Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 14, брой 3/2, 2016 г.
Научно списание http://www.mtc-aj.com **статия № 1397**

ДЪРВОТО НА ОТКАЗИТЕ КАТО СИСТЕМЕН МОДЕЛ НА БЕЗОПАСНОСТТА НА РИСКОВИТЕ СИСТЕМИ

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

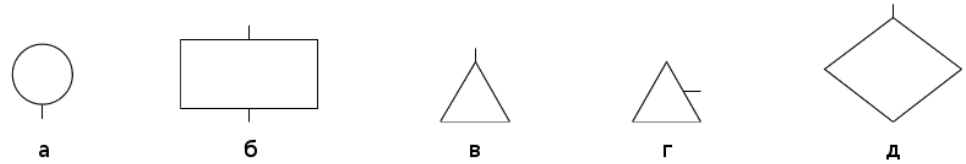
Висше транспортно училище „Тодор Каблешков”
София, бул. „Гео Милев” №158
БЪЛГАРИЯ

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

Резюме: *Човешката дейност е съпроводена с разширяване обхвата на така наречените „Рискови системи”. Това са системи за управление на технологични процеси, които при определени нарушения, могат да предизвикат значителни материални и морални щети. Оценката на риска за такива нарушения се превръща в основна част от развойната и инвестиционна дейност. В предложения доклад е направен един подробен анализ на дървото на отказите, като надеждностен модел на системите. Направени са класификации, посочени са предимства и недостатъци на отделните разновидности и областите на приложение. Известното дърво на отказите не може да моделира надеждностното поведение на системи, в които е от значение последователността на възникване на отделните откази. Представено е така наречената Динамично дърво на отказите, което моделира процесите във времето. Отчита и реда на възникване на отказите, което го прави приложимо за всяка система.*

1. УВОД

През последните години, като надеждностен модел на различни системи се налага дървото на отказите (ДО). То представлява ацикличен насочен граф, състоящ се от два вида възли: събития и логически символи. Събитието е явление вътре в системата, най-често отказ на подсистема от един компонент. На фиг.1.1 са показани символите за събития. Те могат да се разделят на базови събития (БС) (фиг.1.1а), които се случват произволно, и на междинни събития (фиг.1.1б), които са причинени от едно или повече БС. Те са подходящи за документиране, но не влияят върху анализа на ДО. Върховото събитие се намира най-отгоре на анализираното дърво и моделира отказа на разглежданата (под)система. Ако ДО е твърде голямо за една страница, се използват



Фиг.1.1 – Символи на събития в ДО

триъгълници (фиг.1.1в,г) за преход между няколко ДО, които да играят ролята на едно цяло. Понякога подсистемите не са БС, но няма достатъчна информация за него или не се счита за важно да се развие подсистемата в клон. Това е изобразено на фиг.1д.

Логическите символи представят разпространението на отказите в системата, например как отказите в подсистемите се обединяват, за да предизвикат системен отказ. Всеки логически символ има един изход и един или няколко входове. Използваните логически символи в статичните ДО (а също и в динамичните ДО) са илюстрирани на фиг.1.2. Знакът И е представен на фиг.1.2а и изходното събитие възниква, ако всички входни събития протичат едновременно. Знакът ИЛИ е изобразен на фиг.1.2б и изходното събитие настъпва, ако възникне кое да е от входните събития. Знакът за мажоритиране m от N се намира на фиг.1.2в и изходното събитие се случва, ако възникнат най-малко m от N входни събития. Знакът за забрана е показан на фиг.1.2г и входното събитие предизвиква появата на изходното, но само, ако е възникнало едно друго – условно.

Фиг.1.2 – Логически символи в СДО и ДДО

В този им вид ДО са *статични* надеждностни модели (СДО) (standard/static fault trees - SFTs). Те имат предимствата да са сравнително опростени и информативни, но те не могат да моделират основни и често случващи се особености на надеждността. Поради тази причина са предложени някои допълнения съм СДО и в резултат са получени нови видове ДО. За разлика от СДО, те могат да опишат някои характерни особености на системите, като например: управление на излишъка (при fault-tolerant системи), различни режими на работа и зависими събития. СДО се прилагат за моделиране безопасността на рискови системи, но те отчитат само надеждността на отделните елементи на системите. Това води до опростяване на количествените изчисления, но до определена неточност при fail-safe решения в посока на по-ниско ниво на безопасност от реалното, което означава по-скъпи системи от необходимото, тъй като не се отчита възможостта системите да отказват защитно.

В работата авторите анализират възможността, за преодоляване на посочения проблем.

2. ДИНАМИЧНИ ДО – ОПИСАНИЕ И АНАЛИЗ

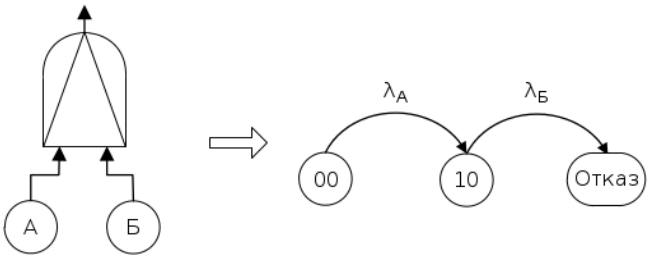
СДО моделират системи, при които комбинация от отказали компоненти води до отказ на системата, независимо кога всяко от тези събития се е случило. В действителност, някои системи могат да останат работоспособни при определена последователност от откази, но да откажат, ако същите компоненти загубят своята работоспособност в друг ред. Предложени са [1, 4] «Динамични ДО» (ДДО) (DFTs), посредством които може да се моделира поведението на системата във времето.

Тъй като ДДО разглеждат поведението на системата във времето, методите за количествен и качествен анализ на СДО не могат директно да се приложат върху ДДО. Ще се разгледат само някои количествени методи, като за по-прости ДДО се използват трансформации до Марковски вериги (МВ) (с дискретни състояния в непрекъснато време), а за по-сложни ДДО може да се приложи директно симулация с изчислителен софтуер/хардуер по метода Монте Карло. Други методи се споменават в [1].

Структурата на ДДО е сходна с тази на СДО, като разликите се състоят в добавянето на някои нови логически символи. Фиг.2.1 до фиг.2.4 изобразяват

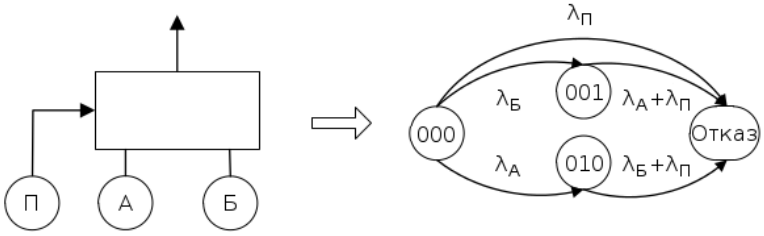
преходите от тези нови логически символи в ДДО към МВ при невъзстановими системи, като интензивностите на отказите на БС са означени с λ.

- Приоритетно И (PAND) - изходът става активен когато всички входове откажат отляво надясно (фиг.2.1).



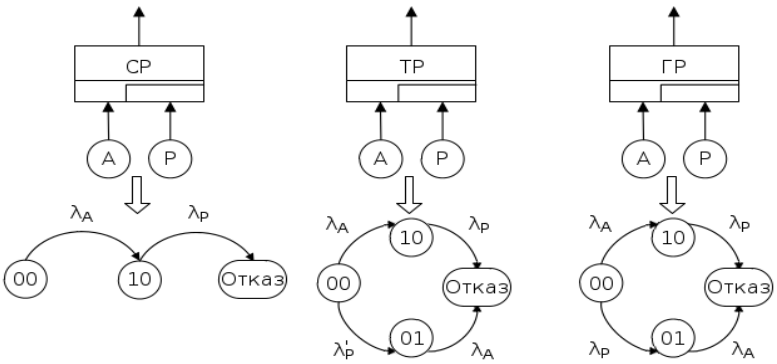
Фиг.2.1 – Логически символ „Приоритетно И" и преход към МВ

- Функционална зависимост (FDEP) (Function DEPendency) - изходът е фиктивен и не се реализира, но когато пусковото събитие П вляво се случи, всички други входни събития също настъпват. (фиг.2.2).



Фиг.2.2 – Логически символ „Функционална зависимост" и преход към МВ

- Излишък (SPARE) - представлява компонент, който може да бъде заменен от един или повече резервни. Когато основният елемент откаже, включва се първия резервен. Когато резевния загуби работоспособност се включва следващия и така, докато резервните елементи (РЕ) се изчерпят. Всеки елемент може да бъде свързан към няколко SPARE логически символа, но веднъж активиран не може да бъде използван от друг. БС може да имат допълнителен параметър α, наречен латентен фактор. Той е със стойност между 0 и 1 и намалява вероятността за отказ на БС до част от неговата номинална вероятност за отказ ако БС е неактивен вход към SPARE. Коефициентът α не се отнася за БС, които не са входове на SPARE. На фиг.2.3 са показани три частни случая на елемента и прехода към МВ.



Фиг.2.3 – Логически символ „Излишък" и преход към МВ

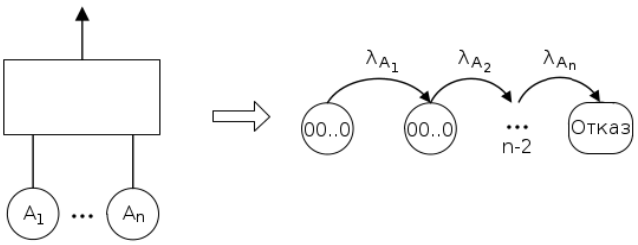
-- *Студен резерв (СР)* (Cold Spare) - частен случай на SPARE с латентен фактор 0. В този случай резервите не могат да откажат преди да бъдат активирани.

-- *Топъл резерв (ТР)* (Warm Spare) - частен случай на SPARE, където α е между 0 и 1.

Следователно вероятността за отказ на резервите е намалена с латентния фактор (PE е включен в подготвителен режим). Това е отразено в интензивността λ'_P.

-- *Горещ резерв (ГР)* (Hot Spare) - частен случай на SPARE, където латентния фактор на разервните елементи е 1. С други думи вероятността за отказ на резервите е същата като на основния елемент, защото PE работи винаги с основния.

- Поредност (SEQ) (Sequence Enforcing) - изходът става активен когато всички входове откажат в определена последователност (фиг.2.4).

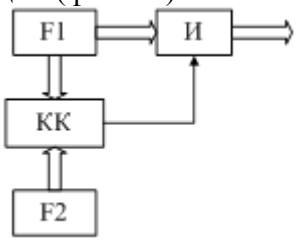


Фиг.2.4 – Логически символ „Поредност" и преход към МВ

3. МОДЕЛИРАНЕ БЕЗОПАСНОСТНОТО ПОВЕДЕНИЕ НА СИСТЕМИ ИЗГРАДЕНИ НА FAIL-SAFE ПРИНЦИП ПОСРЕДСТВОМ ДДО

Тъй като ДДО може да моделира поведението на системата във времето, то се оказва подходящо за *моделиране* отказовото поведение на системи, изградени на fail-safe принцип, кадето е от значение характера на отказите и реда на възникването им.

По-долу е разгледан пример с осигурителна система изградена на известния двуканален (квази fail-safe) принцип (фиг.3.1).

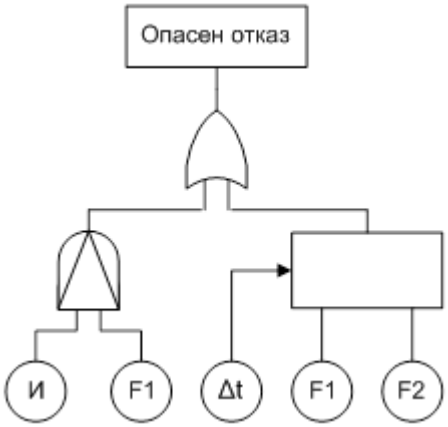


Фиг.3.1 - Двуканална структура

Разглеждаме изходно събитие опасен отказ на системата. В общ случай такова е извеждането на грешна информация от функционалната единица *F1*. Когато другите посочени единици са изправни извеждането на такава информация се изключва. Пораждащите събития, които могат да предизвикат изходното събитие са:

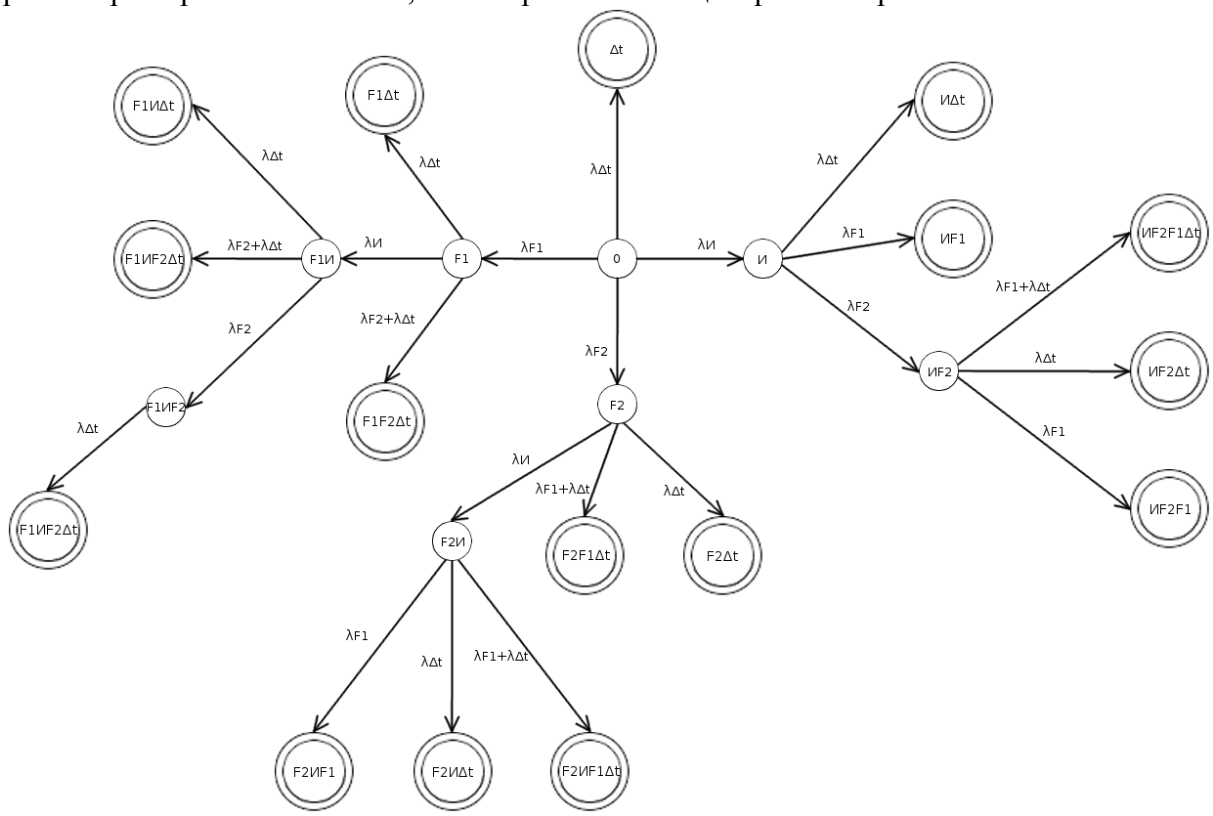
- *F1* – отказ във функционалната единица *F1*, което означава попадане в информационно състояние различно от функционолното и подаване на грешна информация към управлявания обект;
- *F2* – отказ във функционалната единица *F2*, което означава попадане в информационно състояние различно от функционолното;
- *КК* – опасен отказ в контролния канал *КК,* което означава отказова логическа единица на изхода на КК (колкото и вероятността за това да е малка);
- *И* – опасен отказ в изключвателя *И*;

На фиг.3.2 е представено ДДО, моделиращо безопасностното поведение на системата.



Фиг.3.2 - ДДО за двуканална структура

Пораждащите събития *И* и *F1* са свързани с логически символ приоритетно И (PAND). Могат да предизвикат опасен отказ в системата при условие, че възникнат в отбелязаната последователност - първо *И* и след това *F1*. Вторият сценарий, по който може да възникне опасен отказ е едновременнно възникване на събитията *F1* и *F2* в рамките на времето за изявяване на отказите *Δt* - функционална зависимост (FDEP). Фиг.3.3 представя МВ в непрекъснато време и дискретни стойности за двуканалната структура, като са приети експоненциални разпределения за отказите. Нулевото състояние показва, че нито един елемент (от дървото) не е отказал. Всички други събития индицират елементите, които са отказали. Състоянията, при които се реализира върховото събитие, са изобразени с концентрични окръжности.



Фиг.3.3 – МВ за ДДО за двуканална структура

4. ЗАКЛЮЧЕНИЕ

В предложената работа е направен анализ на възможността за моделиране безопасностното поведение на системи, изградени на fail-safe принцип. Могат да се

направят следните изводи:

- Статичното дърво на отказите не е подходящо за моделиране безопасностното поведение на такива системи, поради невъзможност да се отчете развитието на отказите във времето;
- По-подходящо е динамичното дърво на отказите, тъй като отчита развитието на отказите във времето. ДДО позволява да се определят количествените характеристики на системите, чрез преминаване към Марковски вериги;

ЛИТЕРАТУРА:

[1] Ruijters, E., M. Stoelinga, Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools, Computer Science Review 15-16 (2015), pp. 29-62, 2015.

[2] Hao, G., H. Guan, D. Qiu, W. Du, Reliability Analysis of Relay Protection Based on the Fuzzy-Markov Model, International Journal of Hybrid Information Technology Vol.8, No.10 (2015), pp.115-128, 2015.

[3] 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.

[4] 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.

THE FAULT TREE AS A SYSTEM MODEL FOR SAFETY OF RISK SYSTEMS

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

Todor Kableshkov University of Transport,
158 Geo Milev Street, Sofia,
BULGARIA

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

Abstract: *Mankind activity is accompanied with expansion of range of the so-called "Risk systems". These are systems for management of technological processes, which on certain conditions, can cause dramatic material and moral damages. The assessment of risk for such violations becomes a vital part of development and investment activity. In the proposed excerpt a thorough analysis of the fault tree as a dependability model is performed. Classifications are made, advantages and disadvantages of every kind of tree and the application areas are indicated. The known (static) fault tree cannot model the dependability behavior of systems in which the consistency of origins of failures is crucial. The so-called Dynamic fault tree is presented, which models processes in time. It also gives an account of the sequence of origination of failures, which makes it appropriate for every system.*