{9,10}$	=	0	$q_{9,11}$	=	0	$q_{9,12}$	= 0
$-q_{10,10}$	=	$-(3\lambda_4+\lambda_2+\lambda_3+\lambda_8+\lambda_9+\mu_1+\mu_7)$	$q_{10,11}$	=	0	$q_{10,12}$	= 0
$q_{11,10}$	=	0	$-q_{11,11}$	=	$-(\mu_1+\mu_9)$	$q_{11,12}$	= 0
$q_{12,10}$	=	0	$q_{12,11}$	=	0	$-q_{12,12}$	= $-(\mu_3+\mu_4)$
$q_{13,10}$	=	0	$q_{13,11}$	=	0	$q_{13,12}$	= 0
$q_{14,10}$	=	0	$q_{14,11}$	=	0	$q_{14,12}$	= 0
$q_{15,10}$	=	0	$q_{15,11}$	=	0	$q_{15,12}$	= 0
$q_{16,10}$	=	0	$q_{16,11}$	=	0	$q_{16,12}$	= 0
$q_{17,10}$	=	0	$q_{17,11}$	=	0	$q_{17,12}$	= 0
$q_{18,10}$	=	0	$q_{18,11}$	=	0	$q_{18,12}$	= 0
$q_{19,10}$	=	0	$q_{19,11}$	=	0	$q_{19,12}$	= 0
$q_{20,10}$	=	0	$q_{20,11}$	=	0	$q_{20,12}$	= μ_1
$q_{21,10}$	=	0	$q_{21,11}$	=	0	$q_{21,12}$	= 0
$q_{22,10}$	=	μ_4	$q_{22,11}$	=	0	$q_{22,12}$	= 0
$q_{23,10}$	=	0	$q_{23,11}$	=	μ_4	$q_{23,12}$	= 0
$q_{24,10}$	=	μ_2	$q_{24,11}$	=	0	$q_{24,12}$	= 0
$q_{25,10}$	=	μ_3	$q_{25,11}$	=	0	$q_{25,12}$	= 0
$q_{26,10}$	=	μ_7	$q_{26,11}$	=	0	$q_{26,12}$	= 0
$q_{27,10}$	=	μ_9	$q_{27,11}$	=	μ_7	$q_{27,12}$	= 0
$q_{28,10}$	=	0	$q_{28,11}$	=	0	$q_{28,12}$	= μ_7
$q_{29,10}$	=	0	$q_{29,11}$	=	0	$q_{29,12}$	= 0
$q_{30,10}$	=	0	$q_{30,11}$	=	0	$q_{30,12}$	= 0
$q_{31,10}$	=	0	$q_{31,11}$	=	0	$q_{31,12}$	= 0
$q_{32,10}$	=	0	$q_{32,11}$	=	0	$q_{32,12}$	= 0
$q_{33,10}$	=	0	$q_{33,11}$	=	0	$q_{33,12}$	= 0
$q_{34,10}$	=	0	$q_{34,11}$	=	0	$q_{34,12}$	= 0
$q_{35,10}$	=	0	$q_{35,11}$	=	0	$q_{35,12}$	= 0
$q_{36,10}$	=	0	$q_{36,11}$	=	0	$q_{36,12}$	= 0

$q_{1,13} = 0$	$q_{1,14} = 0$	$q_{1,15} = 0$
$q_{2,13} = 0$	$q_{2,14} = 0$	$q_{2,15} = 0$
$q_{3,13} = 0$	$q_{3,14} = 0$	$q_{3,15} = 0$
$q_{4,13} = 2\lambda_4$	$q_{4,14} = 2\lambda_7$	$q_{4,15} = \lambda_9$
$q_{5,13} = 0$	$q_{5,14} = 3\lambda_4$	$q_{5,15} = 0$
$q_{6,13} = 0$	$q_{6,14} = 0$	$q_{6,15} = 0$
$q_{7,13} = 0$	$q_{7,14} = 0$	$q_{7,15} = 0$
$q_{8,13} = 0$	$q_{8,14} = 0$	$q_{8,15} = 0$
$q_{9,13} = 0$	$q_{9,14} = 0$	$q_{9,15} = 0$
$q_{10,13} = 0$	$q_{10,14} = 0$	$q_{10,15} = 0$
$q_{11,13} = 0$	$q_{11,14} = 0$	$q_{11,15} = 0$
$q_{12,13} = 0$	$q_{12,14} = 0$	$q_{12,15} = 0$
$-q_{13,13} = -\mu_4$	$q_{13,14} = 0$	$q_{13,15} = 0$
$q_{14,13} = 0$	$-q_{14,14} = -(\lambda_1+\lambda_3+2\lambda_4+\lambda_7+\lambda_9+\mu_4+\mu_7)$	$q_{14,15} = 0$
$q_{15,13} = 0$	$q_{15,14} = 0$	$-q_{15,15} = -(\mu_4+\mu_9)$
$q_{16,13} = 0$	$q_{16,14} = 0$	$q_{16,15} = 0$
$q_{17,13} = 0$	$q_{17,14} = 0$	$q_{17,15} = 0$
$q_{18,13} = 0$	$q_{18,14} = 0$	$q_{18,15} = 0$
$q_{19,13} = 0$	$q_{19,14} = 0$	$q_{19,15} = 0$
$q_{20,13} = 0$	$q_{20,14} = 0$	$q_{20,15} = 0$
$q_{21,13} = \mu_1$	$q_{21,14} = 0$	$q_{21,15} = 0$
$q_{22,13} = 0$	$q_{22,14} = \mu_1$	$q_{22,15} = 0$
$q_{23,13} = 0$	$q_{23,14} = 0$	$q_{23,15} = \mu_1$
$q_{24,13} = 0$	$q_{24,14} = 0$	$q_{24,15} = 0$
$q_{25,13} = 0$	$q_{25,14} = 0$	$q_{25,15} = 0$
$q_{26,13} = 0$	$q_{26,14} = 0$	$q_{26,15} = 0$
$q_{27,13} = 0$	$q_{27,14} = 0$	$q_{27,15} = 0$
$q_{28,13} = 0$	$q_{28,14} = \mu_3$	$q_{28,15} = 0$
$q_{29,13} = \mu_7$	$q_{29,14} = \mu_4$	$q_{29,15} = 0$
$q_{30,13} = 0$	$q_{30,14} = \mu_7$	$q_{30,15} = 0$
$q_{31,13} = 0$	$q_{31,14} = \mu_9$	$q_{31,15} = \mu_7$
$q_{32,13} = 0$	$q_{32,14} = 0$	$q_{32,15} = 0$
$q_{33,13} = 0$	$q_{33,14} = 0$	$q_{33,15} = 0$
$q_{34,13} = 0$	$q_{34,14} = 0$	$q_{34,15} = 0$
$q_{3513} = 0$	$q_{35,14} = 0$	$q_{35,15} = 0$
$q_{36,13} = 0$	$q_{36,14} = 0$	$q_{36,15} = 0$

$q_{1,16} = 0$	$q_{1,17} = 0$	$q_{1,18} = 0$	$q_{1,19} = 0$
$q_{2,16} = 0$	$q_{2,17} = 0$	$q_{2,18} = 0$	$q_{2,19} = 0$
$q_{3,16} = 0$	$q_{3,17} = 0$	$q_{3,18} = 0$	$q_{3,19} = 0$
$q_{4,16} = 0$	$q_{4,17} = 0$	$q_{4,18} = 0$	$q_{4,19} = 0$
$q_{5,16} = \lambda_3$	$q_{517} = \lambda_7$	$q_{5,18} = \lambda_9$	$q_{5,19} = 0$
$q_{6,16} = 0$	$q_{6,17} = 0$	$q_{6,18} = 0$	$q_{6,19} = 0$
$q_{7,16} = 0$	$q_{7,17} = 0$	$q_{7,18} = 0$	$q_{7,19} = 0$
$q_{8,16} = 0$	$q_{8,17} = 0$	$q_{8,18} = 0$	$q_{8,19} = 0$
$q_{9,16} = 0$	$q_{9,17} = 0$	$q_{9,18} = 0$	$q_{9,19} = \lambda_2$
$q_{10,16} = 0$	$q_{10,17} = 0$	$q_{10,18} = 0$	$q_{10,19} = 0$
$q_{11,16} = 0$	$q_{11,17} = 0$	$q_{11,18} = 0$	$q_{11,19} = 0$
$q_{12,16} = 0$	$q_{12,17} = 0$	$q_{12,18} = 0$	$q_{12,19} = 0$
$q_{13,16} = 0$	$q_{13,17} = 0$	$q_{13,18} = 0$	$q_{13,19} = 0$
$q_{14,16} = 0$	$q_{14,17} = 0$	$q_{14,18} = 0$	$q_{14,19} = 0$
$q_{15,16} = 0$	$q_{15,17} = 0$	$q_{15,18} = 0$	$q_{15,19} = 0$
$q_{16,16} = -(\mu_3+\mu_7)$	$q_{16,17} = 0$	$q_{16,18} = 0$	$q_{16,19} = 0$
$q_{17,16} = 0$	$-q_{17,17} = -\mu_7$	$q_{17,18} = 0$	$q_{17,19} = 0$
$q_{18,16} = 0$	$q_{18,17} = 0$	$-q_{18,18} = -(\mu_7+\mu_9)$	$q_{18,19} = 0$
$q_{19,16} = 0$	$q_{19,17} = 0$	$q_{19,18} = 0$	$-q_{19,19} = -(\mu_2+\mu_4)$
$q_{20,16} = 0$	$q_{20,17} = 0$	$q_{20,18} = 0$	$q_{20,19} = 0$
$q_{21,16} = 0$	$q_{21,17} = 0$	$q_{21,18} = 0$	$q_{21,19} = 0$
$q_{22,16} = 0$	$q_{22,17} = 0$	$q_{22,18} = 0$	$q_{22,19} = 0$
$q_{23,16} = 0$	$q_{23,17} = 0$	$q_{23,18} = 0$	$q_{23,19} = 0$
$q_{2416} = 0$	$q_{24,17} = 0$	$q_{24,18} = 0$	$q_{24,19} = 0$
$q_{25,16} = \mu_1$	$q_{25,17} = 0$	$q_{25,18} = 0$	$q_{25,19} = 0$
$q_{2616} = 0$	$q_{26,17} = \mu_1$	$q_{26,18} = 0$	$q_{26,19} = 0$
$q_{27,16} = 0$	$q_{27,17} = 0$	$q_{27,18} = \mu_1$	$q_{27,19} = 0$
$q_{28,16} = \mu_4$	$q_{28,17} = 0$	$q_{28,18} = 0$	$q_{28,19} = 0$
$q_{29,16} = 0$	$q_{29,17} = \mu_4$	$q_{29,18} = 0$	$q_{29,19} = 0$
$q_{30,16} = 0$	$q_{30,17} = 0$	$q_{30,18} = \mu_4$	$q_{30,19} = 0$
$q_{31,16} = 0$	$q_{31,17} = 0$	$q_{31,18} = 0$	$q_{31,19} = 0$
$q_{32,16} = 0$	$q_{32,17} = 0$	$q_{32,18} = 0$	$q_{32,19} = \mu_7$
$q_{33,16} = 0$	$q_{33,17} = 0$	$q_{33,18} = 0$	$q_{33,19} = 0$
$q_{34,16} = 0$	$q_{34,17} = 0$	$q_{34,18} = 0$	$q_{34,19} = 0$
$q_{35,16} = 0$	$q_{35,17} = 0$	$q_{35,18} = 0$	$q_{35,19} = 0$
$q_{36,16} = 0$	$q_{36,17} = 0$	$q_{36,18} = 0$	$q_{36,19} = 0$

$q_{1,20} = 0$	$q_{1,21} = 0$	$q_{1,22} = 0$
$q_{2,20} = 0$	$q_{2,21} = 0$	$q_{2,22} = 0$
$q_{3,20} = 0$	$q_{3,21} = 0$	$q_{3,22} = 0$
$q_{4,20} = 0$	$q_{4,21} = 0$	$q_{4,22} = 0$
$q_{5,20} = 0$	$q_{5,21} = 0$	$q_{5,22} = 0$
$q_{6,20} = 0$	$q_{6,21} = 0$	$q_{6,22} = 0$
$q_{7,20} = 0$	$q_{7,21} = 0$	$q_{7,22} = 0$
$q_{8,20} = 0$	$q_{8,21} = 0$	$q_{8,22} = 0$
$q_{9,20} = \lambda_3$	$q_{9,21} = 2\lambda_4$	$q_{9,22} = 2\lambda_7$
$q_{10,20} = 0$	$q_{10,21} = 0$	$q_{10,22} = 3\lambda_4$
$q_{11,20} = 0$	$q_{11,21} = 0$	$q_{11,22} = 0$
$q_{12,20} = 0$	$q_{12,21} = 0$	$q_{12,22} = 0$
$q_{13,20} = 0$	$q_{13,21} = 0$	$q_{13,22} = 0$
$q_{14,20} = 0$	$q_{14,21} = 0$	$q_{14,22} = \lambda_1$
$q_{15,20} = 0$	$q_{15,21} = 0$	$q_{15,22} = 0$
$q_{16,20} = 0$	$q_{16,21} = 0$	$q_{16,22} = 0$
$q_{17,20} = 0$	$q_{17,21} = 0$	$q_{17,22} = 0$
$q_{18,20} = 0$	$q_{18,21} = 0$	$q_{18,22} = 0$
$q_{19,20} = 0$	$q_{19,21} = 0$	$q_{19,22} = 0$
$-q_{20,20} = -(\mu_1+\mu_3+\mu_4)$	$q_{20,21} = 0$	$q_{20,22} = 0$
$q_{21,20} = 0$	$q_{21,21} = -(\mu_1+\mu_4)$	$q_{21,22} = 0$
$q_{22,20} = 0$	$q_{22,21} = 0$	$-q_{22,22} = -(\lambda_2+\lambda_3+\lambda_5+\lambda_8+\lambda_9+\mu_1+\mu_4+\mu_7)$
$q_{23,20} = 0$	$q_{23,21} = 0$	$q_{23,22} = 0$
$q_{24,20} = 0$	$q_{24,21} = 0$	$q_{24,22} = 0$
$q_{25,20} = 0$	$q_{25,21} = 0$	$q_{25,22} = 0$
$q_{26,20} = 0$	$q_{26,21} = 0$	$q_{26,22} = 0$
$q_{27,20} = 0$	$q_{27,21} = 0$	$q_{27,22} = 0$
$q_{28,20} = 0$	$q_{28,21} = 0$	$q_{28,22} = 0$
$q_{29,20} = 0$	$q_{29,21} = 0$	$q_{29,22} = 0$
$q_{30,20} = 0$	$q_{30,21} = 0$	$q_{30,22} = 0$
$q_{31,20} = 0$	$q_{31,21} = 0$	$q_{31,22} = 0$
$q_{32,20} = 0$	$q_{32,21} = 0$	$q_{32,22} = \mu_2$
$q_{33,20} = \mu_7$	$q_{33,21} = 0$	$q_{33,22} = \mu_3$
$q_{34,20} = 0$	$q_{34,21} = \mu_7$	$q_{34,22} = \mu_4$
$q_{35,20} = 0$	$q_{35,21} = 0$	$q_{35,22} = \mu_7$
$q_{36,20} = 0$	$q_{36,21} = 0$	$q_{36,22} = \mu_9$

$q_{1,23} = 0$	$q_{1,24} = 0$	$q_{1,25} = 0$	$q_{1,26} = 0$
$q_{2,23} = 0$	$q_{2,24} = 0$	$q_{2,25} = 0$	$q_{2,26} = 0$
$q_{3,23} = 0$	$q_{3,24} = 0$	$q_{3,25} = 0$	$q_{3,26} = 0$
$q_{4,23} = 0$	$q_{4,24} = 0$	$q_{4,25} = 0$	$q_{4,26} = 0$
$q_{5,23} = 0$	$q_{5,24} = 0$	$q_{5,25} = 0$	$q_{5,26} = 0$
$q_{6,23} = 0$	$q_{6,24} = 0$	$q_{6,25} = 0$	$q_{6,26} = 0$
$q_{7,23} = 0$	$q_{7,24} = 0$	$q_{7,25} = 0$	$q_{7,26} = 0$
$q_{8,23} = 0$	$q_{8,24} = 0$	$q_{8,25} = 0$	$q_{8,26} = 0$
$q_{9,23} = \lambda_9$	$q_{9,24} = 0$	$q_{9,25} = 0$	$q_{9,26} = 0$
$q_{10,23} = 0$	$q_{10,24} = \lambda_2$	$q_{10,25} = \lambda_3$	$q_{10,26} = \lambda_8$
$q_{11,23} = 0$	$q_{11,24} = 0$	$q_{11,25} = 0$	$q_{11,26} = 0$
$q_{12,23} = 0$	$q_{12,24} = 0$	$q_{12,25} = 0$	$q_{12,26} = 0$
$q_{13,23} = 0$	$q_{13,24} = 0$	$q_{13,25} = 0$	$q_{13,26} = 0$
$q_{14,23} = 0$	$q_{14,24} = 0$	$q_{14,25} = 0$	$q_{14,26} = 0$
$q_{15,23} = 0$	$q_{15,24} = 0$	$q_{15,25} = 0$	$q_{15,26} = 0$
$q_{16,23} = 0$	$q_{16,24} = 0$	$q_{16,25} = 0$	$q_{16,26} = 0$
$q_{17,23} = 0$	$q_{17,24} = 0$	$q_{17,25} = 0$	$q_{17,26} = 0$
$q_{18,23} = 0$	$q_{18,24} = 0$	$q_{18,25} = 0$	$q_{18,26} = 0$
$q_{19,23} = 0$	$q_{19,24} = 0$	$q_{19,25} = 0$	$q_{19,26} = 0$
$q_{20,23} = 0$	$q_{20,24} = 0$	$q_{20,25} = 0$	$q_{20,26} = 0$
$q_{21,23} = 0$	$q_{21,24} = 0$	$q_{21,25} = 0$	$q_{21,26} = 0$
$q_{22,23} = 0$	$q_{22,24} = 0$	$q_{22,25} = 0$	$q_{22,26} = 0$
$-q_{23,23} = -(\mu_1+\mu_4+\mu_9)$	$q_{23,24} = 0$	$q_{23,25} = 0$	$q_{23,26} = 0$
$q_{24,23} = 0$	$-q_{24,24} = -(\mu_2+\mu_7)$	$q_{24,25} = 0$	$q_{24,26} = 0$
$q_{25,23} = 0$	$q_{25,24} = 0$	$-q_{25,25} = -(\mu_1+\mu_3+\mu_7)$	$q_{25,26} = 0$
$q_{26,23} = 0$	$q_{26,24} = 0$	$q_{26,25} = 0$	$-q_{26,26} = -(\mu_1+\mu_7)$
$q_{27,23} = 0$	$q_{27,24} = 0$	$q_{27,25} = 0$	$q_{27,26} = 0$
$q_{28,23} = 0$	$q_{28,24} = 0$	$q_{28,25} = 0$	$q_{28,26} = 0$
$q_{29,23} = 0$	$q_{29,24} = 0$	$q_{29,25} = 0$	$q_{29,26} = 0$
$q_{30,23} = 0$	$q_{30,24} = 0$	$q_{30,25} = 0$	$q_{30,26} = 0$
$q_{31,23} = 0$	$q_{31,24} = 0$	$q_{31,25} = 0$	$q_{31,26} = 0$
$q_{32,23} = 0$	$q_{32,24} = 0$	$q_{32,25} = 0$	$q_{32,26} = 0$
$q_{33,23} = 0$	$q_{33,24} = 0$	$q_{33,25} = \mu_4$	$q_{33,26} = 0$
$q_{34,23} = 0$	$q_{34,24} = 0$	$q_{34,25} = 0$	$q_{34,26} = 0$
$q_{35,23} = 0$	$q_{35,24} = 0$	$q_{35,25} = 0$	$q_{35,26} = \mu_4$
$q_{36,23} = \mu_7$	$q_{36,24} = \mu_4$	$q_{36,25} = 0$	$q_{36,26} = 0$

$q_{1,27} = 0$	$q_{1,28} = 0$	$q_{1,29} = 0$	$q_{1,30} = 0$
$q_{2,27} = 0$	$q_{2,28} = 0$	$q_{2,29} = 0$	$q_{2,30} = 0$
$q_{3,27} = 0$	$q_{3,28} = 0$	$q_{3,29} = 0$	$q_{3,30} = 0$
$q_{4,27} = 0$	$q_{4,28} = 0$	$q_{4,29} = 0$	$q_{4,30} = 0$
$q_{5,27} = 0$	$q_{5,28} = 0$	$q_{5,29} = 0$	$q_{5,30} = 0$
$q_{6,27} = 0$	$q_{6,28} = 0$	$q_{6,29} = 0$	$q_{6,30} = 0$
$q_{7,27} = 0$	$q_{7,28} = 0$	$q_{7,29} = 0$	$q_{7,30} = 0$
$q_{8,27} = 0$	$q_{8,28} = 0$	$q_{8,29} = 0$	$q_{8,30} = 0$
$q_{9,27} = 0$	$q_{9,28} = 0$	$q_{9,29} = 0$	$q_{9,30} = 0$
$q_{10,27} = \lambda_9$	$q_{10,28} = 0$	$q_{10,29} = 0$	$q_{10,30} = 0$
$q_{11,27} = 0$	$q_{11,28} = 0$	$q_{11,29} = 0$	$q_{11,30} = 0$
$q_{12,27} = 0$	$q_{12,28} = 0$	$q_{12,29} = 0$	$q_{12,30} = 0$
$q_{13,27} = 0$	$q_{13,28} = 0$	$q_{13,29} = 0$	$q_{13,30} = 0$
$q_{14,27} = 0$	$q_{14,28} = \lambda_3$	$q_{14,29} = 2\lambda_4$	$q_{14,30} = \lambda_7$
$q_{15,27} = 0$	$q_{15,28} = 0$	$q_{15,29} = 0$	$q_{15,30} = 0$
$q_{16,27} = 0$	$q_{16,28} = 0$	$q_{16,29} = 0$	$q_{16,30} = 0$
$q_{17,27} = 0$	$q_{17,28} = 0$	$q_{17,29} = 0$	$q_{17,30} = 0$
$q_{18,27} = 0$	$q_{18,28} = 0$	$q_{18,29} = 0$	$q_{18,30} = 0$
$q_{19,27} = 0$	$q_{19,28} = 0$	$q_{19,29} = 0$	$q_{19,30} = 0$
$q_{20,27} = 0$	$q_{20,28} = 0$	$q_{20,29} = 0$	$q_{20,30} = 0$
$q_{21,27} = 0$	$q_{21,28} = 0$	$q_{21,29} = 0$	$q_{21,30} = 0$
$q_{22,27} = 0$	$q_{22,28} = 0$	$q_{22,29} = 0$	$q_{22,30} = 0$
$q_{23,27} = 0$	$q_{23,28} = 0$	$q_{23,29} = 0$	$q_{23,30} = 0$
$q_{24,27} = 0$	$q_{24,28} = 0$	$q_{24,29} = 0$	$q_{24,30} = 0$
$q_{25,27} = 0$	$q_{25,28} = 0$	$q_{25,29} = 0$	$q_{25,30} = 0$
$q_{26,27} = 0$	$q_{26,28} = 0$	$q_{26,29} = 0$	$q_{26,30} = 0$
$-q_{27,27} = -(\mu_1+\mu_7+\mu_9)$	$q_{27,28} = 0$	$q_{27,29} = 0$	$q_{27,30} = 0$
$q_{28,27} = 0$	$-q_{28,28} = -(\mu_3+\mu_4+\mu_7)$	$q_{28,29} = 0$	$q_{28,30} = 0$
$q_{29,27} = 0$	$q_{29,28} = 0$	$-q_{29,29} = -(\mu_4+\mu_7)$	$q_{29,30} = 0$
$q_{30,27} = 0$	$q_{30,28} = 0$	$q_{30,29} = 0$	$-q_{30,30} = -(\mu_4+\mu_7)$
$q_{31,27} = 0$	$q_{31,28} = 0$	$q_{31,29} = 0$	$q_{31,30} = 0$
$q_{32,27} = 0$	$q_{32,28} = 0$	$q_{32,29} = 0$	$q_{32,30} = 0$
$q_{33,27} = 0$	$q_{33,28} = \mu_1$	$q_{33,29} = 0$	$q_{33,30} = 0$
$q_{34,27} = 0$	$q_{34,28} = 0$	$q_{34,29} = \mu_1$	$q_{34,30} = 0$
$q_{35,27} = 0$	$q_{35,28} = 0$	$q_{35,29} = 0$	$q_{35,30} = \mu_1$
$q_{36,27} = \mu_4$	$q_{36,28} = 0$	$q_{36,29} = 0$	$q_{36,30} = 0$

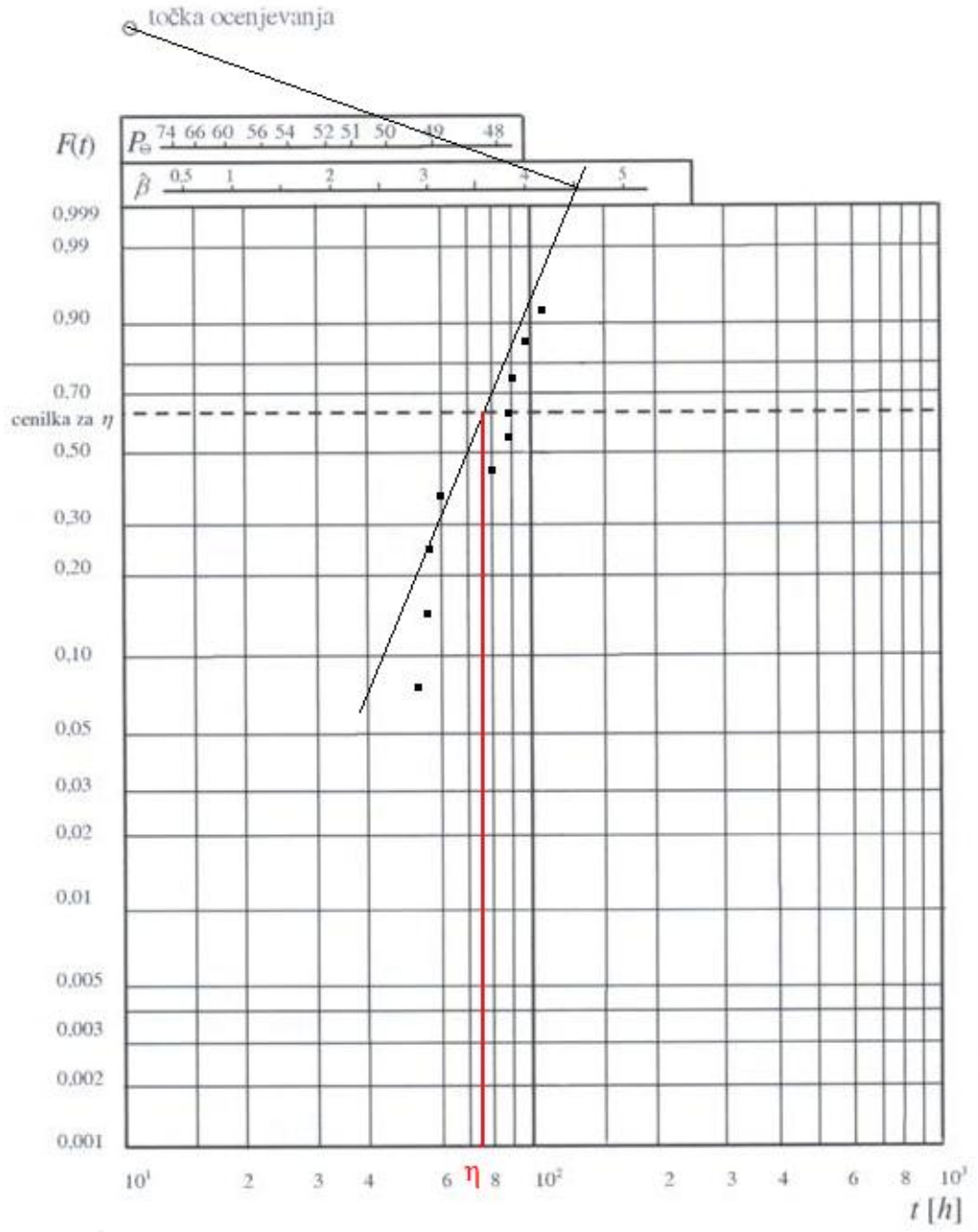
$q_{1,31} = 0$	$q_{1,32} = 0$	$q_{1,33} = 0$
$q_{2,31} = 0$	$q_{2,32} = 0$	$q_{2,33} = 0$
$q_{3,31} = 0$	$q_{3,32} = 0$	$q_{3,33} = 0$
$q_{4,31} = 0$	$q_{4,32} = 0$	$q_{4,33} = 0$
$q_{5,31} = 0$	$q_{5,32} = 0$	$q_{5,33} = 0$
$q_{6,31} = 0$	$q_{6,32} = 0$	$q_{6,33} = 0$
$q_{7,31} = 0$	$q_{7,32} = 0$	$q_{7,33} = 0$
$q_{8,31} = 0$	$q_{8,32} = 0$	$q_{8,33} = 0$
$q_{9,31} = 0$	$q_{9,32} = 0$	$q_{9,33} = 0$
$q_{10,31} = 0$	$q_{10,32} = 0$	$q_{10,33} = 0$
$q_{11,31} = 0$	$q_{11,32} = 0$	$q_{11,33} = 0$
$q_{12,31} = 0$	$q_{12,32} = 0$	$q_{12,33} = 0$
$q_{13,31} = 0$	$q_{13,32} = 0$	$q_{13,33} = 0$
$q_{14,31} = \lambda_9$	$q_{14,32} = 0$	$q_{14,33} = 0$
$q_{15,31} = 0$	$q_{15,32} = 0$	$q_{15,33} = 0$
$q_{16,31} = 0$	$q_{16,32} = 0$	$q_{16,33} = 0$
$q_{17,31} = 0$	$q_{17,32} = 0$	$q_{17,33} = 0$
$q_{18,31} = 0$	$q_{18,32} = 0$	$q_{18,33} = 0$
$q_{19,31} = 0$	$q_{19,32} = 0$	$q_{19,33} = 0$
$q_{20,31} = 0$	$q_{20,32} = 0$	$q_{20,33} = 0$
$q_{21,31} = 0$	$q_{21,32} = 0$	$q_{21,33} = 0$
$q_{22,31} = 0$	$q_{22,32} = 0$	$q_{22,33} = 0$
$q_{23,31} = 0$	$q_{23,32} = 0$	$q_{23,33} = 0$
$q_{24,31} = 0$	$q_{24,32} = 0$	$q_{24,33} = 0$
$q_{25,31} = 0$	$q_{25,32} = 0$	$q_{25,33} = 0$
$q_{26,31} = 0$	$q_{26,32} = 0$	$q_{26,33} = 0$
$q_{27,31} = 0$	$q_{27,32} = 0$	$q_{27,33} = 0$
$q_{28,31} = 0$	$q_{28,32} = 0$	$q_{28,33} = 0$
$q_{29,31} = 0$	$q_{29,32} = 0$	$q_{29,33} = 0$
$q_{30,31} = 0$	$q_{30,32} = 0$	$q_{30,33} = 0$
$-q_{31,31} = -(\mu_4+\mu_7+\mu_9)$	$q_{31,32} = 0$	$q_{31,33} = 0$
$q_{32,31} = 0$	$-q_{32,32} = -(\mu_2+\mu_4+\mu_7)$	$q_{32,33} = 0$
$q_{33,31} = 0$	$q_{33,32} = 0$	$-q_{33,33} = -(\mu_1+\mu_3+\mu_4+\mu_7)$
$q_{34,31} = 0$	$q_{34,32} = 0$	$q_{34,33} = 0$
$q_{35,31} = 0$	$q_{35,32} = 0$	$q_{35,33} = 0$
$q_{36,31} = \mu_1$	$q_{36,32} = 0$	$q_{36,33} = 0$

$q_{1,34} = 0$	$q_{1,35} = 0$	$q_{1,36} = 0$
$q_{2,34} = 0$	$q_{2,35} = 0$	$q_{2,36} = 0$
$q_{3,34} = 0$	$q_{3,35} = 0$	$q_{3,36} = 0$
$q_{4,34} = 0$	$q_{4,35} = 0$	$q_{4,36} = 0$
$q_{5,34} = 0$	$q_{5,35} = 0$	$q_{5,36} = 0$
$q_{6,34} = 0$	$q_{6,35} = 0$	$q_{6,36} = 0$
$q_{7,34} = 0$	$q_{7,35} = 0$	$q_{7,36} = 0$
$q_{8,34} = 0$	$q_{8,35} = 0$	$q_{8,36} = 0$
$q_{9,34} = 0$	$q_{9,35} = 0$	$q_{9,36} = 0$
$q_{10,34} = 0$	$q_{10,35} = 0$	$q_{10,36} = 0$
$q_{11,34} = 0$	$q_{11,35} = 0$	$q_{11,36} = 0$
$q_{12,34} = 0$	$q_{12,35} = 0$	$q_{12,36} = 0$
$q_{13,34} = 0$	$q_{13,35} = 0$	$q_{13,36} = 0$
$q_{14,34} = 0$	$q_{14,35} = 0$	$q_{14,36} = 0$
$q_{15,34} = 0$	$q_{15,35} = 0$	$q_{15,36} = 0$
$q_{16,34} = 0$	$q_{16,35} = 0$	$q_{16,36} = 0$
$q_{17,34} = 0$	$q_{17,35} = 0$	$q_{17,36} = 0$
$q_{18,34} = 0$	$q_{18,35} = 0$	$q_{18,36} = 0$
$q_{19,34} = 0$	$q_{19,35} = 0$	$q_{19,36} = 0$
$q_{20,34} = 0$	$q_{20,35} = 0$	$q_{20,36} = 0$
$q_{21,34} = 0$	$q_{21,35} = 0$	$q_{21,36} = 0$
$q_{22,34} = 0$	$q_{22,35} = 0$	$q_{22,36} = 0$
$q_{23,34} = 0$	$q_{23,35} = 0$	$q_{23,36} = 0$
$q_{24,34} = 0$	$q_{24,35} = 0$	$q_{24,36} = 0$
$q_{25,34} = 0$	$q_{25,35} = 0$	$q_{25,36} = 0$
$q_{26,34} = 0$	$q_{26,35} = 0$	$q_{26,36} = 0$
$q_{27,34} = 0$	$q_{27,35} = 0$	$q_{27,36} = 0$
$q_{28,34} = 0$	$q_{28,35} = 0$	$q_{28,36} = 0$
$q_{29,34} = 0$	$q_{29,35} = 0$	$q_{29,36} = 0$
$q_{30,34} = 0$	$q_{30,35} = 0$	$q_{30,36} = 0$
$q_{31,34} = 0$	$q_{31,35} = 0$	$q_{31,36} = 0$
$q_{32,34} = 0$	$q_{32,35} = 0$	$q_{32,36} = 0$
$q_{33,34} = 0$	$q_{33,35} = 0$	$q_{33,36} = 0$
$-q_{34,34} = -(\mu_1+\mu_4+\mu_7)$	$q_{34,35} = 0$	$q_{34,36} = 0$
$q_{35,34} = 0$	$-q_{35,35} = -(\mu_1+\mu_4+\mu_7)$	$q_{35,36} = 0$
$q_{36,34} = 0$	$q_{36,35} = 0$	$-q_{36,36} = -(\mu_1+\mu_4+\mu_7+\mu_9)$

18.6 DODATEK 4: POJASNILA K DOKTORSKEM DELU (WEIBULLOV VERJETNOSTNI PAPIR)

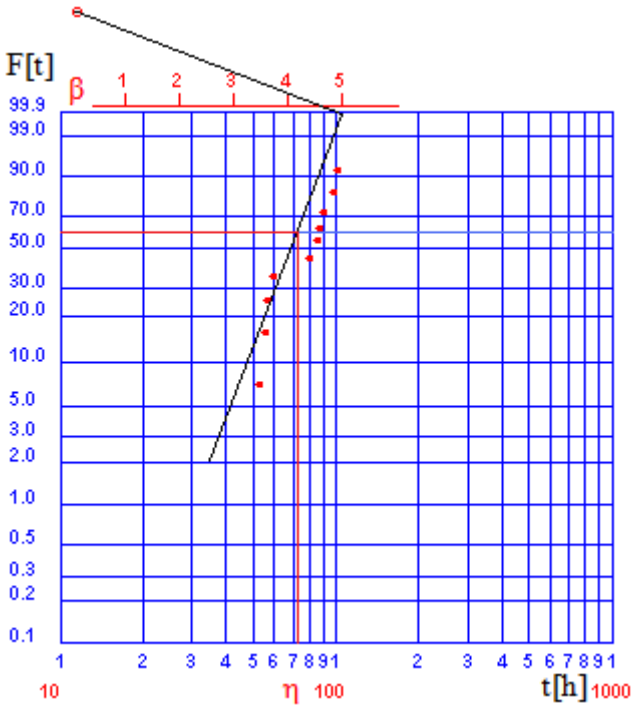
Obravnavali bomo Weibullovo verjetnostno mrežo (slika 17.1) in kratko razpravljali o uporabi grafične metode za določitev ocen parametrov porazdelitve, ki je dobra tudi v primerih, ko imamo na razpolago malo podatkov. Skozi ocenjevalno točko (estimation point) potegnemo pravokotnico na premico, ki jo dobimo, če v mrežo vrišemo eksperimentalne podatke (pare (t_i, $F(t_i)$)). Potem na zgornjih nomogramih (glej sliko) odčitamo oceno parametra oblike β in verjetnost P_Θ. S to zadnjo vrednostjo vstopimo na ordinatno os, jo čez premico projiciramo na abscisno os in tako dobimo oceno povprečne življenjske dobe Θ. Projekcija presečišča F=0,63 (črtkana vodoravna črta na Weibullovem verjetnostnem papirju) prek dobljene premice na abscisno os, da oceno karakteristične življenjske dobe η. Z dobljenimi ocenami parametrov lahko izračunamo tudi oceno standardnega odmika σ:

Za vnešene točke na sliki 17.1, iz verjetnostne mreže odčitamo točkaste ocene za parametre β=4,6 in η=73 kar potrjuje preračune v izvedeni raziskavi (poglavje 10.4). Manjša razlika v rezultatih je prisotna zaradi manj natančne ročne grafične metode.

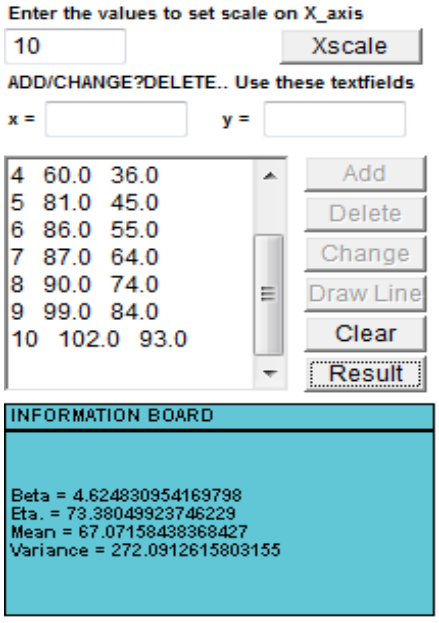


17.1: Weibullova verjetnostna mreža

Parametre, ki smo jih določili in odčitali s pomočjo Weibullovega verjetnostnega papirja lahko preverimo s pomočjo programske opreme Kokoaye za računanje Weibullove porazdelitve (Victoria University of Technology, 2010). Za merjene podatke časov do prve odpovedi v tabeli 10.7, bomo določili točkaste ocene parametrov β in η (slika 17.2). Z vnosom koordinat x(t_i) in y(F_i) določimo točke na Weibullov verjetnostni papir. Skozi točke potegnemo premico, na katero program skozi ocenjevalno točko določi pravokotnico. Za podatke iz tabele 10.7 so s programom dobljene točkaste ocene parametrov β=4,62 in η=73,3.



Slika 17.2: Weibullov verjetnostni papir in preračun



Slika 17.3: Preračun parametrov s pomočjo programa Kokoaye

ŽIVLJENJEPIS

Robert Brumnik roj. 17.06.1971 v Slovenj Gradcu, je l.1991 zaključil srednjo strojno tehnično šolo na Ravnah na Koroškem ter pridobil naziv, strojni tehnik. Študij je nadaljeval na Univerzi v Mariboru, ter zaključil univerzitetni program strojništva, smer konstruiranje in gradnja strojev.
Kot študent, je spoznal razvojno-tehnološki proces avtomobilske industrije, v družbi Prevent d.d. ter Johnson Controls d.d. v Slovenj Gradcu, kjer se je l.1998 tudi redno zaposlil kot razvojni tehnolog. V l.1999, je službovanje nadaljeval v družbi Grammer Automotive d.d., kot tehnolog kakovsti in postal odgovoren za izvedbo presoj procesa, v skladu z evropskimi in ameriškimi standardi avtomobilske industrije. V okviru zagotavljanja kvalitete proizvodov v avtomobilski industriji, je spoznal standardizacijo ter postopke preverjanja skladnosti procesov, glade na standarde ISO9001:2000, QS9000, VDA, TS16694. Pridobil je znanja za planiranje procesov ter opravil izpit, za vodilnega presojevalca sistemov kakovosti, po ISO 9001:2000.
L.2000 se je zaposlil v družbi Metra inženiring d.o.o. v Trzinu na mestu vodje kakovosti ter se vključil v razvojno raziskovalno skupino, ki deluje v okviru družbe. Z aktivnim vključevanjem v izvedbo razvojno-raziskovalnih projektov, na temo identifikacijskih sistemov ter pristopne kontrole, je l. 2004 pridobil naziv samostojni razvijalec. V družbi je bil odgovoren za vzpostavitev in vzdrževanje sistema vodenja kakovosti ter za CE certificiranje proizvodov, po evropskih EC regulativah.
L.2005 se je vpisal na podiplomski študij Management kakovosti, Fakultete za organizacijske vede v Kranju. Aktivno se udeležuje mednarodnih konferenc ter objavlja znanstvene članke, v mednarodnih revijah.
L.2006 je v okviru reinženiringa podjetja, vodil projekt implementacije integralnega informacijskega sistema ter ga skupaj z sodelujočimi, uspešno zaključil l.2007. Njegova raziskovalna dejavnost, se navezuje na mednarodne razvojno raziskovalne projekte, katerih rezultat so mednarodno registrirani patenti. S prispevki se udeležuje mednarodnih znanstvenih konferenc, s področja informatike in informacijske varnosti.

PRILOGA 4

UNIVERZA V MARIBORU

FAKULTETA ZA ORGANIZACIJSKE VEDE KRANJ

IZJAVA DOKTORSKEGA KANDIDATA

Podpisani ROBERT BRUMNIK, vpisna številka 41003265

izjavljam,

da je doktorska disertacija z naslovom »Učinkovitost in zanesljivost biometričnega sistema pri osebni indetifikaciji«

- rezultat lastnega raziskovalnega dela,
- da predložena disertacija v celoti ali v delih ni bila predložena za pridobitev kakršnekoli izobrazbe po študijskem programu druge fakultete ali univerze,
- da so rezultati korektno navedeni in
- da nisem kršil-a avtorskih pravic in intelektualne lastnine drugih.

Kraj, datum: Kranj, 23.05.2011

Podpis doktorskega kandidata:

Robert Brumnik