Three Approaches to Safety Engineering

- Civil Aviation
- Nuclear Power
- Defense

Civil Aviation

- *Fly-fix-fly*: analysis of accidents and feedback of experience to design and operation
- *Fault Hazard Analysis*:
  - Trace accidents (via fault trees) to components
  - Assign criticality levels and reliability requirements to components
  - Specify development procedures (e.g., DO-178B, Software Certification Requirements
- *Fail Safe Design*: “No single failure or probable combination of failures during any one flight shall jeopardize the continued safe flight and landing of the aircraft”
- Other airworthiness requirements (seat belts, oxygen)

Fail-Safe Design in Aviation

- Design integrity and quality
- Redundancy
- Isolation (so failure in one component does not affect another)
- Component reliability enhancement
- Failure indications (telling pilot a failure has occurred, may need to fly plane differently)
- Specified flight crew procedures

Fail-Safe Design in Aviation (2)

- Design for checkability and inspectability
- Failure containment
- Damage tolerance
  - Systems surrounding failures should be able to tolerate them in case failure cannot be contained
- Designed failure paths
  - Direct high energy failure that cannot be tolerated or contained to a safe path
  - E.g. use of structure “fuses” in pylons so engine will fall off before it damages the structure

Fail-Safe Design in Aviation (3)

- Safety margins or factors
- Error tolerance
  - Design so human cannot make mistakes or errors are tolerated

    Examples:

    - Careful design of cockpit layouts and switches
    - Use of color coding or different shape connectors in wiring

Nuclear Power (Defense in Depth)

- Multiple independent barriers to propagation of malfunction
- High degree of single element integrity and lots of redundancy
- Handling single failures (no single failure of any components will disable any barrier)
- Protection (“safety”) systems: automatic system shut-down
  - Emphasis on reliability and availability of shutdown system and physical system barriers (using redundancy)

Why are these effective?

- Relatively slow pace of basic design changes
  - Use of well-understood and “debugged” designs
- Ability to learn from experience
- Conservatism in design
- Slow introduction of new technology
- Limited interactive complexity and coupling

BUT software starting to change these factors

(Note emphasis on component reliability)

Defense: System Safety

- Emphasizes building in safety rather than adding it on to a completed design
- Looks at systems as a whole, not just components
  - A top-down systems approach to accident prevention
- Takes a larger view of accident causes than just component failures (includes interactions among components)
- Emphasizes hazard analysis and design to eliminate or control hazards
- Emphasizes qualitative rather than quantitative approaches

System Safety Overview

- A planned, disciplined, and systematic approach to preventing or reducing accidents throughout the life cycle of a system.
- “Organized common sense” (Mueller, 1968)
- Primary concern is the management of hazards

Hazard	**Through**
identification	analysis
evaluation	design
elimination	management
control	

- MIL-STD-882

System Safety Overview (2)

- **Analysis***:*

  Hazard analysis and control is a continuous, iterative process throughout system development and use.

- **Design**: Hazard resolution precedence

  1. Eliminate the hazard
  2. Prevent or minimize the occurrence of the hazard
  3. Control the hazard if it occurs
  4. Minimize damage

- **Management**:

  Audit trails, communication channels, etc.

Hazard Analysis

- The heart of any system safety program.
- Used for:
  - Developing requirements and design constraints
  - Validating requirements and design for safety
  - Preparing operational procedures and instructions
  - Test planning and evaluation
  - Management planning

Types (Stages) of Hazard Analysis

- Preliminary Hazard Analysis (PHA)
  - Identify, assess, and prioritize hazards
  - Identify high-level safety design constraints
- System Hazard Analysis (SHA)
  - Examine subsystem interfaces to evaluate safety of system working as a whole
  - Refine design constraints and trace to individual components (including operators)

Types (Stages) of Hazard Analysis (2)

- Subsystem Hazard Analysis (SSHA)
  - Determine how subsystem design and behavior can contribute to system hazards
  - Evaluate subsystem design for compliance with safety constraints
- Change and Operations Analysis
  - Evaluate all changes for potential to contribute to hazards
  - Analyze operational experience

Preliminary Hazard Analysis

1. Identify system hazards
2. Translate system hazards into high-level system safety design constraints
3. Assess hazards if required to do so
4. Establish the hazard log

Classic Hazard Level Matrix

LIKELIHOOD	SEVERITY I Catastrophic	II Critical	III Marginal	IV Negligible
A Frequent	I–A	II–A	III–A	IV–A
B Moderate	I–B	II–B	III–B	IV–B
C Occasional	I–C	II–C	III–C	IV–C
D Remote	I–D	II–D	III–D	IV–D
E Unlikely	I–E	II–E	III–E	IV–E
F Impossible	I–F	II–F	III–F	IV–F

Another Example Hazard Level Matrix

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

Hazard Level Assessment

- Not feasible for complex, human/computer controlled systems
  - No way to determine likelihood
  - Almost always involves new designs and new technology
- Severity is usually adequate to determine effort to spend on eliminating or mitigating hazard.

Hazard Log Information

- System, subsystem, unit
- Description
- Cause(s)
- Possible effects, effect on system
- Category (hazard level)
- Safety requirements and design constraints
- Corrective or preventive measures, possible safeguards, recommended action

Hazard Log Information (2)

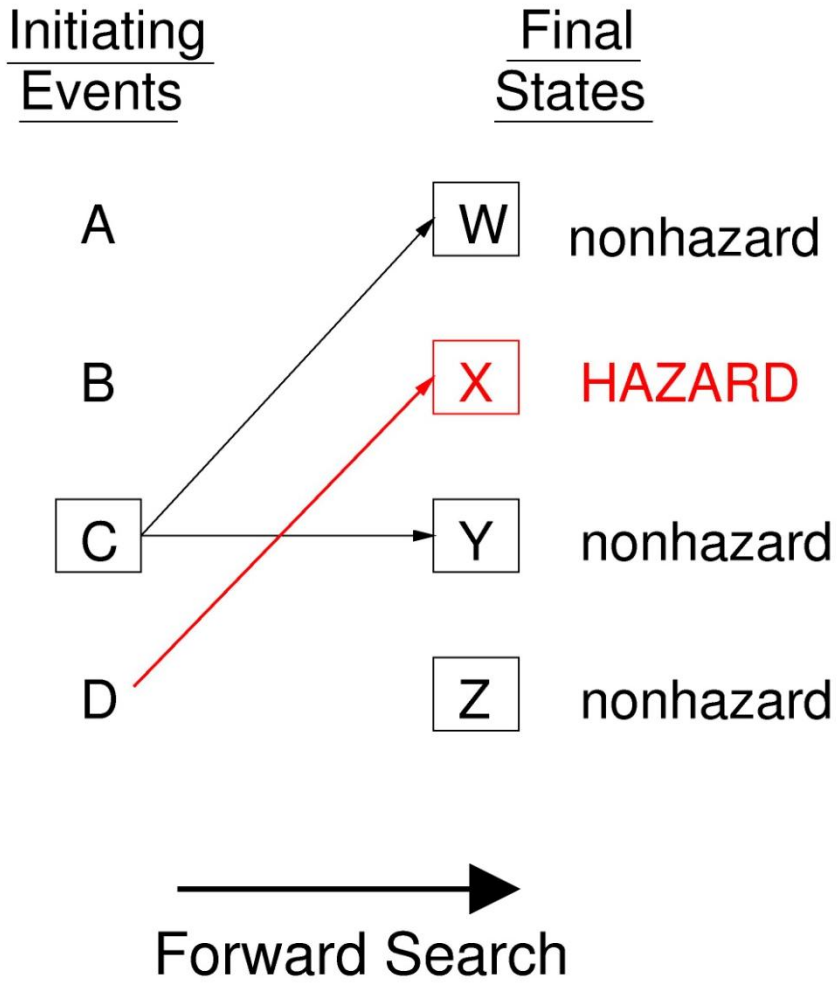
- Operational phases when hazardous
- Responsible group or person for ensuring safeguards are provided
- Tests (verification) to demonstrate safety
- Other proposed and necessary actions
- Status of hazard resolution process
- Etc.

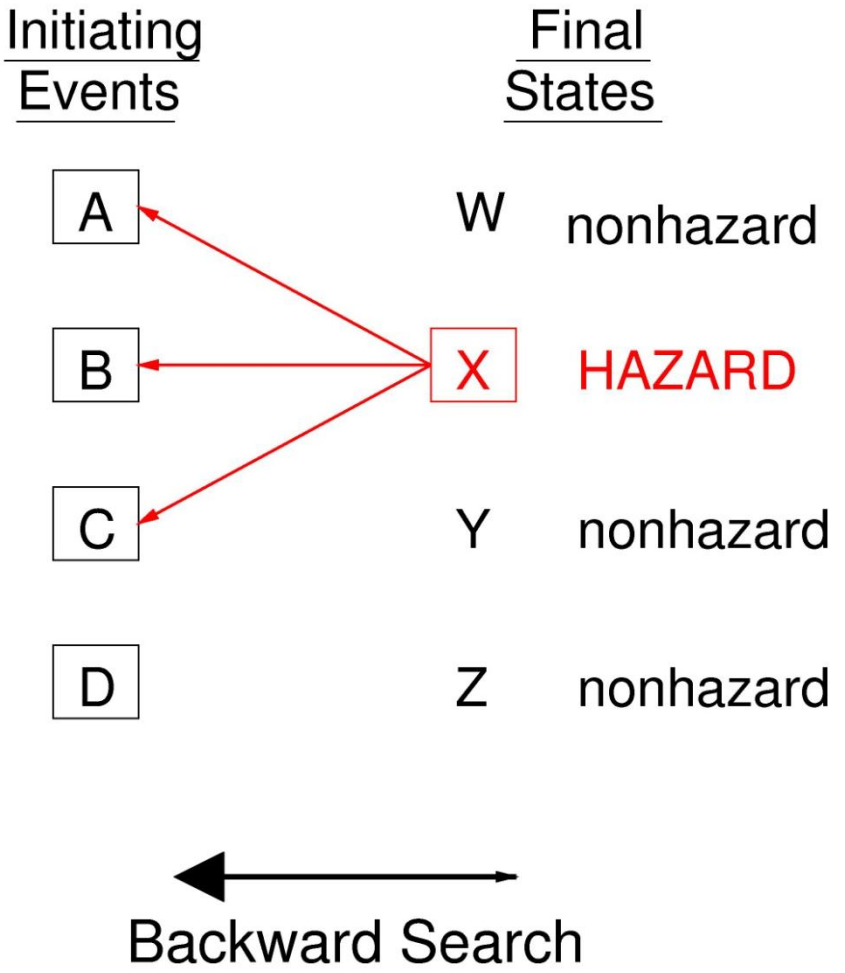
Hazard (Causal) Analysis

- “Investigating an accident before it happens”
- Requires
  - An accident model
  - A system design model (even if only in head of analyst)
- Almost always involves some type of search through the system design (model) for states or conditions that could lead to system hazards.

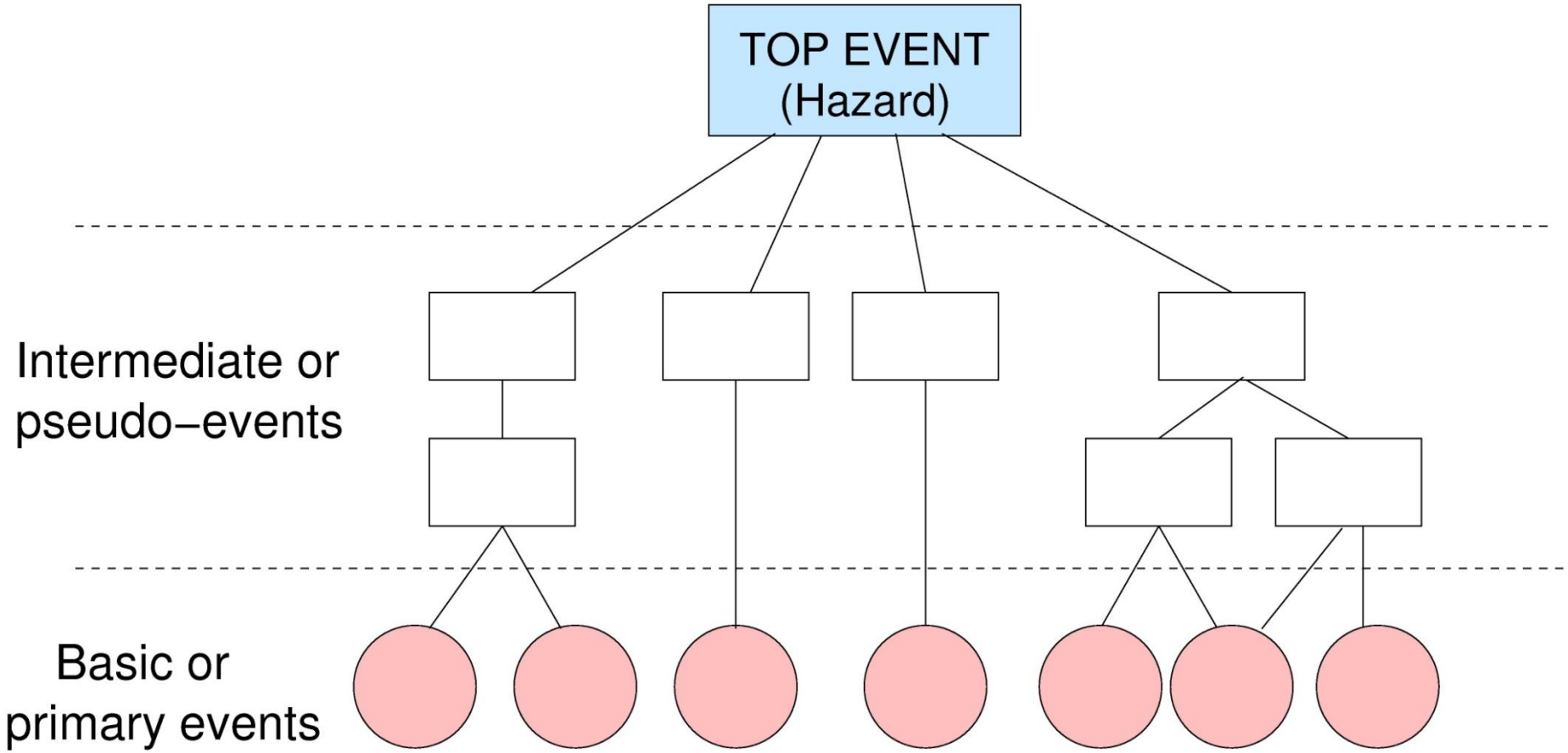
Forward
Backward
Top-down
Bottom-up

Forward vs. Backward Search

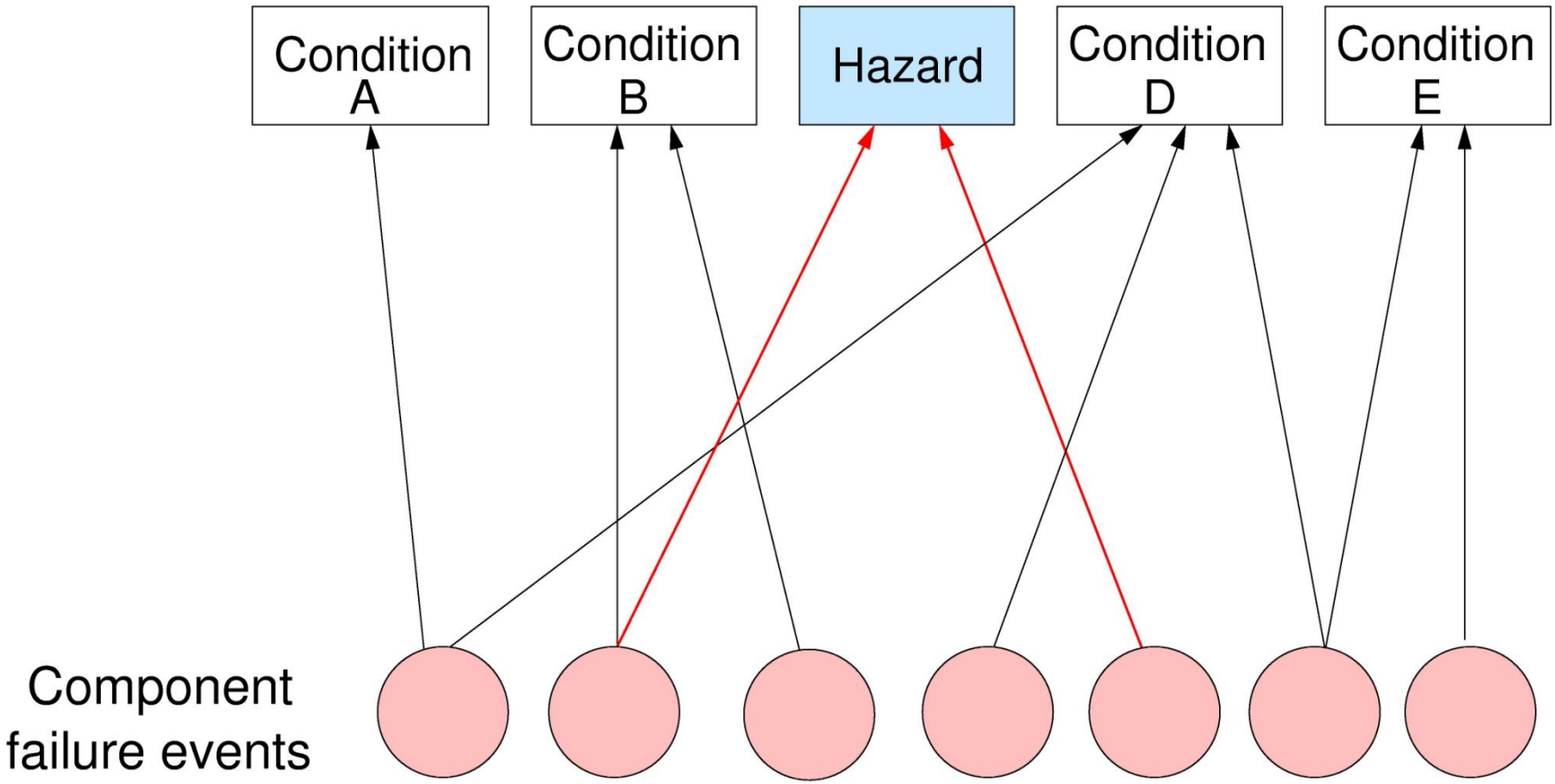




Top-Down Search



Bottom-Up Search



FMEA or FMECA

Failure Modes and Effects (Criticality) Analysis

- Developed to predict equipment reliability
- Forward search based on underlying single chain-of-events and failure models (like event trees)
- Initiating events are failures of individual components
- Quickly become impractical for complex systems

FMEA for a System of Two Amplifiers in Parallel

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

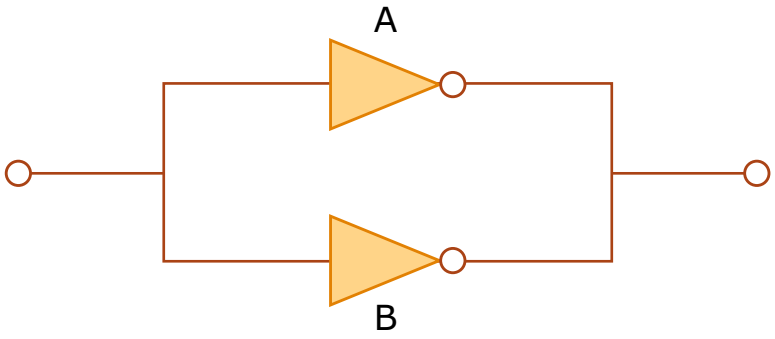


Image by MIT OpenCourseWare.

A Sample FMECA

Failure Modes and Effects Criticality Analysis

Subsystem _____

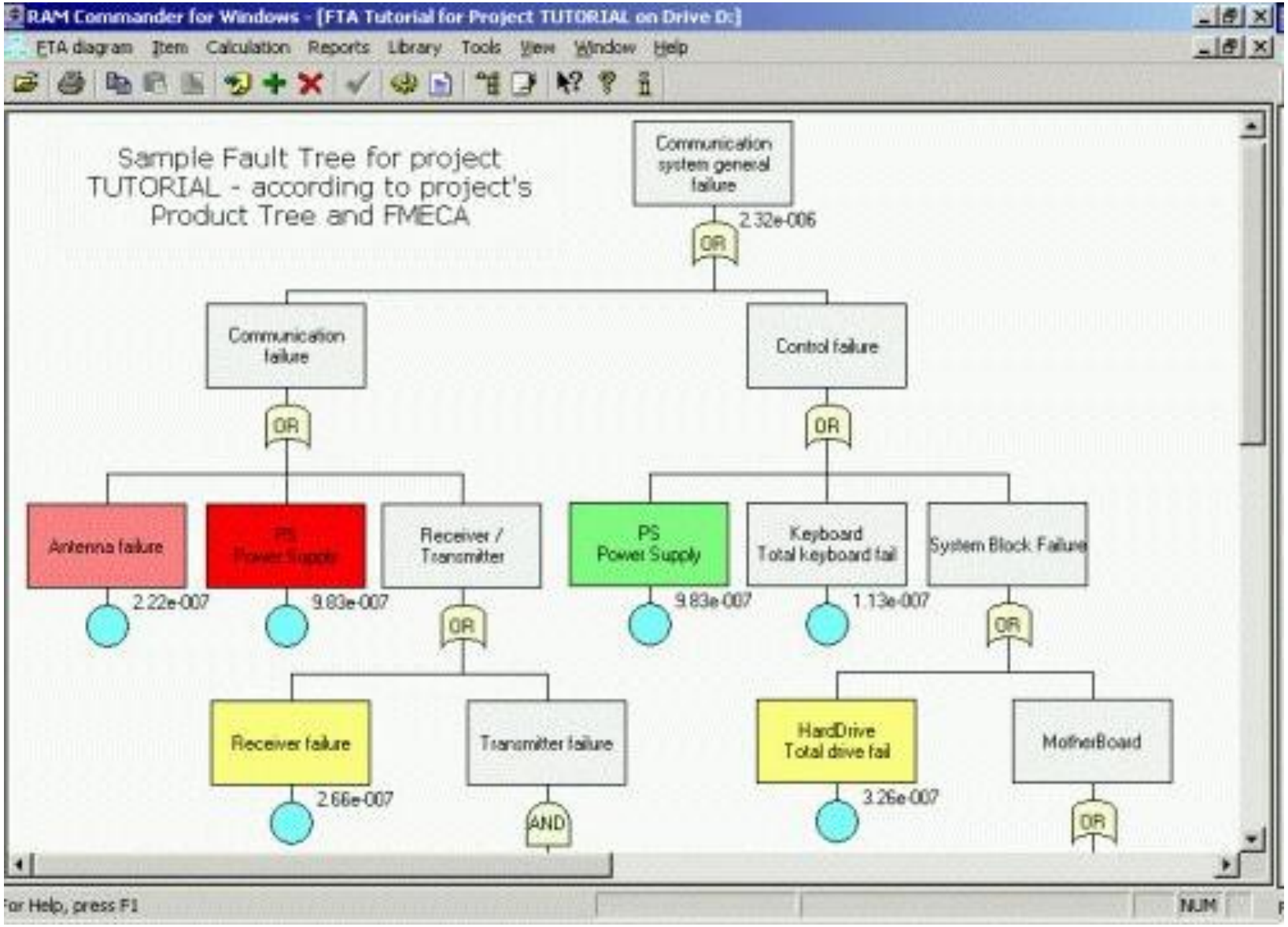
Prepared by _____

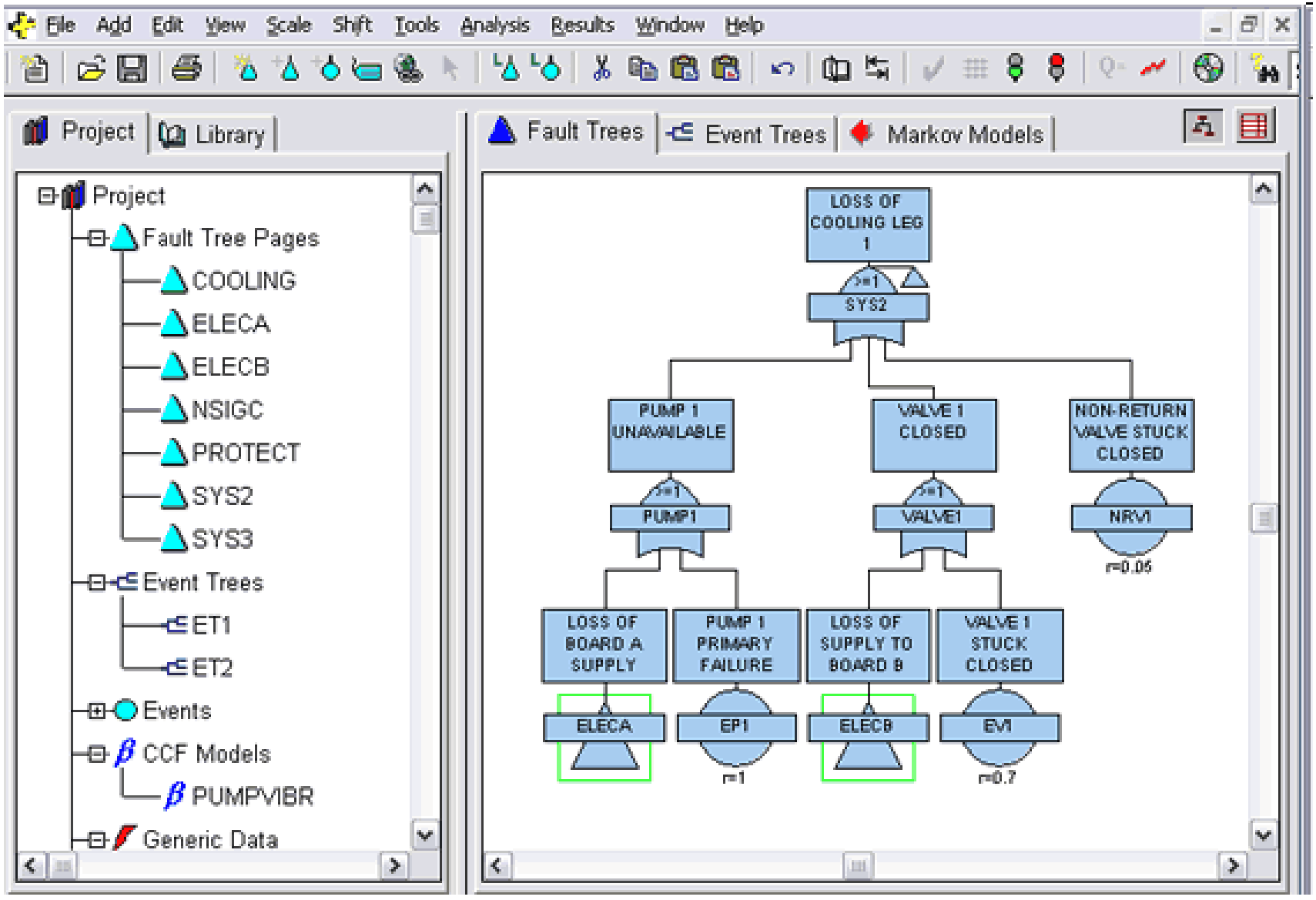
Date _____

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

Fault Tree Analysis

- Developed originally in 1961 for Minuteman
- Top-down search method
- Based on converging chains-of-events accident model.
- Tree is simply record of results; analysis done in head
- FT can be written as Boolean expression and simplified to show specific combinations of identified basic events sufficient to cause the undesired top event (hazard)
- If want quantified analysis and know individual probabilities (or pdf's) for all basic events, frequency of top event can be calculated.


RAM Commander for Windows - [FTA Tutorial for Project TUTORIAL on Drive D:]
FTA diagram Item Calculation Reports Library Tools View Window Help
Sample Fault Tree for project TUTORIAL - according to project's Product Tree and FMECA
Communication system general failure
2.32e-006
OR
Communication failure
Control failure
OR
OR
Antenna failure
PS Power Supply
Receiver / Transmitter
PS Power Supply
Keyboard Total keyboard fail
System Block Failure
2.22e-007
9.83e-007
OR
9.83e-007
1.13e-007
OR
Receiver failure
Transmitter failure
HardDrive Total drive fail
MotherBoard
2.66e-007
AND
3.26e-007
OR
For Help, press F1
NUM


File Add Edit View Scale Shift Tools Analysis Results Window Help
Project
Library
Project
Fault Tree Pages
COOLING
ELECA
ELECB
NSIGC
PROTECT
SYS2
SYS3
Event Trees
ET1
ET2
Events
CCF Models
PUMPVIBR
Generic Data
Fault Trees
Event Trees
Markov Models
LOSS OF COOLING LEG 1
>=1
SYS2
PUMP 1 UNAVAILABLE
VALVE 1 CLOSED
NON-RETURN VALVE STUCK CLOSED
>=1
PUMP1
>=1
VALVE1
NRV1
r=0.05
LOSS OF BOARD A SUPPLY
PUMP 1 PRIMARY FAILURE
LOSS OF SUPPLY TO BOARD B
VALVE 1 STUCK CLOSED
ELECA
EP1
ELECB
EV1
r=1
r=0.7

Exercise

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

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

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

Draw a fault tree for this hazard and system design.

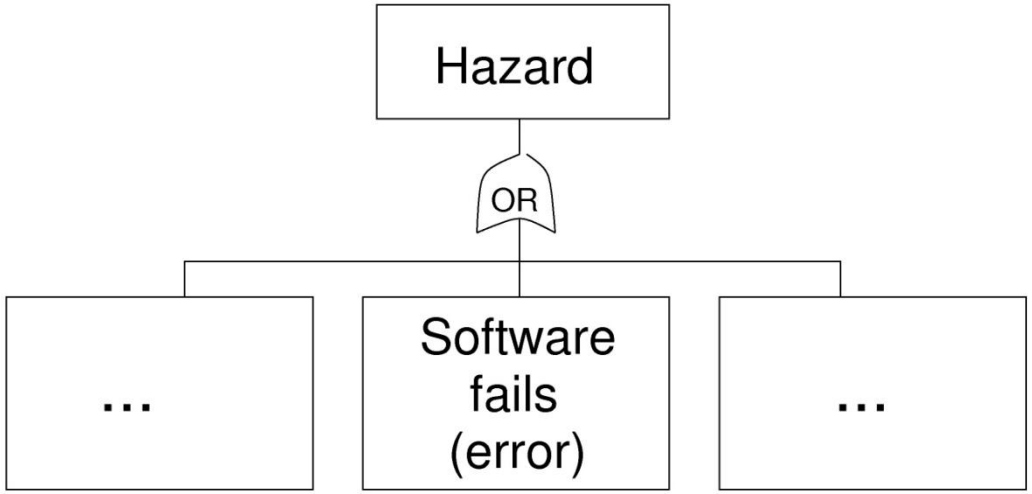
Example of Unrealistic Risk Assessment Leading to an Accident

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

Software in Fault Trees

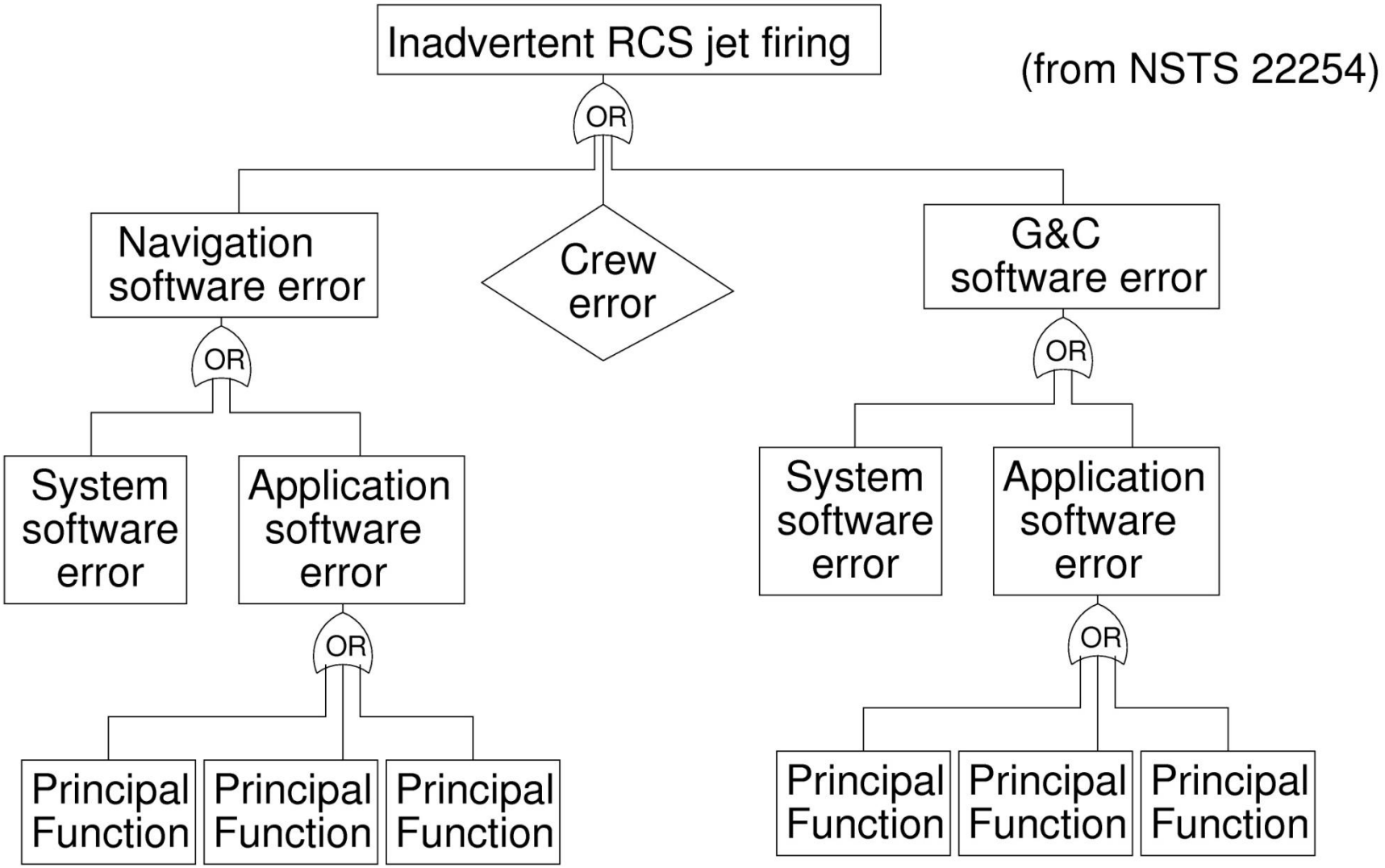
- Software in fault trees should be treated no differently than unsafe hardware behavior
- Software does not “fail” like hardware
- Cannot get numbers for software
  - Fault tree can be used to derive software safety constraints but fault tree analysis provides little or no guidance for this process

Typical Fault Trees



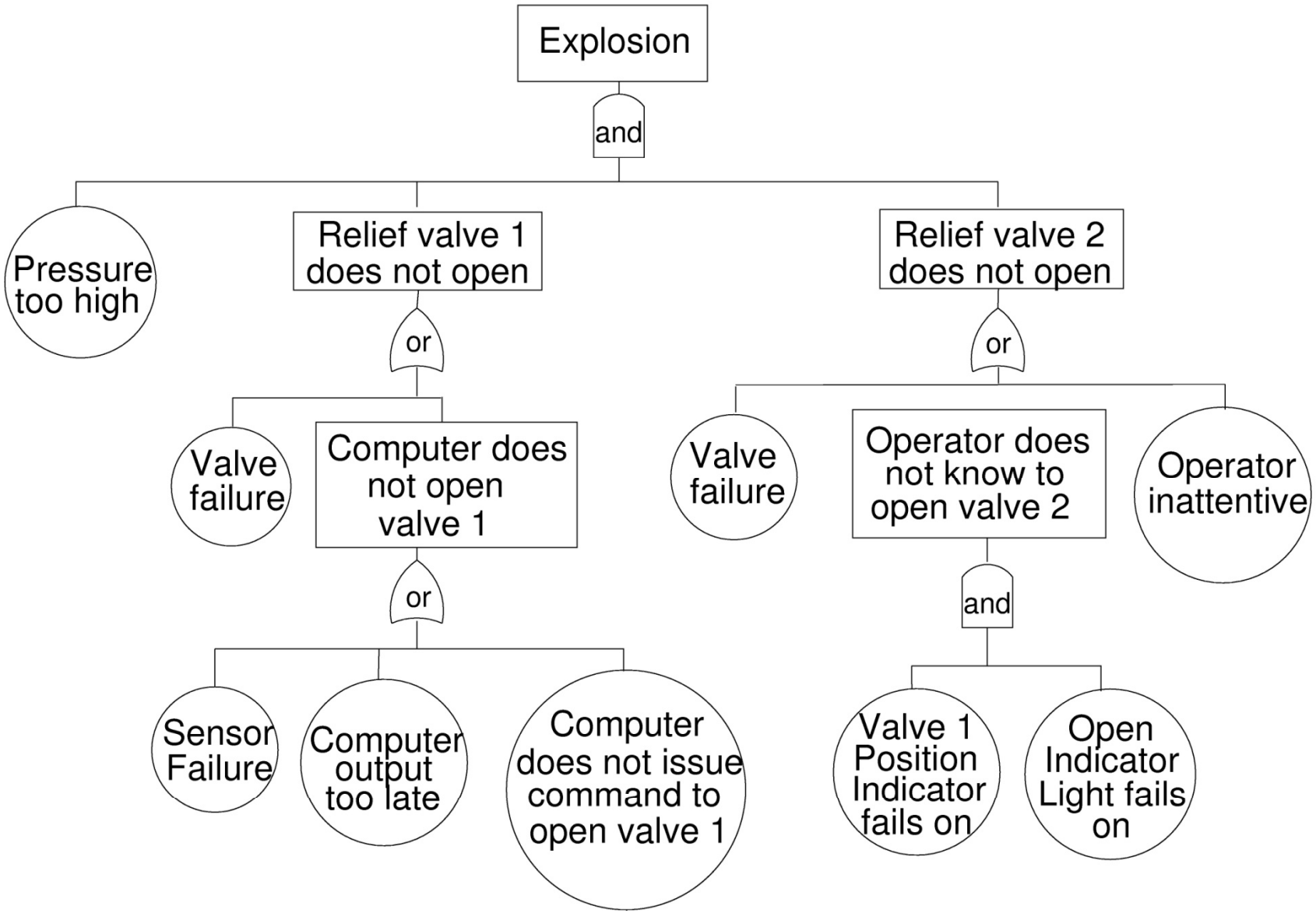
Hazard Cause	Probability	Mitigation
Software Error	0	Test software

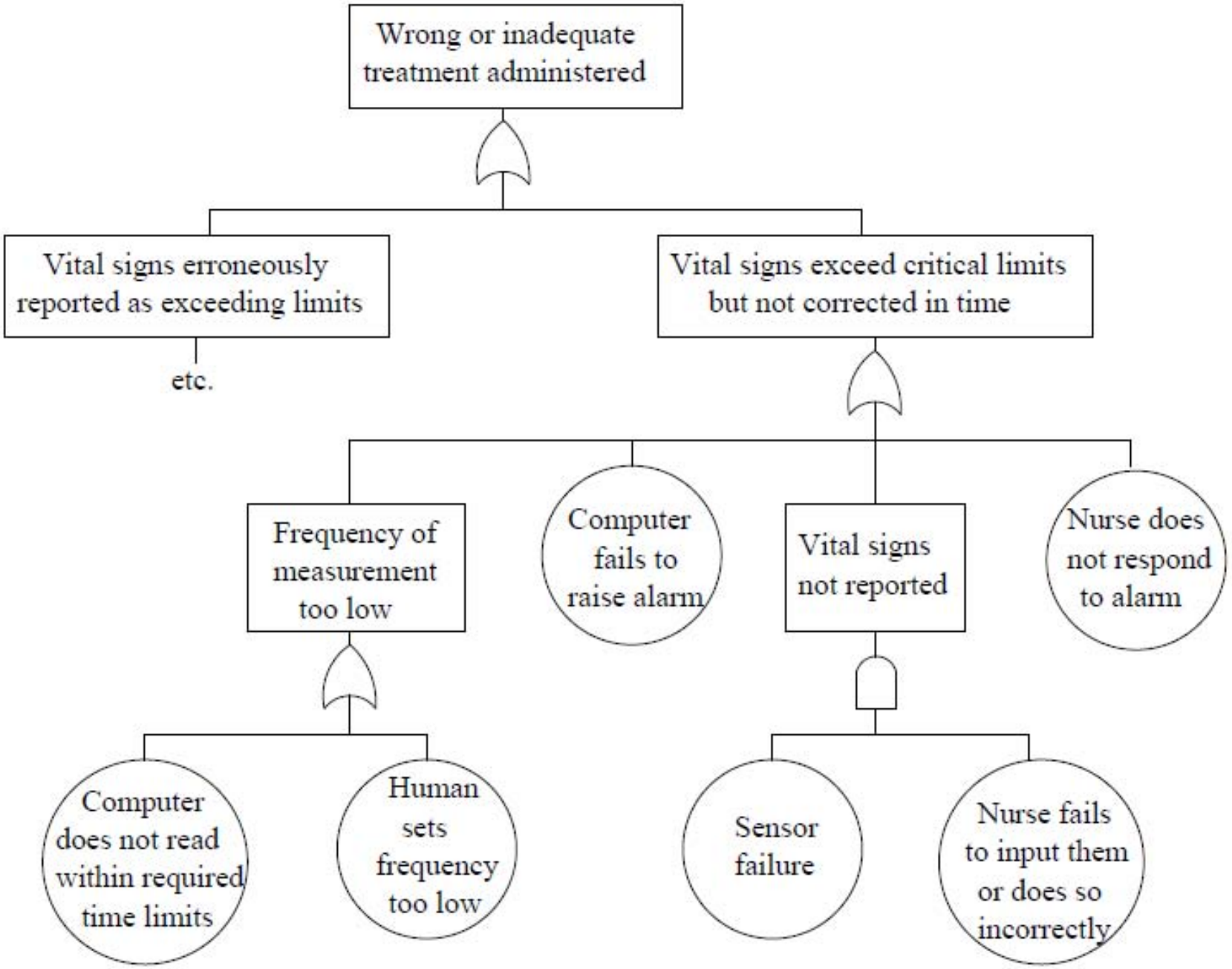
Another Useless Way to Do It



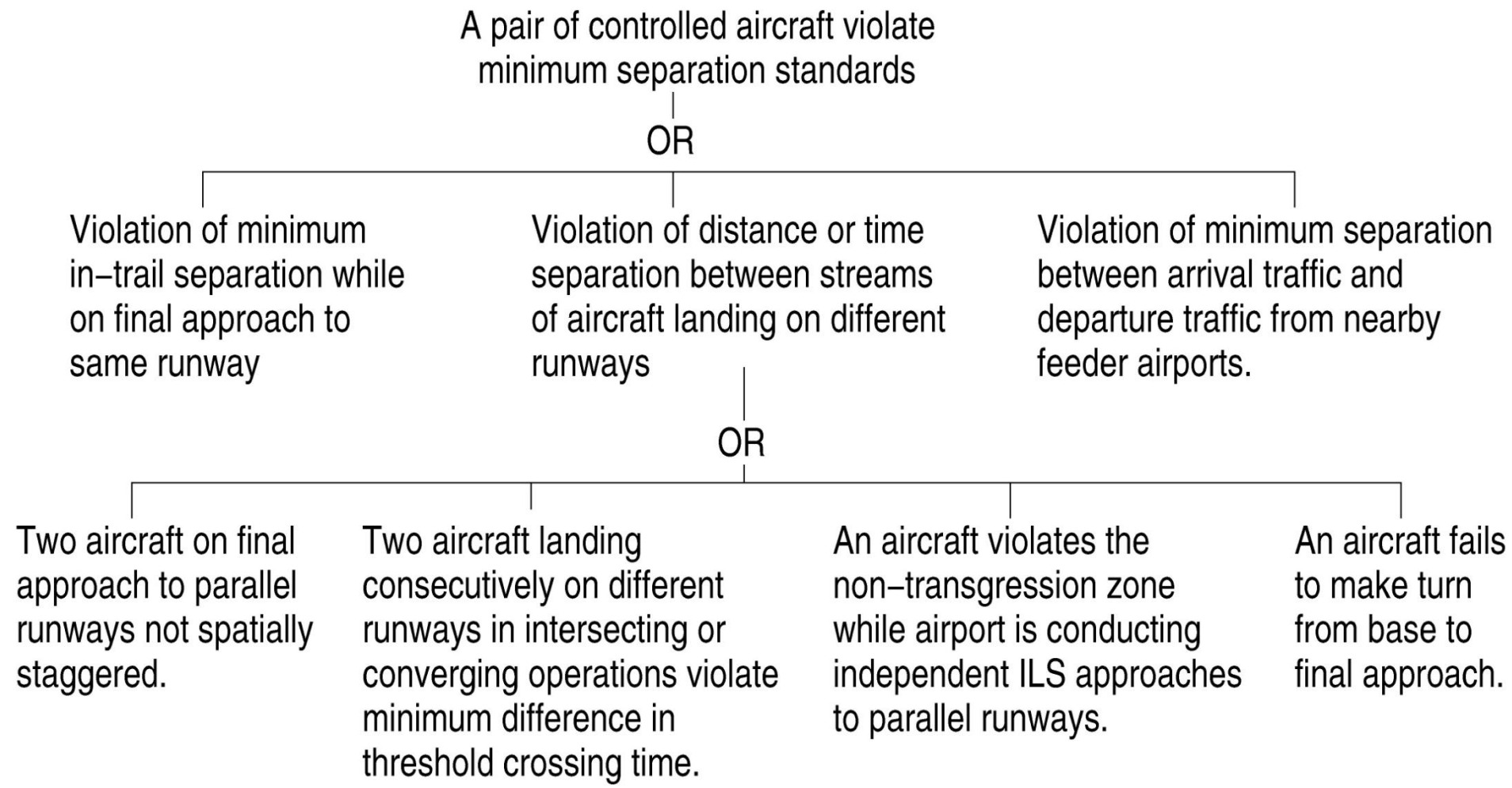
(from NSTS 22254)

Fault Tree Example with a Computer

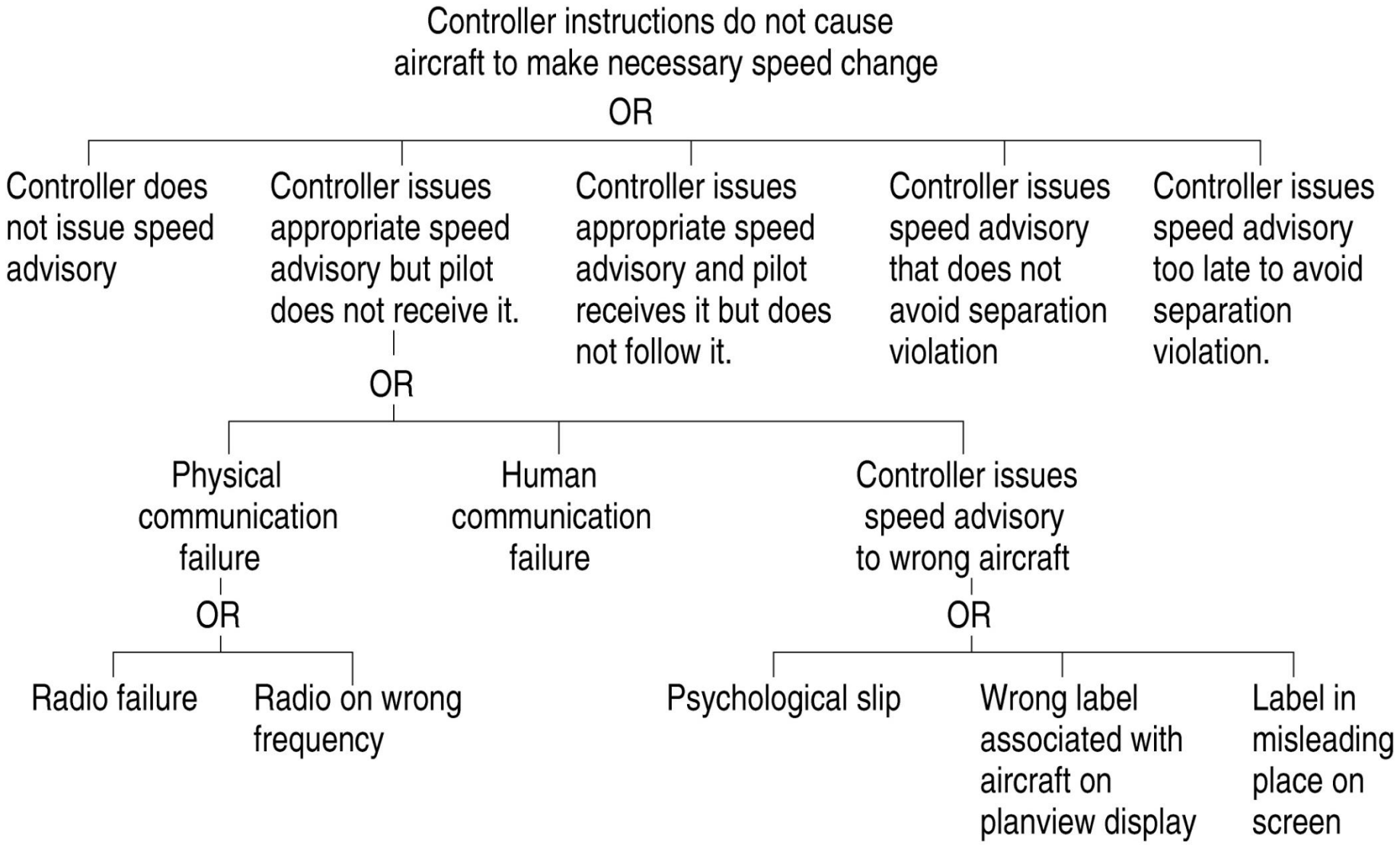



Wrong or inadequate treatment administered
Vital signs erroneously reported as exceeding limits
etc.
Vital signs exceed critical limits but not corrected in time
Frequency of measurement too low
Computer fails to raise alarm
Vital signs not reported
Nurse does not respond to alarm
Computer does not read within required time limits
Human sets frequency too low
Sensor failure
Nurse fails to input them or does so incorrectly

Example Fault Tree for ATC Arrival Traffic



Example Fault Tree for ATC Arrival Traffic (2)



FTA Evaluation

- Graphical format helps in understanding system and relationship between events.
- Can be useful in tracing hazards to software interface and identifying potentially hazardous software behavior.
- Little guidance on deciding what to include
- Tends to concentrate on failures, but does not have to do so.
- Quantitative evaluation may be misleading and lead to accidents.

FTA Evaluation (2)

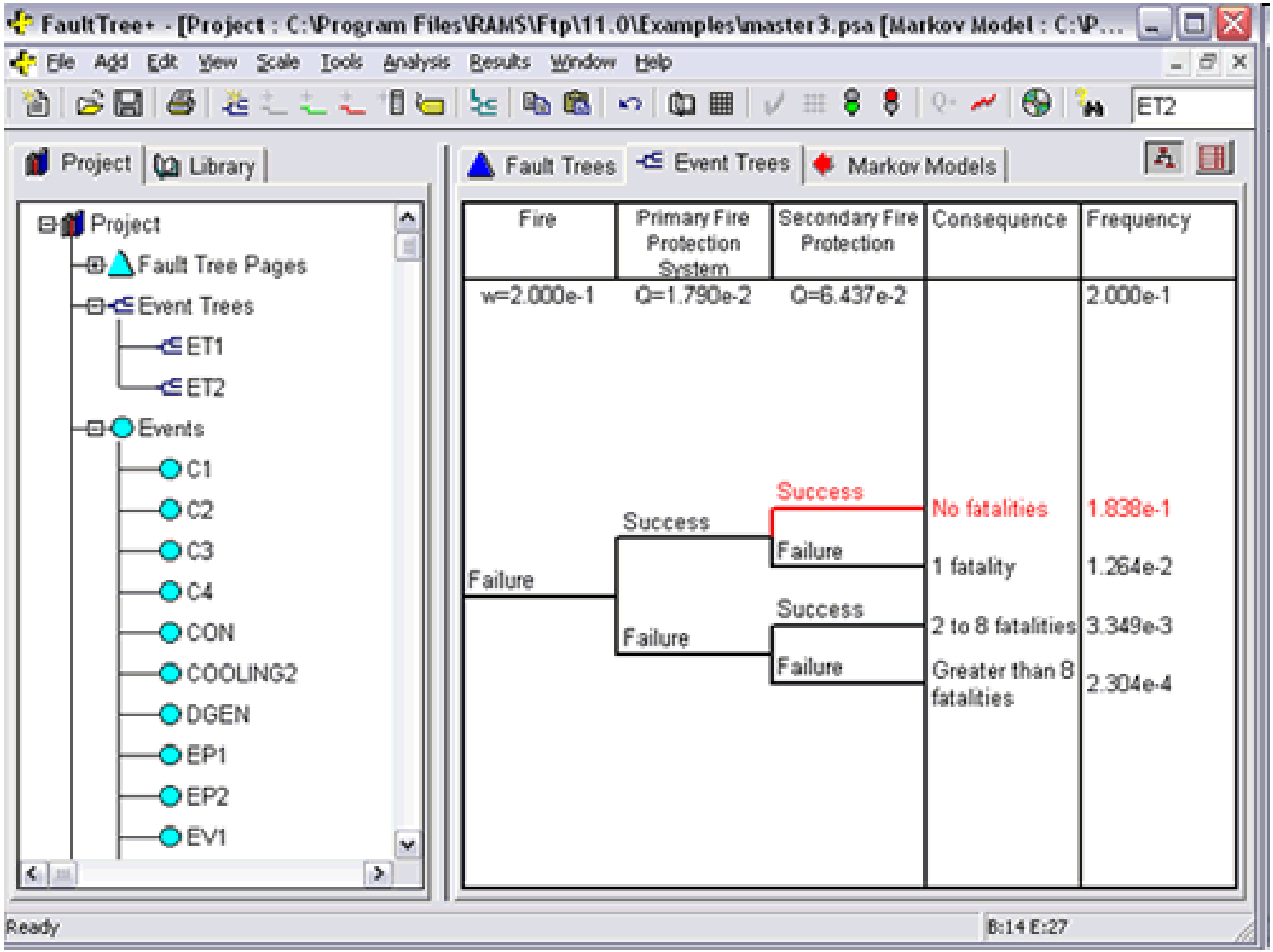
- "On U.S. space programs where FTA (and FMEA) were used, 35% of actual in-flight malfunctions were not identified or were not identified as credible." (Union of Concerned Scientists)

See http://sunnyday.mit.edu/nasa-class/follensbee.html

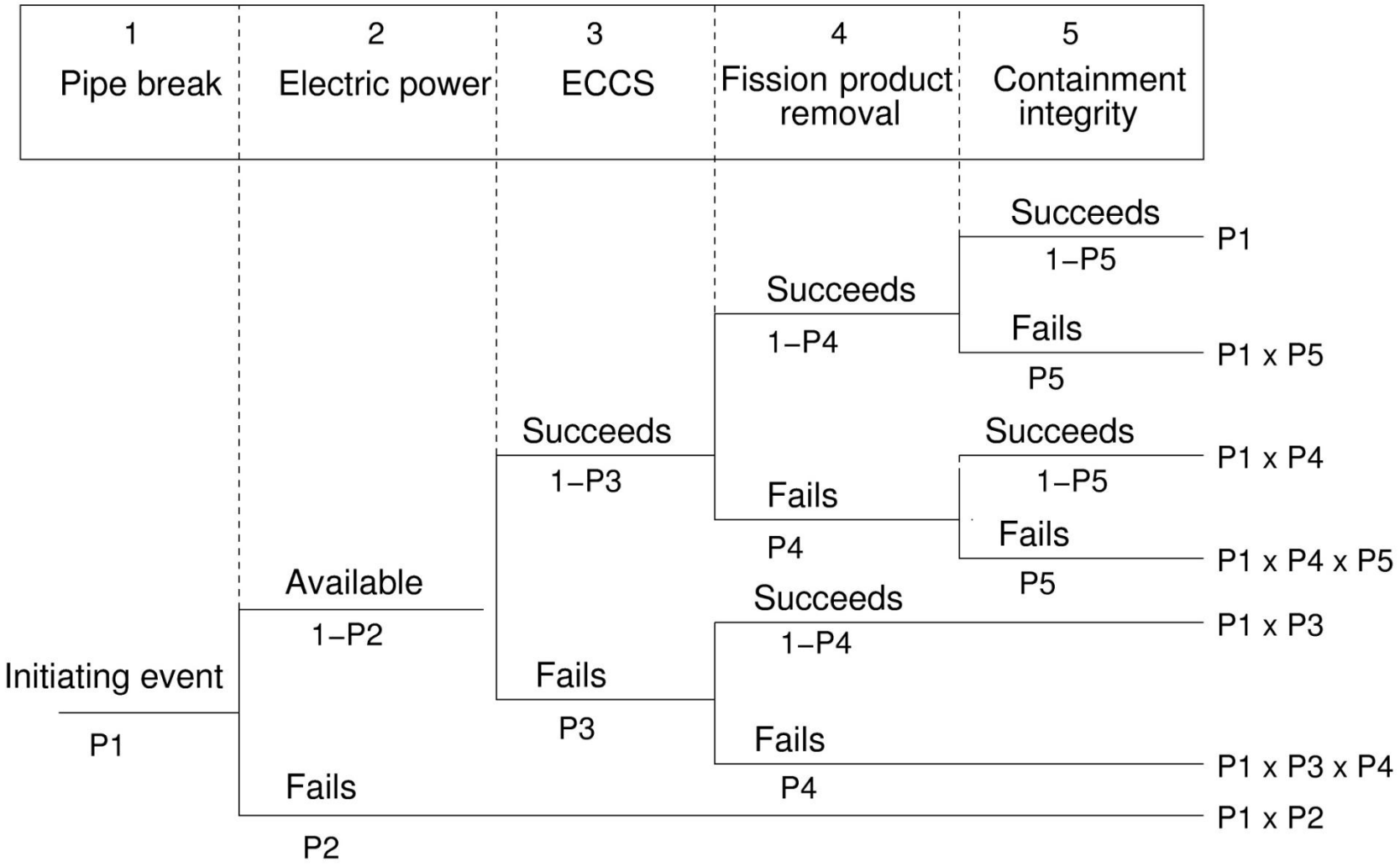
(list of aircraft accidents with calculated risk of 10^{-9} or greater)

Event Tree Analysis

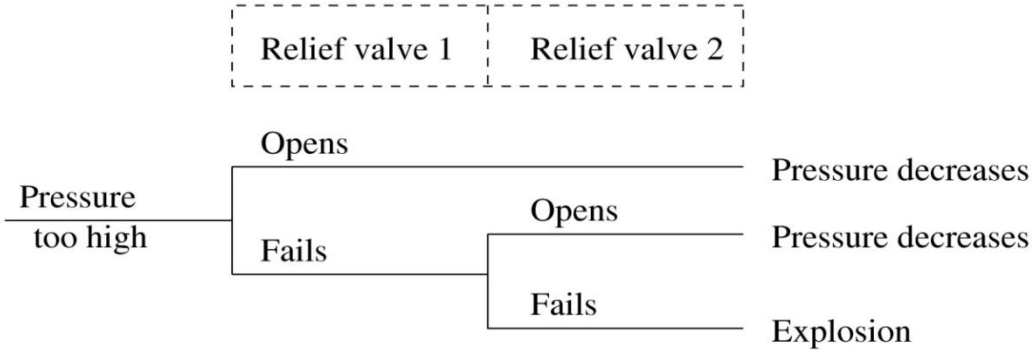
- Developed for and used primarily for nuclear power
- Underlying single chain-of-events model of accidents
- Forward search
- Simply another form of decision tree
- Problems with dependent events

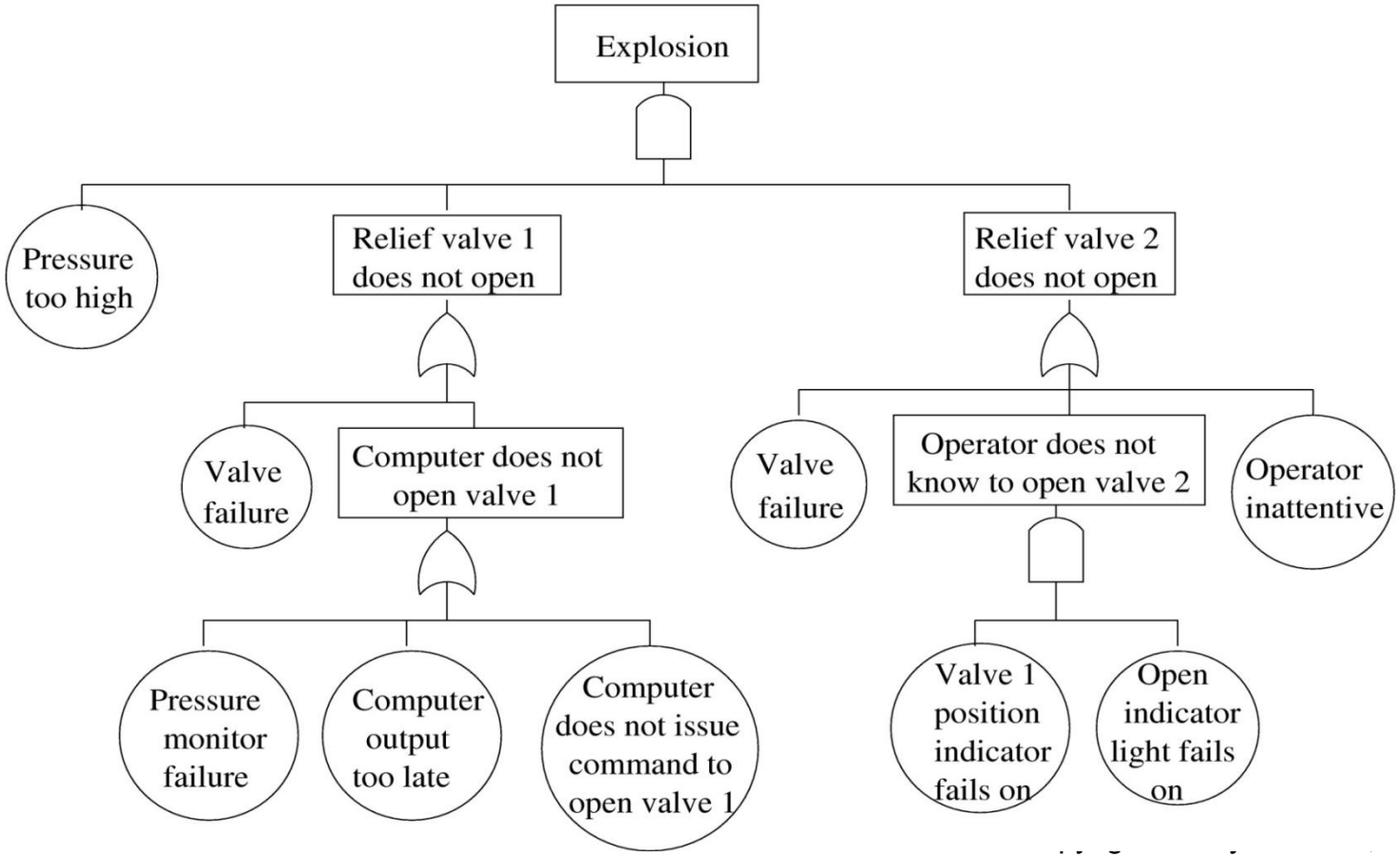

FaultTree+ - [Project : C:\Program Files\RAMS\Ftp\11.0\Examples\master3.psa [Markov Model : C:\P...
File Add Edit View Scale Tools Analysis Results Window Help
ET2
Project
Library
Project
Fault Tree Pages
Event Trees
ET1
ET2
Events
C1
C2
C3
C4
CON
COOLING2
DGEN
EP1
EP2
EV1
Fault Trees
Event Trees
Markov Models
Fire
Primary Fire Protection System
Secondary Fire Protection
Consequence
Frequency
w=2.000e-1
Q=1.790e-2
Q=6.437e-2
2.000e-1
Success
No fatalities
1.838e-1
Success
Failure
1 fatality
1.264e-2
Failure
Success
2 to 8 fatalities
3.349e-3
Failure
Failure
Greater than 8 fatalities
2.304e-4
Ready
B:14 E:27

Event Tree Example



Event Trees vs. Fault Trees





ETA Evaluation

- Event trees are better at handling ordering of events but fault trees better at identifying and simplifying event scenarios.
- Practical only when events can be ordered in time (chronology of events is stable) and events are independent of each other.
- Most useful when have a protection system.
- Can become exceedingly complex and require simplification.

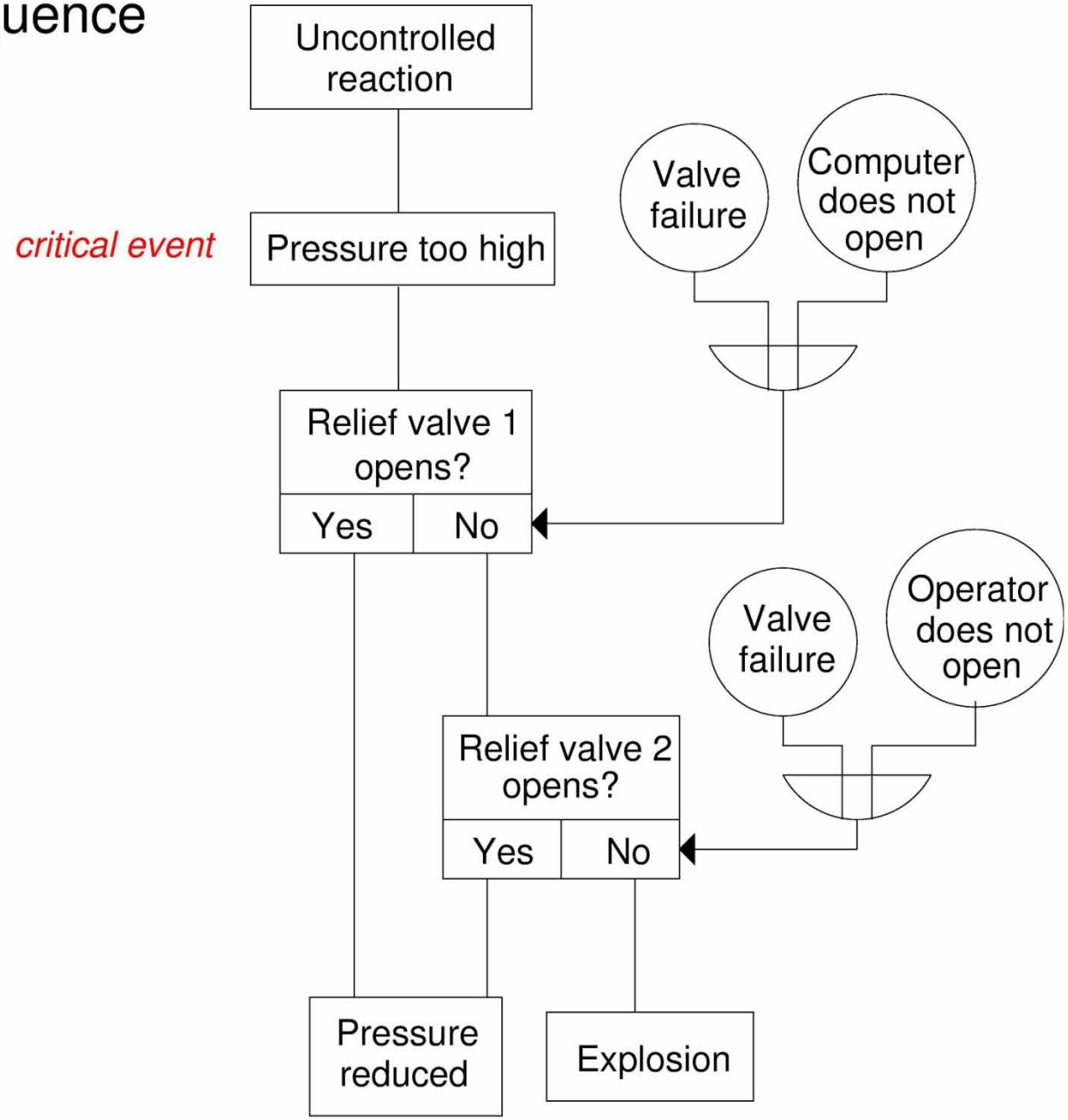
ETA Evaluation (2)

- Separate tree required for each initiating event.
  - Difficult to represent interactions among events
  - Difficult to consider effects of multiple initiating events
- Defining functions across top of event tree and their order is difficult
- Depends on being able to define set of initiating events that will produce all important accident sequences
- Probably most useful in nuclear power plants where
  - All risk associated with one hazard (overheating of fuel)
  - Designs are fairly standard
  - Large reliance on protection and shutdown systems

Cause-Consequence Analysis

- Used primarily in Europe
- A combination of forward and top-down search
  - Basically a fault tree and event tree attached to each other
- Again based on converging chain-of-events model
- Diagrams can become unwieldy
- Separate diagrams needed for each initiating event

Cause–Consequence Diagram



HAZOP: Hazard and Operability Analysis

- Based on model of accidents that assumes they are caused by deviations from design or operating intentions.
- Purpose is to identify all possible deviations from the design's expected operation and all hazards associated with these deviations.
- Unlike other techniques, works on a concrete model of plant (e.g., piping and wiring diagram)
- Applies a set of guidewords to the plant diagrams.

HAZOP Guidewords

Guideword	*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 physical 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).

Example Entry in a HAZOP Report

Guide Word	*Deviation*	*Possible Causes*	*Possible Consequences*
NONE	No flow	1. Pump failure 2. Pump suction filter blocked 3. Pump isolation valve closed.	1. Overheating in heat exchanger. 2. Loss of feed to reactor.

Task and Human Error Analyses

- Qualitative Techniques
  - Break down tasks into a sequence of steps
  - Investigate potential deviations and their consequences
- Quantitative Techniques
  - Assign probabilities for various types of human error
  - Most effective in simple systems where tasks routine
  - Not effective for cognitively complex tasks operators often asked to perform today
  - Focus on reducing number rather than eliminating hazard

Typical Human Error Data

Probability	Activity
10^{-2}	General human error of omission where there is no display in the control room of the status of the item omitted, such as failure to the return a manually operated test valve to the proper position after maintenance.
ne 3 x 10^{-3}	Errors of omission where the items being omitted are embedded in a procedure rather than at the end.
3 x 10^{-2}	General human error of commission, such as misreading a label and therefore selecting the wrong switch.
3 x 10^{-2}	Simple arithmetic errors with self-checking, but without repeating the calculation by re-doing it on another piece of paper.
10^{-1}	Monitor or inspector failure to recognize an initial error by operator.
10^{-1}	Personnel on different workshift fail to check the condition of hardware unless required by a checklist or written directive.

Typical Error Rates Used for Emergency Situations

Probability	Activity
0.2-0.3	The general error rate given very high stress levels where dangerous activities are occurring rapidly.
1.0	Operator fails to act correctly in first 60 seconds after the onset of an extremely high stress condition
9×10^{-1}	Operator fails to act correctly in the first 5 minutes after the onset of an extremely high stress condition.
10^{-1}	Operator fails to act correctly in the first 30 minutes of an extreme stress condition.
10^{-2}	Operator fails to act correctly in the first several hours of a high stress condition.

Other Techniques

- “What if” analysis
- Fishbone (Ishikawa) Diagrams
- 5 Whys

5 Whys Example

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?

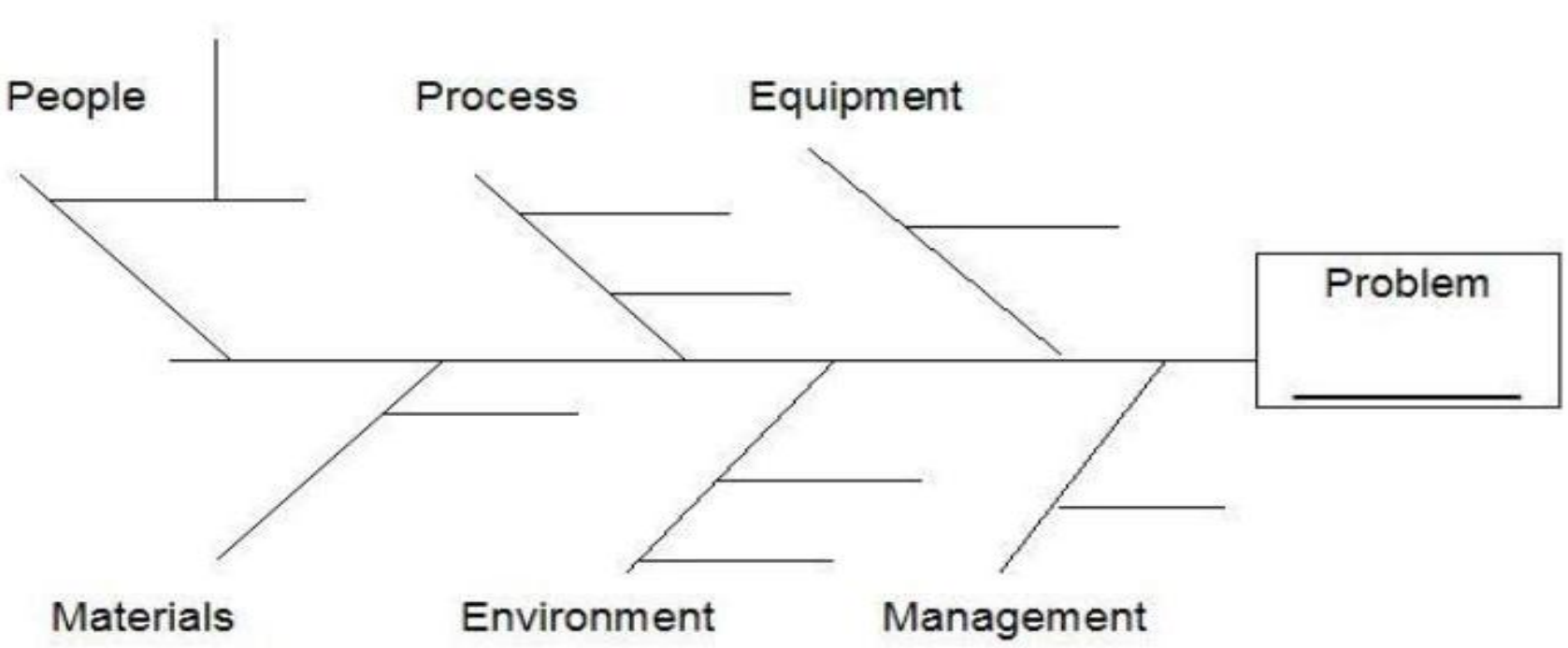
They eat gnats and lots of gnats at monument

Why so many gnats?

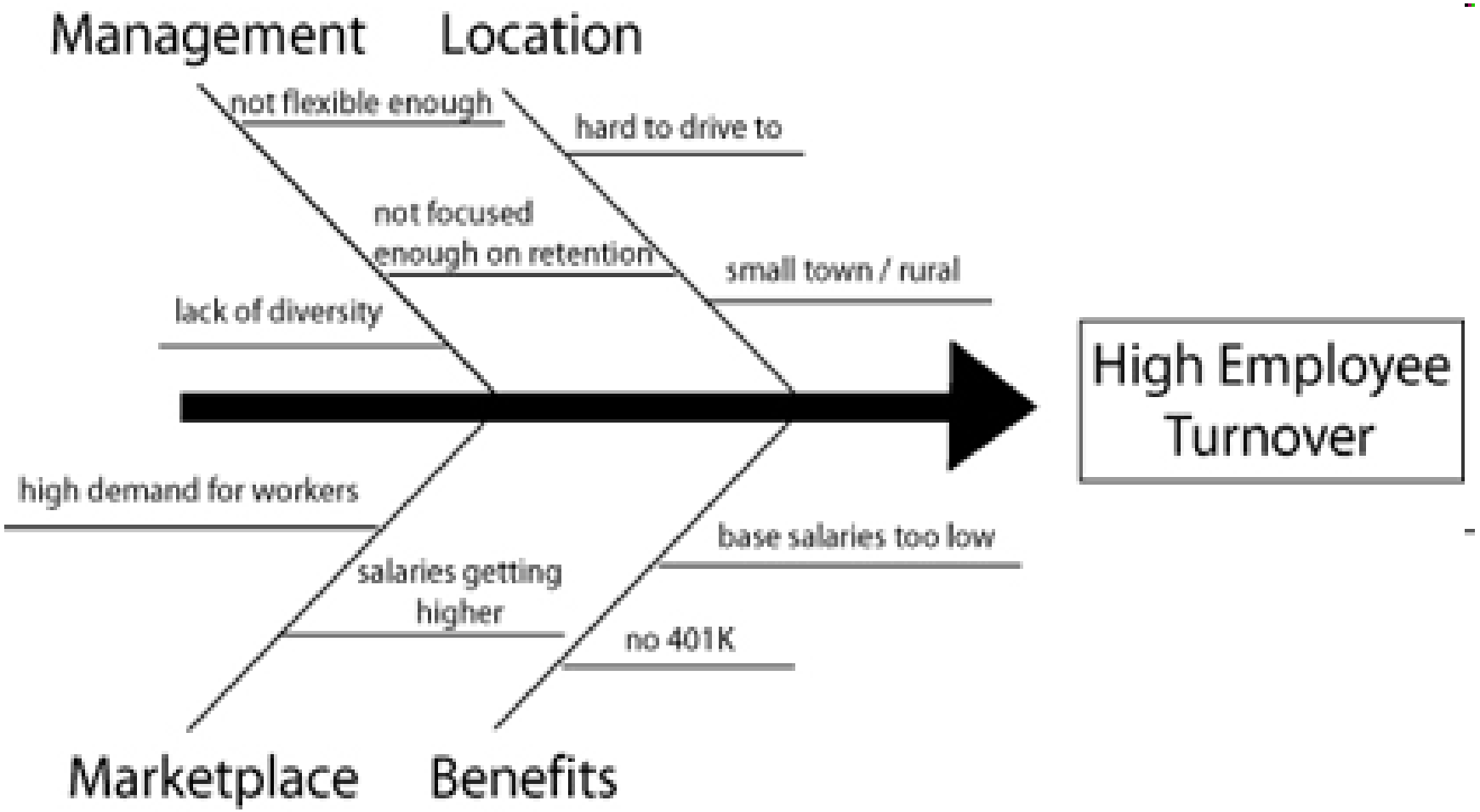
They are attracted to the lights at dusk

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

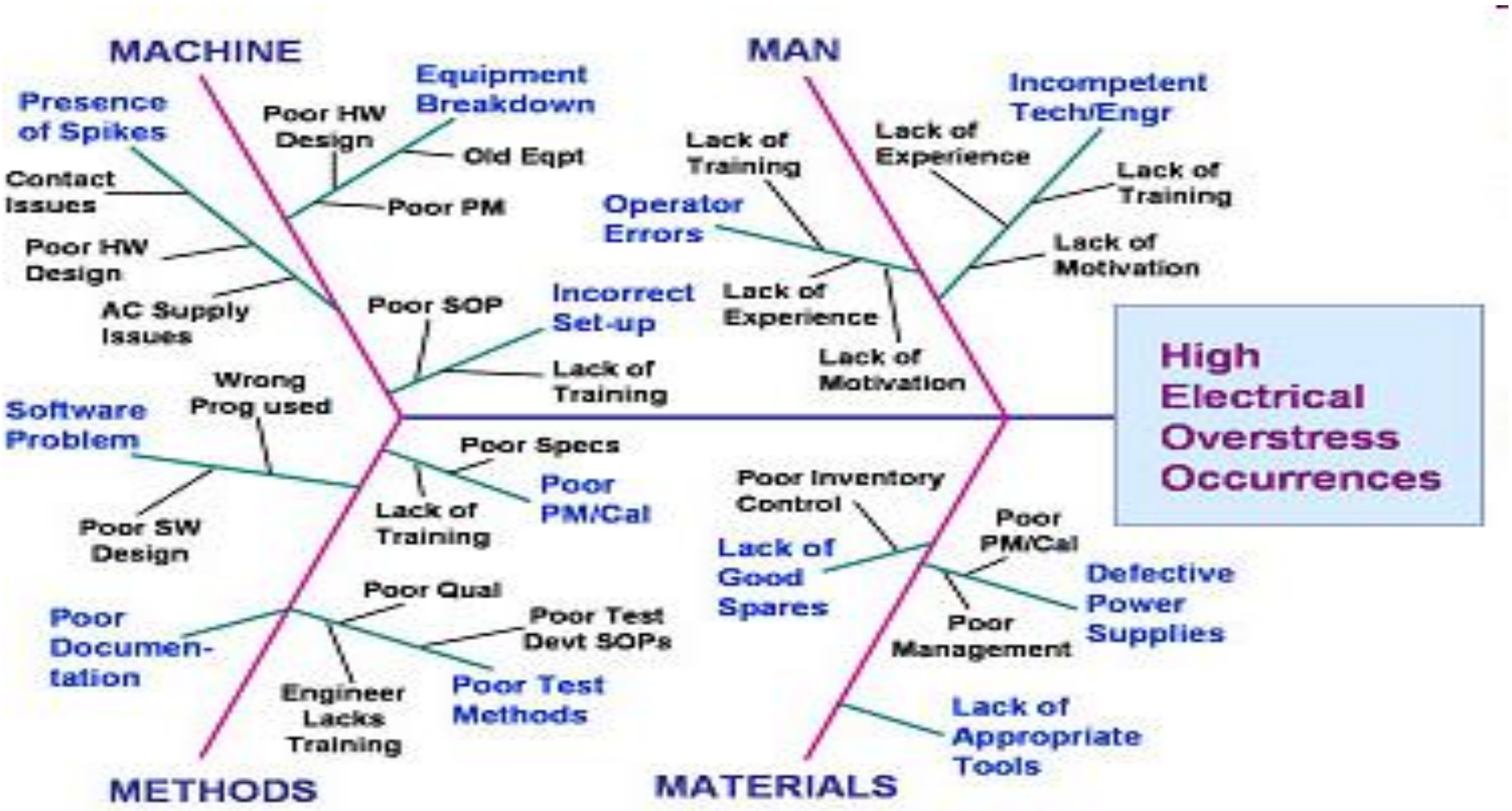
Fishbone (Ishikawa) Diagrams

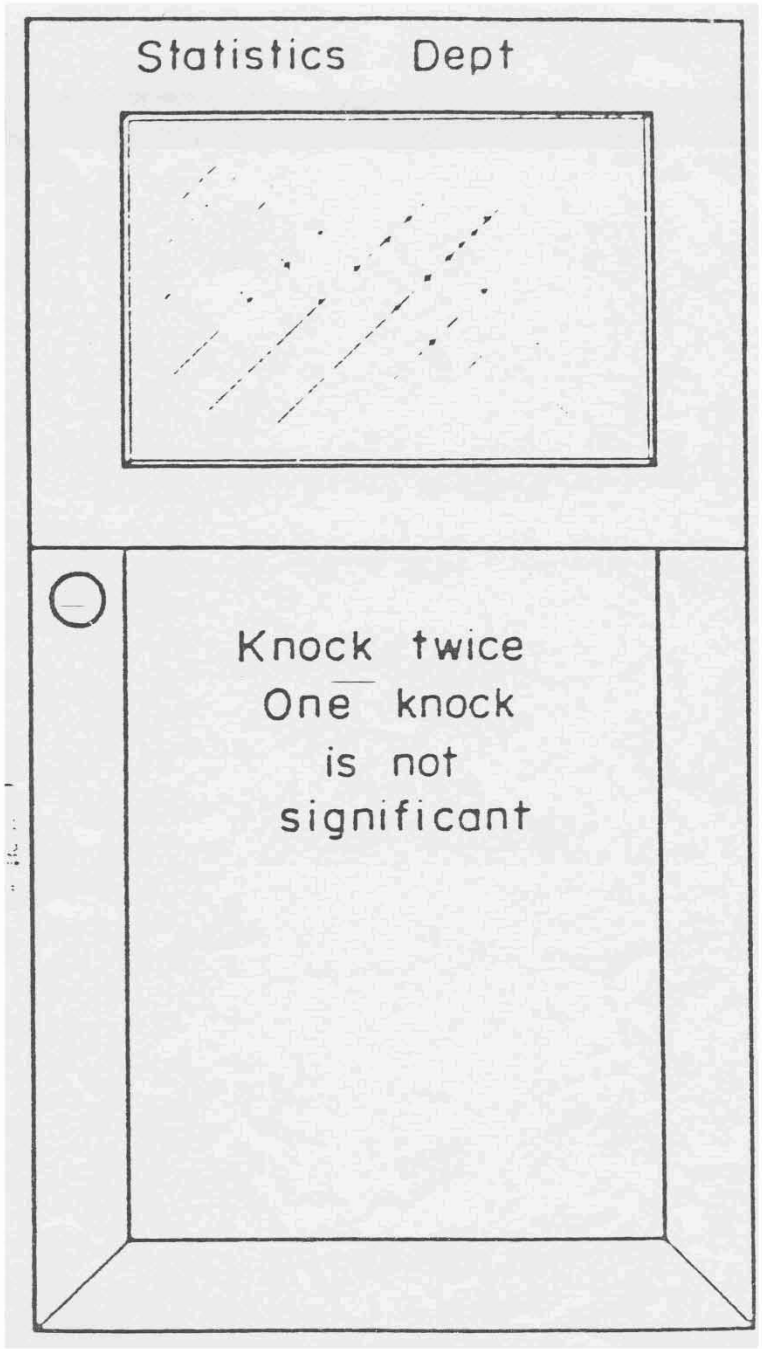


- **Just a fault tree drawn differently**


Management
Location
not flexible enough
hard to drive to
not focused enough on retention
small town / rural
lack of diversity
High Employee Turnover
high demand for workers
base salaries too low
salaries getting higher
no 401K
Marketplace
Benefits

Example Fishbone Diagram




Statistics Dept
Knock twice
One knock
is not
significant

Probabilistic Risk Assessment

- Based on chain-of-events model
- Usually assumes independence between events
- Events chosen will affect accuracy, but usually arbitrary (subjective)
- Usually concentrates on failure events

Risk Measurement

- Risk = f (likelihood, severity)
- Impossible to measure risk accurately
- Instead use risk assessment
  - 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

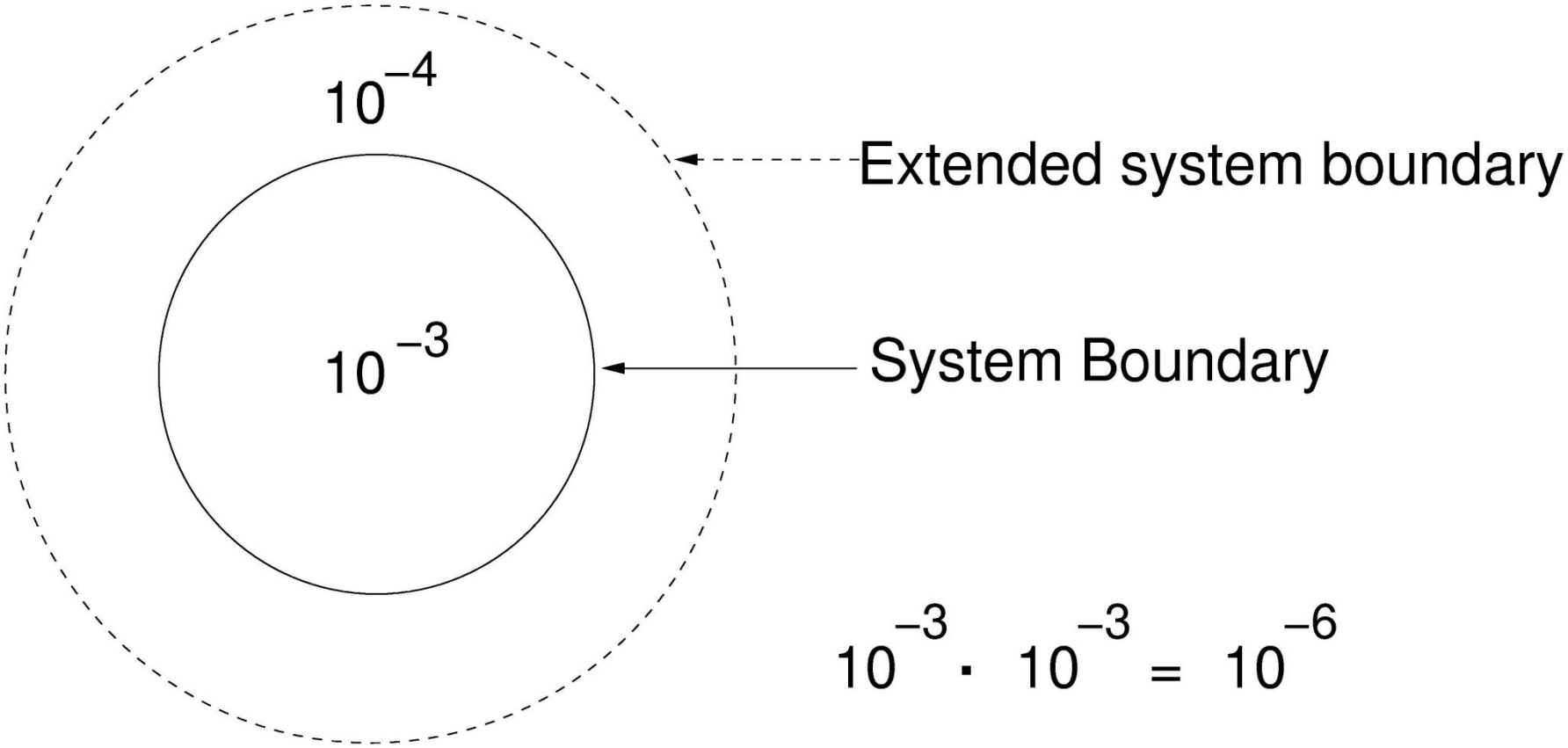
Risk Modeling

- In practice, models only include events that can be measured.
- Most causal factors involved in major accidents are unmeasurable.
- Unmeasurable factors tend to be ignored or forgotten
- Can be measure software? (what does it mean to measure “design”)?

> *“Risk assessment data can be like the captured spy; if you torture it long enough, it will tell you anything you want to know,”*
>
> William Ruckleshaus

Misinterpreting Risk

Risk assessments can easily be misinterpreted:



16.863J / ESD.863J System Safety

Spring 2011