Julija FREIMANE, Mareks MEZITIS, Baglan TOGIZBAEVA

MARKOV MODELS OF FAIL-SAFE DEVICES OF AUTOMATION AND TELECONTROL SYSTEMS OF RAILROAD TRANSPORT

Streszczenie

The article introduces the concept of fail-safety of devices of automation and telecontrol of railroad transport. It proposes a fail-safety indicator for a complex evaluation of device safety and reliability. A model scheme of a fail-safe device of railroad automation and telecontrol is developed. Markov models of devices are developed to evaluate the level of fail-safety of these device.

INTRODUCTION

The task of choosing the most suitable complex indicator describing the safety and reliability of railroad automation and telecontrol is not a trivial one. Such task has been considered [1], where, along with such reliability indicators as possibility of fail-safe operation, possibility of dangerous failures, intensity of dangerous failures, average operating time per dangerous failure, a complex indicator is offered — the reliability factor K_d.

1. DEFINITION OF FAIL-SAFE TECHNICAL SYSTEMS

Fail-safety is a feature of a system enabling the performance of basic functions in case of failures in hardware or software components of the system. In terms of manner of performance, fail-safety can be divided into passive and active.

Active fail-safety is based on the use of additional means of hardware and software allowing to find and localise the failure and reconfigure the system so that it can perform its functions. Failures are found using means of control, they are localised using means of diagnostics and eliminated using automatic reconfiguration of the system. Reconfiguration is a change of the system in a way that damaged components are isolated from the functioning part.

Passive fail-safety is a feature of a system that prevents it from losing its functions in case of failure of individual elements of the system. Passive fail-safety is linked to an increased number of hardware means, and such fail-safety is implemented through various redundancy systems.

Fail-safe devices of railroad automation and telecontrol systems can be developed on the basis of passive fail-safety methods by employing certain active fail-safety elements. Means of control and diagnostics for finding and localising failures can be used as active fail-safety elements. These means form an additional structure that ensures monitoring of the current technical status of devices of railroad automation and telecontrol systems.

The use of such structure allows significant reductions of time necessary for regeneration of the working capacity of devices following failures in such devices.

In this way, passive fail-safe method study ensures an increased fail-safety of railroad automation and telecontrol devices, whereas the use of active fail-safety elements ensures reduced regeneration time.

Both of these factors allow to substantially increase the value of the readiness factor by approximating it to 1. It can be concluded that these devices feature high safety and reliability

2. STRUCTURE OF FAIL-SAFE DEVICES OF RAILROAD AUTOMATION AND TELECONTROL SYSTEMS

One of the possible versions of a structure of fail-safe devices of railroad automation and telecontrol systems is shown in Fig. 1.

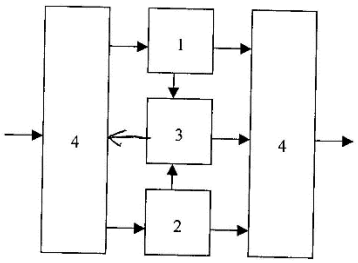

Fig. 1 *Structure of fail-safe devices*

Such structure is implemented in a form of a duplicate system, which is comprised of:

1. basic function block;
2. duplicate function block;
3. block of monitoring the current status of functional blocks;
4. two blocks ensuring switching between functional blocks following monitoring block signals.

Depending on the value and operating features of fail-safe devices of railroad automation and telecontrol systems, the redundancy blocks can be in one of the following modes:

a) Unused redundancy mode. In this mode, the redundancy working capacity resources of the block are not used.
If the basic block intensity λ_1 has a certain value, the redundancy block intensity $\lambda_2 = 0$.

b) Used redundancy mode. In this mode, the redundant working capacity resources are used the same way that the basic block resources.
In this case, λ_1 and λ_2 will have certain values if the reliability properties of the basic and redundancy blocks are identical, then $\lambda_1 = \lambda_2$.

c) Reduced mode is interpreted as an interim mode between the unused redundancy mode and used redundancy mode. In this mode, the redundancy block can fail at a certain intensity λ_2.

If $\lambda_2 = 0$, then the reduced mode becomes the unused redundancy mode, if $\lambda_1 = \lambda_2$, then used redundancy mode.

3. MARKOV MODELS OF FAIL-SAFE DEVICES OF RAILROAD AUTOMATION AND TELECONTROL SYSTEMS

The mathematical description of fail-safe duplicate device of railroad automation and telecontrol systems (Fig. 1) can be considered in a form of an exponential model. In the development of such model, it is considered that the failure-free operating time and the regeneration time of modelled device blocks are subject to exponential division.

4. DEVICE MODEL WITH UNUSED REDUNDANCY

Failures can occur in the functioning operation block of a railroad automation and telecontrol system device (Fig. 1). In case of a failure, after a signal formed with the monitoring block, the redundancy block is immediately activated and the failed block begins regeneration. As a result of regeneration, the failed block fully recovers its properties. The redundancy block does not use up its working capacity resources.

Failure-free operating time of functional blocks is subject to exponential division with parameter λ. The duration of restoration of a failed block is also subject to exponential division with parameter γ. It is necessary to develop a device functioning process model for the duplicate device of railroad automation and telecontrol systems.

A failure of such duplicate device occurs if both functional blocks are in a non-operating state.

The railroad automation and telecontrol system device (Fig. 1) can be in one of the following three states:

S_0 – both functional blocks are in working condition;

S_1 – one of the blocks either basic - 1 or redundant – 2 is failing;

S_2 – both blocks 1 and 2 are failing, i.e. S_2 state is duplicate device failure.

To determine the probability of failure-free operation in a given time interval *t* the Markov model is used wherein the device failure state S_2 is damping [4].

In this case, the process of functioning of the device is considered only up until the failure (when both blocks 1 and 2 (Fig. 1) have failed). Differential equations system describing the proess of the system functioning case

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -\lambda P_0(t) + \gamma P_1(t) \\ \dfrac{dP_1(t)}{dt} = -(\lambda+\gamma) P_1(t) + \lambda P_0(t) \\ \dfrac{dP_2(t)}{dt} = \lambda P_1(t) \end{cases} \quad (1)$$

where: $P_0(t)$, $P_1(t)$, $P_2(t)$ – the probability of that in the time moment *t* the device is in S_0, S_1, S_2 state respectively.

For initial premises $P_0(0) = 1$, $P_1(1) = 0$, $P_2(2) = 0$ the differential equation system can be resolved analytically by following the described methodology [3].

When resolving the equation system, the probability of failure-free operation of the device can be determined R(τ), equalling the sum of the probabilities $P_0(t)$ and $P_1(t)$:

$$R(\tau) = P_0(t) + P_1(t) \quad (2)$$

$$R(t) = e^{-(\lambda+\frac{\gamma}{2})t}\left[ch\left(\frac{t}{2}\sqrt{4\lambda\gamma+\gamma^2}\right)+\frac{2\lambda+\gamma}{\sqrt{4\lambda\gamma+\gamma^2}}sh\left(\frac{t}{2}\sqrt{4\lambda\gamma+\gamma^2}\right)\right] \quad (3)$$

To determine the fail-safe factor of the device, the average values of failure-free operating time and regeneration are necessary.

The average regeneration time T_R, by using the exponential division rule with parameter γ, equals $T_R = 1/\gamma$.

To determine the average failure-free operating time T_0, an equation known in safety theory is used, linking T_0 and the probability of failure-free operation of the device R(τ), i.e.:

$$T_0 = \int_0^\infty R(t)dt \quad (5)$$

$$T_0 = \frac{2}{\lambda} + \frac{\gamma}{\lambda^2} \quad (6)$$

The value of regeneration intensity γ normally is considerably higher than the λ value, i.e. regeneration takes place faster than the failure-free operating period ends.

5. DEVICE MODEL WITH USED REDUNDANCY

In this model, it is suggested that both functional blocks 1 and 2 (Fig. 1) are in operating mode. Thus, the transitional intensity from state S_0 to state S_1 will be equal to 2λ. Other operating premises of the device are analogically reviewed in Section V.

The differential equation system that describes the process of the case of device functioning is as follows

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -2\lambda P_0(t) + \gamma P_1(t) \\ \dfrac{dP_1(t)}{dt} = -(\lambda+\gamma) P_1(t) + 2\lambda P_0(t) \end{cases} \quad (7)$$

For the initial premises $P_0(0) = 1$, $P_1(1) = 0$, a computing procedure described in [3] is used.

The probability R(τ) of failure-free operation of a device with used redundancy equals the sum of probabilities $P_0(t)$ and $P_1(t)$:

$$R(\tau) = P_0(t) + P_1(t) \quad (8)$$

$$R(t) = e^{-\frac{3\lambda+\gamma}{2}t}\left[ch\left(\frac{t}{2}\sqrt{\lambda^2+6\lambda\gamma+\gamma^2}\right)+C\right] \quad (9)$$

$$C = \frac{3\lambda}{\sqrt{\lambda^2+6\lambda\gamma+\gamma^2}}ch\left(\frac{t}{2}\sqrt{\lambda^2+6\lambda\gamma+\gamma^2}\right) \quad (10)$$

The fail-safe factor K_0 is determined using a method that is analogical to the method reviewed in Section V. T_o and T_R was expressed according to the equations

$$T_0 = \int_0^\infty R(t)dt \quad 11)$$

$$T_R = \frac{1}{\gamma} \quad (12)$$

and the obtained results were inserted in equation K_0.

$$T_0 = \int_0^\infty R(t)dt = \frac{3}{2\lambda} + \frac{\gamma}{2\lambda^2}, \quad (13)$$

$$T_R = \frac{1}{\gamma}, \quad (14)$$

$$K_0 = \frac{T_0}{T_0 + T_R} \quad (15)$$

6. DEVICE MODEL IN REDUCED REDUNDANCY BLOCK MODE

In this model, the failure flow intensity of the operating block is equal to λ and of the redundancy block λ_1; furthermore, $\lambda_1 < \lambda$. Thus, the transitional intensity from state S_1 to state S_2 will be equal to λ.

The differential equation system that describes the process of the case of device functioning is as follows

$$\begin{cases} \frac{dP_0(t)}{dt} = -(\lambda + \lambda_1)P_0(t) + \gamma P_1(t) \\ \frac{dP_1(t)}{dt} = -(\lambda + \gamma)P_1(t) + (\lambda + \lambda_1)P_0(t) \end{cases} \quad (16)$$

As a result of resolving this system for this initial premises $P_0(0) = 1$, $P_1(1) = 0$ we obtain an equation determining $P_0(t)$ and $P_1(t)$, by summing them, we obtain an equation of the duplicate device with the reduced redundancy block mode for calculating failure-free operating probability R(τ).

$$R(t) = e^{(-\lambda + \frac{\lambda+\gamma}{2})t}[A + B], \quad (17)$$

$$A = ch\left(\frac{t}{2}\sqrt{\lambda_1^2 + 2\gamma(2\lambda + \lambda_1) + \gamma^2}\right), \quad (18)$$

$$B = \frac{2\lambda + \lambda_1 + \gamma}{\sqrt{\lambda_1^2 + 2\gamma(2\lambda + \lambda_1) + \gamma^2}} \cdot sh\left(\frac{t}{2}\sqrt{\lambda_1^2 + 2\gamma(2\lambda + \lambda_1) + \gamma^2}\right)$$

To calculate the fail-safe factor, we determine the average duration of failure-free operations, by using the equation.

$$T_0 = \int_0^\infty R(t)dt$$

Then, we find the value of K_0 by using the equation:

$$K_0 = \frac{T_0}{T_0 + T_R} \quad T_R = \frac{1}{\gamma}$$

CONCLUSION

Comparison:

Bez rezerves	Ar rezervi
$K_g = 0.9$	$K_g = 0.99$
P(t=100) = 0.75	P(t=100) = 0.85
R(τ) = 0.6	R(τ) = 0.79
Without redundancy	With redundancy

The value of technical system availability factor is 1 — it is a reliability threshold which to approximate in the formation of a technical system.

Improved reliability is linked to increased consumption in the process of forming these systems. Not only the device manufacturing requirements should be compared, but also the economic losses after device failure due to accident.

Some devices must be subject to very high security requirements; solutions must be sought for ensuring such requirements.

Fail-safe systems — modern centralisation microprocessor systems, which use duplication schemes of central processor blocks.

By using active and passive fail-safe methods, high reliability values that are close to the threshold values will be ensured.

The results — at low reliability level of functional blocks, the factor is close to 1, which reaches 1 upon increasing the restoration intensity.

ACKNOWLEDGEMENTS

The value of technical system availability factor is equal to 1 — it is a reliability threshold which to approximate in the formation of technical systems, the failure of which can lead to catastrophic outcomes. Thus, it is known that one of the most complex questions in safety theory is the choice of justified numerical safety requirements for technical devices of various purposes.

Increased safety of technical systems is related to increased consumptions in the manufacture of these systems, however, in justifying the safety requirements, not only the consumption of manufacturing of devices must be compared, but also economic losses that would be caused as a result of an accident or catastrophe in case of device failure.

Systems ensuring safety of railroad traffic contain devices, the failure of which can lead to tragic consequences. Safety requirements of such devices must be particularly high, and in these situations, the problem is not the price of such devices, but rather how to technical implement such requirements.

The method proposed in the article is an attempt to create practically failure-free devices.

Modern microprocessor centralisation systems, in which schemes duplicating the central processor block are used, can serve as an example of effectuating a fail-safe computer system.

Bearing in mind the possibilities offered by microprocessor technologies, it can be claimed that duplicating schemes with automatic control of the technical status of the functional block can be used for various device types. The use of active and passive fail-safety in the development of devices of railroad automation and telecontrol systems

will ensure high reliability values that approximate the maximum possible values.

Modelling results of fail-safe devices having the considered structure show that, even given a comparatively low functional block safety, the safety factor of the considered structure is close to one, and by increasing the regeneration intensity it becomes equal to one.

REFERENCES

1. Сертификация и доказательство безопасности систем железнодорожной автоматики. Под редакцией В.В. Сапожникова. М. Транспорт, 1997 г.
2. Теория проектирования вычислительных машин, систем и сетей. Под ред. В.И. Матова. Москва, изд. МАИ.
3. B. Epstein, T. Hasford. Reliability of some two unit redundant systems. Proc. 6-th Nat. Symposium on Reliability and Quality Control, 1960 y.
4. В. Козлов, И. Ушаков. Справочник по расчету надежности. М. Советское радио, 1975 г.