Engineering Reliability

Fault Trees and Reliability Block Diagrams

Harry G. Kwatny

Department of Mechanical Engineering & Mechanics
Drexel University

Outline

Diagrams

Fault Trees

- Fault Tree Definition
- Qualitative Analysis
  - Logic
  - Cut Sets
- Quantitative Analysis
  - Cut Set & Top Event Probabilities
  - Basic Event Probability

Summary

Introduction

We will be concerned with how the structure of a system affects its reliability. We consider the two graphical representations of systems used for reliability analysis:

- Fault Tree –
  - The fault tree shows all possible combinations of failure events that may cause a *specific* system failure.
  - Fault trees are constructed by considering deductively what caused the failure.
  - Component failures and other events are combined through logical 'AND' ($\cap$) and 'OR' ($\cup$) operations to provide a logical description of the failure.
- Reliability Block Diagram –
  - A reliability block block diagram shows how the functioning of components or subsystems enable the satisfaction of a *specific* system function.
  - These diagrams facilitate the computation of reliability indices and elucidate the role of redundancy.

Fault Tree Analysis

- Fault tree analysis (FTA) is a top-down approach to failure analysis, starting with a possible failure event, called a TOP event, and then determining the ways it can happen.
- The analysis proceeds by determining how the TOP event is caused by lower level failure events.
- The primitive or basic failure events that ultimately cause the TOP event are connected through logical AND-gates and OR-gates.

Some History of Fault Tree Analysis

- FTA was first used by Bell Labs in connection with the safety analysis of the Minuteman missile launch control system in 1961.
- Boeing further developed the technique, applying it to the entire Minuteman system and then to commercial aircraft.
- Boeing applied FTA as part of a comprehensive safety review of the Apollo system following the launch pad fire on January 27, 1967.
- FTA was used in the WASH-1400 study (1976) conducted to review nuclear plant power design and to assure the public that the probability of nuclear accidents was very small. The 3-mile island accident occurred March 28, 1979.

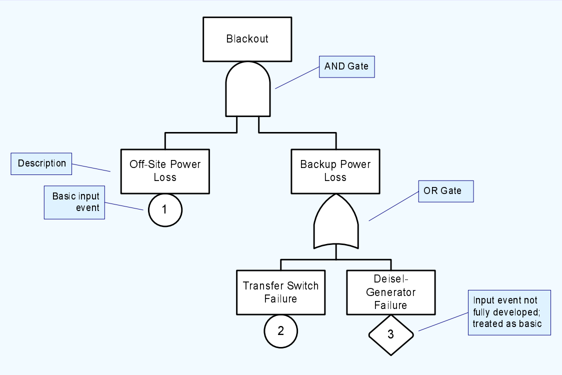
Example: Power Supply

The power supply system consists of the following elements:

- an offsite power supply
- a backup power system, containing
  - A diesel driven generator,
  - An automatic transfer switch.

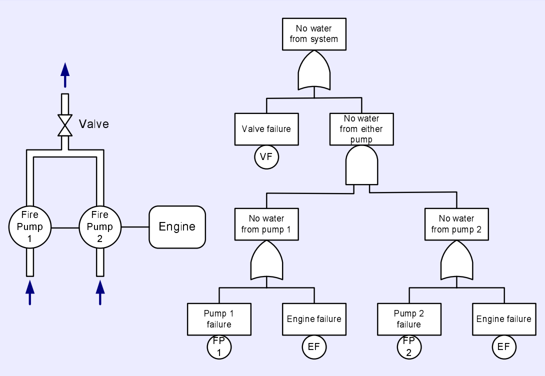
Example: Power Supply – 2

- the system ‘fails’ upon blackout – when power is not available
- blackout occurs when both off-site power and backup power fail
- the diagram is developed from the top down terminating at ‘basic’ failure events



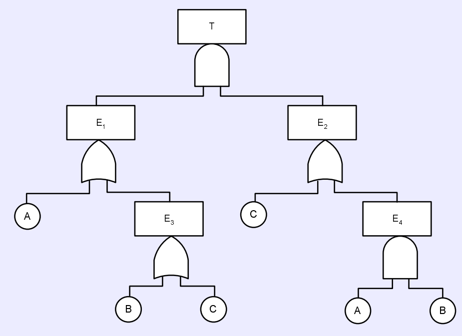
Example: Fire Pump System

- The fire pump system shown below has two pumps driven by a single engine.
- the TOP failure event is the failure to supply water to the fire hose.



Fault Tree Logic

In the fault tree shown below primary faults appear multiple times – this is typical of redundant systems.



The following logical expression defines the tree:

$$T = E_1 \cap E_2 = (A \cup E_3) \cap (C \cup E_4)$$
$$= (A \cup (B \cup C)) \cap (C \cup (A \cap B))$$

Rules of Boolean Algebra

The following logical relationships are identical to corresponding set relationships that can be derived from the Venn diagram.

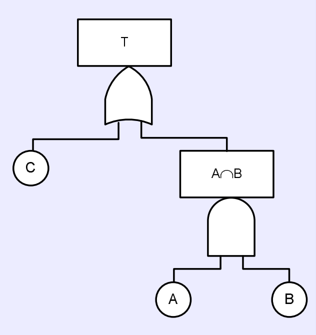
Expression	Description
$X \cap Y = Y \cap X$	Commutative Law
$X \cup Y = Y \cup X$	
$X \cap (Y \cap Z) = (X \cap Y) \cap Z$	Associative Law
$X \cup (Y \cup Z) = (X \cup Y) \cup Z$	
$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	Distributive Law
$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	
$(X \cap Y)^c = X^c \cup Y^c$	de Morgan's Law
$(X \cup Y)^c = X^c \cap Y^c$	

FAULT TREE LOGIC – 2

Using the Boolean logic rules, the expression for T can be reduced to:

$$T = C \cup (A \cap B)$$

This corresponds to the simplified fault tree shown below.



Cut Sets

Definitions:

- A cut set is a set of basic events whose simultaneous occurrence insures that the TOP event occurs.
- A cut set is minimal if it cannot be reduced without losing its status as a cut set.

Notes:

- The TOP event will occur if the basic events in a minimal cut set occur at the same time.
- The minimal cut sets describe the combinations of events that cause the TOP event to occur.

Examples of Cut Sets

Example (Power Supply System)

- cut sets

$$\{1, 2, 3\}, \{1, 2\}, \{1, 3\}$$

- minimal cut sets

$$\{1, 2\}, \{1, 3\}$$

Example (Fire Pump System)

- cut sets

$$\{VF, EF, FP1, FP2\}, \{VF, EF, FP1\}, \{VF, EF, FP2\}, \{VF, EF\}, \{VF, FP1\}, \{VF, FP2\}, \{EF, FP1\}, \{EF, FP2\}, \{FP1, FP2\}, \{VF\}, \{EF\}$$

- minimal cut sets

$$\{VF\}, \{EF\}, \{FP1, FP2\}$$

Note:

- Conjunction: logical propositions connected by AND
- Disjunction: logical propositions connected by OR

Logic Expression Normal Forms:

- Conjunction Normal Form (CNF) a logical formula which is a conjunction of disjunctive clauses

$$A,\ A \cap B,\ (A \cup B) \cap C$$

- Disjunctive Normal Form (DNF) a logical formula which is a disjunction of conjunctive clauses

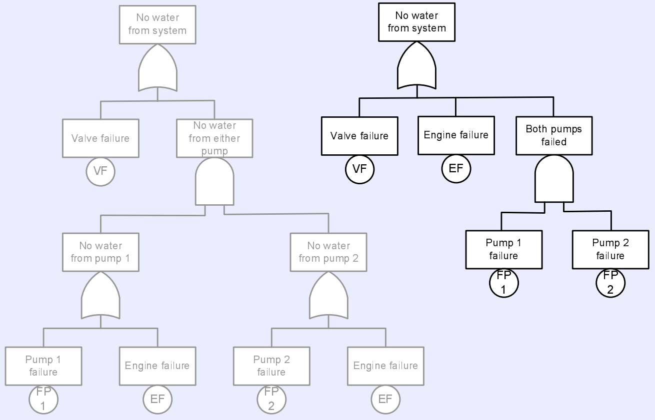
$$A,\ A \cup B,\ (A \cap B) \cup C$$

If the minimal cut sets of a fault tree are identified, the logical expression defining the tree can be expresses in DNF.

Example (Fire Pump System)

$$T = VF \cup EF \cup (FP1 \cap FP2)$$

Example: Fire Pump Reduced Fault Tree



Setup

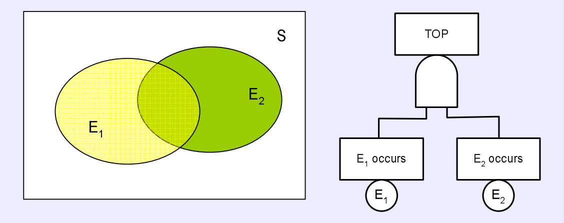
Definitions:

- $E_i(t)$ denotes that the i^{th} component (or event) is in a failed state at time t.
- A minimal cut set is said to fail (or be in a failed state) when all of its basic events are in a failed state at the same time.

Notation:

- $Q_0(t)$ = probability that TOP event occurs (is true) at time t.
- $q_i(t)$ = probability that basic event i occurs (is true) at time t.
- $\breve{Q}_j(t)$ = probability that the minimal cut set j occurs (is true) at time t.

Single AND-Gate



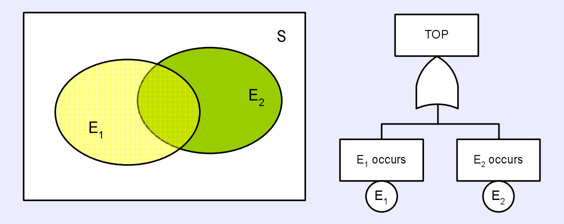
When the basic events are independent, the TOP event probability is:

$$Q_0(t) = P(E_1(t) \cap E_2(t)) = P(E_1(t))\, P(E_2(t)) = q_1(t)\, q_2(t)$$

For a single AND-gate with m basic events:

$$Q_0(t) = \prod_{i=1}^{m} q_i(t)$$

SINGLE OR-GATE



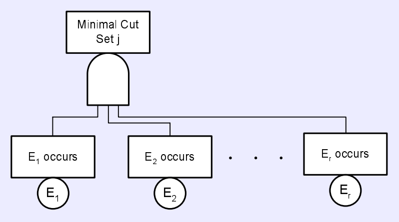
When the basic events are independent, the TOP event probability is:

$$Q_0(t) = P(E_1(t) \cup E_2(t)) = P(E_1(t)) + P(E_2(t)) - P(E_1(t) \cap E_2(t))$$
$$= q_1(t) + q_2(t) - q_1(t)\, q_2(t) = 1 - (1 - q_1(t))(1 - q_2(t))$$

For a single OR-gate with m basic events:

$$Q_0(t) = 1 - \prod_{i=1}^{m} (1 - q_i(t))$$

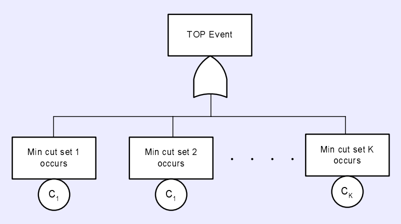
Cut Set Probability



- A minimal cut set fails if and only if all basic events $E_1, \ldots, E_r$ fail at the same time.
- Assume the r basic events are independent and the probability of failure of the i^{th} event is $q_{j,i}$, $i = 1, \ldots, r$.
- The probability of failure of minimum cut set j is

$$\breve{Q}_j(t) = \prod_{i=1}^{r} q_{j,i}(t)$$

Top Event Probability



- The top event if at least one min cut set occurs.
- In general, some of the min cut sets will contain common elements, so we cannot assume they are independent.
- The best we can do is derive the *upper bound*

$$Q_0(t) \leq 1 - \prod_{i=1}^{K} \left(1 - \breve{Q}_i(t)\right)$$

SUMMARY