# Failure Analysis Methods

## What, Why and How

MEEG 466 – Special Topics in Design

Jim Glancey

Spring, 2006

# Failure Analysis Methods

- Every product or process has modes of failure.
- An analysis of potential failures helps designers focus on and understand the impact of potential process or product risks and failures.
- Several systematic methodologies have been develop to quantify the effects and impacts of failures.

# Failure Analysis Methods . . .

Why perform failure analysis?

- Product Development:
  - Prevent product malfunctions.
  - Insure product life.
  - Prevent safety hazards while using the product.
- Process Development:
  - –Insure product quality
  - –Achieve process reliability
  - –Prevent customer dissatisfaction
  - –Prevent safety or environmental hazards

# Common Failure Analysis Techniques

- Cause-Consequence Analysis
- Checklist
- Event Tree Analysis
- Failure Modes & Effects Analysis *(FMEA)*
- Failure Modes, Effects and Criticality Analysis *(FMECA)*
- Fault Tree Analysis *(FTA)*
- Hazard & Operability Analysis *(HAZOP)*
- Human Reliability
- Preliminary Hazard Analysis *(PHA)*
- Relative Ranking
- Safety Review
- What-If / Checklist Analysis
- What-If Analysis

For the purpose of this class, two common but fundamentally different techniques will be presented in detail:

1. Failure Modes Effects Analysis (FMEA)
2. Fault Tree Analysis

# Part 1: Failure Modes Effect Analysis

# Failure Modes & Effects Analysis (FMEA)

- Tabulation of equipment/components and their associated single point failure modes, consequences and safeguards.
- Identification/assessment of risk is derived from looking at each component (or machine in the case of multi-unit manufacturing).
- This is commonly referred to as a bottom-up approach.

Simple Example: Car

| Item | Identification | Description | Failure Modes | Effects | Safeguards | Actions |
|---|---|---|---|---|---|---|
| 1 | Car Tire | -Supports Weight<br>-Traction<br>-Cornering<br>-Smooth Ride | Flat | -Stranded<br>-Loose Control | Spare Tire In Trunk | Acceptable as is |
| 2 | Gas Tank | Holds fuel | -Empty<br>-Blows up | -Stall<br>-Car Destroyed | -Fuel Gage<br>-Locate away from Engine | Acceptable as is |

# Implementing FMEA

An FMEA can be implemented using a hardware or functional approach, and often due to system complexity, be performed as a combination of the two methods.

Hardware = loss of a component

Functional = loss of a function or feature

# Failures

- Need to understand failures which can be any of the following:
  - Failure is any loss that interrupts the continuity of production.
  - Failure is a loss of asset availability.
  - Failure is the unavailability of equipment.
  - Failure is a deviation from the status quo.
  - Failure is not meeting target expectations.
  - Failure is any secondary defect

# Failures . . .

- Failures can be:
  - pump not working
  - seized valve
  - broken wire
  - software crash
  - system down
  - reactor melt down
  - no money in a checking account (inevitable for college student)

# Failures . . .

- Defining the possible (and relevant) failures is the key for the analysis to produce meaningful results.
- For instance, if all we care about are failures that cause injuries or death, then the analysis would be much different than one that was interested in economical problems.

# FMEA Procedure

- Review and understand product or process design; breakdown into components (product) or steps (process).
- Brainstorm modes of failure.
- Rate the **severity** of each effect of failure.
- Rate the likelihood of **occurrence** for each failure.
- Rate the likelihood of **detection** for each cause of failure (*i.e.* the likelihood of detecting the problem before it reaches the customer or operator).
- Compute the Risk Priority Number, RPN = Severity x Occurrence x Detection
- Implement corrective actions to minimize the occurrence of the more significant failure modes (i.e. the highest RPN's).
- Re-assess the product or process by another cycle of FMEA after the actions have been completed.
- Perform regular (re)assessments of failures as needed.

# FMEA Table

## Example: Hydraulic Hose Failure

| B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Failure Modes Effect Analysis Template** | | | | | | | | |
| | | | MEEG 467 - Special Topics in Design | | | | | | | | |
| | | | | 24-Mar-06 | | | | | | | |
| **Component or Process Function** | **Failure Mode** | **Cause of Failure** | **Possible Effect** | **Potential Severity** | **Probability of Occurance** | **Probability of Not Detecting** | **Risk Priority Number (RPN)** | **Preventative Action** | | | |
| Example: | | | | | | | | | | | |
| Hydraulic Hose | Burst | Over - Pressure | Loss of Operation (Catastrofic) | 10 | 4 | 10 | 400 | Install Pressure Relief Valve | | | |
| | Leak | Weathering | Oil Drip | 4 | 1 | 2 | 8 | Shield UV Light | | | |
| | Leak | Pinching | Oil Drip | 4 | 7 | 2 | 56 | Re-Route Hoses Around Pinch-Points | | | |

- Severity, Occurance and Detection ratings are based on a 1 = low to 10 = high scale.

- The FMEA results clearly show the greatest risk is associated with over-pressure failure, and the lowest risk is due to weathering-related failure.

- The excel template shown is above is available at:
  *http://research.me.udel.edu/~jglancey/FMEA_Template.xls*

# Part 2: Fault Tree Analysis

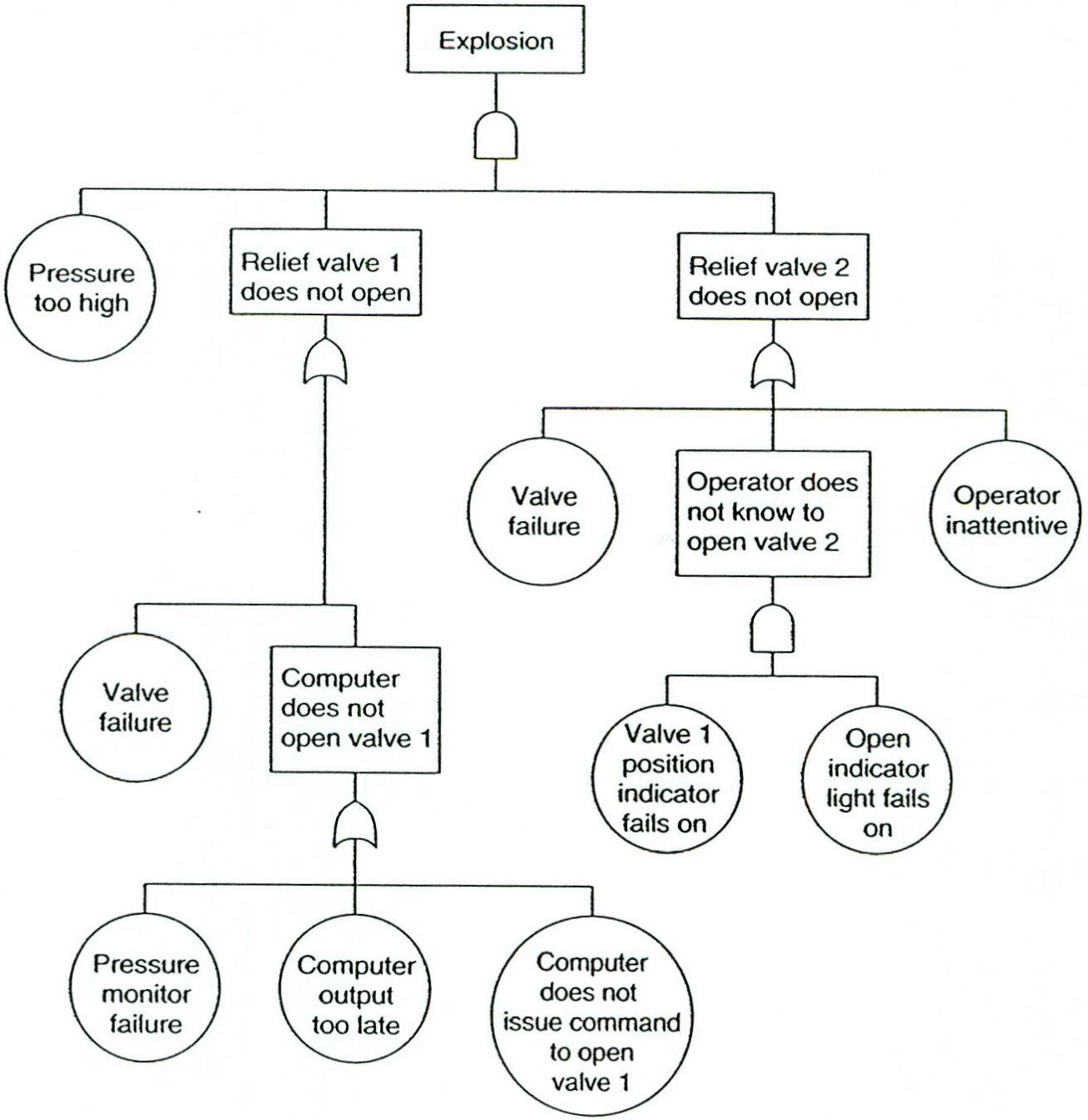
# Fault Tree Analysis (FTA)

- Graphical model that displays the various combinations of equipment failures and human errors that can result in the main system failure of interest.
- Identification/assessment of risk is derived by first identifying faults/hazards.
- A top down approach.

# Definitions

- **FAULT**
  - An abnormal undesirable state of a system or a system element* induced 1) by presence of an improper command or absence of a proper one, or 2) by a failure (see below). All failures cause faults; not all faults are caused by failures. A system which has been shut down by safety features has not faulted.
- **FAILURE**
  - Loss, by a system or system element*, of functional integrity to perform as intended, e.g., relay contacts corrode and will not pass rated current closed, or the relay coil has burned out and will not close the contacts when commanded –the relay has failed; a pressure vessel bursts –the vessel fails.

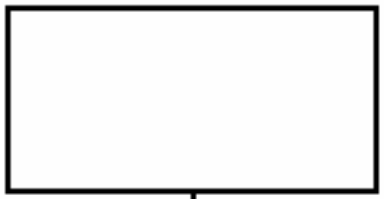
# Fault Tree Example



# Fault Tree Construction

- Each node in the tree can be represented by a combination of events that cause the occurrence of the event, by means of logic gates
- Each gate has inputs and outputs
- An input can be a basic event or an output of another gate
- The development of a fault tree model relies on the analyst's understanding of the system being analyzed
- It is very important to understand the system first in order to build a unbiased fault tree

# Logic (Boolean) Gates

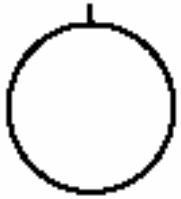


**TOP Event** – forseeable, undesirable event, toward which all fault tree logic paths flow,or **Intermediate event** – describing a system state produced by antecedent events.

Most Fault Tree Analyses can be carried out using only these four symbols.


**"Or" Gate** – produces output if any input exists. Any input, individual, must be (1) necessary and (2) sufficient to cause the output event.


**"And" Gate** – produces output if all inputs co-exist. All inputs, individually must be (1) necessary and (2) sufficient to cause the output event

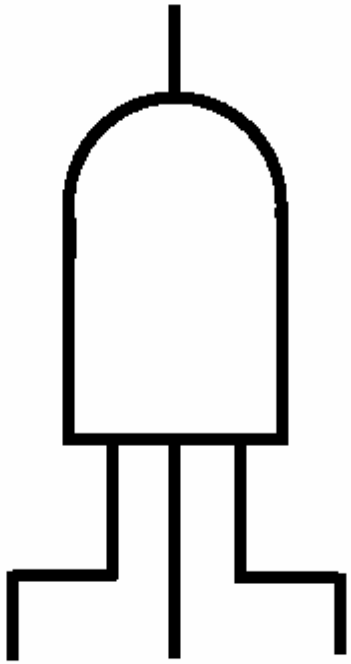


**Basic Event** – Initiating fault/failure, not developed further. (Called "Leaf," "Initiator," or "Basic.") The Basic Event marks the limit of resolution of the analysis.

**Events** and **Gates** are **not** component parts of the system being analyzed. They are symbols representing the logic of the analysis. They are bi-modal. They function flawlessly.

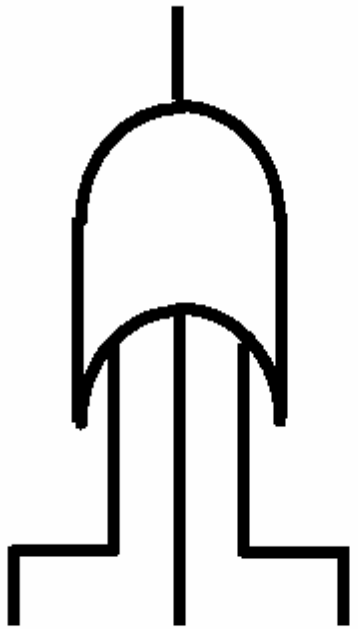
# Standard Symbols for FTA Construction

## AND GATE



Next level failure if **ALL** inputs fail.

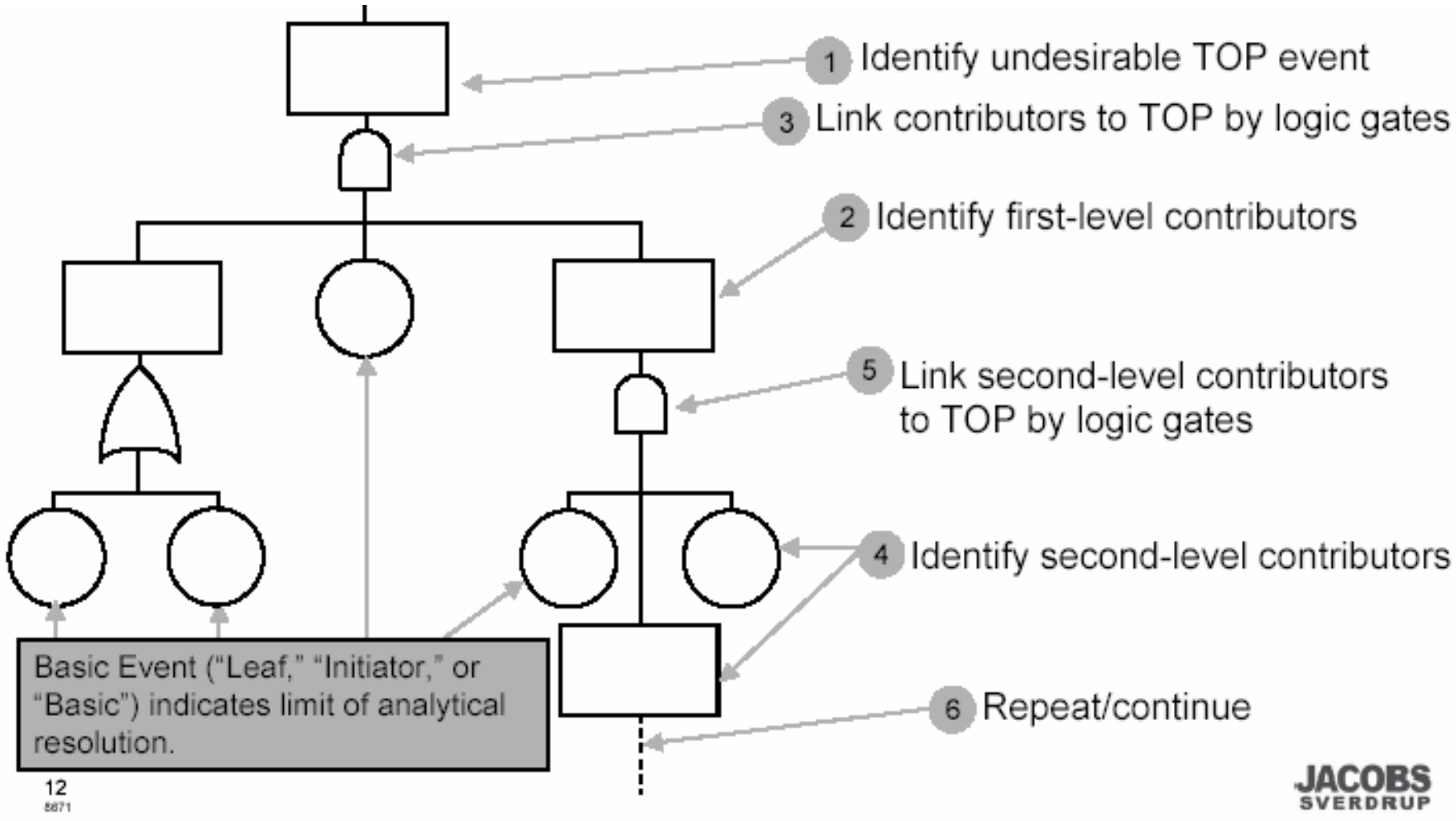
## OR GATE



Next level failure if **ANY** inputs fail.

Table - FTA

# FTA Structure



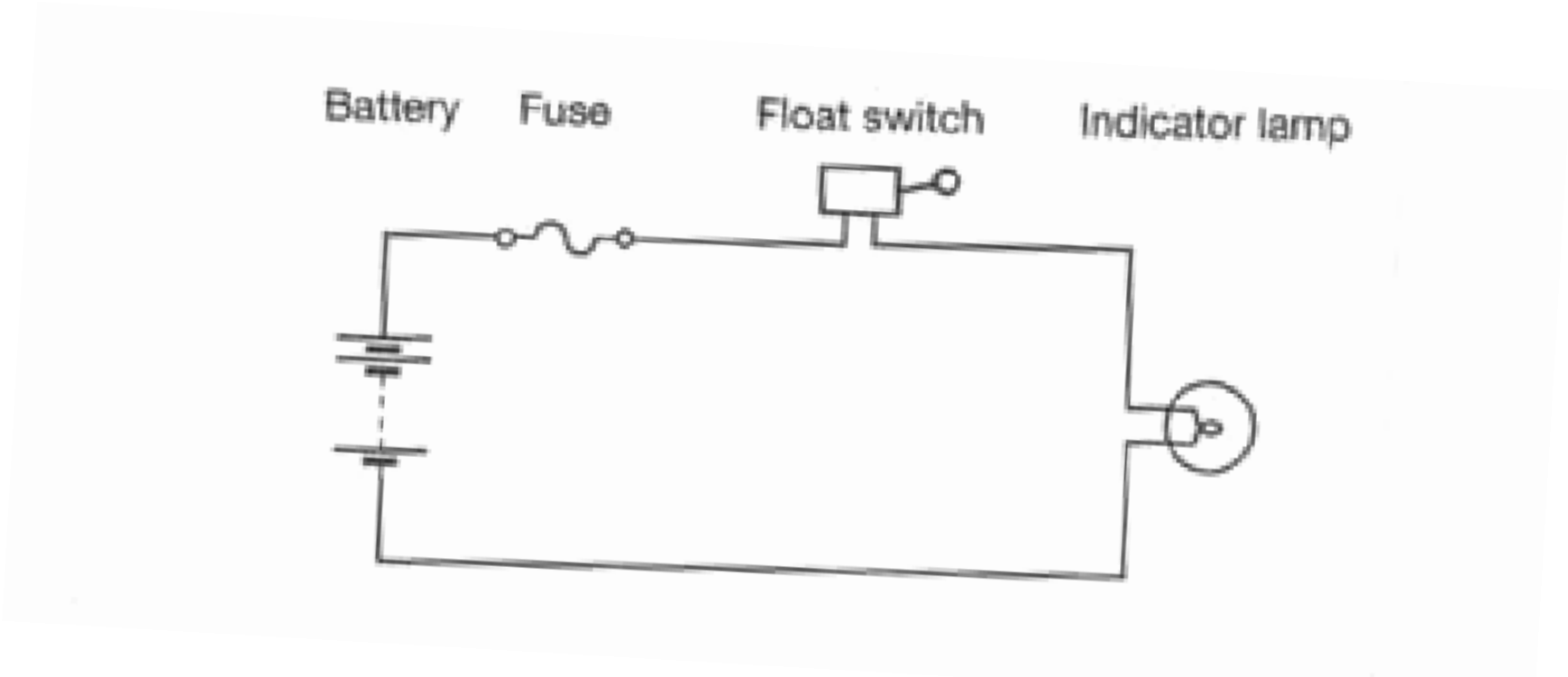



JACOBS SVERDRUP

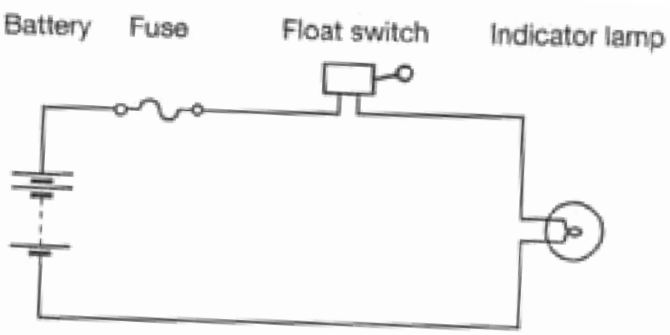
# Identifying TOP Events

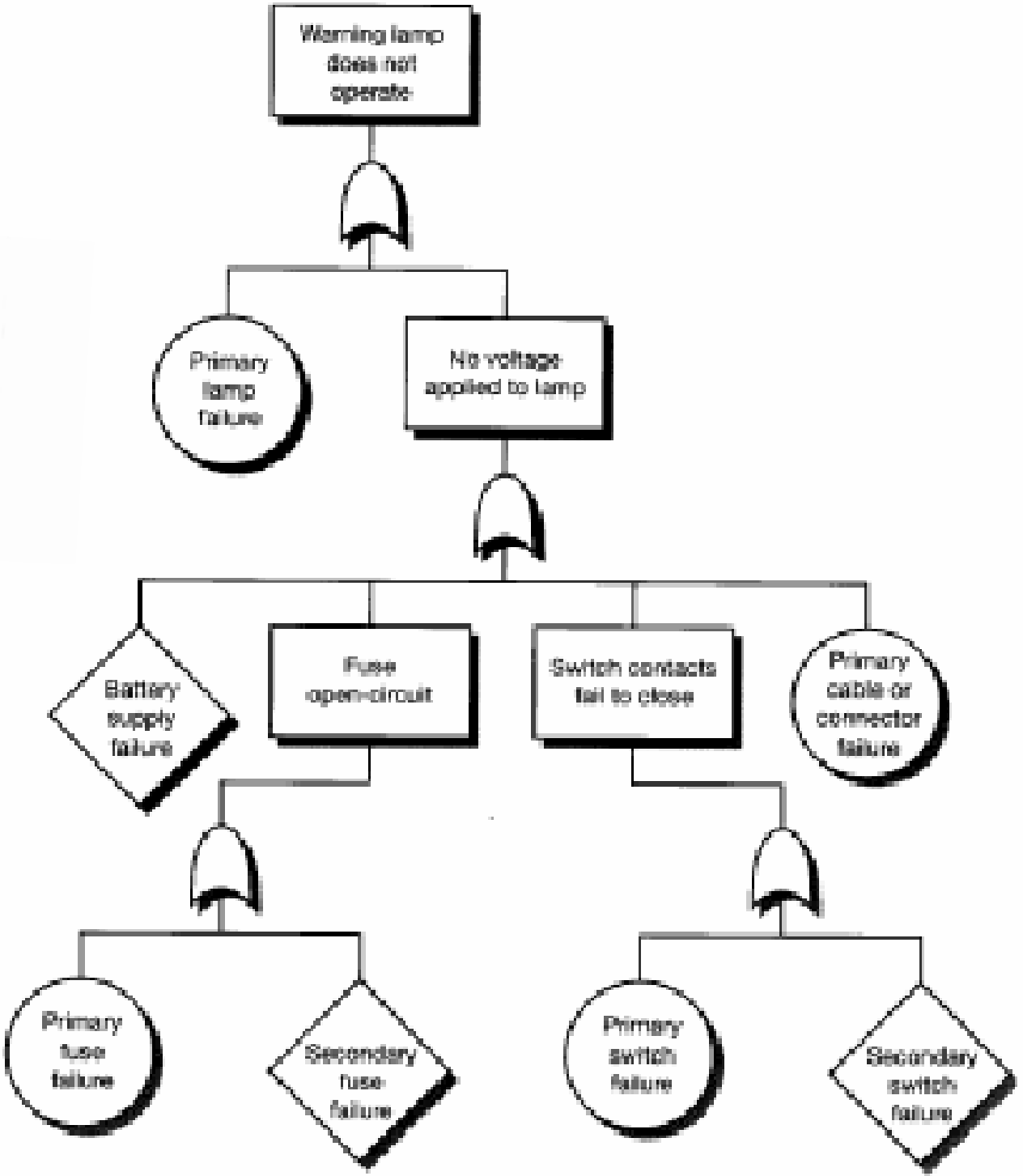
- Explore historical records (own and others).
- Look to energy sources.
- Identify potential mission failure contributors.
- Development “what-if” scenarios.
- Use “shopping lists.”

# FTA Example




Consider lamp failing to illuminate when the fluid level is too low.


Battery
Fuse
Float switch
Indicator lamp


Warning lamp does not operate
Primary lamp failure
No voltage applied to lamp
Battery supply failure
Fuse open-circuit
Switch contacts fail to close
Primary cable or connector failure
Primary fuse failure
Secondary fuse failure
Primary switch failure
Secondary switch failure

# Fault Tree Constraints and Shortcomings

- Undesirable events must be foreseen and are only analyzed singly.
- All significant contributors to fault/failure must be anticipated.
- Each fault/failure initiator must be constrained to two conditional modes when modeled in the tree.
- Initiators at a given analysis level beneath a common gate must be independent of each other.
- Events/conditions at any analysis level must be true, immediate contributors to next-level events/conditions.
- Each Initiator's failure rate must be a predictable

# FTA vs. FMEA

| Selection Characteristic | Preferred | |
|---|---|---|
| | FTA | FMECA |
| Safety of public/operating/maintenance personnel | √ | |
| Small number/clearly defined TOP events | √ | |
| Indistinctly defined TOP events | | √ |
| Full-Mission completion critically important | √ | |
| Many, potentially successful missions possible | | √ |
| "All possible" failure modes are of concern | | √ |
| High potential for "human error" contributions | √ | |
| High potential for "software error" contributions | √ | |
| Numerical "risk evaluation" needed | √ | |
| Very complex system architecture/many functional parts | √ | |
| Linear system architecture with little/human software influence | | √ |
| System irreparable after mission starts | √ | |

*Adapted from "Fault Tree Analysis Application Guide," Reliability Analysis Center, Rome Air Development Center.

# Preparation of a FTA