SCIENTIFIC PAPERS
OF THE UNIVERSITY OF PARDUBICE
Series B
The Jan Perner Transport Faculty
15 (2009)

HAZARD RATE OF REDUNDANT STRUCTURE 2oo2

Jiří KONEČNÝ

Department of electrical and electronic engineering and signaling in transport

1. Purpose and operation principle of railway interlocking systems

Most railway accidents in history were caused by human factor malfunction in rail traffic control. Therefore, since the beginning of railway signaling and interlocking systems which aim is to check and replace the human factor have been used.

An interlocking system must fulfil requirements on functional and technical safety. Functional safety concerns the correct system behaviour in a failure-free state: values on outputs must not be less restrictive than a corresponding conditions. Technical safety can be characterized by the words „fail-safe“. It means that the system is safe not only in failure-free state, but also during failure. After the system or subsystem failure its outputs must be set immediately on restrictive values.

2. Principles of detection and negation of random faults

State-of-the-art railway interlocking systems are electronic, and mostly processor-oriented. A microprocessor and memory are large-scale integrated circuits, it is almost impossible to identify all random fault modes that may occur. Therefore it is supposed, that a potentially dangerous failure can occur in these circuits, which could lead to an unrestricted state on the outputs.

To ensure technical safety of programmable electronic systems there are two different generally used safety architectures: a reactive fail-safety and a composite fail-safety.

In order to ensure the technical safety of certain functions (eg. data comparison and negation of failure) in programmable electronic systems there are also circuits used with inherent fail-safety, i which when applied each random fault mode in view must lead to safe mode, ie, a restrictive state on the output. These electronic circuits consist mostly of descrete components – it´s possible to identify all random fault modes and prove that they do not cause hazard.

Reactive fail-safety

Reactive fail-safety relates mainly to single channel structures. A nonrestrictive state on the outputs of system at failure is permissible only for a shorter time than is a reaction time of a controlled object (eg. switch-on time of relay). Reactive systems are not subject of this paper.

Composite fail-safety

Composite fail-safety is based on redundancy, mainly on hardware redundancy: the same safety – relevant functions are performed by more functional units (channels). Basic output values are compared, but usually input and intermediate values are also compared. Other than the restrictive values on the device outputs can be set only when compared data coincide. The redundant structure 2oo2 monitors a semantic match between the two channels, while in redundant voting structures (eg. 2oo3) then the data of most channels match. If there is a disagreement in the data comparison, a safety reaction must follow: outputs of a defective channel (or outputs of the whole system) are irreversibly set into restrictive, usually unexcitated state (except of some special cases, eg. output for control of red light warning lights of a level-crossing‘s equipment, or output of red light signal).

Commonly used redundant structures in railway signaling are 2oo2, 2 x 2oo2, or 2oo3. In the case of two channel structure after failure there are restrictive values set on the outputs of the whole structure (system, subsystem). In 2oo3 structure only the channel which is outvoted by the other two channels is shut down at first. The whole device is shut down only after a failure of another of the two remaining channels. Commissioning into a basic, (ie a nonrestrictive) state is possible only after a failure disposal, after specific tests have been performed successfuly and after failure-free state is confirmed by a maintenance worker.

The safety of mutichannel (redundant) structures is generally based on an assumption that **no single random fault is dangerous** – a single channel failure must not result in an occurance of a dangerous state on the output. Only multiple random fault could be dangerous, ie, hardware failure in multiple channels. Certain safety risks are also connected to common cause failures (CCF), such as electromagnetic interference in multiple channels simultaneously, a power supply failure, etc. An occurence of common

cause failures is prevented by a set of systematic measures to ensure a functional and physical independency of the channels.

An occurence of a multiple random fault is prevented by:

- high reliability of each channel of the redundant structure,
- comparison with a requirement for the shortest possible detection and negation time of single random fault,
- periodic on-line tests, whose purpose is to decrease an occurence probability of undetected random failures of hardware;

Failure rate of a single channel of a redundant structure

To simplify the calculations an exponential distribution of failure probability is usually taken into account. Then, the failure rate of one channel element can be calculated as a reciprocal of mean time to failure:

$$\lambda = 1 / MTTF \quad [h^{-1}] \tag{1}$$

Reliability of one channel can be described as a serial reliability model. Then, the failure rate of the whole channel is constant over time, and it can be calculated as a sum of the failure rates of individual elements (components):

$$\lambda_{1K} = \lambda_1 + \lambda_2 + \ldots + \lambda_n \quad [h^{-1}] \tag{2}$$

One channel of the redundant structure contains usually large - scale integrated circuits, such as microprocessor, memory, gate array, communication contollers, etc. Less demanding applications used microprocessors with program and data memory on a single chip (single - chip microcomputers). Currently, semiconductor manufacturers declare very high values of mean time to failure (MTTF). For microprocessors are commonly reported values greater than ten million hours. For example, for sixteen - bit C167CS microprocessor manufacturer indicates a mean time to failure 500 million hours. MTTF values of RAM and ROM memories move in order of millions of hours. Failures of discrete components and wiring assemblies usually occur safely. Based on these findings, 1 million hours MTTF is considered in the following model calculations for one channel of the redundant structure 2 out of 2.

According to standard [1], twenty times lower failure rate may be considered for a stored device (without power supply).

Detection and negation time of single random fault

Detection time of single random fault can vary greatly:

- seconds, minutes and hours – failure is detected and negated automatically by the device,
- half a year to 5 years – the fault is detected and negated by a maintenance worker during a regular inspection and device tests,
- 5-10 years – the device is stored in the long-term and subsequently is put into operation after comprehensive verification,
- life time of the device (20-40 years) – an undetected single failure may persist in the system throuhout its operational life;

In railway signaling equipment, the negation time of failure is mostly neglected because it is usually several orders of magnitude shorter than the time to failure detection.

Automatic detection of single random fault

Single random fault in the redundant structure is detected by data comparison and periodic on-line tests, whereas comparison of output values must be fail-safe according to [1]. Also, periodic on-line tests should be evaluated safely, ie, test failure should be detected by a second, independent entity. However, this requirement is not clearly declared in the standard [1].

Time to failure detection is dependent on a comparison data cycle and on a periodic on-line test cycle. Typical time for comparison output cycle is several hundred milliseconds. Test cycle time is dependent on the complexity and extensiveness of the test. Simpler tests (eg, CRC datagram check) last in order of magnitude hundreds of milliseconds. However, processor and memory tests may take several minutes or even hours.

Automatic negation of single random fault

Hazard can occure on the outputs of a defective unit, therefore a negation of single random failure is carried out immediately after its detection:

- the whole defective unit is irreversibly shut down, and thus all its outputs too, or
- only safe outputs of the unit are irreversibly shut down;

The term „safe output“ means a data bus or an analog output, from which the safety-relevant commands are given. Control interlocking system can communicate with other control interlocking systems or it can control the external elements (switches, signal lights, etc.) directly.

Negation of single random fault lasts typically the units of milliseconds. If a larger system is considered, a transmission delay is applied between the defective unit and the negated output (usually hundreds of milliseconds to seconds units).

Negated failures and diagnostic coverage

It´s almost impossible to identify all fault modes in large integrated circuits. Certain types of single, potentially dangerous failures can remain hidden in the system and may come to light after some time in combination with another fault. Such multiple fault could be already dangerous.

Diagnostic coverage is defined in the standard [2] as ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic tests:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{D\_total}} \quad [-] \tag{3}$$

DC diagnostic coverage

λ_{DD} rate of detected (potentially) dangerous failures

λ_{D_total} rate of the total number of (potentially) dangerous failures

It should be emphasized that the term „diagnostic test“ means here, besides automated on-line tests, comparison of output, input and intermediate values too.

Depending on the context, in addition to the definition (3), the term "diagnostic coverage" means also the proportion of safe failures to all equipment failures. A "safe failure" is considered as automatically detected and negated failure in the standard [2], which is debatable, since, according to the requirements of railway standard [1] no single random failure may be dangerous (detected and undetected).

3. Hazard rate calculation of redundant structure 2 out of 2

Futhermore, only 2oo2 system is considered, in which only[1)] double fault can be dangerous. Such a fault may arise hypothetically as a combination of two affirmative single random faults (two failures in two channels have the same effect on output). Combination of two affirmative faults, which can possibly occur, can not be detected by comparison, on which is based safety of redundant systems. Therefore, a double fault occurence must be prevented by an early detection and negation of a single fault. An occurance of double random fault is evaluated by *quantitative* measures: HR must be

lower then THR. By contrast, defense against the consequences of single random fault is evaluated by *qualitative* measures: no single random fault may cause a hazard.

Note 1):

An occurence of systematic failures or common-cause failures (CCF) is not considered in the calculation.

Definition: Hazard rate of 2oo2 structure means a rate of occurence of double random, potentially dangerous failure (ie, rate of occurence of two affirmative random failures in both channels) during one automated test (comparison cycle, etc.).

Consequences of double random fault may be as follows: release of dangerous command to set a point, swith on of permitting sign during unmet conditions, inaccurate measurement of safety critical time, an inability to detect a trailing point, a blockage of failure detection or failure negation (automated tests malfunction, SW comparison and negation malfunction), etc.

The formula (A.1) of standard [1] may be used for hazard rate calculation of 2oo2 structure:

$$HR_{2/2} \approx \frac{\lambda_A}{SDR_A} \times \frac{\lambda_B}{SDR_B} \times \left(SDR_A + SDR_B\right) \ [\mathrm{h}^{-1}] \qquad (4)$$

Explanation:

HR hazard rate of 2oo2 structure,

λ rate of single random failures of A or B channel,

SDR rate of safe state achievement (safe down rate) – reciprocal of the time to failure detection and negation;

The formula (4) is presented without any proof in the standard. Minutes of the formula shows that it is a simplification of another, more accurate formula.

For most 2oo2 interlocking systems, the same failure rates (λ) and time to failure detection and negation (Tdn) are assumed in both channels of the redundant structure, since both channels are usually identical from hardware point of view. According to the formula (4), the hazard rate (HR) of the 2oo2 system is quadratically dependent on the failure rate of each channel (λ) and linearly dependent on the time of failure detection and negation (Tdn):

$$HR_{2/2} \approx \frac{\left(\lambda \times Tdn\right)^2}{Tdn} \times 2 = 2 \times \lambda^2 \times Tdn \ [\mathrm{h}^{-1}] \qquad (5)$$

Validation of the formula A.1 of the standard EN 50 129

To calculate the hazard rate of 2oo2 redundant structure konwledge of reliability theory can be applied, namely RBD method (reliability block diagram). However, it is necessary to distinquish between reliability and safety during modeling of the structure. In the case of double channel 2oo2 structure applies, it is the structure of the serial arrangement of elements in terms of reliability, but also with the parallel arrangement of elements in terms of safety. The dangerous failure on the output of the structure occurs only if affirmative, potentially dangerous faults arise *in both* channels.

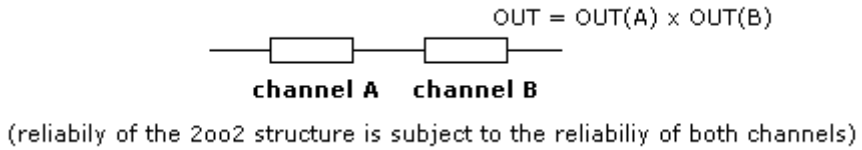

Fig. 1 *Serial reliability model of 2oo2 redundant structure*

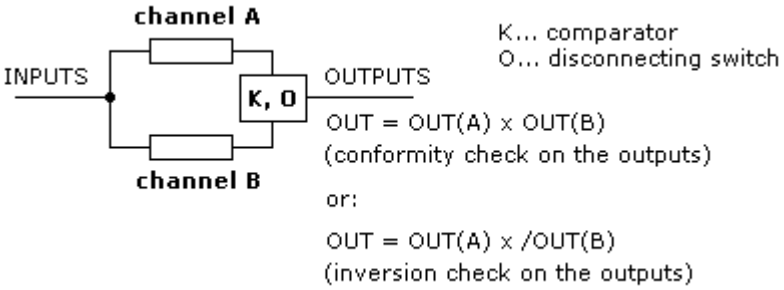

Fig. 2 *Paralel safety model of 2oo2 redundant structure*

As in equation (5), rate of dangerous and safe failures and automated tests efficiency will be disregarded. Each fault of one channel of the redundant structure is considered to be potentially dangerous and each double failure is considered to be dangerous.

Then for probability of hazard occurence is applied the following equation:

$$Q(t)_{2/2} = \left(1 - e^{-\lambda t}\right)\left(1 - e^{-\lambda t}\right) = 1 - 2e^{-\lambda t} + e^{-2\lambda t} \quad [-] \qquad (6)$$

where „λ“ is failure rate (λ) and „t“ represents time to detection and negation of the single random failure.

Then, hazard rate can be derived as:

$$HR_{2/2} = \frac{f(t)}{R(t)} = \frac{\frac{dQ(t)}{dt}}{R(t)} = \frac{2\lambda e^{-\lambda t} - 2\lambda e^{-2\lambda t}}{2e^{-\lambda t} - e^{-2\lambda t}} \quad [h^{-1}] \qquad (7)$$

Equations (5) and (7) were compared by a simple simulation method in Excel spreadsheet. A dependence of hazard rate on time to failure detection and negation was observed. Failure rate of each channel was considered as a constant: $\lambda = 1x10^{-6}$ $[h^{-1}]$. This corresponds to the mean time to failure $1x10^{6}$ hours. The simulation results are graphically illustrated in figures 3 and 4. Figure 3 shows that both HR courses ovelap.

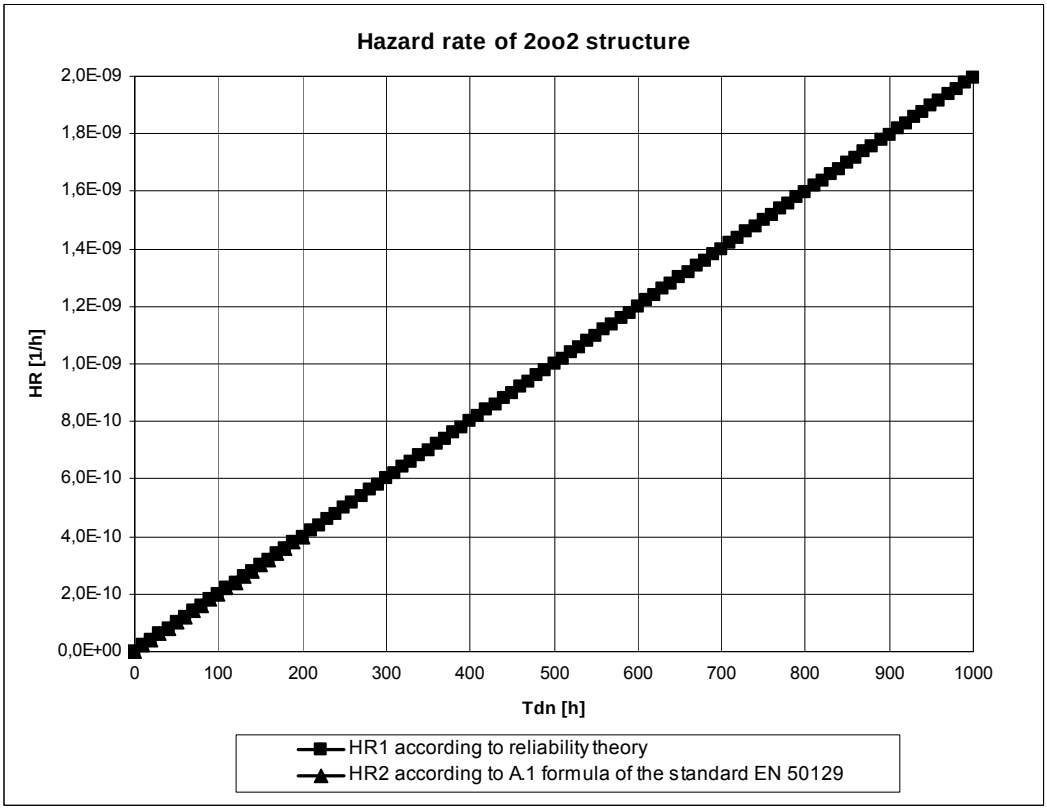

***Fig. 3** Hazard rate of 2oo2 structure with $\lambda = 1x10^{-6}$ $[h^{-1}]$ and Tdn 0 to 1000 hours*

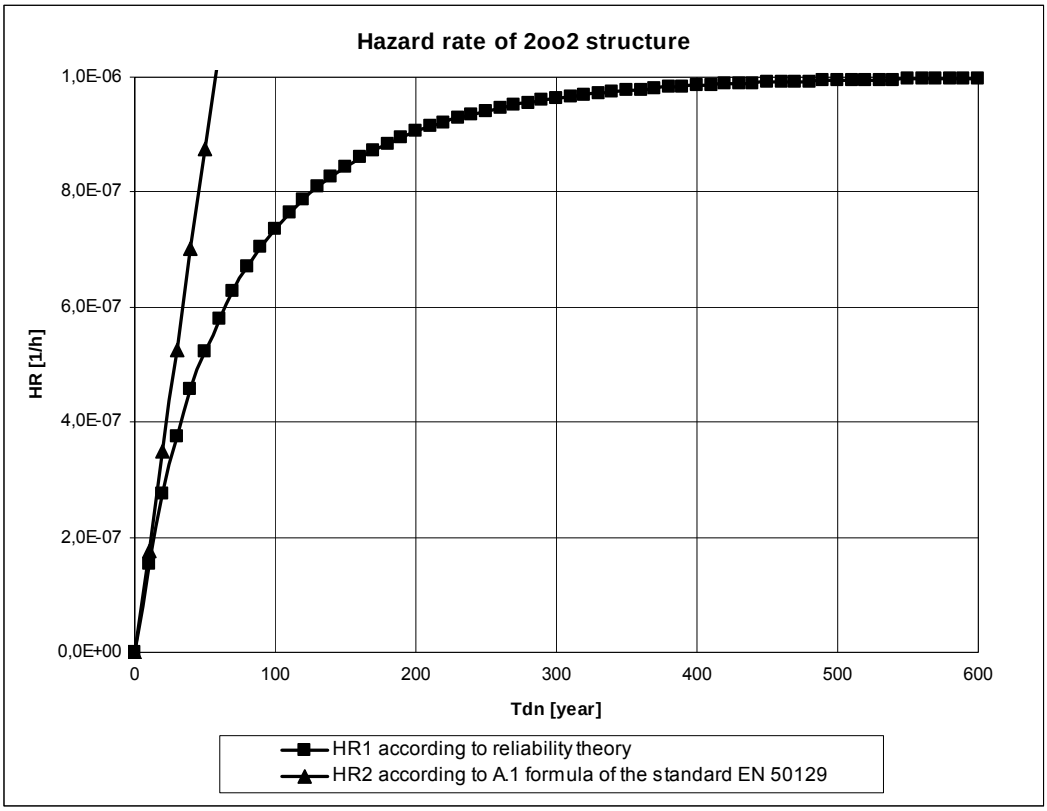

Fig. 4 *Hazard rate of 2oo2 with $\lambda = 1x10^{-6}$ [h^{-1}] and Tdn 0 to 600 years*

From the obtained results were made these partial conclusions:

- formula (5) is linear approximation of formula (7),
- real HR has got an asymptotic course with increasing Tdn, it converges to λ at infinity,
- formula (5) can be obtained from formula (7), if an expression $(1 - e^{-\lambda t})$ in formula (7) is replaced by expression λ.t (it is the first member of the development of the term in question). It is acceptable only under the assumption, that holds: $\lambda.t << 1$,
- the results begin to vary significantly for the Tdn / MTTF ratio higher than 1:100 (more than 1,5 %),
- formula (5) when compared with formula (7) is pessimistic – gives the same or worse results,
- formula (7) better reflects reality for a longer period of failure detection and negation;

Undetected random failures and hazard rate

In the context of this paper the term "undetected failure" means such a random failure, which is not detected neither automatically, nor at periodic inspections. The redundant structure 2 of 2 may contain elements, which are not reviewed or tested during the life of the system. In practical terms, an interesting finding is that the double channel structure with highly reliable components may reach a level of safety integrity SIL 4, even if all kinds of random failures are considered to be undetected. This can be used to demonstrate safety.

Example:

One channel of the 2oo2 redundant structure embodies a mean time to failure 10 million hours. All single random failures of the structure are undetected. An assumed life cycle of the equipment is 40 years. The resulting hazard rate of the 2oo2 redundant structure is $7x10^{-9}$ $[h^{-1}]$*, wich complies with the safety integrity level SIL 4.*

By calculating the hazard rate it is not necessary to include such failures (detected and undetected), which are not potentially dangerous. However, for this purpose it is necessary to know the proportion of dangerous failures to the total number of failures.

Rate of potentially dangerous failures

The traditional approach applied in the standard [1] can be restrictive in some cases - for more complex structures a required safety integrity level may not be achievable. Traditionally, this problem can be solved by using components with higher reliability, shortening time to detection and negation of failure or by changing the system architecture. Another possible solution is that for each element the ratio of safe and dangerous failures will be considered. Such a possibility is excluded in standard [1], but in the future, particularly with regard to the standard [2], revision of this conservative approach is possible.

Taking info account the rate of dangerous random failures to all random failures, the following formula may be used:

$$\lambda_D = PNP \cdot \lambda \quad [h^{-1}] \tag{8}$$

Explanation:

λ_D rate of single, potentially dangerous random failures,

PNP proportion of dangerous failures – ratio of dangerous random failures to all random failures of one channel of the redundant structure,

λ failure rate of all single random failures;

Then, this formula can be used in formulas (5) and (7), resulting in the following formulas:

$$HR_{2/2\_PNP} \approx \frac{(\lambda_D \times Tdn)^2}{Tdn} \times 2 = 2 \times \lambda_D{}^2 \times Tdn \quad [h^{-1}] \tag{9}$$

(basic calculation)

$$HR_{2/2\_PNP} = \frac{2\lambda DCe^{-\lambda_D.t} - 2\lambda e^{-2.\lambda_D.t}}{2e^{-\lambda_D.t} - e^{-2.\lambda_D.t}} \quad [h^{-1}] \tag{10}$$

(more precised calculation)

Explanation:

$HR_{2/2\_PNP}$ hazard rate of the structure 2oo2 with the assumed part of dangerous failures

Example:

The redundant structure 2oo2 is given. Rate of all random failures of each channel is assumed to be constant: λ = 1x10^{-6} [h^{-1}]. Time to detection and negation of failure is 1 hour. It is reasonable to assume that the ratio of potentially dangerous random failures to all random failures is 0,5.

After substituting these data into the formula (5) or (7) the resulting hazard rate is 2x10^{-12} [h-1]. However, when taking into account the ratio of potentially dangerous random failures to all the random failures, then the resulting hazard rate is 5x10^{-13} [h-1], which is a four times smaller value.

For different times to failure detection and negation (comparative cycle) the simulation results have got a similar process, as shown in Figures 3 and 4. Using the formula (9), hazard rate increases linearly as in formula (5), however, the resulting values are four times smaller. Hazard rate according to formulas (7) and (10) has got the asymptotic process, which in infinity converges to the λ value for the formula (7) and to the λ_D value for the formula (10).

Taking into account a diagnostic coverage

In the following calculations a diagnostic coverage is considered as a test effectiveness – a proportion of random failures detectable by the appropriate test to all random failures that may occur in the channel.

Generally, the following cases can be considered:

- one channel of the redundant structure contains elements, in which random failures are detectable (by comparison, periodic on-line tests or during the

equipment inspection), and elements, whose random failures are not detectable throughout the whole system life cycle,

- one channel of the redundant structure contains an element, at which only a part of random failures is detectable,
- combination of the two previous cases;

By "traditional" HR calculation according to formulas (5) or (7), even by taking into account the part of dangerous failures according to formulas (9) or (10), 100% comparison efficiency is expected. But it is clear that the mere comparison of the values of outputs and inputs and possibly of certain intermediate values do not reveal all random faults that may occur in the system. To this end, further periodic tests are carried out whit the aim to reveal those faults, which do not show theirselves in the comparison. For example, so called „disable test“ is implemented in two-state safe outputs, when all outputs are shortly excitated and both channels check, if their value is logic 0.

Writing and reading test is carried on in the case of RAM memory, there may be also used a safety code. A content of ROM memory is usually secured with safety code (eg CRC), which is periodically checked. There are also possible other tests – such as CPU (ALU) tests, bus tests, tests of some discrete components, tests of cetain performed functions, etc.

Generally, it is possible to take into account the effectiveness of these periodic tests when calculating the hazard rate. Then it is necessary to demonstrate adequately the test effectiveness (analytically or experimentally). The failure probability should also taken into account. For two-channel conducted test, this probability is given by the duration of the test cycle and the failure rate of one channel, see formula (6). In the case of tests, which results are compared in no way in the redundant structure, the probability of their malfunction is given by the system life cycle and failure rate of one channel.

When RBD method is applied, the formula (6) can be adapted, taking into account a proportion of dangerous failures:

$$Q(t)_{2/2\_PNP} = 1 - 2e^{-PNP.\lambda.t} + e^{-2.PNP.\lambda.t} = PS \quad [-] \qquad (11)$$

Explanation:

PNP proportion of dangerous failures (ratio of dangerous random failures to all random failures of one channel of the redundant structure 2oo2),

PS probability of test malfuction;

Comparison can also be viewed as a "test", therefore it is possible to calculate the probability of its malfunction. The probability of hardware comparison malfunction is negligible, provided that it is executed by an inherent-safety circuit. In the case of software comparison, it is not possible to make such a conclusion, because in only one comparison cycle are not tested all possible combinations of compared data.

Theoretically, in a redundant structure could arise such a double fault, in which certain combinations of erroneous data would not be detected by sofware comparison.

Analogously, it is possible to consider the probability malfunction of software negation. The probability of malfunction of hardware negation, which is implemented by a circuit with inherent safety, can be ignored.

Theoretically, it is also possible to consider the effectiveness of inspections and tests performed by maintanance staff or equipment supplier.

Apparently, despite all efforts to the maximum diagnostic coverage, certain part of undetectable faults remain in the system (undetected failures).

When calculating the hazard rate with diagnostic coverage considered, it is appropriate to take into account the temporal sequence of executed tests. This is based on several following assumptions:

- The same ratio of dangerous failures is considered for each test thoughout the system life cycle.
- The test effectiveness (the ratio of detected failures) can be taken into account only if the entire test is executed, therefore the effectiveness of certain test is taken into account in the calculation until the next test.
- Failure detected in the test is no longer reflected in the following test, because this test will not be executed - the system goes into a safe shutdown (so-called safe fallback state). Therefore, the effectiveness of all previous tests is considered in the following tests on the condition that the sets of random faults detected in each test are different (effectiveness of test "x" refers to a different set of faults than the effectiveness of test "y", no intersection of these sets exists). This condition holds rather theoretically and serves just to demonstrate a phased process of failures occurance and failures detection.

Note:

The independence of sets of failures detected by different tests is difficult to prove in real systems, but in the context of this paper is considered. The aim is to demonstrate a mechanism of origin and detection of double random undetected failure.

The result of all above presented considerations is a formula that probably best represents the real hazard rate, but which is ultimately quite complicated and difficult to use in practise:

$$HR_{2/2} = HR_{2/2\_T1} + HR_{2/2\_T2} + ... + HR_{2/2\_TN-1} + HR_{2/2\_TN} \quad [h^{-1}] \qquad (12)$$

Explanation:

$HR_{2/2}$ the resulting hazard rate taking into account the diagnostic coverage and the rate of potentially dangerous failures,

$HR_{2/2\_T1}$ hazard rate at the end of the first test cycle, taking into account the ratio of potentially dangerous single failures,

$HR_{2/2\_T2}$ hazard rate at the end of the second test cycle, taking into account the ratio of potentially dangerous single failures, the effectiveness of the first test (eg comparison) and probability of its malfunction,

$HR_{2/2\_TN-1}$ hazard rate at the end of the last test cycle, taking into account the ratio of potentially dangerous single failures, the effectiveness of all previous tests and probability of their malfunction,

$HR_{2/2\_TN}$ rate of dangerous, undetected double faults at the end of system life cycle, taking into account the ratio of potentially dangerous single failures, the effectiveness of all executed tests and probability of their malfunction;

First term:

$$HR_{2/2\_T1} = \frac{2.PNP.\lambda.e^{-PNP.\lambda.t} - 2.PNP.\lambda.e^{-2.PNP.\lambda.t}}{2e^{-PNP.\lambda..t} - e^{-2.PNP.\lambda.t}} \quad [h^{-1}] \qquad (13)$$

Explanation:

PNP ratio of single, potentially dangerous random failures to all random failures of one channel of the redundant structure 2oo2),

λ failure rate of one channel of the redundant structure 2oo2,

t duration of the test cycle;

Second term:

$$HR_{2/2\_T2} = \frac{2.PNP.(1-(1-PS1).UT1).\lambda.e^{-PNP.(1-(1-PS1).UT1).\lambda.t} - 2\lambda e^{-2.PNP.(1-(1-PS1).UT1).\lambda.t}}{2e^{-PNP.(1-(1-PS1).UT1).\lambda.t} - e^{-2.PNP.(1-(1-PS1).UT1).\lambda.t}} \quad [h^{-1}] \qquad (14)$$

Explanation:

1-PS1 probability that the first test will not fail

UT1 effectiveness of the first test (its diagnostic coverage)

Other terms of the formula (12) can be expressed analogically.

The second term expresses the fact that in the first test detected only a certain portion (subset) of potentially dangerous single random failures. Effectiveness of the first test is taken into account with the probability, that the first test was processed successfully (1-PS1). In the case of the test, which is processed and compared in thow-channels, the probability of its malfunction may be neglected, if the test cycle is short enough. For the

tests processed in one channel it is necessary to take into account the probability of malfunction, which is given by system reliability and system life cycle:

$$PS_{1K} = 1 - e^{-PNP.\lambda.t} \quad [h^{-1}] \tag{15}$$

Where PS_{1K} is the probability of malfunction of the one-channel processed test.

Example:

One channel of the redundant structure 2oo2 has got a mean time to failure 1 million hours. 40 years system life cycle is assumed. Ratio of potentially dangerous single random failures to the total number of channel faults is uknown (PNP = 1). Some periodic tests of the structure are processed and evaluated only in one channel – without any comparison of test result with the second channel. Then the probability of malfunction of these tests is: $PS_{1K} \cong 0{,}3$ *[-].*

If 10 million hours MTTF is taken into account in the same example, then the probability of malfunction of the one-channel processed test is almost negligible: 0,034 [-].

n-th term of the formula (12):

$$HR_{2/2\_TN} = \frac{2.PNP.\left(1 - \sum_{i=1}^{n-1} UT_i.PNS_i\right).\lambda.e^{-PNP.\left(1-\sum_{i=1}^{n-1} UT_i.PNS_i\right).\lambda.t} - 2\lambda e^{-2.PNP.\left(1-\sum_{i=1}^{n-1} UT_i.PNS_i\right).\lambda.t}}{2e^{-PNP.\left(1-\sum_{i=1}^{n-1} UT_i.PNS_i\right).\lambda.t} - e^{-2.PNP.\left(1-\sum_{i=1}^{n-1} UT_i.PNS_i\right).\lambda.t}} \quad [h^{-1}] \tag{16}$$

Explanation:

PNS_i probability that the test „i“ will not fail ($PNS_i = 1\text{-}PS_i$)

UT_i effectiveness of the test „i“ (its diagnostic coverage)

4. Conclusion

The formula in the standard EN 50 129 for hazard rate calculation of the redundant structure is healthy pessimistic in some way - each single random failure is considered to be potentially dangerous. In other respects, however, this formula is too optimistic - each single random failure is considered to be detectable through comparison and other tests performed. Neither the possibility of comparison malfunction (failure detection malfunction), nor the possibility of isolationg switch malfunction (failure negation malfunction) are considered as well. However, based on practical experience with redundant interlocking systems it can be assumed that the pessimistic assumption prevails over the optimistic - most of the failures of microprocessor circuits are detectable and occur in a safe way. Formula (5) marked in the standard [1] as A.1 is probably

correct and applicable to all cases where the time to detection and negation of a single failure (Tdn) compared with the mean time to failure of one channel (MTTF) is negligible, ie at least two orders of magnitude shorter. Otherwise, the formula (7) obtained using RBD method can be applied.

Both formulas (5) and (7) indicate the rate of the double fault at the end of the comparative cycle, but they do not take into account the fact that some random failures remain undetected.

A more accurate model can be created taking into account the proportion of potentially dangerous failures and the efficiency of the tests, see formula (8) to (16). However, this is necessary to have reliable information on the proportion of safe and dangerous failures of one channel of the redundant structure, eventually for each self-test (including comparison) is neccessary to declare the appropriate test efficiency and probability of the test malfunction (if it can not be ignored). Standard [2] gives in this respect some guidance, but without any guarantee of credibility. For example, there is nowhere indicated that no single random failure of the system (detected and undetected) may be dangerous and that considered diagnostic tests should be fail safe (an eventual test failure should be detected by comparison with the values of the second channel of the redundant structure). As a result, completely meaningless results can be obtained. For the above reasons this standard should be used very cautiously and prudently. It is fully the responsibility of safety assessor, if accepts the calculation of the hazard rate with consideration of the proportion of potentially dangerous failures, or not.

Conclusions drawn from the conducted analysis and calculations can be summarized as follows:

- Simple redundant system 2 out of 2, which is highly reliable, can meet the safety integrity level SIL 4 even in case that all random failures considered undetected. This could possibly be used as an argument in the approval process in addressing the undetected failures.
- Malfunction of diagnostic tests carried out in a redundant structure should be detected by data comparison. By the way, this point relates to so called „on-line tests“ recommended in the standard [1].
- The effectiveness of several diagnostic tests may be taken into account in hazard rate calculation assuming that the efficiency of each test relates to another set of random failures.
- The effectiveness of a diagnostic test can be taken into account in hazard rate calculation only after execution of the test.
- The correctness of the declared values of the ratio of dangerous random failures and values of diagnostic coverage must be proved. Otherwise, the basic formula (5) according to standard [1] shall be used or the more accurate formula (7) obtained by using RBD method.

Submitted: 03. 05. 2010

Literature:

[1] EN 50129. *Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling.* [s.l.] : [s.n.], 2003. 98 p. ISBN 0 580 41814 6.

[2] EN 61508-1-6. *Functional safety of electrical / electronic / programmable electronic safety-related systems.*

[3] RÁSTOČNÝ, K. - KUNHART, M. - ZAHRADNÍK, J. *Bezpečnost železničných zabezpečovacích systémov*. 1. vyd. Žilina: EDIS, 2004. 276 s. ISBN 80-8070-296-9.

Summary

HAZARD RATE CALCULATION OF RAILWAY INTERLOCKING SYSTEM 2 OUT OF 2

Jiří Konečný

In the introduction of this article the purpose and operation principle of railway interlocking systems is briefly explained. Further there are presented results of an analysis, which aim was to prove validity of a formula recommended by EN 50129 standard for a hazard rate calculation of the interlocking systems with a redundant structure 2oo2. Hazard rate was calculated by two independent ways, namely for different failure rates of single channels and for a different safe-down time. In the first case the formula presented in EN 50129 was used, in the latter case a calculation was carried out by RBD method. Results of both methods were matched. In most cases both results coincide. Greater diversions arise only in such cases, when a safe-down time of a single fault is comparable in order of magnitude with a mean time to failure of a single channel of the redundant structure. This can occur for instance during long term system storage, or if an undetected failure occurs during a system operation.

Possibility of an undetected failure is not quantitatively captured in EN 50129 standard (each single random failure is considered to be detected at the end of the test), therefore the last aim of the work was to analyse in detail a mechanism of origin, detection and negation of double random faults. The results of this analysis can be used for a quantitative evaluation of the impact of undetected random failures on a hazard rate of a redundant structure 2 out of 2.

The main risk for the technical safety of redundant systems, besides common cause failures, are undetected failures. One point of this paper is a recommendation that the data comparison and the fault negation should be carried out in such a way that would minimize or completely eliminate the possibility of undetected malfunction of these key safety functions.