AACE INTERNATIONAL RECOMMENDED PRACTICE

131R-23

INTRODUCTION TO FAULT TREE ANALYSIS FOR PROJECTS

AACE INTERNATIONAL

Rev. October 14, 2024

AACE® International Recommended Practice No. 131R-23

INTRODUCTION TO FAULT TREE ANALYSIS FOR PROJECTS

TCM Framework: 3.2 – Asset Planning
3.3 – Investment Decision Making
7.5 – Value Analysis and Engineering
7.6 – Risk Management
11.4 – Quality and Quality Management

Rev. October 14, 2024

Note: As AACE International Recommended Practices evolve over time, please refer to web.aacei.org for the latest revisions.

Any terms found in AACE International Recommended Practice 10S-90, *Cost Engineering Terminology*, supersede terms defined in other AACE work products, including but not limited to, other recommended practices, the *Total Cost Management Framework*, and *Skills & Knowledge of Cost Engineering*.

Contributors:

Disclaimer: The content provided by the contributors to this recommended practice is their own and does not necessarily reflect that of their employers, unless otherwise stated.

Dr. David T. Hulett, FAACE (Primary Contributor)
H. Lance Stephenson, CCP, FAACE Hon. Life (Primary Contributor)
James E. Arrow, DRMP
Tim Boatwright, EVP
Francisco Cruz, CCP
Larry R. Dysert, CCP CEP DRMP FAACE Hon. Life
Rafi Polak
John R. Schuyler, CCP DRMP
Pei Tang, PRMP PSP

AACE® International Recommended Practice No. 131R-23

INTRODUCTION TO FAULT TREE ANALYSIS FOR PROJECTS

TCM Framework: 3.2 – Asset Planning
3.3 – Investment Decision Making
7.5 – Value Analysis and Engineering
7.6 – Risk Management
11.4 – Quality and Quality Management

October 14, 2024

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Purpose

This document is intended to provide a guideline, not a standard, for using fault tree analysis (FTA) to improve the quality of the outputs of the project or product by providing a comprehensive and systematic way to identify, assess, and prioritize risks. FTA enhances a decision-maker's understanding of the complex relationships regarding potential risks or failure points that should be addressed to improve or optimize project outcomes. This document further provides practitioners with the opportunity to improve the reliability of design and to improve the quality by reducing potential failures. Examining what would potentially cause the product to be less reliable is also related to decision analysis. For an organization that executes capital projects, the FTA is also applicable in providing insight into performing other analyses, such as:

- Functional analysis of highly complex systems
- Evaluation of safety requirements and specifications
- Evaluation of system reliability and the identification of potential design defects and safety hazards
- Simplification of design to support operations and maintenance requirements (for lifecycle cost analysis)
- Evaluation of human interfaces (project teams and systemic risks)

System failure analysis is an overarching process that includes different techniques, which include fault tree, logic tree, fishbone diagrams, failure mode and effects analysis, etc. Fault tree analysis is just one tool that can be used in system failure analysis. With that said, this RP is intended to introduce the purpose and basic methods[1] of developing a fault tree, calculating the consequence for the failure of the overall system (called the *top event*) given the structure of the tree and the probability (P)[2] that the building block elements (called *gates* and *events*) occur, and identifying the most important sources of potential failure for inspection and action.

FTA is a deductive[3], top-down method aimed at analyzing the effects of initiating faults and events on a complex system and is defined as "a risk analysis method used to evaluate risk threats employing a deductive logic tree linking a parent event to the combinations of sub-events that could cause it." [1] A fault tree is not the same as an event tree[4] analysis. Fault trees assist project teams in examining undesired events, identifying the cause(s) leading to potential failures, and determining how to prevent them in the future.

Fault tree analysis necessitates a robust level of engineering that accurately represents events and their interactions. This requires an engineering framework that delineates basic events and their interactions, enabling the construction of the fault tree. Even in early partial designs, FTA can identify major causes of system failure, guiding engineering efforts to mitigate these issues, for example, by incorporating backup systems for failure-prone events.

The use of fault trees supports Sections 3.2 Asset Planning, 3.3 Investment Decision Making, 7.6 Risk Management, and 11.4 Quality and Quality Management in the *Total Cost Management Framework*. [2] Using the FTA methods described in this RP assists in asset planning. These planning efforts include the optimization, optioning, and value-engineering assessments of the equipment and systems. This further includes improving the quality of the design to

[1] Fault tree analysis can be quite complex, and therefore, this RP will only discuss the basics of performing the FTA. This RP does not discuss minimum path sets.

[2] P denotes probability.

[3] Deductive reasoning begins with a general statement and proves it with a logical conclusion. It is a thinking process that uses the top-down approach to go from the more general to the more specific. It involves using general assumptions and logical premises to arrive at a conclusion. Inductive reasoning moves from a specific observation to a broader and generalized conclusion. This approach uses induction mapping (brainstorming) and categorization. Failure mode and effects analysis is an example of an inductive reasoning tool.

[4] Event tree analysis (ETA), while similar in nature to fault tree analysis (FTA), focuses on the multiple circumstances that take place after the event occurs (lagging). FTA looks at leading causes. While both analysis types are failure tracing methods, they differentiate based on when the event occurred. In summary, FTA introduces preventative measures, while ETA introduces mitigation measures.

ensure the operability, reliability, and maintainability of the asset(s). Asset planning, value engineering, and quality management all support risk management functions. These efforts ultimately determine the lifecycle cost of the equipment, systems, etc., which supports the decision to invest[5] in the asset.

1.2. Background

System failure analysis aids project leaders in strategic decision-making, as well as in the design and production of systems and products, by enhancing their resistance to failure and improving the reliability and safety of the delivered outcomes. Implementing system failure analysis leads to more successful project results, whether these projects involve complex buildings with multiple interacting systems, products like airplanes or automobiles, process plants requiring high reliability and safety, or new equipment and instruments such as satellites, where repair may be impractical or impossible.

System failure analysis, using the application of fault tree analysis introduced in this recommended practice,

- Identifies the events, called cut sets, that can, by themselves or in combination, cause the project/system to fail to achieve the required level of quality, an imperative project objective.
- Computes the probability of system failure given the FTA structure and components' (*events occurring*) failure probability data.
- Leads to actions that will provide significant improvement in the reliability of the final product with more reliable components or redundancy to drive down the probability of failure events.

The Six Sigma Study Guide summarizes the background and general purpose of system failure analysis on their website: "Fault tree analysis (FTA) is a graphical tool to explore the causes of system level failures. It uses Boolean[6] logic to combine a series of lower-level events, and it is basically a top-down approach to identify the component level failures (basic events) that cause the system level failure (top event) to occur. Consider the top event as the feared event. Fault tree analysis consists of top events, *events* and *logic gates*, which connect the events to identify the cause of the top undesired event." [3]

The most useful aspect of FTA is that it provides a basic cause analysis technique that can help the user visualize and understand the relationships between different factors contributing to the failure. While there are many positives to using FTA, it does come with some challenges. With this said, the Six Sigma study guide [3] outlines some of the key advantages and disadvantages of using the FTA method.

Advantages of fault tree analysis:

- The fault tree visually depicts the analysis that will help the team to work on the cause of an event in a logical way that leads to failure.
- Highlights the critical components related to system failure.
- Provides an efficient method to analyze the system.
- Unlike other analysis methods, human errors are also included in the analysis.
- It helps to prioritize the action items to solve the problem.
- Provides qualitative and quantitative analysis.

[5] While this recommended practice (RP) does not address the feasibility of the identified solutions, it is important to note that project teams might be constrained in implementing the best preventative measures due to their associated costs. Therefore, it is crucial to carefully assess the organization's risk appetite regarding failure prevention..

[6] A fault tree is considered a pictorial representation of Boolean relationships between the fault events that cause the top event to occur. The fault tree can be translated into an equivalent set of Boolean equations. Therefore, an understanding of the rules of Boolean algebra is required as the probability of the failure is obtained from the equivalent Boolean equations. Simple examples are provided in this RP.

Disadvantages of fault tree analysis:

- There can be too many potential events and gates (relationships between events) to be considered for large system analysis.
- The primary disadvantage is that it examines only one top event.
- Common cause failures[7] are not always obvious.
- It is challenging to capture time-related and other delay factors.
- Experienced individuals are needed to understand the logical gates.

1.2.1. When Would FTA be Recommended for Use

Fault tree analysis can be used to perform all types of system-level risk assessment processes.[8] The purpose of FTA is to identify effectively the causes of system failure and mitigate the risks before it occurs. This is an invaluable tool for complex systems that visually display the logical way of identifying the problem. The analysis may also lead to identifying practical actions to increase the reliability of the system. This tool also assists in completing a reliability analysis. Reliability analysis plays a crucial role in the design process. The use of the FTA is essential to increase the reliability of a system. It is also one of the tools used for estimating the reliability of a system and, therefore, the life cycle achievement of rated performance and costs[9].

1.2.2. Context

As stated earlier, fault tree analysis helps organizations prevent, mitigate, or solve potential failures. The following statements are examples of where the use of FTA would have identified ways to mitigate the consequences of a failure before it happened or at least narrowed down the cause of a failure event. Using the FTA helps identify and eliminate risk and safety issues, prevent reputational damage, and save time and money.

The SAE (Society of Automotive Engineers) supports research into successful predicting of project performance, including reliability, quality, durability, safety, recalls, and profits of automobile companies worldwide. One measure of quality is the number of automobiles recalled for quality problems. Automobile failures contribute to accidents and even death, and one finding in 2014 was that "GM has recalled more than 18 million vehicles in the US since January 2014," which is threatening to undermine the company's reputation for quality. Further, SAE concludes that "The ability to predict in the systems-technical performance area is especially underdeveloped… (this) relates to the successful predicting of the performance components and new technology…. Reliable predicting of total product life cycle costs (is) crucial for the life cycle management of products… cannot be sufficiently determined through deterministic calculations due to the stochastic and the dynamic nature of the problems… The basic way for improving the above situation is to develop a predicting methodology and obtain accurate initial information for predicting specific product." [5]

[7] Common cause failures (CCF) represent a dependent failure in which two or more component fault states exist simultaneously or within a short time interval and are a direct result of a shared cause - Space industry (NASA PRA guide, 2002). Examples of CCFs for a mechanical system include abnormally high or low temperature, abnormally high or low pressure, stress above design limits, impact, and vibration. Environmental examples include earthquakes, tornados, floods, etc.

8 As indicated by the International Crisis Management Association, "Fault tree analysis is a top-down approach that was originally developed in Bell laboratories by H. Watson and A. Mearns for the Air Force in the year 1962. This concept, later adopted by Boeing, is widely today used in aerospace, automobile, chemical, nuclear and software industries, especially reliability and safety related events." [4]

[9] Life-cycle cost analysis is the process during which the project team assesses the cost of a plants, buildings, building materials, or pieces of equipment throughout its entire useful life. This in turn allows the project team to not only properly estimate the project costs, but also assist in determining operational costs (from start-up to refurbishment to replacement).

In a different context, the James Webb Space Telescope of NASA had many single points of failure (a fault that can by itself cause the project to fail. Such an event does not need to be paired with another event, such as a backup system fails, in part because there may be no backup system), all to be experienced before deploying (the heat shield) with a distributed system to be stationed a million miles away. "There are 344 single-point-of-failure items on average," Menzel[10] said about the Webb mission, adding that "approximately 80% of those are associated with the deployment (of the heat shield). It's hard to avoid when you have a release mechanism. It's hard to put full redundancy into that. We have what we call a critical item control plan, and we always throw in extra inspection points… And we've done extra offline testing on these devices," Menzel said. He added that for every one of these items identified, NASA and Northrop Grumman have done extra inspections and tests to understand the different ways that it could fail and to be as prepared as possible. "We've given our single-point-failure items a lot of attention." [6]

The presence of failure events on the James Webb space telescope affected the program dramatically in 2018. "Then, an independent review in 2018 found that a handful of human errors caused major delays and increased costs. The telescopic propulsion valves were damaged when engineers used the wrong solvent to clean them. Dozens of screws holding the telescope's giant sunshield were loosened during vibration tests. And during testing, the faulty wiring sent excess voltage to the observatory's transducer. The error should have been traced back to the inspector, who did not perform the inspection but relied on the technician's word that he did the wiring correctly,' the 2018 report said. There are fears that the test accidents will prompt NASA to raise its $8 billion development funding cap. The report said human errors cost the program $600 million and caused an 18-month delay." [7]

"Because of its relative complexity and detail, it is normally not cost effective to use the FTA against risks assessed below the level of extremely high or high. The method is used extensively in the acquisition of new weapons systems and other complex systems where, due to the complexity and criticality of the system, the tool is a must." [4]

2. RECOMMENDED PRACTICE

2.1. Introduction

An FTA is traditionally conducted to analyze the possible ways that a facility, product, or system may fail. Partial system failure is an *event*, whereas total system failure is the *top event*. The basic events that may produce the top event, by themselves or in combination with other events to cause total system failure, are called cut sets. Identifying cut sets provides an analytical calculation of the network's reliability and probability of occurrence. Reducing the probability of failure of the event is the main objective of FTA. The design of the system needs to be analyzed to identify the ways failure modes can cause system failures. Fault trees can be used, among other applications, to:

- Improve the reliability of the product deliverable by reducing the likelihood of events leading to failure or the consequence of its failure.
- Discover why a failure happened (e.g., as used by the National Transportation Safety Board (NTSB) investigation of a plane crash).
- Evaluate different competing designs from the perspective of possible failure while in use, identifying costs, profit, and reputational consequences if a failure occurs.
- Determine optimal maintenance and repair schedules.

Constructing a fault tree is a critical engineering task that involves linking system components to their impact on the system's availability. It requires modeling the sequences of events that lead to desired or undesired end states. This straightforward modeling approach begins with the initiation of an event, identifies the subsequent failure or success

[10] Michael Menzel is the NASA Mission Systems Engineer for the James Webb Space Telescope, at Goddard Space Flight Center, Greenbelt, Maryland.

of the system, and calculates the outcome of the final end state. Using the fault tree, the consequences can be predicted probabilistically, sources can be identified, and the design can be altered to either avoid or be engineered out of the system. Examples of the structure of the fault tree, including the layout of the events and logic gates, are provided in the following sections.

2.1.1. Failure Domain Structures

The definition of failure (and success) within an organization is dependent on its point of view. Whether it's a process plant, hospital, high-rise residential building, or infrastructure (bridges and roads), organizations (asset owners) will determine failure based on what is important to them to keep their operations going. In terms of operational excellence, it is a balance between maintaining, increasing, or reducing revenue. To achieve this balance, the organization will need to recognize the different types of factors that may impact the probability of failure, also known as modes of failure. These include:

- Mortality failure – the system physically fails and is unable to perform its functions.
- Capacity failure – the system is operational but is unable to achieve the required physical capacity needed or achieve its design capacity level in operation.
- External failure (level of service) – the system is unable to meet demand due to limited or elimination of an external service provider.

The factors described above create financial inefficiency by either increasing operational costs or depleting revenue streams. Organizations should examine the three failure modes to make informed judgments about the probability of failure across their respective operations.

With this understanding, organizations can proceed to clearly define what constitutes failure for them. This will be determined by their risk approach and decision-making policies. An organization's risk approach can be expressed by defining 1.) the level of risk the organization is willing to take on (risk appetite) to achieve its objectives and 2.) their acceptable deviation (risk tolerance) from those levels. [8] Defining the risk approach will guide the organization in making the appropriate decisions. For the FTA, risk appetites and risk tolerances need to be defined for its system(s). Please note that not all systems within an organization will carry the same appetites or tolerances, i.e., be critical to operations.[11]

To achieve this, organizations need to define the minimum anticipated probability of failure rate, the maximum anticipated probability failure rate, and the maximum tolerable probability failure rate for each of their systems (or subsystems, etc.). This provides direction to project teams when determining mitigation strategies to reduce failures of the system(s) they are designing and subsequently operating. Table 1 is an example that illustrates the listing of an organization's systems and their respective probability of failure.

[11] Critical operation is defined as a business output that, if interrupted during the operational period, will cause financial loss, damage, or interruption to the delivery of goods or services essential to the organization's continued operation or success. [17]

ID	System	Top Event	System Type	Critical	Minimum Anticipated PoF*	Maximum Anticipated PoF*	Maximum Tolerable PoF*	FTA
0001	System 1	Top Event A	Process	No	0.075	0.095	0.135	0.103
0002	System 2	Top Event B	Utility	No	0.029	0.055	0.085	0.051
0003	System 3	Top Event C	Process	Yes	0.025	0.048	0.085	0.098
0004	System 3	Top Event D	Process	Yes	0.025	0.048	0.085	0.041
0005	System 4	Top Event E	Utility	Yes	0.035	0.063	0.092	0.069
0006	System 5	Top Event F	Process	No	0.041	0.059	0.100	0.040

*Probability of Failure

Table 1: Probability of Failure Thresholds[12]

Another feature provided in the table above is the identification of system criticality. The table demonstrates that not all components are equally important to the organization; some systems are highly critical while others are not. Defining criticality assists the project team in measuring the risk associated with a component. Systems should be prioritized based on a criticality analysis to determine where an organization should focus its efforts, specifically in determining the probability of failure for a system. For instance, System 3 of Table 1 is considered critical. It was identified through an FTA that Top Event C (ID 0003) was beyond the maximum tolerable probability failure rate. Based on these findings, the project team can introduce measures to minimize the probability of failure for a critical system within their organization. The criticality of the system may be location-specific. Specific systems or components may be critical in one location but less critical in another.

Failure of an asset, system, or element depends on the measures that the organization implements. Selecting the correct pump is one element of the failure component; the quality program (e.g., maintenance) is the other. A good quality program will ensure that there is a planned balance of prevention, appraisal, and failure costs. If not, failure of the system or element will be inevitable. Organizations must examine the systems in their inventory to carefully determine which systems will fail and why.

2.1.2. Boundaries and Failure Type Considerations

Analyzing a system or partial system (and the elements within) for failure can be a complex undertaking. This analysis can be further compounded by factors outside of the project team's control. External factors and conditions create a boundary that separates the organization from the external environment in which it operates. Figure 1 illustrates the concept of boundaries. Boundary and system definition is critical as this establishes the extent of the analysis.

[12] Similar to estimating continency for a project, organizations should design the probabilities of failure that incorporate unexpected surges to their facility to create a more favorable outcome.