

# Fault Tree Analysis

## Goal

---

This training program will introduce the basics of Fault Tree Analysis (FTA).

## Objective

---

The individual will demonstrate understanding of Fault Tree Analysis principles.

## Background

---

Engineers developed FTA to improve the safety of missile systems. They reasoned most accidents/incidents result from failures or malfunctions within a system. A system consists of people, equipment, material, and environmental factors. This system performs specific tasks using prescribed methods. The components of a system and its environment are interrelated, and a failure in any part can affect the other parts.

A negative event can be a near miss or an incident that could have resulted in personal injury to an employee or equipment/property damage.

## Analytical Trees

---

Analytical trees are graphic representations or pictures of a project or event. They use deductive reasoning in that they start with a general top event or output event and develop down through the branches to specific input events that must occur in order for the output to be generated. Analytical trees are called trees because their structure resembles a tree, narrow at the top with a single event symbol and then branching out as the tree is developed.

## Fault Trees

---

Negative analytical trees or fault trees are excellent troubleshooting tools. They can be used to prevent or identify failures prior to their occurrence, but are more frequently used to analyze accidents or as investigative tools to pinpoint failures. When an accident or failure occurs, the root cause of the negative event can be identified.

Each event is analyzed by asking, "How could this happen?" In answering this question, the primary causes and how they interact to produce an undesired event are identified. This logic process continues until all potential causes have been identified.

Throughout this process, a tree diagram is used to record the events as they are identified. Tree branches stop when all events

leading to the negative event are complete.

Symbols are used to represent various events and describe relationships:



**And gate** - represents a condition in which all the events shown below the gate (input gate) must be present for the event shown above the gate (output event) to occur. This means the output event will occur only if all of the input events exist simultaneously.

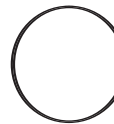


**Or gate** - represents a situation in which any of the events shown below the gate (input gate) will lead to the event shown above the gate (output event). The event will occur if only one or any combination of the input events exists.

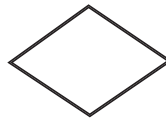
There are five types of event symbols:



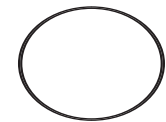
1. **Rectangle** - The rectangle is the main building block for the analytical tree. It represents the negative event and is located at the top of the tree and can be located throughout the tree to indicate other events capable of being broken down further. This is the only symbol that will have a logic gate and input events below it.



2. **Circle** - A circle represents a base event in the tree. These are found on the bottom tiers of the tree and require no further development or breakdown. There are no gates or events below the base event.



3. **Diamond** - The diamond identifies an undeveloped terminal event. Such an event is one not fully developed because of a lack of information or significance. A fault tree branch can end with a diamond. For example, most projects require personnel, procedures, and hardware. The tree developer may decide to concentrate on the personnel aspect of the procedure and not the hardware or procedural aspects. In this case the developer would use diamonds to show "procedures" and "hardware" as undeveloped terminal events.



4. **Oval** - An oval symbol represents a special situation that can only happen if certain circumstances occur. This is spelled out in the oval symbol. An example of this might be if switches must be thrown in a specific sequence before an action takes place.



5. **Triangle** - The triangle signifies a transfer of a fault tree branch to another location within the tree. Where a triangle connects to the tree with an arrow, everything shown below the connection point transfers to another area of the tree. This area is identified by a corresponding triangle that is connected to the tree with a vertical line. Letters, numbers or figures identify one set of transfer symbols from another. To maintain the simplicity of the analytical tree, the transfer symbol should be used sparingly.

# Fault Tree Analysis

FTA involves the following steps:

1. Define the top event.
2. Know the system.
3. Construct the tree.
4. Validate the tree.
5. Evaluate the tree.
6. Study tradeoffs.
7. Consider alternatives and recommend action.

**Define the top event.** To define the top event the type of failure to be investigated must be identified. This could be whatever the end result of an incident may have been, such as a forklift overturning.

**Determine all the undesired events in operating a system.** Separate this list into groups having common characteristics. Several FTAs may be necessary to study a system completely. Finally, one event should be established representing all events within each group. This event becomes the undesired event to study.

**Know the system.** All available information about the system and its environment should be studied. A job analysis may prove helpful in determining the necessary information.

**Construct the fault tree.** This step is perhaps the simplest because only the few symbols are involved and the actual construction is pretty straightforward.

**Principles of construction.** The tree must be constructed using the event symbols listed above. It should be kept simple. Maintain a logical, uniform, and consistent format from tier to tier. Use clear, concise titles when writing in the event symbols. The logic gates used should be restricted to the and gate and or gate with constraint symbols used only when necessary. An example would be the use of the oval constraint symbol to illustrate a necessary order of events that must happen to have an event occur. The transfer triangle should be used sparingly if at all. The more the transfer triangle is used, the more complicated the tree becomes. The purpose of the tree is to keep the procedure as simple as possible.

**Validate the tree.** This requires allowing a person knowledgeable in the process to review the tree for completeness and accuracy.

**Evaluate the fault tree.** The tree should then be scrutinized for those areas where improvements in the analysis can be made or where there may be an opportunity to utilize alternative procedures or materials to decrease the hazard.

**Study tradeoffs.** In this step, any alternative methods that are implemented should be further evaluated. This will allow evaluators to see any problems that may be related with the new procedure prior to implementation.

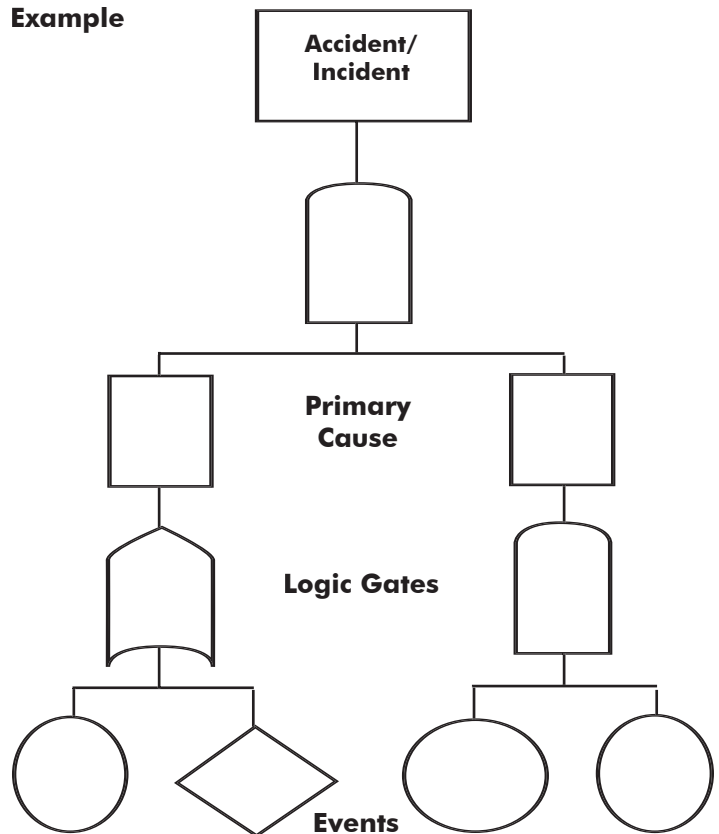
**Consider alternatives and recommend action.** This is the last step in the process where corrective action or alternative measures are recommended.

## Example

**Benefits:** The primary advantages of fault tree analyses are the meaningful data they produce which allow evaluation and improvement of the overall reliability of the system. It also evaluates the effectiveness of and need for redundancy.

**Limitation:** A limitation of the fault tree analysis is that the undesired event evaluated must be foreseen and all significant contributors to the failure must be anticipated. This effort may be very time consuming and expensive. And finally, the overall success of the process depends on the skill of the analyst involved.

### Example



## Resources

---

The Texas Department of Insurance, Division of Workers' Compensation (TDI/DWC) Resource Center offers a workers' health and safety video tape library. Call (512) 804-4620 for more information or visit our web site at [www.tdi.state.tx.us](http://www.tdi.state.tx.us).

Disclaimer: Information contained in this training program is considered accurate at time of publication.

## Review Questions

---

1. What is meant by the term "negative event?"
  - a. A political rally for a negative candidate.
  - b. A near miss, or accident that results in personal injury or property damage.
  - c. An automobile race where all the vehicles drive in reverse.
  - d. A series of events that if there are two together they will actually make a positive event.
2. What is a benefit of the fault tree analysis?
  - a. It offers shade on a sunny day.
  - b. You can determine the amount of money it will cost to implement a procedure.
  - c. You will get meaningful data about the overall reliability of the system.
  - d. It takes little time and expense to create.
3. What does the circle symbol used in the formation of the tree represent?
  - a. The negative event that will be studied.
  - b. The transfer of a branch to another location on the tree.
  - c. A terminal event that doesn't need to be developed further.
  - d. A base event with no events below it.
4. What was the fault tree analysis created to do?
  - a. To evaluate the production of baked goods.
  - b. To increase the safety level of the space program.
  - c. To improve the safety of missile systems.
  - d. To illustrate how to safely set up a Christmas tree.
5. A fault tree analysis should be as complicated as possible. T/F

5. F The purpose of the fault tree analysis is to illustrate a procedure or event in a way that can be visualized and if it is complicated, it will no longer be an effective tool.

1. B  
2. C  
3. D  
4. C  
5. F

**Quiz Answers**

The Texas Department of Insurance,  
Division of Workers' Compensation (TDI/DWC)  
E-mail [resourcecenter@tdi.state.tx.us](mailto:resourcecenter@tdi.state.tx.us)  
or call 1-800-687-7080 for more information.

*Safety Violations Hotline*  
**1-800-452-9595**  
[safetyhotline@tdi.state.tx.us](mailto:safetyhotline@tdi.state.tx.us)