MODELLING OF FAILURE EFFECTS TO INTEGRITY OF SYSTEM

Karol Rástočný
Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita, Veľký diel, 010 26 Žilina, e-mail: karol.rastocny@fel.utc.sk

Summary The interlocking systems are typically resisting against hazardous faults. Failure effects on the system can be determined directly by monitoring the original system installation, by simulation of the system operation using its model, or by computing or theoretical reasoning. The process of system ageing can be described with the help of the random failure time. Essential majorities of computer-based interlocking system elements are electronic elements that are not exposed to mechanical wear. The failure distribution of these elements is assumed to be exponential.

1. INTRODUCTION

Fail-safety is the typical behaviour of railway signalling systems. In consideration of the reached knowledge-level and limited technical and economical possibilities it is realistic to recognise that there is still certain hazard and that it is practically not possible to avoid it completely. That's why the term „safety" has to be understood relatively and quantitative methods should be used for its quantification [1], [2]. For a successful solution of this problem a systematic approach is necessary. It could be characterised as a searching process of the optimal strategy for safety assurance. This process concern all phases of the product life-cycle. To reach the safety of a signalling system, the pre-production phases of his life-cycle are important, because the system has to be already born with safety. It is not possible to „add" the safety to the system [3].

In order to raise the reliability or safety of the system, following measurements could be applied - but they drive to redundancy:

- of the hardware – reservation of construction-parts at all levels of the system;
- of the software – implementation of diagnostic systems (they are not necessary for the operational function), program for repeating or multiple repeating calculation;
- of the information – using of coding for failure detection or correction;
- of the time – additional raising of time request for the calculation together with information and software redundancy or prolongation of the calculation time as a consequence of the repeating.

As a rule, one form of redundancy implicate another forms of redundancy. For this reason, redundancy usually can be divided into:

- space redundancy;
- time redundancy.

Space redundancy is bound to the hardware, and its using can be caused not only by the hardware redundancy but also by the software and information redundancy, because the existence of this both forms of redundancy is bound to the hardware. Time redundant is usually bound to the software, information and time redundancy.

Which form of redundancy and what extent it will be used to, should be decided in the beginning phase of the system life-cycle, when on the basis of reliability and safety specification the future structure of the system will be designed. By choosing the system structure, simple models describing safety characteristics of the system can be used.

In the following phases of the system life-cycle a much more complicated model could be constructed, depending on the concrete solution of the system.

2. PROBABILITY MODEL OF THE FAILURE EFFECTS

The failure rate of the component could be considered as a phenomenon (a common expression in the technical literature is event). As a common rule we can consider that if the phenomenon $A_1,..., A_n$ are:

- statistically dependent, then probability of their intersection

$$P_{\left(\bigcap_{i=1}^{n} A_i\right)} = P_{(A_1)} \cdot P_{(A_2|A_1)} \cdot P_{(A_3|A_1A_2)} \cdots P_{(A_n|A_1A_2 \ldots A_{n-1})}; \quad (1)$$

- conjoint, then probability of their union

$$P_{\left(\bigcup_{i=1}^{n} A_i\right)} = \sum_{i=1}^{n} P_{(A_i)} - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} P_{(A_i \cap A_j)} + \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} P_{(A_i \cap A_j \cap A_k)} \cdots + (-1)^{n-1} P_{\left(\bigcap_{i=1}^{n} A_i\right)}; \quad (2)$$

- statistically independent, then probability of their intersection

$$P_{\left(\bigcap_{i=1}^{n} A_i\right)} = \prod_{i=1}^{n} P_{(A_i)}; \quad (3)$$

- mutually exclusive (disjoint), then probability of their union

$$P_{\left(\bigcup_{i=1}^{n} A_i\right)} = \sum_{i=1}^{n} P_{(A_i)}. \quad (4)$$

Two phenomena are mutually exclusive, if it is not possible for them to occur contemporary. Two phenomena are independent, if the occurrence of one of

them does not change the occurrence probability of another.

The occurrence of the event A_i when it is known that A_j has occurred, is know as the conditional event. The probability of this conditional event is defined as

$$P_{(A_i/A_j)} = \frac{P_{(A_i \cap A_j)}}{P_{(A_j)}}, \tag{5}$$

under the premise, that $P_{(A_j)} \neq 0$.

The occurrence of the failure is considered as unavoidable and that's why the signalling systems must include mechanisms to manage (to negate) the failure consequences. The measurements for failure control are effective only if the failure can be identified. Therefore, computer-signalling systems are equipped with a functional diagnostic system and as a rule with a testing diagnostic system too.

Let assume that the failure detection and negation mechanism operate in the way, that if a failure was detected during the time interval $\langle (k-1)t_0, k t_0 \rangle$, then in the end of this time interval the system will get into pre-defined safety state, but if no failure was detected during the time interval $\langle (k-1)t_0, k t_0 \rangle$, so the system can continue his work as failure-free (where k = 1, 2, 3, ...). Because of security reason, the probability of the hazard state occurrence must be detected during this time interval.

2.1. Model for a system *n* oo *n*

We think of a multi-channel system with an evaluation circuit (Fig. 1). Voting element should accompolish only the voting function *n* oo *n* and should feature ideal characteristics regarding reliability and safety.

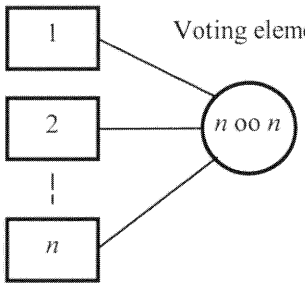

Fig. 1. Principal diagram of a multi-channel system n oo n.

The occurrence of the event A_n means the occurrence of failure of n channels (units) during the time interval $(t, t + t_0\rangle$ under the premise, that up to time t no failure of no n unit occurred. Concerning the safety reason, occurrence of the event A_n should be seen as dangerous.
Probability of occurrence of the event A_n

$$P_{(t\langle T_1 \le t+t_0, t\langle T_2 \le t+t_0, \ldots, t\langle T_n \le t+t_0 | T_1\rangle t, T_2\rangle t, \ldots, T_n\rangle t)} = \frac{P_{(t\langle T_1 \le t+t_0, t\langle T_2 \le t+t_0, \ldots, t\langle T_n \le t+t_0, T_1\rangle t, T_2\rangle t, \ldots, T_n\rangle t)}}{P_{(T_1\rangle t, T_2\rangle t, \ldots, T_n\rangle t)}} = \frac{P_{(t\langle T_1 \le t+t_0, t\langle T_2 \le t+t_0 \ldots, t\langle T_n \le t+t_0)}}{P_{(T_1\rangle t, T_2\rangle t, \ldots, T_n\rangle t)}}, \tag{6}$$

In the case of exponential distribution of failure occurrence for each unit the probability of failure occurrence of all n elements in the time interval $(t, t + t_0\rangle$ is defined by

$$P_{(t\langle T_1 \le t+t_0, t\langle T_2 \le t+t_0, \ldots, t\langle T_n \le t+t_0)} = \prod_{i=1}^{n} \left(1 - e^{-\lambda_i t_0}\right) e^{-\lambda_i t} \tag{7}$$

and probability of failure-free operation of all units n in the time $T \le t$

$$P_{(T_1 \le t, T_2 \le t, \ldots T_n \le t)} = \prod_{i=1}^{n} e^{-\lambda_i t_0}, \tag{8}$$

where λ_i means the failure rate of the i-th unit.

Then

$$P_{(t\langle T_1 \le t+t_0, t\langle T_2 \le t+t_0, \ldots, t\langle T_n \le t+t_0 | T_1\rangle t, T_2\rangle t, \ldots, T_n\rangle t)} = \prod_{i=1}^{n} \left(1 - e^{-\lambda_i t_0}\right). \tag{9}$$

We think of following systems:

- One-channel system; this system comprehends only one unit with constant of failure rate λ_1. Failure of the unit means also occurrence of an undesirable incident. Then

$$P_{(t\langle T_1 \le t+t_0, | T_1\rangle t)} = \left(1 - e^{-\lambda_1 t_0}\right). \tag{10}$$

- Two-channel system 2 oo 2; this system comprehends two units with constant of failure rate λ_1 and λ_2. A contemporaly occurrence of failure of both units means also occurrence of an undesirable incident . Then

$$P_{(t\langle T_1 \le t+t_0, t\langle T_2 \le t+t_0 | T_1\rangle t, T_2\rangle t)} = \left(1 - e^{-\lambda_1 t_0}\right)\left(1 - e^{-\lambda_2 t_0}\right). \tag{11}$$

- Three-channel system 3 oo 3; this system comprehends three units with constant of failure rate λ_1, λ_2 a λ_3. A contemporaly occurrence of failure of all three units means also occurrence of an undesirable incident. Then

$$P_{(t\langle T_1 \le t+t_0, t\langle T_2 \le t+t_0, t\langle T_3 \le t+t_0 | T_1\rangle t, T_2\rangle t, T_3\rangle t)} = \left(1 - e^{-\lambda_1 t_0}\right)\left(1 - e^{-\lambda_2 t_0}\right)\left(1 - e^{-\lambda_3 t_0}\right). \tag{12}$$

2.2. Model for the system *m* oo *n*

We think of a multi-channel system with an evaluation circuit. Evaluation circuit should accomplish

only the voting function m oo n and should feature ideal characteristics regarding reliability and safety.

Occurrence of the event A_i means failure rate of some m units of the entire number of n units during the time interval $(t, t + t_0\rangle$ under the premise, that up to time t no failure of no m unit occurred. Concerning the safety reason, occurrence A_i should be seen as dangerous. The total number of different events A_i for the system m oo n is defined by

$$k = \binom{n}{m} = \frac{n!}{m!.(n-m)!}. \tag{13}$$

Then the occurrence probability of at least one A_i

$$P_{\left(\bigcup_{i=1}^{k} A_i\right)} = \sum_{i=1}^{k} P_{(A_i)} - \sum_{i=1}^{k-1}\sum_{j=i+1}^{k} P_{(A_i \cap A_j)} + \tag{14}$$
$$+ \sum_{i=1}^{k-2}\sum_{j=i+1}^{k-1}\sum_{l=j+1}^{k} P_{(A_i \cap A_j \cap A_l)} \ldots + (-1)^{k-1} P_{\left(\bigcap_{i=1}^{k} A_i\right)}$$

where A_i is i-th event of the entire number k.

Railway signalling systems are often designed as 2 oo 3 systems. In the case of a 2 oo 3 system we should assume the occurrence of following events:

- Event A_1 – failure occurrence of the unit 1 and unit 2 during the time interval $(t, t + t_0\rangle$ under the premise, that up to time t no failure occurred at unit 1 nor at unit 2.
- Event A_2 – failure occurrence of the unit 1 and unit 3 during the time interval $(t, t + t_0\rangle$ under the premise, that up to time t no failure occurred at unit 1 nor at unit 3.
- Event A_3 – failure occurrence of the unit 2 and unit 3 during the time interval $(t, t + t_0\rangle$ under the premise, that up to time t no failure occurred at unit 2 nor at unit 3.

Occurrence probability of event A_k

$$P_{\left(\forall \langle T_i \le t+t_0, t \langle T_j \le t+t_0 | T_i \rangle t, T_j \rangle t\right)} = \left(1 - e^{-\lambda_i t_0}\right).\left(1 - e^{-\lambda_j t_0}\right), \tag{15}$$

where $k = 1, 2, 3$, while $i \neq j$ and λ_i means rate of the i-th unit.

Events A_1, A_2, A_3 are statistically depending on each other. Conditional probability of failure occurrence 2 of 3 units during the time interval $(t, t + t_0\rangle$ under the premise, that up to time t no failure occurred at unit 1 nor at unit 2, nor at unit 3.

$$P_{\left(\bigcup_{i=1}^{3} A_i\right)} = P_{(A_1)} + P_{(A_2)} + P_{(A_3)} - P_{(A_1 \cap A_2)} - \tag{16}$$
$$- P_{(A_1 \cap A_3)} - P_{(A_2 \cap A_3)} + P_{(A_1 \cap A_2 \cap A_3)}$$

In the case of exponential distribution of failure occurrence for each one unit

$$P_{(2z3)} = \left(1 - e^{-\lambda_1 t_0}\right).\left(1 - e^{-\lambda_2 t_0}\right) + \left(1 - e^{-\lambda_1 t_0}\right).\left(1 - e^{-\lambda_3 t_0}\right) + \left(1 - e^{-\lambda_2 t_0}\right).\left(1 - e^{-\lambda_3 t_0}\right) - 2.\left(1 - e^{-\lambda_1 t_0}\right).\left(1 - e^{-\lambda_2 t_0}\right)\left(1 - e^{-\lambda_3 t_0}\right) \tag{17}$$

If there is a system supplied with identical channels $(\lambda_1 = \lambda_2 = \lambda_3 = \lambda)$

$$P_{(2z3)} = 1 - 3.e^{-2\lambda t_0} + 2.e^{-3\lambda t_0}. \tag{18}$$

Fig, 2 shows the probability of failure occurrence diagram of critical failure occurrence function, for various structures of multi-channel systems. We can see at Fig. 1, that by judging the safety of the system only by integrity, in this case a 2 oo 3 system features worse parameters than 2 oo 2 or 3 oo 3 system.

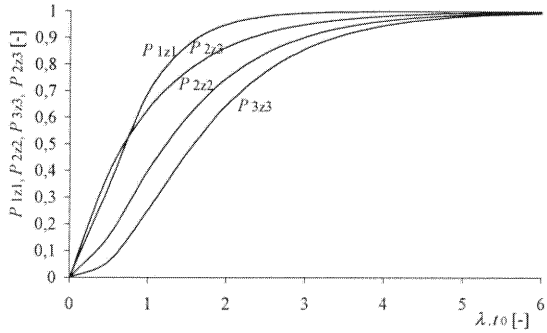

Fig. 2. Diagram of probability of critical failure occurrence at several multi-channel systems.

Regarding complex systems there is a real assumption, not to detect and master all failures within the pre-defined time interval.

Should

$$\delta = \frac{1}{MTDF}, \tag{19}$$

where $MTDF$ is the mean time to failure detection and δ is the rate of failure detection.

We assume multi-channel systems according to Fig. 1 with an evaluation circuit accomplishing the voting function 2 oo 2 or 2 oo 3. The channels of the proposing systems are identical and are characteristic by their constant failure rate λ and constant rate of failure detection δ. For the proposed systems there are in [4] divided following relation to calculate the probability of hazardous system state:

$$P_{2z2} = \frac{\lambda}{\lambda + \delta} + \frac{\lambda}{\lambda - \delta} e^{-2\lambda t} - \frac{2\lambda^2}{\lambda^2 - \delta^2} e^{-(\lambda+\delta)t}, \tag{20}$$

$$P_{2z3} = \frac{2\lambda}{2\lambda + \delta} + \frac{2\lambda}{\lambda - \delta}.e^{-3\lambda t} - \frac{6\lambda^2}{(\lambda - \delta)(2\lambda + \delta)}.e^{-(2\lambda+\delta)t}. \tag{21}$$

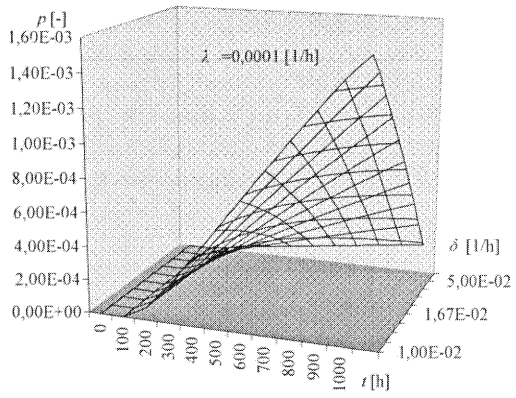

Fig. 3. Probability hazardous state of the system 2 oo 2.

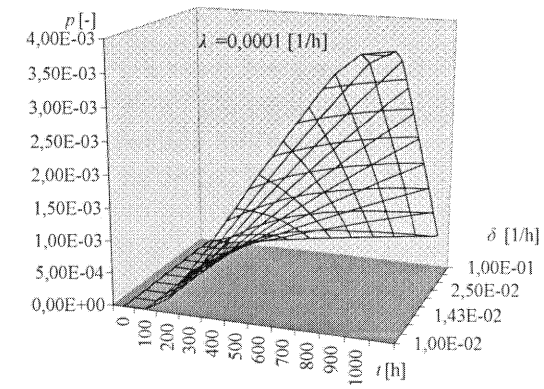

Fig. 4. Probability hazardous state of the system 2 oo 3.

Fig. 3 (Fig. 4) a diagram is demonstrating the probability hazardous state for the system 2 oo 2 (2 oo 3) for precise value λ and δ. The diagrams show, that probability hazardous state of the system is depending at a high degree on the failure detection time. We can conclude, that multi-channel systems can reach the required safety level also with standard elements under the condition of early failure detection. Generally, the better the reliability parameters are, the lower the requirements for the failure diagnostic system are.

3. CONCLUSION

It is characteristic for an unit (system) with exponential distributed probability of failure occurrence, that if this unit (system) at time t has not yet failed, its failure rate within the next time interval $(t, t + t_0)$ is not depending on time t, but on the time interval $(t, t + t_0)$.

A signalling system is considered to be a system in continual operation and in the case of failure responsibility for the railway traffic changes to the human operator. The error rate of a human being is much higher then of the system. Hence, the final hazard related to the signalling system operation depends on the system reliability too. To compare the integrity and availability could change the situation in favour of the system 2 oo 3.

Generally, the safety of a system could be understood as a collection of its characteristics, where we can include, beside others, the system integrity and readiness. System safety integrity is a dominant, but not the only safety attribute of the system. There is a usual approach to build a model for each system characteristic. Such an approach can reach local optimum for particular characteristics. There is certain dependency between essential characteristics of the system. So it is useful to build a model, which allows to find a global optimum while respecting required minimal levels of characteristics and economical acceptation of the proposed solution. Such a model could be advanced to the process operation level and accept the hazards coming from the persons participating at the controlling.

REFERENCES

[1] RÁSTOČNÝ, K.: Probability Model of Failure Effects Analysis. 4th international scientific conference ELEKTRO '01, May 22 - 23, 2001 Žilina. Zborník ss. 84 – 89. ISBN 80-7100-837-0.

[2] RÁSTOČNÝ, K.: Analýza rizika železničného signalizačného systému. AEEE No. 3-4 Vol. 2/2003. ss. 24 – 29. ISSN 1336-1376.

[3] STN EN 50 129: Dráhové aplikácie. Komunikačné a signalizačné systémy a systémy na spracovanie údajov. Elektronické signalizačné systémy súvisiace s bezpečnosťou 2004.

[4] RÁSTOČNÝ, K.: Modely pre analýzu bezpečnosti. Habilitačná práca. 1998.

[5] LAMOŠ, F.; POTOCKÝ, R.: Pravdepodobnosť a matematická štatistika. Bratislava, Alfa 1989.