

Fault Tree Analysis

Table of Contents

Introduction	3
Fault Tree Analysis	3
Basic Events	4
Advantages	4
Limitations	4
Notation.....	5
General Procedure for Fault Tree Analysis.....	6
Rules of Fault Tree Construction	7
Considerations.....	11
Fault Tree Evaluation	12
Boolean Algebra	12
<i>The OR Gate</i>	12
<i>The AND Gate</i>	12
Qualitative Analysis	14
<i>Minimal Cut Sets</i>	14
<i>Criticality</i>	14
Quantitative Analysis.....	16
<i>Common-Cause Failures</i>	16
References.....	18

Introduction

- there is a need to analyze all the possible **failure** mechanisms in complex systems (e.g. nuclear power plants)
- also perform probabilistic analyses for the expected rate of failures
- estimate probabilities of events that are modelled as logical combinations or logical outcomes of other random events
- two main methods:
 - **fault tree** analysis
 - **event tree** analysis
- **decision trees** also exist and are used in **risk** analysis (combines all feasible alternatives, possible outcomes and their probabilities, monetary consequences and utility evaluations)
- other graphical methods include
 - reliability block diagrams
 - functional logic diagrams
 - Failure Modes and Effects Analysis (FMEA)

Fault Tree Analysis

A technique by which many events that interact to produce other events can be related using simple logical relationships.

- a good reference is NRC “The Fault Tree Handbook”
(<http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/sr0492.pdf>)
- also Chapter 8 and 10 in McCormick (1981)
- one of the principal methods of probabilistic safety (or risk) analysis (PRA)
- developed by Bell Telephone Laboratories in 1962 for the U.S. Air Force Minuteman system, later adopted and extensively used by Boeing Company
- fault tree diagrams
 - are used most often as a system-level risk assessment technique
 - can model the possible combinations of equipment failures, human errors, and external conditions that can lead to a specific type of accident
 - follow a top-down structure and represent a **graphical** model of the pathways within a system between **basic events** that can lead to a foreseeable loss event (or a failure) referred to as the **top event**
- the contributory events and conditions are interconnected using standard logic symbols (AND, OR, etc.), also referred to as **gates**
- events that must **coexist** to cause the top event are described using the **AND** relationship
- alternate events that can **individually** cause the top event are described using the **OR** relationship

- the occurrence of a top event may or may not lead to a serious or adverse **consequence**
- the relative likelihood of a number of potential consequences will depend on the conditions or subsequent events that follow
- potential consequences can be systematically identified using an **event tree**

Basic Events

An event that cannot be developed any further.

- all basic events are generally assumed to be **statistically independent** unless they are **common cause failures** (i.e. failures arising from a common cause or an initiating event)
- basic events can be either
 - **primary** fault events, i.e. subsystem failure due to a basic mode such as a structural fault, failure to open or close, or to start or stop, or
 - **secondary** fault events, i.e. subsystem failure due to excessive operational or environmental stress resulting in the system element to be out of tolerance

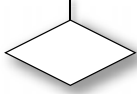
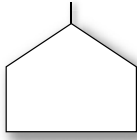
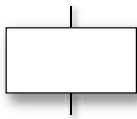
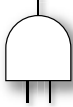
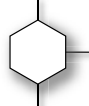
Advantages

- allow the use of reliable information on component failure and other basic events to estimate the overall risk associated with new system designs for which no historical data exists
- simple to understand and easy to implement
- **qualitative** descriptions of potential problems and combinations of events causing specific problems of interest
- **quantitative** estimates of failure frequencies and likelihoods, and relative importances of various failure sequences and contributing events
- lists of recommendations for reducing risks
- quantitative evaluations of recommendation effectiveness

Limitations

- difficult to conceive all possible scenarios leading to the top event
- construction of fault trees for large systems can be tedious
- correlations between basic events (e.g. failure of components belonging to the same batch) are difficult to model and exact solutions to correlated events do not exist
- subjective decisions regarding the level of detail and completeness are often necessary

Notation

Symbol	Name	Description
<u>Primary Event Symbols</u>		
	Circle	Basic Event – a basic initiating fault requiring no further development
	Oval	Conditioning Event – specific conditions or restrictions that apply to any logic gate (used with INHIBIT gate)
	Diamond	Undeveloped Event – an event that is not developed further because it is of insufficient consequence or because information is unavailable
	House	External Event – an event which is normally expected to occur (not a fault event)
<u>Intermediate Event Symbols</u>		
	Rectangle	A fault event that occurs as a result of the logical combination of other events
<u>Gate Symbols</u>		
	OR Gate	The union operation of events, i.e. the output event occurs if (at least) one or more of the inputs occur
	AND Gate	The intersection operation of events, i.e. the output event occurs if and only if all the inputs occur
	INHIBIT Gate	The output event occurs if the (single) input event occurs in the presence of an enabling condition (i.e. Conditioning Event (oval) drawn to the right of the gate)
<u>Transfer Symbols</u>		
	Triangle-in	Indicates that the tree is developed further someplace else (e.g. another page)
	Triangle-out	Indicates that this portion of the tree is a sub-tree connected to the corresponding Triangle-In (appears at the top of the tree)

General Procedure for Fault Tree Analysis

- from the U.S. Coast Guard Risk-based Decision-making Guidelines, Vol. 3 - Risk Assessment Tools Reference, Chapter 9 – Fault Tree Analysis (FTA) (<http://www.uscg.mil/hq/g-m/risk/E-Guidelines/RBDMGuide.htm>)

- Step 1.* Define the **system** of interest.
Specify and clearly define the boundaries and initial conditions of the system for which failure information is needed.
- Step 2.* Define the **top event** for the analysis.
Specify the problem of interest that the analysis will address (e.g. a specific quality problem, shutdown, safety issue, etc.).
- Step 3.* Define the **treetop** structure.
Determine the events and conditions (i.e., intermediate events) that most directly lead to the top event.
- Step 4.* Explore each branch in successive levels of **detail**.
Determine the events and conditions that most directly lead to each intermediate event. Repeat the process at each successive level of the tree until the fault tree model is complete.
- Step 5.* Solve the fault tree for the **combinations** of events contributing to the top event.
Examine the fault tree model to identify all the possible combinations of events and conditions that can cause the top event of interest. A combination of events and conditions *sufficient* and *necessary* to cause the top event is called a **minimal cut set**.
- Step 6.* Identify important **dependent** failure potentials and adjust the model appropriately (qualitative common cause failure analysis).
Study the fault tree model and the list of minimal cut sets to identify potentially important dependencies among events. Dependencies are single occurrences that may cause multiple events or conditions to occur at the same time.
- Step 7.* Perform **quantitative analysis** (if necessary).
Use statistical characterizations regarding the failure and repair of specific events and conditions in the fault tree model to predict future performance for the system.
- Step 8.* Use the results in **decision making**.
Use results of the analysis to identify the most significant vulnerabilities in the system and to make effective recommendations for reducing the risks associated with those vulnerabilities.

Rules of Fault Tree Construction

- a fault tree should only be constructed once the functioning of the entire system is fully understood
- objective is to identify all the component failures, or combinations thereof that could lead to the top event (Steps 2 - 4 above)
- after *McCormick* (1981)

Rule 1. State the fault event as a fault, including the description and timing of a fault condition at some particular time.

Include

- (a) what the fault state of that system or component is,
- (b) when that system or component is in the fault state.

Test the fault event by asking

- (c) is it a fault?
- (d) is the what-and-when portion included in the fault statement?

Rule 2. There are two basic types of fault statements, state-of-system and state-of-component.

To continue the tree,

- (a) if state-of-system fault statement, use Rule 3
- (b) if state-of-component fault statement, use Rule 4

Rule 3. A **state-of-system** fault may use an AND, OR, or INHIBIT gate or no gate at all.

To determine which gate to use, the faults must be then

- (a) minimum necessary and sufficient fault events,
- (b) immediate fault events.

Rule 4. A **state-of-component** fault always uses an OR gate.

To continue, look for the primary, secondary, and command failure fault events. Then state those fault events.

- (a) **primary failure** is failure of that component within the design envelope or environment
- (b) **secondary failures** are failures of that component due to excessive environments exceeding the design environment
- (c) **command faults** are inadvertent operation of the component because of a failure of a control element

Rule 5. No gate-to-gate relationships.

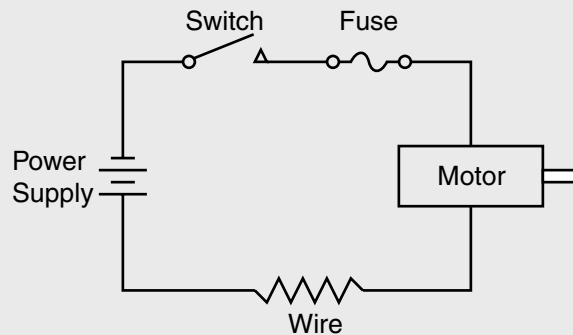
Put an event statement between any two gates.

Rule 6. Expect **no miracles**.

Those things that would normally occur as the result of a fault will occur, and only those things. Also, normal system operation may be expected to occur when faults occur.

- Rule 7.* In an OR gate, the input does not cause output.
If any input exists, the output exists. Fault events under the gate may be a restatement of the output events.
- Rule 8.* An AND gate defines a **causal** relationship.
If the input events coexist, the output is produced.
- Rule 9.* An INHIBIT gate describes a causal relationship between one fault and another, but the indicated condition must be present.
The fault is the direct and sole cause of the output when that specified condition is present. Inhibit conditions may be faults or situations, which is why AND and INHIBIT gates differ.

Example: (McCormick, 1981) Construct a fault tree for the simple electric motor circuit shown below.



Solution:

Step 1. Define the system of interest.

Need to identify

- *Intended Functions*
- *Physical Boundaries* (to avoid overlooking key elements of a system at interfaces and penalizing a system by associating other equipment with the subject of the study)
- *Analytical Boundaries* (to limit the level of analysis resolution, to explicitly exclude certain types of events and conditions, such as sabotage, from the analysis)
- *Initial Conditions*, (including equipment that is assumed to be out of service initially, which affect the combinations of additional events necessary to produce a specific system problem)

For this particular problem we have,

- | | |
|-----------------------|---|
| Intended Function | – the motor is used for some (unknown) purpose |
| Physical Boundaries | – power supply |
| Analytical Boundaries | – include all contributors in the above diagram |
| Initial Conditions | – switch closed, motor on |

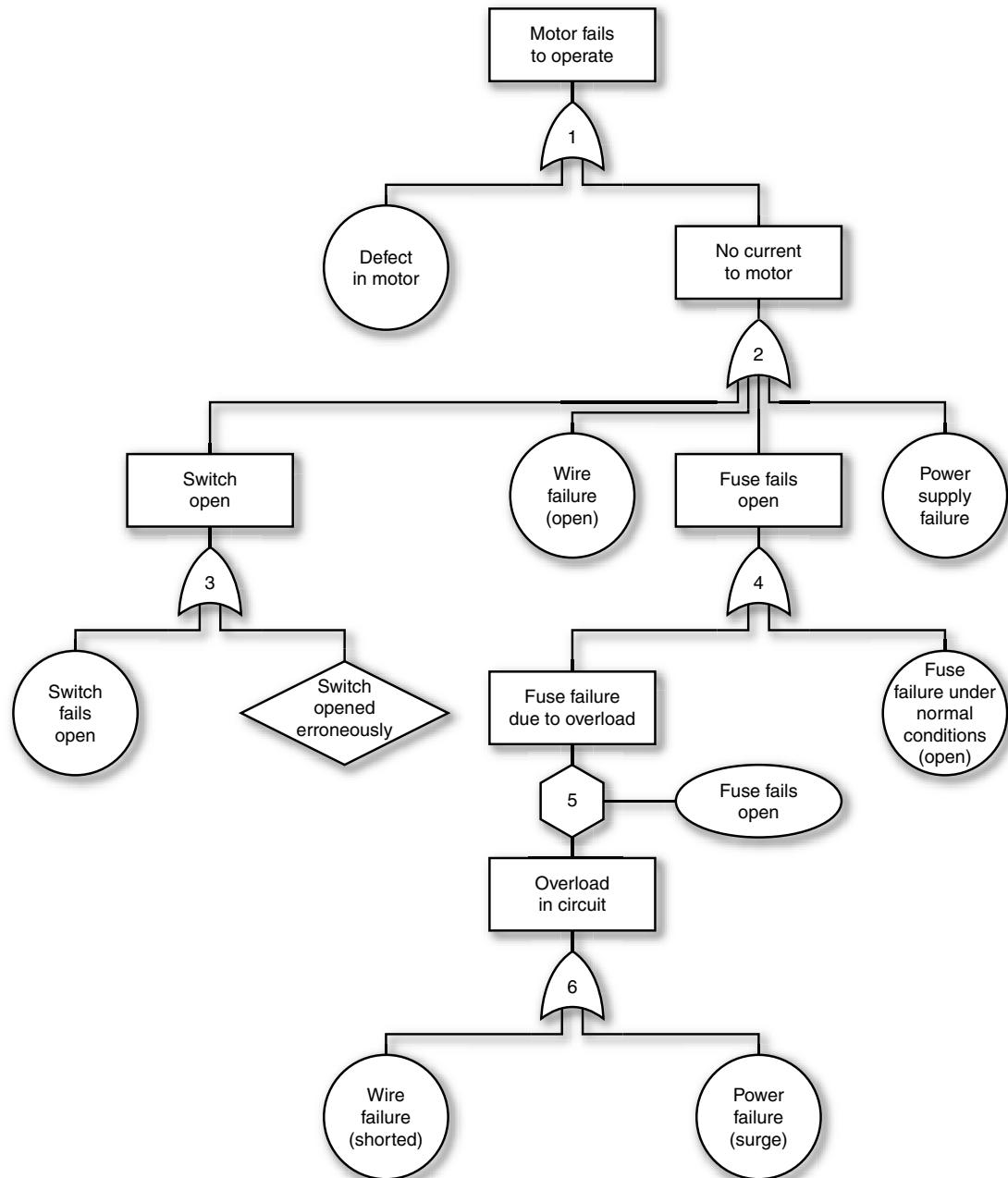
Step 2. Define the top event.

We are interested in the event that the motor fails to operate. Therefore, the top event is defined as

Motor fails to operate

Step 3. Construct the fault tree, starting from the top, i.e., define the treetop structure. Identify the main contributing events, including all events and scenarios that may cause the top event.

Step 4. Explore each branch in successive levels of detail, following the rules of fault tree construction.



Fault Tree Construction

Gate 1. One primary failure event is the failure of the motor itself (for example, due to a wiring failure within the motor or loss of lubrication to the bearings). This event is a basic event because no details of the motor are given, therefore, the event cannot be developed further. The other possibility is the event that no current is supplied to the motor.

Gate 2. The event “No current in motor” is the result of other events and is therefore developed further. The lack of current to the motor can result from a broken connection in any of the other four components in the circuit, including the failure of the wire or power supply (basic events), the switch being open, or failure of the fuse.

Gate 3. The open switch may be due to a basic failure of the switch, or the event that the switch was opened erroneously. The erroneous opening of the switch is due to human error, which could be developed further into more basic events (i.e. operator is inexperienced, under stress, etc.). However, due to insufficient information, the event is not explored further. This purposely undeveloped event is therefore denoted with the diamond symbol.

Gate 4. The fuse failure event may be caused by fuse failure under normal conditions (primary failure) or due to overload from the circuit.

Gate 5. The secondary fuse failure can occur if the fuse does not open every time an overload is present in the circuit (because all conditions of an overload do not necessarily result in sufficient overcurrent to open the fuse). This is why a conditional gate, denoted by the hexagon, is used. The condition, i.e. “Fuse fails open” is placed in the connecting oval, and the conditional gate is treated similarly to an AND gate in subsequent tree analysis.

Gate 6. The overload in the circuit may be caused either by a short or a power surge, both of which are primary (i.e. basic) events.

Considerations

- construction of a fault tree is **subjective**
- need to take into account
 - **Level of Detail** – the number of basic events should be defined such that the size of the tree is reasonable with respect to the scope of the analysis
 - **Probability Assignment** – need to stop development at the level where probability or failure data is available
 - **Meaningfulness** – the level of detail should be such that the basic and undeveloped events correspond to the design aspects being analyzed

Fault Tree Evaluation

- identify critical events and event combinations that lead to the top event
- calculate the probability of the **top event** based on the probabilities of the **basic** and **undeveloped** events in the fault tree
- two types of analysis
 - qualitative
 - quantitative
- based on Boolean logic

Boolean Algebra

- fault trees describe the relationships between events using Boolean logic
- a fault tree can be translated into an equivalent set of Boolean equations

The OR Gate

Represents the **union** of events at the gate. For event Q with two input events A and B attached to the OR gate, the probability is obtained as

$$P(Q) = P(A) + P(B) - P(A \cap B) \quad (1)$$

or

$$P(Q) = P(A) + P(B) - P(A)P(B | A) \quad (2)$$

If A and B are **mutually exclusive** events then $P(A \cap B) = 0$ and

$$P(Q) = P(A) + P(B) \quad (3)$$

If A and B are **independent** events then $P(B | A) = P(B)$ and

$$P(Q) = P(A) + P(B) - P(A)P(B) \quad (4)$$

If event B is **completely** dependent on event A then $P(B | A) = 1$ and

$$P(Q) = P(A) + P(B) - P(A)(1) = P(B) \quad (5)$$

Therefore, the approximation of

$$P(Q) = P(A) + P(B) \quad (6)$$

is **always** a **conservative** estimate for the probability of event Q (because $P(A \cap B)$ is small compared with $P(A) + P(B)$ for very low probability events). Event Q will occur if any (at least) one of the input events to the OR gate occur.

The AND Gate

Represents the **intersection** of events at the gate. For event Q with two input events A and B attached to the AND gate, the probability is obtained as

$$P(Q) = P(A)P(B | A) = P(B)P(A | B) \quad (7)$$

If A and B are **independent** events then $P(B | A) = P(B)$ and $P(A | B) = P(A)$ therefore

$$P(Q) = P(A)P(B) \quad (8)$$

If A and B are **not independent**, then Q may be significantly greater than $P(A)P(B)$. Event Q is caused only if every (all) input event attached to the AND gate occur.

Rules of Boolean Algebra

Mathematical Notation	Engineering Notation	Designation
$X \cap Y = Y \cap X$	$X \cdot Y = Y \cdot X$	Commutative Law
$X \cup Y = Y \cup X$	$X + Y = Y + X$	
$X \cap (Y \cap Z) = (X \cap Y) \cap Z$	$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z$	Associative Law
$X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X(YZ) = (XY)Z$	
$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	$X \cdot (Y + Z) = X \cdot Y + X \cdot Z$	Distributive Law
$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X + (Y \cdot Z) = (X + Y) \cdot (X + Z)$	
$X \cap X = X$	$X \cdot X = X$	Idempotent Law
$X \cup X = X$	$X + X = X$	
$X \cap (X \cup Y) = X$	$X \cdot (X + Y) = X$	Law of Absorption
$X \cup (X \cap Y) = X$	$X + (X \cdot Y) = X$	
$X \cap \bar{X} = \phi$	$X \cdot \bar{X} = \phi$	Complementation
$X \cup \bar{X} = \Omega = I$	$X + \bar{X} = \Omega = I$	
$\overline{X \cap Y} = \bar{X} \cup \bar{Y}$	$\overline{X \cdot Y} = \bar{X} + \bar{Y}$	de Morgan's Rule
$\overline{X \cup Y} = \bar{X} \cap \bar{Y}$	$\overline{X + Y} = \bar{X} \cdot \bar{Y}$	
$\phi \cap X = \phi$	$\phi \cdot X = \phi$	Operations with ϕ and Ω
$\phi \cup X = X$	$\phi + X = X$	
$\Omega \cap X = X$	$\Omega \cdot X = X$	
$\Omega \cup X = \Omega$	$\Omega + X = \Omega$	
$\bar{\phi} = \Omega$	$\bar{\phi} = \Omega$	
$\bar{\Omega} = \phi$	$\bar{\Omega} = \phi$	
$X \cup (\bar{X} \cap Y) = X \cup Y$	$X + (\bar{X} \cdot Y) = X + Y$	Other relationships
$\bar{X} \cap (X \cup \bar{Y}) = \bar{X} \cap \bar{Y}$	$\bar{X} \cdot (X + \bar{Y}) = \bar{X} \cdot \bar{Y}$	

ϕ is the empty or null set which is equal to zero
 Ω or I is the universal set which is equal to one

Qualitative Analysis

- used for identifying
 - critical events
 - potential system weaknesses
 - best ways to reduce the risk associated with the top event
- conducted using **minimal cut sets**

Minimal Cut Sets

The smallest combination of basic events which, if they occur, will cause the top event to occur.

- can be seen as a specific **scenario** that leads to the top event
- cut sets are **combinations** (intersections) of component failures sufficient for the top event
- the occurrence of **all** events in a minimal cut set is necessary for the occurrence of the top event, i.e. if one of the failures in a cut set does not occur, then the top event will not occur (by this combination)
- there are a **finite** number of minimal cut sets for each fault tree, which are unique for the top event
- one-component minimal cut sets represent failures which will cause the top event to occur
- the minimal cut sets for a fault tree are obtained by
 - translating the tree to its equivalent Boolean equations (assume that events are **independent**)
 - using top-down or bottom-up substitution
 - using the Distributive Law and Law of Absorption to remove redundancies

Criticality

- the importance of each minimal cut set can be based on its relative contribution to the total probability of the top event
- the minimal cut sets for a fault tree can be used to identify the most critical basic events using the following criteria
 - minimal cut sets that include a **small** number of events represent less redundancy and so have **higher** criticality
 - events that appear on a **large** number of minimal cut sets are more important because they can contribute to the top event in several scenarios
- must also consider the relative probabilities of each of the events
 - the importance of each event can be based on the total probability of the cut sets to which the basic event contributes (i.e. represents the total probability of failure involving the event)

Example: Determine all the minimal cut sets for the small motor problem.

Solution:

Let T denote the top event

Let P denote primary events (circles)

Let G denote intermediate events (rectangles)

Let S denote undeveloped events (diamonds)

Let C denote conditioning events (ovals)

Therefore

T = motor fails to operate

P1 = defect in motor

P2 = wire failure (open)

P3 = power supply failure

P4 = switch fails open

P5 = fuse failure under normal conditions (open)

P6 = wire failure (shorted)

P7 = power failure (surge)

G1 = no current to motor

G2 = fuse fails open

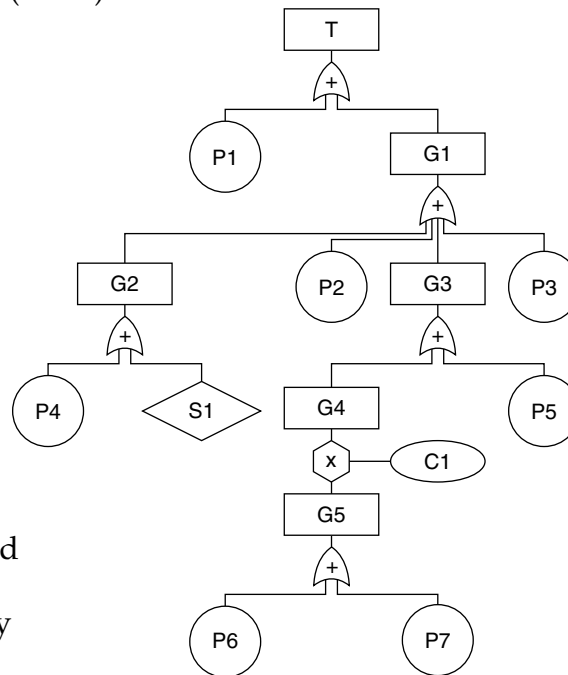
G3 = switch open

G4 = fuse failure due to overload

G5 = overload in circuit

S1 = switch opened erroneously

C1 = fuse fails to open



Writing equations for each gate of the tree

$$T = P1 + G1 \quad (9)$$

$$G1 = P2 + P3 + G2 + G3 \quad (10)$$

$$G2 = P4 + S1 \quad (11)$$

$$G3 = G4 + P5 \quad (12)$$

$$G4 = C1 \cdot G5 \quad (13)$$

$$G5 = P6 + P7 \quad (14)$$

Using the **top-down** approach we get by substitution

$$T = P1 + G1 \quad (15)$$

$$= P1 + P2 + P3 + G2 + G3 \quad (15.1)$$

$$= P1 + P2 + P3 + P4 + S1 + G3 \quad (15.2)$$

$$= P1 + P2 + P3 + P4 + S1 + G4 + P5 \quad (15.3)$$

$$= P1 + P2 + P3 + P4 + S1 + (C1 \cdot G5) + P5 \quad (15.4)$$

$$= P1 + P2 + P3 + P4 + S1 + P5 + C1 \cdot (P6 + P7) \quad (15.5)$$

$$= P1 + P2 + P3 + P4 + S1 + P5 + (C1 \cdot P6) + (C1 \cdot P7) \quad (15.6)$$

The top event, therefore, contains 6 single component minimum cut sets and 2 double component minimum cut sets.

Quantitative Analysis

- calculate the **probability** of occurrence of the top event, given the fault tree and the probability of occurrence of the basic events
- common approaches include
 - assume all basic events are **independent**
 - assume the probabilities of basic events are **small** (rare-event approximation)
- if each basic event on the fault tree occurs only **once**, then the tree branches emanating from any given gate in the tree are independent
- the probability of the top event is given by the probability of the **union** of the minimum cut sets
- results in a **conservative** estimate of the probability of failure

Common-Cause Failures

Multiple failures originating from a common cause that fails the system.

- the basic events may not always be independent
- failure events can be caused by a **common environment** or have **factors** in common (e.g. an operator has miscalibrated all sensors)
- common causes often arise from factors such as manufacturer, environment, energy sources, and humans
- the evaluation of probabilities will require **conditional** or **joint** probabilities

Example: Calculate the probability of occurrence of the top event for the simple motor example. Assume the probability of occurrence of each basic event is equal to 0.01 and the probability of the event S1 “Switch opened erroneously” is equal to 0.001. Also assume that the condition C1 “Fuse fails open” has a probability of occurrence of 0.50.

Solution:

Using the same notation as before we are given

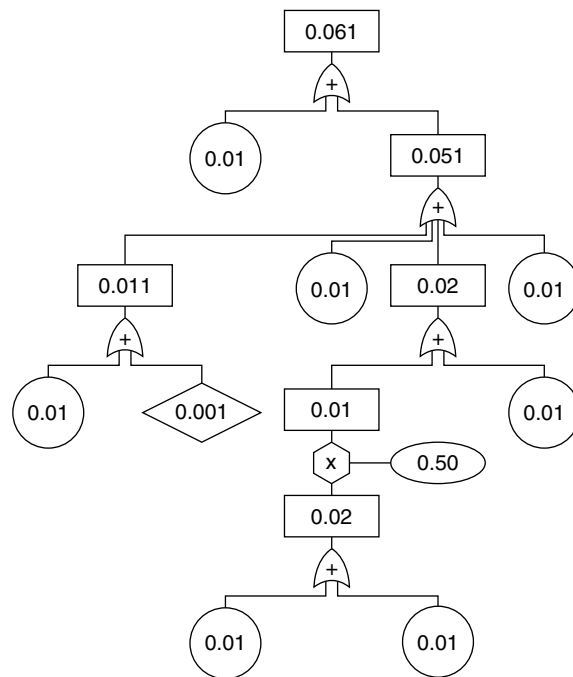
Event	Description	Probability
P1	Defect in motor	0.01
P2	Wire failure (open)	0.01
P3	Power supply failure	0.01
P4	Switch fails open	0.01
P5	Fuse failure under normal conditions (open)	0.01
P6	Wire failure (shorted)	0.01
P7	Power failure (surge)	0.01
S1	Switch opened erroneously	0.001
C1	Fuse fails open	0.50

The probability of **intermediate** events can be evaluated using the fault tree.
The probability of the top event is given by the union of the minimum cut sets determined before as

$$T = P1 + P2 + P3 + P4 + S1 + P5 + (C1 \cdot P6) + (C1 \cdot P7) \quad (16)$$

$$= 0.01 + 0.01 + 0.01 + 0.01 + 0.001 + 0.01 + (0.50)(0.01) + (0.50)(0.01) \quad (16.1)$$

$$= 0.061 \quad (16.2)$$



References

- McCormick, N.J. 1981. *Reliability and Risk Analysis: Methods and Nuclear Power Applications*. Academic Press, New York.
- United States Coast Guard. 2004. Risk-based Decision-making (RBDM) Guidelines (3rd Ed.), Vol. 3 – Risk Assessment Tools Reference, *Chapter 9 – Fault Tree Analysis*.
(<http://www.uscg.mil/hq/g-m/risk/E-Guidelines/RBDMGuide.htm>)
- United States Nuclear Regulatory Commission (NRC). 1981. *Fault Tree Handbook*. NUREG-0492. Systems and Reliability Research Office of Nuclear Regulatory Research, Washington, D.C.
(<http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/sr0492.pdf>)