Годишник Телекомуникации 2019, том 6, с. 115-123

Yearbook Telecommunications 2019, vol. 6, p. 115-123

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.12

АНАЛИЗ И ОЦЕНКА НА РИСКА ОТ РИСКОВИ ТЕХНИЧЕСКИ СИСТЕМИ ПРИ РАЗРАБОТВАНЕТО НА МЕТОДИКА ЗА ОБУЧЕНИЕТО НА СТУДЕНТИ ВЪЗ ОСНОВА НА МЕТОДА ДИНАМИЧНО ДЪРВО НА ОТКАЗИТЕ (DYNAMIC FAULT TREE)

Цветелина Симеонова

ANALYSIS AND RISK ASSESSMENT OF RISK TECHNICAL SYSTEMS TO DEVELOP OF METHODOLOGY FOR TEACHING STUDENTS USING THE METHOD DYNAMIC FAULT TREE

Tsvetelina Simeonova

Резюме: Цел на настоящата работа е да се разработи методика за провеждане на упражнения по анализ и оценка на риска чрез уеб базиран инструмент, като се определи и анализира рискът за възникване на опасно събитие чрез метода динамично дърво на отказите.
Като резултат е показана разработка съгласно предложена методика, приложима в обучението на студенти по анализ и оценка на риска, като съгласно направени приемания са показани подходи за качествено и количествено определяне на риска при приета стойност на вредите.
Като принос е разработена и предложена методика за анализ и оценка на риска, чрез метода динамично дърво на отказите, приложима за обучение на студенти по анализ и управление на риска.
Ключови думи: динамично дърво на отказите, риск, анализ на риска, оценка на риска, методика за обучение.

Abstract: The aim of the present work is to develop a methodology for conducting exercises for analysis, assessment and management of risk, using a web based tool, by identifying and analyzing the risk of occurrence of a dangerous event through the dynamic fault tree method.
As a result, a framework is presented according to the proposed methodology applicable to the students' training in risk analysis, evaluation and management, and according to accepted assumptions. Approaches for qualitative and quantitative risk assessment are presented at the assumed value of the damages.
In addition, a methodology for risk analysis, assessment and management applicable to student training on risk analysis and management, through the dynamic fault tree method, has been developed and proposed.
Keywords: Dynamic Fault Tree, risk, risk analysis, risk assessment, methodology for training.

1. ВЪВЕДЕНИЕ

Дървото на отказите FT (Fault Tree) е качествен и количествен метод, при който се задава нежеланото явление и се търсят причините, които могат да го породят. От вероятността за поява на тези причини се определя общата вероятност за поява на нежелано явление [1, 2]. Анализът чрез метода дърво на отказите е дедуктивен анализ на отказ "отгоре-надолу", при който се анализира нежелано състояние на системата, използвайки булева логика, като се комбинират серия от събития от по-ниско ниво.
Логическият анализ се използва за построяване на дървовидната структура и намиране на комбинация от събития (откази), които водят до отказ на системата. Логическата връзка се представя във вид на логическа схема, по която се търси вероятността за поява на дефинирания отказ (опасен отказ) или друг показател на надеждността (например

интензивност). Дървото на отказите позволява както качествен (логически), така и количествен (вероятностен) анализ.
Основните етапи от този процес са:
- задаване показателите на надеждност за всяко от въвеждащите се събития;
- построяване на "дървото на отказите" в подходяща компютърна моделираща програма;
- съставяне на списък на събитията, водещи до финално събитие (отказ на системата) и списък на минималните сечения;
- изчисляване на риска.

Дърво с един или повече динамични логически символи се нарича динамично дърво на отказите (DFT). Изходите на динамичните логически символи са чувствителни към реда, в който входовете отказват.

Динамичното дърво на отказите [1, 2, 3] също има статични логически символи за връзка (AND, OR, ...), основни събития, междинни събития и финално събитие. Освен това, има и динамични логически символи за връзка (които улесняват моделирането в инженеринга на надеждността), например:

- PAND (приоритетно "И")- логическият елемент има два или повече входа, които могат да бъдат основни или междинни събития и един изход. Изходното събитие възниква, ако всички входове се случват от ляво на дясно.
- SPARE - логическият елемент има един главен вход и други резервни входове. Когато основният модул откаже, се активира първият резервен.
- FDEP (функция DEPendency) - Изходно събитие се появява само когато се появи задействащо събитие.

При динамичното дърво на отказите чрез базовите събития се моделират компонентите на инженерната система[1]. Чрез логическите елементи се моделират подсистемите (съставени от основни компоненти), като логическият елемент показва как отказите на компонентите се комбинират, за да произведат отказ на подсистемата. Дървото на отказите е математически модел за това, как отказите на компонентно ниво в инженерната система се комбинират, за да произведат откази на системно ниво. Вероятностната оценка на надеждността, използваща дърво на отказите, изисква задаване на вероятностни разпределения към основните събития на дървото на отказите.
Програмният продукт за симулиране на динамично дърво на отказите може да използва и относителни времеви единици. Приема се относителна единица, съобразно нейното съответствие с абсолютната единица. В процеса на симулиране използването на относителни времеви единици спомага за намаляване на времето на симулиране. Поради същата причина може да се използва по-малка стъпка на относителните времеви единици.
Анализът чрез дървото на отказите е важен подход за вероятностната оценка на риска в инженерните системи. За изследване и анализ на динамично дърво на отказите се използва web-базирания freeware програмен продукт DFTCalc [4]. В [3] е показано използване на друг сходен програмен продукт "Галилео", който е софтуерен инструмент за изследване и анализ на динамично дърво на отказите (Dynamic Fault Tree Analysis).

[1] Присвояването на разпределение на вероятността на базовото събитие моделира как този компонент отказва с времето.

Годишник Телекомуникации 2019, том 6, с. 115-123

Yearbook Telecommunications 2019, vol. 6, p. 115-123

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.12

2. МЕТОДИКА ЗА АНАЛИЗ И ОЦЕНКА НА РИСКА ЧРЕЗ МЕТОДА "Динамично дърво на отказите (Dynamic Fault Tree)"

Цел на настоящата работа е разработването на методика за обучението на студенти въз основа на метода "Динамично дърво на отказите (Dynamic Fault Tree)", като в процеса на обучение се анализира рискът за възникване на опасно събитие.

Примерно задание може да бъде по зададените описания на дървовидни структури да се определи риска (R) чрез метода "Динамично дърво на отказите", като се определя вероятността за поява на финалното събитие P(t) и като се извършат изчисления с използване на web-базиран програмен продукт.

Може да бъдат направени следните приемания:

1. Приема се, че всички елементи са със зададени параметри.
2. Вредата (тежест на очакваната вреда) в измерителни единици (например левове загуба, дни на неработоспособност, левове за възстановяване) е със зададена условна стойност за всички приети случаи.

2.1. Вариант на задача за изпълнение може да бъде:

- Да се изчисли вероятността за отказ на компютърна система[2] при допустими повреди на критичните компоненти - отказ на: - дискова памет, - захранване, - оперативна памет.
- Да се изчисли риска чрез вероятността за отказ на компютърна система. Изчисленият риск, както и вероятността за реализиране на финалното събитие да се нанесат в табл. 1.

Табл. 1. Изследване на риска и на вероятността за реализиране на финалното събитие.

	Дърво на отказите	
№	**P(t)** Вероятност за реализиране на финалното събитие (отказ на техническата система)	**R** **Риск**
1		
2		
3		

Приема се, че вътрешната шина на компютърната система не може да откаже.

Всички критични компоненти са резервирани, с приети стойности на интензивностите на отказите, посочени в табл. 2.

Таблица 2. Описание на динамично дърво на отказите.

toplevel "System";		
"System" or "DISK" "POWER" "MEMORY";		
"DISK" wsp "D1" "D2";		
"POWER" or "P1" "P2";		
"MEMORY" wsp "M1" "M2" "M3";		
Вариант 1	**Вариант 2**	**Вариант 3**
"P1" lambda=0.01 dorm=0;	"P1" lambda=0.02 dorm=0;	"P1" lambda=0.03 dorm=0;

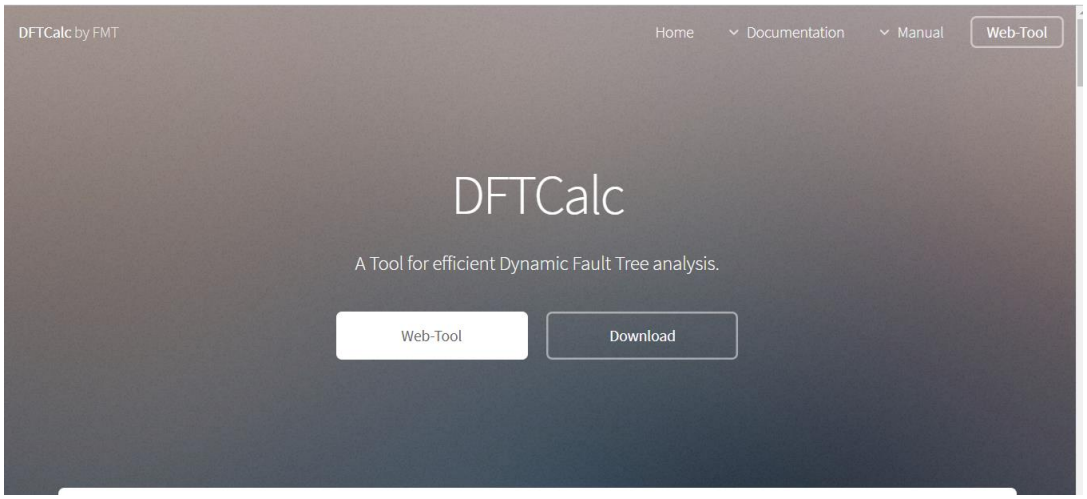
[2] Изследването се извършва само за дефинирания компютърен модул.

"P2" lambda=0.1 dorm=0;	"P2" lambda=0.2 dorm=0;	"P2" lambda=0.3 dorm=0;
"D1" lambda=0.1 dorm=0;	"D1" lambda=0.2 dorm=0;	"D1" lambda=0.3 dorm=0;
"D2" lambda=0.1 dorm=0.5;	"D2" lambda=0.2 dorm=0.5;	"D2" lambda=0.3 dorm=0.5;
"M1" lambda=0.01 dorm=0;	"M1" lambda=0.02 dorm=0;	"M1" lambda=0.03 dorm=0;
"M2" lambda=0.01 dorm=0.5;	"M2" lambda=0.02 dorm=0.5;	"M2" lambda=0.03 dorm=0.5;
"M3" lambda=0.01 dorm=0.5;	"M3" lambda=0.02 dorm=0.5;	"M3" lambda=0.03 dorm=0.5;

В web-базирания програмен продукт **DFTCalc** е необходимо да се уточнят условията при които са провежда симулирането, като се въведе начина и времето за симулиране (в относителни единици).
Маркира се **Compute unreliability** за обхват (range) на стойностите (съответно от:, до:, стъпка:) при from:1.0; to:3.0; step:1.0.[3]
След това маркираме в **Model checker**: IMCA (IMCA = Interactive Markov Chains Analysis, Interactive Markov Chains Analyzer).

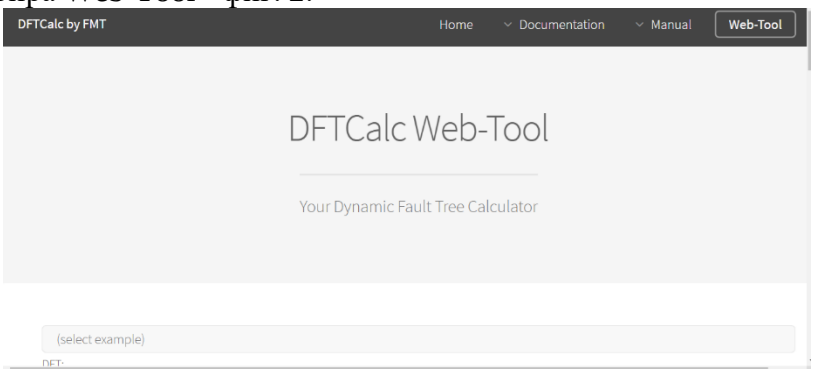
2.2. Последователност на методиката.

2.2.1. Стартиране на програмата DFTCalc (фиг. 1):
https://fmt.ewi.utwente.nl/tools/dftcalc/



Фиг. 1. Начален екран на DFTCalc.

След това се избира Web-Tool - фиг. 2.



Фиг. 2. DFTCalc Web-Tool.

[3] Числовите стойности се задават в посочения формат.

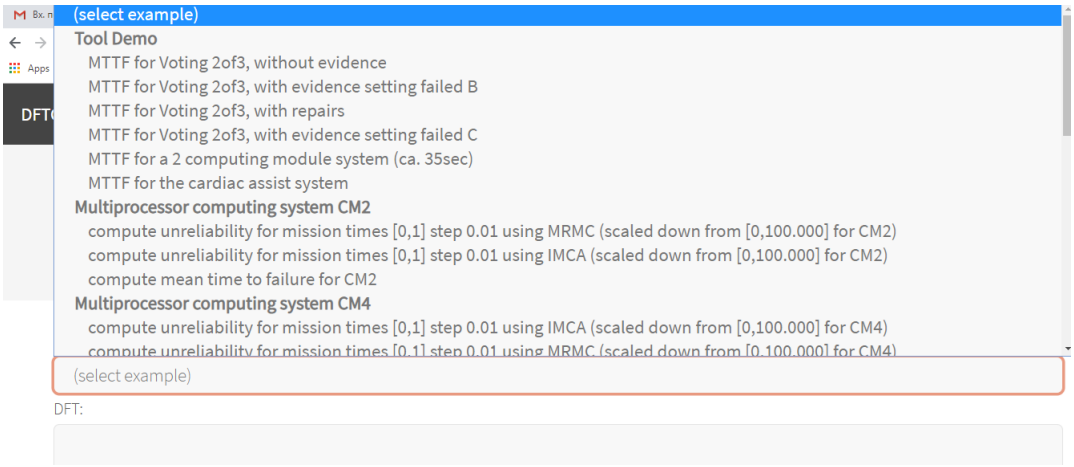
Годишник Телекомуникации 2019, том 6, с. 115-123

Yearbook Telecommunications 2019, vol. 6, p. 115-123

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.12

Чрез **Select Example** може да се избере готов пример - фиг. 3. Всеки от тях се зарежда със съответните настройки. Посредством **Show Result** и **Show Plot** и др., може директно да се изведат резултатите при условията на готовия пример.



Фиг. 3. Варианти на готови примери.

2.2.2. Въвеждане на описанието.

Под **Select Example**, в полето **DFT** се въвежда съответният пример (от табл. 2), който ще използваме, например:

toplevel "System";
"System" or "DISK" "POWER" "MEMORY";
"DISK" wsp "D1" "D2";
"POWER" or "P1" "P2";
"MEMORY" wsp "M1" "M2" "M3";
"P1" lambda[4]=0.02 dorm=0;
"P2" lambda=0.2 dorm=0;
"D1" lambda=0.2 dorm=0;
"D2" lambda=0.2 dorm=0.5;
"M1" lambda=0.02 dorm=0;
"M2" lambda=0.02 dorm=0.5;
"M3" lambda=0.02 dorm=0.5;

Примерът се отнася за изчисляване на ненадеждността (Compute unreliability), описано в задачата и таблицата към нея.

2.2.3. Задава се начин на изследване

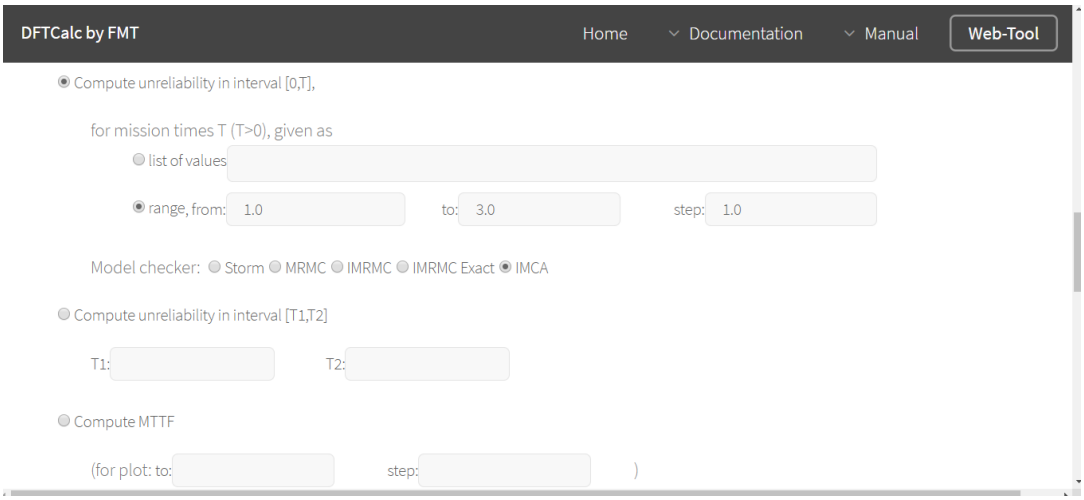
След въвеждането е необходимо да се уточнят настройките, т.е. условията при които се провежда симулирането, с цел изчисляване на ненадеждността и анализ на динамичното дърво на отказите - фиг. 4.

Необходимо е да се въведе времето за симулиране (в относителни единици), за което има два варианта (маркира се**: Compute unreliability** in interval [0,T], for mission times T (T>0), given as):

[4] "lambda" е интензивност, а "dorm" е латентност.

- списък стойности = list of values
- обхват на стойностите (съответно от:, до:, и стъпка:) = range, from: to: step:

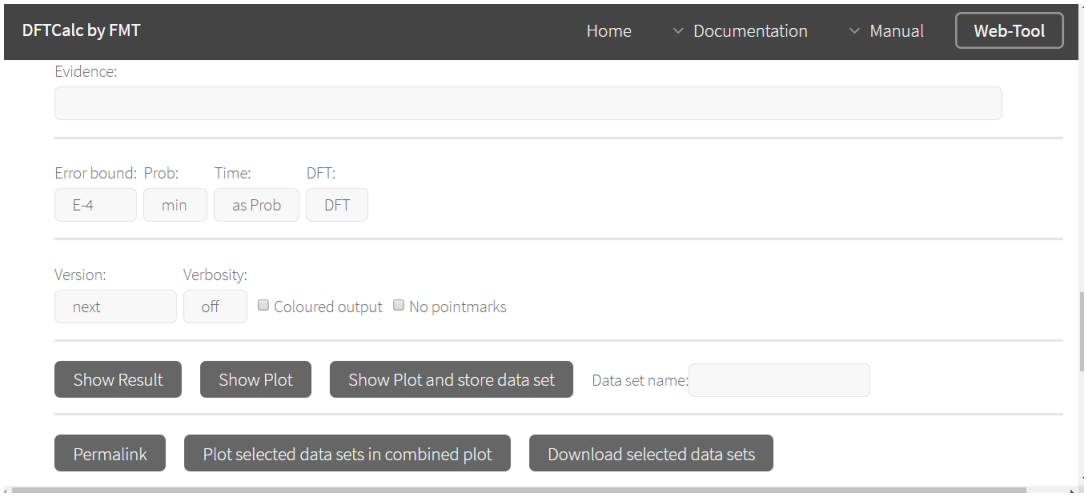
За нашия пример ще маркираме втория вариант (range) при from:1.0; to:3.0; step:1.0.[5]
След това маркираме в **Model checker**: IMCA
IMCA = Interactive Markov Chains Analysis, Interactive Markov Chains Analyzer.
Има и други варианти за избор на модел: Model checker: Storm, MRMC, IMRMC, IMRMC Exact (тук не се разглеждат).



Фиг. 4. Условия при които са провежда симулирането.

Следващите опции се оставят по подразбиране и не се маркират (фиг. 5):

- Compute unreliability in interval [T1,T2] T1: T2:
- Compute MTTF (for plot: to: step:)
- Compute steady-state availability Evidence:
- Error bound: Prob: Time: DFT:
- Version: Verbosity: Coloured output No pointmarks



Фиг. 5. Опции, които се оставят по подразбиране и не се маркират.

[5] Числовите стойности се задават в посочения формат.

Годишник Телекомуникации 2019, том 6, с. 115-123

Yearbook Telecommunications 2019, vol. 6, p. 115-123

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

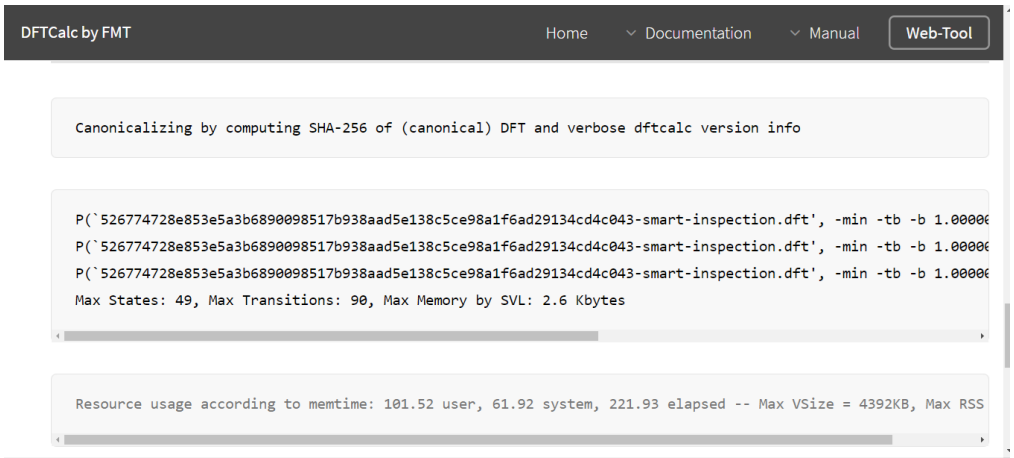
DOI: https://doi.org/10.33919/YTelecomm.19.6.12

2.2.4. Стартиране на симулирането и получаване на резултати

Получаването на резултати е чрез **Show Result** (описателно) и **Show Plot** (в графичен вид) - съответно фиг. 6 и фиг. 7. Чрез конкретния избор се стартира симулирането и се получават резултатите в зададения формат.

Симулирането отнема известно време, което се индикира от програмата.

В случай на грешка, тя също се визуализира.



Фиг. 6. Получаване на резултати чрез Show Result (описателно), които са необходими за изчисляване на риска.

2.2.5. Сваляне на данните

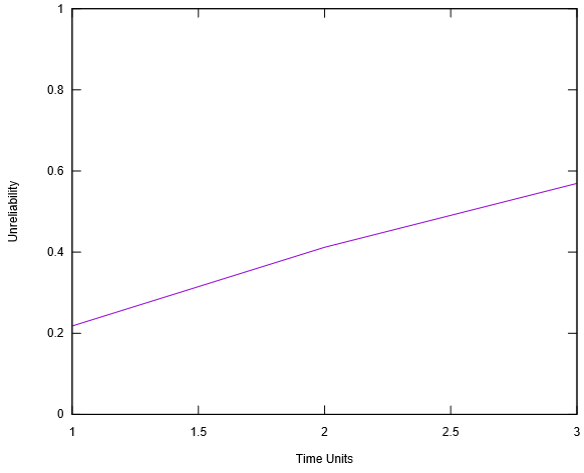
Show Result:

P(`526774728e853e5a3b6890098517b938aad5e138c5ce98a1f6ad29134cd4c043-smart-inspection.dft', -min -tb -b 1.000000 -T 3.000000 -i 1.000000 -e 0.0001, 1, fails) **=0.2178944326**

P(`526774728e853e5a3b6890098517b938aad5e138c5ce98a1f6ad29134cd4c043-smart-inspection.dft', -min -tb -b 1.000000 -T 3.000000 -i 1.000000 -e 0.0001, 2, fails) **=0.411821315**

P(`526774728e853e5a3b6890098517b938aad5e138c5ce98a1f6ad29134cd4c043-smart-inspection.dft', -min -tb -b 1.000000 -T 3.000000 -i 1.000000 -e 0.0001, 3, fails) **=0.5693419526**

Show Plot



Фиг. 7. Получаване на резултатите чрез Show Plot.

За получаването на последователни графични резултати, понякога е необходимо да се извърши обновяване на екрана, чрез двоен клик върху празния екран или върху предишна графика.

2.3. Изчисляване на риска

Рискът се дефинира във връзка с оценката на ефективността на технико-икономическите системи като продукт, получен от произведението на вероятността за претърпяване на вреда и тежестта на вредата, отнесено към определена времева единица [7]. Изчисляването на риска (степента на риска) се определя като математическо очакване на вредата от нежеланото събитие, т.е.:

R = P.W,

където: P – вероятност за поява на събитието (например отказ на техническа система), W – вреда, нежелани последствия.

За целта на изчисляването на риска, рискът се анализира с цел да се определи вероятността да се сбъдне и евентуалните последици. Необходимо е да се постави количествена оценка на всеки отделен риск на база, на която те да бъдат приоритизирани (за целите на модифицирането на системите). Необходимо е да се вземе предвид факта, че конкретният момент на настъпване на риска има значение върху последиците, които ще окаже. Използвайки тези два показателя се въвежда т.нар. матрица за оценка на степента на риска [5], съобразно стандарта БДС ISO 31000 [6].

3. ЗАКЛЮЧЕНИЕ

Предложена е и е описана методика за анализ и оценка на риска използваща метода динамично дърво на отказите въз основа на уеб базиран инструмент. Методиката е приложима за обучение на студенти по анализ и управление на риска, включваща описание и варианти за изчисляване.

В резултат на методиката може да се направят например следните изводи:

- анализ кои от събитията (откази) оказват най-съществено влияние върху стойността на риска по така описаната дървовидна структура.
- анализ на възможните варианти за намаляване на риска, в случай, че получената му стойност е неприемлива.
- анализ на резултатите съгласно целевата стойност на риска и варианти за управление на риска.

ЛИТЕРАТУРА

1. 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.
2. 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, 2015.
3. Sullivan Kevin (Computer Science), Joanne Bechta Dugan (Electrical Engineering). *Galileo User's Manual & Design Overview* (Version 2.11-Alpha). Copyright 1996, 1997, 1998 University of Virginia. [Accessed on: 17 Dec. 2018]. Viewed in: https://www.cse.msu.edu/~cse870/Materials/FaultTolerant/manual-galileo.htm
4. Софтуерен продукт за изследване на динамично дърво на отказите (online) DFTCalc [Accessed on: 18 Nov. 2018]. Viewed in: https://fmt.ewi.utwente.nl/tools/dftcalc/. Softueren produkt za izsledvane na dinamichno darvo na otkazite
5. Управление на риска. Уикипедия. [Accessed on: 11 Nov. 2018]. Viewed in: [https://bg.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BD%D0%B0_%D1%80%D0%B8%D1%81%D0%BA%D0%B0]. Upravlenie na riska. Uikipediya.

Годишник Телекомуникации 2019, том 6, с. 115-123

Yearbook Telecommunications 2019, vol. 6, p. 115-123

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.12

6. ISO 31000:2018, Risk management – Guidelines; БДС ISO 31000:2018 - Управление на риска. Принципи и указания.
7. Юридическият термин „риск“ в националната сигурност на Република България. [Accessed on: 11 Nov. 2018]. Viewed in: http://conf.uni-ruse.bg/bg/docs/cp15/7/7-24.pdf. YUridicheskiyat termin „risk“ v natsionalnata sigurnost na Republika Balgariya.

Информация за автора:
Ас. д-р инж. Цветелина Богданова Симеонова, София 1574, ул. Гео Милев 158, ВТУ „Т. Каблешков”, Тел.: 02 9709296, e-mail: ts.b.simeonova@abv.bg

Contacts:
Assist. professor Tsvetelina Simeonova PhD, T.Kableshkov University of Transport, 158 Geo Milev St., Sofia, office phone: +359 2 9709296, e-mail: ts.b.simeonova@abv.bg

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 05.01.2019.
Дата на приемане за публикуване (Date of adoption for publication): 05.03.2019.