Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 19, брой 3, 2021 г.
Научно списание **http://www.mtc-aj.com** **статия № 2151**

ИЗСЛЕДВАНЕ НА ДИВЕРСИТЕТА КАТО СРЕДСТВО ЗА ОТКАЗОУСТОЙЧИВОСТ В ДВУКАНАЛНИ КОМПЮТЪРНИ СИСТЕМИ

Христо Христов, Мария Христова
hristo.hristov@vtu.bg, mhristova@vtu.bg

Висше транспортно училище „Тодор Каблешков“
София, ул. „Гео Милев № 158
РЕПУБЛИКА БЪЛГАРИЯ

Ключови думи*: диверситет, отказ, излишък, надеждност, отказоустойчивост*

Резюме: *Припомнят се двете алтернативни възможности на диверситета: да открива грешки и неизправности (fail-safe средство) и да маскира грешки и неизправности (fault – tolerance средство). Показани са схемно-алгоритмичните решения за постигане на отказоустойчивост чрез диверситет в система 1+1* в двата варианта – постоянно включен резерв и резервиране чрез заместване и се разкриват техните отказоустойчиви свойства.

Поставя се целта да се намери и изследва математичен модел за количествено определяне на влиянието и големината на диверситета върху отказоустойчивостта на двуканалните системи. Въвежда се мярка за дълбочина на диверситета D като относителен дял на независимите откази на каналите към всички откази в системата.

За математическото моделиране се прилага логико-вероятностен подход. Извеждат нови формули за показателите за надеждност в зависимост от дълбочината на диверситета. Направени са изследвания за невъзстановими системи, които илюстрират ефекта от дълбочината на диверситета. Изведена е нова формула за средното време до отказ на двуканалната диверситета система, по която е направено изчисление. Установено е теоретично, че най благоприятно влияние на отказоустойчивостта има пълната независимост на двата канала. На базата на изложения подход могат да се намерят резултати и за възстановими системи, в които ефектът е на порядък по силен.

1. ПОСТАНОВКА

1.1. Понятийни уточнения

Тази статия изхожда от понятийното покритие на използваните термини [1, 4]:

Повредата е случайно събитие, причина за извеждане на обекта в неизправност. Тя може да се дължи на физическо, механическо, химическо, метеорологическо или друго обективно въздействие (износване, остаряване, умора, разрегулиране, счупване, изхабяване и пр.), т.е. присъща е на хардуерните компоненти и апаратни средства.

Грешката (*Error*) е неволно отклонение от възприет критерий за вярност от някаква установена норма (алгоритъм, правило).

В комуникационните и компютърни системи често се говори за грешка по единичен импулс, грешка на брояч, на компютърно устройство и т.н., което тук се счита за разширително тълкуване на понятието. В тази статия обхватът на понятието е по-строго ограничен и свързан със субекта. Тя е грешка *на човека:*

- създател на системата (програмист, проектант, конструктор, технолог, монтажник);
- потребител (оператор, диспечер, ръководител, абонат, ползвател и т.н.);
- поддържащ персонал (техник, системен администратор, технолог и т.н.).

Отказът (*Failure*) е случайно събитие, от което обектът става неработоспособен, нарушава се поне едно негово съществено свойство, свързано с присъщата му функционалност. Отказът може да се предизвика както от повреда, така и от грешка.

Отказоустойчивостта на системата се постига чрез **излишък** (*Redundancy*) – структурен, информационен, функционален, енергиен и др. Излишъкът се състои от работоспособни средства, аналогични на работещите, но в повече от необходимите за изпълнение на функционалните изисквания съгласно спецификацията на системата.

Диверситетът е *redundancy метод* за решаване на задача (математическа, логическа, техническа и пр.) по два (А и В) различни начина (метода, алгоритъма, реализации) като за решението и в двата случая се ползват еднакви входни данни. Ако две програми А и В, съставени от различни програмисти, независими един от друг, изпълняват една и съща задача, то А и В са диверситетни (софтуерен диверситет), така, както и ако два микропроцесора с еднаква функционалност са произведени по различни схеми и технологии от различни несвързани фирми (хардуерен диверситет).

За всички едносерийни устройства от един и същ производител, грешките (в софтуера, проектирането, документацията, технологията на изработката и т.н.) са едни и същи – системни, еднакви за цялата произведена серия. Такива устройства са **хомогенни**, което е антином на **диверситетни**. Грешките в хомогенните устройства са „по рождение“.

Повредите водят до неизправности, които, ако засегнат съществени свойства, могат да предизвикат отказ. По време на експлоатация неизправностите се появяват във всяка хардуерна единица отделно и независимо, без значение дали хардуерът е диверситетен. Чрез сравнение на резултатите от работата на изходите на двата канала такива откази са *откриваеми* (α-Fault). Ако двата канала работят по копия на една и съща програма $A \equiv B$ (хомогенен софтуер), грешките на единствената програма водят до еднакви некоректни резултати, а отказите им остават *неоткриваеми* чрез сравнение (η-Fault).

При безгрешен софтуерен диверситет $A \neq B$ изходните резултати са винаги съответни. Но ако в програмите има грешки, те се откриват с много голяма вероятност, защото са случайни и на различни случайни места в програмата. Активират се в различно време и при различни входни данни, затова водят до несъответни резултати. В дълбоко диверситетните канали между грешките липсва зависимост. Както и хардуерните неизправности, грешките могат да водят до откриваеми откази и да се считат за α – Fault.

1.2 Възможности на диверситета

Диверситетът като подход може да се използва за постигане на две противоположни цели:

1. Да **открива** грешки и неизправности (*fail-safe средство*);
2. Да **маскира** грешки и неизправности (*fault – tolerance средство*).

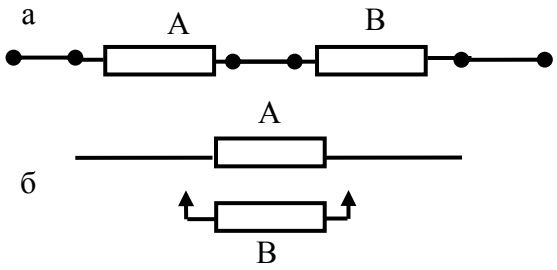
Като fault-tolerance средство диверситетът има противоположното на fail-safe предназначение. На различието в двата канала се разчита не за **откриване** на отказите, а за да ги **толерират** с цел запазване на работоспособността. Системата продължава да работи по изправния канал, който маскира, потиска и преодолява влиянието на отказалия канал. Ако обаче програмите им са хомогенни, ще се получат еднакви, но грешни резултати.

В софтуерно диверситетна система отказоустойчивост се постига благодарение на това, че ако в А-програма се е активирала Fault, то при обработката на В-програма ще се получи вярно и валидно решение (вж. по-долу), защото или в нея няма грешка, или ако има, тя не се е активирала.

Целта на това изследване е да се намери математичен модел за количествено определяне на влиянието и големината на диверситета върху отказоустойчивостта на най-често използваните двуканални системи, както и да се проведат изчисления на съответните показатели за надеждност.

2. ДИВЕРСИТЕТНА СИСТЕМА 1+1

За да стане fault-tolerance средство, двуканалната $2 \vee 2$ (фиг.1,а) fail-safe система [2], се преконфигурира в диверситетна система $1+1$ (фиг.1,б)**.**



Фиг.1 Реконфигурация на $2 \vee 2$ в $1+1$

Освен независими по неизправности, каналите могат да са и независими по грешки. Това може значително да подобри надеждността на системата, ако се постигне чрез диверситет.

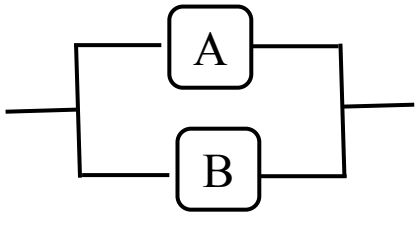
Целта на изследването е *да се моделира надеждността на системата* $1+1$*, изградена с диверситетно резервиране, като се установи количествено ефектът от диверситета върху показателите за надеждност.* Задачата се свежда до моделиране на показателите за надеждност – функцията на надеждността (Reliability) $R_{1+1}(t)$ на системата и средното време до отказ на системата MTTF с отчитане дълбочината на диверситета (степента на независимост на А и В).

3. АЛГОРИТМИЧНО РЕШЕНИЕ

За fault-tolerance системи с независими канали са възможни две техники, съответно две различни схеми на реализации.

3.1 Постоянно включен резерв

Каналите са равнозначни, няма основен и резервен. Резервът е постоянно включен (фиг.2).

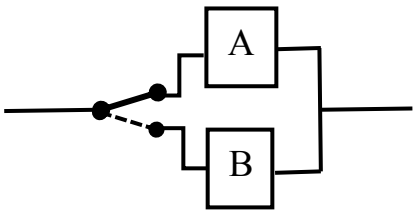


Фиг.2. Схема на постоянно включено диверситетно резервиране

Този метод може да се прилага ограничено, тъй като различава работещ от неработещ канал, но не и функциониращ с грешни изходни резултати. Ако трябва да се прилага и в тези случаи, трябва да има критерий за вярност на резултата, свързан с произтичащо от това схемно усложнение. В други случаи се въвежда цикличен режим (примерно с цикъл 1 s). Ако във всеки цикъл се извежда „високоотговорна единица (1)“, верността се потвърждава, значи отказ няма. Изчезне ли единицата, въздействието се стопира, което е fail-safe.

3.2 Резервиране чрез заместване

Разглеждаме софтуерен диверситет. Нормално се използва само едната (базова) програма (фиг.3). Програмата се секционира, а на границата между секциите (Check Point**)** се проверява за отказ. Средствата за откриване на отказа могат да бъдат: наблюдателни таймери (watchdog timers), контрол по четност, абсолютен тест, сравнение на изходни резултати (относителен тест) и др. [4]



Фиг. 3. Схема за резервиране с диверситетно превключване

След обработката по **A** тестът установява работоспособността на канала. Ако няма отказ, работата продължава и резервът **B** не се използва. Когато има отказ, програмата се връща в контролна точка (технология Recovery blocks). Отук са възможни две решения:

Ако се счита достатъчно да се толерират кратковременни импулсни смущения и транзитивни откази, втора програма **B** не е нужна. Обработката може да е многократна като циклично се връща по същата **A** програма, докато се „изчисти“ смущението. Това е по-просто и евтино.

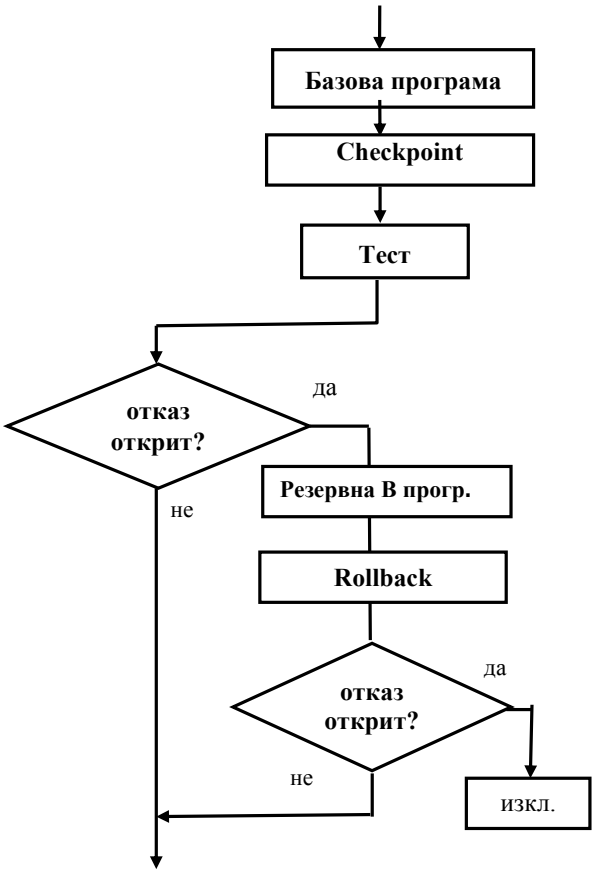
Да се потискат и устойчиви откази без втора програма е невъзможно. Необходим е софтуерен **диверситет**. Когато се открие отказ се превключва към резервната диверситетна B-програма (фиг.4.). В този случай, поради различието в A и B, е твърде вероятно повредата в хардуера или грешката в програмата да не се активират и по втората програма да се получи верният резултат, на което се и разчита за постигане на отказоустойчивост.

4. ЕКВИВАЛЕНТНА СХЕМА НА ОТКАЗОУСТОЙЧИВА СИСТЕМА С НЕЗАВИСИМИ КАНАЛИ

Колкото и двата канала **A** и **B** да са независими, системата 1+1 не може да няма общи компоненти: общо захранване, обща среда, общ компаратор (ако е нужно сравнение на A и B резултати) и др. Може в един хардуер да работят две програми (1H+2S) или в два хардуера една програма (2H+1S), което е по-икономично. Очевидно е, че ако причината за отказ е в общите компоненти, тя не може да се толерира и да изявява отказ. Откази по такива причини, ще именуваме η откази (η*-Fault*).

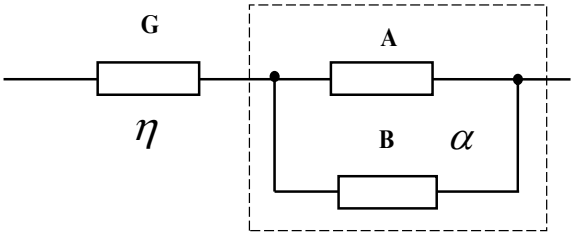
След тези уточнения може да се приеме, че така разглежданата $\alpha - \eta$ диверситетна система има еквивалентна по надеждност схема, показана на фиг.5. В надеждностно отношение схемата е последователно-паралелна. На общите части съответства G-компонента, последователно свързана с двете независими компоненти A

и B. Системата ще работи, ако няма отказ по обща за двата канала (G) причина (η-Fault) и поне в един канал (A или B) няма α - Fault.



Фиг.4 Алгоритъм за диверситетно резервиране по софтуер

Еквивалентната схема може да няма много общо с физическата реализация. Например, ако софтуерът е един и същ и в двата канала, той се изнася в общата G-компонента. В случай, че има някакви други общи причини (електромагнитна съвместимост, захранване, смущения, радиация), те се включват в тази обща част. В хомогенните канали грешките са едни и същи и отказите, които генерират, са напълно зависими.



Фиг. 5 Еквивалентна схема по надеждност

Всеки от двата канала има свои α-Fault, независими от другия канал. Хардуерната независимост е валидна и за хомогенните, и за диверситетните канали. Не такава е зависимостта обаче при откази от грешки (e-Fault). Както другите грешки (Error), така и (най-вече) програмните, ако са общи за двата канала, се отнасят към $\eta = \eta_e$ *Fault*. В дълбоко диверситетните канали между софтуерните грешки на A и B няма зависимост. В идеалния случай може да се приеме $\lambda_{\eta e} = 0$.

5. МОДЕЛИРАНЕ НА НАДЕЖДНОСТТА НА ОТКАЗОУСТОЙЧИВА СИСТЕМА С НЕЗАВИСИМИ КАНАЛИ

Тук се разглеждат само невъзстановими системи и изследванията са ограничени до два показателя - вероятност $R_{1+1}(t)$ за безотказна работа и математическо очакване $MTTF_{1+1}$ на отработката до отказ.

5.1 Функция на надеждност

Интензивността на отказите от двата вида λ_α и λ_η зависят не само от броя и вида на причините за откази, но и от това, дали и колко често те се активират, което зависи от алгоритъма и режима на работа на системата.

Нека интензивностите на независимите откази в каналите А и В да са $\lambda_{\alpha A}$ и $\lambda_{\alpha B}$. При възникването на α-отказ системата може да работи, защото другият канал е независим от отказалия. Булевата функция F на работоспособността на схемата (фиг.5) има вида:

(1) $$F_{1+1} = z_\eta^0\left(z_{\alpha A}^0 \vee z_{\alpha B}^0\right)$$

където z_i^1 (във функция (2)) е логическа променлива на твърдението, че „нещо" се е случило, а z_i^0, че не се е случило. „Нещото" тук е причината, която след активирането си води до отказ.

Тъй като Булевата функция (1) е безповторна, тя може директно да се използва за преход към вероятностна функция [1]. Но за целта трябва да се преработи и в базис „конюнкция-отрицание". Тази форма се получава след преобразование по Де Морган:

(2) $$F_{1+1} = z_\eta^0\left(z_{\alpha 1}^0 \vee z_{\alpha 2}^0\right) = z_\eta^0 . \overline{z_{\alpha 1}^1 z_{\alpha 2}^1}$$

Като се приложат правилата за преход от логически към вероятностни функции [1], от (2) се намира формула за вероятността за безотказна работа на системата от два канала.

(3) $$R_{1+1}(t) = R_\eta\,(1 - Q_{\alpha A}.Q_{\alpha B})$$

където Q_α е вероятността да се получи локален отказ в съответния канал, а R_η вероятността за работоспособност при отсъствие на общи причини за отказ.

Като се замести в (3) с вероятност каналът да работи $Q_\alpha = 1 - R_\alpha$ за общата надеждност на системата се получава:

(4) $$R_{1+1} = R_\eta\,\{1 - [1 - R_{\alpha A}][1 - R_{\alpha B}]\}$$

където R_η е функцията на надеждността на общите компоненти на системата, а $R_{\alpha A}$ и $R_{\alpha B}$ са надеждностите на А и В канали.

Ако се приеме експоненциално разпределение на отработката до отказ, формулата придобива вида:

(5) $$R_{1+1} = e^{-\lambda_\eta t}\left[1-(1-e^{-\lambda_{\alpha A} t})(1-e^{-\lambda_{\alpha B} t})\right]$$

5.3 Показател за независимост на отказите.

Нека в диверситетната система има поток от откази с интензивност λ_d. Те се състоят от откази в общата част G с интензивност λ_η? които ще наречем η -откази

(Common Vjde Failures CMF) и α - откази в двата паралелни клона A с интензивност $\lambda_{\alpha A}$ и B с интензивност $\lambda_{\alpha B}$. Нека при това сумата от интензивностите на всички откази остава една и съща: $\lambda_d = \lambda_\eta + \lambda_{\alpha A} + \lambda_{\alpha B}$.

Въвежда се мярка за диверситета D като се предполага, че съотношението между отказите в паралелните клонове и общата част G се променя. Отказите в диверситетните клонове се редуцират с което диверситетът $D = \frac{\lambda_\alpha}{\lambda_d}$ намалява за сметка на CMF или обратното, когато D расте, но така, че общата сума на интензивностите остава постоянна.

При $\lambda_{\alpha A} = \lambda_{\alpha B} = \lambda_\alpha$ от (5) се получава: $D = \frac{\lambda_\alpha}{\lambda_d} = \frac{\lambda_\alpha}{\lambda_\eta + 2\lambda_\alpha}$

(6) $$R_{1+1}(t) = e^{-(1-D)\lambda_d t}\left[1-(1-e^{-D\lambda_d t})^2\right].$$

Видно е, че ако каналите са независими, т.е. D = 1, $\lambda_\eta = 0$, системата се редуцира на паралелна и достига пределния максимум на надеждността:

(7) $$P_{1+1}(t) = 1 - (1 - e^{-0,5\lambda_d t})^2.$$

Когато D = 0 всички причини за откази са общи, няма $\alpha-$откази ($\lambda_\alpha = 0$, $\lambda_\eta = \lambda_d$). Системата се редуцира на последователна по надеждност, достига минималната си стойност, а формулата придобива своя класически вид - пределния минимум на надеждността:

(10) $$P_{1+1}(t) = e^{-\lambda_\eta t}.$$

Изменяйки относителния дял D на отказите в каналите спрямо всички откази по (5) и (8) може да се проследи влиянието на показателя за независимост D върху надеждността на система 1+1.

7. СРЕДНО ВРЕМЕ ДО ОТКАЗ

Както е известно, средното време до отказ MTTF е решението на интеграла от вероятността за безотказна работа в граници от 0 до ∞

(11) $$MTTF = \int_0^\infty P(t)\,dt \ \text{[h]}$$

За да се намери средното време до отказ в случая трябва да се реши определеният интеграл от функцията на надеждността (4). Когато при експоненциално разпределение двата канала имат равна надеждност, той се опростява:

(12) $$MTTF_{1+1} = \int_0^\infty e^{-(1-D)\lambda t}\left[1-(1-e^{-D\lambda t})^2\right]dt$$

Намерено е следното решение на **неопределения** интеграл на (12) :

(13) $$MTTF_{1+1} = \frac{e^{-(D-1)\lambda t}\left[1-2(D+1)e^{-D\lambda t}\right]}{(D+1)\lambda}.$$

Определеният интеграл е в граници $\infty, 0$

(14) $$MTTF_{1+1} = \frac{e^{-(D+1)\lambda t}\left[1-2(D+1)e^{-D\lambda t}\right]}{(D+1)\lambda}\Bigg|_0^\infty$$

Като се заместят по правилата за определен интеграл горната и долната граници се получава търсеното решение:

(15) $$MTTF_{1+1} = \frac{1}{\lambda}\left(2-\frac{1}{D+1}\right) = MTTF\left(2-\frac{1}{D+1}\right)$$

Това е нов, оригинален резултат, определящ средното време $MTTF_{1+1}$ до отказ на система 1+1, който съдържа в експлицитна форма дълбочината на диверситета D на каналите.

Когато няма диверситет, D = 0 и еквивалентната схема се редуцира до единствения компонент G (фиг.4). $MTTF_{1+1} = 1/\lambda$, което следваше да се очаква. Когато диверситетът е пълен D = 1 еквивалентната схема (фиг.4) се редуцира в паралелна схема и

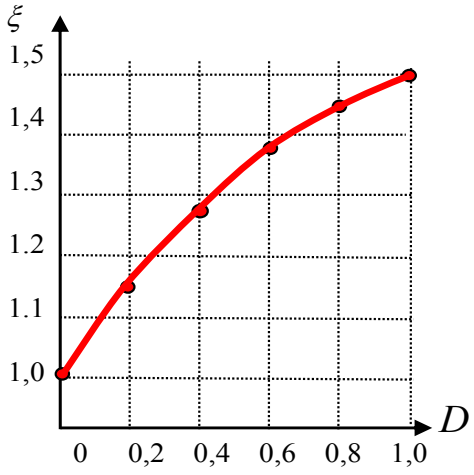
(16) $$MTTF_{1+1} = \frac{1}{\lambda}\left(2-\frac{1}{1+1}\right) = \frac{1}{\lambda}\left(1+\frac{1}{2}\right)$$

което също е очаквано. Това е познатото време на живот на паралелна схема.

Увеличението на средната продължителност на живота на системата

(17) $$\xi = 2 - \frac{1}{D+1}$$

е представено графично на фиг. 6.



Фиг.6 Удължаване на живота на системата в зависимост от диверситета

Видно е, че диверситетът има почти линейно влияние върху увеличаването на средното време до отказ на системата – и малък диверситет има ефективен резултат.

Изследванията се отнасят до невъзстановими системи. Увеличението на средното време до отказ не може да е повече от 50%, както се вижда от фиг.6. Когато системата е възстановима средното време между отказите може да е на порядъци по–голямо.

ОБОБЩЕНИЯ

От така изведените модели и направените изследвания могат да се дадат следните важни обобщения:

1. Изведена е формула за средното време на отказ на двуканадна система в засисимост от диверситета на каналите. Колкото по-дълбок е диверситетът, толкова по голяма е надеждността.

2. С изменение на дълбочината на диверситета от 0 на 1 надеждността се изменя, както при постепенен преход от последователна към паралелна по надеждност система.

3. Полученият резултат може да се прилага за количествено оценяване на ефективността на диверситета и показва неговата ефективност, особено при пълна независимост.

ЛИТЕРАТУРА

[1] Христов, Х. А., В. Г. Трифонов. Надеждност и сигурност на комуникациите. Нови знания. 2007 .

[2] Христов Хр., М. Христова, Изследване върху вероятността за опасен отказ в критични по безопасност системи от вида 2V2, Механика, Транспорт, Комуникации, ISSN 1312-3823 (print), ISSN 2367-6620 (online), art ID 1884, 2019

[3] Christov Chr., N. Stoytcheva, M. Christova. Diversity as a Mean for Reliability and Safety, Transport Systems Telematics (2010), ISBN: 978-3-642-16471-2 (Print) 978-3-642-16472-9 (Online), DOI 10.1007/978-3-642-16472-9, vol.104, pp.308-319,© Springer-Verlag Berlin Heidelberg, New York (2011)

[4] Синягина Н., Б. Юруков, Г. Калпачка и др., ISBN 978-954-00-0089-3, 2016

STUDY OF DIVERSITY AS A MEANS FOR FAULT TOLERANCE IN DUAL-CHANNEL COMPUTER SYSTEMS

Hristo Hristov, Mariya Hristova
hristo.hristov@vtu.bg, mhristova@vtu.bg

Todor Kableshkov University of Transport,
Sofia, 158 Geo Milev Str.
THE REPUBLIC OF BULGARIA

Key words: *Diversity, Failure, Redundancy, Reliability, Fault tolerance,*

Abstract: *The two alternative possibilities of diversity are recalled: to detect errors and fault (fail-safe means) and to mask errors and fault (fault - tolerance means). The article presents the circuit-algorithmic solutions for achieving fault tolerance through diversity in the 1 + 1 system in both variants - permanently included reserve and redundancy reservation. Their fault tolerance properties are shown.*

The article aims to find and study a mathematical model for quantifying the influence and magnitude of diversity on the fault tolerance of two-channel systems. A measure of the depth of diversity D is introduced as a relative share of the independent channel failures to all failures in the system. A logical-probabilistic approach is applied to mathematical modeling. New formulas for reliability indicators are derived depending on the depth of diversity. Studies have been made of non-recoverable systems that illustrate the effect of depth of diversity. A new formula for the mean time to failure of the two-channel diversity system is derived, according to which a calculation is made. It has been theoretically found that the complete independence of the two channels has the most favorable effect on fault tolerance. Based on the approach presented, results can be found for recoverable systems in which the effect is tens and hundreds of times stronger.