Hazard Analysis

Hazard (Causal) Analysis

- "Investigating an accident before it happens"
- Goal is to identify causes of accidents (before they occur) so can eliminate or control them in
  - Design
  - Operations

Results can be used in many ways

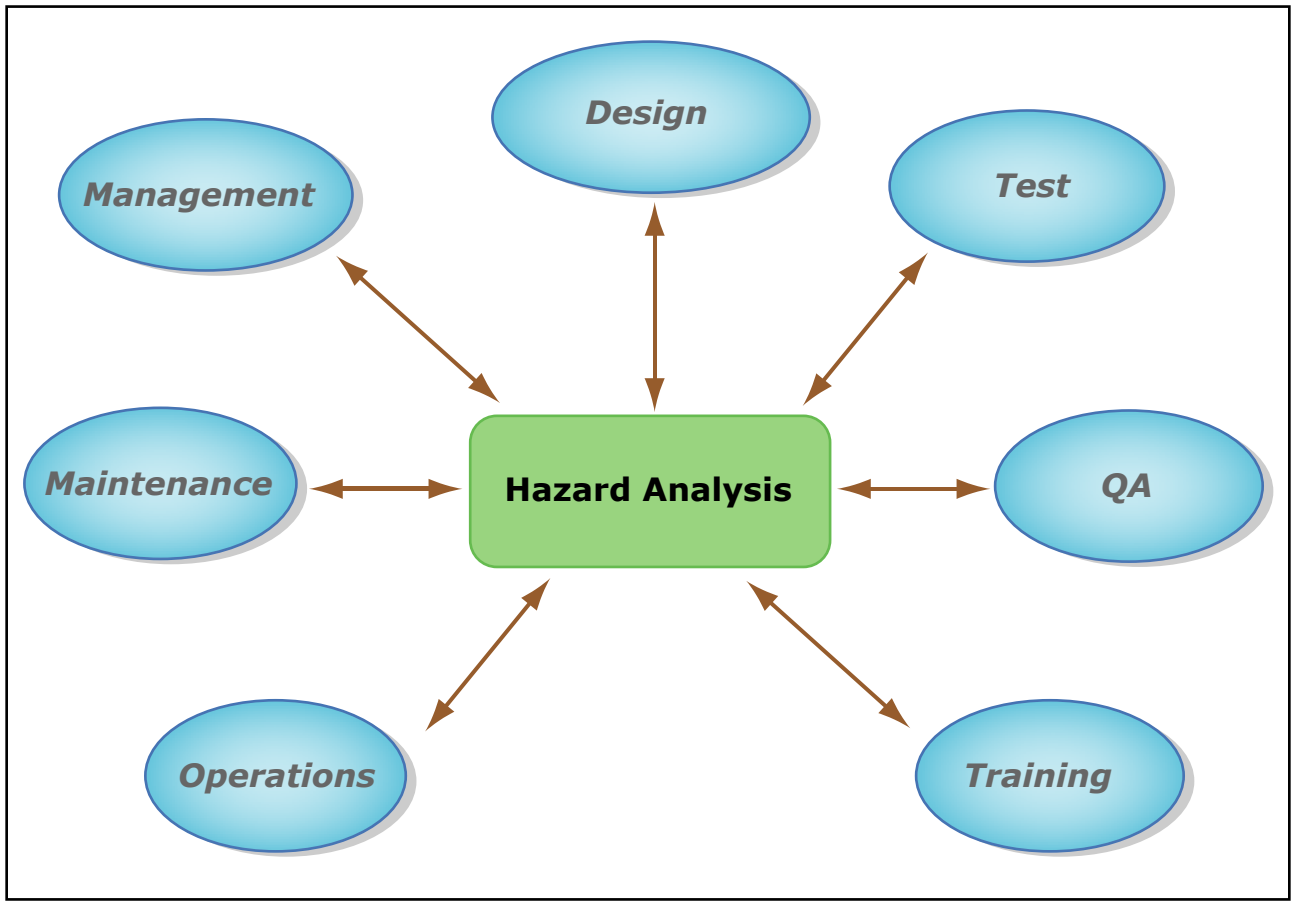


Image by MIT OpenCourseWare.

Hazard (Causal) Analysis

- Requires
  - An accident model
  - A system design model (even if only in head of analyst)

Accident Causality Models

- Underlie all our efforts to engineer for safety
- Explain why accidents occur
- Determine the way we prevent and investigate accidents
- May not be aware you are using one, but you are
- Imposes patterns on accidents

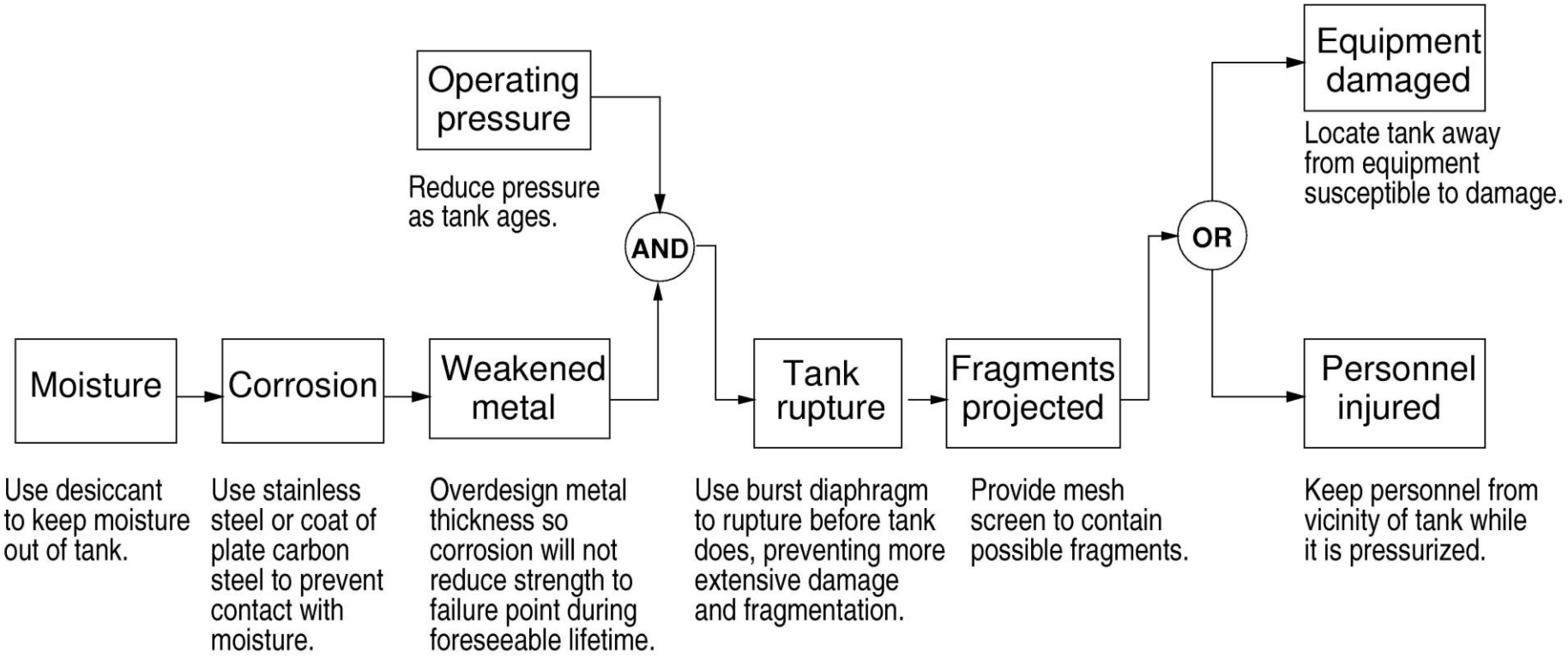
"All models are wrong, some models are useful"

George Box

Chain-of-Events Model

- Explains accidents in terms of multiple events, sequenced as a forward chain over time.
  - Simple, direct relationship between events in chain
- Events almost always involve component failure, human error, or energy-related event
- Forms the basis for most safety engineering and reliability engineering analysis and for design:

Chain-of-events example



From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Informal Class Exercise

- What is the chain of events for the Forest Service helicopter (Carson) crash?
- Are the factors you found for the exam in the chain of events? Which ones are missing?
- This was only one accident. How difficult do you think it would be to find all the different paths to a loss of the helicopter?

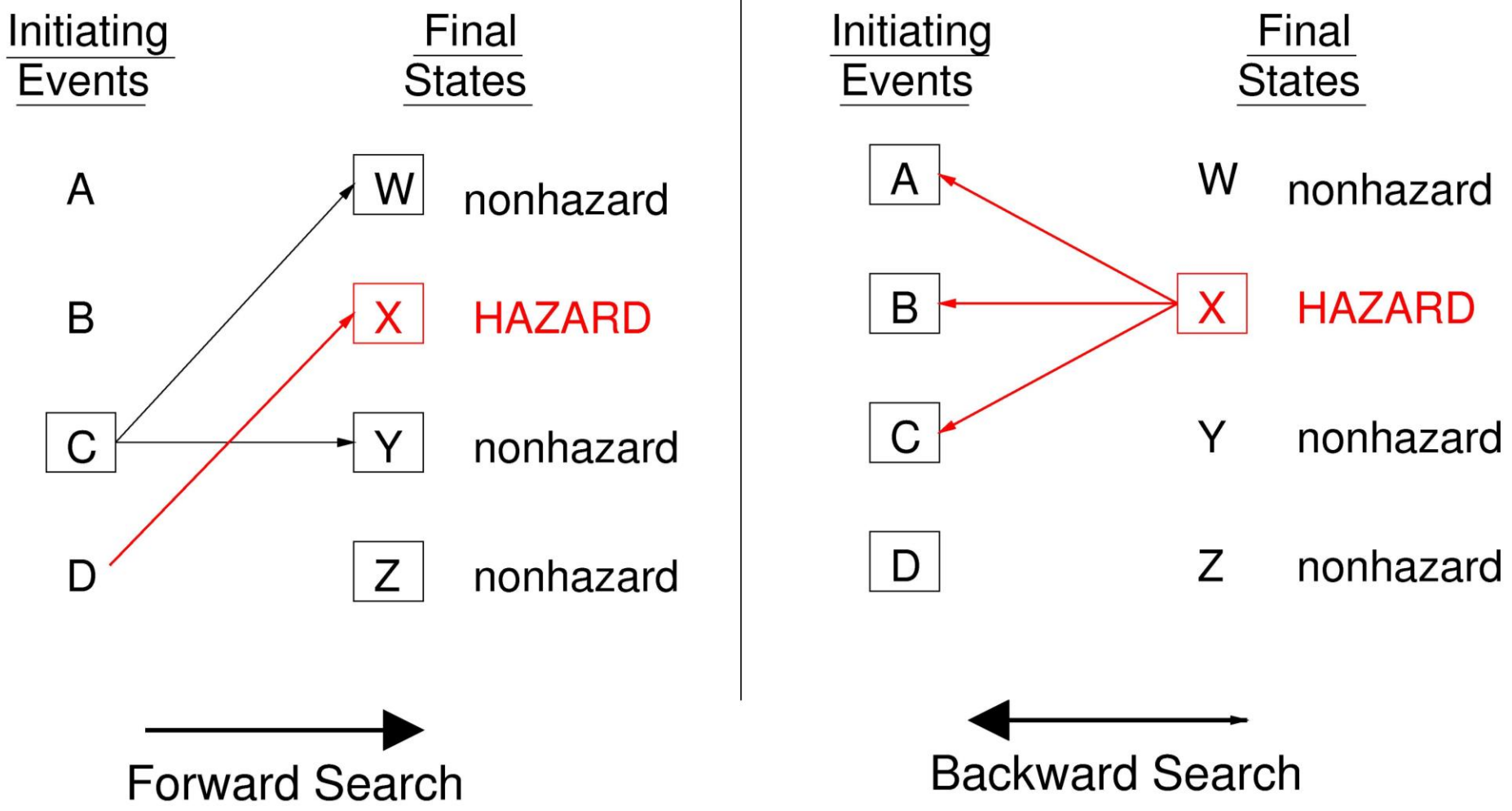
How Find the Possible Chains Without Having An Accident First?

- Almost always involves some type of search through the system design (model) for states or conditions that could lead to system hazards.

  Forward
  Backward
  Top-down
  Bottom-up

  Need some way to organize the search

Forward vs. Backward Search



FMEA: A Forward Search Technique

FMEA for a System of Two Amplifiers in Parallel

Component	Failure probability	Failure mode	% Failures by mode	Effects	
				Critical	Noncritical
A	$1x10^{-3}$	Open	90		X
		Short	5	$5x10^{-5}$	
		Other	5	$5x10^{-5}$	
B	$1x10^{-3}$	Open	90		X
		Short	5	$5x10^{-5}$	
		Other	5	$5x10^{-5}$	

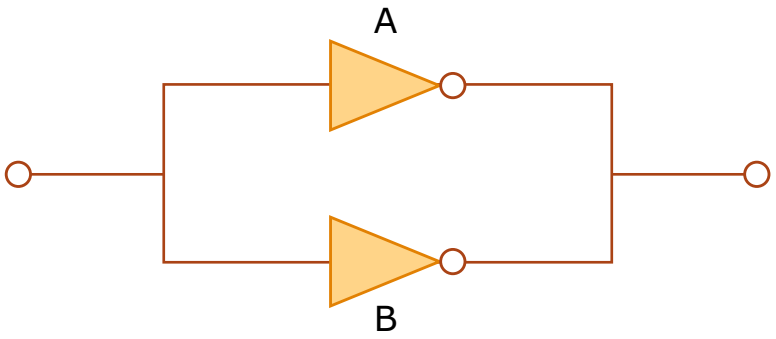


Image by MIT OpenCourseWare.

A Sample FMECA

Failure Modes and Effects Criticality Analysis

Subsystem _____

Prepared by _____

Date _____

Item	Failure Modes	Cause of Failure	Possible Effects	Prob.	Level	Possible action to reduce failure rate or effects
Motor case	Rupture	a. Poor workmanship b. Defective materials c. Damage during transportation d. Damage during handling e. Overpressurization	Destruction of missile	0.0006	Critical	Close control of manufacturing process to ensure that workmanship meets prescribed standards. Rigid quality control of basic materials to eliminate defectives. Inspection and pressure testing of completed cases. Provision of suitable packaging to protect motor during transportation.

Image by MIT OpenCourseWare.

5 Whys Example (A Backwards Analysis)

Problem: The Washington Monument is disintegrating.

Why is it disintegrating?

Because we use harsh chemicals

Why do we use harsh chemicals?

To clean pigeon droppings off the monument

Why are there so many pigeons?

They eat spiders and there are a lot of spiders at monument

Why are there so many spiders?

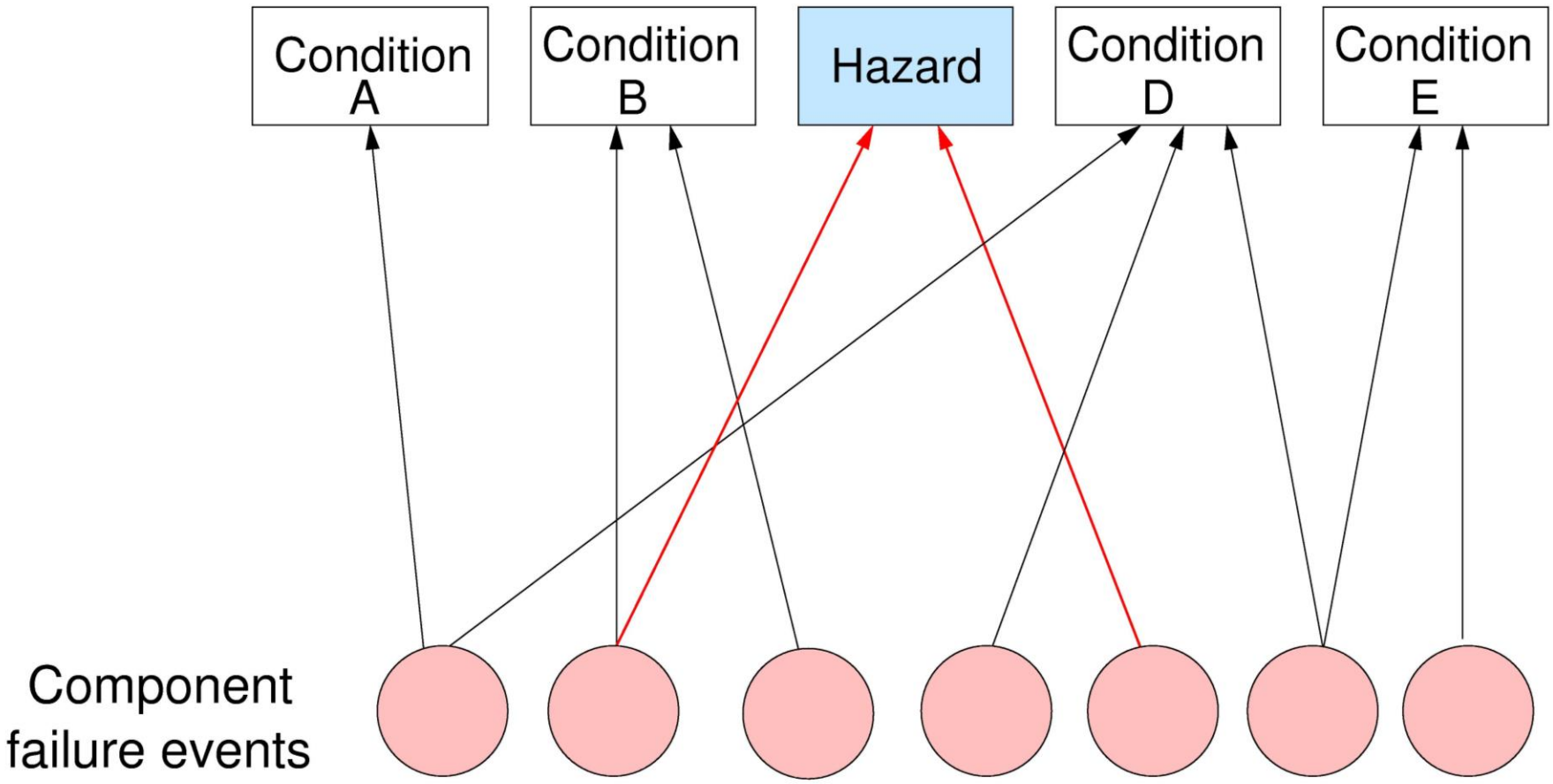
They eat gnats and lots of gnats at monument

Why so many gnats?

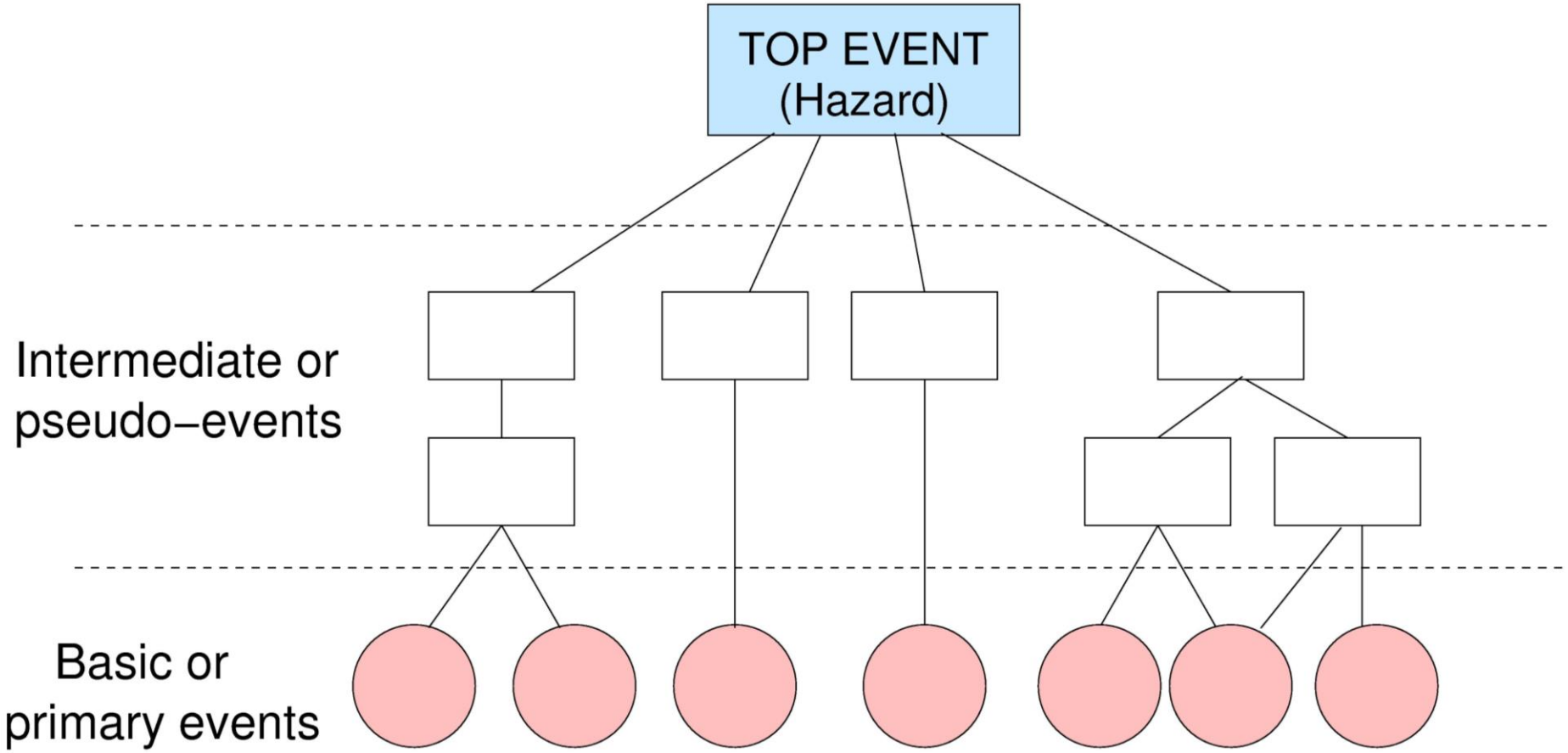
They are attracted to the lights at dusk

<u>Solution</u>: Turn on the lights at a later time.

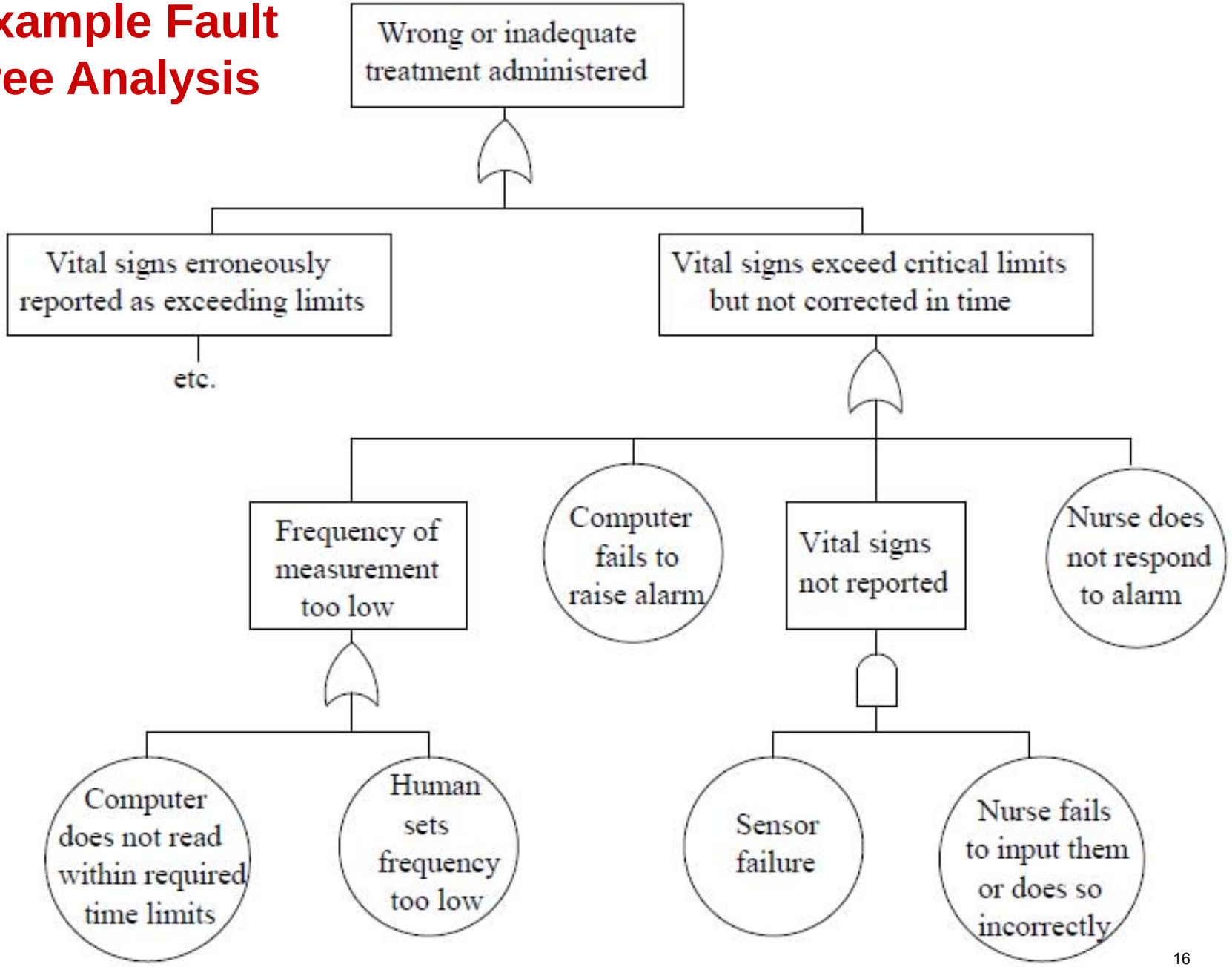
Bottom-Up Search



Top-Down Search



Example Fault Tree Analysis



Fault Tree Example

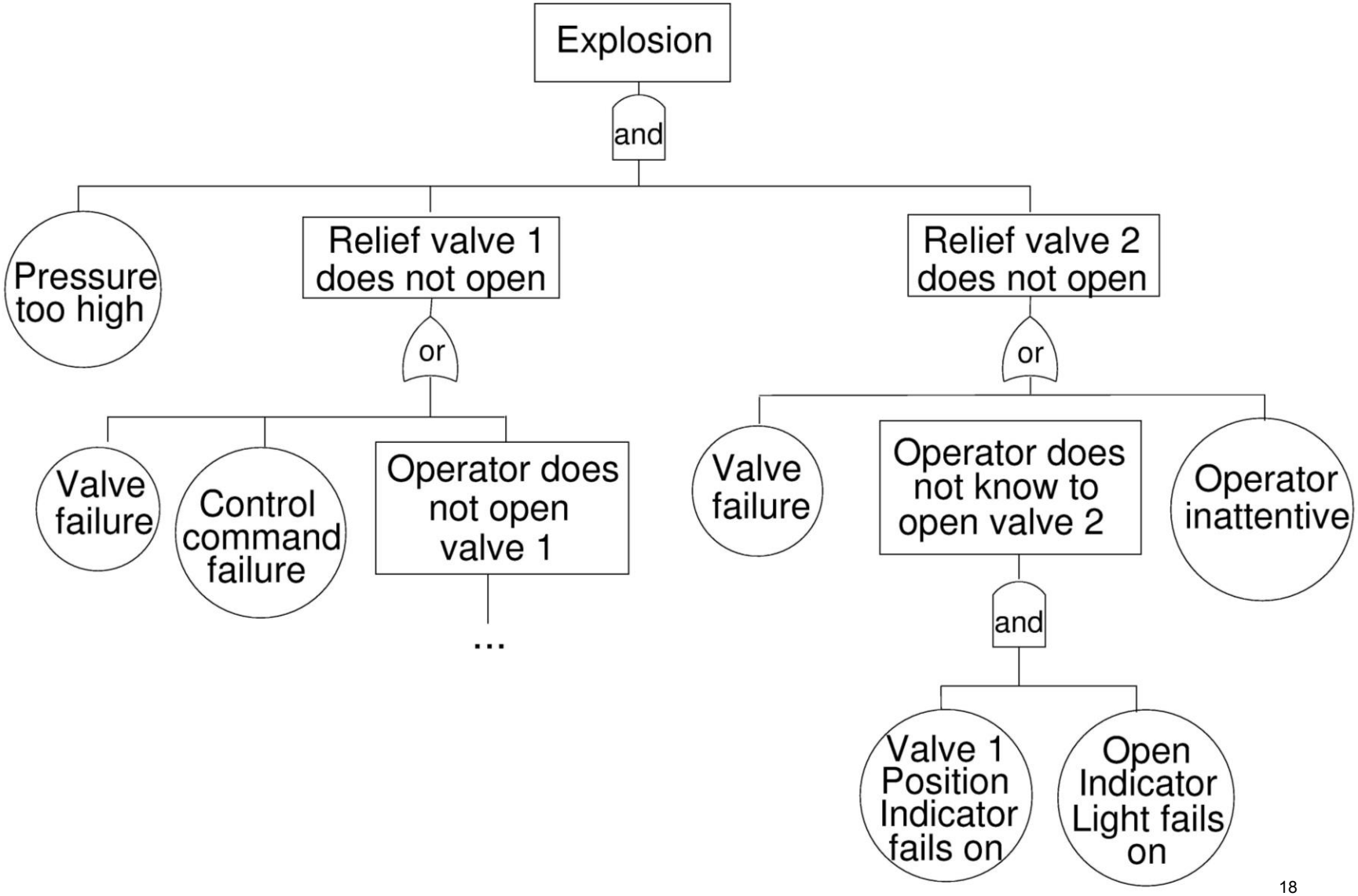
- **Hazard**: Explosion
- **Design**:

  System includes a relief valve opened by an operator to protect against over-pressurization. A secondary valve is installed as backup in case the primary valve fails. The operator must know if the primary valve does not open so the backup valve can be activated.

  Operator console contains both a primary valve position indicator and a primary valve open indicator light.

Draw a fault tree for this hazard and system design.

Fault Tree Example



Example of Unrealistic Risk Assessment Leading to an Accident

- **System Design**: previous over-pressurization example
- **Events**: The open position indicator light and open indicator light both illuminated. However, the primary valve was NOT open, and the system exploded.
- **Causal Factors**: Post-accident examination discovered the indicator light circuit was wired to indicate presence of power at the valve, but it did not indicate valve position. Thus, the indicator showed only that the activation button had been pushed, not that the valve had opened. An extensive quantitative safety analysis of this design had assumed a low probability of simultaneous failure for the two relief valves, but ignored the possibility of design error in the electrical wiring; the probability of design error was not quantifiable. No safety evaluation of the electrical wiring was made; instead, confidence was established on the basis of the low probability of coincident failure of the two relief valves.

16.63J / ESD.03J System Safety
Fall 2012