Traditional Safety Analysis

Quantitative Methods

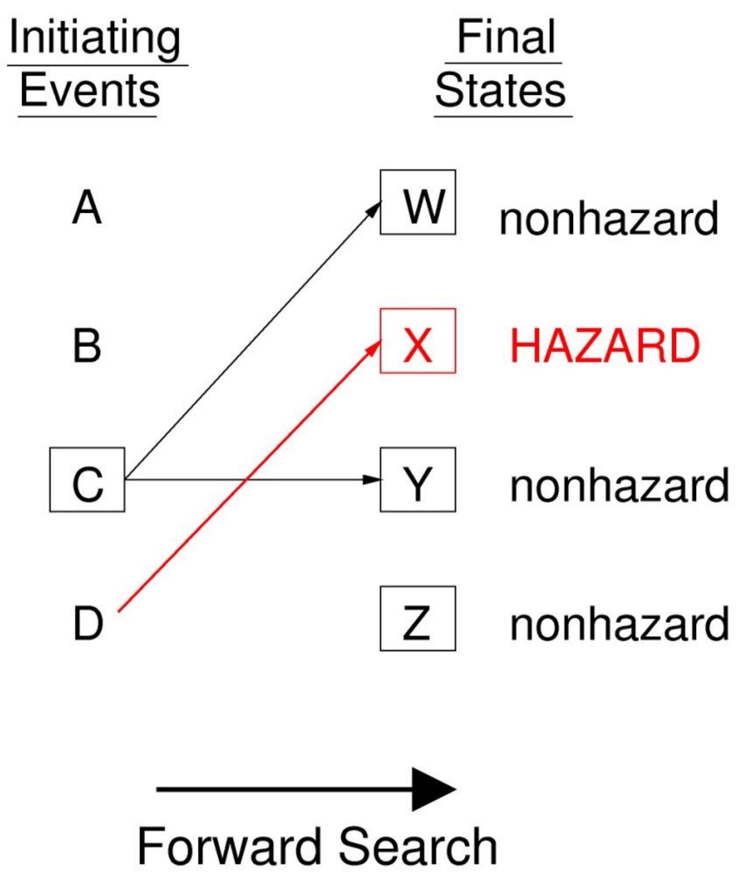
Agenda

- Last time: Qualitative methods
  - FMEA
  - FTA
  - Limitations
- Today
  - More Qualitative methods
    - ETA
    - HAZOP
  - Quantitative methods
    - FMECA
    - FTA
    - ETA
    - PRA
  - Limitations

Event Tree Analysis

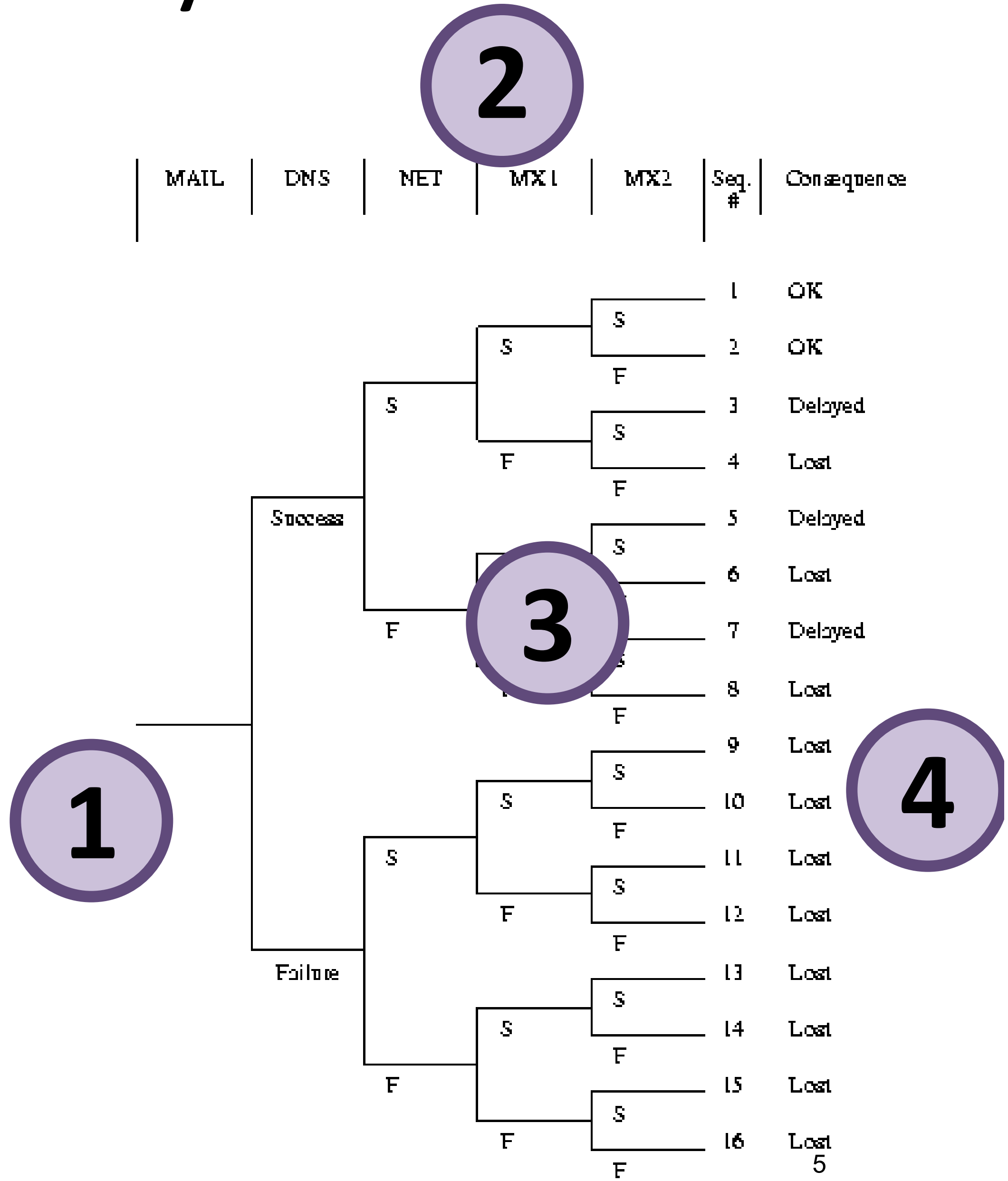
Event Tree Analysis

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



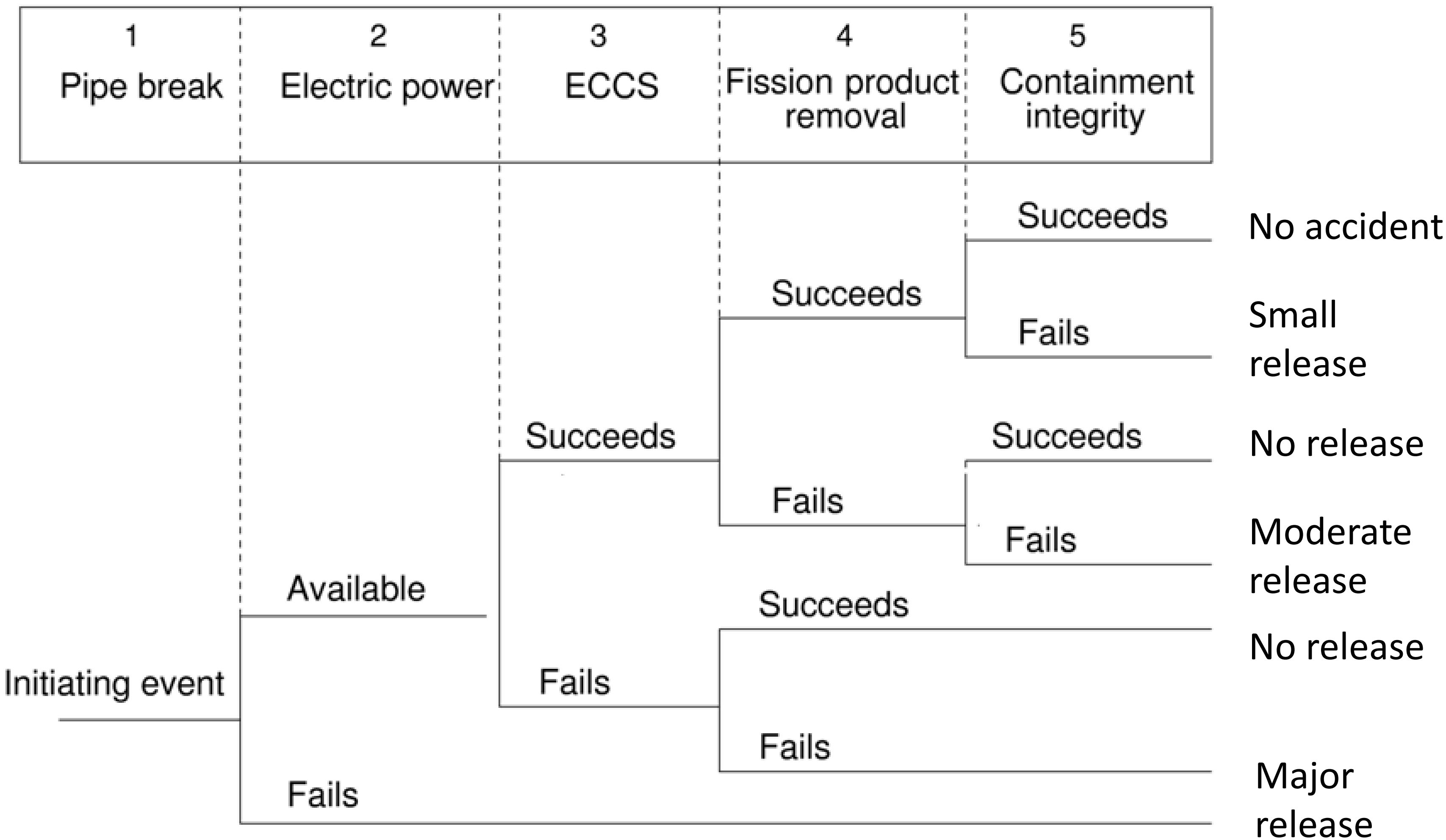
Event Tree Analysis: Process

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

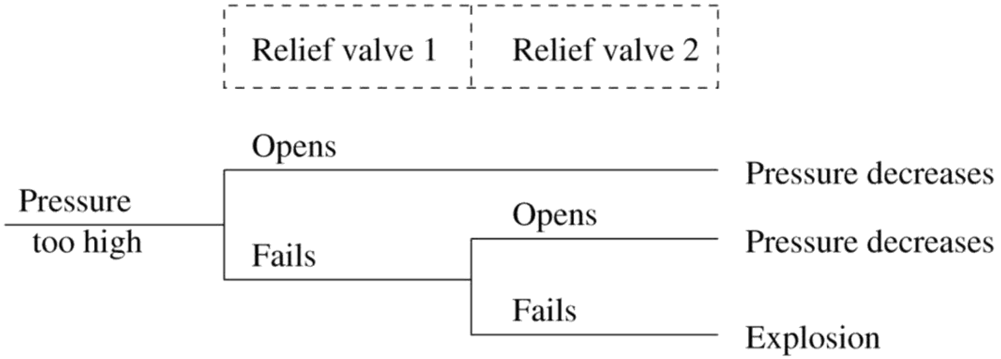


Courtesy of USENIX. Used with permission.

Event Tree Example



Event Trees
vs.
Fault Trees

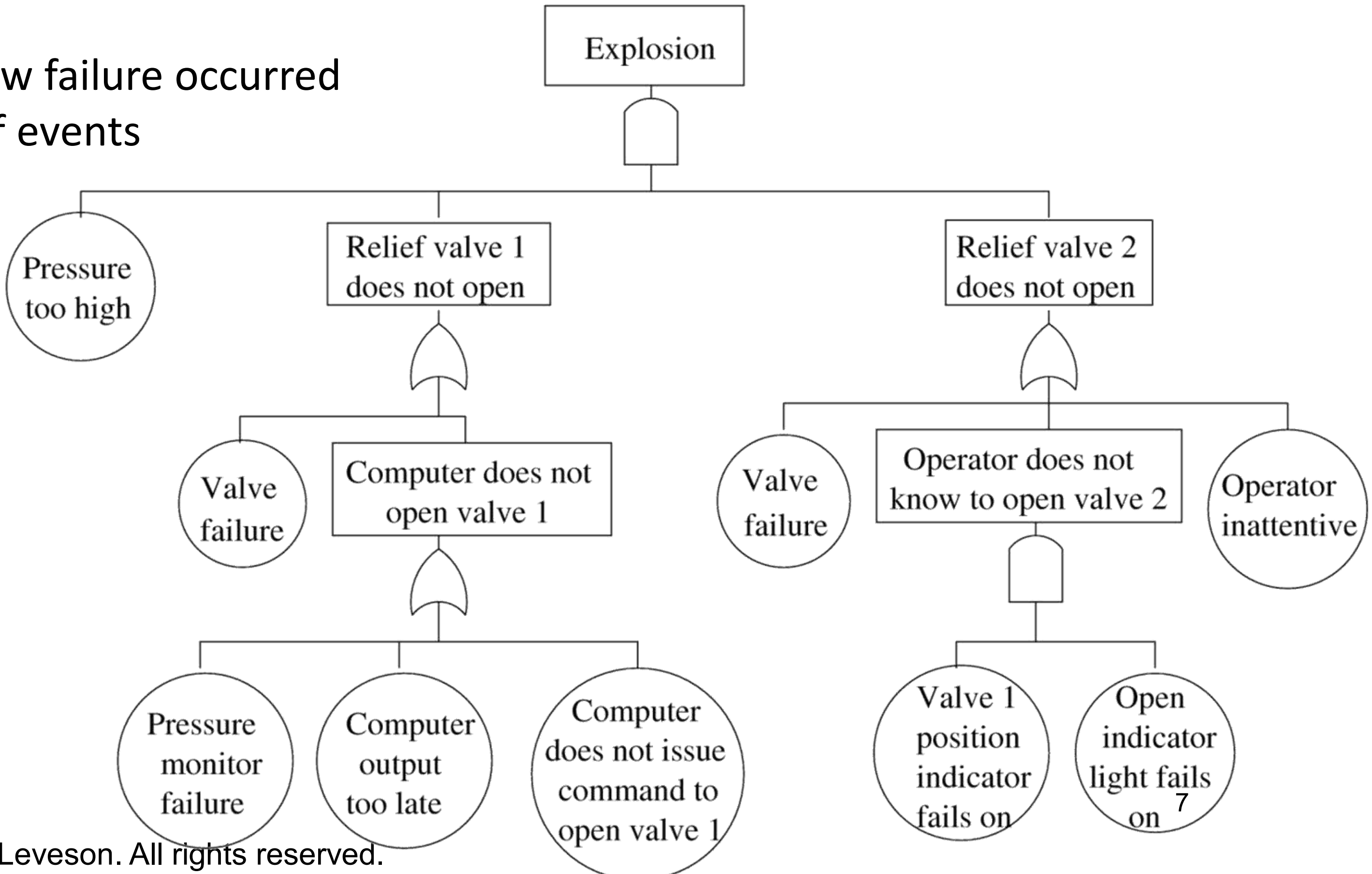


Event Tree

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

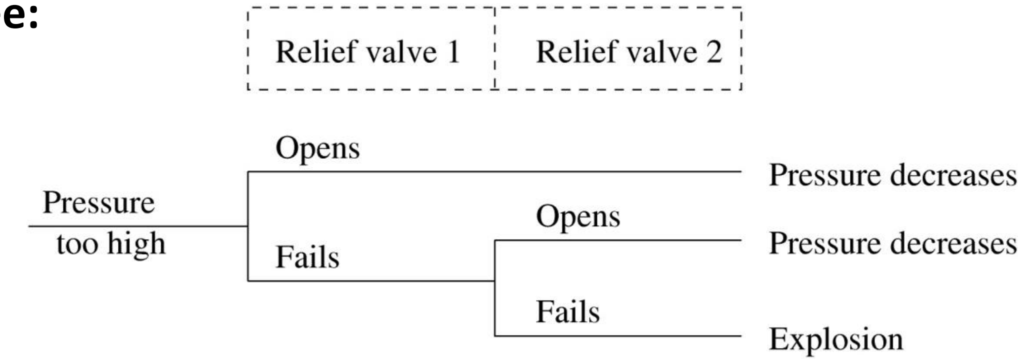
Fault Tree

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

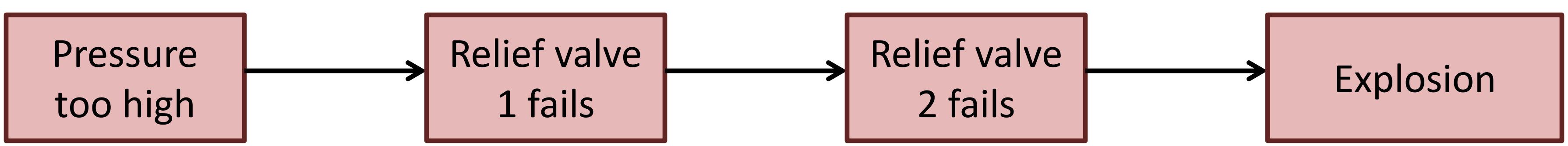


ETA uses an accident model

Event Tree:



Accident model: Chain-of-events



Event Tree Analysis: Exercise

Elevator

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

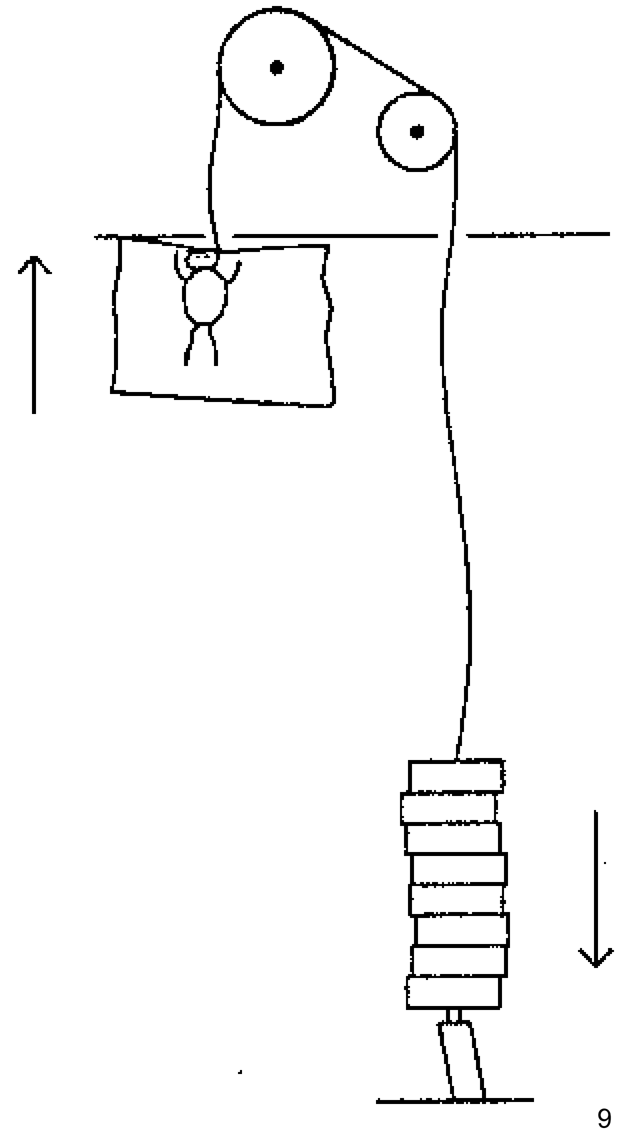


Image : Public Domain. USMSHA.

Event Tree Analysis: Exercise

Images removed due to copyright restrictions. See: http://science.howstuffworks.com/science-vs-myth/everyday-myths/question730.htm

What are the barriers?

Event Tree Analysis: Strengths

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

Event Tree Analysis: Limitations

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

Event Tree Analysis: Limitations (cont)

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

HAZOP
Hazard and Operability Analysis

HAZOP: Hazards and Operability Analysis

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

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)

Figure removed due to copyright restrictions. See: Leveson, Nancy. *Safeware: System Safety and Computers*. Addison-Wesley Professional, 1995. pp. 337.

HAZOP Strengths

- Considers more than failure accidents
- Can identify **new hazards**
  - Not limited to previously identified hazards
- **Easy** to apply
  - A simple method that can uncover complex accidents
- Applicable to **new designs** and new design features
- Performed by **diverse study team**, facilitator
  - Method defines team composition, roles
  - Encourages cross-fertilization of different disciplines

HAZOP Limitations

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

Quantitative Methods

Quantitative methods

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

- Seems intuitive to multiply:

  Risk = Severity * Likelihood

Quantitative methods

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

Good assumptions?

Quantitative methods

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

Good assumptions?

-Software?

-Humans?

-Hardware?

Risk Matrix

- Based on common idea:

  Risk = Severity * Likelihood

Likelihood

Very Likely					
Likely					
Possible					
Unlikely					
Rare					
	Negligible	Minor	Moderate	Significant	Severe

Severity

Risk Matrix

- Based on common idea:

  Risk = Severity * Likelihood

Uses expected values (averages)

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

Severity

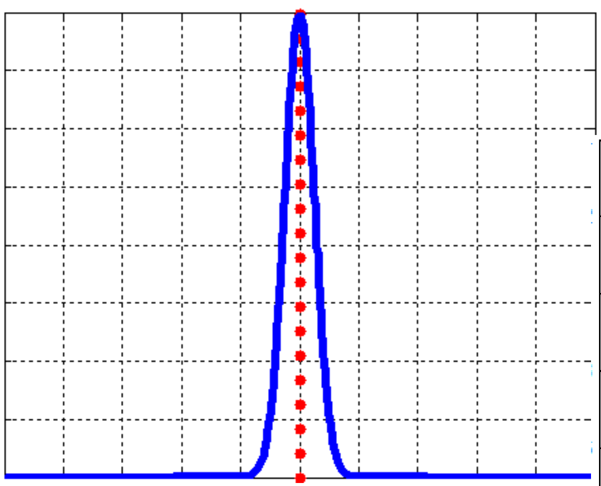
Expected Value Fallacy

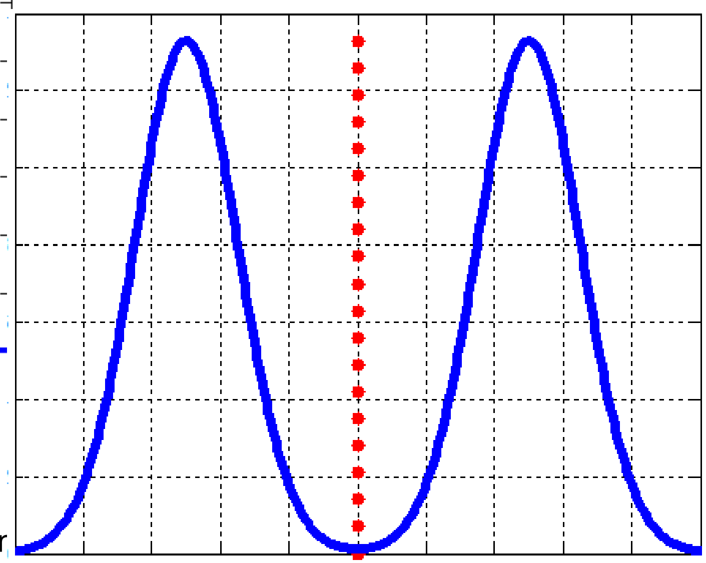
aka P-value Fallacy

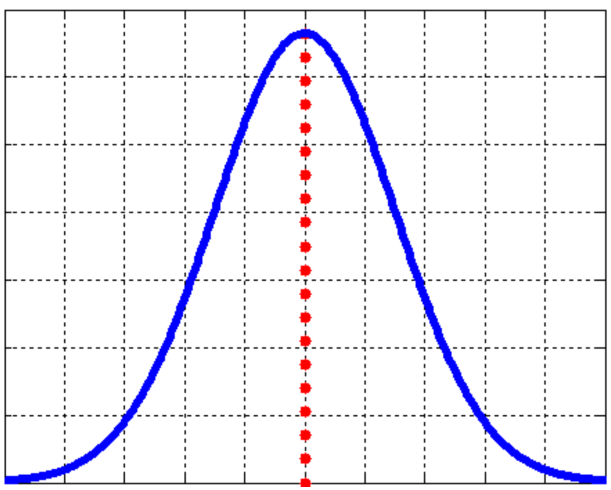
aka Flaw of Averages

aka Jensen's Law

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







Expected Value Fallacy

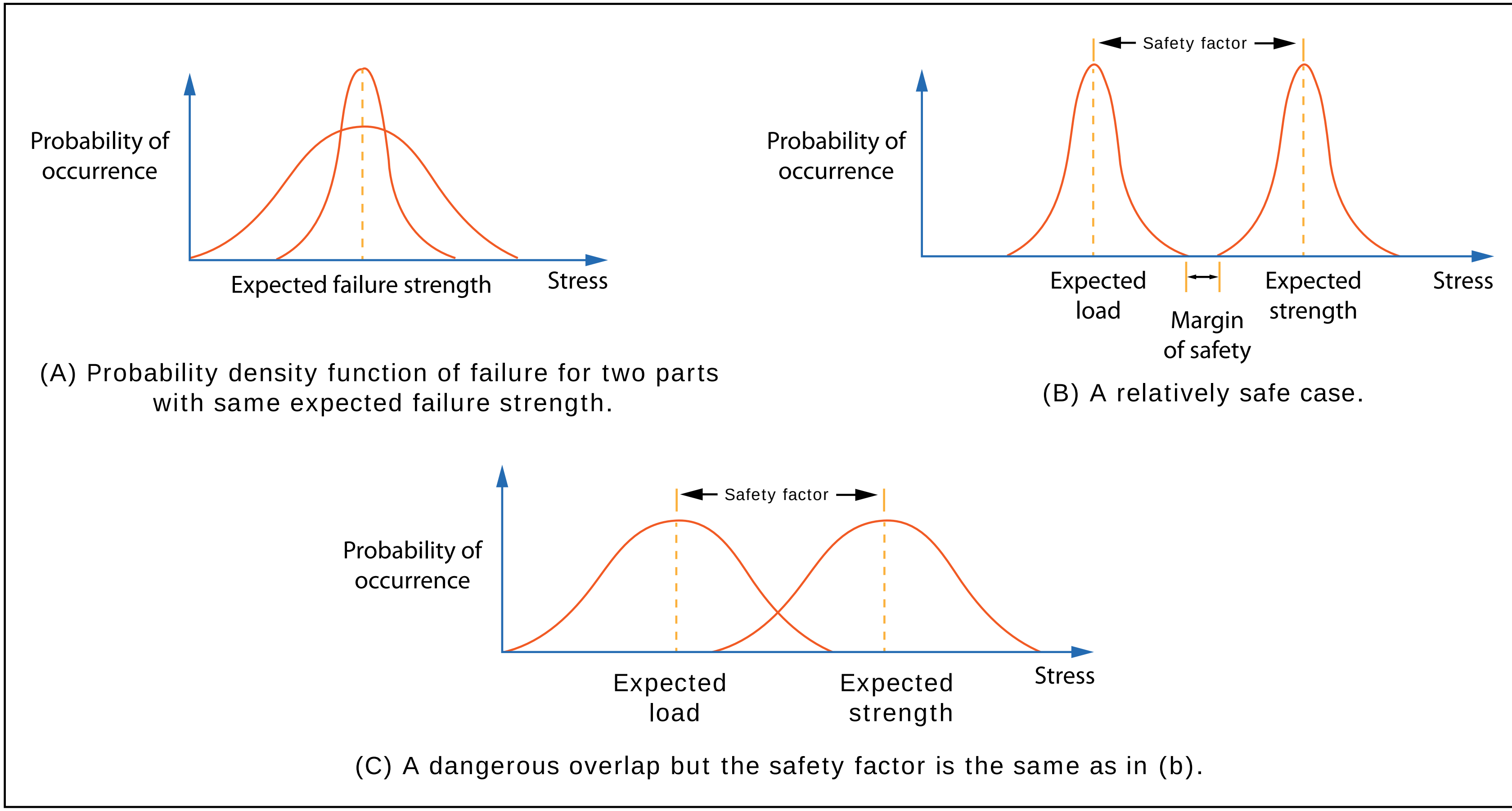
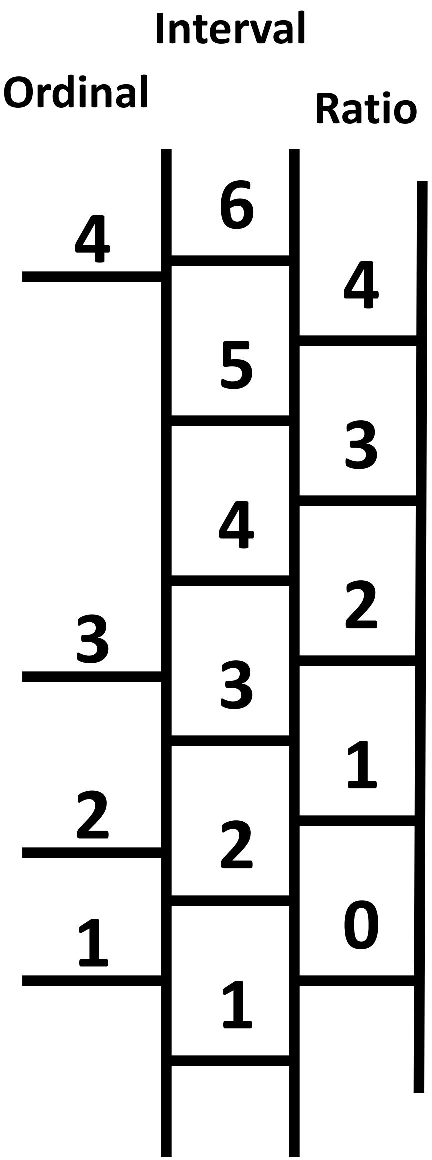


Image by MIT OpenCourseWare.

Remember this?

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 problem

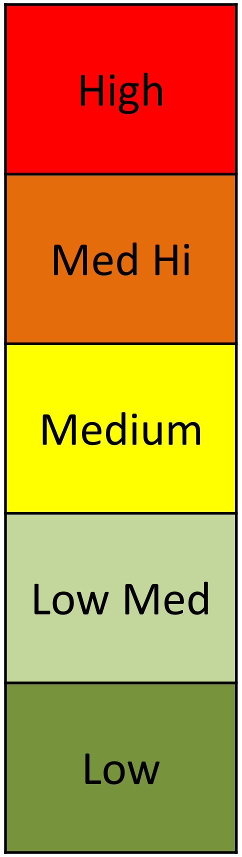
Another Example Hazard Level Matrix

	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 Assessment

- Not feasible for complex, human/computer controlled systems
- No way 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
  - Modern systems almost always involve new designs and new technology
    - Historical data may be irrelevant
- **Severity is usually adequate** to determine effort to spend on eliminating or mitigating hazard.

Hazard Level or Risk Level:



FMECA
Failure Modes Effects and Criticality Analysis

FMECA

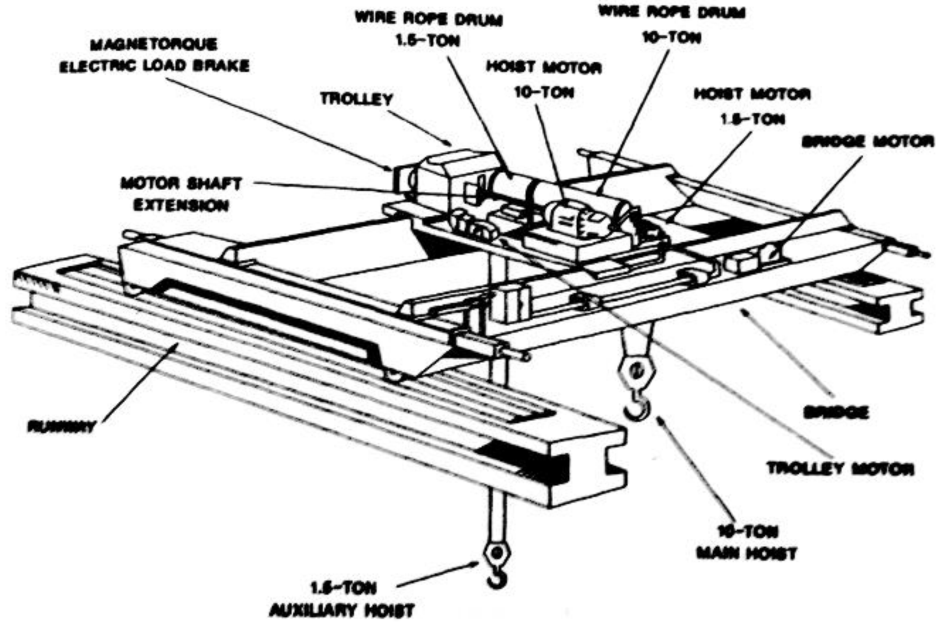
- Same as FMEA, but with “criticality” information

- Criticality
  – Can be ordinal severity values
  – Can be likelihood probabilities
  – An expression of concern over the effects of failure in the system*

*Vincoli, 2006, Basic Guide to System Safety

FMEA worksheet

Bridge crane system



Failure Mode and Effect Analysis

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

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

*FMEA example adapted from (Vincoli, 2006)

Severity Level Examples

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

*Otto et al., 2001, Product Design

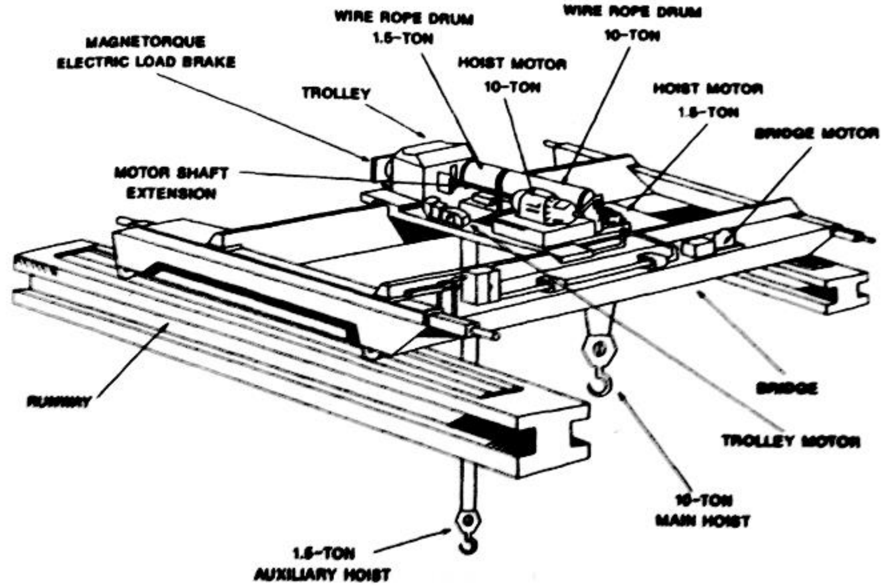
Severity Level Examples

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

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

FMEA 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)

Quantitative FTA

Quantitative Fault Tree Analysis

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

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

Any assumptions being made?

Quantitative Fault Tree Analysis

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

- AND gate
  - P(A and B) = P(A) * P(B)

Only if events A,B are independent!

- OR gate
  - P(A or B) = P(A) + P(B)

Only if events A,B are independent!

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

Quantitative Fault Tree Analysis

Fault trees removed due to copyright restrictions. See RTCA DO-312 Safety, Performance and Interoperability Requirements Document for the In-Trail Procedure in the Oceanic Airspace (ATSA-ITP) Application http://www.rtca.org/store_product.asp?prodid=1095.

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 and Relation to Quantitative Probability for Basic Causes

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

Image by MIT OpenCourseWare. Based on qualitative-quantitative conversion from RTCA DO-312.

Quantitative ETA

Quantitative Event Tree Analysis

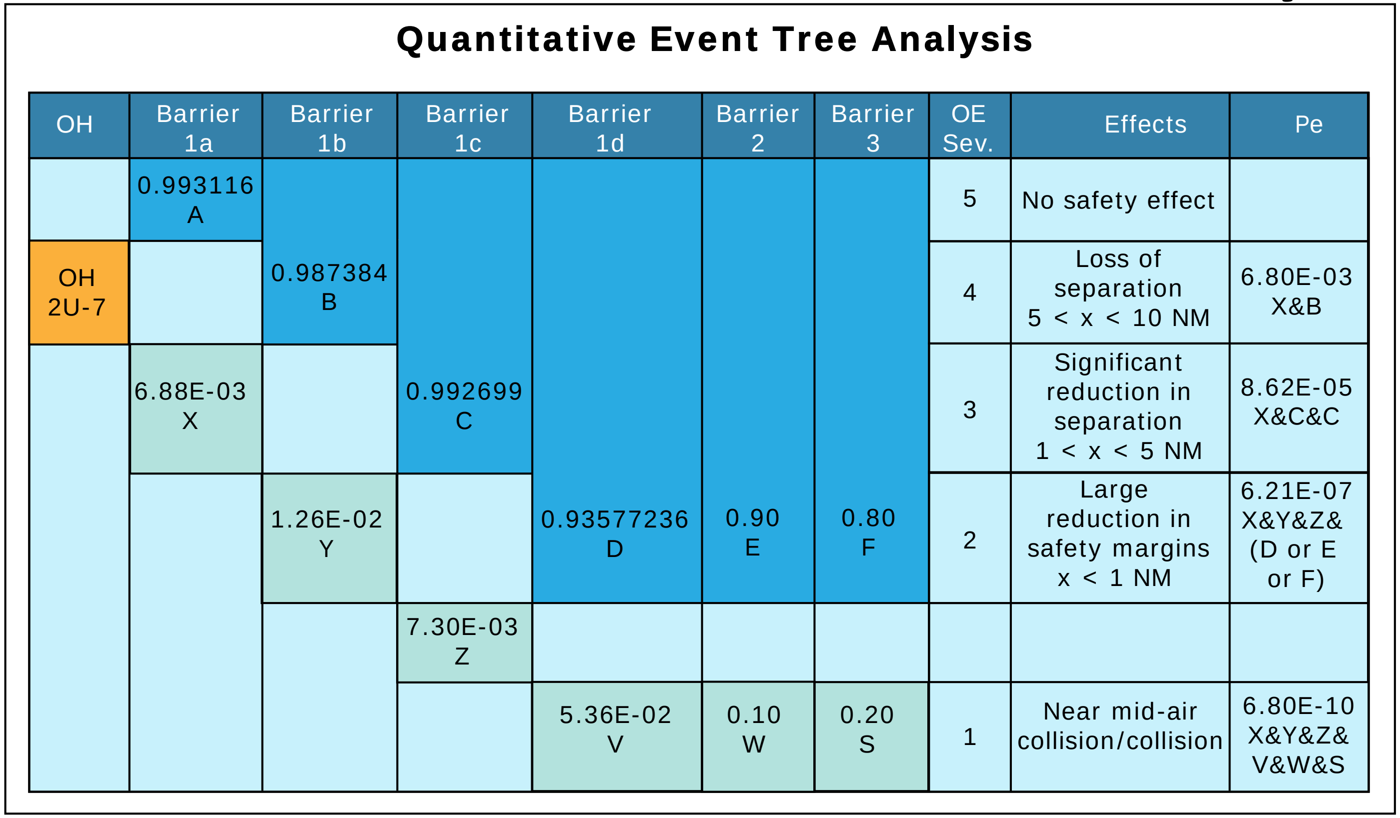


Image by MIT OpenCourseWare. Based on event tree from RTCA DO-312.

- 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

PRA
Probabilistic Risk Assessment

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

- 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

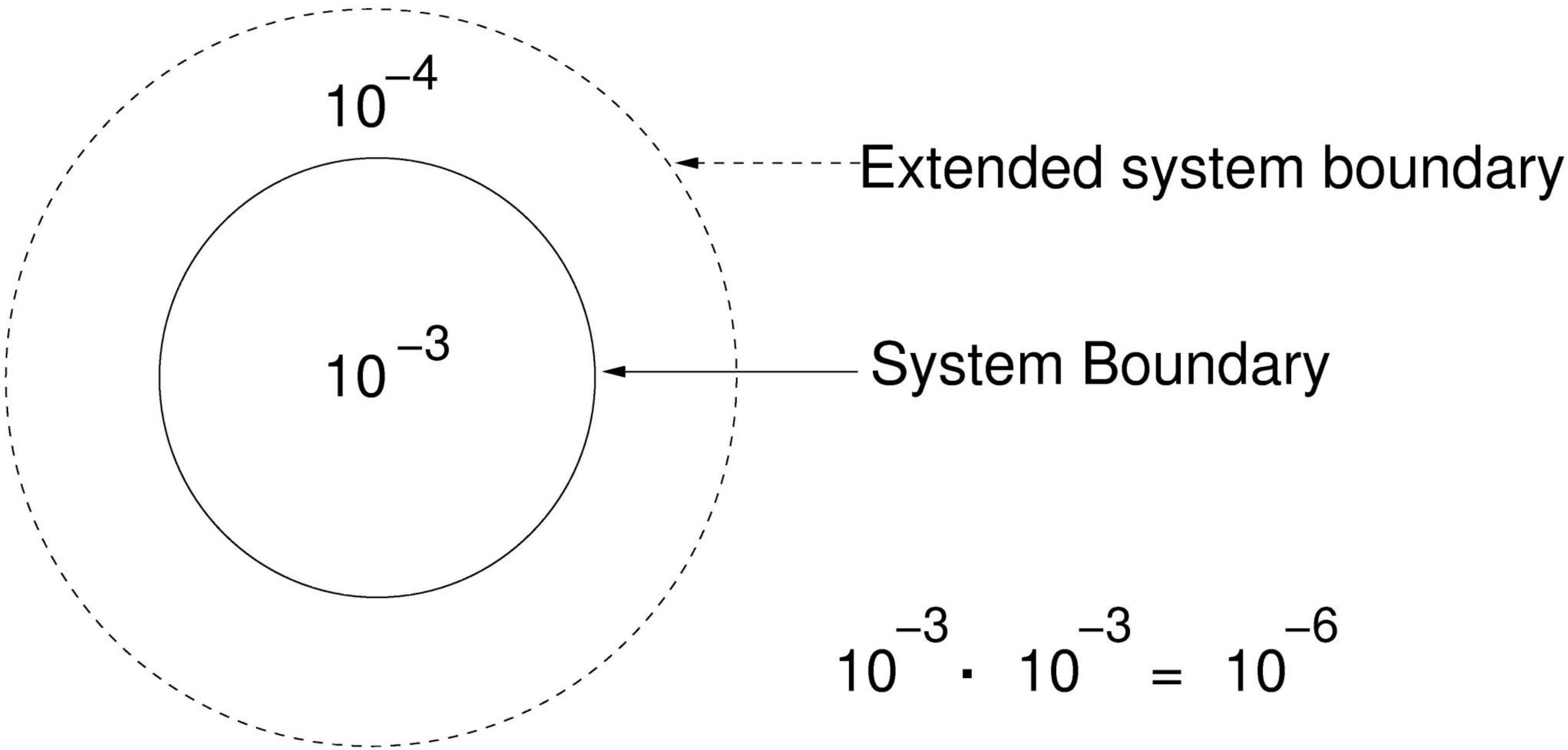
- In practice, models only include events that can be measured.
- Most causal factors involved in major accidents are unmeasurable.
  - Unmeasurable factors tend to be ignored or forgotten
- Can we measure software? (what does it mean to measure "design")?

"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:



Fukushima

- Power plants heavily based on probabilistic risk assessments
- Despite the reaction, probability theory is not really “safe” or “unsafe”
  - It just has certain limitations

16.63J / ESD.03J System Safety
Fall 2012