Risk assessment techniques with applicability in marine engineering

E Rudenko¹, F V Panaitescu² and M Panaitescu²
¹Odessa National Maritime University, 34, Mechnikov Street, Odessa, 65029, Ukraine
²Constanta Maritime University, Faculty of Naval Electro-Mechanics, 104 Mircea cel Batran Street, 900663, Constanta, Romania

E-mail: magnit_od@ua.fm

Abstract. Nowadays risk management is a carefully planned process. The task of risk management is organically woven into the general problem of increasing the efficiency of business. Passive attitude to risk and awareness of its existence are replaced by active management techniques. Risk assessment is one of the most important stages of risk management, since for risk management it is necessary first to analyze and evaluate risk. There are many definitions of this notion but in general case risk assessment refers to the systematic process of identifying the factors and types of risk and their quantitative assessment, i.e. risk analysis methodology combines mutually complementary quantitative and qualitative approaches. Purpose of the work: In this paper we will consider as risk assessment technique Fault Tree analysis (FTA). The objectives are: understand purpose of FTA, understand and apply rules of Boolean algebra, analyse a simple system using FTA, FTA advantages and disadvantages. Research and methodology: The main purpose is to help identify potential causes of system failures before the failures actually occur. We can evaluate the probability of the Top event. The steps of this analyze are: the system’s examination from Top to Down, the use of symbols to represent events, the use of mathematical tools for critical areas, the use of Fault tree logic diagrams to identify the cause of the Top event. Results: In the finally of study it will be obtained: critical areas, Fault tree logical diagrams and the probability of the Top event. These results can be used for the risk assessment analyses.

1. Introduction

Any danger is realized, bringing damage, as a result of any cause or multiple causes, so preventing hazards or protection from them is only possible at revealing the causes. Between dangers realized and causes there is a causal relationship: the danger is a consequence of a cause which, in turn, is a consequence of another cause, and so on. Thus, the causes and dangers form hierarchical, chain structure or systems. Graphic representation of these dependencies resembles a branching tree, so in the literature analyzing safety of objects is used term "fault tree".

Fault tree underlies the logical-probabilistic model of cause-effect relationships of system failures with failures of its elements and other events (impacts). In the analysis of a fault, fault tree consists of sequences and combinations of faults and disturbances, and thus it is a multilevel graphological structure of casual relationships received as a result of tracking hazardous situations in the reverse order to find their possible causes [1].

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

Published under licence by IOP Publishing Ltd
The objectives of FTA are [2]:

- identification of the cause or combination of causes leading to the final (top) event;
- identification the causes which can affecting the reliability, safety, efficiency and other performance characteristics of the analyzed system;
- identification of conflicting requirements or specifications that may affect the reliability, safety and other performance characteristics;
- determination of whether system characteristics meet the established requirements;
- identification of common cause failures (common events).

The steps for construction a Fault Tree logic diagrams are: 1) description of the system, when boundaries and data needs are determined (description of the processes, characteristics of the materials and equipments, description of the maintenance procedure, etc.); 2) the identification of the hazard (site inspections, check-lists, hazard and operability studies); 3) the construction of the Fault Tree (events and gates) [1, 2, 4]; 4) the qualitative analyse of the structure of the Fault Tree (using the laws of Boolean algebra); 5) the quantitative evaluation of the Fault Tree (the calculus of the Top event frequency or probability [1, 3, 4].

2. Basic components of Fault Tree Analysis

2.1. The diagrams of Fault Tree.

Fault Tree diagrams consist of gates (AND, OR) and events. These are connected with lines. Classical FTA use different shapes for the events (rectangle – for the negative event; this shape is located at the Top of the tree and it is the only symbol that will have a logic gate and input events below it; circle – for the base event; this shape is located on the bottom tiers of the tree (figure 1).

![Figure 1. Basic components of Fault Tree.](image)

a) AND gate; b) OR gate; c) rectangle (the negative event); d) circle (the base event).

2.2. Case studies of Fault Tree Analysis

Case study 1

A necessary condition of human death from electrical is his or her body inclusion in electric circuit with sufficient for death amperage. Therefore, occurring the accident (Top event "A") needs simultaneous existence of three conditions (figure 2).

Event "B" – a potentially high voltage on the electrical installation.
Event "C" means the appearance of a man on a conductive surface connected to ground.
Event "D" – a human body touching of electrical installation.

In turn, the event "B" may be the result of either of two events – prerequisites "E" and "F", where "E" – lowering the resistance of insulation of live parts and the event "F" – live parts touching of electrical installation.

Event "C" is also due to two assumptions: "F" – joining a man on a conductive surface, and "Z" – a human body touching of grounded elements of the room.

Event "D" is the result of the appearance of one of three prerequisites: "I" – the need for repair, "J" – the need for maintenance and "K" – intended use of the electrical installation, or normal operation of the installation.
Analytically the expression equation (1) for condition of realization of the accident (Top event "A") takes the form:

\[ P(A) = P(B) \times P(C) \times P(D) = [P(E) + P(F)] \times [P(G) + P(H)] \times [P(I) + P(J) + P(K)] \]  \hspace{1cm} (1)

*Note.* On fault trees the failure probabilities tend to be small with very small error term [1], [4]. For this, we can make an assumption (equation (2)) for specially events:

\[ P(X \text{ or } Y) \approx P(X) + P(Y), \quad P(X \cap Y) = 0. \]  \hspace{1cm} (2)

*Case study 2*

Unloading operation is one of the most intensive technological operations for tanker. It requires a lot of energy and leads to high load of SPP (ship power plant) comparable to energy consumption during vessel motion.

In case of failure of the above technical facilities performance degradation of cargo-pumping system occurs, that leads to an increase in the discharge time and downtime of the tanker, at a cost to the shipowner in the tens of thousands of dollars per day.
Figure 3 shows the developed model (fault tree) needed for solving the problem of finding the frequency of tanker cargo-pumping system failure during unloading. Values of the probabilities can be taken from the practice of exploitation of this and similar equipment.

Event "A" (Top event) – failure of cargo-pumping system, that leads to an increase of tanker unloading time.

For the cargo-pumping system failure occurring of one of the following three events is sufficient:

- Event "B" – reducing the cargo-pumping system supply because of stopping one of the cargo pumps.
- Event "C" – reducing the cargo-pumping system supply because of failure one of the auxiliary boilers.
- Event "D" – ship de-energization.

For the event "B" to occur one of the following three events is sufficient:

- Event "E" – cargo pump № 1 stopping.
- Event "F" – cargo pump № 2 stopping.
- Event "G" – cargo pump № 3 stopping.

For the event "C" to occur one of the following two events is sufficient:

- Event "H" – auxiliary boiler № 1 failure.
- Event "I" – auxiliary boiler № 2 failure.

For the event "D" to occur the following three events must occur simultaneously:

- Event "J" – diesel-generator № 1 failure.
- Event "K" – diesel-generator № 2 failure.
- Event "L" – diesel-generator № 3 failure.

For the event "E" to occur one of the following two events is sufficient:

- Event "M" – cargo pump № 1 failure.
- Event "N" – cargo pump № 1 drive failure.

For the event "F" to occur one of the following two events is sufficient:

- Event "O" – cargo pump № 2 failure.
- Event "Q" – cargo pump № 2 drive failure.

For the event "G" to occur one of the following two events is sufficient:

- Event "R" – cargo pump № 3 failure.
- Event "S" – cargo pump № 3 drive failure.

Analytically the expression (equation (3)) for condition of realization of the accident (Top event "A") takes the form [5]:

\[
P(A) = P(B) + P(C) + P(D) = \left\{ \left[ P(M) + P(N) \right] + \left[ P(O) + P(Q) \right] + \left[ P(R) + P(S) \right] \right\} + \left[ P(H) + P(I) \right] + \left[ P(I) \times P(J) \times P(K) \right].
\]  \hspace{1cm} (1)

Advantages of FTA [1, 2, 3, 6]:

- easy to read and understand;
- can construct many combinations of failures;
- can manage the actions to minimize the risk;
- can manage the data for the risk assessment process.

Disadvantages of FTA:

- FTA involves thorough details for designing a system;
- significant training and experience is necessary to use this technique properly;
- in calculating the probability of an event in FTA there is uncertainty regarding the basic events;
- there is the possibility of errors when they are omitted causal links.
3. Conclusions

Fault Tree analysis is a technique that allows the existing situation analysis: analyse current needs, identification of key issues in their context, arrangement of issues according to the cause-effect relationship in the form of charts/tree, analyse quantitatively the systems and possible causes and ways of failure occurrence, analyse in the each stage of operation how can you determine the most significant failures can occur and which are the connections between causes, failures and importance of the different ways of fault tree analysis.

In the finally of study it will be obtained:
1) critical areas: in the case study 1-the accident (top event “A”), in the case study 2- failure of cargo-pumping system,
2) fault tree logical diagrams- Fault tree for electrical injury and Fault tree for cargo-pumping system failure and the probability of the Top event. On fault trees the failure probabilities tend to be small with very small error term and for this we must make an assumption for specialy events (e.g. joining a man on a conductive surface, a human body touching of grounded elements of the room).
3) the developed models (fault trees) needed for solving the problem of finding a necessary condition of human death from electrical domain for body inclusion in electric circuit with sufficient for death amperage or finding the frequency of tanker cargo-pumping system failure during unloading.
4) The analitical expressions for the failure probabilities which we have obtained can be used for the risk assessment analyses.

Acknowledgements

This article is a result of the project “Increasing quality in marine higher education institutions by improving the teaching syllabus according to International Convention STCW (Standards of Training, Certification and Watchkeeping for Seafarers) with Manila amendments” POSDRU/156/1.2/G/141534. This project in co funded by European Social Fund through The Sectorial Operational Programme for Human Resources Development 2007-2013, coordinated by Constanta Maritime University. The content of this scientific article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed in the article lies entirely with the authors.

References

[1] Ericson C 1999 Fault Tree Analysis. A History Proceedings of the 17th International System Safety Conference 1(9) pp 150-163
[2] Vesely W et al. 1981 Fault Tree Handbook NUREG-0492 Nuclear Regulatory Commission pp 33-54
[3] American Institute of Chemical Engineers 1989 Guidelines for Chemical Process Quantitative Risk Analysis pp 548-740
[4] http://www.academia.edu/6621646/M3_4c_Fault_Tree. Accesed:09/03/2015
[5] http://en.wikipedia.org/wiki/Fault_tree_analysis. Accesed: 26/02/2015
[6] http://psam12.org/proceedings/paper/paper_581_1.pdf. Accesed: 01/12/2014