The fault tree stochastic analysis

A Chovanec, A Breznická and P Mikuš
Faculty of Special Technology, Department of Mechanical Engineering, Alexander Dubček University of Trenčín, Pri parku 19, 911 06 Trenčín, Slovakia
E-mail: pavol.mikus@tnuni.sk

Abstract. This article presents a solution of the fault tree quantitative analysis with application of knowledge of probability distribution type into the failure and distribution parameters in case of non-renewed objects or objects being restored. It brings a look at fault tree solving based on statistical view using mathematical modeling. In this article present relations of FTA analysis for quantitative deterministic approach that is most commonly used.

1. Introduction
Fault tree analysis (FTA) is an analytic methodology commonly used to assess risk and reliability. The fault tree is a logical illustration of the events and their relationships that provide the necessary and sufficient means for the undesired event to occur. It computes the probability that the undesired event will occur and provides insight on the importance of the basic events modeled within the tree. Fault trees facilitate investigative methods to increase system reliability, reduce opportunities for system failure, and identify the most important contributors to system effectiveness, ultimately in an attempt to minimize risk. Fault Tree Analysis (FTA) is a method used to model reliability, alertness and risk in qualitative and quantitative way since 1962. The results and first thoughts are documented in the Fault Tree Handbook with Aerospace Applications. After 1979, probabilistic risk assessment approach was used to assess the safety of critical objects. FTA quantitative deterministic approaches well-known, widely used standards. So far, they serve as methodical basis for a wide range of mathematical, stochastic, simulation, and dynamic approaches. Thus, we can understand the present methodology as one of the most important logical and probabilistic techniques for assessing system reliability and risk probability. Failure Tree Analysis is one of the classical methods for identifying risks, among deductive methods. It is used to identify combinations of causes that can lead to failures and mismatches. There are many variations of this method, for all of them, there are common symbols to describe the causes of the failure. The method can be used for both qualitative and quantitative analysis. It makes it easy to find system weaknesses and reveals important aspects of reliability. It is proven, well-developed method useful in designing and operating machinery and processes. Knowing how to choose the top event and responsibly build fault tree is very important when using this method [1].

STN EN 61025 "Failure Tree Analysis" standard has been issued for tree compilation and sets the criterions for writing trees. FTA method identifies and analyzes all possible causes that cause or contribute to the consequences of an event. It proceeds from the top event (consequence of an accident event) to underlying causes. To do this, a tree diagram that breaks down the causes into individual levels is used. Specific feature of this method is that it also specifies the conditions under which these causes occur. The level of risk is determined by calculating the probability of a failure occurring [2]. Stochastic analysis using mathematical modeling is performed using the probability distributions of
failures of individual fault tree components. It is implemented on the principle of a program cycle with uniform time step shift [3].

2. Deterministic approach

Fault tree models consist of a top event and lower hierarchical system components linked by logic gates to the lowest level. Vice-versa, quantitative solution has a logical approach for accepting input data of lower-level components and considering gate-gate-gates logical rules to determine higher-level failure probability [4]. In this way the overall probability of system failure is reached. For engineering systems, fault trees most often contain two basic types of gates, OR and AND, the other types are special cases of these two basic ones, derived by adding certain logical rules and conditions. Fault tree quantitative calculation method corresponds to theoretical knowledge of equivalent series/parallel systems behavior, using the basic relations of reliability block diagram /RBD/ calculations, considering relations of failure rate solution [5].

"OR" gate is used in case of event branching if the output event occurs when any input event occurs (logical sum).

**Table 1.** OR gate expressed in FTA and its equivalent in RBD.

| Name of Gate Symbol | Classic FTA | Description RBD Equivalent |
|---------------------|-------------|-----------------------------|
| OR                  | ![OR Diagram](image) | The output event occurs if at least one of the input events occurs. Series Configuration. |

Resulting probability of occurrence of an event at the "OR" gate output in case of independence of incoming events can be expressed by equation:

\[
P_{OR} = 1 - ((1 - P_A) \times (1 - P_B) \times (1 - P_C) \times \ldots \times (1 - P_M)),
\]

where: \(P_{OR}\) is the probability of occurrence of an event at "OR" gate output, \(P_A \ldots P_M\) are the probabilities of occurrence of events entering "OR" gate. This corresponds to the characteristics of series system reliability rating.

"AND" gate is used for event branching if the output event occurs only when all the input events (collation) occur simultaneously. It is an analogy of the behavior of the parallel system.

**Table 2.** AND gate expressed in FTA and RBD.

| Name of Gate Symbol | Classic FTA | Description RBD Equivalent |
|---------------------|-------------|-----------------------------|
| AND                 | ![AND Diagram](image) | The output event occurs if all input events occur. Simple Parallel Configuration. |
Resulting probability of occurrence of an event at the "AND" gate output in case of independence of incoming events can be expressed by equation:

$$P_{\text{AND}} = P_A \times P_B \times P_C \times \ldots \times P_N,$$

where: $P_{\text{AND}}$ is the probability of occurrence of an event at "AND" gate output, $P_A, P_B, P_C, \ldots, P_N$ are the probabilities of occurrence of events entering "AND" gate.

Above relations between event probabilities branching to sub-events via gates "AND" or "OR" are used to calculate probability of occurrence of a top event by a bottom-up approach.

Remind that these are events such as failure, mismatch, etc., which are expressed by equivalent of probability of failure.

Such an approach is called static and is constant over time. It does not consider the type of failure probability distribution [6].

### 3. Stochastic approach

It is assumed that the system's failure rate is time-dependent, we have data on all object events in the form of probability distribution and distribution parameters. Failure analysis of the system is performed in order to gain distribution of the whole system failure based on the probability of partitioning the failures of its part. Each object is characterized by a failure probability – a failure in the form of a statistical expression of distribution of random variable in the form of a function:

- Probability density $f(t)$ (probability density pdf) – shows probability of obtaining a random variable in the exploration interval.
  This is the likelihood of product failure at infinitely small time unit after given moment, applies that:
  $$f(t) = \frac{dF(t)}{dt}$$  
  where: $F(t)$ – cumulative density.

- Cumulative density $F(t)$ (The cumulative density cdf) – it is created by gradual summarization of areas under the probability density curve within the limits of the reliability indicator.
  It expresses the probability of failure of the object within a certain time $t$ from its commissioning. Applies that:
  $$F(t) = P(X \leq t)$$

The relation between probability of failure $F(t)$ and probability density $f(t)$ is:

$$F(t) = \int_{0}^{\infty} f(t) \, dt$$

- Additional function $R(t)$ to cumulative density $F(t)$ – expresses the probability of failure-free operation.
  Applies that:
  $$R(t) + F(t) = 1, \quad R(t) = F(t)$$

- Intensity of random variable $\lambda(t)$ is expressed as:
  $$\lambda(x) = \frac{f(x)}{1 - F(x)}$$
  where: $f(t)$ – probability density, $F(t)$ – cumulative density [4].
We can realize stochastic analysis by mathematical modeling. MATLAB allows, with knowledge of distribution of randomly variable time between TTF failures and distribution parameters, determination of failure probability over the entire cumulative density \( F(t) \) and probability density \( f(t) \) of each system component. Let us show a case of mathematical modeling of the probability of "OR" and "AND" gates failure [7].

3.1. Stochastic simulation using mathematical modeling

The OR gate associates 3 components 1, 2 and 3 with failure probability distributions:
- Weibull (Beta = 1.5, Eta = 1000), \( \beta \) – the shape parameter, \( \eta \) – the scale parameter.
- Weibull (Beta = 1.1, Eta = 800).
- Exponential (\( \lambda = 3000 \)), \( \lambda \) = constant rate.

With MATLAB commands, we assign the failure probability value to the components at a given time \( t \) from the \( cdf \) distribution functions.

The course of the failure rate by the functions \( pdf \) and \( cdf \) of the individual components is shown in figure 1 and figure 2.

![Figure 1. The course of pdf components up to 14,000 operating hours.](image1)

![Figure 2. The course of cdf components up to 14,000 operating hours.](image2)

Resulting probability of occurrence of an event at "OR" gate output in case of incoming event independence can be expressed by relation:

\[
F_{or} = 1 - ((1 - F_1) \cdot (1 - F_2) \cdot (1 - F_3))
\]  \( (8) \)

We graphically express the course of resulting \( cdf \) from components 1, 2, 3 at the output of "OR" gate [8].
Figure 3. The course of cdf system from components 1, 2, at the output of "OR" gate up to 1 600 hours.

After 500 hours of operation, the probabilities of component failures are: $F_1 = 0.2978$, $F_2 = 0.4492$, $F_3 = 0.1535$ and system $F_s = 0.6726$.

System failure in accordance with theory achieves a greater probability than the probability of the most failing system element at any time of operation until a failure probability of 1 is reached. The system failure probability exceeds 0.99 by approximately 1 600 hours of operation.

In a similar way, we express the way of modeling the resulting failure rate of "AND" gate components.

Figure 4. The course of cdf system from components 1, 2, 3 at the output of "AND" gate up to 14 000 hours.

From graphical outputs of figure 1 to figure 4 we can see how individual objects participate in the resulting failure rate through the course of disturbance functions, which enters fault tree analysis of the failures at higher level. System failure rate is lower than component failure rate. After reaching the cdf components $F_1$ and $F_2$ with value 1, cdf of the system copies the cdf value of component $F_3$. After 500 hours of operation, probabilities of component failures are: $F_1 = 0.2978$, $F_2 = 0.4492$, $F_3 = 0.1535$ and system $F_s = 0.0205$ [9, 10].

Compared to OR gate results, operating interval increased when probability of failure exceeds 0.99 quantile after approximately 14 000 hours of operation. On the basis of stochastic variables, the course of probability of failures in time is reached. However, we are unable to identify occurrence of a failure event of individual components of the system and the system as a whole on a timeline. The result is inherently static, determined by deterministic relations. Resulting cumulative density cdf is non-
parametric. We know its course, we have calculated values but we don't know the kind of distribution and parameters.

When solving series-parallel system from two OR and AND gates, we choose system decomposition method and include AND gate into the parallel system. This option has been chosen to make graphical outputs more transparent. In figure 5 we can see that the resulting cdf of the system – marked black – changes slightly exceeds cdf at the output of AND gate – marked blue. The AND gate serial components affect it and reaches value 1 after 7 500 hours of operation [11, 12].

4. Conclusions

In this article, we have presented relations of FTA analysis for quantitative deterministic approach that is most commonly used. This analysis is based on a calculation using mean component failure rates. It does not give us an idea of the behavior of the course of failures in components and the system over time. Stochastic simulation by mathematical modeling removes these drawbacks. In case of different types of component failure distribution, graphical representation of courses of statistical functions is an important tool to determine the failure probability after a particular period of operation. We can determine the interval at which individual components participate on the failure rate and make decisions about how to balance the system by changing reliability attributes of components. Stochastic mathematical approach of modeling is diametrically more suitable than deterministic calculations using mean values. We have a clear idea of the failure rates of components and systems over time. However, the results are deterministic and correspond to theoretical solution of the problem [13, 14].

5. References

[1] Stodola J and Furch J 2018 Reliable design: Basic approach MATEC Web of Conferences 198 1–5
[2] Vališ D, Pokora O and Koláček J 2019 System failure estimation based on field data and semi-parametric modeling Engineering Failure Analysis 101 473–484
[3] Valis D, Zak L and Vintr Z 2015 System Condition Assessment Based on Mathematical Analysis IEEE International Conference on Industrial Engineering and Engineering Management 2 441–459
[4] Vališ D and Mazurkiewicz D 2018 Application of selected Levy processes for degradation modelling of long range mine belt using real-time data Archives of Civil and Mechanical Engineering 18 1430–1440
[5] Peikert T, Garbe H and Potthast S 2017 Fuzzy-based risk analysis for IT-systems and their infrastructure EEE Transactions on Electromagnetic Compatibility 59 1294–1301
[6] Varcholová T and Dubovická L 2008 New risk management (Bratislava: Iura) ISBN 978-80-8078-191-0 (in Slovak)
Acknowledgments

This work was supported by the Slovak Research and Development Agency under the contract No. APVV-15-0710.