Reliability and System Risk Analysis Workshop

Dr. John Thomas

Today's Agenda

- Intro to reliability and system risk
- Overview of analysis techniques
- Traditional qualitative techniques
    - Failure Modes and Effects Analysis
    - Fault Tree Analysis
    - Event Tree Analysis
    - HAZOP
- Traditional quantitative techniques
    - Quant. Fault Tree Analysis
    - FMECA
    - Quant. ETA

Tomorrow:
- Human factors
- System-theoretic techniques

Introduction: Reliability and System Risk Analysis

- What is Reliability?
  - Probability that a component or system will perform its specified function (for a prescribed time under stated conditions)
- What is Risk?
  - Threat of damage, injury, liability, loss, or any other negative occurrence that may be avoided through preemptive action.
- What is a Failure?
  - Inability of a component to perform its specified function (for a prescribed time under stated conditions)
- What is Safety?
  - Freedom from undesired losses (e.g. loss of life, loss of mission, environmental damage, customer satisfaction, etc.)

Two basic types of losses

- Losses caused by component failure
  - Focus of reliability analysis

Today’s class

- Losses caused by component interactions
  - Often occur without failures
  - Can be more difficult to anticipate

Tomorrow’s class

Three Mile Island

Events: A critical relief valve fails (stuck open) and begins venting coolant. Despite best efforts, operators are unable to mitigate this problem in time and the reactor experiences a meltdown. Radioactive materials are released. $1B cleanup costs.

Component failure losses

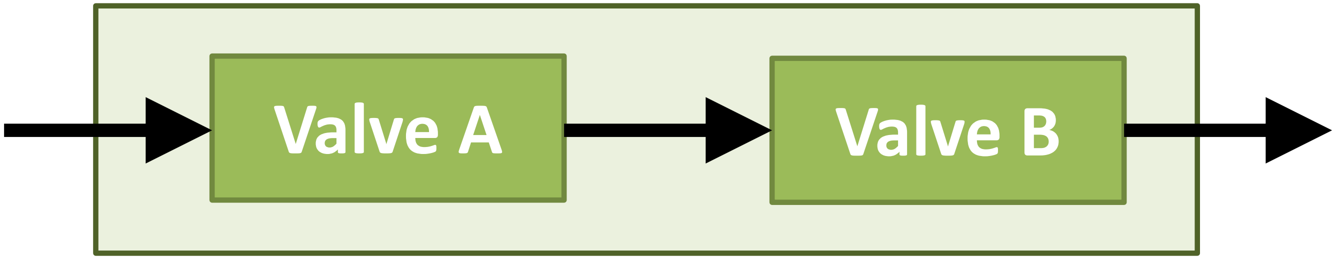
- These are losses caused by physical component failures
  - E.g. valve stuck open
  - Failure: Component does not perform as specified

- What would you do about this?
  - Make valve more reliable
  - Use redundant valves
  - More frequent maintenance / testing
    - E.g. ATLAS compressors

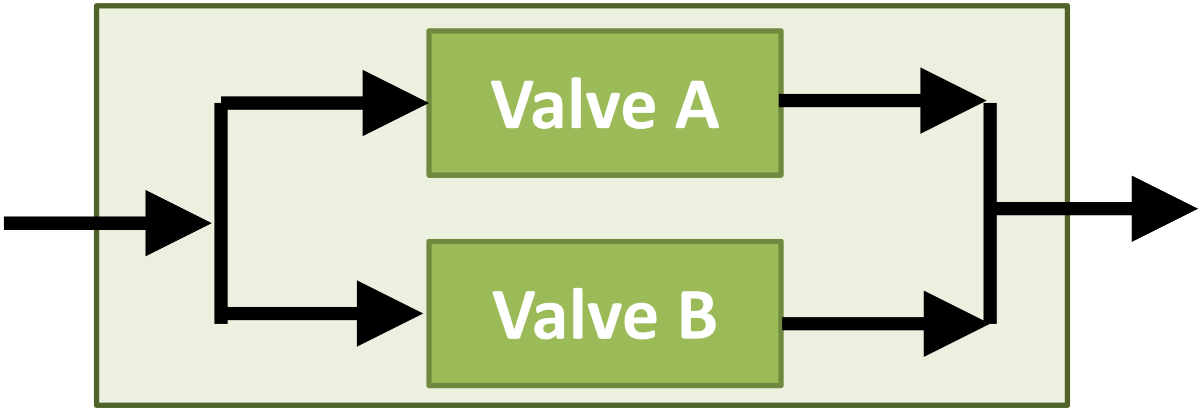
Classic reliability solutions

Redundancy

Two valves in series:



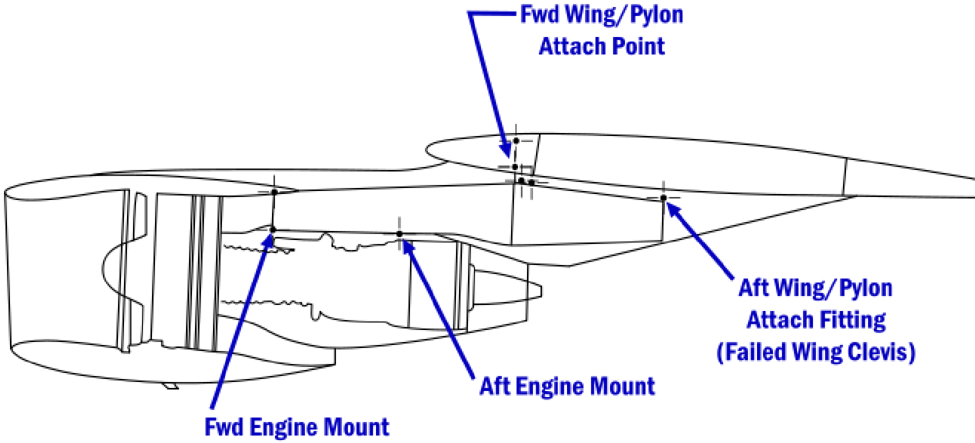
Two valves in parallel:



What happens if one valve is stuck open or stuck closed?

Dealing with component failures

- Potential solutions:
  - Eliminate failure
  - Reduce effect of failure
    - Use redundancy
    - Design to fail in a safe state
    - Design to tolerate the failure
  - Make failure less likely
    - Improve component reliability
  - Reduce duration of failure
  - Etc.



Component failure losses

- Beware of “tunnel vision”
  - Very easy to focus only on the physical failure
  - There are usually deeper systemic factors too

Three Mile Island

Events: A critical relief valve fails (stuck open) and begins venting coolant. Despite best efforts, **operators are unable to mitigate this problem in time** and the reactor experiences a meltdown. Radioactive materials are released. $1B cleanup costs.

Deeper systemic factors?

Three Mile Island

Other Causal Factors:

- Post-accident examination discovered the “open valve” indicator light was configured to show presence of power to the valve (regardless of valve position).

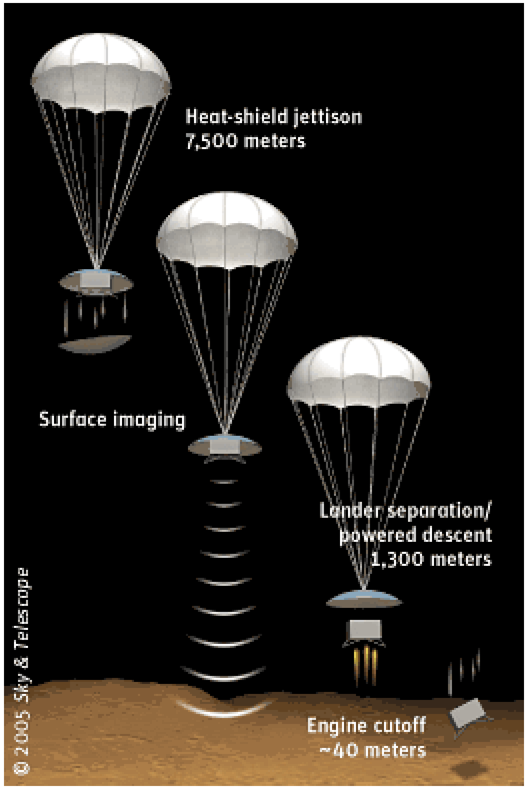
Design flaw!
Communication problems!
Inadequate procedures!
Etc.

CSB video

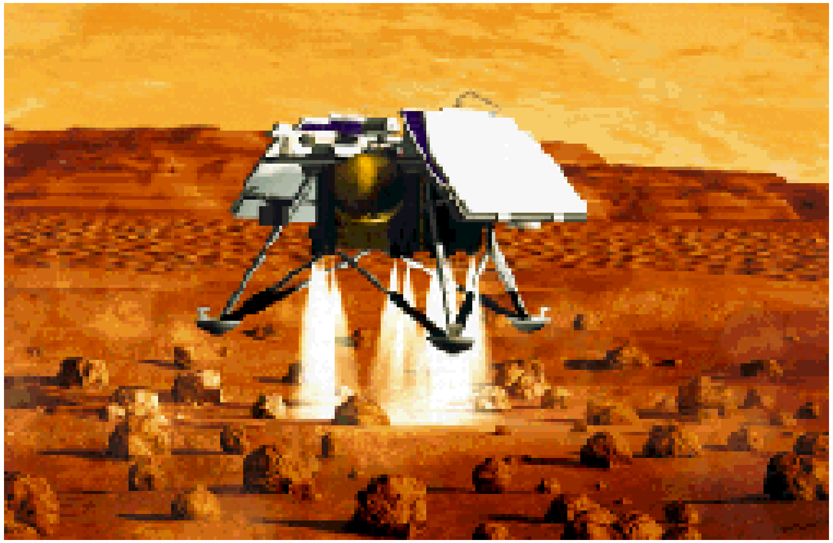
- Cooling system incident
  - “Shock to the System” video on YouTube
- Discuss “Sharp end” vs. “Blunt end”
- Discuss types of recommendations generated

Mars Polar Lander

- During the descent to Mars, the legs were deployed at an altitude of 40 meters.
- Touchdown sensors (on the legs) sent a momentary signal
- The software responded as it was required to: by shutting down the descent engines.
- The vehicle free-fell and was destroyed upon hitting the surface at 50 mph (80 kph).



© 2005 Sky & Telescope



No single component failed. All components performed as designed.

Component interaction losses

- … are losses caused by interactions among several components
  - May not involve any component failures
  - All components may operate as designed
    - But the design may be wrong
    - Requirements may be flawed
  - Related to complexity
    - Becoming increasingly common in complex systems
    - Complexity of interactions leads to unexpected system behavior
    - Difficult to anticipate unsafe interactions
  - Especially problematic for software
    - Software always operates as designed

Systems-Theoretic Approaches

- Focus of tomorrow’s class
- Need to identify and prevent failures, but also:
  - Go beyond 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.

Today's Agenda

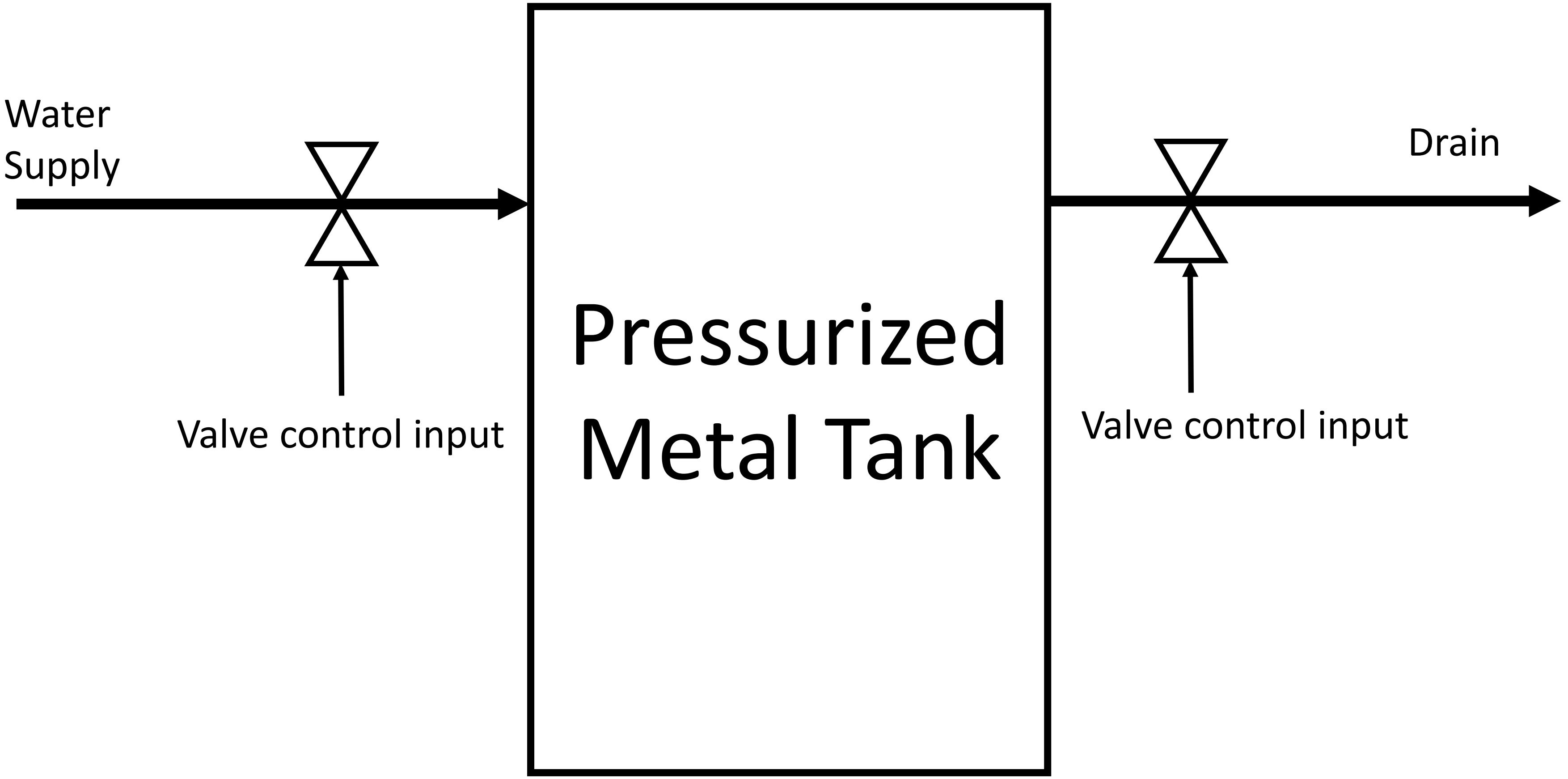
- ✓ Intro to reliability and system risk
- ➡ Overview of analysis techniques
- Traditional qualitative techniques
  - Failure Modes and Effects Analysis
  - Fault Tree Analysis
  - Event Tree Analysis
  - HAZOP
- Traditional quantitative techniques
  - Quant. Fault Tree Analysis
  - FMECA
  - Quant. ETA

Risk/Hazard/Causal Analysis

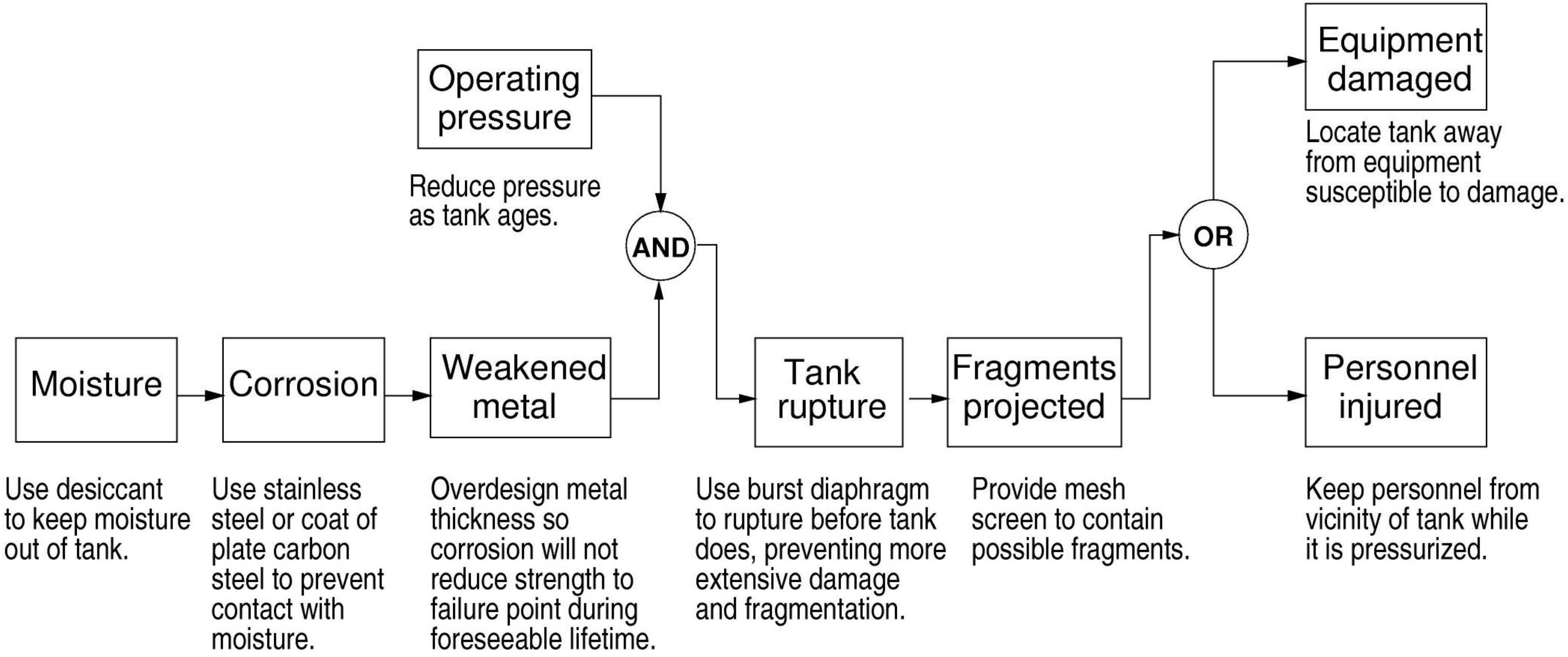
- "Investigating a loss before it happens"
- Goal is to identify causes of losses (before they occur) so we can eliminate or control them in
  - Design
  - Operations
- Requires
  - An accident causality model
  - A system design model

"Accident" is any incident, any undesired loss

System Design Model (simplified)



Accident model: Chain-of-events example



Operating pressure

Reduce pressure as tank ages.

AND

Moisture

Use desiccant to keep moisture out of tank.

Corrosion

Use stainless steel or coat of plate carbon steel to prevent contact with moisture.

Weakened metal

Overdesign metal thickness so corrosion will not reduce strength to failure point during foreseeable lifetime.

Tank rupture

Use burst diaphragm to rupture before tank does, preventing more extensive damage and fragmentation.

Fragments projected

Provide mesh screen to contain possible fragments.

OR

Equipment damaged

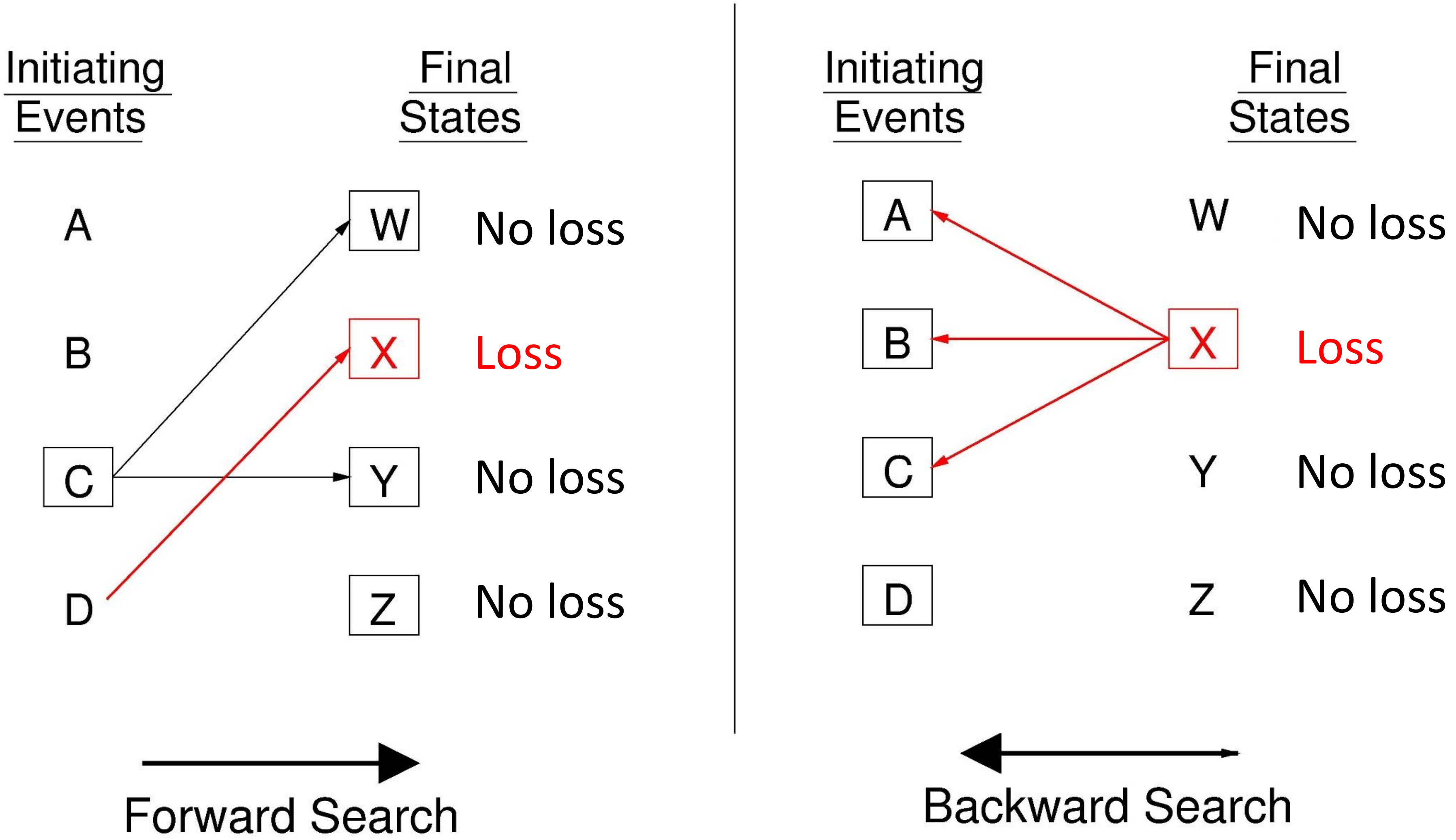
Locate tank away from equipment susceptible to damage.

Personnel injured

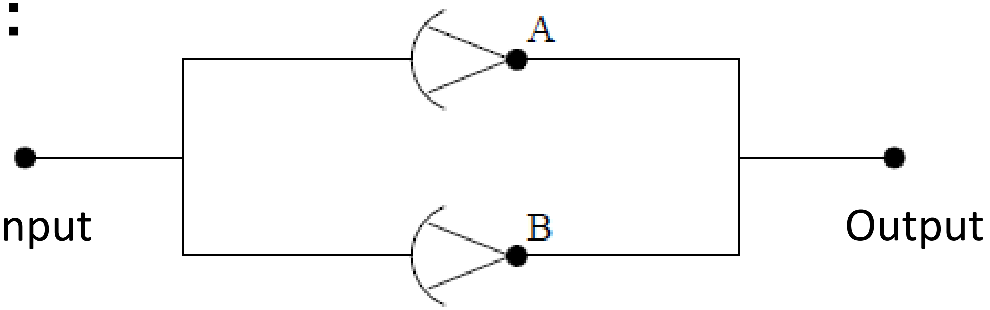
Keep personnel from vicinity of tank while it is pressurized.

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

Forward vs. Backward Search



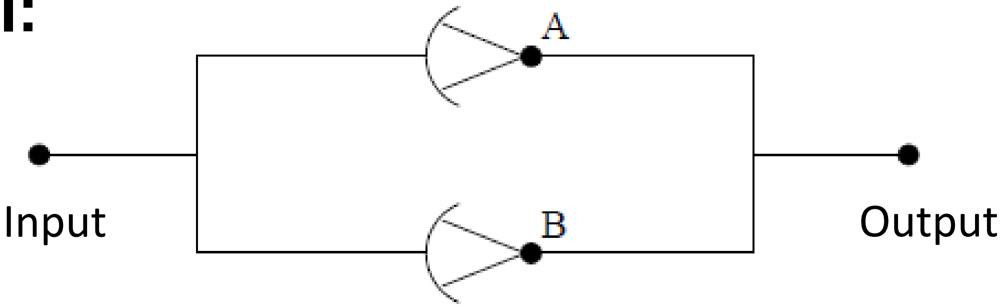
System Model:



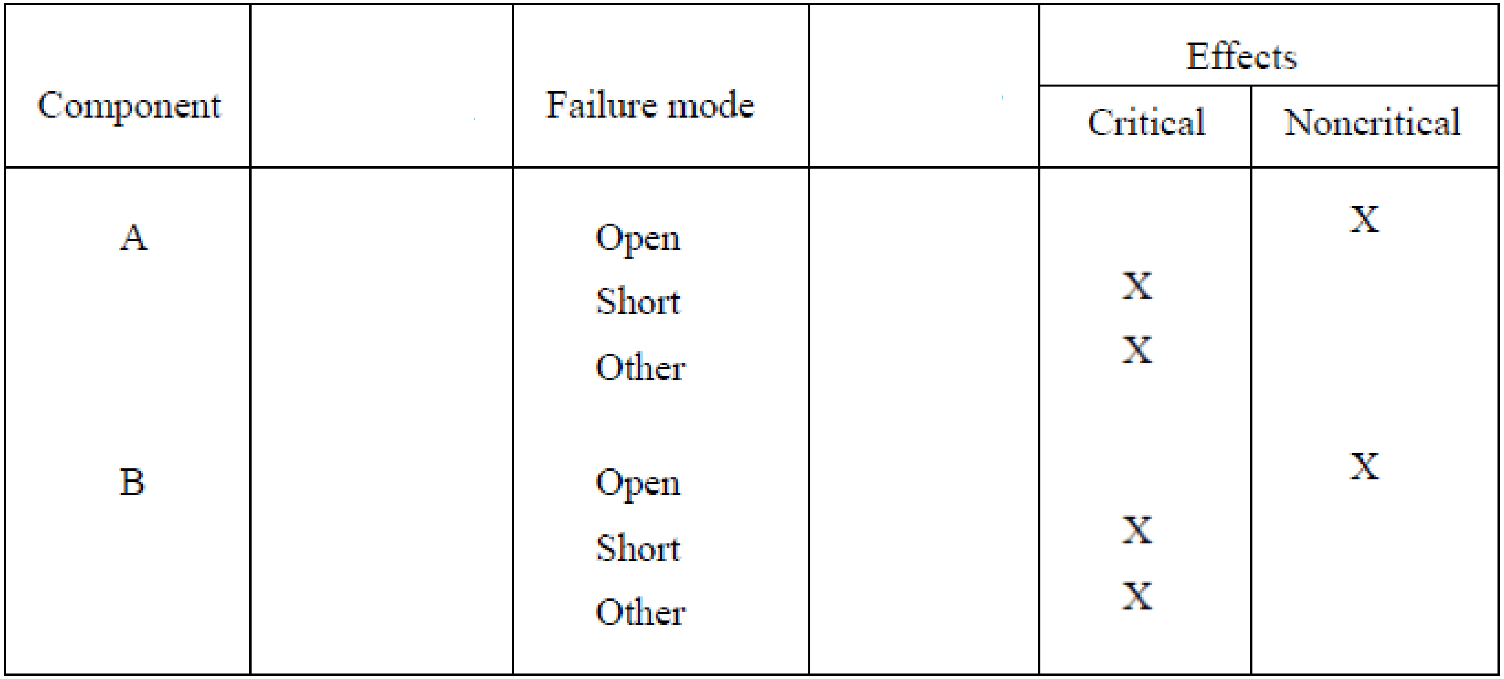
Forward search?

a system of two amplifiers in parallel.

System Model:



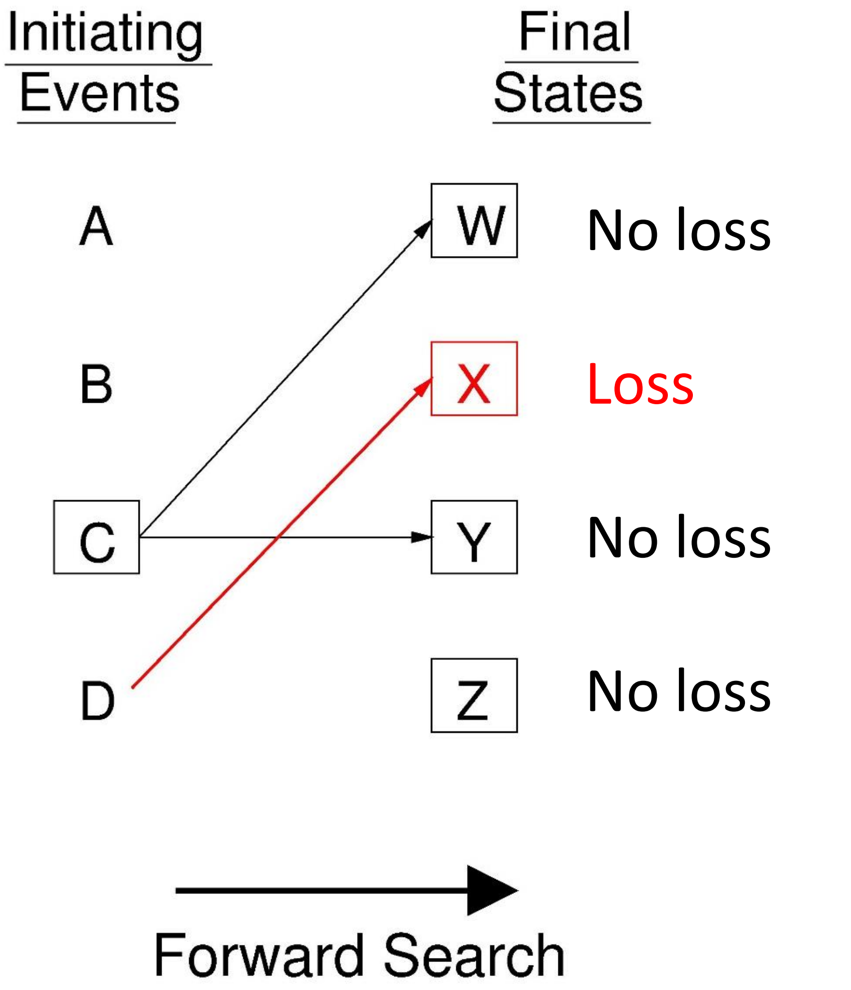
Forward search:

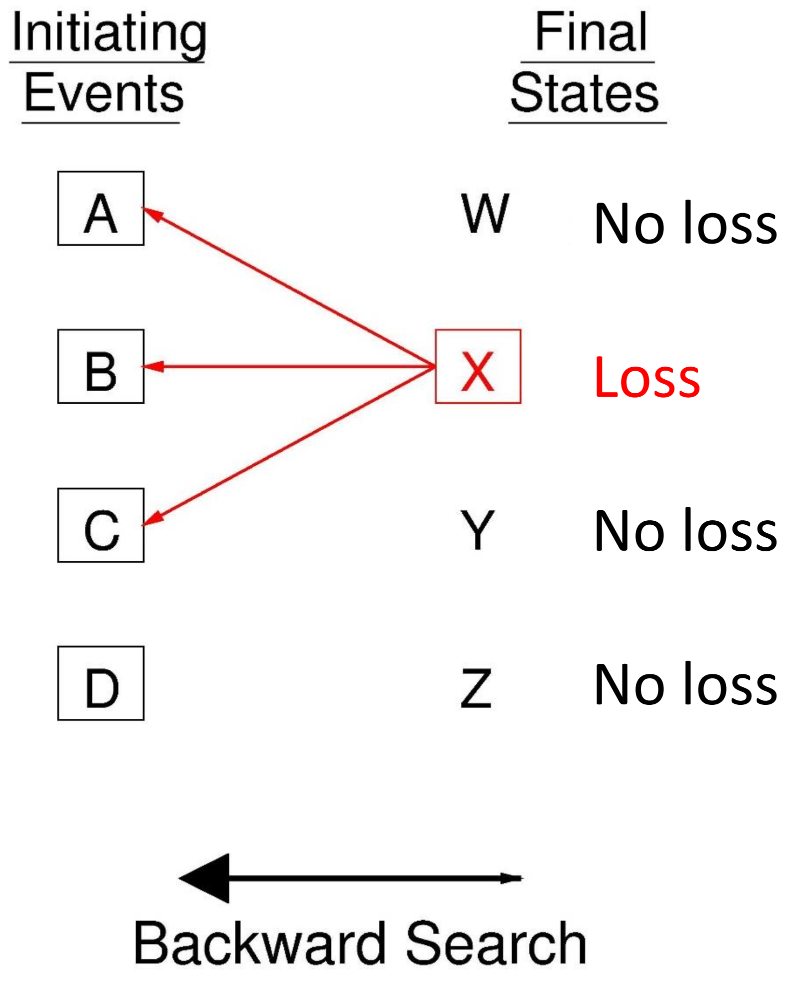


Component		Failure mode		Effects	
				Critical	Noncritical
A		Open			X
		Short		X	
		Other		X	
B		Open			X
		Short		X	
		Other		X	

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?

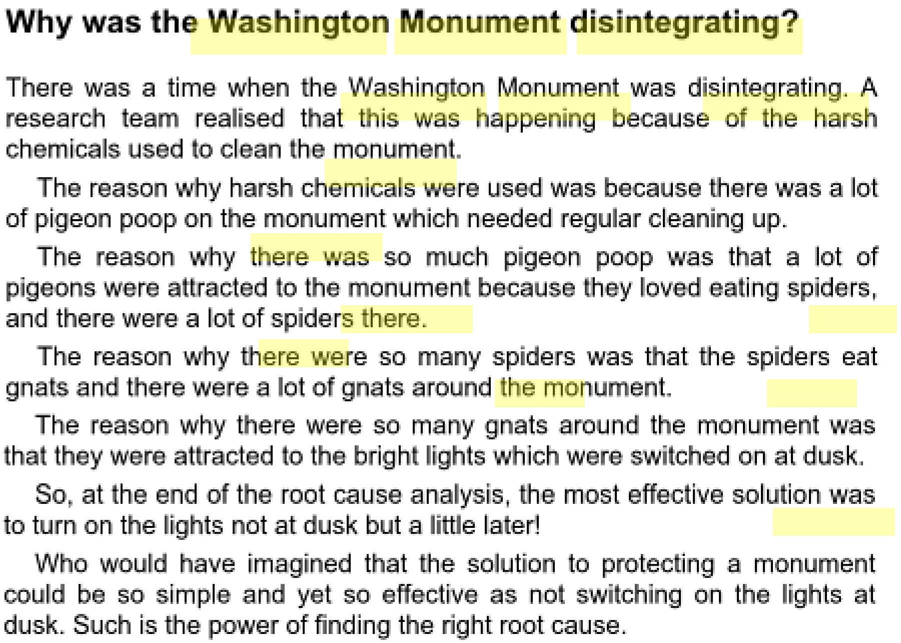
They eat gnats and lots of gnats at monument

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.

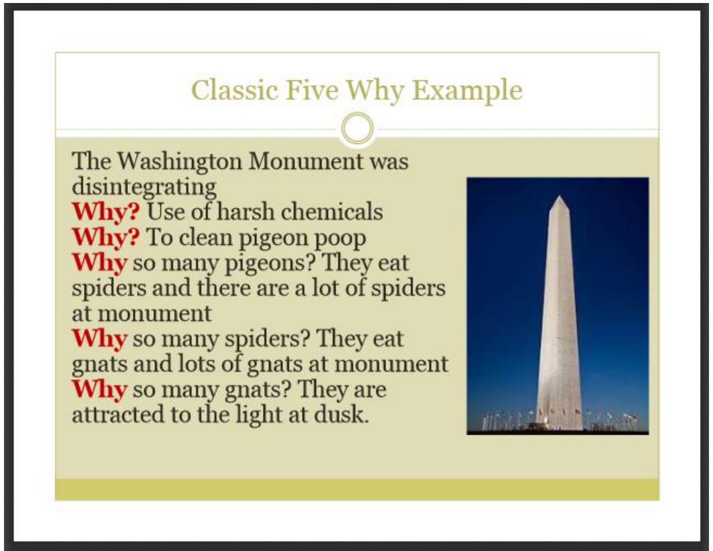
The reason why there was so much pigeon poop was that a lot of pigeons were attracted to the monument because they loved eating spiders, and there were a lot of spiders there.

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.

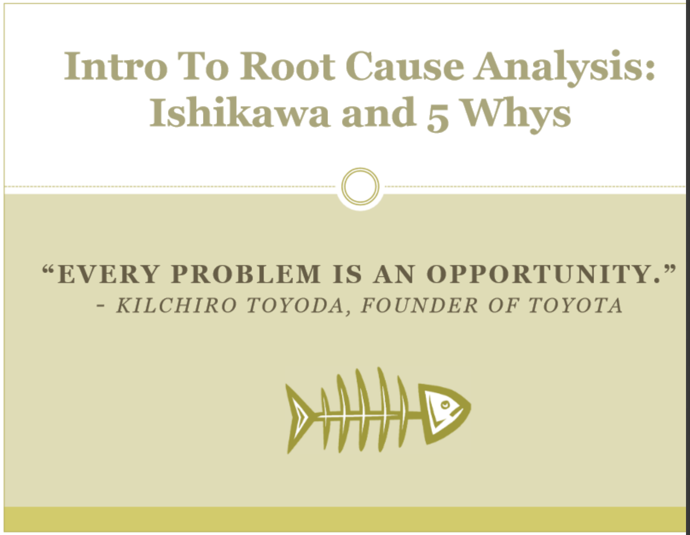
So, at the end of the root cause analysis, the most effective solution was to turn on the lights not at dusk but a little later!

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.



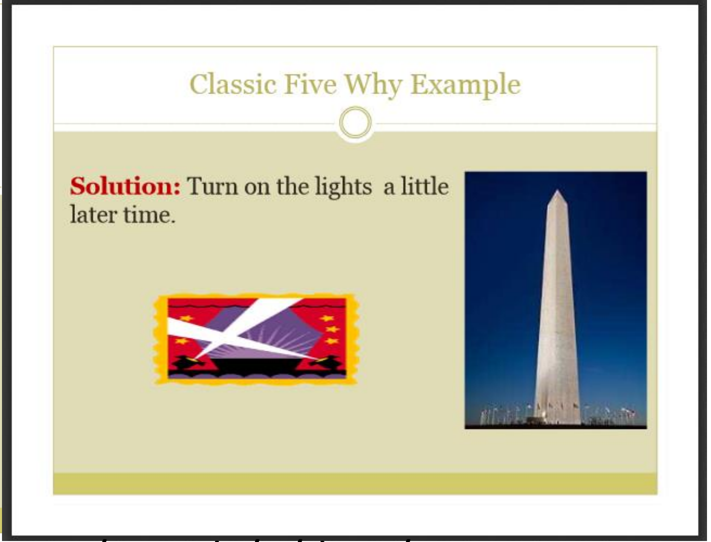
Classic Five Why Example

The Washington Monument was disintegrating
Why? Use of harsh chemicals
Why? To clean pigeon poop
Why so many pigeons? They eat spiders and there are a lot of spiders at monument
Why so many spiders? They eat gnats and lots of gnats at monument
Why so many gnats? They are attracted to the light at dusk.



Intro To Root Cause Analysis: Ishikawa and 5 Whys

“EVERY PROBLEM IS AN OPPORTUNITY.”
- *KILCHIRO TOYODA, FOUNDER OF TOYOTA*



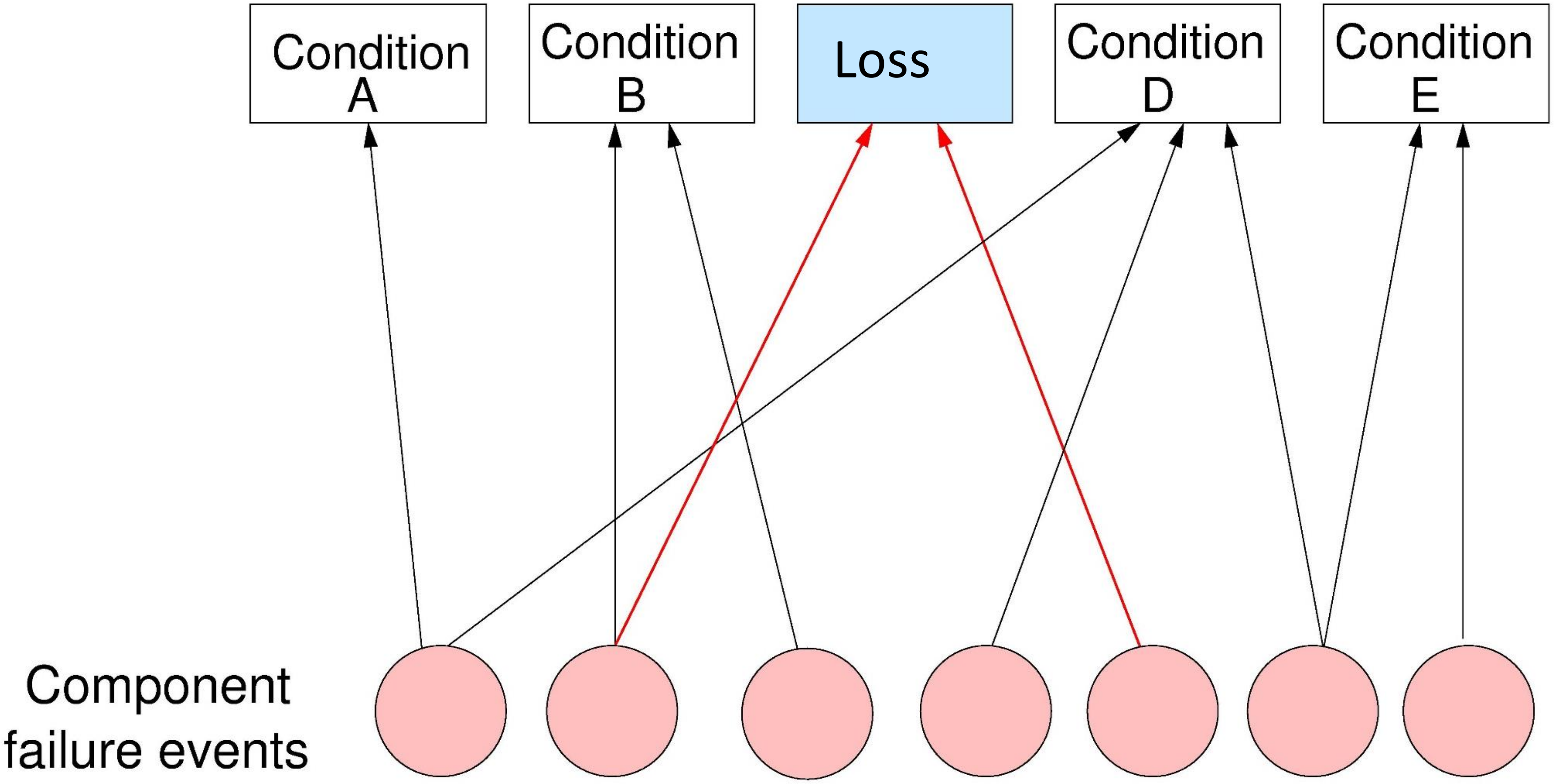
Classic Five Why Example

Solution: Turn on the lights a little later time.

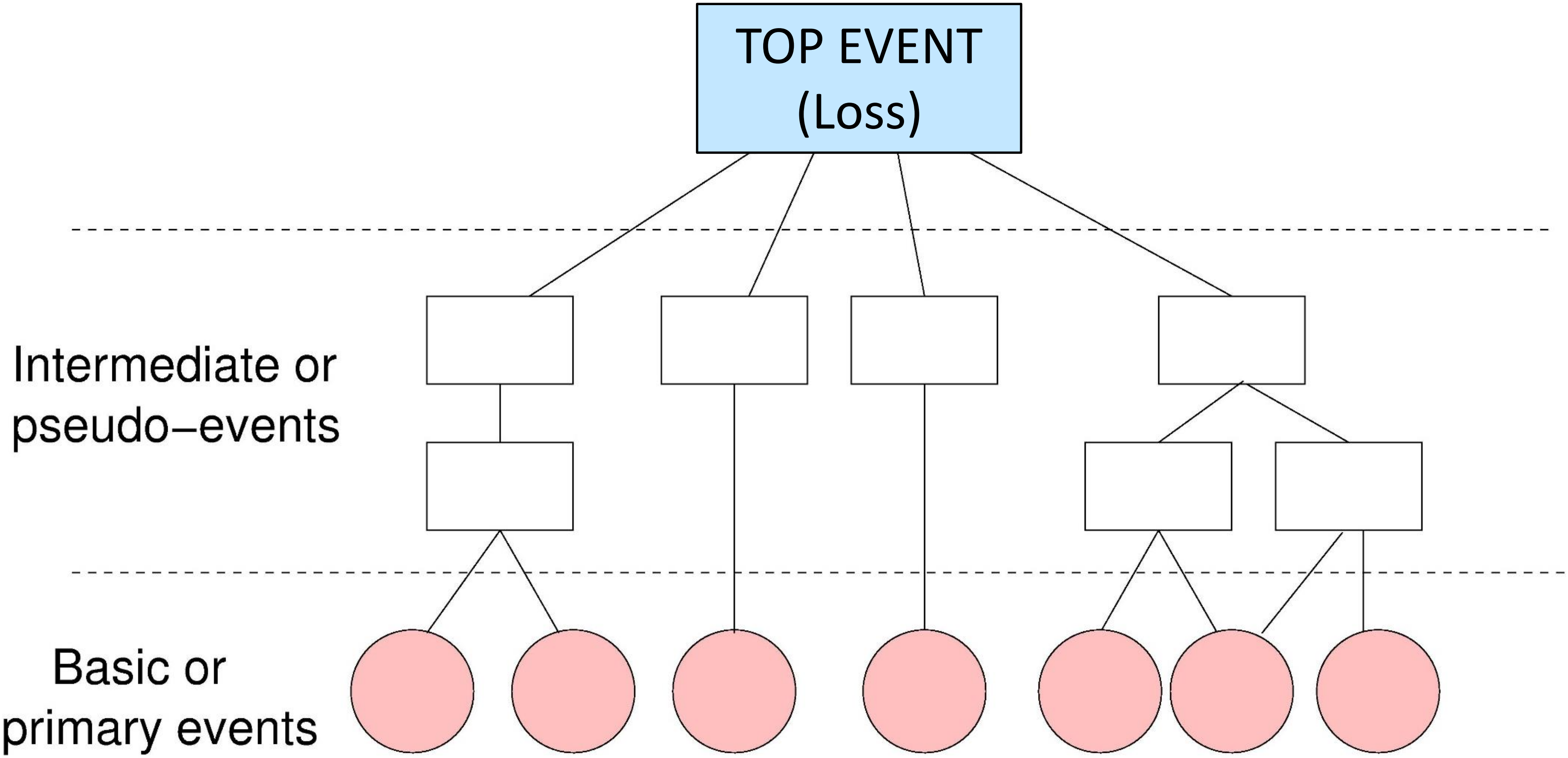
“Breaking the accident chain of events” (see video)

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

Bottom-Up Search



Top-Down Search



Top-Down Example

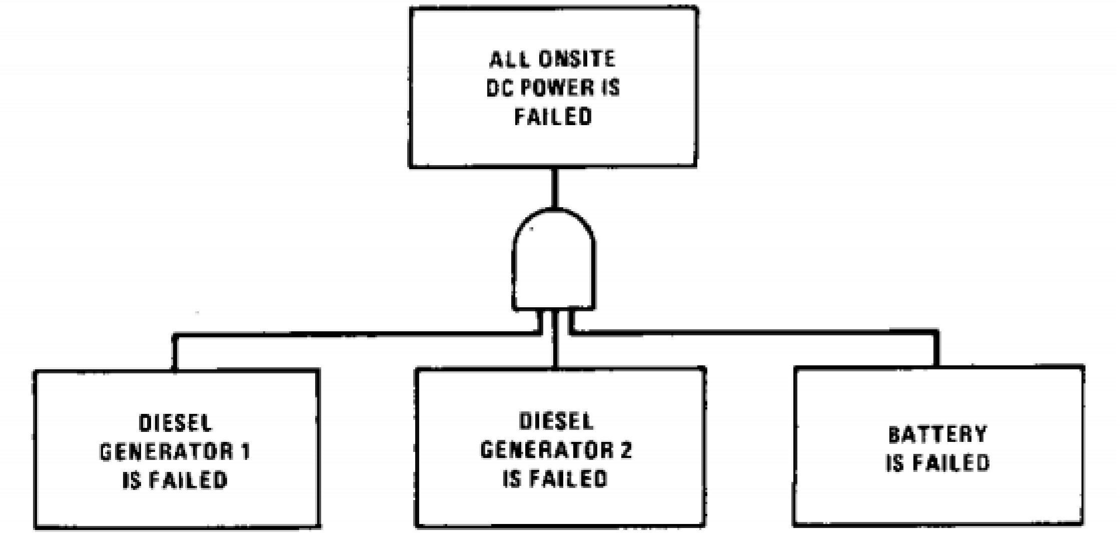
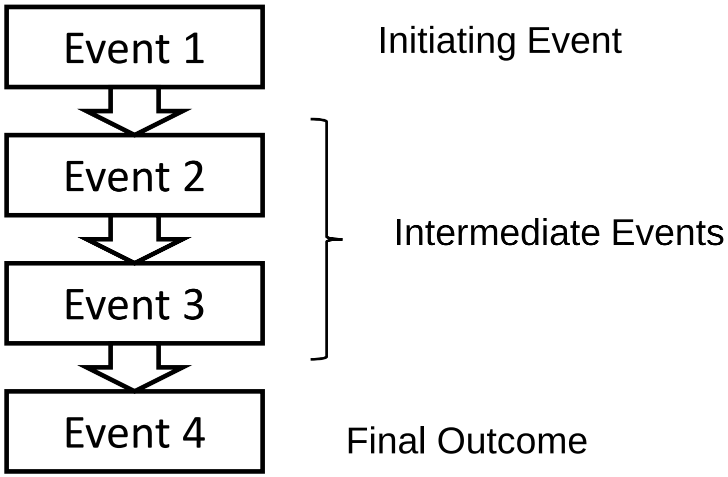


Image from Vesely

Accident models

- Chain-of-events model is very popular
  - Intuitive, requires little or no training
  - Can be traced to Aristotle (300 BC) and earlier
    - “Aristotle claims that in a chain of efficient causes, where the first element of the series acts through the intermediary of the other items, it is the first member in the causal chain, rather than the intermediaries, which is the moving cause (See *Physics* 8.5, Aristotle, 257a10–12).”
  - Forms basis for many other accident models



Event 1

Initiating Event

Event 2

Event 3

Intermediate Events

Event 4

Final Outcome

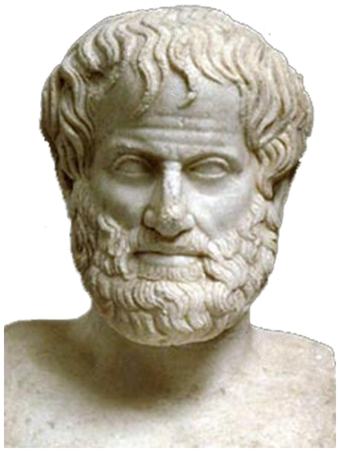
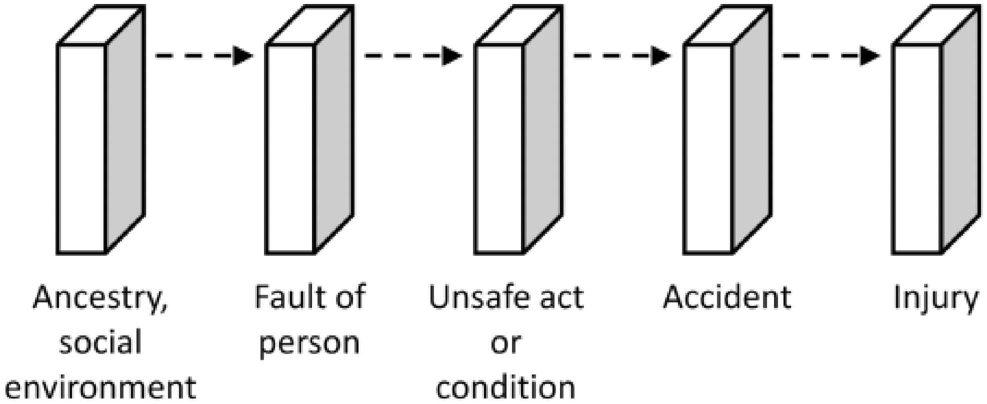


Image from: http://en.wikipedia.org/wiki/File:Aristotle_Bust_White_Background_Transparent.png
Quote from: http://plato.stanford.edu/entries/aristotle-natphil/

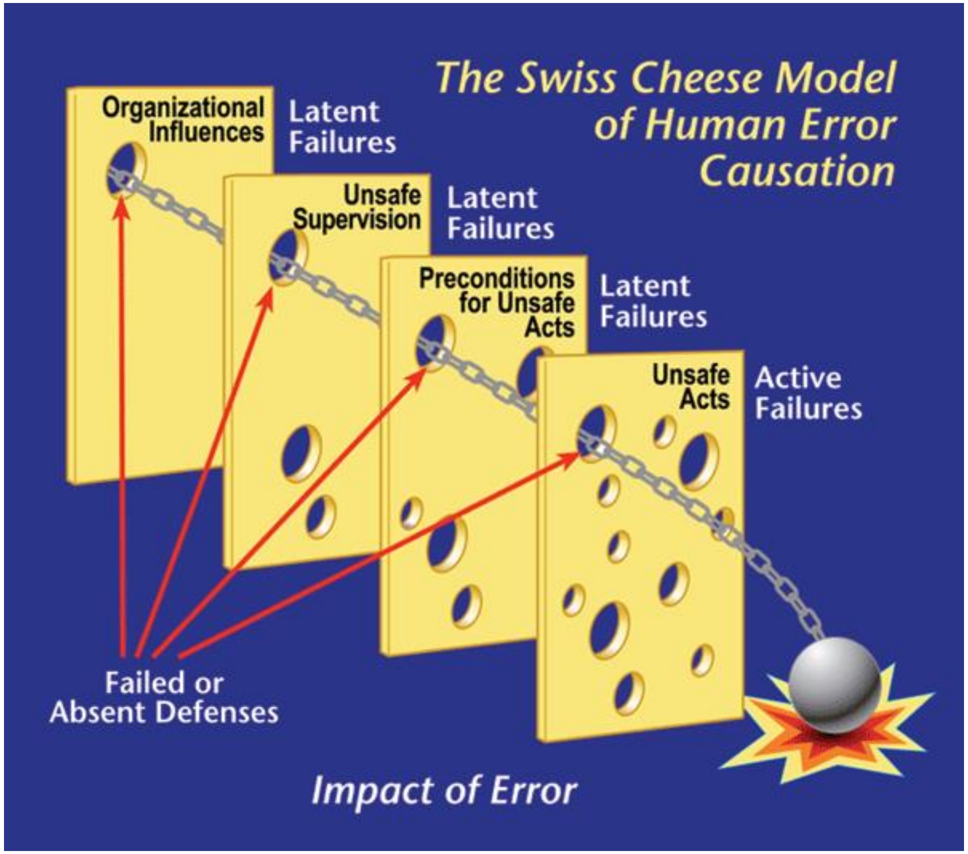
Other accident models

- Domino model
  - Herbert Heinrich, 1931
  - Essentially a chain-of-events model
  - What additional assumptions are made?



Other accident models

- Swiss cheese accident model
  - James Reason, 1990
  - Essentially a chain-of-events model


The Swiss Cheese Model of Human Error Causation
Organizational Influences
Latent Failures
Unsafe Supervision
Latent Failures
Preconditions for Unsafe Acts
Latent Failures
Unsafe Acts
Active Failures
Failed or Absent Defenses
Impact of Error

- Additional assumptions
  - Accidents caused by unsafe acts
  - Random behavior
  - Solved by adding layers of defense
  - Omits systemic factors
    - I.e. how are holes created?

Image from: http://www.fireengineering.com/articles/print/volume-163/issue-3/features/managing-fireground-errors.html

Other accident models

- Parameter deviation model
  - Used in HAZOP (1960s)

- Incidents caused by deviations from design or operating intentions
  - E.g. flow rate too high, too low, reverse, etc.

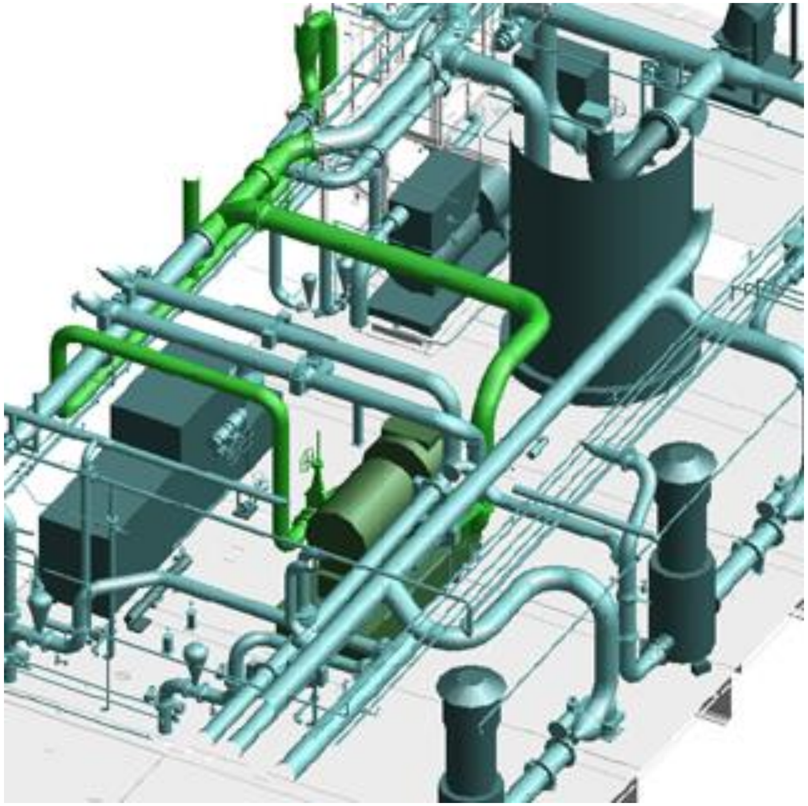


Image from: http://www.akersolutions.com/en/Global-menu/Products-and-Services/Maintenance-modifications-and-operations/Technology-services/Hazard-and-operability-analysis-HAZOP/

Other accident models

- STAMP
  - Systems theoretic accident model and processes (2002)
- Accidents are the result of inadequate control
  - Lack of enforcement of safety constraints in system design and operations
- Captures:
  - Component failures
  - Unsafe interactions among components
  - Design errors
  - Flawed requirements
  - Human error

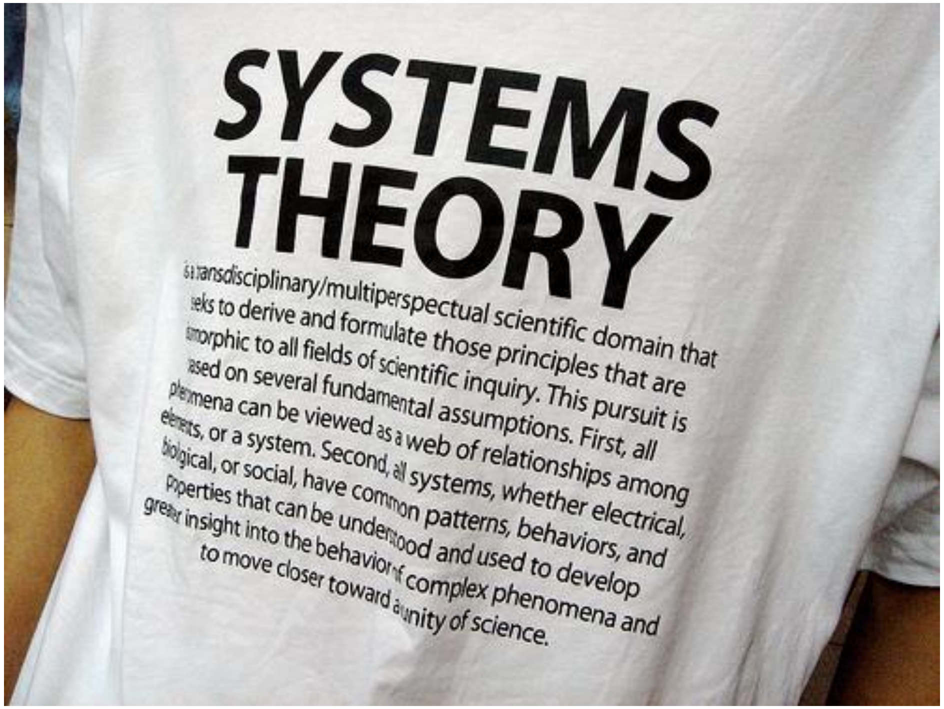

SYSTEMS
THEORY
is a transdisciplinary/multiperspectual scientific domain that
seeks to derive and formulate those principles that are
isomorphic to all fields of scientific inquiry. This pursuit is
based on several fundamental assumptions. First, all
phenomena can be viewed as a web of relationships among
elements, or a system. Second, all systems, whether electrical,
biological, or social, have common patterns, behaviors, and
properties that can be understood and used to develop
greater insight into the behavior of complex phenomena and
to move closer toward a unity of science.

Image from: http://organisationdevelopment.org/five-core-theories-systems-theory-organisation-development/

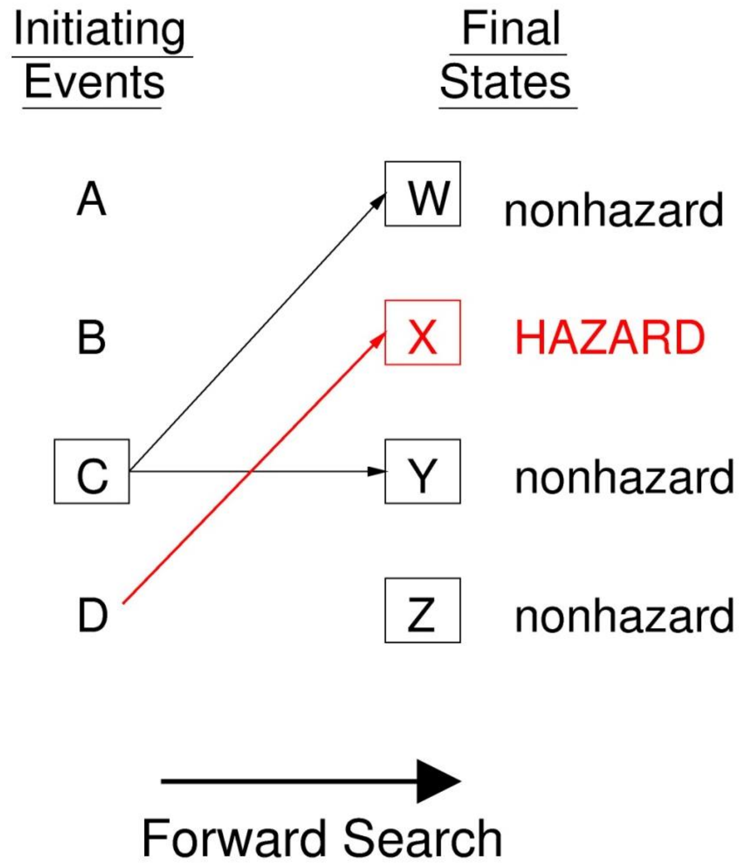
Today’s Agenda

- ✓ Intro to reliability and system risk
- ✓ Overview of analysis techniques
- ➡ Traditional qualitative techniques
  - Failure Modes and Effects Analysis
  - Fault Tree Analysis
  - Event Tree Analysis
  - HAZOP
- Traditional quantitative techniques
  - Quant. Fault Tree Analysis
  - FMECA
  - Quant. ETA

Traditional Qualitative Methods

FMEA: Failure Modes and Effects Analysis

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

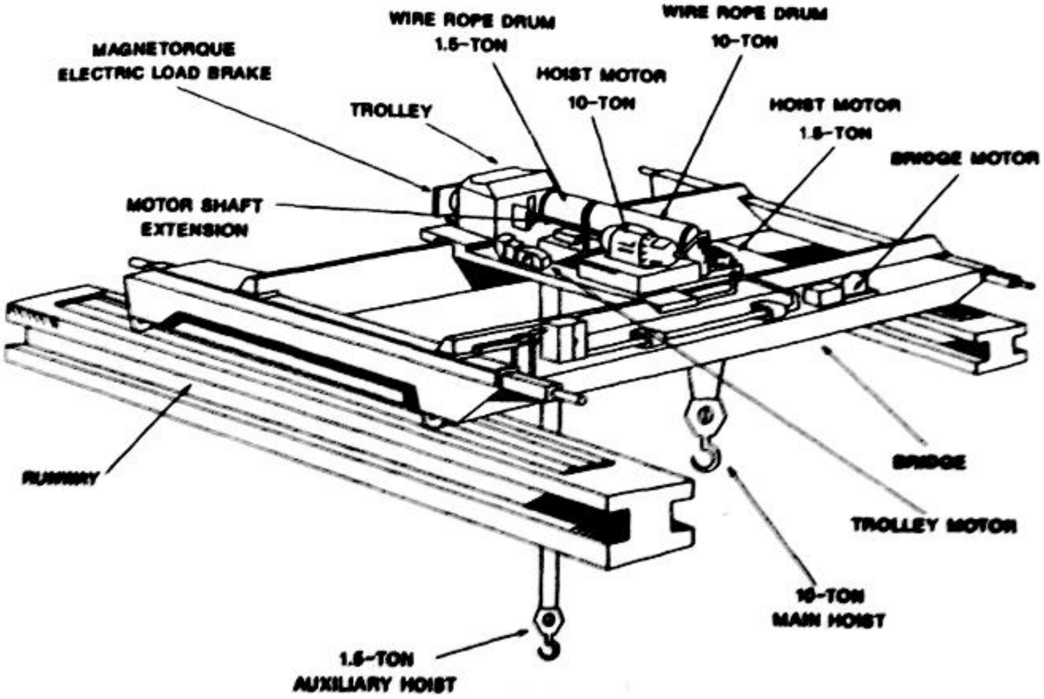


General FMEA Process

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

FMEA worksheet

Example: Bridge crane system



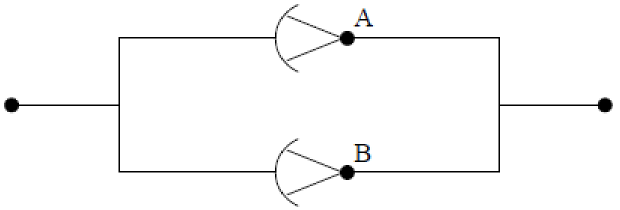
Failure Mode and Effect Analysis

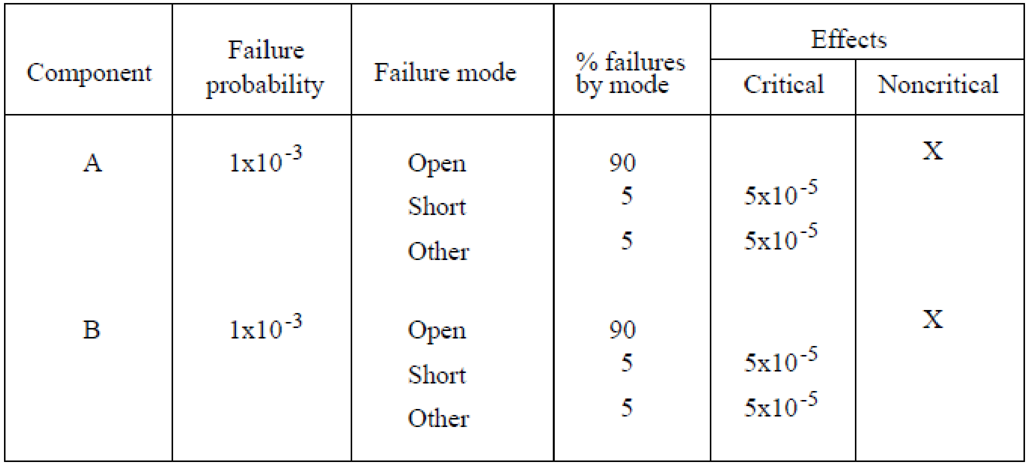
Program:_________ System:_________ Facility:________
Engineer:_________ Date:___________ Sheet:_________

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.

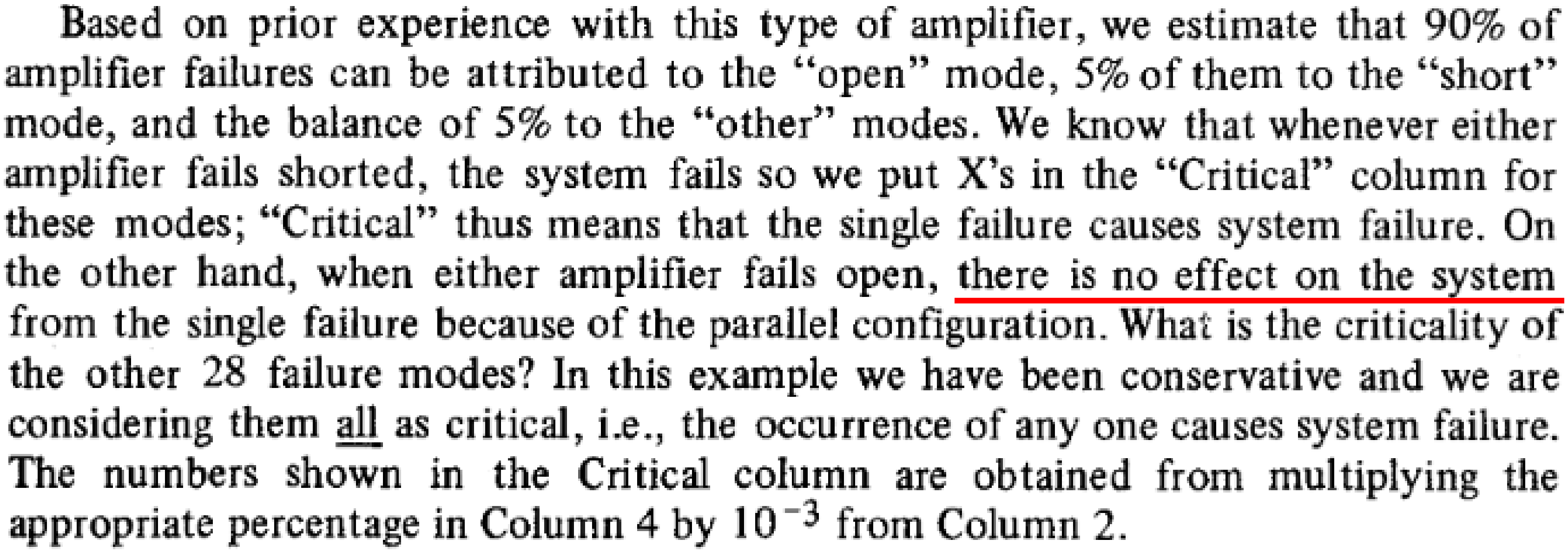
*FMEA example adapted from (Vincoli, 2006)

FMECA: A Forward Search Technique





Component	Failure probability	Failure mode	% failures by mode	Effects	
				Critical	Noncritical
A	$1\text{x}10^{-3}$	Open	90		X
		Short	5	$5\text{x}10^{-5}$	
		Other	5	$5\text{x}10^{-5}$	
B	$1\text{x}10^{-3}$	Open	90		X
		Short	5	$5\text{x}10^{-5}$	
		Other	5	$5\text{x}10^{-5}$	



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

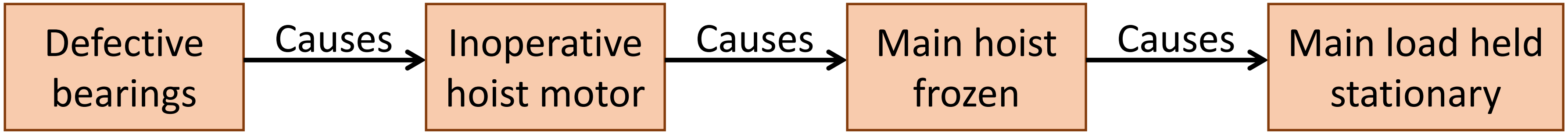
FMEA method:

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.

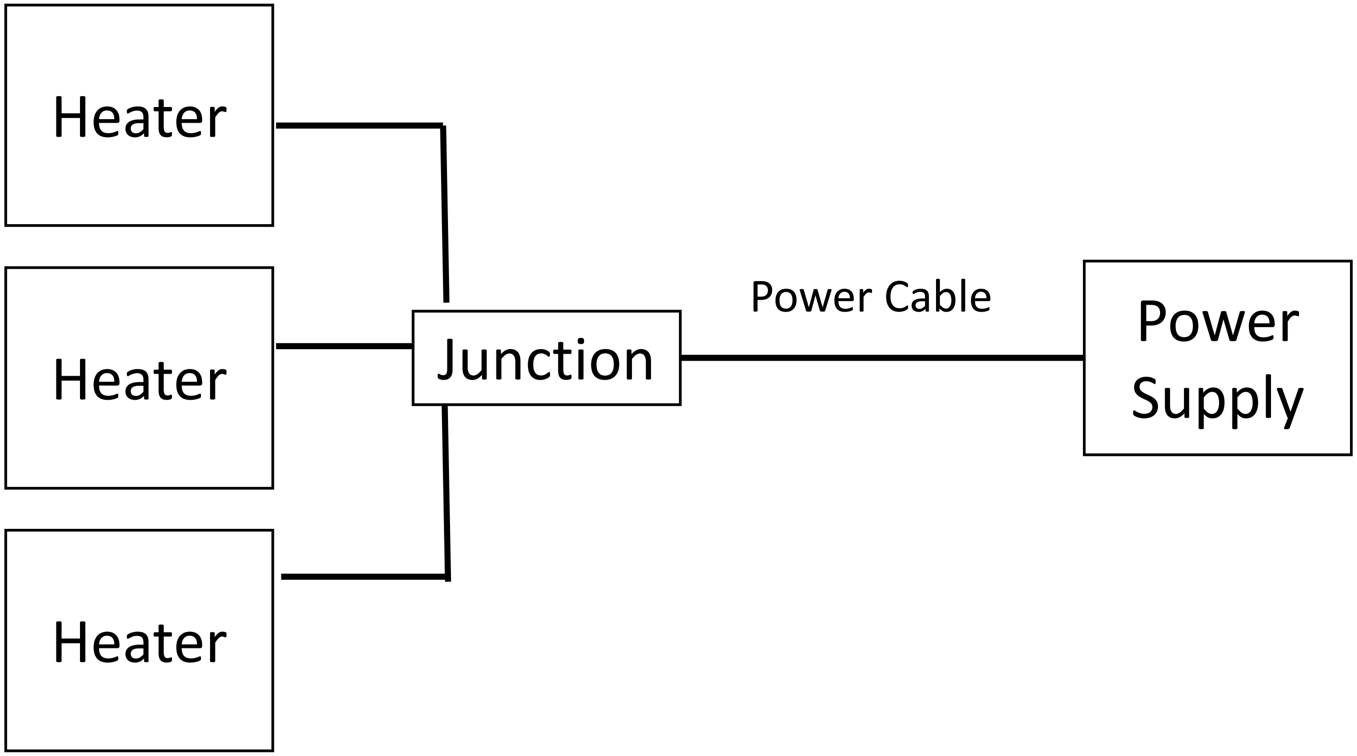
Accident model: Chain-of-events



Defective bearings → Causes → Inoperative hoist motor → Causes → Main hoist frozen → Causes → Main load held stationary

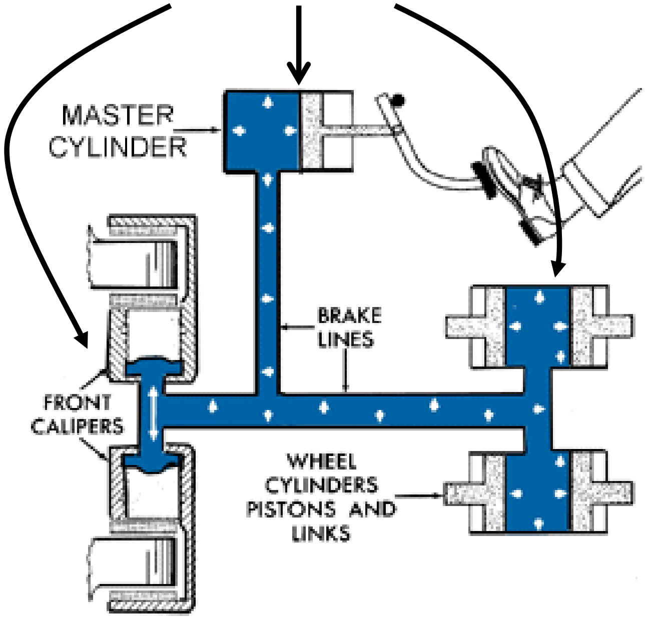
*FMEA example adapted from (Vincoli, 2006)

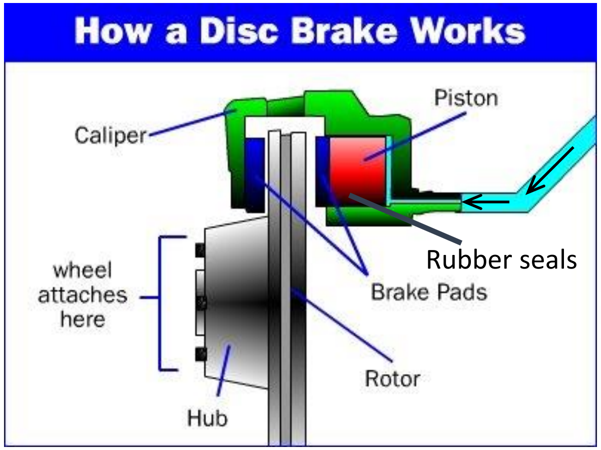
Real example:
LHC ATLAS Return Heaters



FMEA Exercise Automotive brakes

Rubber Seals





Rubber seals

System components

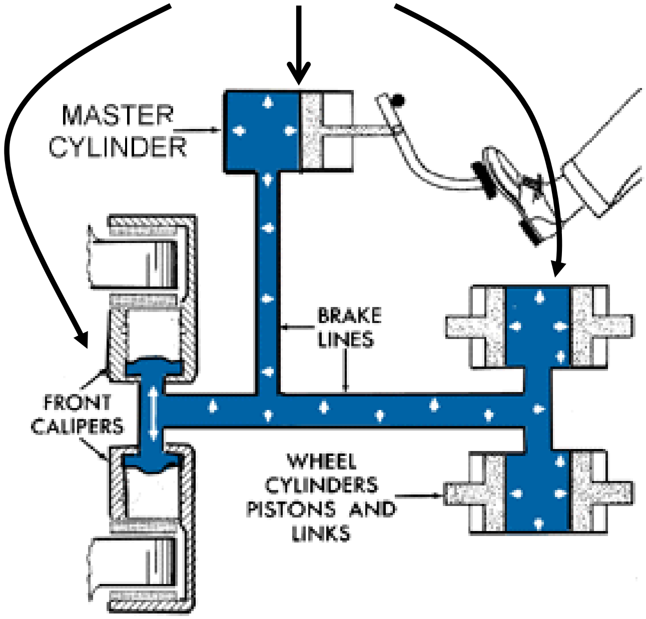
- Brake pedal
- Brake lines
- Rubber seals
- Master cylinder
- Brake pads

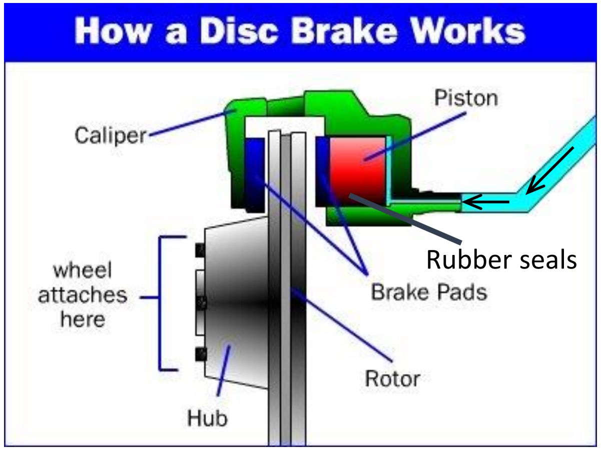
FMEA worksheet columns

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

FMEA Exercise
Automotive brakes

Rubber Seals





System components

- Brake pedal
- Brake pads

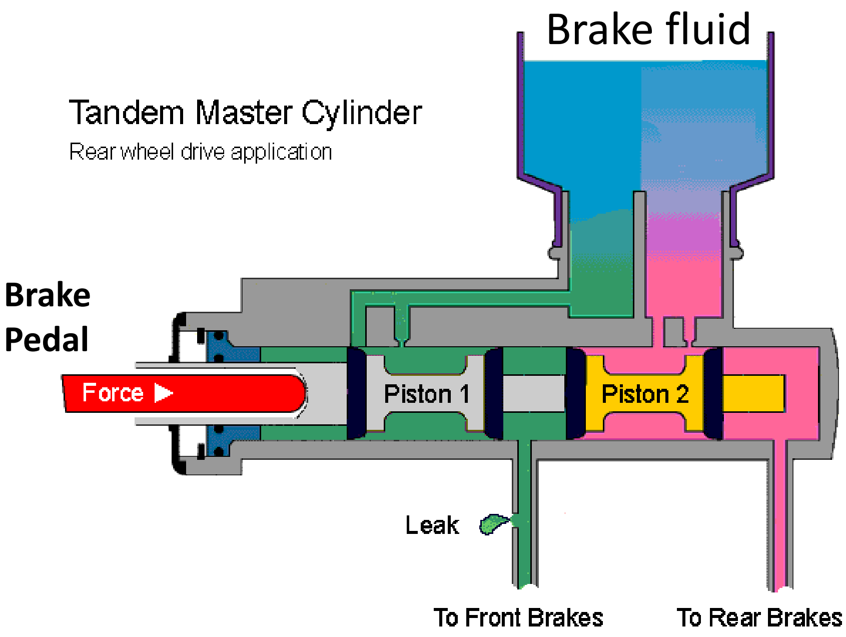
FMEA worksheet columns

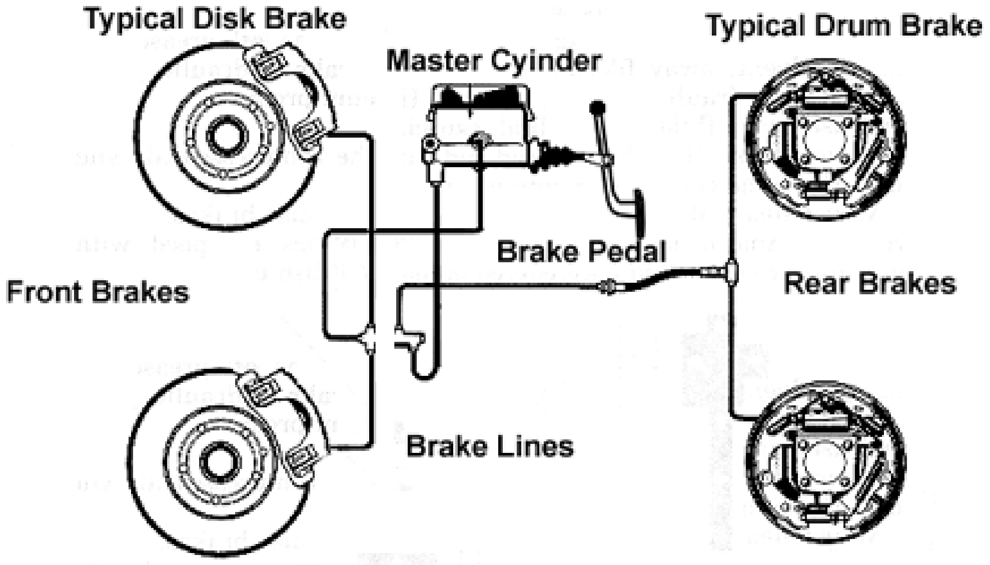
– Component

– Failure effect (system)

How would you make this system safe?
The type of analysis affects the solutions you identify

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

Definitions

Reliability

- Probability that a component or system will perform its specified function (for a prescribed time under stated conditions)

Failure

- Inability of a component to perform its specified function (for a prescribed time under stated conditions)

Risk

- Threat of damage, injury, liability, loss, or any other negative occurrence that may be avoided through preemptive action.

Safety

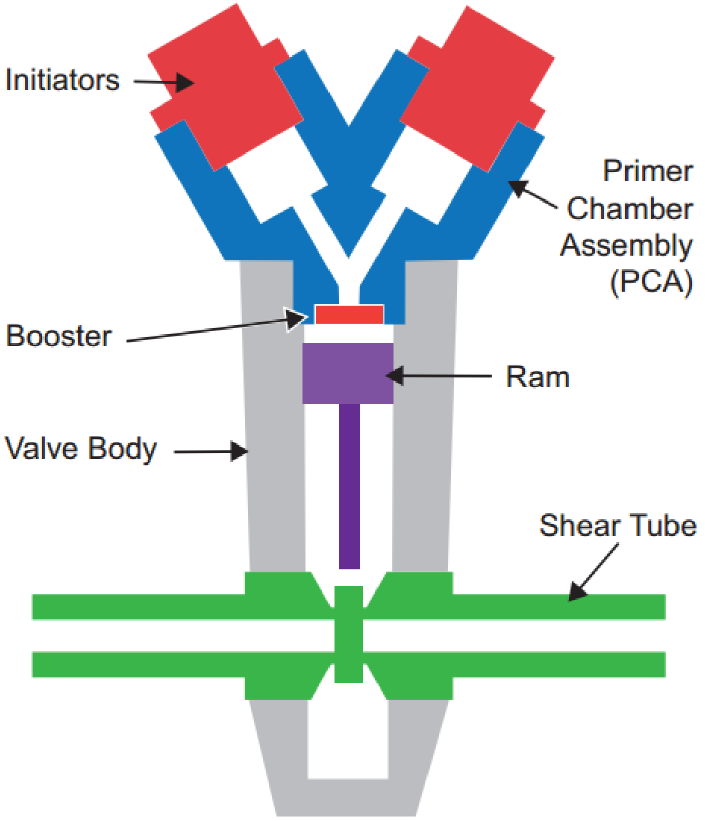
- Freedom from undesired losses (e.g. loss of life, loss of mission, environmental damage, customer satisfaction, etc.)

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
  - Can limit how early analysis can be applied
- Works best on hardware/mechanical components
  - **Human** operators? (Driver? Pilot?)
  - **Software** 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

New failure modes and redundancy

- Pyrovalves with dual initiators
- “No-fire” failures investigated by NASA Engineering and Safety Center
- Failures occurred when redundant pyrovalves triggered at same time
  - More reliable to trigger a single valve at a time



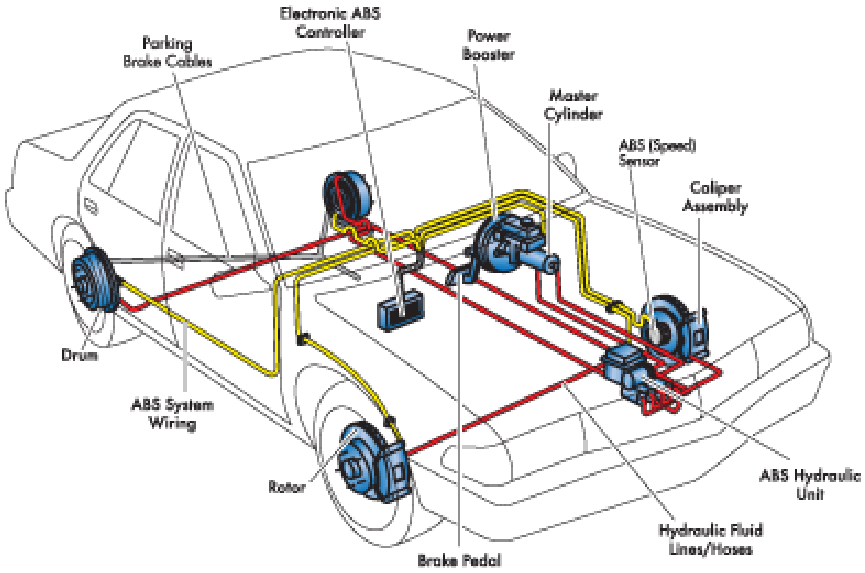
A normally closed pyrovalve

Safety vs. Reliability

- Common assumption:

  Safety = reliability

- How to achieve system goals?
  - Make everything more reliable!



- Making car brakes achieve system goals
  - – Make every component reliable
  - – Include redundant components

Is this a good assumption?

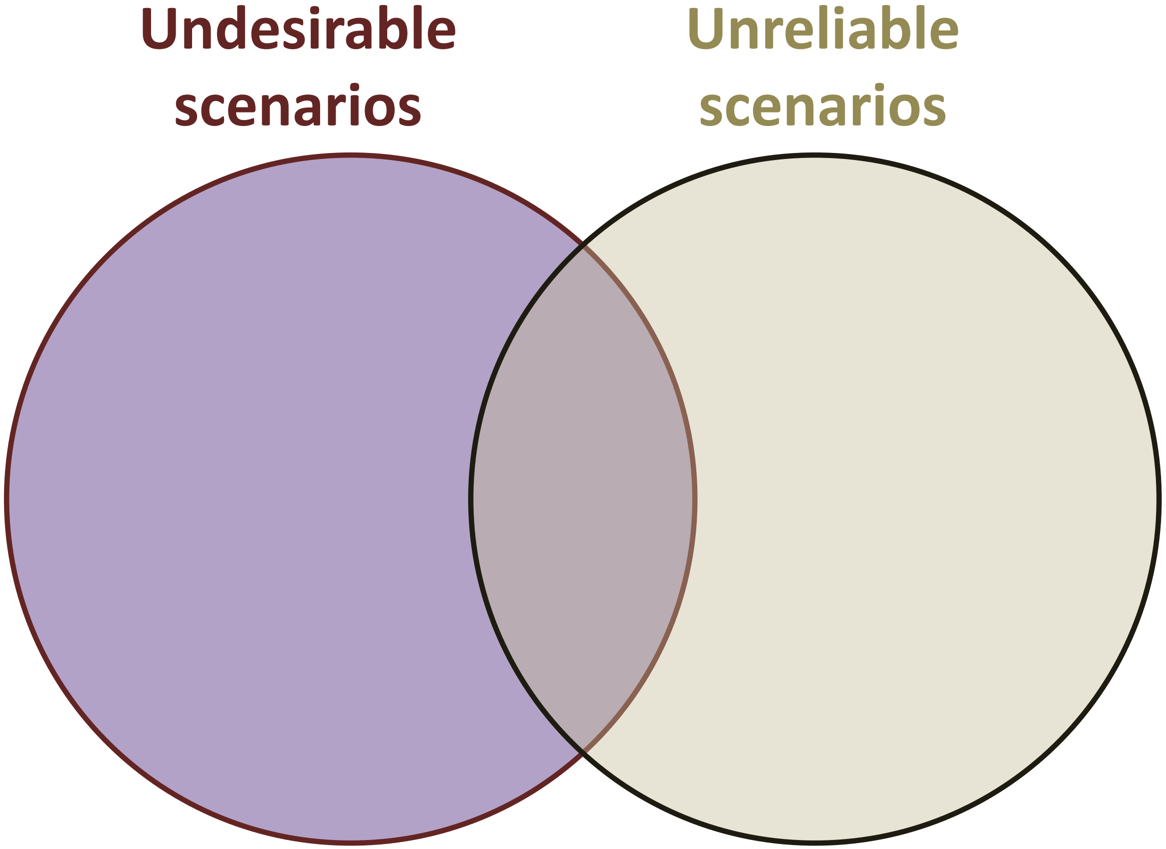
*Image from midas.com

Safety vs. reliability

Reliability ←→ Failures } Component property

Safety ←→ Incidents } System property

Safety vs. Reliability



Undesirable scenarios

Unreliable scenarios

Safe ≠ Reliable

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

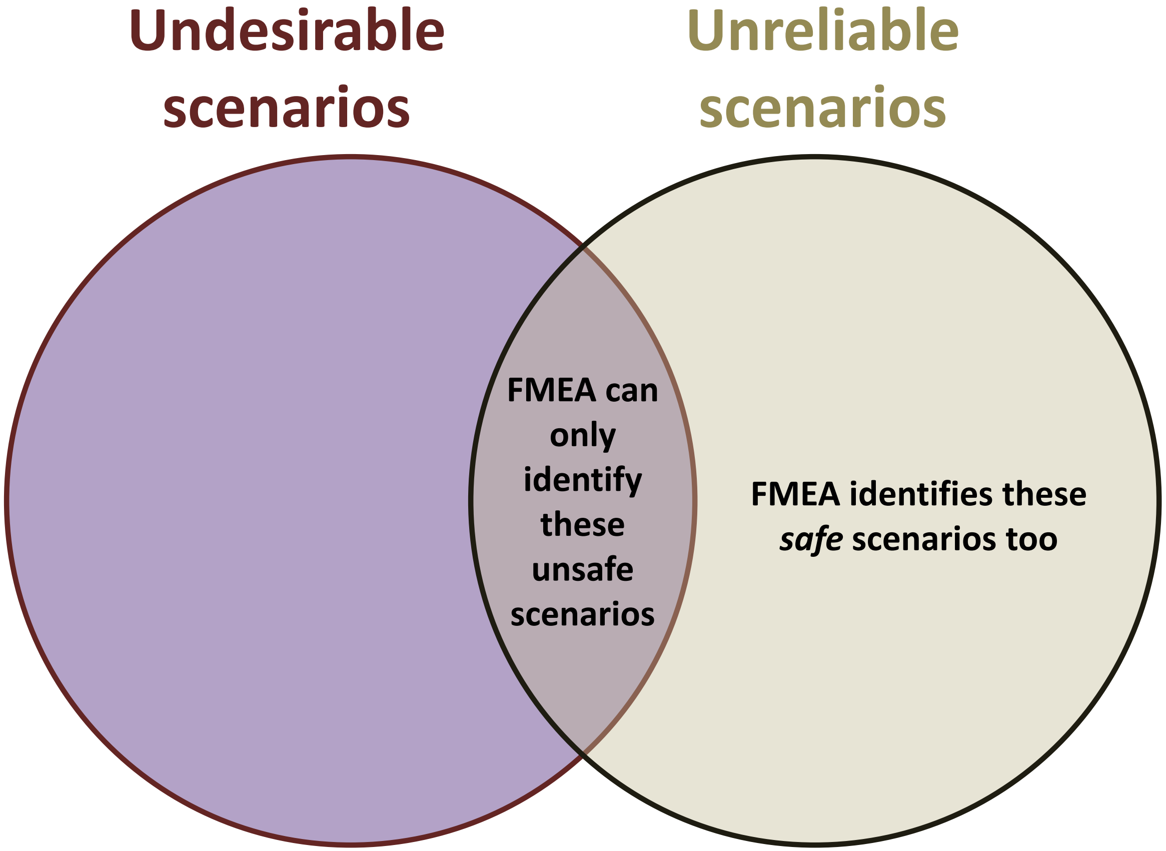
	Safe	**Unsafe**
Reliable	•Typical commercial flight	
Unreliable		•Aircraft engine fails in flight

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

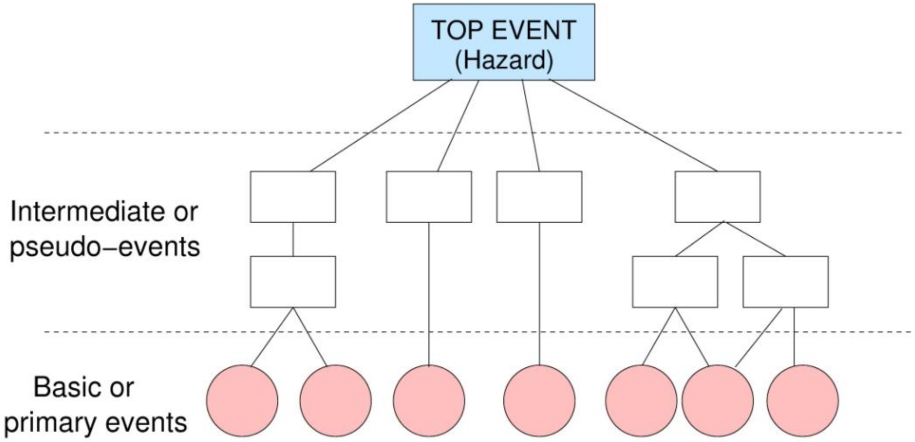

Undesirable scenarios
Unreliable scenarios
FMEA can only identify these unsafe scenarios
FMEA identifies these *safe* scenarios too

- FMEA is a *reliability* technique
  - Explains the inefficiency
- FMEA sometimes used to prevent undesirable outcomes
  - Can establish the end effects of failures

FTA
Fault Tree Analysis

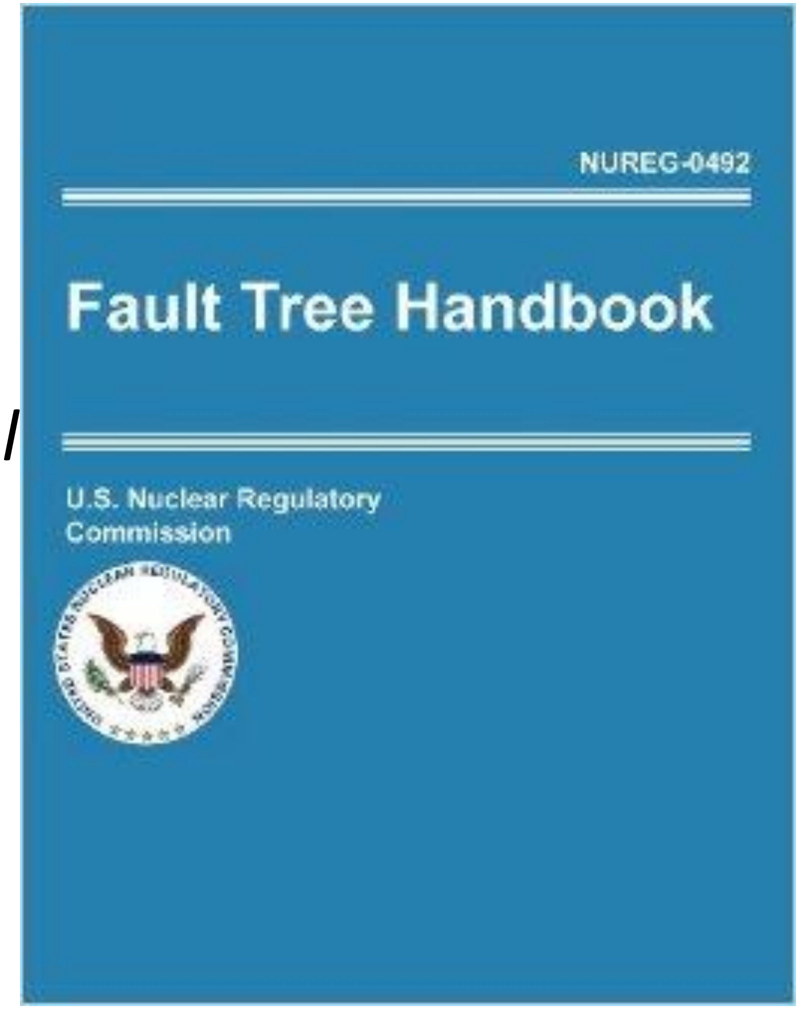
FTA: Fault Tree Analysis

- 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



FTA Process

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



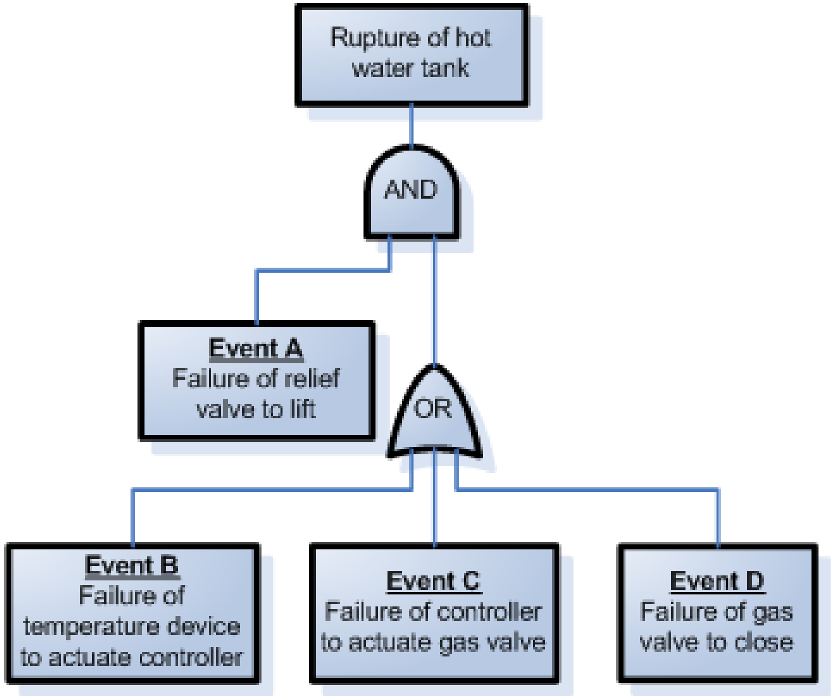
NUREG-0492

Fault Tree Handbook

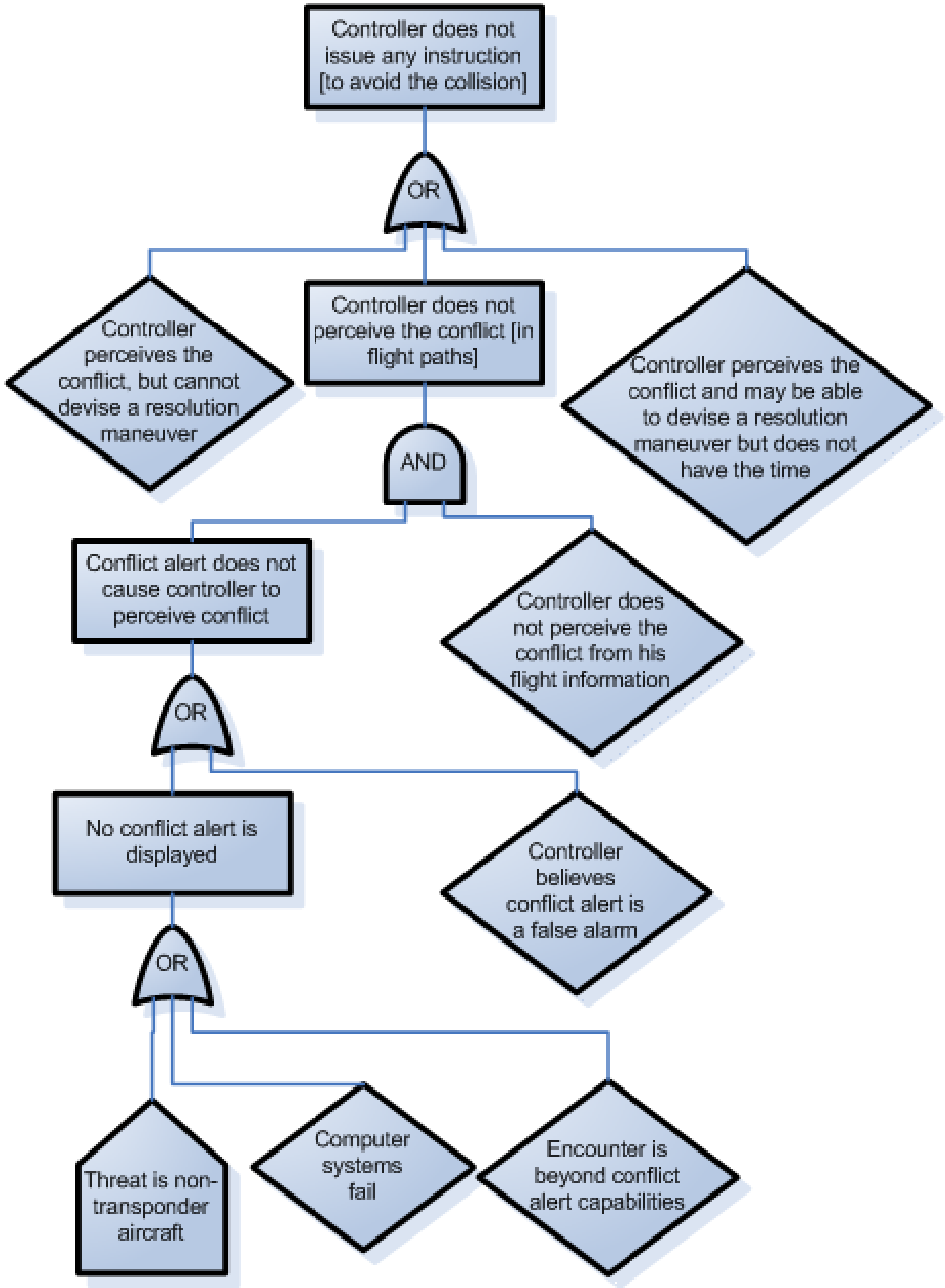
U.S. Nuclear Regulatory
Commission

Vesely

Fault tree examples

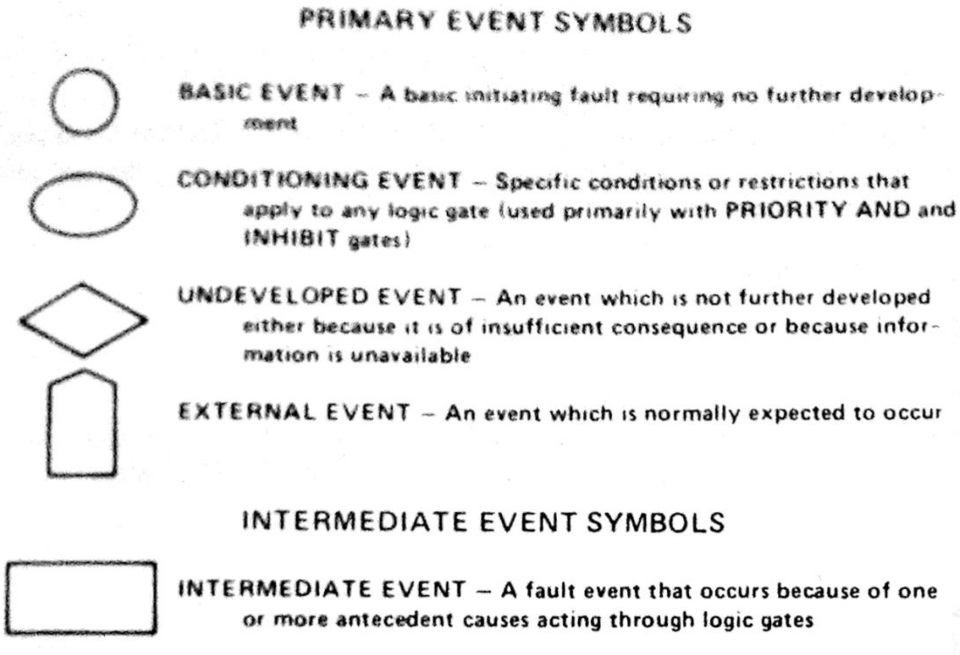

Rupture of hot water tank
AND
Event A
Failure of relief valve to lift
OR
Event B
Failure of temperature device to actuate controller
Event C
Failure of controller to actuate gas valve
Event D
Failure of gas valve to close

Example from original 1961 Bell Labs study


Controller does not issue any instruction [to avoid the collision]
OR
Controller perceives the conflict, but cannot devise a resolution maneuver
Controller does not perceive the conflict [in flight paths]
Controller perceives the conflict and may be able to devise a resolution maneuver but does not have the time
AND
Conflict alert does not cause controller to perceive conflict
Controller does not perceive the conflict from his flight information
OR
No conflict alert is displayed
Controller believes conflict alert is a false alarm
OR
Threat is non-transponder aircraft
Computer systems fail
Encounter is beyond conflict alert capabilities

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

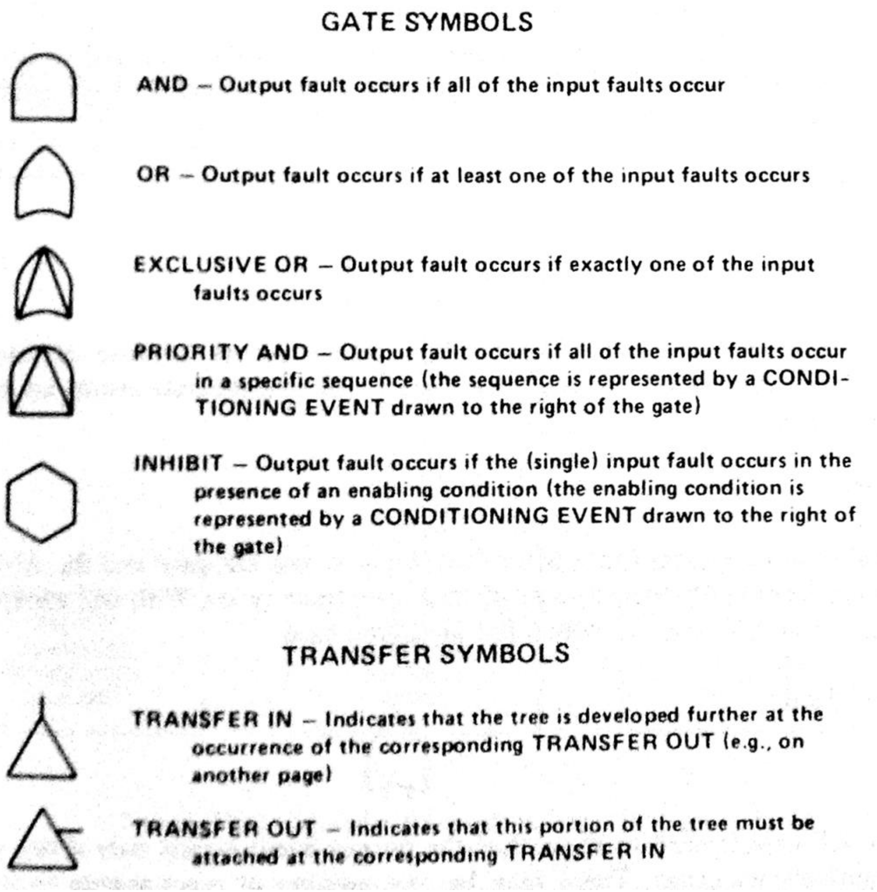
CONDITIONING EVENT – Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)

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)

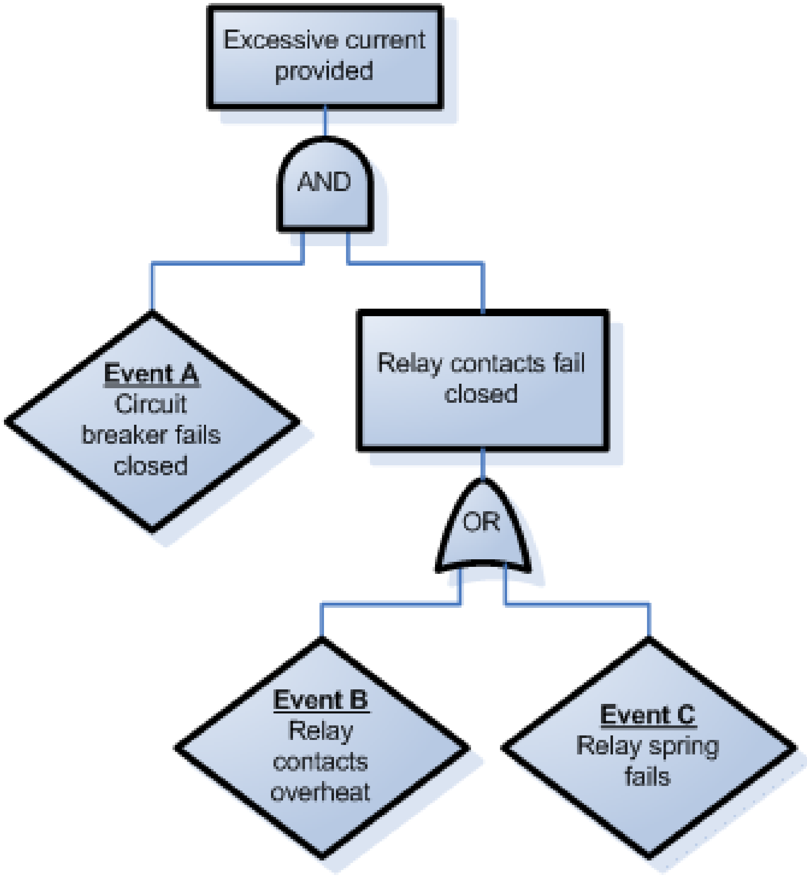
TRANSFER OUT – Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

From NUREG-0492 (Vesely, 1981)

Fault Tree cut-sets

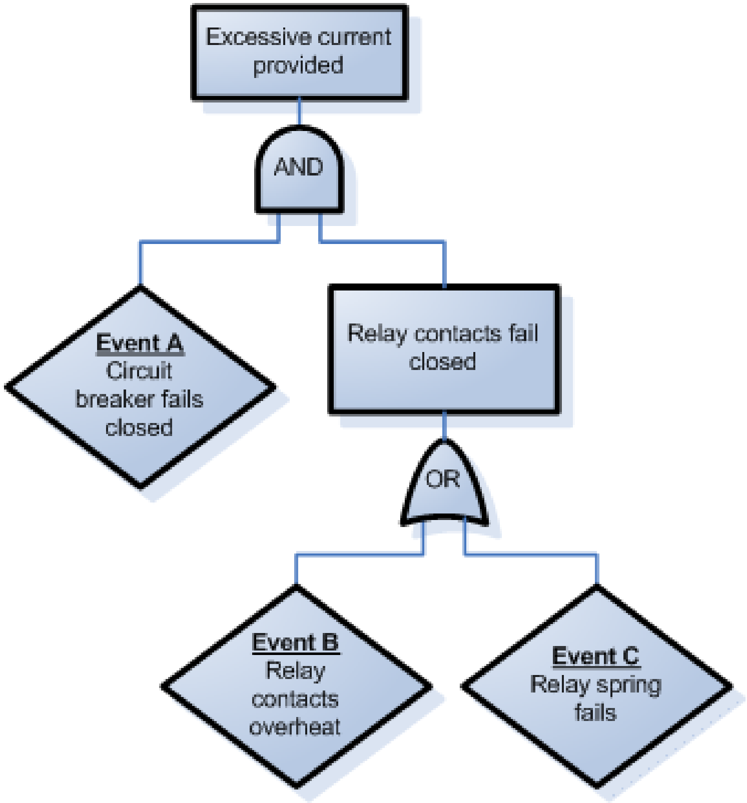
- *Cut-set*: combination of basic events (leaf nodes) sufficient to cause the top-level event
  - Ex: (A and B and C)

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

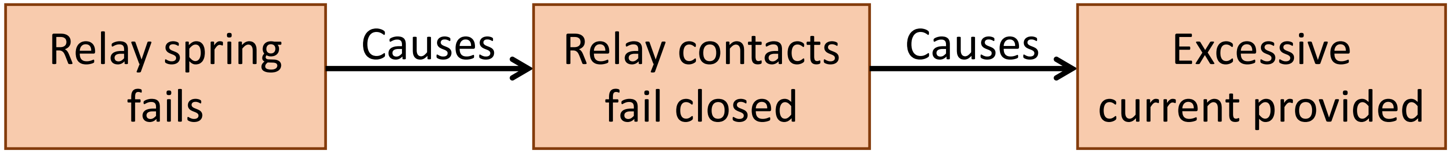

Excessive current provided
AND
Event A
Circuit breaker fails closed
Relay contacts fail closed
OR
Event B
Relay contacts overheat
Event C
Relay spring fails

FTA uses an accident model

Fault Tree:


Excessive current provided
AND
Event A
Circuit breaker fails closed
Relay contacts fail closed
OR
Event B
Relay contacts overheat
Event C
Relay spring fails

Accident model: Chain-of-failure-events



Relay spring fails

Causes

Relay contacts fail closed

Causes

Excessive current provided

Fault Tree Exercise

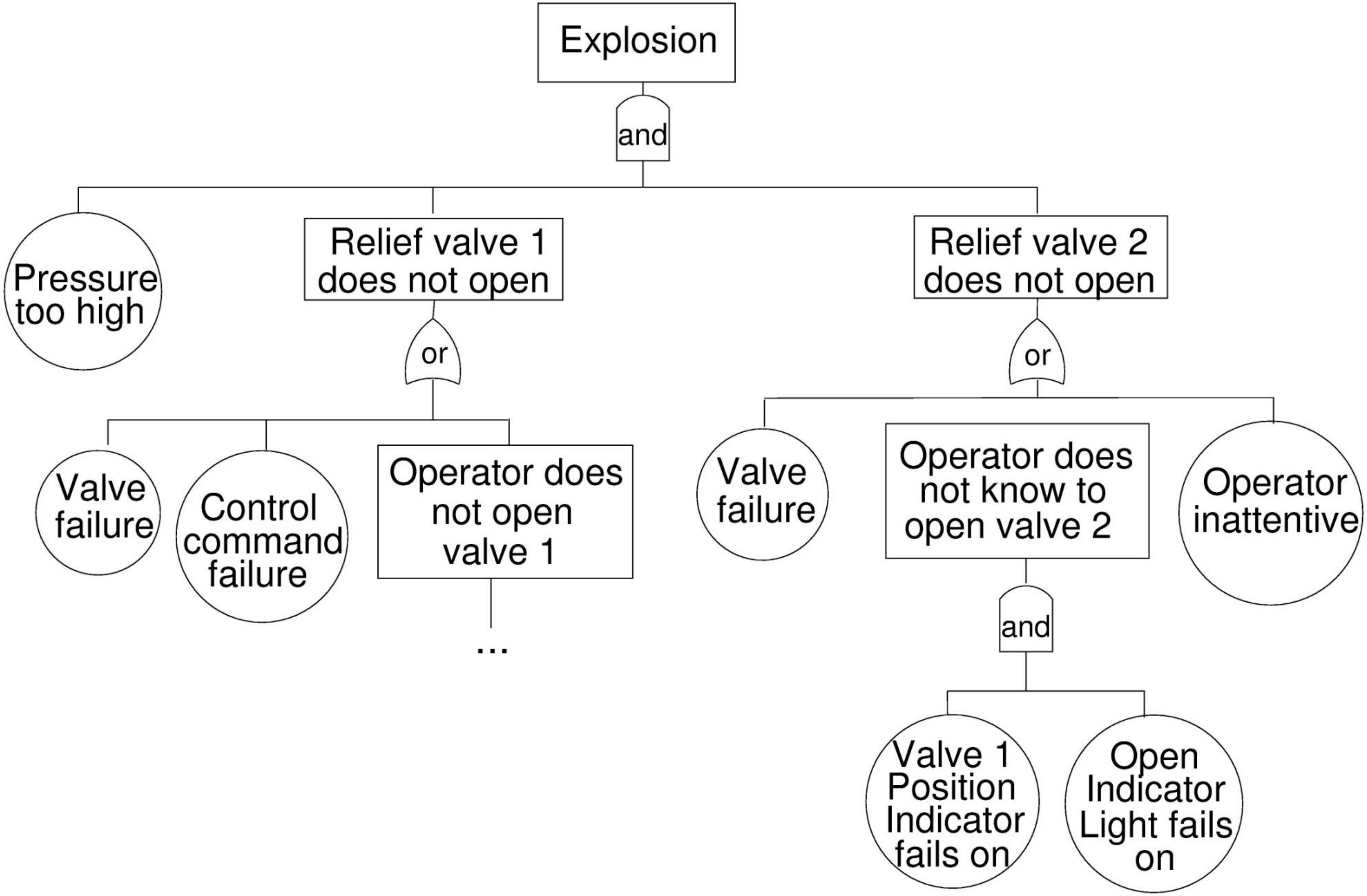
- **Hazard**: Toxic chemical released
- **Design**:

Tank 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 Exercise


Explosion
and
Pressure too high
Relief valve 1 does not open
or
Valve failure
Control command failure
Operator does not open valve 1
...
Relief valve 2 does not open
or
Valve failure
Operator does not know to open valve 2
and
Valve 1 Position Indicator fails on
Open Indicator Light fails on
Operator inattentive

Example of an actual incident

- **System Design**: Same
- **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.

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 had 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.
  - After accident, recovery from 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 fail to operate on landing.

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

Warsaw Accident

- 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

2012 accident

- Tu-204 in Moscow
- Red Wings Airlines Flight 9268

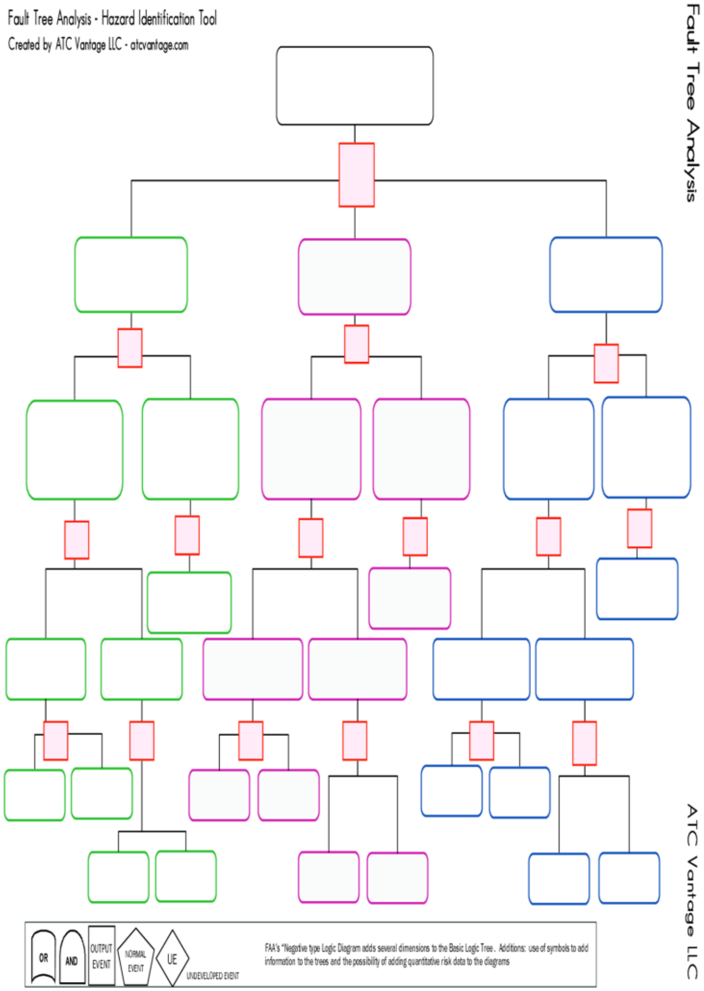
- The soft 1.12g touchdown made runway contact a little later than usual. With the crosswind, this meant weight-on-wheels switches did not activate and the thrust-reverse system could not deploy, owing to safety logic which prevents activation while the aircraft is airborne.
- With limited runway space, the crew quickly engaged high engine power to stop quicker. Instead this accelerated the Tu-204 forwards eventually colliding with a highway embankment.

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**

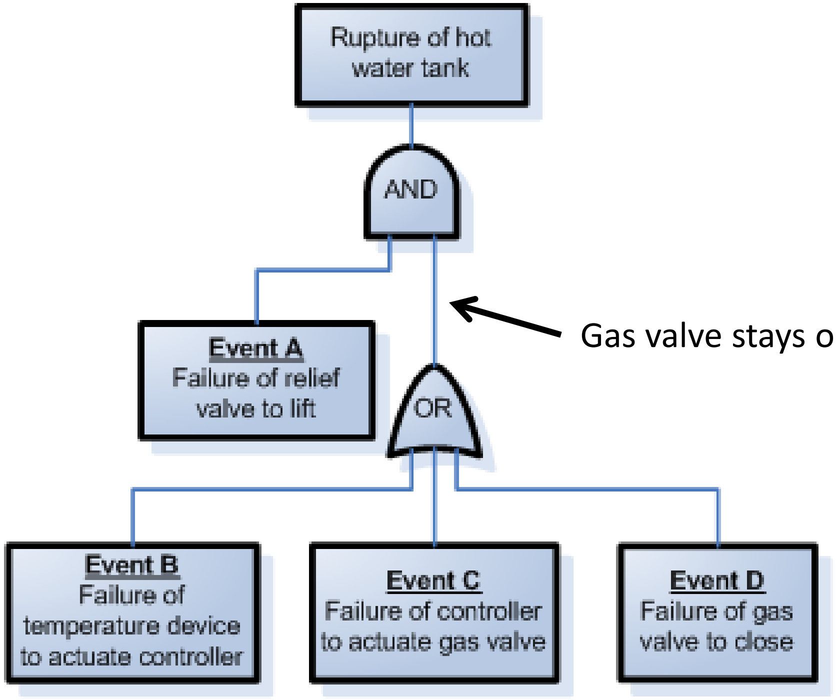

Fault Tree Analysis - Hazard Identification Tool
Created by ATC Vantage LLC - atcvantage.com
Fault Tree Analysis
ATC Vantage LLC
OR
AND
OUTPUT EVENT
NORMAL EVENT
UE
UNDEVELOPED EVENT

FAA's *Negative type Logic Diagram adds several dimensions to the Basic Logic Tree. Additions: use of symbols to add information to the trees and the possibility of adding quantitative risk data to the diagrams

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 examples



Rupture of hot water tank

AND

Event A Failure of relief valve to lift

OR

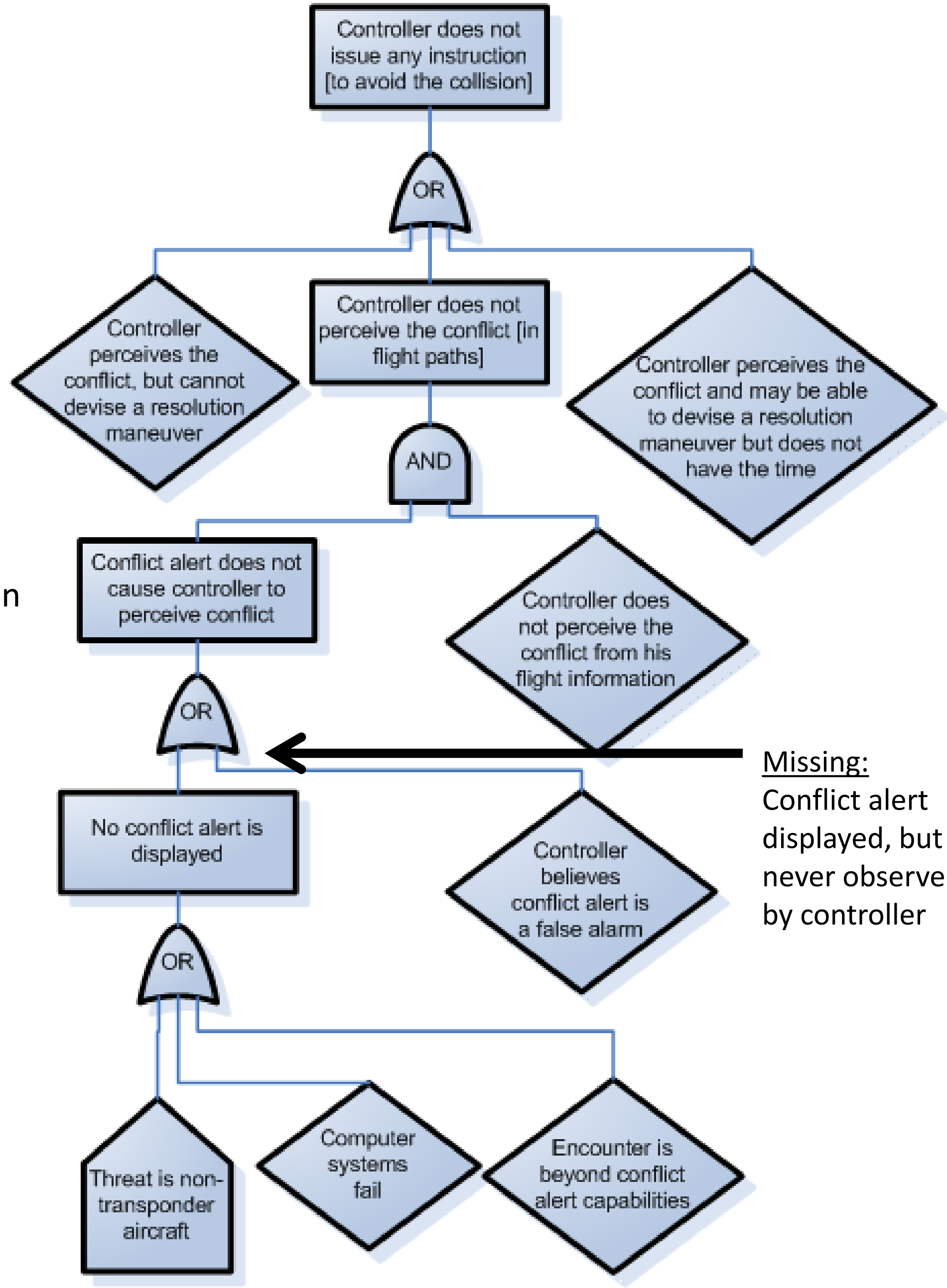
Event B Failure of temperature device to actuate controller

Event C Failure of controller to actuate gas valve

Event D Failure of gas valve to close

Gas valve stays open

Example from original 1961 Bell Labs study



Controller does not issue any instruction [to avoid the collision]

OR

Controller perceives the conflict, but cannot devise a resolution maneuver

Controller does not perceive the conflict [in flight paths]

Controller perceives the conflict and may be able to devise a resolution maneuver but does not have the time

AND

Conflict alert does not cause controller to perceive conflict

Controller does not perceive the conflict from his flight information

OR

No conflict alert is displayed

Controller believes conflict alert is a false alarm

OR

Threat is non-transponder aircraft

Computer systems fail

Encounter is beyond conflict alert capabilities

Missing:
Conflict alert displayed, but never observed by controller

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

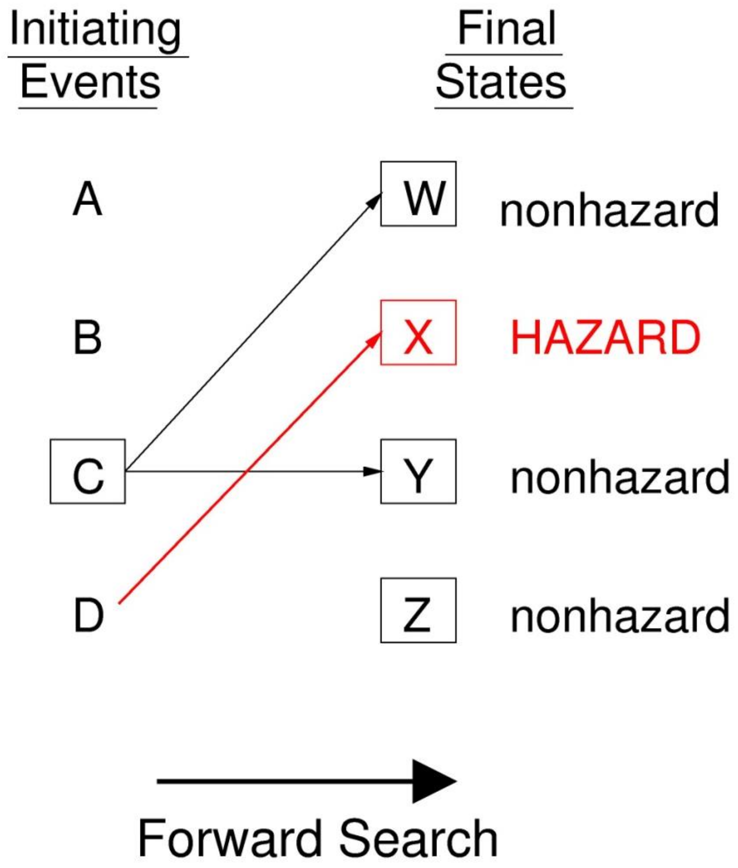
Vesely FTA Handbook

- Considered by many to be the textbook definition of fault trees
- Read the excerpt (including gate definitions) on Stellar for more information

Event Tree Analysis

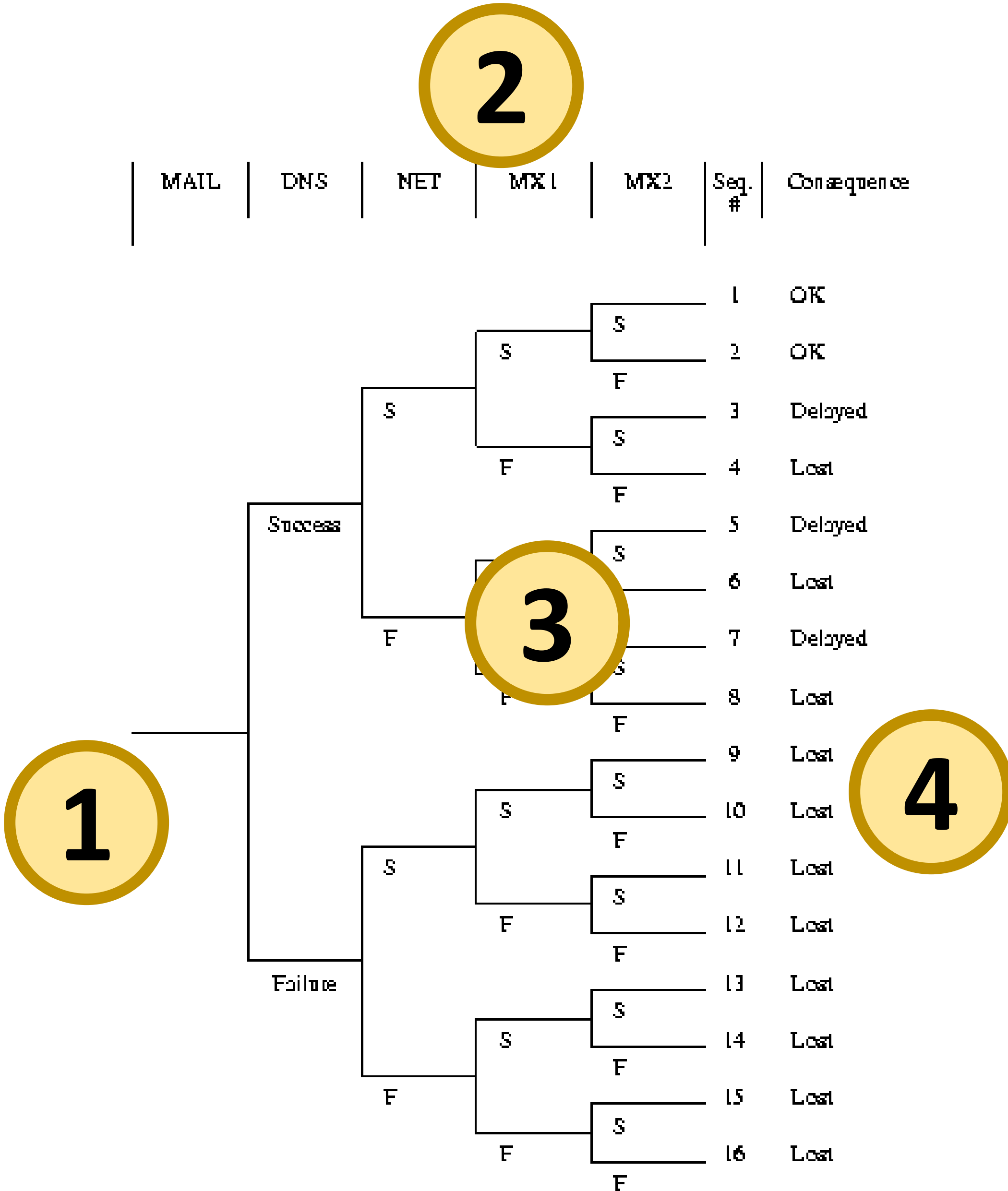
Event Tree Analysis

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

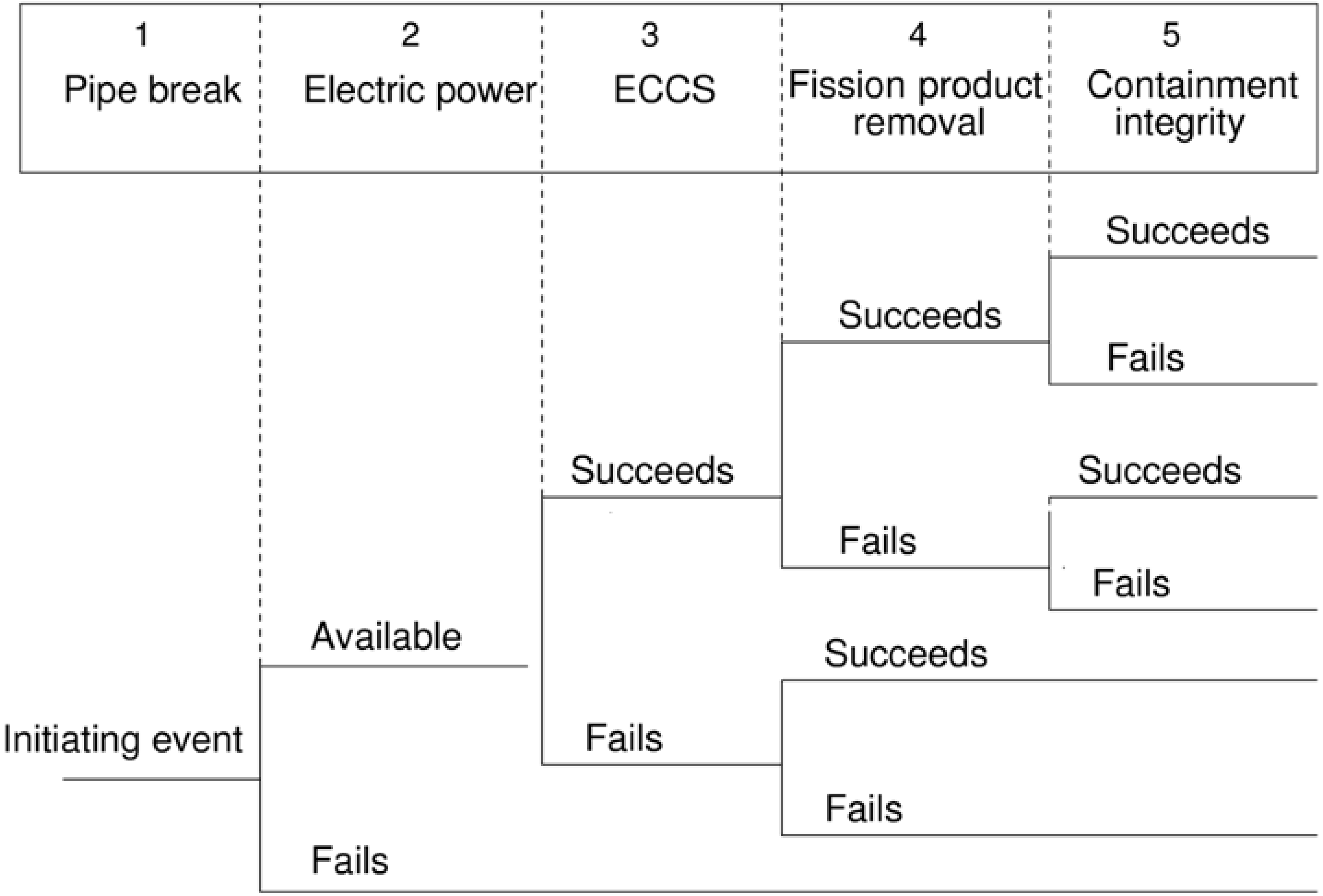


Event Tree Analysis: Process

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



Event Tree Example



No accident

Small release

No release

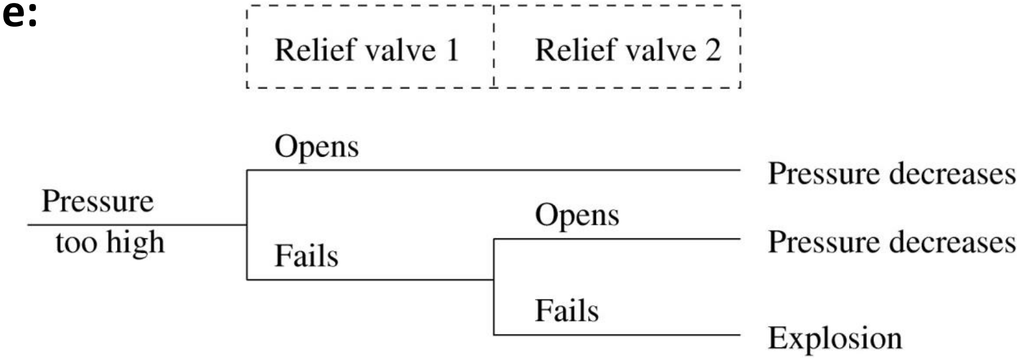
Moderate release

No release

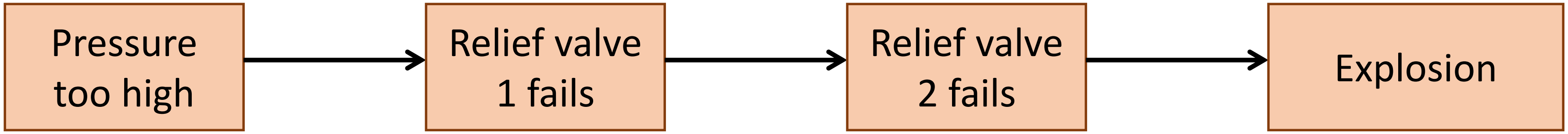
Major release

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

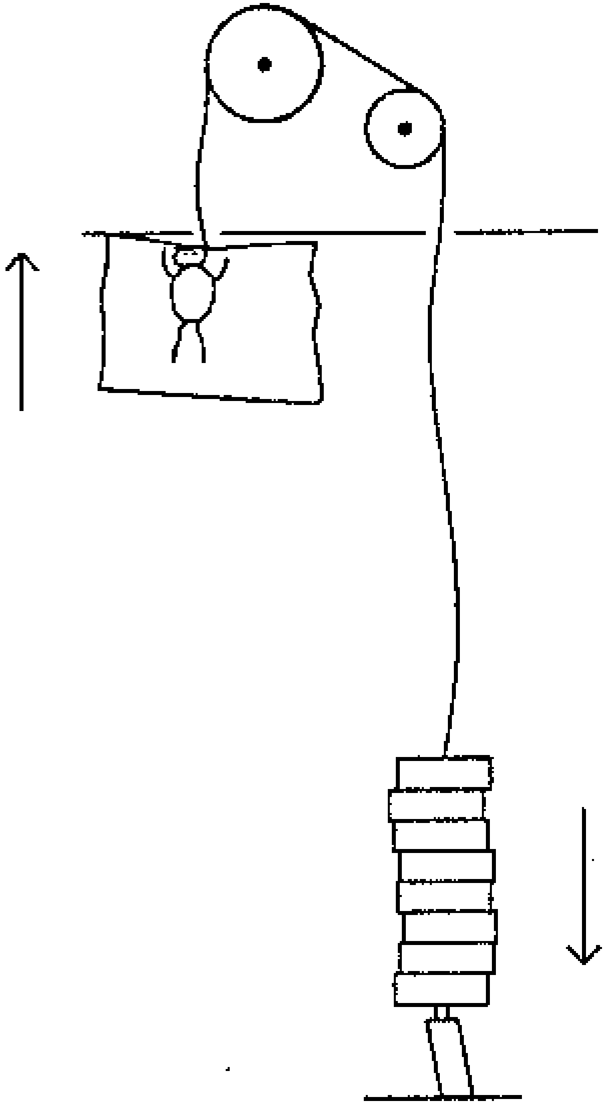
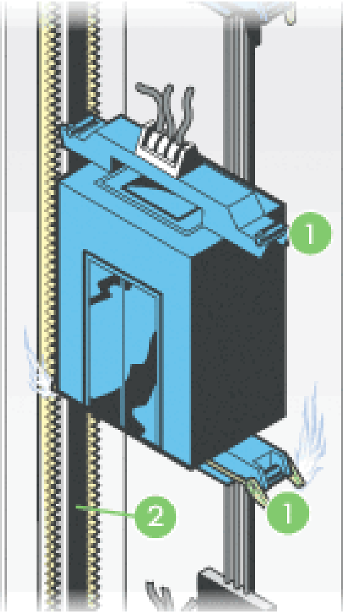


Image from official U.S. Dept of Labor, Mine Safety and Health Administration paper: http://www.msha.gov/S&HINFO/TECHRPT/HOIST/PAPER4.HTM

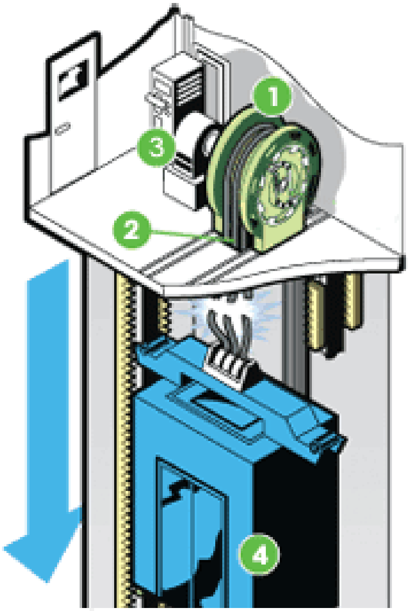
Event Tree Analysis: Elevator



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**.

©2004 HowStuffWorks

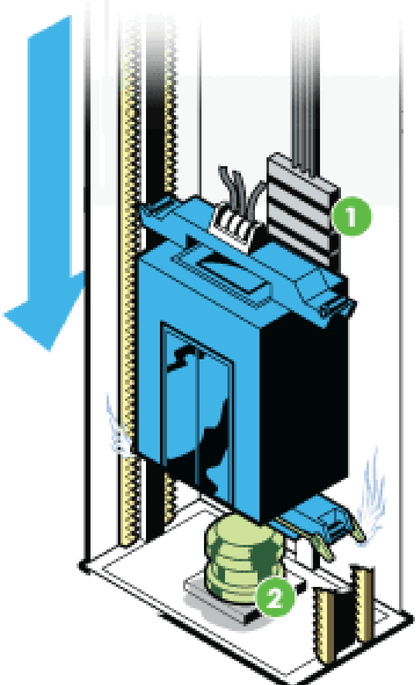


1. Steel cables bolted to the the car loop over a **sheave.**

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.



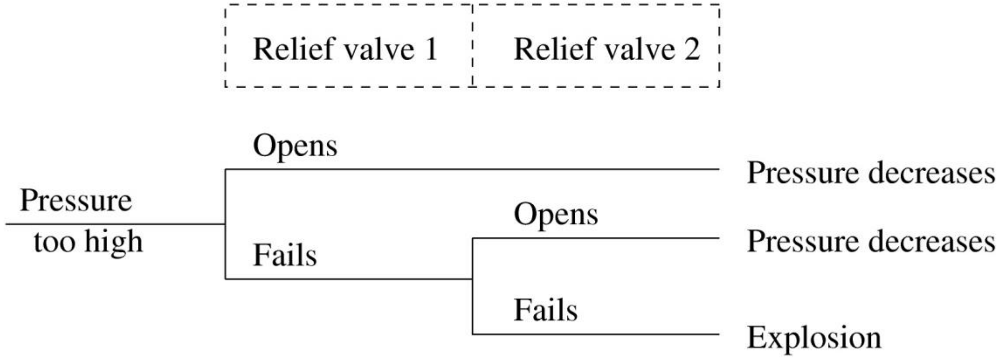
1. The cables that lift the car are also connected to a **counterweight,** which hangs down on the other side of the sheave.

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.

Exercise

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

Event Trees
vs.
Fault Trees

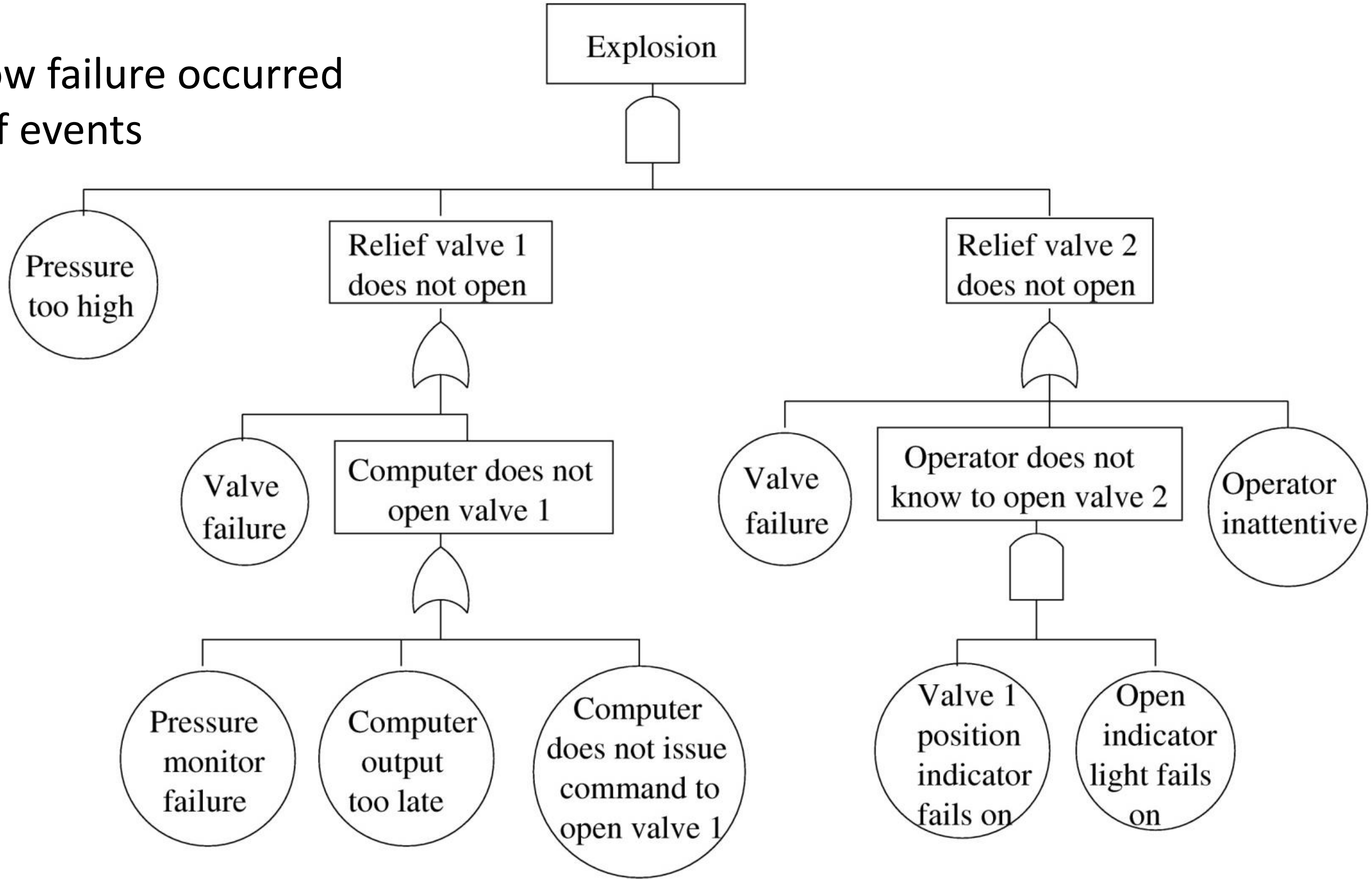


Event Tree

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

Fault Tree

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


Explosion
Pressure too high
Relief valve 1 does not open
Relief valve 2 does not open
Valve failure
Computer does not open valve 1
Valve failure
Operator does not know to open valve 2
Operator inattentive
Pressure monitor failure
Computer output too late
Computer does not issue command to open valve 1
Valve 1 position indicator fails on
Open indicator light fails on

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 small set of initiating events that will produce all important incident 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

Accident model:

- ~~Accidents caused by chain of failure events~~ (finally!)
- Accidents caused by deviations from design/operating intentions

HAZOP

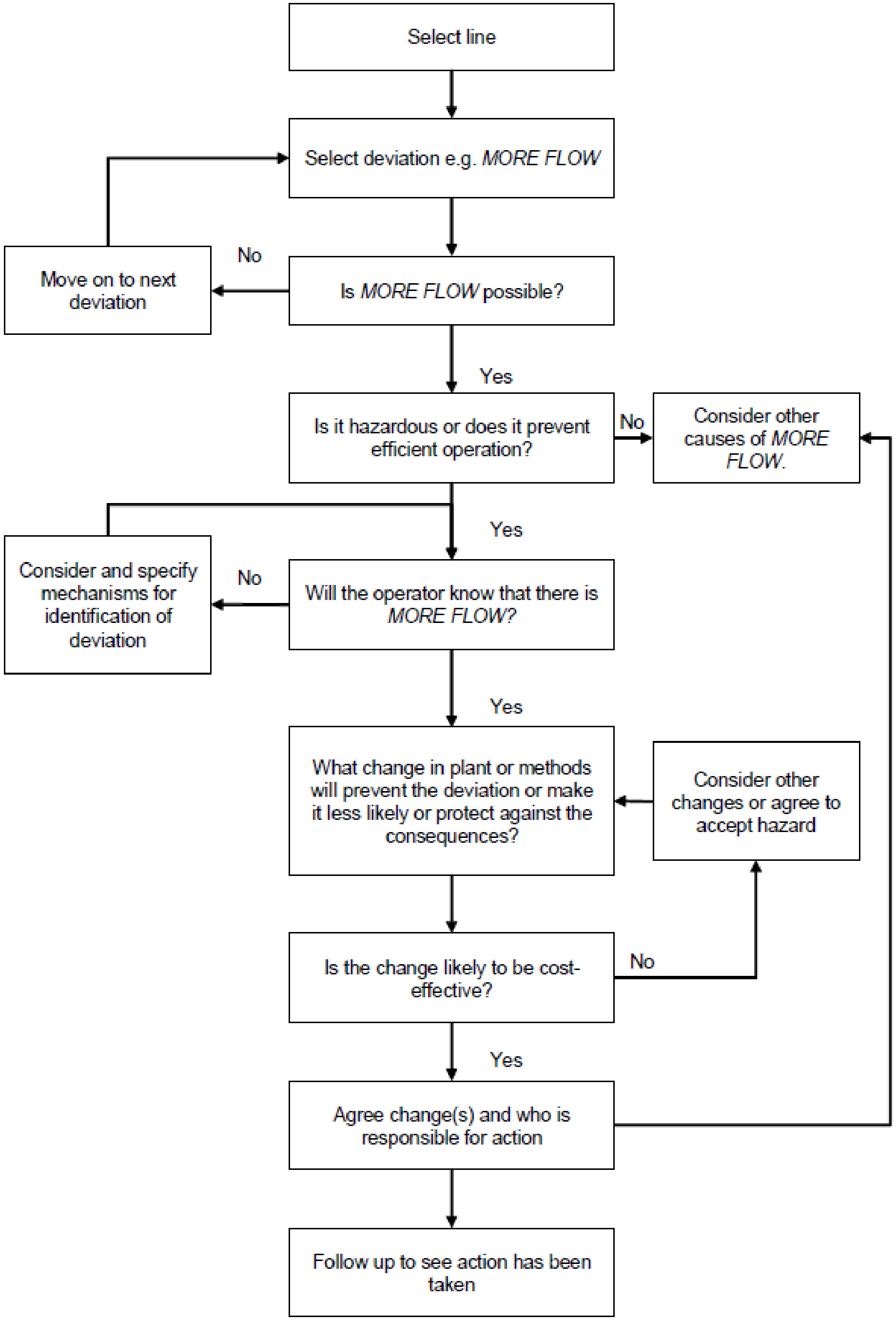
- Guidewords applied to variables of interest
  - E.g. flow, temperature, pressure, tank levels, etc.
- Team considers potential causes and effects

- **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)



Select line

Select deviation e.g. *MORE FLOW*

Is *MORE FLOW* possible?

No

Move on to next deviation

Yes

Is it hazardous or does it prevent efficient operation?

No

Consider other causes of *MORE FLOW*.

Yes

Will the operator know that there is *MORE FLOW?*

No

Consider and specify mechanisms for identification of deviation

Yes

What change in plant or methods will prevent the deviation or make it less likely or protect against the consequences?

Consider other changes or agree to accept hazard

Is the change likely to be cost-effective?

No

Yes

Agree change(s) and who is responsible for action

Follow up to see action has been taken

HAZOP Strengths

- **Easy** to apply
  - A simple method that can uncover complex incidents
- 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

Discussion of Overall Limitations/Comparison

- Failure Modes and Effects Analysis
- Fault Tree Analysis
- Event Tree Analysis
- HAZOP

Summary

- All are 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 (except FMEA)
  - Application to well-understood mechanical or physical systems

General limitations

- Component failure accidents only
    - Design issues?
    - Requirements issues?
- Requires detailed system design
- Failure mechanisms must already be known
    - Best for standard parts with few and well-known failure modes
- Works best on hardware/mechanical components
    - **Human** operators?
    - **Software** doesn’t fail
    - Organizational factors (management pressure? culture?)
- “Stopping rule” unclear
- Other methods may be better suited to deal with the challenges introduced with complex systems

Today’s Agenda

- ✓ Intro to reliability and system risk
- ✓ Overview of analysis techniques
- ✓ Traditional qualitative techniques
  - Failure Modes and Effects Analysis
  - Fault Tree Analysis
  - Event Tree Analysis
  - HAZOP
- ➡ Traditional quantitative techniques
  - Quant. Fault Tree Analysis
  - FMECA
  - Quant. ETA

Quantitative Techniques

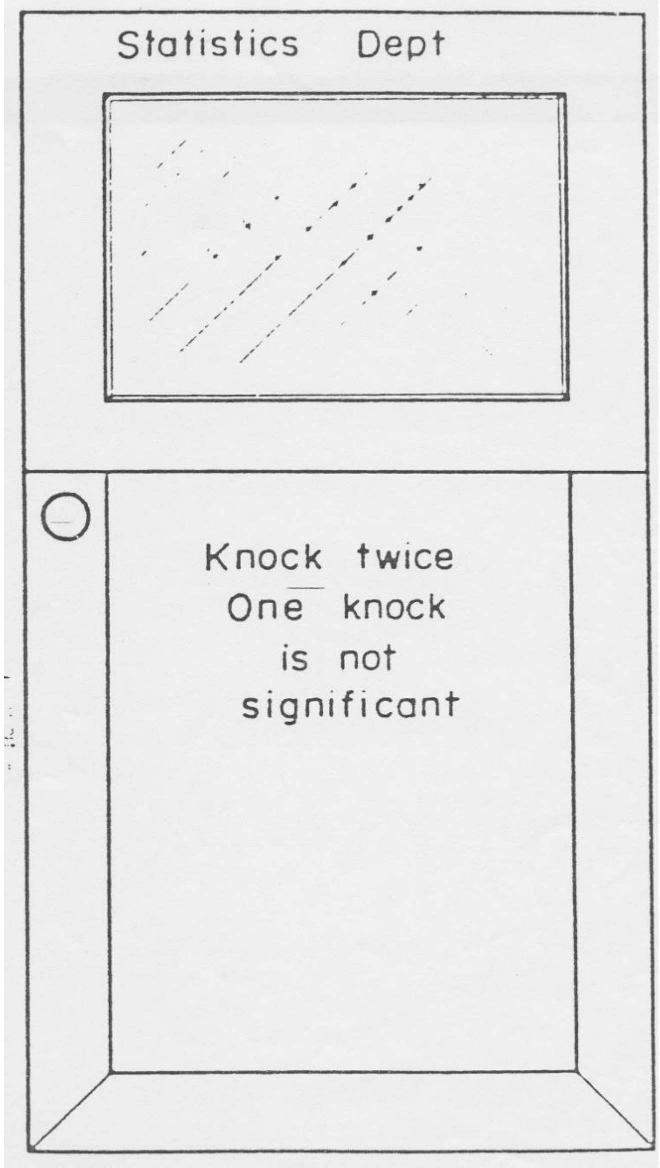
Quantitative analysis

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

Quantitative methods

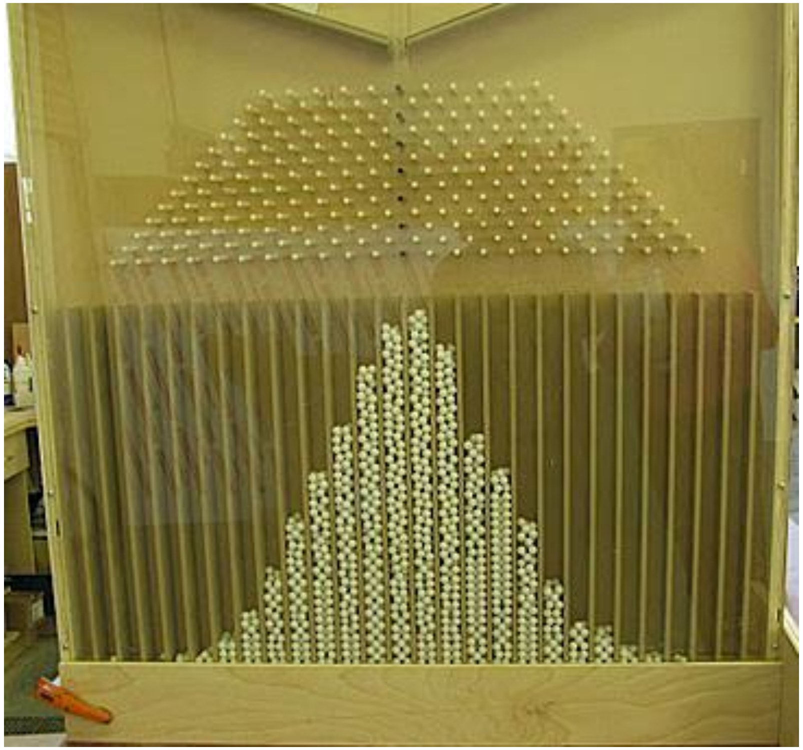
- The quantification is usually based on probability theory and statistics
- Common assumptions
  - Behavior is random
  - Each behavior independent

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



Good assumptions?

-Hardware?

-Humans?

-Software?

Risk Matrix

- Based on common quantification:

  Risk = Severity * Likelihood

Likelihood

Very Likely					
Likely					
Possible					
Unlikely					
Rare					
	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

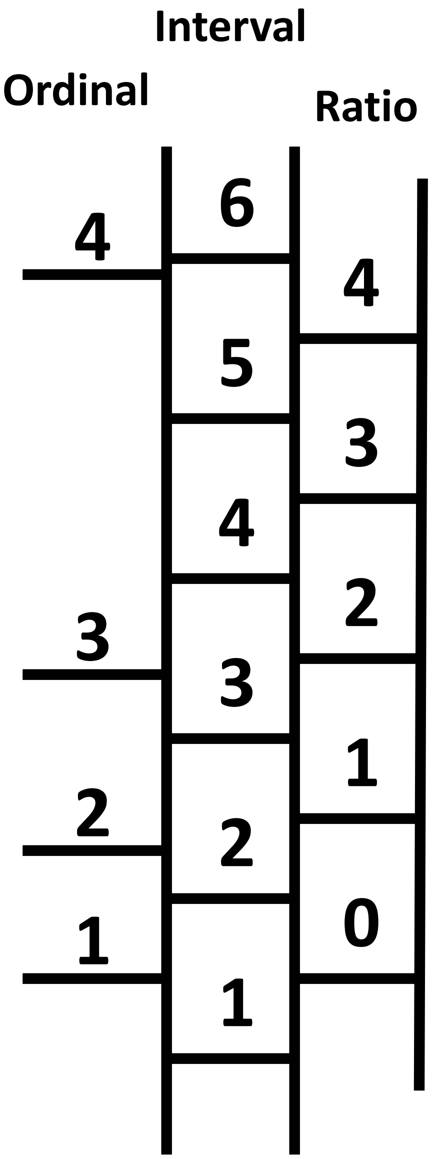
- Level 1: Catastrophic
  - Failure may cause crash.
  - Failure conditions prevent continued safe flight and landing
- Level 2: Severe
  - Failure has negative impact on safety, may cause serious or fatal injuries
  - Large reduction in functional capabilities
- Level 3: Major
  - Failure is significant, 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

How to quantify?

From ARP4671, DO-178B

Ordinal Values

- 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

Risk Matrix

- Based on common idea:

  Risk = Severity * Likelihood

Uses expected values (averages)

Likelihood

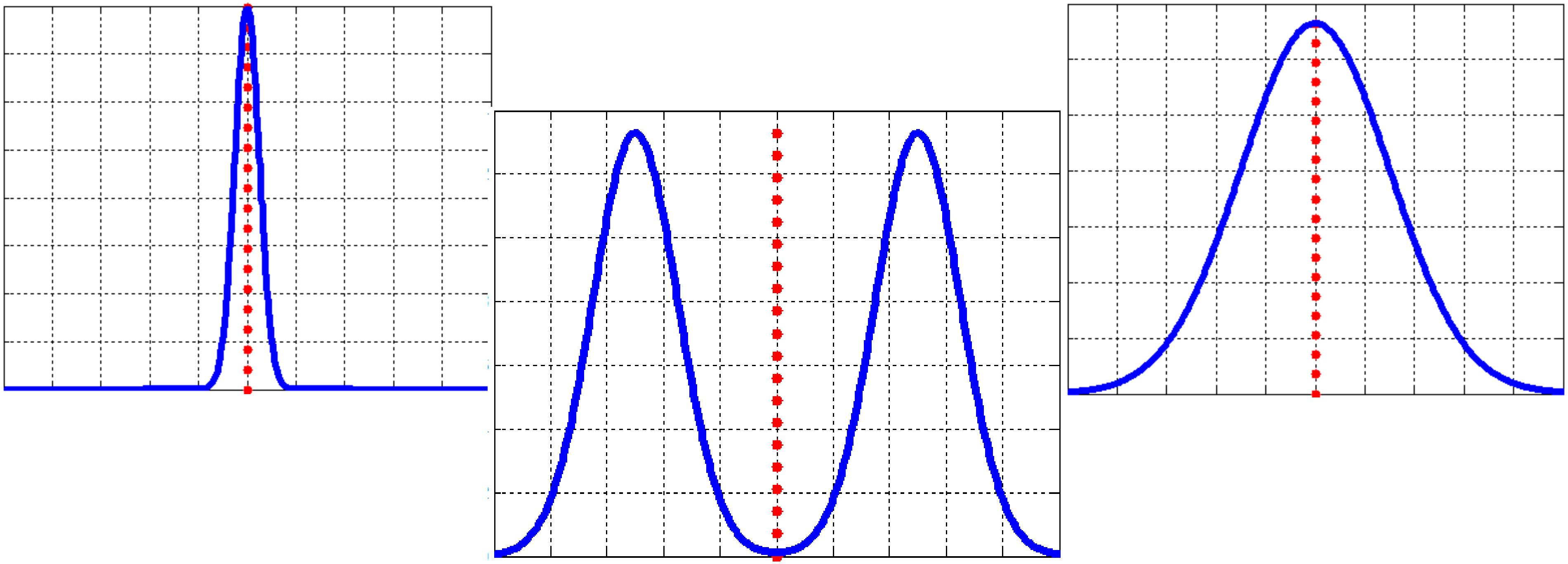
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Rare	Low	Low	Low Med	Medium	Medium
	Negligible	Minor	Moderate	Significant	Severe

Severity

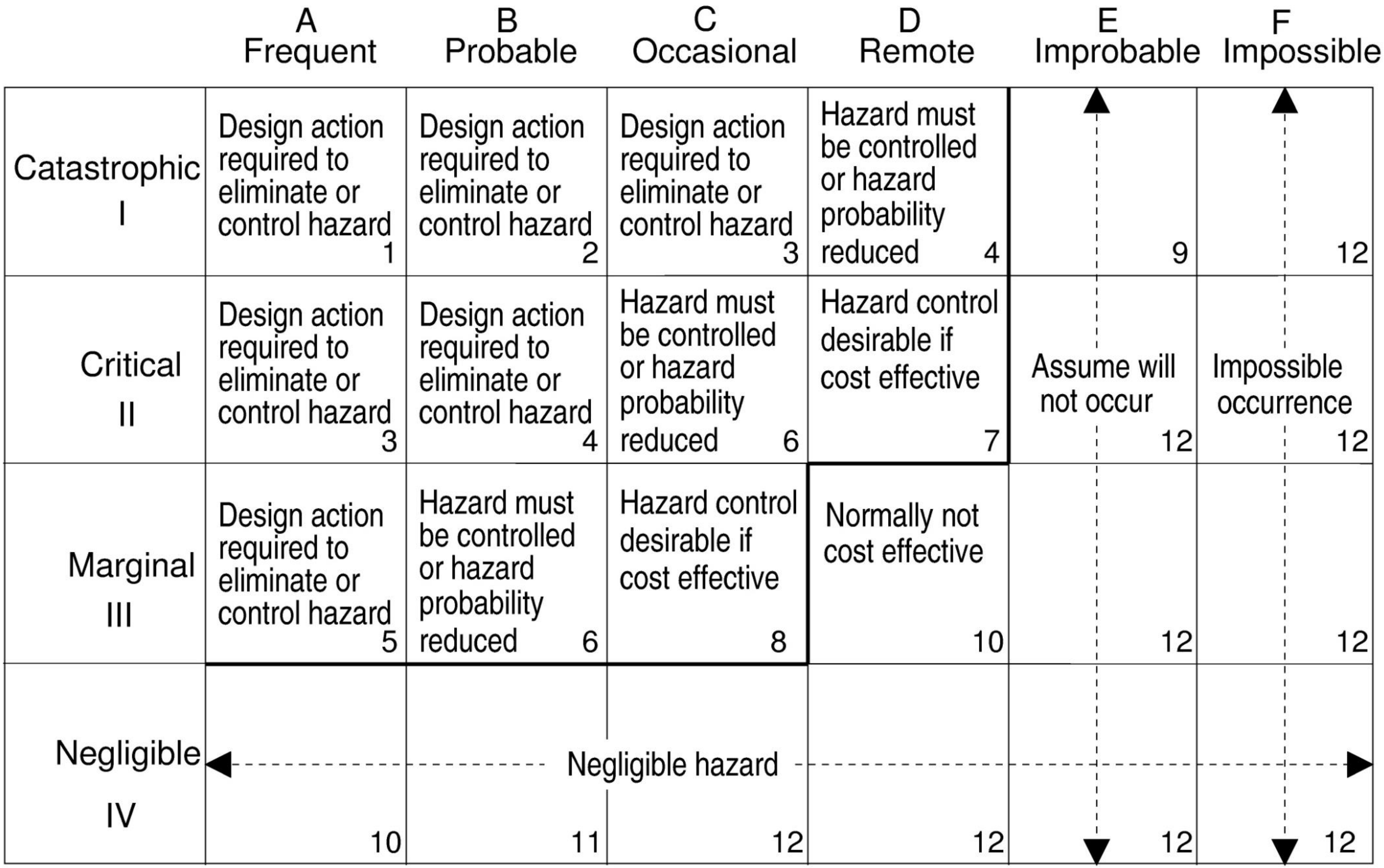
Expected Value Fallacy

aka P-value Fallacy
aka Flaw of Averages
aka Jensen’s Law

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



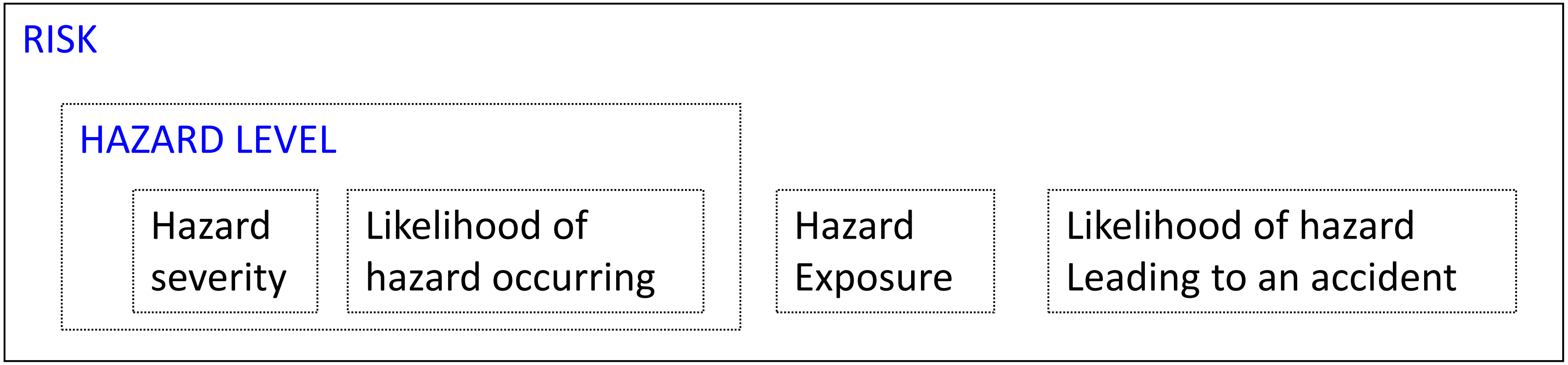
Another Example Hazard Level Matrix



	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	Negligible hazard 10	11	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.



RISK

HAZARD LEVEL

Hazard severity

Likelihood of hazard occurring

Hazard Exposure

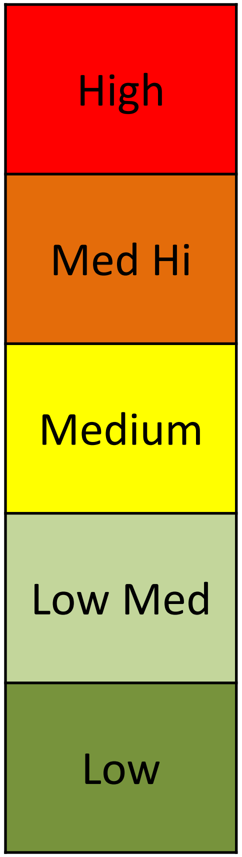
Likelihood of hazard Leading to an accident

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:



High

Med Hi

Medium

Low Med

Low

FMECA
Failure Modes Effects and Criticality Analysis

FMECA

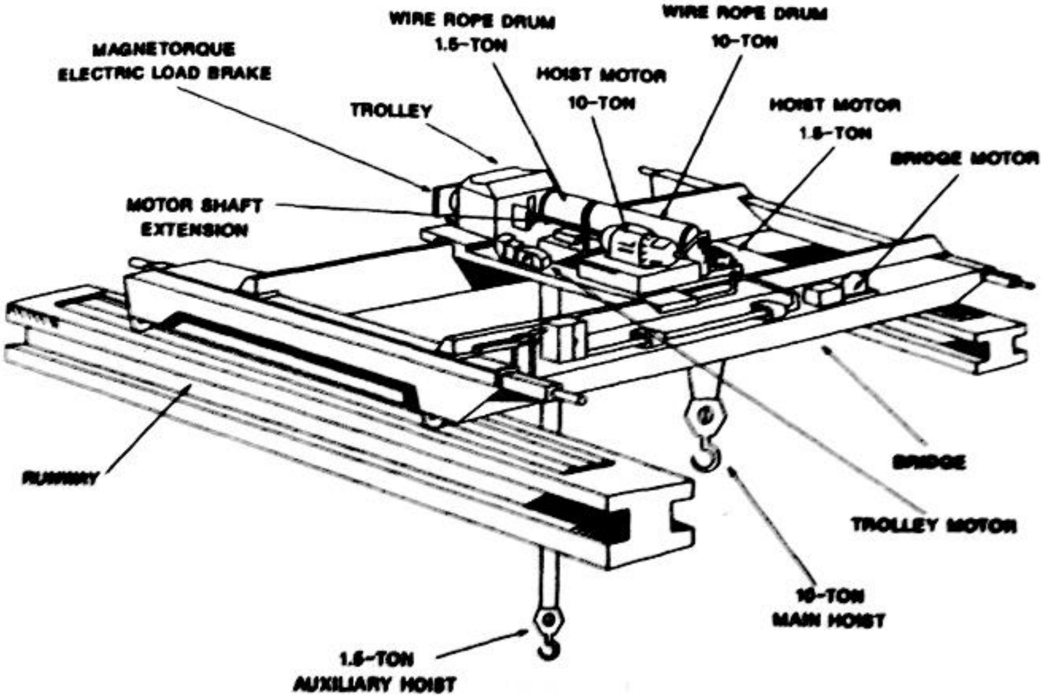
- Same as FMEA, but with “criticality” information

- 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

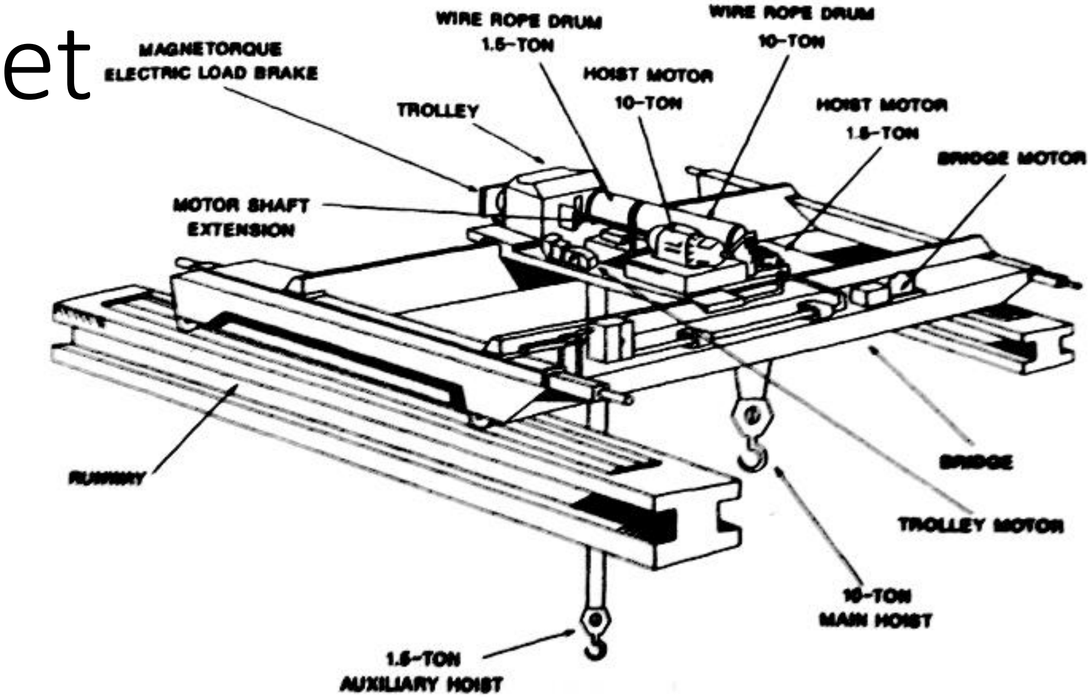
Rating	Severity of Effect
10	Safety issue and/or non-compliance with government regulation without warning.
9	Safety issue and/or non-compliance with government regulation with warning.
8	Loss of primary function.
7	Reduction of primary function.
6	Loss of comfort/convenience function.
5	Reduction of 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



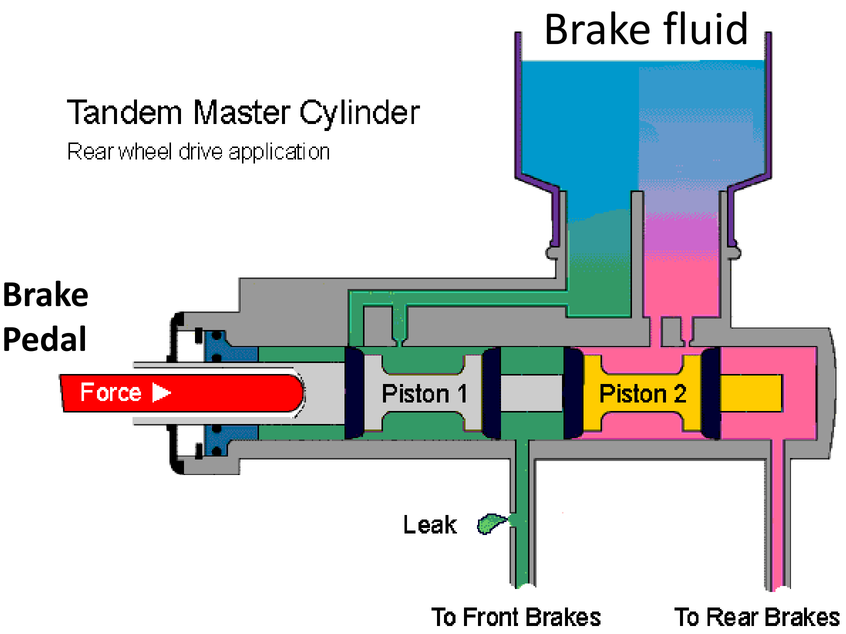
Failure Mode and Effect Analysis

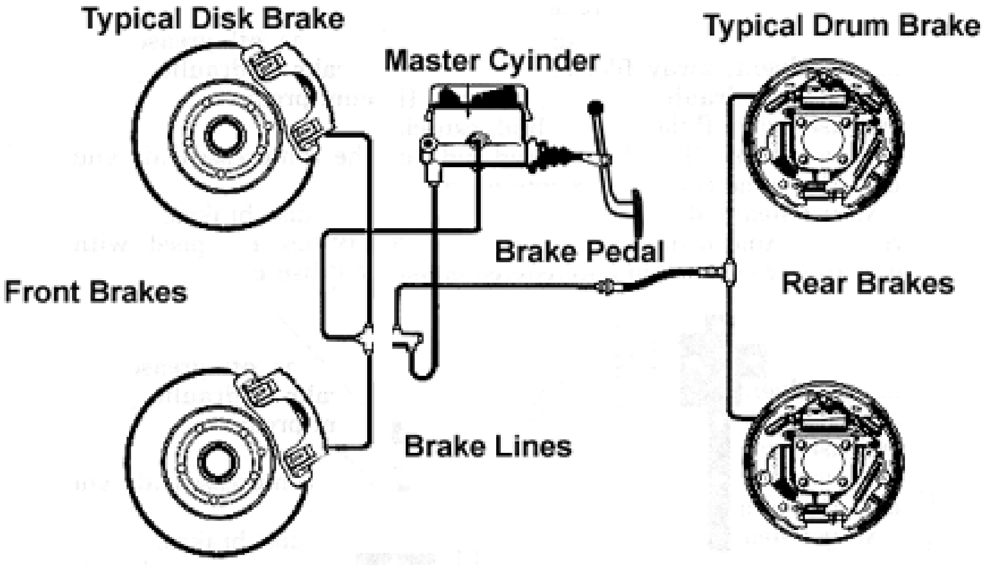
Program:__________ System:__________ Facility:_________
Engineer:__________ Date:_____________ Sheet:__________

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

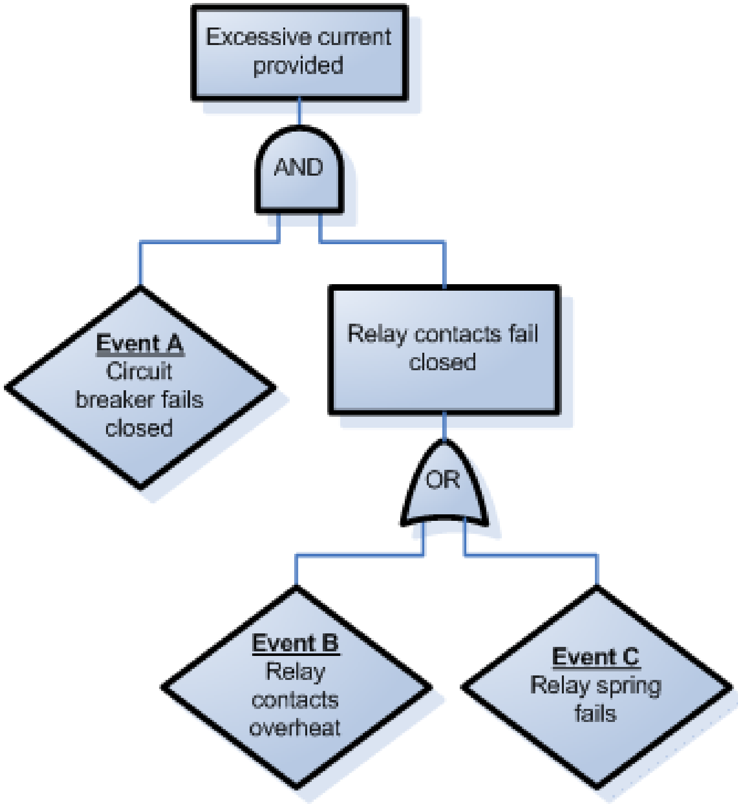
1. No effect
2. Minor, not noticed by average customer
3. Major, loss of primary function
4. Catastrophic, injury/death

Quantitative 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!

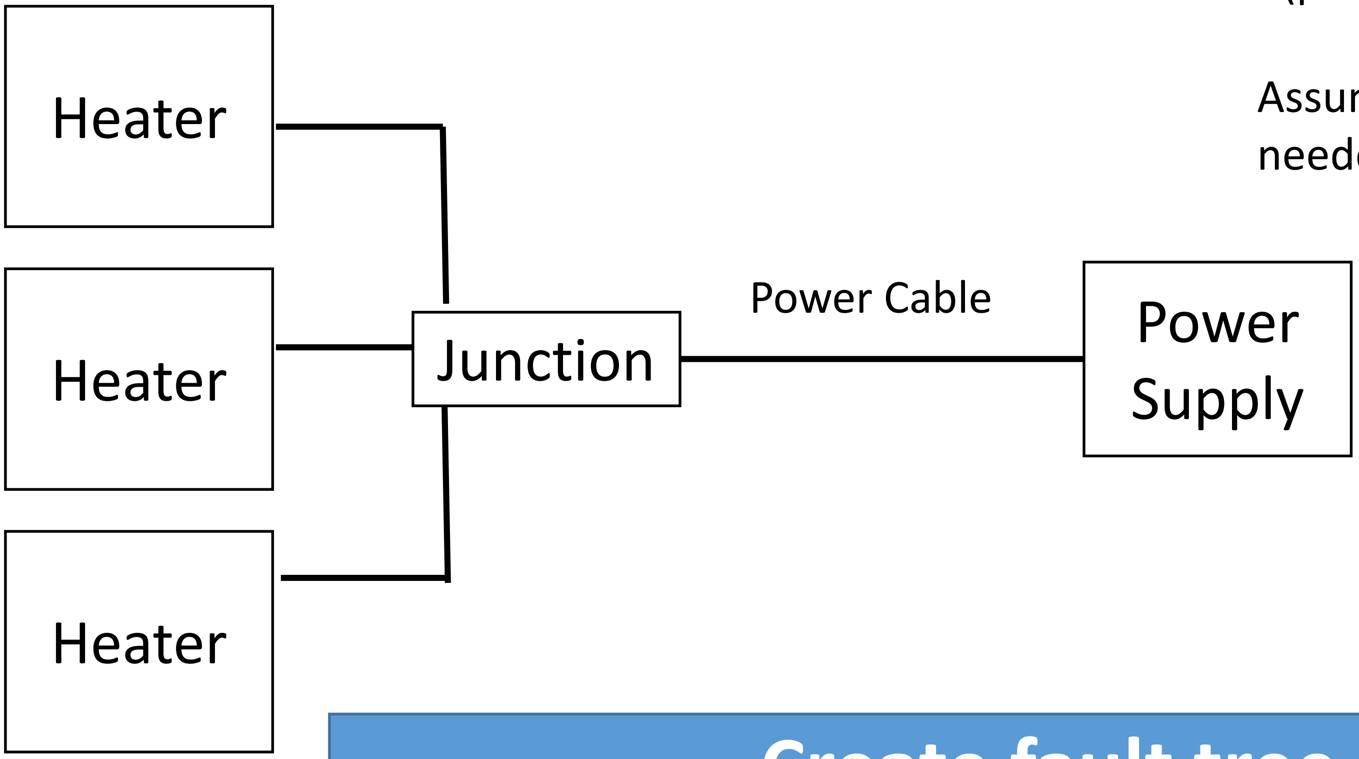
- AND gate
  - P(A and B) = P(A) * P(B)
- OR gate
  - P(A or B) = P(A) + P(B)


Excessive current provided
AND
Event A
Circuit breaker fails closed
Relay contacts fail closed
OR
Event B
Relay contacts overheat
Event C
Relay spring fails

Exercise:
LHC ATLAS Return Heaters

P(heater fails) = 0.33
P(heater wire) = 0.25
P(junction fails) = 0.10
P(power cable fails) = 0.05
P(power supply fails) = 0.01

Assume at least 1 heater is needed to function

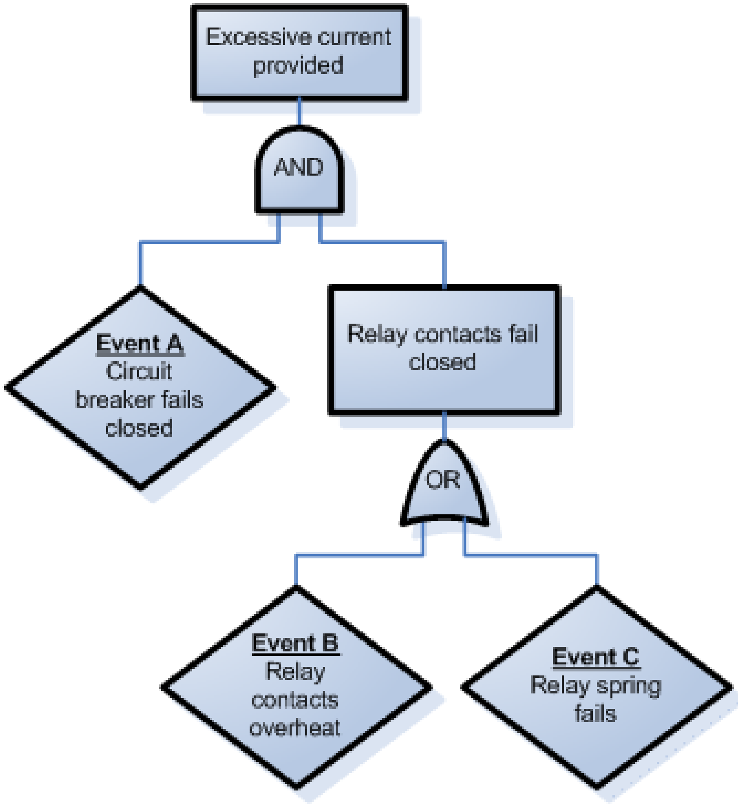


Create fault tree
Identify minimum cutsets
Calculate overall probability of failure

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)


Excessive current provided
AND
Event A
Circuit breaker fails closed
Relay contacts fail closed
OR
Event B
Relay contacts overheat
Event C
Relay spring fails

Any assumptions being made?

Quantitative Fault Tree Analysis

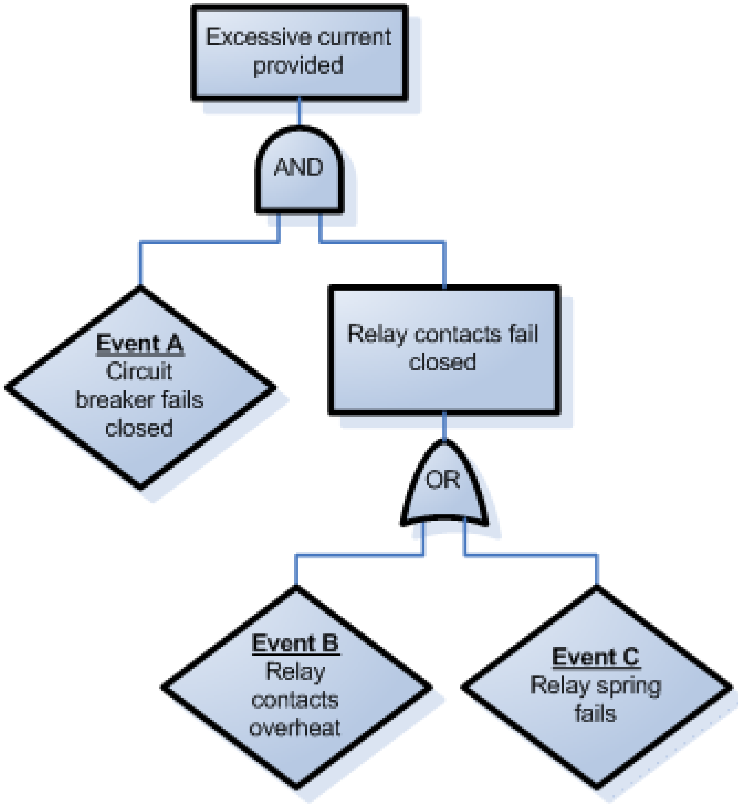
- If we can assign probabilities to lowest boxes…
  - Can propagate up using probability theory
  - Can get overall total probability of hazard!

- 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

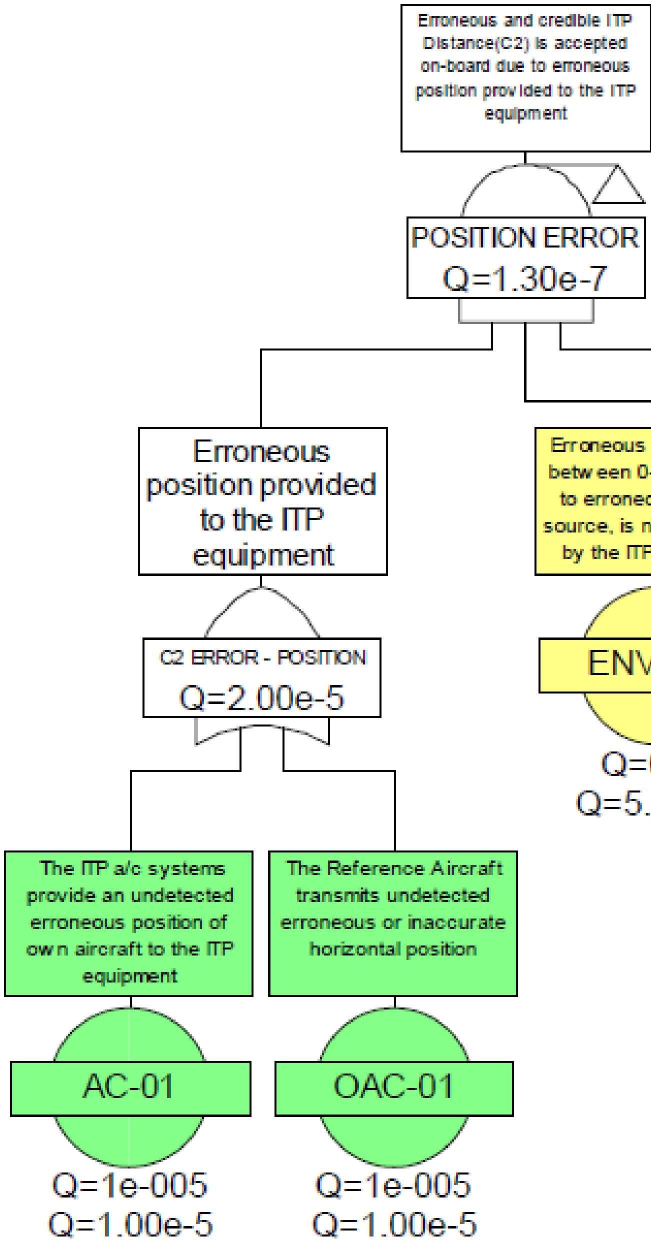
- If we can assign probabilities to lowest boxes…
  - Can propagate up using probability theory
  - Can get overall total probability of hazard!


Excessive current provided
AND
Event A
Circuit breaker fails closed
Relay contacts fail closed
OR
Event B
Relay contacts overheat
Event C
Relay spring fails

- 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



Erroneous and credible ITP Distance(C2) is accepted on-board due to erroneous position provided to the ITP equipment

POSITION ERROR
Q=1.30e-7

Erroneous position provided to the ITP equipment

C2 ERROR - POSITION
Q=2.00e-5

The ITP a/c systems provide an undetected erroneous position of own aircraft to the ITP equipment

AC-01
Q=1e-005
Q=1.00e-5

The Reference Aircraft transmits undetected erroneous or inaccurate horizontal position

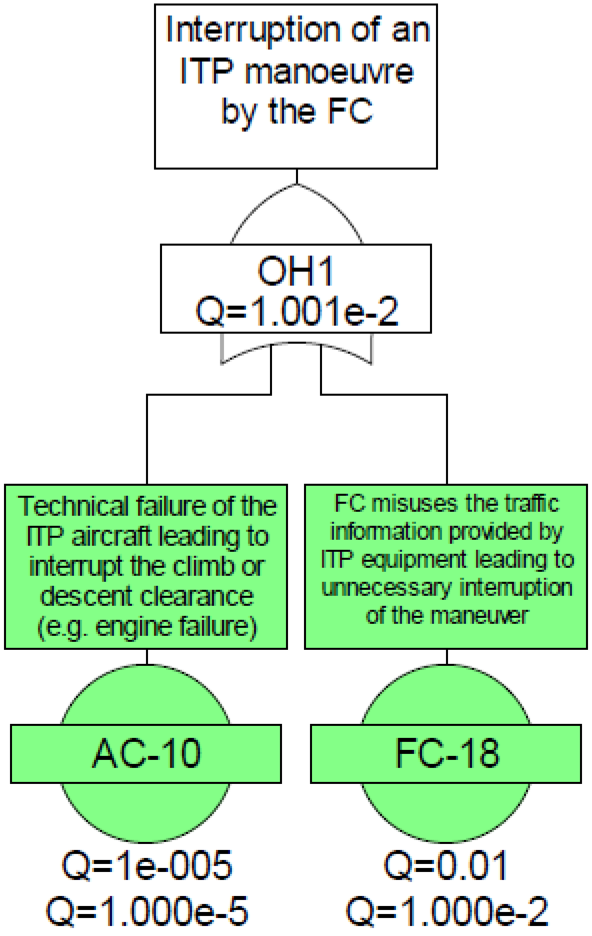
OAC-01
Q=1e-005
Q=1.00e-5

Erroneous ITP distance between 0-500NM, due to erroneous position source, is not filtered out by the ITP equipment

ENVT-12
Q=0.05
Q=5.00e-2

The erroneous ITP distance (15NM-80NM) due to erroneous position source is such that the crew believes it is valid

FC-06
Q=0.13
Q=1.30e-1



Interruption of an ITP manoeuvre by the FC

OH1
Q=1.001e-2

Technical failure of the ITP aircraft leading to interrupt the climb or descent clearance (e.g. engine failure)

AC-10
Q=1e-005
Q=1.000e-5

FC misuses the traffic information provided by ITP equipment leading to unnecessary interruption of the maneuver

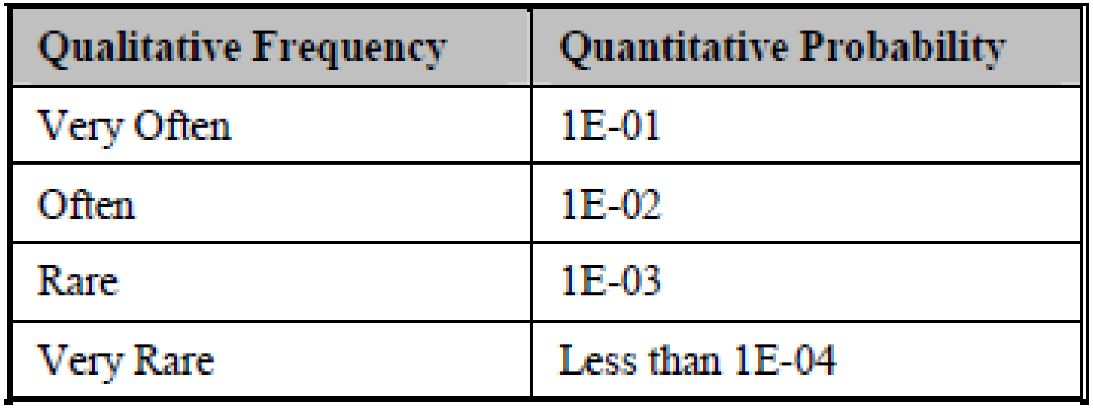
FC-18
Q=0.01
Q=1.000e-2

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?



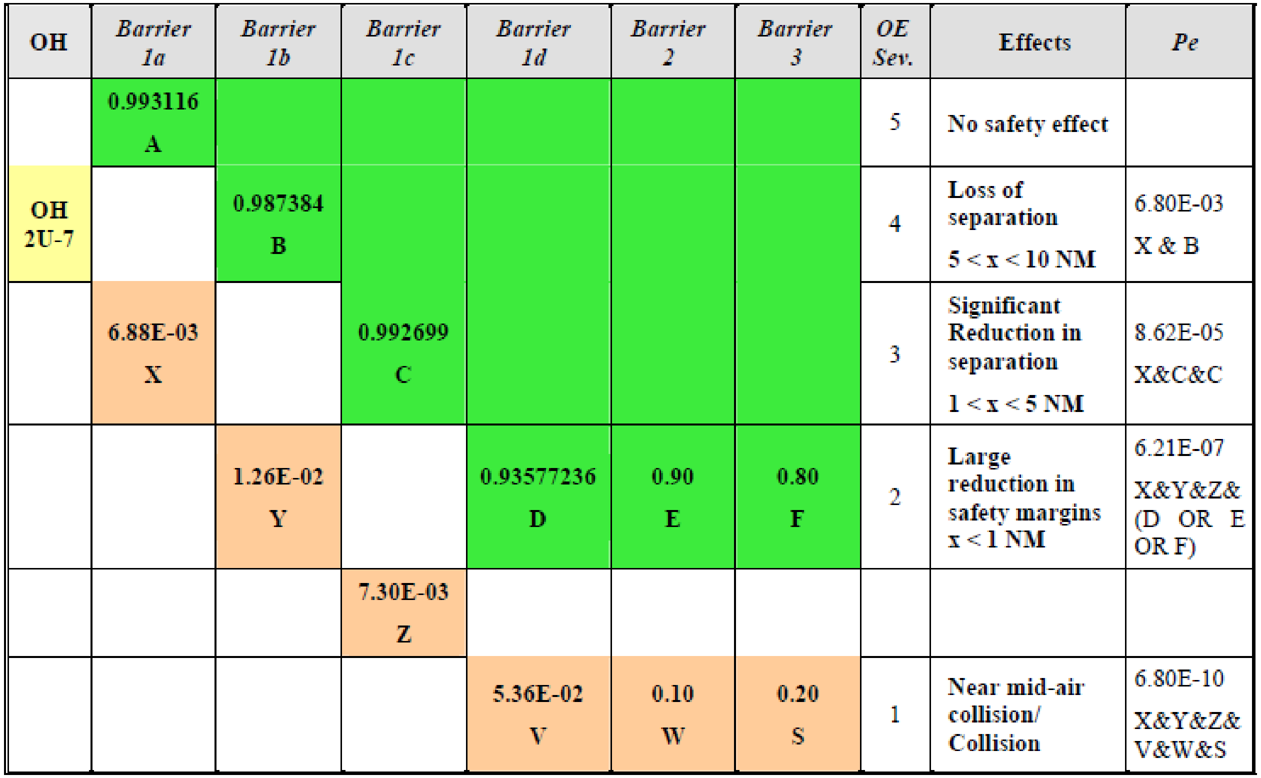
Qualitative Frequency	Quantitative Probability
Very Often	1E-01
Often	1E-02
Rare	1E-03
Very Rare	Less than 1E-04

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

*Actual qualitative-quantitative conversion from RTCA DO-312

Quantitative ETA

Quantitative Event Tree Analysis

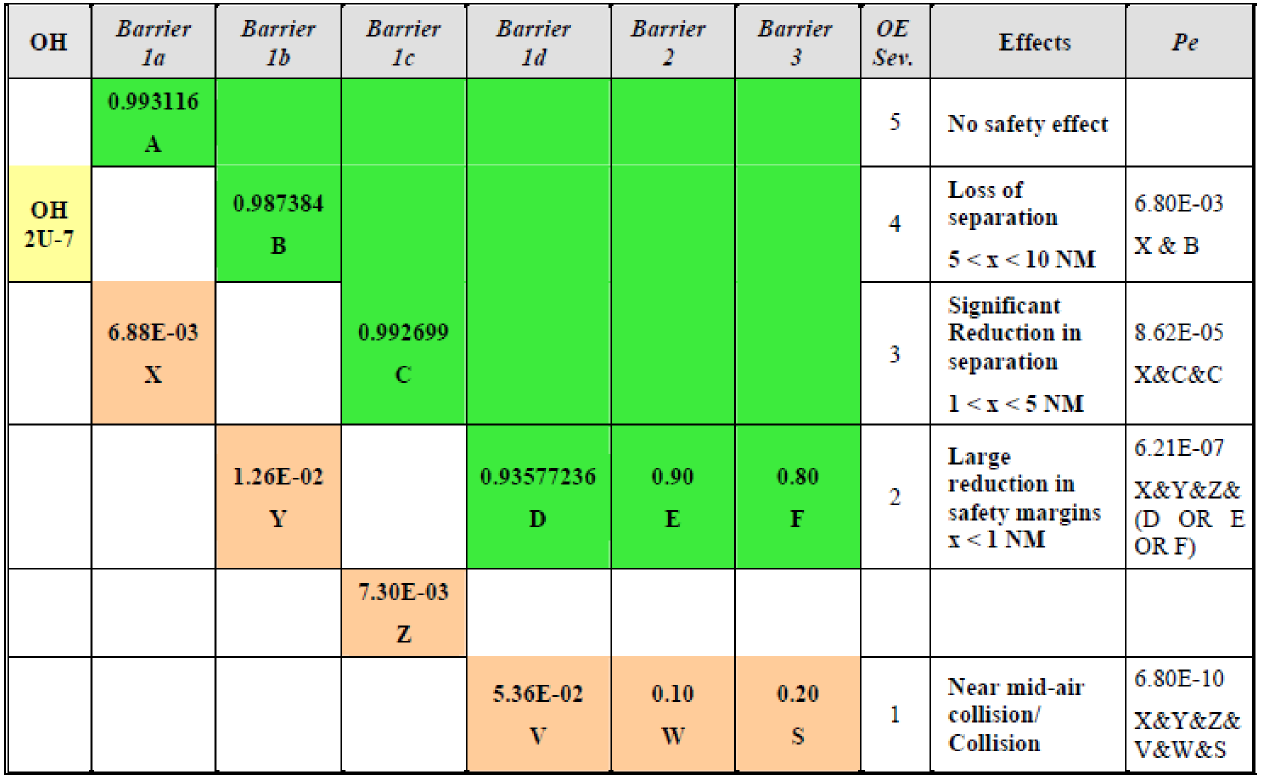


OH	*Barrier 1a*	*Barrier 1b*	*Barrier 1c*	*Barrier 1d*	*Barrier 2*	*Barrier 3*	*OE Sev.*	Effects	*Pe*
	0.993116 A						5	No safety effect	
OH 2U-7		0.987384 B					4	Loss of separation $5 < x < 10$ NM	6.80E-03 X & B
	6.88E-03 X		0.992699 C				3	Significant Reduction in separation $1 < x < 5$ NM	8.62E-05 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 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

From RTCA DO-312

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

From RTCA DO-312

Probabilistic Risk Assessment

- Based on chain-of-events model
    - Usually concentrates on failure events
- Combines event trees and fault trees
    - 1975 : WASH-1400 NRC report
    - Fault trees were too complex
    - Used event trees to identify specific events to model with fault trees
- Usually assumes independence between events
- Events chosen will affect accuracy, but usually arbitrary (subjective)

Risk Measurement

- Can be hard to measure risk directly and accurately
  - Accuracy of such assessments is controversial

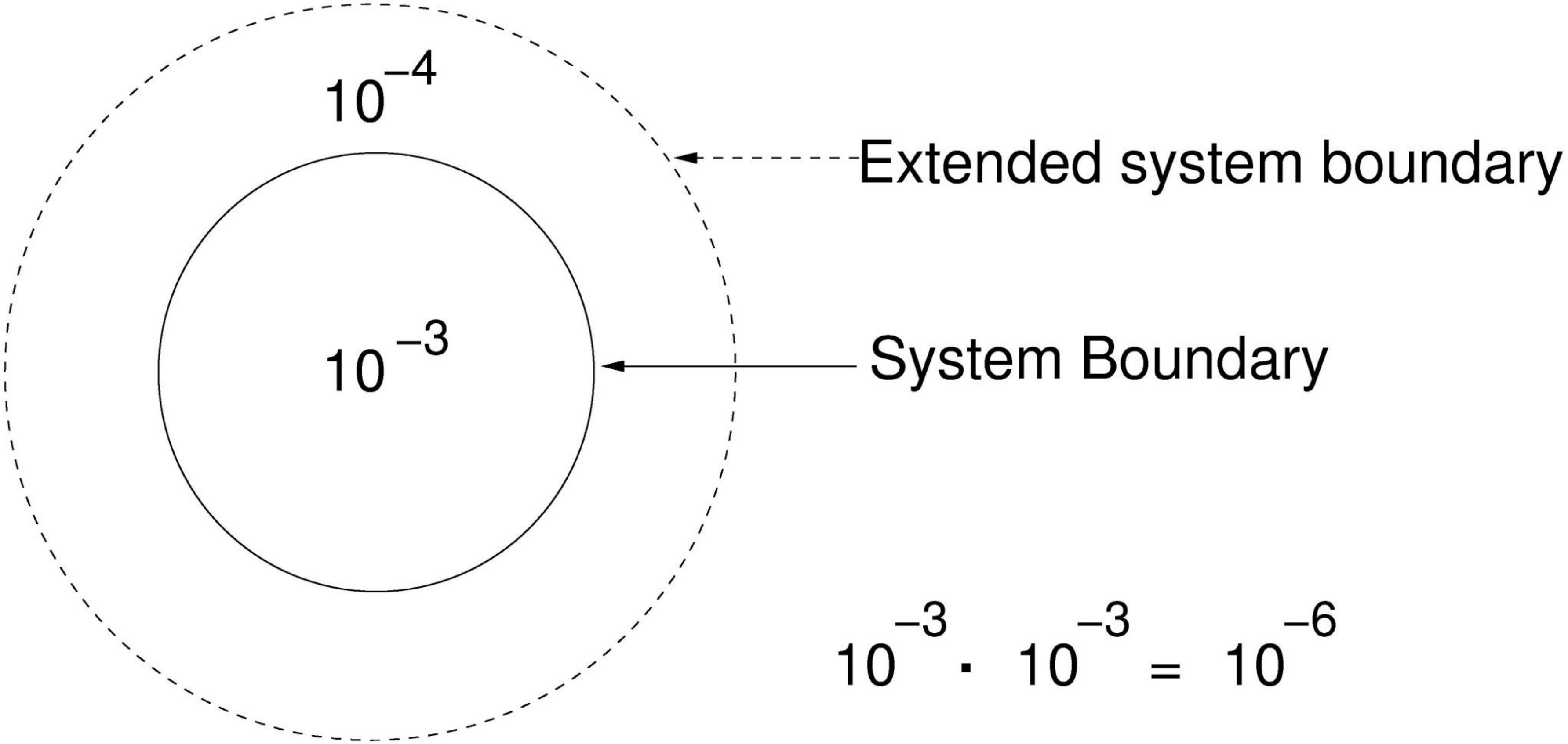
    "To avoid paralysis resulting from waiting for definitive data, we assume we have greater knowledge than scientists actually possess and make decisions based on those assumptions."

    William Ruckleshaus

  - Cannot evaluate probability of very rare events directly
  - So use models of the interaction of events that can lead to an accident

Misinterpreting Risk

Risk assessments can easily be misinterpreted:



Discussion

- Quantitative techniques have been around for decades
  - Nuclear industry was first to adopt
- Some have tried to evaluate their effectiveness using historical data

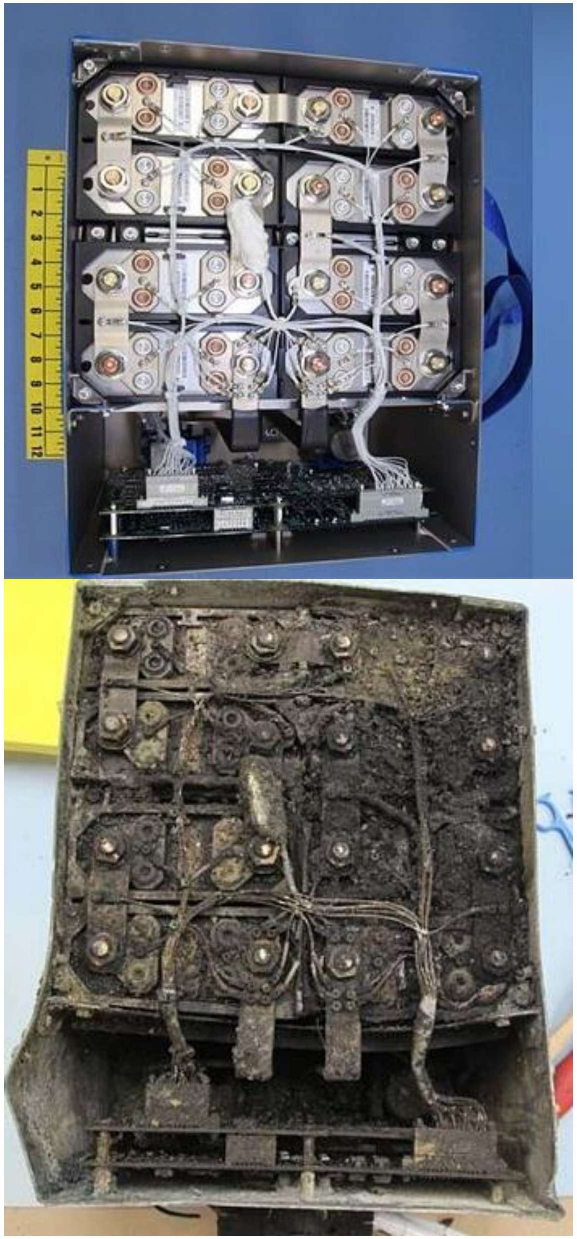
- http://www.energypolicyblog.com/2011/04/27/reassessing-the-frequency-of-partial-core-melt-accidents/

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 x 10^4 flight hours [NTSB 2013]



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

Some factors are difficult to predict in quantitative analysis

- Mars Polar Lander
  - Missing software requirements, leg deployment caused engine shutdown
- Mars Climate Orbiter
  - Software requirements misunderstanding, units
- Toyota Unintended Acceleration
  - Poor quality software, etc.
- Deepwater Horizon
  - Inadequate cement requirements, incorrect test procedures, etc.
- Etc.

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]

more Lord Kelvin Quotes

- “Radio has no future.”
- “Wireless [telegraphy] is all very well but I'd rather send a message by a boy on a pony!”
- Writing to Niagara Falls Power Company: "Trust you will avoid the gigantic mistake of alternating current.“
- "I can state flatly that heavier than air flying machines are impossible."

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)