https://doi.org/10.53656/isct-2025.24

RELIABILITY ASSESSMENT OF RAILWAY SIGNALING SYSTEMS USING FAULT TREE ANALYSIS

Vasil Ivanov, Emiliya Dimitrova
Todor Kableshkov University of Transport, Sofia, Bulgaria

Abstract. The report presents the application of the fault tree analysis method in evaluating the reliability of equipment included in railway signaling systems. To calculate the reliability indicators, the algebra of random events is applied, where failures of individual components are treated as such events. The study aims to identify the relationships between failures of individual components and the overall (final) system failure through logical modeling of their interdependencies. Fault tree analysis provides a symbolic representation of the conditions that may lead to a system failure, using logical operators to define the relationships between individual component failures and the final failure. This approach helps identify weak points, assess redundancy, and verify compliance with the specified safety and reliability requirements. As an example of logical modeling using fault tree analysis, an automatic level crossing system (ALCS) was examined. The analysis aims to present the relationship between failures in the barrier mechanism, the control circuitry, and the track sensors, and how they may lead to a common system-level failure – in this case, the crossing remaining open when a train is approaching. Based on the constructed fault tree and predefined failure rate values, the main reliability indicators related to the final system failure were calculated: probability of failure-free operation, probability of failure, failure rate, downtime factor, availability factor. The methodology enables assessment of the current state of these indicators and supports planning, technical maintenance, and informed decision-making for the optimization of railway infrastructure systems. The method is applicable both to existing systems and at the design stage.

Keywords: fault tree analysis; reliability; railway transport; failure rate; downtime factor; availability factor

1. Introduction

The interconnection of technical components (e.g., railway transport facilities) in terms of reliability can be realized in three ways: series, parallel, or mixed. In

series connection, the failure of a single component leads to the failure of the entire system. In parallel connection, all components must fail for the system to fail. Mixed connection is obtained by combining serial and parallel connection. Reliability calculation can be carried out by formulating a mathematical model of the system or by means of a functional diagram. The second method is applicable only when the elements in the system are connected in series. After compiling a model of the technical system, the stage of performing analysis follows. During the analysis, mathematical expressions must be defined, allowing for the direct substitution of experimental data in order to calculate the system's reliability indicators [1].

The purpose of constructing fault trees is to trace which specific failures (of components or subsystems) can lead to failure of the entire system. The construction of these trees is achieved by logically connecting the individual events – the failures of the basic elements – using the operators "AND" and "OR".

It is characteristic of the logical "OR" operator that it is used to represent series-connected elements. When the failure rate of the initial elements is constant, the resulting failure rate represents their sum. When using the probabilities of failure-free operation $P(t)$, the resulting probability is the product of the probabilities of the initial elements.

The logical operator "AND" is used to represent parallel connected elements. When the failure rate of the initial elements is constant, the output failure rate is a function of time. When using the probabilities of failure, the resulting probability is the product of the probabilities of the initial elements. Therefore, when calculating the logical "AND" operator, unlike the logical "OR" operator, the probability of failure $Q(t)$ is used instead of the probability of failure-free operation.

When combining the above-mentioned operators, a third logical operator is obtained – the quorum function. It is characteristic that a precisely defined number of basic elements M, out of all N elements, must fail in order for the entire system to fail. When $M = 1$, the quorum function is equivalent to the "OR" operator, and when $M = N$, the operator corresponds to "AND" [2].

When calculating the downtime factor, the following formulas are used:

– For the logical "OR" operator:

$$(1)\ K_D = 1 - \prod_{i=1}^{n} \frac{\mu_i}{\lambda_i + \mu_i}$$

– For the logical "AND" operator:

$$(2)\ K_D = \prod_{i=1}^{n} \left(1 - \frac{\mu_i}{\lambda_i + \mu_i}\right),$$

where K_D is the downtime factor, n is the number of elements, included in the input of the logical operator, λ_i is the failure rate of the i-th basic element, μ_i is the repair rate of the i-th basic element.

When calculating the availability factor, the following formula is used:

(3) $K_A = 1 - K_D$

When *calculating* failure rates, the following formulas are used for the logical operators:

– For the logical "OR" operator:

(4) $\lambda_p(t) = \lambda_1(t) + \lambda_2(t) + \ldots + \lambda_n(t)$, if $\lambda_1(t) = \lambda_2(t) = \ldots = \lambda_n(t) =$ const, then

(5) $\lambda_p(t) = \lambda_p = n.\lambda$,

where λ_p denotes the failure rate of the system under consideration as a whole (the top-level failure), expressed as a function of the failure rates of the individual components in the fault tree structure. The index *p* comes from the English word "primary" [3].

– For the logical "AND" operator:

(6) $\lambda_p(t) = \{\sum_{i=1}^{n} \lambda_i(Z_i - 1)\}\{\prod_{j=1}^{n} Z_j - 1\}^{-1}$, where:

(7) $Z_j = \frac{1}{1-e^{-\lambda_j t}}$

In reliability theory, it is accepted that for every technical element or system, the probability of failure-free operation $P(t)$ and the probability of failure $Q(t)$ always sum to 1. This is because the two events are considered complementary, mutually exclusive, and collectively exhaustive of all possibilities [4]:

(8) $P(t) + Q(t) = 1$

2. Calculation of Reliability Indicators using the Fault Tree

2.1. Description of the Fault Tree Diagram

An automatic level crossing system (ALCS) is considered, with the top event being the failure of the crossing to close when a train approaches (Fig. 1). Three events are presented, and a fault tree has been constructed. Normally, when the level crossing is open, the road signal relay (RSR) is activated. The condition for closing the level crossing is the occupation of any of the pre-crossing sections, as a result of which the RSR releases and activates the light and sound signals. The barrier mechanism is controlled by a closing relay (CR) – it is normally activated and the barriers are raised. When the conditions for closing the level crossing are met, it releases and triggers the lowering of the barrier gates. When the conditions

for opening the level crossing are met, the CR is activated again, and the barriers are raised. The RSR is also reactivated when all conditions for opening the level crossing are met, i.e., when the train has cleared the crossing and the barriers are raised. To register the actual passage of the train through the crossing and to activate the RSR and CR, a normalizing relay (NR) is also included in the circuit. Two auxiliary direction relays (even and odd) are also used to determine the direction of the train's movement [5].

The train's entry into a given pre-crossing section is detected by a track sensor. The presence of a train can be detected using track circuits or point sensors. In the first case, two track circuits cover the two pre-crossing sections, with one acting as the entry circuit for the train movement and the other as the exit circuit. To register the train's entry, the track relay of the entry circuit is released, which closes the level crossing. To open it, a third track circuit is required, which controls the level crossing itself. Failure to activate any of the track circuits leads to untimely opening of the crossing when accidental occupation and release of sections of the track occur [6, 7].

In the second case (the level crossing has point sensors), four sensors are required. Two of them correspond to the train entering a given pre-crossing section, while the other two monitor the actual passing of the train.

If any of the sensors fail to activate, it leads to untimely opening of the level crossing.

In the constructed fault tree, the first event is assumed to be the failure of the track sensor to activate.

The second event is a dangerous failure in the control circuitry – manifested as a violation of the condition for closing the level crossing when the pre-crossing section is occupied. The RSR remains activated [8, 9].

A logical "AND" operator is used for the two events, as both failures must occur in order for a train to enter without the level crossing being closed.

The third event leading to the final failure is included through the logical "OR" operator – failure in the barrier mechanism. The cause of the failure may be a malfunction in the CR, which fails to send the closing command, or a failure in the barrier's drive mechanism [10, 11].

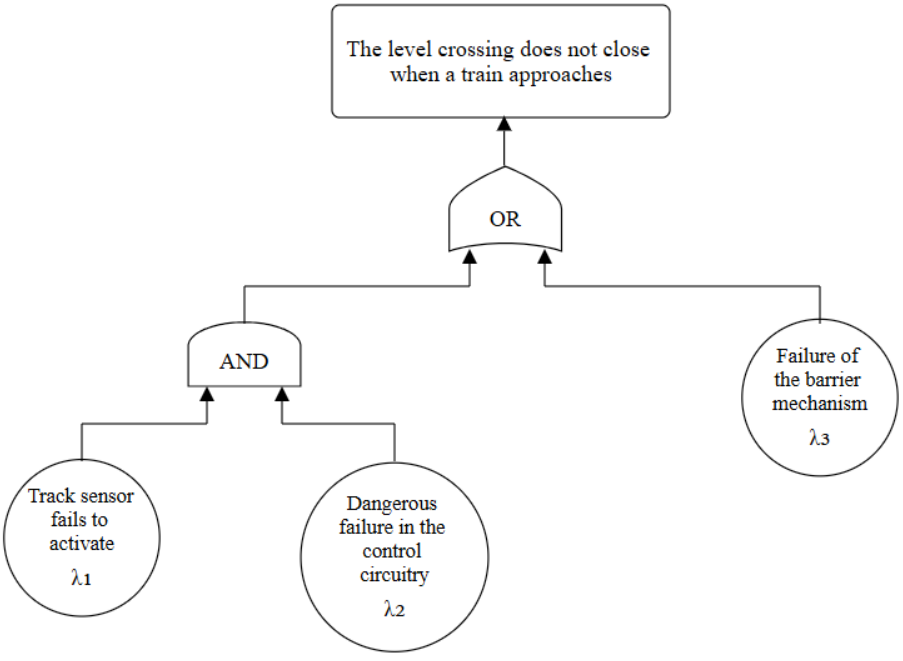

Figure 1. Fault tree representing the conditions leading to a specific failure in the ALCS

2.2. Algorithm for calculating reliability indicators

The basic elements are described by an exponential distribution, using the formula:

(9) $P(t) = e^{-\lambda t} e^{-\lambda t}$

The following indicators need to be determined:

i. The probability of failure-free operation of the technical object for 1300 h – $P(1300) = ?$, using formula (9) (The probability of failure-free operation of the top event from the fault tree shown in Fig. 1 is to be determined). The initially given values for the basic elements are as follows:

$$\lambda_1 = 13.10^{-5}\ \frac{1}{h},\ \lambda_2 = 17.10^{-5}\ \frac{1}{h},\ \lambda_3 = 21.10^{-5}\ \frac{1}{h};$$

ii. The failure rate for an operating time of $t = 1000$ h, if the initially given values for the basic elements are as follows:

$\lambda_1 = 11.10^{-5}\ \frac{1}{h}$, $\lambda_2 = 15.10^{-5}\ \frac{1}{h}$, $\lambda_3 = 27.10^{-5}\ \frac{1}{h}$ using the formulas (4), (5), (6) and (7);

iii. The downtime and availability factors of the top event, assuming the repair rate is μ = 0,05 $\frac{1}{h}$ and the initially given values for the basic elements are:

$\lambda_1 = 47.10^{-4}\ \frac{1}{h}$, $\lambda_2 = 53.10^{-4}\ \frac{1}{h}$, $\lambda_3 = 47.10^{-5}\ \frac{1}{h}$ using the formulas (1), (2) and (3);

2.3. Calculation Results

Performed calculations for the three groups of indicators:

i. The calculation is performed in parts, as there are two blocks. In the first block, the logical operator is "AND" – "The resulting probability of failure *Q*(*t*) is equal to the product of the failure probabilities of the basic elements". For this reason, the probabilities of failure and failure-free operation of the basic events are first determined:

– Probability of failure-free operation of the first basic event $P_1(t)$:

$$P_1(t) = e^{-\lambda_1 t} = e^{-13.10^{-5}.1300} = e^{(-0,169)} \approx\approx 0,84$$

– Probability of failure of the first basic event $Q_1(t)$:

$$(10)\ Q_1(t) = 1 - P_1(t) \approx\approx 1 - 0,84 \approx\approx 0,16$$

(The formula is a direct application of the algebra of events, as the events "failure" and "failure-free operation" are considered complementary events) [12].

– Probability of failure-free operation of the second basic event $P_2(t)$:

$$P_2(t) = e^{-\lambda_2 t} = e^{-17.10^{-5}.1300} = e^{(-0,221)} e^{(-0,221)} \approx 0,80$$

– Probability of failure of the second basic event $Q_2(t)$:

$$Q_2(t) = 1 - P_2(t) \approx 1 - 0,80 \approx 0,20$$

After calculating the probabilities of failure and failure-free operation of the basic elements, the probabilities for the two branches of the tree and the top event are also determined.

First block (branch):

Since the logical operator is "AND", the resulting probability of failure is the product of the failure probabilities of the initial elements.

(11) $Q_{block\,1} = Q_1(t) \,.\, Q_2(t) \approx 0{,}16 \,.\, 0{,}2 \approx 0{,}032$

$P_{block\,1} = 1 - Q_{block\,1} \approx 1 - 0{,}032 \approx 0{,}968$

Second block (branch):

It contains only one event, so the probability of failure-free operation is calculated directly:

$P_{block\,2} = e^{-\lambda_3 t} = e^{-21.10^{-5}.1300} = e^{(-0{,}273)} \approx 0{,}76$

Finally, the probability of failure-free operation of the top event is determined:

With the logical "OR" operator, the values of the failure-free operation probabilities of the two blocks are multiplied [13]:

(12) $P_{\text{Top event}} = P_{block\,1} \,.\, P_{block\,2} \approx 0{,}968 \,.\, 0{,}76 \approx 0{,}736$

ii. The failure rate is to be determined for an operating time of t = 1000 h

For Block 1, with a logical "AND" operator, formulas (6) and (7) are used:

From formula (6) it follows: $\lambda_{block\,1}(t) = \lambda_{block\,1}(1000) = \frac{\lambda_1(z_1-1)+\lambda_2(z_2-1)}{z_1.z_2-1}$

The two basic events have the following values: $\lambda_1 = 11.10^{-5}\ \frac{1}{h}$

and $\lambda_2 = 15.10^{-5}\ \frac{1}{h}$

From formula (7) it follows: $z_1 = \frac{1}{1-e^{-\lambda_1 t}} = \frac{1}{1-e^{-11.10^{-5}.1000}}$

$= \frac{1}{1-e^{-0{,}11}} = \frac{1}{1-0{,}896} \approx 9{,}62$

$z_2 = \frac{1}{1-e^{-\lambda_2 t}} = \frac{1}{1-e^{-15.10^{-5}.1000}} = \frac{1}{1-e^{-0{,}15}} = \frac{1}{1-0{,}86} \approx 7{,}14$

$z_1 . z_2 = 9{,}62 \,.\, 7{,}14 = 68{,}68$

$\lambda_1 . (z_1 - 1) = 11.10^{-5}. 8{,}62 \approx 9{,}48.10^{-4}$

$\lambda_2 . (z_2 - 1) = 15.10^{-5}. 6{,}14 \approx 9{,}21.10^{-4}$

$\lambda_1 . (z_1 - 1) + \lambda_2 . (z_2 - 1) = 9{,}48.10^{-4} + 9{,}21.10^{-4} = 18{,}69.10^{-4}$

The final result is:

$$\lambda_{block\,1}(t) = \lambda_{block\,1}(1000) = \frac{\lambda_1(z_1-1)+\lambda_2(z_2-1)}{z_1.z_2-1} = \frac{18,69.10^{-4}}{68,68-1} = 2,76\,.\,10^{-5}\ \frac{1}{h}$$

The failure rate of Block 2 is given by the problem statement, as it contains only one basic element:

$$\lambda_{block\,2}(t) = \lambda_3 = 27.10^{-5}\ \frac{1}{h}$$

The failure rate of the top event is formed as the sum of the failure rates of the two input blocks, since there is a logical "OR" operator. As indicated in formula (4), the individual failure rates will be added:

$$\lambda_{\text{Top event}}(t) = \lambda_{block\,1}(t) + \lambda_{block\,2}(t) = 2,76.\,10^{-5} + 27.\,10^{-5} =$$

$$29,76.\,10^{-5}$$

iii. The two blocks are considered again, and formulas (1), (2), and (3) are used: For Block 1, the operator is logical "AND":

$$K_D^{block\,1} = \left(1 - \frac{\mu}{\mu+\lambda_1}\right).\left(1 - \frac{\mu}{\mu+\lambda_2}\right) =$$

$$\left(1 - \frac{0,05}{0,05+0,0047}\right).\left(1 - \frac{0,05}{0,05+0,0053}\right) \approx 0,00823$$

In Block 2, there is only one basic event, and its downtime factor is:

$$K_D^{block\,2} = \frac{\lambda_3}{\mu+\lambda_3} = \frac{0,00047}{0,05+0,00047} \approx 0,009312$$

The downtime factor of the top event is:

(13) $K_D^{\text{Top event}} = 1 - \left(1 - K_D^{block\,1}\right).\left(1 - K_D^{block\,2}\right)$=1–(1–0,00823) . (1–0,009312)=0,01746

The availability factor of the top event, according to formula (3), is:

$$K_A^{\text{Top event}} = 1 - K_D^{\text{Top event}} = 0,9826$$

Analysis of the Results

The calculated probabilities of failure-free operation $P(t)$ and of failure $Q(t)$ for the basic events in the fault tree reveal a distinction between elements with varying levels of reliability within the system. The probability of failure-free operation for the first basic event is approximately 0,84, for the second it is 0,80, and for the third it is lower – 0,76. This draws attention to the third component, which in this case is the barrier mechanism.

The probability of failure for the first block, obtained through the logical "AND" operator, is relatively low – 0,032, which results in high reliability of this branch, $P(t) \approx 0{,}968$. The final probability of failure-free operation of the ALCS (the top event), obtained through the logical "OR" operator, is approximately 0,736. This means that, given the specified parameters, there is approximately a 74% probability that the ALCS will operate without failure up to the defined moment. Accordingly, there is about a 26% risk of failure.

The obtained values confirm the effectiveness of the fault tree method for identifying weak links and highlight the need for targeted improvements in elements with high failure rates.

For Block 1 (logical "AND" operator), the value of the downtime factor is approximately 0,00823, and for Block 2 it is approximately 0,009312.

For the final event, a downtime factor of approximately 0,01746 was obtained, and the corresponding availability factor is approximately 0,9826. This means that, at the given moment, the system is capable of performing its function about 98% of the time.

Conclusion

The fault tree method is distinguished by its high clarity, the ability to clearly present the logical dependencies between system components, and the comparative ease of calculations. Compared to Markov models, which require a complex transition matrix and often assume equal probability of states, fault trees allow for flexible description of different scenarios through the use of logical operators. The method is particularly suitable for the design phase, as well as for the analysis of existing systems with partial or aggregated data [13].

REFERENCES

[1] GINDEV, E., Introduction to the Theory and Practice of Reliability. Part 1. Fundamentals of Applied Reliability. Sofia: Prof. Marin Drinov Publishing House, 2000, pp. 74 – 245, ISBN: 954-430-608-0 (4.1).

[2] THEEG, G., VLASENKO, S., et al. Railway Signalling and Interlocking. 3rd edition. Hamburg: PMC Media House GmbH, 2020. ISBN 978-3962451779.

[3] PACHL, J., Railway Signalling Principles. Braunschweig: Technische Universität Braunschweig, 2020.

[4] MORGAN, C., A System of Automatic Train Control. Norderstedt: Creative Media Partners, LLC, 2022. ISBN 978-1016245411.

[5] IVANOV, E., DIMITROVA, E., Automatic Control of Traffic. First edition., Sofia: Todor Kableshkov University of Transport, 2012, pp. 156-166, ISBN: 978-954-12-0223-4.
[6] HUANG, C., EL HAMI, A.; RADI, B., Overview of Structural Reliability Analysis Methods – Part I: Local Reliability Methods, ISTE OpenScience, ISTE Ltd. London, UK, 2016.
[7] ROSS, SH., Introduction to Probability Models, In Introduction to Probability Models, 13th Ed., Elsevier Inc. 2024, ISBN: 9780443187612.
[8] BASTIDAS-ARTEAGA, E.; SOUBRA, A.-H., Reliability Analysis Methods. In Stochastic Analysis and Invers Modelling, Grenoble, 2014, pp. 53 – 77. ISBN 978-2-9542517-5-2.
[9] TERJE, A., Introduction to reliability analysis, In Risk Analysis, John Wiley & Sons Ltd., 2015, ISBN 978-1-119-05779-6.
[10] KUMAR, V., SINGH, L., TRIPATHI, A. K., Reliability analysis of safety-critical and control systems: a state-of-the-art review, IET Software, 2018, vol. 12, no. 1, pp. 1 – 18. ISSN 1751-8806. DOI: 10.1049/iet-sen.2017.0053.
[11] EFANOV, D., OSADCHY, G., KHÓROSHEV, V., New Stage in Safety Traffic Control Technologies Development: Digital Railroad Crossing, 2019 International Russian Automation Conference (RusAutoCon), Sochi, Russian Federation, IEEE, 2019, pp. 1 – 6. ISBN 978-1-7281-2731-1. DOI: 10.1109/rusautocon.2019.8867700.
[12] YUN, J., TANG, W., Automatic Threshold Adjustment for Predictive Level Crossing Sampling Data Converters, IEEE 67th International Midwest Symposium on Circuits and Systems (MWSCAS), Springfield, MA, USA, pp. 1033-1035, ISBN 979-8-3503-8718-6, doi: 10.1109/MWSCAS60917.2024.10658886, 2024.
[13] EFANOV, D., KHÓROSHEV, V., OSADCHY, G., Principles of Safety Signalling and Traffic Control Systems Synthesis on Railways, 2023 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Sochi, Russian Federation, pp. 634 – 638, ISBN 978-1-6654-7595-2, DOI: 10.1109/icieam57311.2023.10139292t.

✉ **Dr. Vasil Ivanov, Assist. Prof.**
Department of Telecommunications and Signalling
Todor Kableshkov University of Transport
158, Geo Milev St., 1574 Sofia, Bulgaria
E-mail: vivanov@vtu.bg

✉ **Prof. Dr. Emiliya Dimitrova**
ORCID iD: 0000-0001-6813-0563
Department of Telecommunications and Signalling
Todor Kableshkov University of Transport
158, Geo Milev St., 1574 Sofia, Bulgaria
E-mail: edimitrova@vtu.bg