ИЗСЛЕДВАНЕ НА НАДЕЖДНОСТТА И СЛЕДОТКАЗОВАТА БЕЗОПАСНОСТ НА МИКРОКОМПЮТЪРНИ ОСИГУРИТЕЛНИ СИСТЕМИ С ГОРЕЩ РЕЗЕРВ

проф. дтн Христо Ангелов Христов, гл.ас. Нели Иванова Стойчева, гл. ас. Мария Петкова Семова, ВВТУ "Т. Каблешков"

Abstract. In this article is analyze the "1+1stand by" dynamic redundant systems build on the microcomputers. The problem addressed to research and modeling of the system reliability and safety based on the Markov processes.

For dangerous failure is accepted the state where or the main channel or the reserve channel are not discover error or fault.

The formulae for probability of dangerous work and the system availability are worked out. It reflects dependence on the safety criterion after the system's failure from the influence factors. The models up to now consist of following parameters: the failure rate and the restoration rate of the system's units and the probability failure to be discovered by means of control and switch over.

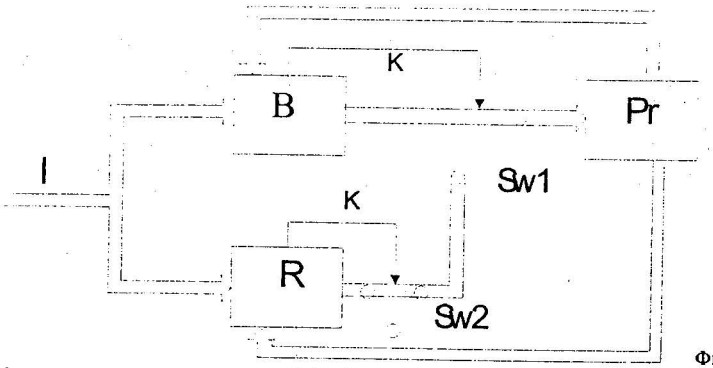
1. Постановка на проблема

1.1 Предмет на изследване в този труд е отказоустойчива (fault tolerance) микрокомпютърна осигурителна структура с горещ резерв (1+1stand by), най-общата блокова схема на която е показана на фиг.1. С такива системи се управляват отговорни технологични процеси ОТП, нарушението на параметрите на които може да доведе до опасност за живота и здравето на хората, както и за загуба на големи материални, духовни или природни ценности.

1.2 Двата канала **B (основен)** и **R (резервен)** се състоят от информационно-обработващи устройства **F** (микрокомпютри, контролери или електронни схеми с твърда логика) с вградени средства за самоконтрол **K** на отказите им. И двата канала получават едновременно входната информация от оператора и контролната информация от ОТП и са винаги в еднакво информационно състояние. Ако в канала настъпи отказ, на изходите му може да се формира некоректен резултат, който може да има нерегламентирани и опасни последствия. Затова след откриване на отказа средствата за самоконтрол **K** въздействат на превключвател **Sw,** който комутира изходите на канала. Ако това е канал **B**, той превключва управлението на ОТП към канал **R.** Ако това е канал **R,** той изключва процеса, предпазвайки го от некоректно и възможно опасно управление. Така дефинираният предмет на изследване е **възстановима fault tolerance система с горещ резерв**. *Аспектът,* в който този предмет се изследва, е **надеждността и безопасността.**

Надеждността ще измерваме с два показателя:

• *готовност* **A(t).** Може да се докаже, че при стойностите на надеждностните параметри λ и параметрите на възстановяване μ, които представляват интерес



Фиг.1

функцията на готовността **A(t)** бързо достига до коефициента на готовност:

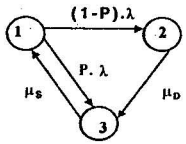
(1) $\lim_{t\to\infty} A(t) = K_A = \frac{\mu}{\mu+\lambda}$, след което готовността не се изменя.

• *математическото очакване на времето между последователните откази* **MTBF,** което е реципрочната стойност на честотата **H** на отказите. Известно е напр. от [1], че

(2) $$H_{SYS} = K_A.\lambda$$

Безопасността е ограничението, което трябва да се спазва при синтезиране на осигурителни системи. Изследването й в тази статия е в аспекта следотказовата безопасност (fail-safe).

Както каналите **B** и **R**, така и системата като цяло, могат да имат три състояния (фиг.2): **1 - работоспособно (A),** когато към процеса се формират коректни управляващи въздействия; **2 - опасно отказово (D),** когато отказът остава неоткрит за време, по-голямо от времето на допустимата от процеса информационна неопределеност t_{DIN}. В този случай некоректните управляващи въздействия могат да имат непредвидими, а значи и опасни последствия.**3 - защитно отказово (S),** когато се формира грешен изходен сигнал, но за t_{DIN} отказът се открива и превключвателят изключва грешните сигнали.



фиг.2

Критерият за безопасност на системата е: *безопасна е система, която при всички допустими откази след време t_{DIN} не подава некоректни сигнали към ОТП.*

Безопасността в разглеждания аспект се оценява по показателите:

• *функция на опасната работа* **D(t),** с който се определя изменението на вероятността системата да се намира в опасно отказово състояние в течение на

отработката t. След достатъчно време тя нараства до коефициента на опасната работа K_D.

• *средно време между последователните опасни откази* **MTBDF**. Намира се като реципрочна стойност на честотата на влизане в опасно състояние H_d.

1.3 *Задачата на това изследване е : да се изведат формули за сравнение на показателите, по които се оценява надеждността и следотказоватa безопасност на микрокомпютърната структура от фиг.1 и да се установи зависимостта им от влияещите фактори.*

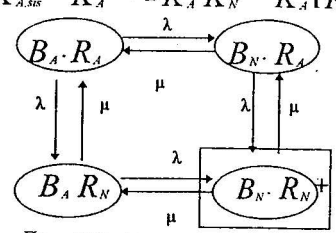
2. Апарат за изследване

Като инструментариум за решаване на задачите, поставени по-горе, се използва теорията на марковските случайни процеси [1]. Приема се, и това е вярно с достатъчна за инженерните изчисления точност, че потокът от откази и възстановявания на двата канала е пуасонов. По-нататък на тази основа се използват вече постигнати в науката решения и резултати.

3. Изследване на надеждността

Всеки от двата канала има готовност K_A и неготовност: $K_N = 1 - K_A$. Граф с който може да се моделира следотказовото поведение на системата, има вид фиг. 3. Без ущърб за общността се приема, че двата канала се идентични, поради което имат еднакви интензивности на откази λ и на възстановявания μ. Очевидно неработоспособно е само състоянието $B_N \cdot R_N$, когато и двата канала са неработоспособни. Коефициентът на готовност $K_{A.sys}$ се определя като сума от вероятностите за пребиваване в другите три състояния:

(3) $K_{A.sis} = K_A^2 + 2K_A K_N = K_A[K_A + 2(1-K_A)]$



фиг.3

Да приемем, че готовността на единичният канал е в порядъка K_A = 0,999. Като се замести в (3) се получава $K_{A.sys}$ = 0,999999. Средното време до отказ $MTBF_{SYS}$ се определя като реципрочна стойност на честотата на отказите $H_{SYS} = 2K_A K_N \lambda$:

(4) $$MTBF_{SYS} = \frac{1}{2K_A(1-K_A)\lambda}.$$

За да се разбере, с колко се подобрява "живота" на системата в сравнение с "живота" на канала, образуваме отношението: (5) $$\xi = \frac{MTBF_{SYS}}{MTBF} = \frac{1}{2(1-K_A)}$$

Ако приемем отново $K_л$ = 0,999 ще установим, че по този показател надеждността е нараснала 500 пъти.

4. Показатели за безопасност на единичния канал

Състоянието на информационно-обработващия канал може да се опише с графа на фиг.2, където значението на състоянията са дадени в т.1.2. Преходите се осъществяват с интензивности, както следва: **p** - вероятност, настъпилият отказ на канала да е открит (*разпознаваемост на отказите)* за време t_{DIN}; μ_D - интензивност на откриване на отказите в опасно състояние **D**; μ_S- интензивност на възстановяване на работоспособното състояние.

Надеждностно-безопасностните показатели на канала могат да се намерят като се реши системата диференциални уравнения на Колмогоров, съставена за графа от фиг.3. В резултат от решението се намират функциите на готовност **A(t),** на опасна работа **D(t)** и на защитни престои **S(t)** [1,3]. След достатъчно дълго време функциите, клонят към пределните си вероятности: $\lim \mathbf{A(t)} = \mathbf{K_{Av}}$ - коефициент на готовност; $\lim \mathbf{D(t)} = \mathbf{K_D}$ - коефициент на опасна работа; $\lim \mathbf{S(t)} = \mathbf{K_S}$ - коефициент на защитни престои.

За пределните вероятности на състоянията се получава [1]:

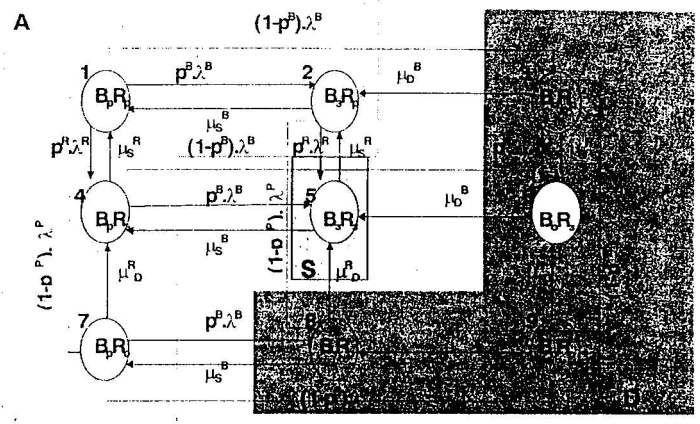
(6)

$$K_{av} = \frac{\mu_D \cdot \mu_S}{\mu_D \cdot \mu_S + \lambda.[\mu_D + \mu_S.(1-p)]} \qquad K_D = \frac{\mu_S.\lambda.(1-p)}{\mu_D \cdot \mu_S + \lambda.[\mu_D + \mu_S.(1-p)]} \qquad K_S = \frac{\mu_D.\lambda}{\mu_D \cdot \mu_S + \lambda.[\mu_D + \mu_S.(1-p)]}$$

5. Моделиране на безопасността на системата

5.1. Граф на парциалните състояния

Съгласно метода за моделиране на безопасността на система [2] се строи граф на парциалните й състояния (фиг.4), където $\mathbf{B_i}$ $\mathbf{R_j}$ са комбинациите от състоянията на каналите **B** и **R**, а i и j приемат означенията: **a** - работоспособно, **s**- защитно и **d**- опасно. По надолу се използват еднакви означения за двата канала поради предположението за тяхната еднаквост. След това се прилага възприетият за случая критерий за безопасност на системата, за да се определи принадлежността на парциалните състояния към работоспособното, опасно и защитно състояния на системата. Въз основа на критерия за безопасност (т.1.3) се определят следните принадлежности: В състояние 1, 4 и 7 канал **B** е работоспособен и независимо от състоянието на канал **R** системата е в състояние на готовност. В състояние 2 канал **B** е отказал защитно, поради което към процеса е включен канал **R**, който е работоспособен - състояние на готовност. В състояние 3, 6 и 9 канал **B** е отказал опасно, поради което не е осъществен преход към канал **R**. Системата работи опасно, тъй като в канал **B** отказът не е открит. В състояние 5 каналите са защитно отказали, поради което и системата е в защитно състояние. В състояние 8 канал **B** е защитно отказал, а канал **R** - отказал опасно.Системата е в опасно състояние. Вероятността за всяко парциално състояние се получава като произведение от вероятностите за състоянията, комбинация от които е то.



Фиг.4

5.2 Вероятност за опасна работа

За да се намери **функцията на опасната работа на системата** трябва да се сумират вероятностите за опасните парциални състояния. След тези прости операции и преработка на получения резултат се получава:

(7) (а) $\mathbf{D_{sys}(t) = D(t).\,[1+.S(t)]}$ (б) $K_{D.SIS} = K_D.[1 + K_S]$

На фиг.5 е показана *функцията на опасна работа на системата* за определен набор от практически интересни стойности.

- Вижда се, че тя може да е екстремална. Наличието на максимум на функцията за опасна работа потвърждава направеното заключение в [3,4], че пределната вероятност за опасна работа не е максималната й стойност.
- С намаляване на параметъра **p** и с увеличаване на интензивността на отказите λ се увеличава коефициента на опасна работа.
- С увеличаване на μ_S изчезва екстремумът. С намаляване на **p** вероятността за опасна работа се увеличава значително. Аналогичен резултат се получава и при намаление на μ_S.

5.2. Средно време между опасните откази

За да се намери показателят MTBDF, трябва да се изходи от формулите на Кохс [1] и да се проследят преходите в графа на фиг.3. Получава се:

(8) $H_0=(1-p).\lambda K_A.(1+K_S) + p.\lambda.K_A.K_D$

За да се определи влиянието на структурата върху безопасността на системата, може да се образува отношението:

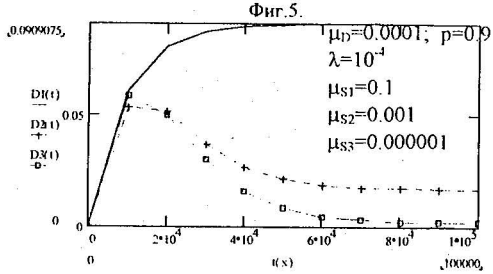
(9) $\eta = \dfrac{MTBF_{SIS}}{MTBF}$,

с което се установява как се променя безопасността на системата в сравнение с безопасността на канала, измервана с този параметър. Като се замести в (9) се получава:

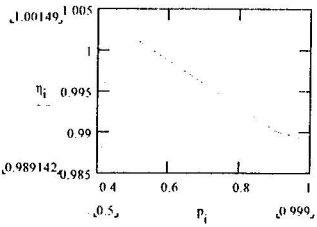
$$(10)\ \eta = \frac{1-p}{(1-p)(1+K_S)+p.K_H}$$

На базата на това уравнение на фиг.6 е построена кривата на зависимостта η(p) за практически интересни стойности на надеждностно-безопасностните параметри.

Фиг.5.



Фиг.6



Вижда се, че ако разпознаваемостта на отказите е малка (p=0,5÷0,8) безопасността на единичния канал е по-ниска от тази на системата (η>1). Ако е висока (p=0,99÷0,9999), безопасността е по-ниска от тази на канала.

6.Изводи

1. Математическото очакване на времето на живот на системата е на порядъци по-голямо от това на канала и зависи от неговите параметри λ и μ съгласно установената в (4)зависимост.
2. Разпознаваемостта на отказите води до намаляване на вероятността за опасна работа на канала но влошава безопасността на системата по формула(8).
3. В изследваната система надеждността се повишава значително за сметка на слабо влошаване на безопасността й.

Литература

1. Христов,Хр., *"Основи на осигурителната техника"*, изд. "Техника", София, 1990г.
2. Хр.Христов, Н.Стойчева, *Алгоритми за аналитично определяне на безопасността на осигурителни системи,* Сборник доклади от научна конференция на ВВТУ "Т.Каблешков", 1992г.
3. Сапожников,Вл.В., Сапожников,В.В., Христов, Х.А., Гавзов, Д.В., *"Методы построения микроелектронных систем железнодорожной автоматики и телемеханики"*, "Транспорт", Москва, 1995
4. Christov,Ch, N.Stoycheva, *Railway real-time control systems- modeling of dynamic redundant systems reliability*, Second International Scientific Conference "Modern Supply Systems and Drives for Electric Traction", Conference Proceedings, Poland, Warsaw, October, 1995, pp.42-47