Safety

Safety engineering efforts are normally worked in unison with reliability engineering activities. The reliability engineering activities include FMECA and RCM. These analyses can be used to support various safety engineering tasks. Listed are an examples of the types of safety analyses which would use the reliability engineering analysis. A safety engineering program could be set up following Mil-Std-882 System Safety Program Requirements.

- Hazard Analysis
- Fault Tree
- Sneak Circuit Analysis

Hazard Analysis

Hazard Analyses is a technique which by qualitative or quantitative analysis is used to identify hazards, their causes and effects. The hazard elimination, or risk mitigation would be documented in the hazard analysis. This analysis can be conducted to identify hazard associated with the system, subsystem, components, personnel, ground support equipment, GFE, facilities, and take into consideration their interrelationship and impact with the logistic support, training, maintenance, and operational environments.

Fault Tree Analysis

A Fault Tree Analysis, contrary to the FMECA, is a top-down analysis. It takes on a deductive approach defining the events and sub-event, which may cause the top event to occur. The relationship between these events is governed by their logical relationship to each other. The level that the deductive approach could be taken down to is a basic event. These basic events can be the failure modes of components or functions, as identified in the FMECA. Other factors can also be taken into consideration in the development of the fault tree.

The fault tree can be represented in a qualitative or quantitative manner. The qualitative would provide the illustrated or graphical relationship of the top event and all of its subordinate events and their basic events. Whereas the quantitative would also include "probability of occurrence" of all events rolled up to the top event. The probability of occurrence can be expressed in Boolean algebra. Therefore the laws apply where in some cases the Boolean expression could be simplified. This would simplify the actual calculation of the final end event.

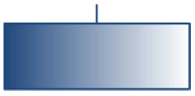
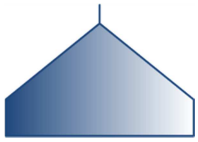
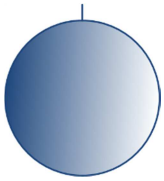
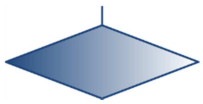
Contact email: info@mtain.com

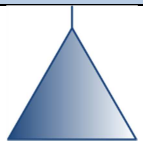
The simplification of the whole Boolean algebra expression would be important where, for example a basic event (know failure mode) appeared in more than one location (branches) in the fault tree. For complex fault trees the use a dedicated software program to build and run the calculations would be warranted.

In constructing a fault tree special attention must be made to the logical relationship between the events. It could be easy to have two or more events flowing into an OR gate when in fact the gate should be an AND gate. This building of a fault tree can be further complicated by a system's redundant elements and characteristics.

Fault Tree Analysis Symbols

The following is a summary of the common symbols used in a fault tree development.

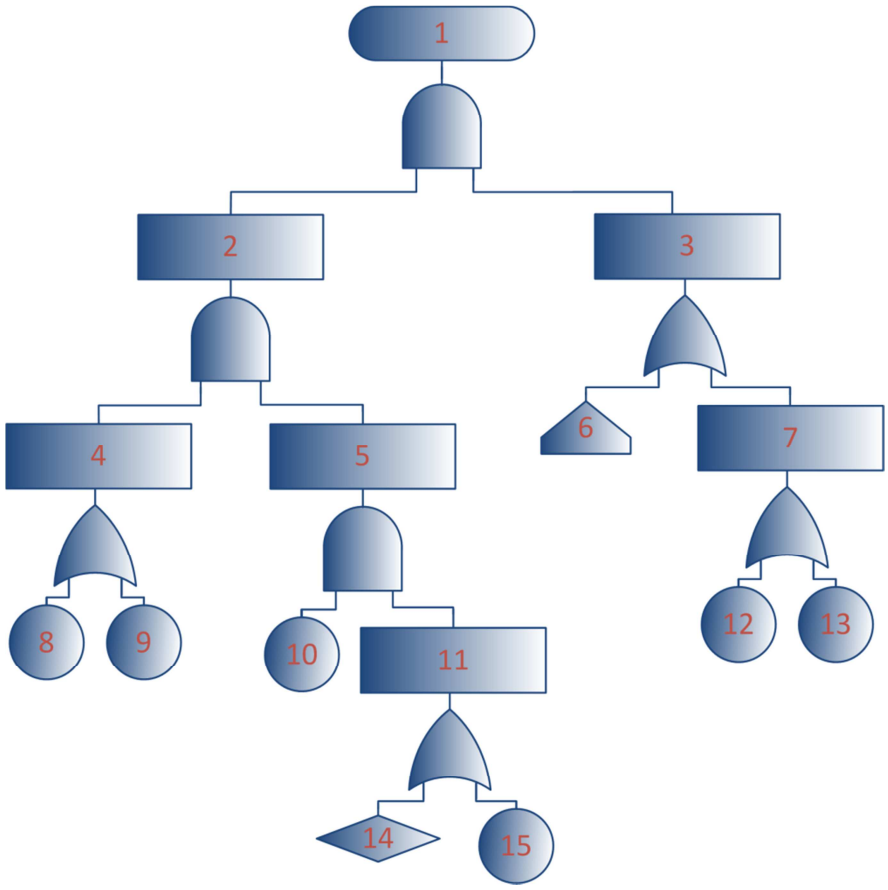
Symbol	Symbol Description
	**Top Event:** This symbol represents the end event that is being considered in the Fault tree Analysis.
	**Fault Event:** This block contains a description of the logical result of lower events.
	**House Event:** This represents a system operation condition, that could in the normal sequence of events cause a state change in the logic.
	**Basic Event:** This represents an event at the lowest level of the system under examination. This event could be a failure mode as identified in the Failure Modes and Effects Criticality Analysis (FMECA).
	**Undeveloped Event:** This symbol represents a condition that cannot or has yet to be developed further.
	**Transfer Function:** These symbols "transfer out" and "transfer in" represent a connection between two (or more) points in the fault tree. This can be used to minimize the duplication of an developed branch in the fault tree.

Symbol	Symbol Description
	
	**AND Gate:** An output will occur when all inputs are present thus for a two input gate A and B = output.
	**OR Gate:** An output will occur when either one or all inputs are present, thus for a two input gate A or B = output.
	**Ordered AND Gate:** Similar to the AND Gate, but the inputs must occur in a specific sequence.

Contact email: info@mtain.com

Fault Tree - Example

This is a simple example of how a fault tree could be represented. In this example it illustrates the qualitative approach to the "End Event" in question. A quantitative result could be derived by determining the probabilities of the each event and developing the Boolean expression.



1. Cargo Bay Opens	10. "Hold Off" relay fails shorted
2 .Failure of the Control Logic	11. "Hold Off" relay prematurely energized
3. Failure of the Command Logic	12. Switch (SW1) Fails short circuit (see Failure Mode 12.A4.009
4. Control Circuit "A" Fails	13. Switch (SW2) Fails short circuit (see Failure Mode 12.A4.019)
5. Control Circuit "B" Fails	14. Software error (not developed)
6. Operator Depresses "Open" Button	15. "Hold Off" relay logic fails Hi (see Failure Mode 14.B4.019).
7. Failure of the Command Logic Switch circuitry	
8. Inhibit "A" "open" Logic Function fails low (see Failure Mode 11.A3.017)	
9. Inhibit "B" "open" Logic Function fails low (see Failure Mode 11.A6.017)	

Contact email: info@mtain.com