Механика Транспорт Комуникации

Научно списание

ISSN 1312-3823

том 11, брой 3, 2013 г.

статия № 0862

http://www.mtc-aj.com

МОДЕЛИРАНЕ НА НАДЕЖДНОСТТА НА ОТКАЗОУСТОЙЧИВИ СИСТЕМИ С ХОМОГЕННО РЕЗЕРВИРАНЕ

Христо Христов[1], Мария Христова[2]
ac@epu.bg, mhristova@vtu.bg

[1]Технически Университет, София, бул."Кл. Охридски" 8
[2]Висше транспортно училище „Т. Каблешков", София, ул. „Гео Милев" 158
БЪЛГАРИЯ

***Ключови думи**: надеждност, излишък, готовност, системи за реално време, критични по безопасност системи, отказоустойчиви системи*

***Резюме:** Предмет на теоретично изследване са системи с висока отговорност, включително в управлението на транспортни процеси. Изхожда се от презумпцията, че такива системи трябва да имат готовност и средно време между отказите, значително по-добри от обичайните стойности за системи в реално време. Предлага се високата надеждност, каквато се изисква от тях, да се постигне чрез отказоустойчивост, основното средство на която е излишъкът. В тази статия той има формата на постоянно включено резервиране. Резервирането може да е хомогенно или диверситетно. Тук е разгледан случаят, когато заместващата компонента е идентична с отказалата единица. Новост на подхода, е че като изходна структура се използва система с резервирана дробна кратност на структурния излишък. За пръв път се стига до извода, че последователна и паралелна по надеждност системи могат да се моделират чрез общата формула за надеждност на изходната структура в двете екстремни крайности на параметрите ѝ. Получени са формули за готовността и средното време между отказите MTBF. Направени се изводи, свързани с факторите, от които зависи подобрението на надеждността. Показано е, че при осигурени ресурси може да се стигне до произволно висока предварително зададена надеждност.*

1. ПОСТАНОВКА НА ПРОБЛЕМА

Класиката на осигурителните системи е свързана със специфични градивни елементи, от които се синтезират автоматите и структурите на *критични по безопасност системи*. Изхожда се от презумпцията, че забраненият преход 0-1 в тези елементи след отказ е недопустим и невъзможен.

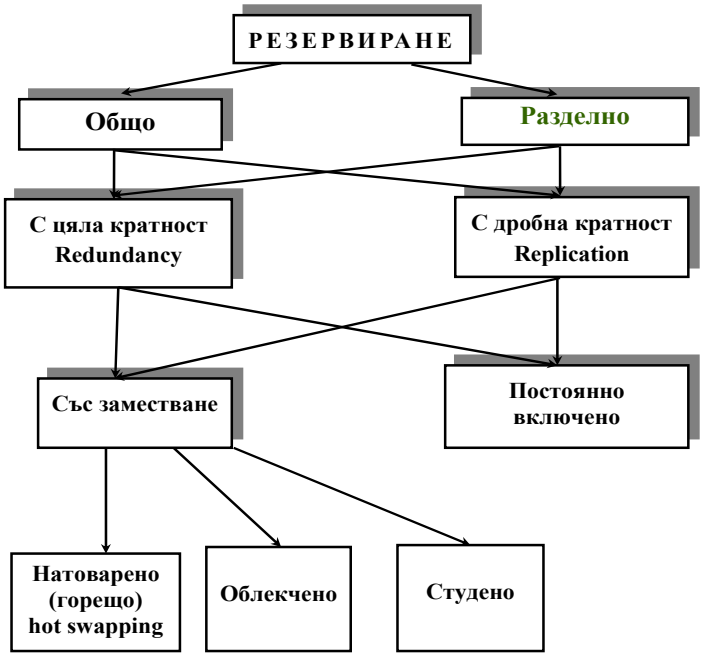
Бурното развитие на науката и практиката на съвременните комуникации през изтеклите десетилетия позволиха да се постигне равнище, когато през мрежата се управляват огромни ресурси и процеси, отговорни за живота и здравето на човека, системи за обществена безопасност, космически мисии, банкиране и транзакции т.н., съизмерими с отговорността на критичните по безопасност системи. Новото поколение осигурителни системи се основава на принципно нова философия. Вместо на безопасни след отказ логически елементи и свързани с тях обособени методи за синтез, твърде неефективни

днес поради своята специфичност, се използват методи за отказоустойчивост, прилагани в други сфери. Безопасност след отказ се постига чрез надеждност.

Средство с първостепенно значение за постигане на надеждност по този подход е излишъкът. **Излишъкът** е *повече от необходимите за функциониране на системата работоспособни средства (хардуер, софтуер, време, информация), чрез които неизправностите на елементите и грешките при създаване на системата се толерират (до определена граница), потискат (маскират) така, че тя запазва работоспособност въпреки тяхното наличие*.

Отказоустойчивостта се разбира [3] като нарастване на вероятността за безотказна работа или готовността благодарение на излишъка, въпреки откази на отделни компоненти, от които е изградена.

Излишъкът се използва най-често за **резервиране**. Една класификация на резервирането е дадена на фиг.1.



фиг. 1. Класификация на резервирането

Ако за резервиране на даден компонент се използва такъв със същото предназначение, резервирането е **с цяла кратност**: едно-, дву-, трикратно и т.н. *m*-кратно резервиране.

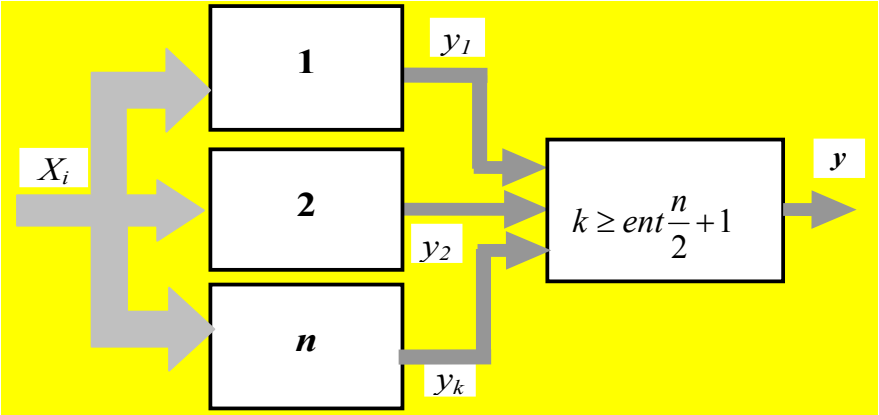
Нека една система има $\boldsymbol{m}$ еднакви елементи, но да може да работи с по-малко на брой - $\boldsymbol{k}$ елемента („$\boldsymbol{k} < \boldsymbol{m}$"). Резервирането е **с дробна кратност** $\frac{m-k}{m}$**.** Най-често се прилага, за да се осигури т. нар. кворум функция $\boldsymbol{k} < \boldsymbol{m}$.

Когато дадена единица е резервирана с идентична такава, резервирането е *хомогенно*.

Целта на настоящата статия е в различни случаи на хомогенно резервиране да се изведат аналитични зависимости за надеждността, за да се установи, кои са факторите и как те ѝ влияят с цел да се намерят ефективни средства за повишаването на готовността.

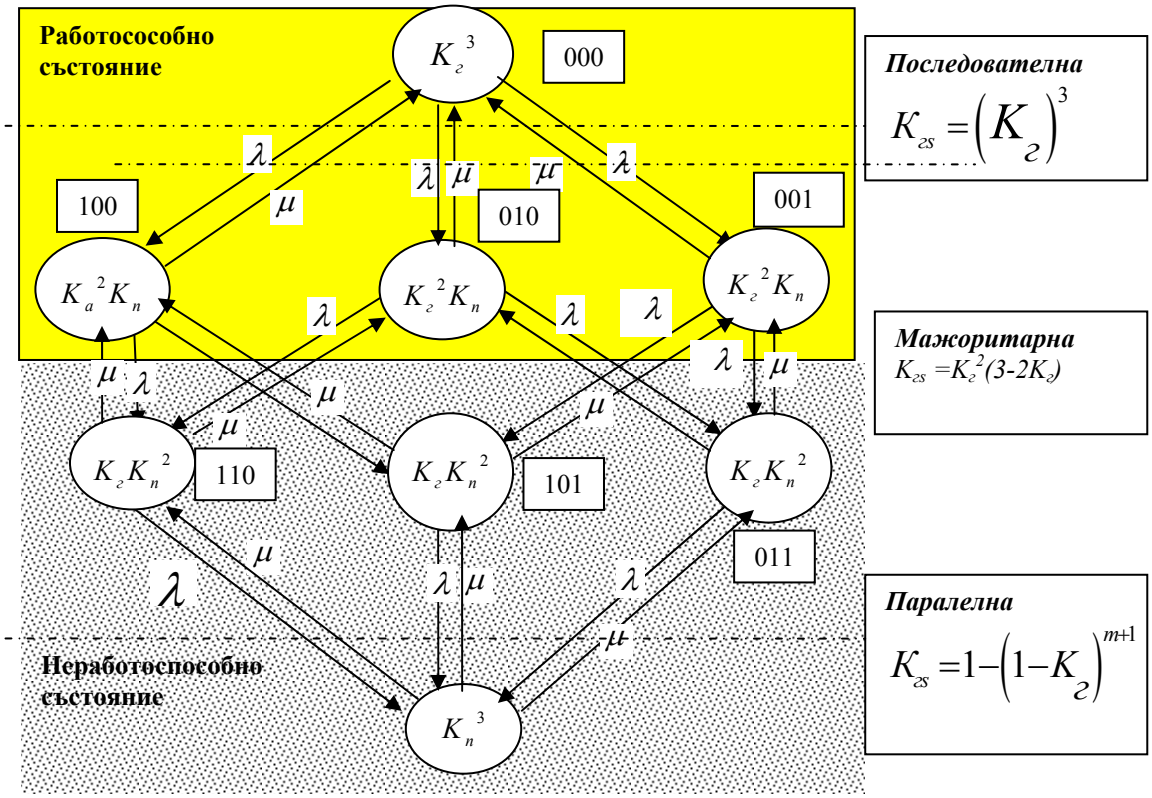
2. РЕЗЕРВИРАНИ ВЪЗСТАНОВИМИ СИСТЕМИ

Най-общият случай на структурен излишък е резервирането с дробна кратност – фиг.1. Една възстановима система „k от n", която е работоспособна по критерия $k \geq ent\frac{m}{2}+1$ за просто мажоритерине, има вида на фиг. 2.



Фиг 2 Резервиране с дробна кратност

Параметри на всеки от елементите (*1, 2, n*), участващи в структурата [1]: *p(t)* – вероятност за безотказна работа; $K_г$ - неговата готовност, λ - интензивност на отказите му, $H = K_г\lambda$ - честота на отказите средно време до отказ $MTTF = \frac{1}{\lambda}$ и средното време между отказите на елемента $MTBF = \frac{1}{H} = \frac{1}{K_г\lambda}$ [1].



Фиг. 3 Граф на състоянията за система 2 от 3

За да е работоспособна системата, трябва да работят $k \geq ent\frac{n}{2}+1$ единици. Докато другите поддържат работоспособността, отказалата единица се възстановява с интензивност μ и отново се включва в работа.

Един от ефективни начини за моделиране на готовността е чрез пространството на състоянията, което се описва с граф на парциалните състояния и преходите между тях. На фиг.3 е показан такъв граф за най-простата от тези структури – „2 от 3".

3. ИЗВОД НА ФОРМУЛИТЕ ЗА ГОТОВНОСТ НА СИСТЕМИ СЪС СТРУКТУРНО РЕЗЕРВИРАНЕ

Моделът на вероятността *P(t)* за безотказна работа се търси по логико-вероятностния преход. Решението в общия случай е намерено в [1]:

(1) $P(t) = p^n + np^{n-1}q + C_n^2 p^{n-2}q^2 + \ldots + C_n^{n-k}p^k q^{n-k}$.

Когато няма резервиране, структурата се реконфигурира в последователна по надеждност и моделът на вероятността *P(t)* за безотказна работа се опростява:

(2) $P(t) = p^n$

При възстановими системи се преминава към коефициент на готовност $K_г$. Когато всички елементи работят, вероятността системата да е в парциално състояние 000 на фиг.4 определя нейната готовност при последователна структура. Границата между глобалните състояния „работи-не работи" минава под този връх. Тогава по аналогия с (2) готовността на системата ще бъде:

(3) $K_{гS} = K_г^{\,n}$

При едноканалното резервиране (резервиране с един слой) системата работи и в *n* парциални състояния, в които някой от *n*-те елемента е отказъл. Вероятността за тези парциални състояния е $K_г^{\,n-1}(1-K_г)$. Общата готвоност е:

(4) $K_{гS} = K_г^{\,n} + nK_г^{\,n-1}(1-K_г)$

За общия случай при *n-k* – резервиране:

(5) $K_{гS} = K_г^{\,n} + nK_г^{\,n-1}(1-K_г) + C_m^2 K_г^{\,n-2}(1-K_г)^2 + \ldots + C_m^k K_г^{\,k}(1-K_г)^{n-k}$, т.е.

(6) $K_{гS} = \sum_{i=0}^{n-k} C_n^{\,i} K_г^{\,(n-i)} K_г^{\,i}$

Когато прагът на мажоритарност намалява и, минавайки през преобладание, стигне до *k =1*, структурата дегенерова в паралелна:

(7) $K_{гS} = K_г^{\,n} + nK_г^{\,n-1}(1-K_г) + C_m^2 K_г^{\,n-2}(1-K_г)^2 + \ldots + C_m^k K_г^{\,k}(1-K_г)^{n-k} + \ldots + K_г(1-K_г)^{n-1}$

По теоремата за пълната вероятност в (7) липсва само един член $(1-K_г)^n$, за да бъде сумата равна на 1:

(8) $K_г^{\,n} + nK_г^{\,n-1}(1-K_г) + C_m^2 K_г^{\,n-2}(1-K_г)^2 + \ldots + C_m^k K_г^{\,k}(1-K_г)^{n-k} + \ldots + K_г(1-K_г)^{n-1} + (1-K_г)^n = 1$

Ако се преработи това равенство па паралелните системи, когато разграничителната линия минава над най-долния парциален връх на графа (фиг. 3), ще се получи формулата:

(9) $K_{гS} = 1 - K_г^{\,n}$

За система „2 от 3”

(10) $K_{гS} = K_г^{\,3} + 3K_г^{\,2}(1-K_г)$

За система „3 от 5”:

(11) $K_{гS} = K_г^{\,n} + 5K_г^{\,4}(1-K_г) + 10K_г^{\,3}(1-K_г)^2$

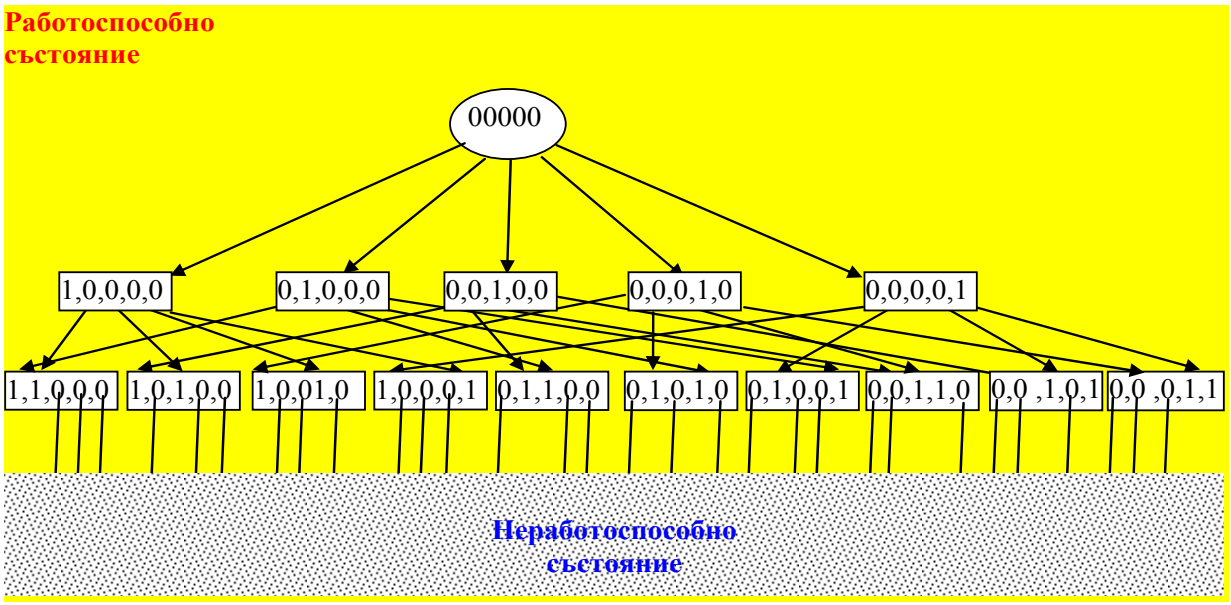
Както е видно, случаят на дробно кратно резервиране е най-общ и от него могат да се изведат всички случаи на структурно резервиране. Това се прави за пръв път тук.

4. ИЗВОД НА ФОРМУЛИТЕ ЗА ВРЕМЕВИТЕ ПАРАМЕТРИ

Времевите параметри на системите с възстановяване след отказ са: интензивност на възстановяването и средно време между отказите *MTBFs* [2]. За да се изведе формулата за средното време, графът се усложнява (фиг.4) с повече канали.

От всеки връх на графа, който има връзка със състоянието на неработоспособност, излизат откази с интензивност λ, респ. в този връх влизат възстановявания с интензивност μ В общия случай графът ще има C_n^k гранични върха, от които се прави преход към неработоспособно състояние. Вероятността за пребиваване в съответния връх i е

(12) $P_i = K_г^{\,k}(1-K_г)^{n-k}$



фиг. 4 ***Марковски граф на състоянията в система „3 от 5”***

Като се изходи от класическата връзка „честота - готовност – интензивност” всяка от тези честоти ще има стойност:

(13) $H_i = K_г^{\,k}(1-K_г)^{n-k}\lambda_i$

Глобалната честота на прехода H_s е сумата от локалните честоти:

(14) $H_{вх.j} = \sum_{i=1}^{n} H_{ij}$

Трябва да се определи броят на локалните честоти на преходите. Все още работещите елементи във всяко гранично състояние преди прехода към неработоспособност на графа са *k.* На границата от работоспособност към неработоспособност стои нивото, в което има толкова работещи елементи, колкото е прага *k (Фиг.4)*. Преходите между работоспособно и неработоспособно състояние са k-

пъти повече от върховете, защото все още работещите елементи във всяко от C_n^k-те върха могат един по един да отказват и да преминават в различни съседни неработоспособни състояния.

Честотата на преход от работоспособност в неработоспособност от кое да е гранично състояние при отказ на кой да е от работещите елементи е:

(15) $$H_i = K_г^k K_n^{n-k} \lambda$$

Тогава глобалната честота H_s на преход на системата в неработоспособност е

(16) $$H_s = \sum_{i=1}^{C_n^k} H_i \underset{H_i = H}{=} C_n^k k K_г^k (1 - K_г)^{n-k} \lambda$$

В общия случай средното време между отказите на системата ***"k от n"*** е:

(17) $$MTBF_s = \frac{1}{H_s} =$$

$$\frac{1}{C_n^k k K_г^k (1 - K_г)^{n-k} \lambda} = \frac{MTBF}{C_n^k k K_г^{k-1} (1 - K_г)^{n-k}}$$

За случая, когато системата „2 от 3" се състои от еднакви по надеждност елементи:

(18) $$MTBF_s = \frac{1}{H_s} = \frac{1}{C_3^2 2 K_г^2 (1 - K_г) \lambda} = \frac{MTBF}{6 K_г (1 - K_г)}$$

За система е „3 от 5":

(19) $$MTBF_s = \frac{1}{H_s} = \frac{1}{C_5^3 3 K_г^3 (1 - K_г)^2 \lambda} = \frac{MTBF}{30 K_г^2 (1 - K_г)^2}$$

Може да се изчисли, че при висок коефициент на готовност времето на живот на системата се увеличава на няколко порядъка. Но колкото готовността на елемента е по-ниска, толкова по-слаб е ефектът от излишъка. Стига се дотам, че система „2 от 3" става по-ефективна от система „3 от 5".

От формула (19) могат да се намерят и очакваните времена на живот на последователните и паралелните по надеждност системи:

Последователна система (консенсус) ***k = n*:**

(20) $$MTBF_s = \frac{1}{H_s} = \frac{1}{C_n^n n K_г^n (1 - K_г)^0 \lambda} = \frac{1}{K_г^n n \lambda} = \frac{MTBF}{n K_г^{n-1}}$$

Паралелна система (*1* от *n*) *k = 1:*

(21) $$MTBF_s = \frac{1}{H_s} = \frac{1}{C_n^k K_г (1 - K_г)^{n-1} \lambda} = \frac{MTBF}{n (1 - K_г)^{n-1}}$$

Или, ако се приемат обозначенията за един базов елемент и m-пласта резерв ($n = m+1$),

(22) $$MTBF_s = \frac{MTBF}{(m + 1)(1 - K_г)^m}$$

Ако се заместят числови стойности може да се установи, колко ефективен е методът за постигане на отказоустойчивост, при който може да се постигне хиляди пъти по-дълъг живот на системата в сравнение с изграждащите я структурни елементи.

ЗАКЛЮЧЕНИЕ

Приносите в тази статия се свеждат до:

1. Предложен е метод, въз основа на който от общия случай на резервиране с дробна кратност се извеждат формулите за готовността на системи с цяла кратност, както и на последователни и паралелни структури.
2. Установени са нови зависимости, чрез които системната готовност може да се определи от броя на елементите в системната структура, тяхната интензивност на откази и на възстановяване и начина на тяхното свързване в надеждостен смисъл.
3. Изведени са формули за времевите параметри на възстановимите системи като функции на системата структура и първичните надеждностни параметри.

ЛИТЕРАТУРА

[1] Христов, Хр. В. Трифонов**,** *Надеждност и сигурност на комуникациите,* Нови знания, 2005,

[2] John Downer**,** *When Failure is an Option: Redundancy, reliability and regulation in complex technical systems,*. London School of Economics and Political Science, 2009

[3] Medikonda S., P.S. Panchumarthy, *An Approach to Modeling Software Safety in Safe-Critical Systems*. Journal of Computers Science (5), 2009

MODELING RELIABILITY OF FAULT TOLERANT SYSTEMS WITH HOMOGENEOUS RESERVATION

Hristo Hristov, Mariya Hristova
ac@epu.bg, mhristova@vtu.bg

[1]*Technical University of Sofiya, Bulgaria, Sofiya, 1000, boul. Kliment Ohridski 8,*
[2]*Todor Kableshkov University of Transport , Sofia, Geo Milev 158,*
BULGARIA

Key words: *reliability, redundancy, availability, mean time between failures, Real Time Systems, Safety Critical Systems, Fault Tolerant Systems*

Abstract: *The subject of the theoretical research is the systems with high responsibility including the management of transport processes. It is preceded from the assumption that such systems must be ready and have mean time between failures (MTBF) significantly better than the usual values for Real Time Systems. It is proposed to achieve the high reliability required for them by a fault-tolerance approach, the primary means of which is a redundancy. In this article it has the form of permanent reserving. The reservation can be homogeneous or diversity. The case examined here is the one where the replacement component is identical to the failed unit. The novelty of the approach is the use of a system with redundant fractional multiplicity of structural surplus as a starting structure. It is for the first time to conclude that systems of series and parallel by reliability can be modelled by the general formula for reliability of the output structure in the two extreme excesses of its parameters. Formulas for the availability and mean time between failures are obtained. The conclusions about the factors that determine the improved reliability are made. It is shown that with dedicated resources arbitrary predetermined high reliability can be reached.*