UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Gregor Žnidaršič

ANALIZA VZROKOV IN NAČINOV ODPOVEDI PROGRAMSKE REŠITVE E-TRANS

DIPLOMSKO DELO
visokošolskega strokovnega študija

Ljubljana, 2008

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Gregor Žnidaršič

ANALIZA VZROKOV IN NAČINOV ODPOVEDI PROGRAMSKE REŠITVE E-TRANS

DIPLOMSKO DELO
visokošolskega strokovnega študija

Mentor: izr. prof. dr. Miha Mraz
Somentor: doc. dr. Iztok Lebar Bajec

Ljubljana, 2008

Zahvala

Rad bi se zahvalil mentorjema izr. prof. dr. Mihu Mrazu in doc. dr. Iztoku Lebarju Bajcu za vse pripombe, strokovne nasvete in izkazano pomoč, ki sta mi jo nudila pri izdelavi diplomskega dela. Zahvalil bi se Andreji za lekturo. Velika zahvala gre staršem za podporo v času študija.

Za vse spodbude in razumevanje se zahvaljujem Teji, ki mi vsa ta leta stoji ob strani.

Kazalo

Seznam kratic in simbolov

UI - uporabniški vmesnik (angl. *user interface*)
BLL - nivo poslovne logike (angl. *business logic layer*)
DAL - podatkovni nivo (angl. *data access layer*)
MBR - zagonski sektor (angl. *master boot record*)
MTBF - povprečni čas med dvema napakama (angl. *mean time between failure*)
MTTR - povprečni čas odprave napake (angl. *mean time to repair*)
FTA - analiza drevesa napak (angl. *fault tree analysis*)
FMEA - analiza načinov odpovedi in njihovih posledic (angl. *failure mode and effect analysis*)
RPN - faktor tveganja (angl. *risk priority number*)

Povzetek

Diplomska naloga obravnava možne načine odpovedi programske rešitve za logistično informacijsko podporo E-Trans, ki jo ponuja škofjeloško podjetje E-Soft d.o.o.. Zanesljivost programskih rešitev je danes zelo pomembna, zato so pri njihovem razvoju potrebni dodatni ukrepi za izboljšanje. Za boljše razumevanje sem najprej opisal programsko rešitev E-Trans, potem pa naštel njene možne načine odpovedi, poiskal vzroke zanje in jih analiziral s pomočjo dveh priznanih metod.

Prva metoda je analiza drevesa napak (FTA). Analiza temelji na risanju diagrama drevesa napak, kjer je neželeno stanje nekega sistema analizirano z uporabo Boolove logike. Neželeno stanje nastopa v korenu drevesa, vsi možni vzroki za to stanje pa so navedeni kot listi v drevesu, povezani z logičnimi operatorji. S to metodo pridobimo odvisnost med vzroki za odpoved sistema.

Druga metoda je analiza načinov odpovedi ter njihovih posledic (FMEA), kjer za vsak način odpovedi izračunamo faktor tveganja in tako pridobimo tabelarni prikaz načinov odpovedi. Tabela, padajoče urejena po faktorju tveganja, je prioritetna lestvica načinov odpovedi in nam pove, kateri način odpovedi povzroča največjo nevarnost za odpoved sistema.

Ključne besede

analiza drevesa napak, diagram drevesa napak, analiza načinov odpovedi in njihovih posledic, razpoložljivost

Summary

This paper deals with possible failure modes in software for logistic E-Trans application, which is provided by company E-Soft d.o.o. in Škofja Loka. Because reliability of software is very important today, its development demands additional steps for improvement. At the beginning of this paper I describe the E-Trans application, then I compile a list of failure modes and try to find out reasons for them and at the end I analyze them with two known methods.

The first method is called fault tree analysis (FTA) and is founded on designing of a fault tree diagram. Undesired condition of a system is analyzed with Bool logic and is founded in the root of the tree. All the possible causes for this condition are stated as leaves on the tree, which are connected to the logic gate symbols. By this method dependence between causes for system failure is acquired.

The second method, which is used in this paper, is failure modes and effects analysis (FMEA) where the risk priority number for every failure mode is calculated. This is how we get a tabulated review of failure modes. A table, sorted decreasingly by risk priority number presents a priority list and shows which failure mode causes the highest danger for system failure.

Key words

fault tree analysis, fault tree diagram, failure modes and effects analysis, availability

1 Uvod

V hitrem poslovnem svetu smo neprestano soočeni s konkurenco, zato se mnoga podjetja znajdejo v situaciji, ko je potrebno povečati učinkovitost in kvaliteto ter zmanjšati stroške, hkrati pa zagotoviti čim večjo odzivnost na zahteve kupcev. Razmišljanja vodilnih se običajno vrtijo predvsem okrog povečanja učinkovitosti v proizvodnji, medtem pa logistika mnogokrat ostaja zanemarjena.

Obvladovanje transportne logistike postaja za podjetja vse večjega pomena. Točnost dobave reprodukcijskega materiala, obvladovanje odpreme, zmanjševanje stroškov transportov in nadzor točnosti dobave izdelkov kupcem postajajo vse pomembnejši elementi. S povečevanjem obsega poslovanja podjetje sčasoma naleti na problem obvladljivosti. Časi, ko so se logistični procesi obvladovali s papirjem in svinčnikom, so se iztekli. Na področju logistike so procesi informacijsko vedno bolj podprti. Eno od ustreznih rešitev na tem področju ponuja tudi podjetje, v katerem sem zaposlen. E-Soft d.o.o. zagotavlja informacijsko podporo za upravljanje s transporti, imenovano E-Trans. Programska rešitev E-Trans je namenjena podjetjem, ki nimajo urejene informatike na področju transportne logistike, imajo sorazmerno veliko število transportnih storitev dnevno in želijo izboljšati njihovo preglednost.

Ker so zahteve na trgu vedno večje, programska oprema pa vsak dan naprednejša, se v podjetju E-Soft d.o.o. pripravljamo na novo verzijo aplikacije E-Trans. Vsaka aplikacija zahteva zanesljivo in varno delovanje programa, saj lahko njen nekajurni izpad pomeni določeno izgubo. Ob načrtovanju nove verzije je potrebno podrobno poznati obstoječo rešitev, njeno delovanje in zanesljivost. Ker se največ naučimo iz napak, smo se odločili, da poiščemo vse možne odpovedi stare verzije aplikacije E-Trans, jih zberemo in upoštevamo pri izdelavi nove verzije. Odpravljanje napak in okvar, ki so že nastale (razen v izjemnih primerih), danes ni več primarna dejavnost vzdrževanja. Ta se je preusmerila k razmišljanju in dejanjem, kot so kdaj, kje in kako preprečiti sam nastop napake in odpovedi. Ob tem se nam poraja vprašanje, kako varna in zanesljiva je trenutna verzija rešitve E-Trans, kakšne so možne odpovedi, kaj gre lahko narobe in kakšne so posledice. Vse te informacije so zelo pomembne pri svetovanju stranki o nakupu primerne strojne opreme, ki bo zadostovala za nemoteno delovanje aplikacije in preprečila neželeno izgubo podatkov. Ob vsem tem je pomembno, da

so stranke opozorjene na možne odpovedi, pripravljene na njihove posledice in na njihovo čimprejšnjo odpravo.

Metod in analiz za določanje sistemske zanesljivosti je več. Za njen izračun potrebujemo podroben spisek vseh možnih odpovedi in njihovih verjetnosti. V tem diplomskem delu se bom osredotočil predvsem na možne načine odpovedi. Če jih poznamo, jih lažje odpravimo, zmanjšamo njihovo verjetnost ali pa se pripravimo na odpravo njihovih posledic. Primerni analizi za iskanje in računanje odpovedi sta analiza načinov odpovedi in njihovih posledic ter analiza drevesa napak. Pri prvi analizi iščemo prioritetni spisek načinov odpovedi, da te lažje odpravimo ali omejimo. Pri drugi analizi nas predvsem zanima, kako se različne odpovedi med seboj povezujejo in če so med seboj odvisne.

V uvodnem poglavju sem opisal uporabnost aplikacije E-Trans in prikazal, zakaj je pomembna zanesljivost programskih paketov. Opisal sem razloge, zaradi katerih smo se odločili za izdelavo analize načinov odpovedi. V drugem poglavju sem podrobneje opisal delovanje programske rešitve E-Trans, njeno arhitekturo, orodja, s katerimi je bila napisana, in navedel primer strojne opreme, na kateri je nameščena. Natančneje sem opisal možne izpade in vzroke za njihov nastanek. V tretjem poglavju sem opisal, kaj predstavlja analiza drevesa napak, kaj je diagram drevesa napak, kakšen je postopek za izdelavo analize in kakšne so najpogostejše napake pri izdelavi le-te. V nadaljevanju sem opravil analizo na aplikaciji E-Trans. Četrto poglavje sem namenil opisu analize načinov odpovedi in njihovih posledic, prikazal, kdaj se analiza uporablja, kakšne tipe poznamo in kakšen je postopek njene izdelave. Za tem sem metodo uporabil za analizo programske rešitve E-Trans. V petem poglavju sem predstavil težave, s katerimi sem se spoprijel med izdelavo diplomske naloge in podal zaključke ter ugotovitve.

2 Logistika in E-Trans

2.1 Logistika

Izraz logistika označuje fizični tok materiala in proizvodov ter informacij od dobavitelja surovin prek proizvajalca in morebiti trgovca do končnega potrošnika gotovih izdelkov [1]. Izraz transport se večinoma uporablja za opis aktivnosti prenosa oseb in blaga, torej brez prenosa informacije.

2.2 Osnovne funkcije programske rešitve E-Trans

Programska rešitev E-Trans je sestavljena iz šestih modulov. Skupaj tvorijo rešitev za podjetja, ki sama skrbijo za transportno logistiko. Namenjena je tako podjetjem, ki potrebujejo nekaj sto transportov dnevno, kot tudi podjetjem z nekaj transporti dnevno.

Funkcionalnosti transportnih procesov v sistemu E-Trans omogočajo planiranje, organizacijo in spremljanje transportov v okviru poslovanja podjetja. S pomočjo transportnih funkcionalnosti je mogoče kreirati dobave (od dobavitelja do prevzemnega obrata), odpreme (od dobavnega obrata do kupca), obračuna transportnih stroškov – specifikacije ter statistične obdelave in poročila.

Proces organiziranja transporta v E-Transu lahko po vrsti razdelimo na:

- izdelavo dobavnice,
- naročilo transporta,
- izbiro prevoznika in cene,
- dejanski transport,
- izdelavo specifikacije računa s strani prevoznika.

Dobavnica je elektronski dokument, ki jo naredi prodajni referent. Vsebuje vse podatke, ki so potrebni, da se proizvodi in storitve dobavijo naročniku v obliki, vsebini in času, kot je bilo dogovorjeno z nakupno pogodbo (naročilnico). Dobavnica vsebuje vrsto in količino naročenega blaga, podatke o kupcu in prejemniku blaga, kraju in času nakladanja, kraju in

času razkladanja ter ostale administrativne podatke (enota v podjetju, referent, namen prevoza …).

Naročilo transporta v podjetjih se organizira v službi za transportno logistiko. Z nastankom dobavnice v prodajni službi je nastala potreba po transportni storitvi. Naročeno blago je potrebno dostaviti kupcu. Tako nastane elektronski dokument, imenovan transportni nalog. Sestavljen je iz dobavnice (lahko jih je tudi več), kjer je določen vrstni red nakladanja. Glede na znane podatke se določi vrsto potrebnega transportnega sredstva.

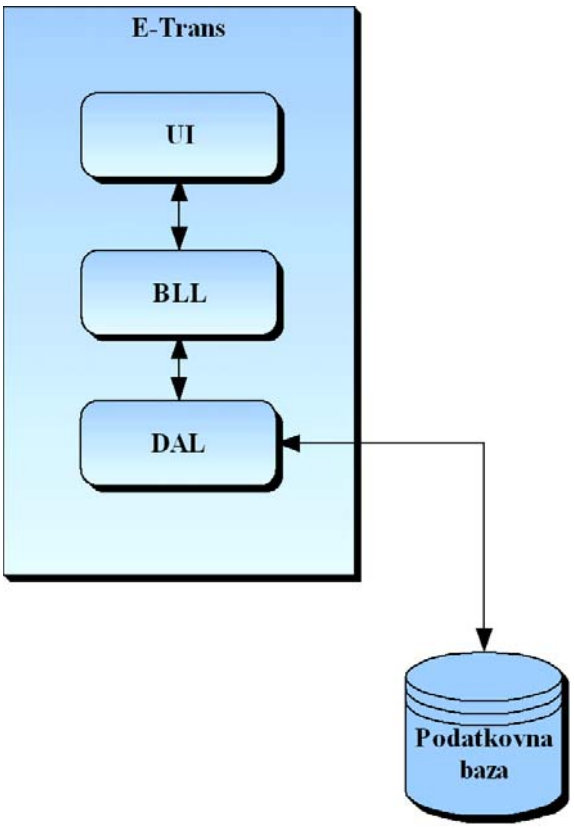
Izbira prevoznika in cene je odvisna od prej določenih pogodb med prevozniki in njihovimi ceniki. Vsak prevoznik ima s podjetjem podpisano pogodbo, kjer je določen način obračunavanja transportnih storitev in njihovih cen. S pogodbo je določen cenik za države, regije in kraje. Cenik velja za vse prevoznike, lahko pa je določen samo za določenega prevoznika. Če je krajev razklada v enem prevozu več, pripada prevozniku tudi dodaten znesek za enega, dva ali več krajev, ki je lahko določen za vse prevoznike, ali pa samo za določene. Poleg cenikov so v pomoč pri izbiri tudi kvote - pogodbeni procenti. Kvota je delež, ki pripada nekemu prevozniku, in je prav tako lahko določena za države, regije ali kraje. S kvoto ima prevoznik zagotovilo, kolikšen delež vseh transportov bo opravil v nekem obdobju za določeno lokacijo.

E-Trans ponuja dva načina izbire prevoznika. Prvi način je fiksna dodelitev transporta izbranemu prevozniku, kjer je izbira slednjega prepuščena logistu. Drugi način izbire prevoznika je borzni način. Potreba po transportni storitvi se objavi na borzi, kjer se prevozniki prijavijo na razpisan transport. V primeru, da se na nek transport prijavi več prevoznikov, E-Trans izbere prevoznika, ki najbolj ustreza danim kriterijem cene in kvote. Logist zatem le potrdi izbranega prevoznika.

Za *dejanski transport* poskrbi prevoznik, ki pošlje transportno sredstvo ob dogovorjenem času in odpremi blago do stranke.

Izdelava specifikacije računa s strani prevoznika je precej enostavna, saj so vsi podatki že znani, cena pa določena. Specifikacija je elektronski dokument, ki vsebuje podatke o transportnem nalogu (lahko jih je več) in finančne podatke. Ob zaključku transporta prevoznik

v modulu E-Specifikacija naredi specifikacijo, ki je kot priloga računu za opravljeno transportno storitev v veliko pomoč pri likvidaciji računov.



Slika 1: Struktura programske rešitve E-Trans.

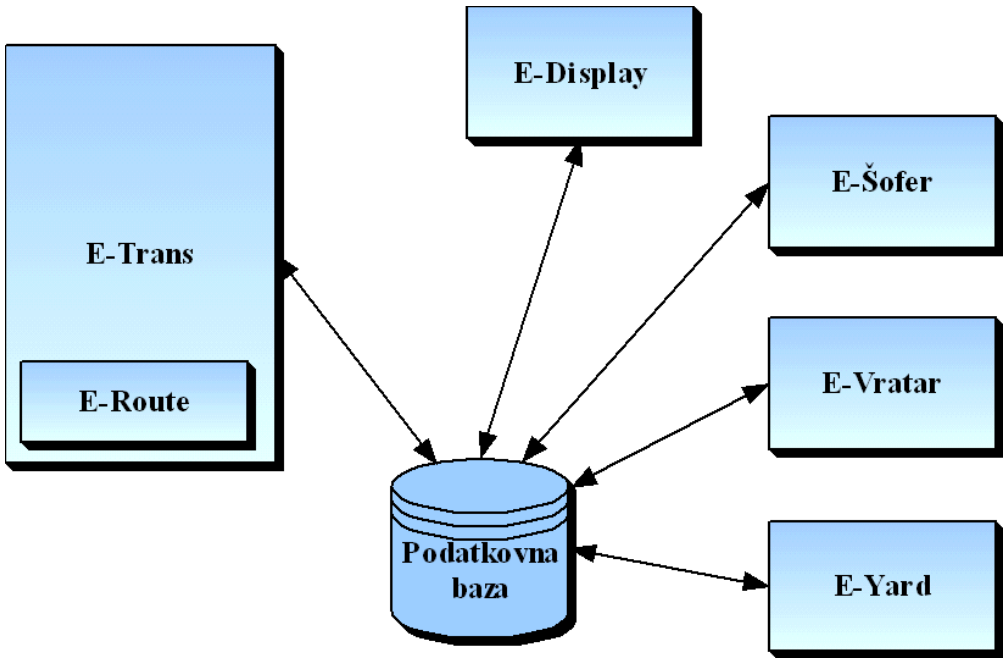
E-Trans je objektno zasnovan porazdeljen sistem. Sestavljen je iz treh nivojev (glej sliko 1). Prvi nivo je uporabniški vmesnik - UI (angl. *user interface*). Ta opisuje procedure in metode, s katerimi uporabnik upravlja računalniški program in je napisan s tehnologijo ASP v jeziku VBScript. Drugi nivo je nivo poslovne logike - BLL (angl. *business logic layer)* in je napisan v programskem jeziku Microsoft Visual Basic 6.0. Tu je vsebovana vsa logika in funkcionalnost, ki skrbi za povezovanje med uporabniškim vmesnikom in podatkovno bazo. Tretji nivo je podatkovni nivo - DAL (angl. *data access layer*). Ta skrbi za shranjevanje in branje podatkov iz podatkovnih baz in je napisan v programskem jeziku Microsoft Visual Basic 6.0. Za podatkovno bazo je uporabljen strežnik SQL.

2.3 Arhitekturna rešitev E-Trans

Programsko rešitev E-Trans se nadgrajuje z dodatnimi moduli (glej sliko 2):

- E-Šofer,
- E-Vratar,
- E-Yard,
- E-Display,
- E-Route.

Skupaj povečujejo funkcionalnost rešitve E-Trans ter izboljšujejo in dodajajo večjo preglednost samega dogajanja in spremljanja od trenutka, ko šofer prispe v podjetje, do trenutka, ko je nalaganje končano in šofer zapusti podjetje.



Slika 2: Shema programske rešitve E-Trans nadgrajena z dodatnimi moduli.

2.3.1 E-Šofer

Modul E-šofer je bil razvit za lažjo evidenco o prispelih transportnih sredstvih, njihovem razvrščanju na nakladalna mesta in podatkih o šoferjih. Da bi potrebne podatke vpisovali kar šoferji sami, je pred vhodom v podjetje postavljen terminal za registriranje. Modul za lažje delo šoferjev ob prijavi omogoča uporabo zaslona na dotik (angl. *touch screen*). Šofer na terminalu vpiše svoje podatke, podatke o vozilu in petmestno številsko kodo za identifikacijo

transportnega naloga, po katerem je pripeljal blago. Kodo za identifikacijo transportnega naloga prevoznik dobi ob potrditvi transporta. V primeru odpovedi terminala lahko logist opravi ročni postopek registracije. Vnos podatkov je zamudnejši, vendar mogoč.

Programski modul je Microsoft Windows aplikacija, napisana v programskem jeziku Microsoft Visual Basic 6.0. Nameščena je na lokalnem računalniku (terminalu). Do podatkov v strežniku SQL dostopa preko lokalnega omrežja, za oddaljene lokacije pa ima možnost dostopa tudi prek spletnih storitev.

2.3.2 E-Vratar

Ena izmed nalog vratarja v podjetjih je, da ima nadzor nad vstopi transportnih in ostalih vozil v podjetje. V E-Vratar modulu ima vratar spisek prijavljenih šoferjev iz modula E-Šofer. Na spisku poišče šoferja in ga spusti v podjetje. Ob vstopu vozila v podjetje vratar v svojem vmesniku zabeleži vstop transportnega sredstva v podjetje, ob izhodu pa zabeleži izstop. Skupaj z modulom E-Šofer obstajajo vsi podatki o gibanju transportnega sredstva (prihod, vstop in izstop iz podjetja).

Programski paket je Windows aplikacija in je napisana v Microsoftovem Visual Basicu 6.0. Do podatkov strežnika SQL dostopa preko lokalnega omrežja, za oddaljene lokacije pa tudi prek spletnih storitev. V primeru okvare računalnika je možna ročna registracija prihodov in odhodov.

2.3.3 E-Yard

E-Yard ali dvoriščni logist skrbi za transportno logistiko znotraj podjetja. Pomembno je, da se vozila ob prihodu v podjetje kar najhitreje in optimalno razporedijo na mesta za nakladanje. Optimalno razporejanje vozil na prosta in prava nakladalna mesta je za večja podjetja kar precejšen zalogaj. Če zraven dodamo še razporejanje nakladalnih in razkladalnih ekip in upoštevamo dejstvo, da ekipe in nakladalna mesta med seboj niso enakovredne, si dela brez računalniško podprte rešitve ne moremo predstavljati.

Logist ob prispetju transportno sredstvo razdeli na opravila glede na število potrebnih nakladalnih mest in število potrebnih nakladalnih ekip. S tem dobimo za vsak prevoz poljubno število opravil, ki vsebujejo en vir, ta pa vsebuje eno nakladalno mesto in eno ekipo.

S tem smo omogočili razporejanje vozila na več mest in mu omogočili možnost izbire med večimi različnimi ekipami za nakladanje ali razkladanje. V aplikaciji logist lahko poljubno prestavlja opravila po časovnih oseh in s tem določi transportnemu sredstvu, kje in kdo ga bo naložil oz. razložil. Ko so vsa opravila opravljena, je zaključen tudi nakladalni ali razkladalni del transporta. S tako zbranimi podatki lahko za potrebe optimizacije naredimo analizo o zadrževanju transportnih sredstev v podjetju in učinkovitosti nakladalnih ekip.

Windows aplikacija je napisana v C# .NET jeziku. Do podatkovne baze dostopa prek lokalnega omrežja. Nameščena je na lokalnem računalniku dvoriščnega logista. V primeru okvare računalnika se lahko program brez večjih problemov namesti na drug računalnik.

2.3.4 E-Display

Ob prihodu pred podjetje in po prijavi šoferja na terminalu le-ta ne more in še ne sme vstopiti v podjetje. Logist v modulu E-Yard določi kje, kdo in kdaj bo nakladal ali razkladal določeno vozilo oz. opravilo. Ob določitvi vseh parametrov potrebnih za nakladanje oz. razkladanje je potrebno šoferju sporočiti, kam naj zapelje transportno sredstvo. Pred parkiriščem je postavljen LED prikazovalnik, kjer šoferji čakajo na poziv za vstop v podjetje. Na prikazovalniku so vsi potrebni podatki za šoferja, tako da ve, kateri je v čakalni vrsti, kdaj naj vstopi in predvsem, kam naj se postavi. Modul E-Display skrbi za komunikacijo med dvoriščnim logistom in grafičnim prikazovalnikom. Ta modul nima ključnega pomena za samo delovanje logističnega procesa. Grafični prikazovalnik krmili Windows storitev, ki glede na izračun iz baze podatkov te prikaže šoferju.

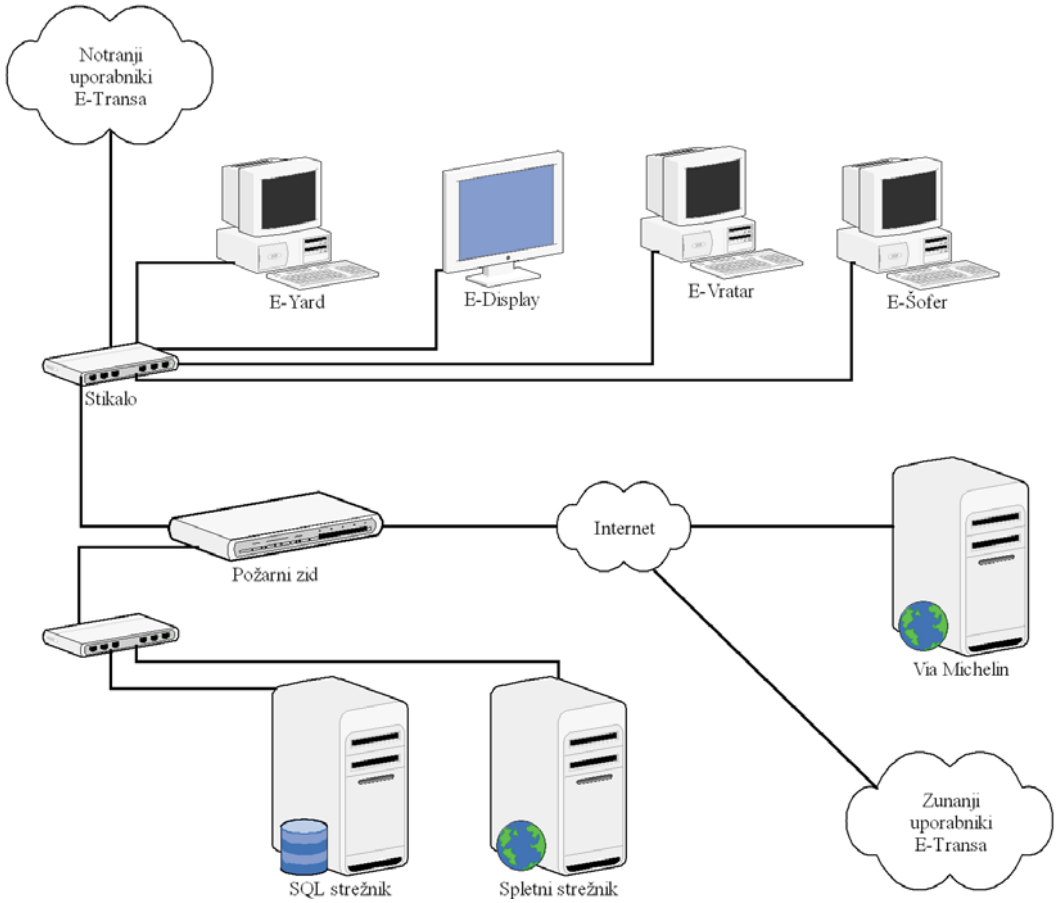
2.3.5 E-Route

Pri določanju cene za prevozno storitev moramo poznati razdaljo, ki jo bo opravil prevoznik. Za natančno določanje razdalje med kraji E-Trans uporablja zunanjo spletno rešitev, ki jo ponuja ViaMichelin [3]. E-Route modul je sestavljen iz dveh delov. V prvem delu se za kraj naklada in razklada v transportu prek spletnega servisa pridobi geografske koordinate. Za določitev geografske koordinate potrebujemo podatke o nazivu, naslovu, pošti in državi. Več kot imamo podanih podatkov, bolj natančno imamo geografsko koordinato. Spletni servis vrača več geografskih lokacij, če obstajajo kraji z istim imenom, ali če je podatkov premalo. V tem primeru mora uporabnik iz vrnjenega rezultata in opisa izbrati pravo geografsko

koordinato. Drugi spletni servis iz dveh ali več podanih geografskih koordinat poišče optimalno pot in njeno razdaljo med njimi.

V modulu E-Route največkrat pride do napak zaradi napačno vnesenih ali pomanjkljivih podatkov. Uporabnik lahko med izbiro lokacij izbere napačno geografsko koordinato. Možnost je izpad sistema ViaMichelin, zato E-Route hrani poizvedbe za določen čas. Za uporabnike je pomemben podatek o razdalji, ki se ga lahko v primeru težav vnese tudi ročno in kasneje dopolni s pravimi podatki.

2.4 Strojna oprema za podporo programske rešitve E-Trans



Slika 3: Strojna oprema rešitve E-Trans.

Odvisno od zahtevnosti programske opreme se določi zmogljivost strojne opreme. Zahteve po zmogljivosti v E-Transu so odvisne od števila uporabnikov, ki hkrati uporabljajo E-Trans ali katerega od njegovih modulov. Strojna oprema je odvisna tudi od politike podjetja v vlaganje

za nakup strojne opreme ali pa od že obstoječe opreme v podjetju. Primerna sestava strojne opreme sistema E-Trans (glej sliko 3) vključuje več strežnikov in računalnikov, na katerih so nameščeni moduli. Pri manjših podjetjih, kjer zahteve po zmogljivostih niso tako velike, lahko podatkovno bazo namestimo na spletni strežnik, s čimer prihranimo pri nakupu enega strežnika. Med strojno opremo štejemo tudi vso mrežno opremo za povezovanje strežnikov in računalnikov med seboj, kot so stikala, usmerjevalniki, modemi in požarni zid.

2.5 Možni načini odpovedi sistema E-Trans

Vsaka strojna oprema je podvržena staranju, različnim napakam ter poškodbam. Podatki so lahko nedostopni iz različnih razlogov, največkrat zaradi odpovedi strojne opreme in mehanskih napak, pa tudi zaradi poškodovanih datotek, napak v programski opremi in seveda zaradi človeških napak.

Tipične težave so:

- nedosegljivi diskovni pogoni ali particije,
- poškodovani podatki,
- premalo testirana programska oprema,
- problemi z virusi,
- odpoved elektronike na matični plošči,
- izguba in/ali poškodovanje registra strežniške konfiguracije,
- okvara zagonskega sektorja – MBR (angl. *master boot record*) na disku,
- poškodbe zaradi vode ali ognja,
- nenamerno formatiranje particij, pogonov,
- nenamerno brisanje podatkov,
- izpad električne energije,
- udar strele,
- sunki električne energije,
- itd.

Ob vseh teh težavah in napakah lahko predvidimo nekatere možne načine odpovedi sistema. Vsak tak način odpovedi lahko pripelje do delnega ali popolnega izpada rešitve E-Trans ali katerega od njegovih modulov. Odpovedi podsistema, ki lahko zaustavi delovanje celotnega sistema, pravimo enojna točka izpada - SPOF (angl. *single point of failure*). Cilj vsakega

sistema je imeti čim manj enojnih točk izpada. Poleg tega je pomembna tudi razpoložljivost sistema

$$Razpoložljivost\ sistema = \frac{MTBF}{MTBF + MTTR},$$

ki jo izračunamo s pomočjo časa med dvema okvarama oziroma izpadoma – MTBF (angl. *mean time between failure*) in povprečnim časom odprave okvare oziroma napake – MTTR (angl. *mean time to repair*).

Visoka razpoložljivost predstavlja tisti nivo razpoložljivosti sistema, pri katerem lahko sistem v skladu s pričakovanji končnega uporabnika opravlja vse naloge, za katere je bil načrtovan, ali pa pričakovanja pri opravljanju teh nalog celo preseže.

Strategije za višanje razpoložljivosti sistema so:

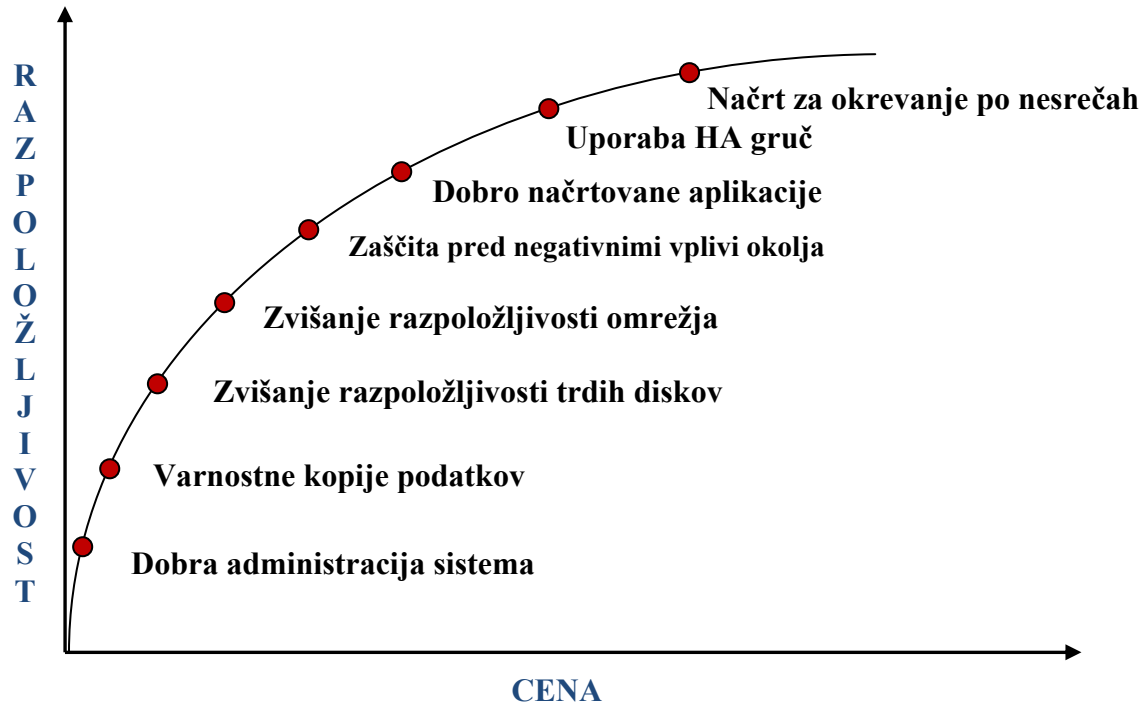
- programska oprema z minimalnim številom napak,
- dobra administracija sistema,
- varnostne kopije podatkov,
- višanje razpoložljivosti trdih diskov,
- višanje razpoložljivosti omrežja,
- zaščita pred negativnimi vplivi okolja,
- dobro načrtovane aplikacije (nadzorne točke, shranjevanje stanja),
- uporaba visoko razpoložljivih HA (angl. *high availability*) gruč,
- načrt za okrevanje po katastrofah.

Zavedati se je treba, da vsaka strategija za višanje razpoložljivosti sistema predstavlja za podjetje določen strošek (glej sliko 4).

Možni načini odpovedi sistema E-Trans so:

- izpad električne energije,
- izpad notranjega omrežja,
- izpad spletnega omrežja,
- izpad podatkovne baze,
- izpad spletnega strežnika,
- vdor v spletni strežnik,
- okvara LED prikazovalnika,
- izpad modula E-Vratar,
- izpad modula E-Šofer,

- izpad modula E-Yard,
- napake v programski opremi,
- večja napaka v programski opremi,
- izpad modula E-Route.



Slika 4: Razmerje med razpoložljivostjo in ceno [6].

2.5.1 Izpad električne energije

Samo bolnice in večja podjetja imajo zagotovljenih več različnih virov dobave električne energije z elektrodistribucijskimi podjetji. Nekateri uporabljajo tudi dizelske agregate za zagotavljanje najnujnejše oskrbe z električno energijo. Večina porabnikov pa danes uporablja brezprekinitvena napajanja. V primeru izpada električne energije in če je le-ta daljši od avtonomije brezprekinitvenega napajanja, strežniki ne morejo delovati. Pogostost izpada električne energije je do dvakrat letno, ponekod pa tudi večkrat, saj dobavo lahko prekine že malo večja nevihta ali podrto drevo.

2.5.2 Izpad notranjega omrežja

Vsi strežniki so povezani v lokalnem omrežju, preko katerega komunicirajo med seboj. Izpad je lahko posledica okvare stikala, prek katerega so povezani strežniki, okvara njegovega napajanja ali pa izpad zaradi preobremenjenosti. Prenos podatkov med njimi je tako onemogočen, prav tako pa tudi dostop in shranjevanje podatkov. Posledica je nedelovanje tistega modula, pri katerem je prišlo do izpada ali pa celotne rešitve E-Trans, če je do izpada prišlo pri strežnikih. Ponovna uporaba je mogoča potem, ko je napaka odpravljena.

2.5.3 Izpad spletnega omrežja

Danes so izpadi povezave do spleta dokaj pogosti, odvisni pa so predvsem od tega, kakšne povezave so uporabljene. Optične povezave so zanesljivejše od bakrenih, pomembno pa je tudi, kako zanesljiv je ponudnik storitev dostopa do spleta. Do napake lahko pride že na samem modemu v podjetju, pri okvari stikala, izpadu požarnega zidu, napak na linijah do ponudnika ali dalje na vozliščih. Do izpada lahko pride tudi zaradi drugačnih vrst napak, npr. odpovedi DNS strežnikov, usmerjevalnikov, napak na povezavah, kjer prenos paketov po linijah ne pride do želenega cilja. Pogostost tovrstnega izpada je nekajkrat letno, resnost pa je odvisna od trajanja izpada. Nekajminutni izpadi so morda še dopustni, če pa je izpad daljši od ene ure ali celo dneva, potem je resnost izpada večja, saj zunanji uporabniki ne morejo dostopati do rešitve E-Trans.

2.5.4 Izpad podatkovne baze

Podatki so ključnega pomena pri programskih sistemih. Poleg specifičnih napak in poškodb baz podatkov, lahko podatke v bazah na strežnikih doleti podobna usoda kot trde diske v osebnih računalnikih. Možni dogodki so:

- poškodovani podatki,
- sistem se preneha odzivati,
- neuspelo pisanje podatkov v bazo,
- neuspelo branje podatkov iz baze,
- nenameren izbris podatkov (tabele, sistemski objekti),
- I/O napake na strežniku SQL,
- vrivanje SQL (angl. *SQL injection*),
- podatkovna baza se postavi v sumljiv način (angl. s*uspected mode*).

Nekaj od zgoraj naštetih napak predstavlja veliko nevarnost izgube podatkov, zato je pomembno redno arhiviranje podatkovne baze. Sama konfiguracija strežnika SQL mora biti taka, da je verjetnost pojava katerekoli od zgornjih napak kar najmanjša. Izpad strežnika SQL pripelje do popolnega izpada sistema.

2.5.5 Izpad spletnega strežnika

Vsak izpad spletnega strežnika onemogoča uporabo programa E-Trans. Možnih je več vzrokov za izpad strežnika, od napak na strojni ali programski opremi pa vse do človeškega faktorja.

2.5.6 Vdor v spletni strežnik

Pri uporabi spleta je varnost danes ključnega pomena, saj lahko kakršenkoli vdor v strežnik povzroči ogromno škodo. Ni sicer nujno, da vsak vdor pripelje do izpada strežnika, lahko pa onemogoči normalno delovanje sistema. Zelo pomembno je, da se strežnik redno posodablja s popravki. Dostop in uporaba sistemskih funkcij morata biti omejena in dovoljena samo za tiste funkcije, ki so potrebne za delovanje.

2.5.7 Izpad modula E-Display

Do izpada modula E-Display lahko pride zaradi okvare samega prikazovalnika, motenj na komunikacijah ali pa odpovedi strežnika, ki krmili LED prikazovalnik.

2.5.8 Izpad modula E-Vratar

Do izpada modula E-Vratar lahko pride zaradi okvare računalnika, na katerem je nameščen ta modul, lahko pa pride do izpada podatkovne baze ali pa napak na notranjem omrežju.

2.5.9 Izpad modula E-Šofer

Do izpada modula E-Šofer lahko pride zaradi okvare računalnika, na katerem je nameščen ta modul, lahko pa pride do izpada podatkovne baze ali pa napak na notranjem omrežju.

2.5.10 Izpad modula E-Yard

Do izpada modula E-Yard lahko pride zaradi okvare računalnika, na katerem je nameščen ta modul, lahko pa pride do izpada podatkovne baze ali pa napak na notranjem omrežju.

2.5.11 Napake v programski opremi

Noben sistem ni popoln. Nekatere napake v programiranju se odkrijejo že v času razvoja, nekatere v času testiranj, spet druge pa med samo uporabo programske opreme. Nekatere manjše napake lahko ostanejo skrite za vedno. Tudi te lahko pripeljejo do odpovedi sistema ali pa samo povzročajo slabo voljo pri uporabnikih.

2.5.12 Večja napaka v programski opremi

Do večjih napak pride pri namestitvah programske opreme ali menjavah verzij programa, ko te niso bile dovolj testirane. Take napake (npr. prekoračitev sklada, angl. *stack overflow*) se odkrijejo hitro, saj onemogočajo normalno uporabo sistema.

2.5.13 Izpad modula E-Route

Izpad zunanjega ponudnika storitve lahko pripelje do delne odpovedi sistema oziroma do nedostopnosti potrebnih podatkov, ko jih potrebujemo.

3 Analiza drevesa napak

Analiza drevesa napak (FTA, angl. *fault tree analysis*) je analiza odpovedi, kjer je neželeno stanje nekega sistema analizirano z uporabo Boolove logike, ki sestavlja serijo nižjih dogodkov [7]. Ta analitična metoda se v glavnem uporablja za količinsko določanje verjetnosti pojava nevarnosti. Večinoma so za izdelavo FTA zadolženi inženirji. Analiza zahteva ljudi s popolnim poznavanjem sistema, ki ga analizirajo.

Prvoten razvoj FTA je bil namenjen projektom, kjer do napak ne sme priti (v jedrskih elektrarnah napake niso tolerantne). Podjetje Bell Telephone Laboratories je FTA razvil leta 1962 za potrebe ameriškega letalstva (U.S. Air Force), za namen razvoja raket vrste »minuteman«. Kasneje so koncept posvojili in izboljšali pri Boeing Company, obsežnejše pa so ga uporabljale ameriške jedrske elektrarne.

Izdelava FTA je lahko draga in potratna izkušnja, zato je potrebno razmišljati o manjših podsistemih. Taki sistemi jamčijo manj napak pri analizi, predvsem pa so analize manj zahtevne. Dobro analiziran velik sistem je sestavljen iz več podsistemov.

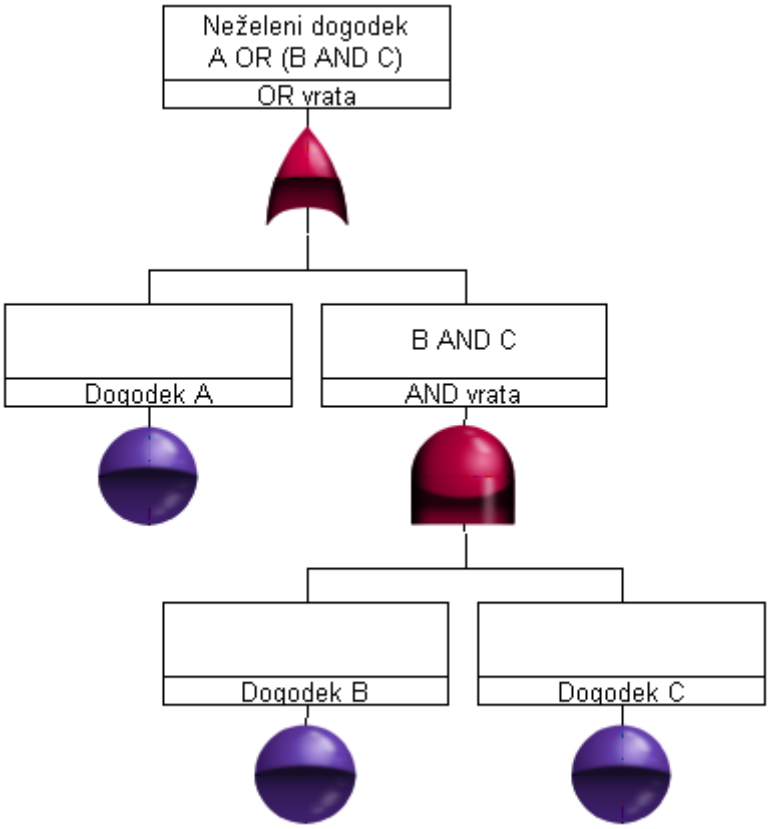
Največkrat se analiza drevesa napak uporablja za:

- iskanje nevarnih, kritičnih komponent,
- potrditev zahteve izdelka,
- certificiranje zanesljivosti izdelka,
- določanje varnosti izdelka,
- preiskave nesreč in nepričakovanih dogodkov,
- določanje načrtovanih sprememb,
- identifikacijo vzrokov in posledic dogodkov,
- iskanje običajnih napak.

3.1 Diagram drevesa napak

Ker noben sistem ni popoln, se je potrebno zavedati možnih napak. Možnost delnega ali popolnega delovanja je večja kot možnost delne ali popolne odpovedi. Na ta način je izdelava drevesa napak hitrejša, kot bi bila izdelava drevesa uspešnosti. Diagram drevesa napak je logični blok diagram, ki kaže stanje sistema (glavni dogodek) v odvisnosti od njegovih

komponent – dogodkov (slika 5). V korenu diagrama nastopa neželeni glavni dogodek, listi v drevesu pa nastopajo kot posamezni dogodki, ki preko logičnih vrat (OR, AND, XOR …) pripeljejo do neželenega glavnega dogodka. V listih nastopajo odpovedi opreme, človeški faktor in ostali faktorji, na katere nimamo vpliva. Tako hitro vidimo, da bo sistem zanesljiv, če imamo veliko AND vrat, še bolje pa, če imamo veliko večvhodnih AND vrat, kar pomeni, da mora biti izpolnjenih več pogojev za nek dogodek. Obratno iz tega sledimo cilju imeti čim manj OR vrat, kjer že en dogodek lahko pripelje do neželenega dogodka. Koncept gradnje diagrama drevesa napak je od zgoraj navzdol (angl. *top-down*).



Slika 5: Zgled diagrama drevesa napak.

Najpogostejše napake pri gradnji drevesa napak so:

- uporaba prevelikega področja za glavni dogodek, kar pripelje do velikega in kompleksnega diagrama drevesa,
- uporaba različnih nomenklatur za enake dogodke, kar onemogoča iskanje dogodkov, ki se ponavljajo v več vejah drevesa,

- uporaba enake nomenklature za podobne, vendar različne dogodke, kar povzroči določitev istega dogodka za več scenarijev, vendar ti dogodki nastopijo ob različnih predpogojih,
- razdelitev drevesa na veje po električnih, mehaničnih in strukturnih podsistemih, pozabi pa se na vmesnike in povezovanja v celoto.

3.2 Metodologija

FTA je deduktivna analiza napak, ki temelji na enem glavnem neželenem dogodku in nam poda metodo za določanje vzroka za ta dogodek [8]. Glavni neželeni dogodek je na korenu drevesa in večinoma pripelje do popolne, delne ali katastrofalne odpovedi sistema. Za glavni dogodek lahko vzamemo npr. strmoglavljenje potniškega letala, odtekanje hladilne tekočine pri hlajenju jedrskega reaktorja, neuspešen vžig avtomobila, odpoved računalniškega sistema v podjetju …

Glavni dogodek je samo eden in vsi ostali dogodki pripeljejo do glavnega neželenega dogodka. Nato se vsak dogodek, ki bi lahko pripeljal do napake, doda drevesu napak kot zaporedje logičnih izrazov. Za vsak dogodek je potrebno določiti verjetnost njegovega pojava, ki pa jo je v praksi zaradi dragih testiranj zelo težko določiti. Ob vseh poznanih podatkih računalniški programi izračunajo verjetnost odpovedi podsistemov ali sistema.

3.3 Postopek

Obstaja kar nekaj postopkov izgradnje analize drevesa napak, vendar lahko najpogostejšega razdelimo v pet korakov. Pomembno je, da je drevo napak uporabljeno za analizo glavnega neželenega dogodka in samo ta dogodek je lahko analiziran z enim drevesom napak.

Koraki za izgradnjo analize drevesa napak so:

- definicija glavnega neželenega dogodka,
- spoznavanje in razumevanje sistema,
- gradnja diagrama drevesa napak,
- vrednotenje drevesa napak,
- upravljanje najdene nevarnosti.

3.3.1 Definicija glavnega neželenega dogodka

Definicija glavnega neželenega dogodka je včasih težavna, zato je potrebno, da pri tem sodelujejo ljudje, ki podrobno poznajo sistem in lahko navedejo več neželenih dogodkov, od katerih določimo glavnega. Če glavni dogodek ni jasno določen, lahko nastane veliko, nejasno in kompleksno drevo napak. Zato potrebujemo točno določen glavni dogodek na točno določenem področju.

3.3.2 Spoznavanje in razumevanje sistema

Ob znanem glavnem neželenem dogodku je potrebno vse dogodke, ki lahko pripeljejo do neželenih dogodkov, preštudirati in analizirati. Pridobiti prave vrednosti verjetnosti pojava je lahko dolg in drag proces, zato jih velikokrat določajo računalniški programi, kar pripelje do cenejših analiz. Sistemski analitiki pomagajo pri razumevanju celotnega sistema, razvijalci sistema pa ga podrobno poznajo. Pomembno je sodelovanje vseh, da se ne izpusti kakšnega neželenega dogodka. Za vsak najden dogodek je potrebno določiti verjetnost pojavljanja.

3.3.3 Gradnja diagrama drevesa napak

Ko imamo znane vse dogodke in njihove verjetnosti pojavljanja, lahko zgradimo drevo napak. Drevo običajno temelji na AND, OR in XOR vratih, ki definirajo glavne karakteristike drevesa napak. AND vrata uporabimo, kadar so za pojav nekega izhodnega dogodka pogoj pojavitve vseh vstopnih dogodkov, OR vrata pa, kadar je za pojav izhodnega dogodka potreben pojav vsaj enega vstopnega dogodka.

3.3.4 Vrednotenje drevesa napak

Ko je bilo zgrajeno drevo napak za specifičen neželen dogodek, je potrebno proučiti rezultate, narediti analizo za možne izboljšave in preprečitev neželenih dogodkov ali pa vsaj omiliti njihove posledice. Tukaj najdemo in definiramo vse možne nevarnosti, ki lahko direktno ali indirektno vplivajo na sistem.

3.3.5 Upravljanje najdene nevarnosti

Ta korak je zelo specifičen in se zelo razlikuje od enega do drugega sistema, vendar glavni cilj vedno ostaja isti. Ob odkritju nevarnosti je potrebno z vsemi možnimi metodami zmanjšati možnost pojava tega dogodka.

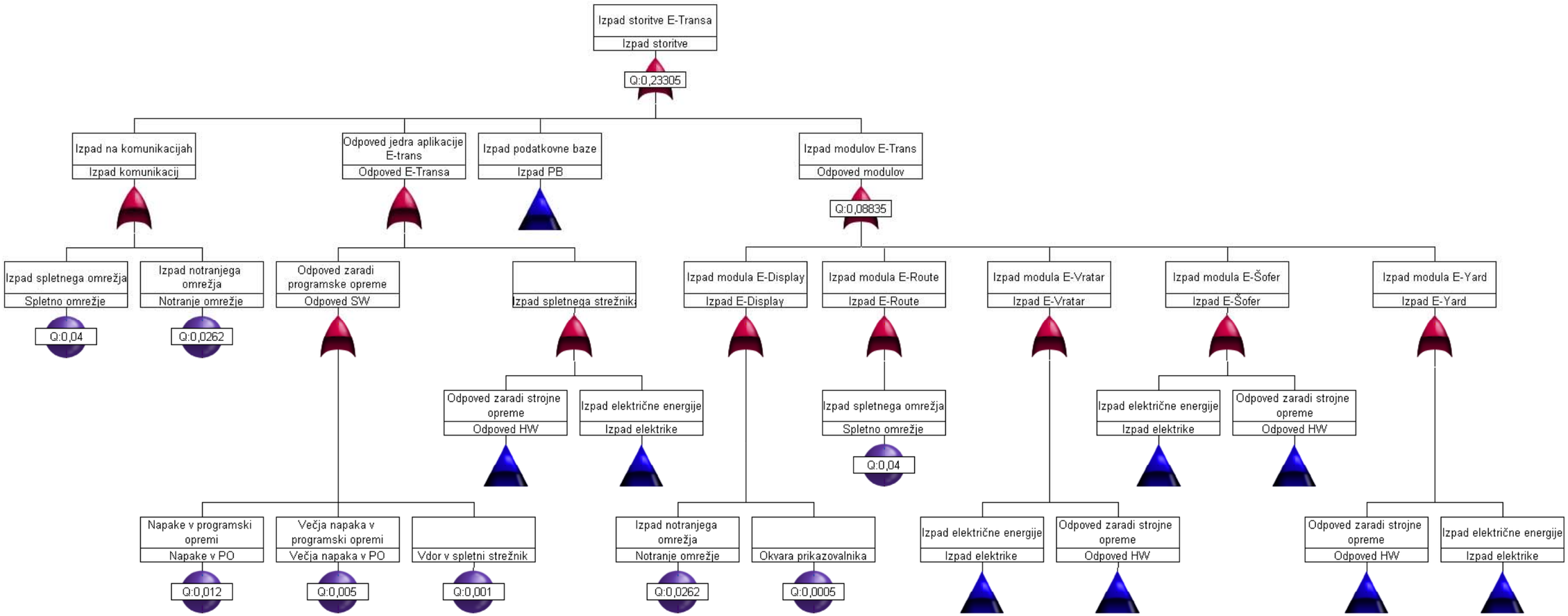
3.4 Izvedba analize na programski rešitvi E-Trans

Za analizo na programski rešitvi E-Trans sem uporabil demo program Relex Architect [4]. Ker ima demo verzija programa omejeno število možnih vrat in dogodkov, sem se pri izvedbi analize zaradi kompleksnosti problema osredotočil na en način odpovedi. Zaradi velikosti drevesa bi bil za vse načine odpovedi diagram drevesa napak prevelik in nepregleden, zato sem nekaj dogodkov izločil iz samega diagrama in jih predelal posebej. Dogodke, ki sem jih podrobneje razdelal z ostalimi diagrami drevesa napak, sem označil z modrimi trikotniki. Ostali dogodki so prikazani s krogi vijolične barve, na katerih je zapisana verjetnost dogodka.

Za glavni dogodek sem izbral izpad storitve E-Trans (slika 6). Možne odpovedi sem razdelil na izpad komunikacij, izpad podatkovne baze, odpoved jedra aplikacije E-Trans in na odpovedi modulov. Izpad na komunikacijah je posledica izpada spletnega omrežja in izpada notranjega omrežja. Izpad jedra aplikacije E-Trans je razdeljen na odpoved zaradi programske opreme in na izpad spletnega strežnika. Izpad podatkovne baze je predelan kasneje in je označen z modrim trikotnikom (slika 6).

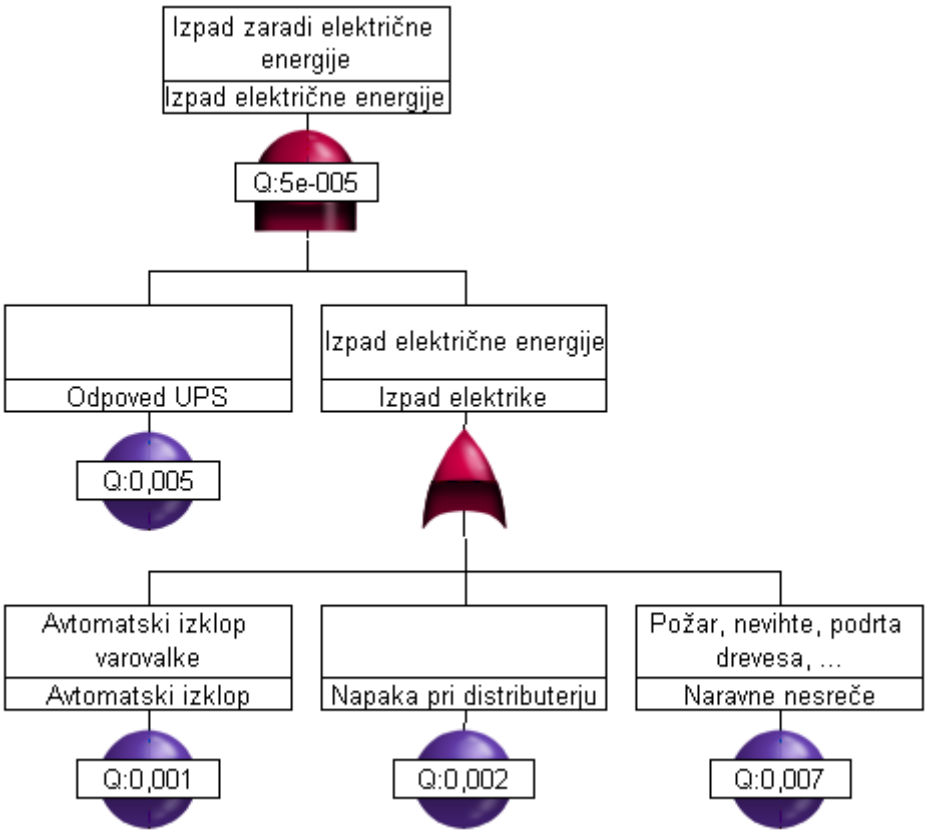
Zadnja skupina je izpad modulov. Moduli E-Vratar, E-Šofer, E-Yard so predvsem odvisni od strojne opreme, programske opreme in električne energije. Izpad modul E-Route je odvisen od izpada spletnega omrežja, modul E-Display pa od okvare prikazovalnika ali izpada notranjega omrežja.

Izpad električne energije je vzrok za večino odpovedi, vendar ga zaradi omejenega števila vrat nisem dodajal vsem izpadom, sem pa upošteval vrednost njegove pojavitve pri določenem izpadu. Izpadi električne energije so označeni z modrimi trikotniki.



Slika 6: Diagram drevesa napak: izpad storitve programske rešitve E-Trans.

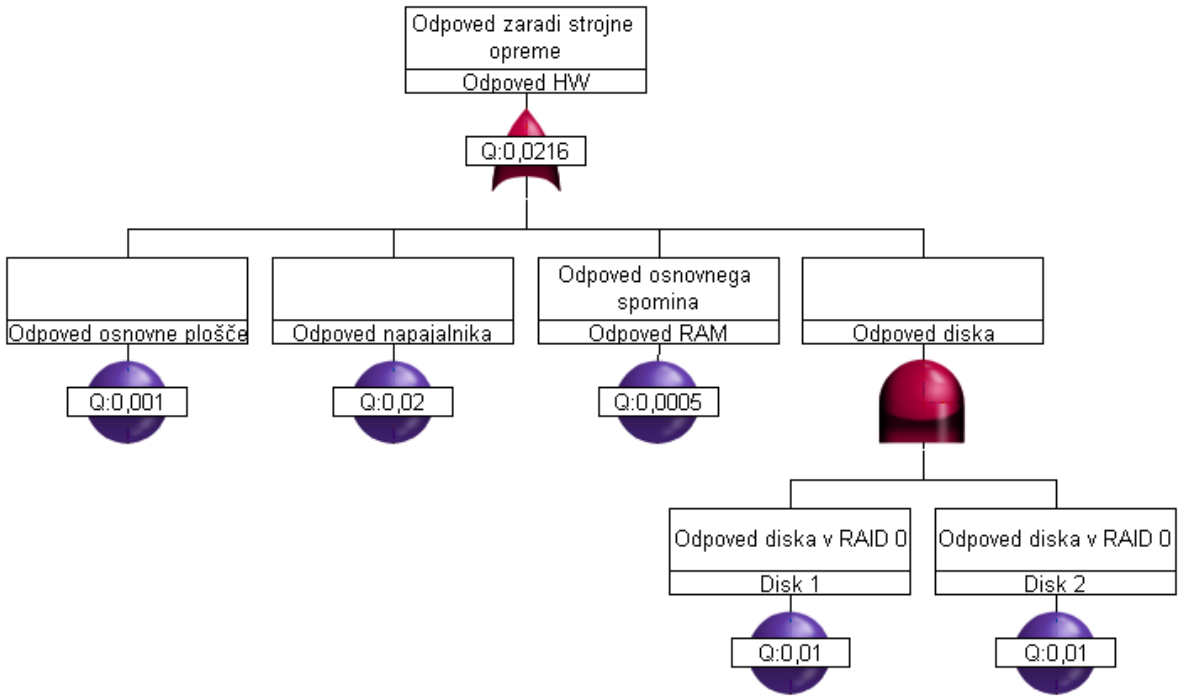
Izpad električne energije (slika 7) je vključen tudi pri drugih načinih odpovedi, saj brez električne energije delovanje računalnika ni možno. V diagramu je kot možen dogodek za izpad električne energije navedena odpoved UPS. Zaradi okvare bližnje naprave lahko zaradi kratkega stika izklopi avtomatsko varovalko. Lahko pride do motenj pri dobavi elektrike zaradi naravnih nesreč, podrtega drevesa ali pa pride do večje napake pri distributerju. Najvišjo verjetnost pojava imajo naravne nesreče, je pa odvisno od lokacije odjemalca električne energije in pogostosti neviht ter grmenja.



Slika 7: Diagram drevesa napak: izpad električne energije.

Drugi diagram predstavlja napako na strojni opremi. Vsebuje štiri dogodke (glej sliko 8), ki so najpogostejši pri okvarah računalnikov oziroma strežnikov. Razlikujejo se predvsem po zanesljivosti in varnosti, saj so strežniške komponente precej zanesljivejše kot komponente v namiznih računalnikih, kar se pozna tudi pri ceni teh komponent. Odpoved napajalnika ima največjo verjetnost pojavitve. Dovolj pogosta napaka je odpoved diska, sledita pa okvara

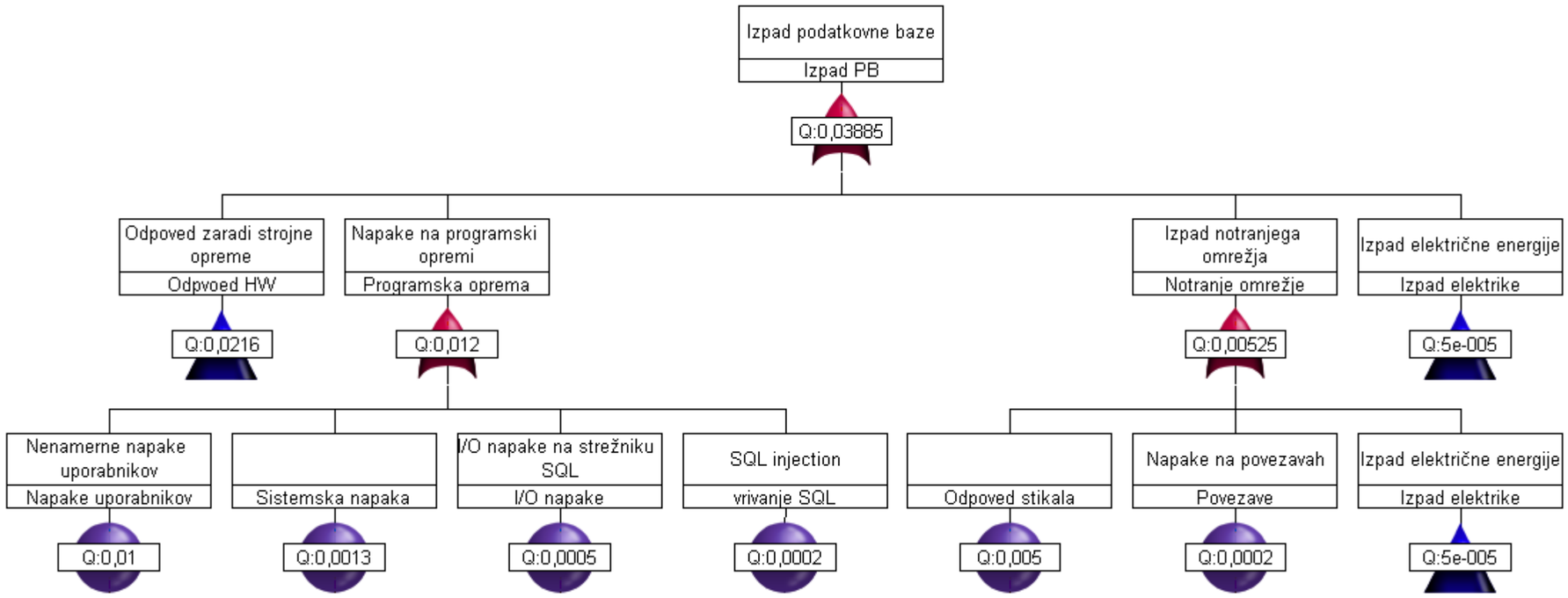
osnovnega spomina in osnovne plošče. Ta način je zelo odvisen od konfiguracije sistema, saj so nekateri strežniki organizirani v gruče, kar zelo poveča odpornost na napake ali odpovedi.



Slika 8: Diagram drevesa napak: odpoved zaradi strojne opreme.

Izpad podatkovne baze je posledica štirih skupin dogodkov (glej sliko 9), kot so izpad električne energije, napake na strojni opremi, napake na programski opremi in izpad notranjega omrežja.

Verjetnost pojavljanja posameznega dogodka je ocena, ki pa se od realnih podatkov lahko zelo razlikuje, saj ima vsak uporabnik različno strojno opremo. Prav bi prišli tudi podatki proizvajalca strojne opreme, če s takimi podatki razpolaga, izključiti pa ne bi smel mnenja serviserjev opreme, saj bi natančneje poznali ocene možnosti pojava kakšne okvare. Za natančnejšo analizo bi se tako moral osredotočiti na točno določeno vrsto strojne opreme določenega proizvajalca ali celo opraviti meritve na obstoječem delujočem sistemu. S tem bi pridobil realnejše podatke, saj stranke uporabljajo različne vrste strežnikov. Nekatera podjetja prispevajo več finančnih sredstev za zanesljivost opreme, druga manj.



Slika 9: Diagram drevesa napak: izpad podatkovne baze.

Večji poudarek bi lahko namenil programski opremi, katere delovanje je bolj odvisno od človeškega faktorja in programa. Vsakdo razume, da se pokvari npr. napajalnik pri strežniku, težje pa je opravičiti odpoved sistema zaradi površnosti programerja ali administratorja.

4 Analiza načinov odpovedi in njihovih posledic

Kakovost in zanesljivost izdelkov sta pri današnjih kupcih ključnega pomena. Z napredkom tehnologije so ti izdelki vedno bolj kompleksni, proizvajalci pa vedno težje zagotovijo kakovost, zanesljivost in varnost. Do nedavnega so kakovost izdelkov dosegali s testiranjem izdelkov ob koncu načrtovanja izdelka ali procesa, kar je podaljšalo čas načrtovanja in podražilo izdelek.

Analiza načinov odpovedi in njihovih posledic (FMEA, angl. *failure mode and effect analysis*) je sistematična metoda iskanja in preprečevanja problemov v procesih in okvar izdelkov, preden ti nastanejo. Analize so osredotočene na preprečevanje okvar, večanje varnosti in povišanje kupčevega zadovoljstva.

Cilj analize je najti vse možne odpovedi izdelka ali procesa. Za napako na izdelku gre, kadar ne deluje kot bi moral ali pa sploh ne deluje. Napake niso omejene samo na izdelke, saj lahko nastanejo tudi zaradi uporabnikovih pomot in jih je prav tako potrebno vključiti v analizo.

4.1 Kdaj vršiti FMEA analizo

Idealno je, če se analiza naredi že v načrtovanju izdelka ali procesa, kljub temu pa analiza na že obstoječih izdelkih ali procesih prinese veliko koristi. Analiza možnih napak in njihovih posledic je živ dokument. Med razvojnim ciklom izdelka prihaja do sprememb in popravkov izdelka ali procesa. Vsaka taka sprememba lahko pripelje do novih napak, zato je pomembno, da se pri vsaki spremembi popravi in dopolni tudi analizo možnih napak.

4.2 Tipi FMEA analize

Obstaja nekaj tipov analiz možnih napak in njihovih posledic. Nekatere se uporabljajo večkrat kot druge:

- sistemska,
- načrtovalska,
- procesna, za proizvodne procese,
- servisna,

- programska analiza.

4.3 Uporaba FMEA analize

Proces FMEA je široko uporaben, saj se ne uporablja samo za načrtovanje izdelkov in procesov. Kot osrednji steber procesa jo uporabljajo številne razvojne skupine v podjetjih. FMEA zagotavlja strukturiran pristop, možnost zgodnje analize verige vzrokov za neuspeh izdelka, ocenitev resnosti vplivov in preverjanje učinkovitosti strategij. Rezultat analize so oblikovani akcijski načrti preprečitve neuspeha, odkrivanja ali zmanjševanja vpliva potencialnih oblik neuspeha novega izdelka.

4.4 Izdelava FMEA analize

Izdelek ali proces lahko odpove na več načinov. Vsak način odpovedi ima potencialno posledico in nekatere posledice so bolj verjetne kot druge. Vsaka potencialna posledica ima določeno tveganje. Analiza je proces iskanja napak, posledic in tveganj v procesu ali izdelku, s katero izračunamo oceno kritičnosti za vsak način.

Ocena kritičnosti je sestavljena iz treh faktorjev [2]:

- resnosti posledic odpovedi (angl. *severity*),
- pogostosti pojavitve (angl. *occurrence of failures*),
- možnosti pravočasnega zaznavanja odpovedi (angl. *detection of failures*).

S podatki in poznavanjem procesa ali izdelka določimo za vsak način odpovedi subjektivno vse tri faktorje (resnost - S, pogostost - O in zaznavanje - D) z ocenami od 1 do 10. Z množenjem vseh treh faktorjev

$$RPN = S \times O \times D$$

dobimo faktor tveganja – RPN (angl. *risk priority number*) za vsak način odpovedi. Velikost faktorja tveganja je od 1 do 1.000. Uporablja se pri izdelavi prioritetne lestvice za odpravo vzrokov odpovedi. Lestvico načinov odpovedi sortiramo padajoče po faktorju tveganja in resnosti posledice. Najprej je potrebno odpraviti vzroke z vrha lestvice, potem pa se določi

nov faktor tveganja. Izboljšave in popravke je potrebno izvajati tako dolgo, dokler nov faktor tveganja ni na zadovoljivi ravni.

4.5 Prednosti FMEA analize

FMEA je orodje za izboljšanje kakovosti in zanesljivosti načrtovanja. Pravilna uporaba omogoča kar nekaj prednosti:

- poveča kakovost in zanesljivost,
- poveča kupčevo zadovoljstvo,
- omogoča zgodnje odkrivanje in odstranitev potencialnih odpovedi,
- ponuja prioritetno lestvico pomanjkljivosti,
- povzame znanje o izdelku oz. procesu,
- poudarja preventivne ukrepe,
- dokumentira tveganost in rešitve za zmanjšanje tveganja,
- minimizira kasnejše spremembe, popravke in s tem povezane stroške.

4.6 Izvedba analize na programski rešitvi E-Trans

Vrednosti ocene kritičnosti na programski rešitvi E-Trans so informativne, saj so vnešeni podatki zgolj subjektivna ocena in izhajajo iz lastnih izkušenj pri njeni uporabi. Za natančnejše ocene kritičnosti bi potreboval večjo ekipo, saj je pri takih projektih pomembno združiti znanje in izkušnje več strokovnjakov. Poleg tega bi potrebovali več časa in več sredstev, da bi lahko naredili prave meritve in ocene resnosti, pojavitve in detekcije.

Glede na znane podatke in oceno tveganja je največje tveganje rešitve E-Trans izpad podatkovne baze (tabela 1). Tega izpada se popolnoma ne da preprečiti, smo pa zagotovili redno arhiviranje baze podatkov in predlagali uporabo gruč za strežnik SQL, kjer je to mogoče. S to rešitvijo se verjetnost izpada zelo zmanjša.

Na drugem mestu po faktorju tveganja je vdor v spletni strežnik. Po izkušnjah se velikokrat zaradi neznanja v administraciji strežnika odpre in omogoči vse sistemske funkcije, kar predstavlja veliko varnostno luknjo. Administracijo strežnika naj opravlja oseba, ki je izobražena za to in ima potrebna znanja.

Tabela 1: Analiza načinov odpovedi in njihovih posledic.

Sistem/ Komponenta/ Funkcija	Možne napake	Možne posledice napak	Veljavni modelni nadzorni mehanizmi	Resnost (*S*)	Možnost pojava (*O*)	Detekcija (*D*)	Faktor tveganja (*RPN*)	Priporočljivi ukrepi
Izpad podatkovne baze	Disk, napajalnik	Izguba podatkov, Nedelovanje E-Transa	Dnevno arhiviranje baze	10	4	3	120	RAID, arhiv podatkov, zanesljivejši strežnik
Vdor v spletni strežnik	Vdor, brisanje podatkov,moteno delovanje strežnika	Kraja podatkov	Požarni zid	8	3	4	96	Požarni zid, varnostne posodobitve
Izpad spletnega strežnika	Disk, napajalnik, matična plošča	Nedelovanje E-Transa		8	4	3	96	Rezervni strežnik ali zanesljivejši strežnik
Napaka v programski opremi	Hrošči, človeške napake, varnostne luknje	Slaba volja uporabnikov		4	6	4	96	Temeljito testiranje
Izpad spletnega omrežja	Izpadi linij, ponudnik			6	7	2	84	Optika
Izpad notranjega omrežja	Odpoved stikala, poškodovani kabli	Nedelovanje E-Transa		7	4	3	84	Redno vzdrževanje
Izpad elektrike	Napovedani in nenapovedani izpadi	Nedelovanje E-Transa	UPS, avtonomija 2 minuti	6	7	2	84	Močnejši UPS
Izpad modula E-Route	Izpad spletnega omrežja, izpad požarnega zida	Onemogočen dostop do podatkov		5	5	3	75	
Izpad modula E-Šofer	Disk, napajalnik, matična plošča	Onemogočena prijava šoferjev		5	5	3	75	Rezervni napajalnik, RAID disk
Izpad modula E-Vratar	Disk, napajalnik, matična plošča	Onemogočeno delo vratarja		5	5	3	75	Namestitev programa na več računalnikih
Izpad modula E-Yard	Disk, napajalnik, matična plošča	Onemogočeno delo logista		5	5	3	75	Namestitev programa na več računalnikih
Večja napaka v programski opremi	Napake pri namestitvi ali menjavi verzij sistema	Nedelovanje E-Transa		6	4	3	72	Testiranje
Okvara LED prikazovalnika	Okvara diod, okvara krmilne logike	Ne dela		4	4	4	64	

Pričakovano je na tretjem mestu izpad spletnega strežnika. Ob odpovedi tega strežnika lahko moduli rešitve E-Trans delujejo, pride pa do izpada jedra E-Trans, kar je treba odpraviti v najkrajšem možnem času.

Izpad napajanja je šele na sedmem mestu, čeprav bi pričakoval, da bo višje na lestvici. Z uporabo brezprekinitvenega napajanja se krajše izpade obide. V primeru večjega izpada pa tudi drugi sistemi v podjetju ne bodo delovali.

5 Zaključek

Ob zaključku diplomskega dela opažam, da so pri FTA analizi rezultati presenetljivo visoki. Prvi vzrok je verjetno v tem, da so vse vrednosti ocen pri analizah zgolj informativne, saj ne izhajajo iz natančnih meritev in analiz, ampak so podane zgolj iz izkušenj načrtovalcev, programerjev in uporabnikov aplikacije E-Trans. Drugi razlog je verjetno ta, da načini odpovedi niso bili tako natančno definirani, kar je tudi pripeljalo do neobičajnega drevesa napak.

Pri obeh analizah sem prišel do zaključka, da je samo jedro aplikacije E-Trans zanesljiva aplikacija. Ravno obratno pa je pri modulih, saj so nameščeni na več uporabniških računalnikih. Kljub temu izpad enega modula ni tako kritičen, saj se lahko v najslabšem primeru hitro zamenja računalnik in ponovno namesti modul. Ponavadi je E-Trans nameščen na strežnike, ki jih podjetja že uporabljajo za druge namene, zato tudi podjetja sama poskrbijo za vzdrževanje in varnost teh strežnikov.

Potrebno je tudi razlikovati izpade, na katere lahko vplivamo in jih omejimo. Zato smo več pozornosti namenili izpadom na programski opremi. E-Trans je prilagojen procesom podjetja, ti pa se redno spreminjajo. Tako je potrebno tudi E-Trans vedno prilagajati in dograjevati. S tem se vedno veča možnost pojava napak v programski opremi, časa za temeljito testiranje pa je vedno premalo. Hitri popravki lahko velikokrat privedejo do izpadov zaradi neprevidnosti. Zato smo se v podjetju dogovorili, da se ob vsaki menjavi verzije pridobi avtorizacijo stranke. Ta pred tem tudi sama testira delovanje programa in s tem prevzame del odgovornosti za morebiten izpad zaradi programske opreme.

Dane ugotovitve bomo pri razvoju nove aplikacije prav gotovo upoštevali. Premislili bomo o možnostih, da se kateri od modulov naredi kot spletna aplikacija, kar bi zelo zmanjšalo možnost njegovega izpada.

6 Viri in literatura

[1] D. Požar, »Teorija in praksa (transporta in logistike)«, Maribor: Založba Obzorja, 1985

[2] R. McDermott, R. Mikulak, M. Beauregard, »The basics of FMEA«, Portland: Productivity, Inc., 1996

[3] (2008) ViaMichelin Web ServicesEasy Integration. Dostopno na: http://business.viamichelin.co.uk/b2b/webservices_uk.html

[4] (2008) Relex Architect Studio. Dostopno na: http://www.relex.com/

[6] (2008) Visoka razpoložljivost. Dostopno na: http://marvin.fri.uni-lj.si/PVIS/Razpolozljivost.ppt

[7] (2008) Fault tree analysis. Dostopno na: http://en.wikipedia.org/wiki/Fault_tree_analysis

[8] (2008) U.S. Nuclear Regulatory Commission Fault Tree Handbook. Dostopno na: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/sr0492.pdf