Годишник Телекомуникации 2019, том 6, с. 29-36

Yearbook Telecommunications 2019, vol. 6, p. 29-36

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

DOI: https://doi.org/10.33919/YTelecomm.19.6.3

ИЗСЛЕДВАНЕ НА РИСКА ПРИ СВЕТОФОРНА СХЕМА КАТО РИСКОВА ТЕХНИЧЕСКА СИСТЕМА ЧРЕЗ МЕТОДА ДЪРВО НА ОТКАЗИТЕ

Цветелина Симеонова

STUDY OF THE RISK OF SCHEME OF TRAFFIC LIGHT AS RISK TECHNICAL SYSTEM WITH THE FAULT TREE METHOD

Tsvetelina Simeonova

Резюме: Цел на работата е да се разработи методика за анализ и оценка на риска от рискова техническа система (светофорна схема) чрез метода дърво на отказите.
Резултати: Анализът на риска от рискови технически системи чрез дърво на отказите дава еднозначна връзка между параметри на елементи и параметри на еквивалентни елементи, описващи система или подсистема. Показан е пример за анализ на риска от рискова техническа система (светофорна схема) чрез метода дърво на отказите (Fault Tree), приложим в обучението на студенти по анализ и управление на риска, включващ примерна схема и дървовидна схема (съгласно направени приемания) и с възможност за изчисления по нея и определяне на риска при приета стойност на вредите.
Приноси: Предложена е разработена методика за анализ и оценка на риска от рискови технически системи (светофорна схема) и е разработен пример, приложим в обучението на студенти по анализ и управление на риска.
Ключови думи: дърво на отказите, рискови технически системи, риск.

Abstract: The aim of the paper is to develop a methodology for risk analysis and risk assessment of a risk technical system (traffic light scheme) using the fault tree method.
Results: Analysis of the risk of risk technical systems through a fault tree gives an unambiguous relationship between element parameters and parameters of equivalent elements describing a system or a part of a system.
An example of risk analysis of a risk technical system (traffic light-scheme) is shown with the fault tree method applicable to students training on risk analysis and management, including a sample scheme and a tree scheme (according to accepted assumptions) and with the possibility of calculating it and determining the risk at the assumed value of the damage.
Contributions: A methodology for analysis and risk assessment of risk technical systems (traffic light-scheme) has been developed and an example has been developed for the students' training in risk analysis and management.
Key words: Fault tree, risk technical systems, risk.

1. ВЪВЕДЕНИЕ

Прогнозирането на риска въз основа на анализ на поведението на рискова техническа система се характеризира с това, че се решава вероятностна задача, като бъдещото поведение на системата се определя с някаква степен на достоверност и вероятностно се оценява състоянието, в което тя би се намирала след определен период от време при различни условия на експлоатация.

При прогнозирането на риска е необходимо да се използват методите на математическото моделиране със задължителна проверка на адекватността на модела. Моделът за определяне на надеждностните параметри, а чрез тях и определяне на риска (за случаите когато няма дефинирано защитно състояние след отказ), следва да се структурира съобразно функционалното предназначение, съществуващите елементи и връзки, както и

характерните особености. За целта е необходимо да се изгради надеждностна блокова диаграма (или дърво на отказите или дърво на събитията) и да се дефинират отделните елементи.

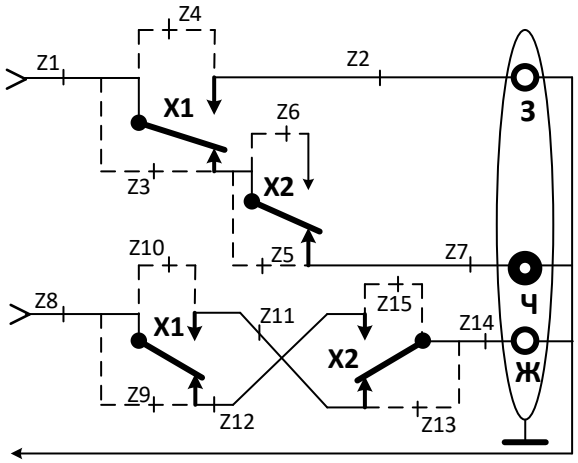
Предложена е методика за определяне и анализ на риска при възникване на опасно събитие от светофорна схема чрез метода дърво на отказите, приложима при обучението на студенти.

Изследването на риска от светофорна схема, разглеждана като невъзстановим обект на осигурителната техника (с невъзстановими елементи), и таблица, описваща входните и нормалните изходни сигнали, се извършва като се построи дърво на отказите и се определи вероятността за поява на финалното събитие.

При използването на метода дърво на отказите [1, 2] се отразява топологията на схемата, отчита се свързването (последователно/паралелно) на елементите. Този подход се отличава с максимална простота и нагледност.

2. МЕТОДИКА ЗА ОПРЕДЕЛЯНЕ И АНАЛИЗ НА РИСКА ПРИ ВЪЗНИКВАНЕ НА ОПАСНО СЪБИТИЕ ЧРЕЗ МЕТОДА ДЪРВО НА ОТКАЗИТЕ, ПРИЛОЖИМА ПРИ ОБУЧЕНИЕТО НА СТУДЕНТИ

Изследване на риска чрез метода дърво на отказите от примерна светофорна схема (рискова техническа система) на светофор с четири сигнални показания - фиг.1 [3].



Фиг.1. Примерна схема на светофорна схема за четиризначна автоблокировка (на фигурата със Z са означени прекъсванията и залепванията на съответните места).

Схемата на светофора има три изхода, които управляват съответната лампа. Входовете са два, като на всеки от тях се подава информация от датчик за състоянието свободно/заето.

В осигурителните устройства такава информация се получава от пътни релета, които са задействани (състоянието им е единица), когато състоянието е свободно, а когато е заето, релетата са отпуснати (състоянието им е нула). Таблицата на истинност е показана в табл.1.

Табл. 1. Таблица на истинност на схемата от фиг. 1.

№	Входен набор	Нормален изходен сигнал
1	x1=1, x2=1	100 - зелена светлина
2	x1=1, x2=0	101 - зелена и жълта светлина
3	x1=0, x2=1	001 - жълта светлина
4	x1=0, x2=0	010 - червена светлина

Годишник Телекомуникации 2019, том 6, с. 29-36

Yearbook Telecommunications 2019, vol. 6, p. 29-36

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

DOI: https://doi.org/10.33919/YTelecomm.19.6.3

За конкретен входен набор сигнали, по схемата циклично се проследява какъв би могъл да бъде изходният сигнал. За всеки подаден входен набор, последователно по схемата се проверява дали би могло да възникне опасно сигнално показание (при всеки конкретен изходен набор, който би могъл да предизвика опасност). Ако това е така, причините (прекъсване на проводник или залепване на контакт) се описват чрез дърво на отказите. Тези причини се означават (Z_1, , Z_n) и в схемата, а след това и в дървото.
Условията на функциониране и на изследване са:
- Приема се, че съответните вероятности за всички прекъсвания на връзки и компоненти, както и всички залепвания на тилови (и фронтовите, където са допустими) контакти на релета, са с еднакви параметри.
- Не се разглежда отсъствието на сигнал на светофорната схема (защитен отказ).
- Рискът от опасно показание се изчислява като се отчита особеността, че до индивидуален риск, финансов риск, с изключение на риск изразен чрез загуби от времезадръжка на технологичния процес, може да се достигне като получената по метода дърво на отказите вероятност се умножи по вероятност отчитаща наличие или отсъствие и на други необходими събития (тази условна вероятност (за която приемаме условна стойност) може да бъде проследена по дърво на събитията), двете вероятности общо водят до инцидент. Вследствие на този инцидент се получава вреда (тежест на очакваната вреда), в измерителни единици (например левове загуба, дни на неработоспособност, левове за възстановяване), която се приема с условна стойност.

Предложената методика за анализ на риска от рискови технически системи, базирана на дървовидна структура, приложима както при надеждностни изследвания, така и при определяне на риска, включва като вариант 1 следното (съобразно фиг.1):
А. Построяване на дървета на отказите за всеки от входните набори сигнали, при допустими повреди:
- всички прекъсвания на връзки и компоненти;
- залепване на тиловите и фронтовите контакти на релетата (фронтовите контакти на първокласните по надеждност релета не залепват).
Б. Въз основа на построените дървета на отказите се определя вероятността за поява на финалното събитие P(t) при невъзстановима система, за случая когато разпределението на входните опасности не е известно.
В. Изчислява се рискът от всеки от входните набори сигнали, съобразно изчисленията, направени по построените дървета на отказите (при което се задават вероятност за залепване и вероятност за прекъсване), при зададена стойност на вредата (щети).

Като вариант 2, в методиката се приема, че допустимите повреди са:
- всички прекъсвания на връзки и компоненти;
- залепване на тиловите контакти на релетата (фронтовите контакти на първокласните по надеждност релета не залепват).

На така дадената схема са означени с пунктирани линии отразяващи залепване, или непосредствено при прекъсване, като се извършва тяхното номериране с променливата Z, която приема стойности от 1 до n, където n е броят залепвания и прекъсвания, съгласно условието.

За построяване на дърво на отказите за всеки възможен опасен изходен набор, при конкретен входен набор може да се използва примерът на фиг. 2 и фиг. 3.

2.1. Определяне на вероятността за възникване на опасност

Софтуерният продукт, който се използва е Fault Tree Analyser (на фирмата ALD Software, web-базиран, freeware).
Методиката включва следните стъпки:
1. Зарежда се началният прозорец [4]: https://www.fault-tree-analysis-software.com/fault-tree-analysis?type=Railway
2. Стартира се построяването на ново дърво (Create New) от меню Fault Tree.
3. Построяване на дърво на отказите се извършва чрез следните стъпки:
    3.1. Специфициране на логически елемент е чрез двойно кликване върху него, като се избира адекватен тип съгласно заданието.
    3.2. След това чрез меню Edit се добавят логически елементи, като за всеки от тях преди добавянето маркираме финалното събитие. Междинните събития се присвояват автоматично към добавените логически елементи, като ги обозначаваме чрез Description.
    3.3. Чрез меню Edit добавяме инициращи събития (Add New Event), като преди това за всяко от тях сме маркирали съответно всеки един от добавените логически елемента.

Заб.: При по-големи дървета, последователността е аналогична.
4. Анализ на построеното дърво на отказите
    4.1. Въз основа на построеното дърво на отказите (в което сме задали структурата, логическите елементи и параметрите на събитията), от меню Reports се избира Gate Report. Виждат се резултатите (като описание и стойност на вероятността) за всички междинни събития и за финалното събитие.
    4.2. Въз основа на построеното дърво на отказите от меню Analysis се избира Probability Calculation (MCS - Minimal Cut Set's).

Въз основа на получените стойности може да се направят изводи за минималните сечения.
Минимални сечения на дървото на отказите [5]: Качествената и количествената оценка се основават на минималните сечения на дървото на отказите. Най-малката подгрупа на всяко сечение, която предизвиква отказ на системата, се нарича минимално сечение. Може да се даде следното определение: минимално сечение е такава група, която се състои от най-малко на брой елементи, чиито едновременен отказ ще предизвика отказ на системата.
За да се получи количествена оценка за готовността (или неготовността) на системата трябва да се комбинират нейните минимални сечения.

Пример въз основа на схемата от фиг. 1, съгласно вариант 2.

- За входен набор x_1=1 и x_2=1 (зелена светлина), какъвто и да е изходният сигнал, при разрешено преминаване не представлява опасност, т.е. няма опасен отказ.
- За входен набор x_1=1, x_2=0 (едновременно има зелена и жълта светлина), са възможни всички видове откази (скрити, защитни и опасни), като само опасен отказ представлява интерес.

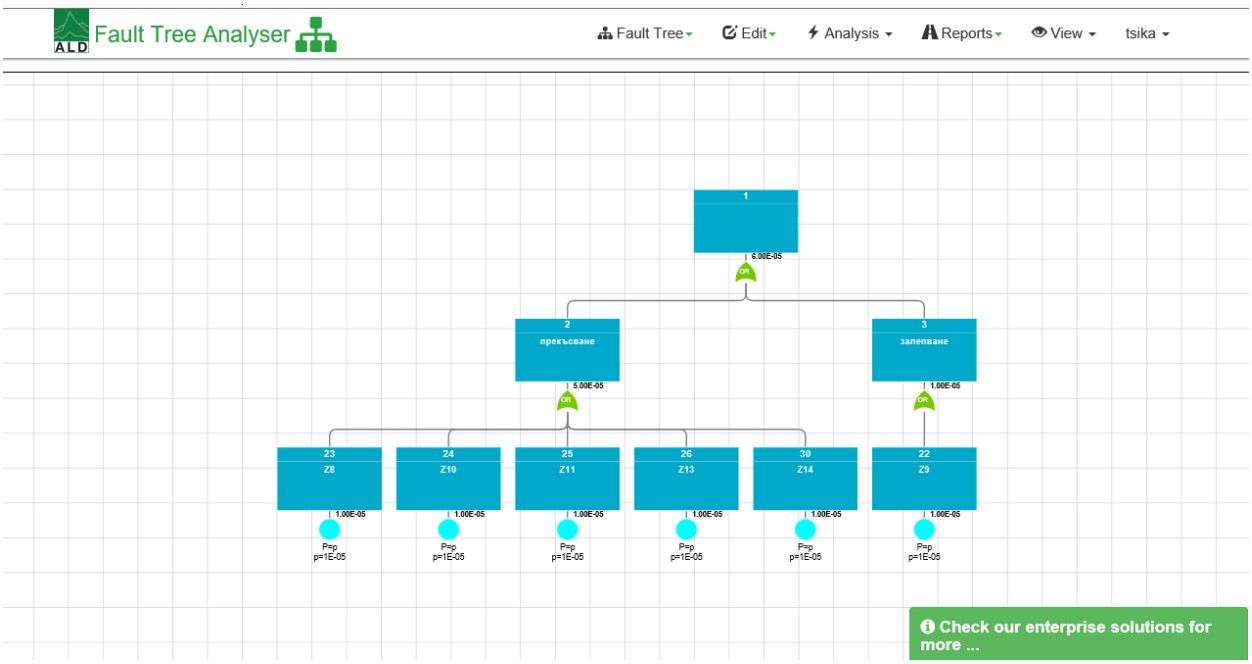
Построява се дърво на отказите (за изходен сигнал 100, който е опасен, съответства на изходно показание да свети само зелена светлина) при входен набор x_1=1, x_2=0.
Приети са стойности за примера: Constant Probability, като p=0.00001, t=10000.

Годишник Телекомуникации 2019, том 6, с. 29-36

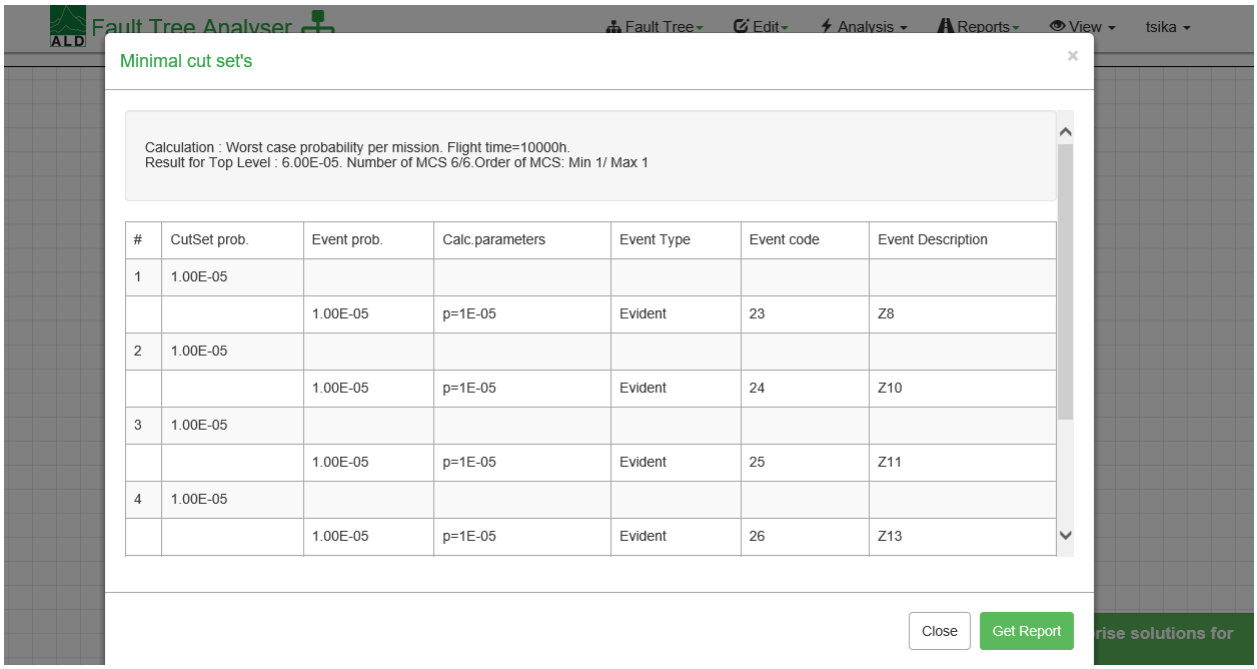
Yearbook Telecommunications 2019, vol. 6, p. 29-36

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

DOI: https://doi.org/10.33919/YTelecomm.19.6.3



Фиг. 2. Дърво на отказите при входен набор x_1=1, x_2=0, с направен анализ при зададени стойности.



Фиг. 3. Репорт за минималните сечения от дървото на отказите при входен набор x_1=1, x_2=0.

- За входен набор x_1=0, x_2=1 (жълта светлина), няма опасен отказ.
- За входен набор x_1=0, x_2=0 (червена светлина), няма опасен отказ. Опасни състояния не могат да възникнат, което се обяснява с недопустимостта на прехода

от 0-1 на релетата за управление на сигнала, както и недопустимостта на повредата залепване на фронтов контакт.

2.2. Изчисляване на риска

Анализът и оценката на риска е процес, при който рискът се анализира с цел да се определи вероятността да се сбъдне и евентуалните последици. Целта е да се постави количествена оценка на всеки риск на база, на която те да бъдат приоритизирани (за целите на модифицирането им). 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 (табл. 2 и табл. 3) [6].
Рискът се дефинира в контекста на 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] или изчисляването на риска се извършва чрез степента на риска, която 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.

2.3. Анализът на резултатите може да се направи по следния начин [8].
При анализ на риска, от една страна се прави анализ на причините и последствията и от друга страна - количествена оценка на риска, която е разделена на следните стъпки:

1. Моделиране,
2. Изчисление на честотата на поява,
3. Определяне на категорията на риска.

Известни са различни подходи за определяне приемливата граница на риска. В стандарт EN50126 и свързаните с него, се препоръчва да се използва един от следните три принципа [8, 9, 10, 11, 12]:

- MEM (“minimal endogenous mortality”). При този принцип е определена някаква приемлива степен на риска, която удовлетворява обществото. Според EN50126 за техническите системи, респективно за жп транспорт, този допустим риск означава, че вероятността за смърт на един участник в железопътния процес, за една година в резултат на произшествие, свързано с този процес, може да бъде не повече от 10^{-5}.
- ALARP (“as low as reasonably practicable”). Съгласно този принцип общественият риск може да бъде изследван, когато има възможност за катастрофа, въвличайки голям брой произшествия.
- GAMAB (“globally at least as good”). Новите системи трябва да предложат ниво на риска поне на нивото на съществуваща еквивалентна система.

В таблица 2 са дефинирани количествените категории на риска и действията, които трябва да бъдат приложени за всяка категория. Националният орган по безопасността (ИА „ЖА”) е отговорен за определяне и прилагане на принципа и за допустимото ниво на риска (THR) за различните категории.

Годишник Телекомуникации 2019, том 6, с. 29-36

Yearbook Telecommunications 2019, vol. 6, p. 29-36

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

DOI: https://doi.org/10.33919/YTelecomm.19.6.3

Таблица 2. Категории на риска.

	Категория на събитието	**Действие, което трябва да бъде приложено (намаление на риска/контрол)**
1	Недопустимо	Трябва да бъде елиминирано (поне на допустимо ниво)
2	Нежелателно	Трябва само да бъде прието, когато намалението на риска не е практически осъществимо със съгласието на НОБ (Национален орган по безопасност)
3	Допустимо	Приема се с адекватен контрол и със съгласието на НОБ
4	Незначително	Приема се без съгласието на НОБ

Слагайки дефинираните нива на риска в Матрицата „Честота - Последствие" се получава Матрица на Риска - Таблица 3 съгласно [8, 9].

Таблица 3. Матрица на риска.

Честота на поява на опасното събитие	**Нива на риска**			
често	нежелан	недопустим	недопустим	недопустим
вероятно	допустим	нежелан	недопустим	недопустим
нередовно	допустим	нежелан	нежелан	недопустим
малко вероятно	незначителен	допустим	нежелан	нежелан
слабо вероятно	незначителен	незначителен	допустим	допустим
невероятно	незначителен	незначителен	допустим	допустим
	незначителен	**оскъден**	**критичен**	**катастрофичен**
	нива на строгост на последствията от отказа			

За оценката на риска се извършва анализ на допустимата степен на риск (THR) за всеки риск, който е бил оценен приемливо (например допустим/незначителен). Това THR може да се разглежда като мярка на максимално допустимото ниво на поява на определена опасност. По този начин оценката на риска е в съответствие с принципа на ОМБ (Общоевропейски мерки за безопасност), както е посочено в Европейската директива за безопасността.

ЗАКЛЮЧЕНИЕ

Разработена е методика за анализ и оценка на риска от рискова техническа система, базирана на дърво на отказите. Предимствата на предложената методика за определяне на вероятността за опасно събитие са нагледност и ясни връзки.

Показан е пример за анализ на риска от рискова техническа система (светофорна схема) чрез метода дърво на отказите (Fault Tree), приложим в обучението на студенти по анализ и управление на риска, включващ примерна схема, еквивалентна дървовидна схема съгласно направени приемания и възможност за изчисления по нея, както и определяне на риска при приета стойност на вредите.

Въз основа на предложената методика може да се анализират разглежданите откази и последствията до които водят, както и да се предлагат решения за предотвратяването им.

Би могло да се правят изводи, например, кои от събитията (откази) оказват най-съществено влияние върху стойността на риска по така построената дървовидна структура. Също така какви са възможните варианти за намаляване на риска, в случай, че получената му стойност е неприемлива.

ЛИТЕРАТУРА

1. Гиндев Е. *Увод в теорията и практиката на надеждността* - част 1 и 2: АИ "Проф. Марин Дринов". 2000, 2002. Gindev E. Uvod v teoriyata i praktikata na nadezhdnostta - chast 1 i 2: AI "Prof. Marin Drinov". 2000, 2002
2. Христов Хр., В. Трифонов. *Надеждност и сигурност на комуникациите*. София, Изд. Нови знания, 2005. Hristov Hr., V. Trifonov. Nadezhdnost i sigurnost na komunikatsiite. Sofiya, Izd. Novi znaniya, 2005
3. Христов Хр. *Основи на осигурителната техника*. София, изд. Техника, 1990. Hristov Hr. Osnovi na osiguritelnata tehnika. Sofiya, izd. Tehnika, 1990
4. Софтуерен продукт за изследване на "дърво на отказите" (online) [Accessed on: 12 Dec. 2018]. Viewed in: https://www.fault-tree-analysis-software.com/fault-tree-analysis?type=Railway; Softueren produkt za izsledvane na "darvo na otkazite"
5. Манчев Б. (Рис инженеринг ООД), Б. Маринов (Рис инженеринг ООД), н.с. I ст. Б. Ненкова (ИИ - БАН). Приложение на метода "дърво на отказите" за анализ на системи. [Accessed on: 11 Nov. 2018]. Viewed in: https://inis.iaea.org/collection/NCLCollectionStore/_Public/32/007/32007930.pdf; Manchev B. (Ris inzhenering OOD), B. Marinov (Ris inzhenering OOD), n.s. I st. B. Nenkova (II - BAN). Prilozhenie na metoda "darvo na otkazite" za analiz na sistemi
6. 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
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
8. Стойчева Н. Монография. *Управление на безопасността и ролята му в инвестиционния процес на съвременните железопътни осигурителни системи*. Изд. ВТУ „Тодор Каблешков” София, 2013. Stoycheva N. Monografiya. Upravlenie na bezopasnostta i rolyata mu v investitsionniya protses na savremennite zhelezopatni osiguritelni sistemi. Izd. VTU „Todor Kableshkov” Sofiya, 2013
9. CENELEC, EN 50126: Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). EN50126 “Приложения в жп транспорта – определяне и демонстриране на надеждност, готовност, ремонтопригодност, безопасност (RAMS)”
10. CENELEC, EN 50128: Railway applications –Communications, signaling and processing systems – Software for railway control and protection systems. EN50128 “Приложения в жп транспорта – софтуер за железопътни управляващи и контролни системи”
11. CENELEC, EN 50129: Railway applications – Safety-related electronic systems for signaling. EN 50129 “Безопасност на електронните железопътни осигурителни системи”
12. CENELEC, EN 50159-1/-2: Railway applications - Communication, signaling and processing systems - Safety-related communication in open/closed communication systems. EN50159 “Приложения в жп транспорта – телекомуникационна техника, осигурителна техника и системи за обработка на данни”

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.