Reliability and System Risk Analysis Workshop

Dr. John Thomas

Schedule

Monday, July 20, 2015: Classical Techniques

1000-1030	Introduction, overview of failure search techniques
1030-1100	Qualitative Failure Modes and Effects Analysis (examples and exercise)
1100-1130	Qualitative Fault Tree Analysis (examples and exercise)
1130-1230	Other Qualitative Techniques (Event Tree Analysis, HAZOP)
Lunch	
1400-1430	Quantitative Fault Tree Analysis
1430-1515	Other Quantitative Techniques (FMEA, ETA)
1515-1545	Practical strengths and limitations, lessons learned
Break	
1615-1645	Wrap-up and discussion

Tuesday, July 21, 2015: Systems-Theoretic Techniques

0900-0915	Introduction and overview to Systems-Theoretic Techniques
0915-1000	Human factors introduction
1000-1030	Systems Theoretic Accident Models and Processes (STAMP)
Break	
1050-1220	System Theoretic Hazard Analysis (STPA)
Lunch	
1400-1600	STPA examples and exercises
1600-1630	Wrap-up and discussion

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

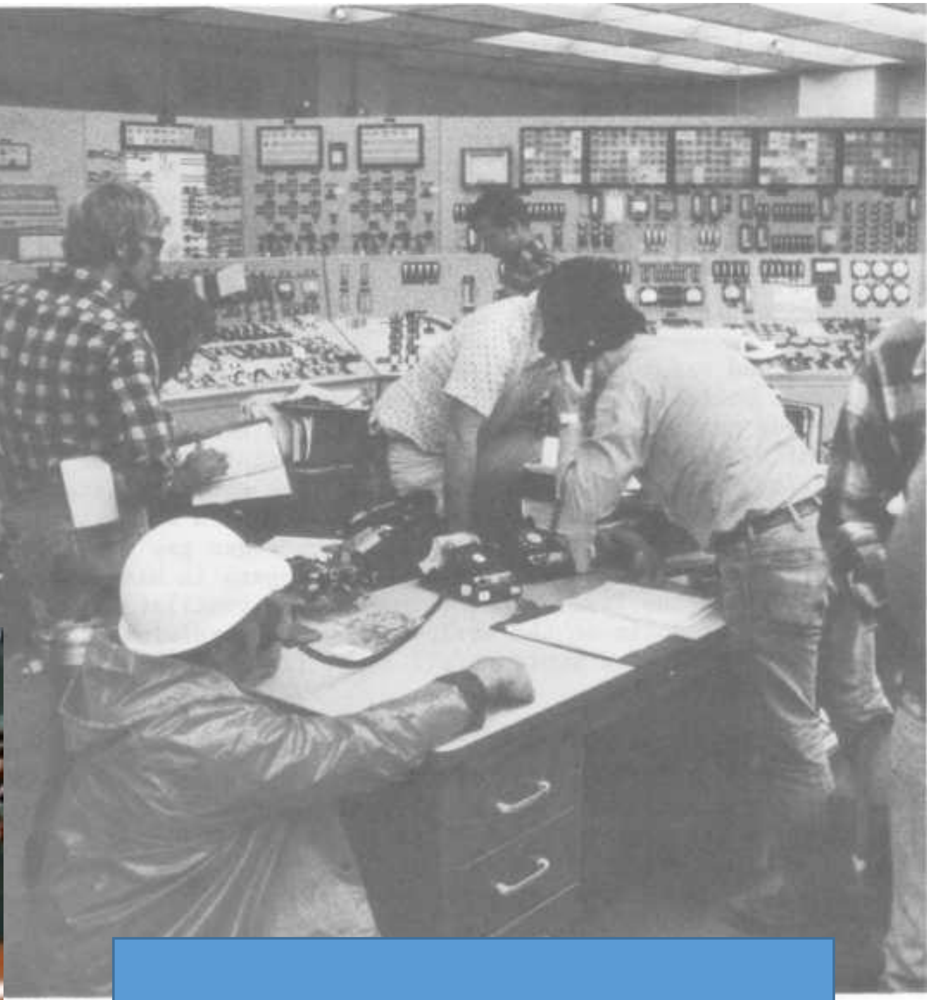
Today's class

- 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.



Root cause?

Component failure losses

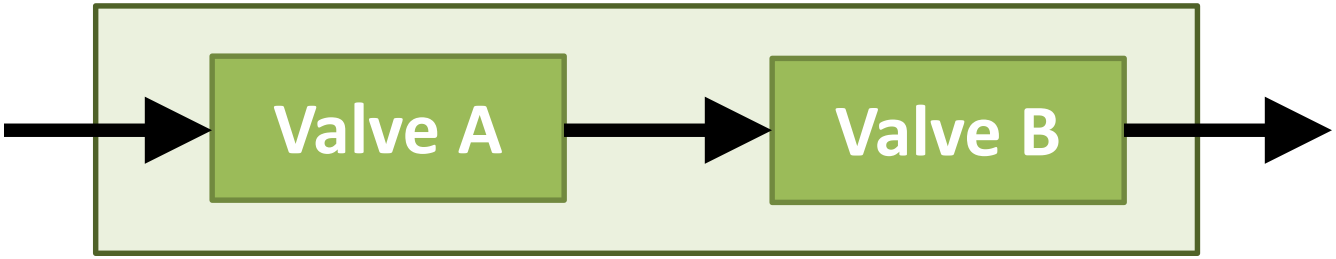
- These are losses caused by physical component failures
  - E.g. valve stuck open
  - Failure: Component does not perform as specified

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

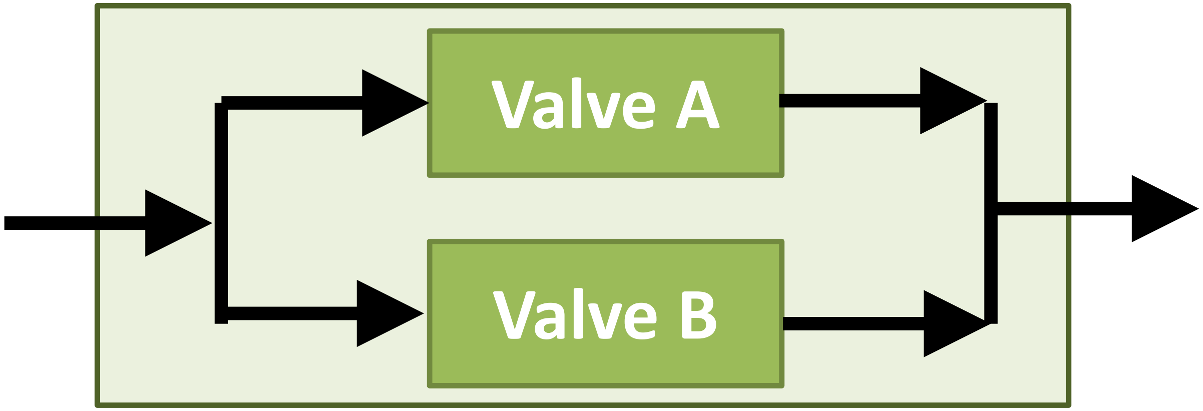
Classic reliability solutions

Redundancy

Two valves in series:



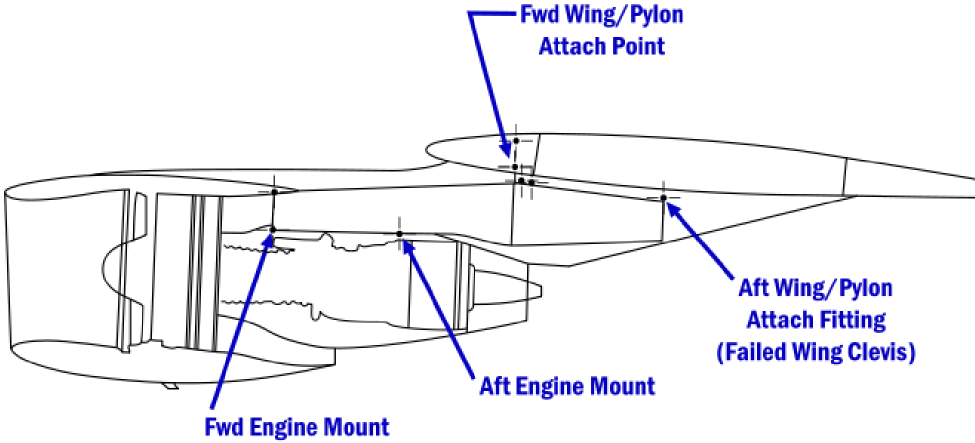
Two valves in parallel:



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.


Fwd Wing/Pylon Attach Point
Aft Wing/Pylon Attach Fitting (Failed Wing Clevis)
Aft Engine Mount
Fwd Engine Mount

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

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).
- Operators were not told how the light was designed, only that it indicated whether valve was open.

Design flaw!
Communication problems!
Inadequate procedures!
Etc.

CSB video

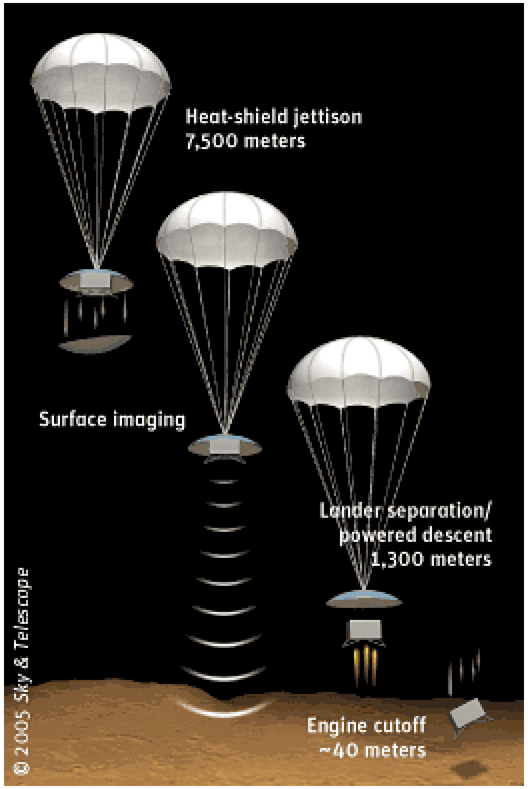
- Cooling system incident
- Discuss “Sharp end” vs. “Blunt end”

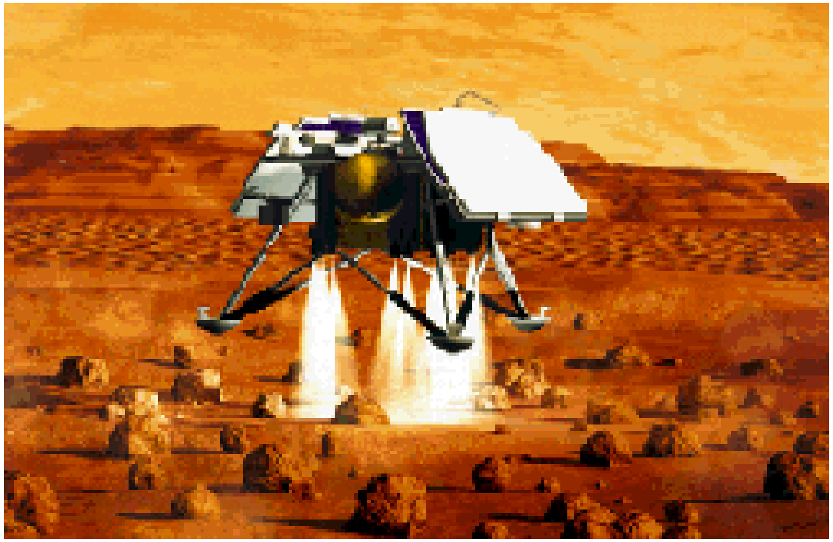
CSB video – Cooling system incident

- Recommendations:
  - Avoid manual interruption of evaporators
  - Add more redundant valves (obeying the same flawed software?)
  - Emergency shutdown recommendation
    - Activate emergency shutdown in the event of an ammonia release if a leak cannot be promptly isolated and controlled
- Inadequate checks and reviews were supposed to catch these problems before the incident
  - Technical reviews
  - Emergency procedure reviews
  - Regulations and Standards
  - Safety Management System

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).





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

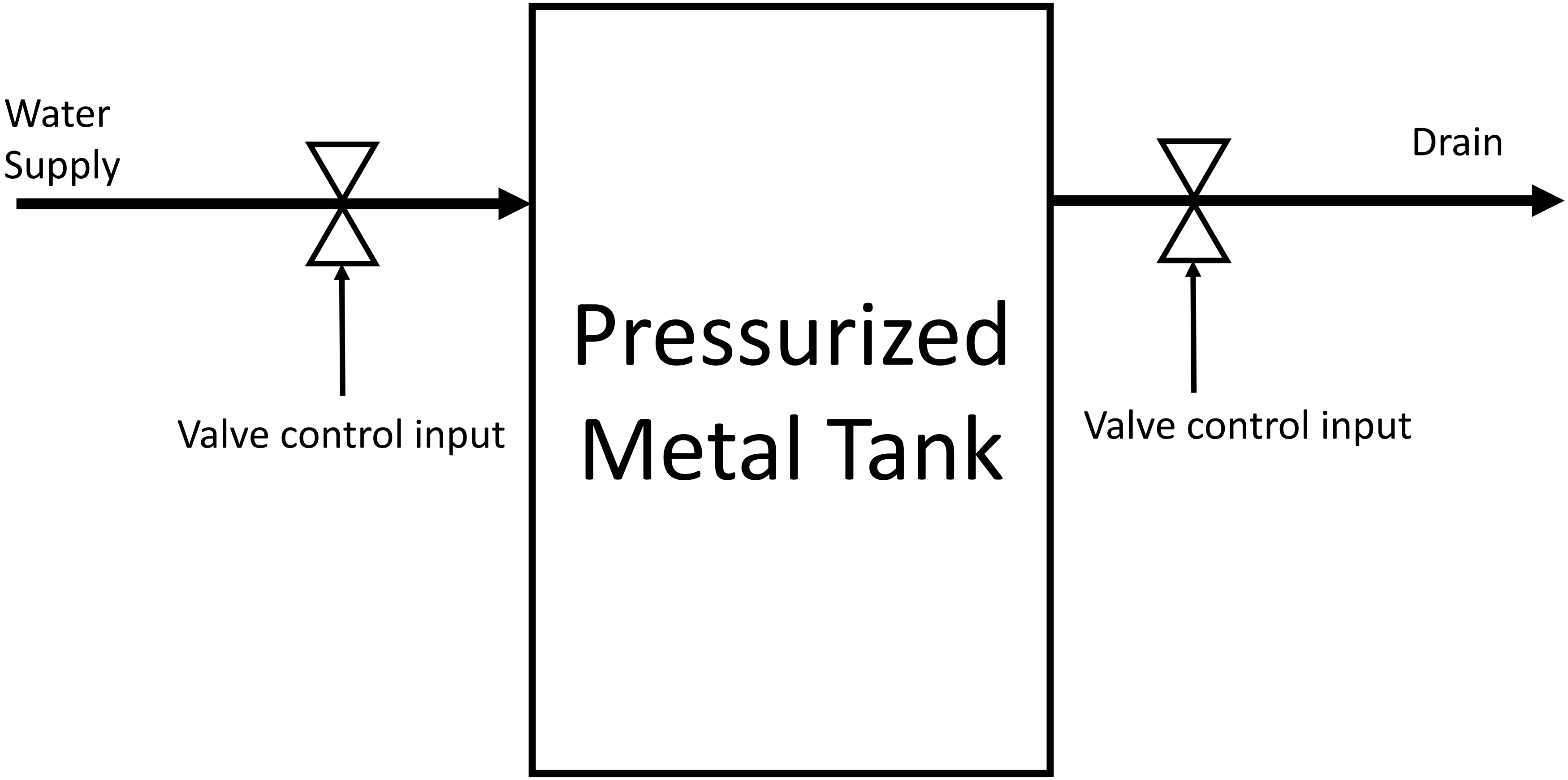
- ✓ Intro to reliability and system risk
- ➡ Overview of analysis techniques
- Traditional qualitative techniques
  - Failure Modes and Effects Analysis
  - Fault Tree Analysis
  - Event Tree Analysis
  - HAZOP
- Traditional quantitative techniques
  - Quant. Fault Tree Analysis
  - FMECA
  - Quant.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



Water Supply

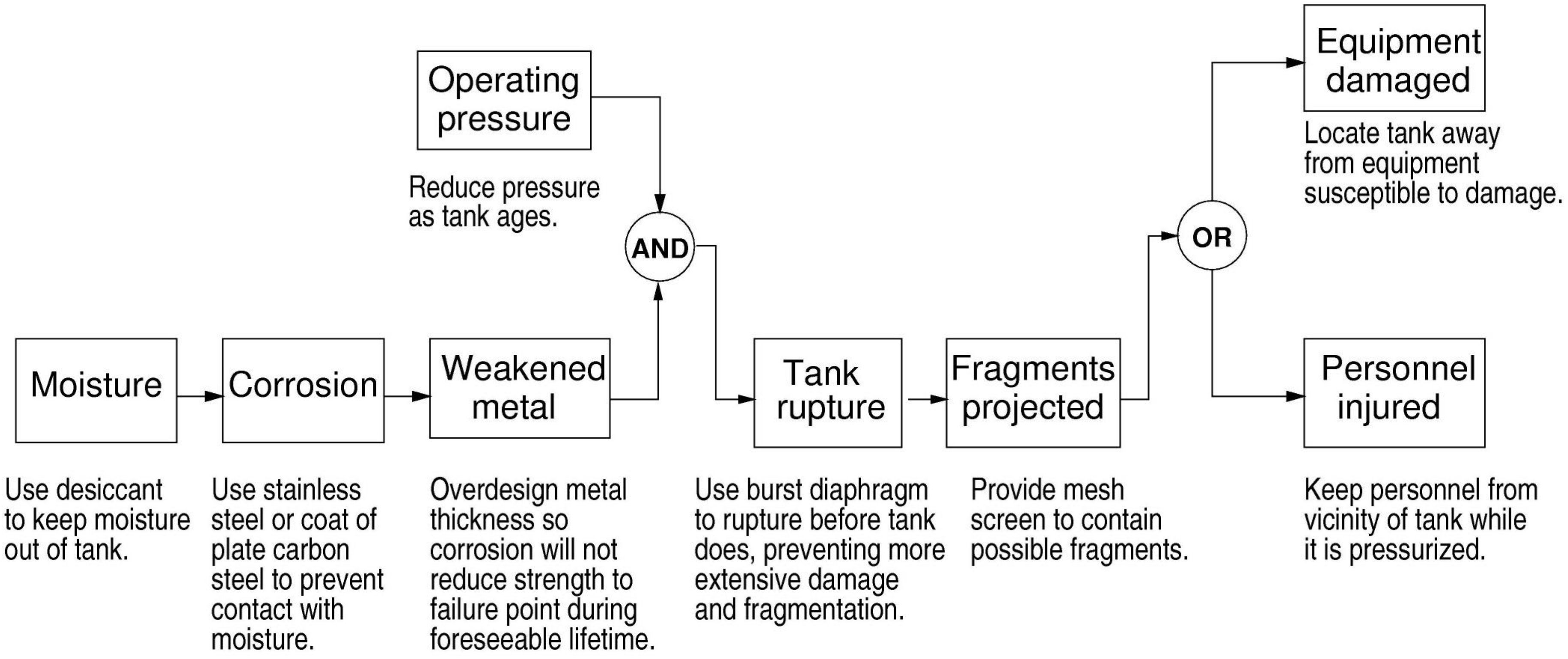
Valve control input

Pressurized Metal Tank

Drain

Valve control input

Accident model: Chain-of-events example



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.

Operating pressure

Reduce pressure as tank ages.

AND

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

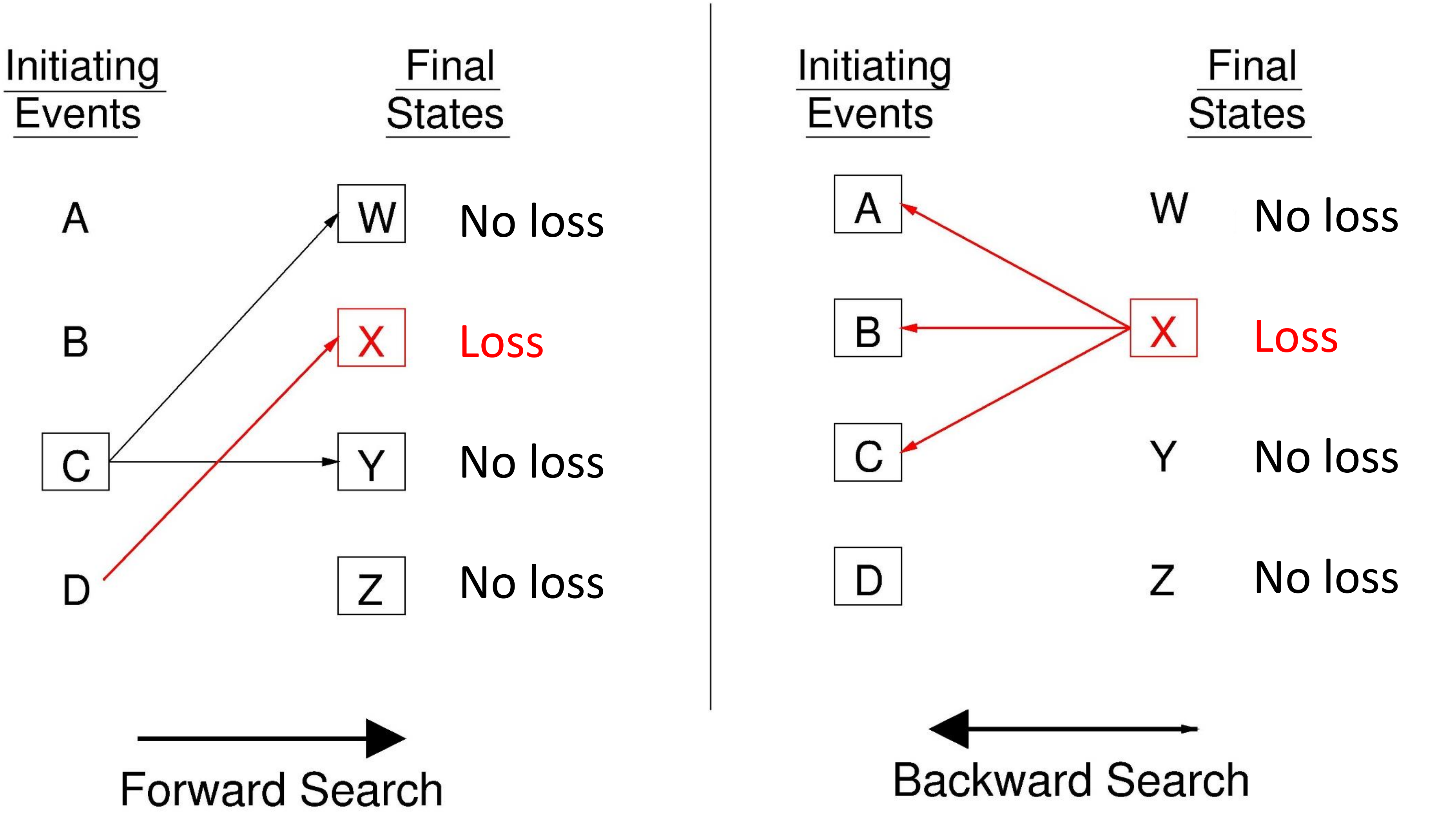
Locate tank away from equipment susceptible to damage.

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



Initiating Events

Final States

A

B

C

D

W No loss

X Loss

Y No loss

Z No loss

Forward Search

Initiating Events

Final States

A

B

C

D

W No loss

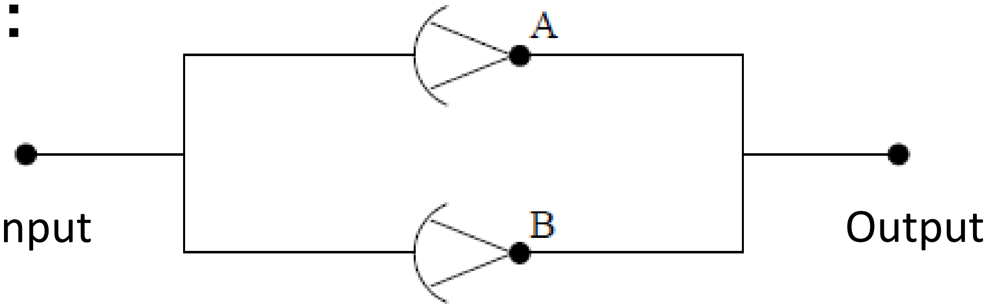
X Loss

Y No loss

Z No loss

Backward Search

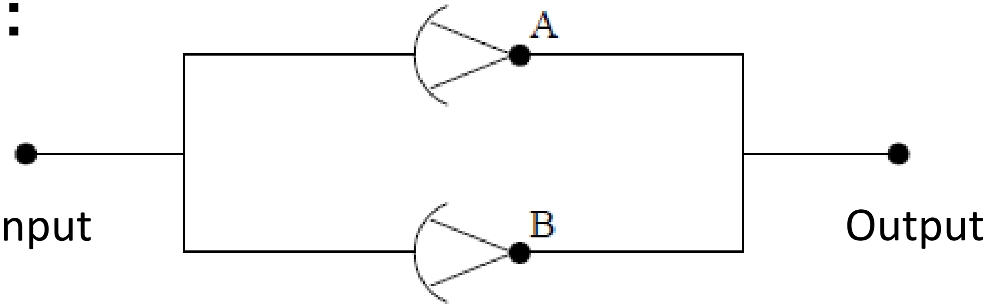
System Model:



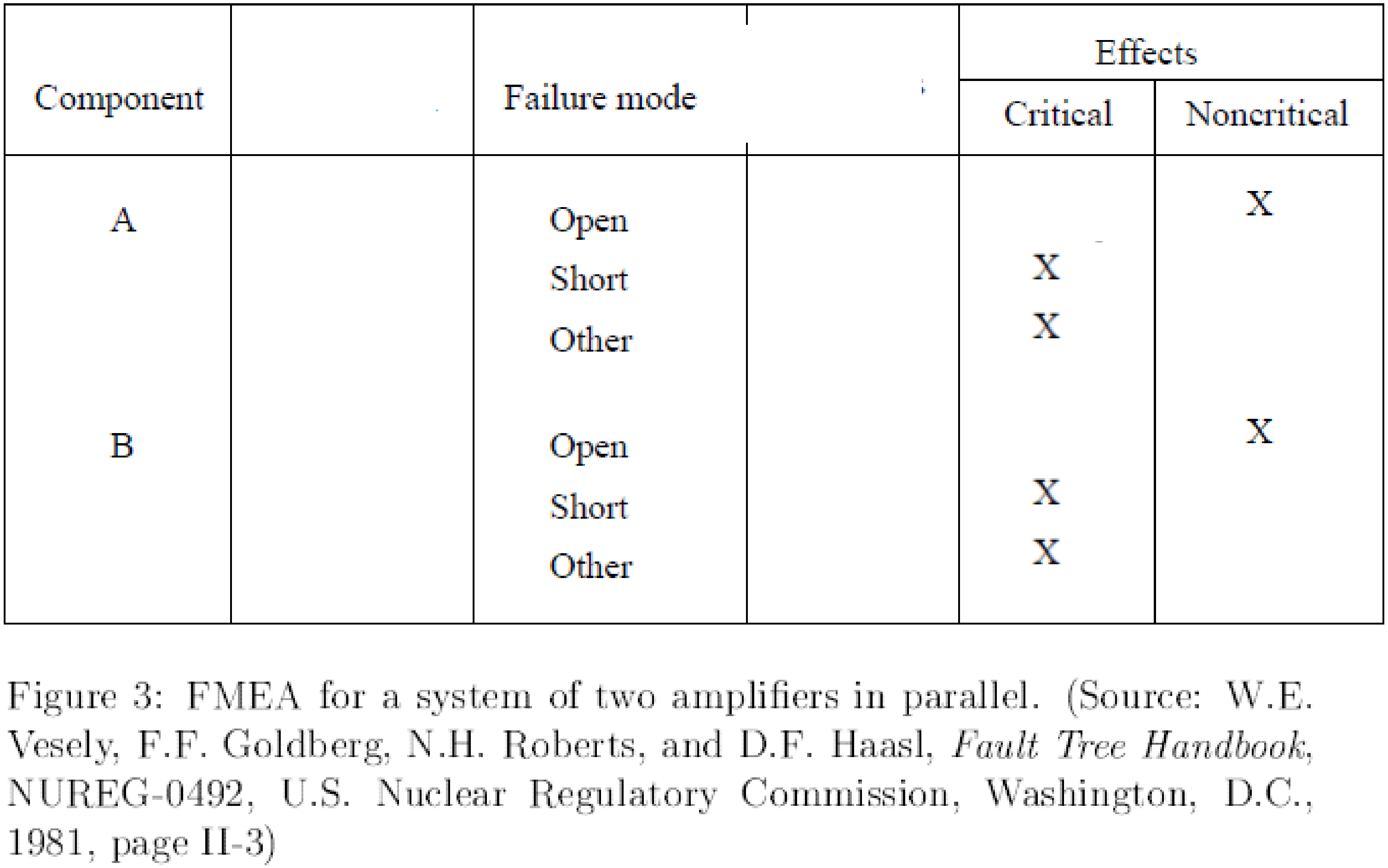
Forward search?

a system of two amplifiers in parallel.

System Model:



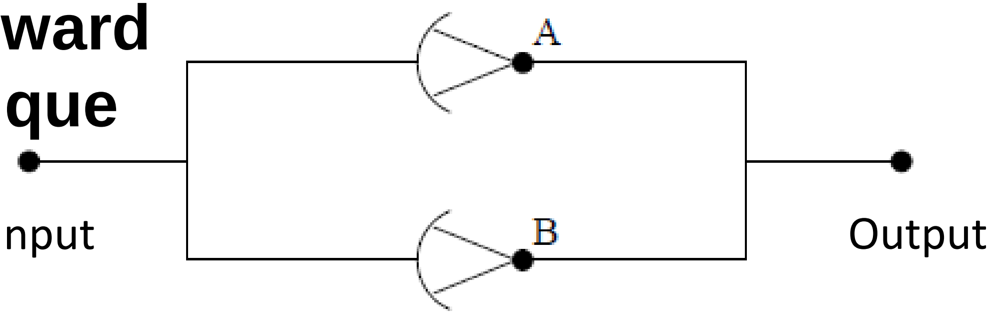
Forward search:

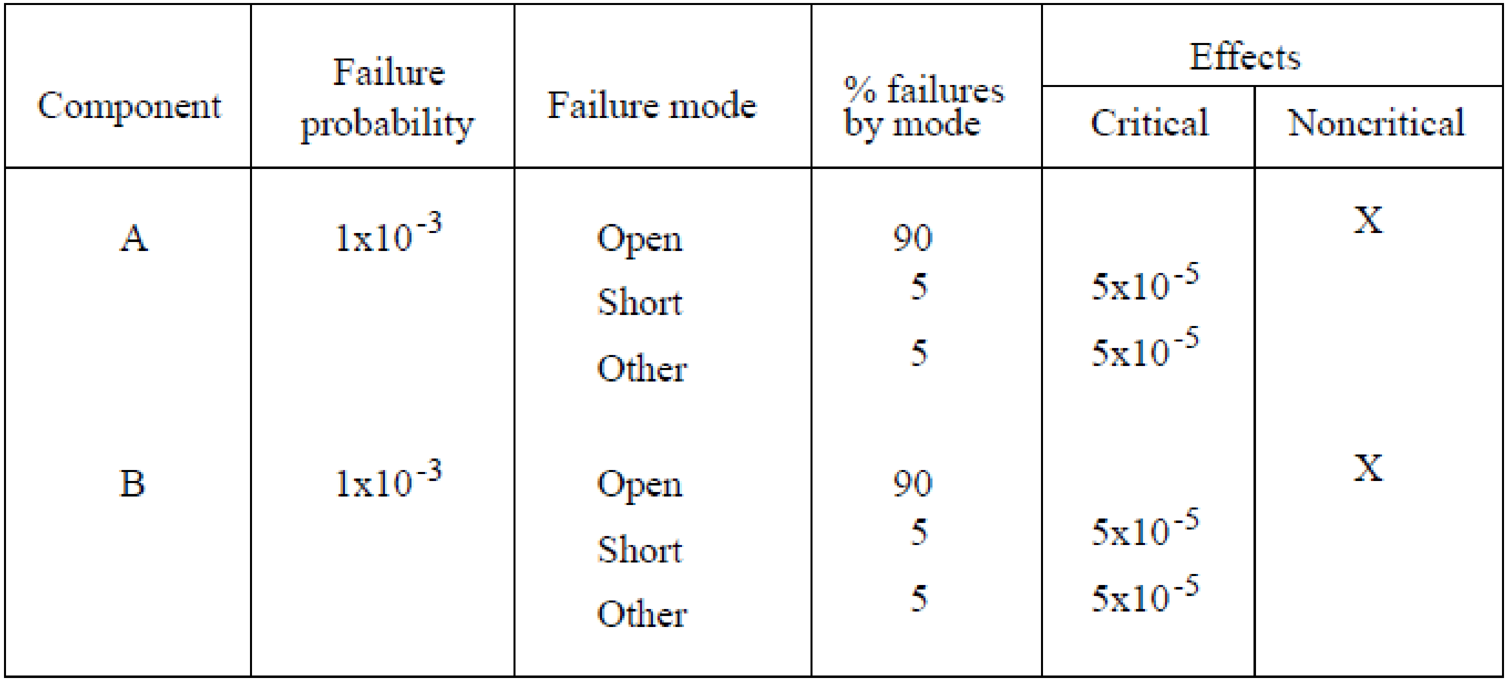


Component		Failure mode		Effects	
				Critical	Noncritical
A		Open			X
		Short		X	
		Other		X	
B		Open			X
		Short		X	
		Other		X	

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)

FMECA: A Forward Search Technique

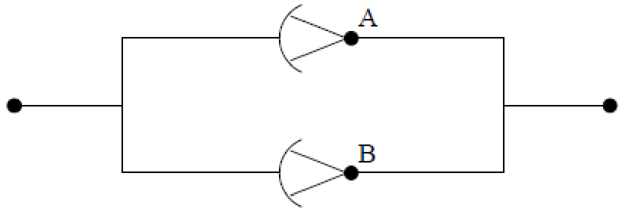


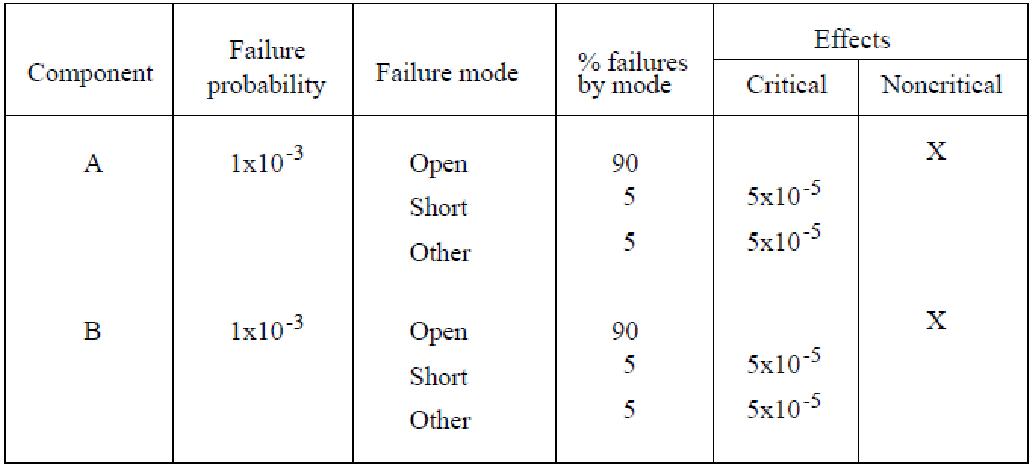


Component	Failure probability	Failure mode	% failures by mode	Effects	
				Critical	Noncritical
A	$1x10^{-3}$	Open	90		X
		Short	5	$5x10^{-5}$	
		Other	5	$5x10^{-5}$	
B	$1x10^{-3}$	Open	90		X
		Short	5	$5x10^{-5}$	
		Other	5	$5x10^{-5}$	

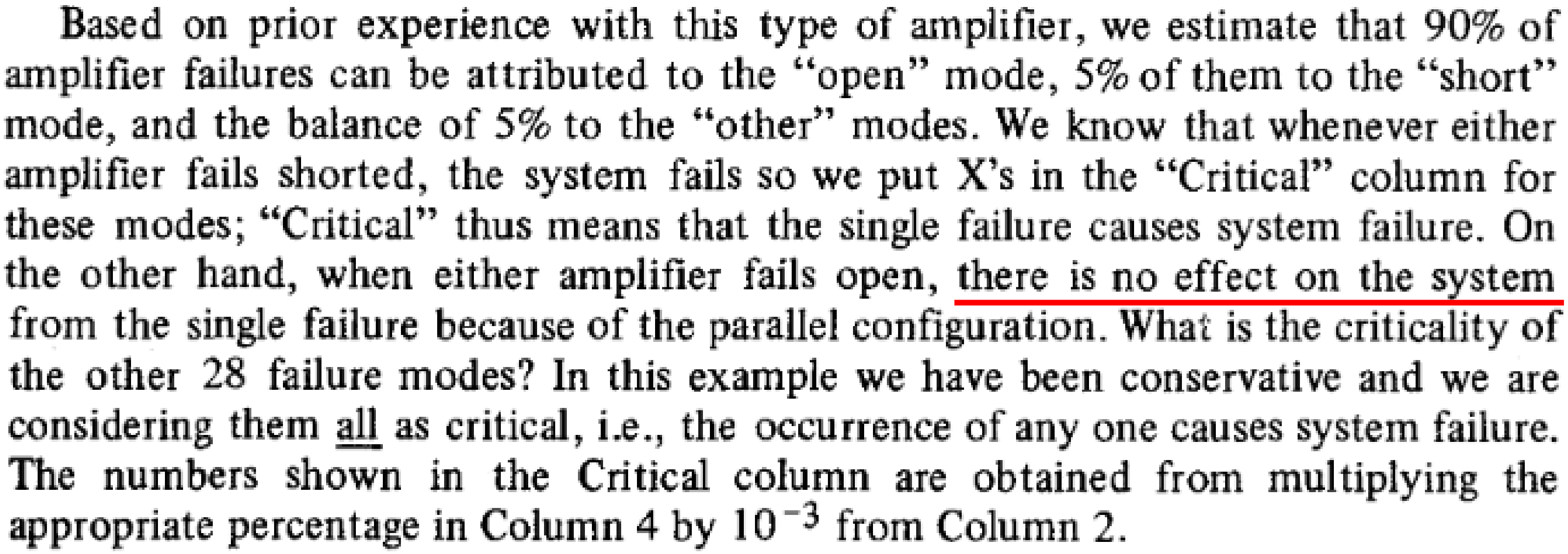
Figure 3: FMEA for a system of two amplifiers in parallel. (Source: W.E. Vesely, F.F. Goldberg, N.H. Roberts, and D.F. Haasl, *Fault Tree Handbook*, NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, D.C., 1981, page II-3)

FMECA: A Forward Search Technique



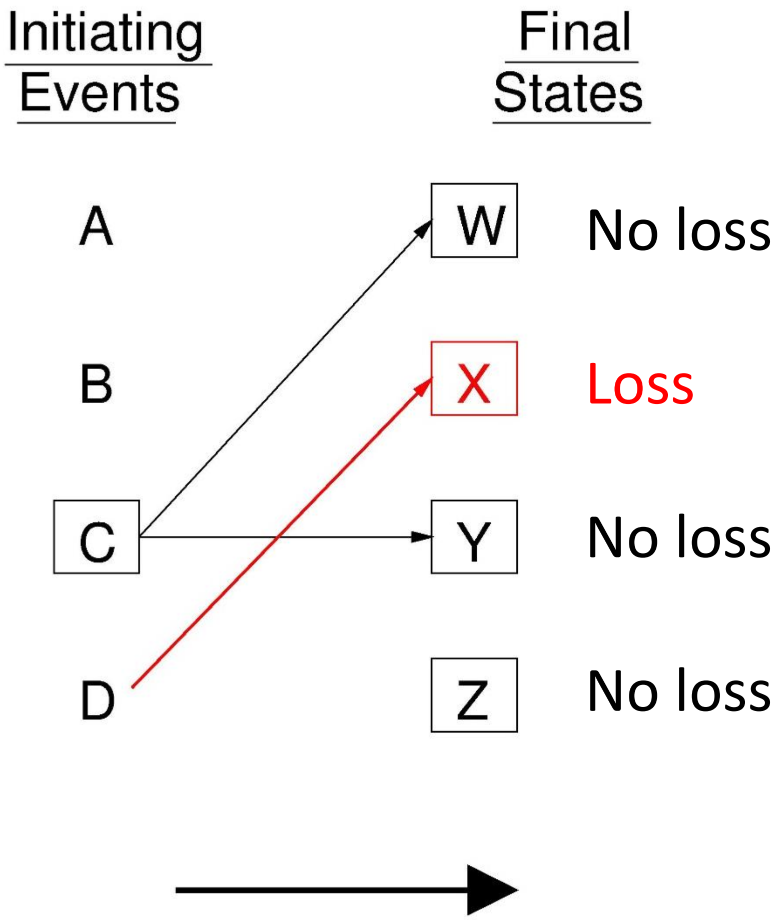


Component	Failure probability	Failure mode	% failures by mode	Effects	
				Critical	Noncritical
A	$1x10^{-3}$	Open	90		X
		Short	5	$5x10^{-5}$	
		Other	5	$5x10^{-5}$	
B	$1x10^{-3}$	Open	90		X
		Short	5	$5x10^{-5}$	
		Other	5	$5x10^{-5}$	



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.

Forward vs. Backward Search



Initiating Events

Final States

A

B

C

D

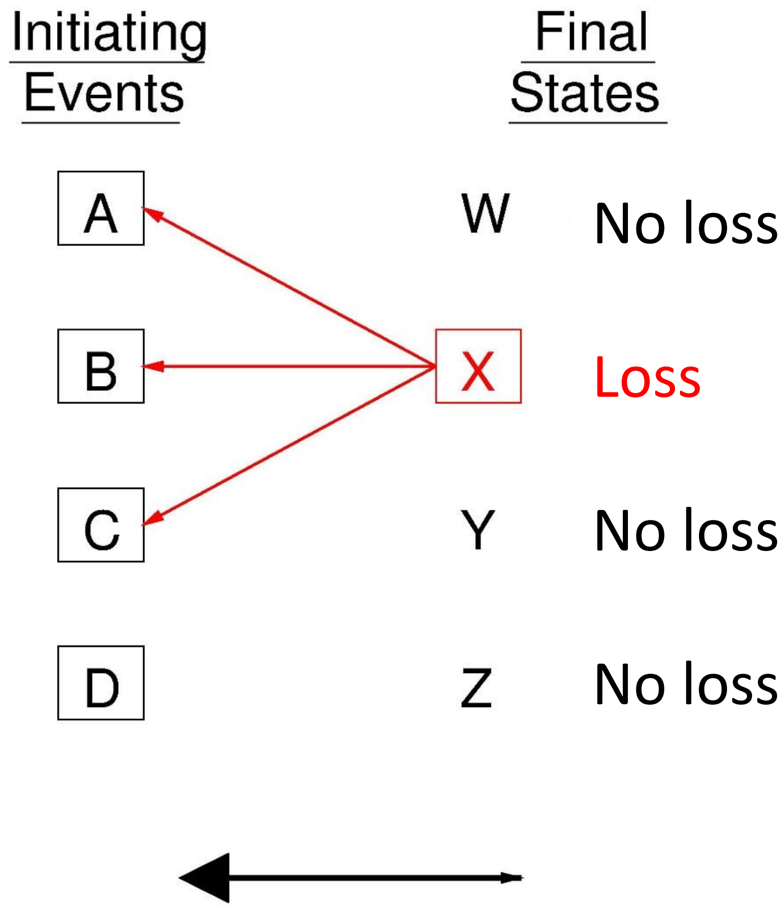
W No loss

X Loss

Y No loss

Z No loss

Forward Search



Initiating Events

Final States

A

B

C

D

W No loss

X Loss

Y No loss

Z No loss

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?

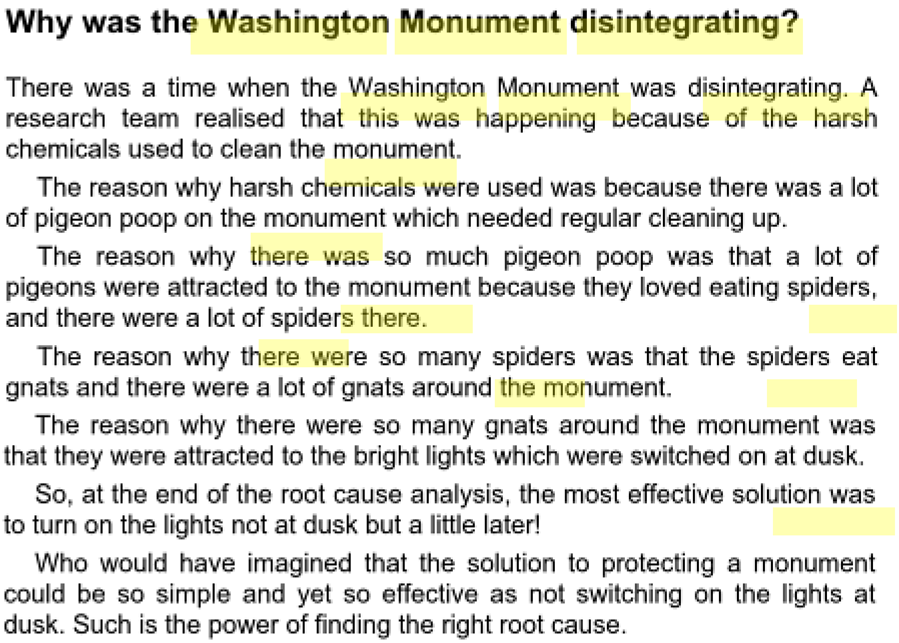
They eat gnats and lots of gnats at monument

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.

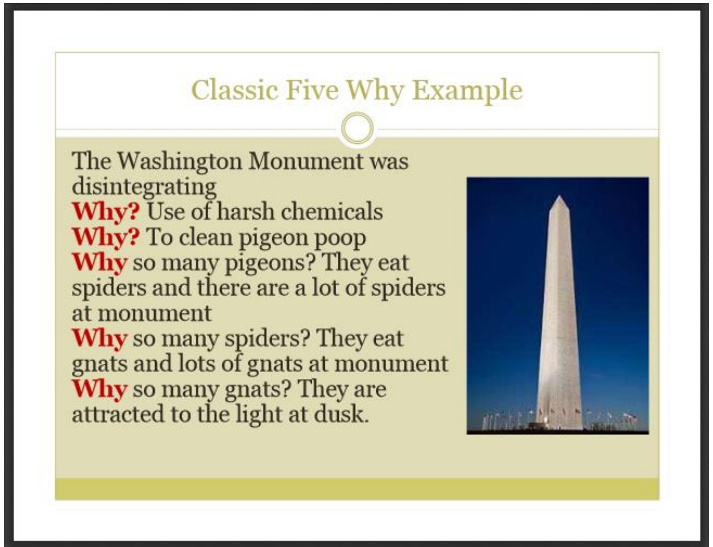
The reason why there was so much pigeon poop was that a lot of pigeons were attracted to the monument because they loved eating spiders, and there were a lot of spiders there.

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.

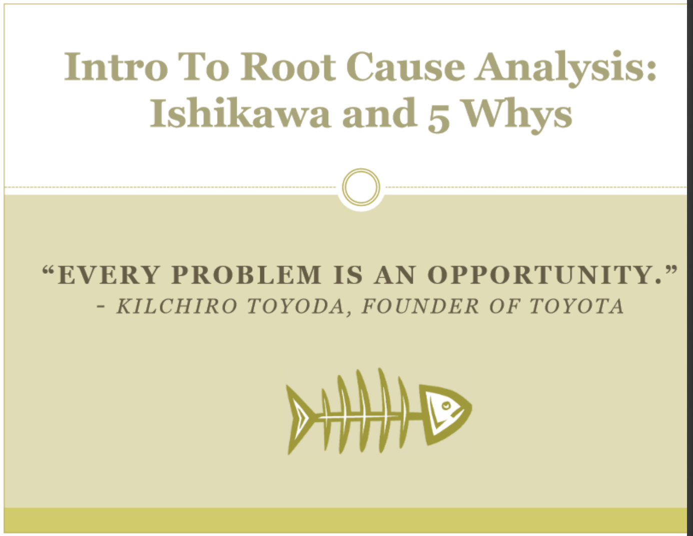
So, at the end of the root cause analysis, the most effective solution was to turn on the lights not at dusk but a little later!

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.



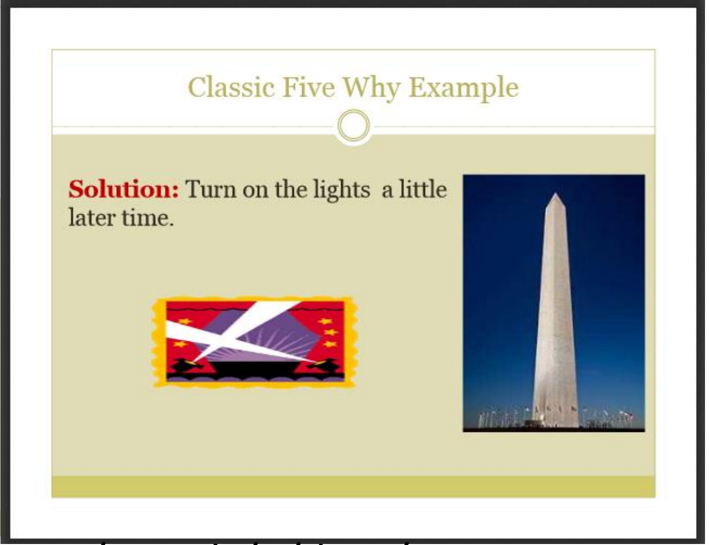
Classic Five Why Example

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



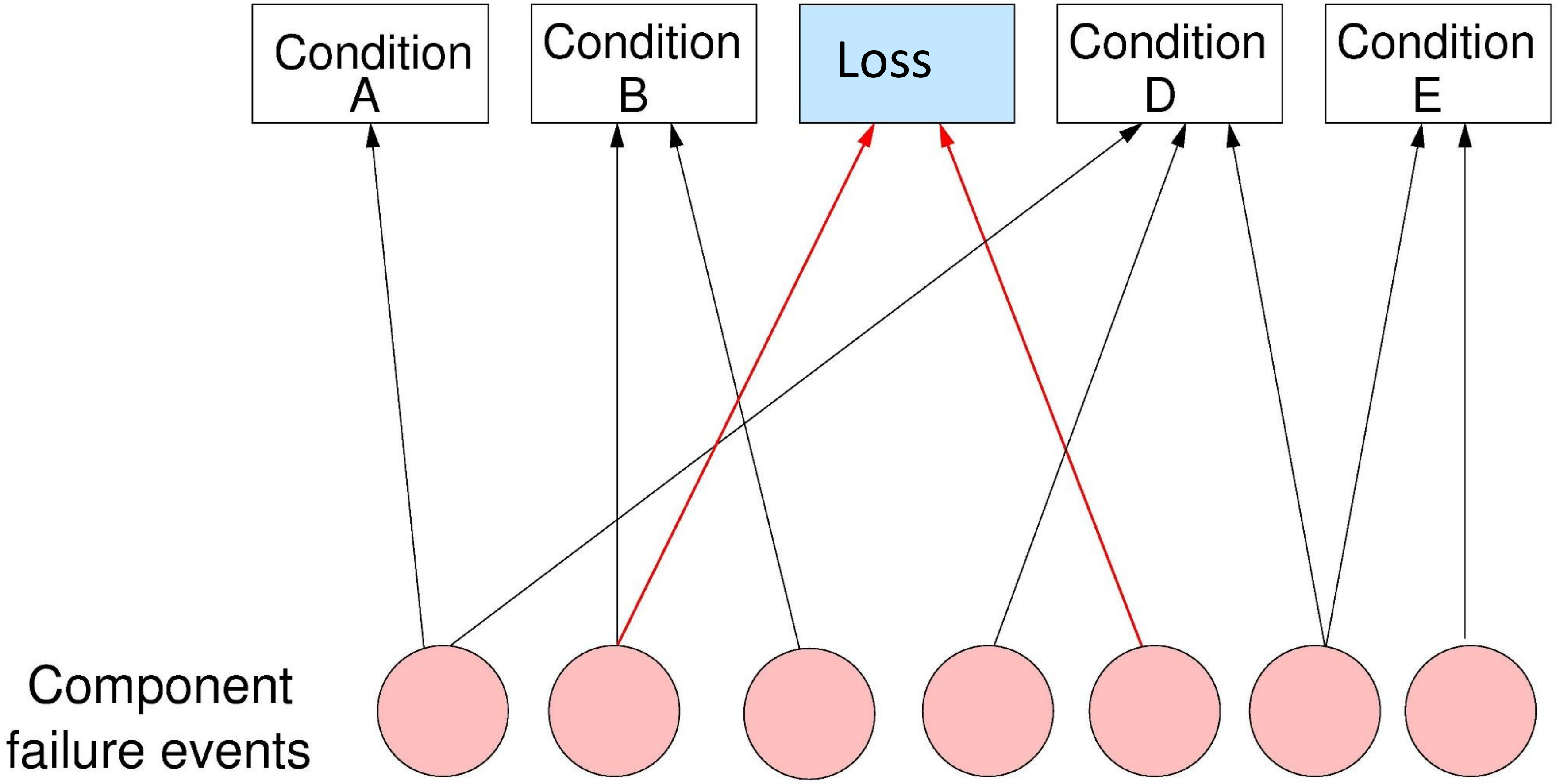
Classic Five Why Example

Solution: Turn on the lights a little later time.

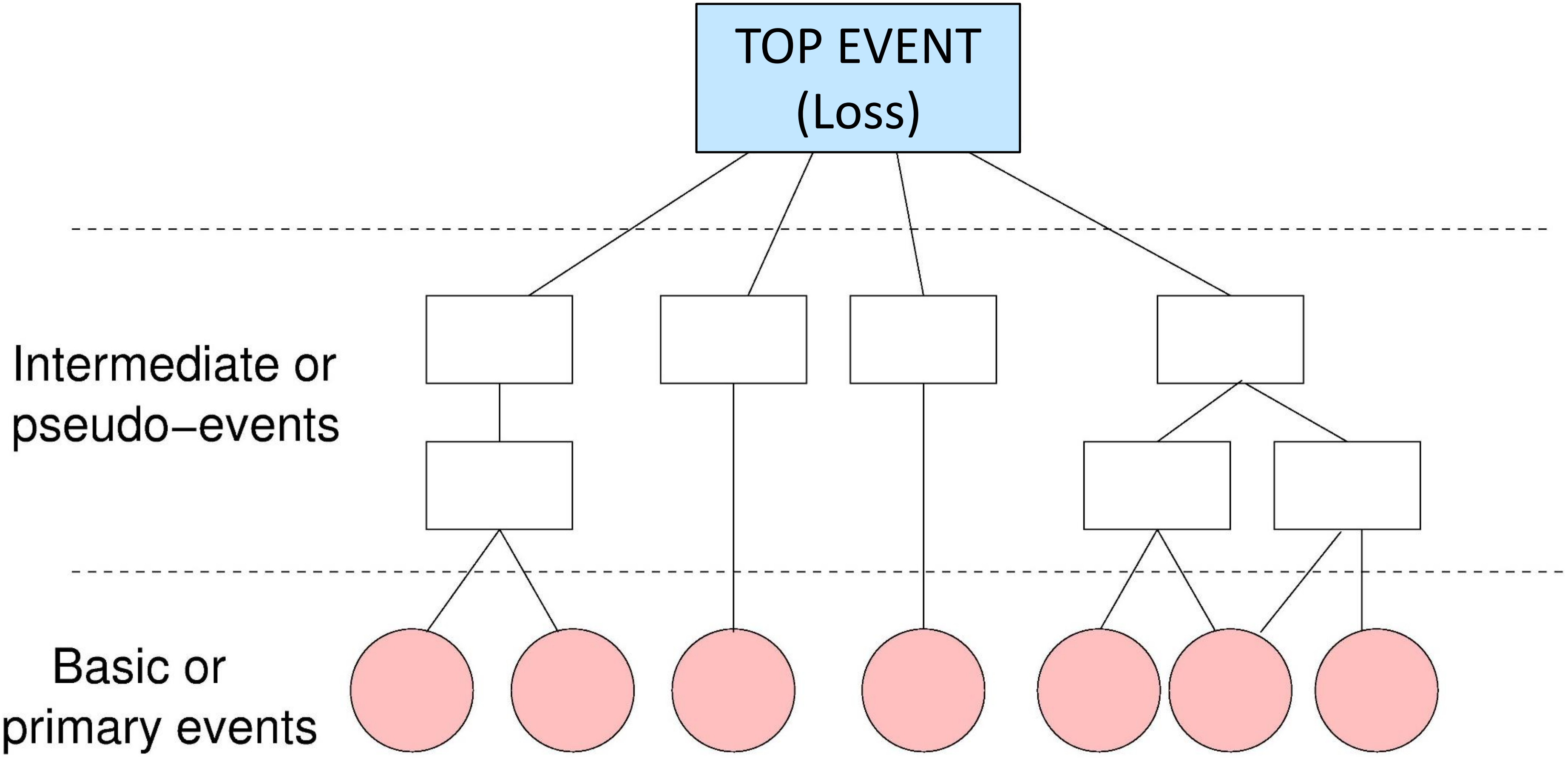
"Breaking the accident chain of events" (see video)

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

Bottom-Up Search



Top-Down Search



Top-Down Example

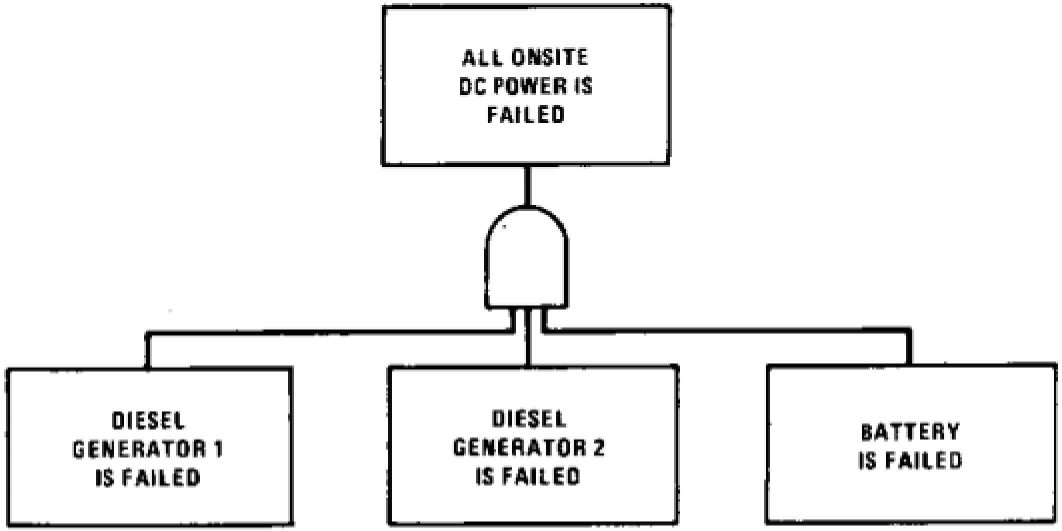
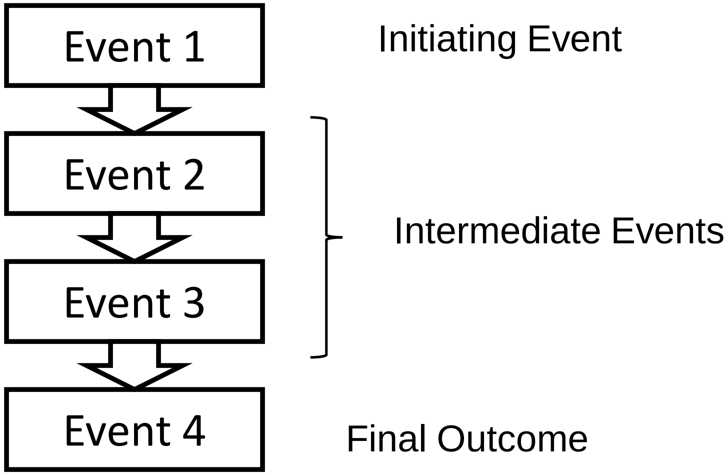

ALL ONSITE DC POWER IS FAILED
DIESEL GENERATOR 1 IS FAILED
DIESEL GENERATOR 2 IS FAILED
BATTERY IS FAILED

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

Event 2

Event 3

Event 4

Initiating Event

Intermediate Events

Final Outcome

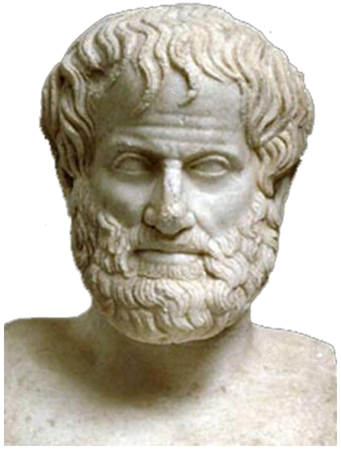
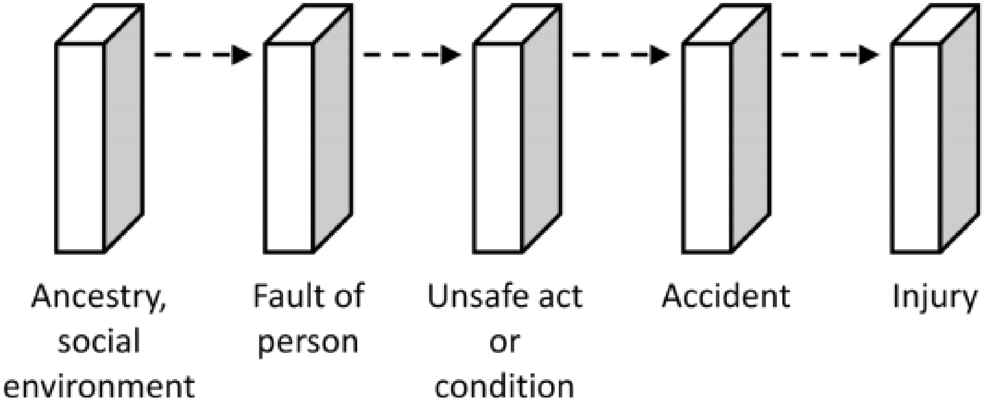


Image from: http://en.wikipedia.org/wiki/File:Aristotle_Bust_White_Background_Transparent.png
Quote from: http://plato.stanford.edu/entries/aristotle-natphil/

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

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

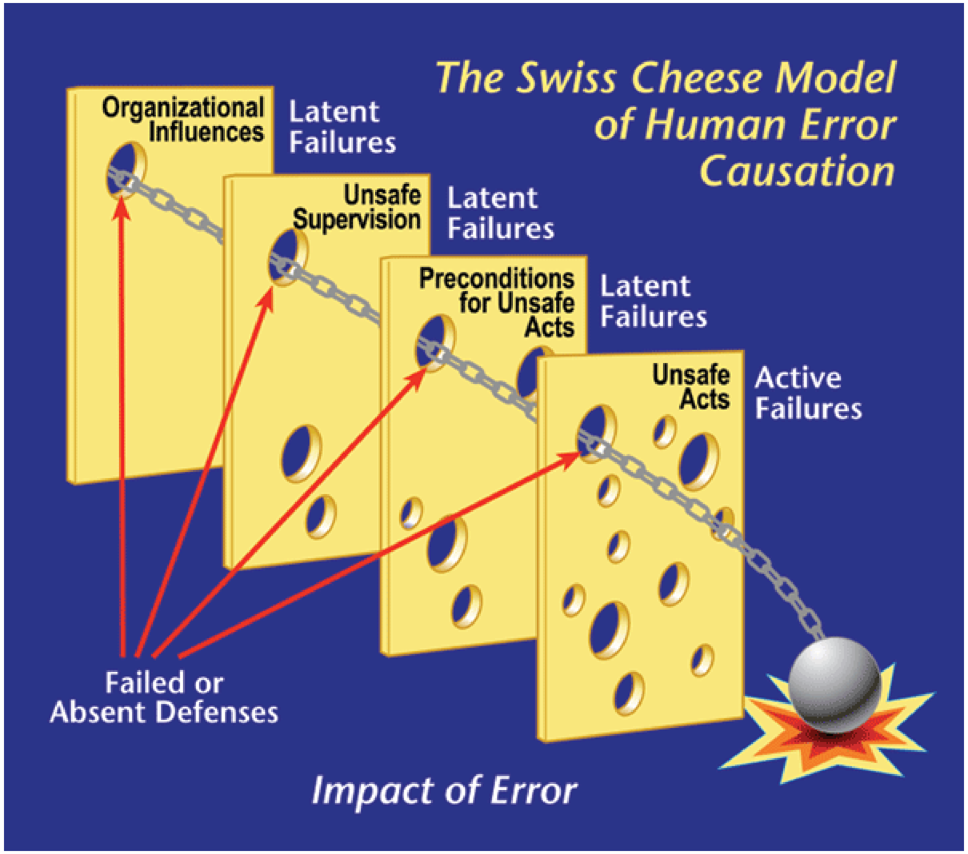

The Swiss Cheese Model of Human Error Causation
Organizational Influences
Latent Failures
Unsafe Supervision
Latent Failures
Preconditions for Unsafe Acts
Latent Failures
Unsafe Acts
Active Failures
Failed or Absent Defenses
Impact of Error

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.

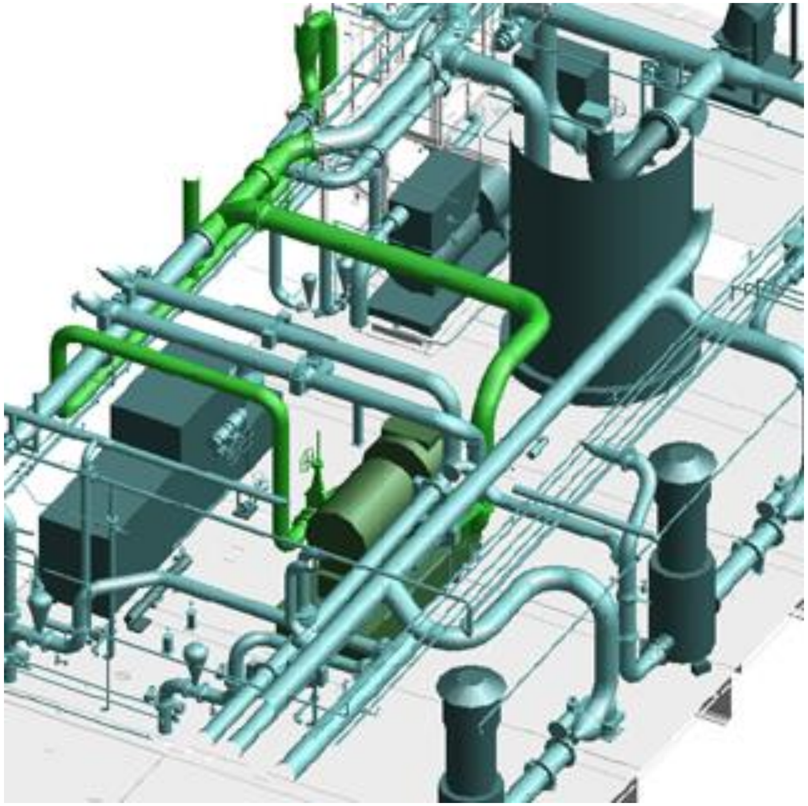


Image from: http://www.akersolutions.com/en/Global-menu/Products-and-Services/Maintenance-modifications-and-operations/Technology-services/Hazard-and-operability-analysis-HAZOP/

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

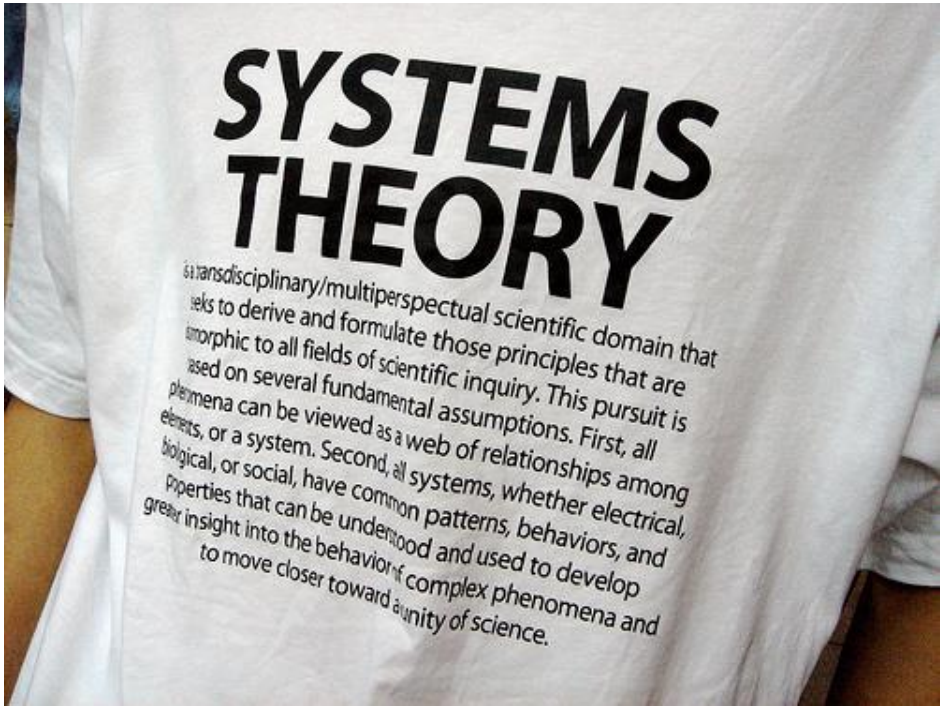

SYSTEMS
THEORY
is a transdisciplinary/multiperspectual scientific domain that
seeks to derive and formulate those principles that are
isomorphic to all fields of scientific inquiry. This pursuit is
based on several fundamental assumptions. First, all
phenomena can be viewed as a web of relationships 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

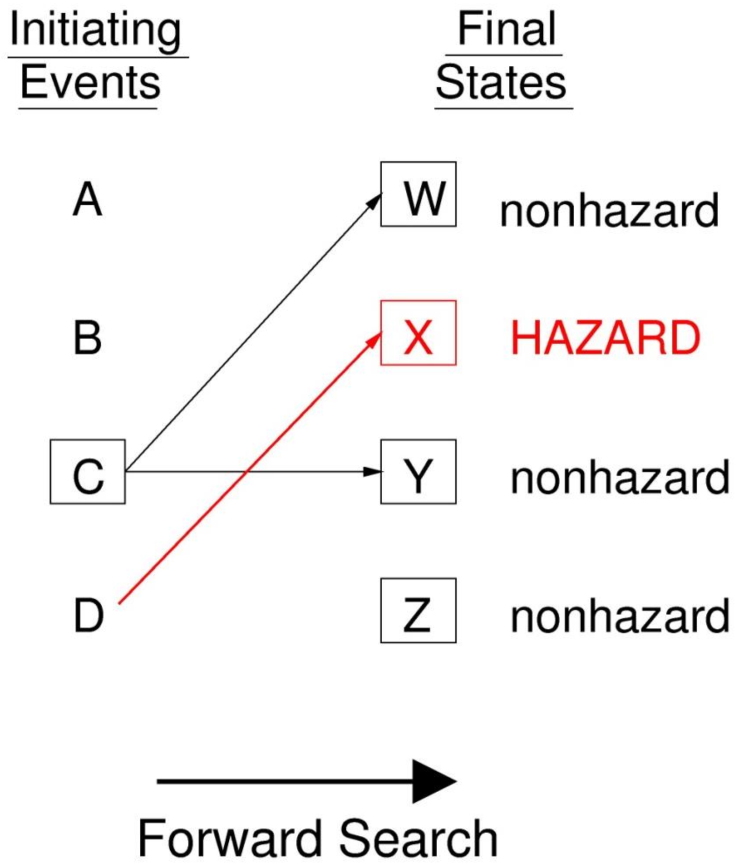
- ✓ Intro to reliability and system risk
- ✓ Overview of analysis techniques
- ➡ Traditional qualitative techniques
  - Failure Modes and Effects Analysis
  - Fault Tree Analysis
  - Event Tree Analysis
  - HAZOP
- Traditional quantitative techniques
  - Quant. Fault Tree Analysis
  - FMECA
  - Quant.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

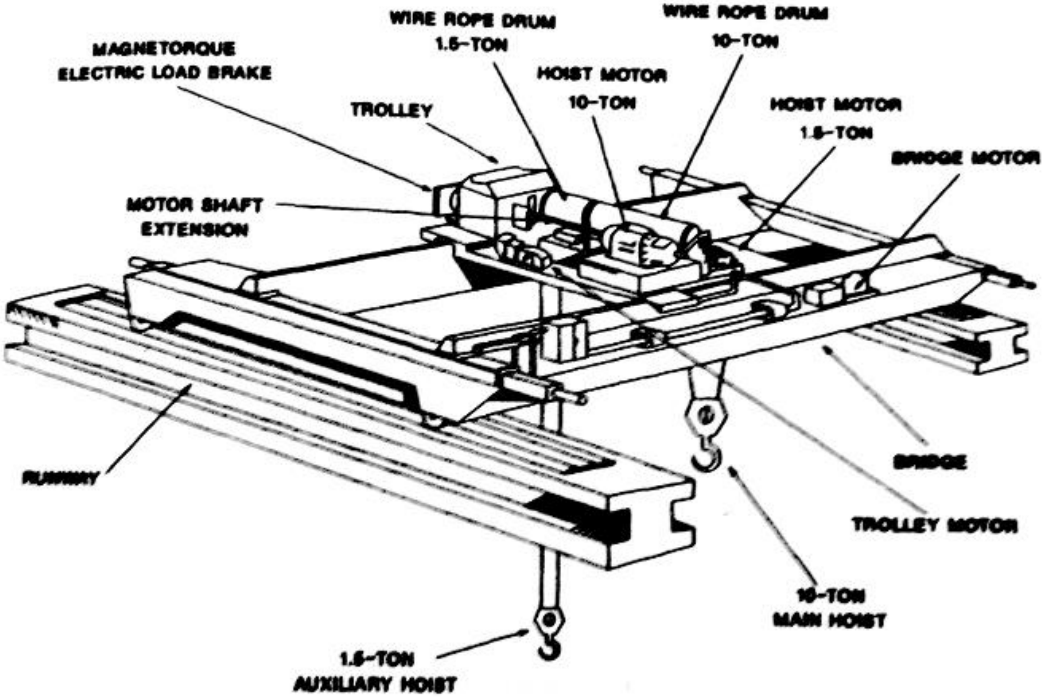


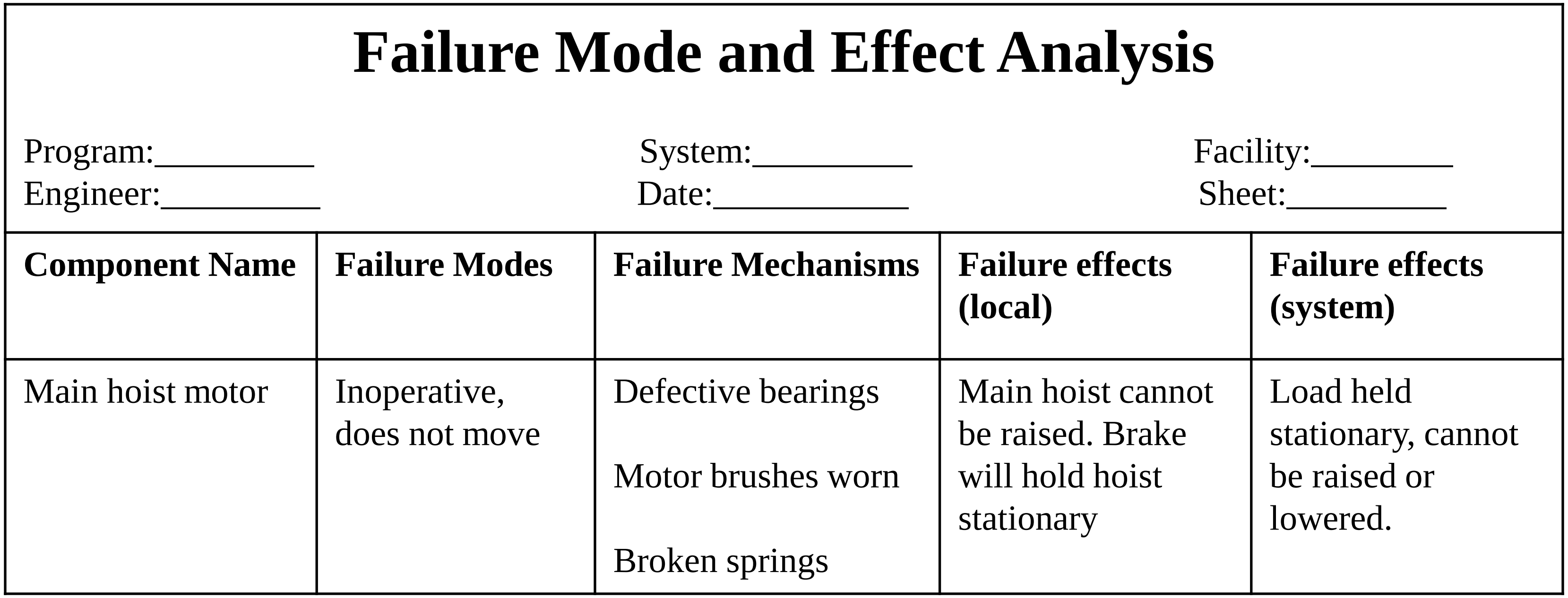
General FMEA Process

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

FMEA worksheet

Example: Bridge crane system





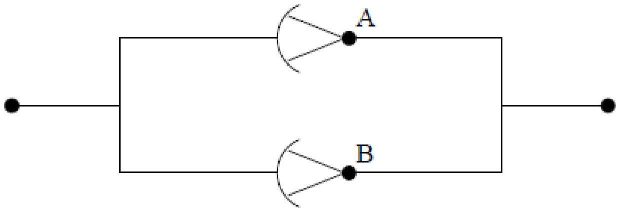
Failure Mode and Effect Analysis

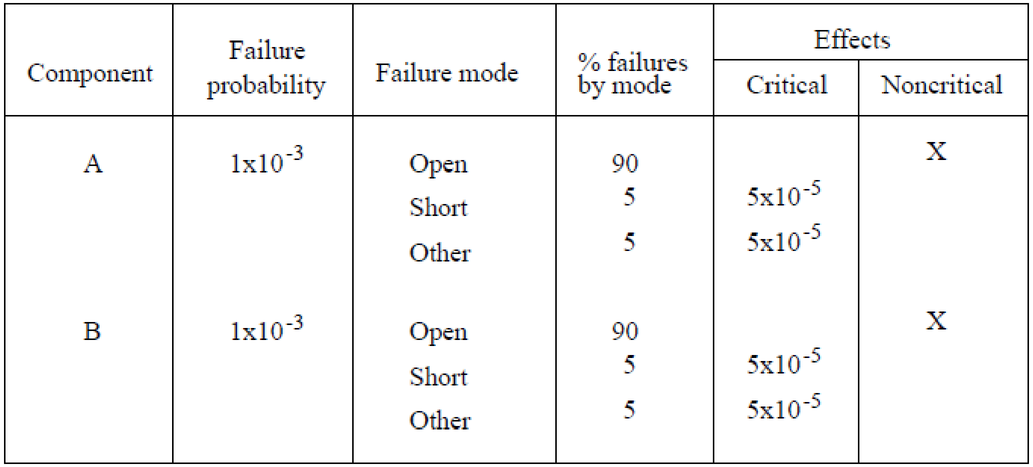
Program:_________ System:_________ Facility:________
Engineer:_________ Date:___________ Sheet:_________

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.

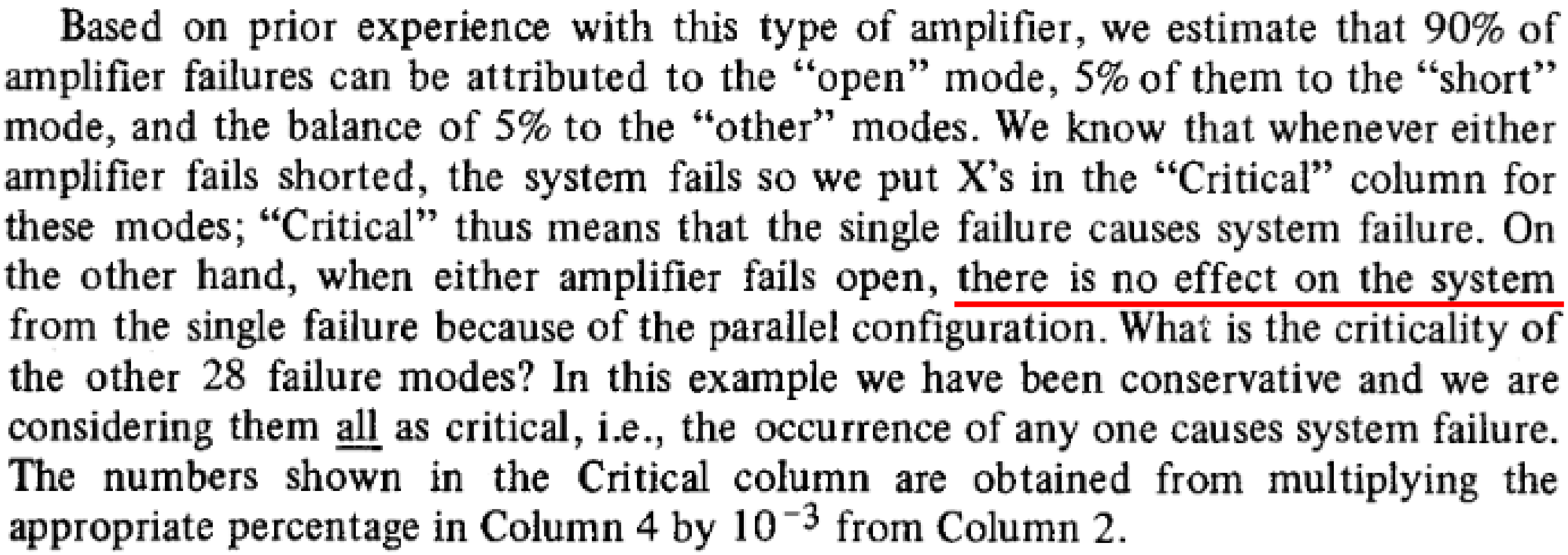
*FMEA example adapted from (Vincoli, 2006)

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

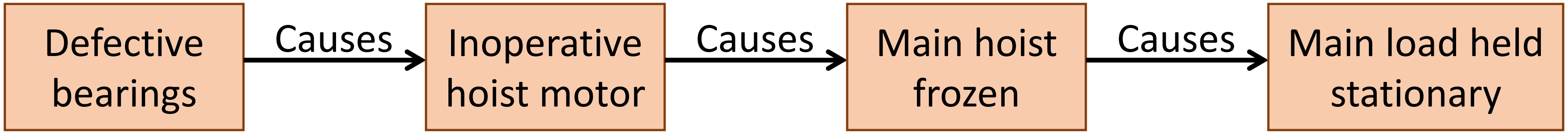
FMEA method:

Failure Mode and Effect Analysis

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

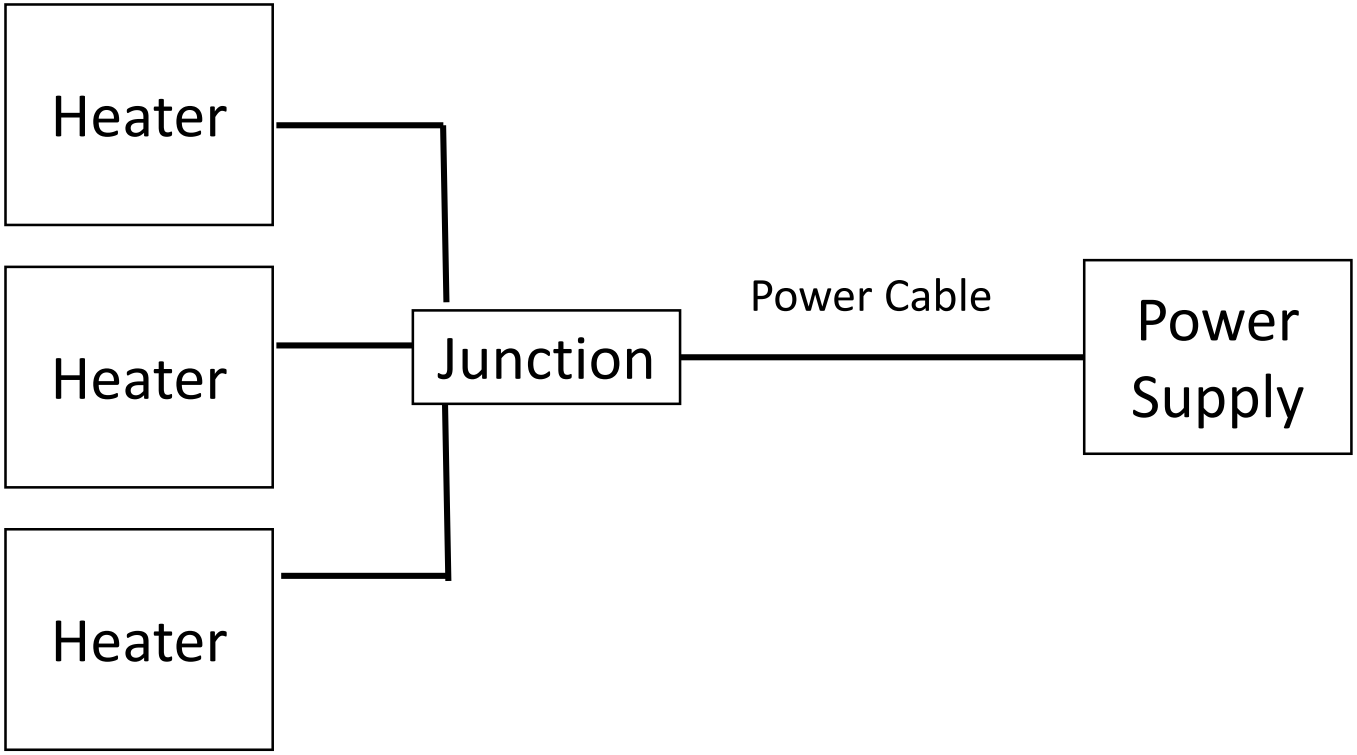
Component Name	Failure Modes	Failure Mechanisms	Failure effects (local)	Failure effects (system)
Main Hoist Motor	Inoperative, does not move	Defective bearings Loss of power Broken springs	Main hoist cannot be raised. Brake will hold hoist stationary	Load held stationary, cannot be raised or lowered.

Accident model: Chain-of-events

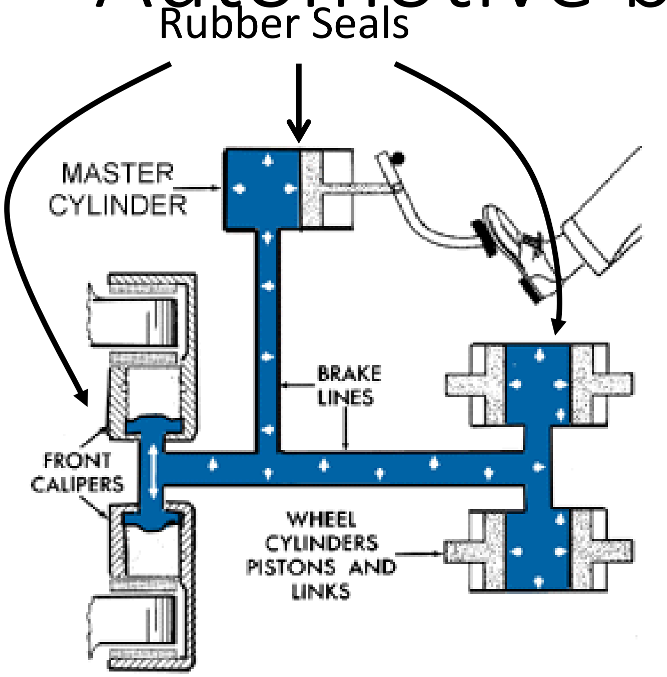


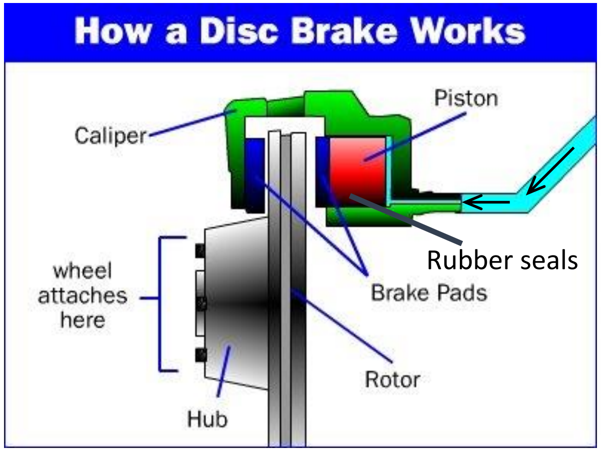
*FMEA example adapted from (Vincoli, 2006)

Real example:
LHC ATLAS Return Heaters



FMEA Exercise Automotive brakes





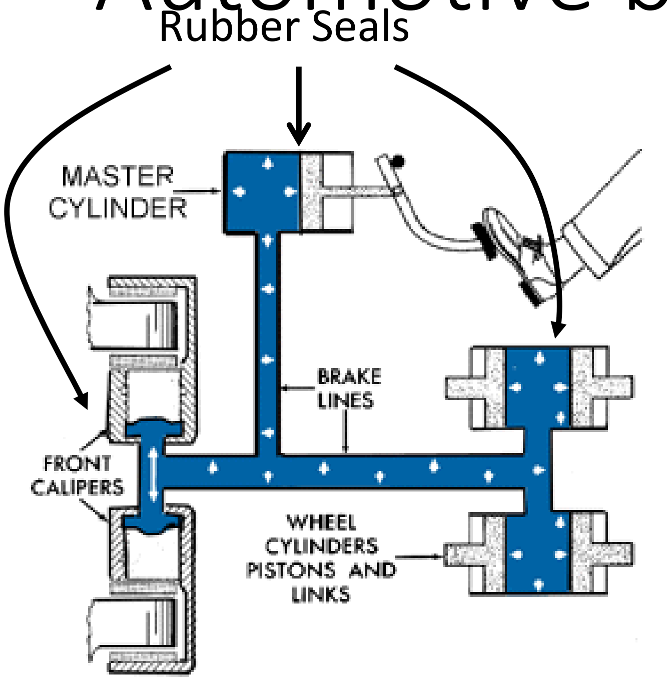
System components

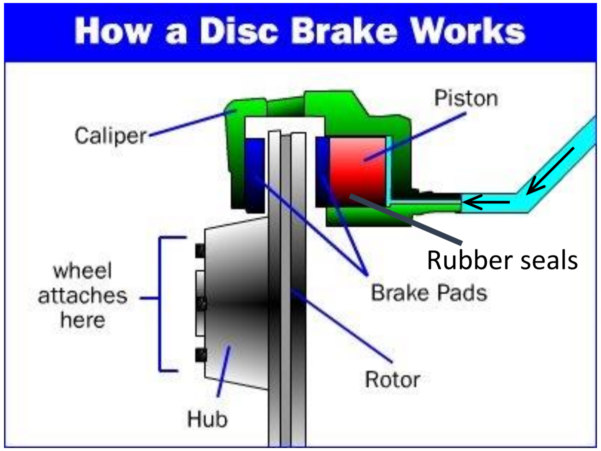
- Brake pedal
- Brake lines
- Rubber seals
- Master cylinder
- Brake pads

FMEA worksheet columns

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

FMEA Exercise
Automotive brakes





System components

- Brake pedal

How would you make this system safe?

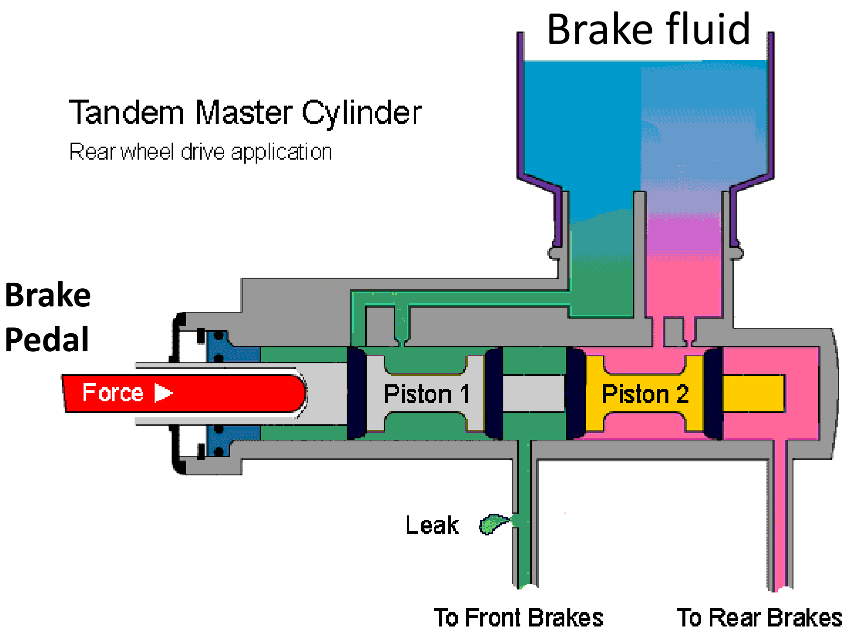
- Brake pads

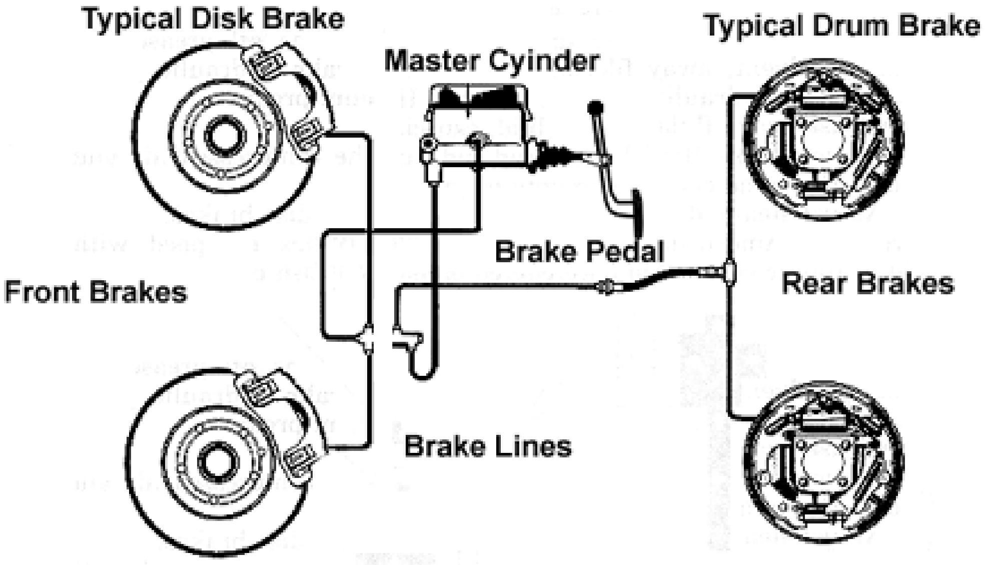
FMEA worksheet columns

– Component

– Failure effect (system)

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

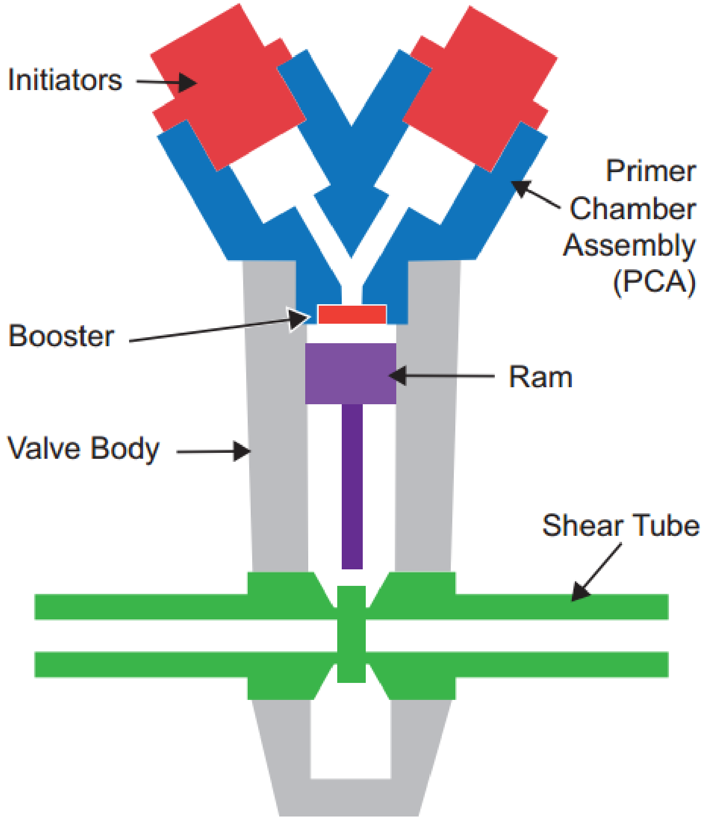
- Freedom from undesired losses (e.g. loss of life, loss of mission, environmental damage, customer satisfaction, etc.)

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
  - Limits 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



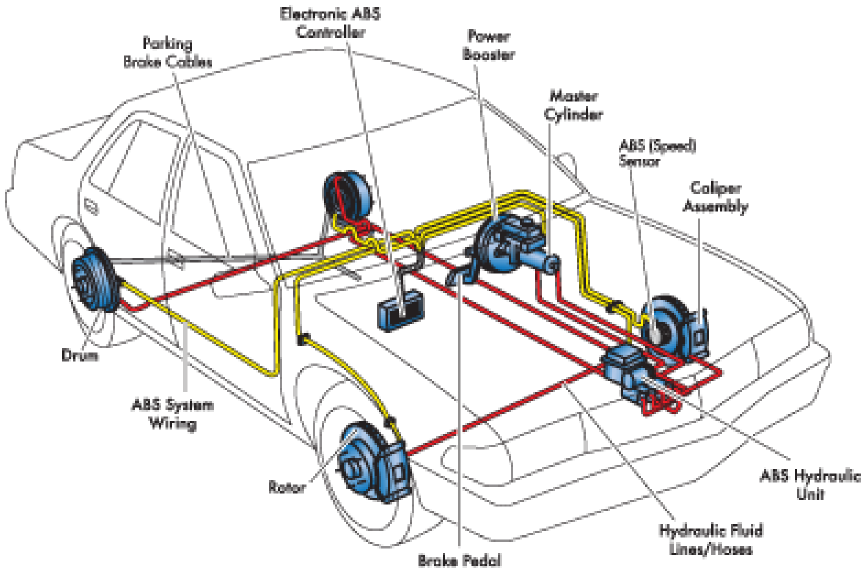
A normally closed pyrovalve

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?

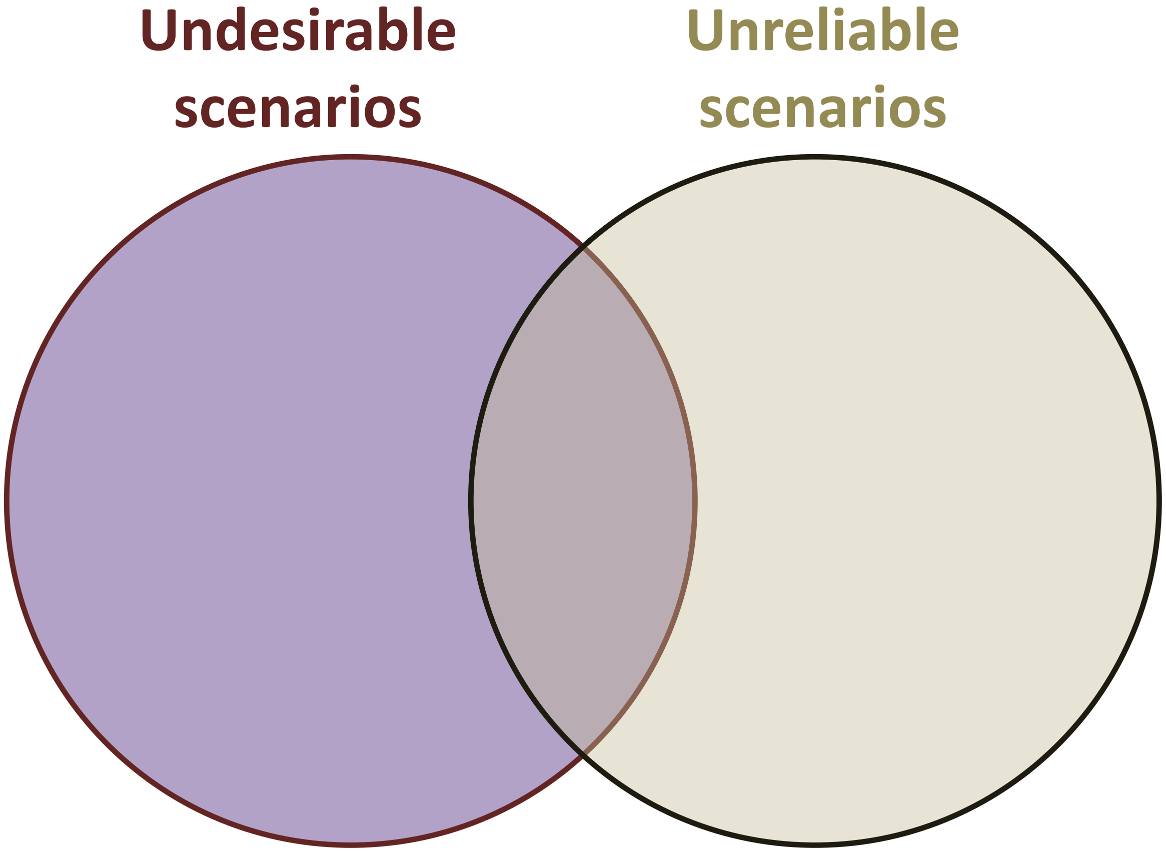
*Image from midas.com

Safety vs. reliability

Reliability ←→ Failures } Component property

Safety ←→ Incidents } System property

Safety vs. Reliability



Undesirable scenarios

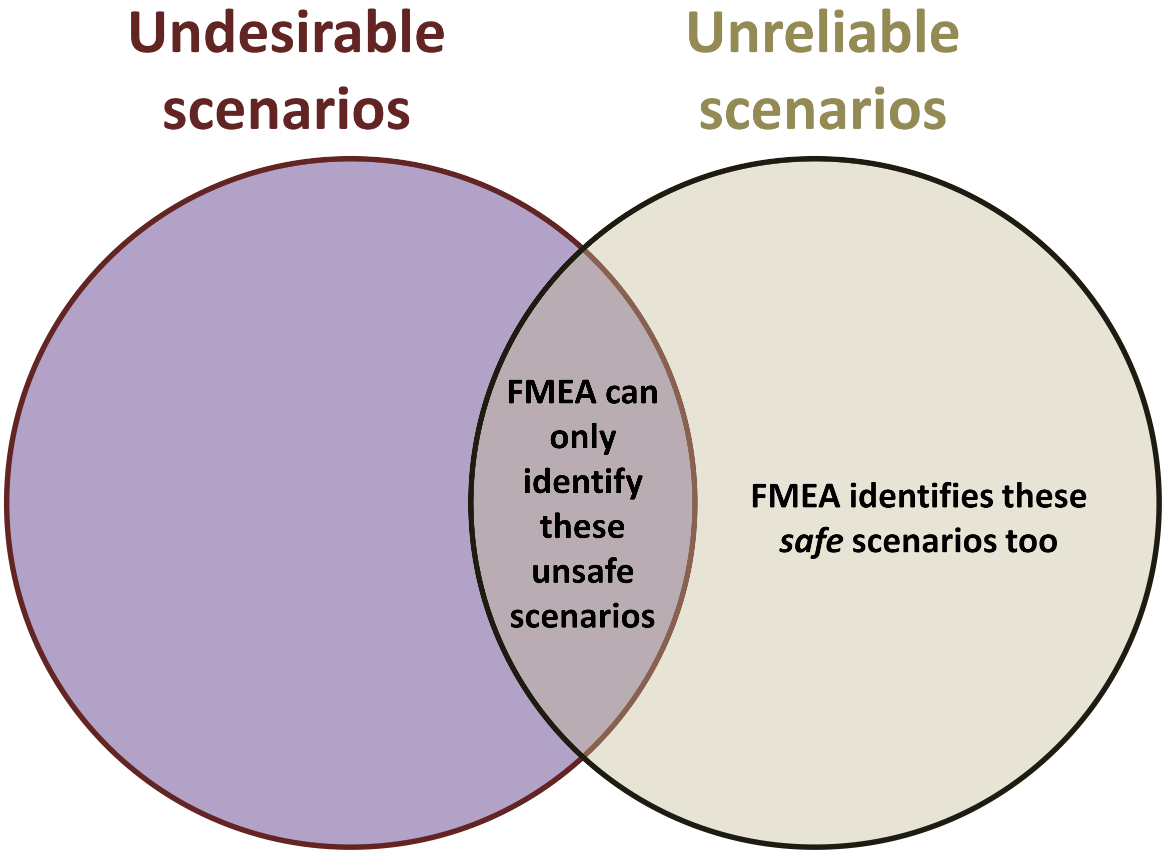
Unreliable scenarios

Safe ≠ Reliable

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

	Safe	**Unsafe**
Reliable	•Typical commercial flight	•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

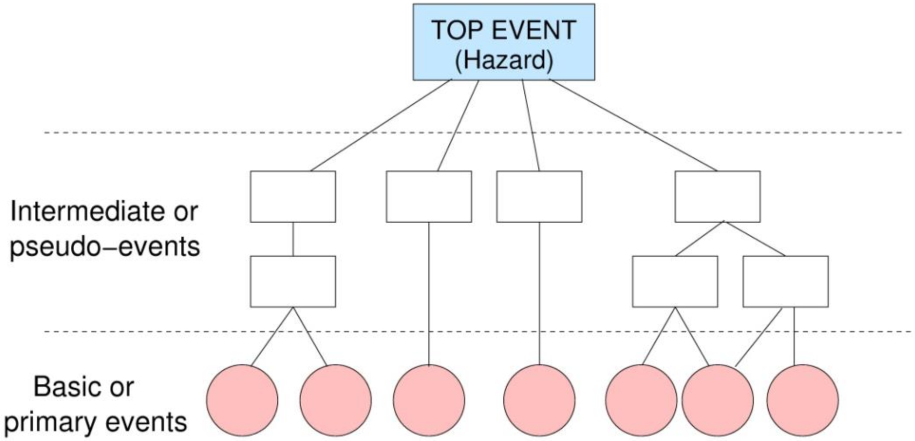

Undesirable scenarios
Unreliable scenarios
FMEA can only identify these unsafe scenarios
FMEA identifies these *safe* scenarios too

- 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

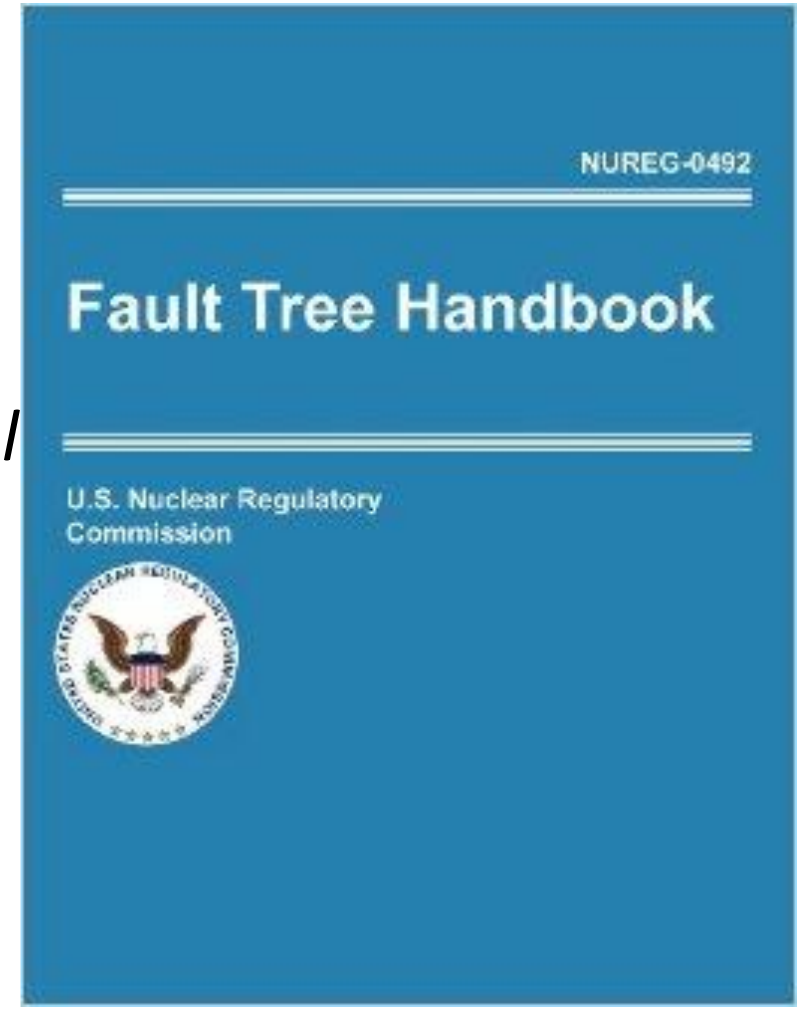
- 1961: Bell labs analysis of Minuteman missile system
- Today one of the most popular hazard analysis techniques
- Top-down search method
  - Top event: undesirable event
  - Goal is to identify causes of hazardous event



© Copyright 2014 John Thomas

FTA Process

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



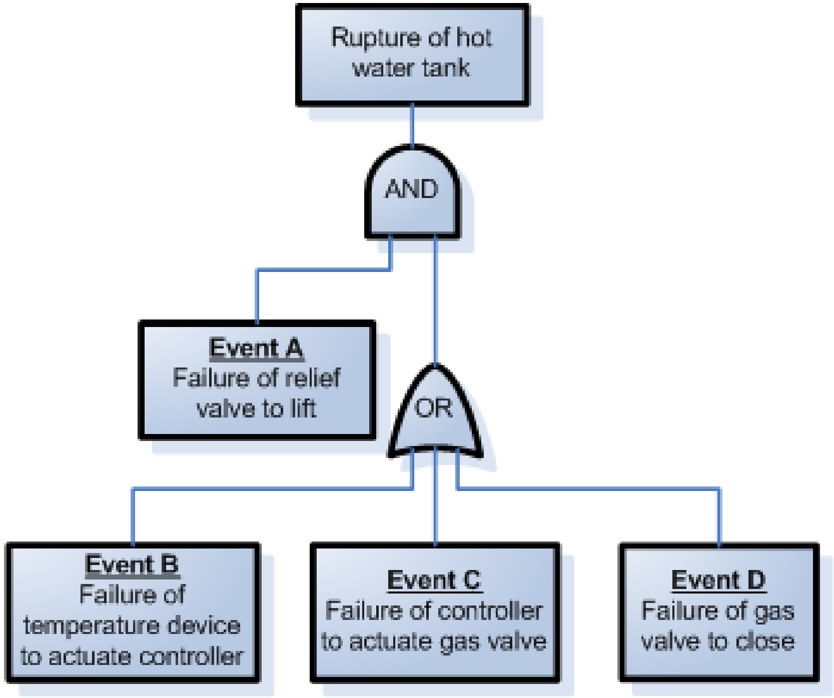
NUREG-0492

Fault Tree Handbook

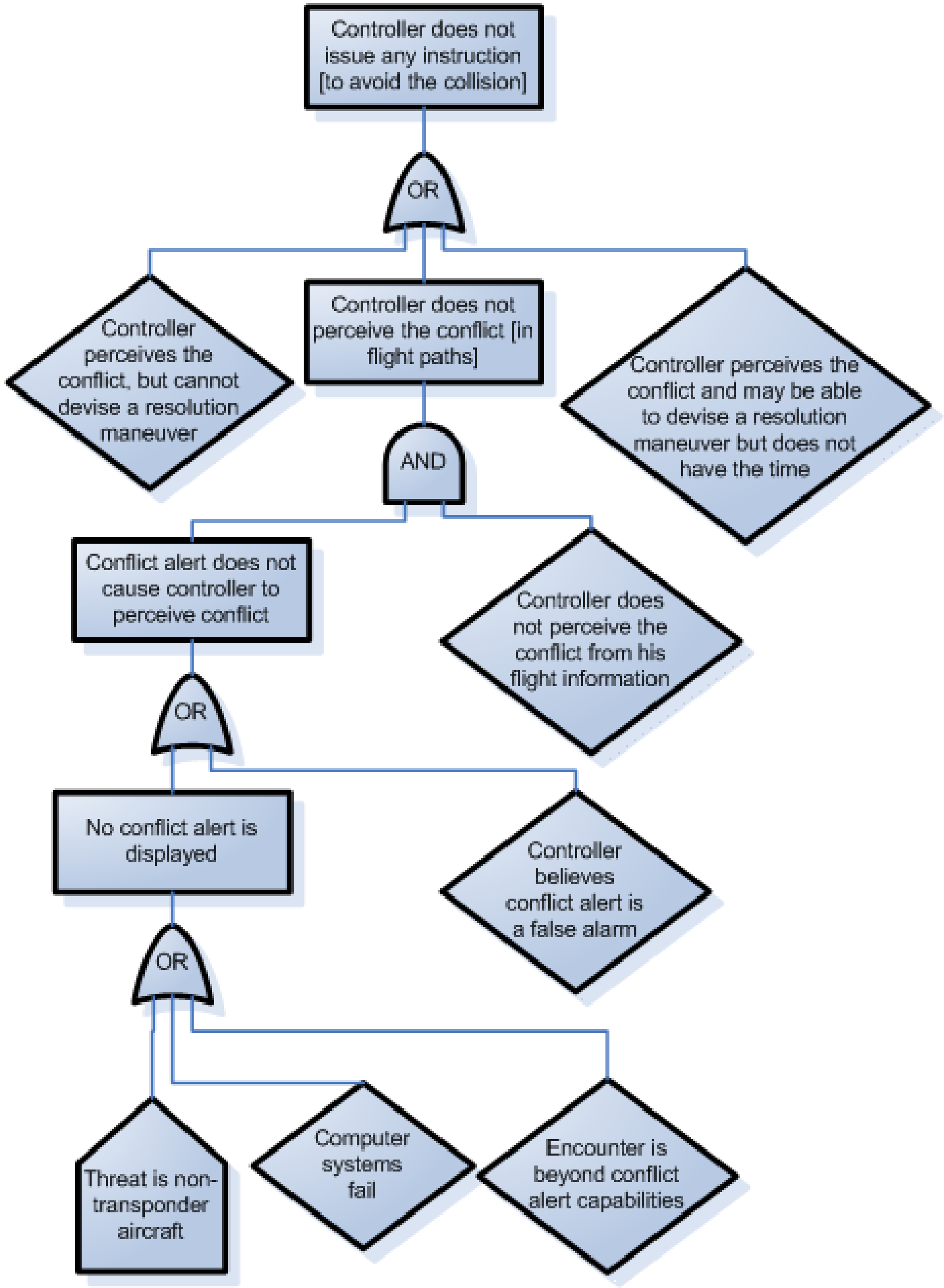
U.S. Nuclear Regulatory Commission

Vesely

Fault tree examples

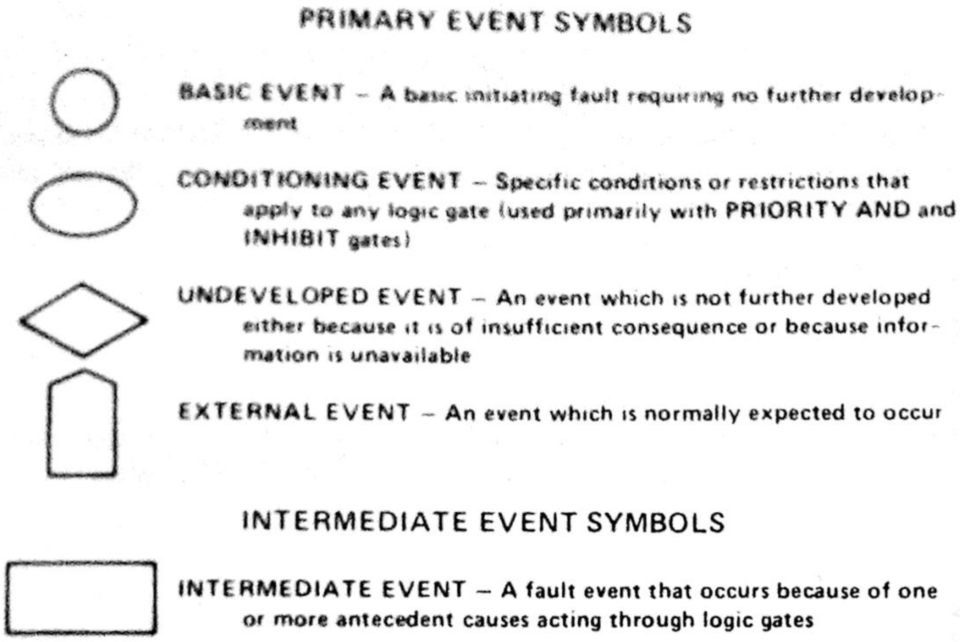

Rupture of hot water tank
AND
Event A Failure of relief valve to lift
OR
Event B Failure of temperature device to actuate controller
Event C Failure of controller to actuate gas valve
Event D Failure of gas valve to close

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

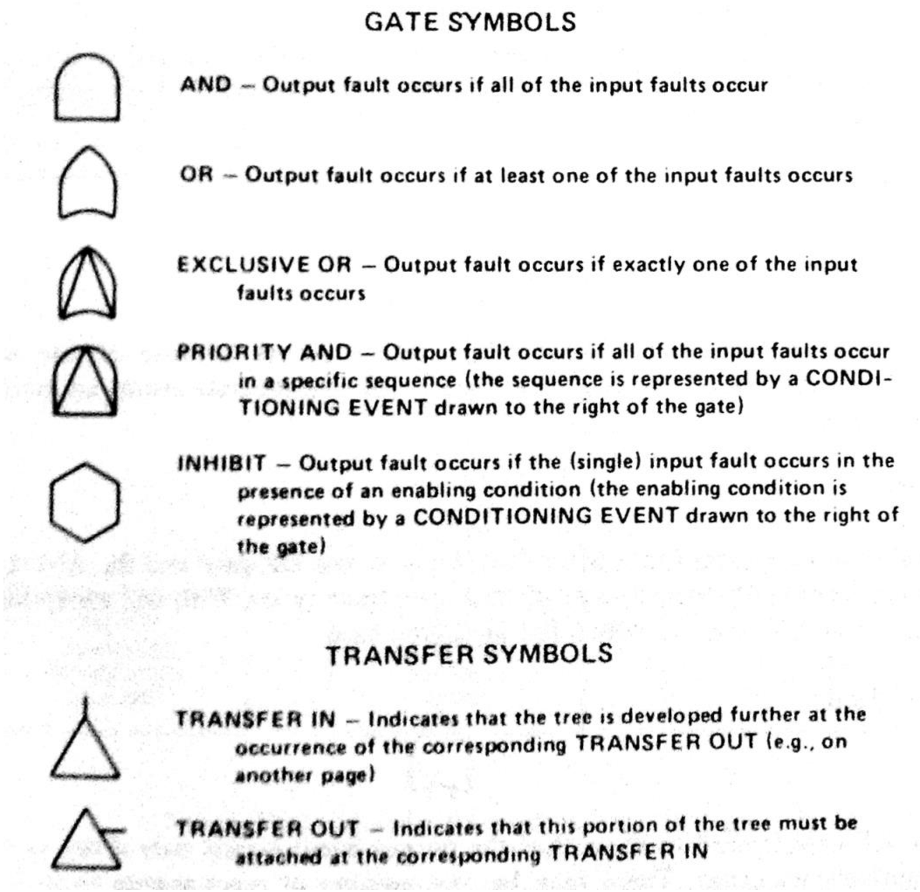
CONDITIONING EVENT – Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)

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)

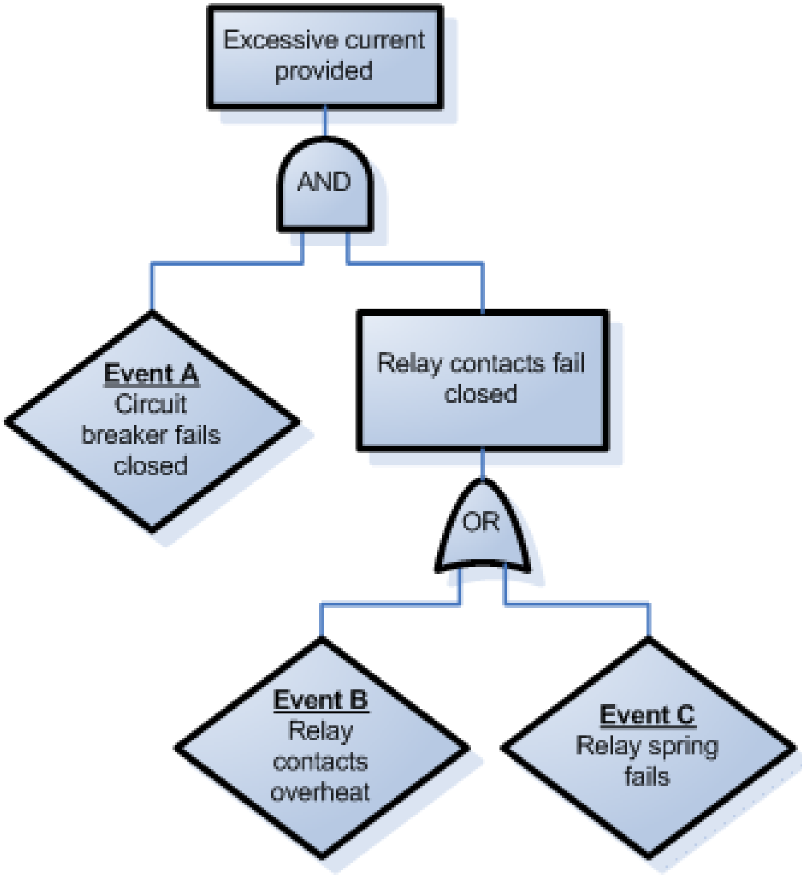
TRANSFER OUT – Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

From NUREG-0492 (Vesely, 1981)

Fault Tree cut-sets

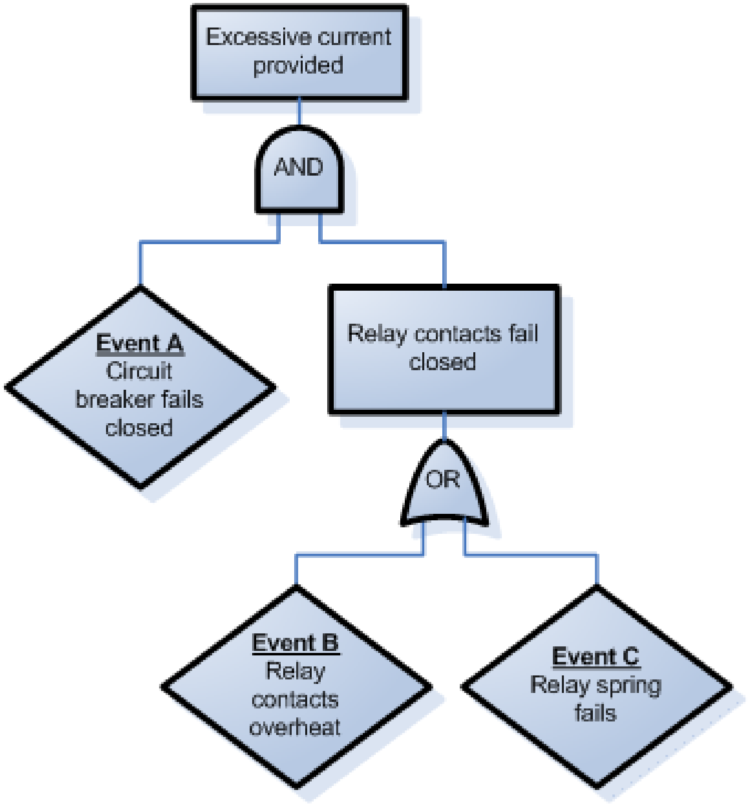
- *Cut-set*: combination of basic events (leaf nodes) sufficient to cause the top-level event
  - Ex: (A and B and C)

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

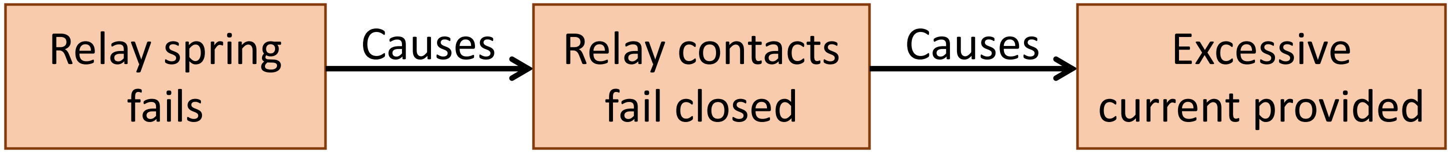

Excessive current provided
AND
Event A
Circuit breaker fails closed
Relay contacts fail closed
OR
Event B
Relay contacts overheat
Event C
Relay spring fails

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



Fault Tree Exercise

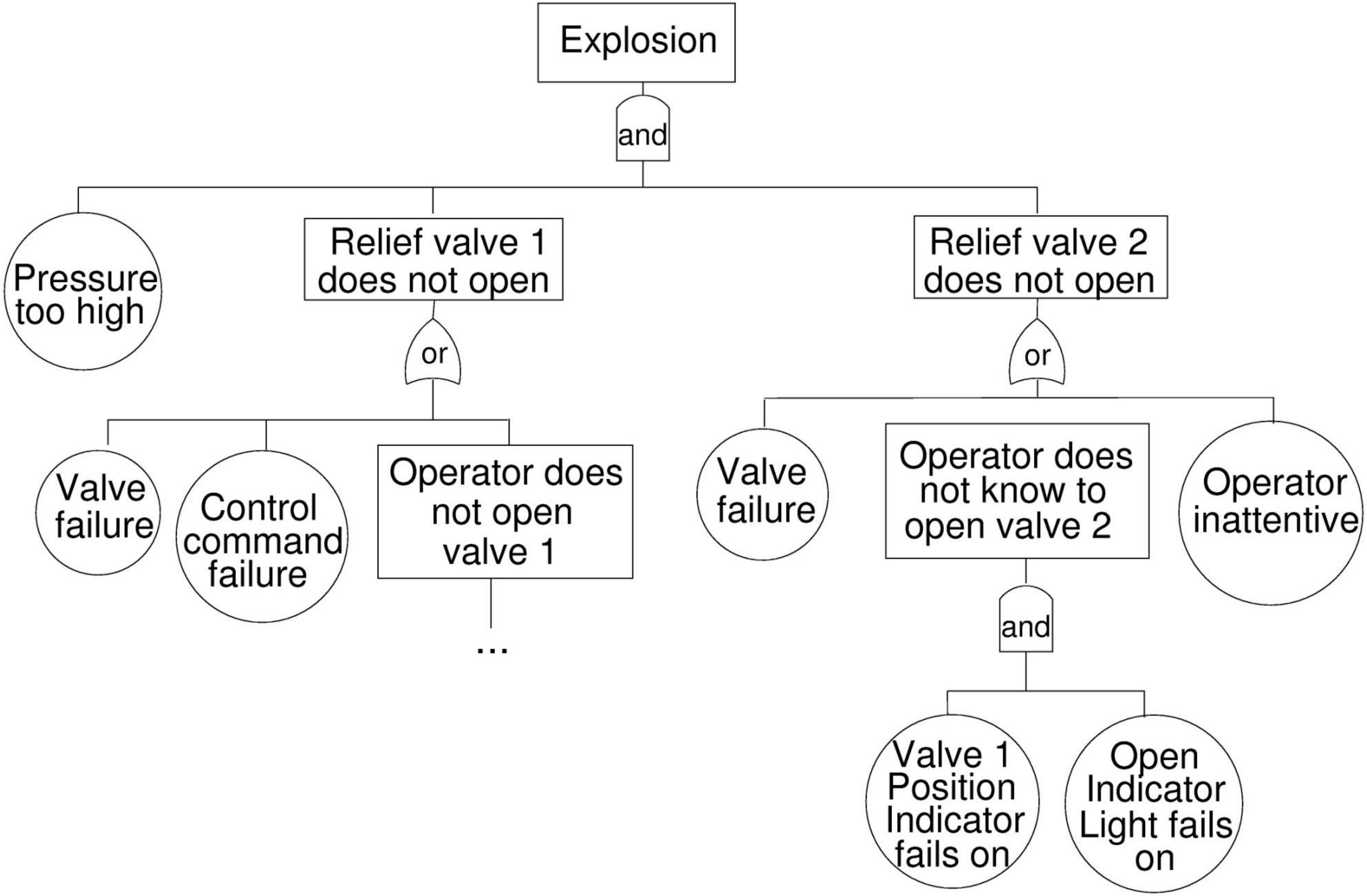
- **Hazard**: Toxic chemical released
- **Design**:

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 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 "Aircraft unable to stop upon landing".

Top event: Reverse thrusters fail to 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

2012 accident

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

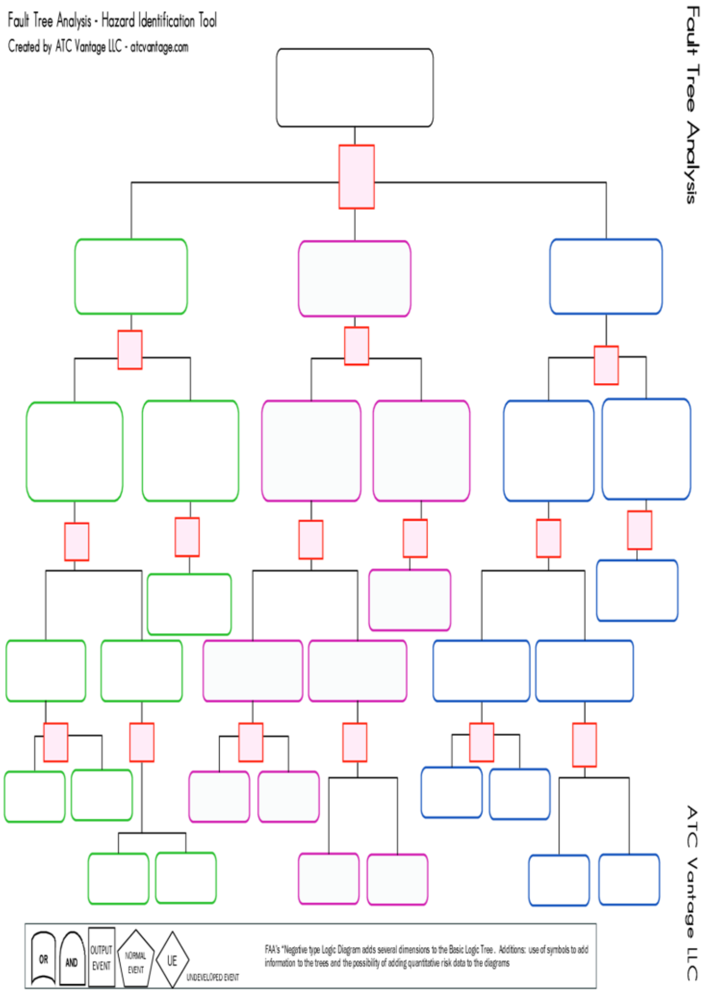
- The soft 1.12g touchdown made runway contact a little later than usual. With the crosswind, this meant weight-on-wheels switches did not activate and the thrust-reverse system could not deploy, owing to safety logic which prevents activation while the aircraft is airborne.
- With limited runway space, 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

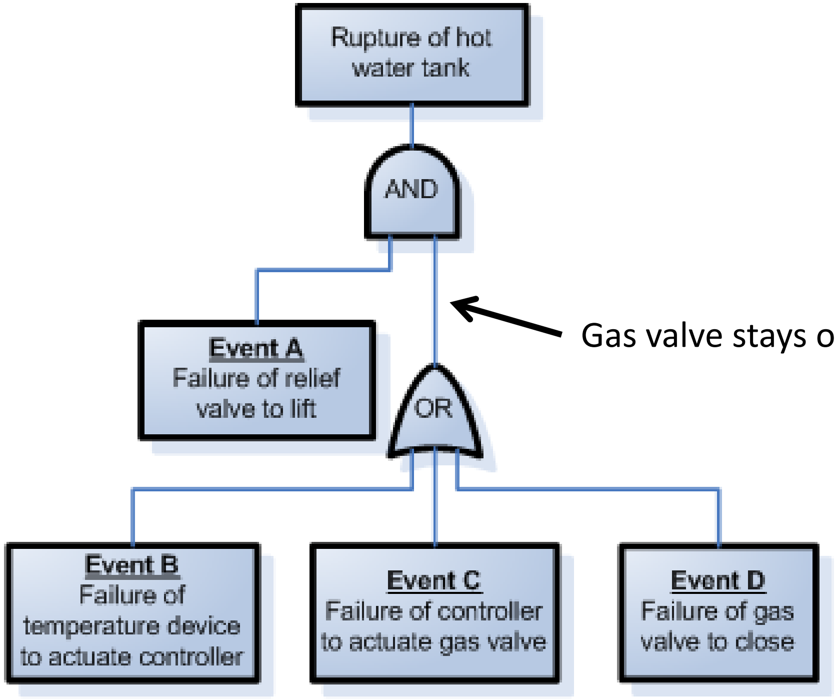
- **Independence** between events is often assumed
- **Common-cause failures** not always obvious
- Difficult to capture **non-discrete** events
  - E.g. rate-dependent events, continuous variable changes
- Doesn’t easily capture **systemic factors**


Fault Tree Analysis - Hazard Identification Tool
Created by ATC Vantage LLC - atcvantage.com
Fault Tree Analysis
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
ATC Vantage LLC

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

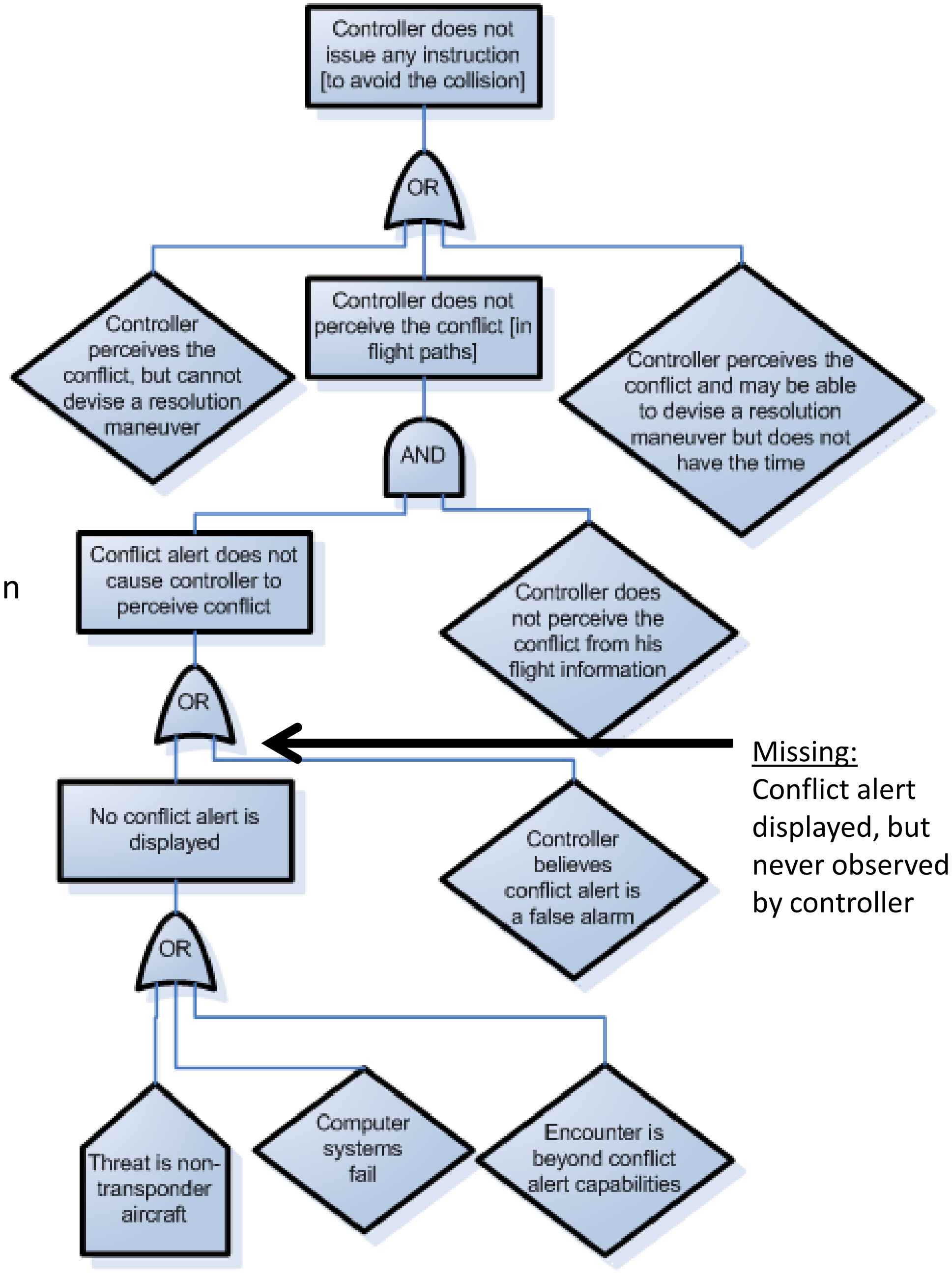
Event B Failure of temperature device to actuate controller

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