Mareks MEZITIS[1]
Vladimirs LUBINSKIS[1]
Julija KREPSHA[1]

AUTOMATION AND REMOTE CONTROL SYSTEMS SAFETY ESTIMATION BY ELEMENTS RELIABILITY ON RAILWAY TRANSPORT

ANNOTATION

It is discussed validity of the dangerous and safety failures concept by automation and remote control systems safety estimation. There is estimated error in automation and remote control systems calculation on safety levels that is based on the unsafe failures. It is proposed new decision to develop automation and remote control systems safety models that is based on the "unsafe" elements conception. It is developed three automation and remote control systems Markov models for systems different configurations. It is developed and explored computer models, obtained automation and remote control systems safety indicators numerical values:

- automation and remote control systems unsafe conditions probability,
- safety coefficient,
- probability of systems safe work.

1. CONCEPT OF SAFETY

Safety can be external and internal in systems like automation and remote control systems.

External safety is related to systems protection as an object and can be disrupted due to external influences.

Internal security is systems property to safe good, usable and protective condition. Considering systems safety estimations problem, it means systems internal security.

In the exploitation process system can be serviceable and defective.

If system is serviceable, it can be in three states:

- defective, but useable, when some systems elements failures don't effect systems basic functions;
- not usable, but protective, when all parameters values, that describe systems ability to perform its functions for ensuring train traffic safety and corresponds regulatory-technical and (or) design documentation;

[1] Riga Technical University (Riga, Latvia), mareks.mezitis@rtu.lv, vladimirs.lubinskis@apollo.lv, julia_225@inbox.lv

- not usable, unsafe, even if one of all parameters that describes systems ability to perform given functions for ensuring train traffic safety not corresponds regulatory-technical and (or) design documentation.

So system can be in four states:
- the correct,
- defective but usable,
- defective, not usable, but protective,
- unsafe.

Systems transfer from correct condition to one of defective is realized under the influence of two types:
- protective that transfer system from correct or defective but usable condition to inoperable but safe condition,
- not safe, whose appearance transfer system to inoperable and not safe condition.

Automation and remote control systems safety estimation problem is reduced to calculations by the formulas of reliability theory:

P(t) – *no-failure operation probability* – probability that within a given operating time t systems not safe failure does not occur;

Q(t) – *not safe failures probability* – probability that within a given operating time t not safe failure occurs at least once;

T – *mean operating time to not safe failure* – systems operating times mean value to the first not safe failure;

K – *safety coefficient* – probability that system will be in usable or protective condition at any given time.

If it is given value of not safe failures flow with an exponential distribution law, with exponential distribution law of safe work time, listed above safety indicators are defined by:

$$P(t) = e^{-\lambda t}, \quad Q(t) = 1 - P(t); \quad T_1 = \frac{1}{\lambda}, \quad K = \frac{T_1}{T_1 + T_2},$$

T_2 – is mean regeneration time.

2. ESTIMATION OF PRECISION FOR EXPONENTIAL PROBABILITY SAFETY MODEL

Safety probability model and adopted on it basis safety norms are mostly common and accepted. However, used for this models construction concept of division of system failures to dangerous and not dangerous is not perfect.

Legitimacy of using probabilistic models for various estimates calculations, including safety estimations, can be based only on a sufficiently large content of statistical data.

Meanwhile, automation and remote control systems not safe failures statistical data is not enough to construct probabilistic safety model. To collect necessary statistical data content on not safe failures is problematically because of the nature of them which appear very rarely.

Taking the assumption of exponential time distribution of no-failure operation, significantly simplify mathematical calculations to develop different probabilistic models – "law without memory".

In other words, if system is not denied to the time t, its no-failures operation time distribution will be the same if in this moment starts to use a completely new system.

Time distributions exponential dispersion between not safe failures is another interesting moment. Dispersion is $1/\lambda$ and standard deviation equal to mean value.

Purpose – to establish the accuracy and reliability of safety indicators obtained estimates according to statistical date content, using automation and remote control systems exponential probabilistic safety model.

Random quantity which examine – is time interval between not safe failures in automation and remote control systems devices in separate station.

3. UNSAFE ELEMENTS CONCEPTION

It's possible to use another approach for automation and remote control systems safety estimation. The nature of the proposed approach is that in analysed system total failure flow is not divisible to two different flows – safe and not safe failures. All systems elements failures are ordinary failures that lead element or device to defective condition. This failures flow intensity characterizes elements safety. Data about flow intensity or information about safety usually are recorded in elements technical passports.

Rejection not safe failures conception and based on the not safe elements conception it is not necessary to divide failures flow with intensity λ to two different flows – safe and not safe. All this flow failures are homogeneous, any flows failure leads system element to inoperable condition.

However, elements fault can bring system, which structure includes this element, to different conditions.

Automation and remote control systems elements variety M depends on system condition and can be divided for separated subsets:

- M_d – elements subset, even if one of all this subsets element will be fault system become to a defective but usable condition,
- M_p – elements subset, even if one of all this subsets element will be fault system become to a protective condition,
- M_n - elements subset, even if one of all this subsets element will be fault system become to not safe condition.

4. FORMULATION OF THE PROBLEM FOR AUTOMATION AND REMOTE CONTROL SYSTEMS SAFETY ESTIMATION BY THE ELEMENTS SAFETY

System – it is an object that is a set of elements that interacts in certain number of tasks perform process, and that are functionally interrelated.

Systems element – it is an object that is a set of systems simplest part, separate parts does not represent independent interest under consideration.

Consider automation and remote control systems safety estimations problem, systems element is its part with which failure system becomes to one of this conditions:

- defective but usable,
- inoperable protective,
- inoperable, not safe.

$N=n_d+n_p+n_n$, where n_d, n_p, n_n is elements number in the M_d, M_p, M_n subsets.

In the process automation and remote control system can be in one of conditions:

- S_0 – systems operative condition, all systems elements N are operative and perform its functions completely,
- S_1 – defective, but usable condition, if M_n subsets some elements are defective. This subsets elements failure does not affect operation of the system, so in case of failure of these elements system can perform its basic functions,
- S_2 – defective, inoperable protective condition, in this condition the system goes with one of the M_p subsets elements failure;
- S_3 – not safe condition.

System transition from operative condition S_0 to S_1, S_2 or S_3 condition is by the appearance of failures in M_d, M_p, M_n subsets elements. Failures flow intensity in this elements subsets are known, intensity values characterizes elements reliability and they are in elements technical documentations.

In M_d, M_p, M_n subsets elements failure appearance elements operative is restored by technical personal that services automation and remote control system. Elements mean time to restoration can be defined by automation and remote control systems exploitation experience on the accumulated statistical data processing basis.

To establish automation and remote control systems safety are known initial data:

- n_d , n_p, n_n – number of elements in M_d, M_p, M_n subsets respectively,
- λ_d , λ_p, λ_n – failures flow intensities vector values in the M_d, M_p, M_n subsets elements respectively. These vectors elements are λ_{di} , λ_{pj}, λ_{nk}.
- μ_d , μ_p, μ_n - regenerations flow intensities vector values in the M_d, M_p, M_n subsets elements respectively. These vectors elements are μ_{di} , μ_{pj}, μ_{nk}

5. AUTOMATION And REMOTE CONTROL SYSTEMS SAFETY MARKOV MODELS

5.1. *Models with unreserved elements description*

Systems model – Markov, on hypothesis repair flows are Poisson. In model are presented N unregistered systems elements variety that is divided to subsets M_d, M_p, M_n.

At any time system can be in one of four conditions – S_0, S_1, S_2, S_3. Systems conditions changes by the total influence - failures flow in the M_d, M_p, M_n subsets elements and the faulty elements regenerates flow.

Total failures flows are defined by ratio:

$$\lambda_1 = \sum_{i=1}^{n_d} \lambda_{di}, \quad \lambda_2 = \sum_{j=1}^{n_p} \lambda_{pj}, \quad \lambda_3 = \sum_{k=1}^{n_n} \lambda_{nk},$$

Where λ_1, λ_2, λ_3 - is M_d, M_p, M_n subsets elements failures total flows intensity.

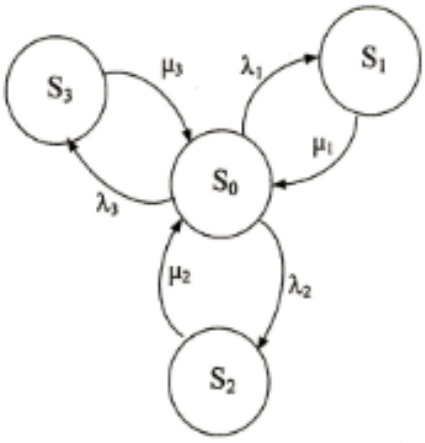
M_d, M_p, M_n subsets elements intensity regenerations mean values are defined:

$$\mu_1 = \frac{\sum_{i=1}^{n_d} \mu_{di}}{n_d}, \qquad \mu_2 = \frac{\sum_{j=1}^{n_p} \mu_{pj}}{n_p}, \qquad \mu_3 = \frac{\sum_{k=1}^{n_n} \mu_{nk}}{n_n},$$

Where T_{di}, T_{pi}, T_{ni} – faulty elements regeneration times mean values in the M_d, M_p, M_n subsets.

5.2. *State graph and differential equations system of Kolmogorov*

State graph:



By the graph states compose differential equations system of Kolmogorov:

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

Solving the problem for initial conditions:

t=0, $P_0(t=0)=1$, $P_1(t=0)=0$, $P_2(t=0)=0$, $P_3(t=0)=0$

will get state probabilities $P_0(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$ as time function.

5.3. *Automation and remote control systems limiting state probabilities*

In the automation and remote control systems exploitation process initial at t=0 systems original condition will change and at $t \to \infty$ $P_0(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$ probabilities values will seek to limited stationary values.

P_0, P_1, P_2, P_3 – limited conditions probabilities, can get by solving algebraic equations system:

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

P_0, P_1, P_2, P_3 conditions limited states values characterizes systems staying mean relative times in one of this state S_0, S_1, S_2, S_3.

By the results of solving algebraic equations system are defined safety indicators:

- Systems not safe conditions probability P_{ns}, this probability is equal to P_3,
- Systems safety coefficient: $K_s=1- P_3$,
- Probability of systems defective but usable condition – P_1,

- Probability of systems defective, not usable but protective condition – P_2.

5.4. *Automation and remote control systems Markov model with reserved elements*

5.4.1. *M_0 subsets all elements reservation*

Not safe conditions S_3 probability P_3 can be reduced by the elements reservation, which failure brings system into a dangerous state.

For automation and remote control systems safety indicators definition it is necessary to modify Markov system model that was described above. The difference between these models is that all M_0 subsets elements in the modify model are reserved with reservation coefficient equal one.

Anyone M_0 subsets elements failure leads system in not safe condition, that's why M_0 elements subset is necessary to submit in modify model as structures sequence that consider n_0 elements which are connected successively.

5.4.2. *M_0 subsets elements partial reservation*

Need for the M_0 subsets elements partial reservation may arise in cases, if subsets separate elements failure probability is small and this elements reservation is inappropriate. It is possible that some subsets elements cannot be reserved for some reasons. In such cases can use elements partial reservation.

6. CONCLUSION

1. Safety probability model and adopted on it basis safety norms are mostly common and accepted. However, used for this models construction concept of division of system failures to dangerous and not dangerous is not perfect.
2. There is proposed new approach to estimate automation and remote control systems safety. The essence of the approach is that in safety probability models different elements failures are homogeneous normal faults. Depending on whether failure is detected system can be in one of states:
- defective, but usable.
- defective, not usable, but protective,
- defective and dangerous.
3. In conformity with adopted concept of "dangerous" element are developed three automation and remote control systems Markov safety models:
- with unreserved "dangerous" items,
- with all "dangerous" items reservation,
- with least safety "dangerous" elements partial reservation.

7. REFERENCES

[1] Сертификация и доказательство безопасности систем железнодорожной автоматики, под ред. Вл.В. Сапожникова, Транспорт, 1997.
[2] Вентцель Е.С. Теория вероятностей, Наука, 1964.
[3] Б. Козлов, И. Ушаков. Справочник по расчету надёжности. М. Сов.Радио, 1969.