THE MARKOV'S MODEL TO EVALUATE SAFETY PARAMETERS OF RAILROAD SIGNALLING SYSTEMS

MARKOVA MODELIS DZELZCEĻA AUTOMĀTIKAS SISTĒMU DROŠĪBAS PARAMETRU NOVĒRTĒŠANAI

V.Lubinsky, L.Sergejeva, I.Korago

Keywords: safety, stochastic models, markov's processes, computer realisation

Introduction

The rightful of conception of dangerous and protective faults to notify saety of railway signalling systems (RSS) is shown. Error of calculations, based on dangerous faults conseption, of RSS safety level is evaluated. The new method, based on „dangerous" element conception, of creation of safety models of RSS is propossed. Three versions of markov models is developed to evaluate parameters of RSS safety for vareous system configurations, the technology of their computer realisation is proposed too.

Conception of dangerous element

RSS stochastic safety models and safety norms, accepted based on them, are the most distributed and admitted. But the conception, used for creation of those models, to split system faults to dangerous and not dangerous is not blameless. The new method to evaluate parameters of RSS functional safety, based on „dangerous" element conception is proposed. System's element – it is system indivisible part, and because of it fault the system can operate in one of the possible modes: "not dangerous fault but system operates", "not dangerous fault and system is in protective mode", "dangerous fault". The essence of method proposed is that general failure flow is not sleeted in to two dangerous and not dangerous sub flows. All faults inside this flow are considered like normal faults and element is out of service because of them. But element, which is out of operation, can arise different system operational modes. For example, fault of one of the system elements can arise "not dangerous fault but system operates" mode of system, but fault of another element can arise "dangerous fault" mode of system. The total amount of RSS elements can be split in to separate subsets according to influence of their faults to system operational modes: $M_н$ – subset of elements, which arises "not dangerous fault but system operates" system operational mode because of fault of one of the element inside this subset; $M_з$ – subset of elements, which arises "not dangerous fault and system is in protective mode" system operational mode because of fault of one of the element inside this subset; Mo – subset of elements, which arises "dangerous fault" system operational mode because of fault of one of the element inside this subset. To include element in one of the subsets, it is necessary to do bought analyses of functional schemas and analyses of functionality of system.

Target

The system with total amount of elements $N= n_н + n_з + n_o$ (where $n_н$, $n_з$, n_o – the number of elements in $M_н$, $M_з$, Mo subsets accordingly) during it operation can be in one of the following states: S0 – system is intact, when all N elements fulfil their functions in full amount; S1 – system has fault but it still operates, when some of elements from $M_н$ subset is out of service; S2 – protective state which can arise because of fault of one of the elements from $M_з$ subset; S3 – dangerous state. The state S0 of system can be changed to S1, S2, S3 after faults has happen in elements of appropriate $M_н$, $M_з$, Mo subsets. The rates of occurrences of faults in elements of that subsets are $\lambda_н$, $\lambda_з$, λ_o massive. $\lambda_{нi}$, $\lambda_{зj}$, λ_{ok} – are the elements of that massive, where i= 1,2,... $n_н$, j = 1,2,...$n_з$, k= 1,2..no.. The rates of occurrences of recovery of

elements of Мн, Мз, Мо subsets are λн, λз, λо massive μні , μзj, μоk, where і=1,2...nн; j = 1,2,...nз , к= 1,2, ... no . At the end the target of evaluation of RSS safety can be formulated like follows: it is necessary to define probability of no failure Рбс = 1 – Роп., if the total amount of nн, nз, no elements is known inside Мн, Мз, Мо subsets and the rate of occurrence of faults λні , λзj, λоk and the rate of occurrence of recovery of elements μні , μзj, μоk of this subsets is known too, where Рбс – probability of fact, that system will be in operable or protective state, Роп – probability of fact, that system will have dangerous state.

Elaboration of models

The target to define safety parameters of complex systems could be determined by elaboration of markov models of system operation with different configurations, it means: with not redundant elements, with redundant elements and with partly redundant elements of RSS. The basic markov model of system without redundant elements has been elaborated at the beginning.
Let it be set of N not redundant elements of system, which are pleated to Мн, Мз, Мо subsets. The system can be in one of the stable S_0, S_1, S_2, S_3 states at any time. The states of system can change because of influence of total failure flow of elements from Мн, Мз, Мо subsets and because of influence of total recovery flow of elements with fault:

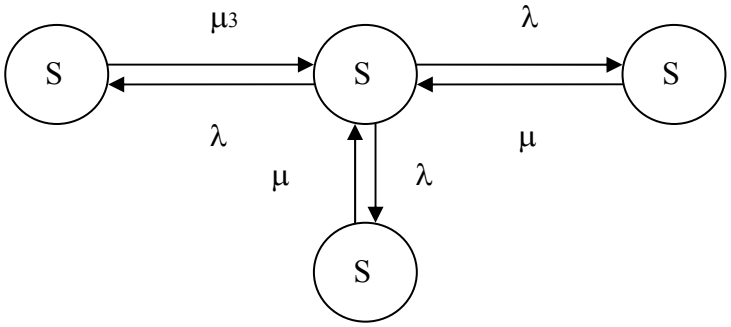
$$\lambda_1 = \sum_{i=1}^{n_H} \lambda_{Hi}, \quad \lambda_2 = \sum_{j=1}^{n_З} \lambda_{Зj}, \quad \lambda_3 = \sum_{k=1}^{n_O} \lambda_{Ok}$$

, where λ_1, λ_2 , λ_3 – total failure flow of elements from Мн, Мз, Мо subsets accordingly.
The middle values of failure flow of elements from Мн, Мз, Мо subsets can be calculated like follows:

$$\mu_1 = \frac{\sum_{i=1}^{n_H} \mu_{Hi}}{n_H}, \qquad \mu_2 = \frac{\sum_{j=1}^{n_З} \mu_{Зj}}{n_З}, \qquad \mu_3 = \frac{\sum_{k=1}^{n_O} \mu_{Ok}}{n_O},$$

where $\mu_{Hi} = \frac{1}{T_{н1}}$, $\mu_{Зj} = \frac{1}{T_{Зj}}$, $\mu_{Ok} = \frac{1}{T_{Ok}}$,

where $T_{ні}$, $T_{зj}$, T_{ok} – the middle time of recovery of fault elements in Мн , Мз, Мо subsets accordingly.To evaluate the target has been defined the markov graph of states is constructed:



The Colmogorov collection of differential equations has been created based on graph of states.

$$\begin{cases} \frac{dP_o}{dt} = \mu_1 P_1 + \mu_2 P_2 + \mu_3 P_3 - P_o(\lambda_1 + \lambda_2 + \lambda_3) \\ \frac{dP_1}{dt} = \lambda_1 P_o - \mu_1 P_1 \\ \frac{dP_2}{dt} = \lambda_2 P_o - \mu_2 P_2 \\ \frac{dP_3}{dt} = \lambda_3 P_o - \mu_3 P_3 \end{cases}$$

This collection has been solved for $P_o(0)=1$, $P_1(0) = 0$, $P_2(0)=0$, $P_3(0)=0$ beginning conditions and probabilities of state $P_o(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$ achieved in form of functions depending from the time.
The values of probabilities $P_o(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$ will aspires to ultimate stationary values during the exploitation of system and when time goes to infinity value. Such values exists for a complex systems, because the number of system states have limit and system can go to any another state from every state.
The values of infinity probability states Po, P_1, P_2, P_3, which characterize middle relative times of system being in appropriate states, S1, S2, S3, can be calculated after collection of algebraic equations solved. The collection of algebraic equations can be created by transforming basic marcov model shown above:

$$\begin{cases} \mu_1 P_1 + \mu_2 P_2 + \mu_3 P_3 - P_o(\lambda_1 + \lambda_2 + \lambda_3) = 0 \\ \lambda_1 P_o - \mu_1 P_1 = 0 \\ \lambda_2 P_o - \mu_2 P_2 = 0 \\ \lambda_3 P_o - \mu_3 P_3 = 0 \\ P_o + P_1 + P_2 + P_3 = 1 \end{cases}$$

After the collection of algebraic equations is evaluated, the following safety values can be found: probability of dangerous system fault Роп, which equals to Рз; safety coefficient of system Кб = 1-P_3, probability of system state, when there is fault inside it, but it still works - P_1, probability of protective system state, when it doesn't operate - P_2.
Probability P_3 of dangerous system state S_3 can be decreased by using reservation of elements which faults arise system dangerous fault. To find out safety values of RSS system with reserved elements, the shown above basic Marcov's model of system with not reserved elements should be modified. The difference between basic and modified model is that, that all elements of Mo subset is reserved with reservation coefficient equals to one in modified model. The fault of any element of Mo subset of elements arise dangerous fault of system, so, because of this, Mo subset of elements occurs in form of consistent structure consisting of n_o elements.
Probability of fault of element reserved during the time t, when the separate reservation is used with coefficient equals to one, will be: $Q(t) = (1-P_k(t))^2$, where $P_к(t)$ – probability of no failure operation of element not reserved during time t. Probability of no failure operation of element k being reserved equals to $P_к(t) = 1 – (1- P_к(t))^2$. $P_k(t) = e^{-\lambda_{ok}t}$ there and $\lambda_{ок}$ - rate of occurrence of faults of element k of Mo subset, where к = 1,2 ... n_o. Reliability of consistent structure of reserved elements of Mo subset can be found from equation as follows:

$$P_{MO}(t) = \prod_{k=1}^{n_o} (1 - (1 - e^{-\lambda_{ok}t})^2).$$

Average time to fault of reserved elements of Mo subset to one fault is:

$$T_0 = \int_o^{\infty} \prod_{k=1}^{n_o} (1-(1-e^{-\lambda_{ok}t})^2)dt .$$

Intensity of failure flow of reserved elements from Mo subset is:

$$\Lambda_0 = \frac{1}{T} = \frac{1}{\int_o^{\infty} \prod_{k=1}^{n_o} (1-(1-e^{-\lambda_{ok}t})^2)dt} .$$

So, if the total failure flow of elements from Mo subset in basic marcov model of RSS is calculated based on equation $\lambda_3 = \sum_{k=1}^{n_o} \lambda_{ok}$, then intensity of failure flow of elements of Mo subset of modified model is:

$$\Lambda_o = \frac{1}{\int_o^{\infty} \prod_{k=1}^{n_o} (1-(1-e^{-\lambda_{ok}t})^2)dt} .$$

When the probabilities of faults of separate elements from Mo subset are small and to make redundancy of such elements are inadvisable or when some elements of Mo subset is not possible to make redundancy because of some reasons, then redundancy of some elements is used. Let some elements, i.e. m elements of Mo subset with the total amount of elements n_o, have redundancy and $m < n_o$. It is supposed, that m elements are reduced with redundancy coefficient equals to one. The Mo subset is pleated in to two parts – to reduced part with total amount of elements m, and to not reduced one with total amount t of elements equals to $n_o - m$. The total reliability of m elements of Mo subset is $P_{мор}(t) = \prod_{k=1}^{m} (1-(1-e^{-\lambda_{ok}t})^2)$, and the total reliability of elements not having redundancy Mo subset is $P_{мот}(t) = \prod_{k=m+1}^{n_o} e^{-\lambda_{ok}t}$.

The total reliability of reduced and not reduced elements of Mo subset is $P_{мо1}(t) = \prod_{k=m+1}^{n_o} e^{-\lambda_{ok}t} \cdot \prod_{k=1}^{m} (1-(1-e^{-\lambda_{ok}t})^2)$.

So, the average time of partly reduced Mo subset to one dangerous fault is

$$T_{01} = \int_0^{\infty} \prod_{k=m+1}^{n_o} e^{-\lambda_{ok}t} \cdot \prod_{k=1}^{m} (1-(1-e^{-\lambda_{ok}t})^2)$$

The rate of occurrence of faults of partly reduced subset M_o is $\Lambda_{01} = \frac{1}{T_{o1}}$

To find values of safety the computer emulation of markov models of safety has done for RSS different configurations: with not reduced; with redundancy of all "dangerous" elements; with redundancy of the less reliable "dangerous" elements.

The technology of calculation of safety values of RSS by using computerized models is demonstrated on examples. The results of that calculation are shown in table 1. The listings of computer realisation are not shown here because of limits to publications.

Table 1

Models	Version 1	Version 2	Version 3
Probability of dangerous fault	P_3=4,219·10^{-3}	P_3=2,226·10^{-3}	P_3=2,326·10^{-3}
Safety coefficient	1- P_3=0,996	1- P_3=0,998	1- P_3=0,997
Probability of system state, when there is fault inside it, but it still works	P1=6,821·10^{-3}	P_1=4,392·10^{-3}	P_1=4,392·10^{-3}
Probability of protect state of system with fault	P_2=0,044	P_2 = 0,044	P_2 = 0.044

It is necessary to point out, that probability of dangerous state of system, where all “dangerous” elements have redundancy, decreases strongly based on data comparison of table 1. But almost the same result is for system, where the less probable “dangerous” elements have redundancy in comparison with system, where all “dangerous” elements have redundancy.

Conclusion

The marcov model, base on “dangerous” element concept, of evaluation of safety parameters of RSS is proposed. Three versions of marcov models are worked out for different system configuration. The technology of computer realisation of models worked out is proposed. The evaluation of RSS safety parameters by using computer models is demonstrated on real example.

References

1. Materials of international seminar «Испытание систем железнодорожной автоматики и телемеханики на безопасность и электромагнитную совместимость». Gomel, 2003.
2. Сапожников В.В., Сапожников Вл.В., Христов Хр. Методы построения микроэлектронных систем железнодорожной автоматика и телемеханики. М.: Транспорт, 1995.
3. Швалов Д. В. „Автоматизированная система определения технического состояния устройств злектрической централизвции.” Ростов н/Д, 2001.
4. Х. Христов. „О теоретической модели безопасности систем железнодорожной автоматика и телемеханики, вырабатывающих свой ресурсю” Gomel, 2001.
5. Сертификация и доказательство безопасности систем железнодорожной автоматики, под ред. Вл.В.Сапожникова, Транспорт,1997.

Vladimirs Lubinskis, Dr.hab.sc.ing., profesor, Riga Technical university, Faculty of Transport and Machine Engineering, 8a, Indrika street, LV-1004, Riga, Latvia, Phone: +37167089650, faks:+371 7834289, e-mail: lubinskis@dzti.edu.lv

Ludmila Sergeyeva, Dr.sc.ing., asoc.profesor, Riga Technical university, Faculty of Transport and Machine Engineering, 8a, Indrika street, LV-1004, Riga, Latvia, Phone: +37167089650, faks:+371 7834289, e-mail: sla@latnet.lv

Ilja Korago, master degree, doctoral student, Riga Technical university, Faculty of Energetic, 8a, Indrika street, LV-1004, Riga, Latvia, e-mail: iljakor@inbox.lv

Ļubinskis V., Sergejeva., Korago I. Markova modelis dzelzceļa automatikas sistēmu drošības parametru noteikšanai

Tiek novērtēta dzelzceļa automātikas sistēmu drošuma aprēķināšanas kļūda, izmantojot bīstamu atteikumu koncepciju. Tiek dots Markova modelis dzelzceļa automātikas sistēmu drošuma novērtēšanai, kurš balstās uz "bīstama" elementa koncepciju. Tiek izstrādātas trīs modeļu versijas priekš sistēmas dažādām konfigurācijām un tiek piedāvātā to datoru realizācijas tehnoloģija.

Lubinskis V., Sergejeva L., Korago I. **The markov model to evaluate safety parameters of railway signalling systems**

The error of methods, based on conception of dangerous faults, evaluating of safety parameters of railway signalling systems is evaluated. The marcov model, based on conception of “dangerous” element, of evaluation of safety parameters of railway signalling systems is proposed. Three versions of marcov models are worked out and computer realisation of them is proposed, for different system configuration.

Любинский В., Сергеева Л., Кораго И. Марковская модель для определения показателей безопасности систем железнодорожной автоматики

Оценивается погрешность в расчетах уровня безопасности систем железнодорожной автоматики, основанных на концепции опасных отказов. Предлагается марковская модель оценки показателей безопасности систем железнодорожной автоматики, основанная на концепции «опасного» элемента. Для различных конфигураций системы разработаны три версии моделей и предложена технология их компьютерной реализации.