Koncept načrtovanja zanesljivosti sistemov za podporo ukrepanju ob klicu v sili

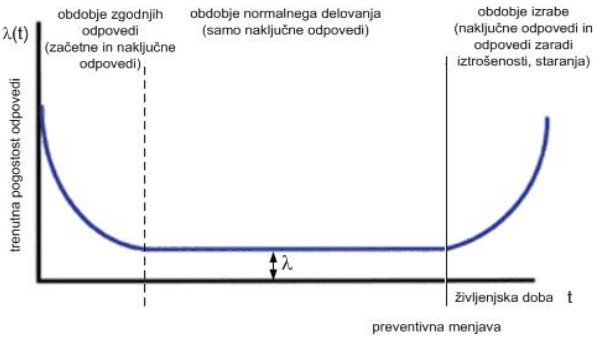
Barbara Brezovec[1], Vojko Matko[1] in Marko Podberšič[2]
[1]Fakulteta za elektrotehniko, računalništvo in informatiko, Univerza v Mariboru
[2]Ministrstvo za obrambo, Uprava Republike Slovenije za zaščito in reševanje, Ljubljana
barbara.brezovec@uni-mb.si, vojko.matko@uni-mb.si, marko.podbersic@urszr.si

Concept of reliability design of modern informatic system for emergency call

System of emergency call needs high reliability rates. It has to be ready and in service at every moment. Systems consists of some number of services that has to receive information and data in order to provide the most quality in service. In the article methods and terms to provide high status of reliability are presented. They were used as a guide and recomendations to software and harware designer of renewed system for dispatching in emergency call.

1. Uvod

Osnovo za podporo ukrepanju ob klicu na enotno evropsko številko za klic v sili 112, ki se izvaja v centrih za obveščanje, predstavljajo različni informacijsko komunikacijski sistemi. Za učinkovito orientacijo v prostoru uporablja operativno osebje v centrih za obveščanje geografsko informacijski sistem, ki omogoča iskanje lokacije, vizualizacijo prostora okrog lokacije dogodka in prostorske analize glede na ogroženost ljudi in okolje.
Sistem obveščanja mora biti pravočasen in zanesljiv, saj odigra veliko vlogo pri življenjsko pomembnih situacijah. S stališča zanesljivosti je potrebno upoštevati, da obsega zanesljivost kot termin različne metode in postopke, ki: določajo, napovedujejo, preučujejo ali povečujejo pravilno delovanje sistema (v našem primeru sistema IT obveščanja) oziroma zmanjšujejo njegovo odpovedovanje.
Na osnovi testiranja celotne dobe uporabe različnih tehničnih sistemov funkcija pogostosti odpovedi $\lambda(t)$ opiše značilno obliko kopalne kadi, ki je prikazana na sliki 1 [1-2].



Slika 1: Krivulja pogostosti odpovedi skozi življenjsko dobo [1-2]

2. Zvišanje zanesljivosti

Analiza stanja napak in posledic (FMEA - Failure modes and effects analysis) je metoda, ki v sistemu obravnava vse načine odpovedi posameznih komponent in ovrednoti njihove vplive na različnih nivojih. Iz jakosti posameznega vpliva lahko ocenimo kritičnost načina odpovedi posamezne komponente na zanesljivost sistema. Metoda zahteva podrobno poznavanje sistema z načrtovalskega vidika in vidika delovanja. S to metodo identificiramo najbolj kritične načine odpovedi in analiziramo njihov vpliv na sistem. Služi za pripravo diagnostičnih postopkov ali tabel s potencialnimi okvarami, saj podaja pregled vplivov posameznih načinov odpovedi komponent in s tem služi za pripravo preventivnih in drugih vzdrževalnih posegov. Omogoča načrtovanje built-in testov, načrtovanje indikatorjev odpovedi in načrtovanje redundanc. V delovnem obrazcu za analizo FMEA zberemo informacije o izdelku ali njegovih komponentah v obliki preglednice.

Tabela 1: Ocena resnosti posledice [1]

(9–10) Možna varnostna tveganja in zakonski problemi, možna izguba življenja ali največje nezadovoljstvo.
(7–8) Možno visoko nezadovoljstvo operaterja – možne resne poškodbe ali največja odstopanja od predpisanega delovanja sistema – razdor.
(5–6) Možno srednje nezadovoljstvo operaterja – možne male poškodbe, neprimerno delovanje sistema / delovanje z zamudo.
(3–4) Operater lahko opazi možno napako in je lahko rahlo nezadovoljen ali vznemirjen.
(1–2) Operater morda ne bo opazil napake – neopažena napaka.

Na podlagi posledic ocenimo verjetnost pojavitve napake.

Tabela 2: Ocena verjetnosti pojavitve napake [1]

(5) Zelo visoka verjetnost, da se pojavi napaka.
(4) Visoka verjetnost, da se pojavi napaka.
(3) Zmerna verjetnost, da se pojavi napaka.
(2) Majhna verjetnost, da se pojavi napaka.
(1) Neznatna verjetnost, da se pojavi napaka.

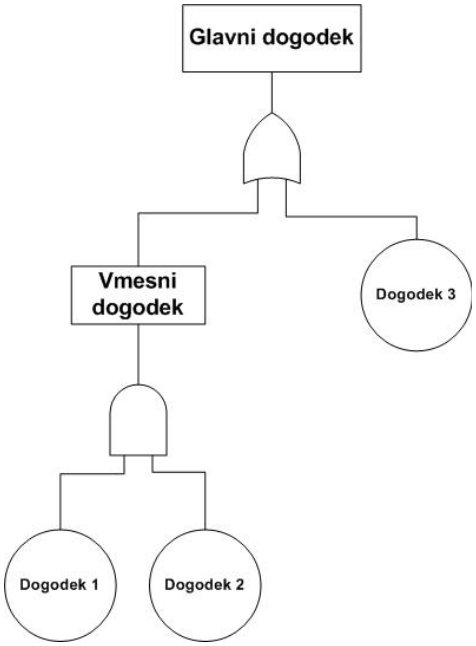
Treba je odkriti in navesti modelne nadzorne mehanizme, ki jih lahko uporabimo, da zmanjšamo ali odstranimo možne napake.
Sestaviti moramo lestvico za detekcijo napak in zabeležiti rezultate meritev.
Tipična ocenjevalna tabela je podana v tabeli 3.

Tabela 3: Ocena verjetnosti detekcije napak [1]

(5) Nična verjetnost, da odkrijemo možen vzrok napake.
(4) Skoraj nična verjetnost, da odkrijemo možen vzrok napake.
(3) Malo verjetno, da odkrijemo možen vzrok napake.
(2) Veliko možnosti, da odkrijemo možen vzrok napake.
(1) Skoraj gotovo, da odkrijemo možen vzrok napake.

Ker je verjetno, da bomo med analizo odkrili več kot eno napako, je pomembno, da te prednostno razvrstimo tako, da vsaki od njih pripišemo številko prednostnega tveganja.
Priporočljivo je, da se zabeležijo vsi ukrepi, ki bodo zmanjšali ali odstranili možne napake. Pomembno je navesti ukrepe, ki se nanašajo na glavni vzrok problema, ne pa na njegove simptome. Vedeti moramo, da je zgornji vzorec generični vzorec za FMEA in da lahko dodamo še več stolpcev glede na kompleksnost projekta.

Analiza drevesa okvar (**Fault tree analysis - FTA)** je analiza napak, kjer se analizira neželeno stanje sistema z digitalno logiko za iskanje povezav med posameznimi dogodki nižje v strukturi. Je deduktivna "Top-down" metoda za analiziranje načrta in delovanja sistema. Obsega podatke glavnega dogodka, ki je analiziran (recimo požar) in ki mu nato sledi identifikacija vseh posledično povezanih elementov v sistemu, ki bi lahko povzročili ta dogodek. Drevo okvar nudi priročno predstavitev s simboli kombinacije dogodkov, ki so rezultat pojava glavnega dogodka. Dogodki in vrata v analizi drevesa okvar so predstavljeni s simboli. Analize dreves okvar so ponavadi izvršene grafično z uporabo logičnih struktur ter z IN in ALI vrati. Včasih se morajo določeni elementi ali osnovni dogodki pojaviti skupaj, da bi lahko povzročili glavni dogodek.



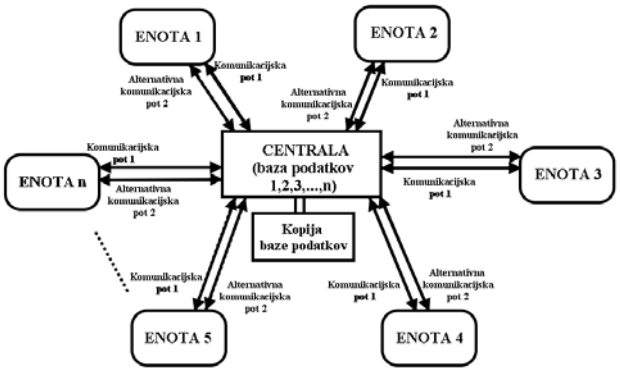
Slika 2: Primer enostavnega drevesa napak (FTA) [1-2]

Z drevesom okvar si pomagamo pri določanju možnih scenarijev na podlagi vzroka in posledice.

3. Zasnova sistema

Zgoraj opisana skupina metod je pomembna pri samem načrtovanju sistema in je dobro upoštevati rezultate obeh metod pri nadaljnjem razvoju, da se poveča nivo zanesljivosti sistema. Pomembno pri tem je tudi, da je sistem

fleksibilen in prilagodljiv v primeru zapiranja in odpiranja posameznih delov sistema, če se recimo ukine en center in odpre novi. Slika 3 prikazuje okvirno postavitev sistema.

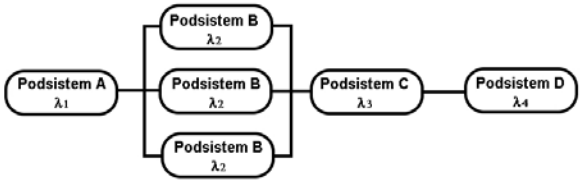


Slika 3: Okvirna zasnova zgradbe sistema

Vsaka enota ima dostop do centrale po eni komunikacijski poti in v primeru odpovedi le-te možnost dostopa in neprekinjen prenos podatkov po drugi alternativni poti, ki je neodvisna od delovanja prve (dvojna ali možnost tudi trojne redundance). Ti podatki so nato tudi dostopni vsaki aktivni enoti.

Nekaj veličin in atributov, ki imajo pomembno vlogo in jih je dobro upoštevati pri zasnovi sistema za pomoč ob klicu v sili je opisanih spodaj.

Pogostost odpovedi je parameter, ki nam poda frekvenco odpovedi sistema in se ponavadi lahko izrazi v številu odpovedi/uro. V praksi se pogosteje uporablja recipročni parameter MTBF (Mean Time Between Failure) za komponente in sisteme višje kakovosti.



Slika 4: Uvedba redundanc

Pri načrtovanju zanesljivosti sistema so pomembne ***redundančne poti***, kar se v veliki meri izkaže tudi s FME(C)A metodo. To pomeni, da se kritične dele sistema ali povezave podpre z dodatnimi moduli v sistemu. Grafično je predstavljen sistem redundanc na sliki 4.

Razpoložljivost je verjetnost, da bo naprava v nekem trenutku oz. časovnem obdobju pod določenimi pogoji uporabe, določenimi vplivi okolja ter določenim vzdrževanjem v stanju delovanju. Stopnja želene razpoložljivosti sistema je tesno povezana s ceno izpada sistema. Stroški, ki nastanejo ob nedelovanju sistema, so ponavadi mnogo večji, kot so stroški, ki jih povzroči nabava dodatne opreme, s katero se poveča razpoložljivost. Maksimalno razpoložljivost sistema in odpornost v primeru napak je moč zagotoviti z redundančnostjo posameznih delov sistema ter dodatnimi orodji, ki sproti preverjajo delovanje posameznih komponent. Razpoložljivost sistema je določena s sledečo enačbo (1).

$$A = \frac{MTBF}{MTBF + MTTR} \qquad (1)$$

A razpoložljivost sistema
MTBF povprečen čas med dvema okvarama
MTTR povprečen čas odprave okvare oziroma napake

Informacijsko komunikacijska infrastruktura centrov za obveščanje mora biti načrtovana in opremljena za zagotavljanje visoke stopnje razpoložljivosti. Cilj je v dosegu razpoložljivosti 99,999 %, kar pomeni tako načrtovan kot nenačrtovan izpad za največ približno 5 min/leto. Dosegati razpoložljivosti 99,999 % je možno samo s skrbnim načrtovanjem, profesionalno opremo in podvajanjem posameznih komponent. Poznati je potrebno delovanje celotnega sistema, določiti cilje in algoritme in na osnovi zadanih ciljev identificirati tiste komponente sistema, ki jim je potrebno posvetiti največjo pozornost (najnezanesljivejši člen) [1-4].

Upoštevati je potrebno tudi ***modularnost*** sistema pri samem načrtovanju, kar pomeni, da je sistem zasnovan tako, da se v primeru pojava napake, poškodovani modul, ki je nepopravljiv, enostavno zamenja z drugim modulom in v tem

času prevzame funkcijo drug modul ter se s tem zagotovi nemoteno delovanje sistema [1] – [6].

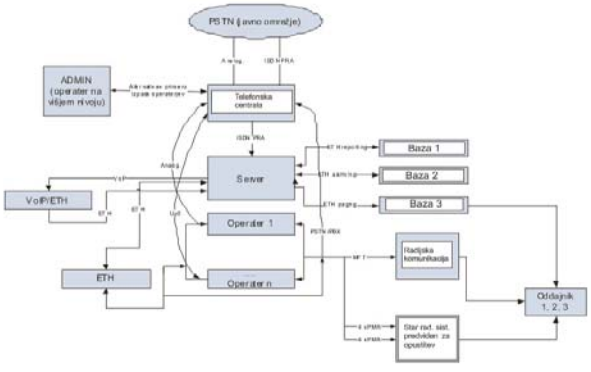
Vzdrževanje je ključ do uspešnega poslovanja v vseh okoljih. Po osnovni definiciji je ***vzdrževalnost*** verjetnost, da se izdelek iz stanja okvare vrne v stanje obratovanja v določenem času. Postopek zagotavljanja vzdrževalnosti izdelka je strukturiran proces, ki se izvaja vzporedno in v povezavi z ostalimi postopki.

MTTR (Mean Time To Repaire) je najbolj razširjeno merilo vzdrževalnosti. Predstavlja povprečen čas potreben za vzdrževalna dela na vseh delih sistema.

4. Blokovni diagrami

Zanesljivostni blokovni diagram (Reliability Block Diagram) je močno odvisen od definicije odpovedi in se lahko razlikuje od shematskega diagrama sistema. Z določanjem zanesljivosti začnemo s posameznimi moduli, ki jih nato združimo v večje sklope.

Zanesljivostni blokovni diagram je grajen nivojsko od zgoraj navzdol. Vključuje vse sklope oz. podsisteme, ki so potrebni za izvajanje predpisane funkcije sistema. Vsak podsistem vključuje skupek sestavov, ki so zgrajeni iz komponent. Vsak element ima samo dve stanji (delovanje, napaka) in samo en način odpovedi. Tako lahko na podlagi vrednosti zanesljivosti določimo tudi skupno zanesljivost sistema, ki ga lahko predstavimo s spodnjim blokovnim diagramom [1] - [6].



Slika 5: Blokovni diagram začetne zasnove funkcij sistema

Za zanesljivost posameznega modula je največkrat uporabljena eksponentna funkcija (2), ki pada s časom delovanja ter je odvisna od parametra MTBF (srednjega časa med posameznimi odpovedmi) [1] - [6].

$$R_s = e^{\frac{-t}{MTBF}} \qquad (2)$$

Upoštevati pa je potrebno, da je pri modulih z visoko zanesljivostjo skupna zanesljivost zmanjšana zaradi vpliva člena, ki ima nižjo zanesljivost, saj je veriga tako zanesljiva, kot je zanesljiv njen najšibkejši člen.

Za povečanje razpoložljivosti računalniškega sistema se uporabljajo visoko razpoložljive računalniške gruče (High Availability Clusters - HA Clusters). Te uporabljajo redundančne strežnike oz. vozlišča, ki zagotavljajo izvajanje programskih servisov pri izpadu določenega računalnika. Razlog za vpeljavo in uporabo HA gruč je povečanje razpoložljivosti in zanesljivosti delovanja sistema. Strežniška gruča zagotavlja nemoteno delovanje sistema v primeru sledečih izpadov [3] - [8]:

- aplikacijski in servisni izpad,
- izpad opera. sistema in strojne opreme,
- izpad specifičnega območja v krajevno porazdeljenem sistemu.

Kakovost izračunanih parametrov zanesljivosti je odvisna predvsem od kakovostnih vhodnih podatkov za komponente, pa tudi module sistema. To so podatki o njihovi pogostosti odpovedi λ(t), srednjem času do prve odpovedi MTTF, srednjem času med dvema odpovedima MTBF, srednjem času popravila MTTR in intenzivnosti popravila μ [1] - [8].

Najbolj verodostojen vir podatkov za izračune bi morali biti proizvajalci komponent in/ali elementov, iz katerih je sistem sestavljen. Glede na to, da morajo svoje izdelke testirati in na nek način tudi spremljati v njihovi uporabi, bi morali tudi organizirati vire teh podatkov. Mogoče, vendar manj zanesljivo glede kakovosti podatkov, je iskanje s pomočjo literature. V tem primeru gre za standarde (IEC, ETSI, IEEE, ITU), priročnike (MIL - HDBK -

217) in ostalo literaturo (knjige, članke). V takih primerih se pogosto zgodi, da so podatki za istovrstne komponente ali elemente iz različnih virov zelo različni [9].

Ob tem velja posebej omeniti pogosto citirani ameriški priročnik MIL - HDBK - 217 (Military Standardization Handbook 217), predvsem zaradi sistematike tvorbe vhodnih podatkov pogostosti odpovedi $\lambda(t)$. Gre predvsem za elemente in nekatera vezja v elektroniki. Običajno je podana osnovna (bazna) pogostost odpovedi $\lambda_b(t)$, v kateri so že upoštevani določeni pogoji (npr. osnovne napetostne in temperaturne obremenitve). Dokončno določitev podatka $\lambda(t)$ pa opravi uporabnik sam z upoštevanjem faktorjev, ki za določen modul zajemajo ostale predvidene vplive, ki so specifični za komponento in za okolje, v katerem sistem opravlja svojo funkcijo. Ti faktorji so izbrani skladno z ugotovljenimi pogoji prav tako v tem priročniku. Vsekakor mora uporabnik zelo dobro poznati tudi razmere, v katerih bo sistem deloval, da bo končni vhodni podatek za izračun kakovosten [9].

Za zagotavljanje visoke stopnje razpoložljivosti centrov za obveščanje je potrebno posvetiti posebno pozornost izpadom sistemske in aplikativne programske opreme, ki lahko nastane bodisi zaradi neodkritih programskih napak, zaradi zlonamernih vdorov ali zaradi rednega vzdrževanja programske opreme. Izpadi zaradi neodkritih programskih napak ter vdori v sistem so nenačrtovani in lahko nastopijo v vsakem trenutku, medtem ko so redna vzdrževalna dela načrtovana. Da takšni izpadi ne vplivajo na razpoložljivost celotnega sistema mora biti sistem toleranten do napak. To lahko dosežemo z grupiranjem, kjer izpad posameznega vozlišča v grupi ne vpliva na razpoložljivost sistema kot celote, ker ostala vozlišča v grupu prevzamejo njegovo funkcijo. Za zagotavljanje razpoložljivosti sistema v primeru naravnih nesreč pa je smiselno uporabiti geografsko redundačen in neodvisen sistem, ki ga najlažje dosežemo s podvajevanjem podatkovne baze [1] - [8].

5. Zaključek

V fazi načrtovanja razvoja sistema je potrebno zmanjševati kompleksnost sistema, vključiti podvajanje za dosego večje tolerance napak, omiliti stresne dejavnike, kvalifikacijsko testirati in revizirati načrtovanje ter dobiti povratne informacije o okvarah za zagotavljanje rasti zanesljivosti. V fazi uporabe sistema je potrebno preverjati primernost navodil za uporabo in vzdrževanje, dobiti povratno informacijo o odpovedih med samim delovanjem, ter omogočiti ustrezne servisne dejavnosti. Višja kot je zanesljivost sistema, manjši so stroški odpovedovanja, saj je manj odpovedi. Za doseganje večje zanesljivosti so potrebni večji stroški. Optimizacija zahteva minimum vsote obeh stroškov. Že v samem načrtovanju sistema želimo zvišati stopnjo zanesljivosti, kar pomeni, da moramo zagotoviti čimmanj kasnejših odpovedi, kar pa dosežemo z različnimi metodami načrtovanja zanesljivosti.

6. Literatura

[1] M. Nagode, M. Fajdiga, Efektivnost proizvodov, Univerza v Ljubljani, Fakulteta za strojništvo, 2003.

[2] Marko Topič, Zanesljivost in vzdrževanje komponent in sistemov, Založba FE, Ljubljana, 2002, ISBN: 961-6371-10-X.

[3] ISO/FDIS 9001:2000, Quality management systems – Requirements.

[4] M. Pivka: Management kakovosti, Univerza v Mariboru, Ekonomsko-poslovna fakulteta Maribor, Maribor 2000.

[5] SIST: Napotki za procesni pristop v sistemu vodenja kakovosti, Nasveti in informacije o posodobitvah ISO 9001 in ISO9004, Slovenski inštitut za standardizacijo, Ljubljana, 2003.

[6] Slovenski inštitut za kakovost in meroslovje (SIQ)- http://www.siq.si

[7] Microsoft TechNet. What Is a Server Cluster? [Online]. Available: http://technet2.microsoft.com/windowsserver/en/library/fb47602c-5d03-42aa-a1f1-eaee8406a1b51033.mspx?mfr=true

[8] Chang, H. Y. et. al., Comparison of parallel and deductive fault simulation methods, IEEE Trans. Comput., Vol. C-23, No. 11, pp. 193-200.

[9] Department of Defense - Military Handbook: Reliability predictions of electronic equipment, MIL-HDBK-217. Analysis Center and Rome Laboratory at Griffiss AFB, NY.