Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 16, брой 3/2, 2018 г.
Научно списание **http://www.mtc-aj.com** **статия № 1737**

ОТНОСНО ВЪЗМОЖНОСТИТЕ ЗА МОДЕЛИРАНЕ НА БЕЗОПАСНОСТТА ПОСРЕДСТВОМ ДЪРВОТО НА ОТКАЗИТЕ

Емил Иванов, Емилия Димитрова, Пламен Атанасов
eivanov.09@abv.bg, edimitrova@bitex.bg, p.atanasov.90@gmail.com

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

Ключови думи: *динамично, дърво, откази, надеждност, безопасност, рискови системи, осигурителни системи.*

Резюме: *Дървото на отказите се наложи, като основен инструмент за моделиране (количествено и качествено) поведението на рисковите системи. Безопасността на човека зависи от правилното функциониране на тези системи. Те управляват особено отговорни технологични процеси (в транспорта, авиацията, енергетиката, медицината и т.н.), чиито откази могат да доведат до загуба на живот, на големи човешки ценности. Споменатите модели всъщност интерпретират надеждностното поведение на техническите системи. Техен недостатък е, че не отразяват наличието на защитни откази. Получава се сливане на понятията надеждност и безопасност. Надеждността (най-общо) е способността на обекта да запазва качеството си на съответствие (съществените си свойства) в течение на отработката (времето за работа) при зададени ограничения. Безопасността е съхранимост, отсъствие на недопустим риск. Рискът е мярка за възможните загуби от нежелани събития, чието настъпване е вероятно. При това сливане на двата термина се допуска грешка, която е в полза на безопасността (реалната безопасност е по-висока от изчислената), но е в ущърб на стойността на системата (финансовите средства за реализация на системата ще са повече). За да определим реалната безопасност и за да има икономически ефект е необходимо моделът да отрази вида на отказите (защитни и опасни).*

В настоящата работа се предлагат нови символи дървото на отказите, които ще позволят да се използва дървото на отказите за моделиране реално на безопасността, като се отчитат само опасните откази.

1. УВОД

Развитието на средствата за производство, съсредоточаването на все по-голямо количество енергия в тях и произтичащото от това нарастване на количеството аварии с повишаване на броя на засегнатите е най–сериозния проблем пред съвременното общество. Авариите в съвременната техносфера по своите мащаби и тежки последствия стават сравними с природните катастрофи и разрушителните последствия от военните

конфликти. Освен блага, някои технологични процеси могат да носят риск за здравето и живота на хората, така също и за околната среда. Тези технологични процеси се наричат *рискови*. Типични примери са ядрената енергетика, авиацията, химическата промишленост, жп транспорт. Техническите системи, управляващи тези технологични процеси се наричат *рискови*. Обществения интерес изисква тези системи да не допускат нарастване на риска за населението над определени приемливи граници.

Процесите на възникване на аварии по вина на управляващите технически системи са вероятностни. Формалното им изследване се основава на теорията на надеждността. Като средство за моделиране на надеждностното поведение на системите се налага *Дървото на отказите,* поради нагледността му и възможността да отрази, както техническата, така и организационната част от причините за опасно развитие на процеса.

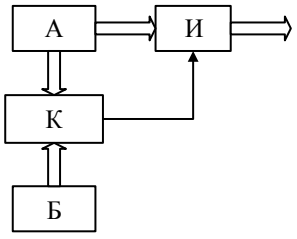
При част от рисковите технологични процеси съществува *критерий за желателно следотказово поведение.* Управляващите такива процеси системи може да се изграждат на така наречения fail-safe принцип. Безопасното поведение се постига, не чрез висока надеждност, а чрез защитно при отказ поведение – отказите водят до желателното развитие на процеса. Това обосновава и различието в понятията „надеждност“ и „безопасност“.

Прилагането на дървото на отказите за моделиране безопасностното поведение и на системи, изградени на fail-safe принцип, предполага грешка, произхождаща от сливането на понятията „надеждност“ и „безопасност“.

В настоящата работа се предлагат нови символи, които позволяват адекватното отразяване на безопасностното поведение на fail-safe системи.

2. ЛОГИЧЕСКИ СИМВОЛ „СИМЕТРИЧНИ ОТКАЗИ“

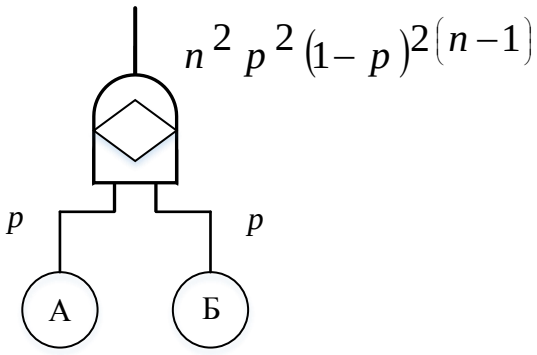
Безопасното поведение в голяма част от рисковите системи се основава на така наречения „двуканален принцип“ (фиг.1). Две еднакви устройства работят едновременно, като еднаквото състояние на характерни (контролни) точки от апаратурата е критерий за изправност. Контролното устройство (К) следи работата на двете устройства и при нарушаване на критерия за изправност привежда системата в защитно състояние, чрез изключвателя И. Последният изключва подаването на команди към обектите, тъй като няма гаранция, че те са безопасни. Появяването на разлика е критерий за наличие на отказ в едно от двете функционални устройства А или Б.



Фиг.1. Двуканална fail-safe структура

Опасна ситуация по вина на управляващата техническа система може да възникне, ако за кратък интервал от време в двете контролирани устройства възникнат еднакви откази (*симетрични откази*). Интервалът от време се определя от инертността на контролиращото устройство К.

Предложеният логически символ (фиг.2) моделира такава ситуация. Той има един изход и два входа. Изходът се активира само когато в двата блока възникнат *симетрични откази*.



Фиг.2. Логически символ
„Симетрични откази“

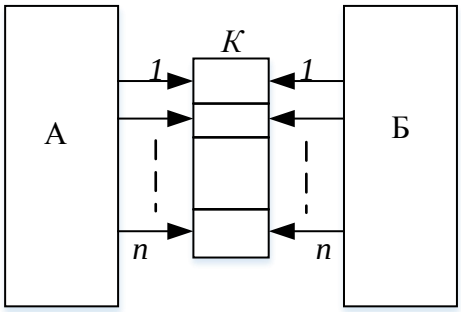
Ако се контролират n контролни точки (фиг.3), вероятността за отказ в една определена контролна точка се определя съгласно формулата на Бернули:

(1) $$P_n(1) = C_n^1.p^1.(1-p)^{n-1} = \mathrm{n}.p.(1-p)^{n-1}$$

p е вероятността за отказ (за появяване на грешна, нефункционална логическа стойност) в коя да е контролна точка.

Вероятността за отказ в една определена контролна точка във втория канал се определя със същия израз. Тогава вероятността за симетричен отказ е:

(2) $$P_n(1) = n^2.p^2.(1-p)^{2(n-1)}$$

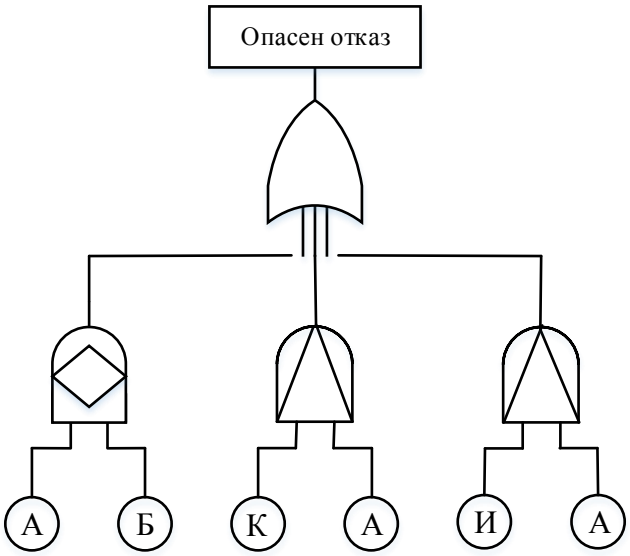


Фиг.3. Контролни точки

3. ПРИЛОЖЕНИЕ

На фигура 4 е представено дървото на отказите за техническа система с двуканална структура. Опасност породена от отказ в техническата система изградена на двуканален принцип може да възникне в резултат на едно от следните три събития:

- Симетрични откази в двата канала А и Б. Двете събития са свързани с логическия символ „симетрични откази”;
- Опасни откази в контролното устройство К и функционалното устройство А, възникващи последователно в реда на изброяване;
- Опасни откази в изключвателя И и функционалното устройство А, възникващи последователно в реда на изброяване.



Фиг.4. Дърво на отказите
за двуканална техническа система

4. ИЗВОДИ

Методът за анализ на риска с дърво на огказите е изключително нагледен. Пряко е свързан с реалните процеси в изследваната система. Затова е един от най-често използваните. В настоящата работа е предложен нов логически символ, който позволява този метод да се прилага при анализа на риска породен от техническите системи, изградени на fail-safe принцип.

Новият символ позволява да се отчетат предимствата на fail-safe подхода.

5. ЛИТЕРАТУРА

[1] Иванов Е., Атанасов П., Дървонто на отказите като системен модел на надеждностното поведение, „Механика, транспорт, комуникации”, том 14, брой 3/2, стр. IX-38 - IX-43, 2016.
[2] Иванов Е., Ц. Симеонова, Изследване влиянието на отказите върху индивидуалния риск при F-K структури, В сб. на 20-та международна научна конференция на ВТУ „Т. Каблешков”, „Механика, транспорт, комуникации”, ч. 3, стр. VIII-32, София, 2011.
[3] Христов Х., Основи на осигурителната техника, Техника, С., 1990.
[4] Boudali, H., P. Crouzen, M. Stoelinga, A Rigorous, Compositional, and Extensible Framework for Dynamic Fault Tree Analysis, IEEE Transactions on Dependable and Secure Computing, Vol. 7, No. 2, April-June 2010.
[5] Medikonda B. and S. Panchumarthy, A Framework for Software Safety in Safety-Critical Systems. SIGSOFT Software Engineering Notes March 2009, Volume 34, Number 2, Pages 1-9.
[6] Tong Y.C., Literature Review on Aircraft Structural Risk and Reliability Analysis. DSTO-TR-1100, AR-011-772, Melbourne, Victoria 3207, 2001.
[7] Zhu G., Y. Sun, G. Zhao, A Dynamic Fault Tree method for availability assessment of the repairable gas transmission system, Safety and Reliability of Complex Engineered Systems: ESREL 2015, pp. 1897-1903, 2015.

ON THE POSSIBILITIES FOR MODELING OF SAFETY BY USING FAULT TREES

Emil Ivanov, Emilia Dimitrova, Plamen Atanasov
eivanov.09@abv.bg, edimitrova@bitex.bg, p.atanasov.90@gmail.com

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

Key words: *dynamic, tree, failures, dependability, safety, risk systems, security systems.*

Abstract: *The dynamic fault tree established itself as a primary instrument for modeling (quantitative and qualitative) the behavior of risk systems. The safety of man depends on the correct functioning of these systems. They control crucial technological processes (in transport, aviation, energetics, medicine etc.), which failures can lead to life loss, loss of great human values. The mentioned models actually interpret the dependability behavior of technological systems. Their disadvantage is that they do not take into account the presence of protective failures. A merge of the notion of dependability and safety is obtained. The term dependability (generally) is the property of the object to keep the quality of compliance (the essential properties) over the course of working (the time of operation) at given restrictions. The term safety is storage, lack of impermissible risk. Risk is a measure for the possible losses from undesirable events, which occurence is probable. This merge of the two terms leads to an error, which is in favor of safety (the real safety is higher than the calculated), but it is in detriment of the value of the system (the funds for realization of the system will be more). In order to determine the real safety and to have economical effect, it is necessary for the model to take into account the type of failures (protective and hazardous).*

In the present paper, new symbols for the fault tree are presented, which will allow the fault tree to model the real safety, as only the protective failures are taken into account.