Dr. sc. Vinko Tomas
Dr. sc. Dubravko Vučetić
Pomorski fakultet Rijeka
Studentska 2
51000 Rijeka

Pregledni članak
UDK: 629.5.064.5
681.518.5
Primljeno: 12. ožujka 2007.
Prihvaćeno: 20. ožujka 2007.

UTJECAJ DIJAGNOSTIKE NA POUZDANOST I SIGURNOST PROCESNIH KONTROLERA

U ovome radu analizira se utjecaj dijagnostike i redundancije za poboljšanje pouzdanosti i sigurnosti upravljačkih uređaja na brodskim električnim strojevima. Pri projektiranju upravljačkog uređaja važni zahtjevi su sigurnost, pouzdanost i raspoloživost sustava. Ako sustav nema ugrađenu dijagnostiku i redundanciju svaki kvar može dovesti do smanjivanja sigurnosti sustava. Analiziraju se koncepcije samodijagnostike i dijagnostike, mogućnosti primjene samodijagnostike i dijagnostike na različite strukture sistema, te utjecaj na pouzdanost i sigurnost sistema upravljanja, a time i na pouzdanost i sigurnost brodskog elektroenergetskog sistema u cjelini. Problem se analizira s dva aspekta. Prvo, koriste se kombinirane tehnike modeliranja za procjenu poboljšanja pouzdanosti i sigurnosti kada se uključuje redundancija u sustav. Drugo, koristi se Markovljev model u istraživanju sigurnosnog aspekta određene arhitekture za projektiranje redundantnog dijagnostičkog sustava. Na taj način vrši se vrednovanje mogućih rješenja kojima se brodska elektroenergetska postrojenja mogu voditi uz znatno povoljniju bezotkaznost (toleriranje grešaka), i analizira se utjecaj kvalitete dijagnostike na ta rješenja.

Ključne riječi: *dijagnostika, brodsko elektroenergetsko postrojenje, pouzdanost, sigurnost, toleriranje otkaza*

1. UVOD

Upravljački uređaj koji se analizira u ovome radu upravlja radom motora u brodskom elektroenergetskom postrojenju. Osnovni dijelovi ovoga sustava su: upravljački senzori, elektronika na samom motoru, mjerni senzori parametra motora i sam motor. Najvažniji element ovoga sustava je upravljački uređaj-kontroler, koji obavlja obradu signala. Pri projektiranju upravljačkog uređaja važni zahtjevi su sigurnost, pouzdanost i raspoloživost sustava.

Analizirajući utjecaje sigurnosti i pouzdanosti na uređaje s redundancijom i bez redundancije, prvo se razmatra izračunavanje pouzdanosti i raspoloživosti kontrolera koji nemaju redundancije. Svakoj komponenti sustava može se pridružiti učestalost kvara λ. Pouzdanost neredundantnog sustava može se modelirati kao [2,9]:

$$_{sustava}(t) = e^{-\lambda_{us}t} e^{-\lambda_p t} e^{-\lambda_k t} e^{-\lambda_e t} e^{-\lambda_e t} e^{-\lambda_s t} e^{-\lambda_s t} e^{-\lambda_{ms} t} e^{-\lambda_{ms} t} = e^{-\lambda_{su}},$$

gdje je učestalost kvarova: λ_{us} – upravljačkog senzora; λ_p – pokazivača; λ_k – kontrolera; λ_e – elekronike na stroju; λ_{ms} – mjernog senzora; λ_s – stroja i $\lambda_{sus} = \lambda_{up} + \lambda_p + \lambda_k + 2\lambda_e + 2\lambda_s + 2\lambda_{ms}$.

Tipične vrijednosti za učestalost kvarova navedenih brodskih komponenti su (uz pretpostavku da se radi o računalnom upravljanju: $\lambda_{us} = 1 \cdot 10^{-6}$, $\lambda_p = 1 \cdot 10^{-6}$, $\lambda_k = 3.5 \cdot 10^{-4}$, $\lambda_e = 5 \cdot 10^{-5}$, $\lambda_s = 1 \cdot 10^{-6}$ i $\lambda_{ms} = 10^{-6}$ otkaza na sat [8]. Prema tome imamo da je ukupna pouzdanost sustava uzimajući gornje podatke za učestalost grešaka:

$$R_{sustava}(t) = e^{-4,56 \cdot 10^{-4} t}.$$

Drugi pristup pouzdanosti sustava je korištenje srednjeg vremena do otkaza MTTF [2,4,5]. Matematički rečeno ako je X promatrana slučajna varijabla-vrijeme do otkaza, MTTF je matematičko očekivanje EX ove varijable. Po definiciji je:

$$EX = \int_{-\infty}^{+\infty} t dF_x(t),$$

gdje je $F_x(t)$ funkcija razdiobe (distribucije) X. Kako je X nenegativna, vrijedi sljedeći rezultat:

$$X = \int_{-\infty}^{+\infty} t dF_x(t) = \int_{-\infty}^{0} t dF_x(t) + \int_{0}^{+\infty} t dF_x(t) = -\int_{0}^{+\infty} t d(1 - F_x(t)) = -\int_{0}^{+\infty} t dR(t) =$$

koristeći parcijalno integriranje slijedi:

$$u = t \rightarrow du = dt$$
$$dR(t) = dv \rightarrow v = R(t)$$

$$H = -\int_{0}^{+\infty} tR(t) + \int_{0}^{+\infty} R(t)dt.$$

Preostalo je još pokazati da je:

$$\lim_{t\to\infty} tR(t) = 0 \ .$$

Pri tome koristimo sljedeće:

"neka je ξ slučajna varijabla s $E|\xi|^r < \infty$. Tada je $\lim_{t\to\infty} t^r P\{|\xi| \ t\} = 0$" .

Kako je X nenegativna varijabla, pa je

$$\lim_{t\to\infty} t^r P\{\xi \ t\} = \lim_{t\to\infty} tR(t) = 0,$$

što je i trebalo dokazati, (slučaj $r \neq 1$ vidi u [7; Propozicija 10.13.]). Dakle, slijedi

$$EX = \int_0^{+\infty} R(t)dt \ .$$

U našem slučaju je $X \sim \varepsilon(\lambda)$, tj. vrijeme do prvog otkaza ima eksponencijalnu razdiobu s parametrom $\lambda > 0$, pa je:

$$MTTF = EX = \frac{1}{\lambda} .$$

Za neredundantni sustav s eksponencijalnom razdiobom slijedi:

$$MTTF = EX = \frac{1}{\lambda} = 2192 \text{ sati} \ .$$

Za razmatrani slučaj zaključujemo da će sustav biti u funkciji u prosjeku samo 2192 sata prije pojave prvog kvara.

Nadalje se analizira raspoloživost sustava, tj. postotak vremena u kojem je sustav raspoloživ izvršavati svoju funkciju. Raspoloživost se mijenja s vremenom, a njegova stacionarna vrijednost je:

$$A = \frac{MTTF}{MTTF + MTTR} = \frac{\frac{1}{\lambda}}{\frac{1}{\lambda} + \frac{1}{\mu}} = \frac{1}{1 + \frac{\lambda}{\mu}} ,$$

gdje su: MTTF - srednje vrijeme do otkaza, MTTR - srednje vrijeme do popravka, λ - učestalost kvarova i μ - učestalost popravaka.

Ako je srednje vrijeme potrebno za popravak jedan tjedan, dobivamo da je raspoloživost nešto veća od 0,92. Nažalost projektanti imaju malo utjecaja na učestalost popravaka brodskih uređaja i strojeva. Učestalost popravaka ovisi o mogućnostima korisnika da dijagnosticira problem ili blizinu odgovarajućeg

servisa ako su korisnici prisiljeni čekati ovlašteni servis (dolazak u određenu luku), period popravaka može se produžiti na puno više od jednog tjedna. Da bi se prevladali ti problemi mnogi korisnici nastoje osigurati rezervne dijelove. To je skupi način koji se može izbjeći kroz razvoj sustava s manjom učestalošću kvarova ili onog sustava koji ima ugrađenu dijagnostiku i redundanciju tako da sustav prevlada kvarove do zamjene neispravne komponente.

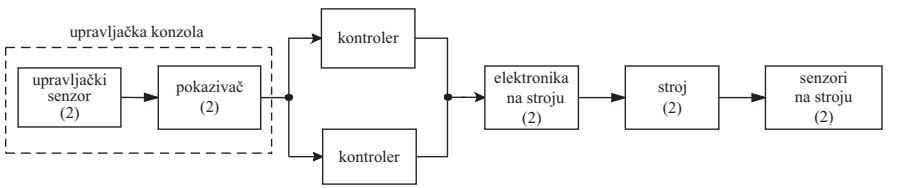
2. DOPRINOSI UGRADNJOM DIJAGNOSTIKE I REDUNDANCIJE

Kao sljedeći korak, ispituju se poboljšanja u sustavu dobivena upotrebom redundancije i dijagnostičkog sustava koji osigurava detekciju, lokalizaciju i toleranciju kvara. Pouzdanost možemo poboljšati ako sustav ima mogućnost toleriranja grešaka koje mogu uzrokovati otkaz sustava. Na primjer, ako dođe do odstupanja vrijednosti napajanja, kontroler može biti projektiran da automatski isključi napajanje i tako spriječi oštećenja strujnih krugova stroja (npr. motora u brodskom elektroenergetskom postrojenju) i da ponovo uključi napajanje kada se stvore zato predviđeni uvjeti.

Raspoloživost može biti poboljšana upotrebom redundancije i dijagnostike koja omogućuje popravak sustava u radnom režimu. Sigurnost može biti poboljšana kroz ugradnju dijagnostike koja osigurava siguran rad sustava. Ako dođe do greške mora postojati način da se detektira postojanje neispravnosti i onemogući da greška uzrokuje neželjeno ponašanje sustava upravljanja.

Kod uvođenja redundancije treba imati u vidu više parametara: učestalost grešaka, dimenzije, cijenu itd., zbog toga u promatrani sustav ima smisla uvesti redundanciju na mjestu kontrolera. Strojevi, elektronika na strojevima i senzori su često preveliki i skupi da bi se duplirali [1,8].

Sustav je dvoredundantan oba procesorska modula izvršavaju iste proračune i svaki je sposoban funkcionirati kao kontroler u sustavu. Ugrađena dijagnostika kroz različite oblike detekcije grešaka omogućava rekonfiguraciju. Procesorski moduli uspoređuju rezultate u određenom dijagnostičkom intervalu da bi izvršili detekciju greške. Analizom redundantnog kontrolera procijenit ćemo poboljšanja koja mogu biti postignuta u pouzdanosti i raspoloživosti sustava.



Slika 1. Blok dijagram pouzdanosti sustava upravljanja s redundantnim kontrolerom [8]

Blok dijagram pouzdanosti redundantnog sustava prikazan je na slici 1., pa je pouzdanost redundantnog sustava

$$R_{sustava}(t) = R_{uk}(t)R_{pk}(t)R_{e}(t)R_{ms}(t)R_{s}(t),$$

gdje je pouzdanost: $R_{uk}(t)$ –upravljačke konzole (serijski dva ulazna senzora); $R_{pk}(t)$ – paralelne kombinacije kontrolera; $R_{e}(t)$ – serijske elektronike na stroju; $R_{ms}(t)$ – serijskih elemenata od dva mjerna senzora; $R_{s}(t)$ – serijskih elemenata od dva stroja.

Poznato je da pokrivanje grešaka C ima značajnu ulogu u pouzdanosti paralelnih sustava i sveukupnoj raspoloživosti sustava upravljanja [3,8]. Upotrebljavajući tehnike za procjenu sustava, pouzdanost $R_{p}(t)$ može se napisati kao [2,4]:

$$R_{pk}(t) = R_{k}(t) \times R_{k}(t) + 2CR_{k}(t)\left[1 - R_{k}(t)\right],$$

gdje je $R_{k}(t)$ – pouzdanost neredundantnog modula, C je matematički definirano kao uvjetna vjerojatnost obnavljanja sistema pod uvjetom da se greška detektirala, što se može pisati kao: C = P(sistem obnovljen | greška postoji).

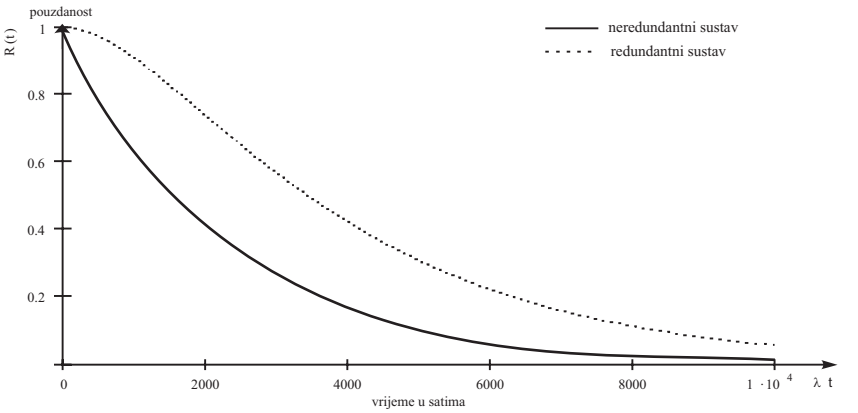
Zbog pretpostavke da za svaki element sustava upravljanja važi eksponencijalni zakon razdiobe otkaza, pouzdanost cijelog sustava je:

$$R_{sustava}(t) = e^{-\lambda_1 t}\left[e^{-2\lambda_k t} + 2Ce^{-\lambda_k t}(1 - e^{-\lambda_k t})\right],$$

gdje je $\lambda_1 = \lambda_{up} + \lambda_p + 2\lambda_e + 2\lambda_s + 2\lambda_{ms}$, λ_k je pouzdanost za neredundantni modul.

Ako je C=1 sustav se može obnoviti od svih grešaka koje se mogu eventualno dogoditi. Vidimo da faktor pokrivenosti greške može imati značajan utjecaj na pouzdanost sustava.

Na slici 2. prikazana je pouzdanost za redundantni i neredundantni sustav kada je pokrivenost greške 0,95 (što se može pretpostaviti kao realna mogućnost uz dobar dijagnostički podsustav [9]). Na početku rada poboljšanja pouzdanosti koja su dobivena upotrebom redundancije nisu velika. Kako vrijeme prolazi povećava se mogućnost kvara i poboljšanja u pouzdanosti postaju veoma značajna. Daljnjim prolaskom vremena poboljšanja u pouzdanosti se počinju smanjivati.. Na primjer, za 500 sati pouzdanost redundantnog sustava je 0,9184, dok je pouzdanost neredundantnog pala ispod 0,8, kako vrijeme prolazi poboljšanja u pouzdanosti se smanjuju zato što je redundancijom povećana količina hardvera koja može otkazati.

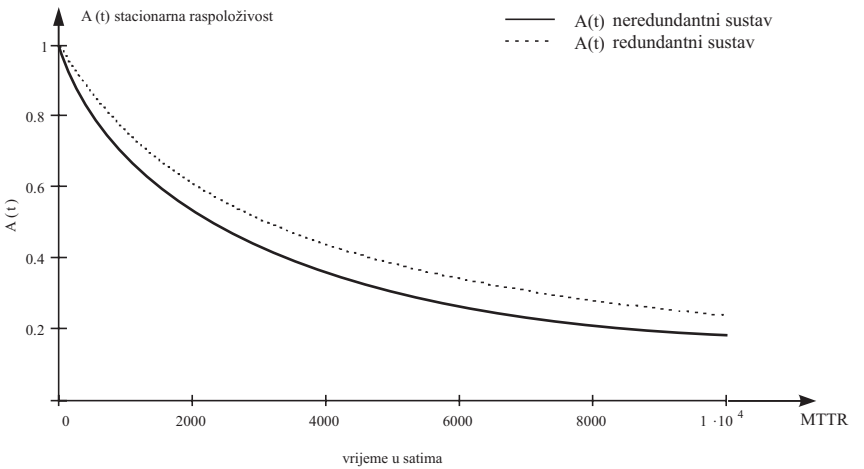


Slika 2. Pouzdanost za redundantni i neredundantni sustav

Raspoloživost se također može poboljšati s ugradnjom redundancije i dijagnostičkih tehnika u fazi projektiranja kontrolera. Da bi se odredila raspoloživost redundantnog sustava, prvo izračunavamo MTTF redundantnog sustava s ugrađenom dijagnostikom [8]:

$$\mathrm{MTTF_{red}} = \int_0^{+\infty} \mathrm{R_{sustava}}(t)dt = \left\{ e^{-\lambda_1 t}\left[e^{-\lambda_k t} + 2Ce^{-\lambda_k t}(1-e^{-\lambda_k t}) \right] \right\} dt \ .$$

Ovaj integral za $C \approx 0.95$ je približno $\mathrm{MTTF_{red}}=3113$ sati, dok je za neredundantni sustav $\mathrm{MTTF_{nered}}=2192$ sata, što znači da se dijagnostika i redundancija poboljšala MTTF za 1,42 puta. Na slici 3. dana je usporedba stacionarne raspoloživosti za redundantni i neredundantni sustav za faktor pokrivenosti C=0,95.



Slika 3. Usporedba stacionarne raspoloživosti

Nadalje analiziramo neke posebnosti ugradnje kontrolera s ugrađenom dijagnostikom i redundancijom u sustav upravljanja. U prethodnom razmatranju pokazani su značajni doprinosi pri ugradnji dijagnostike i redundancije, ali nisu analizirane specifičnosti ugradnje redundancije.

3. SPECIFIČNOSTI UGRADNJE REDUNDANCIJE U KONTROLERE

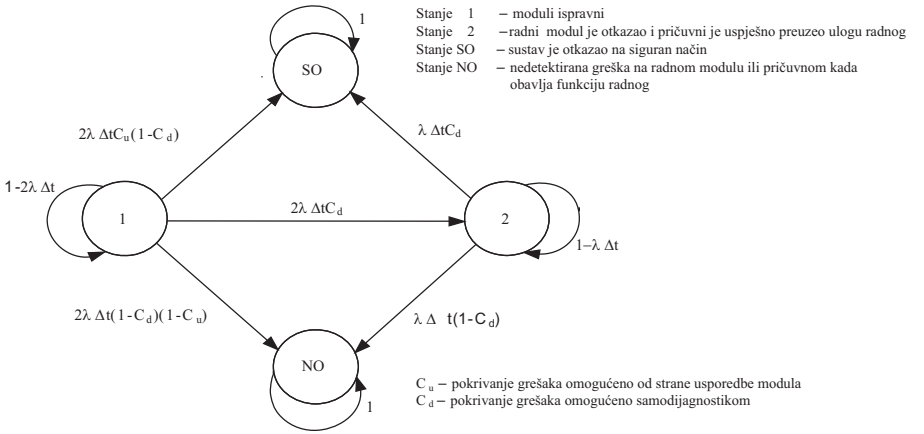
Promatrani dvoredundantni sustav projektiran je da funkcionira na dva načina. Prvi je način već spomenut, gdje oba kontrolera rade istovremeno iste operacije, rezultati se uspoređuju. Svaki modul obavlja samodijagnostiku u slučaju otkrivanja neispravnosti, neispravni modul zaustavlja rad, a kompletne funkcije kontrolera preuzima ispravni modul. Drugi pristup je korištenje jednog modula dok se drugi modul nalazi izvan upotrebe. Kada samodijagnostika otkrije grešku u modulu koji je u upotrebi, tada modul koji je u hladnoj rezervi preuzima funkcije kontrolera.

U fazi projektiranja kontrolera koji mogu uz pomoć dijagnostike i redundancije tolerirati greške, određeni ustupci moraju se učiniti pri odabiru tipa redundantnog sustava koji će biti korišten, zato se analiziraju oba koncepta. Analiza pouzdanosti bit će provedena upotrebom Markovljevih modela. Markovljevi modeli dozvoljavaju fleksibilnost u razmatranju različitih faktora uključujući i proces popravka. Pored toga Markovljevi modeli su jednostavni za konstrukciju i rješavanje [3,5,8]. Jedan od faktora koji je važan je mogućnost analize utjecaja dijagnostike (kroz pokrivanje grešaka) na pouzdanost i raspoloživost. Mogu se razmatrati dva utjecaja na pokrivanje greške u redundantnim sustavima. Prvi je vjerojatnost da će usporedba rezultata redundantnih modula otkriti postojanje neispravnosti, a drugi da će neispravni modul u procesu samodijagnostike ustanoviti kvar i izvršiti rekonfiguraciju. U slučaju da imamo hladnu pričuvu samo će jedan faktor pokrivanja biti prisutan (samodijagnostika).

3.1. Redundantni sustav s toplom pričuvom

Markovljev model redundantnog sustava s toplom pričuvom prikazan je na slici 4. Model sadrži četiri stanja koja predstavljaju sve konfiguracije sustava. Stanje 1 prikazuje slučaj u kojem oba modula ispravno rade. Ovo stanje ranije smo nazvali savršeno stanje i to je stanje u kojem sustav započinje svoj rad. U stanju 2 jedan od dva modula je detektirao neispravnost i nije u funkciji. Stanje SO je stanje sigurnog otkaza, tj. problem je detektiran i prelazak u to stanje je izvedeno na siguran način. U stanju NO (nesiguran otkaz) sustav je otkazao i problem nije detektiran na način koji garantiran

siguran rad sustava. Ako je sustav u stanju NO, moguće su neočekivane i možda nesigurne situacije.



Slika 4. Markovljev model redundantnog sustava s toplom pričuvom

Prijelaz iz stanja 1 u stanje 2 će se dogoditi kada jedan od modula otkaže, a samodijagnostika je detektirala kvar. Otkaz je detektiran i zbog kvara sustav prelazi iz stanja 1 u stanje SO, sustav će biti siguran, ali neće moći izvršavati operacije. Prijelaz iz stanja 1 u stanje NO se događa ako neispravnost nije detektirana od strane samodijagnostike, a niti usporedba rezultata, između modula nije ustvrdila odstupanja. Prijelazi iz stanja 2 posljedica su otkaza zadnjeg ispravnog modula. U tom stanju samodijagnostika je jedini alat za detekciju kvara, ako samodijagnostika detektira problem sustav prelazi u stanje SO, a ako ne sustav prelazi u stanje NO.

Jednadžbe za Markovljev model mogu biti napisane u matičnom obliku [1]:

$$P_{tp}(t + \Delta t) = T_{tp} P_{tp}(t) ,$$

gdje svaki element od $P_{tp}(t)$ je vjerojatnost da je redundantni sustav s **t**oplom **p**ričuvom u određenom stanju u trenutku t. Svaki element od $P_{tp}(t+\Delta t)$ predstavlja vjerojatnost da je sustav u odgovarajućem stanju u vremenu $t+\Delta t$, i T_{tp} je matrica prijelaza. Ovo sve vrijedi uz pretpostavku da je Δt dovoljno malo, tako da se ne mogu simultano dogoditi dva prelaza iz stanja u stanje [6]. To možemo napisati kao:

$$p_{tp}(t+\Delta t) = \begin{bmatrix} p_2(t+\Delta t) \\ p_1(t+\Delta t) \\ p_{SO}(t+\Delta t) \\ p_{NO}(t+\Delta t) \end{bmatrix}$$

$$T_{tp} = \begin{bmatrix} 1 - 2\lambda\Delta t & 0 & 0 & 0 \\ 2\lambda\Delta t C_d & 1-\lambda\Delta t & 0 & 0 \\ 2\lambda\Delta t C_u(1 - C_d) & \lambda\Delta t C_d & 1 & 0 \\ 2\lambda\Delta t (1 - C_d)(1 - C_u) & \lambda\Delta t (1-C_d) & 0 & 1 \end{bmatrix}$$

$$P_{tp}(t) = \begin{bmatrix} p_2(t) \\ p_1(t) \\ p_{SO}(t) \\ p_{NO}(t) \end{bmatrix}$$

Rješavanjem matrične jednadžbe Markovljeva modela možemo dobiti vrijednosti za P(Δt) množenjem vektora početnih vrijednosti P(0) i matrice T_{tp}-matrice prijelaza, a P(2Δt) množenjem P(Δt) i matrice prijelaza T_{tp}. Opće rješenje jednadžbe Markovljeva modela je dano kao

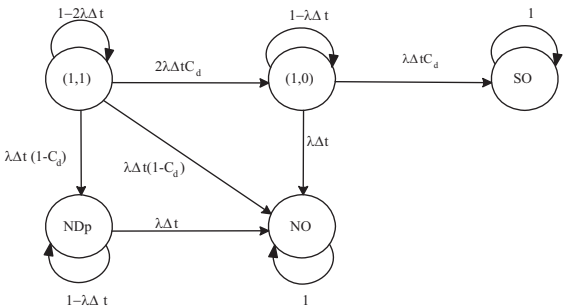
$$P(n \times \Delta t) = T^n P(0) .$$

Pouzdanost redundantnog sustava s toplom pričuvom i ugrađenom dijagnostikom u trenutku t, je vjerojatnost da sustav ispravno radi od početnog trenutka do vremena t. U skladu s Markovljevim modelom pouzdanost redundantnog sustava je vjerojatnost da se sustav nalazi u stanju 1 ili 2 koja su jedina stanja kada sustav ispravno radi. To znači da pouzdanost redundantnog sustava s toplom pričuvom možemo napisati kao zbroj

$$R_{tp}(t) = p_2(t) + p_1(t) .$$

3.2. Redundantni sustav s hladnom pričuvom

Markovljev model redundantnog sustava s hladnom pričuvom može biti konstruiran slično kao redundantni sustav s toplom pričuvom. Na slici 5. prikazan je Markovljev model koji sadrži pet stanja.



Slika 5. Stanja Markovljeva modela za sustav s hladnom pričuvom

Tablica 1. Stanja sustava s hladnom pričuvom [8]

stanje	Definicija stanja sustava
(1,1)	Savršeno stanje, moduli su ispravni
(1,0)	Radni model je otkazao i pričuvni je uspješno postao radni
NDp	Sustav obavlja funkciju - radni modul ispravan. Nedetektiran otkaz u pričuvnom modulu. Može se dogoditi zamjena neispravnog radnog modula s neispravnim pričuvnim modulom
SO	Sustav je otkazao na siguran način - oba modula otkazala korektno
NO	Nedetektirana greška na radnom modulu, ili na pričuvnom modulu kada je on obavljao funkciju radnog. U oba slučaja sustav radi s modulima koji imaju nedetektirane greške

Jednadžbe Markovljeva modela za redundantni sustav s hladnom pričuvom možemo napisati u matičnoj formi [1]:

$$P_{hp}(t+\Delta t) = T_{hp} \times P_{hp}(t) \quad ,$$

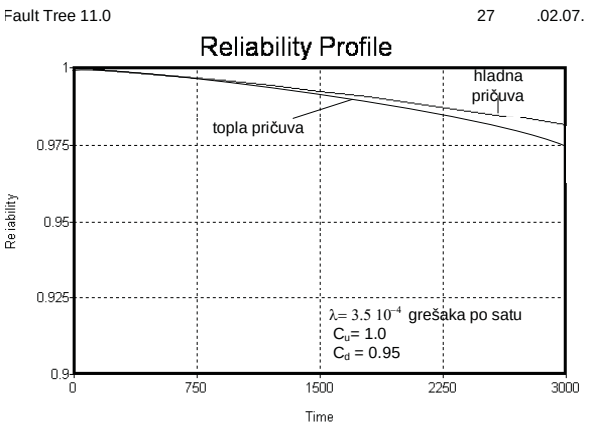
gdje svaki element od $P_{\mathbf{hp}}(t)$ je vjerojatnost da je redundantni sustav s **h**ladnom **p**ričuvom u određenom stanju u trenutku t. Svaki element od $P_{hp}(t+\Delta t)$ predstavlja vjerojatnost da je sustav u odgovarajućem stanju u vremenu $t+\Delta t$, i T_{hp} je matrica prijelaza. To možemo napisati kao:

$$P_{hp}(t) = \begin{bmatrix} P_{(1,1)}(t) \\ P_{(1,0)}(t) \\ P_{(SO)}(t) \\ P_{(NO)}(t) \\ P_{(NDp)}(t) \end{bmatrix} \qquad P_{hp}(t+\Delta t) = \begin{bmatrix} P_{(1,1)}(t+\Delta t) \\ P_{(1,0)}(t+\Delta t) \\ P_{(SO)}(t+\Delta t) \\ P_{(NO)}(t+\Delta t) \\ P_{(NDp)}(t+\Delta t) \end{bmatrix}$$

$$T_{hp} = \begin{bmatrix} 1 - 2\lambda\Delta t & 0 & 0 & 0 & 0 \\ 2\lambda\Delta t \times C_d & 1 - \lambda\Delta t & 0 & 0 & 0 \\ 0 & \lambda\Delta t C_d & 1 & 0 & 0 \\ \lambda\Delta t(1 - C_d) & \lambda\Delta t(1 - C_d) & 0 & 1 & l\Delta t \\ \lambda\Delta t(1 - C_d) & 0 & 0 & 0 & 1 - \lambda\Delta t \end{bmatrix}$$

Sustav s hladnom pričuvom ima tri radna stanja: stanje (1,1), stanje (1,0) i stanje (NDp). Pouzdanost toga sustava možemo napisati kao:

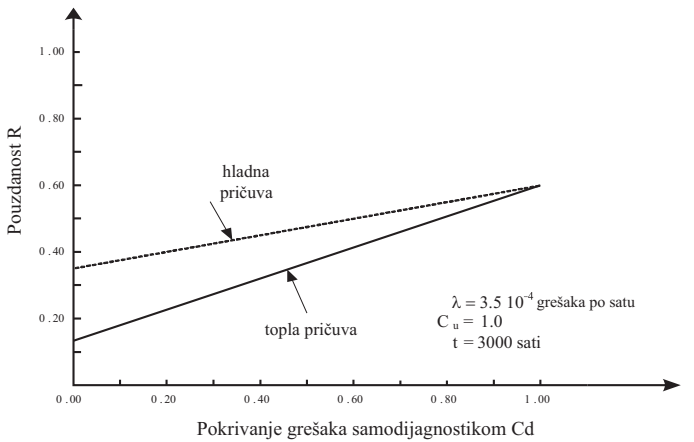
$$R_{hp}(t) = p_{(1,1)}(t) + p_{(1,0)}(t) + p_{(NDp)}(t) .$$



Slika 6. Pouzdanost redundantnog sustava s hladnom i toplom pričuvom

Iz Markovljevog modela vidi se da pouzdanost ovisi o učestalosti otkaza, faktora pokrivanja greški i vremena. Radi usporedbe pretpostavimo da je učestalost kvarova $\lambda = 3{,}5 \cdot 10^{-4}$, pokrivanje grešaka omogućeno od strane usporedbe modula $C_u = 1$, tj. savršeno, i samodijagnostika ima pokrivanje greške $C_d = 0{,}95$. Upotrebom Markovljevog modela možemo pouzdanost oba sustava izračunati u funkciji vremena. Slika 6. daje usporedni prikaz pouzdanosti ta dva

sustava uz zadanu učestalost kvarova i pokrivanja grešaka, proračun je obavljen korištenjem programa [3,5]. Za vrlo visoko pokrivanje grešaka, pouzdanost ova dva pristupa je približno ista. Vrijednost faktora pokrivanja grešaka ima važan utjecaj na pouzdanost sustava.



Slika 7. Pouzdanost redundantnog sustava s hladnom i toplom pričuvom u funkciji C_d

Slika 7. daje pouzdanost kao funkciju faktora pokrivenosti greške C_d. Za danu pouzdanost modula redundantni sustav s hladnom pričuvom postiže veću pouzdanost od sustava s toplom pričuvom. Pouzdanost redundantnog sustava s toplom pričuvom je jednaka vjerojatnosti da su oba modula ispravna, jer proces usporedbe može detektirati postojanje greške, a ne može odrediti njen uzrok [2]. Ako samodijagnostika nema pokrivanje grešaka (C_d=0) svaka greška će rezultirati otkazom sustava.

Usporedimo li ova dva koncepta samo po pouzdanosti mogli bi zaključiti da je bolje upotrijebiti redundantni sustav s hladnom pričuvom. U mnogim primjenama pouzdanost nije jedini uvjet koji nastojimo zadovoljiti. U mnogim slučajevima projektant nastoji osigurati veliku vjerojatnost da sustav kod otkaza, otkaže na siguran način [10,11].

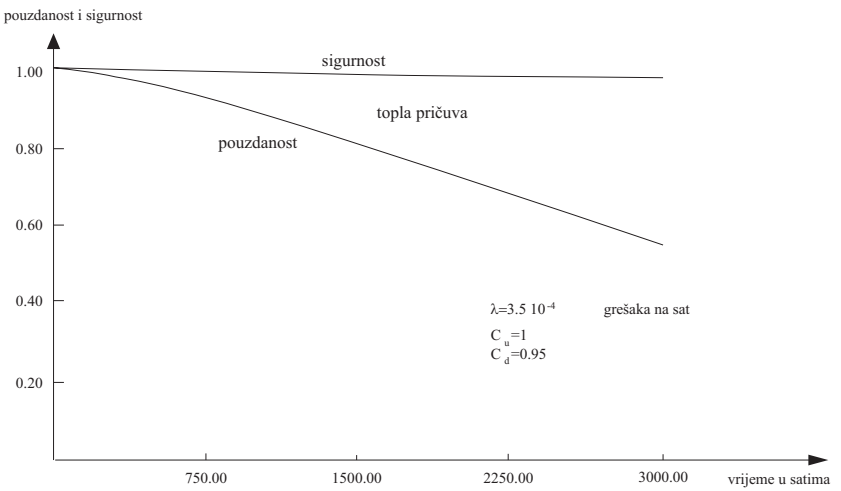
4. UTJECAJ DIJAGNOSTIKE I REDUNDANCIJE NA SIGURNOST

Sigurnost je vjerojatnost da će sustav ili izvršiti svoje funkcije ili će prekinuti svoje funkcije na siguran način [2,4]. S obzirom na Markovljev model sustav s toplom pričuvom prikazan na slici 6. bit će siguran sve dok je u jednom od tri stanja: 1, 2 i SO. Stoga sigurnost sustava s toplom pričuvom S_{tp} možemo opisati kao:

$$S_{tp}(t) = p_2(t) + p_1(t) + p_{SO}(t),$$

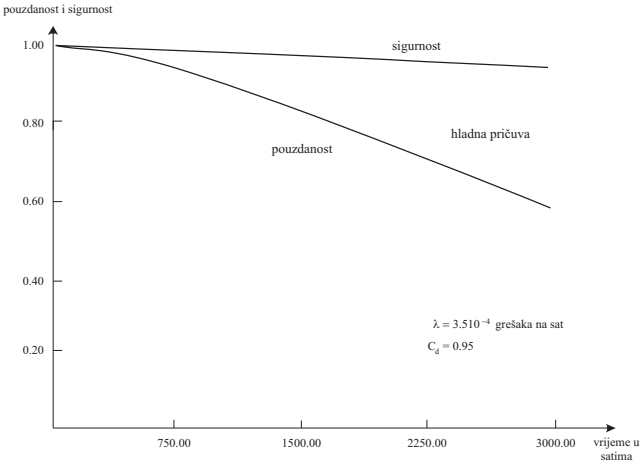
sigurnost sustava s hladnom pričuvom S_{hp} možemo opisati na sličan način kao

$$S_{hp}(t) = p_{(1,1)}(t) + p_{(1,0)}(t) + p_{(SO)}(t) + p_{(NDp)}(t).$$



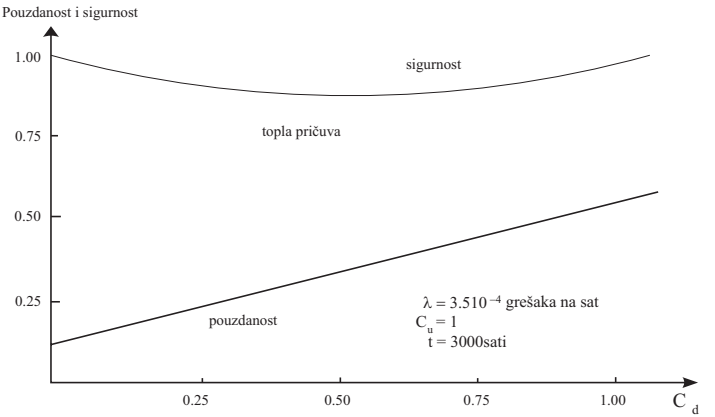
Slika 8. Pouzdanost i sigurnost sustava s toplom pričuvom

Slika 8. i slika 9. prikazuju pouzdanost i sigurnost na obje analizirane arhitekture u funkciji vremena. Vidimo da je sigurnost oba sustava značajno veća od pouzdanosti. Da bi lakše proučili sigurnost, učestalost kvarova i pokrivanje grešaka usporedbom rezultata modula - C_u smatra konstantnim, a pokrivanje grešaka dijagnostikom - C_d promjenljivim. Neka je učestalost kvarova $\lambda = 3{,}5 \cdot 10^{-4}$ grešaka po satu, pokrivanje grešaka usporedbom rezultata $C_u = 1$ (savršeno) izabrano vrijeme t=3000 sati.



Slika 9. Pouzdanost i sigurnost sustava s hladnom pričuvom u funkciji vremena

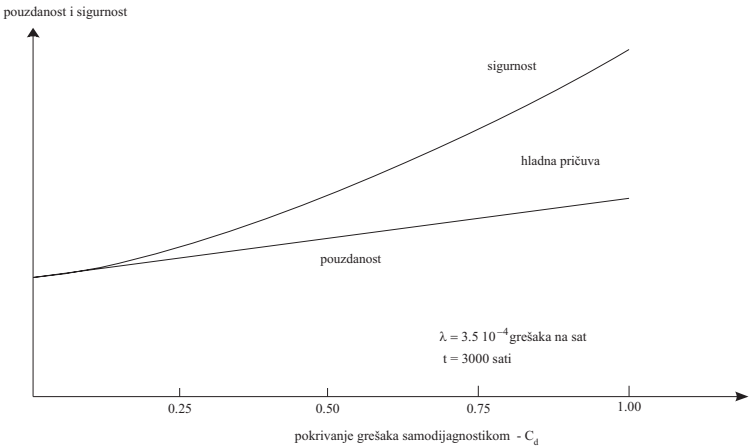
Slike 10. i 11. pokazuju kako se pouzdanost i sigurnost dva sustava mijenja u funkciji mogućnosti samodijagnostike. Sigurnost i pouzdanost sustava s hladnom pričuvom su jednake kada nema pokrivanja grešaka od strane samodijagnostike. Taj sustav ovisi o samodijagnostici da bi ostvario bilo kakvu sigurnost. Sigurnost sustava s toplom pričuvom ima nekoliko interesantnih pojava. Kako se pokrivanje grešaka od strane samodijagnostike povećava od nule do približno 0.5, sigurnost sustava se smanjuje.



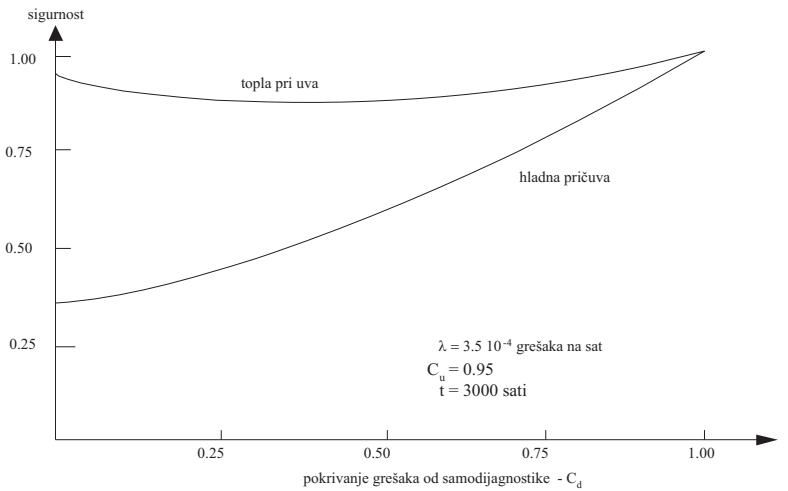
Slika 10. Pouzdanost i sigurnost sustava s toplom pričuvom u funkciji pokrivanja grešaka

To se može objasniti na sljedeći način: kada je pokrivenost grešaka od samodijagnostike nula, sustav se ne rekonfigurira, stoga što se greška ne može

locirati. Proces komparacije modula u tom slučaju je savršen zbog toga će pogreška uvijek biti utvrđena i sigurnost sustava osigurana. Kako se samodijagnostika poboljšava, neke od grešaka bit će locirane i sustav će biti rekonfiguriran, nakon čega sustav ovisi o samodijagnostici, da održi sigurnost. Kada je samodijagnostika slaba, tj. (C_d< 0,5) sigurnost sustava je kompromitirana.



Slika 11. Pouzdanost i sigurnost sustava s hladnom pričuvom u funkciji C_d



Slika 12. Usporedba sigurnosti sustava s toplom i hladnom pričuvom u funkciji C_d

Upotreba usporedbi rezultata između modula nije idealna u najvećem broju primjena, zbog pojava kao što su višestruke greške i načina na koji je usporedba izvedena. Zbog toga proces usporedbe rezultata između modula može biti izveden ignoriranjem nekoliko manje značajnih bitova ili izračunavanjem razlike između dvije vrijednosti i izvođenjem procjene težine odstupanja. Ako ta razlika značajno prelazi maksimalno dozvoljeni nivo, usporedba nije uspješna. To se ogleda u nešto slabijem postotku pokrivanja. U praksi usporedba može biti $\leq 0{,}95$. Slika 12. pokazuje sigurnost za oba sustava u funkciji pokrivanja grešaka od strane samodijagnostike (C_d), uz pretpostavku pokrivanja grešaka od procesa usporedbe rezultata između modula $C_u = 0{,}95$. Kao što vidimo sustav s toplom pričuvom ima puno veću sigurnost od sustava s hladnom pričuvom.

5. ZAKLJUČAK

Iako sustav s hladnom pričuvom ima veću pouzdanost za dano samodijagnostičko pokrivanje grešaka od sustava s toplom pričuvom, zbog zahtijevane veće sigurnosti, u primjenama na brodu ipak treba koristiti sustav s toplom pričuvom.

Važnost sigurnosti sustava je utjecala na potiskivanje ocjene pouzdanosti sustava, zato što i najpouzdaniji sustav nije najpoželjniji u aplikacijama koje zahtijevaju visoku sigurnost rada, u takve aplikacije sigurno spadaju brodska elektroenergetska postrojenja.

U radu su napravljene usporedbe sigurnosti i pouzdanosti na konkretnim sustavima. Analiza je pokazala važnost uvažavanja više faktora tijekom faze projektiranja distribuiranog dijagnostičkog sustava.

LITERATURA

[1] Designing Safe, Reliable Systems Using SCADE, In symposium on leveraging applications of formal methods ISoLA 2004, 2004.
[2] E. Helix Inc.,System Reliability and Availability Calculation, Gaithersburg, Maryland USA, 2003, www.eventhelix.com
[3] Isograph Reliability Software FaultTree+ V 11 version, 2006.
[4] Johnson, B. W., Aylor J.H., Reliability and safety analysis of a fault-tolerant controller", IEEE Transactions on Reliability, Vol. R-35, 1989., 4, str. 355-362.
[5] Markov Analysis Software – MKV Version 3.0, Copyright (C) 2004, Sencer Yeralan
[6] Petrović, R., M. Vujošević, D. Petrović, Optimizacija redundantnih sistema, Beograd, Saobraćajni fakultet, 1993.
[7] Sarapa, N., Teorija vjerojatnosti, Zagreb, Školska knjiga, 1987.
[8] Tomas,V., Model distribuiranog dijagnostičkog sistema brodskih elektroenergetskih postrojenja, doktorska disertacija, Rijeka, V. Tomas, 2003.

[9] Tomas, V., Tehnike toleriranja kvarova u dijagnostičkom sistemu, Pomorstvo, 18(2004), str. 137-146.
[10] Tomas,V., I. Šegulja, D. Čišić, Mogućnosti i problemi primjene suvremenih strategija održavanja u pomorstvu, Pomorstvo, 19(2005), str. 29-41.
[11] Tomas, V., A. Margeta, Next generation control architectures, Pomorstvo, 20(2006), 2, str. 127-136.

Summary

THE INFLUENCE OF DIAGNOSTICS ON THE RELIABILITY AND SAFETY OF THE CONTROL EQUIPMENT

The paper aims at analyzing the influence of diagnostics and redundancy on the improvement of reliability and safety of the control equipment of the ship electrical engines. Safety, reliability and availability of the system are important requirements when designing the control equipment. If diagnostics and redundancy are not built in the system, any engine failure may lead to a gradual decrease of the system safety. The conception of self diagnostics and diagnostics, possibilities of its application on different system structures, as well as its influence on the reliability and safety of the control system, and consequently on the overall ship's electric power plant reliability and safety are analyzed. The analysis is carried out from two aspects: first, we have used the combined modelling techniques to estimate the improvement of reliability and safety when redundancy is included in the system; and, secondly, we have used the Markov's model to research into the safety aspect of two architectures for the design of a redundant diagnostic system. The procedure enables the evaluation of potential solutions by means of which the ship's electric power plant can operate with more suitable fault tolerance. The influence of the quality of diagnostics on these solutions has been also analyzed.

Key words: *diagnostics, ship's electric power plant, reliability, safety, fault-tolerant*

Vinko Tomas, Ph.D.
Dubravko Vučetić, Ph.D.
Faculty of Maritime Studies Rijeka
Studentska 2
51000 Rijeka
Croatia