AI-04576 Fault Tree Analysis FTA

#problem, #cmp

Explain Fault Tree Analysis

Fault Tree Analysis (FTA) is a top-down, deductive risk assessment method used in reliability and safety engineering. It systematically identifies all possible failure paths that could cause a specific undesirable outcome, known as the **Top Event**.

First developed by Bell Telephone Laboratories in 1962 for the Minuteman missile program, FTA converts complex system interactions into clear Boolean logic diagrams.

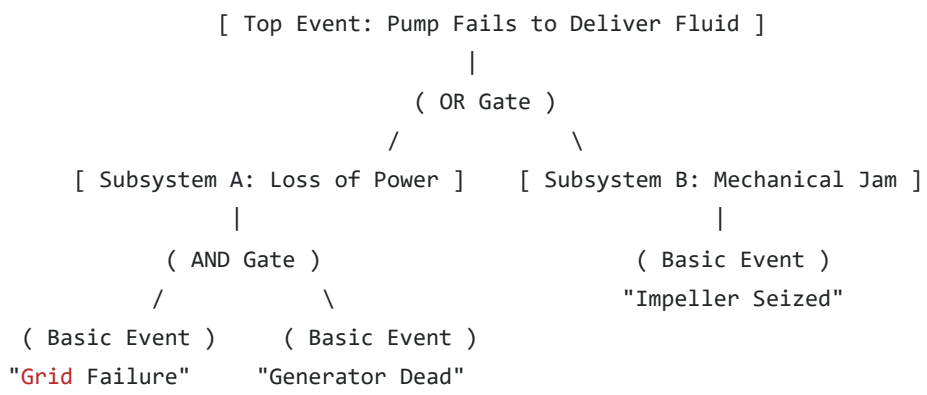
The Building Blocks of a Fault Tree

A fault tree moves from the macro failure down to the micro root causes using standard visual symbols:

- **Top Event (Rectangular Node):** The system-level catastrophic or undesired failure being analyzed (e.g., "*Emergency Diesel Generator Fails to Start*").
- **Basic Event (Circle Node):** The foundational, irreducible failure or root cause (e.g., "*Battery Discharged*" or "*Fuse Blown*").
- **Intermediate Event (Rectangle Node):** A secondary failure condition caused by lower-level events.
- **Logic Gates:**
  - **OR Gate:** Triggers if **any** input condition occurs. Indicates single-point vulnerabilities or lack of redundancy.
  - **AND Gate:** Triggers only if **all** input conditions occur simultaneously. Indicates systems with functional redundancy or requiring multiple simultaneous failures.

How FTA Works: A Step-by-Step Example

Consider a backup pump failure in a industrial plant:



1. **Top Event:** Pump fails to deliver fluid.
2. **First Level (OR Gate):** The pump fails if there is a *Loss of Power* **OR** a *Mechanical Jam*.
3. **Second Level (AND Gate):** Power is lost only if the *Grid Fails* **AND** the *Backup Generator Fails* at the same time.

Qualitative vs. Quantitative Analysis

FTA provides two complementary modes of analysis:

1. Qualitative Analysis (Minimal Cut Sets)

A **Cut Set** is any combination of basic events that causes the Top Event. A **Minimal Cut Set (MCS)** is the smallest combination of basic events that alone triggers the failure.

> **Key Rule:** A Minimal Cut Set with a single basic event highlights a **Single Point of Failure** in your architecture—the primary target for engineering redesign.

2. Quantitative Analysis (Probability Calculation)

If failure rates or probabilities (P) for basic events are known, you can calculate the exact probability of the Top Event using Boolean algebra:

- **For an AND Gate** (Independent events A and B):

$$P(\text{AND}) = P_A \times P_B$$

(Redundancy significantly drops total failure probability.)

- **For an OR Gate** (Independent events A and B):

$$P(\text{OR}) = 1 - (1 - P_A)(1 - P_B) \approx P_A + P_B \quad (\text{for small probabilities})$$

FTA vs. FMEA

Engineering teams frequently pair FTA with **Failure Mode and Effects Analysis (FMEA)**:

Attribute	**Fault Tree Analysis (FTA)**	**Failure Mode & Effects Analysis (FMEA)**
Approach	Top-Down (Deductive)	Bottom-Up (Inductive)
Starting Point	Undesired Top Event	Individual component failure modes
Focus	How multiple failures combine	Impact of a single component's failure
Best For	Safety-critical systems & complex interactions	Component-level design and maintenance planning

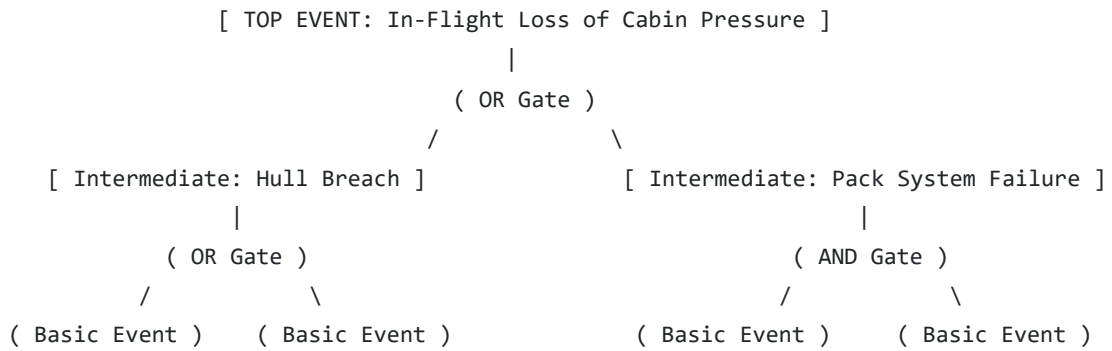
List Examples

Fault Tree Analysis (FTA) is widely used across high-consequence industries where system safety, continuous uptime, and failure mitigation are critical.

Here are real-world examples of Fault Tree Analysis categorized by industry, complete with sample logic tree breakdowns.

1. Aerospace: Loss of Cabin Pressurization

In commercial aviation, maintaining cabin altitude is critical for passenger survival.



```
Door Seal Failure  Cargo Latch Sheared          Primary Pack Fails  Secondary Pack Fails
```

- **Top Event:** Uncontrolled loss of cabin pressurization at cruising altitude.
- **Intermediate Event (Hull Breach - OR Gate):** Occurs if the door seal fails **OR** a structural latch shears.
- **Intermediate Event (Pack System Failure - AND Gate):** Occurs only if the primary air cycle pack fails **AND** the redundant secondary air cycle pack fails simultaneously.

2. Semiconductor Manufacturing: Cleanroom Toxic Gas Release

Semiconductor fabrication uses hazardous gases like Silane (SiH_4) or Arsine (AsH_3). An uncontrolled leak in a cleanroom bay presents severe safety and financial risks.

- **Top Event:** Toxic gas concentration detected in Bay 4 cleanroom air.
- **Logic Breakdown:**
  - **OR Gate (Root Paths):** Gas line containment leak **OR** Human operator purge manifold error.
  - **AND Gate (Double Containment System):** Gas line containment leaks into the bay only if the primary internal stainless steel tubing breaches **AND** the outer coax exhaust sleeve suffers physical damage.
  - **AND Gate (Interlock Failure):** Toxic gas flows continuously if line ruptures **AND** the automated mass flow controller shut-off valve fails to close.

3. Automotive / EV: Battery Pack Thermal Runaway

Electric vehicle (EV) safety engineering relies heavily on FTA to pass safety regulations and prevent battery fires.

Event Type	Event Description	Logic Gate / Condition
Top Event	High-Voltage Battery Thermal Runaway	Target for mitigation
Intermediate	Overcharging Battery Cell	**OR Gate**
Basic Event	Physical puncture from road debris	Direct cause (Single event)
Basic Event	Internal cell short circuit due to manufacturing defect	Direct cause

Intermediate	BMS Fail-Safe Override	**AND Gate** (BMS software fault **AND** mechanical contactor welded closed)

4. Cloud Infrastructure & IT Systems: Database Outage

Site Reliability Engineering (SRE) uses FTA during post-mortems and architecture reviews to prevent cascading outages in distributed systems.

- **Top Event:** Multi-Region Production Database Unavailability.
- **OR Gate (Major Failure Modes):**
  - Network partition isolated all database nodes.
  - Primary database storage volume corruption.
- **AND Gate (Data Loss Path):** Storage volume corrupts **AND** automated snapshot backup service fails **AND** secondary read-replica failover drops connection.

5. Healthcare & Medical Devices: Infusion Pump Over-Dosing

Automated medical infusion pumps deliver precise medication doses to patients in intensive care units.

- **Top Event:** Patient receives $2\times$ prescribed medication dose.
- **OR Gate:** Incorrect rate setting programmed manually **OR** peristaltic motor runaway.
- **AND Gate (Hardware Safeguard Failure):** Motor runaway occurs **AND** the optical drop sensor hardware watchdog fails to interrupt pump power.

Summary of FTA Logic Patterns

- **Single-Point Vulnerabilities (OR Gates):** Identified when a single basic event flows directly into an OR gate to cause an intermediate or top event. These require immediate redesign or structural reinforcement.
- **Redundancy Effectiveness (AND Gates):** Used to prove that parallel safety controls (like primary/secondary power feeds or dual software controls) successfully reduce the overall probability of a catastrophic Top Event.