How Fault Tree Analysis is used to Increase Safety and Reliability

---

A Term Paper

Presented

to the Faculty of

California State University, Dominguez Hills

In Partial Fulfillment of

QAS 512.41

Reliability

Professor Daniel & Pamela Dunahay

Written by

Kenneth Eliazo

10 November, 2015

A REVIEW OF LITERATURE

In a consumer-driven world, industries are expected to provide a level of safety and reliability designed into their products or systems. Every day, consumers vote with their dollar to the product they believe is the most reliable and durable on the market. In response, industries are responsible for providing quality products through constantly monitoring safety and reliability. This can be done by gathering and analyzing data along with continuously improving processes to meet consumer expectations. The consumer's perception of the quality of a company greatly impacts their reputation. During the current state of the legal system, it is standard for manufacturers to be responsible for the product safety and reliability. These standards cause the engineers to be mainly responsible for the design of product to include safety and reliability as criteria (Ebeling, 2010, p.2). Safety and reliability is the paramount goal for industries that wish to achieve a quality reputation among its peers and customers. Various tools, techniques and methodologies have been developed to aid in this goal. They exist to capture how potential hazards or failures occur in a product or system and how to eliminate or mitigate it to prevent mishaps or possible accidents. They minimize risk and maximize safety and reliability for the consumer. These methods prove to be an invaluable tool for safety analysts, reliability engineers and risk assessors whose jobs are to constantly seek a way to design safe and reliable products and systems, while continuing to improve its processes.

One important tool that is used across different industries is known as Fault-Tree Analysis (FTA). Fault tree analysis is a visual representation of a system that uses symbols to model the different combinations of failures, faults, errors and normal events that cause an undesired event (UE) to occur. Mathematics is used to take the events and calculate the probabilities of the failures along the tree leading up to the UE (Ericson, 2011, p.i). FTA allows safety engineers to focus on one undesired event and breakdown individual related events leading up to it. It makes it easier to visualize the different combinations of potential component failures. FTA helps engineers create a diagnostic for the system or process. It allows the analyst to consider many individual failures, different combinations of the interactions between them, and how to prioritize the elimination or mitigation of them.

Designing a fault tree involves both inductive reasoning and mathematical deductive reasoning. Preparing the structure of the fault tree gathers evidence in order to support the truth of the conclusion, which is the undesired event. Symbols describe individual failure components as event symbols. Events could exist independently of each other or in groups dependent on one another. Dependent events determine outcomes up the tree. Relationships between event symbols are depicted as gate symbols, where it denotes if the events are independent or dependent on one another. The combination of event and gate symbols illustrates the potential situations that occur in the system leading up to the UE. An engineer that is experienced with the system is required due to their knowledge of how a system works. Their knowledge is invaluable to get an accurate representation of the fault tree.

Evaluating a fault tree is deductive. It is deductive because the analysis starts with an identified system failure and deduces back to the original cause through considering primary independent faults (Zio, 2007, p.115). Every fault is assigned a probability. As you work through the tree, depending on how events are related, probabilities are computed using reliability mathematics. Probabilities provide a quantitative value for every event in the fault tree. Quantitative analysis of an undesired event is vital because it assigns a magnitude to every failure, individually or compounded with other factors. It gives the engineer a way to assess the importance of different events, and helps them prioritize them. In this manner, an engineer can assess which safety failures are more important to address than others. An error with a higher probability of failure will get more attention than one with a lesser probability. This also aids in the cost efficiency of the analysis, as the company cannot afford the time or money to consider all the failures at once. Fault Tree Analysis gives the safety and reliability engineers a powerful tool in prioritizing system failures.

Besides honing in on failure of products and systems after-the-fact, safety and reliability engineers also use FTA to proactively design safe products or system before failures occur. Fault tree analysis helps the analysts in the design phase of a product by identifying all possible failure events that can lead to an identified failure and focusing on fixing them (Juran & De Feo, 2011, p.117). FTA provides a model that is predictive by utilizing both inductive method and deductive method making it useful for probabilistic risk assessment (PRA) and design assessment. FTA considers external factors that may affect the process or system, in addition to the internal factors, when it comes to the

design phase of a product or system. Also, FTA helps design output/lower level requirements and determines how to minimize and optimize resources. Fault tree analysis meets many goals in order to aid the engineer in decision-making for the design of products and systems.

Fault tree analysis has been implemented by several industries, including: aerospace, nuclear power, chemical, pharmaceutical, medical device, petrochemical, and software industries. FTA is a standard in hazard analysis for many industries; it is a tried-and-true technique that has proven to work in reducing failure in product and system failure. As FTA continues to develop and evolve with new technology and software, its uses are expanding capabilities and applications. It has become more efficient and user-friendly for budding safety and reliability engineers. It is as relevant and useful now as it was when it was first developed.

History

The early concepts of the Fault Tree Analysis were conceived in 1961. H. A. Watson and A. B. Mearns of Bell Laboratories were responsible for birthing the idea of fault tree analysis. They sought to perform a safety study on the Minuteman Launch Control System for the U.S. Air Force. Their goal was to design a safe launch control system (Ericson, 2011, p.123). The study proved to be very effective and it soon evolved into a formal methodology for accomplishing design safety. This new FTA methodology would continue to change the way safety is designed into systems in the following decades.

FTA was recognized as an effective safety system design tool at the Boeing Company. A Boeing employee named Dave Haasl led a team that applied FTA on the Minuteman Missile System. This was an opportunity to correct such undesired events as "inadvertent programmed launch" and "inadvertent motor ignition". FTA was able to quantitatively pinpoint the acceptable risk levels for these potential accidents (Ericson, 2011, p.123). For Dave Haasl, fault tree analysis was vital in creating the Minuteman Missile system. The innovation was so vital for Boeing and Dave Haasl saw it was necessary to develop the concepts of FTA further. He went on to lead a group of engineers and scientists in writing the NUREG-0492, which is the first publication on FTA. This publication is treated as an unofficial FTA reference standard. The more prevalent FTA became for Boeing, the more they felt the need to share it with other industries.

The Boeing Company noticed the effectiveness of FTA on the Minuteman program which prompted them to begin using FTA on designing commercial aircraft. The first System Safety Conference was held in Seattle, Washington, hosted by Boeing and the University of Washington, in 1965. The first-ever papers were presented on FTA, at this conference. This was the beginning of worldwide notoriety on the subject of FTA (Ericson, 2011, p.123). In 1966, computer software related to fault tree analysis was developed. A fault tree simulation program called BACSIM (Boeing Aerospace Corporation Simulation) was created for the evaluation of multi-phase fault trees. This simulation was well ahead of its time, and set the pace for computer software

development in the future. Software played an expansive role in the capabilities of analyzing safety measures.

The aerospace industry paved the path for other industries to follow suit. As the world was attuning to the ideas of FTA, the nuclear power industry discovered its benefits for their practices. They began using FTA for planning and developing nuclear power plants. The nuclear power industry furthered the ideas of FT theory and FT algorithms and computer programs (Ericson, 2011, p.123). Facilitating the evolution of fault tree analysis, the nuclear power industry was responsible in the development of various software for fault tree evaluation, such as: MOCUS, Prepp/Kitt, SETS, FTAP, Importance and COMCAN. These computer software were the foundation for the development of current software. The advent of computer evaluation of fault trees makes it easier and more efficient for the safety engineer to analyze systems.

Theoretical Foundations

Fault tree analysis begins with the identification of an undesired event (UE). According to the Fault Tree Handbook, fault tree analysis focuses on one particular undesired event (UE) which provides a method for determining causes of this event (Vesely, Goldberg, Roberts & Hassl, 1981, p.III-3). The UE is placed at the top of the tree, and subsequent events that led up to the UE are identified. UE identification needs to be just right for the analysis to be effective. If it is too general, the range of events will be too broad for the analysis to be efficient. If it is too specific, the analysis may exclude important aspects of the system. FTA takes time and money for the analysis to be carried

out; the cost of FTA must make sense when compared to the cost of the UE. An undesired event that is related to safety makes FTA the most cost efficient. "A UE is an event, or potential event, that is unwanted because of its undesirable safety consequence" (Ericson, 2011, 28). Some examples of an undesired event for a fault tree analysis are:

1) Brakes on a car lock.
2) Electrical heater produces sparks when plugged in too long.
3) Car engine explodes into fire when rear ended.
4) Bridge collapse.
5) An airplane crash with loss of several hundred lives.

Once the UE has been identified, the potential causes or events need to be assigned to the UE. There are different symbols used depending on the type of event and how events relate to one another. Also, there are symbols for the outcomes of each event and or collection of events. There are three basic building blocks of FTA that go into the construction of the diagram. They fall into the following categories:

1) Basic Events – individual components or subsystems that cause a system to go from operational to non-operational; individual events that make the undesired event true.
2) Logic (Gate) Events – how the basic events are logically combined as fault paths that develop through the system. Outcomes of a collection of basic events or inputs.

3) Transfers – indicates where in the tree a branch is used in another location on the same fault tree.

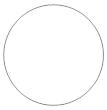
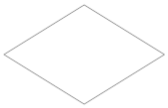
Type	Symbol	Description
Text Box		The rectangle contains the text for all FT nodes. Text goes in the box, and the node symbol goes below the box.
Primary Failure		The circle represents the primary failure mode of a component; a component failure that cannot be further defined in detail.
Secondary Failure		The diamond represents a failure that is induced by an external event or failure. It also represents a failure mode that could be developed in more detail if desired.
Normal Event		The house represents an event or action that is expected to occur as part of normal system operation.

Table 1. Fault Tree Analysis Basic Event Symbols. Adapted from *Fault Tree Analysis Primer*, by C. A. Ericson II, 2011, p.15.

Type	Symbol	Description
AND Gate		The output occurs only if all the inputs occur together.
OR Gate		The output occurs only if at least one of the inputs occurs.
Priority AND Gate		The output occurs only if all of the inputs occur together, and in a priority order. The priority statement is contained in the attached condition symbol.
Exclusive OR Gate		The output occurs if either of the inputs occurs, but not both. The exclusivity statement is contained in the attached condition symbol. Disjoint events.
Inhibit Gate		The output occurs only if the input event occurs and the attached condition is satisfied.

Table 2. Fault Tree Analysis Gate Symbols. Adapted from *Fault Tree Analysis Primer,* by C. A. Ericson II, 2011.

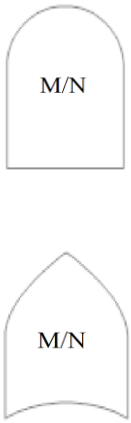
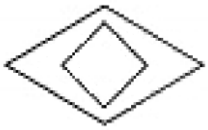
Type	Symbol	Description
M of N Gate		Symbols used to show M of N combinations of inputs causing the output to occur. Also known as Voting gate.
Double Diamond		A symbol that can be used to define a special type of event, as needed.
Internal Transfer		Indicates where a branch or sub-tree is marked for repeated use elsewhere in the current FT.

Table 3. Additional Fault Tree Analysis Symbols. Adapted from *Fault Tree Analysis Primer,* by C. A. Ericson II, 2011.

In addition to FTA symbols, there are terminologies that an analyst needs to understand as they develop a discipline in the methodology. Some of the commonly used terms are, as defined by Ericson (2011, p.19-28):

- Critical Path – is a fault tree path that has the highest probability.

- Cut Set (CS) – A unique set of events that together cause the fault tree top undesired effect to occur.
- Failure – is the inability of an item (e.g. system, subsystem, component or part) to perform its required functions within specified performance requirements.
- Fault – is the occurrence, or existence, of an undesired state of an item; an undesired anomaly in the functional operation of a system, subsystem, component, item or part.
- Intermediate Event (IE) – any gate node in the fault tree, other than the top gate and the bottom gate levels.
- Minimal Cut Set (MinCS or MCS) – Cut set that has been reduced to the minimum number of events that cause the top UE to occur. The CS cannot be further reduced and still guarantee occurrence of the top UE.
- Multiple Occurring Branch (MOB) – a fault tree branch that occurs in more than one place.
- Multiple Occurring Event (MOE) – is the same unique fault tree event that occurs in multiple places.
- Probabilistic Risk Assessment (PRA) – a quantitative evaluation that is performed to determine the probabilistic risk associated with an event.
- Reliability – is the probability that a device will perform its intended function, without failure, during a specified period of time under stated conditions.

- System – a group of individual elements that interact and function together as a whole.

The evaluation of fault tree analysis is predicated on three mathematical disciplines: 1) Probabilistic Mathematics (Probability), 2) Boolean Algebra, 3) Reliability Mathematics. Probability is assigned to each logic gate and/or event. Boolean algebra resolves cut sets and reduces them to simplify a FTA. Reliability mathematics establishes the component probability of failure. An understanding of all three is needed for fault tree evaluation.

Probability theory is used to calculate the likeliness of failure for each fault tree gate, including the top gate. One way to calculate the top gate is to start at the bottom and move towards the top. Each gate probability is calculated along the way. Another way to calculate the top fault tree probability is to segregate the minimal cut sets (CSs) and add them together. When MOEs and MOBs are present in the fault tree, probability theory is not applicable. MOEs are calculated by simplifying the FTA through reduction. This is achieved by using Boolean algebra.

	Rule Statement
R1	The probability of an event is between 0 and 1; $0 \leq P(E) \leq 1$
R2	If an event is certain to occur, then P(E) = 100% = 1.0 If an event is certain not to occur, then P(E) = 0% = 0
R3	It is certain that an event will either occur or not occur, therefore P(E + not E) = P(E) + P(not E) = 1 or P(not E) = 1 – P(E)
R4	The additive property of two probabilities is: a) If two events are disjoint (i.e., both cannot happen) P(E1 *or* E2) = P(E1) + P(E2) b) If two events are non-disjoint (i.e., they can occur together

	P(E1 *or* E2) = P(E1) + P(E2) – P(E1xE2)
R5	The multiplicative property of two probabilities is: a) If two events are mutually independent P(E1 *and* E2) = P(E1) x P(E2) b) If two events are not mutually independent (interdependent) P(E1 *and* E2) = P(E1) x P(E2) = P(E2) x P(E1|E2)

Table 4. Laws of Probability. Adapted from *Fault Tree Analysis Primer*, by C. A. Ericson II, 2011.

Boolean algebra is the mathematics of events and logically depicts the outcome of situations, which are represented by various symbols. Boolean algebra and probability theory are used together to generate a list of CSs from the fault tree failure events and gate events. Boolean reduction of the fault tree is achieved by applying the laws of Boolean algebra. Reduction of CSs is important to simplify a FTA, making the analysis more manageable, more efficient and less repetitive. Below is a table displaying axioms and theorems of Boolean algebra; the most used in FTA are indicated by an X.

	Axiom/Theorem	FTA
A1	ab = ba	X
A2	a + b = b + a	X
A3	(a + b) + c = a + (b + c) = a + b + c	
A4	(ab)c = a(bc) = abc	
A5	a(b + c) = ab + ac	
T1	a + 0 = a	
T2	a + 1 = 1	
T3	a x 0 = 0	
T4	a x 1 = a	
T5	a x a = a	X
T6	a + a = a	X
T7	a x not a = 0	
T8	a + not a = 1	
T9	a + ab = a	X
T10	a(a + b) = b	X
T11	a + (not a)(b) = a + b	

Table 5. Boolean Algebra Axioms and Theorems. Adapted from *Fault Tree Analysis Primer,* by C. A. Ericson II, 2011.

Reliability mathematics is used to calculate the probability of failure every event and subsystem. Most reliability models exhibit an exponential curve and probability is calculated as: $R = e^{-\lambda t}$. Where λ equals the reciprocal of Mean Time Between Failure (MTBF) and *t* equals at what time the probability is measured. There are other models that distribute the failure rates differently such as logarithmic and Weibull distributions. These require a different calculation of probability. The probability of failure depends on the configuration of the system or subsystem. For example, when a sub-system has components arranged in series to each other, the component's probabilities are multiplied together:

$$R = \prod_{i=1}^{n} Ri$$

When a sub-system has components arranged in parallel to each other, the components are calculated differently:

$$R = 1 - \prod_{i=1}^{n} (1 - Ri)$$

An understanding of reliability mathematics is the beginning of fault tree evaluation and is the glue that makes the effectiveness of fault tree analysis possible.

Process and Construction of a Fault Tree Analysis

The process of constructing a fault tree analysis begins with the analyst understanding the system design and operation before the analysis is begun. "Actual construction of fault trees is an art as well as a science and comes mainly through experience" (Zio, 2007, p.126). Experienced engineers that have extensive knowledge of the system works are usually the ones who handle the risk assessment, as their familiarity enables them to readily identify potential causes of failure. They can easily define the system. The following is a general procedure outlined in *Hazard Analysis Techniques for System Safety* by Ericson (2005, p.189):

1) Define the system: Understand system design and operation. Acquire current design data (drawings, schematics, procedures, diagrams, etc.).
2) Define Top Undesired Event: Descriptively define problem and establish the correct undesired event for the analysis. Engineer with wide knowledge of design or System Analyst with engineering background are consulted to define number of events. Obtain an understanding of the system – All causes with probabilities of affecting undesired event.
3) Establish Boundaries: Define analysis ground rules and boundaries. Scope the problem and record all ground rules.
4) Construct Fault Tree: Follow construction process, rules and logic to build FT model of the system. After selecting event + analyzed system, we know all the causing effects (and probabilities).

5) Evaluate Fault Tree: Generate cut sets and probability. Identify weak links and safety problems in the design. Study the risk management/find ways for system improvement.
6) Validate Fault Tree: Check if the FT model is correct, complete, and accurately reflects system design.
7) Modify Fault Tree: Modify the FT as found necessary during validation or due to system design changes. After identifying the hazards all possible methods are pursued to decrease the probability of occurrence.
8) Document the Analysis: Document the entire analysis with supporting data. Provide customer product or preserve for future reference.

Cut sets are important to emphasize. "CSs are identified as a unique set of events that, together, can cause the top UE or the fault tree to occur" (Ericson, 2011, p.20). Cut sets are very important because they highlight main pathways that are making the system fail. CSs make fault tree analysis easier. Large complex fault trees are difficult to decipher just by looking at it. CSs allow us to breakdown a complex fault tree into smaller sub-components. Analysts are able to hone in on the main events that are causing the undesired event at the top of the tree. Personal computer software is available to help the analyst to derive minimal cut sets, which lets the analyst efficiently risk assess. Software used in industries are: MOCUS, Prepp/Kitt, SETS, FTAP, Importance and COMCAN.

FTA Relationship with FMEA

FTA is not 100% sound in answering all the safety and reliability issues in products and systems. FTA is not without its weaknesses and disadvantages. We know that some of the advantages of FTA include: the ability to focus on one failure at a time, overall graphic visualization of a system, and identifying critical failure components through cut sets and software evaluation. Some disadvantages of FTA include: the methodology requires an analyst with experience of the system, it can be time consuming if the analyst is not careful, and it can become the main goal instead of just a tool to solve an errors. To strengthen a safety profile, other tools can be used to compliment FTA.

A methodology often paired with FTA is Failure Mode Effects Analysis (FMEA). Both FMEA and FTA are used to achieve the same goal of the elimination and mitigation of failures and errors in systems. Both were developed in the aerospace and nuclear power industries. Both are used as risk-assessment tools to increase safety and reliability. The differences between the two compensate for each other's weaknesses, making the combination more a sounder risk-assessment tool. "FMEA is an inductive process, while FTA is primarily a deductive process" (Wilhelmsen & Ostrom, 2012, p.227). FTA focuses on deducing from the undesired event, at the top of the tree, and works its way down to potential causes stemming from contributing sub-systems or components. It breaks down complex systems into simpler individual events. FMEA is an inductive method that starts by considering factors that go into the system, in other words from the

opposite end of where FTA starts. By using both approaches, we can find identify failures that one method may potentially miss. Both FTA and FMEA are part of what is called a Probabilistic Risk Assessment (PRA). Probabilistic Risk Assessment combines FTA and FMEA to provide a more complete picture for industries to measure safety and reliability. "The reason to perform a risk assessment is to demonstrate safety to both the workers and the public, as well as, save cost by utilizing available funds in the most efficient manner" (Wilhelmsen & Ostrom, 2012, p.229). FTA is flexible and can be combined with other tools, which adds to its effectiveness in risk assessment. Safety engineers can deploy FTA along with numerous other resources to ensure their industry is meeting consumer standards.

Today, consumer expectations are becoming more specific and demanding. The pace of industries is heightening as standards are being raised. Fault tree analysis is at the forefront of the ever-changing world of safety and reliability. It can prevent failures in products and systems; from minor annoyances to major catastrophes. It is a valuable tool that gives companies confidence that their products and systems are behaving as they should. Advancing technology and developing software dedicated are utilizing algorithms to deduce sources of failures. Industries are improving FTA proactively in the name of quality. Safety engineers are well in control of meeting consumer's safety and reliability expectations. Fault tree analysis is proof that human ingenuity can prevent and overcome human errors.

References

Ebeling, C. E., (2010). *An Introduction to Reliability and Maintainability Engineering.* Long Grove, Illinois: Waveland Press, Inc.

Ericson II, C. A. (2005). *Hazard Analysis Techniques for System Safety.* Hoboken, New Jersey: Wiley-Interscience. Retrieved from http://torofind.csudh.edu/

Ericson II, C. A. (2011). *Fault Tree Analysis Primer*. Charleston, North Carolina: CreateSpace Inc.

Juran, J. M. & De Feo, J. A. (2011). *Juran's Quality Handbook* (6th ed.). New York, New York: McGraw Hill Education. (Juran & De Feo, 2011)

Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). *Fault Tree Handbook.* (Publication No. NUREG-0492). Washington, D. C.: U.S. Government Printing Office. Retrieved from http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/

Wilhelmsen, C., & Ostrom, L.T. (2012). *Risk Assessment: Tools, Techniques, and Their Applications.* Somerset, NJ: John Wiley & Sons. Retrieved from http://www.ebrary.com

Zio, E. (2007). *An Introduction to the Basics of Reliability and Risk Analysis*. Singapore: World Scientific Publishing Company. Retrieved from http://torofind.csudh.edu/