Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 17, брой 3, 2019 г.
Научно списание **http://www.mtc-aj.com** **статия № 1884**

ИЗСЛЕДВАНЕ ВЪРХУ ВЕРОЯТНОСТТА ЗА ОПАСЕН ОТКАЗ В КРИТИЧНИ ПО БЕЗОПАСНОСТ СИСТЕМИ ОТ ВИДА 2V2

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

Висше транспортно училище „Тодор Каблешков”
София 1574, ул. „Гео Милев” № 158
БЪЛГАРИЯ

Ключови думи*: критични по безопасност системи, поведение на системите след отказ, надеждност, безопасност, опасни откази.*

Резюме: *Дефинирано е понятието за опасен отказ в критичната по безопасност осигурителна система. Поставена е задачата за аналитично изследване на вероятността за опасен отказ в широко популярен клас критични по безопасност системи, известни като* $2 \vee 2$ *структури. В контекста на системните откази е направена съпоставка между компютърната обработка и телекомуникационния пренос на съобщения. Известно е, че грешките по импулс на отделните разряди са (се приемат) независими, а кодовото разстояние D между функционалните вектори е средство за ефикасна защита от смущения при линийния пренос на информацията. С увеличаването на дистанцията D вероятността* q^D *за преход към грешен вектор рязко намалява. При компютърната обработка този метод за защита не работи. Един кой да е отказ в микропроцесорното устройство, независимо от неговата природа (хардуерна или софтуерна), може да породи с еднаква вероятност всички грешни изходни вектори* $N=2^v$*, където v е броят на разрядите на вектора. Изследването е направено при приемането на това условие. Върху безопасността на* $2 \vee 2$ *системи влияят две групи откази: Common-Mode Failure (CMF) и accidentally non identification (ANI). Статията е част от по-широко изследване, което обхваща и двете групи, но е фокусирана върху втория вид причини - случайно неоткритите откази ANI. Намерени са формули за оценка на ANI опасните откази и тяхната вероятност в зависимост от дължината на векторите.*

1. ПОСТАНОВКА

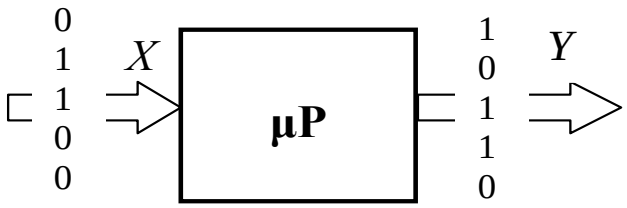
Опасният отказ на компютърната осигурителна система се дефинира като събитие, при което на изхода ѝ се появява сигнал или последователност от сигнали (поведение), различни от функционалните или от предварително определените като защитни.

В критичните по безопасност системи [1,2] се прилагат хардуерни и софтуерни методи и решения, чрез които вероятността за опасен отказ се намалява на порядъци и достига до стойности, хармонизирани със стандартите за съответния клас системи. Измежду множеството *fault-tolerance* [3,4,7] и *fail-safe* методи [5, 6] най-популярна е структурата, известна като $2 \vee 2$ fail-safe система. Цел на настоящата статия е да

моделира вероятността за опасен отказ в критичните по безопасност осигурителни системи от този клас.

2. ОПИСАНИЕ НА СТРУКТУРАТА

Микропроцесорното устройство *μP* (фиг.1), разглеждано като "черна кутия" $1 \vee 1$, е показано на фиг.1. При входен вектор от логически сигнали X_i (x_1 x_2…, x_w) на изходите на микропроцесорното устройство се появява функционален вектор Y_j(y_1 y_2…, y_v) с дължина V бинарни разряда. Съдържателно векторите от входния сигнал X_i, зависят от състоянието на вътрешната памет и от алгоритъма на работа на устройството.



Фиг.1 Обобщена схема на микропроцесорно устройство

В такива устройства вероятността за опасен отказ е твърде висока, поради което те не се използват за високотговорни приложения.

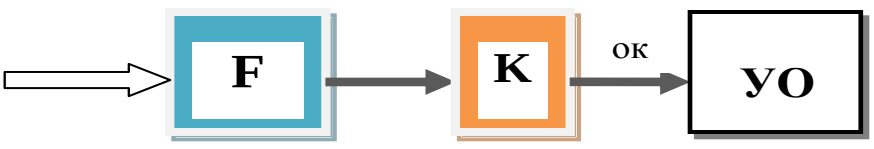
Решенията на проблема се търсят в две посоки:

1. Повишаване на надеждността на много порядъци, най-често чрез отказоустойчиви методи. Така се намалява вероятността за отказ като цяло, включително и като нейна част, вероятността за опасна неработоспособност.

2. Системата, в която е устройството $1 \vee 1$, се проектира с *fail-safe* следотказово поведение. Fail-safe решенията са възможни само тогава, когато естеството на управлявания процес позволява да се премине в предварително дефинирано безопасно състояние.

Статията ограничава обхвата си във втория подход. В съвременните компютърно базирани системи се използва негова *quazi fail-safe* модификация (Фиг.2). Едно микрокомпютърно устройство **F** (от вида на фиг.1) работи като функционално, а друго специфично високоотговорно устройство **K** го контролира, т.нар. F-K структура [4, 5 и др.]. Контролното устройство ***K*** трябва да притежава способността да разпознае отказа и своевременно да превключи към дефинираното следотказово защитно състояние, Това се случва твърде често като изключи устройството или прекрати достъпа до него.

Тази структура дава решения, но поражда и проблеми. Най-същественият от тях е идентификацията на отказите на устройството **F**.

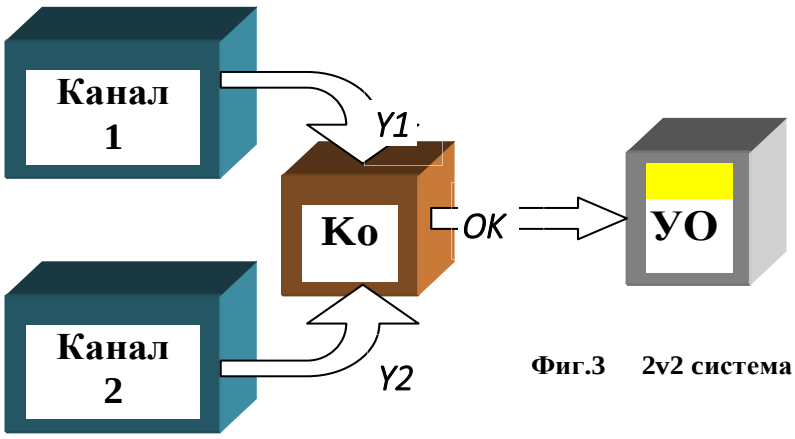


Фиг.2 F–K структура

Откриването на отказа на функционалното устройство **F** в цифровите системи не е тривиална задача. Една възможност е **K** да проверява изходните вектори на четност, но възможностите за подобни методи са силно ограничени. Има и още една много

съществена причина, свързана с особеностите на компютърните устройства, която е решаваща.

В телекомуникациите вероятността да се приеме от линията грешен вектор се изчислява като резултат от умножението на вероятностите за възникване на „грешки по импулс“ в неговите разряди, тъй като отделните битове имат независими „грешки по импулс“. Например, ако грешката по импулс е с вероятност $q = 1.10^{-6}$, вероятността изкривен вектор с два променени бита да се приеме за верен, е $q^2 = 1.10^{-12}$. Кодовото разстояние D между функционалните вектори е средство за ефикасна защита. С увеличаването на D намалява функционалното векторно пространство с мощност Card 2^{ν} , а вероятността q^D за преход към грешен вектор рязко намалява.



Фиг.3 2v2 система

Този метод в компютрите не работи. Тук не се пренасят съобщения по телекомуникационни канали, които могат да бъдат поразени от смущения. Кодовото разстояние губи смисъл. Един отказ в микропроцесорното устройство, независимо от неговата природа (хардуерна или софтуерна), може да породи грешни изходни вектори с еднаква вероятност, без разлика и без връзка с кодовото разстояние между тях. В грубо приближение може да се приеме, че какъв да е отказ в „черната кутия“ предизвиква появата на кой да е от възможните изходни вектори с еднаква вероятност:

$$q = \frac{1}{2^{\nu}} \quad (1)$$

Затова се търсят други, по-ефективни решения, извън Хеминговата дистанция.

Един от най-широко използваните методи е показан на фиг.3. Двете структурни единици (канал 1 и канал 2) от вида на фиг. 1 са постоянно включени в схемата. Изходните им вектори *Y1* и *Y2* с еднаква дължина ν се сравняват във всеки момент от работата на компютърните канали. Тяхното съответствие е критерий за изправност, при която компараторът дава ОК за изпълнение на управляващото въздействие върху обекта УО (Фиг.3). Контролиращото устройство *K*, условно включва компаратора *Ко* и втория канал. Системата е известна като $2 \vee 2$.

3. ДВЕ ГРУПИ ОТКАЗИ – CMF и ANI

Извеждането на нефункционален и възможно опасен сигнал, може да се създаде **по две групи причини**:

1. ***Едновременни независими откази*** в двата канала предизвикват грешни вектори, които в общия случай се разпознават, защото водят до различни изходни вектори в двата канала, а от там - към идентификация на отказ, снемане на ОК и прекъсване на достъпа до УО, което е безопасно. Но, **по случайност,** и двата

сравнявани вектори могат да са едни и същи (или съответни), поради което отказите остават неидентифицирани (**accidentally non identification - ANI**).

2. ***Общи за двата канала причини за отказ*** **- Common-Mode Failure** (CMF). CMF-отказите (**втората група**) са общи за $2 \vee 2$ системата и влияят по един и същ начин крайните резултати от работата на двата канала. Те водят до еднакви (съответни) и *неоткриваеми* чрез сравнение откази, защото компараторът дава ОК на грешено изходно въздействие. Тази група е предмет на следващото изследване.

Безопасността на двуканалните системи се опира на предположението, че каналите са независими, CMF-причините са сведени до минимум, а вероятността за неразпознати ANI е достатъчно малка.

4. ВЕРОЯТНОСТ ЗА СЛУЧАЙНО НЕОТКРИТИ (ANI) ОТКАЗИ

За да има грешни, но еднакви и, оттам, неразпознаваеми чрез сравнение изходни вектори на двата канала, резултатите им трябва да се изкривят от отказите така, че да станат един и същ следотказов вектор Y_j **.** При равно вероятно разпределение на грешните вектори вероятността и на двата канала да се изведе един кой да е от всички 2^v вектори е:

$$(2) \qquad q_{i1} q_{i2\ q_1=q_2} = \frac{1}{2^v}\frac{1}{2^v} = \left(\frac{1}{2^v}\right)^2 .$$

Пример:

Нека v =3, а векторите да се обозначат по възходящ ред на десетичните номера. След отказ в двуканалната система с $2^3 = 8$ вектора. Дава им се десетичен номер:

вектор	№	вектор	№	вектор		вектор	№
000	**0**	010	**2**	100	**4**	110	**6**
001	**1**	011	**3**	101	5	111	**7**

Могат да се образуват четири вида комбинации от вектори (фиг.4) от двете страни на компаратора:

1. *Множество на векторите при разпознати откази* (на матрицата не са маркирани). ОК не се дава поради различието им. Броят им е $2^v - v$.

2. *Единичното множество на функционалните вектори* $\boldsymbol{Y_i}$**.** Управляващото въздействие се валидира, тъй като това е верният вектор. Генерират го и двата канала. Нека в даден момент той да е №3 (010). Комбинацията от верни резултати на двата канала 33 на фиг. 4 е маркирана в червено.

3. *Множество* на векторите ANI, неразпознаваеми чрез сравнение (с еднакви номера), получени след откази в двата канала (маркирани в жълто). След сравнението се получава фалшиво ОК, защото векторите не са функционалните. Възможни са $2^v - 1$ *фалшиви съвпадения* ANI. Броят им е намален с единица заради верният $\boldsymbol{Y_i}$**.**

Канал 1↓

11	21	31	41	51	61	71	81
12	22	32	42	52	62	72	82
13	23	33	43	53	63	73	83
14	24	34	44	54	64	74	84
15	25	35	45	55	65	75	85
16	26	36	46	56	66	76	86
17	27	37	47	57	67	77	87
18	28	38	48	58	68	78	88

Канал 2 →

Фиг. 4 Матрица на векторите

4. Множество *на грешните вектори*, в които единият от двата вектора в комбинацията е верният (маркирани в зелено). Отказал е само единият от двата канала и неговият вектор може да заеме всички стойности.

Ако случайно се получи фалшива

комбинация, макар че не трябва да дава съгласие, компараторът ще бъде "подведен" и ще даде ОК не само на 3-та, но и на 1-та, j-та, k-та и т.н., и във всички останали $2^{\nu}-1$ позиции с еднакви номера (маркирани в жълто), в конкретния случай - 7. За общия случай вероятността за една коя да е едноименна комбинация от двете страни на компаратора (с еднакви номера на изходни вектори) е

$$q.q = q^2 = \left(\frac{1}{2^{\nu}}\right)^2 \quad (3)$$

където q е вероятност да се появи даден (кой да е) вектор след отказ на компютъра (канала). Тъй като от маркираните в жълто съчетания автентичният вектор е само един, то броят на фалшиви разрешения ОК ще бъде $2^3 - 1 = 8 - 1 = 7$, а вероятността такова да се състои ще е

$$Q_{ani}\underset{\nu=3}{=}(2^3-1)\left(\frac{1}{2^3}\right)^2 = 0{,}109 \quad (4)$$

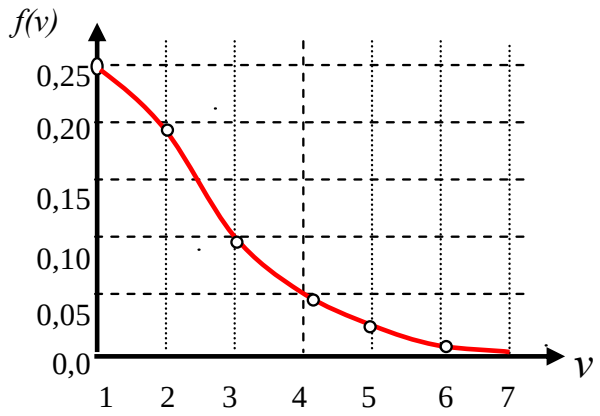
В общия случай броят на фалшиви разрешения ОК от вида ANI е:

$$f(\nu) = \left(2^{\nu}-1\right)\left(\frac{1}{2^{\nu}}\right)^2, \quad (5)$$

Като се изследва функцията $f(\nu)$ ще се установи, че нейната най-висока и неблагоприятна стойност е при $\nu = 1$:

$$f(\nu)_{max} = 0.25. \quad (6)$$

С увеличаване на дължината на сравняваните вектори $f(\nu)$ намалява, както е показано на фиг.5, като при $\nu \to \infty$ клони към нула.



Фиг.5. Зависимост на вероятността за случайно неидентифицирани откази от броя на векторите

Както се отчете вероятността Q_{a1} да настъпи какъв да е отказ в канал 1 и в Q_{a2} канал 2, вероятността Q_{ani} за случайно неидентифициран отказ ще бъде:

$$Q_{ani} = (2^{\nu}-1)\frac{Q_{\alpha 1}}{2^{\nu}}\frac{Q_{\alpha 2}}{2^{\nu}}, \quad (5)$$

Ако каналите са еднакви по надеждност, имат равни вероятности за отказ $Q_{a1} = Q_{a2} = Q_a$, както се предполага при настоящото разглеждане,

(6) $Q_{ani} = (2^{\nu} - 1)\left(\frac{Q_{\alpha}}{2^{\nu}}\right)^2$

С уравнение (4) може количествено да се оценява вероятността за случайна неидентификация Q_{ani} на едновременни независими откази в двата канала.

ЗАКЛЮЧЕНИЕ

Поставена е задачата за изследване на вероятността от случайно съвпадение на грешни, но съответни вектори в двата канала на критична по безопасност система от вида $2 \vee 2$. *Намерена е вероятността f(v) за случайно съвпадащи грешни вектори в двата канала, при които отказът не може да се идентифицира, в зависимост дължината на сравняваните вектори v.* Установена е и графична зависимост, която показва, че в реалната практика тази вероятност е много малка и при вектори със стандартна дължина благоприятства достигането на стандартите за безопасност. Например, при 32 битови вектори тя достига до 0,0000152.

Този подход и схемите на негова основа се използват от много производители във всички сфери на приложение на критични по безопасност системи, но най-вече в железопътния транспорт, от фирми като Siemens, Bombardier, Thales, и др. Разликата в техническите решения и спрямо приетото в тази постановка най-често е в това, кога и какво се сравнява от компаратора К.

ЦИТИРАНА ЛИТЕРАТУРА

[1] Христова М. Софтуер за критични по безопасност системи: проблеми и решения. Издателство ВТУ „Тодор Каблешков”, София, ISBN 978-954-12-0240-1, 2016

[2] Smith David J., K. GL Simpson.The Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety: IEC 61511 (2016 Edition) & Related Guidance

[3] Popov G. N., M. E. Nenova, K. Raynova, Reliability Investigation of TMR and DMR Systems with Global and Partial Reservation, Published in Seventh Balkan Conference on Lightingh, DOI:10.1109/balkanlight.2018.8546926, 2018

[4] Lee P. A., T. Anderson. Fault Tolerance: Principles and Practice, Springer Scince&Business Media, pp. 51-62, 2012

[5] Hristov Hr., M. Hristova, COMPUTER CONTROL SYSTEMS WITH CRITICAL SAFETY APPLICATIONS: PROBLEMS AND SOME SOLUTIONS, Journal of Information Technology and Applications (JITA), ISSN 2232-9625 (PRINT), EISSN: 2233-0194 BANJA LUKA, JITA 7(2017) 2:61-68, vol. 7, issue 2, 2017

[6] Hristov H., W. Bo, Safety Critical Computer Systems: failure Independence and software diversity effects on Reliability of dual channel structures, Information Technologies and Control, № 2, pp. 9-18, 2014

[7] Popov G., Raynova K., Comparative dependability analysis of TMR and DMR systems with general and separate reservation, ITEO'2017, Information Technologies for E-Learning, PanEvropski Universitet Apeiron, Banja Luka, 29-30 Sept, ISBN 978-99976-34-13-9

STUDY ON THE PROBABILITY OF A DANGEROUS FAILURE IN SAFETY CRITICAL SYSTEMS OF THE TYPE 2V2

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

Todor Kableshkov University of Transport
1574 Sofia, 158 Geo Milev Str.
BULGARIA

Key words: *Safety Critical Systems, system behaviour after failure, reliability, safety, dangerous failures.*

Abstract: *The concept of a dangerous failure in the safety critical system is defined. A task is set to analyze the probability of a dangerous failure within a widely popular class of safety critical systems known as* $2 \vee 2$ *structures.*

In the context of system failures, a comparison is made between computer processing and telecommunication transmission of messages. It is known that impulse errors of the individual discharges are (assumed as) independent and the code distance D between the functional vectors is a means of efficient protection against interference during the linear transmission of information. With the increase in distance D the probability q^D *to transition to a wrong vector abruptly decreases. In computer processing, this security method does not work. Any failure in a microprocessor device, irrespective of its nature (hardware or software), may generate with equal probability all erroneous output vectors* $N = 2^v$*, where n is the number of vector discharges. The study is performed with the assumption of this condition. Two groups of failures influence* $2 \vee 2$ *system security: Common-Mode Failure (CMF) and Accidental Non-Identification (ANI). This paper is a part of a more extensive research that covers both groups, and yet it focuses on the second type of causes – accidentally non-identified failures ANI. Formulas are elaborated for assessment of ANI dangerous failures and their probability depending on the length of the vectors.*