Naive Fault Trees for Safety Evaluations in Early Project Phase

Mohammad Rajabalinejad
Laboratory of Design, Production and Management
University of Twente, Enschede, the Netherlands
Tel: +31 643 809 242
Email: m.rajabalinejad@utwente.nl

doi:10.5296/jss.v2i2.10441 URL: http://dx.doi.org/10.5296/jss.v2i2.10441

Abstract

Naive Fault Trees (NFT) aim to extend the application of Fault Trees (FT) and make them appealing for system designers in the early project life cycle. NFT use input intervals and values to estimate the frequency of a top event. This extension facilitates the assignment of failure probability to basic events when exact data is difficult to find, unavailable or even not existent. The formulation of the problem and results are presented in this paper through an application to a real-world example.

Keywords: Fault tree, quantitative, risk, qualitative, uncertainty

1. Introduction

Fault tree analysis (FTA) is used to identify and analyze the conditions and events that may contribute to the occurrence of a top event. The international Electro-technical Commission (IEC) has published an international standard about the FTA and describes this approach in details (IEC, 2006). Fault trees use formalized symbols, identifiers and labels to ensure consistency. FTA is an analytical approach to the evaluation of the flow of states or events that may influence the performance of a system, product or component (safety, reliability, maintainability, availability etc.). It is a graphical representation of basic or intermediate events which contribute to the occurrence of a final outcome which can be a success or failure. This graphical representation is a mean for clear understanding of the problem, and its analysis or rearrangement.

FTA employs a top-down approach to model, evaluate and present the logic combination of expected events and their influence on a pre-defined top-event. It can be performed in a qualitative or quantitative manner. Yet, there are cases that are hard to estimate the probability of unfavorable situations and assign values to fault trees. In such cases, the likelihood of basic events of a fault tree can be described in the form of “highly probable”, “very probable”, “medium probable”, or “low probable”. This helps identifying the minimal cut set and specify how the basic events influence the top event, as this will be discussed further in this paper. If the probability of a failure is known, a qualitative analysis of fault tree can determine the probability of occurrence of the top event. In addition, FTA helps understanding and analyzing complex structures by including interactions between subsystems or components.

FTA can be used to analyze a system under development, take preventive measures, identify potential causes of failures, estimate reliability, prepare probabilistic risk assessment, and develop mitigation plans; safety standards often demand for preventive measures against failure and this can be accomplished by FTA (IEC, 2003). A combination of FTA with FMEA (Failure Mode and Effect Analysis) provide more favorable outcomes because they complement each other, in the sense that FMEA is a bottom-up approach. Any identified unfavorable event by FMEA can be potentially considered as a top event for FTA. FTA can be also combined with ETA (Event Tree Analysis) since any intermediate event can be defined as a top event for the FTA analysis. To extend the functionality of fault trees, it may be combined with Markov analysis, binary decision diagrams, or reliability block diagrams (IEC, 2006; NASA, 2007).

Application of fault trees in estimation of system reliability has been discussed for example in Dutuit & Rauzy (2005). Fault trees have also been used in safety assessment of high speed trains (e.g., Liu, Yang, Gao, Li, & Gao, 2015). This study focuses on a qualitative analysis with fault trees regarding safety. Apart from showing a qualitative application of a FTA, the author also associate probabilities to basic events or the top event; one needs to have the probability of failure for each basic event in order to calculate the probability of failure of top event. This is important for early phases of design, called conceptual design, where the details of a certain design choice are not realized. It is a stage in design where information can be symbolic and not accurate, so the information needed to embody a design concept is not fully available. The next section highlights the importance of conceptual design and justifies the need for a tool that uses the physical or mathematical logics with a range of possible values that ultimately facilitates decision making in early design phases. The need for such a tool has been stated by various authors, such as Kurumatani, Tomiyama, & Yoshikawa (1990).

2. Fault trees in early design phases and the stated problem

IEC suggests developing fault trees in early design stages and keeping that along all stages of product developments. This suggestion is made because fault trees use simple but fundamental logics and are a powerful communication means. Therefore, fault trees can substantially influence early design choices which result in fundamental changes in projects. However, assigning exact values in early project phases could be misleading where the scope and main functions need to be elaborated, thus the requirement for exact values restrict the use of fault trees at this stage. There are a few reasons that explain why a quantitative analysis of fault trees in early design phases are less justified (Sutton, 2007):

- Different people have different understanding of numbers or probability of failures. Concepts like constant failure rate or frequency of occurrence is difficult to use for both of non-experts and experts when the values are uncertain.

- Objectivity of the values assigned to a fault tree can be questionable in the absence of precise data. In early phases of design is almost unlikely to see similar outcomes from two teams or two experts.

- Complex systems may fail in unexpected ways, and risk analyses are unlikely to capture all the failure modes. Having a quantitative analysis with precise values in early design phases may raise the expectations about the accuracy of estimated top-event failure in early design phases.

- The cause of some failures are human errors, and it is hard to assign a certain value to the possibility of having something done correctly or incorrectly by humans. It is difficult, if not impossible, to quantify human behavior.

- Quality of data in early design phases might not be appealing. While early decisions have to be made, designers cannot (and are not advised to) wait to achieve high quality data which may become irrelevant to them for the rest of design.

As a result of the above, it becomes very difficult, if not impossible, to apply a fully quantitative FTA in early design phases. As a result, a qualitative fault tree analysis or a quantitative analysis with embedded flexibilities look more relevant and appealing to system designers/engineers. Given these, there is no surprise that qualitative fault tree analysis absorbs more and more attention (Liu et al., 2015).

3. The objective and the approach

This article aims at broadening the application of FTA and making them appealing for system designers in the early project life cycle. It uses the advantages of both qualitative and quantitative fault trees and makes a powerful tool for evaluation and communication of design process when the information about faults and failures is not accurate and expert opinion is used as the best source of information for this. The paper suggests using a qualitative format for communication with stakeholders. This facilitate collection and integration of the stakeholders' opinion. Based on the collected information and experience, a systems or design engineer forms a naive fault tree to explore the influence of each basic/intermediate event on the top event.

3.1 Quantifying qualities and qualifying quantities

In FTA, the frequency of occurrence of each basic event or its probability of failure is important. In early design phases, a system designer or systems engineer needs to make decisions based on some values which are not precise or certain. In this case, it is possible to assign uncertain values individually or plastically using the available methods suggested in earlier works of the author. This requires identification of relevant categories which are understandable to stakeholders.

These categories can be shown in a table and communicated with the system stakeholders. This enables the stakeholders to freely present their opinions and include their uncertainties. IEC suggests using four different categories: seldom-occurrence, less-often occurrence, frequent occurrence and continuous occurrence considering the occurrence or exposure time for this estimation. These can be presented in a table format (Rajabalinejad, 2016). This allows the stakeholders to freely present their uncertain opinions and integrate them in a pluralistic approach. Here, we assume that the systems engineer or designer has already collected the stakeholders or expert data and formed an opinion about the scope of fault tree, its basic and intermediate events, and the frequency of occurrences which can be assigned to the basic events.

Using expert/stakeholders opinions to assign objective probabilities to a basic event can be difficult because there are obstacles in communication with system stakeholders who can be individuals, corporations, organizations and authorities, with different fields/levels of knowledge and experience (Rajabalinejad & Spitas, 2012b). They all have their own interests, expectations, and preferred alternatives (Zimmermann, 1987). Besides, uncertainty in opinions is natural, and assigning exact values to quantities that are unknown or subject to changes is questionable.

In this context, there is a need for a realistic and intuitive approach that can communicate to stakeholders with different fields of knowledge and expertise. The method must be transparent, easy to implement and readily adaptable by different users. For this purpose, graphs are used to communicate with experts through a qualitative or quantitative scale. Then, a probability density function (PDF) is assigned to the recorded data in order to form a random variable. The principle of the method is described by Rajabalinejad & Spitas (2012a). The next section provides an overview for the mathematics of data integration for NFT.

3.2 Frequency of occurrence

Let m be the number of stakeholders for a system, and let B_i presents the frequency of occurrence for a single basic event in the form of a normally distributed probability density function. Let random variables $b_{i_1}, b_{i_2}, \ldots, b_{i_m}$ present occurrence of this event identified by system experts or stakeholders, where b_{i_k} represents the k-th stakeholder's opinion for i-th event. The first and second moments of these variables are respectively shown $\mu_{i_1}^b, \mu_{i_2}^b, \ldots, \mu_{i_m}^b$ and $\sigma_{i_1}^b, \sigma_{i_2}^b, \ldots, \sigma_{i_m}^b$. As a result, the moments of occurrence for the i-th event are formulated by Equations (1) and (2), respectively.

$$\mu_i^B = \frac{1}{\sum_{k=1}^{m} \alpha_k} \sum_{k=1}^{m} \alpha_k \mu_{i_k}^b \qquad (1)$$

$$\left(\sigma_i^B\right)^2 = \sum_{j=k}^{m} \frac{\alpha_k^2 \left(\sigma_{i_k}^b\right)^2}{\left(\sum_{k=1}^{m} \alpha_k\right)^2} \qquad (2)$$

Where α_k represents the assigned weight to the k-th stakeholder. This means that the collected data for the frequency of occurrence of the i-th event, can be presented by two variables, μ_i^B and σ_i^B. This is a mean to collect and integrate data collected from stakeholders where data about basic events is scarce.

3.3 Mathematical formulation

Let B_i and B_j represent the frequencies assigned to i-th and j-th basic (or intermediate) events of a NFT, respectively. And let their probability of occurrences be represented by $P(B_i)$ and $P(B_j)$. Provided independency between these events, meaning that the basic event B_i has no influence on B_j and that B_j has no influence on B_i, the probability of conjunction and dis-conjunction events are obtained by Equations (3) and (4) , respectively. The scope of this paper is limited to independent basic variables, for more information about the dependent variables and their influence on FTA, the reader is advised to look into Pedroni & Zio (2013).

$$P(B_i \cap B_j) = P(B_i) * P(B_j) \tag{3}$$

$$\begin{aligned} P(B_i \cup B_j) &= 1-(1-P(B_i))(1-P(B_j)) \\ &= P(B_i)+P(B_j)-P(B_i)*P(B_j) \end{aligned} \tag{4}$$

Previous section explained the approach where B_i represents the probability density function of ith basic event. Here, the first moment is used as input for the fault tree. This results in the following equations.

$$P(B_i \cap B_j) = \mu_i^B * \mu_j^B \tag{5}$$

$$\begin{aligned} P(B_i \cup B_j) &= 1-(1-\mu_i^B)(1-\mu_j^B) \\ &= \mu_i^B + \mu_j^B - \mu_i^B * \mu_j^B \end{aligned} \tag{6}$$

4. Application example, the 17th street flood wall

For the purpose of demonstration, we use the fault tree used in a real-world case study in New-Orleans (Rajabalinejad, van Gelder, Vrijling, Kanniing, & van Baars, 2007). The fault tree in this case projects possible events which may lead to the failure of the flood-defense structure, whose design was reviewed after its failure in Hurricane Katrina. Here the fault tree is naively used to estimate the performance of the flood wall by an expert. The outcome is not expected to be fully objective or very precise. The implementation of NFT for this case aims to provide a reflection that structured design-reviews in early stages could have highlighted its weaknesses. Therefore, the integrity of the expert estimates presented in this paper were not subject to verification.

4.1 Fault tree for the flood wall

The main function of designed flood wall in the 17th street canal was protection of the city from flooding; therefore, its failure to do this job is the top event as presented in the fault tree presented in Figure 1. In this figure, there are two main intermediate events showing the importance of reliability analysis in two modes: expected and extreme conditions; in other words, a flood defense system should be stable with the expected loads and able to tolerate extreme conditions. The expected failure as indicated in the fault tree are sliding, piping, overflowing and overtopping. These failure modes have been further explained in the following text.

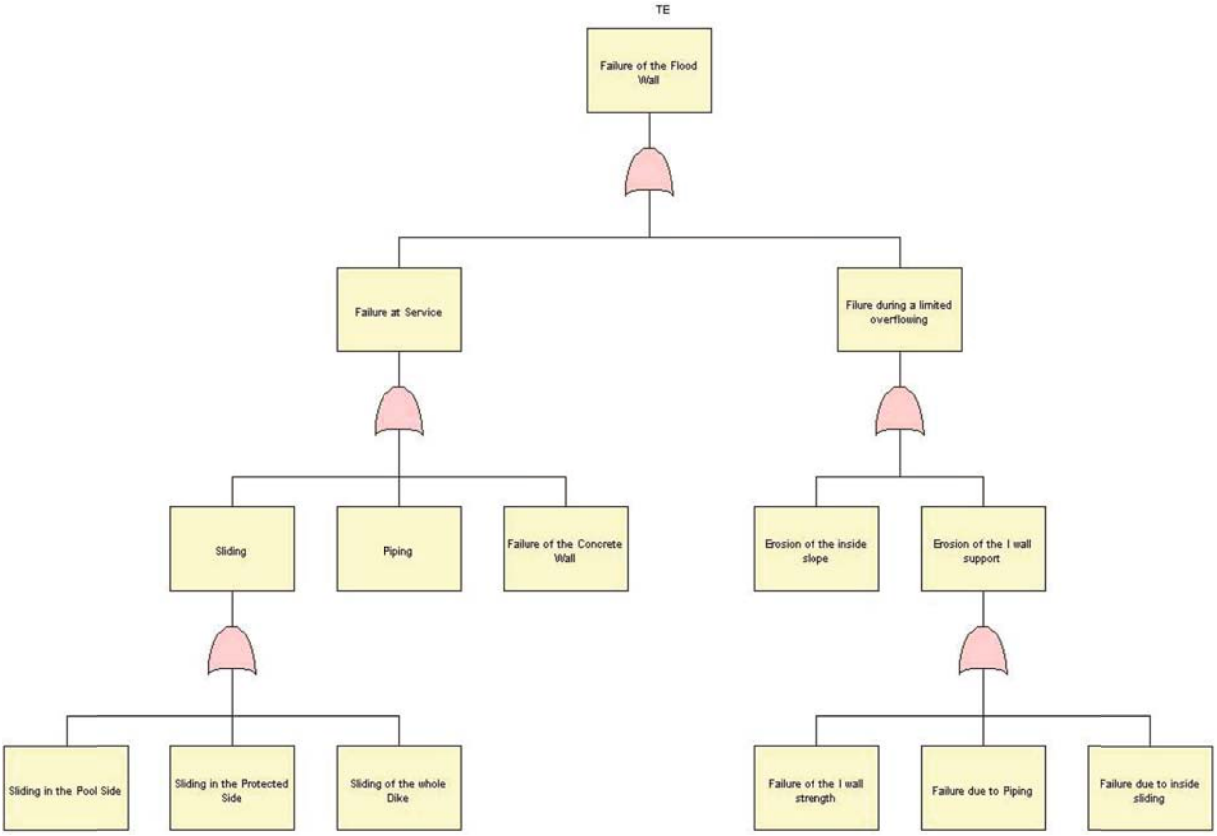
TE
Failure of the Flood Wall
Failure at Service
Filure during a limited overflowing
Sliding
Piping
Failure of the Concrete Wall
Erosion of the inside slope
Erosion of the I wall support
Sliding in the Pool Side
Sliding in the Protected Side
Sliding of the whole Dike
Failure of the I wall strength
Failure due to Piping
Failure due to inside sliding

Figure 1. The fault tree for 17th Street flood wall example (quoted from Rajabalinejad et al., 2007).

4.2 Sliding

The sliding failure mode explains the situation where the complete structure slides as a result of extreme water pressure behind the flood wall. A previous research project concluded that the sliding was the main failure mode of this structure (USACE, 2006).

4.3 Piping

Piping is a situation where water particles move through the foundation and make a narrow pipe in the soil. There are explicit (analytical) limit state functions which can be approximately used to evaluate the probability of piping. Several studies concluded that probability of piping for this structure was very low (see e.g. (USACE, 2006)).

4.4 Overflowing

In the design phase or reliability assessment of a flood defense, the expected time of overflowing should be attended seriously. In other words, an infrastructure like a flood defense should be able to sustain the overflowing conditions to provide resilience. Furthermore, overflowing can cause scour and erode the flood wall support, which can intensify the criticality of situation.

4.5 Forming the Naive FTA for the flood wall

In order to ensure an unambiguous communication, there is a need for a well-defined relationship between qualitative and quantitative metrics. Table 1 defines this relationship and explains how the qualitative definition of, for example, no occurrence is translated to quantitative values. For the given example application, the unexpected events will mainly stay in the category of no-occurrence or seldom-occurrence. If one event happens more than once in 100 years, it will be somewhere between frequent-occurrence and often-occurrence. Following the use of Table 1, Table 2 summarizes the qualitative fault tree, numerical values, simulation results, and the final qualitative outcome for the 17th street flood wall.

Table 1. The relationship between the quantitative and qualitative values.

Qualitative Values	**Quantitative Values***
No-Occurrence	The event is not expected to happen in 10,000 years
Seldom Occurrence	The event may happen 1 time in 10,000 years
Less-frequent Occurrence	The event may happen 1 time in 1000 years
Frequent Occurrence	The event may happen 1 time in 100 years
Often Occurrence	The event may happen 1 time in 10 years
Continuous Occurrence	The event may happen once in a year
* The expert may use some indicative measures in order to make the assessment more objective.	

Table 2. Summary of Results

	Failure mode	Intermediate even	Scenario 1			
			Qualitative*	Numeric data*	Simulation outcome	Qualitative outcome
Failure at normal service	Sliding	in pool side	Seldom	0.0001		
		in protected side	Seldom	0.0001		
		of whole dike	Seldom	0.0001		
	Piping		No	0.00005		
	Failure of the I-wall		No	0.00005		
Failure at extreme events	Sliding	in pool side	Less-freq.	0.001		
		in protected side	Less-freq.	0.001		
		of whole dike	Less-freq. to freq.	0.005		
	Erosion of inner slope		Less-freq.	0.001		
	Erosion of	Erosion of I	seldom	0.0001		

	Failure mode	Intermediate even	Scenario 1			
			Qualitative*	Numeric data*	Simulation outcome	Qualitative outcome
	the support	wall				
		piping	seldom	0.0001		
Top Event		Failure of the flood-wall			≈0.005	Less-freq. to freq.
* This data is imprecise and presents the opinion of one single expert.						

5. Discussion

The example application illustrated in this paper shows the use of NFT for early design evaluation. NFT provides a framework for reviewing the design even in the absence of highly accurate models. In other words, complex calculations can be replaced by simpler models in order to provide estimates for frequency of occurrences. This motivates the use of simpler models for safety evaluation in early design phases.

The suggested approach provides a simple framework for formulation of the problem, the relationship between basic events, and their influence on top event. It does not demand accurate data, and can be used even in the absence of precise models or data. Although the results are shown in the form of a table, it is convenient to use graphical representation on the fault tree and communicate only the qualitative input and output with the user/designer. Furthermore, the changing variable does not necessarily need to be the top event. A designer may set the accepted range for the top event and then explore possible ranges in intermediate or basic level. This provides further insight for the designer to check if the right balance is kept in the course of design. The result of the fault tree for this case study simply shows that even the performance of a very strong flood wall follows the performance of its foundation.

6. Conclusions

Absence of accurate data, imprecise data, or uncertainty in data for the failure rates influence the quality of FTA and raise questions about the reliability of outcome. To address these issues, the paper suggests Naive Fault Trees (NFT) in early design phases where the available data is often imprecise. It replaces a range of values with a single value in order to overcome issues that hinder the use of fault trees. Furthermore, it proposes a basis for integration of precise and imprecise information to support design decisions in early project phases. This approach enjoys the benefits of fault tree analysis and creates further insight to architect a proper solution.

References

Dutuit, Y., & Rauzy, A. (2005). Approximate estimation of system reliability via fault trees. *Reliability Engineering & System Safety, 87*(2), 163-172. doi:DOI 10.1016/j.ress.2004.02.008

IEC. (2003). IEC 60300-3-1 Second edition 2003-01 Dependability management – Part 3-1: Application guide –Analysis techniques for dependability –Guide on methodology.

IEC. (2006). CEI IEC 61025 Fault tree analysis (FTA).

Kurumatani, K. I., Tomiyama, T., & Yoshikawa, H. (1990). Qualitative Representation of Machine Behaviors for Intelligent CAD Systems. *Mech. Mach. Theory, 25*(3), 325-334.

Liu, P., Yang, L. X., Gao, Z. Y., Li, S. K., & Gao, Y. (2015). Fault tree analysis combined with quantitative analysis for high-speed railway accidents. *Safety Science*, *79*, 344-357. doi:10.1016/j.ssci.2015.06.017

NASA Systems Engineering Handbook. (2007). National Aeronautics and Space Administration, NASA Headquarters, Washington, D.C. 20546.

Pedroni, N., & Zio, E. (2013). Uncertainty Analysis in Fault Tree Models with Dependent Basic Events. *Risk Analysis*, *33*(6), 1146-1173. doi:DOI 10.1111/j.1539-6924.2012.01903.x

Rajabalinejad, M. (2016). *Coping with System Hazards in Early Project Life Cycle: Identification and Prioritization*. Paper presented at the The Sixth International Conference on Performance, Safety and Robustness in Complex Systems and Applications, Lisbon, Portugal.

Rajabalinejad, M., & Spitas, C. (2012a). A Gaussian decision-support tool for engineering design proesses. *International Journal of Industrial and Systems Engineering*(In Press).

Rajabalinejad, M., & Spitas, C. (2012b). Incorporating Uncertainty into the Design Management Process. *Design Management Journal, 6*(1), 52-67.

Rajabalinejad, M., van Gelder, P. H. A. J. M., Vrijling, J. K., Kanniing, W., & van Baars, S. (2007). Probabilistic Assessment of the Flood Wall at 17th Street Canal, New Orleans *Risk, Reliability, and Social Safety* (Vol. III, pp. 2227). Stavanger, Norway.

Sutton, I. (2007). *Fault Tree Analysis*. Houston, TX 77041, United States of America: Sutton Technical Books.

USACE. (2006). *Orleans and Southeast Louisiana Hurricane Protection System, Volume III. The Hurricane Protection System. Technical Report 378, U.S. Army Corps*

of Engineers, Report of the Interagency Performance Evaluation Task Force. Retrieved from

Zimmermann, H. J. (1987). *Fuzzy sets, decision making and expert systems* (Vol. 10): Springer.

Copyright Disclaimer