Traditional Hazard Analysis

Agenda

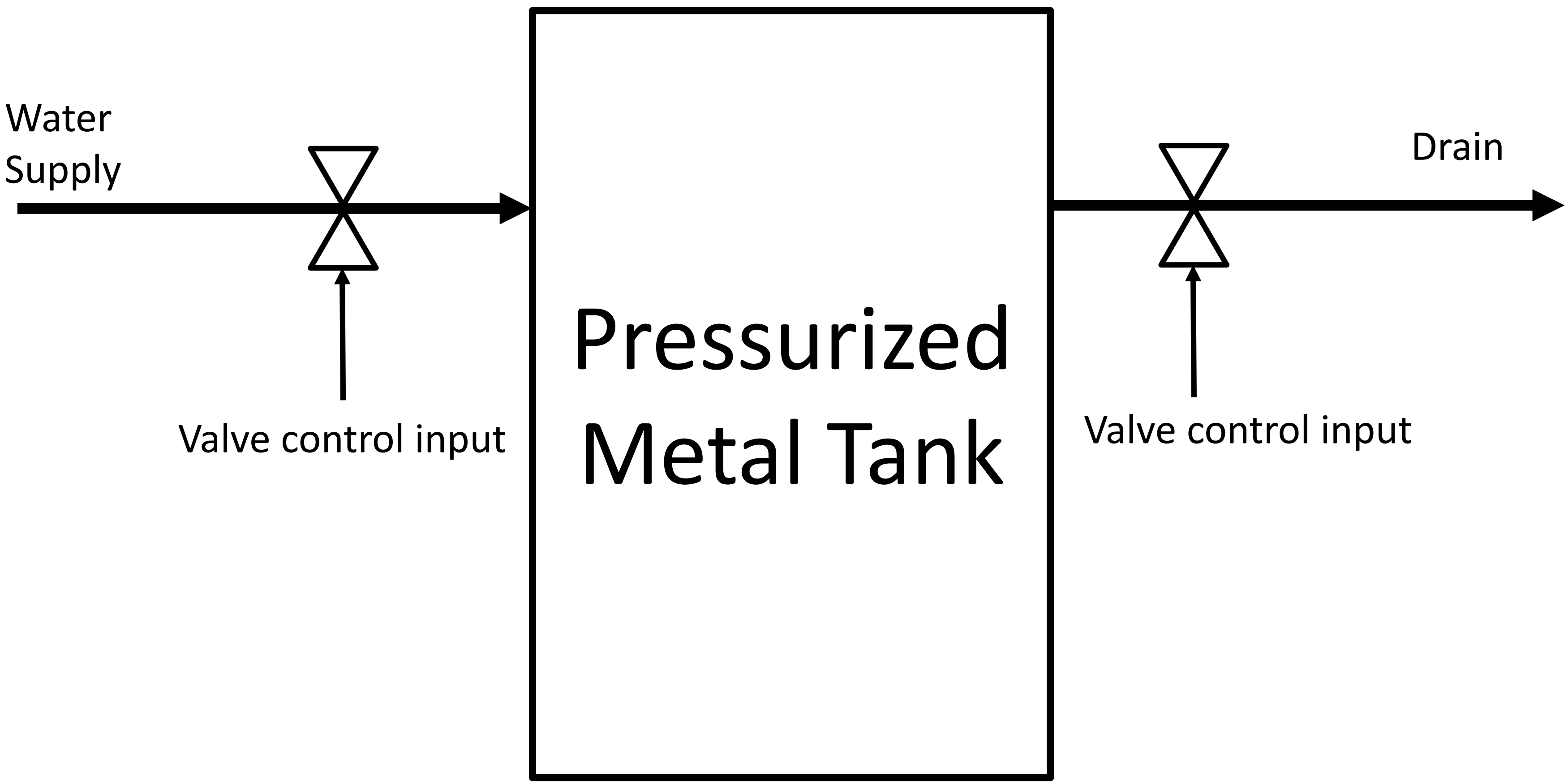
- Today
  - Intro to Hazard Analysis
  - Traditional Qualitative Methods
    - FMEA
    - FTA
    - ETA
    - HAZOP
  - Strengths / Limitations
- Next: Traditional Quantitative Methods
  - FMECA
  - FTA
  - PRA
  - Strengths / Limitations

Hazard (Causal) Analysis

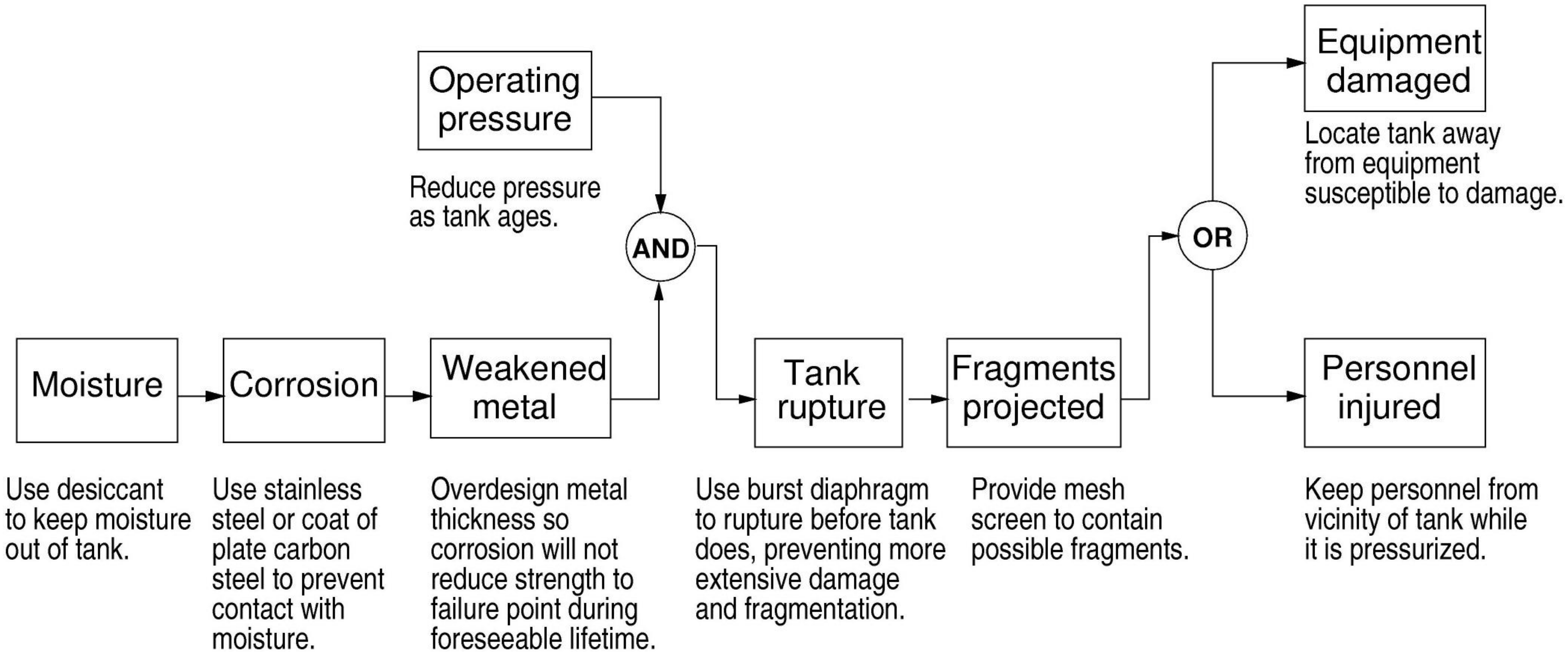
- "Investigating an accident before it happens"
- Goal is to identify causes of accidents (before they occur) so can eliminate or control them in
  - Design
  - Operations
- Requires
  - A system design model
  - An accident model

(even if only in the mind of the analyst)

Physical System Design Model (simplified)



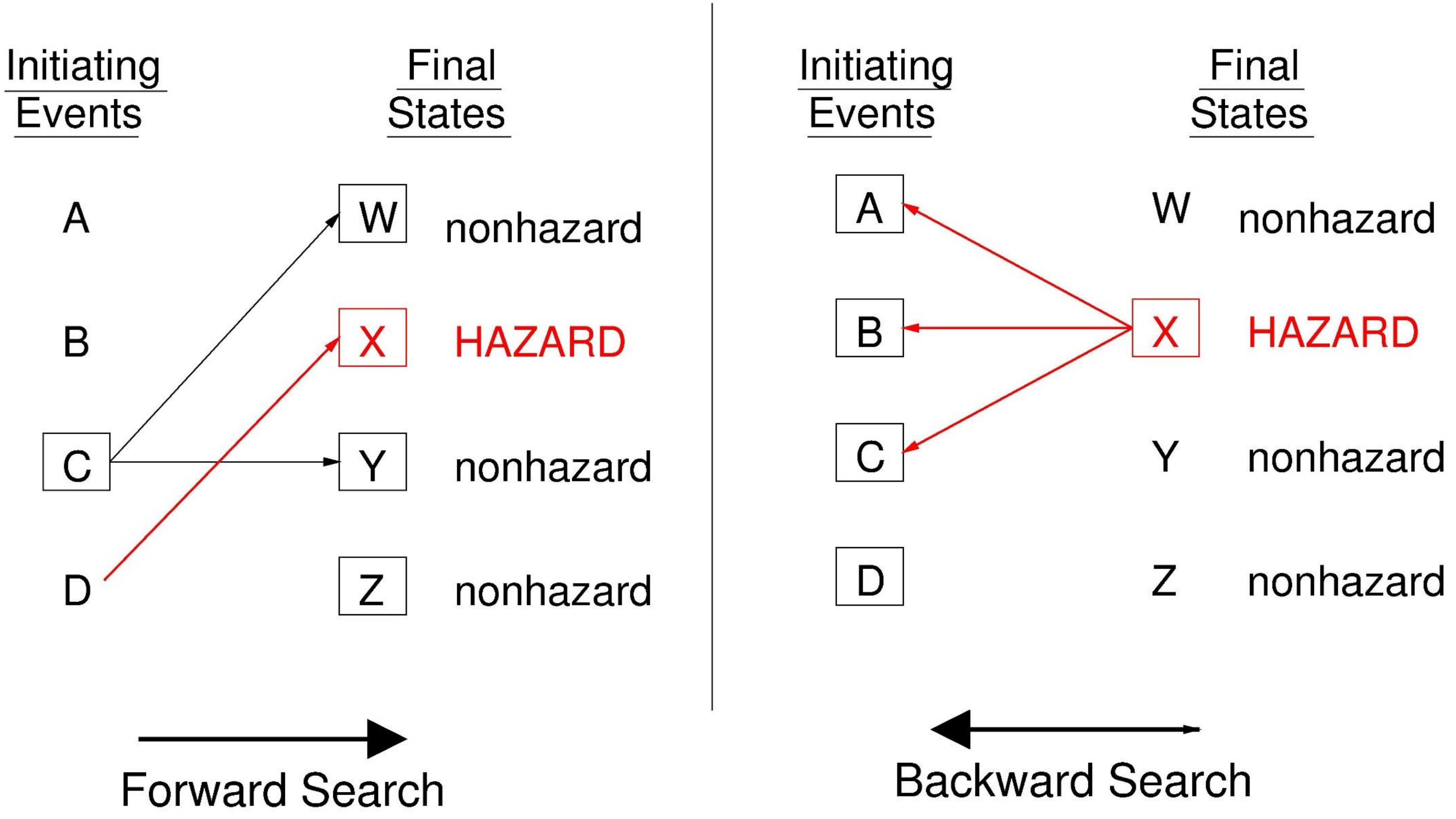
Chain-of-events example



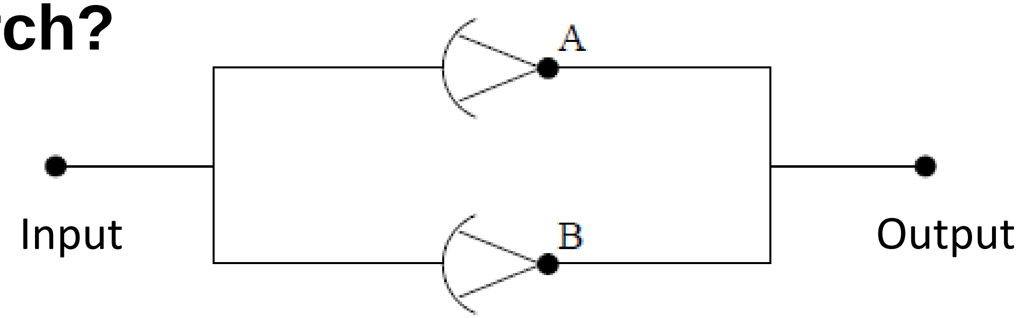
From Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

How do you find the chain of events before an accident?

Forward vs. Backward Search

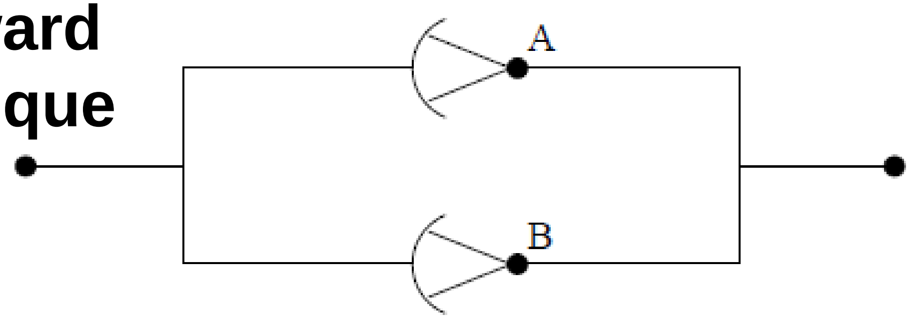


Forward search?



a system of two amplifiers in parallel.

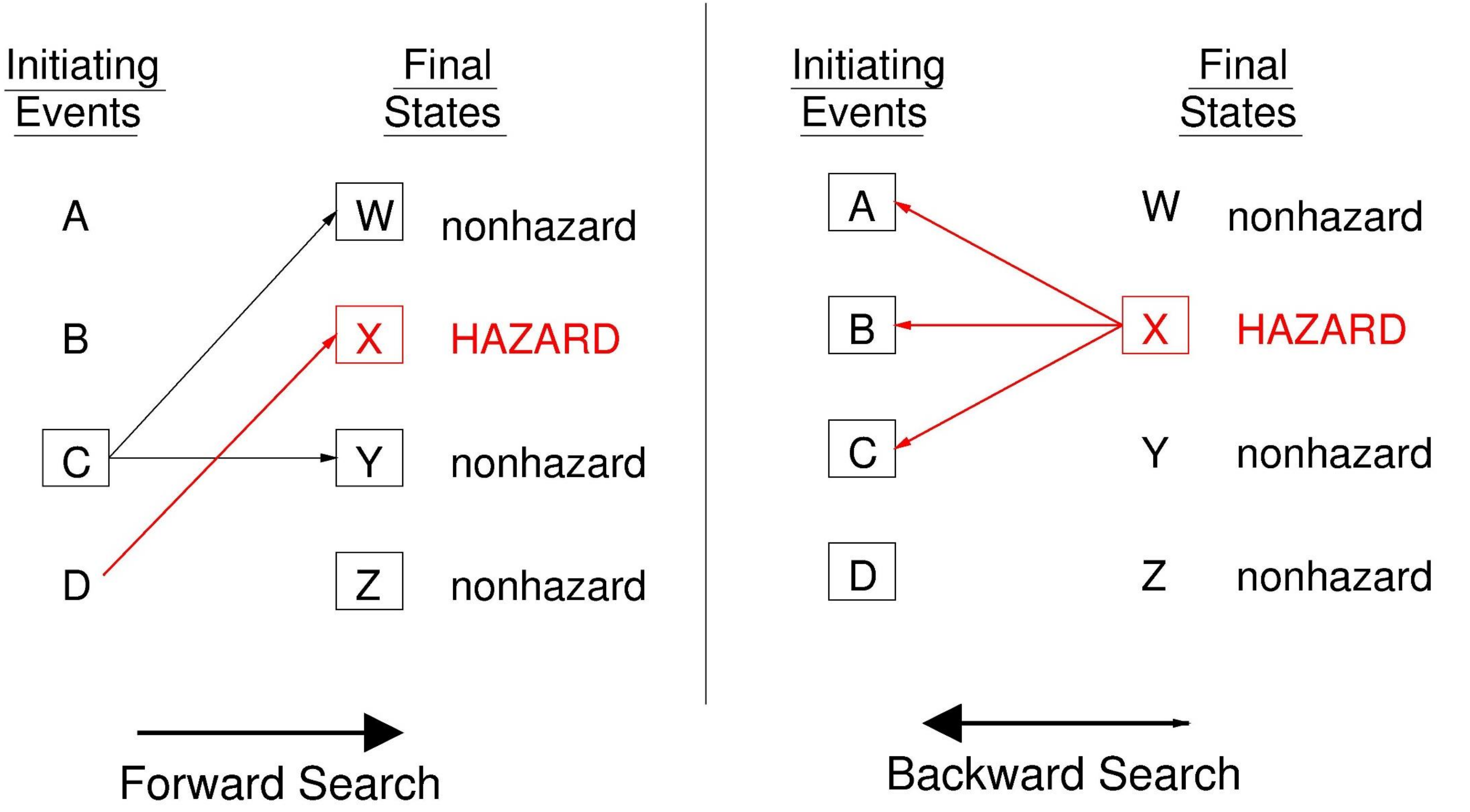
FMEA: A Forward Search Technique



Component		Failure mode		Effects	
				Critical	Noncritical
A		Open			X
		Short		X	
		Other		X	
B		Open			X
		Short		X	
		Other		X	

Figure 3: FMEA for a system of two amplifiers in parallel. (Source: W.E. Vesely, F.F. Goldberg, N.H. Roberts, and D.F. Haasl, *Fault Tree Handbook*, NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, D.C., 1981, page II-3)

Forward vs. Backward Search



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.

Why was the Washington Monument disintegrating?

There was a time when the Washington Monument was disintegrating. A research team realised that this was happening because of the harsh chemicals used to clean the monument.

The reason why harsh chemicals were used was because there was a lot of pigeon poop on the monument which needed regular cleaning up.

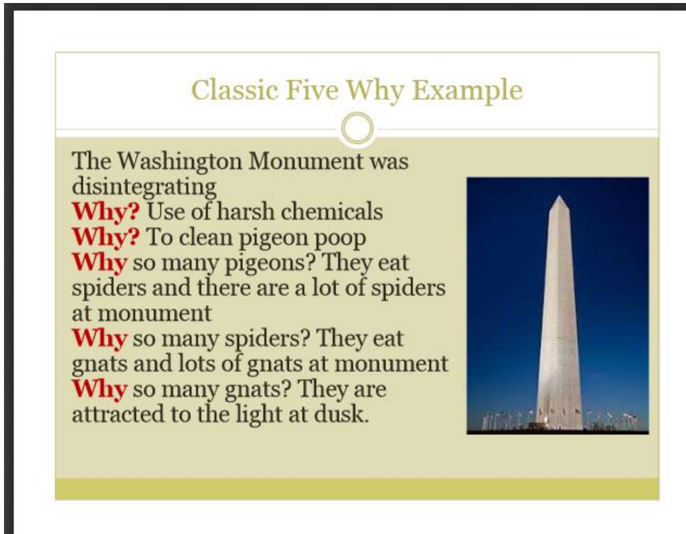
The reason why there was so much pigeon poop was that a lot of pigeons were attracted to the monument because they loved eating spiders, and there were a lot of spiders there.

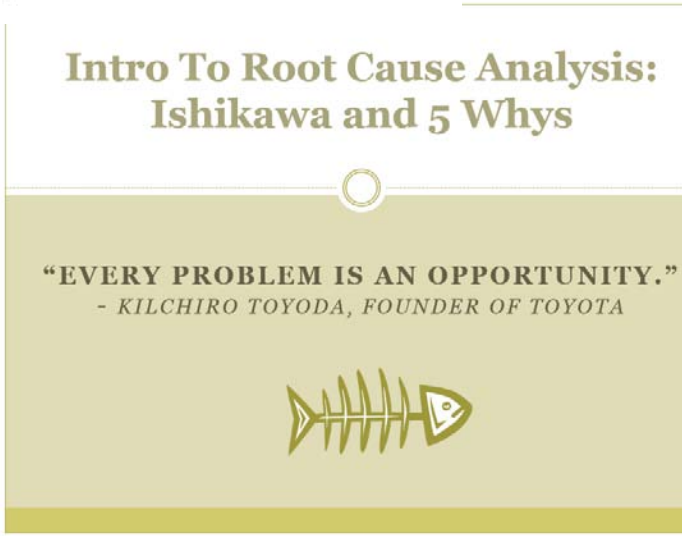
The reason why there were so many spiders was that the spiders eat gnats and there were a lot of gnats around the monument.

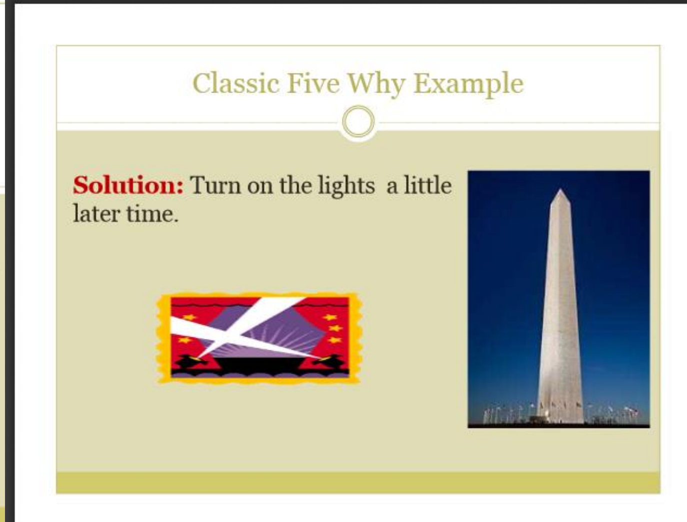
The reason why there were so many gnats around the monument was that they were attracted to the bright lights which were switched on at dusk.

So, at the end of the root cause analysis, the most effective solution was to turn on the lights not at dusk but a little later!

Who would have imagined that the solution to protecting a monument could be so simple and yet so effective as not switching on the lights at dusk. Such is the power of finding the right root cause.



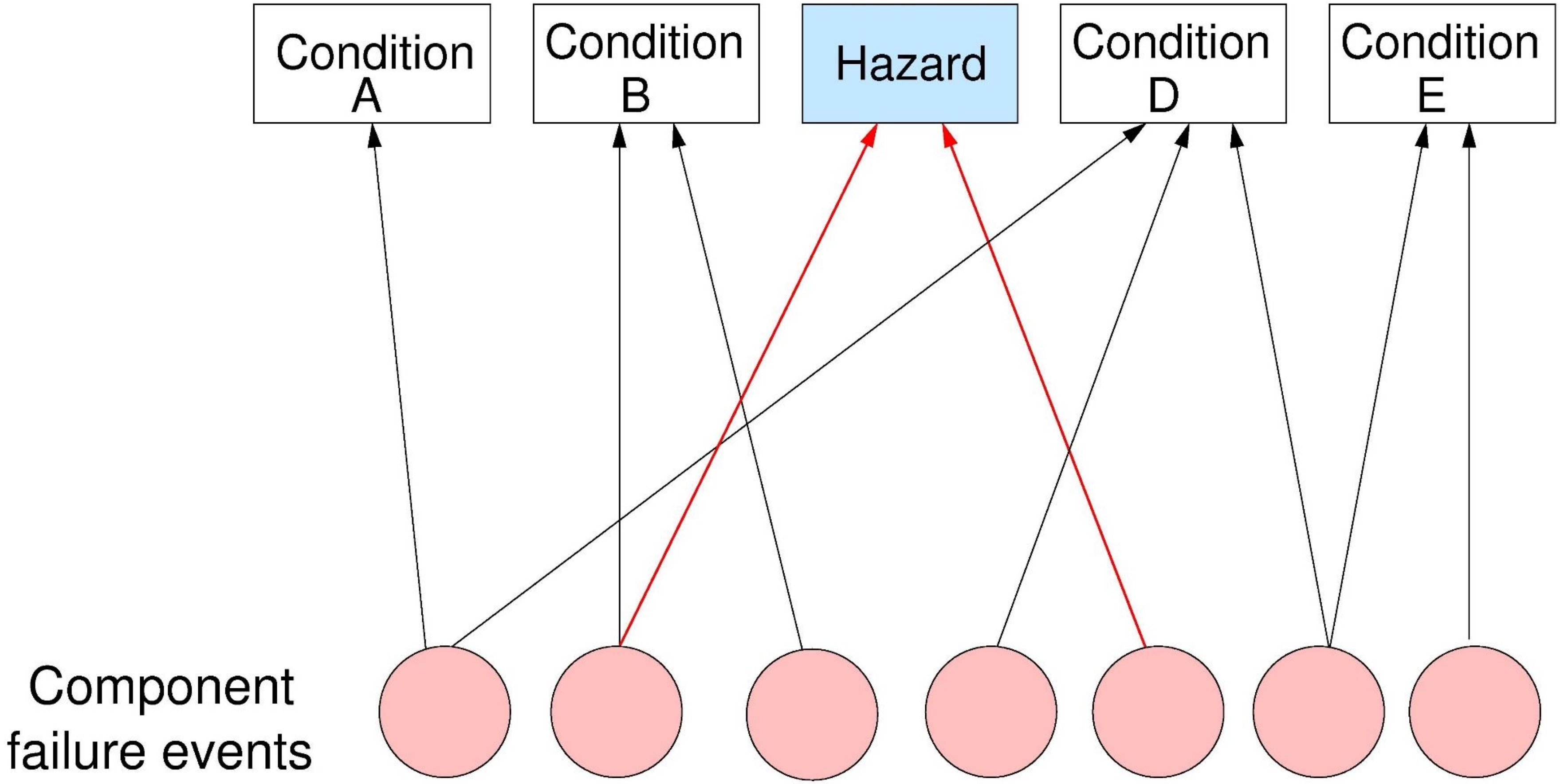




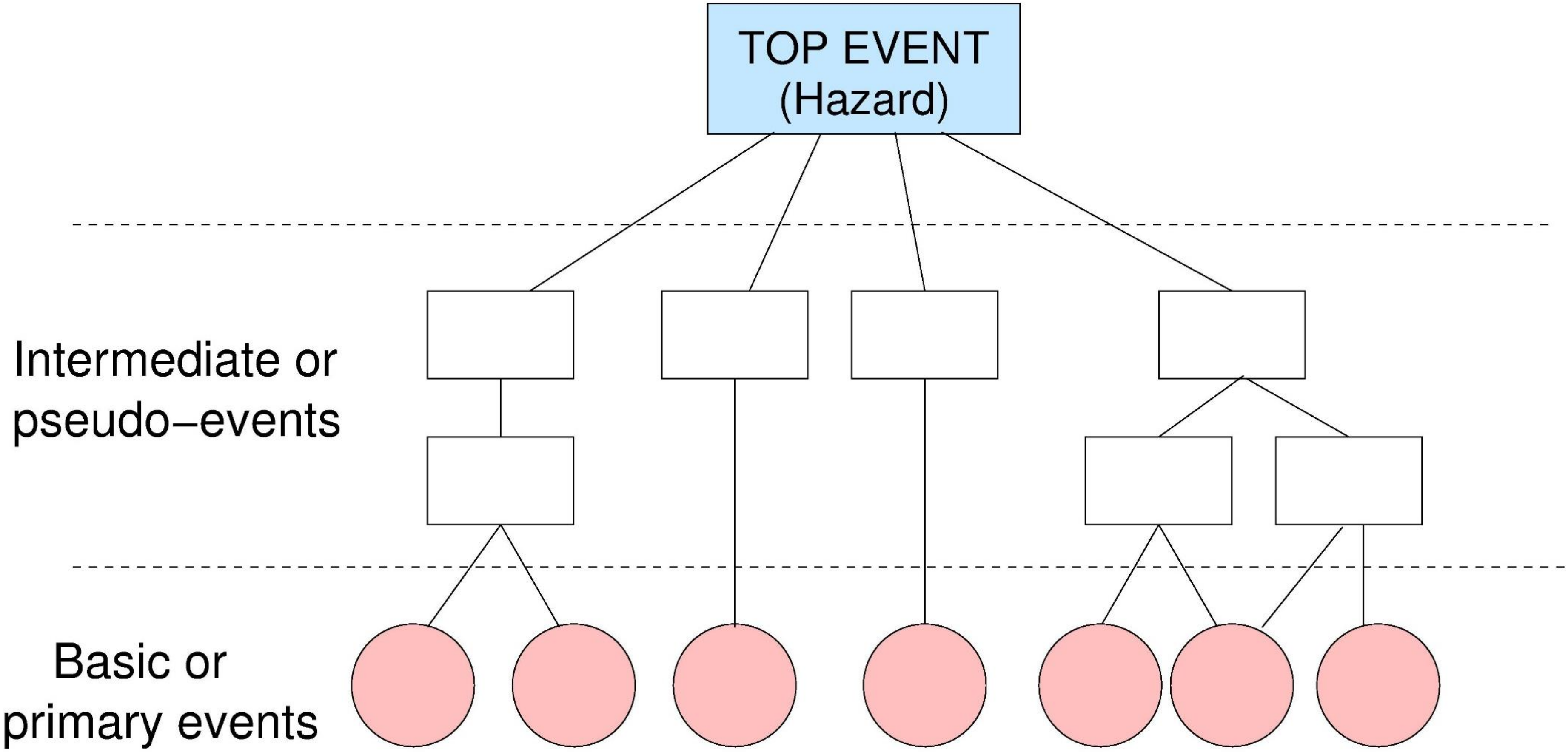
"Breaking the accident chain of events" (see video)

http://www.lean.ohio.gov/Portals/0/docs/training/GreenBelt/GB_Fishbone%20Diagram.pdf

Bottom-Up Search



Top-Down Search



Top-Down Example

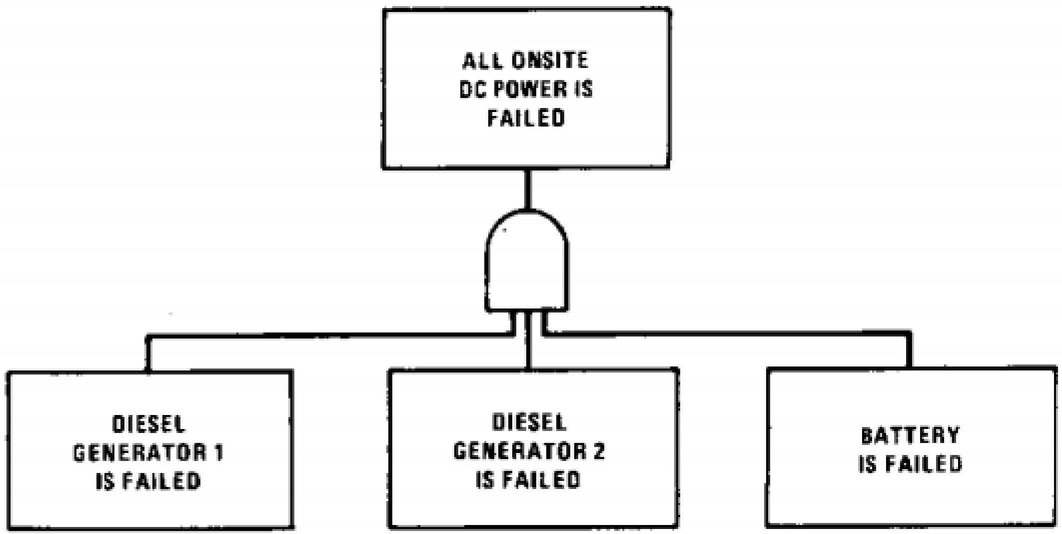


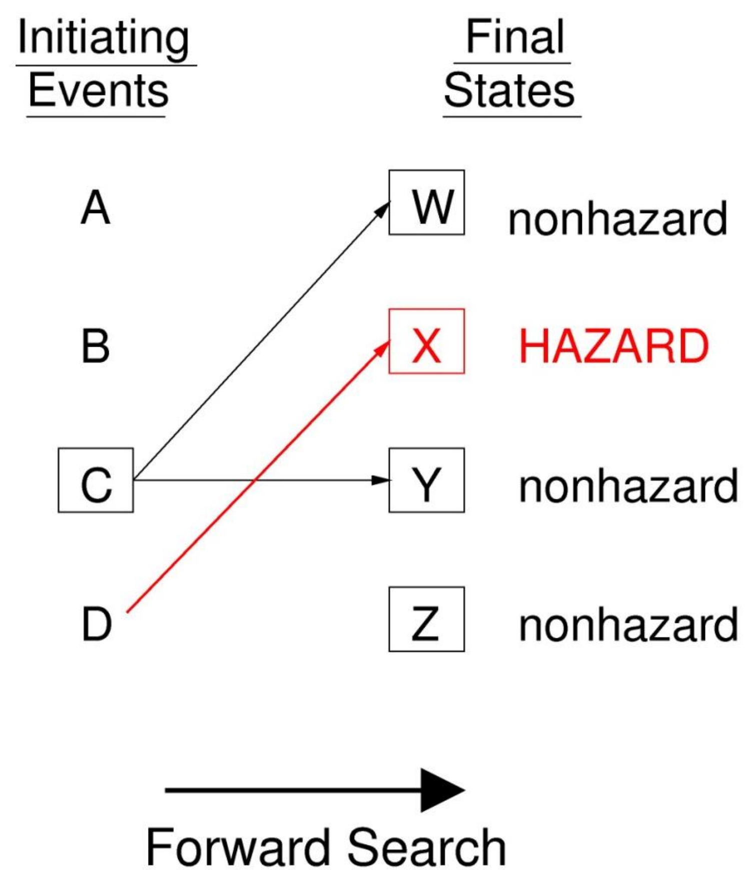
Image from Vesely

Traditional Qualitative Methods

FMEA (Failure Modes and Effects Analysis)

FMEA: Failure Modes and Effects Analysis

- 1949: MIL-P-1629
- Forward search technique
  - *Initiating event*: component failure
  - *Goal*: identify effect of each failure

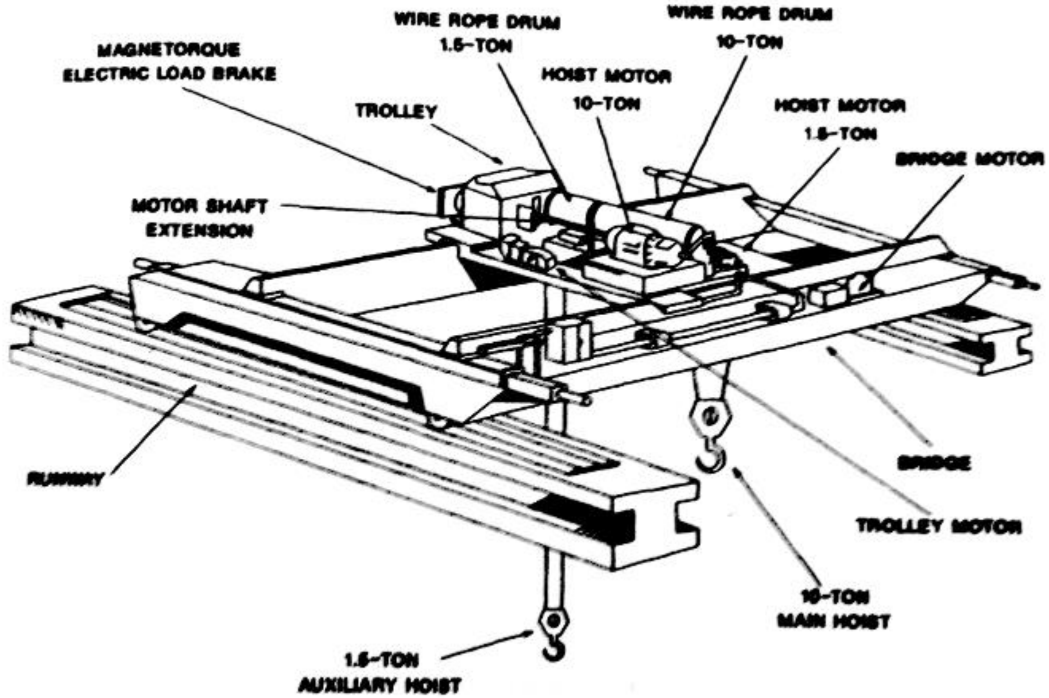


General FMEA Process

1. Identify individual components
2. Identify failure modes
3. Identify failure mechanisms (causes)
4. Identify failure effects

FMEA worksheet

Example: Bridge crane system



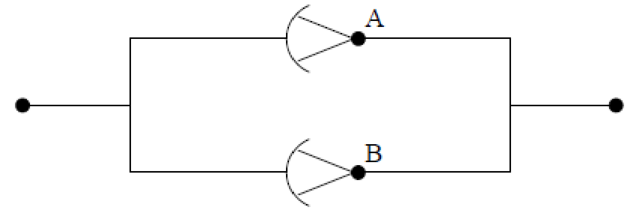
Failure Mode and Effect Analysis

Program:_________ System:_________ Facility:________
Engineer:_________ Date:___________ Sheet:_________

Component Name	Failure Modes	Failure Mechanisms	Failure effects (local)	Failure effects (system)
Main hoist motor	Inoperative, does not move	Defective bearings Motor brushes worn Broken springs	Main hoist cannot be raised. Brake will hold hoist stationary	Load held stationary, cannot be raised or lowered.

*FMEA example adapted from (Vincoli, 2006)

FMECA: A Forward Search Technique



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	$5x10^{-5}$	

Based on prior experience with this type of amplifier, we estimate that 90% of amplifier failures can be attributed to the "open" mode, 5% of them to the "short" mode, and the balance of 5% to the "other" modes. We know that whenever either amplifier fails shorted, the system fails so we put X's in the "Critical" column for these modes; "Critical" thus means that the single failure causes system failure. On the other hand, when either amplifier fails open, there is no effect on the system from the single failure because of the parallel configuration. What is the criticality of the other 28 failure modes? In this example we have been conservative and we are considering them all as critical, i.e., the occurrence of any one causes system failure. The numbers shown in the Critical column are obtained from multiplying the appropriate percentage in Column 4 by 10^{-3} from Column 2.

FMEA uses an accident model

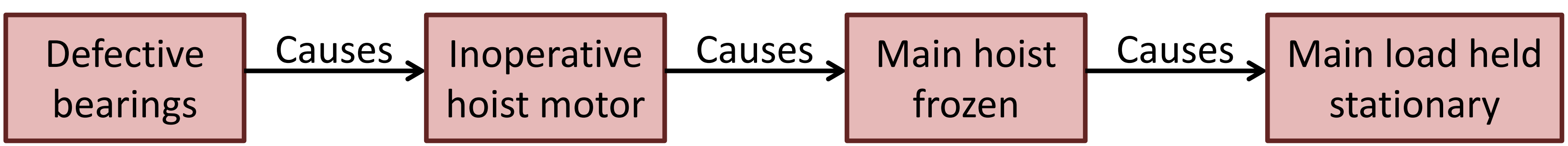
FMEA method:

Failure Mode and Effect Analysis

Program:_________ System:_________ Facility:________
Engineer:_________ Date:___________ Sheet:__________

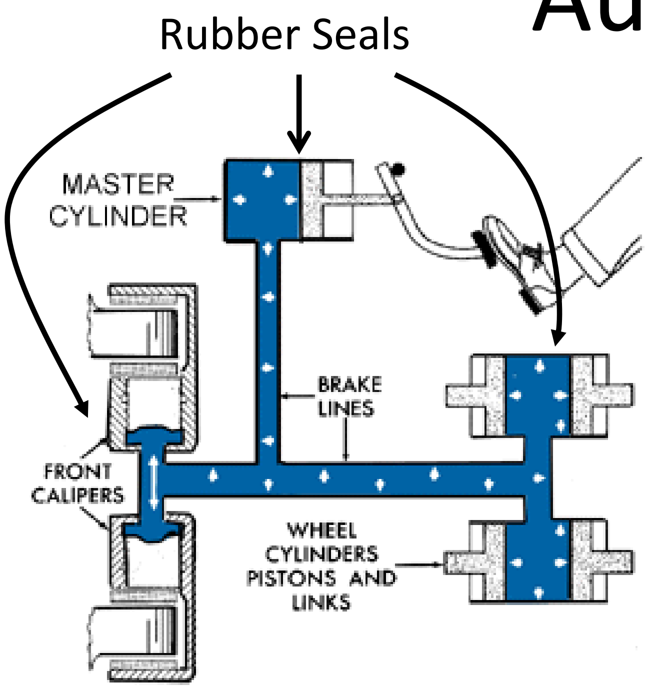
Component Name	Failure Modes	Failure Mechanisms	Failure effects (local)	Failure effects (system)
Main Hoist Motor	Inoperative, does not move	Defective bearings Loss of power Broken springs	Main hoist cannot be raised. Brake will hold hoist stationary	Load held stationary, cannot be raised or lowered.

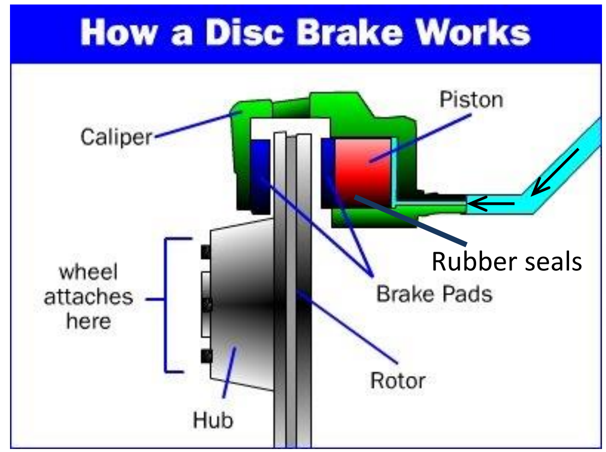
Accident model: Chain-of-events



*FMEA example adapted from (Vincoli, 2006)

FMEA Exercise
Automotive brakes





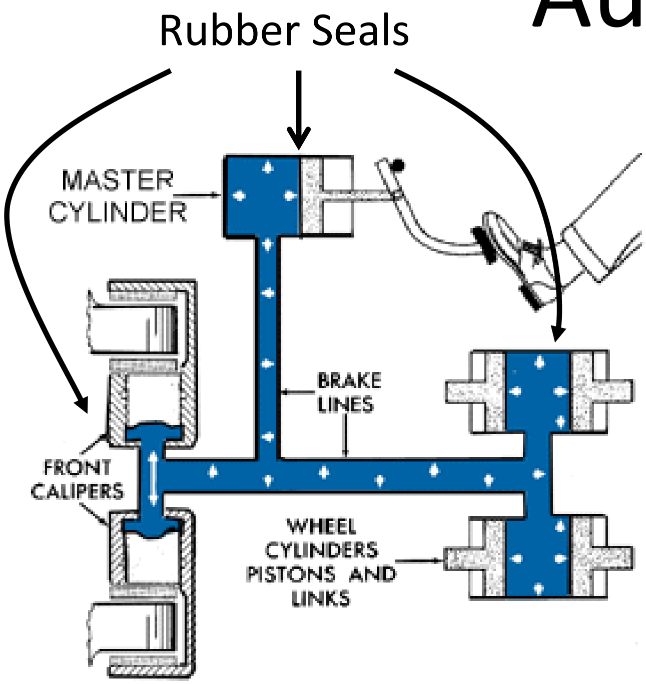
System components

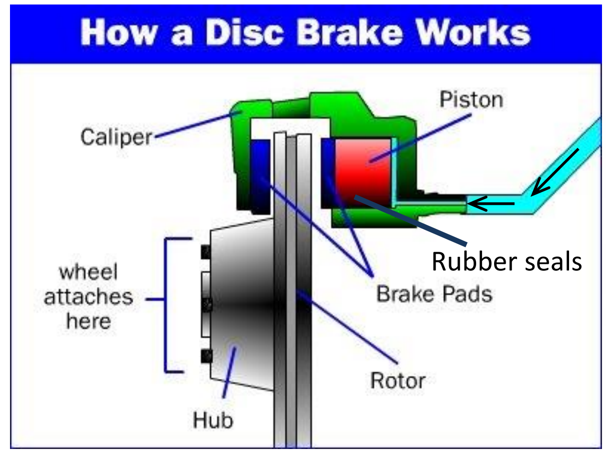
- Brake pedal
- Brake lines
- Rubber seals
- Master cylinder
- Brake pads

FMEA worksheet columns

- Component
- Failure mode
- Failure mechanism
- Failure effect (local)
- Failure effect (system)

FMEA Exercise
Automotive brakes





System components

– Brake pedal

– Brake pads

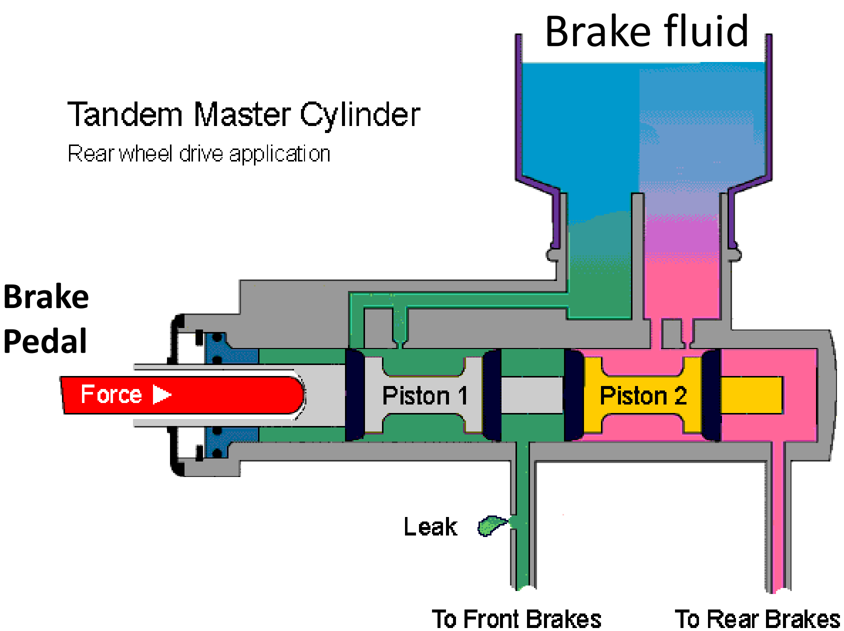
FMEA worksheet columns

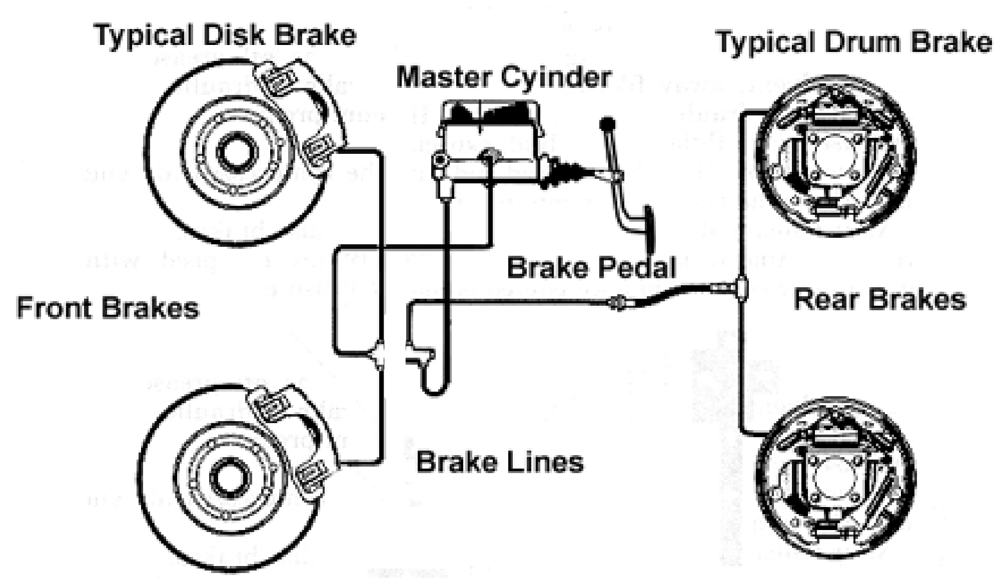
– Component

– Failure effect (system)

How would you make this system safe?

Actual automotive brakes



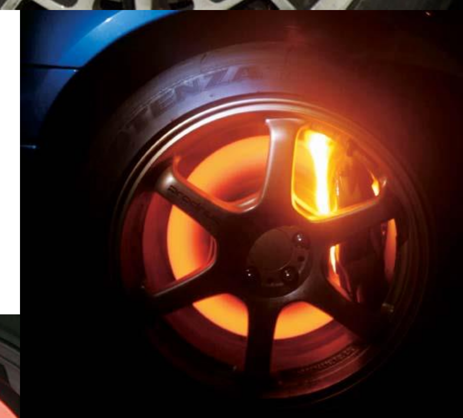


Typical Automotive Braking System

- FMEA heavily used in mechanical engineering
- Tends to promote redundancy
- Useful for physical/mechanical systems to identify single points of failure

A real accident: Toyota's unintended acceleration

- **2004-2009**
  - 102 incidents of stuck accelerators
  - Speeds exceed 100 mph despite stomping on the brake
  - 30 crashes
  - 20 injuries
- **2009, Aug**:
  - Car accelerates to 120 mph
  - Passenger calls 911, reports stuck accelerator
  - Some witnesses report red glow / fire behind wheels
  - Car crashes killing 4 people
- **2010, Jul:**
  - Investigated over 2,000 cases of unintended acceleration



Captured by FMEA?

Failure discussion

- Component Failure

Vs.

- Design problem

Vs.

- Requirements problem

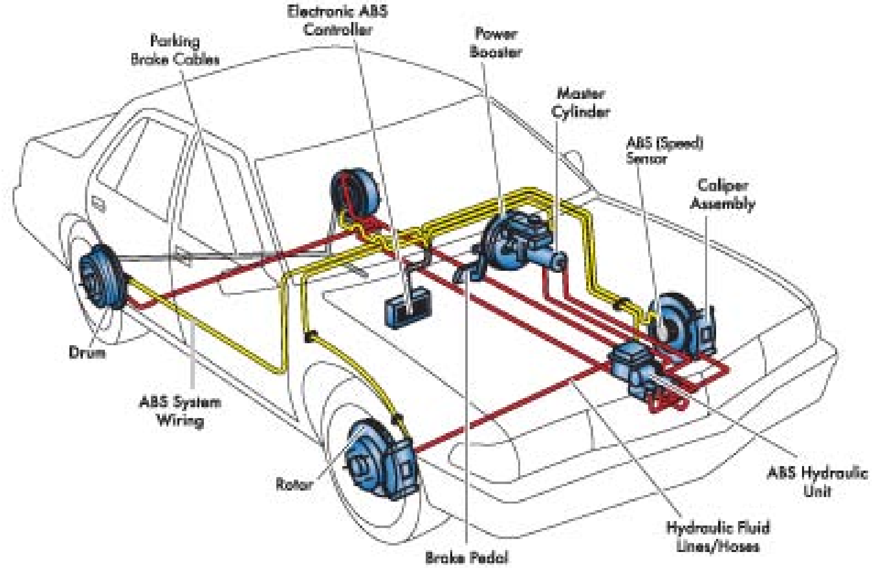
FMEA Limitations

- Component failure incidents only
  - Unsafe interactions? Design issues? Requirements issues?
- Single component failures only
  - Multiple failure combinations not considered
- Requires detailed system design
  - Limits how early analysis can be applied
- Works best on hardware/mechanical components
  - **<u>Human</u>** operators? (Driver? Pilot?)
  - **<u>Software</u>** failure?
  - Organizational factors (management pressure? culture?)
- Inefficient, analyzes unimportant + important failures
  - Can result in 1,000s of pages of worksheets
- Tends to encourage redundancy
  - Often leads to inefficient solutions
- Failure modes must already be known
  - Best for standard parts with few and well-known failure modes

Safety vs. Reliability

- Common assumption:

  Safety = reliability
- How to improve safety?
  - Make everything more reliable!
- Making car brakes safe
  - Make every component reliable
  - Include redundant components



Is this a good assumption?

*Image from midas.com

Safety vs. reliability

Reliability ←→ Failures } Component property

Safety ←→ Incidents } System property

A simpler example

Safe or unsafe?

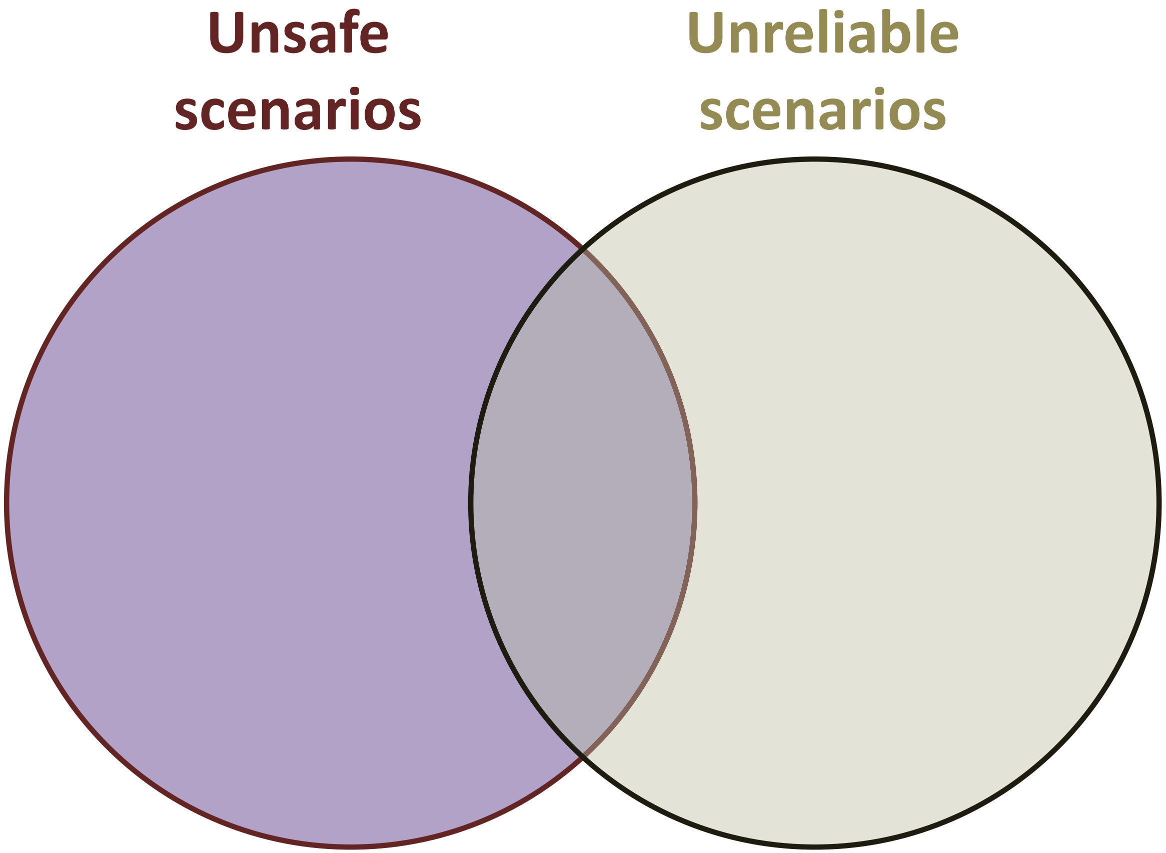
*Image: bluecashewkitchen.com

Safety is not a component property

- Safety is an emergent property of the system
  - Depends on context and environment!

Individual components are not inherently safe or unsafe

Safety vs. Reliability



Safe ≠ Reliable

- Safety often means making sure X never happens
- Reliability usually means making sure Y always happens

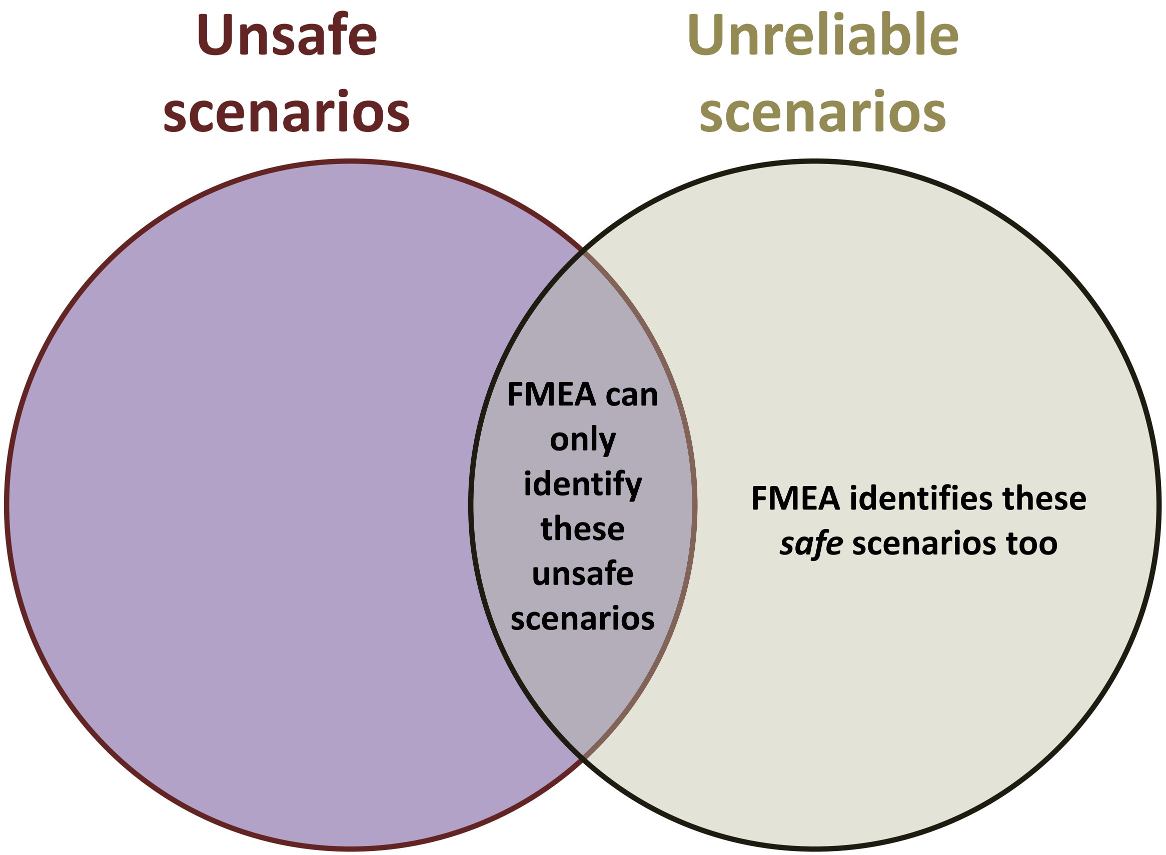
	Safe	**Unsafe**
Reliable	•Typical commercial flight	
Unreliable		•Aircraft engine fails in flight

Safe ≠ Reliable

- Safety often means making sure X never happens
- Reliability usually means making sure Y always happens

	Safe	Unsafe
Reliable	•Typical commercial flight	•Computer reliably executes unsafe commands •Increasing tank burst pressure •A nail gun without safety lockout
Unreliable	•Aircraft engine won't start on ground •Missile won't fire	•Aircraft engine fails in flight

Safety vs. Reliability



- FMEA is a *reliability* technique
  - Explains the inefficiency
- FMEA sometimes used to identify unsafe outcomes

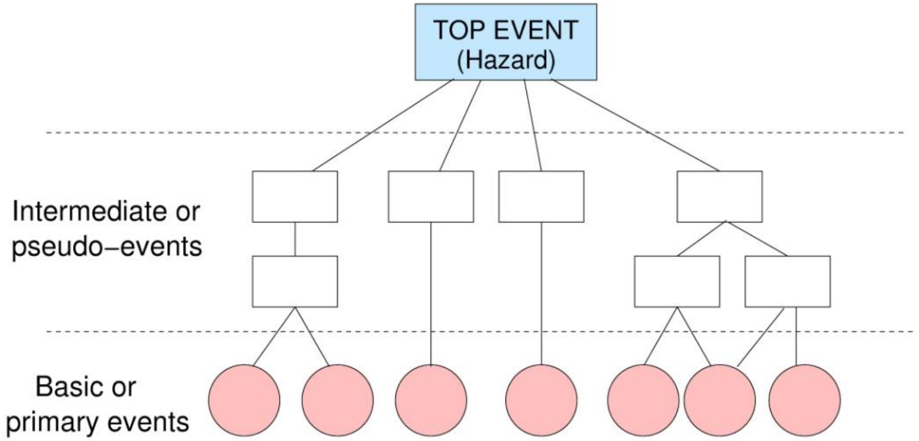
Failure Modes, Mechanisms, Effects

- Examples and definitions of "Failure modes, mechanisms, effects"

FTA
Fault Tree Analysis

FTA: Fault Tree Analysis

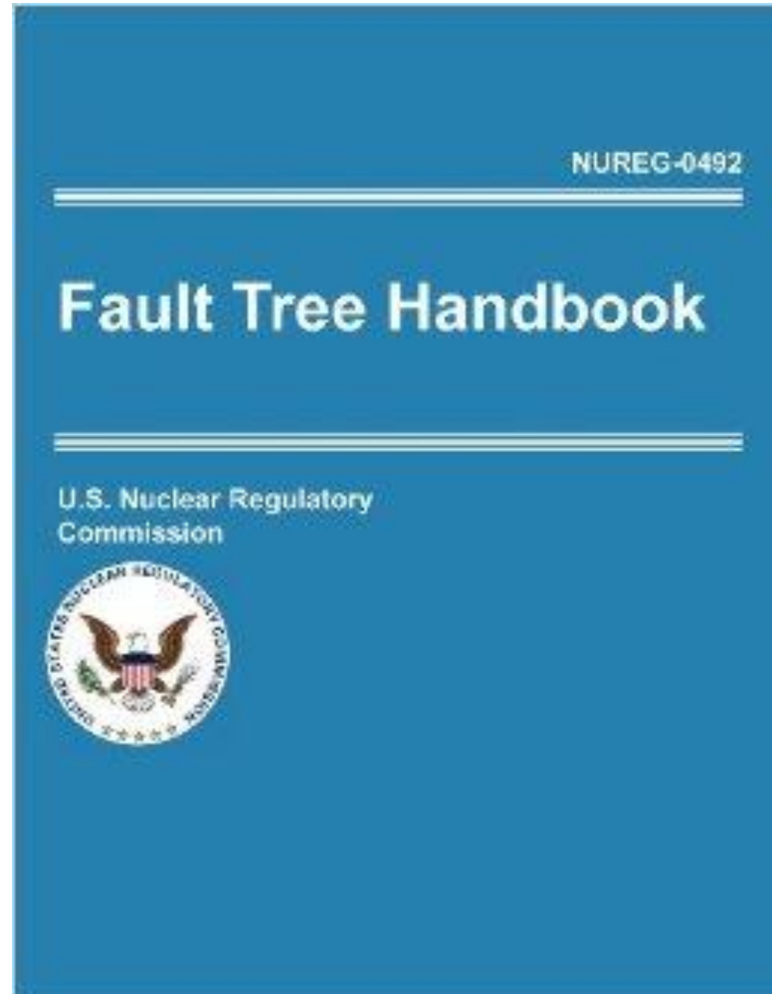
- 1961: Bell labs analysis of Minuteman missile system
- Today one of the most popular hazard analysis techniques
- Top-down search method
  - Top event: undesirable event
  - Goal is to identify causes of hazardous event



Courtesy of John Thomas. Used with permission.

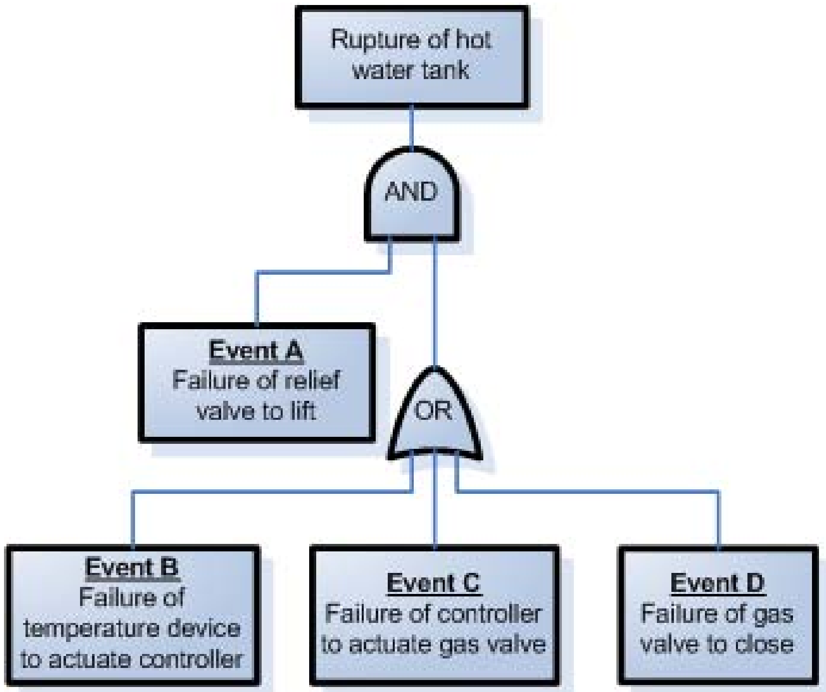
FTA Process

1. Definitions
   – Define top event
   – Define initial state/conditions
2. Fault tree construction
3. Identify *cut-sets* and *minimal cut-sets*

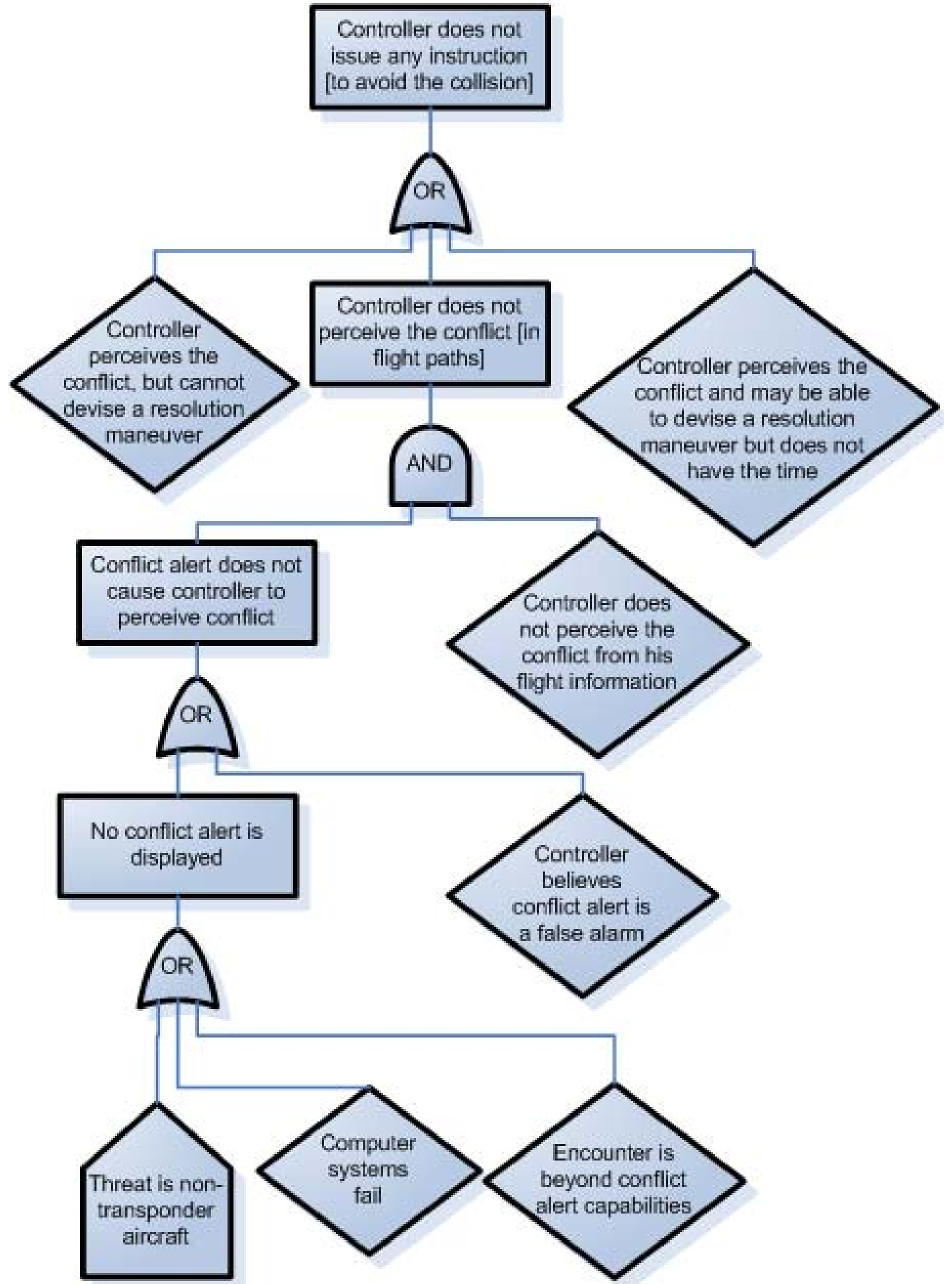


Vesely

Fault tree example

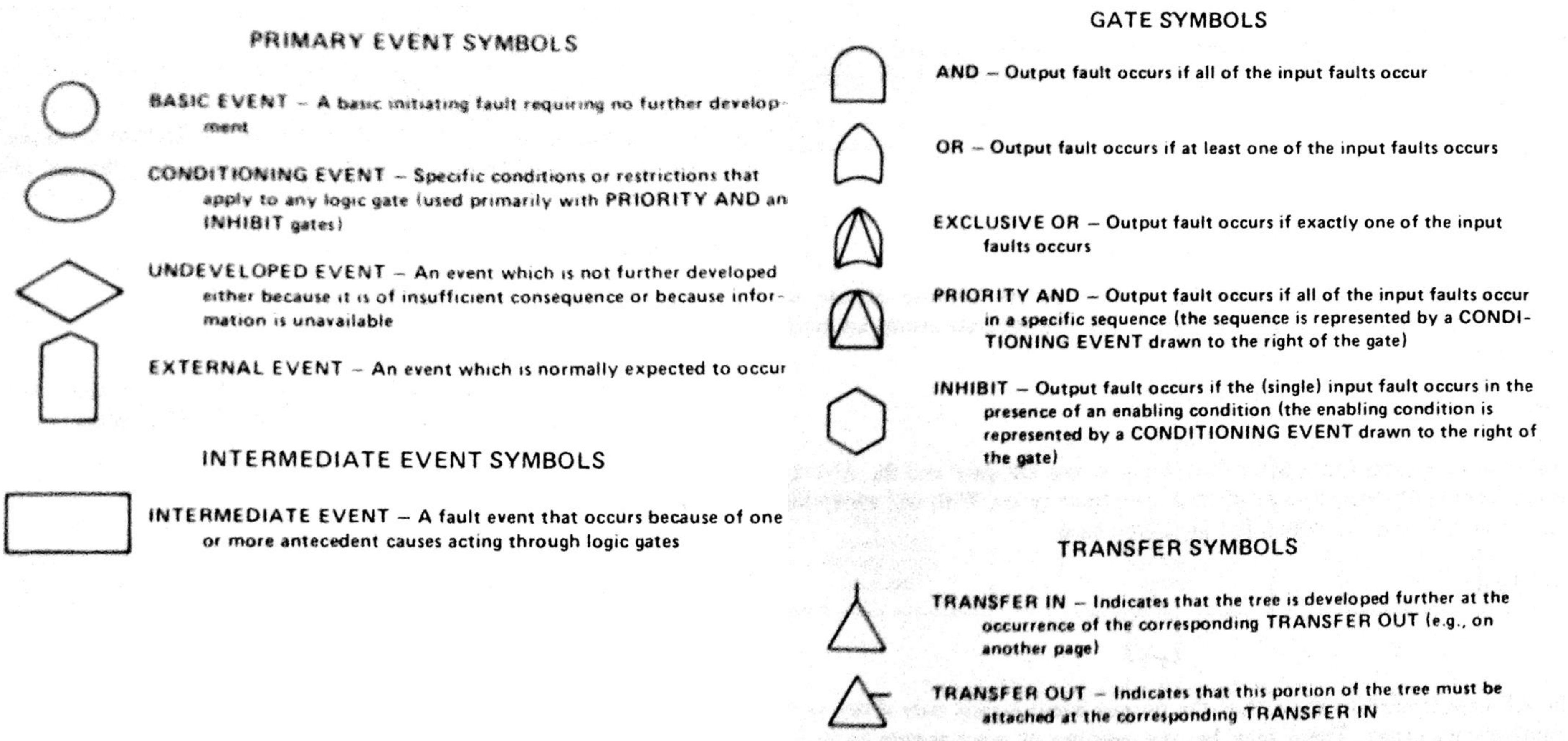


Example from original 1961 Bell Labs study



Part of an actual TCAS fault tree (MITRE, 1983)

Fault tree symbols



PRIMARY EVENT SYMBOLS

BASIC EVENT – A basic initiating fault requiring no further development

CONDITIONING EVENT – Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)

UNDEVELOPED EVENT – An event which is not further developed either because it is of insufficient consequence or because information is unavailable

EXTERNAL EVENT – An event which is normally expected to occur

INTERMEDIATE EVENT SYMBOLS

INTERMEDIATE EVENT – A fault event that occurs because of one or more antecedent causes acting through logic gates

GATE SYMBOLS

AND – Output fault occurs if all of the input faults occur

OR – Output fault occurs if at least one of the input faults occurs

EXCLUSIVE OR – Output fault occurs if exactly one of the input faults occurs

PRIORITY AND – Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)

INHIBIT – Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate)

TRANSFER SYMBOLS

TRANSFER IN – Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT (e.g., on another page)

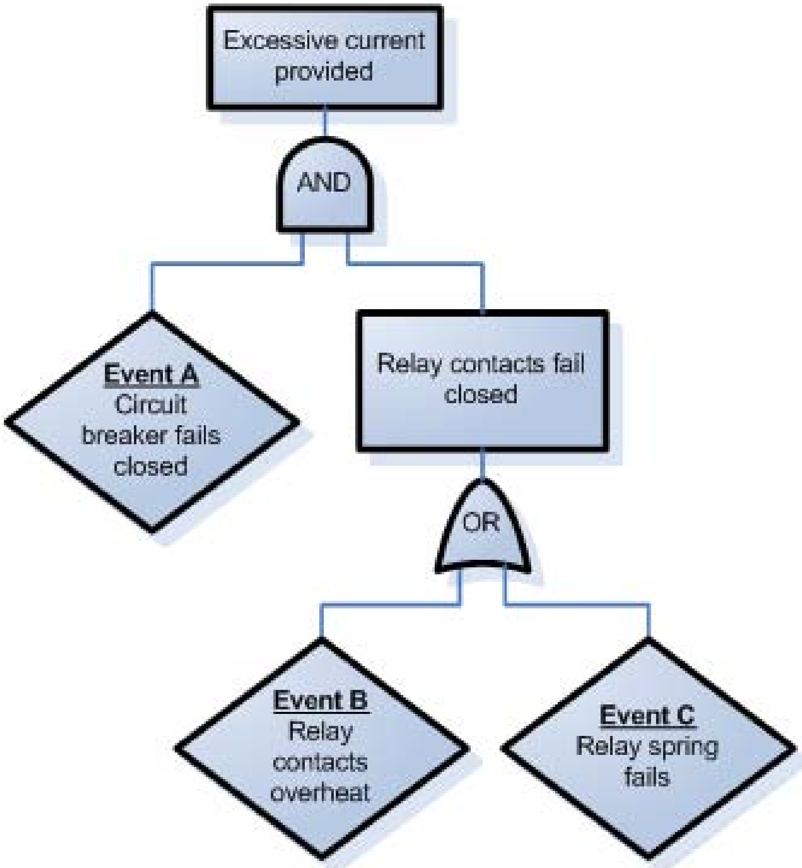
TRANSFER OUT – Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

From NUREG-0492 (Vesely, 1981)

Fault Tree cut-sets

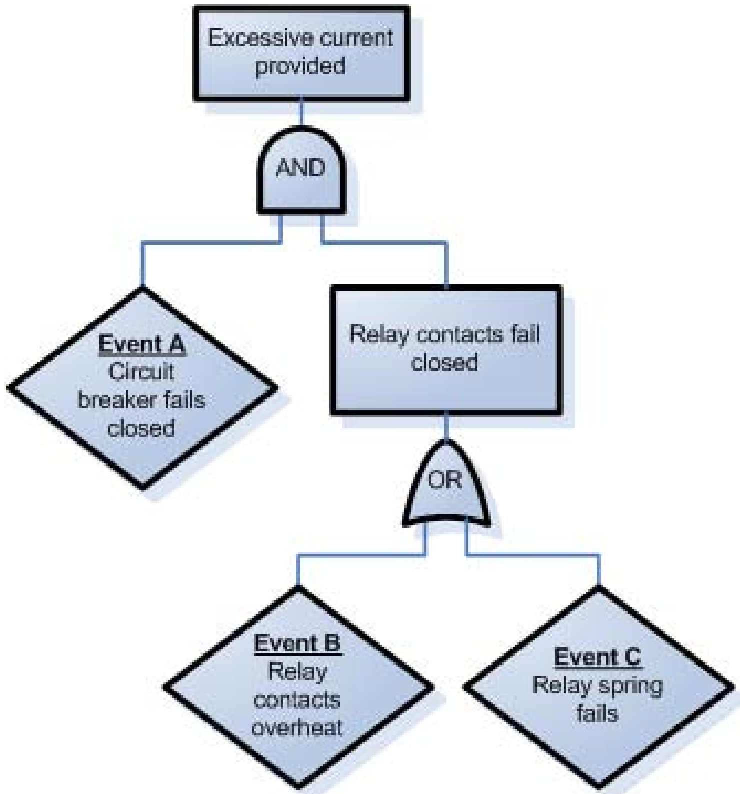
- *Cut-set*: combination of basic events (leaf nodes) sufficient to cause the top-level event
  - Ex: (A and B and C)

- *Minimum cut-set*: a cut-set that does not contain another cut-set
  - Ex: (A and B)
  - Ex: (A and C)



FTA uses an accident model

Fault Tree:



Accident model: Chain-of-failure-events

Thrust reversers

- 1991 Accident
- B767 in Thailand
- Lauda Air Flight 004
  - Thrust reversers deployed in flight, caused in-flight breakup and killing all 223 people. Deadliest aviation accident involving B767
  - Simulator flights at Gatwick Airport which appeared to show that deployment of a thrust reverser was a survivable incident.
  - Boeing had insisted that a deployment was not possible in flight. In 1982 Boeing established a test where the aircraft was slowed to 250 knots, and the test pilots then used the thrust reverser. The control of the aircraft had not been jeopardized. The FAA accepted the results of the test.
  - Recovery from the loss of lift from the reverser deployment "was uncontrollable for an unexpecting flight crew“. The incident led Boeing to modify the thrust reverser system to prevent similar occurrences by adding sync-locks, which prevent the thrust reversers from deploying when the main landing gear truck tilt angle is not at the ground position.

FTA example

- Aircraft reverse thrust
  - Engines
  - Engine reverse thrust panels
  - Computer
    - Open reverse thrust panels after touchdown
    - Fault handling: use 2/3 voting. (Open reverse thrust panels if 2/3 wheel weight sensors AND 2/3 wheel speed sensors indicate landing)
  - Wheel weight sensors (x3)
  - Wheel speed sensors (x3)

Create a fault tree for the top-level event:
Reverse thrusters don't operate on landing.

Image from: http://en.wikipedia.org/wiki/File:Klm_f100_ph-kle_arp.jpg

Warsaw

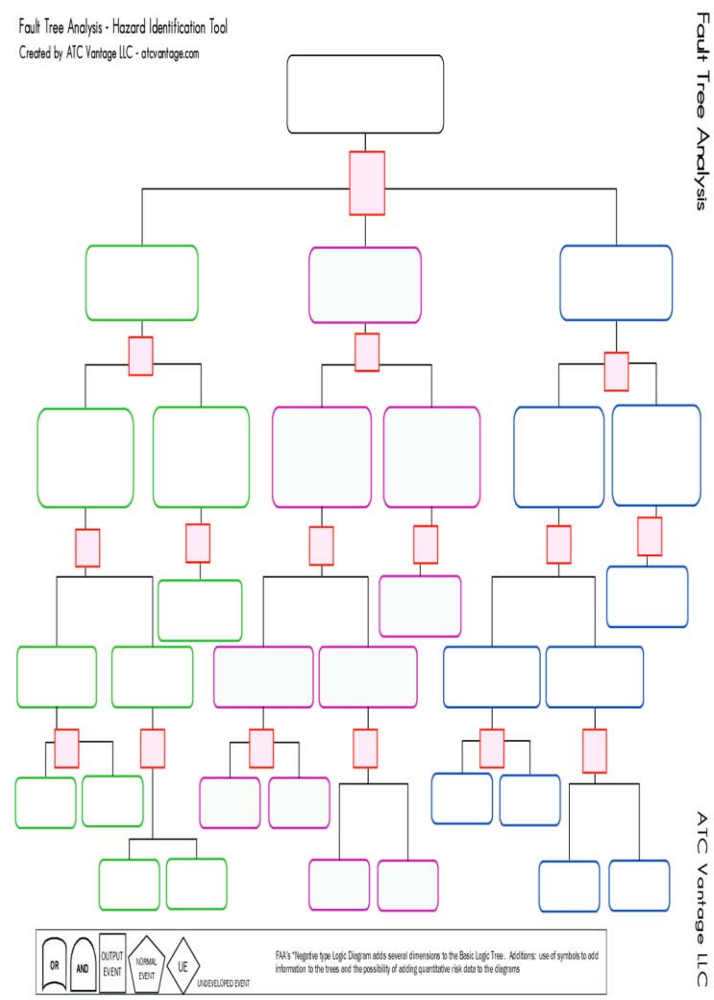
- Warsaw
- Crosswind landing (one wheel first)
- Wheels hydroplaned
- Thrust reverser would not deploy
  - Pilots could not override and manually deploy
- Thrust reverser logic
  - Must be 6.3 tons on each main landing gear strut
  - Wheel must be spinning at least 72 knots

FTA Strengths

- Captures **combinations** of failures
- More **efficient** than FMEA
  - Analyzes only failures relevant to top-level event
- Provides **graphical format** to help in understanding the system and the analysis
- Analyst has to think about the system in great detail during tree construction
- Finding minimum **cut sets** provides insight into weak points of complex systems

FTA Limitations

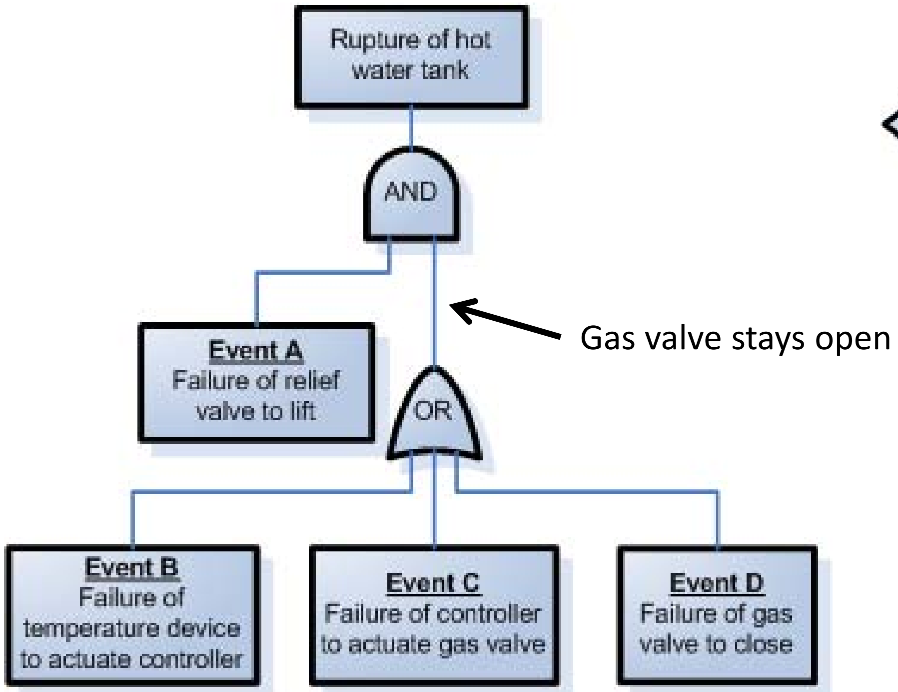
- **Independence** between events is often assumed
- **Common-cause failures** not always obvious
- Difficult to capture **non-discrete** events
  - E.g. rate-dependent events, continuous variable changes
- Doesn't easily capture **systemic factors**



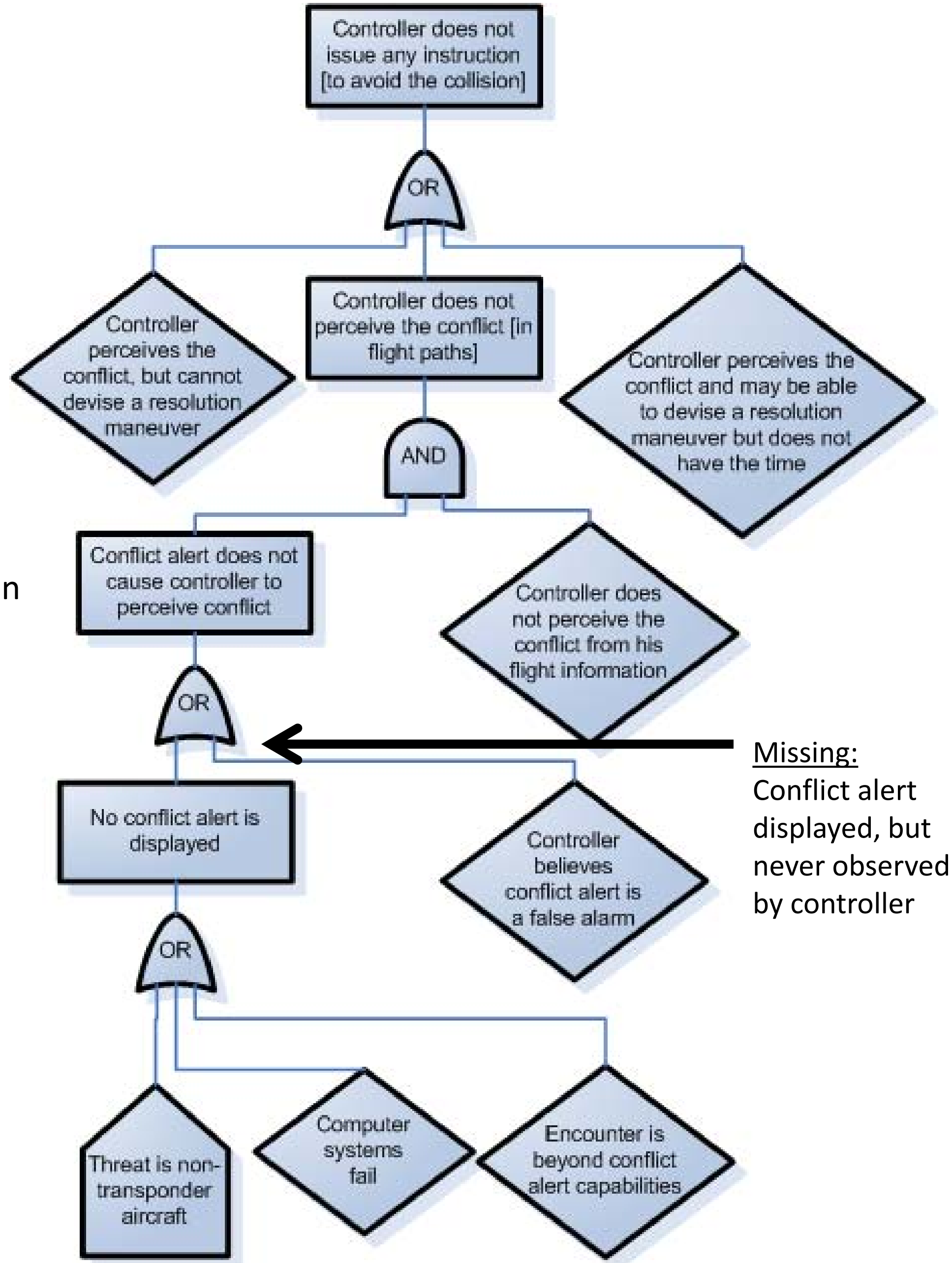
FTA Limitations (cont)

- Difficult to capture delays and other **temporal factors**
- **Transitions** between states or operational phases not represented
- Can be **labor intensive**
  - In some cases, over 2,500 pages of fault trees
- Can become very complex very quickly, can be difficult to **review**

Fault tree example



Example from original 1961 Bell Labs study



Part of an actual TCAS fault tree (MITRE, 1983)

Vesely FTA Handbook

- Considered by many to be the textbook definition of fault trees

Failure-based methods

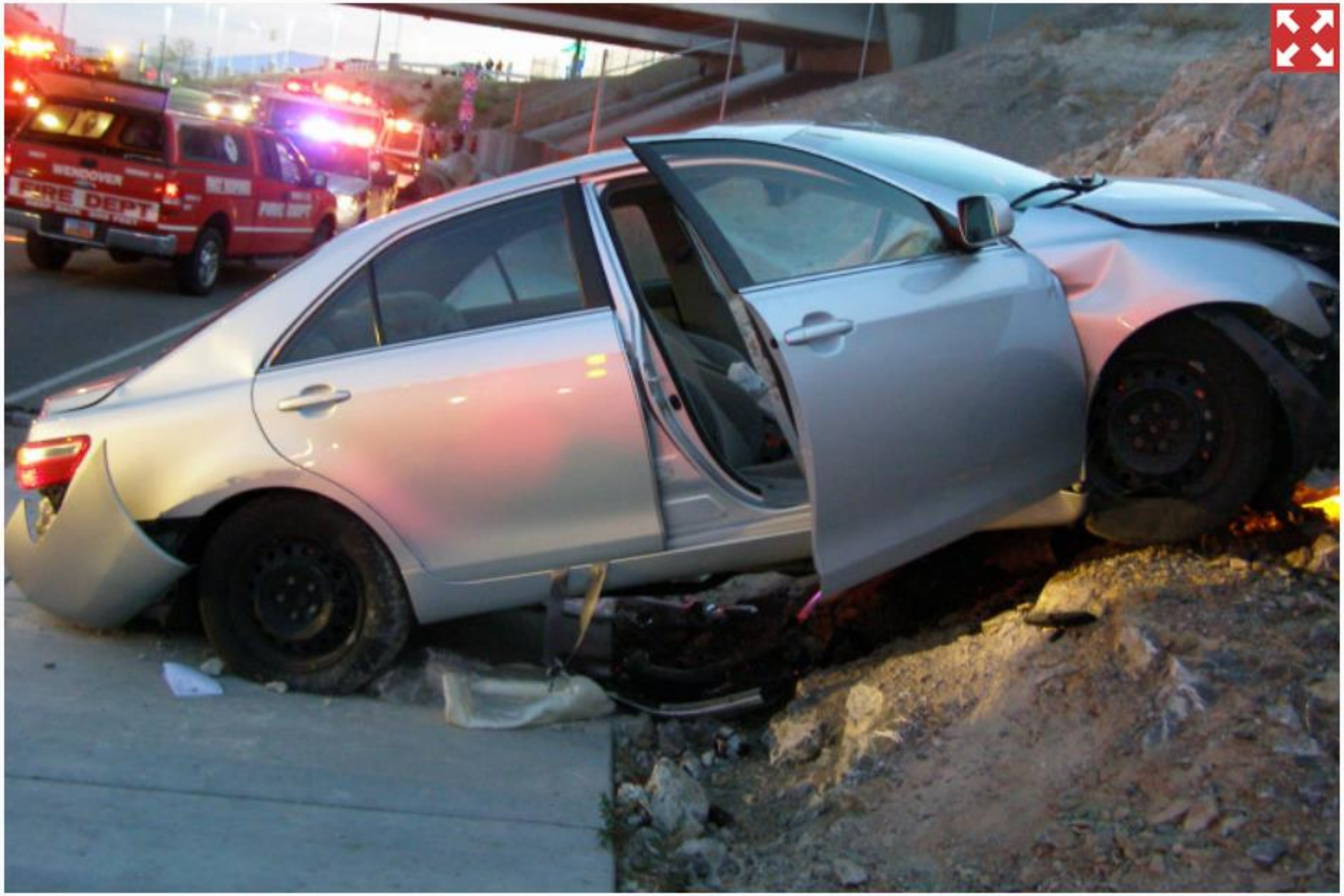
- Tend to treat safety as a component property
- Use divide-and-conquer strategies
- Reductionism

Reasonable?

Toyota to pay $1.2B settlement in vehicle acceleration lawsuit

By Bob Fredericks and Post Wires

March 19, 2014 | 9:19am



Toyota Unintended Acceleration

- **2004-2009:** 102 incidents

Toyota Unintended Acceleration

- **2004:** Push-button ignition
- **2004-2009**
  - 102 incidents of uncontrolled acceleration
  - Speeds exceed 100 mph despite stomping on the brake
  - 30 crashes
  - 20 injuries
- **Today**
  - Software fixes for pushbutton ignition, pedals

Pushbutton was reliable!
Software was reliable!

http://www.reuters.com/article/2010/07/14/us-toyota-idUSTRE66D0FR20100714
http://www.statesman.com/business/u-s-toyota-cite-driver-error-in-many-803504.html

Toyota

- **2004:** Push-button ignition
- **2004-2009**
  - 102 incidents of uncontrolled acceleration
  - Speeds exceed 100 mph despite stomping on the brake
  - 30 crashes
  - 20 injuries
- **2009, Aug**:
  - Car accelerates to 120 mph
  - Passenger calls 911, reports stuck accelerator
  - Car crashes killing 4 people
  - Driver was offensive driving instructor for police
- **Today**
  - Software fixes for pushbutton ignition, pedals

All component requirements were met…
Yet system behavior was unexpected, unsafe!

http://www.reuters.com/article/2010/07/14/us-toyota-idUSTRE66D0FR20100714
http://www.statesman.com/business/u-s-toyota-cite-driver-error-in-many-803504.html

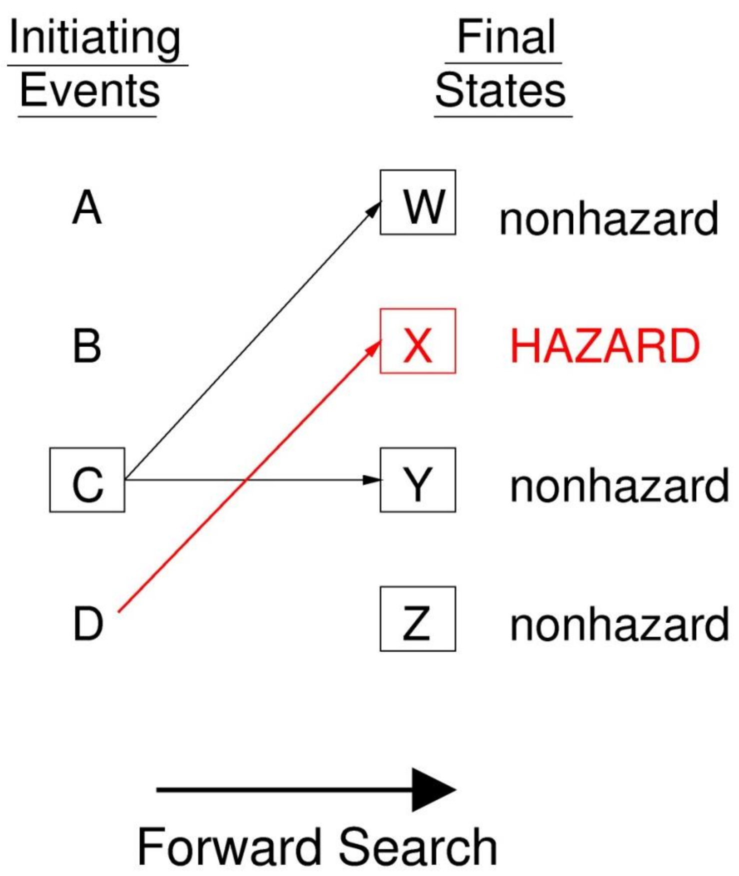
Systems-Theoretic Approaches

- Focus of next class
- Need to identify and prevent failures, but also:
  - Go <u>beyond</u> the failures
  - Why weren't the failures detected and mitigated?
    - By operators
    - By engineers
  - Prevent issues that don't involve failures
  - Human-computer interaction issues
  - Software-induced operator error
  - Etc.

Event Tree Analysis

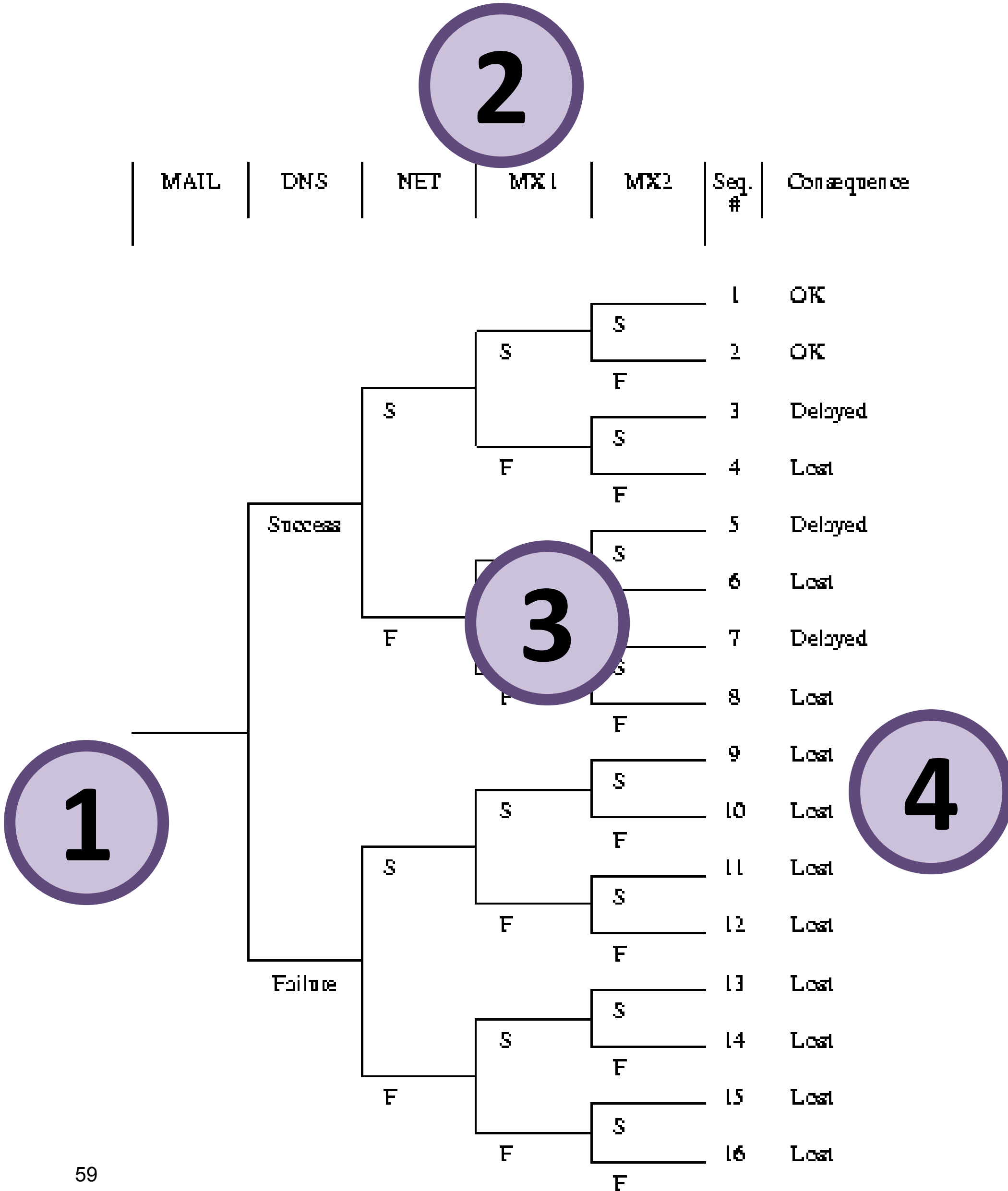
Event Tree Analysis

- 1967: Nuclear power stations
- Forward search technique
  - *Initiating event*: component failure (e.g. pipe rupture)
  - *Goal*: Identify all possible outcomes

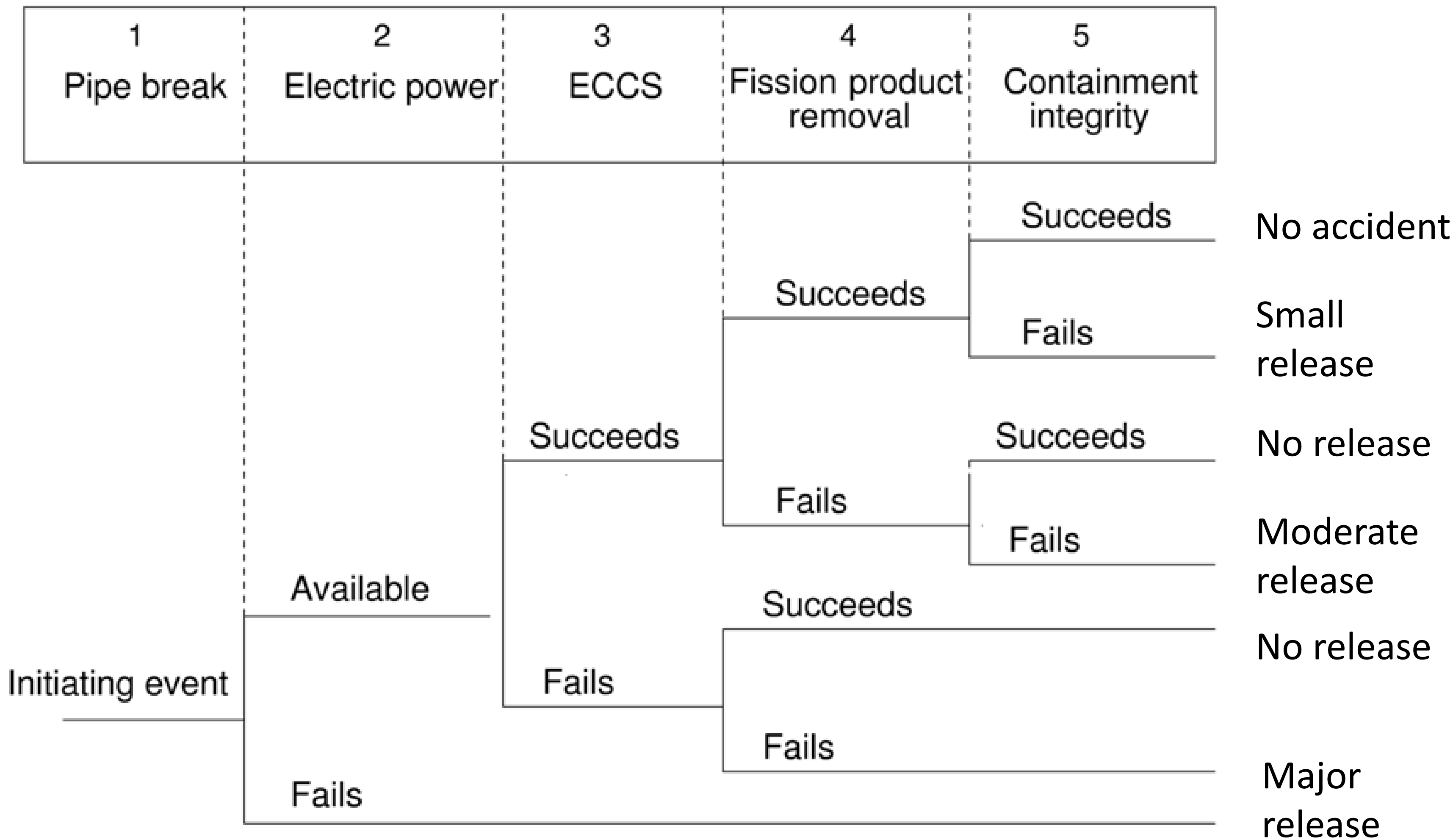


Event Tree Analysis: Process

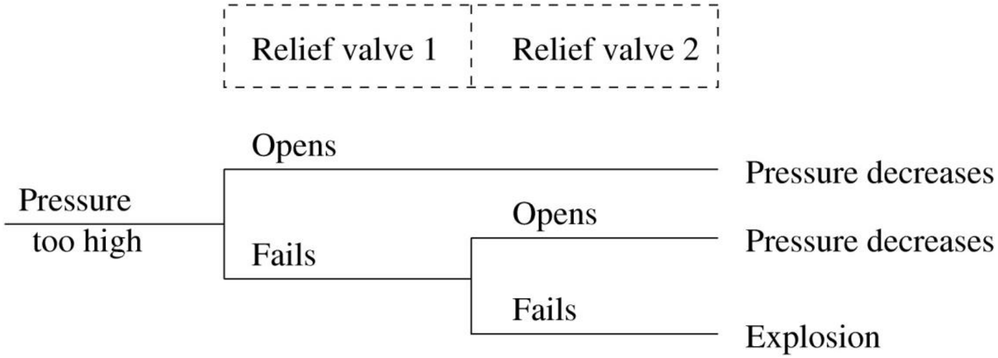
1. Identify initiating event
2. Identify barriers
3. Create tree
4. Identify outcomes



Event Tree Example

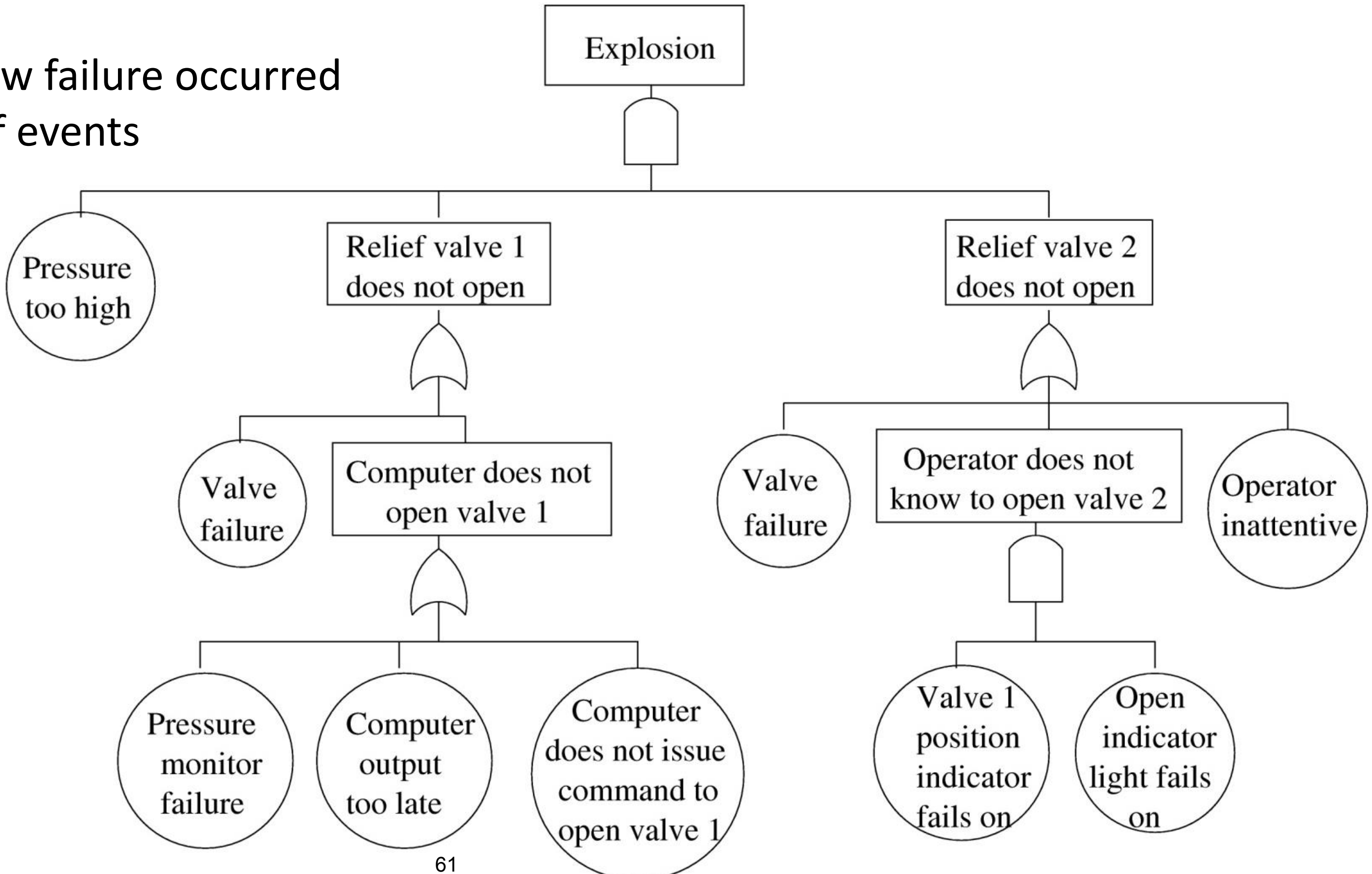


Event Trees
vs.
Fault Trees



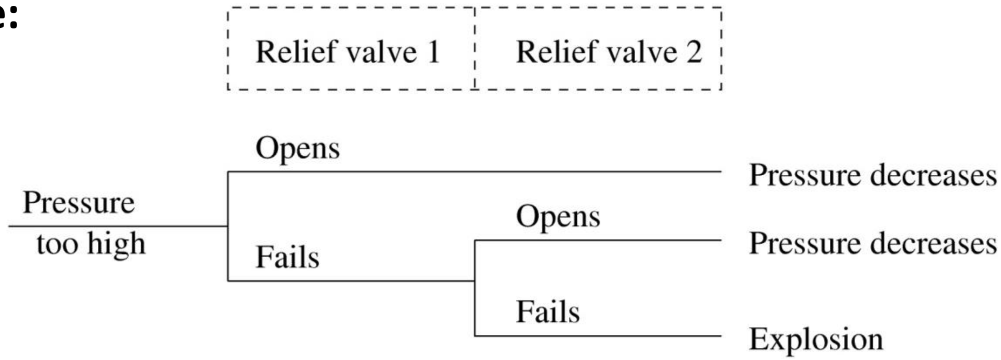
Event Tree
- Shows what failed, but not how.
- Shows order of events

Fault Tree
- Complex, but shows how failure occurred
- Does not show order of events

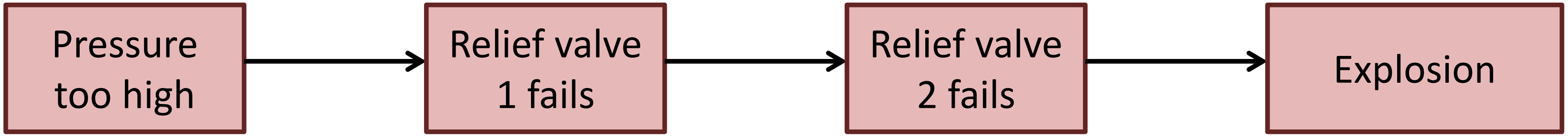


ETA uses an accident model

Event Tree:



Accident model: Chain-of-events



Event Tree Analysis: Exercise

Elevator

1. Identify initiating event
   – Cable breaks
2. List Barriers
3. Create Tree
4. Identify outcomes

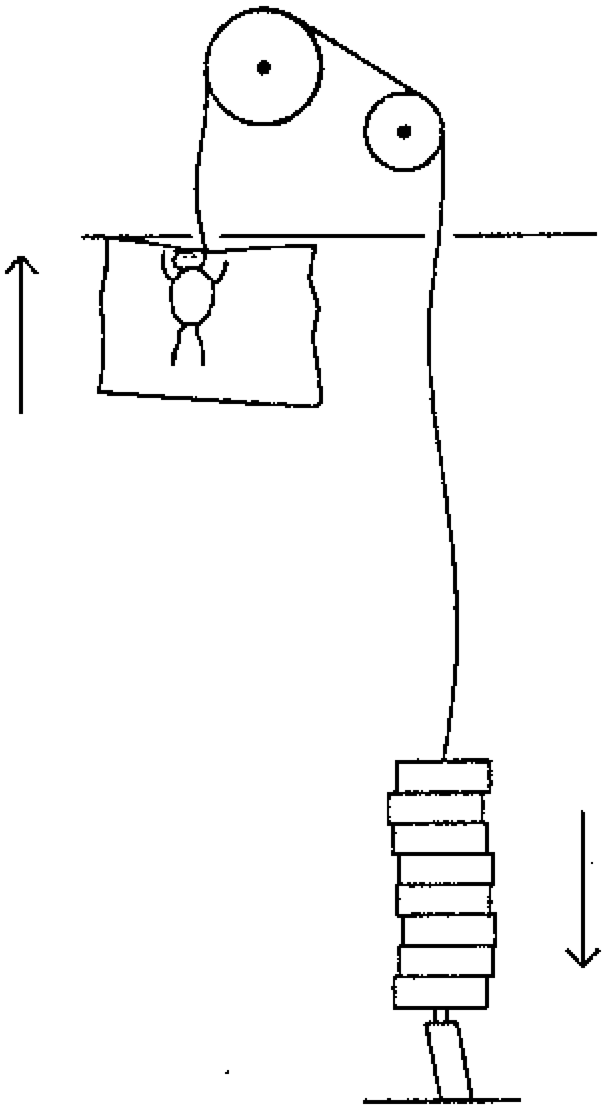
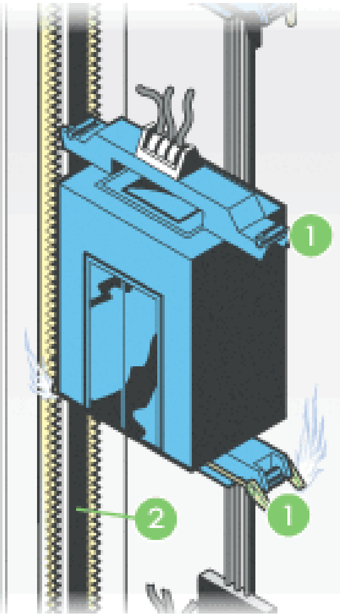
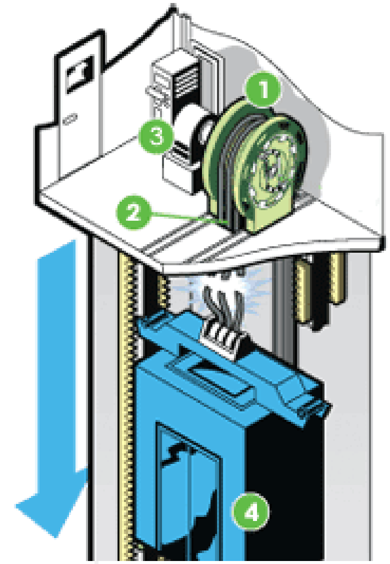


Image from official U.S. Dept of Labor, Mine Safety and Health Administration paper: http://www.msha.gov/S&HINFO/TECHRPT/HOIST/PAPER4.HTM

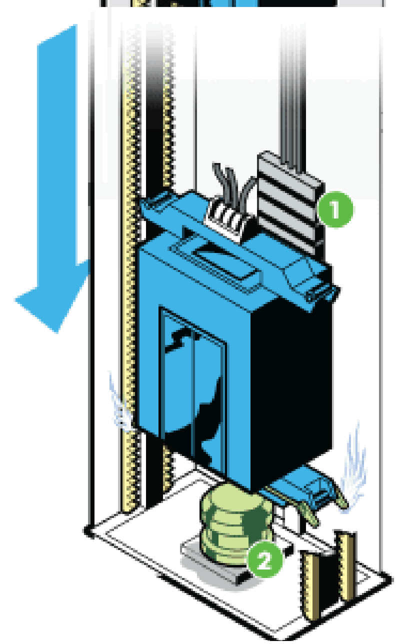
Event Tree Analysis: Exercise



1. If the cables snap, the elevator's **safeties** would kick in. **Safeties** are braking systems on the elevator.
2. Some safeties clamp the **steel rails** running up and down the elevator shaft, while others drive a wedge into the notches in the **rails**.



1. Steel cables bolted to the the car loop over a **sheave**.
2. The sheave's grooves grip the **steel cables**.
3. The **electric motor** rotates the sheave, causing the cables to move, too.
4. As the cables move, the **car** is lifted.



1. The cables that lift the car are also connected to a **counterweight**, which hangs down on the other side of the sheave.
2. The built-in **shock absorber** at the bottom of the shaft - typically a piston in an oil-filled cylinder - helps cushion the imact in the event of snapping cables.

What are the barriers?

Event Tree Analysis: Strengths

- Handles ordering of events better than fault trees
- Most practical when events can be **ordered in time** (chronology of events is stable)
- Most practical when **events are independent** of each other.
- Designed for use with **protection systems** (barriers)

Event Tree Analysis: Limitations

- Not practical when chronology of events is not stable (e.g. when **order of columns may change**)
- Difficult to analyze **non-protection systems**
- Can become exceedingly **complex** and require simplification
- **Separate trees required** for each initiating event
  - Difficult to represent interactions among events
  - Difficult to consider effects of multiple initiating events

Event Tree Analysis: Limitations (cont)

- Can be difficult to define functions across top of event tree and their order
- Requires ability to define set of initiating events that will produce all important accident sequences
- Most applicable to systems where:
  - All risk is associated with one hazard
    - (e.g. overheating of fuel)
  - Designs are fairly standard, very little change over time
  - Large reliance on protection and shutdown systems

HAZOP
Hazard and Operability Analysis

HAZOP: Hazards and Operability Analysis

- Developed by Imperial Chemical Industries in early 1960s
- Not only for safety, but efficient operations

An image of a chemical plant is removed due to copyright restrictions.

Accident model:

- Chain of failure events (that involve deviations from design/operating intentions)

HAZOP

- Guidewords applied to variables of interest
  - E.g. flow, temperature, pressure, tank levels, etc.

Image removed due to copyright restrictions.

- Team considers potential causes and effects

- **Questions** generated from guidewords
  - Could there be no flow?
  - If so, how?
  - How will operators know there is no flow?
  - Are consequences hazardous or cause inefficiency?

HAZOP: Generate the right questions, not just fill in a tree

HAZOP Process

Guidewords	Meaning
NO, NOT, NONE	The intended result is not achieved, but nothing else happens (such as no forward flow when there should be)
MORE	More of any relevant property than there should be (such as higher pressure, higher temperature, higher flow, or higher viscosity)
LESS	Less of a relevant physical property than there should be
AS WELL AS	An activity occurs in addition to what was intended, or more components are present in the system than there should be (such as extra vapors or solids or impurities, including air, water, acids, corrosive products)
PART OF	Only some of the design intentions are achieved (such as only one of two components in a mixture)
REVERSE	The logical opposite of what was intended occurs (such as backflow instead of forward flow)
OTHER THAN	No part of the intended result is achieved, and something completely different happens (such as the flow of the wrong material)

HAZOP Strengths

- **Easy** to apply
  - A simple method that can uncover complex accidents
- Applicable to **new designs** and new design features
- Performed by **diverse study team**, facilitator
  - Method defines team composition, roles
  - Encourages cross-fertilization of different disciplines

HAZOP Limitations

- Requires **detailed plant information**
  - Flowsheets, piping and instrumentation diagrams, plant layout, etc.
  - Tends to result in protective devices rather than real design changes
- Developed/intended for **chemical industry**
- **Labor-intensive**
  - Significant time and effort due to search pattern
- Relies very heavily on judgment of engineers
- May leave out hazards caused by **stable factors**
- Unusual to consider deviations for **systemic factors**
  - E.g. organizational, managerial factors, management systems, etc.
- Difficult to apply to **software**
- **Human behavior** reduces to compliance/deviation from procedures
  - Ignores *why it made sense* to do the wrong thing

Summary

- Well-established methods
- Time-tested, work well for the problems they were designed to solve
- Strengths include
  - Ease of use
  - Graphical representation
  - Ability to analyze many failures and failure combinations
  - Application to well-understood mechanical or physical systems
- Limitations include
  - Inability to consider accidents without failures
  - Difficulty incorporating systemic factors like managerial pressures, complex human behavior, and design/requirements flaws
- Other methods may be better suited to deal with the challenges introduced with complex systems

Quantitative Hazard Analysis

Agenda

- Traditional hazard analysis
  - Qualitative techniques
    - Failure Modes and Effects Analysis
    - Fault Tree Analysis
    - Event Tree Analysis
    - HAZOP
  - Quantitative techniques
    - FMECA
    - Quant. Fault Tree Analysis
    - Quant. ETA

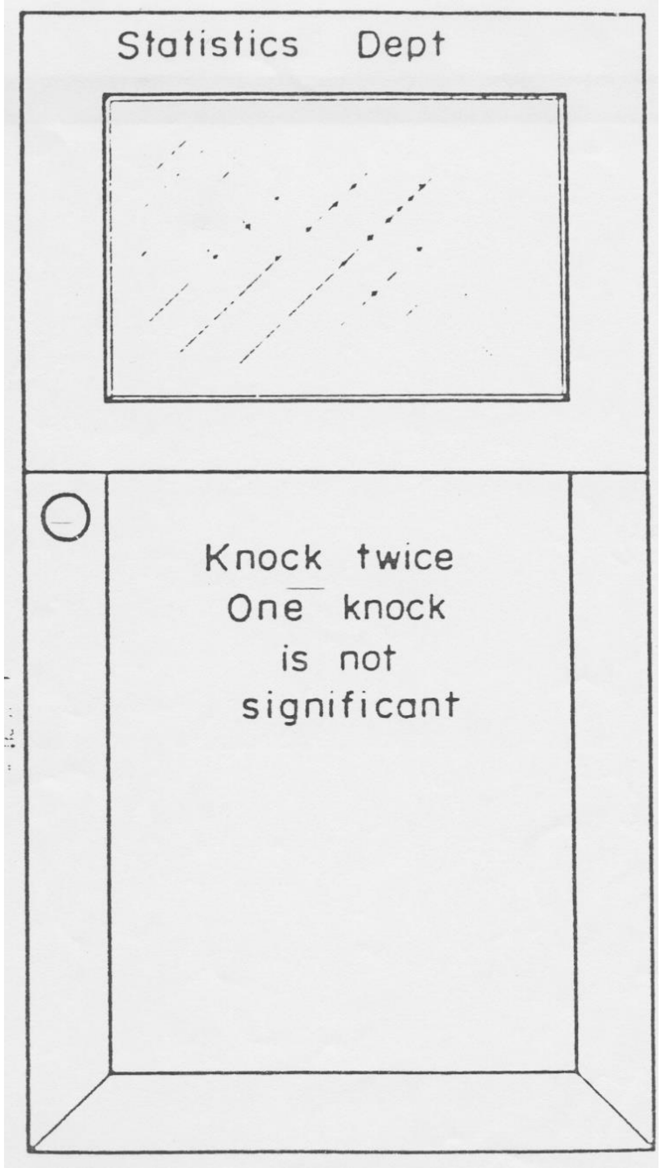
Quantitative analysis

- How do you include numbers and math?
  - What do you quantify?
- Tends to focus on two parameters
  - Severity
  - Probability

Quantitative methods

- The quantification is usually based on probability theory and statistics
- Common assumptions
  - Behavior is random
  - Each behavior independent

Good assumptions?



Quantitative methods

- The quantification is usually based on probability theory and statistics
- Common assumptions
  – Behavior is random
  – Each behavior independent
  – Identical distributions / EV

An image of a pinball table removed due to copyright restrictions.

Good assumptions?

-Hardware?

-Humans?

-Software?

Risk

- Common idea:
  - Some combination of severity and likelihood

- How would you combine severity and likelihood mathematically?
  - Risk = f(Severity, Likelihood)
  - What is f ?

Risk Matrix

- Based on common quantification:

  Risk = Severity * Likelihood

Likelihood					
Very Likely					
Likely					
Possible					
Unlikely					
Rare					
	Negligible	Minor	Moderate	Significant	Severe

Severity

Risk Matrix

- Based on common quantification:

  Risk = Severity * Likelihood

Likelihood					
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Rare	Low	Low	Low Med	Medium	Medium
	Negligible	Minor	Moderate	Significant	Severe

Severity

Automotive Severity Levels

- Level 0: No injuries
- Level 1: Light to moderate injuries
- Level 2: Severe to life-threatening injuries (survival probable)
- Level 3: Life-threatening to fatal injuries (survival uncertain)

From ISO26262

Aviation Severity Levels

- Level 1: Catastrophic
  - Failure may cause crash.
  - Failure conditions prevent continued safe flight and landing
- Level 2: Severe
  - Failure has negative impact on safety, may cause serious or fatal injuries
  - Large reduction in functional capabilities
- Level 3: Major
  - Failure is significant, but less impact than severe
  - Significant reduction in functional capabilities
- Level 4: Minor
  - Failure is noticeable, but less impact than Major
  - Slight reduction in safety margins; more workload or inconvenience
- Level 5: No effect on safety

From ARP4671, DO-178B

Risk Matrix

- Based on common quantification:

  Risk = Severity * Likelihood

Aviation Severity Levels

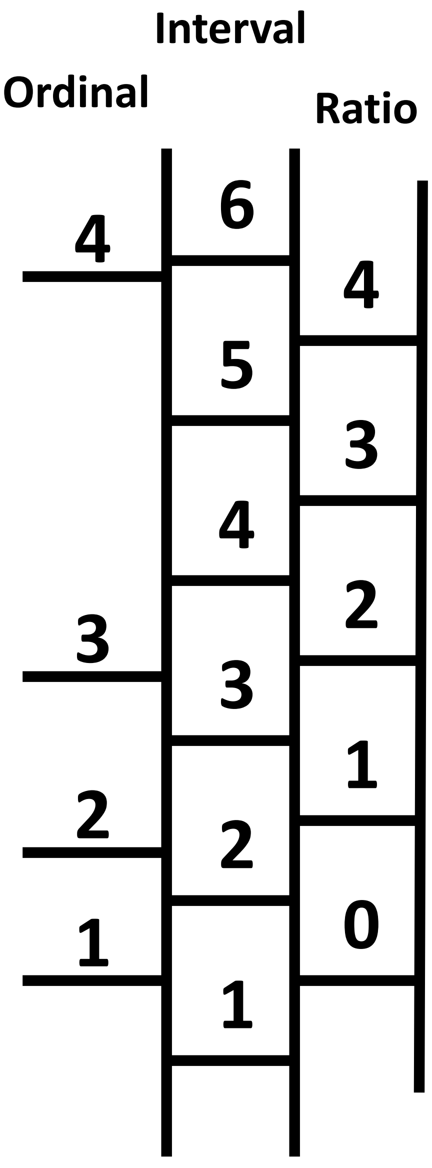
- Level 1: Catastrophic
- Level 2: Severe
- Level 3: Major
- Level 4: Minor
- Level 5: No effect on safety

How to quantify?

Numerical Scales

- Severity is usually *ordinal*
  - Only guarantees ordering along increasing severity
  - Distance between levels not comparable
- Ordinal multiplication can result in *reversals*
  - Multiplication assumes equal distance
    - …and fixed 0
    - Assumes severity 4 is 2x worse than severity 2
  - A "Med Hi" result may actually be worse than "High"

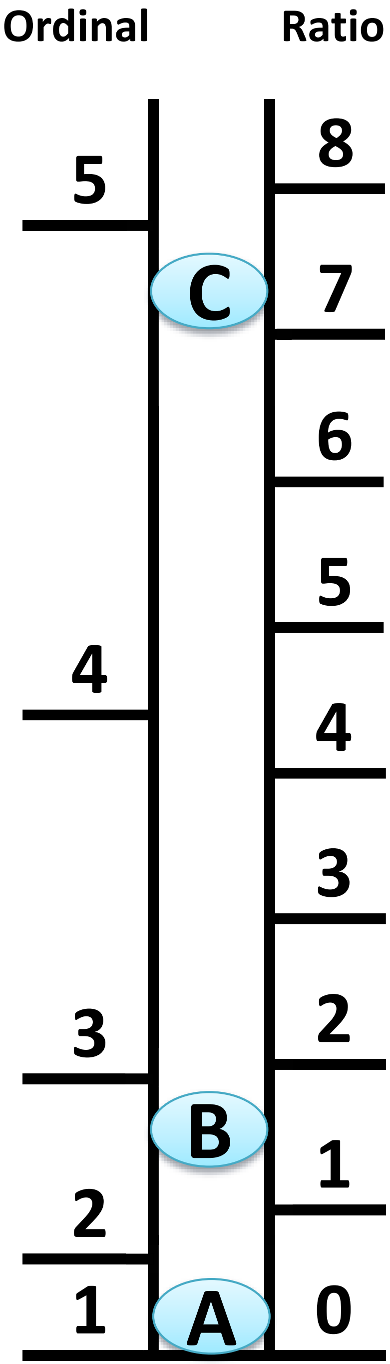
Another challenge



Reversal Example

- Event A
  - Likelihood = 20%
- Event B
  - Likelihood = 10%
- Event C
  - Likelihood = 3%

Calculate risk



Reversal Example

Using <u>Ordinal</u> Scale:

- Event A
  - Likelihood = 20%
  - Severity = 1

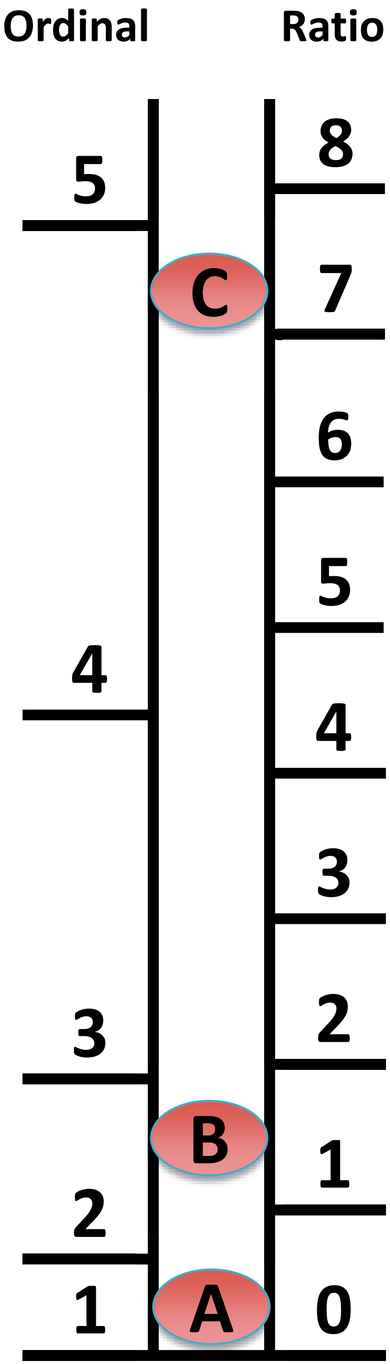
Risk = 0.20

- Event B
  - Likelihood = 10%
  - Severity = 2

Risk = 0.20

- Event C
  - Likelihood = 3%
  - Severity = 4

Risk = 0.12



Reversal Example

Using <u>Ratio</u> Scale:

- Event A
  - Likelihood = 20%
  - Severity = 0

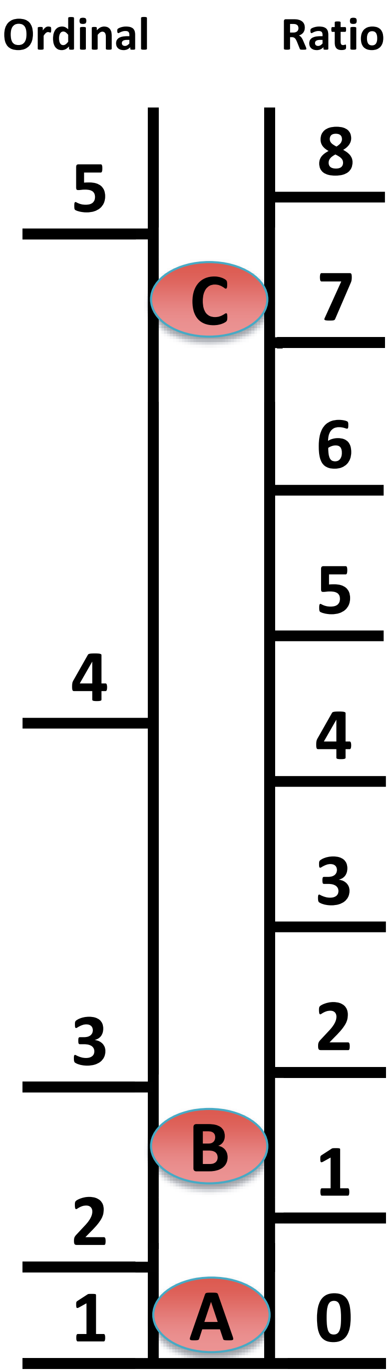
Risk = 0.00

- Event B
  - Likelihood = 10%
  - Severity = 1

Risk = 0.10

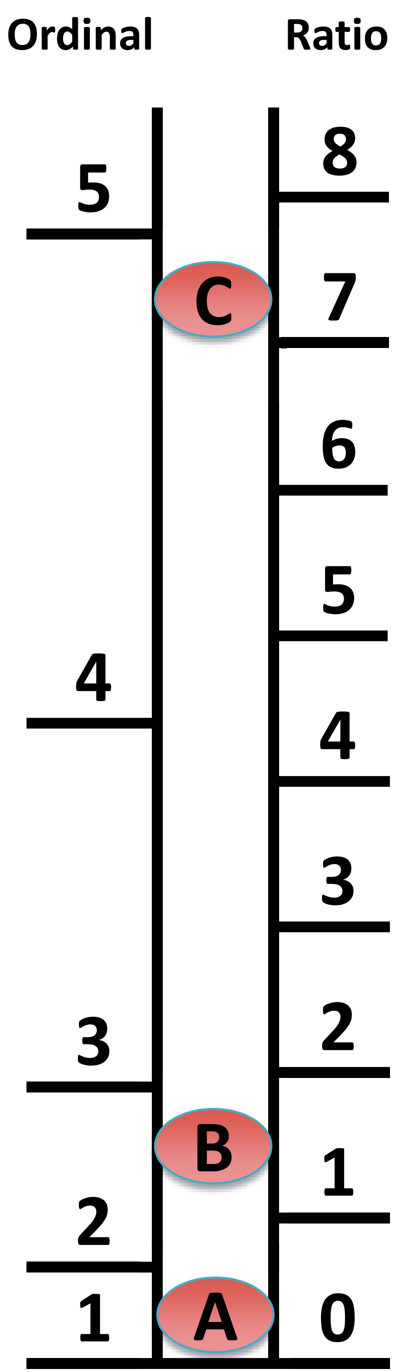
- Event C
  - Likelihood = 3%
  - Severity = 7

Risk = 0.21



Reversal Example

	Risk (using ordinal scale)	Risk (using ratio scale)
Event A	0.20	0.00
Event B	0.20	0.10
Event C	0.12	0.21



Risk Matrix

- Based on common idea:

  Risk = Severity * Likelihood

Uses expected values (averages)

Likelihood	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Rare	Low	Low	Low Med	Medium	Medium

Severity

Expected Value Fallacy

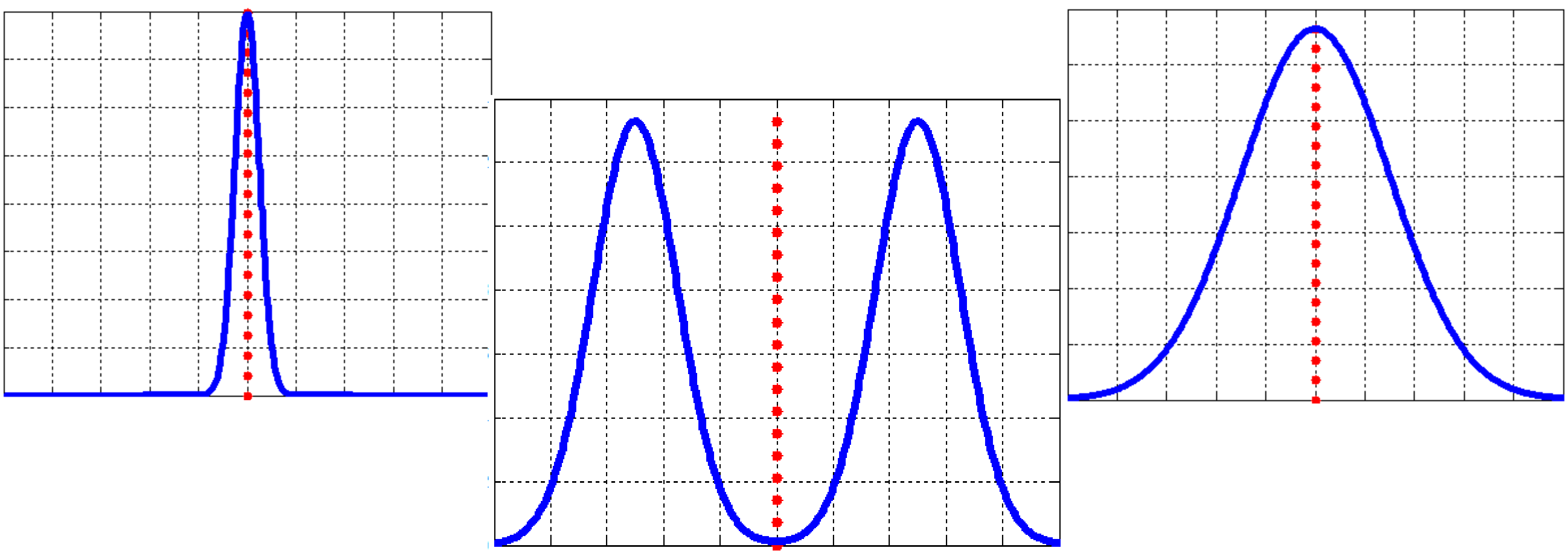
P-value Fallacy

Flaw of Averages

Jensen's Law

Simpson's paradox

- Beware when averages are used to simplify the problem!
  - Can make adverse decisions appear correct

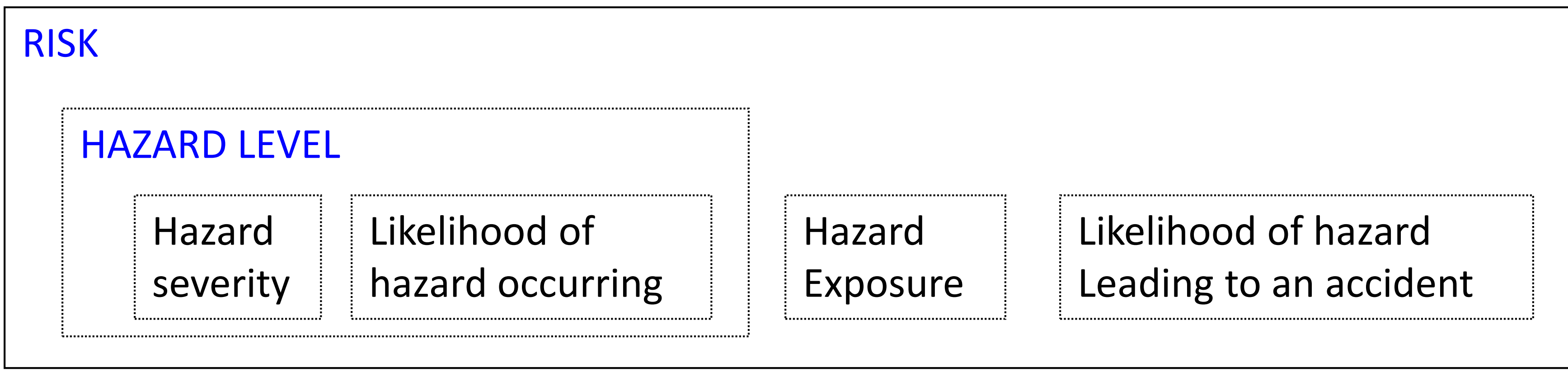


Another Example Hazard Level Matrix

	A Frequent	B Probable	C Occasional	D Remote	E Improbable	F Impossible
Catastrophic I	Design action required to eliminate or control hazard 1	Design action required to eliminate or control hazard 2	Design action required to eliminate or control hazard 3	Hazard must be controlled or hazard probability reduced 4	9	12
Critical II	Design action required to eliminate or control hazard 3	Design action required to eliminate or control hazard 4	Hazard must be controlled or hazard probability reduced 6	Hazard control desirable if cost effective 7	Assume will not occur 12	Impossible occurrence 12
Marginal III	Design action required to eliminate or control hazard 5	Hazard must be controlled or hazard probability reduced 6	Hazard control desirable if cost effective 8	Normally not cost effective 10	12	12
Negligible IV	10	11	Negligible hazard 12	12	12	12

Hazard Level: A combination of severity (worst potential damage in case of an accident) and likelihood of occurrence of the hazard.

Risk: The hazard level combined with the likelihood of the hazard leading to an accident plus exposure (or duration) of the hazard.

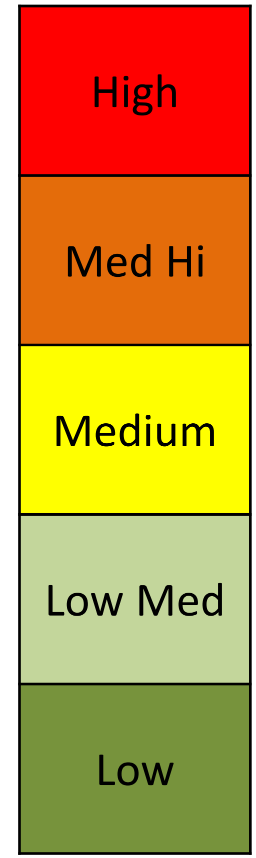


Safety: Freedom from accidents or losses.

Hazard Level Assessment

- Combination of Severity and Likelihood
- Difficult for complex, human/computer controlled systems
- Challenging to determine likelihood for these systems
  - Software behaves exactly the same way every time
    - Not random
  - Humans adapt, and can change behavior over time
    - Adaptation is not random
    - Different humans behave differently
    - Not I.I.D (independent and identically distributed)
  - Modern systems almost always involve new designs and new technology
    - Historical data may be irrelevant
- **Severity is usually adequate** to determine effort to spend on eliminating or mitigating hazard.

Hazard Level or Risk Level:



FMECA
Failure Modes Effects and Criticality Analysis

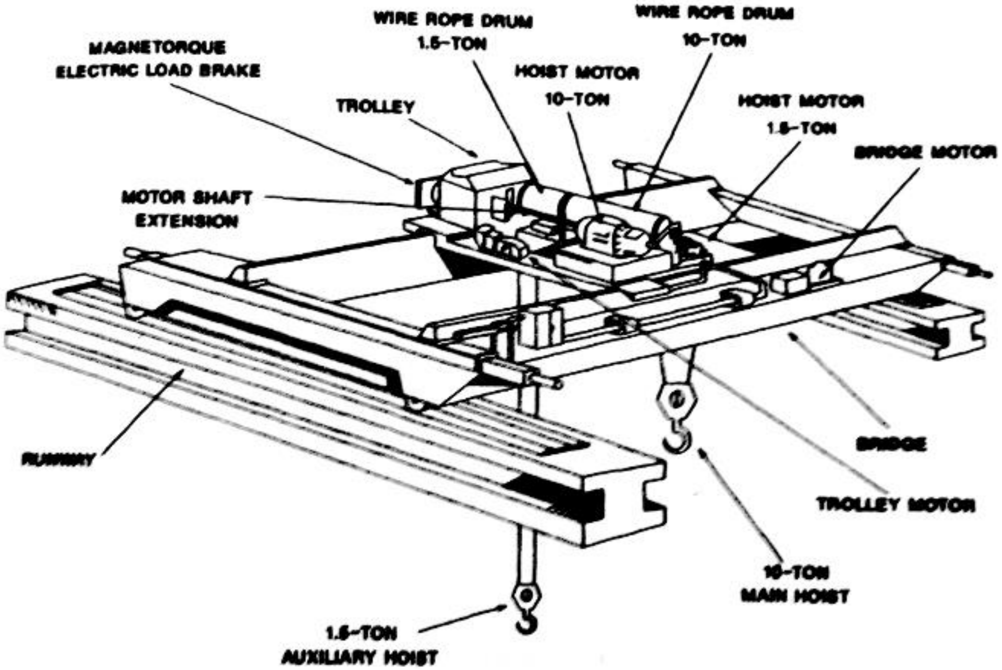
FMECA

- Same as FMEA, but with "criticality" information
- Criticality
  - Can be ordinal severity values
  - Can be likelihood probabilities
  - An expression of concern over the effects of failure in the system*

*Vincoli, 2006, Basic Guide to System Safety

FMEA worksheet

Bridge crane system



Failure Mode and Effect Analysis

Program:_________ System:_________ Facility:________
Engineer:_________ Date:___________ Sheet:_________

Component Name	Failure Modes	Failure Mechanisms	Failure effects (local)	Failure effects (system)	Criticality Level
Main hoist motor	Inoperative, does not move	Defective bearings Loss of power Broken springs	Main hoist cannot be raised. Brake will hold hoist stationary	Load held stationary, cannot be raised or lowered.	(5) High, customers dissatisfied

*FMEA example adapted from (Vincoli, 2006)

Severity Level Examples

Rating	Meaning
1	No effect
2	Very minor (only noticed by discriminating customers)
3	Minor (affects very little of the system, noticed by average customer)
4	Moderate (most customers are annoyed)
5	High (causes a loss of primary function; customers are dissatisfied)
6	Very high and hazardous (product becomes inoperative; customers angered; the failure may result unsafe operation and possible injury)

*Otto et al., 2001, Product Design

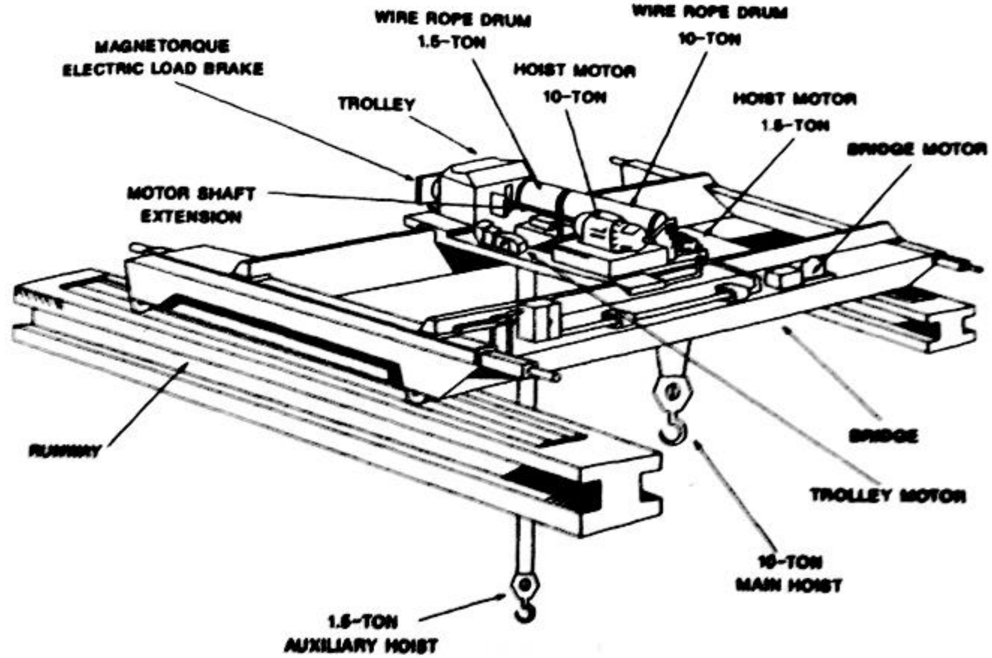
Severity Level Examples

Rating	Severity of Effect
10	Safety issue and/or non-compliance with government regulation without warning.
9	Safety issue and/or non-compliance with government regulation with warning.
8	Loss of primary function.
7	Reduction of primary function.
6	Loss of comfort/convenience function.
5	Reduction of comfort/convenience function.
4	Returnable appearance and/or noise issue noticed by most customers.
3	Non-returnable appearance and/or noise issue noticed by customers.
2	Non-returnable appearance and/or noise issue rarely noticed by customers.
1	No discernable effect.

*http://www.harpcosystems.com/Design-FMEA-Ratings-PartI.htm

FMECA worksheet

Bridge crane system



Could also specify likelihood

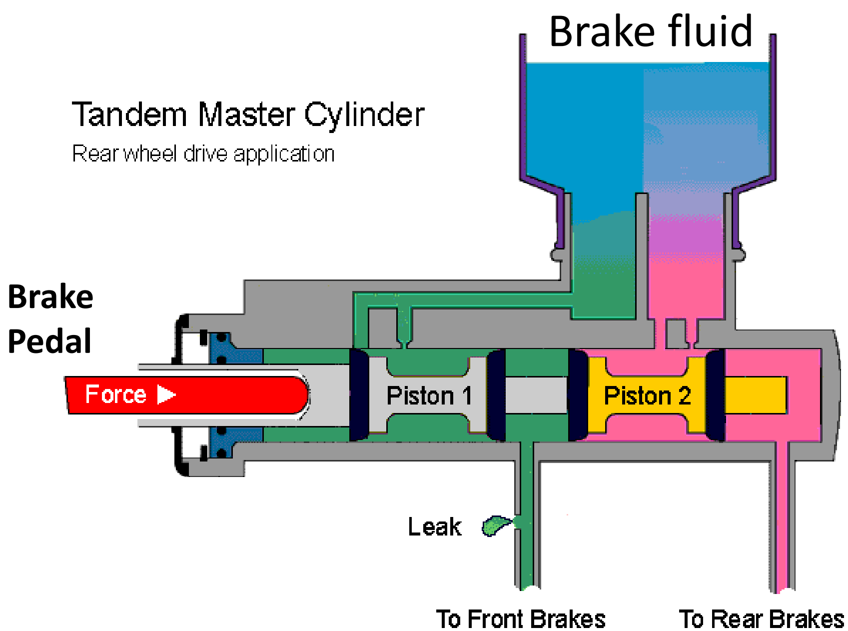
Failure Mode and Effect Analysis

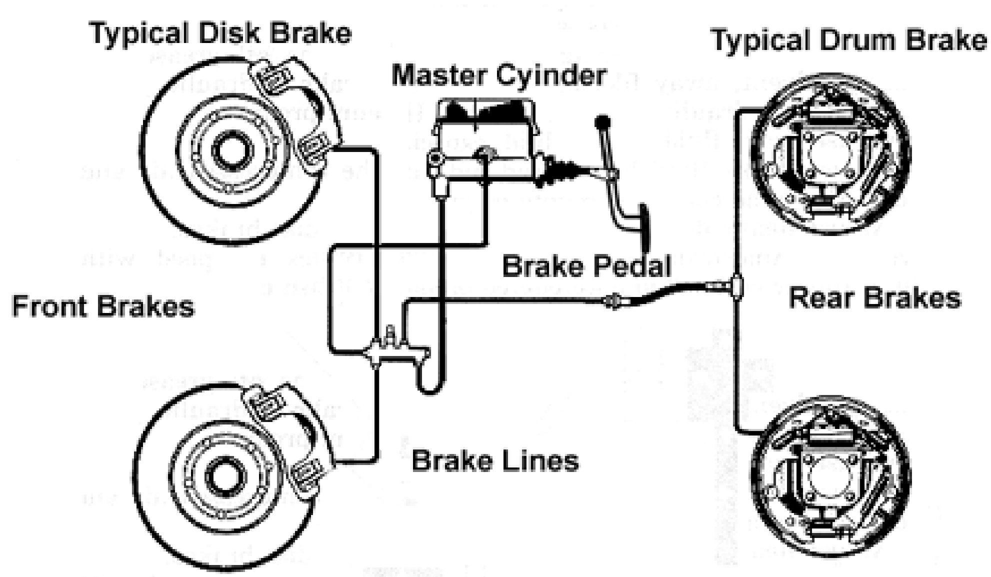
Program:_________ System:_________ Facility:________
Engineer:_________ Date:___________ Sheet:_________

Component Name	Failure Modes	Failure Mechanisms	Failure effects (local)	Failure effects (system)	Probability of occurrence
Main hoist motor	Inoperative, does not move	Defective bearings Loss of power Broken springs	Main hoist cannot be raised. Brake will hold hoist stationary	Load held stationary, cannot be raised or lowered.	0.001 per operational hour

*FMEA example adapted from (Vincoli, 2006)

FMECA Exercise: Actual automotive brakes





Typical Automotive Braking System

FMEA worksheet columns

- Component
- Failure mode
- Failure mechanism
- Failure effect (local)
- Failure effect (system)
- Criticality (Severity)

Severity Levels

1. No effect
2. Minor, not noticed by average customer
3. Major, loss of primary function
4. Catastrophic, injury/death

Quantitative ETA

Quantitative Event Tree Analysis

OH	*Barrier 1a*	*Barrier 1b*	*Barrier 1c*	*Barrier 1d*	*Barrier 2*	*Barrier 3*	*OE Sev.*	Effects	*Pe*
	0.993116 A						5	No safety effect	
OH 2U-7		0.987384 B					4	Loss of separation 5 < x < 10 NM	6.80E-03 X & B
	6.88E-03 X		0.992699 C				3	Significant Reduction in separation 1 < x < 5 NM	8.62E-05 X&C&C
		1.26E-02 Y		0.93577236 D	0.90 E	0.80 F	2	Large reduction in safety margins x < 1 NM	6.21E-07 X&Y&Z& (D OR E OR F)
			7.30E-03 Z						
				5.36E-02 V	0.10 W	0.20 S	1	Near mid-air collision/ Collision	6.80E-10 X&Y&Z& V&W&S

- Quantify p(success) for each barrier
- Limitations
  - P(success) may not be random
  - May not be independent
  - May depend on order of events and context
  - Ex: Fukushima

Fukushima Diesel Generators

Quantitative results are affected by the way barriers are chosen

- Barrier 1a
  - Initial conditions keep aircraft > 10NM apart
  - P(success) = 0.99
- Barrier 1b
  - Initial conditions keep aircraft > 5NM apart
  - P(success) = 0.99
- Barrier 1c
  - Initial conditions keep aircraft > 1NM apart
  - P(success) = 0.99
- Barrier 2
  - Flight crew detects traffic by means other than visual, avoid NMAC
  - P(success) = 0.90
- Barrier 3
  - Flight crew detects traffic by visual acquisition, avoid NMAC
  - P(success) = 0.80

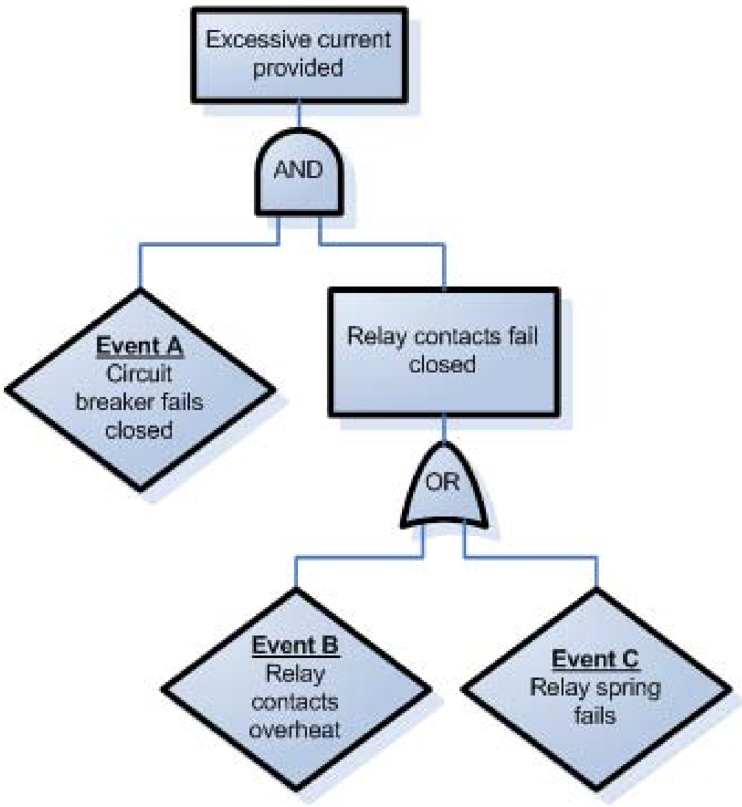
RTCA DO-312

Quantitative FTA

Quantitative Fault Tree Analysis

- If we can assign probabilities to lowest boxes…
  - Can propagate up using probability theory
  - Can get overall total probability of hazard!

- AND gate
  - P(A and B) = P(A) * P(B)
- OR gate
  - P(A or B) = P(A) + P(B)



Any assumptions being made?

Quantitative Fault Tree Analysis

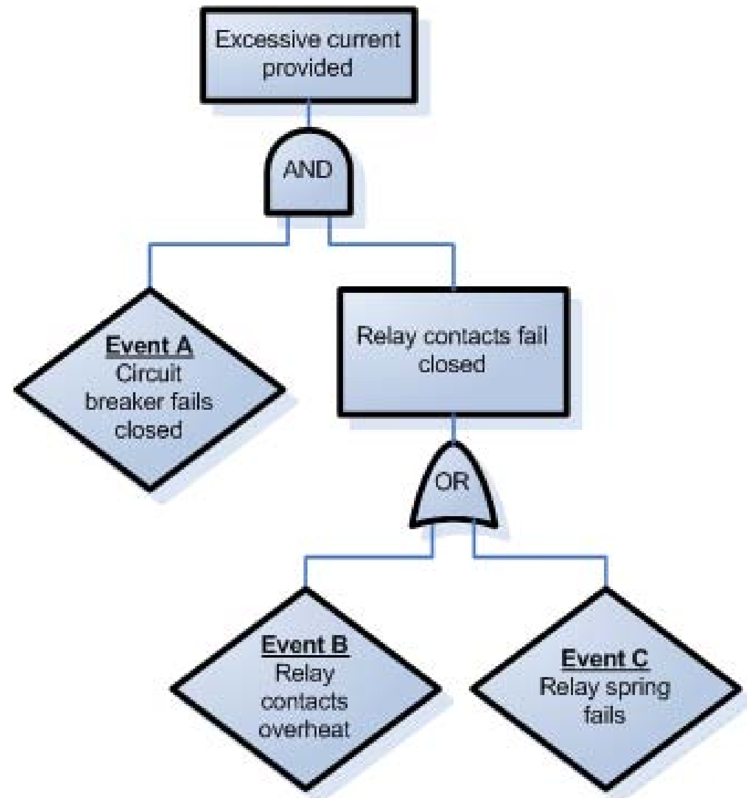
- If we can assign probabilities to lowest boxes…
  - Can propagate up using probability theory
  - Can get overall total probability of hazard!

- AND gate
  - P(A and B) = P(A) * P(B)
- OR gate
  - P(A or B) = P(A) + P(B)

Only if events A,B are independent!

Quantitative Fault Tree Analysis

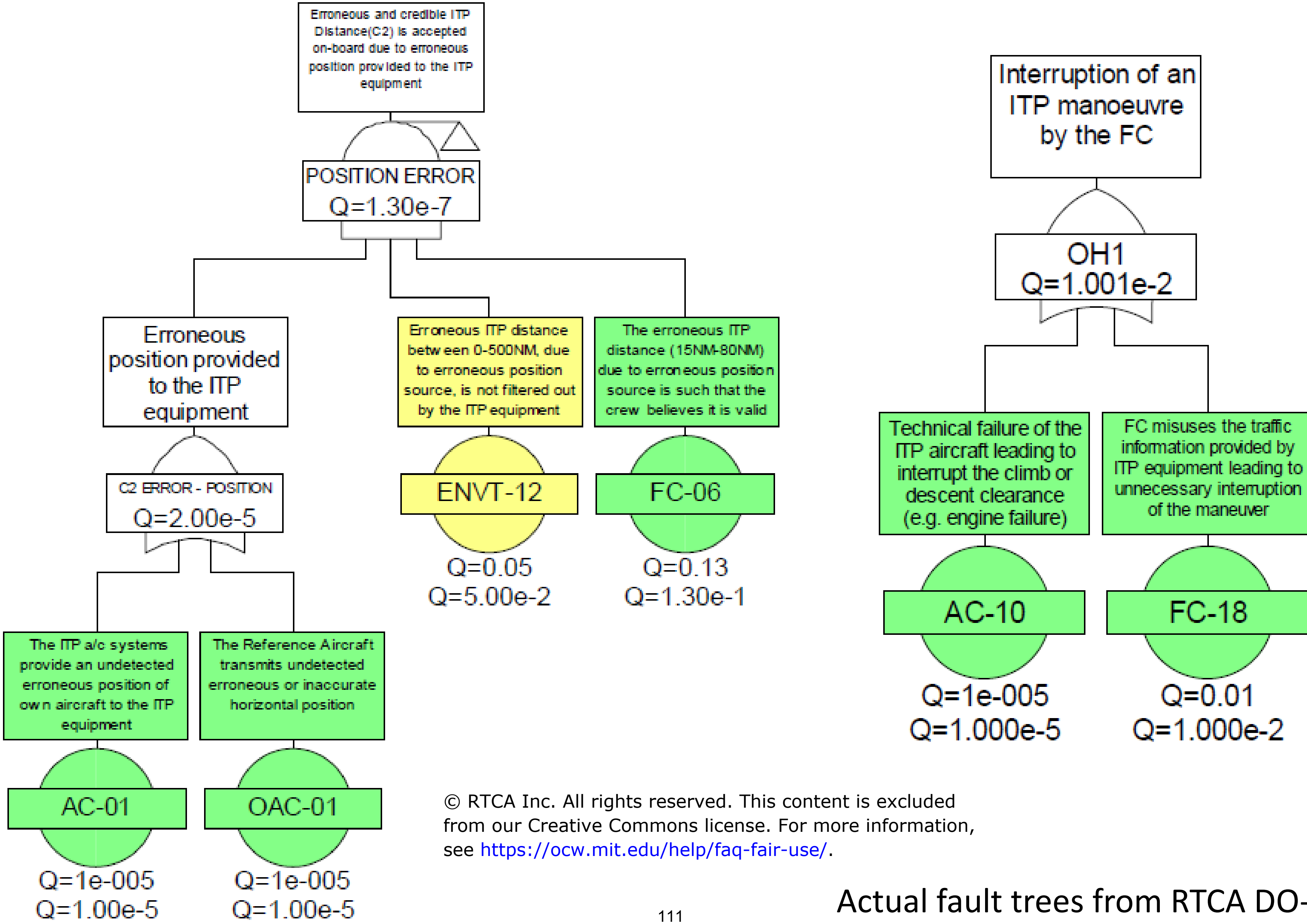
- If we can assign probabilities to lowest boxes…
  - Can propagate up using probability theory
  - Can get overall total probability of hazard!



- AND gate
  - P(A and B) = P(A) * P(B)
- OR gate
  - P(A or B) = P(A) + P(B)

- Is independence a good assumption?
  - Hardware?
  - Software?
  - Humans?

Quantitative Fault Tree Analysis



Actual fault trees from RTCA DO-312

Quantitative Fault Tree Analysis

- Where do the probabilities come from?
  - Historical data
  - Simulations
  - Expert judgment

Are there any issues using these sources?

Qualitative Frequency	Quantitative Probability
Very Often	1E-01
Often	1E-02
Rare	1E-03
Very Rare	Less than 1E-04

Table 3.1 Qualitative Frequency and Relation to Quantitative Probability for Basic Causes

*Actual qualitative-quantitative conversion from RTCA DO-312

Risk Assessment and Preliminary Hazard Analysis (PHA)

Preliminary Hazard Analysis

PROGRAM: ______					DATE: ______	
ENGINEER: ______					PAGE: ______	
ITEM	HAZARD COND	CAUSE	EFFECTS	RAC	ASSESS-MENTS	RECOMM-ENDATIONS
Assigned number	List the nature of the condition	Describe what is causing the stated condition to exist	If allowed to go uncorrected, what will be the effect or effects of the hazardous condition	Hazard Level assign-ment	Probability, possibility of occurrence: -Likelihood -Exposure -Magnitude	Recommended actions to eliminate or control the hazard

[Vincoli, 2005]

Risk Assessment Matrix

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

[US DoD, 2012]

Hardware Example

"Hardware Failure"

Hazard ID	Hazard Name	Hazard Description	Causes	Significance	Likelihood	Assumed Mitigations	Strength of Mitigations	Outcome Risk	Justification
TBO-0004	ADS-B Ground System Comm Failure	GBA does not receive ADS-B message	Receiver failure	High	Low	Redundant equipment; SSR; Primary Radar; Overlapping ADS-B coverage; Multi-Lat; Design and Equipment Certification Requirements	Medium	Medium	Strength of Mitigations depends on the type of backup; Multi-lat should be used if ...

[JPDO, 2012]

Software Example

"Software Flaw"

Hazard ID	Hazard Name	Hazard Description	Causes	Significance	Likelihood	Assumed Mitigations	Strength of Mitigations	Outcome Risk	Justification
TBO-0021	GBA fails to recognize dynamic situation and is unable to find a solution	The software lacks robustness in its implementation that leads to inability to find a solution	Design flaw, coding error, insufficient software testing, software OS problem	High	Med	Comprehensive system testing before certification and operational approval. TCAS; See and avoid. Pilot could recognize in some cases; Controller could recognize in some cases	Low / Medium	Med / High	Anything that is complex can lead to this situation

[JPDO, 2012]

Human Error Example

"Human Error"

Hazard ID	Hazard Name	Hazard Description	Causes	Significance	Likelihood	Assumed Mitigations	Strength of Mitigations	Outcome Risk	Justification
TBO-0045	Incorrect change to 4DT manually entered into GBA	ANSP makes mistake during manual data load into GBA when negotiating a strategic change to the 4DT	Human error	Med	Med	Pilot will have to accept the change; Conformance monitoring; GBA tactical separation; TCAS; Quality of Data check;	High	Medium	Outcome risk depends on design of the system, human factors issues will be key.

[JPDO, 2012]

No.	Task	Hazard	Risk	Risk Reduction	Final Risk
1	Position 3 Tasks, Install ECS	Falling object crushing person or body part	Yellow	Investigate process improvements	Green
2	Site Acceptance Test/Qualification Testing Passerby unauthorized entry	Person entering cell exposed to significant risks from robot, etc,	yellow	IML workstand gates to stop process when entered; Interlocked gates at Brand Scaffolding; access control, signage	Green
3	Robots Crossing Ped aisle in & out of replenishment cell (K)	AGV/moblie equipment impacts person	Yellow	AGV control system, signage, crossing markings on pedestrian aisle,	Green
4	Light Curtain Alternatives Analysis	Exposure to impact, crushing, etc. when safety scanners are deactivated when OML's "leapfrog"	Yellow	Establish safe procedure, use of spotters, hand guiding	Green
5	All Sub-processes All Users normal operation	Exposure to movement of robots, motors and cylinders.	Red	Safety perimeter, category 4, that stops automation when violated; investigate use of Kuka.safesolutions, e-stop control, access control, procedures, training	Green
6	normal operation	mechanical: Drill penetration of fuselage Operator exposes body part to drill penetration	Yellow	Only one operator in workspace, proper training	Green
7	AFB movement systems	AGV trapping person against immovable object or running someone over	Yellow	AGV safety system with scanners	Green
8	Traffic management	mechanical : Impact, pinching, crushing Exposure to impact, pinching, crushing by AGV, OML's, etc	yellow	AGV's equipped with safety Laser scanners with 360 degrees coverage, hand guiding, use of spotters, procedures	Green
9	Maintenance activities	ingress / egress : Exposure to being hit by robot performing maintenance Maintenance person exposed while working on machinery	Yellow	Lock out auto to enter, lock out other sources as required	
10	AGV's & Movement Systems	mechanical : Collision-impact two robots same side of barrier AGV impacts person	Yellow	AGV safeguarding using SICK area scanners 360 degree coverage to stop AGV if violated; people will be clear of cell(another line); walls (Anacortes) or ?light curtains? to stop motion if violated; Training and Amin procedures	Green

Example Risk Assessment: Manufacturing Robot

No.	Task	Hazard	Risk	Risk Reduction	Final Risk
2	Site Acceptance Test/Qualification Testing Passerby unauthorized entry	Person entering cell exposed to significant risks from robot, etc,	Yellow	Access control, signage	Green
3	Robots Crossing Ped aisle in & out of replenishment cell	Mobile equipment impacts person	Yellow	AGV control system, signage, crossing markings on pedestrian aisle,	Green
4	Light Curtain Alternatives Analysis	Exposure to impact, crushing, etc. when safety scanners are deactivated when OML's "leapfrog"	Yellow	Establish safe procedure, use of spotters, hand guiding	Green
	Position 3 Tasks, Install ECS	Falling object crushing person or body part	Red	Investigate process improvements	Green

UH-60MU SAR Hazard Classification

UH-60MU SAR marginal hazards

- Loss of altitude indication in DVE
- Loss of heading indication in DVE
- Loss of airspeed indication in DVE
- Loss of aircraft health information
- Loss of external communications
- Loss of internal communications

UH-60MU SAR identifies various hazards as marginal that actually could lead to a catastrophic accident

STPA Unsafe Control Action

The Flight Crew does not provide collective control input necessary for level flight, resulting in controlled flight into terrain

Scenario 1: The Flight Crew has a flawed process model and believes they are providing sufficient control input to maintain level flight. This flawed process model could result from:

a)The altitude indicator and attitude indicator are malfunctioning during IFR flight and the pilots are unable to maintain level flight

b)The Flight Crew believes the aircraft is trimmed in level flight when it is not

c)The Flight Crew has excessive workload due to other tasks and cannot control the aircraft

d)The Flight Crew has degraded visual conditions and cannot perceive slow rates of descent that result in a continuous descent

e)The Flight Crew does not perceive rising terrain and trims the aircraft for level flight that results in controlled flight into terrain

Current State of the Art: PRA

- Risk and Risk Assessment
  - Little data validating PRA or methods for calculating it
  - Other problems
    - May be significant divergence between modeled system and as-built and as-operated system
    - Interactions between social and technical part of system may invalidate technical assumptions underlying analysis
    - Effectiveness of mitigation measures may change over time
  - Why are likelihood estimates inaccurate in practice?
    - Important factors left out (operator error, flawed decision making, software) because don’t have probability estimates
    - Non-stochastic factors involved in events
    - Heuristic biases

Heuristic Biases

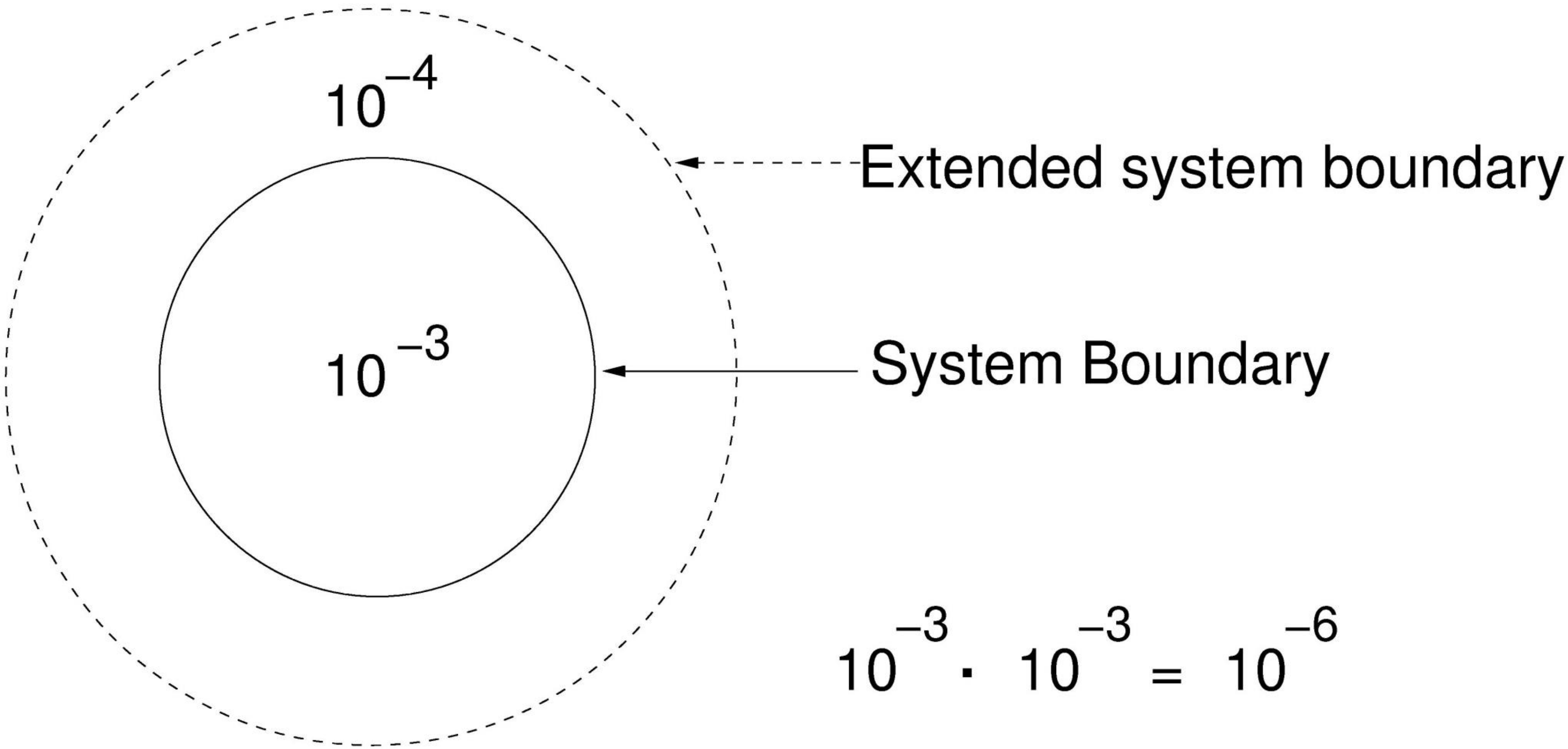
- Confirmation bias (tend to deny uncertainty and vulnerability)
  - People look for evidence that supports their hypothesis
  - Reject evidence that does not
- Construct simple causal scenarios
  - If none comes to mind, assume impossible
- Tend to identify simple, dramatic events rather than events that are chronic or cumulative
- Incomplete search for causes
  - Once one cause identified and not compelling, then stop search
- Defensive avoidance
  - Downgrade accuracy or don't take seriously
  - Avoid topic that is stressful or conflicts with other goals

Controlling Heuristic Biases

- Cannot eliminate completely but can reduce
- Use structured method for assessing and managing "risk"
  - Following a structured process and rules to follow can diminish power of biases and encourage more thorough search
  - Concentrate on causal mechanisms vs. likelihood
  - Require action or procedures (to avoid defensive avoidance)
- Use worst case analysis (vs. "design basis accident")
- "Prove" unsafe rather than "safe"
  - Hazard analysis vs. safety case

Misinterpreting Risk

Risk assessments can easily be misinterpreted:



Cost Benefit Analysis

Cost-benefit analysis

- Goes beyond identifying risk
- Is it worth fixing?

$

How much does it cost to fix?

$

How much does it cost NOT to fix?

Ford Pinto

- Ford noticed design flaw too late to eliminate
  - Fuel tank directly behind axle
  - Rear-end collision can cause disaster
- Engineers developed a patch
  - $11 per car, reinforced structure
- Cost-benefit analysis
  - Total cost to fix: **$137.5 million**
  - Human life is worth $200,000
    - 180 expected burn deaths
  - Serious human injury is worth $67,000
    - 180 expected serious burn injuries
  - Burned out vehicle is worth $700
    - 2,100 expected burned out vehicles
  - Total cost if not fixed: **$49 million**

One lawsuit ruling (1972):
- Ford to pay $2.5 million compensatory damages
- Ford to pay $3.5 million because Ford was aware of design defects before production but did not fix the design

Ford Pinto

- Cost of human life was based on National Highway Traffic Safety Administration regulations
  - $200,725 per life
- Fuel tank location was commonplace at that time in American cars
- California supreme court had tolerated and encouraged manufacturers to trade off safety for cost
- NHTSA recorded 27 Pinto rear-impact fires
  - Lower than average for compact cars at the time

General Motors

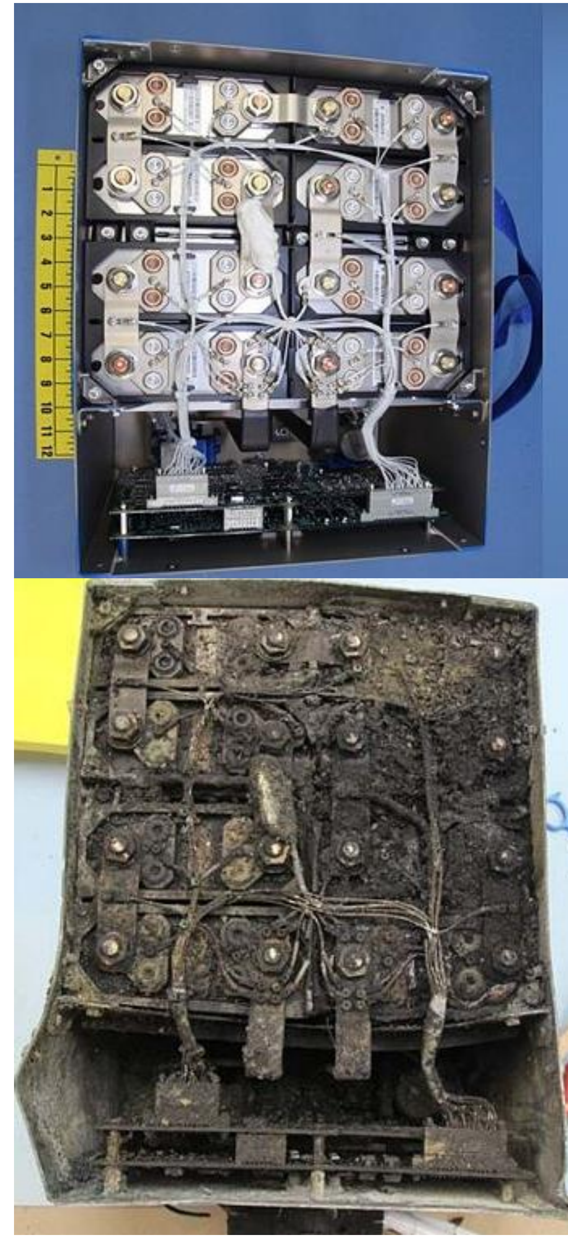
- 13 deaths, 130 reported incidents
- Design flaws
  - Ignition switches easily switch to “off” position
    - Bumps, vehicle collision, heavy keychain, etc.
  - Keys have wide slot, increased torque
  - Airbags and other safety systems immediately disabled when key is off
- Cost-benefit analysis
  - GM aware of problem for over a decade
  - Developed a fix, costs $0.57 per car
  - Recommended no further action because there was “no acceptable business case”
    - Tooling cost and piece price was too high
- CEO response
  - That is very disturbing if true
  - This is not how GM does business
  - If there is a safety issue we take action. We do not look at the cost associated with it.

General Motors

- Systemic factors
  - Wrote service bulletin to fix key slot, but kept it private
  - Knew in 2001 that ignition switches did not meet specification
    - 4-10 vs. 15-25
  - Updated part in 2006
    - Kept old part number, confusion
    - Still didn’t meet specification (10-15 vs. 15-25)

Boeing

- Boeing 787 LiCo Batteries
- Prediction/Certification:
  - No fires within 10^7 flight hours
  - Followed 4761 certification paradigm
- Actual experience:
  - Within 52,000 flight hours – 2 such events
  - 2.6×10^4 flight hours [NTSB 2013]



[http://upload.wikimedia.org/wikipedia/commons/9/95/Boeing_Dreamliner_battery_original_and_damaged.jpg]

Boeing 787 Lithium Battery Fires

- A module monitors for smoke in the battery bay, controls fans and ducts to exhaust smoke overboard.
- Power unit experienced low battery voltage, shut down various electronics including ventilation.
- Smoke could not be redirected outside cabin

All software requirements were satisfied!
The requirements were inadequate

Lord Kelvin quote

- “I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of *Science*, whatever the matter may be.“
  - [PLA, vol. 1, "Electrical Units of Measurement", 1883-05-03]

A response

- "In truth, a good case could be made that if your knowledge is meagre and unsatisfactory, the last thing in the world you should do is make measurements; the chance is negligible that you will measure the right things accidentally.“
  - George Miller (a psychologist)