*XXIX Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2011**, Beograd, 06. i 07. decembar 2011.*

PRIMENA FAZI ANALIZE STABLA OTKAZA U UNAPREĐIVANJU RADA E-MAIL SERVISA

Ranko R. Nedeljković, Slobodan Mitrović, Dragana Drenovac
Univerzitet u Beogradu – Saobraćajni fakultet

Sadržaj: *U ovom radu posmatran je e-mail servis Saobraćajnog fakulteta i razmatrana je njegova pouzdanost kroz mogućnost pristupa tom servisu. Primenjena je Fazi analiza stabla otkaza, određeni su fazi težinski indeksi koji predstavljaju važnost pojedinačnih osnovnih događaja, a dobijeni rezultati su iskorišćeni u procesu razvoja novog e-mail servisa.*

Ključne reči: *Fazi analiza stabla otkaza, e-mail servis, fazi težinski indeks*

To design systems that work correctly we often need to understand and correct how they can go wrong

Dan Goldin, NASA administrator, 2000

1. Uvod

Ovaj rad predstavlja nastavak istraživanja vezanih za primenu fazi analize stabla otkaza u određivanju pouzdanosti e-mail servisa. Naime, proces dizajniranja jednog složenog sistema zavisi od determinacije faktora koji imaju presudan uticaj na ukupnu pouzdanost. Pri tome je poželjno da bude procenjen i uticaj svakog od uočenih faktora na stabilnost rada sistema, odnosno, potrebno je oceniti koliko je za sistem kritičan otkaz svakog osnovnog događaja pojedinačno. Ova vrsta analize osnovnih događaja uključuje formiranje fazi težinskih indeksa za svaki od njih a potom i njihovo rangiranje. U analizi se koriste fazi brojevi jer su njima predstavljene mere mogućnosti osnovnih događaja i time omogućeno razmatranje sistema u uslovima neizvesnosti.

U ovom istraživanju posmatran je e-mail servis Saobraćajnog fakulteta i analizirana je njegova pouzdanost u smislu mogućnosti pristupa tom servisu. Cilj ovog istraživanja je mogućnost primene Analize stabla otkaza (Fault tree analysis – FTA) u procesu razvoja e-mail servisa. Istraživanje je vršeno u dve faze: Prva faza je uključila analizu postojećeg e-mail servisa Saobraćajnog fakulteta, primenom navedene tehnike, što je podrazumevalo definisanje stabla otkaza u kome figurišu determinisani faktori otkaza, odnosno određeni događaji čijom realizacijom dolazi do otkaza pristupa klijenta posmatranom sistemu. Ova faza je opisana u radu objavljenom na Postelu 2010 [6]. Druga faza podrazumeva određivanje fazi težinskih indeksa determinisanih faktora, na osnovu kojih se može uočiti funkcionalna važnost pojedinačnih događaja. Na osnovu toga se pristupa unapređenju postojećeg ili dizajniranju potpuno novog e-mail servisa. Unapređeni sistem se pušta u rad, nakon čega se vrši nova determinacija faktora koji

utiču na pouzdanost sistema, formira se novo stablo otkaza i ponovo vrši određivanje težinskih indeksa.

U ovom radu opisana je druga faza navedenog istraživanja uz prikaz odgovarajućih zaključaka.

2. Pregled prve faze

Prva faza istraživanja analizira meru mogućnosti otkaza koje posmatrani e-mail server može dati klijentskom entitetu. Klijentski entitet može biti e-mail klijent korisnika sistema (korisnik pristupa svojim računarom uz upotrebu e-mail klijentskog programa, poput Outlook Express-a, Eudore, Thunderbird...) ili drugi e-mail server koji namerava da izvrši određenu e-mail transakciju [6]. Posmatrani e-mail servis opslužuje e-mail klijente korisnika upotrebom POP3 protokola komunikacije (za prijem poruka), dok u slučaju slanja poruka upotrebom navedenih e-mail klijenata ili transakcija sa drugim e-mail serverima se koristi SMTP protokol. Navedeni protokoli su realizovani na serveru koji fukcioniše u Linux okruženju, kroz upotrebu Postfix MTA, kao i QPOP *deamon*-a. Komunikacija sa klijentima nije kriptovana i bazirana je na pravilu da je pun pristup omogućen klijentima koji pripadaju IP adresnom opsegu lokalne računarske mreže, kao i adresama odnosno opsezima, koji se nalaze na tzv. *beloj listi*. Ostalim klijentima je omogućen POP3 pristup za preuzimanje poste, ali ne i SMTP za slanje.

Shodno navedenom, otkazi koji se u ovom domenu razmatraju su slučajevi koji mogu nastupiti upravo upotrebom ovih protokola. Otkazi koji mogu nastupiti prema e-mail klijentu korisnika se mogu klasifikovati na sledeći način [6]:

E1 – Neispravno korisničko ime ili šifra

E2 – Isteklo vreme sesije, koje može nastati usled preopterećenosti klijentskog računara, pri čemu je klijentski e-mail program podešen da prijavi slučaj „session timeout“ posle definisanog vremenskog intervala (default vrednost je najčešće 1 minut), ili u slučaju kada je POP datoteka na serveru oštećena (slučaj POP EOF).

E3 – Slanje poruke upotrebom klijentskog e-mail programa uz upotrebu lokalnog e-mail naloga, ali upotrebom internet veze koja ne pripada lokalnom sistemu. Na ovaj način posmatrani server prepoznaje transakciju kroz tzv. „relay access“ pristup, što se smatra nedozvoljenim tipom transakcije, ukoliko e-mail server ima aktiviran sistem restrikcija.

E4 – Pokušaj pristupa sistemu upotrebom identifikatora korisničkog naloga koji ima vrednost manju od 100 (u operativnim sistemima tipa UNIX/BSD/LINUX). Na ovaj način klijent želi iskoristiti jedan od „sistemskih naloga“ na serveru, tj. pokušava „prevariti“ sistem, radi zloupotrebe. Sistem je podešen da ne prima ovakav tip pristupa, zbog čega nastaje otkaz.

E5 – Klijentski program pokušava da započne POP3 sesiju uz upotrebu korisničkog naloga za koji je već, u tom trenutku, započeta sesija, što nije dozvoljeno, usled čega nastaje otkaz.

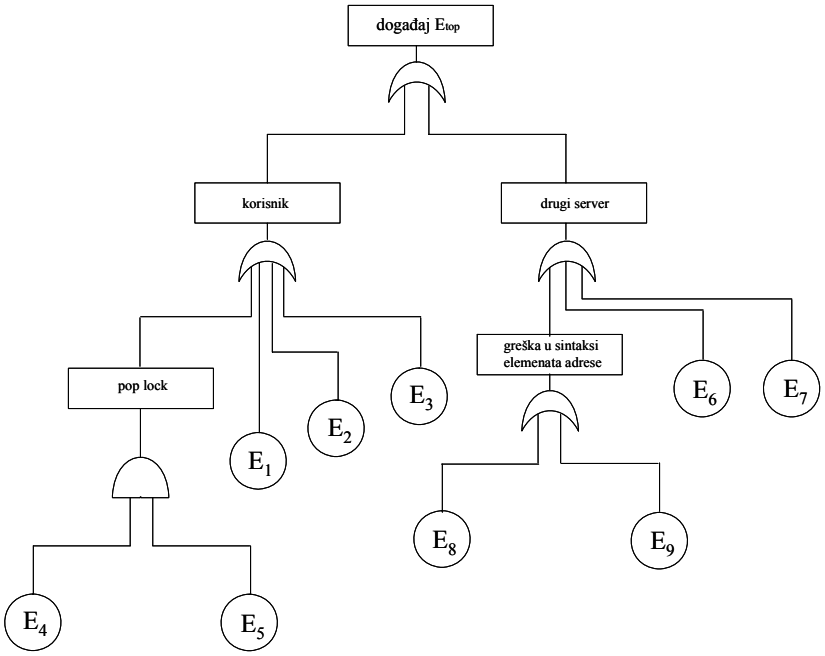
E6 – Server koji pokušava da započne SMTP transakciju nema regularan DNS zapis, zbog čega biva odbijen nakon negativnog odgovora na proveru identiteta kroz reversni DNS upit.

E7 – Server koji pokušava da započne SMTP transakciju nema ispravnu HELO identifikaciju, zbog čega biva odbijen.

E8 – Server pokušava da isporuči poruku na adresu nepostojećeg korisnika u okviru destinacionog internet domena, zbog čega transakcija biva odbijena (User unknown in local recipient table).
E9 – Server pokušava da isporuči poruku sa adresom primaoca koja ima nepostojeći ili neispravan destinacioni internet domen (na primer korisnik@gooogle.com), zbog čega transakcija biva odbijena.

Navedeni događaji predstavljaju faktore koji su vezani, kako za tehničke osobine posmatranog sistema, tako i za same korisnike. Na primer, događaj E1 može biti realizovan unosom neispravnog korisničkog imena ili šifre od strane samog korisnika, ali i neispravnim podešavanjem e-mail klijentskog programa.

Za determinisani skup faktora definisano je stablo otkaza koje je prikazano na slici 1, gde će slučajevi u kojima je došlo do otkaza prema e-mail klijentu korisnika, biti imenovani kao „*korisnik",* a otkazi prema drugom serveru, biti imenovani kao „*server*".



Slika 1. *Stablo otkaza postojećeg e-mail servisa*

Fazi FTA analizom određena je mogućnost otkaza čitavog sistema koja je izražena fazi brojem (0.0662 0.3589 0.5939).

Doprinos svakog osnovnog događaja otkazu čitavog sistema u analizi stabla otkaza naziva se važnost tog događaja i meri se fazi težinskim indeksom. Fazi težinski indeks nekog osnovnog događaja određuje se eliminisanjem tog događaja iz stabla otkaza. Potrebno je odrediti mogućnost otkaza sistema p_{sys} i mogućnost otkaza sistema iz kog je isključen k-ti osnovni događaj $p_{sys(k)}$. Na osnovu ovih vrednosti određuje se

težinski indeks W(p_{sys} , $p_{sys(k)}$) koji predstavlja rastojanje između dva fazi broja p_{sys} i $p_{sys(k)}$.

Za dva fazi broja $\tilde{M} = [a_m^\alpha, b_m^\alpha, c_m^\alpha]$ i $\tilde{N} = [a_n^\alpha, b_n^\alpha, c_n^\alpha]$ rastojanje između njih, u oznaci $\delta(\tilde{M}, \tilde{N})$ definiše se kao

$$\delta(\tilde{M}, \tilde{N}) = 0.5\{\max(\left|a_m^\alpha - a_n^\alpha\right|, \left|b_m^\alpha - b_n^\alpha\right|) + \left|c_m^\alpha - c_n^\alpha\right|\} \quad (1)$$

Po određivanju rastojanja između p_{sys} i $p_{sys(k)}$ potrebno je rangirati dobijene fazi brojeve. Postoji više načina na koje se to može izvršiti, a u ovom radu iskorišćen je metod koji se zasniva na α preseku fazi broja. Neka su za dva uvedena fazi broja $\tilde{M}$ i $\tilde{N}$ α preseci $\tilde{M}_\alpha = [m_\alpha^-, m_\alpha^+]$ i $\tilde{N}_\alpha = [n_\alpha^-, n_\alpha^+]$. $\tilde{M}$ je manje od $\tilde{N}$, ako je $m_\alpha^- \le n_\alpha^-$ i $m_\alpha^+ \le n_\alpha^+$, za $\forall \alpha \in (0,1]$.

Rezultati dobijeni primenom tehnike za određivanje fazi težinskih indeksa prikazani su u sledećoj tabeli:

Tabela 1. *Fazi težinski indeksi osnovnih događaja postojećeg e-mail servisa*

Događaji	Fazi težinski indeksi
E1	0.2672
E2	0.0431
E3	0.002
E4	0.0026
E5	0.0026
E6	0.0485
E7	0.0036
E8	0.0101
E9	0.0109

Fazi težinski indeks označava koliko neki događaj (otkaz) doprinosi ključnom događaju (top event-u). To znači da, što je njegova vrednost veća to je on značajniji i treba više pokloniti pažnje njegovoj eliminaciji u procesu dizajniranja novog sistema. Na osnovu prikazanih podataka može se uočiti važnost determinisanih faktora, koji se može opisati sledećim odnosom:

E1 > E6 > E2 > E9 > E8 > E7 > (E4,E5) > E3

Na osnovu dobijenih podataka, može se reći da ubedljivo najveći uticaj na otkaz transakcije ima faktor koji je vezan za neispravnu autentifikaciju korisnika, za kojim, respektivno posmatrano, slede započinjanje SMTP transakcije sa neregularnim DNS zapisom, isteklo vreme sesije, pokušaj isporuke poruke sa neispravnim domenom u adresi primaoca, itd.

Događaji koji ne pripadaju grupi vezanoj za „ljudski faktor“, nadalje se mogu okarakterisati kao bitni kriterijumi na koje treba obratiti pažnju, prilikom unapređenja postojećeg ili dizajniranja novog e-mail servisa.

3. Faza 2 – Dizajniranje i ispitivanje pouzdanosti novog e-mail servisa

Rezultati dobijeni FTA analizom su opravdali odluku da se pristupi dizajniranju nove generacije e-mail servisa Saobraćajnog fakulteta. Novi servis, sa svojim karakteristikama, osim navedenih kriterijuma pouzdanosti, morao je da zadovolji i sledeće zahteve:

- povećanje funkcionalnosti, što podrazumeva klijentski pristup upotrebom web servisa, kao i mobilnih i desktop platformi, sa bilo koje ip adrese,
- povećanje bezbednosti pristupa upotrebom kriptovanih konekcija,
- upotrebu IMAP protokola, kao i kontinuitet za POP3 protokol,
- stabilnu migraciju postojećih naloga i pripadajuće pošte, kao i kontinuitet platforme serverskog operativnog sistema,
- skalabilnost u pogledu proširenja spektra popratnih servisa,
- kontinuitet i skalabilnost monitoring servisa.

Navedeni servis je morao biti dizajniran na taj način da verovatnoća realizacije određenih događaja, koji utiču na pouzdanost sistema, a koji su uobličeni kroz navedene kriterijume pouzdanosti, bude minimizirana.
Shodno navedenom, rešenje novog sistema podrazumeva integraciju sledećih serverskih servisa na platformi koja je bazirana na operativnom sistemu koji pripada *Linux* familiji:

- *Postfix* Mail Transfer Agent,
- *Dovecot* server,
- antivirus/antispam filter baziran na kombinaciji Amavis/Clamav/Spamassassin,
- *OpenSSL* sa upotrebom 802.1X standarda u bližoj perspektivi,
- monitoring servis baziran na kombinaciji *Syslog/RRDTools/Mailgraph.*

Nakon uspešne implementacije ovog rešenja, novi e-mail servis je pušten u rad da bi se prikupili podaci o događajima koji bi potencijalno uticali na realizaciju *top event*-a, odnosno otkaza sistema zahtevu koji je postavljen od strane klijenta. U toku radnog perioda u trajanju od 6 meseci, identifikovana je realizacija sledećih događaja, odnosno otkaza koji su nastupili prema e-mail klijentu:
E_1 – Neispravno korisničko ime ili šifra
E_2 – Isteklo vreme sesije, koje može nastati usled preopterećenosti klijentskog računara, pri čemu je klijentski e-mail program podešen da prijavi slučaj „session timeout“ posle definisanog vremenskog intervala (default vrednost je najčešće 1min.), ili u slučaju kada je POP datoteka na serveru oštećena (slučaj POP EOF).
E_3 – Slanje poruke upotrebom klijentskog e-mail programa uz upotrebu lokalnog e-mail naloga, ali upotrebom internet veze koja ne pripada lokalnom sistemu, a koja nije kriptovana. Na ovaj način posmatrani server prepoznaje transakciju kroz tzv. „relay access“ pristup, što se smatra nedozvoljenim tipom transakcije, ukoliko e-mail server ima aktiviran sistem restrikcija.

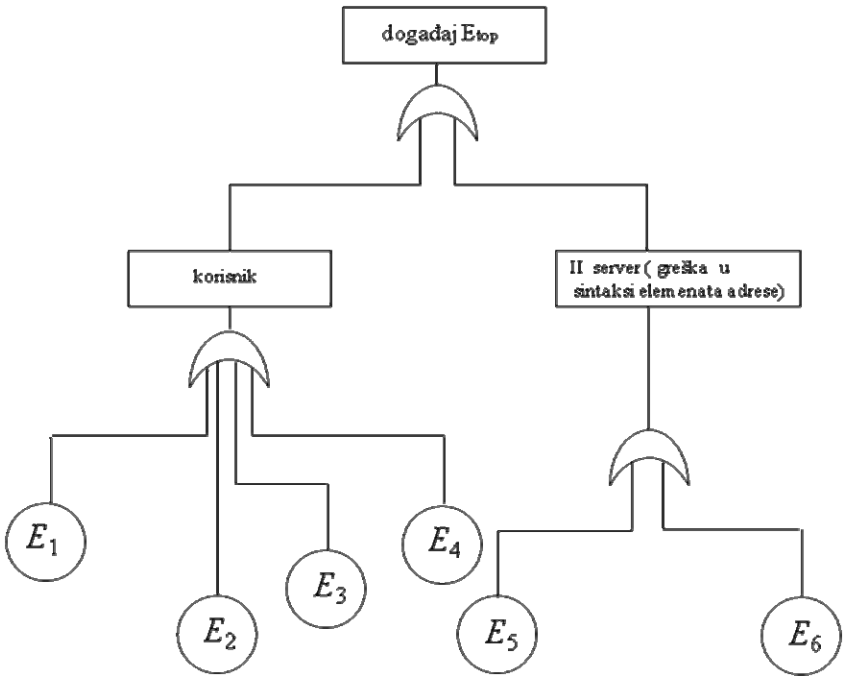
E_4 – Prekid sesije prouzrokovan neispravnim podešavanjima na strani e-mail klijenta, kao što je upotreba pogrešnog mehanizma za kriptovanje šifre i sl.
E_5 – Server pokušava isporučiti poruku na adresu nepostojećeg korisnika u okviru destinacionog internet domena, zbog čega transakcija biva odbijena (User unknown in local recipient table).
E_6 – Server pokušava isporučiti poruku sa adresu adresom primaoca koja ima nepostojeći ili neispravan destinacioni internet domen (na primer korisnik@goooogle.com), zbog čega transakcija biva odbijena.

Na osnovu dostupnih podataka i procene eksperta određeni su fazi brojevi koji predstavljaju meru mogućnosti da se pojedini osnovni događaj realizuje. Podaci su dati u tabeli 2.

Tabela 2. *Dodela fazi brojeva osnovnim događajima*

osnovni događaji	fazi brojevi dodeljeni događajima		
	a - donja granica	b - sredina	c - gornja granica
E1	0.000639915931904	0.000799894914879	0.000959873897855
E2	0.000000542608196	0.000000678260244	0.000000813912293
E3	0.001206037149218	0.001507546436522	0.001809055723827
E4	0.000100020777372	0.000125025971715	0.000150031166058
E5	0.001130614610042	0.001413268262553	0.001695921915063
E6	0.000536820374757	0.000671025468446	0.000805230562135

Za determinisani skup faktora definisano je stablo otkaza koje je prikazano na slici 2.



Slika 2. *Stablo otkaza novog e-mail servisa*

Fazi FTA analizom došlo se do podatka da je mogućnost otkaza čitavog sistema izražena fazi brojem (0.003609144227828 0.004509929142237 0.005410114134559). Ako se dobijeni rezultat uporedi sa rezultatom FTA analize iz prethodnog rada (fazi brojem (0.0662 0.3589 0.5939)), može se videti da ukupna mera mogućnosti otkaza unapređenog sistema ima uočljivo manju vrednost. To znači da je proces determinacije određenih tehničkih nedostataka kao i njihovo uklanjanje izvedeno kroz razvoj novog sistema bio uspešan. Dodatna provera unapređenog sistema obavljena je kroz realizaciju novog kruga determinacije faktora koji mogu uticati na otkaz novog sistema. Determinacija je pokazala da i dalje postoje dve grupe događaja koji dovode do otkaza, odnosno grupa koja se može okarakterisati kao „ljudski faktor“, kao i grupa koja se može okarakterisati „tehnički nedostatak“. Događaji iz druge faze, koji pripadaju grupi tehničkih nedostataka mogu se okarakterisati kao čist podskup ove grupe iz prve faze, tj. kod unapređenog sistema nije uočen nijedan novi događaj koji kao tehnički nedostatak može uticati na realizaciju *top event*-a. Sa druge strane, u grupi događaja koji su vezani za „ljudski faktor“ uočen je još jedan novi događaj. Ovakva ocena opravdava očekivanja da se ljudska greška ni na koji način ne može isključiti iz grupe faktora koji realno imaju krucijalan uticaj na pouzdanost sistema koji pripradaju grupaciji korisničkih servisa.

Primenom tehnike za određivanje fazi težinskih indeksa dobijeni su rezultati, koji su prikazani u sledećoj tabeli:

Tabela 3. *Fazi težinski indeksi osnovnih događaja novog e-mail servisa*

Događaji	Fazi težinski indeksi
E1	0.00087626151294
E2	0.00000074235569
E3	0.001652771386694
E4	0.000136859773822
E5	0.001549248945286
E6	0.000734983658771

Na osnovu prikazanih podataka može se uočiti važnost determinisanih faktora, koji se može opisati sledećim odnosom:

$$E3 > E5 > E1 > E6 > E4 > E2$$

Poređenjem fazi težinskih indeksa događaja iz ove grupe faktora pokazuje da pojedini tip ljudske greške uvek ima dominantan uticaj na vrednost fazi broja kojim se izražava otkaz čitavog sistema, dok će uticaj ostalih tipova biti znatno manji. Nakon unapređenja posmatranog sistema, posmatrani tip ljudske greške ne mora da ostane na dominantnoj poziciji, već može biti zamenjen drugim tipom.

4. Zaključak

Analizom strukture događaja koji utiču na otkaz sistema kod osnovne i unapređene verzije e-mail servisa došlo se do zaključka da je broj tehničkih faktora koji dovode do realizacije *top event*-a znatno umanjen u slučaju unapređene verzije servisa. Sa druge strane pojavio se jedan novi događaj koji pripada grupi ljudskih faktora, a koji se odnosi na neispravno podešavanje email klijenta, što može biti očekivano, jer je

sistem, koji je tehnički unapređen, donekle i komplikovaniji, što se reflektuje i na strukturu podešavanja klijentskih parametara. Uticaj ovog faktora se može eliminisati formiranjem aplikacije za automatizovano konfigurisanje klijenata. Ipak, kompletna slika koja je dobijena na ovaj način ukazuje na osetno povećanje pouzdanosti sistema.

Na ovaj način se može pretpostaviti da sukcesivna upotreba FTA analize može da dovede do potpune eliminacije tehničkih faktora koji dovode do otkaza sistema, odnosno do idealne situacije da na otkaz sistema utiče samo ljudski faktor.

Literatura

[1] Tyagi S.K, Pandey D., Tyagi R., "Fuzzy set theoretic approach to fault tree analysis", *International Journal of Engineering, Science and Technology,* Vol. 2, No. 5, 2010, pp. 276-283

[2] Cheong C. W., Hui Lan A. L., Web Access Failure Analysis – Fuzzy Reliability Approach, *International Journal of The Computer, the Internet and Management* Vol. 12 no.1 (January – April, 2004) pp 65 – 73

[3] Ragheb M., Probabilistic and possibilistic fault tree analysis, 2008 Available: https://netfiles.uiuc.edu/mragheb

[4] Sule, D. R., Watkins T. K. Evaluation of fault tree using fuzzy logic analysis, Available: www.iienet.org/uploadedfiles/IIE/Technical.../ResearchConf5-01-2059.pdf

[5] Klir G.J., Yuan B., *Fuzzy sets and fuzzy logic, theory and applications*, Prentice-Hall, Upper Saddle River, NJ, 1995

[6] Nedeljković R., Drenovac D., Mitrović S., "*Primena fazi aritmetike u određivanju pouzdanosti e-mail servisa*" XXVIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju POSTEL 2010, Beograd

[7] Cheng Y. L., *Uncertainties in fault tree analysis*, www2.tku.edu.tw/~tkjse/3-1/3-1-3.pdf

[8] Yang Z. X., Shimada Y., Suzuki K., Sayama H., *Fuzzy fault diagnostic system based on fault tree analysis*, Fuzzy Systems, 1995. International Joint Conference of the Fourth IEEE International Conference on Fuzzy Systems and The Second International Fuzzy Engineering Symposium

Abstract: *In this paper e-mail service of The Faculty of Traffic and Transport Engineering is observed. Its reliability is considered through the possibility of access to that service. Fuzzy Fault Tree Analysis was applied, fuzzy weighted indices representing the importance of individual basic events are determined and the results are used in the process of developing a new e-mail service.*

Keywords: *fuzzy fault tree analysis, e-mail servce, fuzzy weighted index*

APPLICATION OF FUZZY FAULT TREE ANALYSIS IN E-MAIL SERVICE IMPROVEMENT

Ranko R. Nedeljković, Slobodan Mitrović, Dragana Drenovac