We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,300

Open access books available

172,000

International authors and editors

190M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Fault Tree Analysis and Reliability Block Diagrams

Jaroslav Menčík

Additional information is available at the end of the chapter

<http://dx.doi.org/10.5772/62374>

Abstract

Fault tree analysis (FTA) strives to reveal all possible sources of critical failures. It starts from the most critical event (“top event”) and looks at its reasons, and continues in this way backwards to the initial events leading finally to the failure. So-called fault tree, plotted using the symbols of Boolean algebra can then be used for the construction of a reliability block diagram, which serves for finding the critical way and probability of failure. The principle of Markov analysis is explained as well.

Keywords: Failure, fault tree, fault tree analysis, FTA, top event, reliability block diagram, probability of failure, Boolean algebra

The failure modes and effects analysis (FMEA), explained in the previous chapter, strives for finding all possible sources of future failures. It starts with failures of single elements, with mistakes of personnel, etc., and looks for their consequences for the structure or process. It is very efficient but has two drawbacks. First, it reveals perhaps all sources of many possible failures, but only few of them are really serious and have fatal consequences, such as the collapse of the structure. Moreover, complex objects can fail in various ways. Second, FMEA is a rather qualitative analysis and does not give information on the probabilities of failure.

For these reasons, **fault tree analysis (FTA)** is also often used (IEC 61025). In contrast to the “bottom-up” inductive approach of FMEA, the Fault Tree Analysis is a deductive method and goes “top-down”. It starts with the so-called **top event** (critical event; e.g. the aircraft is falling down) and searches for all possible causes (e.g. failure of all engines, a broken wing, or an explosion in the aircraft). Then, the reasons for each of these causes are looked for, and so on, until basic events. If all these events are depicted, showing how the “upper” event follows the “lower” event, and so on, the so-called **fault tree** is obtained, which shows the straightest ways to critical failures. Special symbols are used for creating these diagrams (Fig. 1).

Figure 1. Symbols for Fault Tree Analysis.

A simple example with electric lighting in a room with two lamps is shown in Fig. 2. The top event is “there is darkness in the room”. This can happen if none of the two lamps lights, and four possible reasons exist for this (either both the lamps have failed, there is no voltage in the network, the switch is off or failed, or the fuse has burnt).

A single fault tree is used to analyze one and only one top event (or undesired event). FTA involves five principal steps:

1. Definition of the undesired event to be studied. A system engineer with a deep knowledge of the system can best help to define the undesired events.
2. Obtaining an understanding of the system. Analysts and system designers can help here.
3. Construction of the fault tree.
4. Evaluation of the fault tree.
5. Control of all identified hazards, with the effort to reduce the probability of their occurrence.

In contrast to FMEA, fault tree analysis is able to consider also events caused by external reasons.

Fault tree analysis is often used in the aviation industry, as well as chemical, petrochemical, nuclear power, and other high-hazard industries.

A fault tree can be converted into a **reliability block diagram (RBD)**. This is a scheme similar to Fig. 4 in Chapter 5, with series and parallel arrangement of blocks representing the individual elements or groups of them. Each element is characterized by a failure rate. A series arrangement fails if any of its elements fails. Parallel paths are redundant, that is, all elements must fail for the parallel network to fail. If the probabilities of individual events are known, one can calculate the failure probability of the system, as shown in Chapter 5.

A reliability block diagram RBD may be drawn using switches instead of blocks, where a closed switch represents a working component and an open switch represents a failed component. If a path may be found through the network of switches from the beginning to the end, the system is still working. The system can also be solved using the rules of Boolean algebra. Series paths can be replaced by AND gates and parallel paths with OR gates, etc.

In complex systems consisting of many blocks, various blocks can fail simultaneously. If connections exist between certain elements, the failure of one or even more blocks does not

Figure 2. Fault tree for two lights in a room.

necessarily mean the failure of the whole system. Reliability in such systems is studied by the **cut set** or **tie set** methods. A cut set is obtained by drawing a line through the blocks, whose failures would cause the failure of the system. Tie sets are obtained by drawing lines through such blocks, which, if working, would ensure the operation of the system. This analysis helps in revealing the possible conditions for failure or in finding an arrangement with high resistance to failure.

Another approach to reliability analysis of complex systems uses the so-called Markov chains or **Markov analysis**. This analysis is suitable for systems whose components can be in two states, failed or not failed, and transitions from one state to another can happen from time to time. The analysis can be applied in cases where the response (or change of state) at a certain instant does not depend on previous events (so-called memoryless system) and the probabilities are known for the transition from operable state to failed state and vice versa; these probabilities are assumed constant. Markov analysis enables one to trace how the system evolves in time from certain initial conditions, and to see how quickly (and whether) it approaches to a steady state after a disturbing event. For example, if the probability of transition from the available state to a failed one is $P_{A \rightarrow F}$ and from the failed state to an available state is $P_{F \rightarrow A}$, and if the component was initially available ($P_0 = 1$), then the probability that it will be in a failed state after one step equals $P_1(F) = P_{A \rightarrow F}$. The probability of a failed state after the second step is $P_2(F) = P_{A \rightarrow F} \times P_{F \rightarrow F} + P_{A \rightarrow A} \times P_{A \rightarrow F}$; here the probability of the transition from the failed state into the failed state is $P_{F \rightarrow F} = 1 - P_{F \rightarrow A}$, whereas the probability of transition from the available state into an available state is $P_{A \rightarrow A} = 1 - P_{A \rightarrow F}$. The evolution can be depicted using Markov state transition diagrams and tree diagrams, which become

more and more complex with each step. Computer support is thus necessary. Markov analysis is used, for example, for the simulation and analysis of reliability of systems for electricity supply or reliability of software.

More details to fault tree analysis and reliability block diagram can be found in the literature [1 - 3]. These methods have also been incorporated into reliability standards, e.g. IEC 61025, and commercial computer programs for FTA are also available. More about cut set and tie sets can be found in [2, 3], more about Markov analysis is in [3 - 5].

Author details

Jaroslav Menčík

Address all correspondence to: jaroslav.mencik@upce.cz

Department of Mechanics, Materials and Machine Parts, Jan Perner Transport Faculty,
University of Pardubice, Czech Republic

References

- [1] Bentley J P. Introduction to Reliability and Quality Engineering. Harlow, England: Addison-Wesley; 1999. 202 p.
- [2] Ireson W G, Coombs C F Jr, Moss R Y. Handbook of reliability engineering and management. 2nd ed. New York: McGraw-Hill; 1996. 816 p.
- [3] O'Connor Patrick D T. Practical Reliability Engineering. 4th ed. Chichester: John Wiley & Sons; 2002. 513 p.
- [4] Freedman D. Markov Chains, Berlin: Springer; 1983. 382 p.
- [5] Bednařík J et al. Reliability techniques in electronic practice (In Czech: Technika spolehlivosti v elektronické praxi). Praha: SNTL; 1990. 336 p.