

Fault Tree and Success Tree Method: Construction, Quantification, Interpretation

Unit 10A

Spring 2022

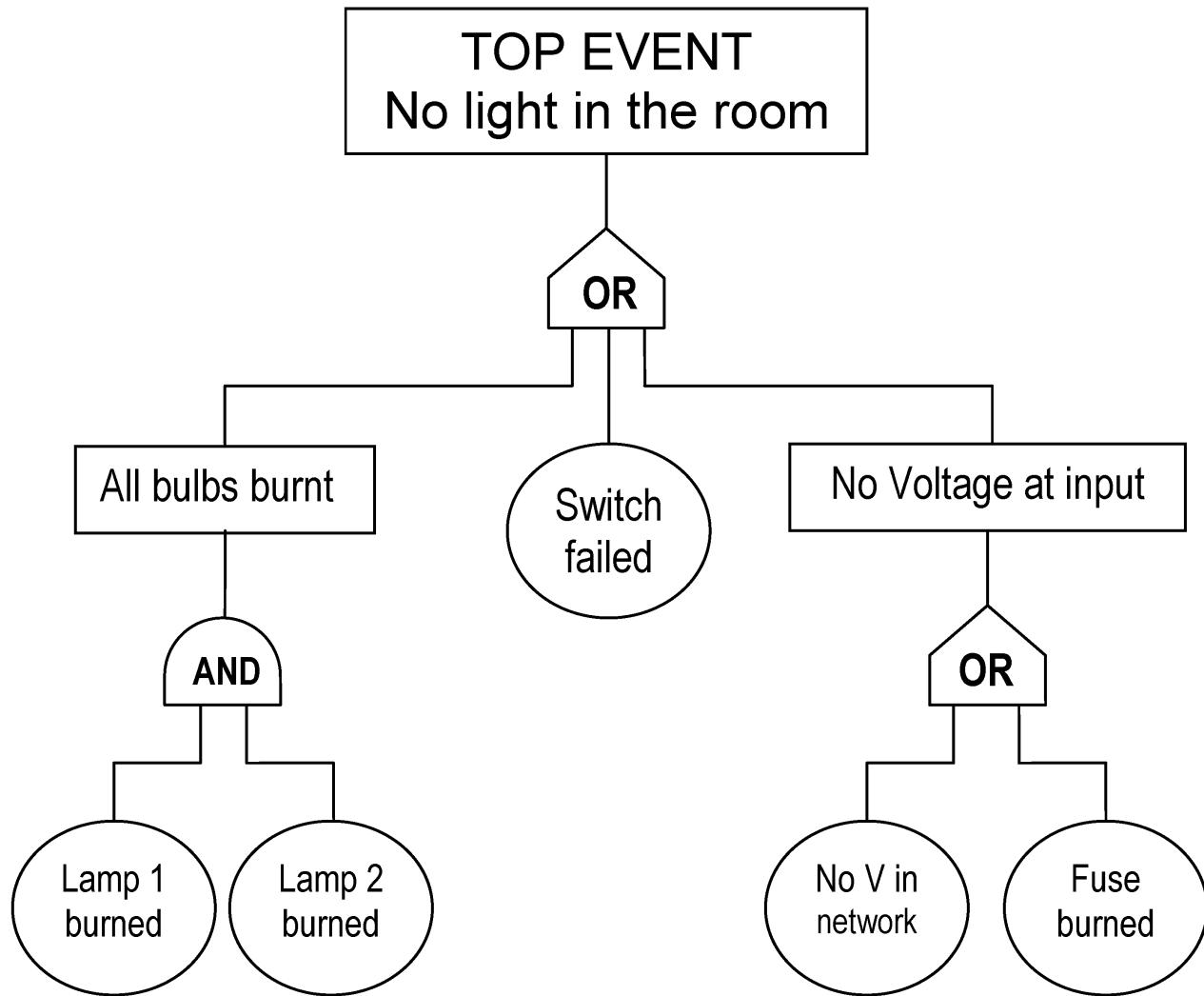
References

- Tweeddale, Mark, *Managing Risk and Reliability of Process Plants*, Elsevier, 2003
- Crowl, D.A. and Louvar, J.F., *Chemical Process Safety*, 4th ed, Prentice Hall, 2019
- Modarres, M., M. Kaminskiy, and V. Krivtsov, *Reliability Engineering and Risk Analysis*, 2nd ed, Taylor&Francis, 2010 (Modarres, RERA)
- Norman Fenton and Martin Neil, “Risk Assessment and Decision Analysis with Bayesian Networks,” CRC Press, 2nd ed., 2019, Chapter 5 (RDBN, 2019)
- Modarres, M., *Risk Analysis in Engineering*, Taylor&Francis, 2006 (Modarres, RAE)
- Rausand, Marvin, *System Reliability Theory*, 2nd edition, Wiley, 2004
- Jordaan, Ian, *Decisions Under Uncertainty— Probabilistic Analysis for Engineering Decisions*, Cambridge University Press, 2005 (Jordaan, 2005)

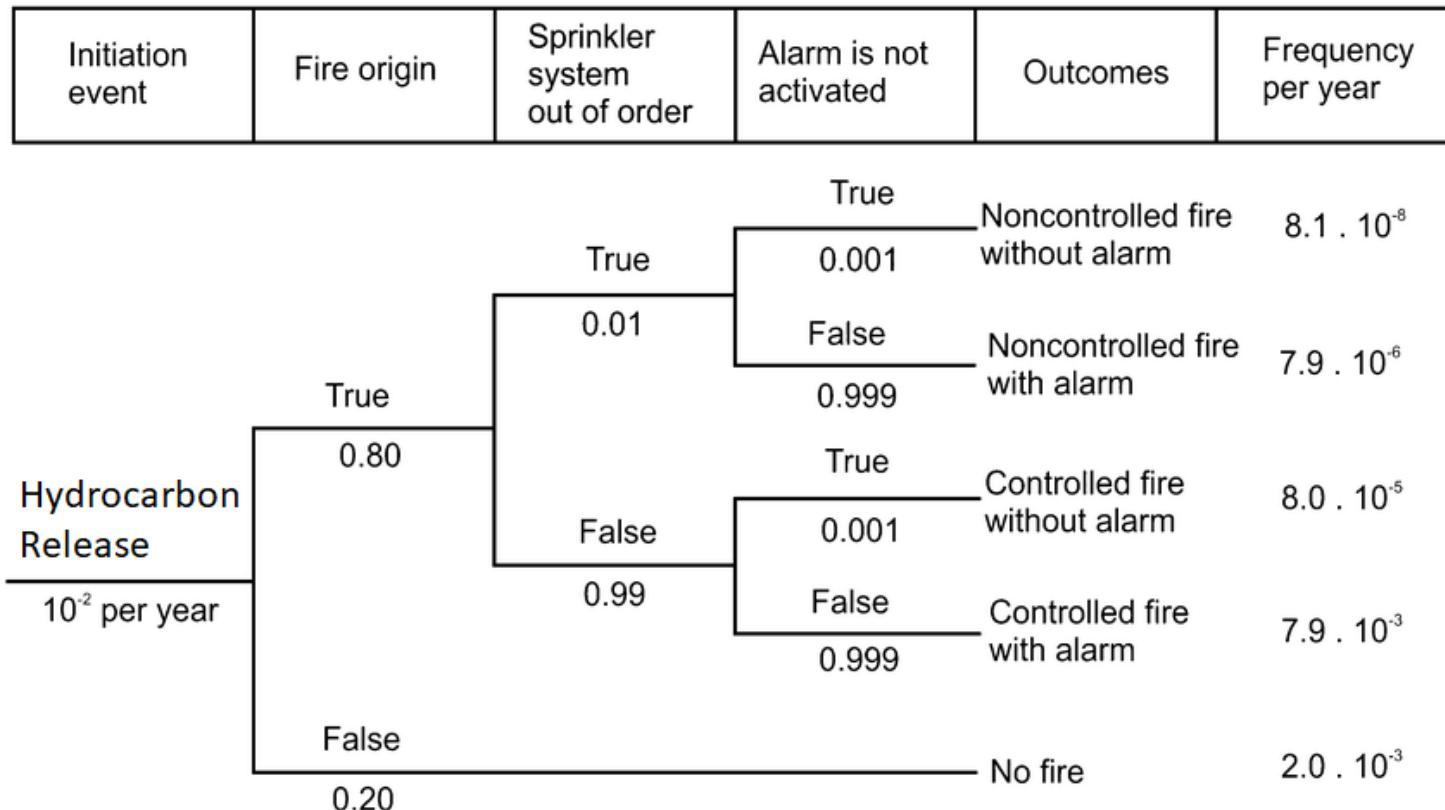
Fault Tree, Event Tree Analysis

- Fault Tree and Event Tree analysis (FTA, ETA) are Boolean (True/False, Fail/Success) logic diagrams for an initial screening approach to analyze system failures.
- A Fault Tree (FT) begins with a potential upset (Top Event), and works downward by diagraming through **Deduction** to show how the Top Event can result from earlier failure events.
- An Event Tree (ET) begins with an initiating event or a ‘top event’, and diagrams all potential events or outcomes by **Induction**.
- A FT top event is connected to lower level or earlier failure events through Boolean logic gates, such as: OR (union operation, \cup), AND (intersection operation, \cap).

Fault Tree Example



Event Tree Example

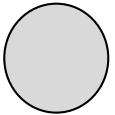


FT Construction

- Connect fault tree (FT) events and conditions via logic gates such as AND, OR.
- Continue deduction of underlying events to an appropriate event level designated ***Base Events*** involving components or human actions for which failure data are available.
- Generally all modeled FT events are **considered independent**, which is unrealistic, so this approach is useful for an initial screening but not sufficient by itself for Social-Technical System event modeling.
- For a System approach, Fault Trees are converted to **Bayesian networks to model dependencies**, multiple states, and to include discrete and continuous distributions and estimates of uncertainties.

Fault Tree Symbols

Basic Event



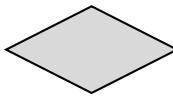
A simple primary event (e.g., a component or human action)

Intermediate Event



Occurs as a result of events at lower levels above base units

Undeveloped



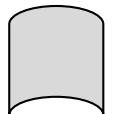
An event for which there is little information about primary events

“And” Gate



Output occurs only if all input events occur

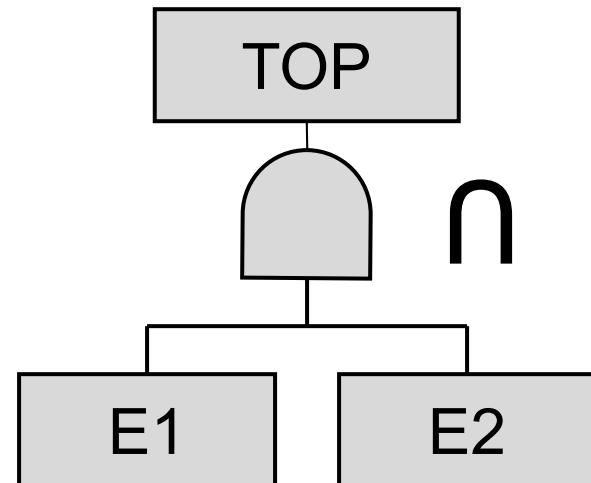
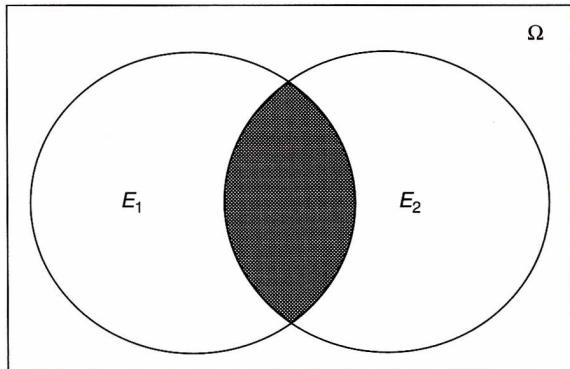
“Or” Gate



Output occurs if any (1 or more) input event occurs

Fault Tree AND-Gate, Intersection

8



Basic events E_1 and E_2 are basic events

The TOP event failure probability, Q_T , at time t is:

$$Q_T = P(E_1 \cap E_2) = P(E_1 | E_2) \cdot P(E_2) = P(E_1) \cdot P(E_2)$$

(~ independent)

With a single AND-gate and $n \sim$ independent basic events occurring at time t,

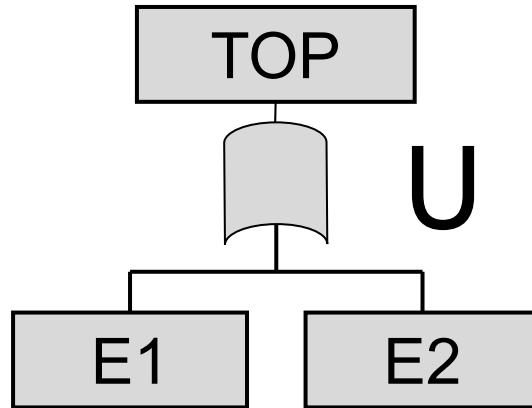
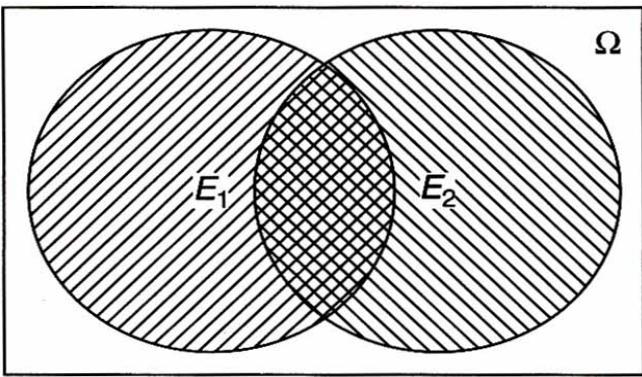
$$Q_T(t) = \prod_{i=1}^n Q_i(t)$$

$Q_i(t) = P(\text{failure})$ of unit i

8

Fault Tree OR-Gate, Union

9



E_1 and E_2 are basic events

The TOP event failure probability at time t is:

$$Q_T = P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2)$$

$$= Q_1 + Q_2 - Q_1 \cdot Q_2 \leftarrow (\text{independent})$$

Compensate for overlap

With a single OR-gate and n basic independent events occurring at time t,

$$Q_T(t) = 1 - \prod_{i=1}^n [1 - Q_i(t)]$$

9

OR-Gate, Rare Event Approximation

- The general expression for OR-gate, given independent Q_i events, adjusts for Q_i event overlap or co-occurrence:

General OR-Gate Expression:

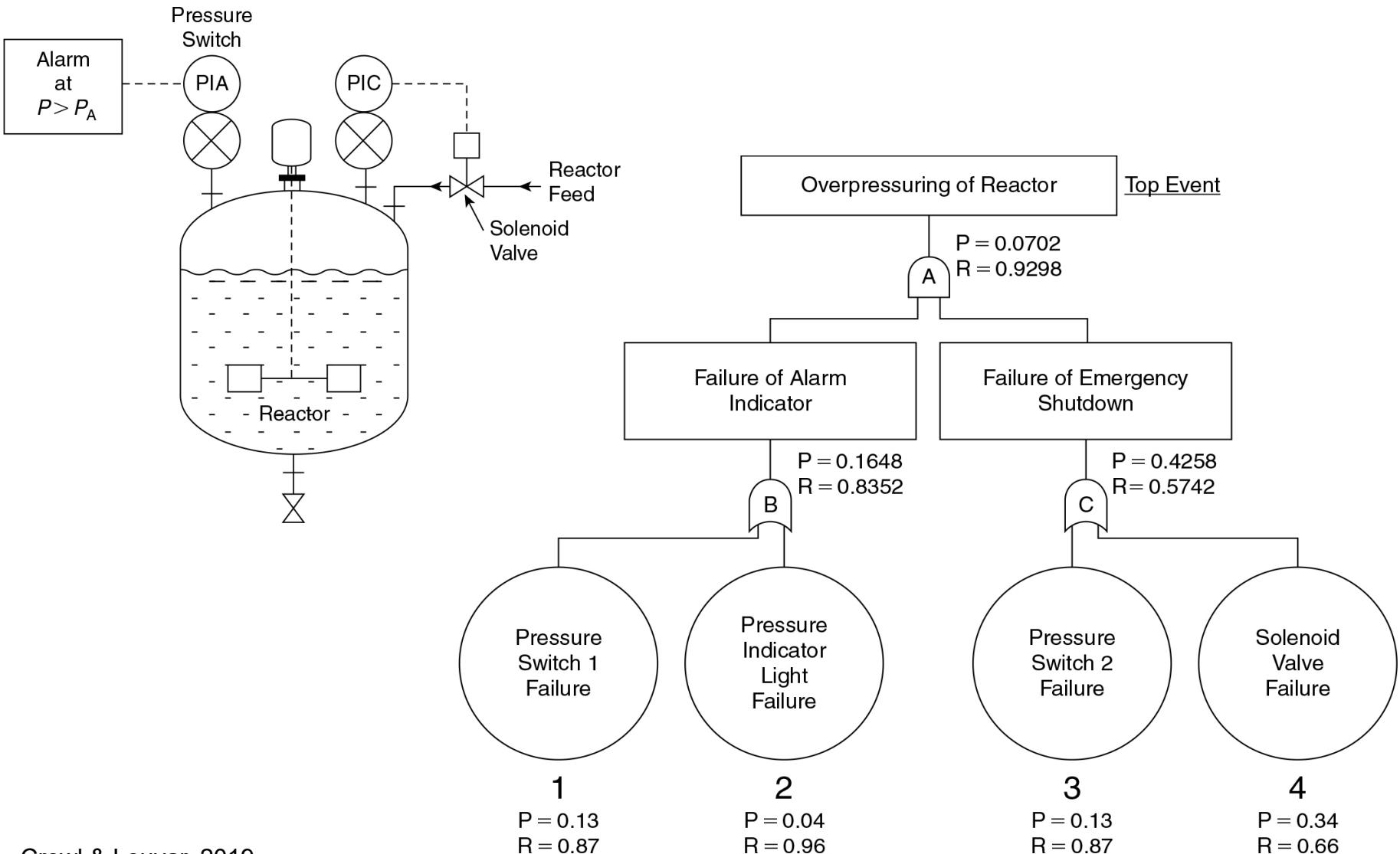
$$Q_T(t) = 1 - \prod_{i=1}^n [1 - Q_i(t)]$$

- If the events are rare events, probabilities of occurrences are very low (so values of Q_i are very small)
- When the Rare Event Approximation (REA) is conditionally acceptable:

OR-Gate Expression with REA:

$$Q_T(t) = \sum_i Q_i$$

Fault Tree Example 1: Reactor Overpressure



OR-Gate , AND-Gate

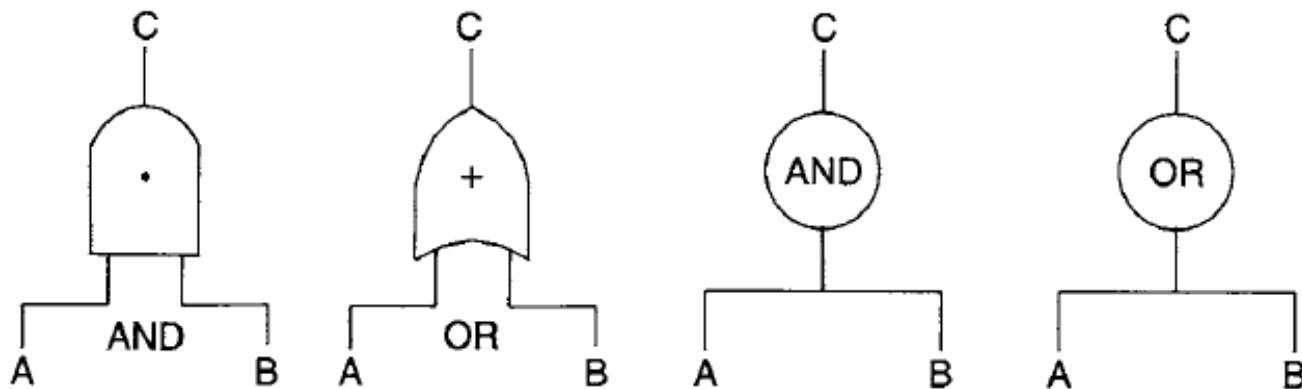


Figure 6-1. Logic gates—alternative representations.

Example 2: Hot Oil Heating System

- Heating section supplying hot oil to bitumen tanks
- Flow through heater must be maintained or heater coils may overheat, rupture, and result in a fire.
- Flow control valve, FCV, opens progressively if flow to heater drops (detected by FE) and recirculates oil back to pump
- Manual bypass valve, MBV, for FCV maintenance.
- If flow is low, FE actuates FS. FS warns operator (through FAL) and also actuates solenoid to close fuel gas supply (TCV), which reduces temperature in heater
- If high temperature switch, TSH, detects extreme high temperature in the output line, it closes TCV
- For this system, construct a Fault Tree based on current knowledge and understanding of the system operation.

Process Control

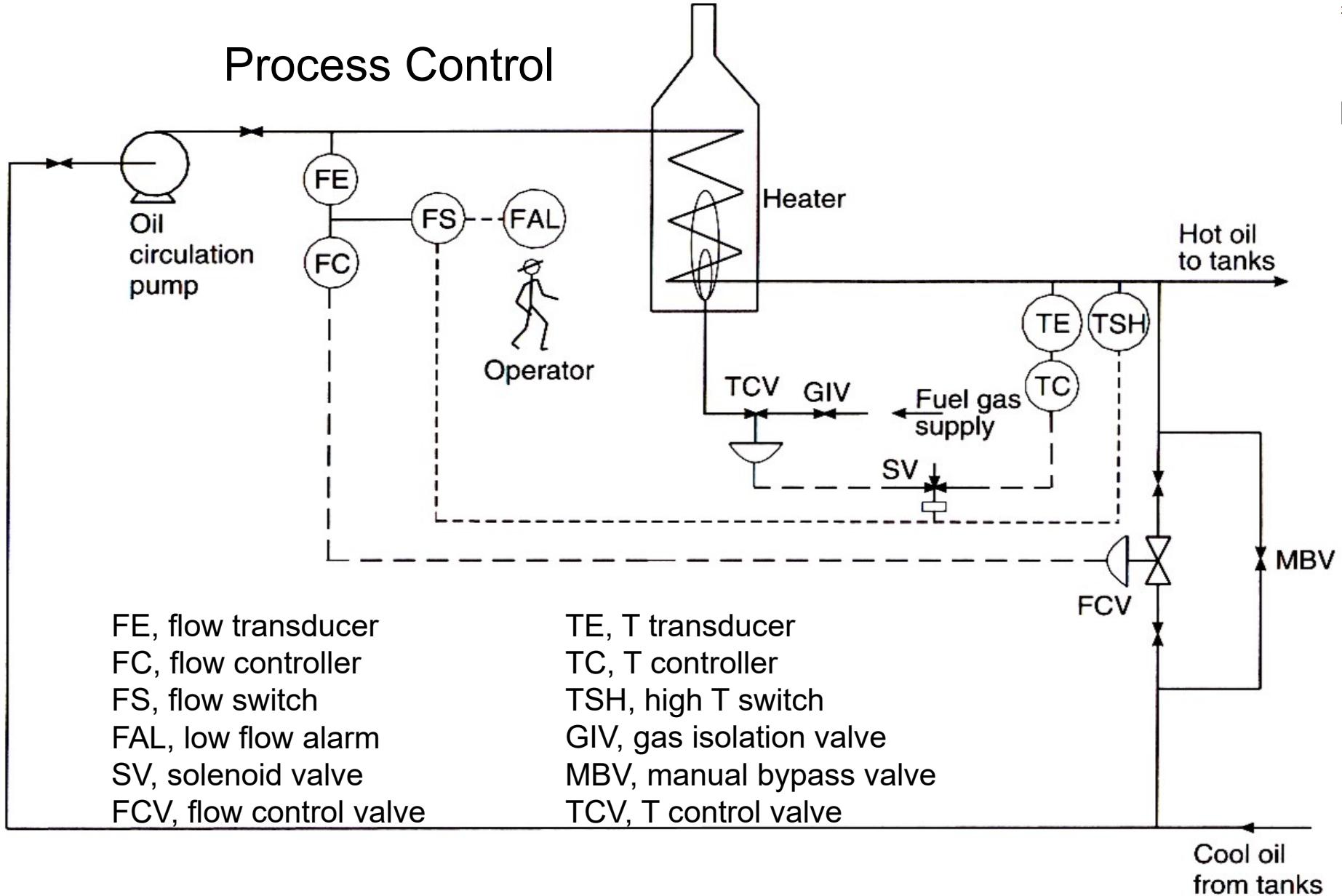


Figure 6-2. Hot oil heating system.

Hazard Identification

- How to diagram the system and develop failure scenarios? Begin by identifying and characterizing the hazards.
- What are the hazards of this oil heating system?

FTA for Heater Coil Burn Out

- For heater Coil Burn Out as the upset (top) event, identify triggering events or system demands:

No or low oil flow:

- Pump failure
- Flow control system failure
- Oil leak (large)
- Pipeline blockage
- Valve closed
- Operator failure to respond to low flow alarm, FAL

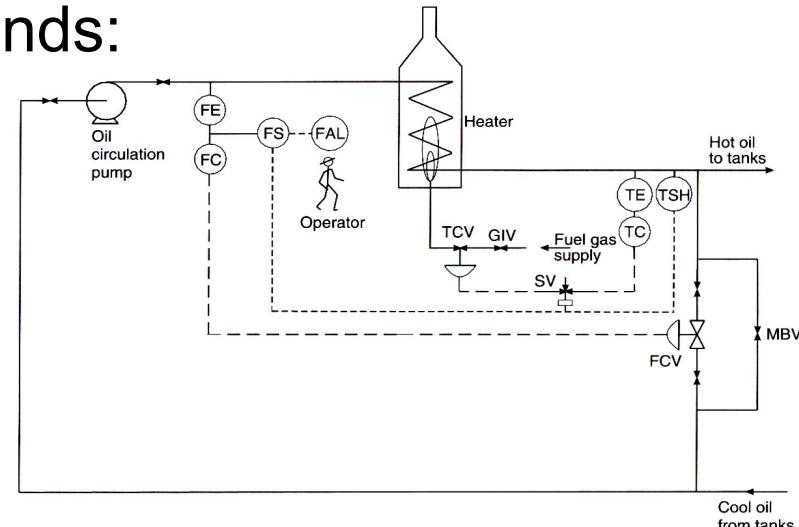


Figure 6-2. Hot oil heating system.

Excess Gas Flow

- Gas flow control system failure

Note: Human and Organizational factors influence all events including test and maintenance, training, leadership etc., but are not modeled explicitly in a Fault Tree

Analyze System from the Logic Diagram

17

- We will focus on heater coil burn-out due to pump failure
 - Over-temperature protection system, (TSH, SV) does not operate if pump stops, because there is insufficient flow to the TSH sensor
 - The oil in the heater can overheat and cause heater coil burn out
 - if pump stops
 - **OR** low flow protection system (FS, SV) fails
 - **OR** FAL(low flow alarm) fails,
 - **OR** operator, OP, fails to cut off fuel to the heater.

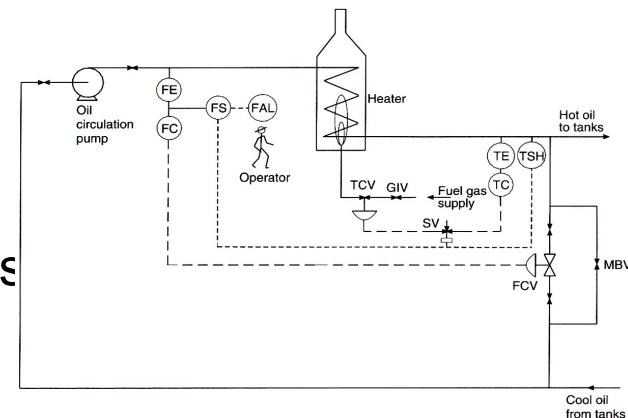
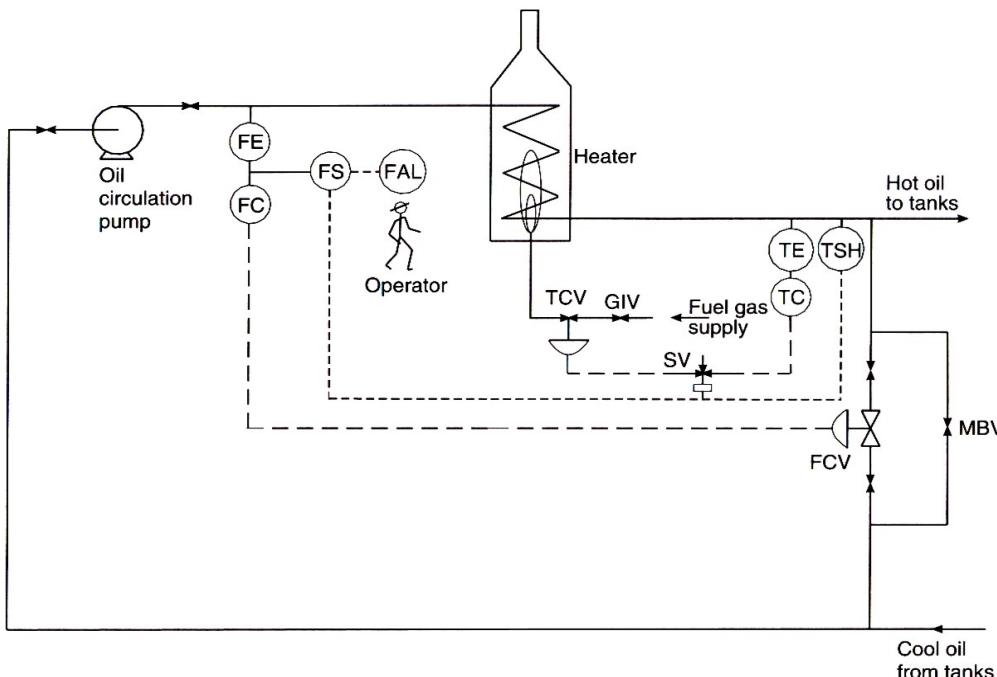


Figure 6-2. Hot oil heating system.

Coil Burn Out Fault Tree Construction

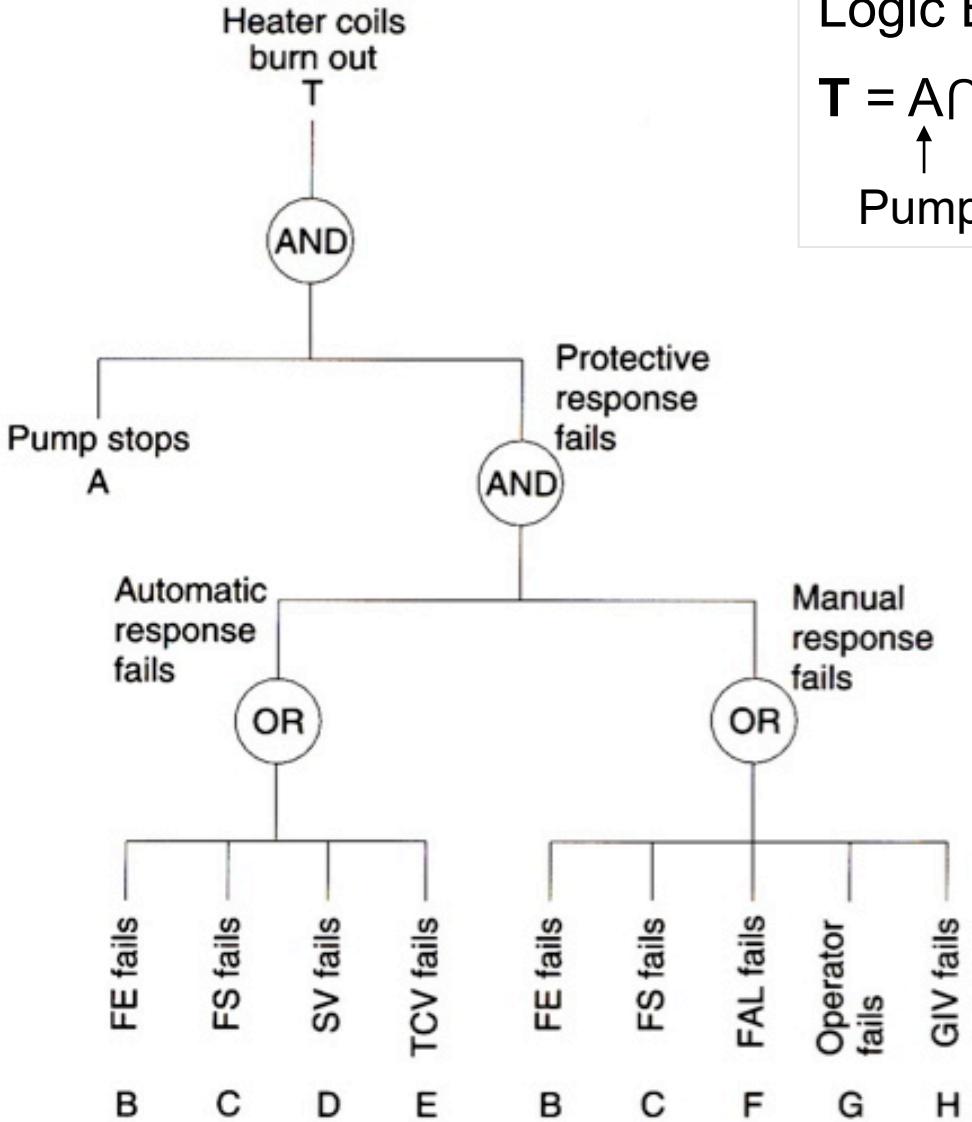
18

- Causes of **Automatic Response failure**: either FE fails OR FS fails OR SV fails OR TCV fails
- Causes of **Manual Response failure**: either FE fails OR FS fails OR FAL fails OR the operator fails OR GIV fails
- Can pump failure itself lead to a coil burn out?



Initial FT and Logic Based on Understanding of System

19

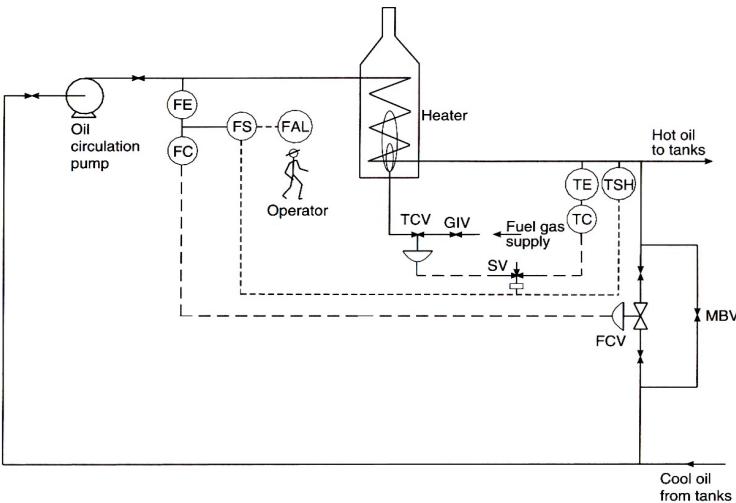


Logic Expression:

$$T = A \cap [(B \cup C \cup D \cup E) \cap (F \cup G \cup H)]$$

↑ ↑ ↑

Pump Automatic response Manual response



(Tweeddale, 2003)

Review: FT Logic Representation

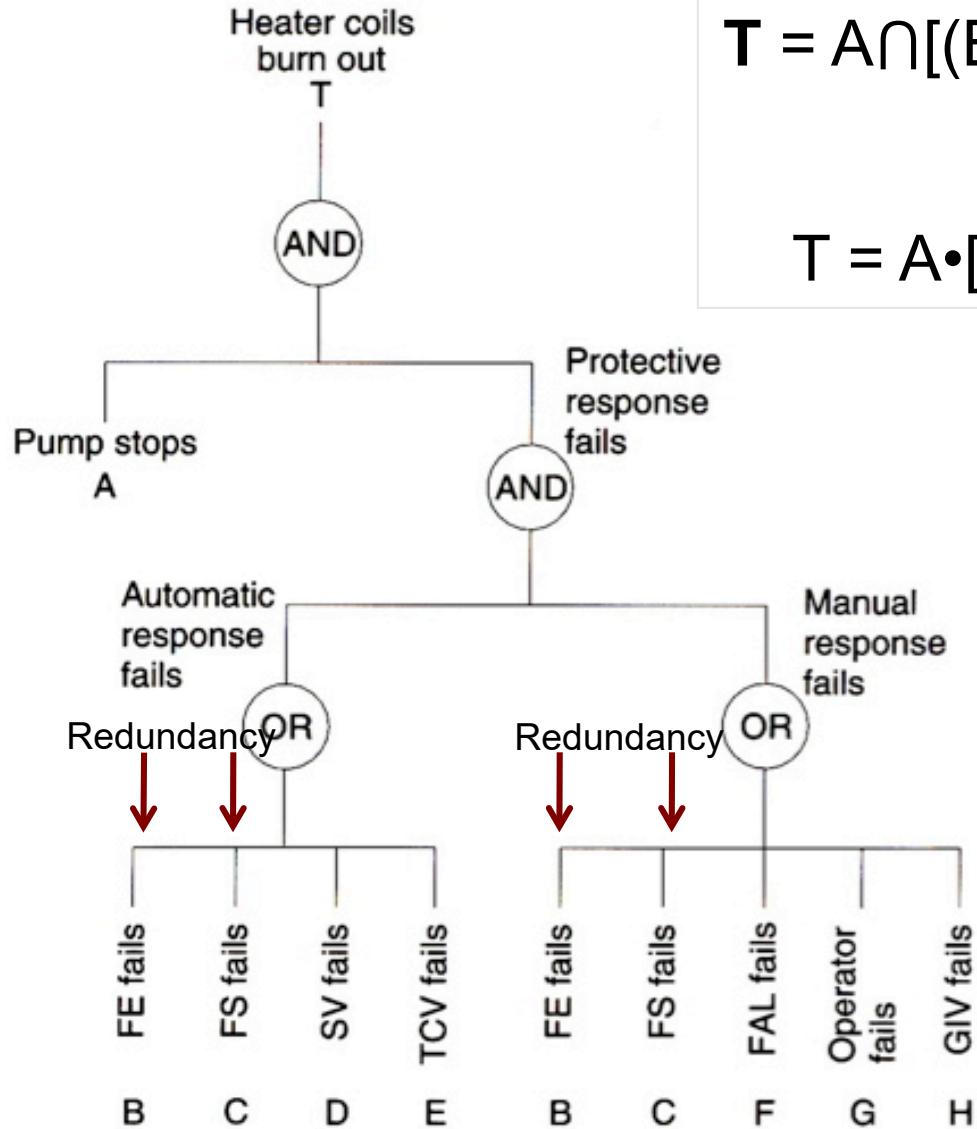
- Represent the mishap or top event by T.
- Events leading to T are represented by letters for system components (from the initial FT).
- Based on approximations, the FT logic can be quantified by converting the Boolean operators or gates to arithmetic operations with approximations (for simplicity):

$$T = A \cdot (B + C + D + E) \cdot (B + C + F + G + H),$$

which follows from **what two assumptions or approximations?**

Modified FT and Logic Expression

21



$$T = A \cap [(B \cup C \cup D \cup E) \cap (B \cup C \cup F \cup G \cup H)]$$

becomes

$$T = A \cdot [(B+C+D+E) \cdot (B+C+F+G+H)]$$

Note the Independence and REA assumptions/approximations in T.

$$\text{OR- Gate: } Q_T(t) = \sum_i Q_i$$

$$\text{AND- Gate: } Q_T(t) = \prod_{i=1}^n Q_i(t)$$

Letters A,B,... designate component failures

Pump Failure Demand Fault Tree



- From the initial fault tree construction, there are two components, FE and FS, that appear in more than one branch of the tree.
- Repetitions can lead to over-counting of failures and inaccurate top event frequency or probability calculations.
- Thus, an initial fault tree is *reduced* to remove repetitions
- From the initial FT prepare a *Reduced Fault Free*.

FT Reduction with Boolean Algebra, 1

- To simplify, the Top Event T logic expression is first expanded (and then reduced):

$$\begin{aligned} T &= A \cdot (B+C+D+E) \cdot (B+C+F+G+H) = \\ &A \cdot (B \cdot B + B \cdot C + B \cdot F + B \cdot G + B \cdot H + C \cdot B + C \cdot C + C \cdot F + \\ &C \cdot G + C \cdot H + D \cdot B + D \cdot C + D \cdot F + D \cdot G + D \cdot H + E \cdot B + E \cdot C + E \cdot F + E \cdot G + E \cdot \\ &H) \end{aligned}$$

Review: FT Reduction with Boolean Algebra

24

$$A \cup A = A \longrightarrow A \text{ OR } A = A$$

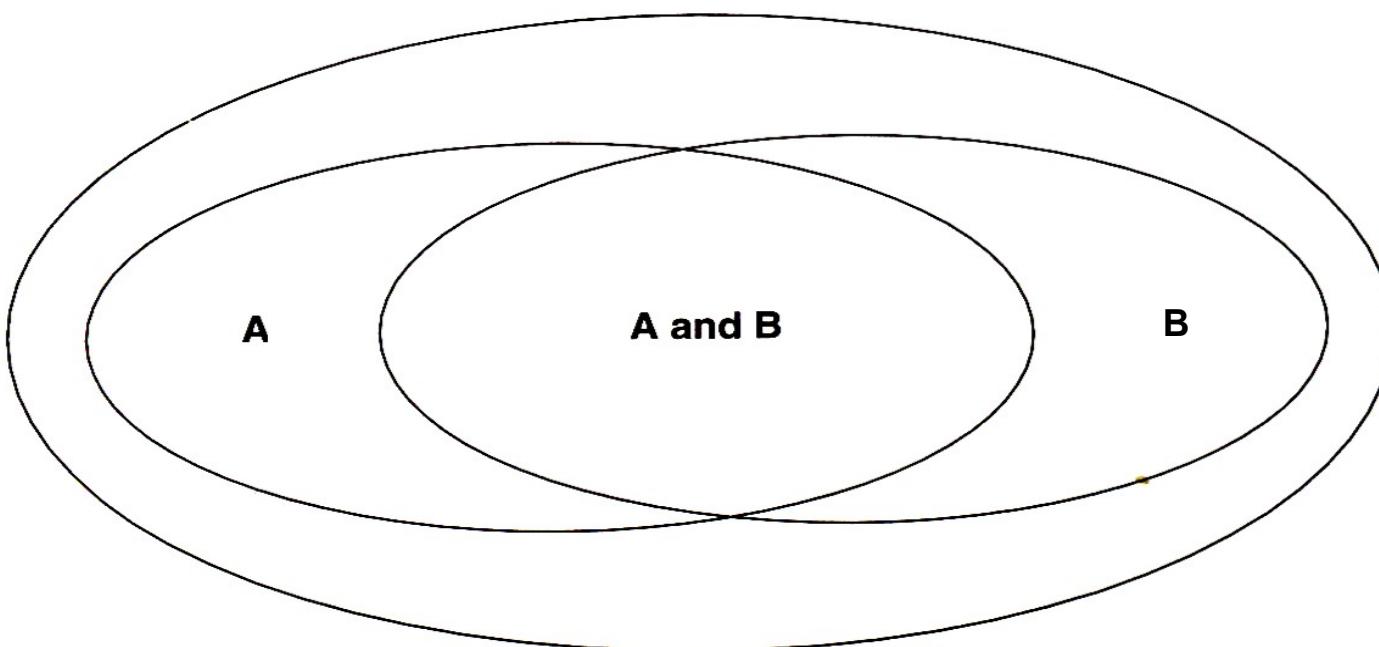
$$A \cap A = A \longrightarrow A \text{ AND } A = A$$

} Idempotent

$$A \cup (A \cap B) = A \rightarrow A \text{ OR } (A \text{ AND } B) = A$$

$$A \cap (A \cup B) = A \rightarrow A \text{ AND } (A \text{ OR } B) = A$$

} Absorption



FT Reduction with Approximations

25

Identify approximation used (rare event, REA, or mutually independent, MI).

$$A \cap A = A$$

$$A \cdot A = A$$

$$A \cup A = A$$

$$A + A = A$$

$$A \cup (A \cap B) = A$$

$$A + (A \cdot B) = A$$

Fault Tree Reduction

- Assume REA and mutual independence of components.
- To Reduce the Fault Tree we use the Idempotent and Adsorption identities to reduce the logic expression for the Top Event, T.

$$\bullet \quad T = A \cdot ($$

B

$$+ C \cdot B + C \cdot C + C \cdot F + C \cdot G + C \cdot H$$

$$+ D \cdot B + D \cdot C + D \cdot F + D \cdot G + D \cdot H$$

$$+ E \cdot B + E \cdot C + E \cdot F + E \cdot G + E \cdot H)$$

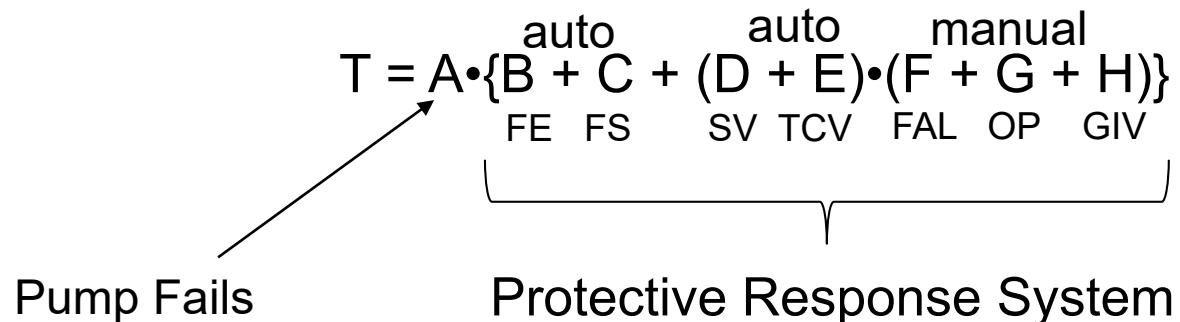
So, $T = A \cdot (B+C+D \cdot F+D \cdot G+D \cdot H+E \cdot F+E \cdot G+E \cdot H)$

Fault Tree Reduction

- $T = A \cdot (B + C + D \cdot F + D \cdot G + D \cdot H + E \cdot F + E \cdot G + E \cdot H)$
- Factor and group this logic expression of T to highlight system functions:

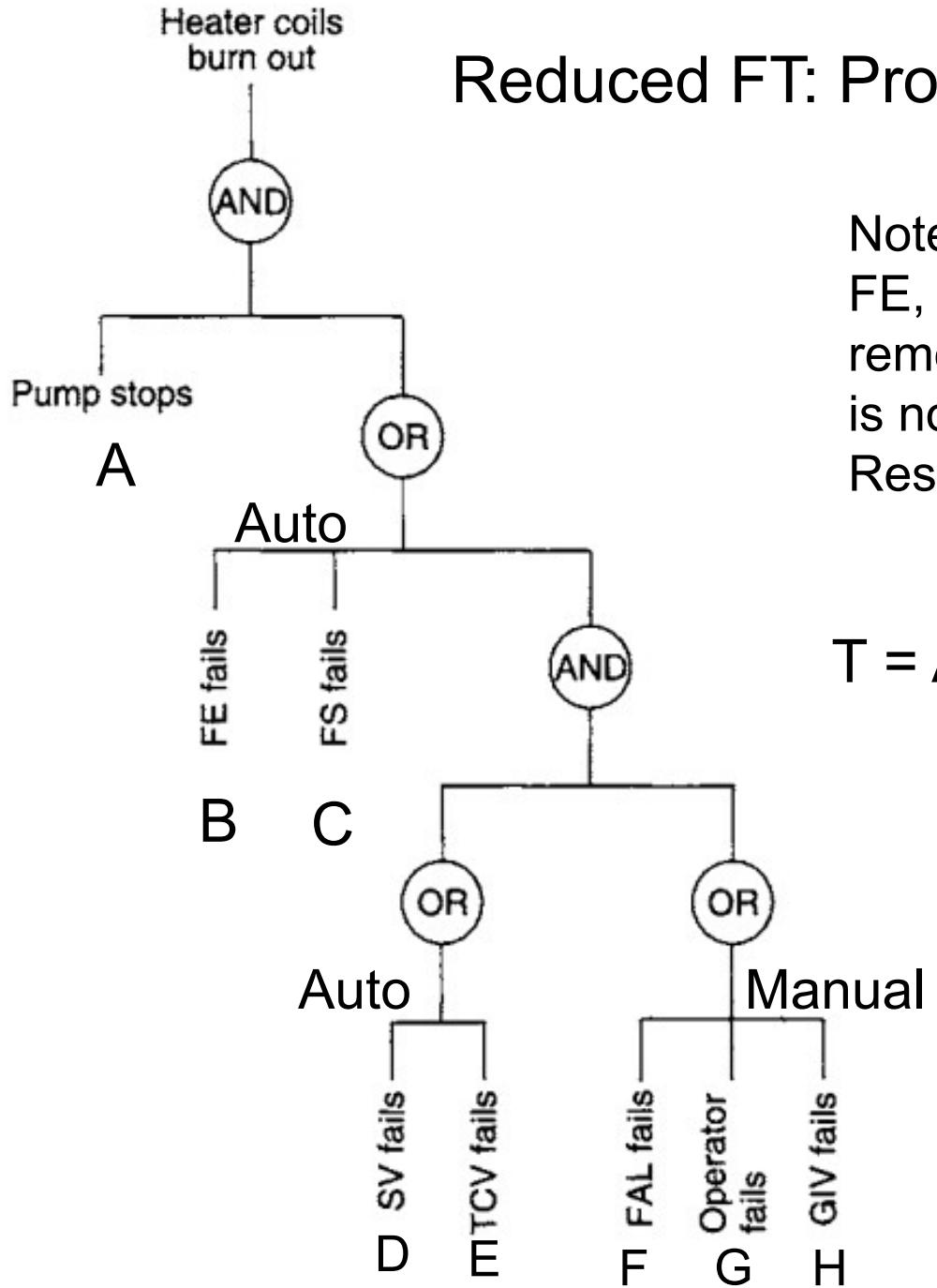
$$T = A \cdot \{B + C + (D + E) \cdot (F + G + H)\}$$

- State the logic expression in words (next slide).



Reduced FT: Protective Response System

28



Note that in the Reduced FT, the FE, FS redundancy has been removed, and the Auto Response is now separated from the Manual Response.

Logic expression:

$$T = A \cdot \{B + C + (D + E) \cdot (F + G + H)\}$$

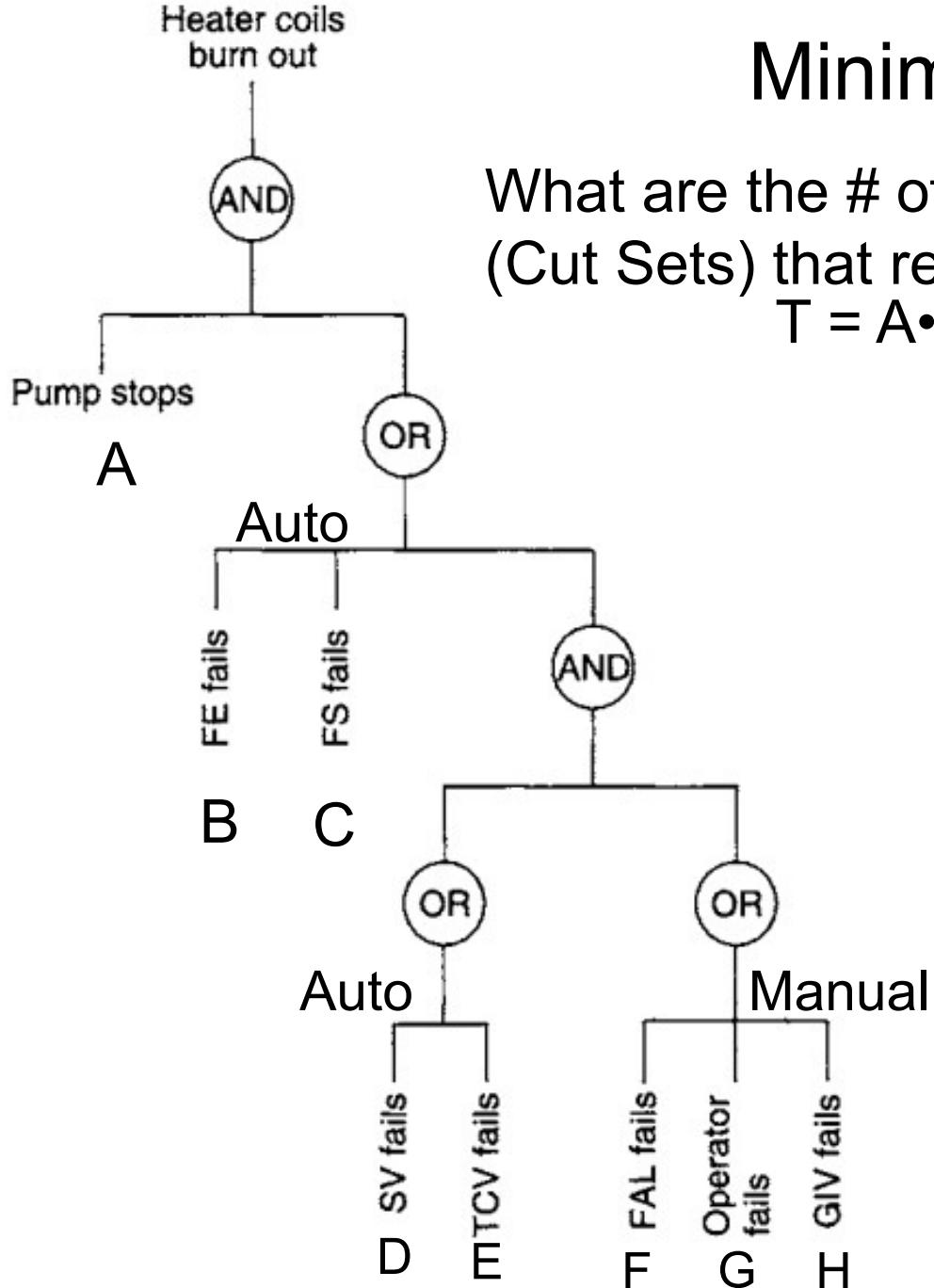
Fault Tree Following Reduction

- The heater coils will burn out if both the pump fails AND the Protective Response fails.
- The Protective Response fails if either FE fails OR FS fails OR if both failures occur.
- A combination of failures leading to failure of the Protective Response System occurs if there is (a failure of either SV OR TCV) AND (a failure of either FAL OR the operator OR GIV).
- How many minimum component failure scenarios are there?

FT Cut Sets

- A fault tree *Cut Set* is a unique set of events leading to the top event T.
- The simultaneous failure of each event in a set causes the top event to occur. Therefore, each cut set represents a failure scenario leading to T.
- By the simultaneous occurrence of each failure event within a cut set, each cut set inactivates or *cuts* all success paths to avert T.
- A *minimum cut set* is a set that cannot be reduced in size (number of components) and is determined directly from the Reduced Fault Tree, top event logic.
- A minimal cut set *fails* when all components of the cut set co-fail simultaneously.

Minimum Cut Sets



What are the # of minimum failure scenarios (Cut Sets) that result in T?

$$T = A \cdot \{B + C + (D + E) \cdot (F + G + H)\}$$

Cut Sets:

Rank 1:

Rank 2:

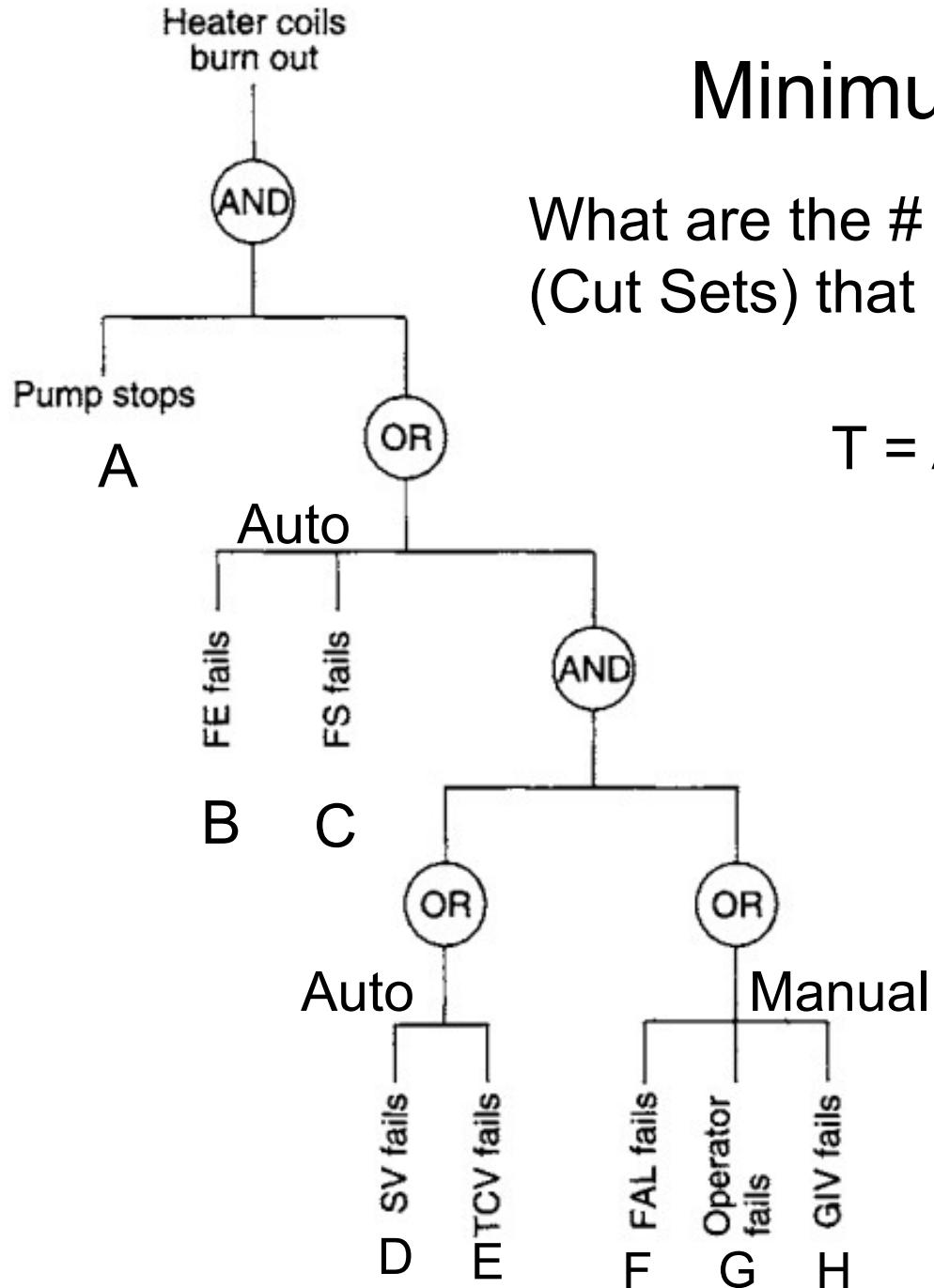
Rank 3:

Number of events in a set

Here, each letter (A,B...) represents a failure event

Minimum Cut Sets

32



What are the # of minimum failure scenarios (Cut Sets) that result in T?

$$T = A \cdot \{B + C + (D+E) \cdot (F+G+H)\}$$

Cut Sets:

0 Rank 1:

2 Rank 2: (A,B), (A,C)

6 Rank 3: (A,D,F), (A,D,G),
(A,D,H),(A,E,F),
(A,E,G),(A,E,H)

Number of alternative paths
in a given rank

Top Event Assessment

- How can events and paths leading to the top event, i.e., cut sets, be assessed with regard to their quantitative contribution to the top event frequency or probability?
- This risk source quantification and prioritization are needed to identify cost effective direction of resources to lower risk if necessary and manage risk within acceptable ranges.

Fault Tree and Success Tree Method: Construction, Quantification, Interpretation

Unit 10B

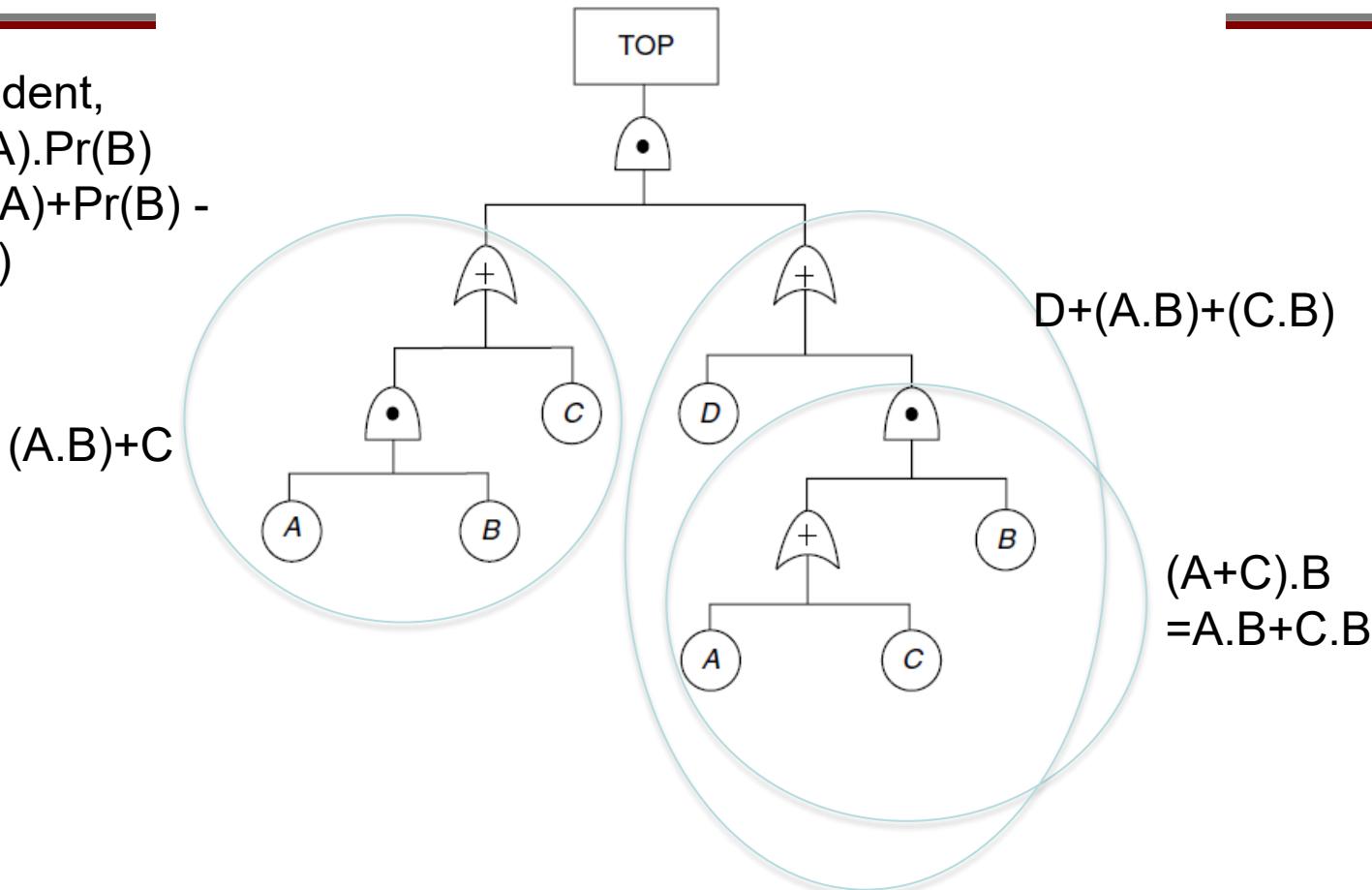
Spring 2022

References

- Tweeddale, Mark, *Managing Risk and Reliability of Process Plants*, Elsevier, 2003
- Crowl, D.A. and Louvar, J.F., *Chemical Process Safety*, 4th ed, Prentice Hall, 2019
- Modarres, M., M. Kaminskiy, and V. Krivtsov, *Reliability Engineering and Risk Analysis*, 2nd ed, Taylor&Francis, 2010 (Modarres, RERA)
- Norman Fenton and Martin Neil, “Risk Assessment and Decision Analysis with Bayesian Networks,” CRC Press, 2nd ed., 2019, Chapter 5 (RDBN, 2019)
- Modarres, M., *Risk Analysis in Engineering*, Taylor&Francis, 2006 (Modarres, RAE)
- Rausand, Marvin, *System Reliability Theory*, 2nd edition, Wiley, 2004
- Jordaan, Ian, *Decisions Under Uncertainty—Probabilistic Analysis for Engineering Decisions*, Cambridge University Press, 2005 (Jordaan, 2005)

Review

If Independent,
 $A \cdot B \equiv \Pr(A) \cdot \Pr(B)$
 $A + B \equiv \Pr(A) + \Pr(B) - \Pr(A)\Pr(B)$



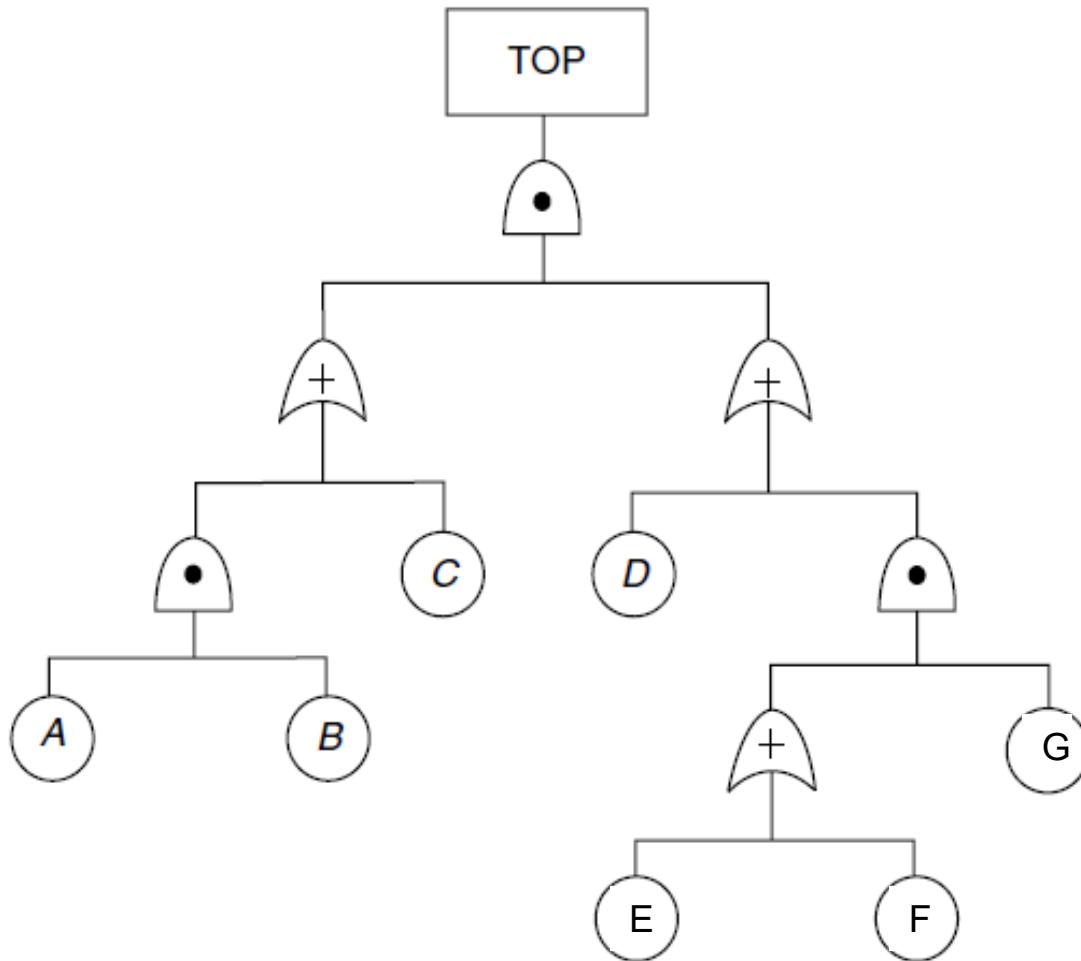
$$\text{TOP} = [(A \cdot B) + C] \cdot [D + (A \cdot B) + (C \cdot B)] = (A \cdot B \cdot D) + (A \cdot B \cdot A \cdot B) + (A \cdot B \cdot C \cdot B) + (C \cdot D) + (C \cdot A \cdot B) + (C \cdot C \cdot B)$$

$$\begin{aligned} \text{TOP} &= (A \cdot B \cdot D) + (A \cdot B) + (A \cdot B \cdot C) + (C \cdot D) + (C \cdot A \cdot B) + (C \cdot B) \\ &\xrightarrow{\quad} (A \cdot B) + (C \cdot D) + (C \cdot B) \end{aligned}$$

If $\Pr(A) = \Pr(B) = \Pr(C) = 0.01$: $\Pr(\text{TOP}) = 3(0.01)^2 = 0.0003$

$$X \cup (X \cap Y) = X$$

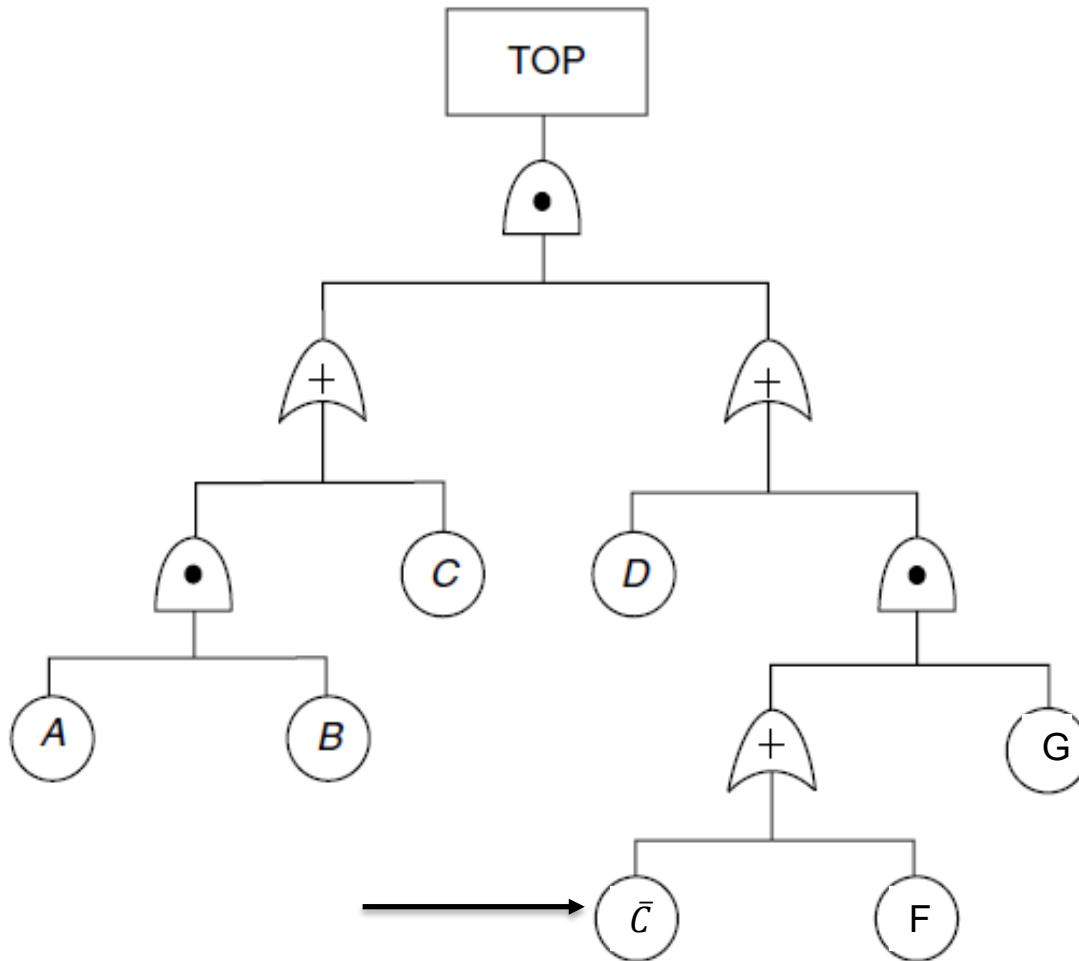
Review



$\text{TOP} = [(\text{A} \cdot \text{B}) + \text{C}] \cdot [\text{D} + (\text{E} + \text{F})] \cdot \text{G}$

: No scope for reduction

Review



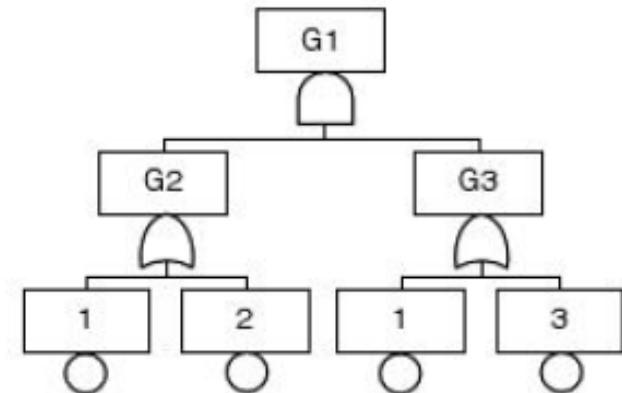
$$\text{TOP} = [(\text{A} \cdot \text{B}) + \text{C}] \cdot [\text{D} + (\bar{\text{C}} + \text{F}) \cdot \text{G}]$$

: No scope for reduction

MOCUS (Method of Obtaining Cut Sets)

1	2	3	4	5	6
G1	G2, G3	1, G3	1, 1	1	1
			1, 3	1, 3	
		2, G3	2, 1	1, 2	
			2, 3	2, 3	2, 3

All CS MinCS



Steps:

1. Enter top gate name.
2. Replace G1 with its inputs, G1 and G2.
3. Replace G2 with its inputs, 1 and 2.
4. Replace G3 with its inputs, 1 and 3.
5. These are the total CS's, some are nonminimal.
6. Eliminate nonminimal CS's.

Bottom-up Algorithm

$$G5 = A \cdot B = AB$$

$$G3 = C + G5 = C + AB$$

$$G4 = B + C$$

$$G2 = A + G4 = A + B + C$$

$$G1 = G2 \cdot G3$$

$$= (A + B + C) (C + AB)$$

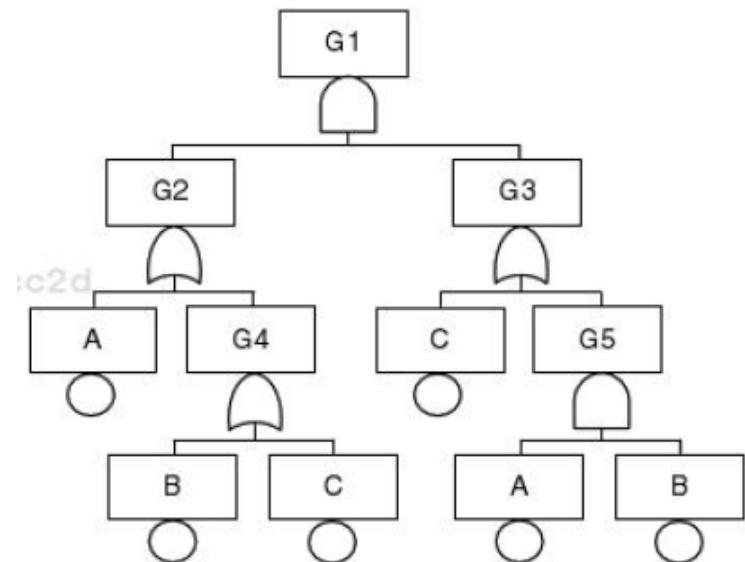
$$= AC + AAB + BC + BAB + CC + CAB$$

$$= AC + AB + BC + AB + C + ABC$$

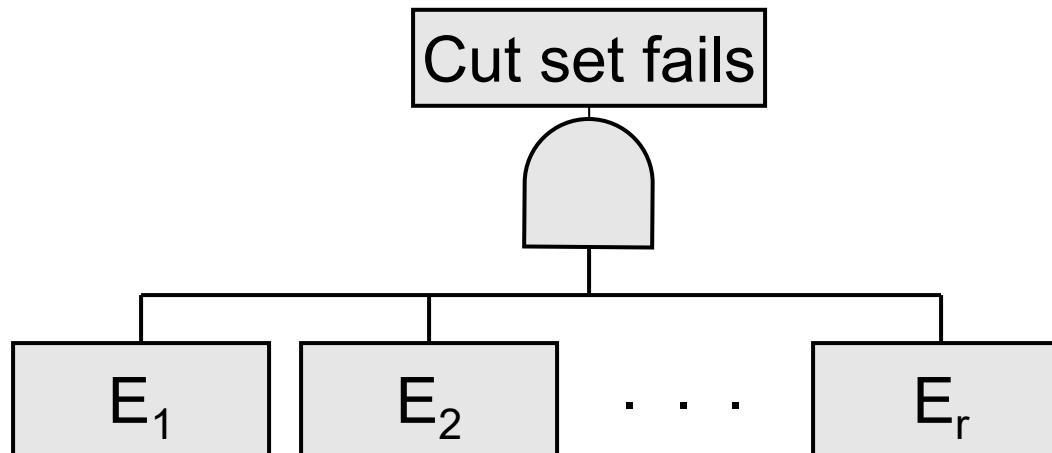
$$= C + AC + BC + AB + ABC$$

$$= C + AB$$

Boolean Algebra



Cut Set Evaluation

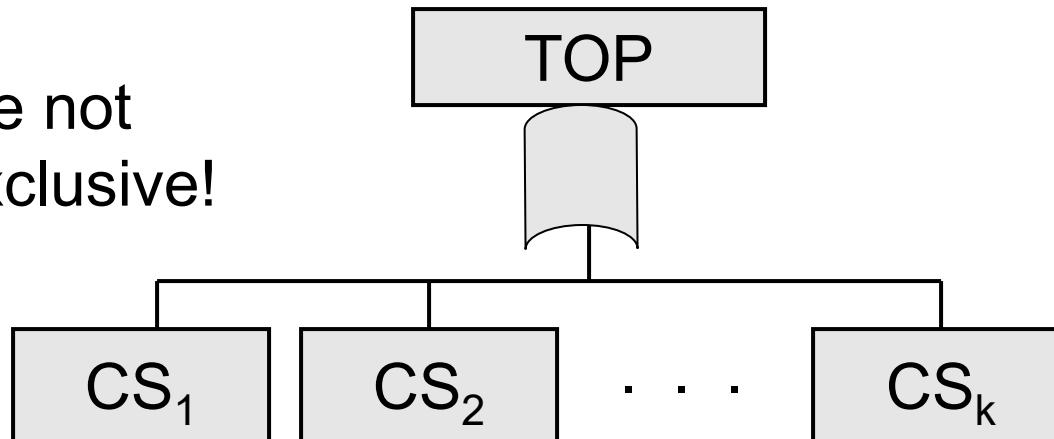


A minimal cut set fails if (and only if) all the basic events in the set simultaneously fail. The probability that cut set s , with r independent events, fails at time t is

$$P_s(t) = \prod_{i=1}^r P_{s,i}(t), \quad P_{s,i}(t) = \text{failure Pr of event } i \text{ in } s$$

TOP Event Probability

Cut sets are not mutually exclusive!



The TOP event occurs if at least one of the k minimal cut sets, S_i , fails. Expressions for *approximation* of the TOP event probability is

failure scenarios:

$$P_T(t) = P_{S1}(t) \cup P_{S2}(t) \cup \dots = 1 - \prod_{i=1}^k [1 - P_{Si}(t)] \sim \sum_{i=1}^k P_{Si}(t), \text{ if REA}$$

↑ ↑

1. for independent events 2. REA approximation

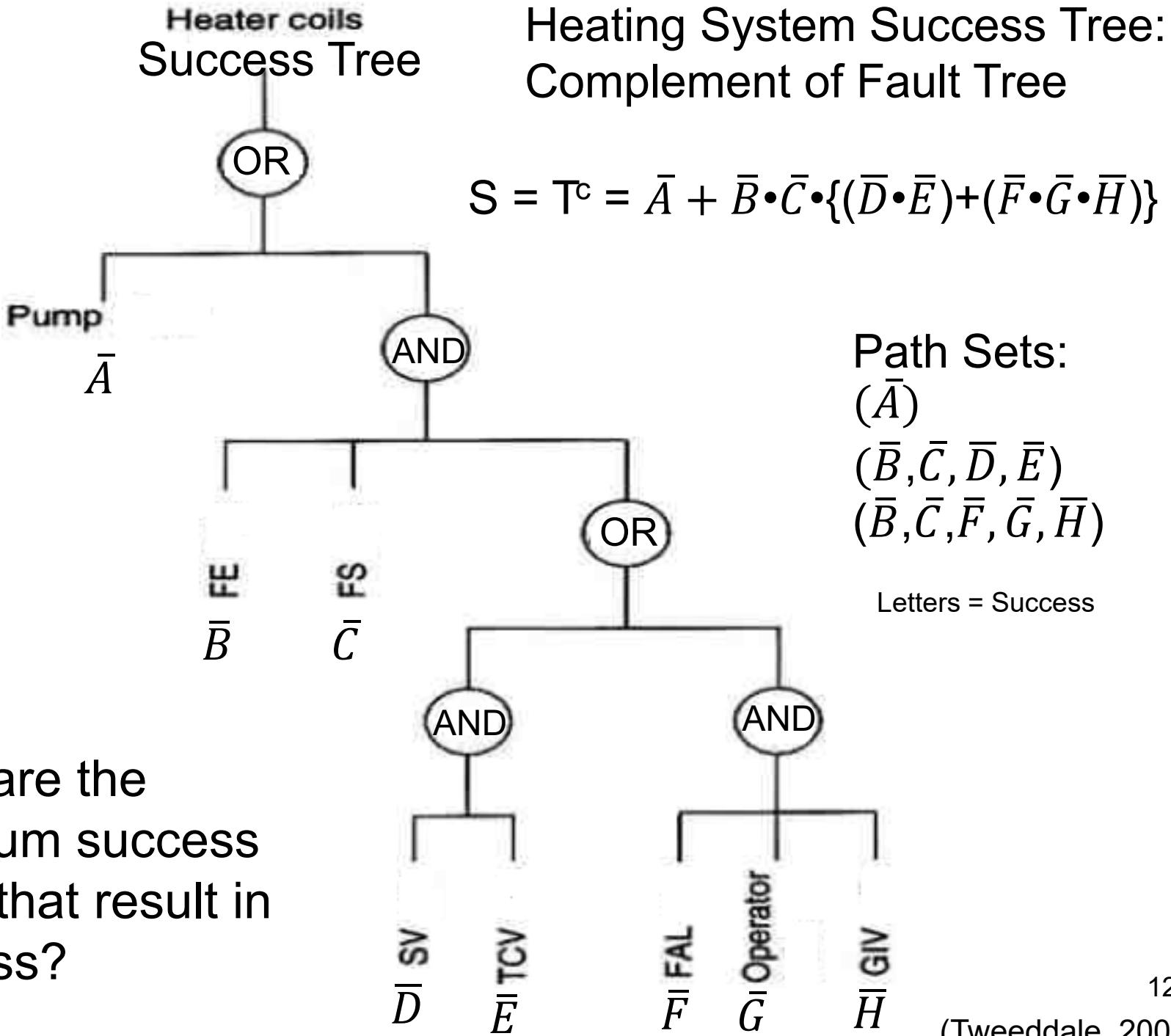
Fault Tree Success Paths

- A FT **Success Path** is a component or group of components' state that prevents the FT top event from occurring.
- A FT can exhibit one or more success paths.
- Success paths form a Success Tree ST, which is the *complement* of a FT with all events and *operations changed to their logical complements* (And-Gates converted to Or-Gates and vice versa).

Success Trees ST

- 1. Shows how a system can perform without failure based on performance of components and human actions
- 2. Facilitate understanding of minimum success requirements, with minimal Path Sets leading to system performance that benefits system designers, operators, and managers.

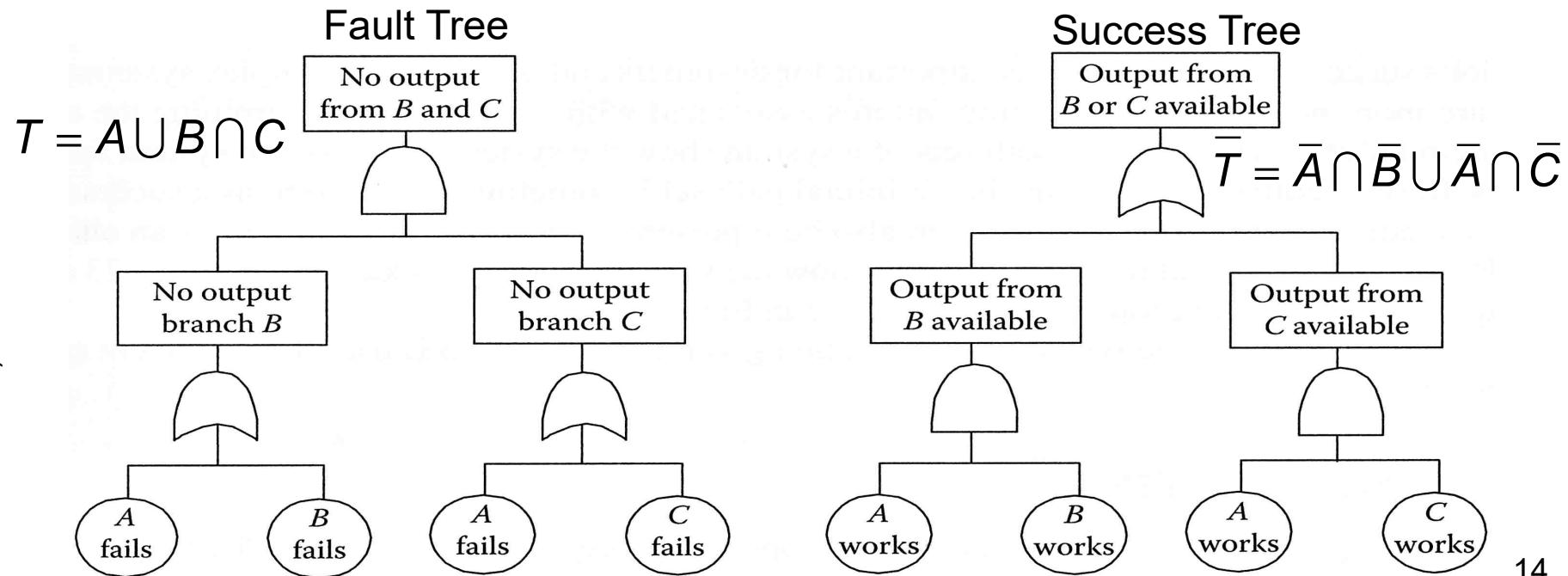
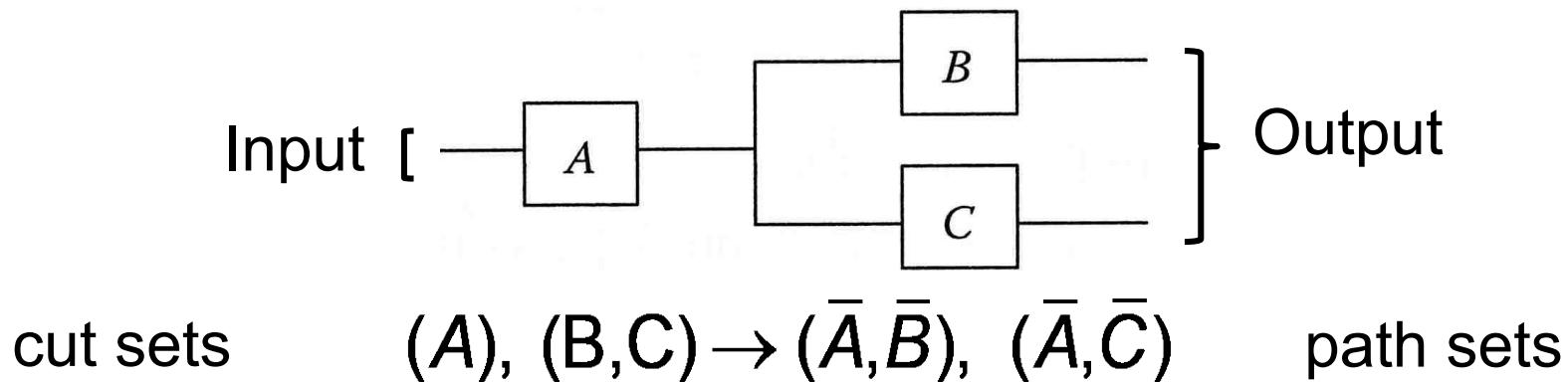
**Heater coils
Success Tree**



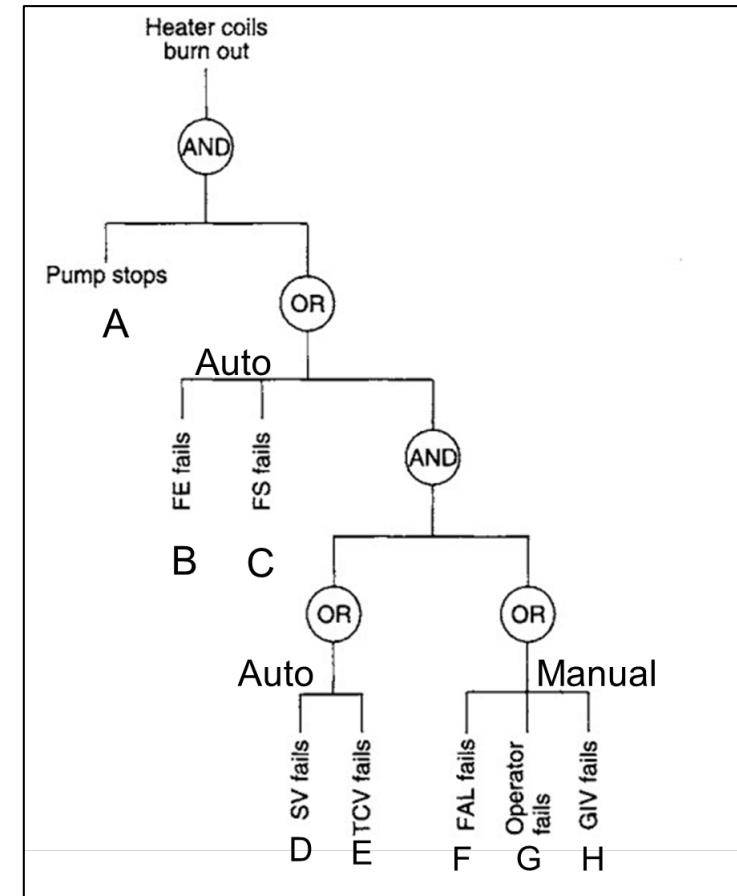
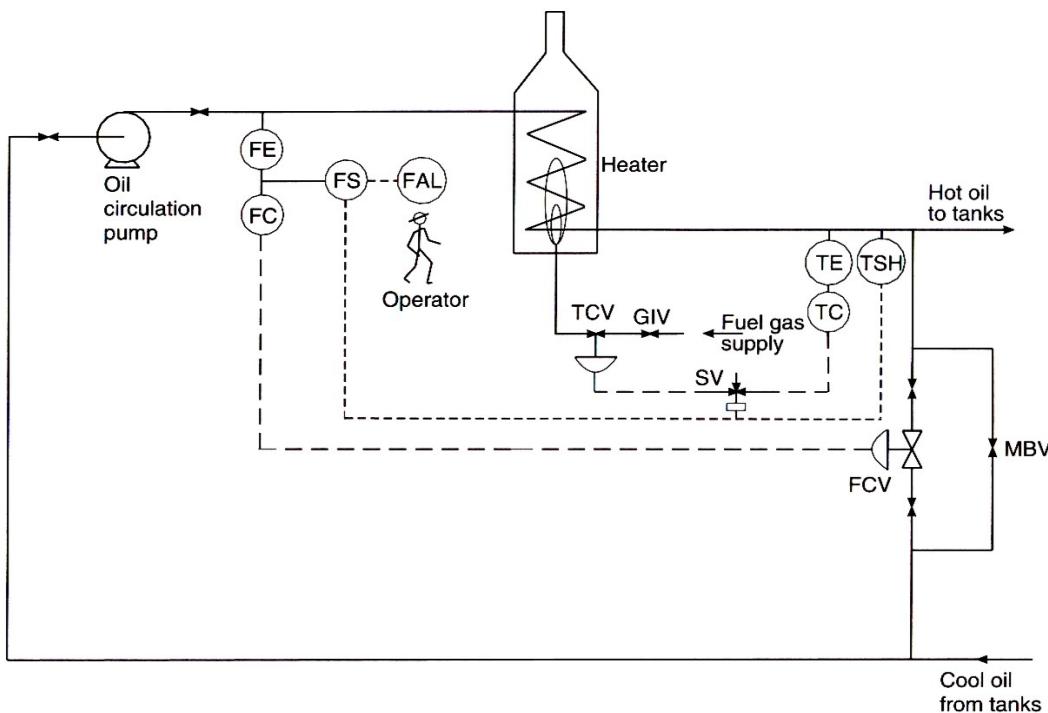
ST Path Sets, Review

- A success tree *Path Set* is an event or set of basic success events, the simultaneous occurrence of which causes the top event of the Success Tree to occur.
- Each path set is a scenario for success.
- A *Minimum Path Set* is a set that cannot be reduced in size (number of components).
- Minimum path sets are determined directly from the reduced Fault or Success Tree, top event logic.

Logic of Cut Sets and Path Sets



Back to the Hot Oil Heating System Problem:



Frequency and Probability

- Systems may be operating continuously, or they may be operating only when demanded
 - Barrier systems such as automatic response systems
- A system operating for time T with a failure rate of λ (constant) has a failure probability given by

$$F(T) = 1 - e^{-\lambda T}$$

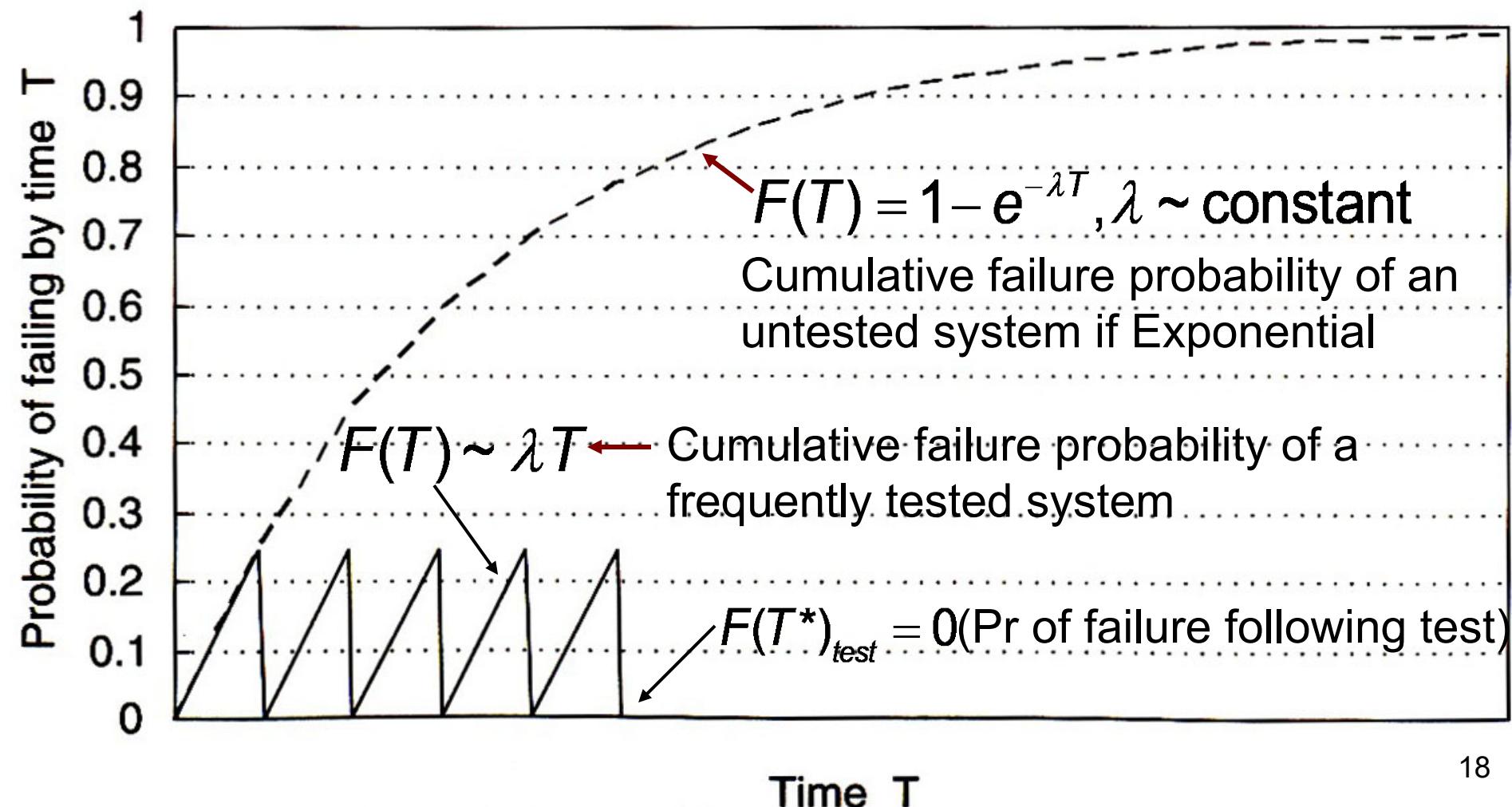
- What about those which operate when demanded?
 - The Probability of Failure on Demand (*PFD*) is the probability that the protective, technical component is in a failed state (latent failure + down time) at the time of the system *demand*, when it is called upon to perform and protect.

What about systems undergoing testing, inspection and maintenance?



- How often is the system tested? How does frequency of testing affect the failure frequency/probability?
- Types of maintenance: Corrective, preventive, predictive
- If the system is tested every T years, what is the probability of the system failing between any test period?
- We will develop a simple method for estimating probability of failure for systems that are demanded (e.g. the automatic response system) and are inspected and maintained from time to time.

As the time between tests increases, indicated by the broken line, the probability of protective system failure approaches 1.



Why test?

- When a component is tested, either it works or it does not work satisfactorily (binary case).
- Each time that the system is tested, for $T = T^*$, it is:
 - Operable or
 - Repaired or replaced and restored to operational condition
- Therefore the probability of being in a failed state is nominally 0 or becomes ~ 0 following repair or replacement.

$$F(T^*)_{test} = 0$$

Exponential Component Behavior, 3

- Expand probability of failure, $F(T) = 1 - e^{-\lambda T}$

$$1 - \left[1 - \lambda T + \frac{(\lambda T)^2}{2!} - \frac{(\lambda T)^3}{3!} + \dots \right] \quad \text{Taylor Series expansion}$$

- If $\lambda T \ll 1$, the higher order terms become negligible.

With this condition, cumulative probability of failure $F(T)$ initially increases \sim linearly with T (and Reliability $R(T)$ initially decreases \sim linearly with T)

**Frequently tested,
sensitive components**

$$\begin{cases} F(T) \sim \lambda T \\ R(T) \sim 1 - \lambda T \end{cases}$$

Probability of Failure on Demand (PFD)

Equal testing intervals = T

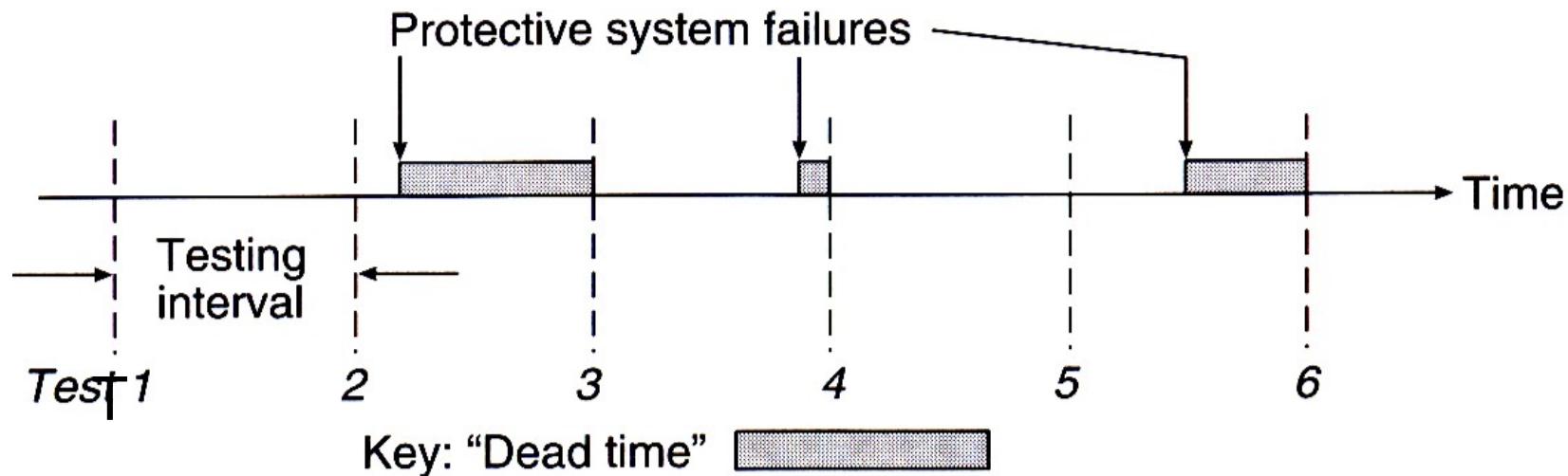


Figure 6-9. Tests of protective systems showing “dead” periods.

To address the question: How often to test a sensitive component?

Component Behavior

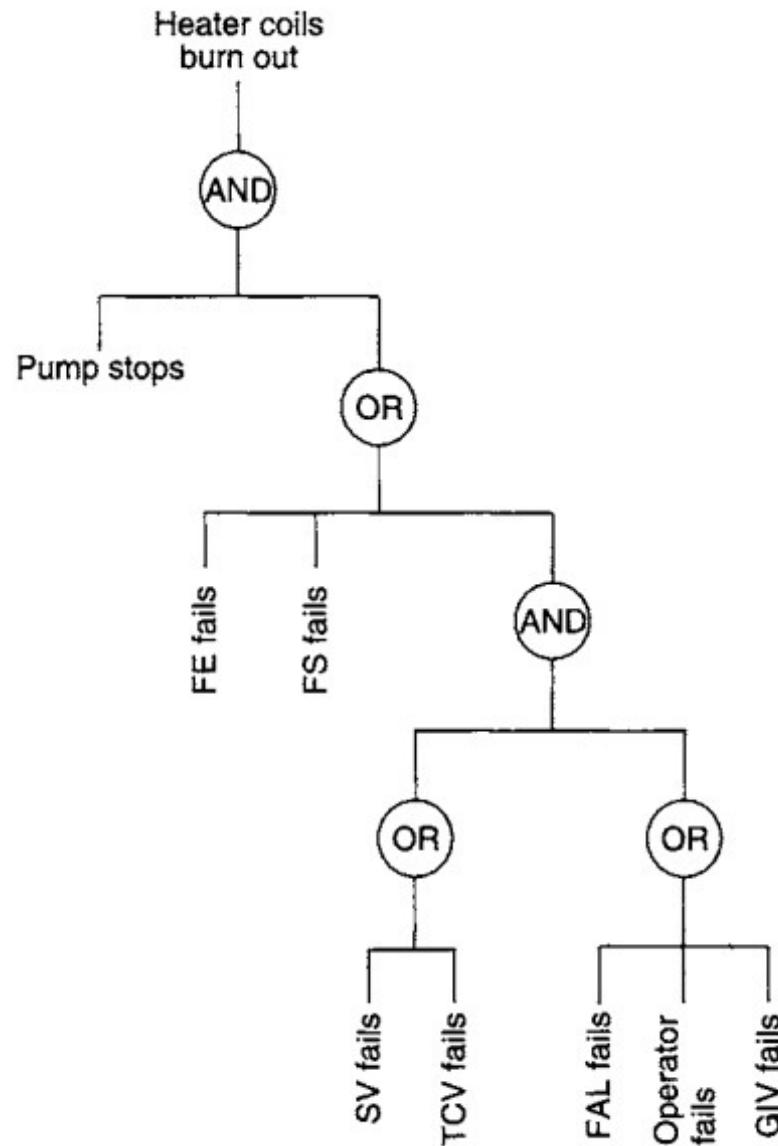
- Assuming probability of failure to be the same at any time between adjacent tests, the average time for an item to be in a failed state, *dead or down time*, is $\sim 1/2$ the time between tests or between $t = 0$ and $t = T$.
- The fraction of time, n/N , the item is in a failed state converts λ to a *Probability/Fraction of Dead Time*, the average expected down time over 0-T multiplied by λ

$$FDT = (1/2)\lambda T$$

- Note that this value of probability is for systems undergoing testing and maintenance where there is a chance of failure in between inspection and maintenance. For systems with no maintenance, use $F(T) = 1 - R(T) = 1 - e^{-\lambda T}$

Fault Tree of the Hot Oil Heating System

- Estimate frequency of heater coil burn out
- Requires estimation of the fractional deadtime of the automatic response system to determine chances that the system will be up and running when demanded



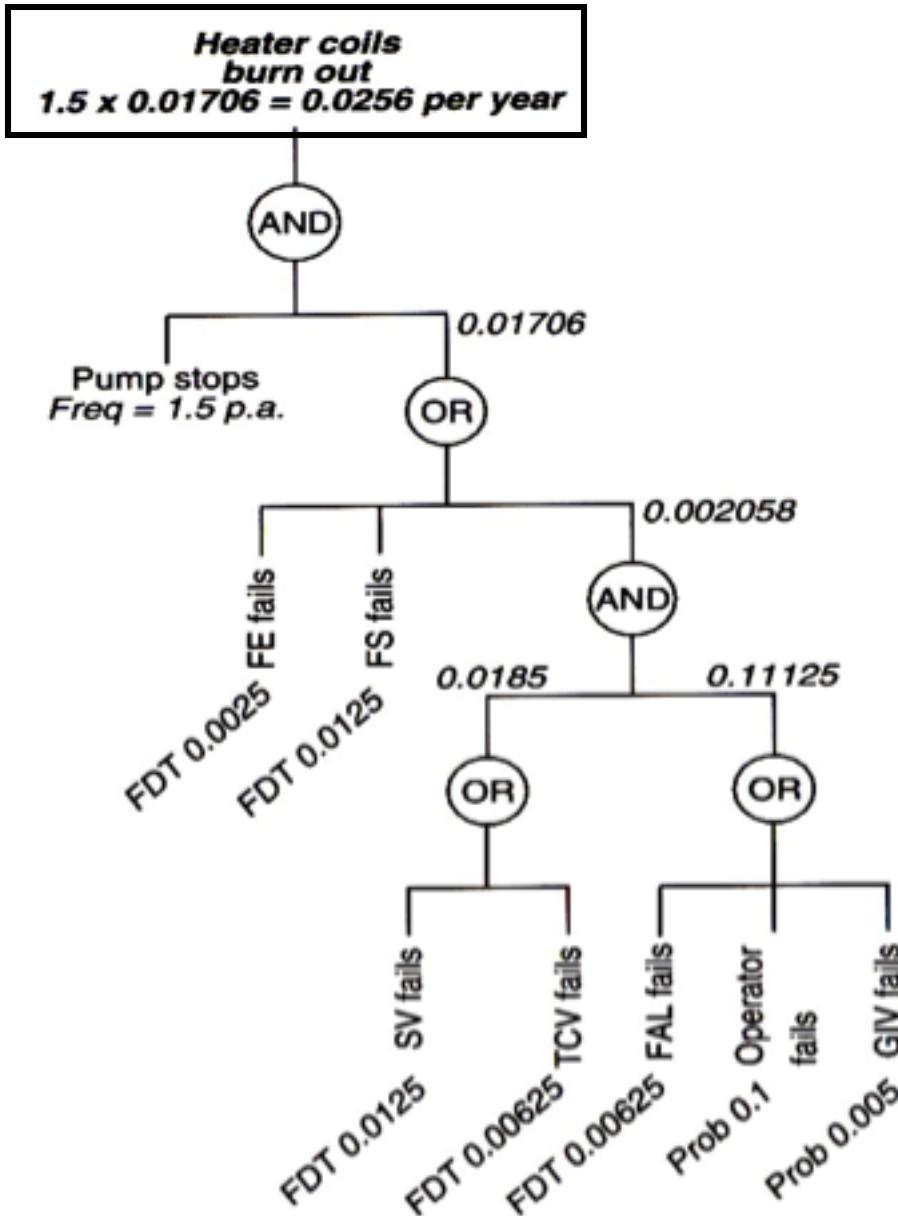
Hot Oil Heating System: Failure Data

Pump	1.5 per year
FE	0.02 per year
FS	0.1 per year
SV	0.1 per year
TCV	0.05 per year
FAL	0.05 per year
Operator	0.1 probability
GIV	0.005 per operation (i.e., a probability of 0.005 of failing when needed)

$$FDT \quad \left\{ \begin{array}{l} FE: \quad 0.5 \times 0.02 \times 0.25 = \quad 0.0025 \\ FS: \quad 0.5 \times 0.1 \times 0.25 = \quad 0.0125 \\ SV: \quad 0.5 \times 0.1 \times 0.25 = \quad 0.0125 \\ TCV: \quad 0.5 \times 0.05 \times 0.25 = \quad 0.00625 \\ FAL: \quad 0.5 \times 0.05 \times 0.25 = \quad 0.00625 \end{array} \right.$$

FDT= fractional down time=(1/2) λT

Hot Oil Heating System



Evaluated Reduced FT

Heater Coil FT Quantification

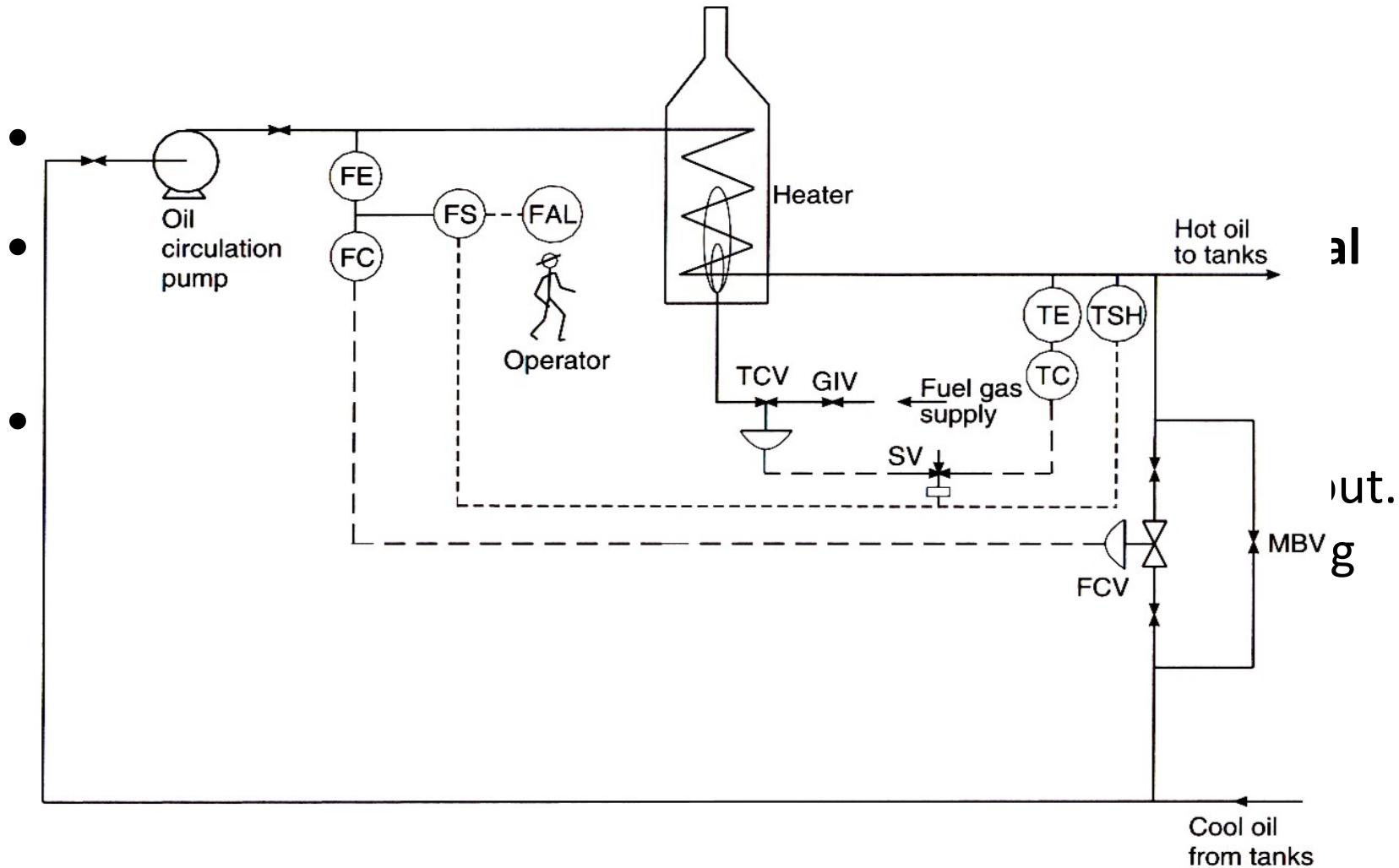


Figure 6-2. Hot oil heating system.

Heater Coil Common Cause Failure

- In this analysis, random failures were approximated conditionally to occur independently, which may be an acceptable starting point.
- Dependent or common-cause failures are influenced by Human and Organizational factors, which are common to two or more components, e.g., quality of Maintenance and level of Training/Retraining.
- *Due to conditional dependencies and common-cause failures, the combined failure probabilities leading to system failure can be much greater than calculated assuming unrealistic independence of components.*
- All such direct dependencies can be included with conditioning arcs and probabilities in a Bayesian Net, which is the next step from an initial FT.

Increase Heater Coil System Reliability

- First: reduce inherent hazards, and then reduce the inherent failure probability using components with a higher intrinsic reliability or lower λ .
- Reduce demand frequency, D : improve containment and control (including human factors).
- Lower FDT of protective systems through test and maintenance sufficiently often with reduced T between tests based on risk level of unit failure.

Increase Heater Coil System Reliability

- Lower FDT = $(1/2) \lambda T$ (down time not included)
 - Reduce λ : more reliable components; design changes
 - Increase testing frequency (cost/risk balance)
 - Install redundant systems: 2 units in parallel

For FDT = 0.01, FDT_{red} = 0.01 x 0.01 = 0.0001

- Actual PFD reduction is less, e.g., components are not fully independent in varying degrees but can be significantly dependent, or subject to common-cause failures.

How to Achieve High Reliability/Availability

- Reduce common-cause failures
 - Use different types or designs for the 2 protective systems to reduce sensitivity to certain conditions
 - Identify, remove likely common-cause contributions and reduce conditions for failures
 - Higher level of diversity in the overall design
 - More frequent tests and maintenance of critical components guided and informed by a risk assessment.

Heater Coil System Reliability

- Separate overall System into a *Control System* (automatic) and a *Protective System* (manual).
 - At present, if Control System fails because of FE failure, the alarm and low-flow Protection System (FE, FS, SV) cannot operate.
 - Solutions?

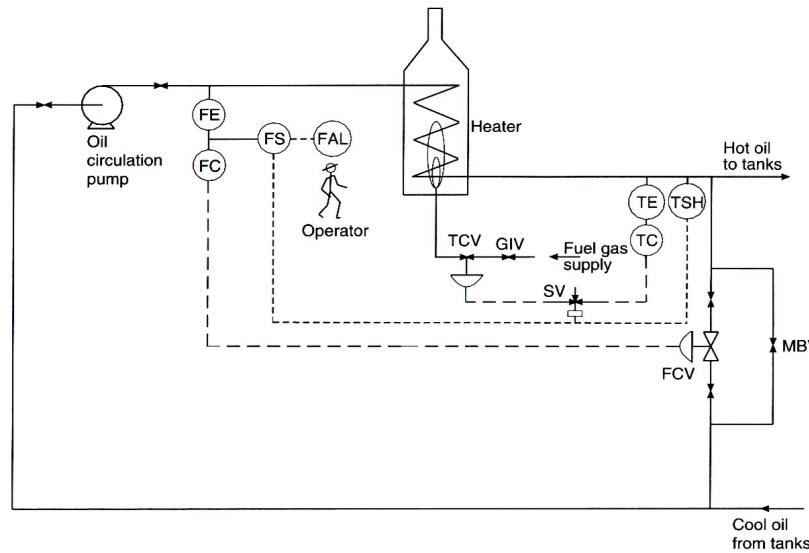


Figure 6-2. Hot oil heating system.

Heater Coil System Reliability

- Separate overall System into a *Control System* (automatic) and a *Protective System* (manual).
 - At present, if Control System fails because of FE failure, the alarm and low-flow Protection System (FE, FS, SV) cannot operate.
 - If the low-flow alarm and relay systems are actuated by a low-flow switch independent of FE, and FS, system Reliability will be greatly improved.

Cut Set Method, Frequency

- For each cut set, calculate the Cut Set Frequency from failure rate information (PU frequency and *PFD* probability values for other components)
- Only one cut set element can be a frequency (PU, pump, in this case), and all other elements must be probabilities.

Cut Set Frequencies

Table 6-1
Evaluation of Cutsets

Cutsets	Frequency FDT/ Probabilities	Cutset Frequency
PU, FE	1.5×0.0025	0.00375 per year
PU, FS	1.5×0.0125	0.01875
PU, SV, FAL	$1.5 \times 0.0125 \times 0.00625$	0.000117
PU, SV, OP	$1.5 \times 0.0125 \times 0.1$	0.001875
PU, SV, GIV	$1.5 \times 0.0125 \times 0.005$	0.000094
PU, TCV, FAL	$1.5 \times 0.00625 \times 0.00625$	0.000059
PU, TCV, OP	$1.5 \times 0.00625 \times 0.1$	0.00094
PU, TCV, GIV	$1.5 \times 0.00625 \times 0.005$	0.000047
	TOTAL	= 0.0256 per year

Note: frequencies in italics

Top event frequency

Identify Main Contributors to the TE and Risk

↓
Magnitude
↓

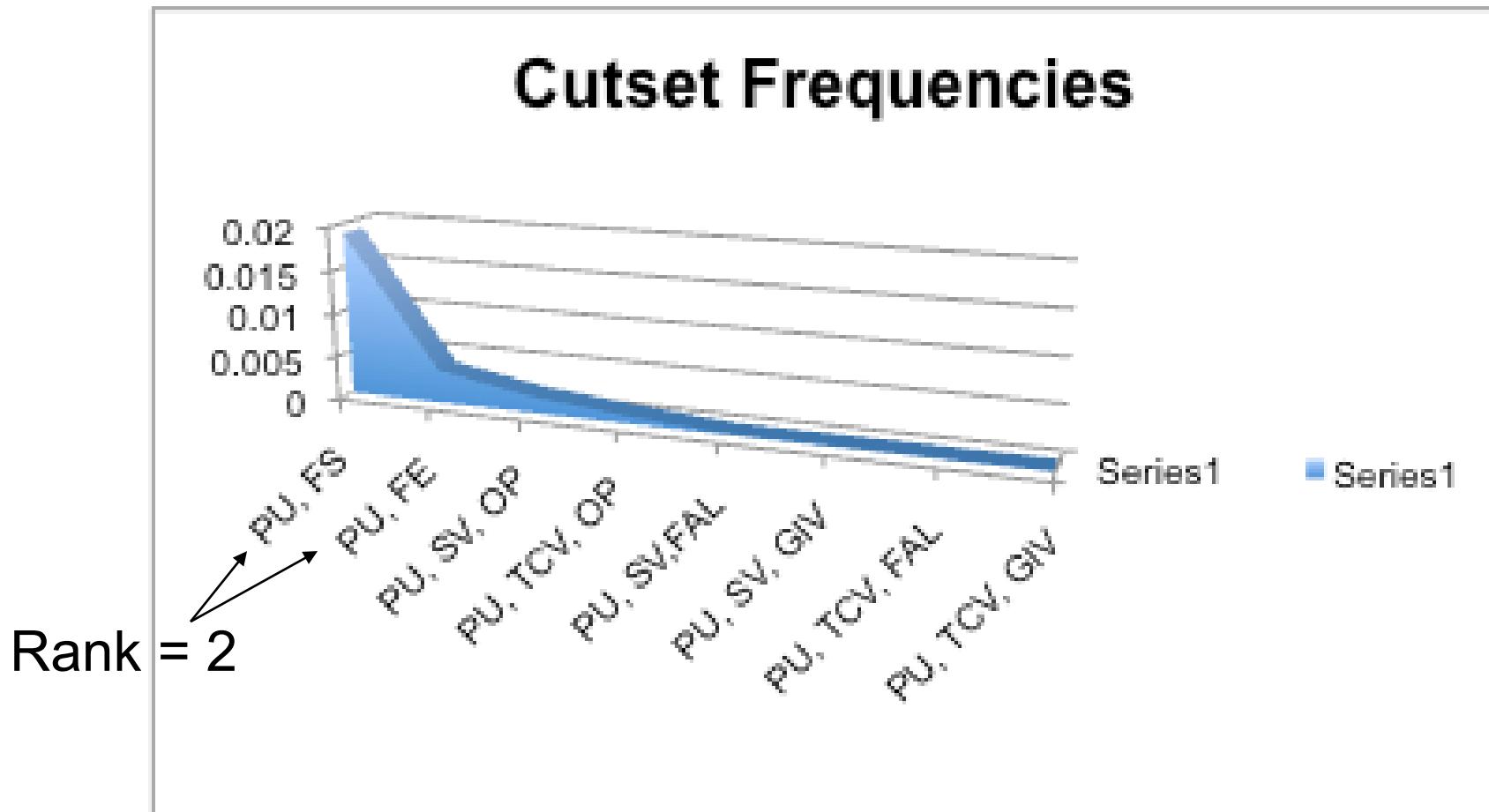
Cut sets	Freq/yr	Rank	IM %	
PU, FS	0.0188	2	73	}
PU, FE	0.0038	2	15	
PU, SV, OP	0.0019	3	7	}
PU, SV, FAL	0.00012	3	4	
PU, TCV, OP	0.00094	3	0.5	}
PU, TCV, FAL	0.00006	3	0.4	
PU, TCV, GIV	0.00005	3	0.23	}
PU, SV, GIV	<u>0.00009</u>	3	0.18	
Top event freq = 0.0256/yr				

88% of total
11% of total
~1.3% of total

Cut sets C_i are categorized by their rank and their **importance, IM_i :**

$$IM_i = \frac{P(C_i)}{P(TE)}, \quad P(C) = \prod_{i \in C} P(c_i), \quad c_i \text{ is component in cut set } C$$

Cut Set Frequencies



Fussell-Vesely Importance

Evaluate contribution of an event to the top event

Evaluation of Cutsets

Minimum Cutsets	Minimum Cutsets	Frequency / Probabilities	Cutset Frequency
AB	PU, FE	1.5×0.0025	0.00375 per year
AC	PU, FS	1.5×0.0125	0.01875
ADF	PU, SV, FAL	$1.5 \times 0.0125 \times 0.00625$	0.000117
ADG	PU, SV, OP	$1.5 \times 0.0125 \times 0.1$	0.001875
ADH	PU, SV, GIV	$1.5 \times 0.0125 \times 0.005$	0.000094
AEF	PU, TCV, FAL	$1.5 \times 0.00625 \times 0.00625$	0.000059
AEH	PU, TCV, OP	$1.5 \times 0.00625 \times 0.1$	0.00094
AEG	PU, TCV, GIV	$1.5 \times 0.00625 \times 0.005$	0.000047
			Total = 0.0256 per year

$$FV_i = \frac{\text{sum of probability of cut sets with event } i}{\text{probability of top event}}$$

$$(FV)_D = (0.000117 + 0.001875 + 0.000094) / 0.0256$$

Some Failure Rate Data Sources

- AIChE, “Guidelines for Process Equipment Reliability Data,” Center for Chemical Process Safety CCPS)
- IEEE Std 500, “IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations.”
- MIL-HDBK-217F, Military Handbook—Reliability Prediction of Electronic Equipment.
- NRPD-2, “Non-electronic Parts Reliability Data,” Reliability Analysis Center at the Rome Air Development Center.
- OREDA, Offshore Reliability Data Handbook, SINTEF: Trondheim, Norway
- Lees, F.P., Loss Prevention in the Process Industries, 3rd Ed., Sam Mannan, ed., Butterworth, Oxford, UK

Event Tree Analysis

Unit 10

Spring 2022

References

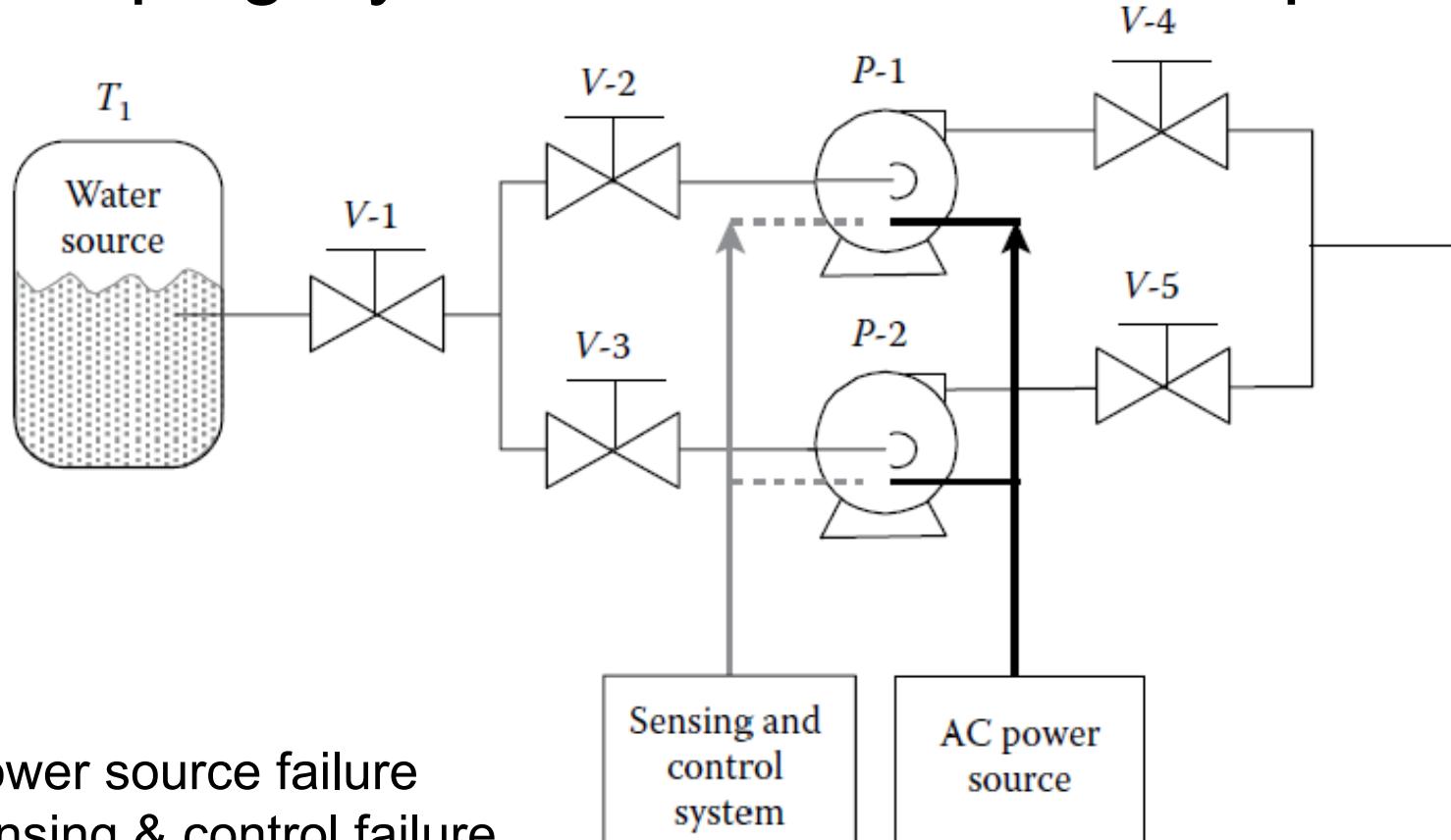
- Modarres, M., *Risk Analysis in Engineering*, CRC Press, 2006 (RAE)
- Norman Fenton and Martin Neil, “Risk Assessment and Decision Analysis with Bayesian Networks,” CRC Press, 2019, 2nd ed., Chap. 13, 426, 436-439
- Tweeddale, M, *Managing Risk and Reliability of Process Plants*, Gulf Professional Publishing, 2003 (Tweeddale, 2003)
- Rausand, Marvin, *System Reliability Theory*, 2nd edition, Wiley, 2004
- Kaplan, S., “On the Inclusion of Precursor and Near Miss Events in QRA: A Bayesian Point of View and a Space Shuttle Example,” *Reliability Engineering and System Safety*, 27, 103–115, 1990 (Kaplan, 1990)

Event Tree Method and Analysis



- Event tree analysis (ETA) is an **inductive** procedure (contrasting with the **deductive** FTA) to diagram events, including hazard guard events that are expected to progress from an Fault Tree Top Event as the **initiating event** of Event Tree scenarios from an initiating event to **intermediate events** and result in **outcome events**, which can be safe events or upset events with losses.
- Sequential events diagrammed in an event tree (ET) include hazard guards or **mitigation barriers** (success or fail) to reduce the Pr of upset event occurrences and mitigate outcome losses.
- In addition to event identification, probabilities of intermediate events and outcomes are calculated from the initiating event frequency and other information. Both ET and FT are **first qualitative**, showing event relationships, and then quantitative, from the **base event failure data**, to estimate **scenario outcome event** probabilities and consequences.

Pumping System Event Tree: Example 1



AC: power source failure

S: sensing & control failure

PS: pumping system failure

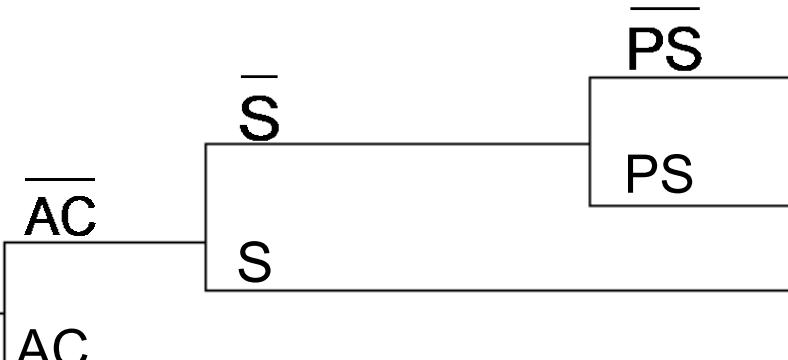
Distinct events: AC, S, and PS to be placed on an ET in order of occurrence or consequence severity, which is ?

(Modarres, RERA, Ch 4)

Pumping System Event Tree: Example 1

Single point failures first

Initiating event I	Elect. power AC	Sensing and control S	Pumping units PS	Sequence logic	Overall system state
				$I \quad \overline{AC} \cdot \overline{S} \cdot \overline{PS}$	S
				$I \quad \overline{AC} \cdot \overline{S} \cdot PS$	F
				$I \quad AC \cdot S$	F
				$I \quad AC$	F



```

graph LR
    I --> AC[AC]
    AC --> S[S]
    S --> PS[PS]
    PS --> S_PS[S]
    S_PS --> F[F]
  
```

(RERA, Ch 4)

AC failure causes failure of S and PS, so place 1st in ET heading.

S failure causes PS failure: place 2nd.

PS failure: place 3rd in sequence.

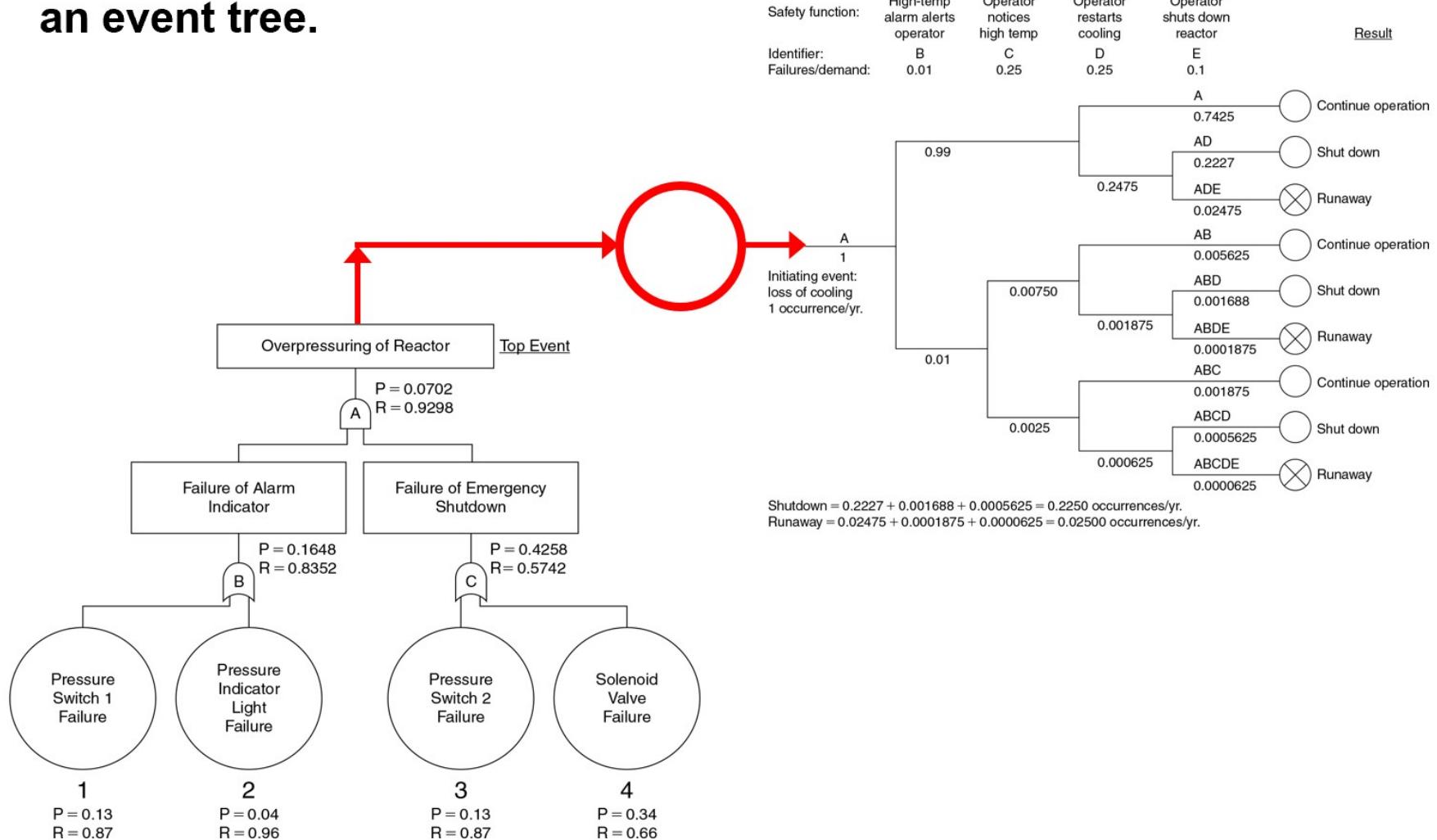
What is the probability of 'system failure' if $\text{Pr}(AC)=0.1$, $\text{Pr}(S)=0.1$, $\text{Pr}(PS)=0.1$?

- A horizontal structure beginning with a FT initiating event on the left with events from left to right in time sequence or based on outcome severity or both.
- Barrier events shown on top of event tree include Boolean operations (success/fail, True/False) of components, subsystems, software response, or human actions.

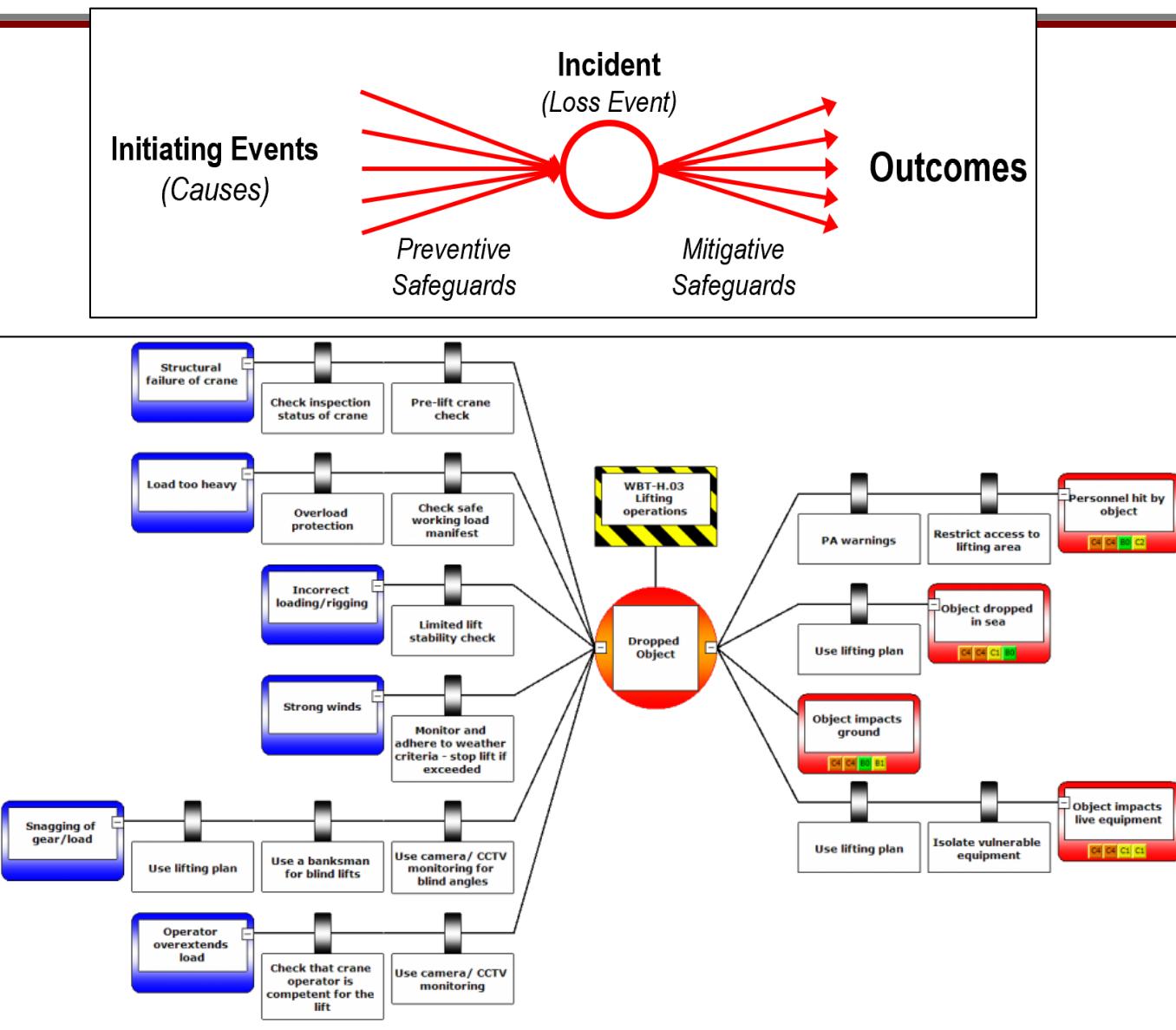
- Note the bowtie structure  that forms when the top event of a FT (rotated 90°) that models causes is connected to ET that models consequences.
- FTs may also connect with different barriers (i.e. probability of success/failure of the initiating event as well as the barriers can come from the top event of a fault tree)
- Successes/failures of the different barriers form the path followed in the ET to different types of scenario outcomes
- As with a FT, a separate Boolean expression corresponds to the sequence logic of each scenario outcome.

Bowties

The top event from a fault tree becomes the initiating event for an event tree.



Bowties



Review: Event Tree Construction

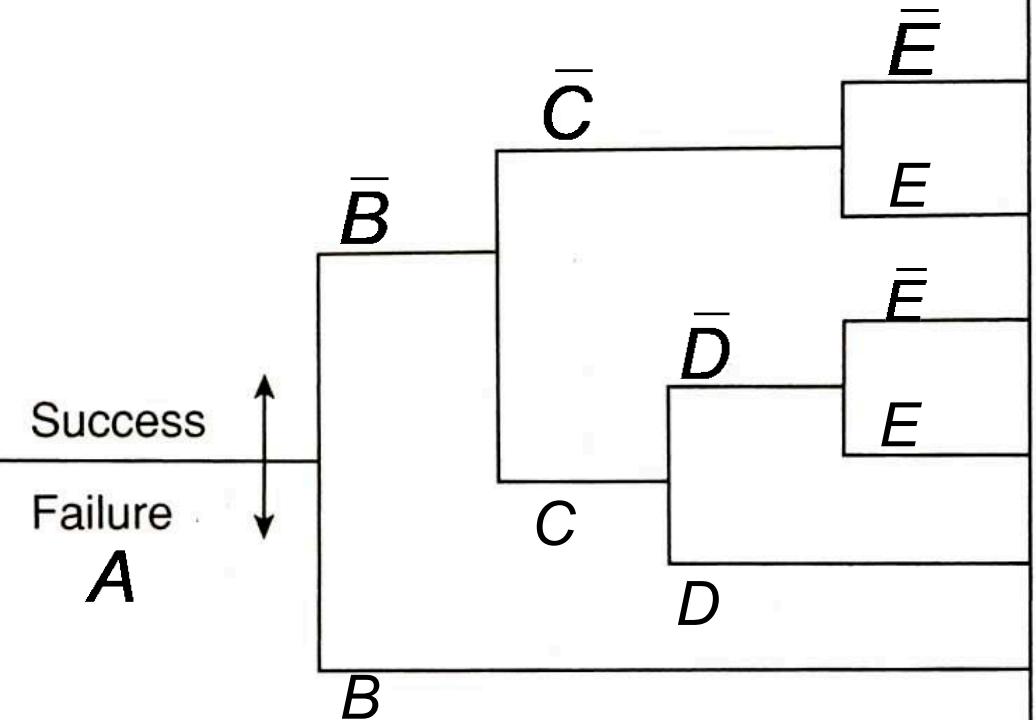
- 1. Identify initiation event; estimate frequency.
 - An ET is developed for each identified initiation event from a FT top event joined to an ET initial event. So a separate Bow Tie is constructed for each FT and ET pair.
- 2. Identify barriers to reduce the probability of event progression, and estimate probabilities of success/failure of each barrier.
 - Calculate or estimate the probabilities of each event tree branch using a FT and base event data for each.
- 3. Develop events in sequence of time and effect.
- 4. Calculate probabilities/frequencies for scenario outcomes; Estimate consequence distributions, and uncertainties.

Example 2: Nuclear Reactor Protection System (NRPS)

10

- Event heading: includes all protective barriers
 - To reduce probabilities of loss outcomes
 - To mitigate consequences of loss outcomes
- Each branch point: success or failure (total probability = 1, MEE (mutually exclusive & exhaustive))
- System Barriers: Event Tree events in heading
 - RP (reactor protection): shutdown
 - Short term, emergency coolant, ECA, ECB, redundant (post shutdown radioactive decay)
 - Long term, emergency coolant, LHR

Example 2: Nuclear Reactor Protection System (NRPS)

Initiating event A	RP B	ECA C	ECB D	LHR E	Sequence logic	Overall system result
 <p>Success</p> <p>Failure</p> <p>A</p> <p>B</p> <p>C</p> <p>D</p> <p>E</p> <p>\bar{E}</p>					<ol style="list-style-type: none"> 1. $A \bar{B} \bar{C} \bar{E}$ 2. $A \bar{B} \bar{C} E$ 3. $A \bar{B} \bar{C} \bar{D} \bar{E}$ 4. $A \bar{B} \bar{C} \bar{D} E$ 5. $A \bar{B} C D$ 6. $A B$ 	<p>S</p> <p>F</p> <p>S</p> <p>F</p> <p>F</p> <p>F</p>

RP= reactor protection system to shut down the reactor

ECA= emergency coolant water pump A

ECB= emergency coolant water pump B

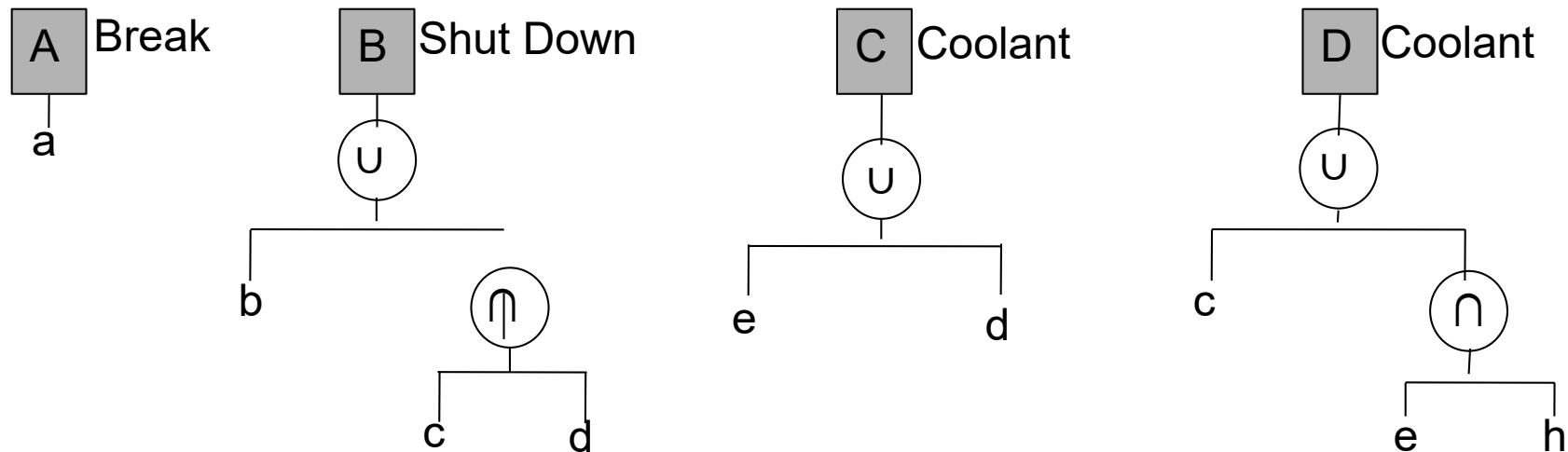
LHR= long-term heat removal

Example 2 NRPS: ET Outcome and Event Probabilities

- How can probabilities of various scenarios/outcomes/consequences be obtained?
 - If probabilities are known, follow the branch to the desired outcome and find the product of the probabilities of each event in the branch, given they are independent
- How can the ET event probabilities be obtained?
 - For some types of barriers (such as relief valves) you can get failure probability data from various equipment databases or manufacturer's specifications
 - ET events are generally FT top events (recall how FT top events were determined). FT top event probabilities can be the probability of a top event, or the probability of a barrier in the event tree.

Example 2 NRPS: FT for each ET Event

13



- For each event in the ET, the FTs are shown above.
- List the cut sets of base events for each Fault Tree:

(a)	(b), (c,d)	(e), (d)	(c), (e,h)
-----	------------	----------	------------
- Write logic expressions for top event occurrences: e.g. $B = b \cup (c \cap d)$

$$A = a$$

$$B = b + c \cdot d$$

$$C = e + d$$

$$D = c + e \cdot h$$

Example 2 NRPS: Evaluation of Scenario 5

Scenario 5 logic:

$$A \cdot \bar{B} \cdot C \cdot D$$

Logic for A, B, C, D
assuming
independence
 and **REA**

$$\left\{ \begin{array}{l} A = a \\ B = b + c \cdot d \\ C = e + d \\ D = c + e \cdot h \end{array} \right.$$

A, initiating event (fail); \bar{B} , reactor shutdown (success); C, short term emergency cooling (fail), D, short term emergency cooling (fail)

Note that c, d, e are common/redundant between B, C and D.
 Use the Boolean expressions to relate top events A, B, C, D to base or primary events, a, b, c, d, h, for which failure data are available to define, quantify, and rank outcomes.

Example 2 NRPS: Evaluation of Scenario 5

15

Reduce the Scenario 5 Boolean logic expression to obtain the minimum contributions, called ***Event Sets*** with all events within a set co-occurring for the set to occur:

$$A \cdot \bar{B} \cdot C \cdot D$$

$$\begin{aligned}\overline{(X \cap Y)} &= \bar{X} \cup \bar{Y} \\ \overline{(X \cup Y)} &= \bar{X} \cap \bar{Y}\end{aligned}$$

$$= a \cdot (\overbrace{b + c \cdot d}^{\text{drop } d \cdot e \cdot h}) \cdot (e + d) \cdot (c + e \cdot h)$$

$$= a \cdot (\bar{b} \cdot \bar{c} + \bar{b} \cdot \bar{d}) \cdot (e \cdot c + e \cdot h + d \cdot c) \quad \bar{c} \cdot c = 0$$

$$=[a \cdot \bar{b} \cdot \bar{c} \cdot e \cdot c + a \cdot \bar{b} \cdot \bar{c} \cdot e \cdot h + a \cdot \bar{b} \cdot \bar{c} \cdot d \cdot c] + [a \cdot \bar{b} \cdot \bar{d} \cdot e \cdot c + a \cdot \bar{b} \cdot \bar{d} \cdot e \cdot h + a \cdot \bar{b} \cdot \bar{d} \cdot d \cdot c]$$

$$= a \cdot \bar{b} \cdot \bar{c} \cdot e \cdot h + a \cdot \bar{b} \cdot c \cdot \bar{d} \cdot e + a \cdot \bar{b} \cdot \bar{d} \cdot e \cdot h$$

The 3 resulting ***Event Sets*** are contributions to a Scenario 5 outcome event of the ET. Note that, unlike FT cut sets or ST path sets, the event sets consist of co-occurring failures and successes due to a combination of event FTs. State the ET ***Minimum Event Sets*** contributing to the Scenario 5 outcome.

Example 2 NRPS: Evaluation of Scenario 5

16

Write the probability expressions corresponding to the previous logic expressions for the Scenario 5 outcome shown in Pr expressions:

$$P(A \cdot \bar{B} \cdot C \cdot D)$$

$$\begin{aligned} &= \Pr(a \cdot \bar{b} \cdot \bar{c} \cdot e \cdot h + a \cdot \bar{b} \cdot c \cdot \bar{d} \cdot e + a \cdot \bar{b} \cdot \bar{d} \cdot e \cdot h) \\ &= \Pr(a \cdot \bar{b} \cdot \bar{c} \cdot e \cdot h) + \Pr(a \cdot \bar{b} \cdot c \cdot \bar{d} \cdot e) + \Pr(a \cdot \bar{b} \cdot \bar{d} \cdot e \cdot h) \end{aligned}$$

Below are the 3 **Event Sets** of the Scenario 5 outcome event. Note the combination of simultaneous component failures and component successes for the **Event Sets** that represent the Scenario 5 outcome:

Event Sets: $(a, \bar{b}, \bar{c}, e, h), (a, \bar{b}, c, \bar{d}, e), (a, \bar{b}, \bar{d}, e, h)$

Example 2 NRPS: Probability of Scenario 5

For this failure outcome, convert base event Pr values to failures:

$$\begin{aligned} &= \Pr(a \cdot \bar{b} \cdot \bar{c} \cdot e \cdot h + a \cdot \bar{b} \cdot c \cdot \bar{d} \cdot e + a \cdot \bar{b} \cdot \bar{d} \cdot e \cdot h) \\ &= \Pr(a \cdot \bar{b} \cdot \bar{c} \cdot e \cdot h) + \Pr(a \cdot \bar{b} \cdot c \cdot \bar{d} \cdot e) + \Pr(a \cdot \bar{b} \cdot \bar{d} \cdot e \cdot h) \\ &= \Pr(a) \cdot [1 - \Pr(b)][1 - \Pr(c)] \Pr(e) \cdot \Pr(h) \\ &\quad + \Pr(a) \cdot [1 - \Pr(b)] \Pr(c) \cdot [1 - \Pr(d)] \Pr(e) \\ &\quad + \Pr(a)[1 - \Pr(b)][1 - \Pr(d)] \Pr(e) \Pr(h) \end{aligned}$$

Pumping System Event Tree: Example 3

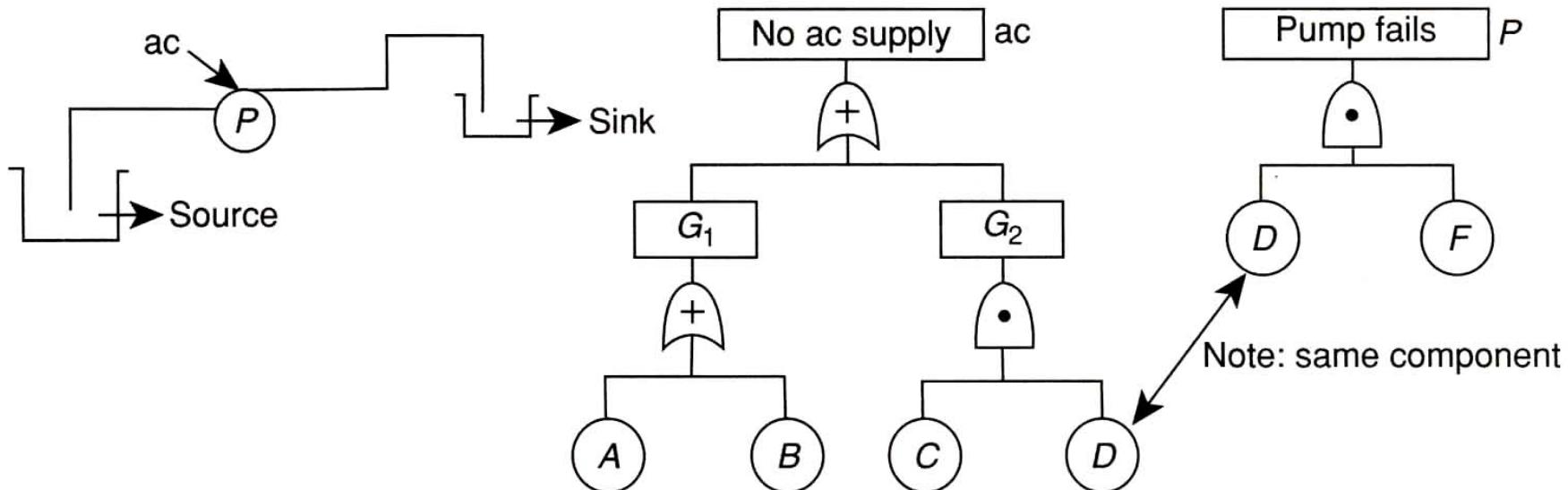
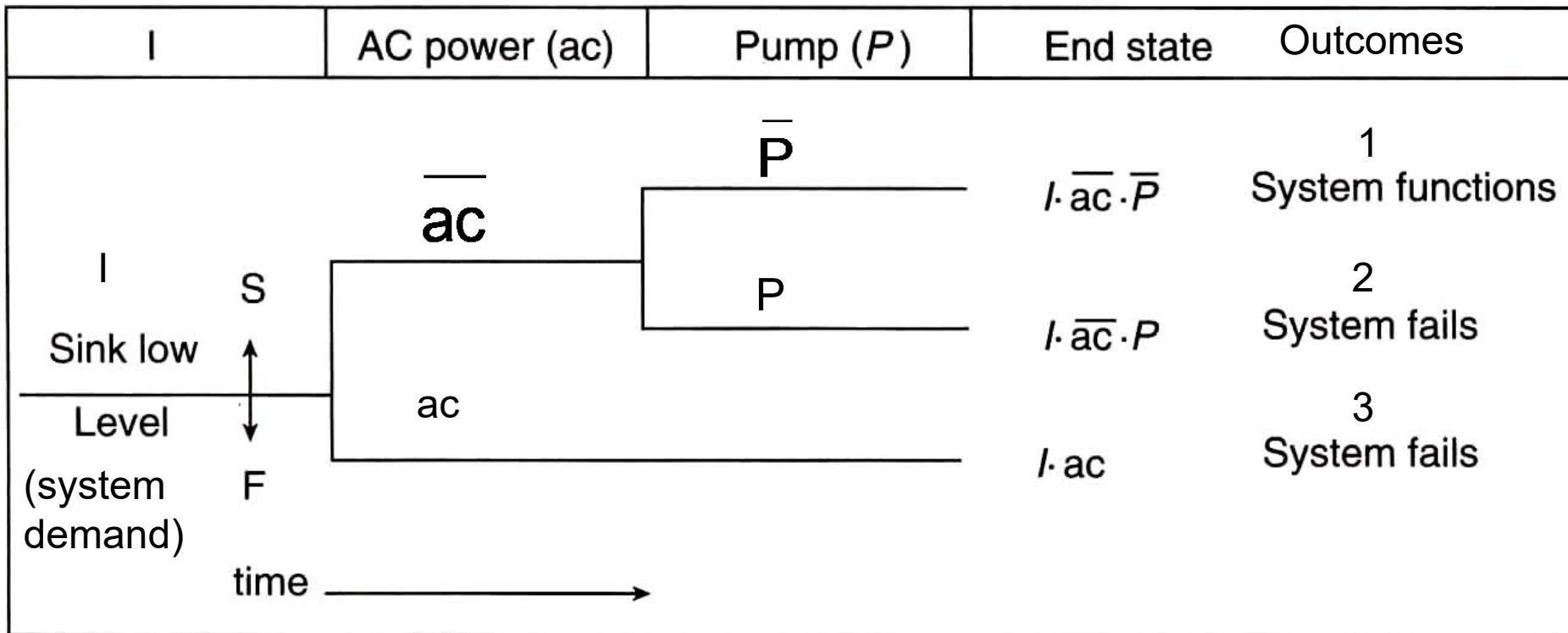


FIGURE 3.23 A simple pumping system and corresponding fault trees of its subsystems.

- Fluid from the source tank is moved to the sink tank assuming that ac power would be needed to start and run the pump when the sink tank level is low. **Develop an event tree for this system.**
- Assume that the events of ‘ac power failure’ and ‘pump failure’ can be represented by the fault trees shown. **Calculate the frequency of each scenario in the event tree and the total frequency of failure of the system.**

Pumping System Event Tree: Example 3



Total frequency of failure will be the sum of outcomes 2 and 3.
 Note that the AC power is the first event.

Each failure outcome will have its own frequency (or Pr) of occurrence distribution and its own consequence distribution.

(Modarres, RAE, Fig 3.24)

Pumping System Event Tree: Example 3

TABLE 3.3

Failure Data for the Events Shown in Figure 3.23

Item	Failure Probability or Frequencies	Success Probability
<i>I</i>	10 per month	—
<i>A</i>	0.01	0.99
<i>B</i>	0.01	0.99
<i>C</i>	0.02	0.98
<i>D</i>	0.05	0.95
<i>F</i>	0.01	0.99

- Take initiating event as ‘sink is low in fluid’
- Note that failure of component “D” appears in both fault trees. That is, it plays two different roles and is called a “replicated event.” For example, it could be failure of a signal that turns on the ac power and starts the pump.

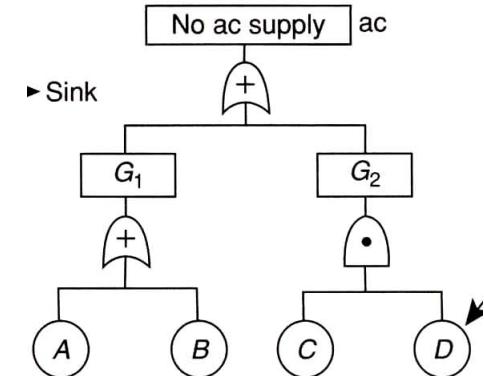
Pumping System Event Tree: Example 3

21

Outcome 3: $I \cdot ac$

- Outcome 3: AC fails
- Failure Outcome 3 is represented by logic expression

$$I \cdot ac = I(A + B + C \cdot D)$$



Adding cut sets
assumes **REA**

which includes the initiating event I
(low sink level AND ac failure).

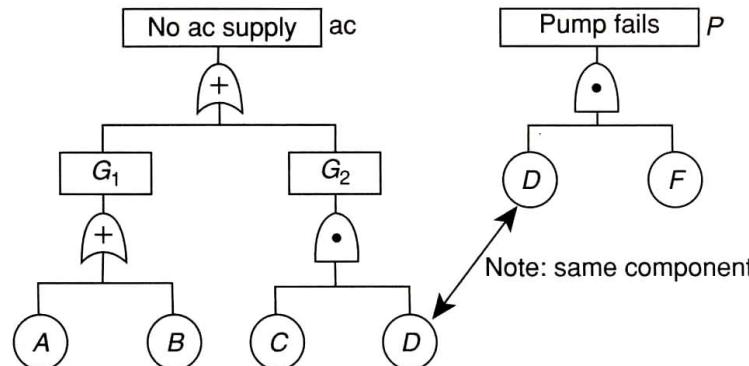
- $\Pr(I.ac) = f(I)[P(A) + P(B) + P(C)P(D)]$

Pumping System Event Tree: Example 3

22

Outcome 2: $I \cdot \overline{ac} \cdot P$

- Outcome 2: AC works, pump fails $I \cdot \overline{ac} \cdot P$
- Logic for Scenario Outcome 2, failure:
- Cut set for pump, P: (D,F)
 - Logic for Pump FT: $P = D \cdot F$
- Cut sets for AC Fault Tree: (A), (B), (C,D)
 - So, Logic for AC Fault Tree: $ac = A + B + C \cdot D$
 - What assumptions?



Pumping System Event Tree: Example 3

23

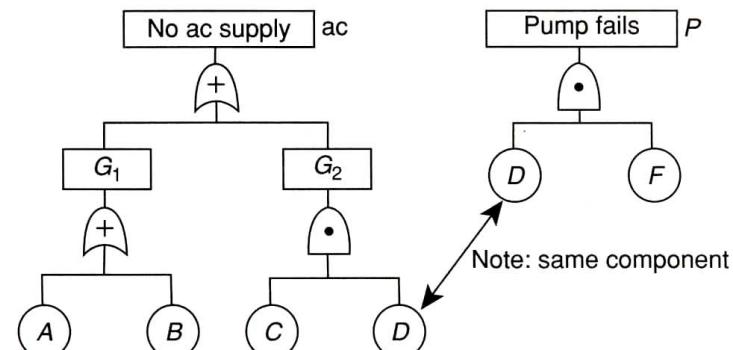
$$\text{Outcome 2: } I \cdot \overline{ac} \cdot P$$

Logic expressions to link events to component failure data

$$\begin{aligned}
 \overline{ac} &= \overline{A + B + C \cdot D} = (\overline{A} \cdot \overline{B}) \cdot (\overline{C} \cdot \overline{D}) \\
 &= \overline{A} \cdot \overline{B} \cdot (\overline{C} + \overline{D}) = \overline{A} \cdot \overline{B} \cdot \overline{C} + \overline{A} \cdot \overline{B} \cdot \overline{D} \\
 \\
 I \cdot \overline{ac} \cdot P &= I \cdot (\overline{A} \cdot \overline{B} \cdot \overline{C} + \overline{A} \cdot \overline{B} \cdot \overline{D}) \cdot P \\
 &= I \cdot (\overline{A} \cdot \overline{B} \cdot \overline{C} + \overline{A} \cdot \overline{B} \cdot \overline{D}) \cdot D \cdot F \\
 &= I \cdot \overline{A} \cdot \overline{B} \cdot \overline{C} \cdot D \cdot F + \underbrace{I \cdot \overline{A} \cdot \overline{B} \cdot \overline{D} \cdot D \cdot F}_{\emptyset}
 \end{aligned}$$

$D \cdot \overline{D} = D \cap \overline{D} = 0(\text{null set})$

$$I \cdot \overline{ac} \cdot P = I \cdot \overline{A} \cdot \overline{B} \cdot \overline{C} \cdot D \cdot F$$



... and corresponding fault trees of its subsystems.

Pumping System Event Tree: Example 3

24

- The frequency of each failure scenario and the frequency of system failure are calculated from the initial event frequency and from failure probabilities of the base components.
 - $f(\text{system failure}) = f(I) \cdot P(\text{ac}) + f(I) \cdot P(\overline{\text{ac}} \cdot P)$
- Scenario 3 Scenario 2

$$= f(I) \cdot \left\{ P[(A+B) + C \cdot D] + P(\overline{A} \cdot \overline{B} \cdot \overline{C} \cdot \overline{D} \cdot F) \right\}$$

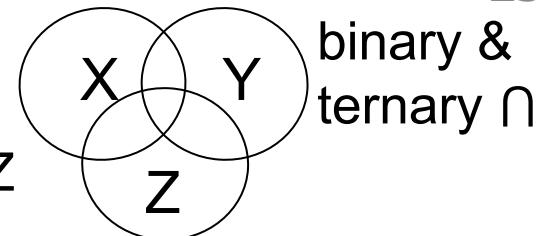
Note: 3 events linked by OR gates to result in Binary & Ternary overlap

AC Pump

We need to expand the expression!

Pumping System Example 3: Failure Frequency

25



- Recall Boolean expression for 3 events linked by OR (with independent approx.):

$$(X \cup Y \cup Z) = (1 - \{(1-X)(1-Y)(1-Z)\}) = X + Y + Z - XY - YZ - XZ + XYZ$$

- Alternate approach: Recall $(X \cup Y) = X + Y - XY$,

$$\begin{aligned} (X \cup Y \cup Z) &= X \cup (Y \cup Z) = X + (Y \cup Z) - X \cdot (Y \cup Z) \\ &= X + Y + Z - YZ - X(Y + Z - YZ) = X + Y + Z - XY - YZ - XZ + XYZ \end{aligned}$$

- We need the base component failure data to calculate the pumping system failure frequency (2 failure scenarios) =

Scenario 3

$$f(I) \cdot \left\{ \Pr[(A \cup B) \cup C \cdot D] + \Pr(\bar{A} \cdot \bar{B} \cdot \bar{C} \cdot D \cdot F) \right\} =$$

Scenario 2

Pumping System Example 3: Failure Frequency



- The system failure frequency based on the component failure data:

26

$$f(I) \cdot \left\{ \Pr[(A \cup B) \cup C \cap D] + \Pr(\bar{A} \cdot \bar{B} \cdot \bar{C} \cdot D \cdot F) \right\} =$$

Scenario 3, AC failure:

$$f(I) \cdot \left\{ \Pr(A) + \Pr(B) + \Pr(C) \cdot \Pr(D) - \Pr(A) \cdot \Pr(B) - \Pr(A) \cdot \Pr(C) \Pr(D) - \Pr(B) \cdot \Pr(C) \Pr(D) + \Pr(A) \cdot \Pr(B) \cdot \Pr(C) \cdot \Pr(D) \right\}$$

Scenario 2, Pump failure

$$+ f(I) \cdot \left\{ \Pr(\bar{A}) \cdot \Pr(\bar{B}) \cdot \Pr(\bar{C}) \cdot \Pr(D) \cdot \Pr(F) \right\}$$

System failure forecast based on unit failure history:

$$= 0.2136/\text{month} \sim 0.21/\text{month} \text{ (2 significant digits)} = \lambda.$$

Mean time to system failure, MTTF $\sim 1/(0.21/\text{mo}) = 4.8 \text{ mo}$

Pumping System Example 3: Failure Frequency

Pr or Frequency of Events

TABLE 3.3
Failure Data for the Events Shown in Figure 3.23

Item	Failure Probability or Frequencies	Success Probability
I	10 per month	—
A	0.01	0.99
B	0.01	0.99
C	0.02	0.98
D	0.05	0.95
F	0.01	0.99

Note frequency time unit.

ETA Summary, Strengths

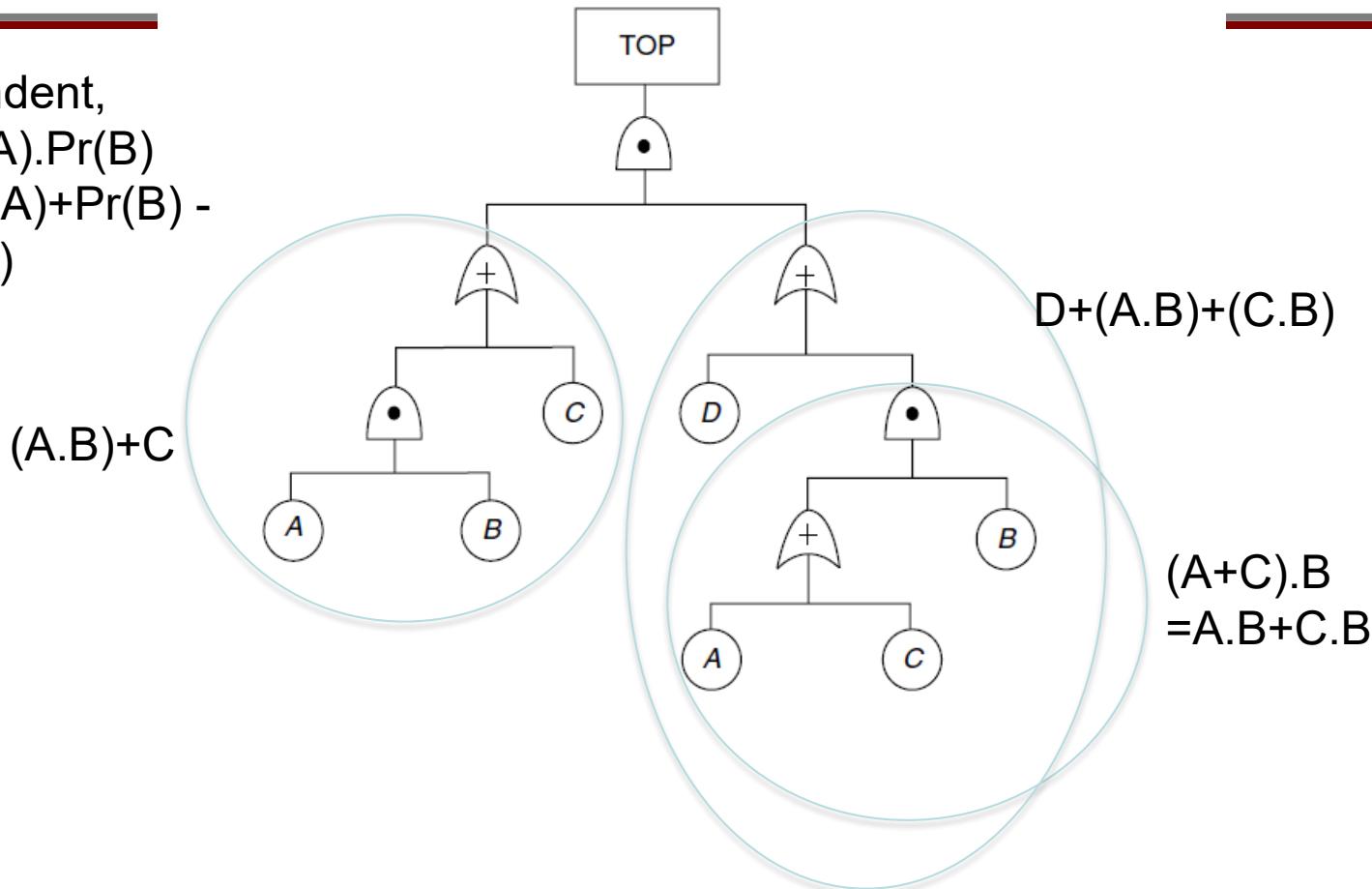
- ET is a simple logic diagram to represent event sequences following an initiating (upset) event and intermediate events involving hazard guards or barriers to control or reduce outcome failure Pr and mitigate consequences with each event generally modeled in a FT (using base event data).
- Use ET to analyze the effectiveness of hazard barriers and activation sequences designed to respond to system demand and act to reduce probabilities of occurrences or mitigate outcomes.
- Evaluate the need for improved procedures and for more **effective and more nearly independent** barriers, by reducing barrier co-failures, to manage hazards.

ETA Summary, Limitations

- Only one initiating event is incorporated in an event tree (also a strength for simplicity). An ET must be developed for each identified initiation event.
- Binary states (success/fail) only. The next step is to convert the ET into a Bayesian network that can include any number of discrete states or continuous states and can model conditional dependencies among components to represent behavior data from system observations.
- As with FTA, ETA is not a systematic method to identify system dependencies but useful as an initial, screening method to identify, diagram, and analyze outcomes of events following an initiation event, I, and to support decisions to manage System Risk within acceptable ranges.

Review

If Independent,
 $A \cdot B \equiv \Pr(A) \cdot \Pr(B)$
 $A + B \equiv \Pr(A) + \Pr(B) - \Pr(A)\Pr(B)$



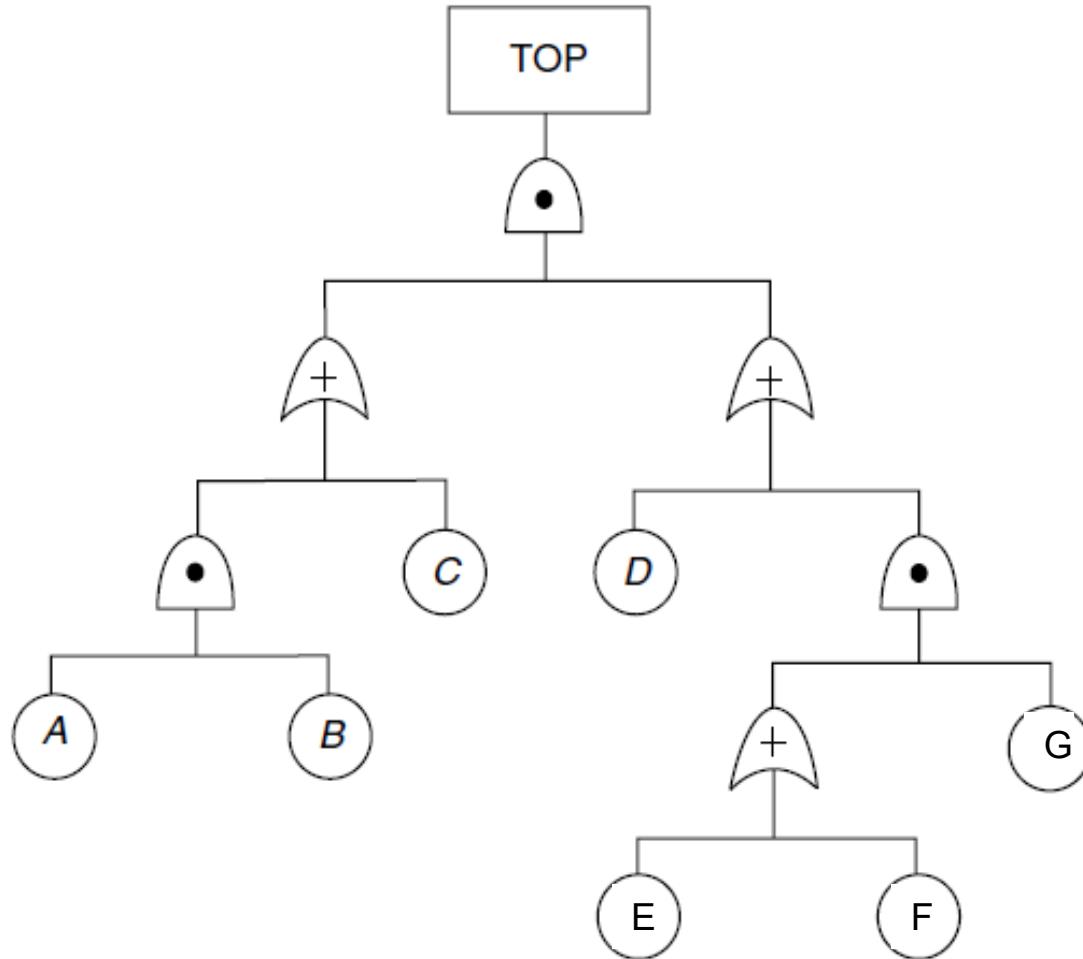
$$\text{TOP} = [(A \cdot B) + C] \cdot [D + (A \cdot B) + (C \cdot B)] = (A \cdot B \cdot D) + (A \cdot B \cdot A \cdot B) + (A \cdot B \cdot C \cdot B) + (C \cdot D) + (C \cdot A \cdot B) + (C \cdot C \cdot B)$$

$$\begin{aligned} \text{TOP} &= (A \cdot B \cdot D) + (A \cdot B) + (A \cdot B \cdot C) + (C \cdot D) + (C \cdot A \cdot B) + (C \cdot B) \\ &\quad \xleftarrow{\text{Simplification}} (A \cdot B) + (C \cdot D) + (C \cdot B) \end{aligned}$$

If $\Pr(A) = \Pr(B) = \Pr(C) = 0.01$: $\Pr(\text{TOP}) = 3(0.01)^2 = 0.0003$

$$X \cup (X \cap Y) = X$$

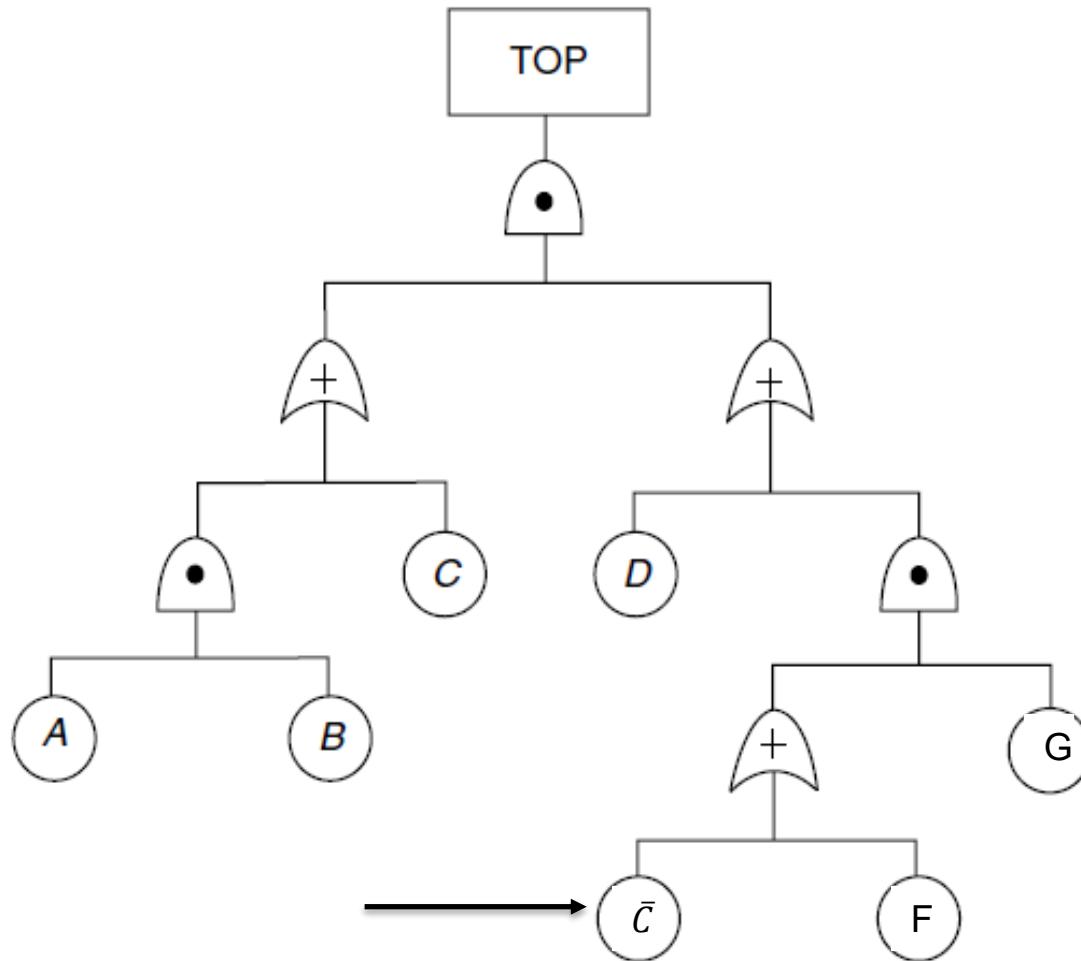
Review



$TOP = [(A \cdot B) + C] \cdot [D + (E + F)] \cdot G$

: No scope for reduction

Review

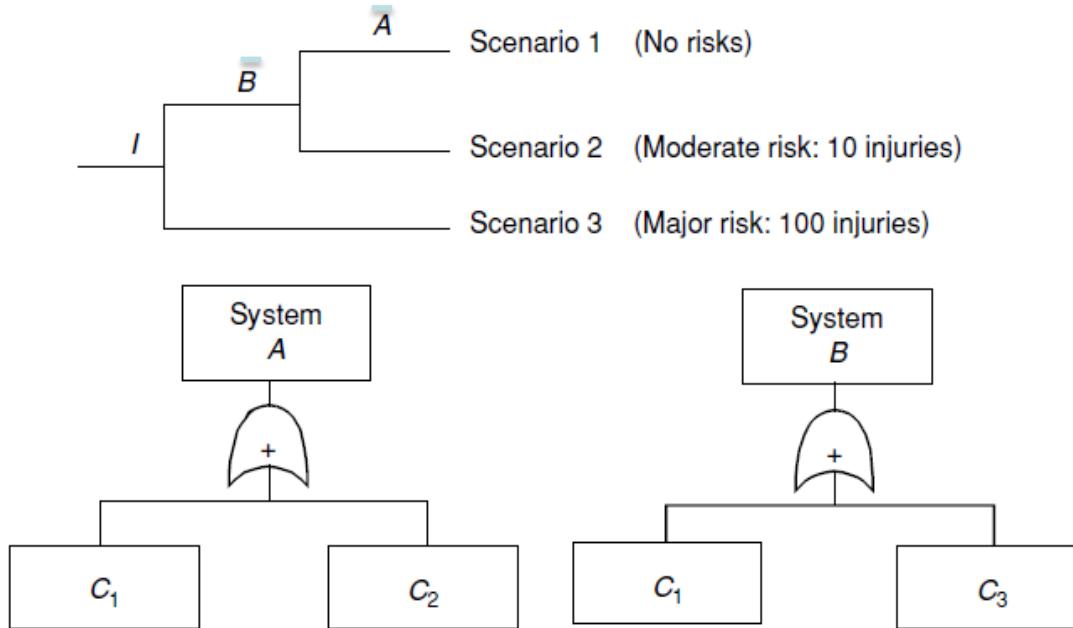


$$\text{TOP} = [(A \cdot B) + C] \cdot [D + (\bar{C} + F) \cdot G]$$

: No scope for reduction

HW Problem

33



- Determine a Boolean equation representing each of the event tree scenarios in terms of the fault tree basic events (C_1 , C_2 , and C_3).
- If the frequency of the initiating event I is $10^{-3}/\text{year}$, and $\Pr(C_1)=0.001$, $\Pr(C_2)=0.008$, and $\Pr(C_3)=0.005$, calculate the risk (injuries per year).
- Plot the risk profile curve (Farmer's curve) for this problem.

Layers of Protection Analysis (LOPA)

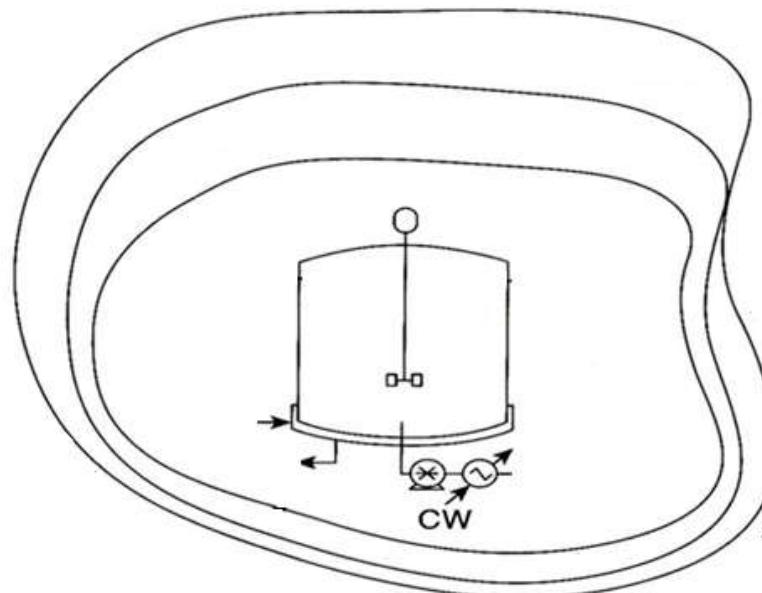
Unit 22

Fall 2021

LOPA

LOPA is a semi-quantitative analytical tool for assessing the adequacy of protection layers used to mitigate process risk.

LOPA builds upon well-known process hazards analysis techniques, applying semi-quantitative measures to the evaluation of the frequency of potential incidents and the probability of failure of the protection layers.



Community emergency response

Plant emergency response

Passive, physical protection:
(dikes, bunds, walls, distance/zoning)

Active effect reducing systems
(steam curtain/water spray/sprinkler)

Automatic action safety systems, SIS
(sensor, processor, actuator)

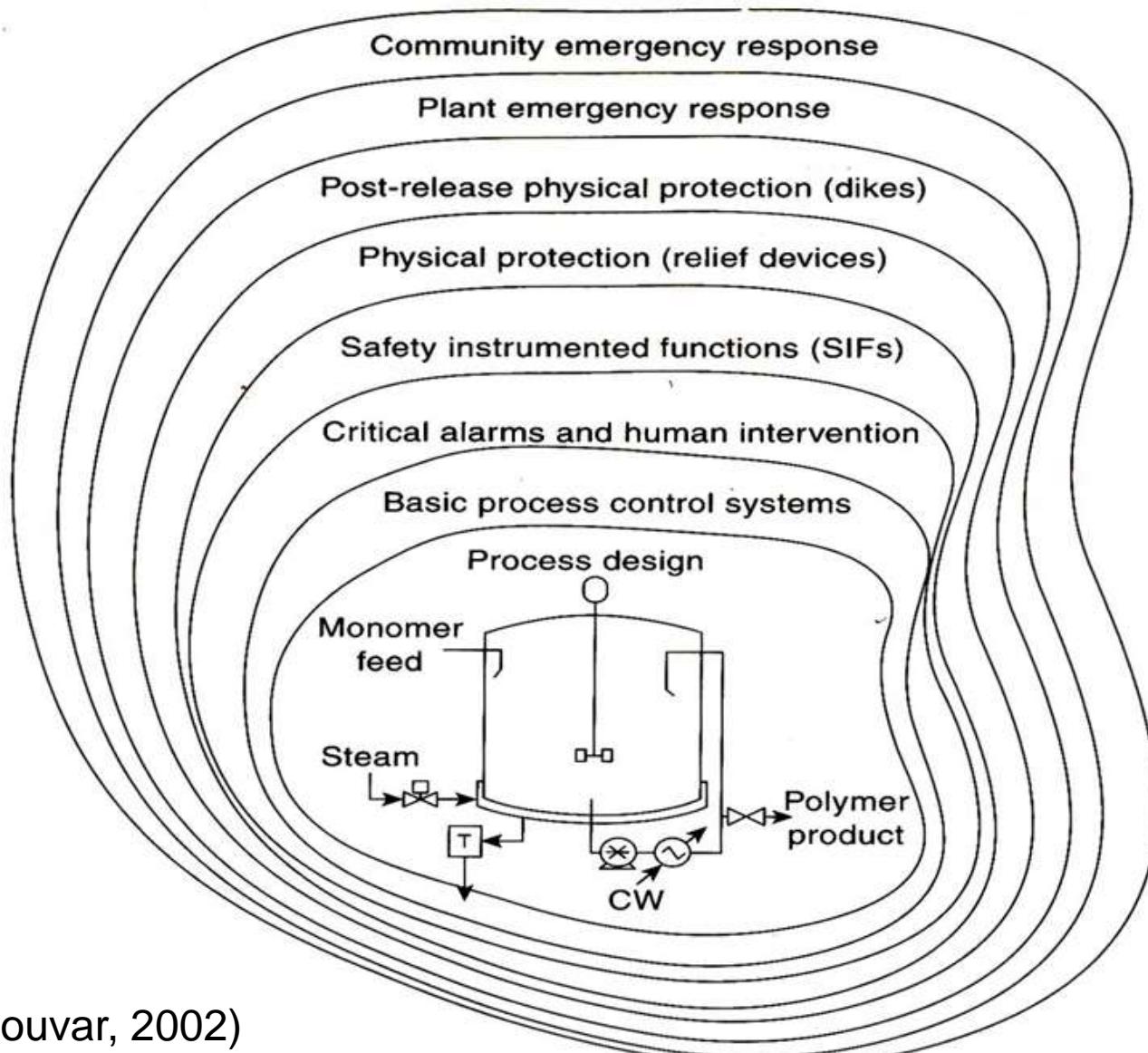
Critical alarms / Supervisor
Manual intervention

Basic process control system,
process alarm, operator supervision

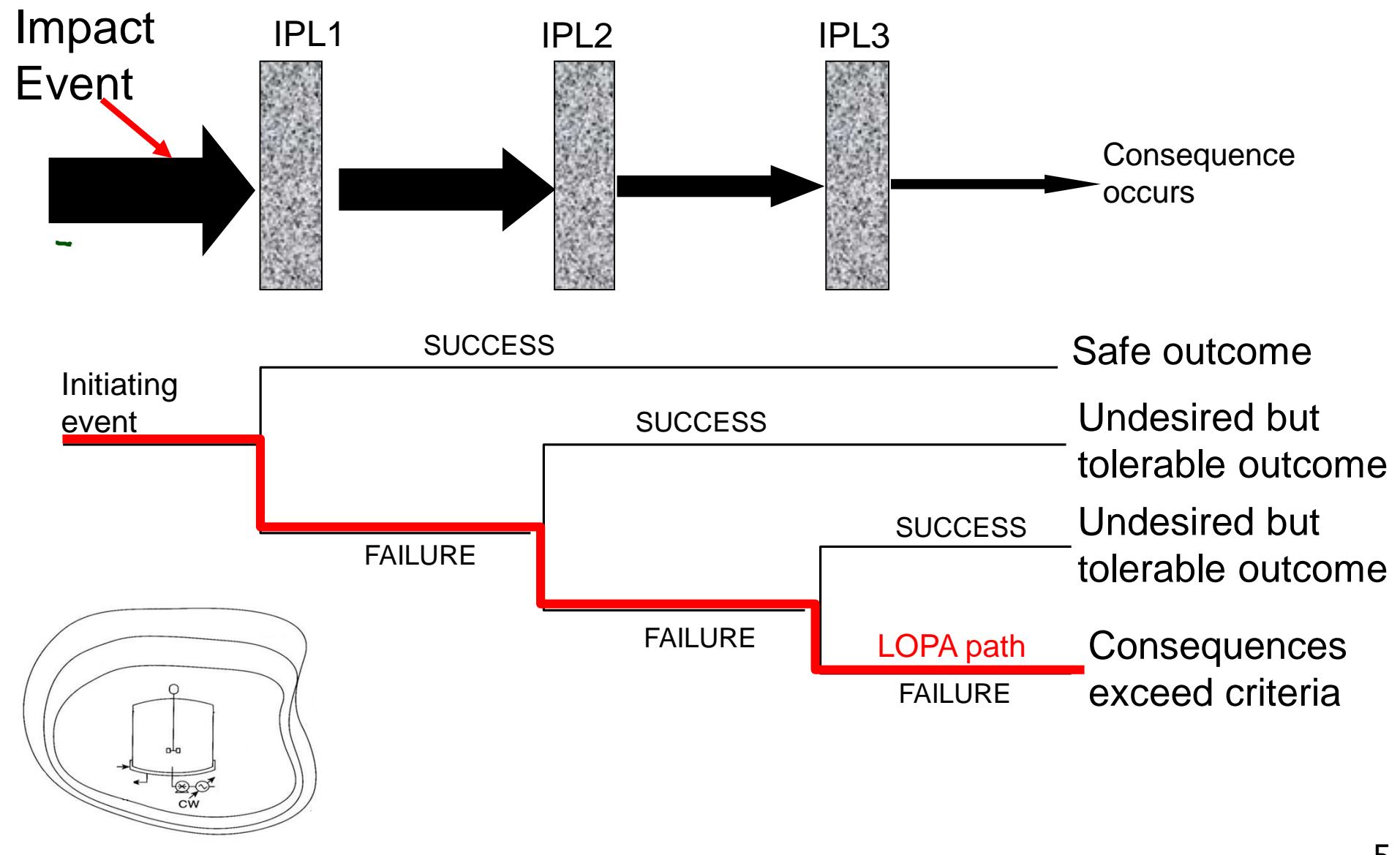
Inherent safer
process design

Independent protection layer- "onion"

Layers of Protection like Onion

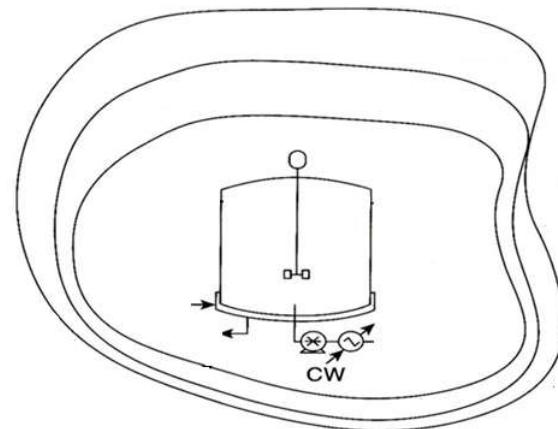
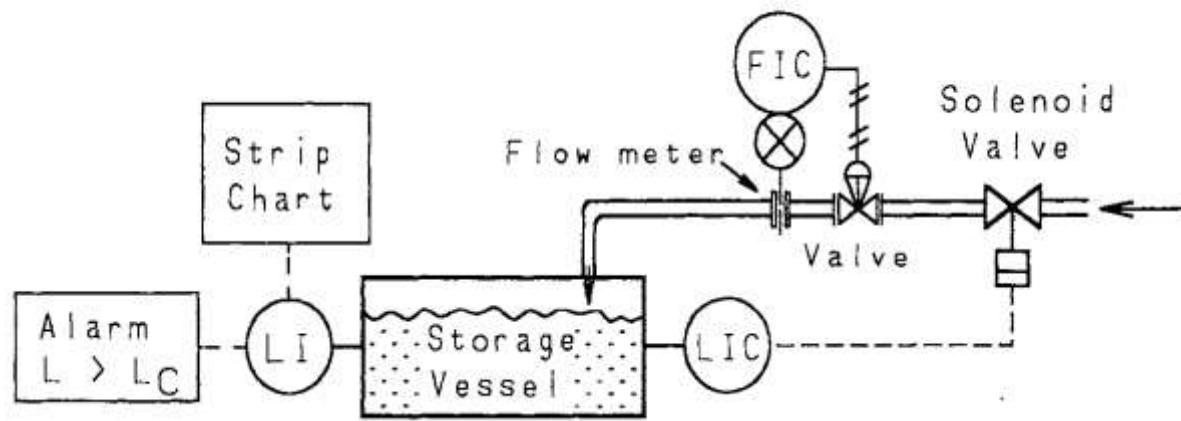


LOPA Concept



Independent Protection Layer (IPL)

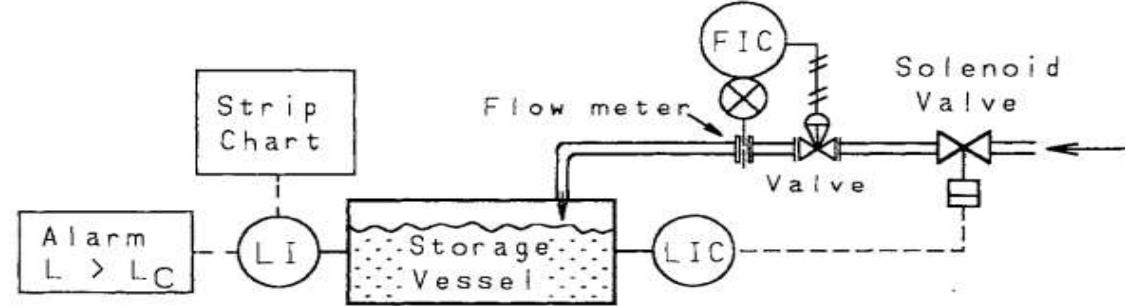
An IPL is a device, system, or action that is capable of preventing a scenario from proceeding to its undesired consequence, independent of the initiating event or the action of any other layer of protection associated with the scenario.



Three conditions for an IPL

1. Effective

- Detection
- Action
- Adequacy
- Timing



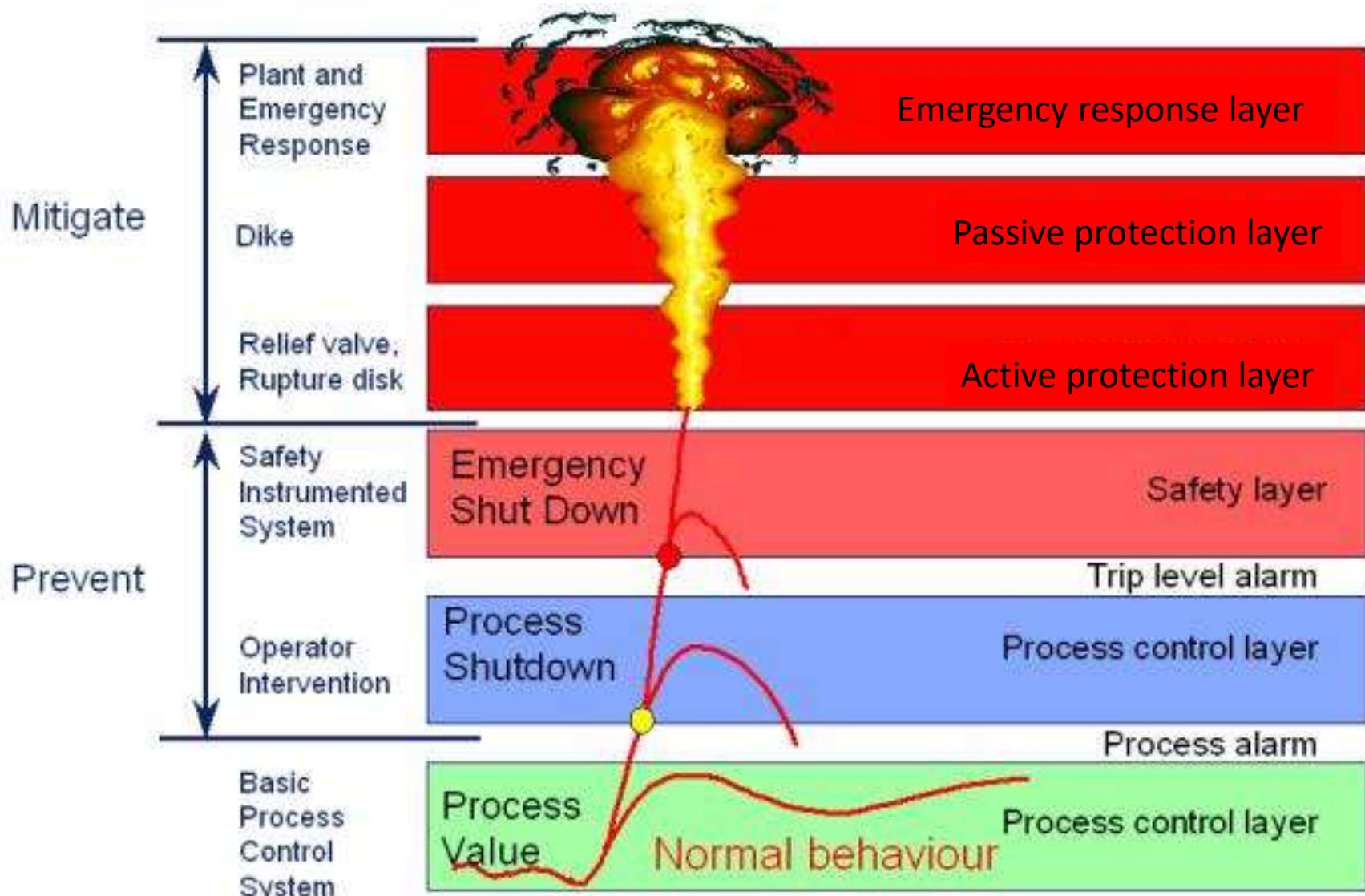
2. Independent

- Independent of initiating event
- Any other IPL

3. Auditable

- Meets risk mitigation requirement
- Test if functioning as designed
- Operational? Well documented?
- Modification made

Protection Layers



Brief description of the layers

Basic Process Control System (BPCS) The first layer is the BPCS. The control system itself provides significant safety through proper design of process control. Failure of BPCS can be an initiating event.

Operator intervention The next layer of protection is also provided by the control system and the system operators. Automated shutdown sequences in the process control system combined with operator intervention to shut down the process are the next layer of safety. Company procedures and training program improves the human performance in the system, but the procedures themselves are not an IPL.

Safety Instrumented System (SIS) The third layer is the SIS. It is a safety system independent of the process control system. It has separate sensors, valves and logic system. No process control is performed in this system, its only role is safety.

These layers are designed to prevent a safety related event. If a safety related event occurs there are additional layers designed to mitigate the impact of the event.

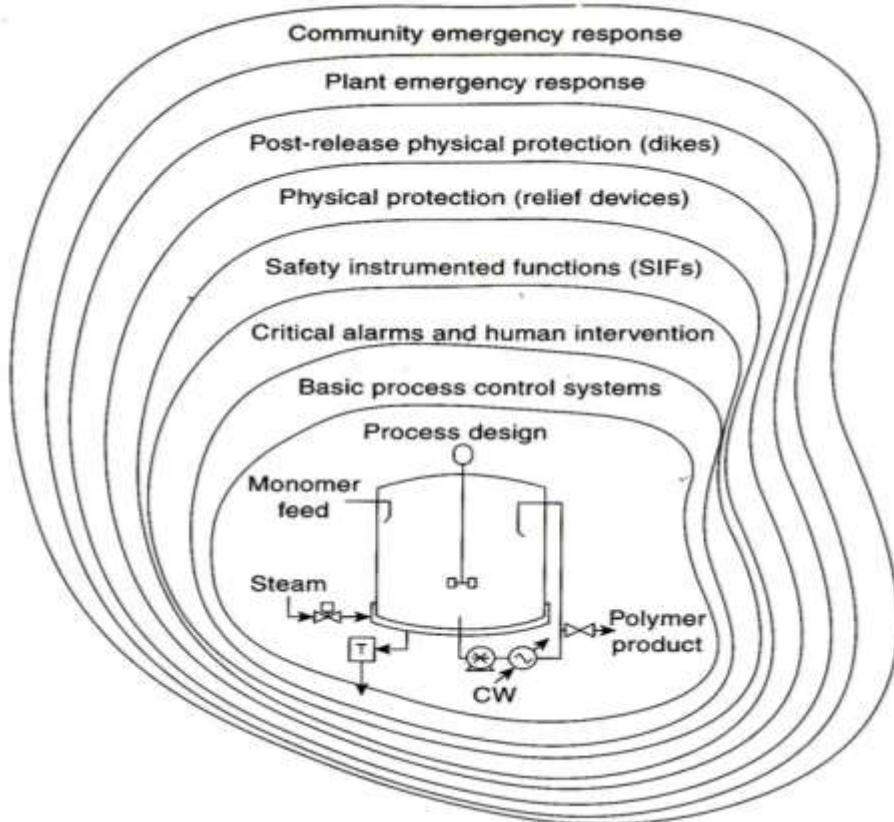
Brief description of the layers

Active protection layer such as Relief valve/rupture disk. The fourth layer is an active protection layer. This layer may have valves or rupture disks designed to provide a relief point that prevents a rupture, large spill or other uncontrolled release that can cause an explosion or fire.

Passive protection layer such as dike. The fifth layer is a passive protection layer. It may consist of a dike or other passive barrier that serves to contain a fire or channel the energy of an explosion in a direction that minimizes the spread of damage.

Emergency response. The final layer is plant and emergency response. If a large safety event occurs this layer responds in a way that minimizes ongoing damage, injury or loss of life. It may include evacuation plans, fire fighting, etc.

IPL-1. Process Design as an IPL

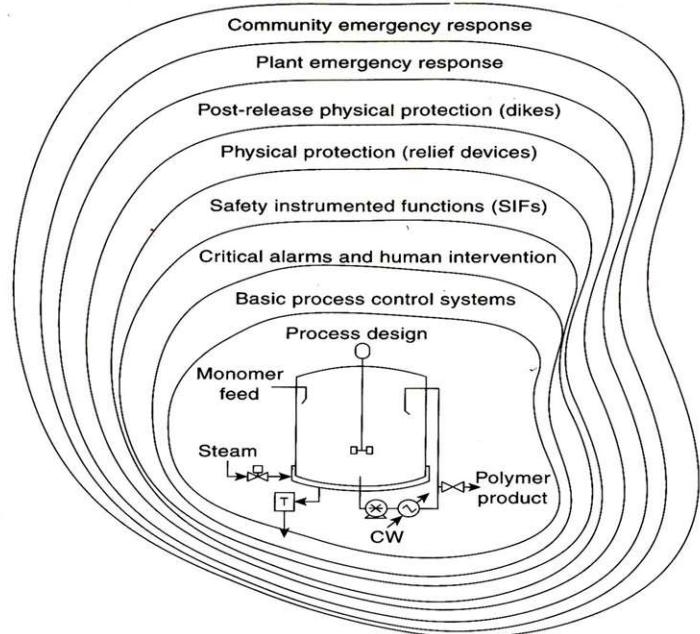


Inherently Safer Design

Example: A pump may have an impeller that is too small to generate high pressure in a down-stream vessel.

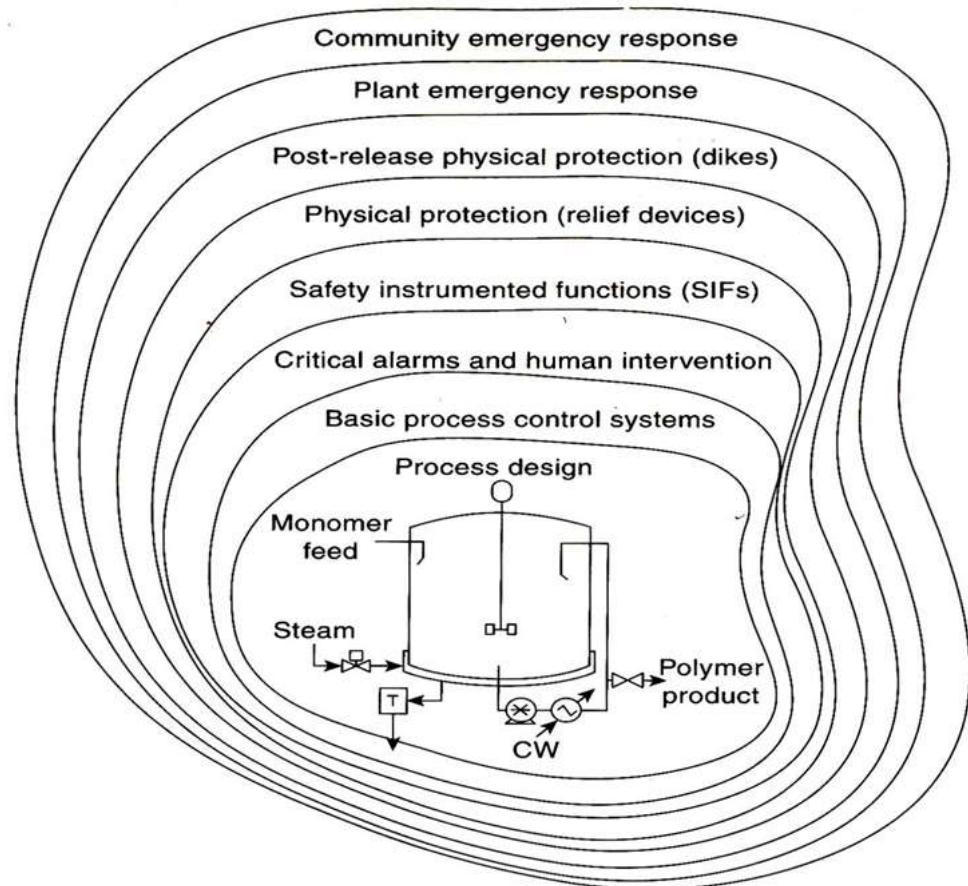
IPL-2. Basic Process Control Systems (BPCS)

- First level of protection during normal operation
- Failure of BPCS can be an initiating event

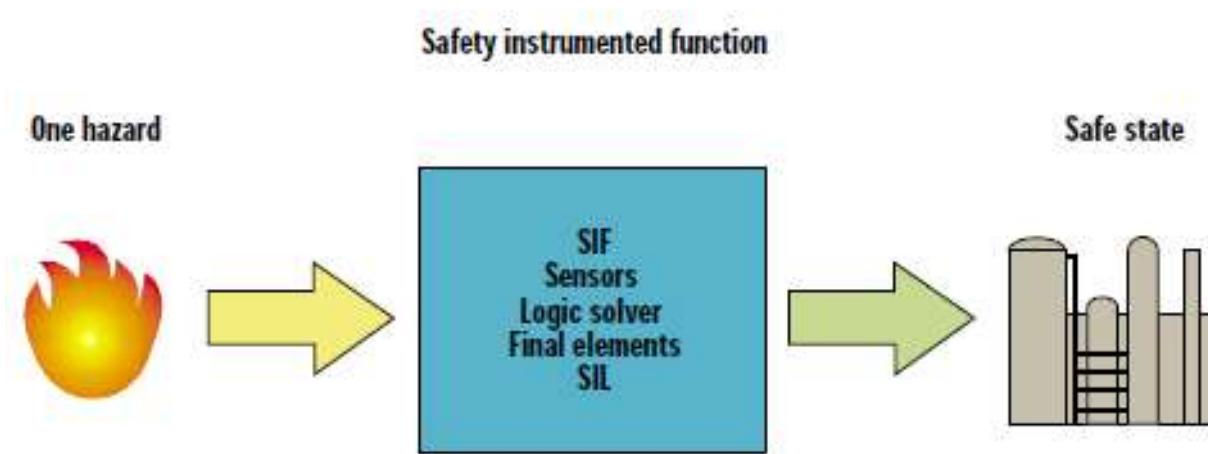


IPL-3. Critical Alarms and Human Intervention

- During normal operation
- Operator action



IPL-4. Safety Instrumented Function (SIF)



A SAFETY INSTRUMENTED FUNCTION (SIF) DETECTS A SPECIFIC HAZARD AND BRINGS THE PROCESS TO A SAFE STATE.

SIFs are identified safety function that provides a defined level of risk reduction or safety integrity level (SIL) for a specific hazard by automatic action using instrumentation. A SIF is made up of sensors, logic solver, and final elements that act in concert to detect a hazard and bring the process to a safe state. SIFs sometimes called safety interlocks and safety critical alarm.

Three Elements of SIF

Sensors

Field sensors are used to collect information necessary to determine if an emergency situation exists. The purpose of these sensors is to measure process parameters (e.g. temperature, pressure, flow) used to determine if the equipment or process is in a safe state. Sensor types range from simple pneumatic or electrical switches to smart transmitters with on-board diagnostics.

Logic Solver

The purpose of this component of SIF is to determine what action is to be taken based on the information gathered. **Highly reliable logic solvers are used which provide both fail-safe and fault-tolerant operation.** It is typically a controller that reads signals from the sensors and executes pre-programmed actions to prevent a hazard by providing output to final control elements.

Final Control Element

It implements the action determined by the logic system. This final control element is typically a pneumatically actuated On-Off valve operated by solenoid valves.

It is imperative that all three elements of the SIS function as designed in order to safely isolate the process plant in the event of an emergency.

Example: Safety instrumented function (SIF)

1. High pressure in a vessel opens a vent valve: the specific hazard is overpressure of the vessel. The high pressure is detected by a pressure-sensing instrument, and logic (PLC, relay, hardwire, etc.) opens a vent valve, bringing the system to a safe state.
2. High fuel gas pressure initiates action to close the main fuel gas valve.
3. High reactor temperature initiates action to open cooling media valve.

Safety Integrity Level (SIL)

- **Safety Integrity Level (SIL)** is level of risk-reduction provided by a safety function, or a target level of risk reduction.
- Each order of magnitude of risk reduction correlates with an increase in one of the required SIL numbers
- **SIL is a measurement of performance required for a Safety Instrumented Function (SIF):**

SIL 1	Single sensor Single logic processor Single final element	$\geq 1 \times 10^{-2} - < 1 \times 10^{-1}$
SIL 2	"Multiple" sensors "Multiple" channel logic processor "Multiple" final elements	$\geq 1 \times 10^{-3} - < 1 \times 10^{-2}$
SIL 3	Multiple sensors Multiple channel logic processor Multiple final elements	$\geq 1 \times 10^{-4} - < 1 \times 10^{-3}$

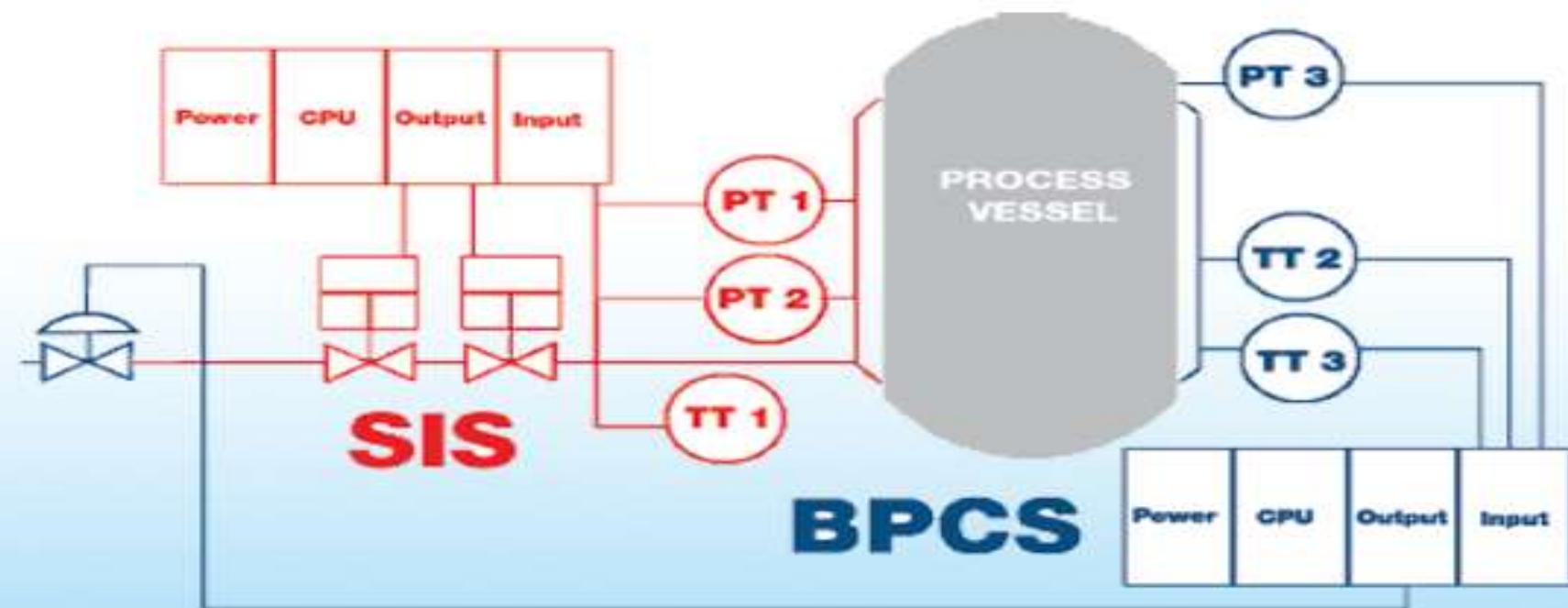
Safety Integrity Level (SIL)

- SIL 1** $PFD \geq 1 \times 10^{-2}$ to $<1 \times 10^{-1}$ [IEC 61511 (IEC, 2001)]. These SIFs are normally implemented with a single sensor, a single SIS logic solver and a single final control element.
- SIL 2** $PFD \geq 1 \times 10^{-3}$ to $<1 \times 10^{-2}$ These SIFs are typically fully redundant from the sensor through the SIS logic solver to the final control element.
- SIL 3** $PFD \geq 1 \times 10^{-4}$ to $<1 \times 10^{-3}$ These SIFs are typically fully redundant from sensor through the SIS logic solver to the final control element and require careful design and frequent proof tests to achieve low PFD figures. Many companies find that they have a limited number of SIL 3 SIFs due to the high cost normally associated with this architecture.
- SIL 4** $PFD \geq 1 \times 10^{-5}$ to $<1 \times 10^{-4}$ These SIFs are included in the IEC 61508 and 61511 standards, but such SIFs are difficult to design and maintain and are not used in LOPA.

SIS-Safety Instrumented System

- A Safety Instrumented System (SIS) is a combination of sensors, logic solvers, and final elements that perform one or more safety instrumented functions (SIFs).
- SIS also known as emergency shutdown system.
- An SIS is engineered to perform "specific control functions" to failsafe or maintain safe operation of a process when unacceptable or dangerous conditions occur.
- **Safety Instrumented Systems must be independent from all other control systems** that control the same equipment in order to ensure SIS functionality is not compromised.
- **SIS is composed of the same types of control elements (including sensors, logic solvers, actuators and other control equipment) as a Basic Process Control System (BPCS). However, all of the control elements in an SIS are dedicated solely to the proper functioning of the SIS.**

SIS vs. BPCS

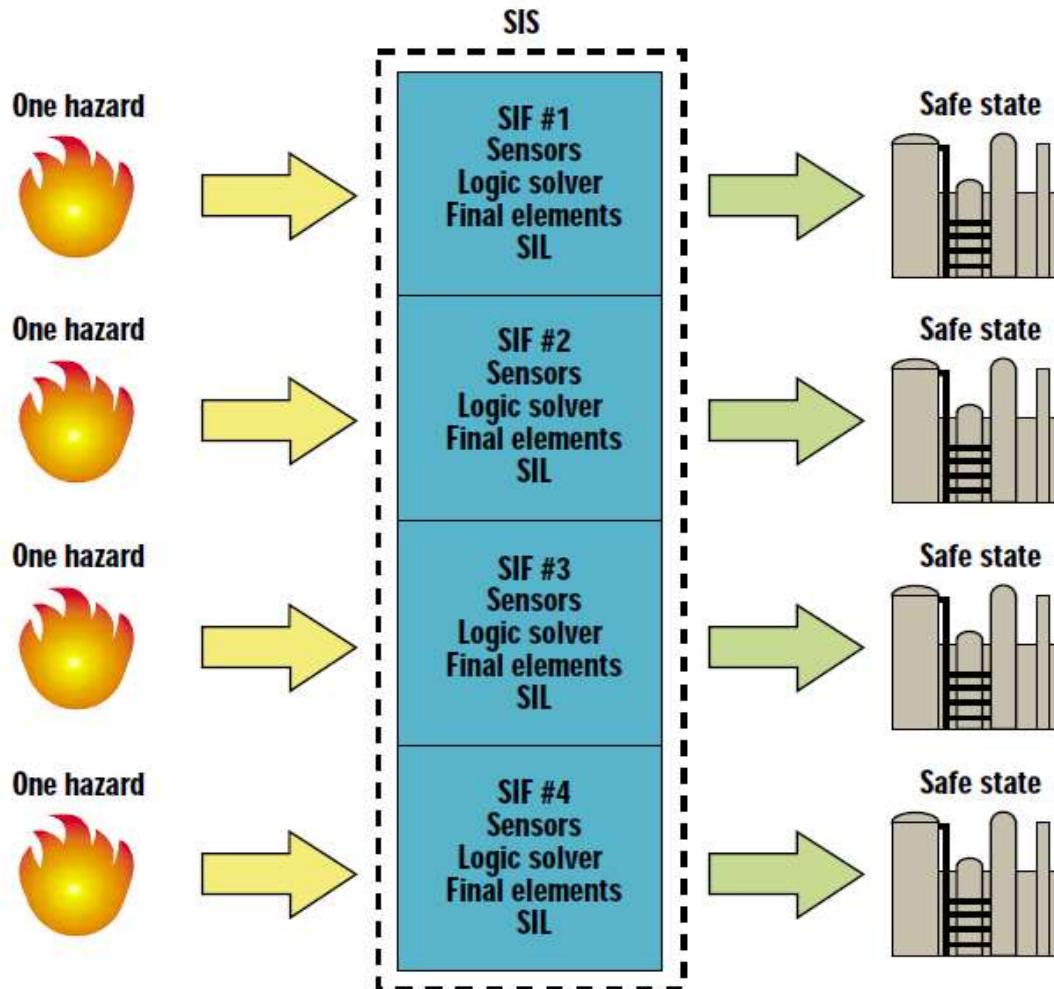


Process schematic showing
functional separation of SIS
(red) and BPCS (blue).

SIS

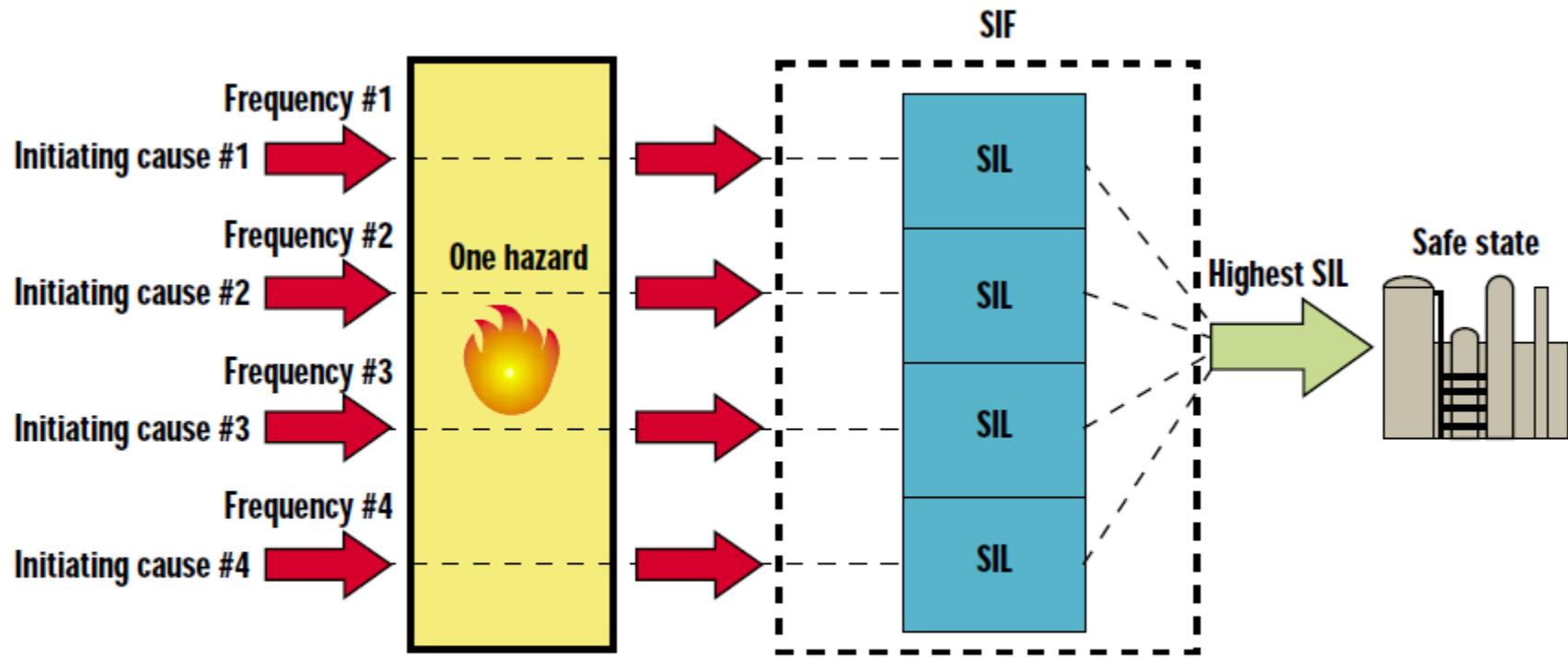
- In most process industry applications, safety instrumented systems are there just in case the human operators and the basic process control system fail to maintain process conditions within a safe operating envelope. By design, safety instrumented systems spend most of their time idling about in stand-by.

SIS and SIF



A SAFETY INSTRUMENTED SYSTEM (SIS) IS A COMBINATION OF ONE OR MORE SAFETY INSTRUMENTED FUNCTIONS (SIFs).

SIF and SIL

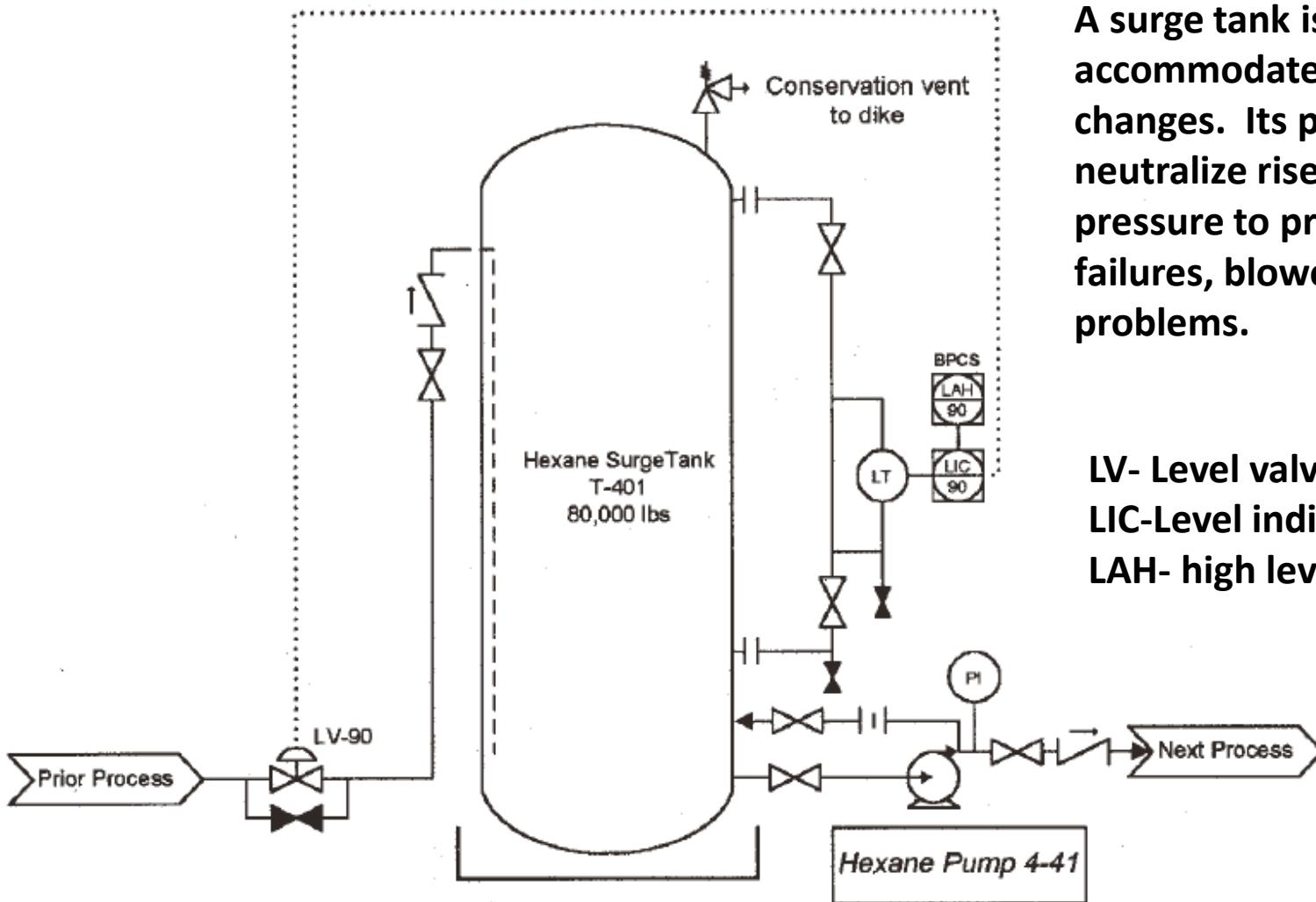


WHEN A SAFETY INSTRUMENTED FUNCTION (SIF) HAS MULTIPLE POTENTIAL CAUSES, EACH WITH ITS OWN SAFETY INTEGRITY LEVEL (SIL) REQUIREMENT, THE HIGHEST SIL IS GENERALLY SELECTED FOR THE ENTIRE SIF.

Safety integrity level (SIL)

The amount of defined risk reduction to be provided by the SIF; also can be seen as the level of dependability of the SIF.

Hexane Surge Tank



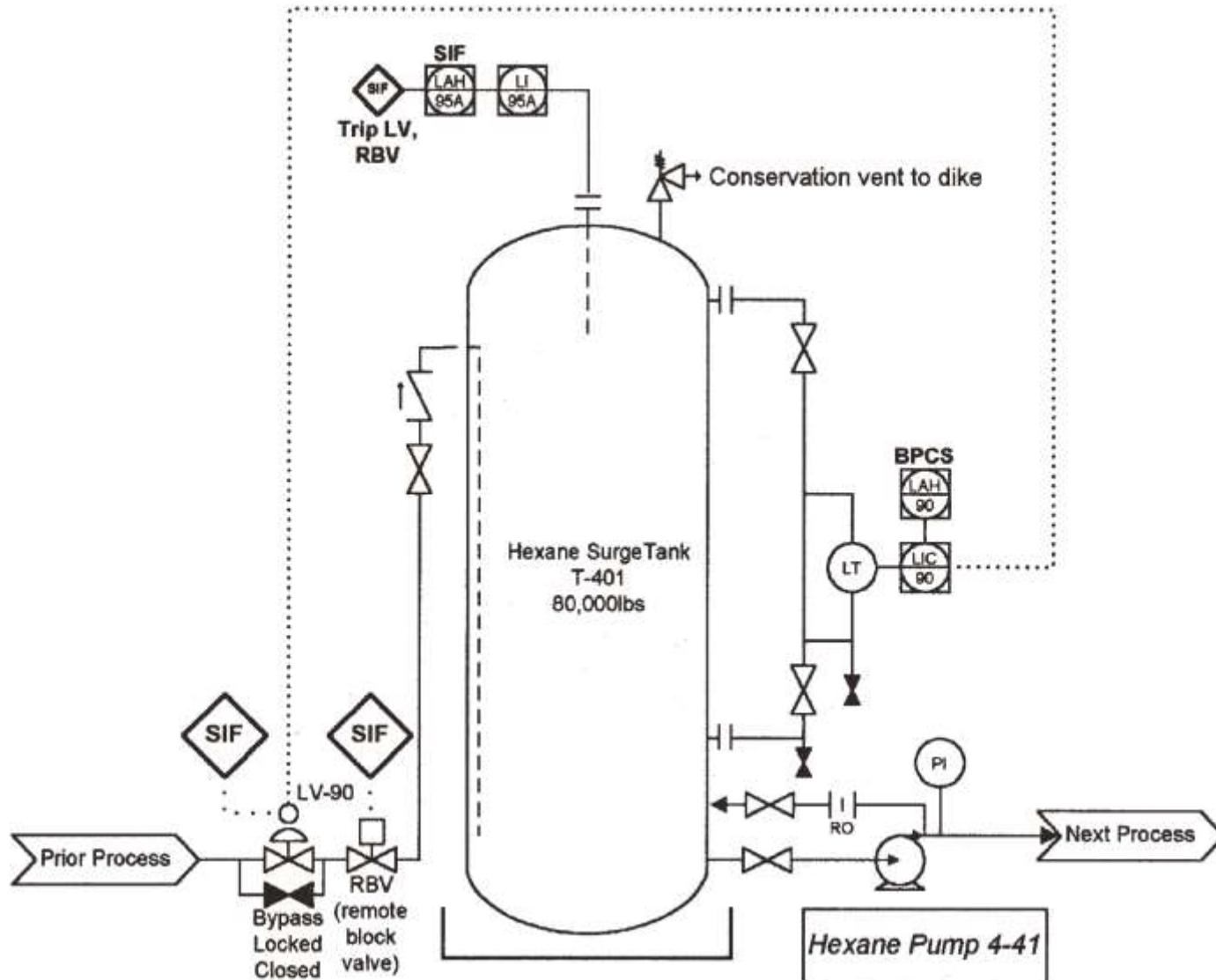
A surge tank is used to accommodate pressure changes. Its purpose is to neutralize rises and falls in pressure to prevent system failures, blowouts, and other problems.

LV- Level valve

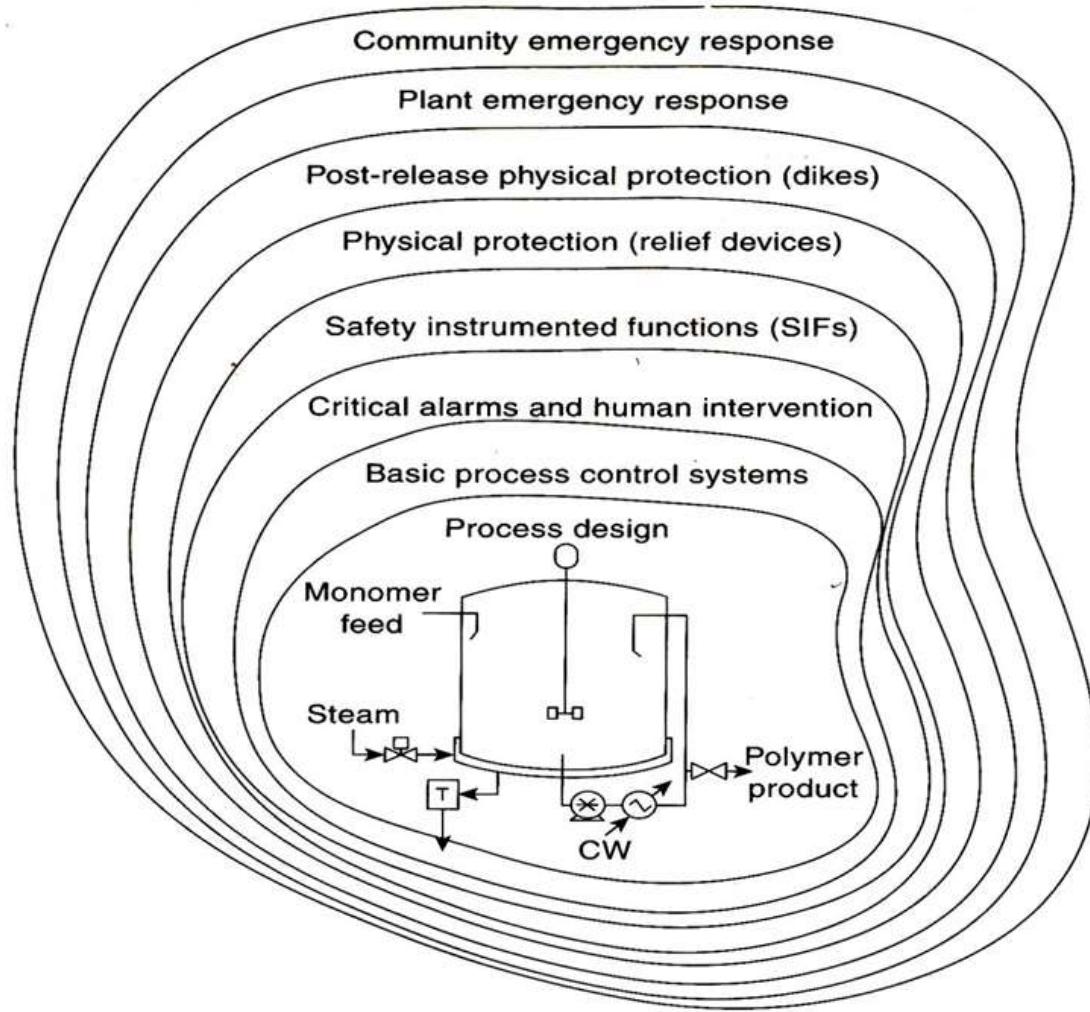
LIC- Level indicator controller

LAH- high level alarm

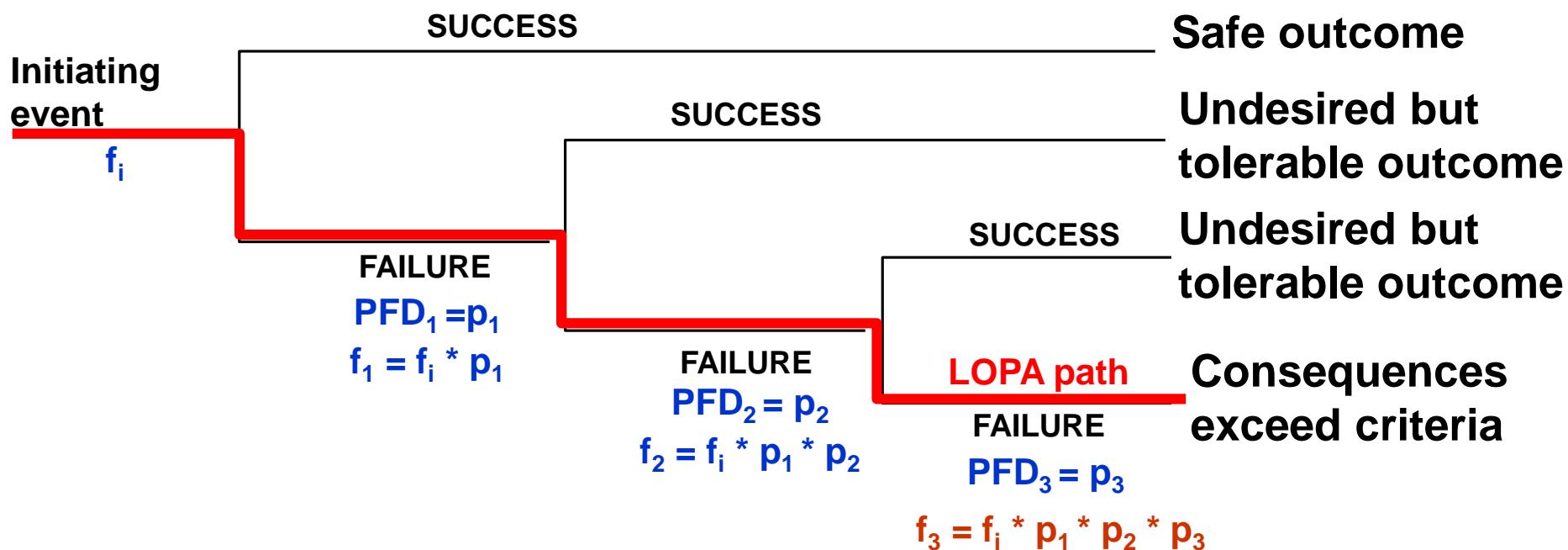
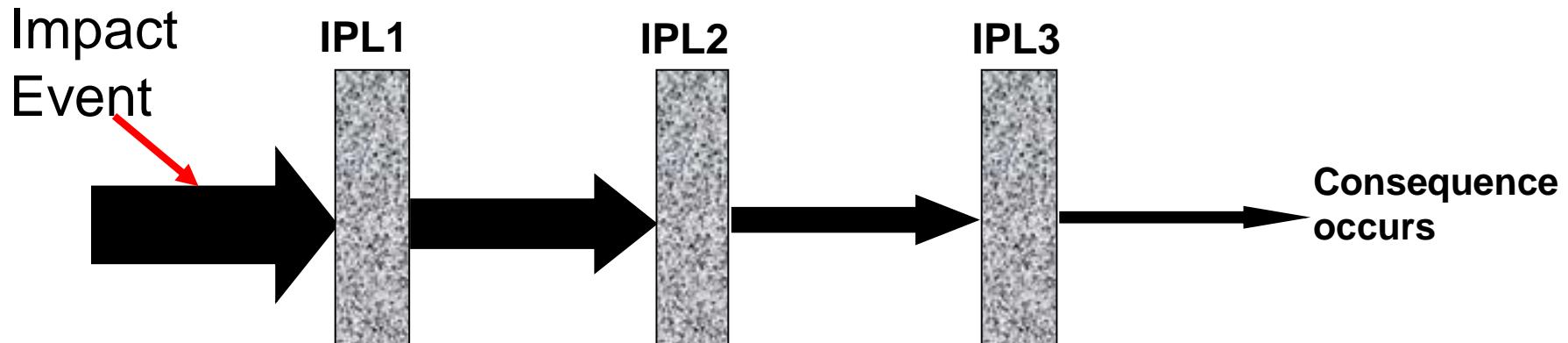
Hexane Surge Tank with added IPL (a SIF)



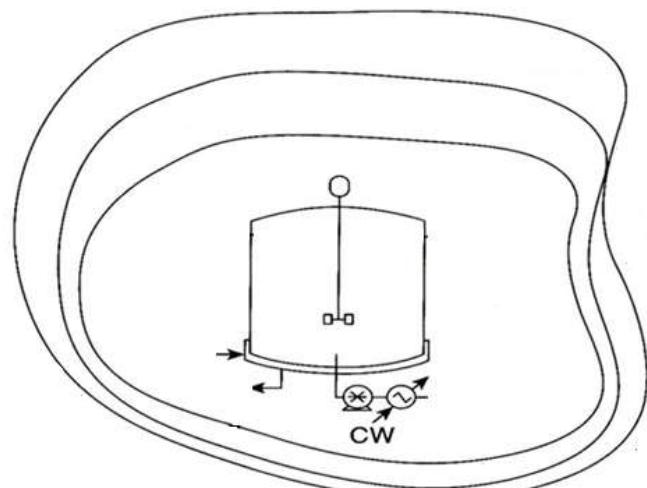
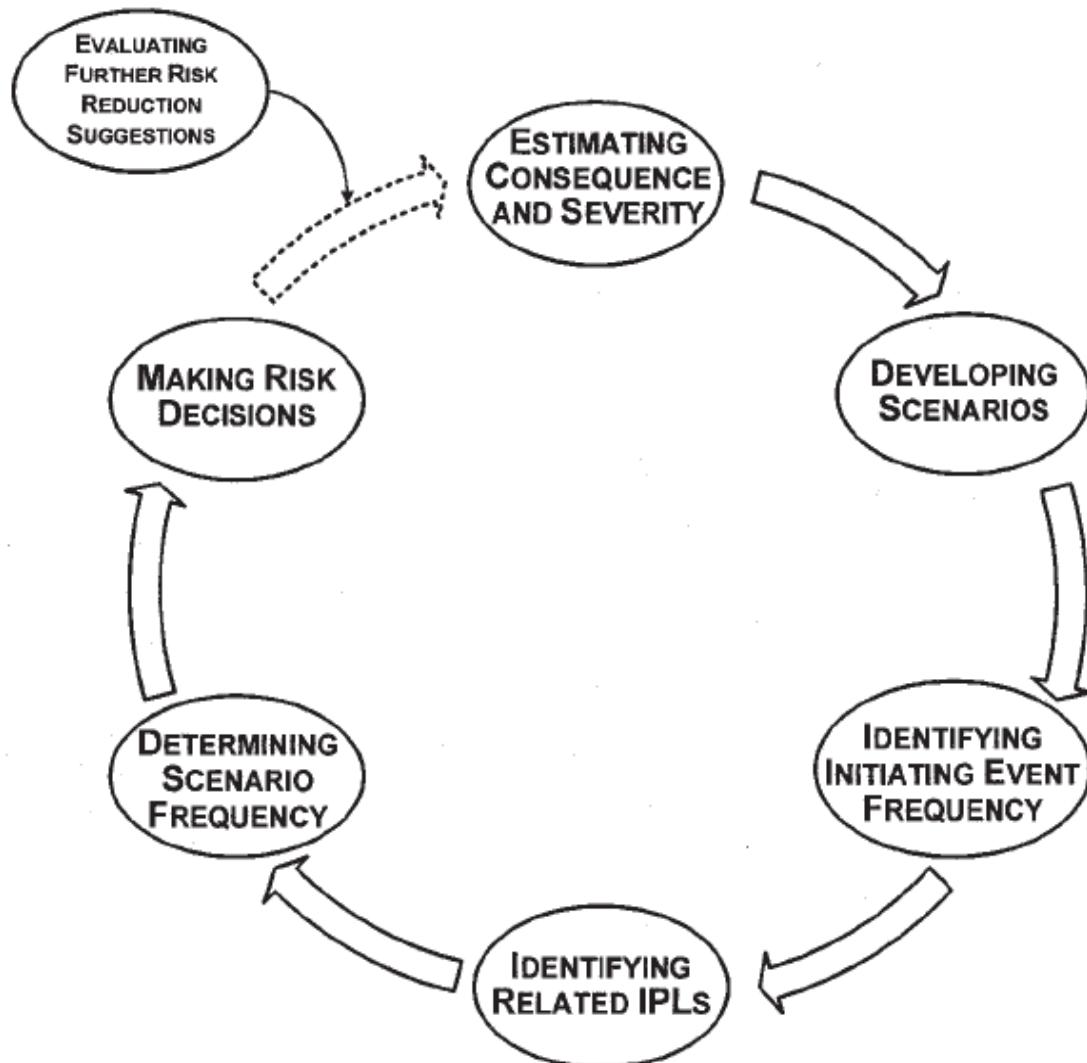
LOPA Procedures



Estimating the frequency of the consequence



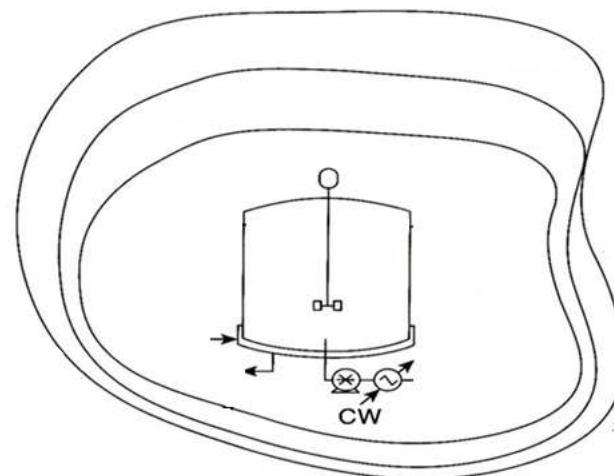
LOPA Procedures



Why do we start with estimating the consequence?

Step 1. Estimating consequence and severity

- Evaluate scenarios identified by other hazard analysis such as HAZOP
- Screen the scenarios by estimating the magnitude. Consequence are approximated by categories.



Method 1: Category Approach without Direct Reference to Human Harm

- Avoid estimating the number of potential injuries or fatalities
- Simple and easy to use because the size and properties of the release are relatively easy to assess

Example Consequence Categorization

Release Characteristic	Size of Release (beyond a dike)					
	1- to 10-pound release	10- to 100-pound release	100- to 1,000-pound release	1,000- to 10,000-pound release	10,000- to 100,000-pound release	>100,000-pound release
Extremely toxic above BP*	Category 3	Category 4	Category 5	Category 5	Category 5	Category 5
Extremely toxic below BP or highly toxic above BP	Category 2	Category 3	Category 4	Category 5	Category 5	Category 5
Highly toxic below BP or flammable above BP	Category 2	Category 2	Category 3	Category 4	Category 5	Category 5
Flammable below BP	Category 1	Category 2	Category 2	Category 3	Category 4	Category 5
Combustible liquid	Category 1	Category 1	Category 1	Category 2	Category 2	Category 3

*BP = atmospheric boiling point

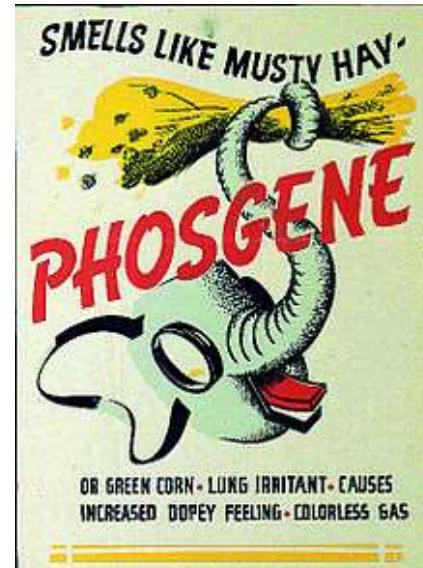
Consequence Characteristic	Magnitude of Loss					
	Spared or non-essential equipment	Plant outage <1 month	Plant outage 1–3 months	Plant outage >3 months	Vessel rupture 3,000 to 10,000 gal 100–300 psi	Vessel rupture >10,000 gal >300 psi
Mechanical damage to large main product plant	Category 2	Category 3	Category 4	Category 4	Category 4	Category 5
Mechanical damage to small by-product plant	Category 2	Category 2	Category 3	Category 4	Category 4	Category 5

Consequence Characteristic	Consequence cost (U.S. dollars)				
	\$0-\$10,000	\$10,000-\$100,000	\$100,000-\$1,000,000	\$1,000,000-\$10,000,000	>\$10,000,000
Overall cost of event	Category 1	Category 2	Category 3	Category 4	Category 5

Note: This table of values is for example only, to indicate what one or more companies use to categorize consequences. CCPS does not endorse one method over another.

Example: State the consequence categories for the following scenarios:

1. Facility damage of \$1,000,000
2. Release of 2,000 lb of isopropanol at 75 °F
(Isopropanol BP is 180 °F).
3. Release of 200 lb of phosgene at 40°F (BP 49°F)



Method 2: Qualitative Estimates with Human Harm

- Uses final impact on humans. Impact on human is estimated based on experience and modeling
- Many people tend to better understand consequence in terms of harm rather than expressing risk in terms of release size
- Assumptions for probability of injury, and the probability that a person is present in the area may over- or underestimated the risk

Low Consequence	
Personnel	Minor or no injury; no lost time
Community	No injury, hazard, or annoyance to public
Environment	Recordable event with no agency notification or permit violation
Facility	Minimal equipment damage at an estimated cost of less than \$100,000 and with no loss of production

Very High Consequence	
Personnel	Fatality or permanently disabling injury
Community	One or more severe injuries
Environment	Significant release with serious offsite impact and more likely than not to cause immediate or long-term health effects
Facility	Major or total destruction of process area(s) at an estimated cost greater than \$10,000,000 or a significant loss of production

TABLE 3.2
Qualitative Categorization (Combined Loss Categories)

Low Consequence	
Personnel	Minor or no injury; no lost time
Community	No injury, hazard, or annoyance to public
Environment	Recordable event with no agency notification or permit violation
Facility	Minimal equipment damage at an estimated cost of less than \$100,000 and with no loss of production
Medium Consequence	
Personnel	Single injury, not severe; possible lost time
Community	Odor or noise complaint from the public
Environment	Release that results in agency notification or permit violation
Facility	Some equipment damage at an estimated cost greater than \$100,000 and with minimal loss of production
High Consequence	
Personnel	One or more severe injuries
Community	One or more minor injuries
Environment	Significant release with serious offsite impact
Facility	Major damage to process area(s) at an estimated cost greater than \$1,000,000 or some loss of production
Very High Consequence	
Personnel	Fatality or permanently disabling injury
Community	One or more severe injuries
Environment	Significant release with serious offsite impact and more likely than not to cause immediate or long-term health effects
Facility	Major or total destruction of process area(s) at an estimated cost greater than \$10,000,000 or a significant loss of production

Method 3. Quantitative Estimates with Human Harm

- This method involves the use of mathematical models to simulate the release (Source term modeling), and the toxic or blast or thermal effect

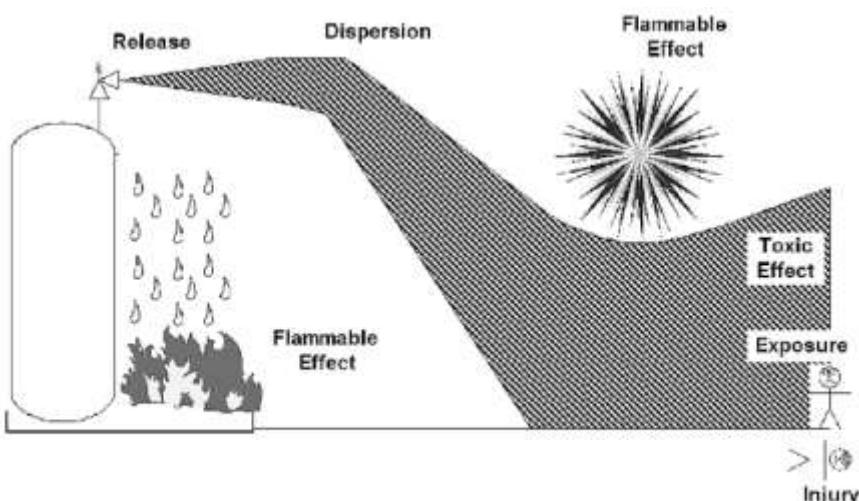


FIGURE 3.1. Potential consequences from a flammable/toxic release.

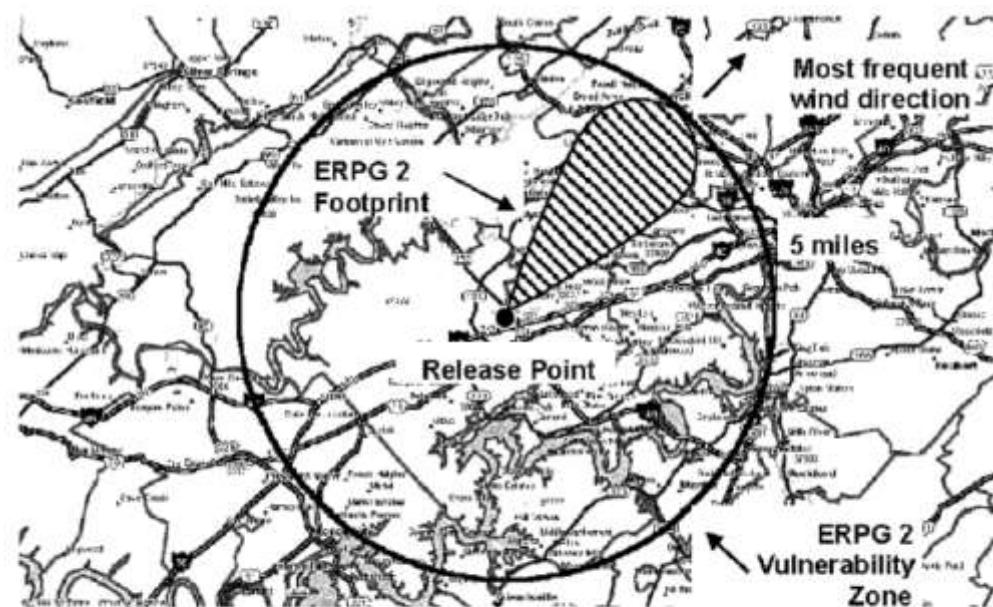
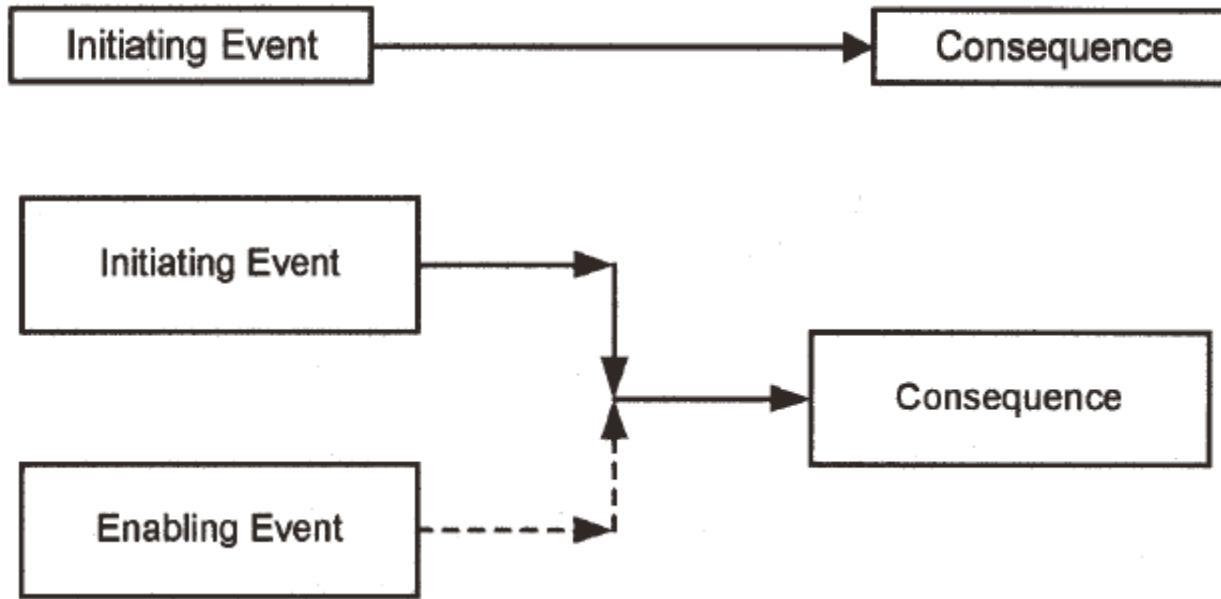


FIGURE 3.2. Typical vulnerability zone from detailed (mathematical) modeling. ERPG 2 is the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to one hour without experiencing or developing irreversible or serious health effects or symptoms which could impair an individual's ability to take protective action.

Book: LOPA, CCPS: AIChE

Step 2. Developing Scenario



Loss of cooling (the initiating event) can result in a runaway exothermic reaction in a batch reactor and overpressure, but only during a portion of the reaction (the enabling condition) when the system is in the reaction exotherm phase and thus vulnerable to loss of cooling.



HAZOP can be used to develop scenario

Step 3. Estimating the frequency of the initiating event

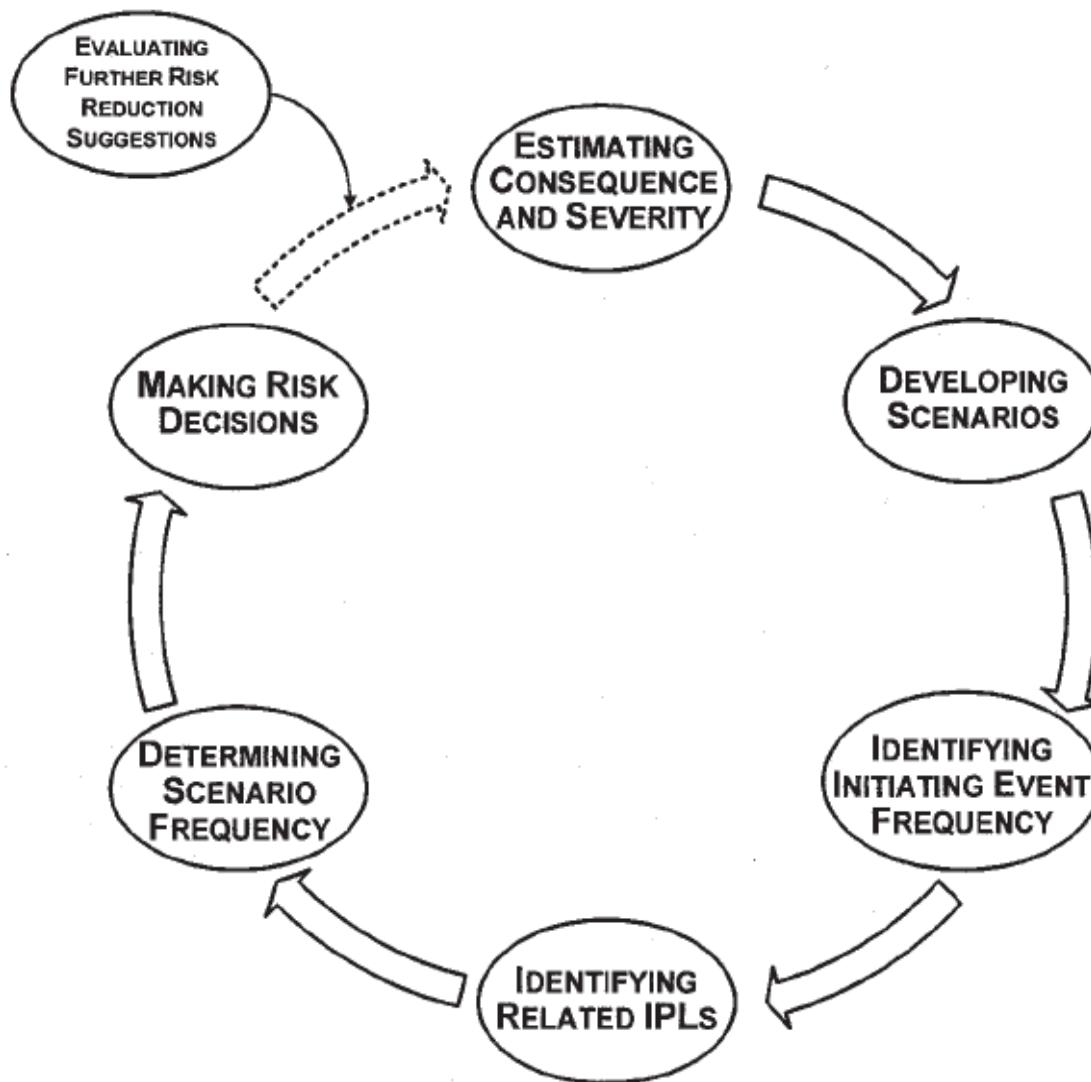
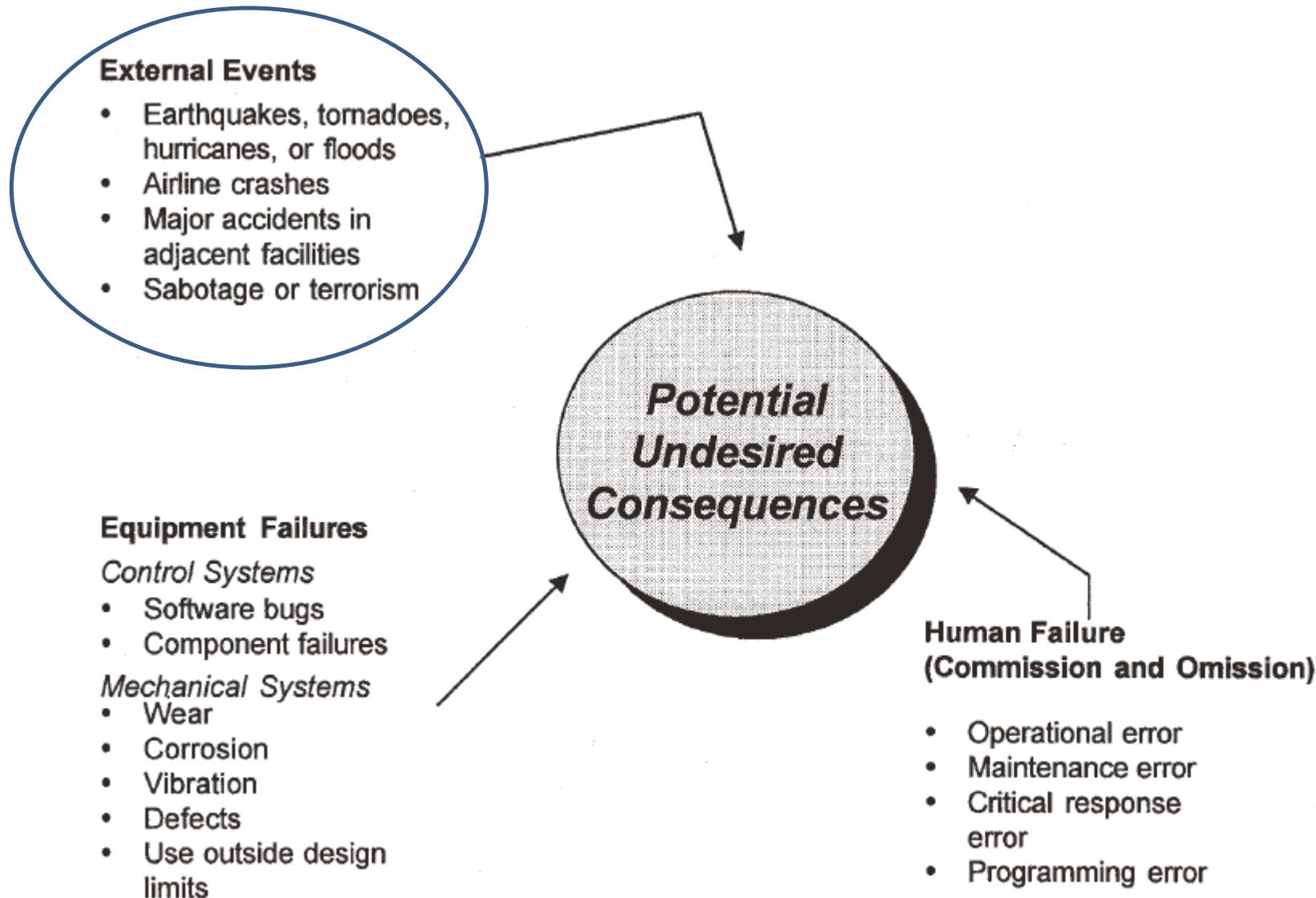


Table 11-3 Typical Frequency Values Assigned to Initiating Events¹

Initiating event	Frequency range from literature (per yr)	Example of a value chosen by a company for use in LOPA (per yr)
Pressure vessel residual failure	10^{-5} to 10^{-7}	1×10^{-6}
Piping residual failure, 100 m, full breach	10^{-5} to 10^{-6}	1×10^{-5}
Piping leak (10% section), 100 m	10^{-3} to 10^{-4}	1×10^{-3}
Atmospheric tank failure	10^{-3} to 10^{-5}	1×10^{-3}
Gasket/packing blowout	10^{-2} to 10^{-6}	1×10^{-2}
Turbine/diesel engine overspeed with casing breach	10^{-3} to 10^{-4}	1×10^{-4}
Third-party intervention (external impact by backhoe, vehicle, etc.)	10^{-2} to 10^{-4}	1×10^{-2}
Crane load drop	10^{-3} to 10^{-4} /lift	1×10^{-4} (/lift)
Lightning strike	10^{-3} to 10^{-4}	1×10^{-3}
Safety valve opens spuriously	10^{-2} to 10^{-4}	1×10^{-2}
Cooling water failure	1 to 10^{-2}	1×10^{-1}
Pump seal failure	10^{-1} to 10^{-2}	1×10^{-1}
Unloading/loading hose failure	1 to 10^{-2}	1×10^{-1}
BPCS instrument loop failure	1 to 10^{-2}	1×10^{-1}
Regulator failure	1 to 10^{-1}	1×10^{-1}
Small external fire (aggregate causes)	10^{-1} to 10^{-2}	1×10^{-1}
Large external fire (aggregate causes)	10^{-2} to 10^{-3}	1×10^{-2}
LOTO (lock-out tag-out) procedure failure (overall failure of a multiple element process)	10^{-3} to 10^{-4} / opportunity	1×10^{-3} (/opportunity)
Operator failure (to execute routine procedure; well trained, unstressed, not fatigued)	10^{-1} to 10^{-3} / opportunity	1×10^{-2} (/opportunity)

¹ Individual companies choose their own values, consistent with the degree of conservatism or the company's risk tolerance criteria. Failure rates can also be greatly affected by preventive maintenance routines.

Types of Initiating event



Step 4. Identifying IPLs and estimating the frequency of the IPLs

- Some accident scenario will require only one IPL
- Recognizing the existing safeguards that meet the requirement of an IPL is important
- Most companies provide a predetermined set of IPL values

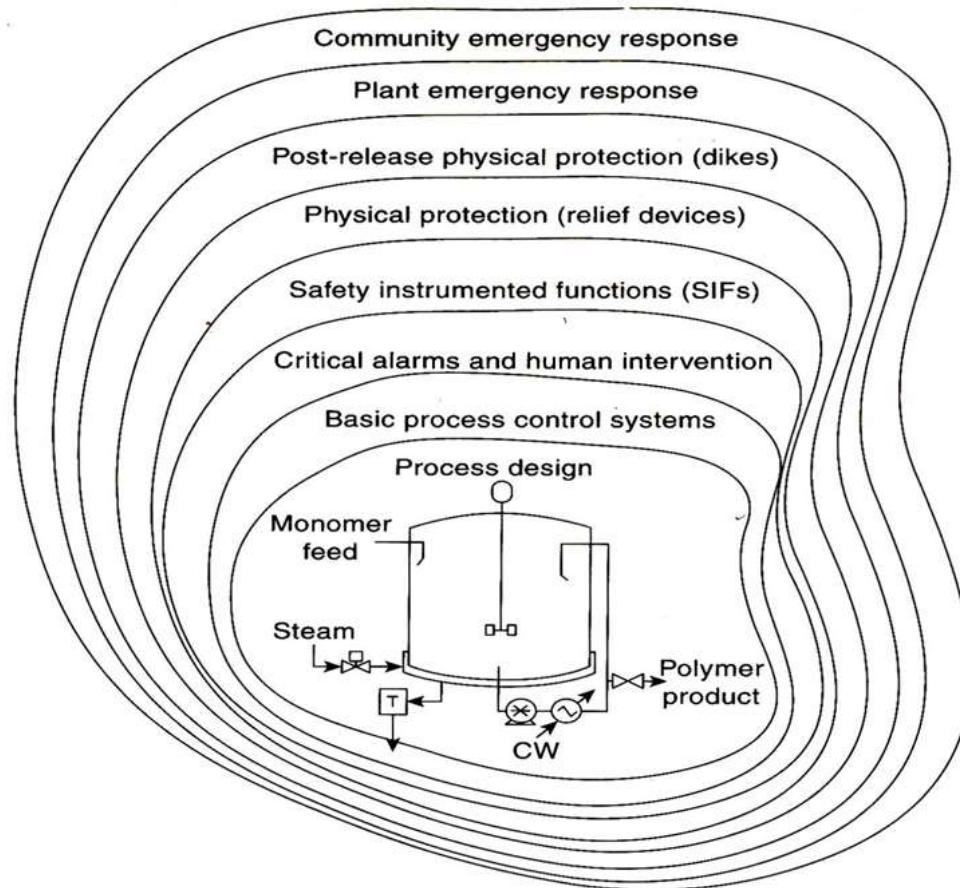


Table 11-5 PFDs for Active IPLs and Human Actions

Active IPL or human action	Comments [assuming an adequate design basis, inspections, and maintenance procedures (active IPLs) and adequate documentation, training, and testing procedures (human action)]	PFDs from industry ¹	PFDs from CCPS ¹
Relief valve	Prevents system from exceeding specified over-pressure. Effectiveness of this device is sensitive to service and experience.	1×10^{-1} to 1×10^{-5}	1×10^{-2}
Rupture disc	Prevents system from exceeding specified over-pressure. Effectiveness of this device can be sensitive to service and experience.	1×10^{-1} to 1×10^{-5}	1×10^{-2}
Basic process control system (BPCS)	Can be credited as an IPL if not associated with the initiating event being considered. See IEC (1998, 2001). ^{2,3}	1×10^{-1} to 1×10^{-2}	1×10^{-1}
Safety instru- mented func- tions (inter- locks)	See IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2001) for life-cycle require- ments and additional discussion. ^{2,3}		
Human action with 10 min response time	Simple well-documented action with clear and reliable indications that the action is required.	1 to 1×10^{-1}	1×10^{-1}
Human action with 40 min response time	Simple well-documented action with clear and reliable indications that the action is required.	1×10^{-1} to 1×10^{-2}	1×10^{-2}

¹CCPS, *Simplified Process Risk Assessment: Layer of Protection Analysis*, D. A. Crowl, ed. (New York: American Institute of Chemical Engineers, 2001) (in press).

²IEC (1998), IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, Parts 1–7*, Geneva: International Electrotechnical Commission.

³IEC (2001), IEC 61511, *Functional Safety Instrumented Systems for the Process Industry Sector, Parts 1–3*. (Draft in Process), Geneva: International Electrotechnical Commission.

Table 11-4 PFDs for Passive IPLs

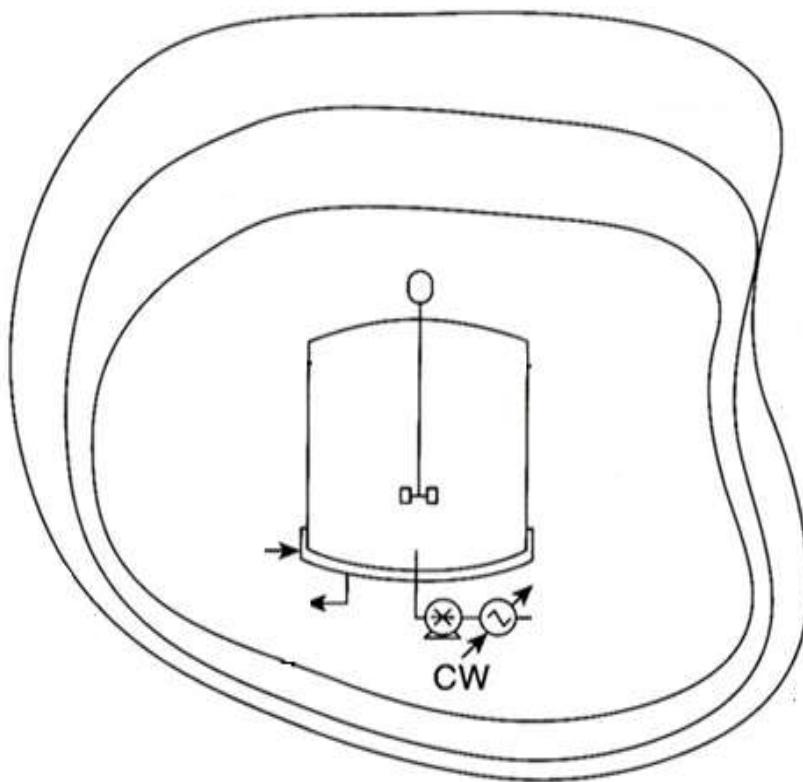
Passive IPLs	Comments (assuming an adequate design basis, inspections, and maintenance procedures)	PFDs from industry ¹	PFDs from CCPS ¹
Dike	Reduces the frequency of large consequences (widespread spill) of a tank overfill, rupture, spill, etc.	1×10^{-2} to 1×10^{-3}	1×10^{-2}
Underground drainage system	Reduces the frequency of large consequences (widespread spill) of a tank overfill, rupture, spill, etc.	1×10^{-2} to 1×10^{-3}	1×10^{-2}
Open vent (no valve)	Prevents overpressure	1×10^{-2} to 1×10^{-3}	1×10^{-2}
Fireproofing	Reduces rate of heat input and provides additional time for depressurizing, fire fighting, etc.	1×10^{-2} to 1×10^{-3}	1×10^{-2}
Blast wall or bunker	Reduces the frequency of large consequences of an explosion by confining blast and by protecting equipment, buildings, etc.	1×10^{-2} to 1×10^{-3}	1×10^{-3}
Inherently safer design	If properly implemented, can eliminate scenarios or significantly reduce the consequences associated with a scenario	1×10^{-1} to 1×10^{-6}	1×10^{-2}
Flame or detonation arrestors	If properly designed, installed, and maintained, can eliminate the potential for flashback through a piping system or into a vessel or tank	1×10^{-1} to 1×10^{-3}	1×10^{-2}

¹CCPS, *Simplified Process Risk Assessment: Layer of Protection Analysis*, D. A. Crowl, ed. (New York: American Institute of Chemical Engineers, 2001) (in press).

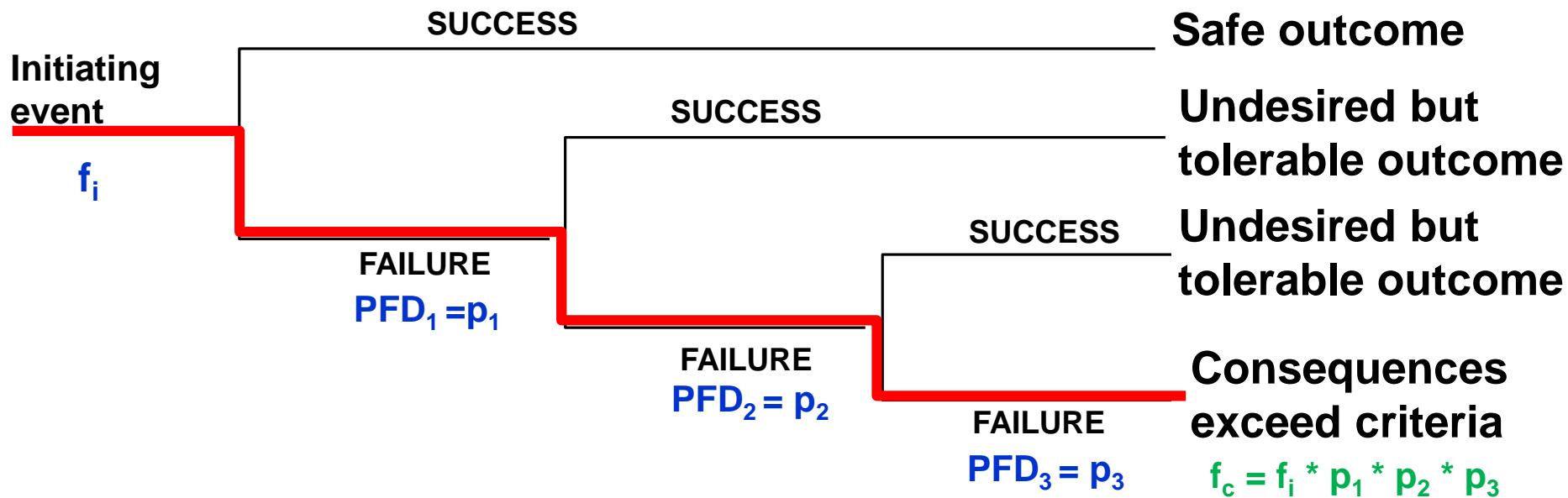
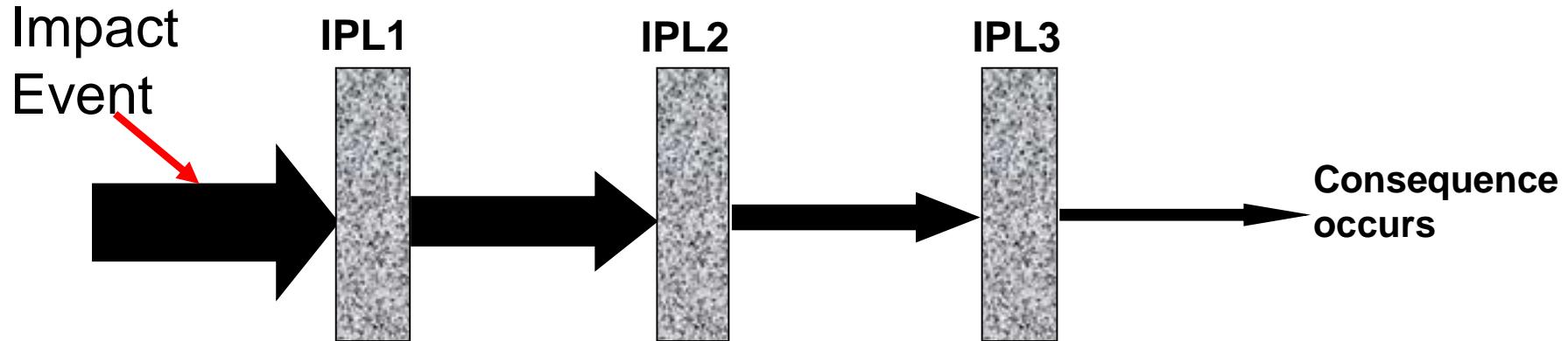
SIL

Safety Instrumented Functions (Interlocks)	See IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2001) for life cycle requirements and additional discussion		
SIL 1	Typically consists of: Single sensor (redundant for fault tolerance) Single logic processor (redundant for fault tolerance) Single final element (redundant for fault tolerance)	$\geq 1 \times 10^{-2} - < 1 \times 10^{-1}$	This book does not specify a specific SIL level. Continuing examples calculate a required PFD for a SIF
SIL 2	Typically consists of: “Multiple” sensors (for fault tolerance) “Multiple” channel logic processor (for fault tolerance) “Multiple” final elements (for fault tolerance)	$\geq 1 \times 10^{-3} - < 1 \times 10^{-2}$	
SIL 3	Typically consists of: Multiple sensors Multiple channel logic processor Multiple final elements	$\geq 1 \times 10^{-4} - < 1 \times 10^{-3}$	

Step 5. Estimating overall scenario or consequence frequency



Estimating the frequency of the consequence



Calculate consequence frequency

The frequency of a consequence from a specific scenario endpoint is:

$$f_i^C = f_i^I \times \prod_{j=1}^J PFD_{ij}$$

f_i^C consequence C frequency (mitigated) for an initiating event i

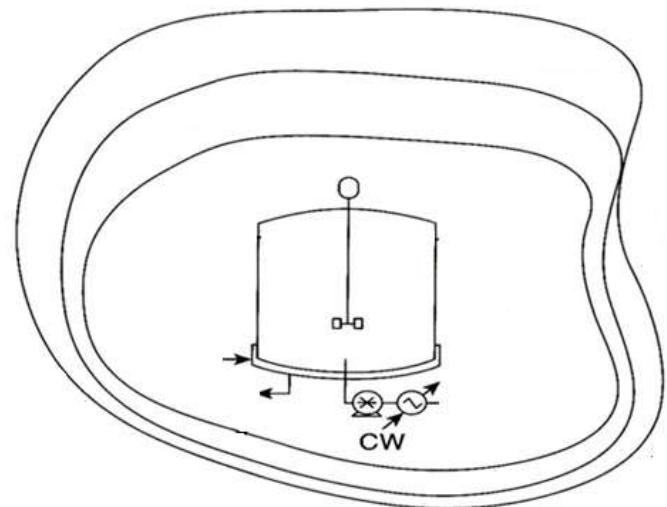
f_i^I frequency for the initiating event i

PFD_{ij} probability of failure that the jth IPL protects against C and the initiating event i .

Frequency of the consequence of several scenarios

$$f^C = \sum_{i=1}^I f_i^C$$

$$f^C = \sum_{i=1}^I (f_i^I \times \prod_{j=1}^J PFD_{ij})$$



Frequency of additional outcomes

$$f_i^{\text{fire}} = f_i^I \times \left(\prod_{j=1}^J \text{PFD}_{ij} \right) \times P^{\text{ignition}}$$

$$f_i^{\text{fire exposure}} = f_i^I \times \left(\prod_{j=1}^J \text{PFD}_{ij} \right) \times P^{\text{ignition}} \times P^{\text{person present}}$$

$$f_i^{\text{fire injury}} = f_i^I \times \left(\prod_{j=1}^J \text{PFD}_{ij} \right) \times P^{\text{ignition}} \times P^{\text{person present}} \times P^{\text{injury}}$$

11. (14 points) Failure of basic process control system (BPCS) loop may initiate overfilling of storage tanks. Often overflow of the storage tanks cause fire and production loss. If BPCS initiate an overflow of a storage tank which has three IPLs in place, what would be the frequency of consequence (overflow causing fire and production loss)? The IPLs are 1) Dike, 2) human action with 40 min response, and 3) underground drainage system. For frequency data use tables shown in next page.

Table 11-5 PFDs for Active IPLs and Human Actions

Active IPL or human action	Comments [assuming an adequate design basis, inspections, and maintenance procedures (active IPLs) and adequate documentation, training, and testing procedures (human action)]	PFDs from industry ¹	PFDs from CCPS ¹
Relief valve	Prevents system from exceeding specified over-pressure. Effectiveness of this device is sensitive to service and experience.	1×10^{-1} to 1×10^{-5}	1×10^{-2}
Rupture disc	Prevents system from exceeding specified over-pressure. Effectiveness of this device can be sensitive to service and experience.	1×10^{-1} to 1×10^{-5}	1×10^{-2}
Basic process control system (BPCS)	Can be credited as an IPL if not associated with the initiating event being considered. See IEC (1998, 2001). ^{2,3}	1×10^{-1} to 1×10^{-2}	1×10^{-1}
Safety instrumented functions (interlocks)	See IEC 61506 (IEC, 1998) and IEC 61511 (IEC, 2001) for life-cycle requirements and additional discussion. ^{2,3}		
Human action with 10 min response time	Simple well-documented action with clear and reliable indications that the action is required.	1×10^{-1} to 1×10^{-4}	1×10^{-1}
Human action with 40 min response time	Simple well-documented action with clear and reliable indications that the action is required.	1×10^{-5} to 1×10^{-2}	1×10^{-2}

¹CCPS, *Simplified Process Risk Assessment: Layer of Protection Analysis*, D. A. Crowl, ed. (New York: American Institute of Chemical Engineers, 2001) (in press).

²IEC (1998), IEC 61506, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, Parts 1-7*, Geneva: International Electrotechnical Commission.

³IEC (2001), IEC 61511, *Functional Safety Instrumented Systems for the Process Industry Sector; Parts 1-3*, (Draft in Process), Geneva: International Electrotechnical Commission.

Table 11-3 Typical Frequency Values Assigned to Initiating Events¹

Initiating event	Frequency range from literature (per yr)	Example of a value chosen by a company for use in LOPA (per yr)
Pressure vessel residual failure	10^{-5} to 10^{-7}	1×10^{-6}
Piping residual failure, 100 m, full breach	10^{-5} to 10^{-8}	1×10^{-5}
Atmospheric tank failure	10^{-3} to 10^{-5}	1×10^{-3}
Turbine/diesel engine overspeed with casing breach	10^{-3} to 10^{-4}	1×10^{-4}
Third-party intervention (external impact by backhoe, vehicle, etc.)	10^{-2} to 10^{-4}	1×10^{-2}
Lightning strike	10^{-3} to 10^{-4}	1×10^{-3}
Safety valve opens spuriously	10^{-2} to 10^{-4}	1×10^{-2}
Cooling water failure	1 to 10^{-2}	1×10^{-1}
Pump seal failure	10^{-1} to 10^{-2}	1×10^{-1}
Unloading/loading hose failure	1 to 10^{-2}	1×10^{-1}
BPCS instrument loop failure	1 to 10^{-2}	1×10^{-1}
Regulator failure	1 to 10^{-1}	1×10^{-1}
Small external fire (aggregate causes)	10^{-1} to 10^{-2}	1×10^{-1}
Large external fire (aggregate causes)	10^{-2} to 10^{-3}	1×10^{-2}
LOTO (lock-out tag-out) procedure failure (overall failure of a multiple element process)	10^{-3} to 10^{-4}	1×10^{-3}
Operator failure (to execute routine procedure; well trained, unstressed, not fatigued)	10^{-1} to 10^{-7}	1×10^{-2}
	opportunity	(opportunity)
	opportunity	(opportunity)

¹Individual companies choose their own values, consistent with the degree of conservatism or the company's risk tolerance criteria. Failure rates can also be greatly affected by preventive maintenance routines.

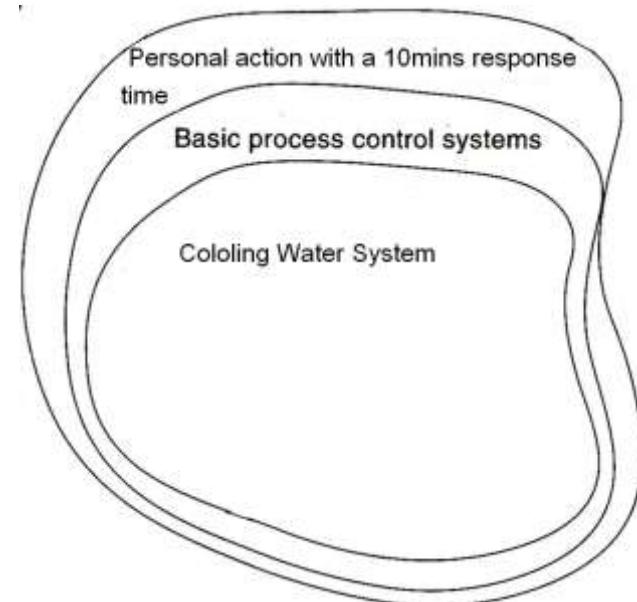
Table 11-4 PFDs for Passive IPLs

Passive IPLs	Comments (assuming an adequate design basis, inspections, and maintenance procedures)	PFDs from industry ¹	PFDs from CCPS ¹
Dike	Reduces the frequency of large consequences (widespread spill) of a tank overfill, rupture, spill, etc.	1×10^{-2} to 1×10^{-3}	1×10^{-2}
Underground drainage system	Reduces the frequency of large consequences (widespread spill) of a tank overfill, rupture, spill, etc.	1×10^{-2} to 1×10^{-3}	1×10^{-2}
Fireproofing	Reduces rate of heat input and provides additional time for depressurizing, fire fighting, etc.	1×10^{-2} to 1×10^{-3}	1×10^{-2}
Blast wall or bunker	Reduces the frequency of large consequences of an explosion by confining blast and by protecting equipment, buildings, etc.	1×10^{-2} to 1×10^{-3}	1×10^{-3}
Flame or detonation arrestors	If properly designed, installed, and maintained, can eliminate the potential for flashback through a piping system or into a vessel or tank	1×10^{-1} to 1×10^{-3}	1×10^{-2}

¹CCPS, *Simplified Process Risk Assessment: Layer of Protection Analysis*, D. A. Crowl, ed. (New York: American Institute of Chemical Engineers, 2001) (in press).

Example-1

- Determine the consequence frequency for a cooling water failure if the system is designed with two IPLs. The IPLs are a basic process control system (BPCS) and human interaction with 10-min response time.

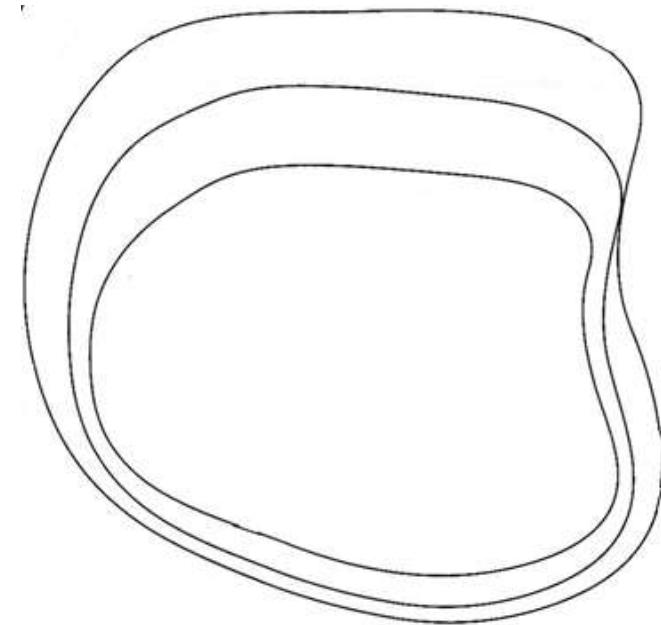


Example-2

For your plant there is a consequence frequency of 10^{-2} . As a safety engineer, determine the number of IPLs that should be added to reduce this consequence frequency to 10^{-6} . Assume every IPL have the same value of PFD with SIL 2.

$$f^c = 10^{-6}$$

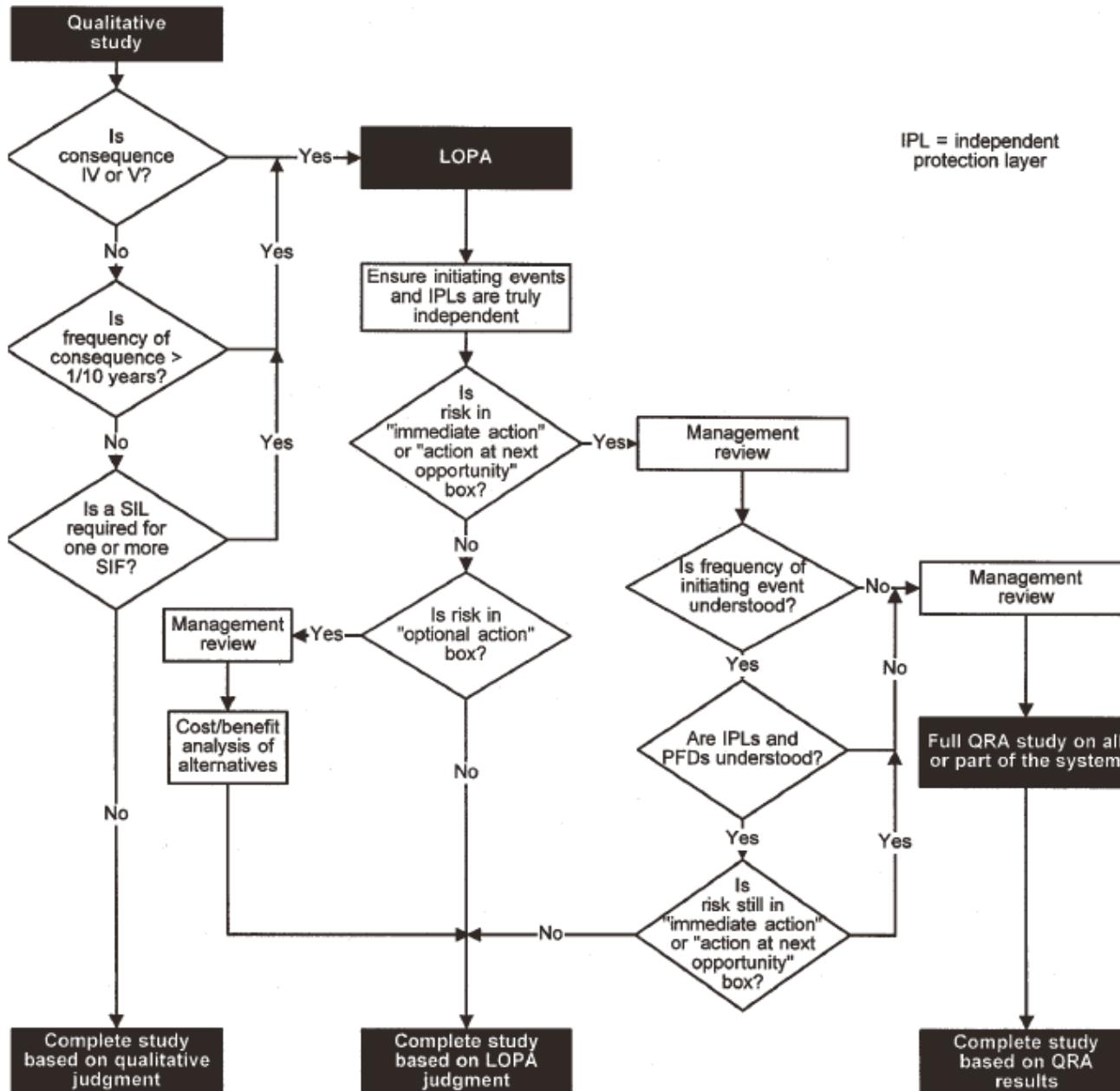
$$\begin{aligned}10^{-6} &= f^I \left(\prod_{j=1}^n PFD \right) \\&= f^I (PFD_1 \times PFD_2 \cdots PFD_n) \\&= f^I (10^{-2})^n \\&= 10^{-2} (10^{-2})^n \\n &= 2\end{aligned}$$



When is LOPA Used?

- **New projects during the design phase**
 - Process flow diagrams are complete
 - P&IDs are under development
- **Existing plants**
 - As part of hazard identification and analysis
- **Safety instrumented functions (SIF) assignment of existing or new plants**

Which risk analysis we should use?



IPL = independent protection layer

One type of risk matrix

Consequence Category \ Frequency of Consequence (per year)*	Category 1	Category 2	Category 3	Category 4	Category 5
10 ⁰	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at next opportunity (notify corporate management)	Immediate action (notify corporate management)	Immediate action (notify corporate management)
10 ⁻¹	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at next opportunity (notify corporate management)	Immediate action (notify corporate management)
10 ⁻²	No further action	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at next opportunity (notify corporate management)	Action at next opportunity (notify corporate management)
10 ⁻³	No further action	No further action	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at next opportunity (notify corporate management)
10 ⁻⁴	No further action	No further action	No further action	Optional (evaluate alternatives)	Optional (evaluate alternatives)
10 ⁻⁵	No further action	No further action	No further action	No further action	Optional (evaluate alternatives)
10 ⁻⁶	No further action	No further action	No further action	No further action	No further action
10 ⁻⁷	No further action	No further action	No further action	No further action	No further action

IPL and Safeguards

- All IPLs are listed as HAZOP safeguards, but not all HAZOP safeguards will meet the IPL criteria.

TABLE 6.1
Examples of Safeguards Not Usually Considered IPLs

Safeguards not Usually Considered IPLs	Comments
Training and Certification	These factors may be considered in assessing the PFD for operator action, but are not – of themselves – IPLs.
Procedures	These factors may be considered in assessing the PFD for operator action, but are not – of themselves – IPLs.
Normal Testing and Inspection	These activities are assumed to be in place for all hazard evaluations and form the basis for judgment to determine PFD. Normal testing and inspection affects the PFD of certain IPLs. Lengthening the testing and inspection intervals may increase the PFD of an IPL.
Maintenance	This activity is assumed to be in place for all hazard evaluations and forms the basis for judgment to determine PFD. Maintenance affects the PFD of certain IPLs.
Communications	It is a basic assumption that adequate communications exist in a facility. Poor communications affects the PFD of certain IPLs.
Signs	Signs by themselves are not IPLs. Signs may be unclear, obscured, ignored, etc. Signs may affect the PFD of certain IPLs.
Fire Protection	Active fire protection is often not considered as an IPL as it is post event for most scenarios and its availability and effectiveness may be affected by the fire/explosion which it is intended to contain. However, if a company can demonstrate that it meets the requirements of an IPL for a given scenario it may be used (e.g., if an activating system such as plastic piping or frangible switches are used). <i>Note:</i> Fire protection is a mitigation IPL as it attempts to prevent a larger consequence subsequent to an event that has already occurred. Fireproof insulation can be used as an IPL for some scenarios provided that it meets the requirements of API and corporate standards.
Requirement that Information is Available and Understood	This is a basic requirement.

Safeguards

- Training and certification
- Procedure
- Normal testing and inspection
- Maintenance
- Communications
- Signs

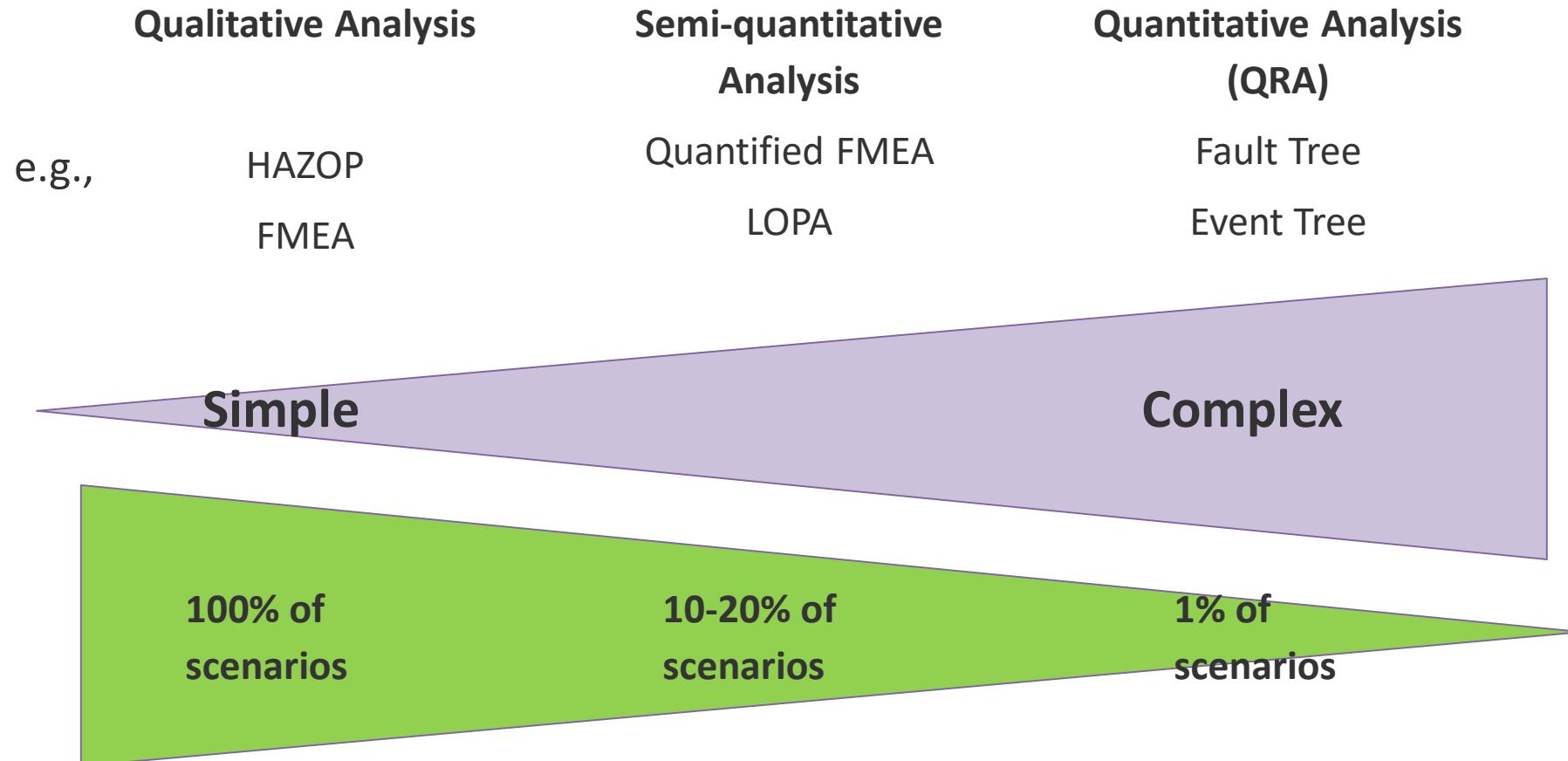
These are **not** IPL

Benefits of LOPA

- Requires less time than QRA (Quantitative Risk Analysis)
- Provides a means of comparing risk from unit to unit or plant to plant

LOPA Limitations

- LOPA is not a tool for identifying hazards
- LOPA may be excessive for simple or low risk decisions
- LOPA may be overly simplistic for very complex systems



Building BN Node Probability Tables

Unit 13

Spring 2022

References

- Fenton, N. and M. Neil, Risk Assessment and Decision Analysis with Bayesian Networks, CRC Press, 2nd ed. 2019, Chapters 7,8 (F&N, 2019)
AgenaRisk Tutorial 2, Partitioned Nodes
- Naderpour, J. Lu, G. Zhang, An abnormal situation modeling method to assist operators in safety-critical systems, Reliability Engineering and System Safety, 133 (2015), 33-47
- Bobbio, A., et al, “Improving the analysis of dependable systems by mapping fault trees into Bayesian networks,” Rel. Eng. and System Safety, 71 (2001) 249–260 (Bobbio, 2001)
- Kjaerulff, U.B. and A.K. Madsen, *Bayesian Networks and Influence Diagrams*, Springer, 2008
- Jensen, F.V. and T.D. Nielsen, *Bayesian Networks and Decision Graphs*, Springer, 2007
- Nicholson, A., *Bayesian Networks and Causal Modeling*, School of Computer Science and Software Engineering, Monash University (Nicholson, Causal Modeling)
- Korb, K.B. and A.E. Nicholson, *Bayesian Artificial Intelligence*, 2nd ed, Taylor & Francis, 2011 (Korb, 2011)
- Michigan Chemical Process Dynamics and Controls Open Text Book (MCPDC)
- Pearl, J., *Probabilistic Reasoning in Intelligent Systems*, Morgan Kaufmann, 1988 (Pearl, 1988)
- Pearl, Judea, Causality: Models, Reasoning, and Inference, 2nd ed, Cambridge, 2009 (Pearl, 2009)
- Neapolitan, R.E., *Learning Bayesian Networks*, Prentice Hall, 2004 (Neapolitan, 2004)
- Neapolitan, R.E., *Probabilistic Methods for Bioinformatics*, Morgan Kaufmann, 2009

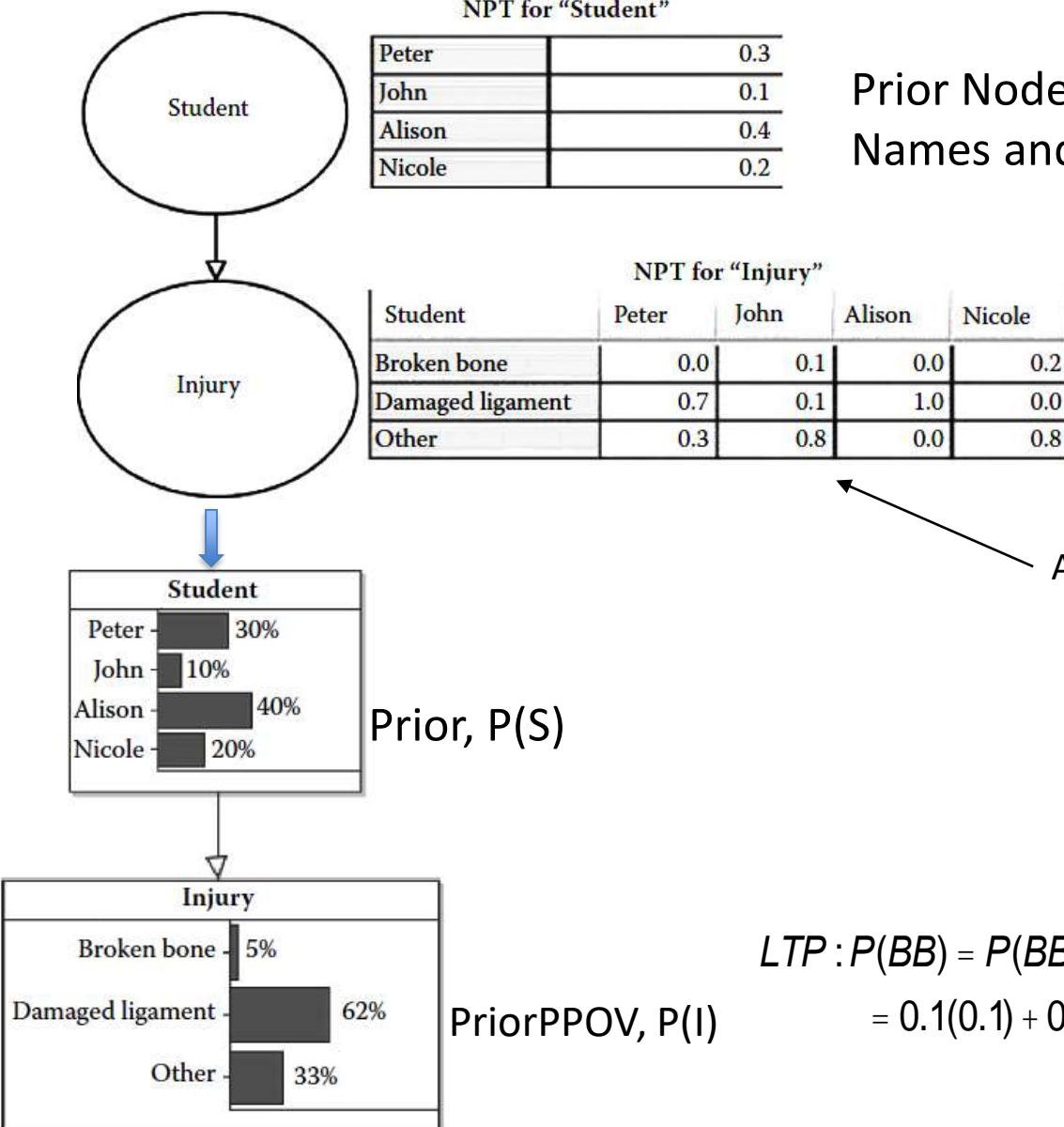
EVERYBODY WHO WENT TO
THE MOON HAS EATEN
CHICKEN!

GOOD GRIEF.
CHICKEN MAKES
YOU GO TO
THE MOON!



Partitioned Nodes with Labeled States

RDBN, p. 249



Prior Node with Student states:
Names and probabilities of involvement

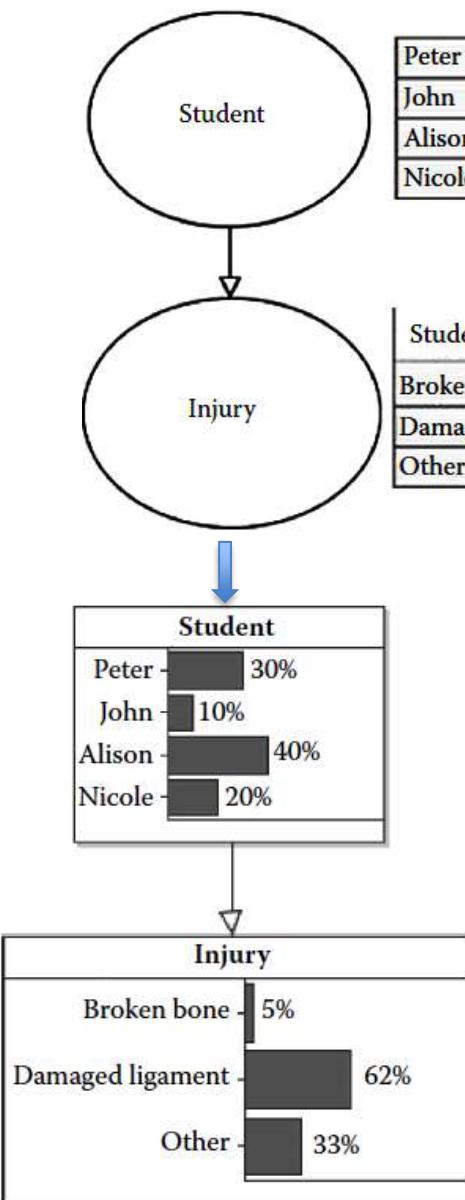
Likelihood of Injury states:
CPT, $P(\text{Injury} | \text{Student})$

$$\begin{aligned}
 LTP : P(BB) &= P(BB | John)P(John) + P(BB | Nicole)P(Nicole) \\
 &= 0.1(0.1) + 0.2(0.2) = 0.05
 \end{aligned}$$

PriorPPOV = Prior Predictive Probability of the Observed Variable, which here is Injury

Partitioned Nodes with Labeled States

RDBN, p. 249



NPT for "Student"

Peter	0.3
John	0.1
Alison	0.4
Nicole	0.2

Prior Node with Student states:
Names and probabilities of involvement

NPT for "Injury"

Student	Peter	John	Alison	Nicole
Broken bone	0.0	0.1	0.0	0.2
Damaged ligament	0.7	0.1	1.0	0.0
Other	0.3	0.8	0.0	0.8

Likelihood of Injury states:
CPT, $P(\text{Injury} | \text{Student})$

Posterior, $P(S | DL)$

Student
Peter - 33.871%
John - 1.613%
Alison - 64.516%
Nicole -

$$P(P|DL) = \frac{P(DL|P)P(P)}{P(DL)}$$

$$= \frac{0.7 \times 0.3}{0.62} = 0.33871$$

Most likely student with
Damaged ligament

**See model tutorial
in AgenaRisk:
9.3 Student injury

NPT for Labeled Nodes

For labeled nodes, if the Pr values are zeros and ones (deterministic), then a comparative expression can populate the NPT, which is easier than manual entry.

Box 9.2 Using Comparative Expressions RDBN, p. 249-252

In some circumstance it may be sufficient to use a simple comparative expression to define a full NPT. Let us return to the BN in Example 8.1. Let us suppose that we have the following prior information about injuries:

- The only possible injury Alison and Nicole can suffer is a damaged ligament.
- The only possible injury Peter can suffer is a broken bone or Other
- The only possible injury John can suffer is “other.”

In that case all the information we need for the node *Injury* is captured using the following logical expression:
then

```
if (student == "Alison" || student == "Nicole", "Damaged ligament"
if (student == "Peter", "Broken bone", "Other"))
    then
        otherwise
```

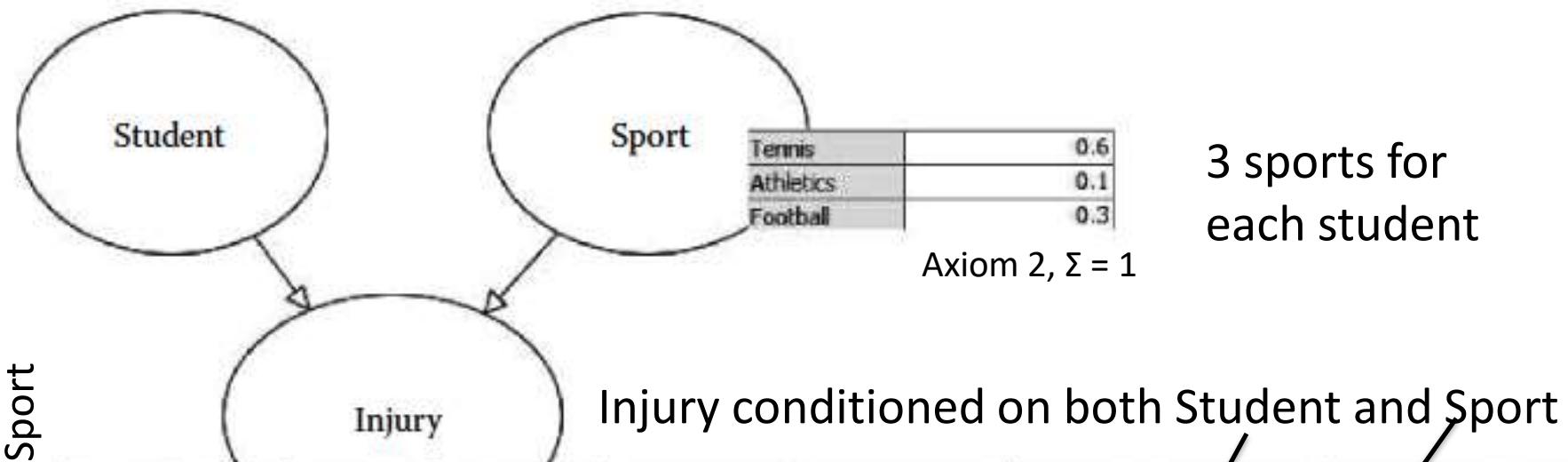
== means ‘equal’

|| means ‘OR’

Expression	RDBN, p. 252	Meaning
A == B		1. A is equal to B. For example, the expression <code>student == "Alison"</code> means student is Alison
A B OR		2. Either A or B is true. For example, the expression <code>student == "Alison" student == "Nicole"</code> means the student is either Alison or Nicole.
A && B		3. Both A and B are true. For example, the expression <code>student == "Alison" && injury == "Damaged ligament"</code> means the student is Alison and <i>injury</i> is damaged ligament.
if (<condition>, "option1", "option2")		4. If <condition> is true then "option1" must be true, otherwise "option2" must be true. This is called a conditional expression. So, for example, <code>if (student == "Alison", "Damaged ligament", "Broken bone")</code> means that if the student is Alison then "damaged ligament" is true, otherwise "broken bone" is true.

Extend BN Partitioning to Include Impact of Sport

Add **Sport** as an additional parent node RDBN, p. 253



Student	Peter			John			Alison			Nicole		
Sport	Tennis	Athletics	Football	Tennis	Athletics	Football	Tennis	Athletics	Football	Tennis	Athletics	Football
Broken bone	0.0	0.0	0.0	0.1	0.33333334	0.33333334	0.0	0.0	0.0	0.2	0.3	0.1
Damaged ligament	0.7	0.6	0.8	0.1	0.33333334	0.33333334	1.0	1.0	1.0	0.0	0.0	0.0
Other	0.3	0.4	0.2	0.8	0.33333334	0.33333334	0.0	0.0	0.0	0.8	0.7	0.9

$$\text{Values in NPT} = (4 \text{ students}) \cdot (3 \text{ sports}) \cdot 3 \text{ (injuries)} = 36$$

NPT from a Partitioned Expression

Box 9.3 Using Partitioned Expressions RDBN, p. 221

If a node has more than one parent, as in Example 8.2, you can use a partitioned expression. Suppose, for example, that we have the following information:

- When Peter's sport is football his injury is a broken bone. For any other sport the injury is "other."
- When John's sport is athletics he can only suffer a damaged ligament. When football he can only suffer a broken bone.
- Alison and Nicole can only suffer a damaged ligament irrespective of what sport played.

Then what we can do is write expressions for injury that are conditioned on the *student*. This is what is meant by an NPT being defined by a partitioned expression. In AgenaRisk if you specify that an NPT for a node is to be a partitioned expression, then you can select what parent node(s) to condition on, as shown in Figure 8.5. The figure shows the blank table. We need to complete each entry with an expression. For example the entry for Peter might be:

```
if (sport == "Football", "Broken bone", "Other")  
    then  
    otherwise
```

Node Probability Table

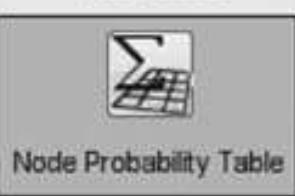
RDBN, Fig 8.5, p. 221

NPT Editing Mode

Partitioned Expression

Partitioned Expression

Select the required parents from the list on the left and add them to the list on the right. The right will contain the parents involved in the partitioned table. The order of the parents determines the configuration of states in the table below.



Node Probability Table



Node Constants



Notes



Appearance

Reset fields to default values▼ Set current field values as new defaults

Cancel

Apply

Add >
Add all >>
<< Remove all
< Remove

Student

Student	Peter	John	Alison	Nicole
Expressions				

Enter a formula for each partition by double-clicking the cell.

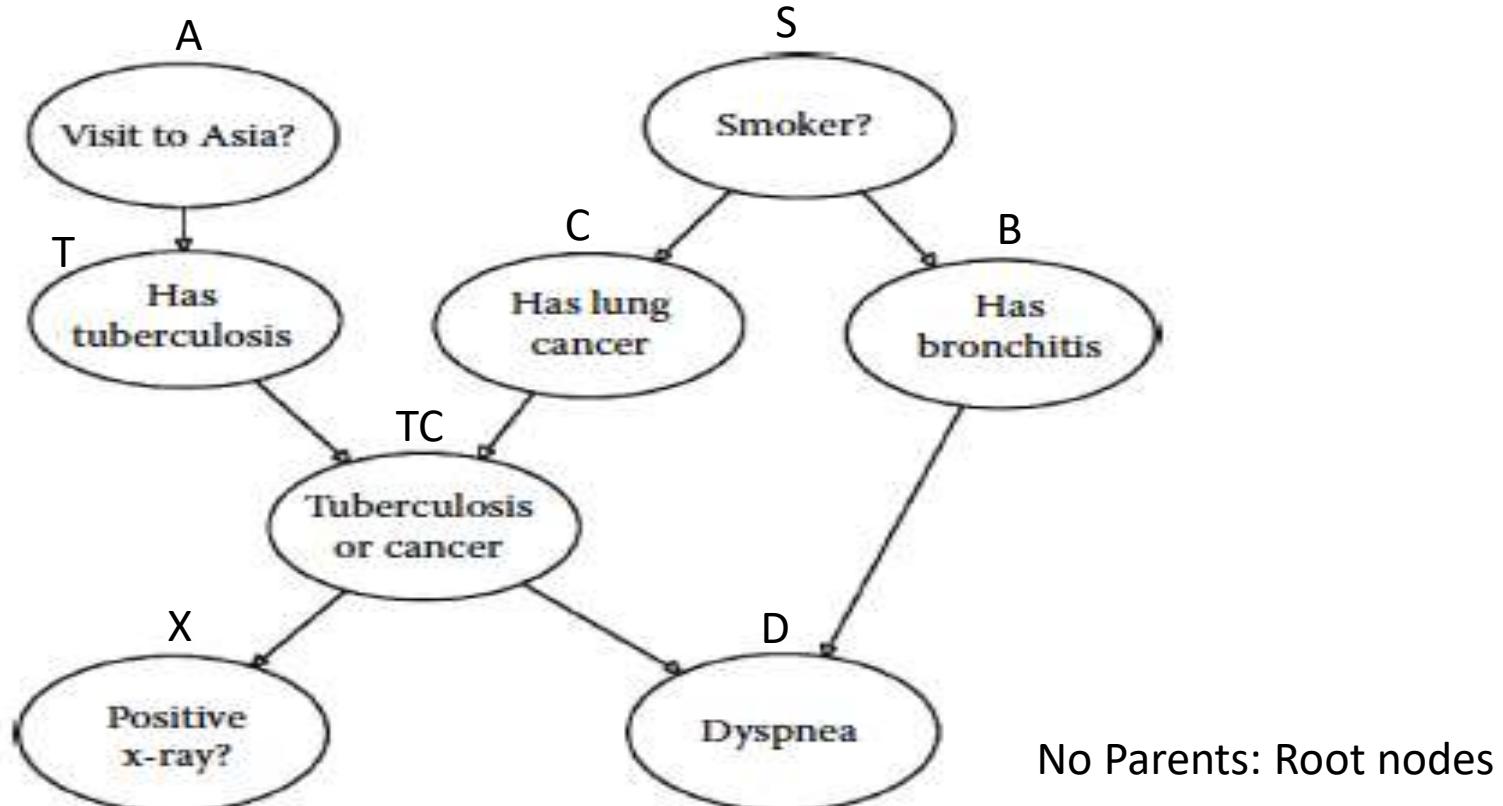
Injury conditioned on the Student with a formula for each

Forensic Case Study: The Asia Model

- BN in which all nodes are Boolean (True/False)
- This model was designed to support medical decisions in a chest clinic for diagnosing the likelihood of 3 conditions: Tuberculosis, T, Lung Cancer, C, and Bronchitis, B
- Diagnosis based on two causal factors or, observed evidence: Smoking, S, and recent visit to Asia, A
- Additional evidence (effect or consequence) can be
 - Patient with shortness of breath (Dyspnea, D)?
 - Positive x-ray test result, X?
- This BN is an excellent example of the power and flexibility of BNs for decision support compared to other decision support systems.

Asia Model

Primary Cause/Effect BN relationships that show simplification through conditional independences, e.g., $P(X|D,B,TC,T,A,C,S) = P(X|TC)$



System pdf:

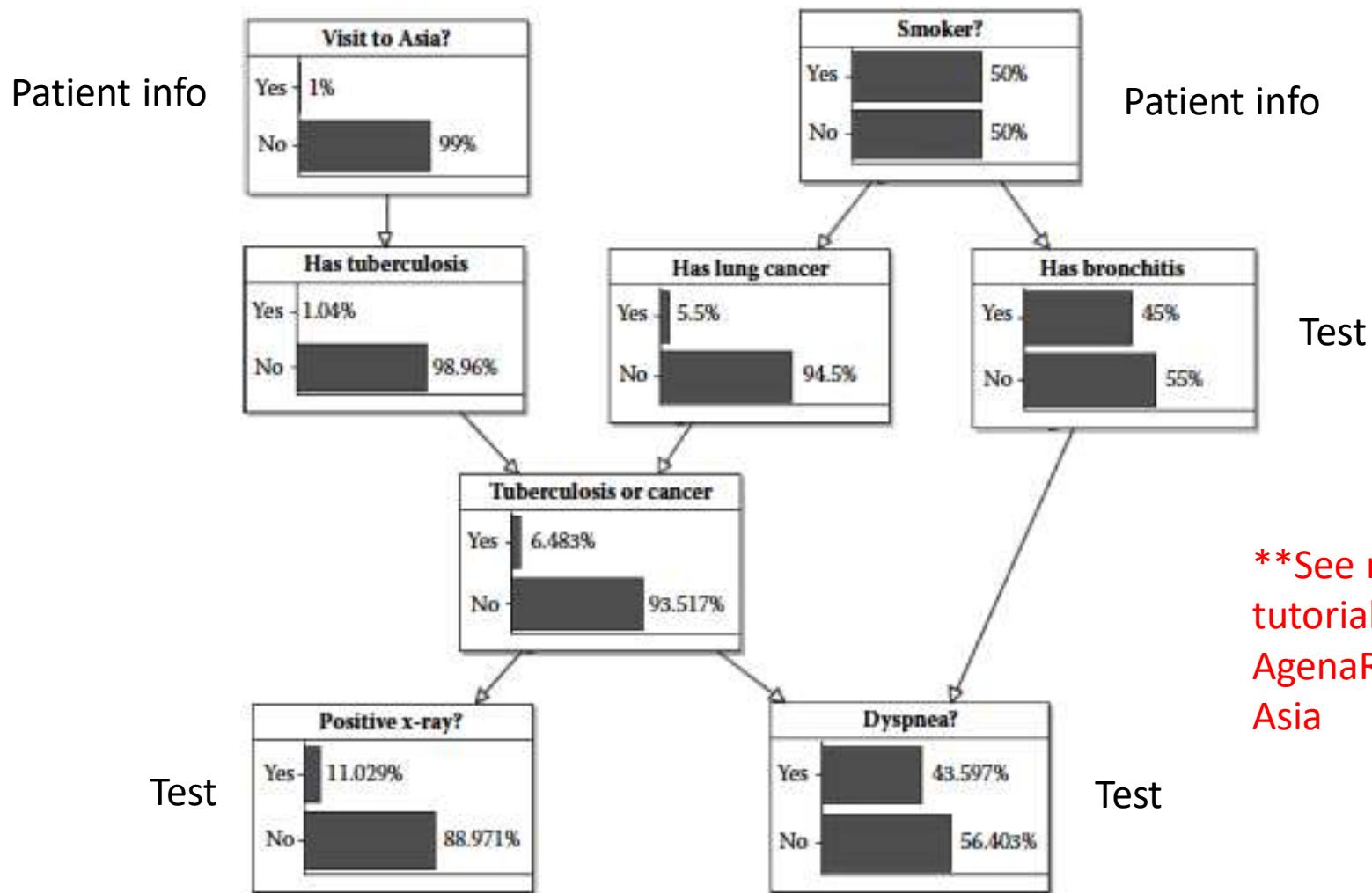
Chain Rule, Simplify

$$P(X,D,B,TC,T,A,C,S) = P(X|TC)P(D|B,TC)P(TC|T,C)P(T|A)P(C|S)P(B|S)P(A)P(S)$$

Each node has no more than two parents, and Boolean nodes have only 2 states, so NPTs contain at most 4 cells.

Node	NPT			Justification																			
Smoker	<table border="1"> <tr> <td>True</td><td>0.5</td><td></td></tr> <tr> <td>False</td><td>0.5</td><td></td></tr> </table>			True	0.5		False	0.5		50% of previous visitors to clinic were smokers.													
True	0.5																						
False	0.5																						
Visit to Asia	<table border="1"> <tr> <td>True</td><td>0.01</td><td></td></tr> <tr> <td>False</td><td>0.99</td><td></td></tr> </table>			True	0.01		False	0.99		1% of previous visitors to clinic had recently visited Asia.													
True	0.01																						
False	0.99																						
Tuberculosis (TB)	<table border="1"> <thead> <tr> <th>Visit to Asia</th><th>True</th><th>False</th></tr> </thead> <tbody> <tr> <td>True</td><td>0.05</td><td>0.01</td></tr> <tr> <td>False</td><td>0.95</td><td>0.99</td></tr> </tbody> </table>			Visit to Asia	True	False	True	0.05	0.01	False	0.95	0.99	Tuberculosis is 5 times more likely given Asian visit but generally very unlikely.										
Visit to Asia	True	False																					
True	0.05	0.01																					
False	0.95	0.99																					
Lung cancer	<table border="1"> <thead> <tr> <th>Smoker</th><th>True</th><th>False</th></tr> </thead> <tbody> <tr> <td>True</td><td>0.1</td><td>0.01</td></tr> <tr> <td>False</td><td>0.9</td><td>0.99</td></tr> </tbody> </table>			Smoker	True	False	True	0.1	0.01	False	0.9	0.99	Figures based on previously diagnosed patients. So, for example, only 1% of nonsmokers were diagnosed with cancer.										
Smoker	True	False																					
True	0.1	0.01																					
False	0.9	0.99																					
Bronchitis	<table border="1"> <thead> <tr> <th>Smoker</th><th>True</th><th>False</th></tr> </thead> <tbody> <tr> <td>True</td><td>0.6</td><td>0.3</td></tr> <tr> <td>False</td><td>0.4</td><td>0.7</td></tr> </tbody> </table>			Smoker	True	False	True	0.6	0.3	False	0.4	0.7	Figures based on previously diagnosed patients. So, for example, only 60% of smokers were diagnosed with bronchitis.										
Smoker	True	False																					
True	0.6	0.3																					
False	0.4	0.7																					
Tuberculosis or cancer	<table border="1"> <thead> <tr> <th>Tuberculosis</th><th colspan="2">True</th><th>False</th></tr> <tr> <th>Cancer</th><th>True</th><th>False</th><th>True</th><th>False</th></tr> </thead> <tbody> <tr> <td>True</td><td>1</td><td>1</td><td>1</td><td>0</td></tr> <tr> <td>False</td><td>0</td><td>0</td><td>0</td><td>1</td></tr> </tbody> </table>			Tuberculosis	True		False	Cancer	True	False	True	False	True	1	1	1	0	False	0	0	0	1	This is simply the Boolean OR function. We use a conjoined node here of both medical conditions because the x-ray test cannot differentiate between them. It detects a shadow on the lung but cannot differentiate the cause.
Tuberculosis	True		False																				
Cancer	True	False	True	False																			
True	1	1	1	0																			
False	0	0	0	1																			
Positive x-ray	<table border="1"> <thead> <tr> <th>TB or Cancer</th><th>True</th><th>False</th></tr> </thead> <tbody> <tr> <td>True</td><td>0.98</td><td>0.05</td></tr> <tr> <td>False</td><td>0.02</td><td>0.95</td></tr> </tbody> </table> <p style="color: red; margin-left: 10px;">← False Pos</p> <p style="color: red; margin-left: 10px;">← False Neg</p>			TB or Cancer	True	False	True	0.98	0.05	False	0.02	0.95	Accuracy figures based on previous patients. 5% of patients without either disease wrongly got a positive x-ray and 2% received a false-negative result.										
TB or Cancer	True	False																					
True	0.98	0.05																					
False	0.02	0.95																					
Dyspnea	<table border="1"> <thead> <tr> <th>Bronchitis</th><th colspan="2">True</th><th>False</th></tr> <tr> <th>Tuberculosis</th><th>True</th><th>False</th><th>True</th><th>False</th></tr> </thead> <tbody> <tr> <td>True</td><td>0.9</td><td>0.8</td><td>0.7</td><td>0.1</td></tr> <tr> <td>False</td><td>0.1</td><td>0.2</td><td>0.3</td><td>0.9</td></tr> </tbody> </table>			Bronchitis	True		False	Tuberculosis	True	False	True	False	True	0.9	0.8	0.7	0.1	False	0.1	0.2	0.3	0.9	Figures based on previous patients.
Bronchitis	True		False																				
Tuberculosis	True	False	True	False																			
True	0.9	0.8	0.7	0.1																			
False	0.1	0.2	0.3	0.9																			

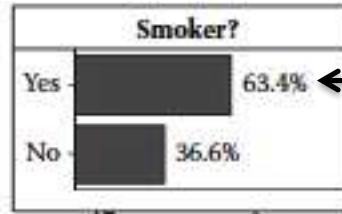
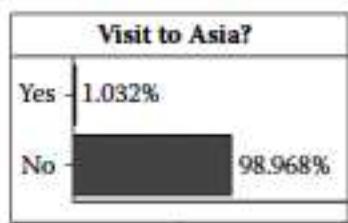
Running the Asia Model: Follow the Story



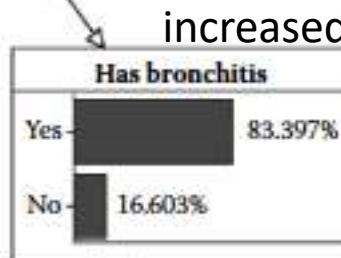
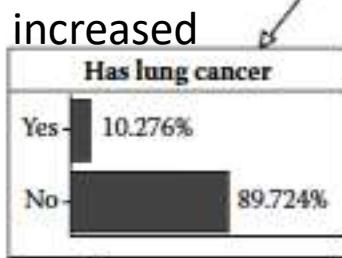
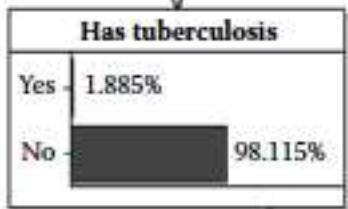
The model in its initial state, given the previous data, represents the state of **medical uncertainty** prior to a patient's arrival at the clinic.

Observation 1: Patient has Dyspnea

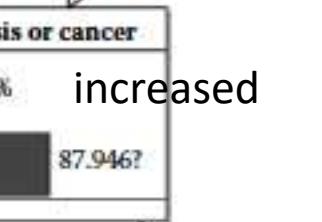
unchanged



Based on evidence of Dyspnea, Smoker Pr increases to 0.63 from 0.5 prior

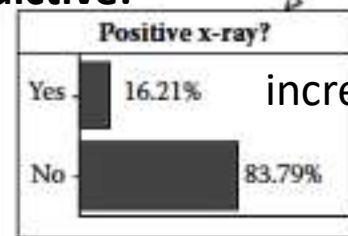


← MLE



Given evidence of Dyspnea, the model recalculates all probabilities to show the likelihood of all diseases compared to the prior values. The most likely explanation, MLE, is Bronchitis

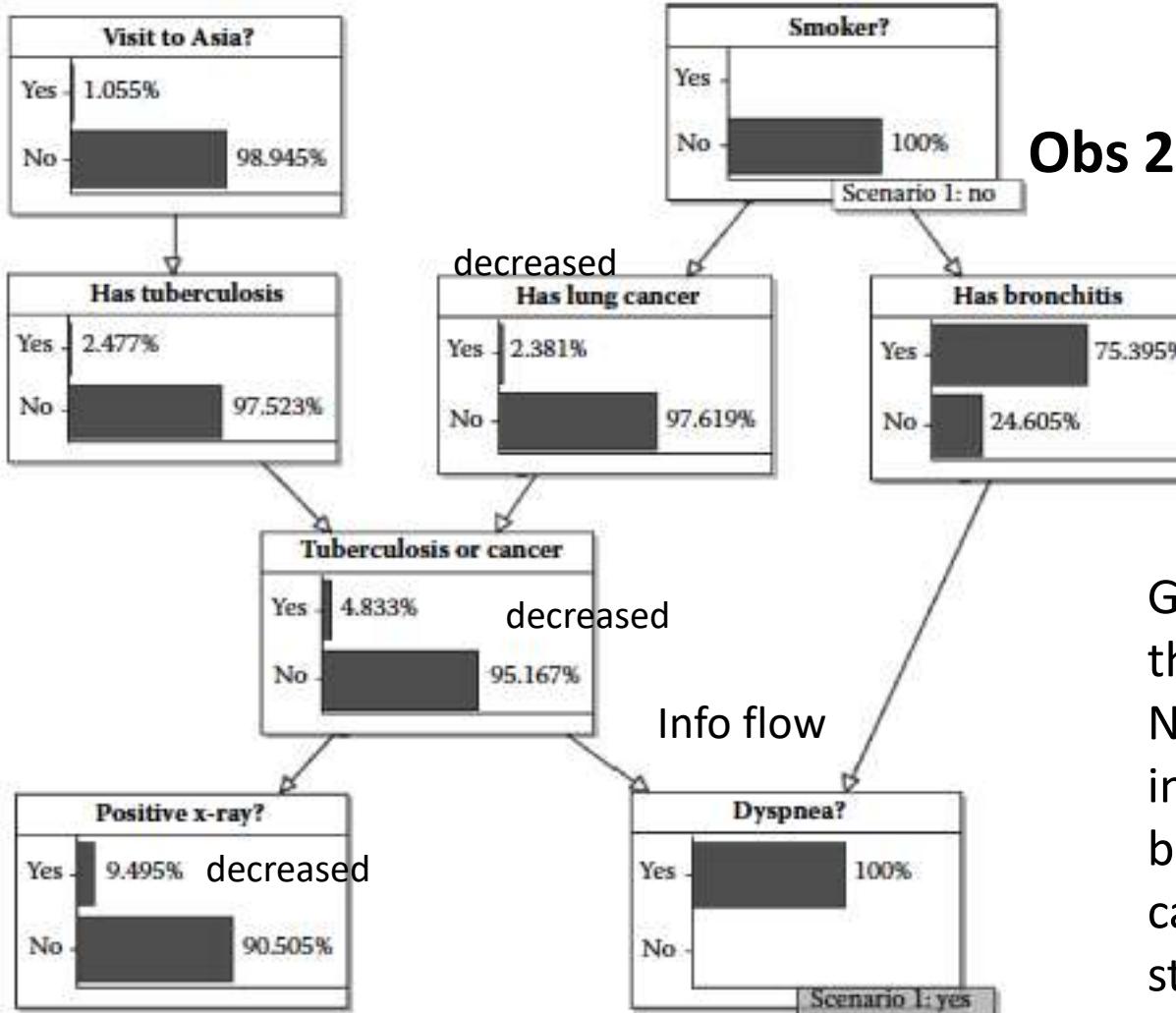
Predictive:



Obs 1: Dyspnea set to true

What evidence is most needed to reduce uncertainty of TB?

Observation 2: Patient does not smoke



Obs 2: Nonsmoker

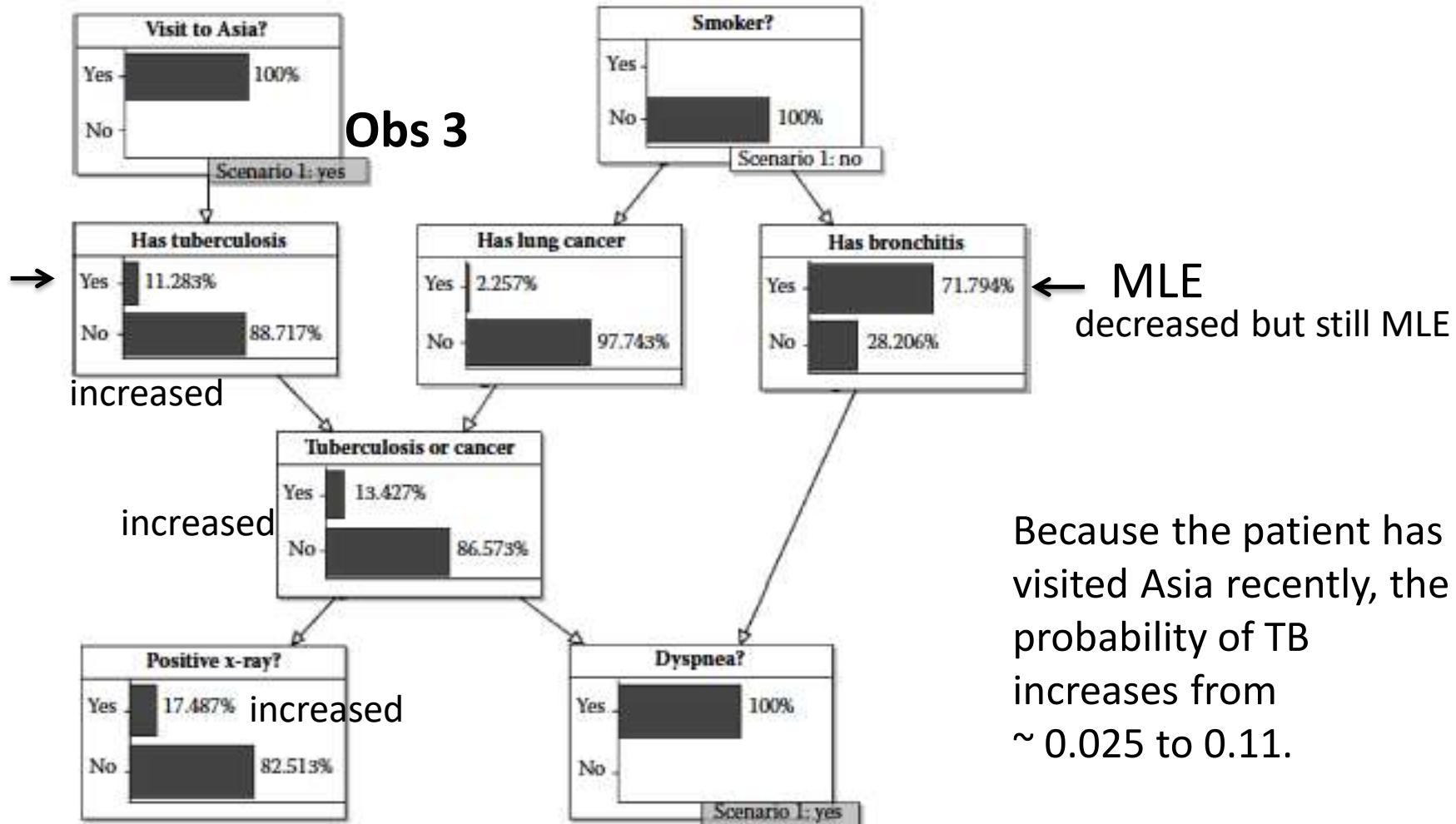
← MLE

Given evidence that the patient is a Nonsmoker, our belief in all diseases change, but Bronchitis as a cause of Dyspnea is still the most likely disease.

Set 'Smoker?' to 'no' based on evidence.

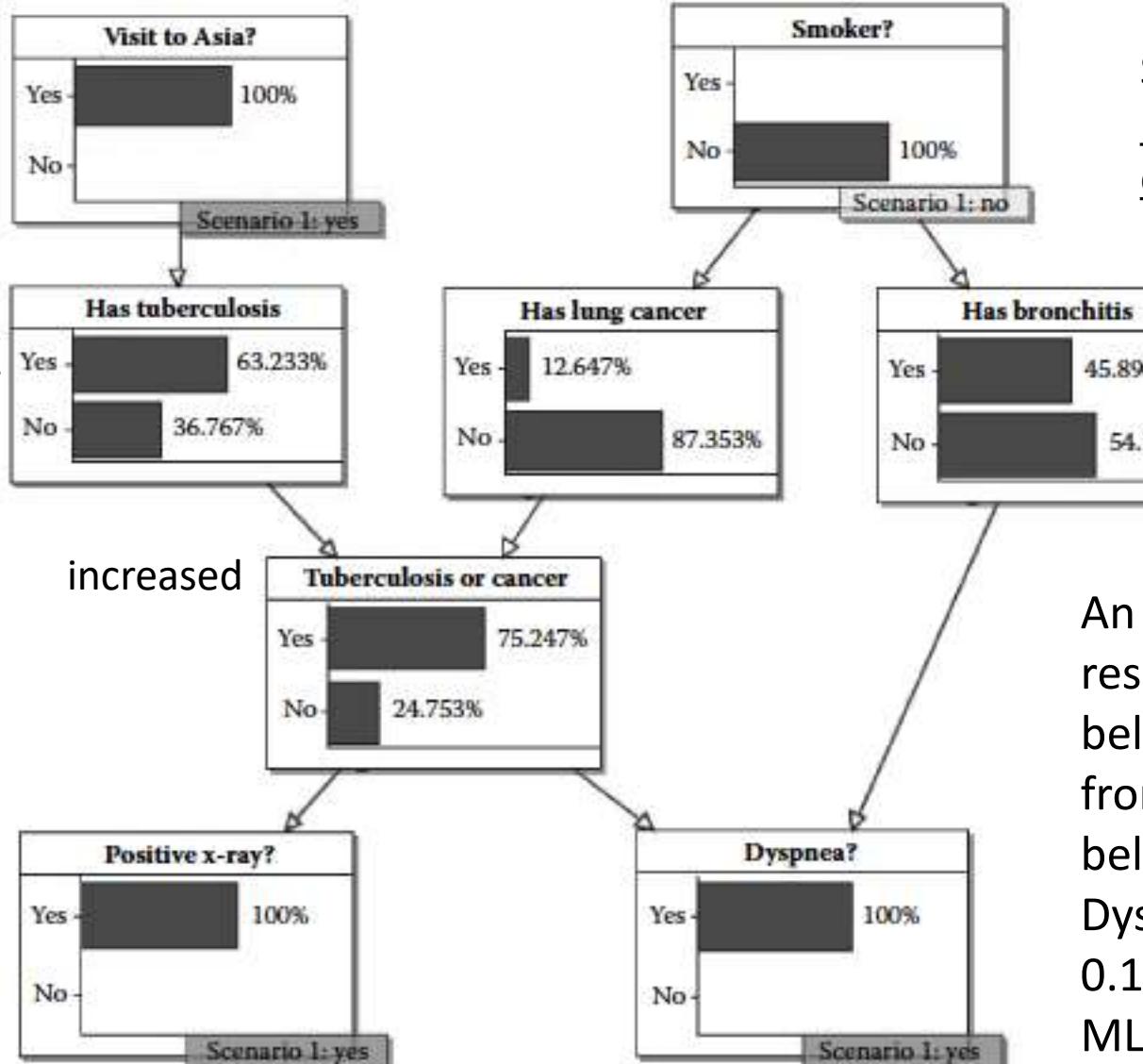
Observation 3: Did patient visit Asia?

Question to Patient: Visit to Asia?



'Visit to Asia?' set to 'yes'

Observation 4: Patient's X-ray results shows positive results



Shows the power of BN to predict the most plausible causes given the evidence

→ drops

An X-ray is positive. As a result of this evidence, our belief in Bronchitis falls from 0.72 to 0.46, and our belief in TB as a cause of Dyspnea, rises from a Pr of 0.11 to 0.75, which is the MLE based on the current evidence.

Obs 4: Positive X-ray

Summary of the Asia Model: Medical Uncertainty Modeling & Prediction

- From the initial evidence of Dyspnea and a Nonsmoker, the model diagnosed Bronchitis as the MLE.
- The new evidence of a recent visit to Asia followed by a positive X-ray with BN update explained the Bronchitis diagnosis showing the MLE is TB and a cause of Dyspnea.
- Updating the medical uncertainty based on observed data to lower the uncertainty and evaluate the state of knowledge is the work of Bayesian networks.
- The prior hypothesis was updated by observed data or evidence to a posterior hypothesis with lower uncertainty of diagnosis, because of the visit to Asia, and the positive X-ray that lowered uncertainty to result in lower credibility of Bronchitis compared with a more evidenced based belief in TB as the MLE cause of the observed Dyspnea.

**WE'VE FOUND THE ROOT CAUSE,
CHIEF**



**THE CREW CHIEF WAS OVERDUE
FOR BLOCK TRAINING BY 2 DAYS**

OR Gate for Boolean Nodes

NPT for Node *Tuberculosis or Cancer*

Tuberculosis		True		False	
		True	False	True	False
Tuberculosis or cancer	True	1	1	1	0
	False	0	0	0	1

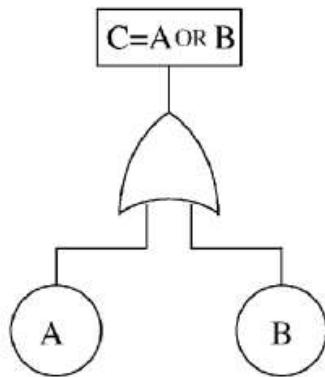
- All information needed in this case for Tuberculosis or Cancer is captured by the logical OR Boolean operator:

```
if (A == "True" || B == "True", "True", "False")
```

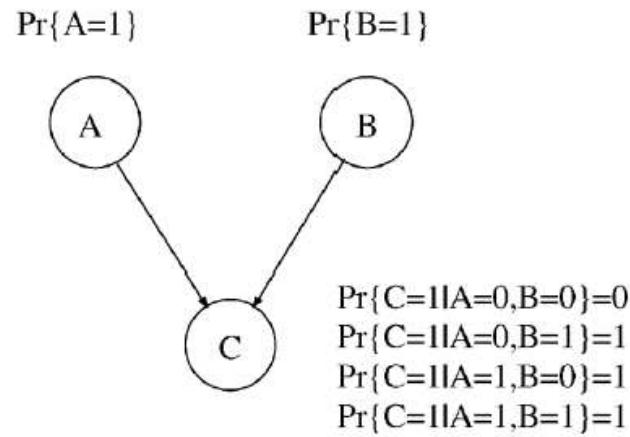
```
if (Tuberculosis == "True" || Cancer == "True",  
    "True", "False")
```

- This OR operator is labor saving, especially when a node has numerous parents.

The OR gate



FAULT - TREE: OR Gate



BAYESIAN NETWORK: OR Node

OR Gate Example: Computer System

- A computer system consists of a CPU, motherboard, hard disk, graphics card, PCI card, screen monitor, keyboard.
- Each of these components is a single point failure (cut set of Rank 1) to cause system failure, so OR for each!
- **Q 1:** What is the Pr that the Computer System will fail during a given session?
- **Q 2:** If the Computer System is observed to fail and we can test and observe that the screen, keyboard, and hard disk are working, what is the most likely failure or MLE?
- Use the following expression to calculate the System NPT:

```
if (CPU == "True" || Motherboard== "True" || hard_disk  
== "True" || graphics_card == "True" || PCI == "True" ||  
Screen == "True" || Keyboard == "True", "True", "False")
```

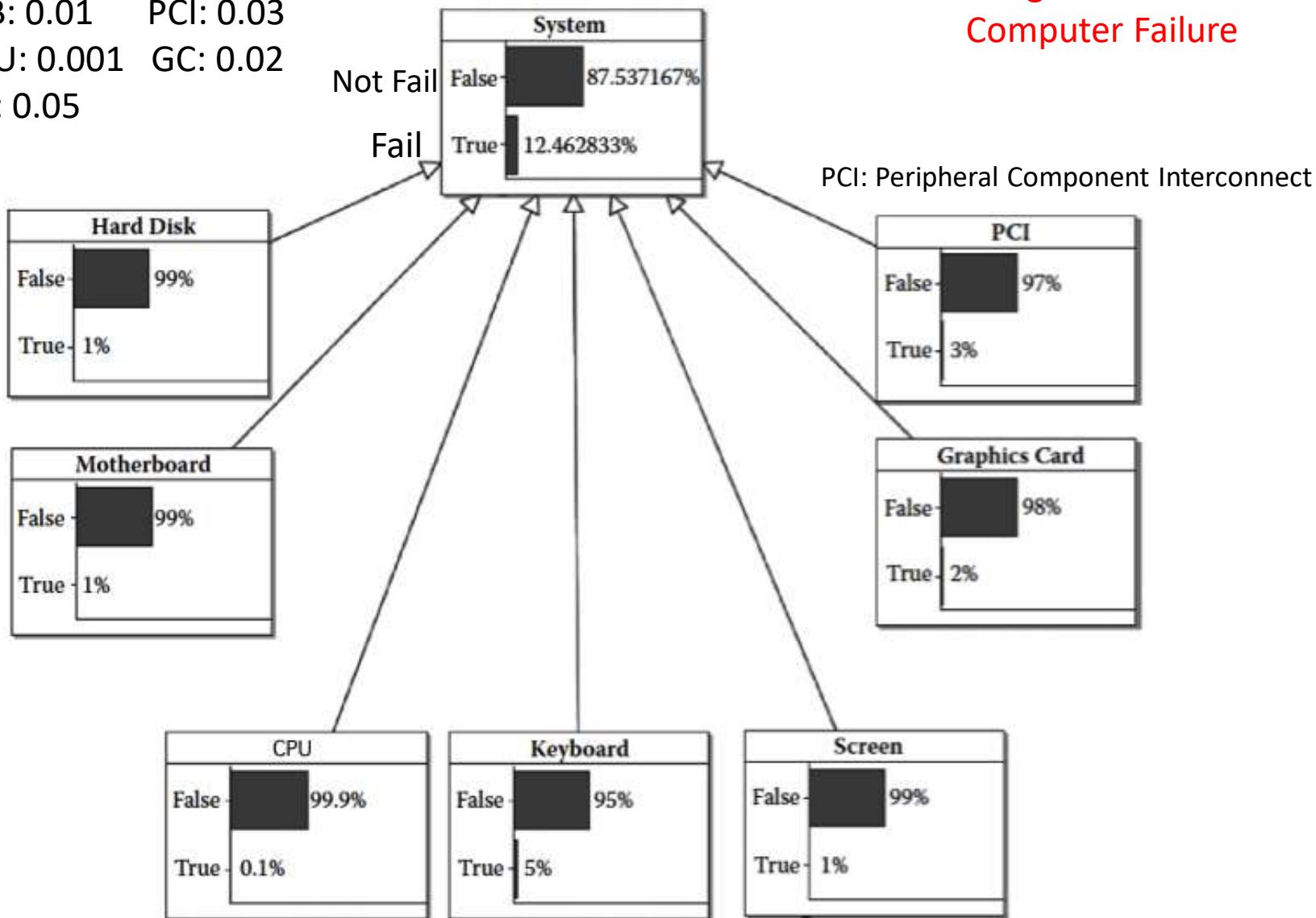
Each component represents a single point failure in a series system.

**See model tutorial
in AgenaRisk: 9.4.2
Computer Failure

Prior
 $P(\text{fail})$

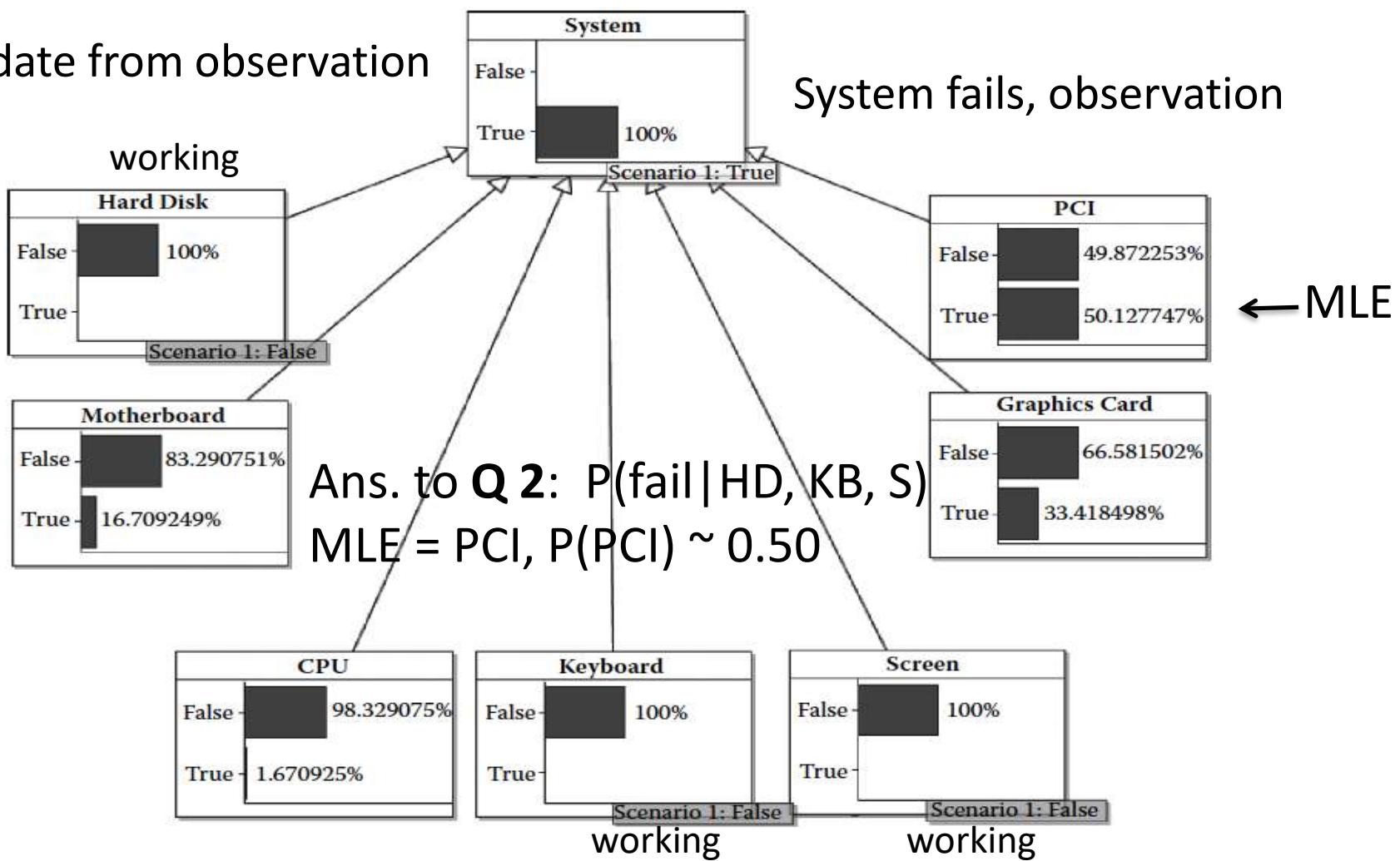
HD: 0.01	SC: 0.01
MB: 0.01	PCI: 0.03
CPU: 0.001	GC: 0.02
KB: 0.05	

Prior State of BN



Answer to Q1: $P(\text{fail}) \sim 0.125$ during a given operation session

Update from observation



Note that we have assumed that all components are considered conditionally independent. If we had data for dependence of CPU and HD (hard drive), such that CPU failure is more likely if HD fails, we will place an arc from CPU to HD and condition the CPU on both the HD and the System.

AND- Gate for Boolean Nodes

- For A AND B, the AND operator is implemented by:

```
if (A == "True" && B == "True", "True", "False")  
    AND  
    otherwise
```

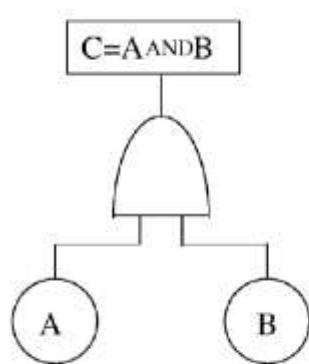
- Example:

The expression for a System with 4 Power supplies is:

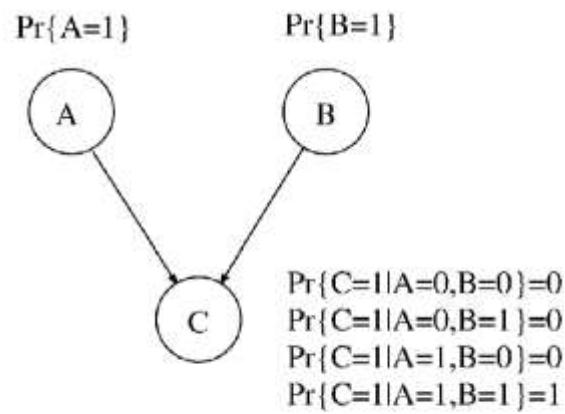
```
if (Power_1 == "True" && Power_2 == "True" && Power_3  
= "True" && Power_4 == "True", "True", "False")  
    AND
```

Using this expression avoids manual writing the $2^5 = 32$ entries required for the NPT of the System conditioned on the four power supplies.

AND- Gate



FAULT - TREE: AND Gate



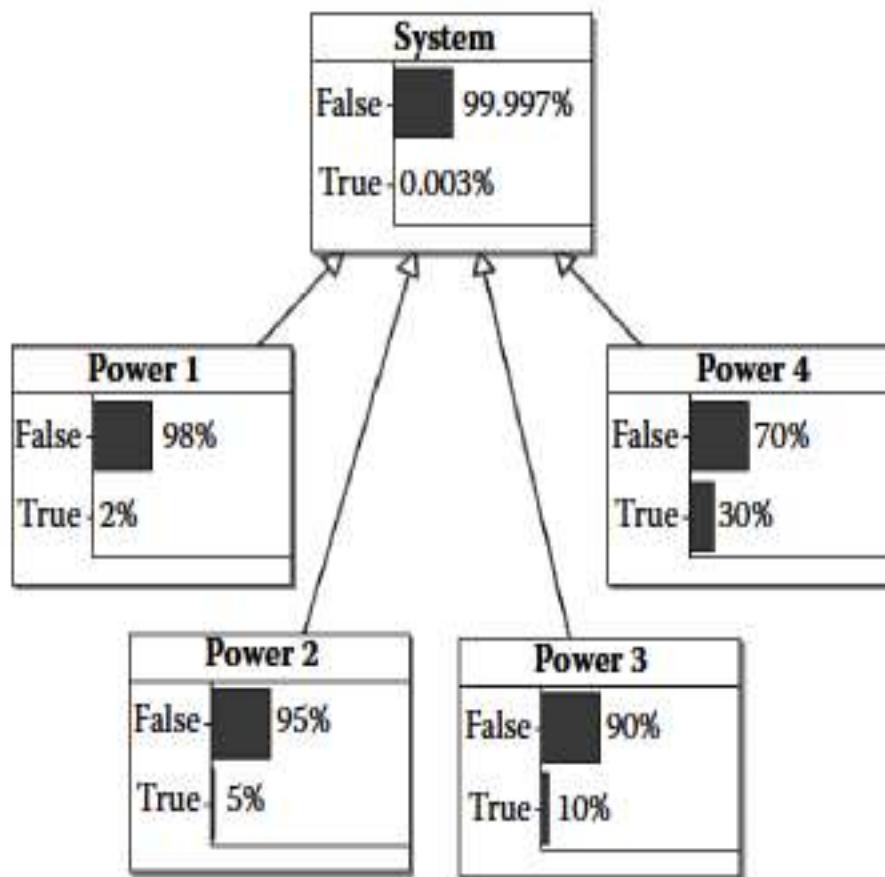
BAYESIAN NETWORK: AND Node

Bobbio, Andrea, et al. "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks." *Reliability Engineering & System Safety* 71.3 (2001): 249-260.

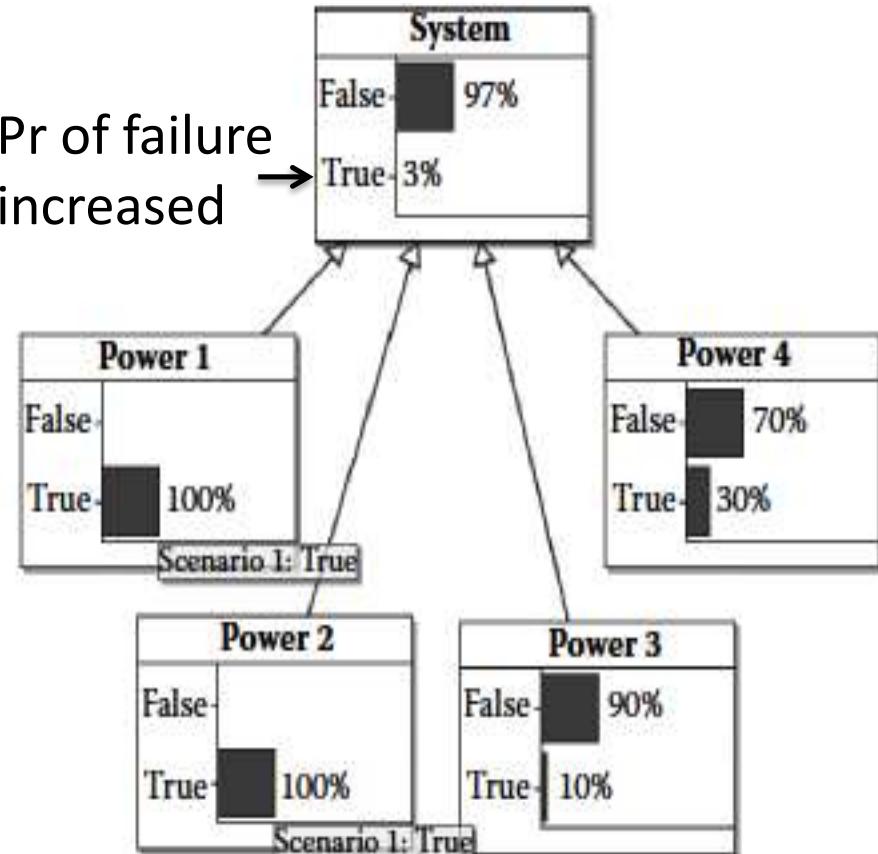
Example: AND-Gate

**See model tutorial
in AgenaRisk: 9.4.3
Power Supply

True is Failure Probability



Pr of failure increased →



M from N Operator

- The M from N operator is True if at least M of its N parents are True, such as, for example, failure will occur if M = 3 or more out of N power supplies fail.
- The M from N operator expression for the System in AgenaRisk given that the System fails only if M = 3 out of N = 4 power supplies fail is:

```
      M  N  
mfromn(3,4, power1 == "True" , power2 == "True" ,  
power3 == "True" , power4 == "True")
```

- If M = 1 (system fails if each unit fails), the M from N operator is the same as the OR operator. If M = N (system fails if all units fail), the M from N operator is the same as the AND operator.

M from N Operator

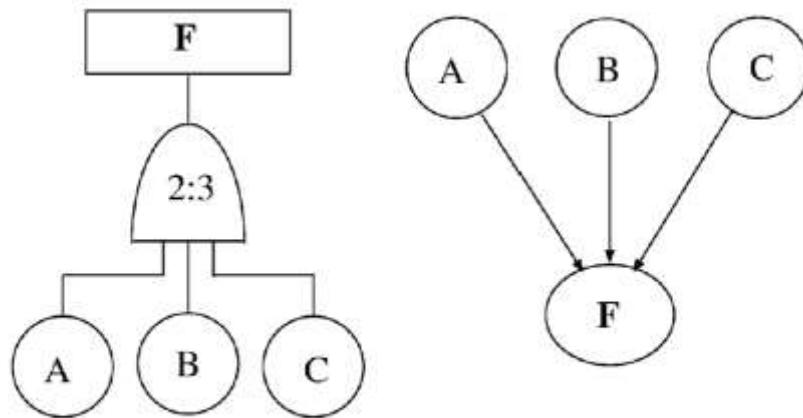


Fig. 2. The 2:3 gate in FT and BN representation.

$$\Pr\{F = 1 | A = 0, B = 0, C = 0\} = 0$$

$$\Pr\{F = 1 | A = 0, B = 0, C = 1\} = 0$$

$$\Pr\{F = 1 | A = 0, B = 1, C = 0\} = 0$$

$$\Pr\{F = 1 | A = 1, B = 0, C = 0\} = 0$$

$$\Pr\{F = 1 | A = 0, B = 1, C = 1\} = 1$$

$$\Pr\{F = 1 | A = 1, B = 0, C = 1\} = 1$$

$$\Pr\{F = 1 | A = 1, B = 1, C = 0\} = 1$$

$$\Pr\{F = 1 | A = 1, B = 1, C = 1\} = 1$$

Bobbio, Andrea, et al. "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks." *Reliability Engineering & System Safety* 71.3 (2001): 249-260.

Noisy OR Function for Boolean Nodes

- When there are numerous parents with effects on a child node that are ~ independent, we can quantify the impact of each causal factor on the child independently of the states of the other parents using the Noisy OR function.
- Each causal factor will be given a probability that the child consequence will be True.
- Also, we specify an additional probability designated the ***leak value*** that captures the probability of one or more additional, unidentified causes of the child consequence to be True.

Box 8.7 General Definition of the NoisyOR Function

Suppose there are n causal factors, X_1, \dots, X_n , of a condition, Y . Suppose also that we can assign a probability value for Y being true when one and only one X_i is true, and all causes other than X_i are false. Then the NoisyOR function can be used. Formally it is defined as

$$\text{NoisyOR}(X_1, v_1, X_2, v_2, \dots, X_n, v_n, l)$$

↑
leak value

where for each i $v_i = P(Y = \text{true} \mid X_i = \text{true}, X_j = \text{false} \text{ for each } j \neq i)$ is the probability of the condition being true if and only if that sole causal factor is true.

The leak factor, l , is the probability that Y will be true when all of the causal factors are false:

$$l = P(Y = \text{true} \mid X_1 = \text{false}, X_2 = \text{false}, \dots, X_n = \text{false})$$

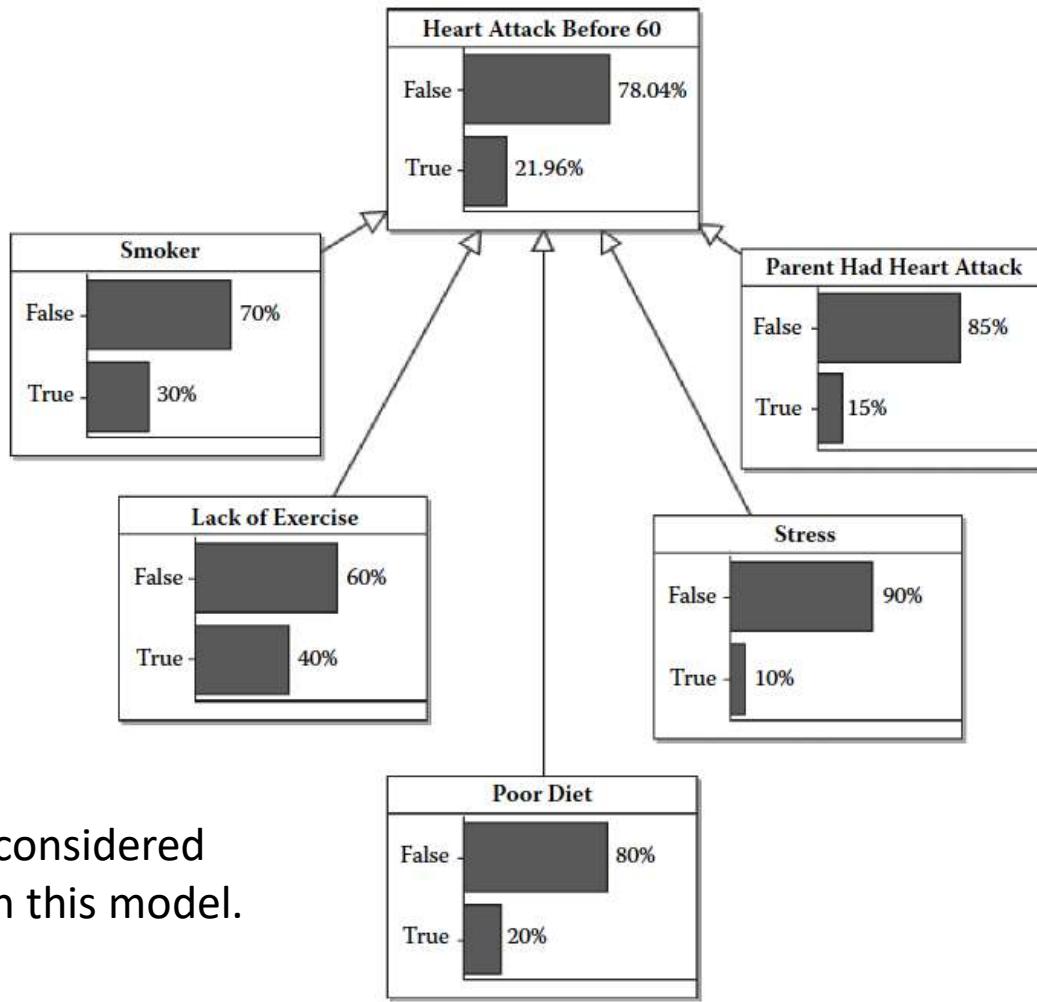
In using the NoisyOR we are assuming we can consider each cause independently of the others in terms of their effects. Formally, we generate the NPT for the NoisyOR function using

$$P(Y = \text{True} \mid X_1, \dots, X_n) \quad \begin{array}{l} \text{Expression for OR when each} \\ \text{variable is considered independent} \end{array}$$

$$= 1 - \prod_{i=1}^n [(1 - P(Y = \text{True} \mid X_i = \text{True})) (1 - P(l))] \quad \begin{array}{l} \uparrow \\ \text{OR general expression} \end{array} \quad \begin{array}{l} \uparrow \\ \text{Added} \end{array}$$

This “independent causal influence” is a key assumption in the use of the NoisyOR function.

$\Pr = 0.3$ that smoking will cause a heart attack < 60 yr

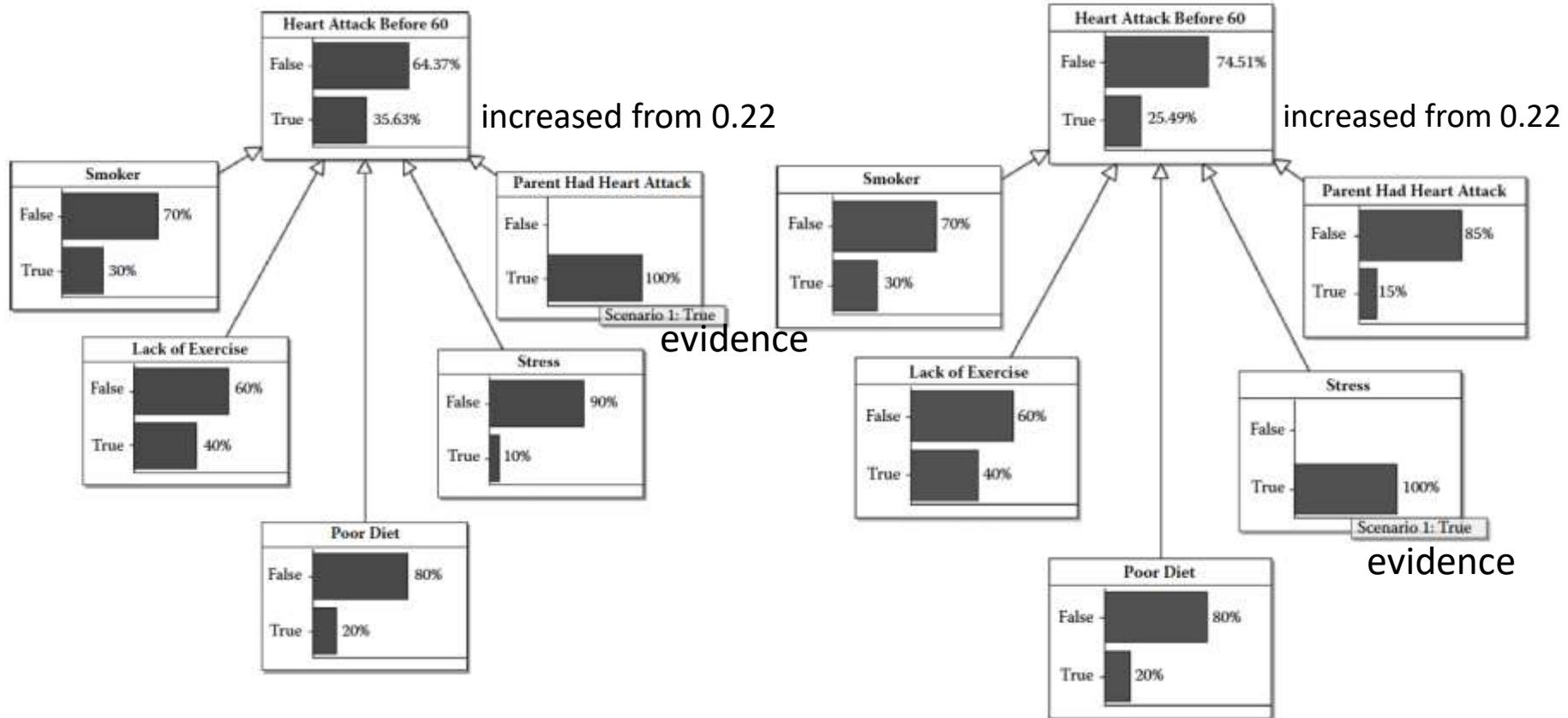


All causes are considered independent in this model.

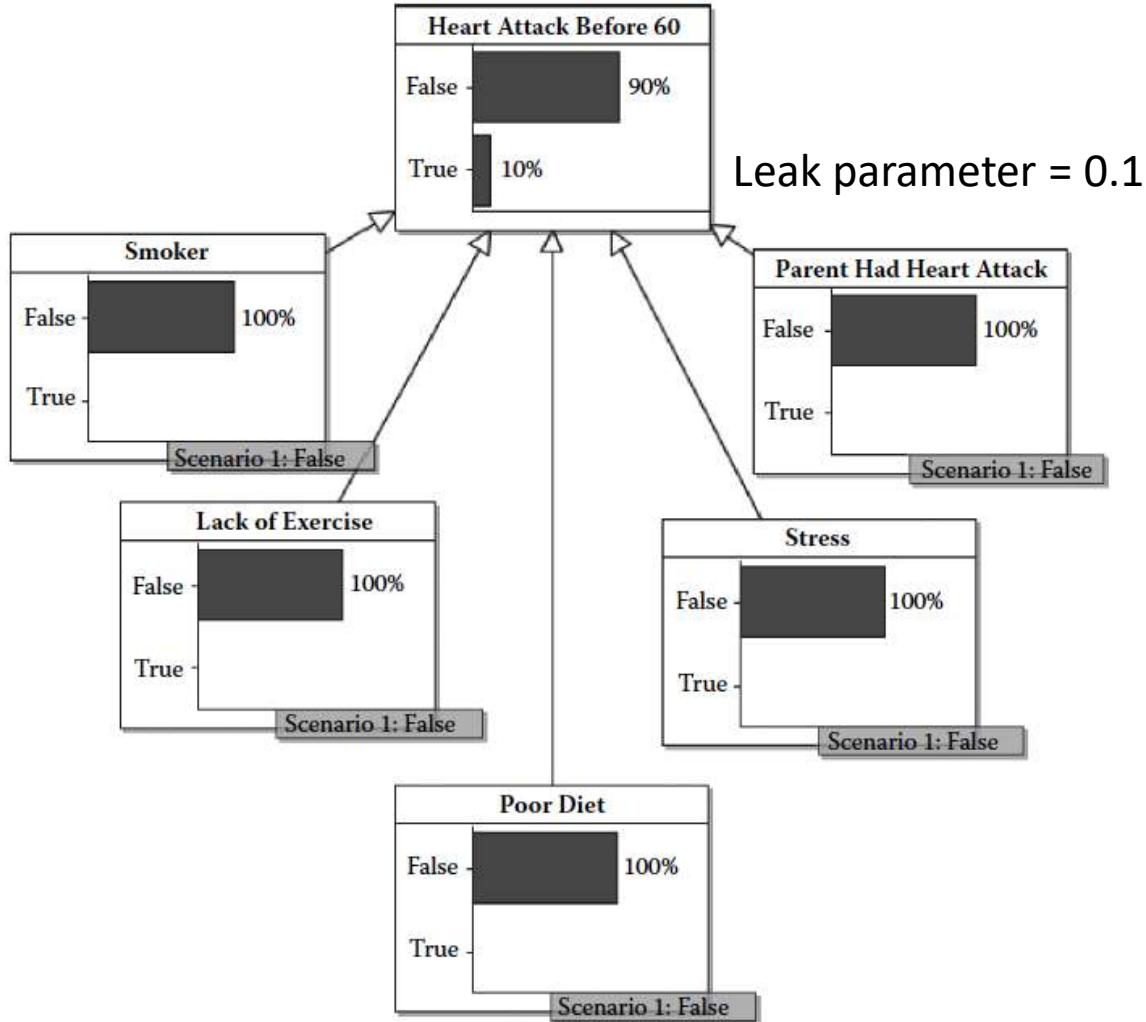
NoisyOR (Smoker, 0.3, Lack of Exercise, 0.4, Poor Diet, 0.2, Stress, 0.1, Parent Had Heart Attack, 0.15, 0.1)

Leak value = 0.1, which is the \Pr of all other causes not in the model.

Heart Attack Posterior given Evidence



Given only the evidence that Patient had a previous heart attack, the updated $\text{Pr}(\text{Heart Attack})$ is increased from 22% to 36%, whereas if the evidence is only observed Stress, the $\text{Pr}(\text{Heart Attack} < 60)$ is increased from 22% to only 26%. Note that Stress intensity and duration are not specified.



- If every causal factor is observed to be false, the $\Pr(\text{Heart Attack} < 60)$ is 0.1, which is the leak parameter or the probability of other causal factors not in the model.
- If the leak value is set to 0 and every causal factor is observed to be false, then the $\Pr(\text{heart Attack} < 60) = 0$

Ranked Nodes

- Ranked nodes are nodes with discrete values given linguistic names, such as low, medium, and high.
- Linguistic ranking by itself is ambiguous, so a range of Pr values within [0,1] in equal intervals must be applied for each level. The ranking here consists of a numerical scale from 0 to 1 in equal intervals:

Table 8.10
Mapping of n -Point Ranked Scale to the Underlying Range [0–1]

Ranked Scale State	Underlying Numerical Equivalent	
State 1 (lowest)	$[0, 1/n]$	$0, 1/3 \quad]$
State 2	$[1/n, 2/n]$	$1/3, 2/3 \quad]$
State 3	$[2/n, 3/n]$	$2/3, 3/3 \quad]$
...	...	
State $n - 2$	$[(n - 2)/n, (n - 1)/n]$	
State $n - 1$	$[(n - 1)/n, 1]$	

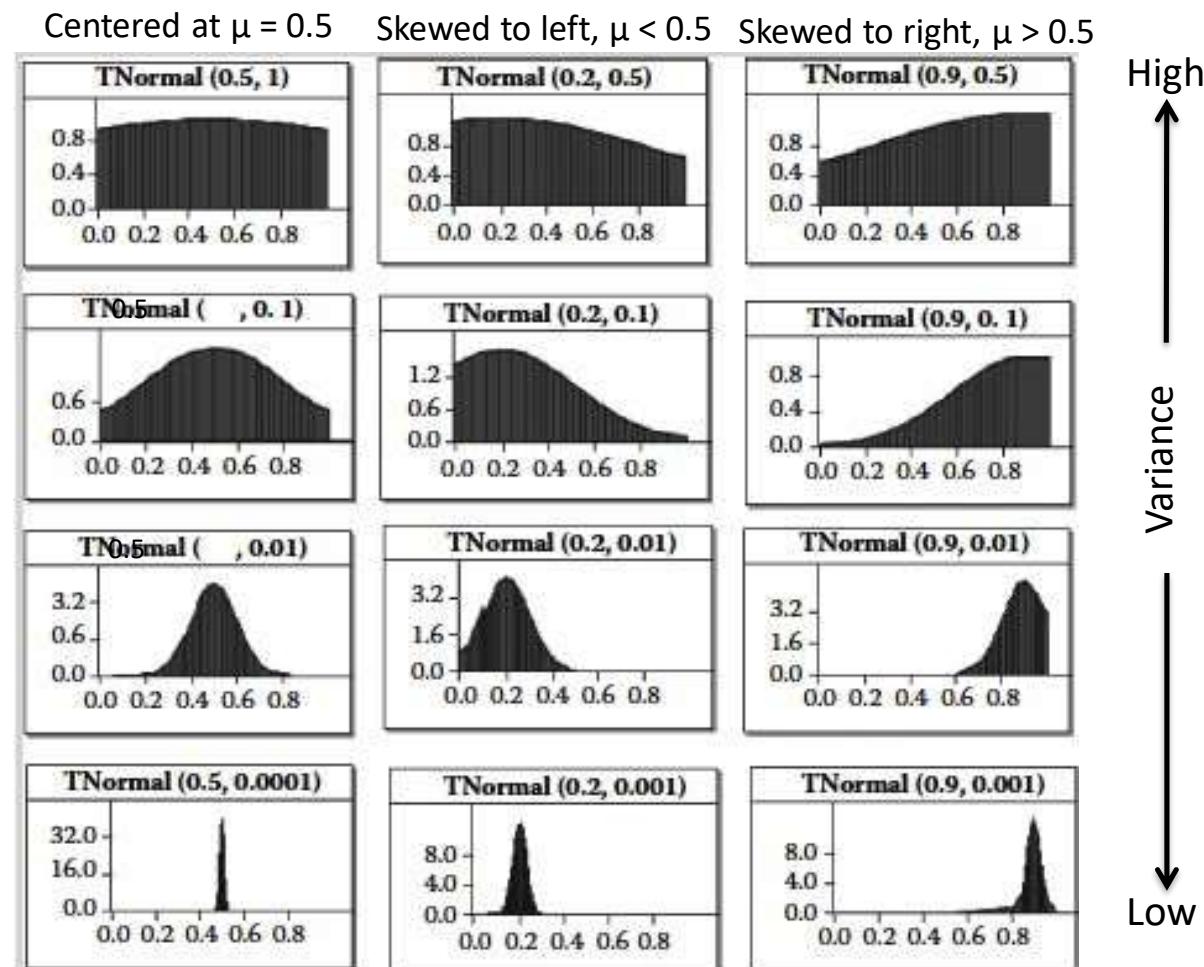
Sample Ranked Nodes with the TNormal Distribution

- The TNormal (truncated) distribution within [0,1] is useful for generating NPTs on the ranked nodes and model a variety of shapes. Tnormal parameters are μ (mode here) for shape, and variance for spread.

μ is position of the mode

- Near uniform shape for $\mu = 0.5$, variance = 1
- Skew increases when mode is farther from 0.5. Spread decreases when variance is lower.
- Experts can estimate μ and variance to avoid detailed elicitation.

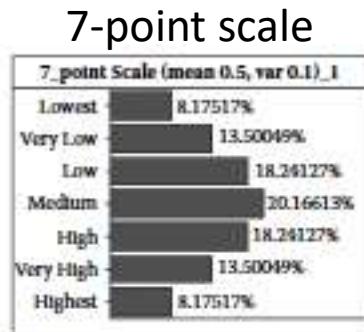
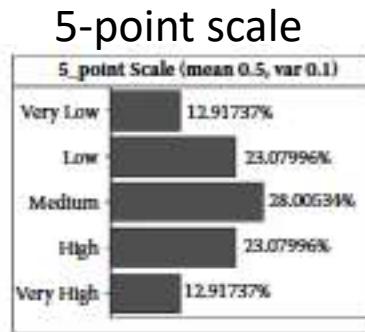
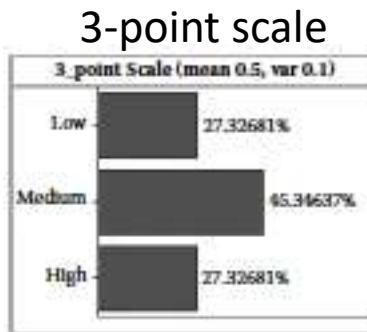
****See model tutorial
in AgenaRisk: 9.5
Rank node examples**



Using the TNormal Distribution to Calculate NPTs

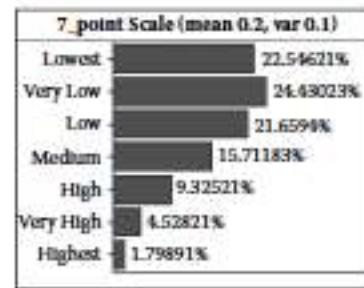
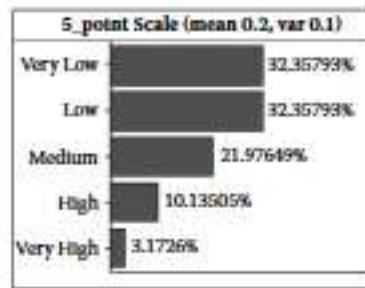
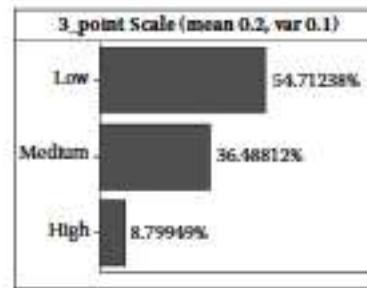
- Instead of only manual entries, NPT values for ranked nodes are conveniently generated in AgenaRisk using TNormal distribution samples of the parent nodes.

$\mu = 0.5$
 $\text{Var} = 0.1$



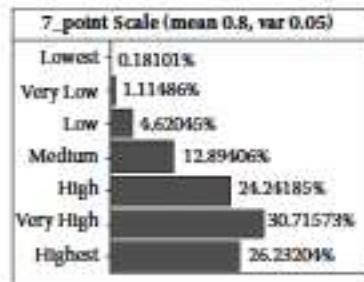
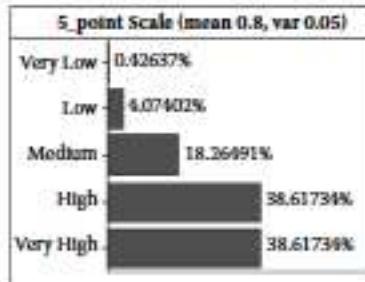
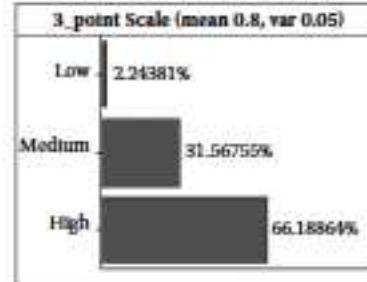
Symmetric

$\mu = 0.2$
 $\text{Var} = 0.1$



Skewed to Low

$\mu = 0.8$
 $\text{Var} = 0.05$



Skewed to High

Fig 8.32, Sample ranked nodes with NPTs defined as TNormal

Using the TNormal Distribution to Calculate NPTs

- NPT values for ranked nodes can be generated in AgenaRisk using a dialog. In the example below, the Testing Quality is low, so a mode of 0.3 and a variance of 0.1 is entered to skew the distribution mode toward low.

Node Probability Table

NPT Editing Mode: Expression

Expression parameters take the form of standard mathematical expressions and can include node names (available by right-clicking in the parameter's text field).

If a parameter is badly formed, the text field will have a red border. You can find out the problem by holding the mouse over the field.

Expression Type: TNormal

Mean: 0.3

Variance: 0.1

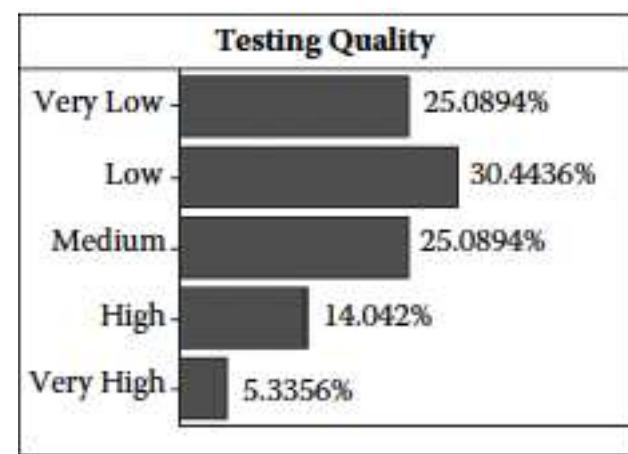


Fig 8.34, Ranked node based on NPT expression TNormal (0.3, 0.1)

Fig 8.33, Entering a TNormal expression for a ranked node

With TNormal, experts estimate **only 2 values**, the mode, most likely value, and variance, instead of time intensive elicitation estimations of all values in a NPT.

- We can define the NPT of the child node Y (Actual Testing Effectiveness) to be TNormal with mode, a weighted average of parent nodes X_1 (weight = 3) and X_2 (weight = 1), and variance of 0.01 in Fig 8.35.

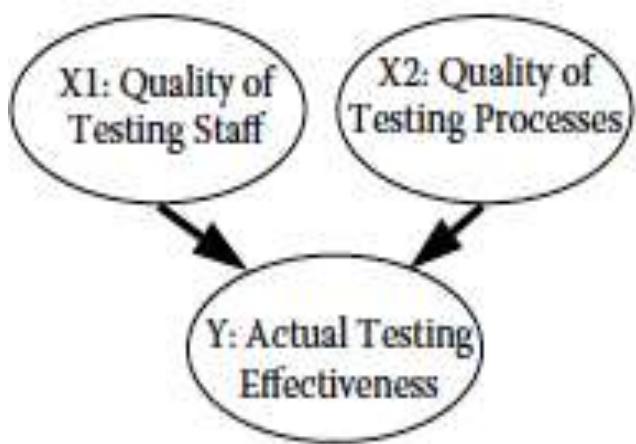
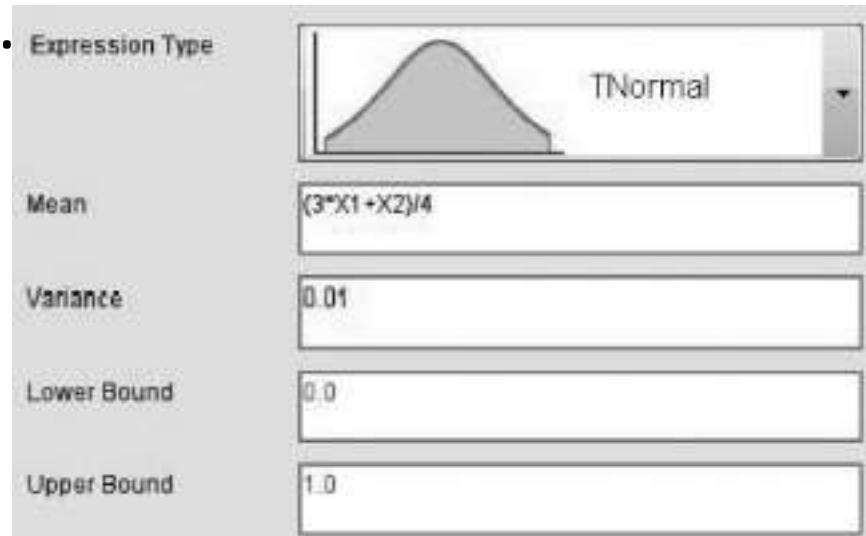


Fig 8.30, BN fragment

Fig 8.35, NPT for node Y defined as a TNormal with mode a weighted average of parents.

This distribution can be entered directly as an expression for the node Y.



- **Predictive Reasoning:** Because X_2 is less influential than X_1 , the effect on the child node Y is biased by 3/1 weighting toward the X_1 value as shown in the figure with observed X_1 and X_2 .

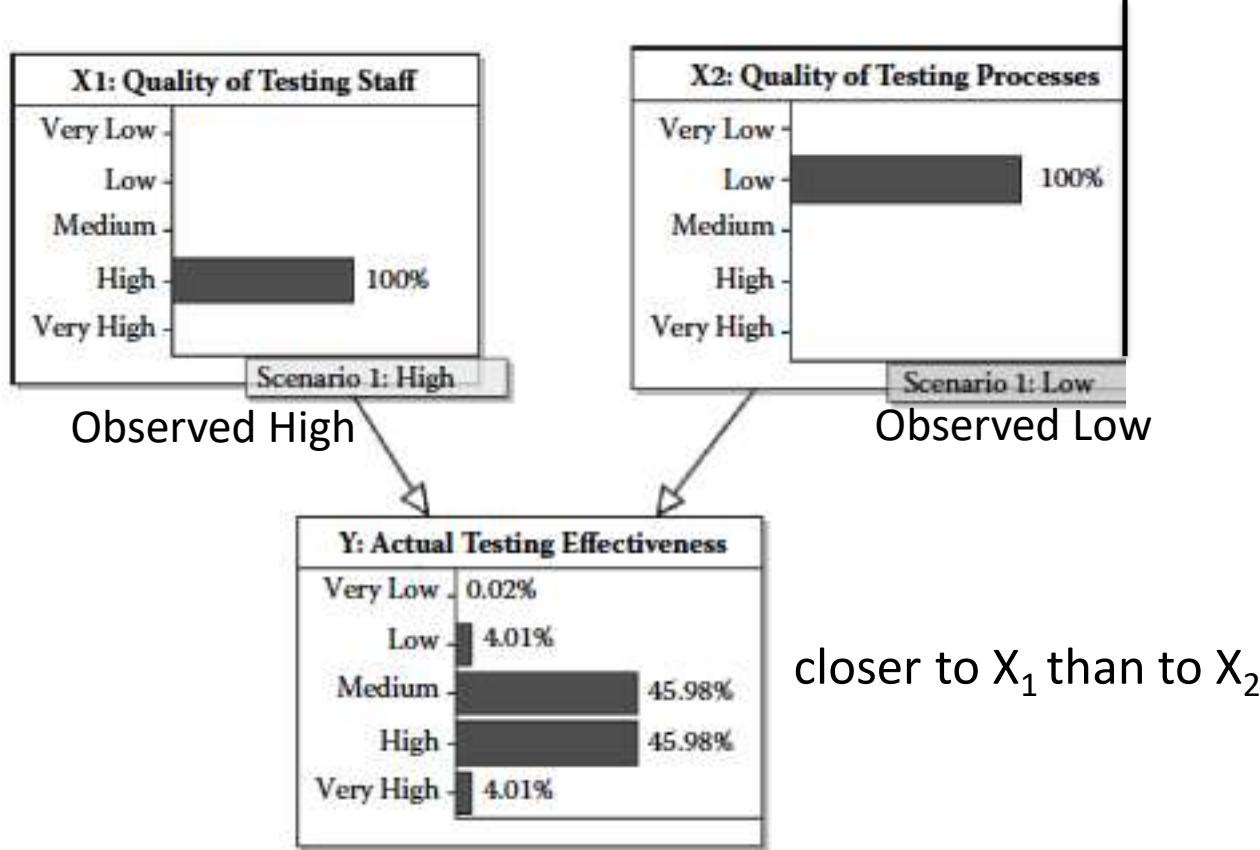
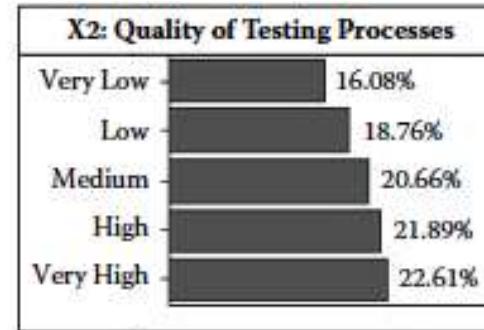


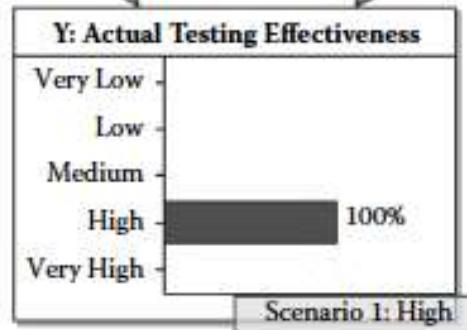
Fig 8.37 Prediction of Y given X_1 high and X_2 low

Example of Uncertainty Modeling

- **Diagnostic Reasoning:** When we update the causes given observed evidence of effects, as shown below for observed Y as High, we see the relative importance of the parent weighting. Nodes with greater weights will appear as the more likely causes of the consequence. Here a high value of X_1 (weight = 3) is identified as the more likely cause of the high value of Y.



Y much closer to X1 than to the more uncertain X2



X2 much higher uncertainty than for X1

X1 and X2 become dependent when common effect Y is observed.

- If we now observe that X_1 is Medium, the High observed value of common effect Y is explained away by our now increased belief in a higher value of X_2 , as shown below.
- Only with BNs is this expected back-propagation capability and **Intercausal Reasoning** achieved.

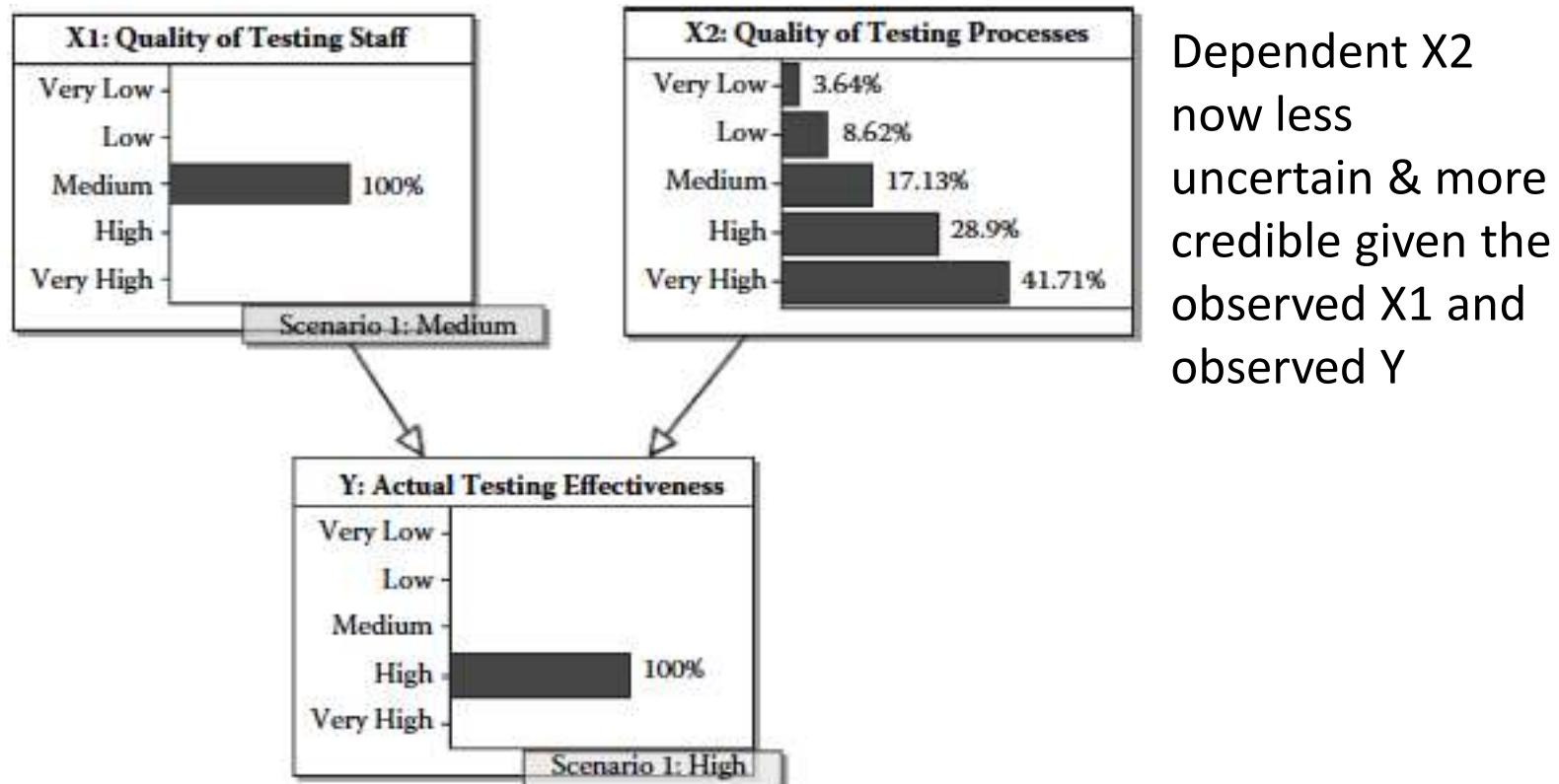


Fig 8.39 Explaining away the high value of Y

Reliability Data Methods

Unit 14

Spring 2022

References

- **Modarres, M., M. Kaminsky, and Vasiliy Krivtsov, *Reliability Engineering and Risk Analysis*, 2nd ed, Taylor&Francis, 2010 (Modarres, RERA)**
- Ebeling, C.E., Introduction to *Reliability and Maintainability Engineering*, 3rd ed, Waveland Press, 2019, Chapter 16 (Ebeling, 2019)
- Triola, M.F., Elementary Statistics, 10th ed., Addison Wesley, 2007 (Triola, 2007)
- **MLE Method:** https://www.youtube.com/watch?v=p3T-_LMrvBc

Fitting Theoretical Distributions

4

- Small sample sizes provide very little information concerning the **failure process**. However, if the sample is consistent with a theoretical distribution, then much "stronger" and reliable results are possible based upon the properties or characteristics of the theoretical distribution.
- Use can be made of the theoretical **Reliability Model** in performing more complex analysis of the failure process.
- Reliability Model makes possible more accurate predictions of component or system behavior to support optimum system decision making under uncertainty, such as updating the test schedule for sensitive components (identified from a risk assessment).

1. Identify the Candidate Distributions
 - Construct a histogram of the data
 - Compute Descriptive Statistics from the data
 - Analyze the empirical conditional failure rate $\lambda(t)$ to identify DFR, CFR, or IFR
 - Use properties of theoretical distributions
2. Estimate distribution parameters
 - a) Calculate data for probability plot
 - b) Plot the data or do Least Squares Fitting (LSF)
 - c) Compare the LSF of candidate distributions and select the distribution with the Index of Fit, r , or coefficient of determination, r^2 , nearest to 1
 - d) Obtain the distribution Parameter values derived from Plot/LSF or, use Maximum Likelihood Estimation, MLE
3. Perform a Goodness-of-Fit test of the distribution using Chi-Square or other tests optimized for each of the distribution model candidates.
4. Construct Confidence Intervals for model parameters.

Step 1:

Histograms to View Empirical Data for Descriptive Statistics

6

- **Sturges' Rule** for Efficient Grouping of Data into Classes

$$k = 1 + 3.3 (\log_{10} n)$$

Where k = number of classes and n = sample size.

For example,

<u>n</u>	<u>k</u>
50	7
500	10
5000	13

- Classes are to be roughly the same size, and classes must be mutually exclusive, so each datum value is in only one class.

Ex. 15.1: Field Data Collected over 6 Months

Sturges' Rule, $k = 1 + 3.3 (\log_{10} n)$

7

Given $n = 35$ Failure Times:

1476	300	98	221	157
1825	499	552	1563	36
246	442	20	796	31
47	438	400	279	247
210	284	553	767	1297
214	428	597	2025	185
467	401	210	289	1024

- From Sturges' Rule:

$$k = 1 + 3.3 (\log_{10} 35) = 1 + 3.3 (1.544) = 6.095 = 6 \text{ classes}$$

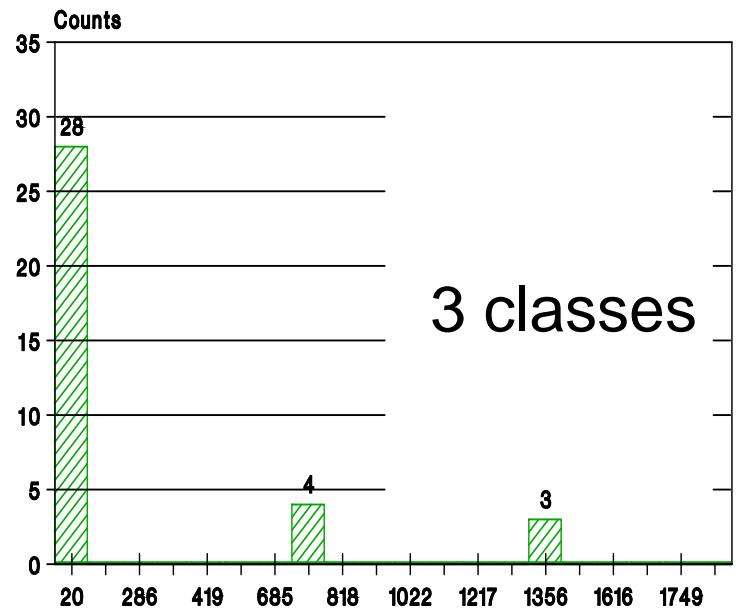
- This is a workable number of classes to group and observe the given data for Descriptive Statistics analysis.

7

Ex 15.1: Field Data Plotted as a Histogram

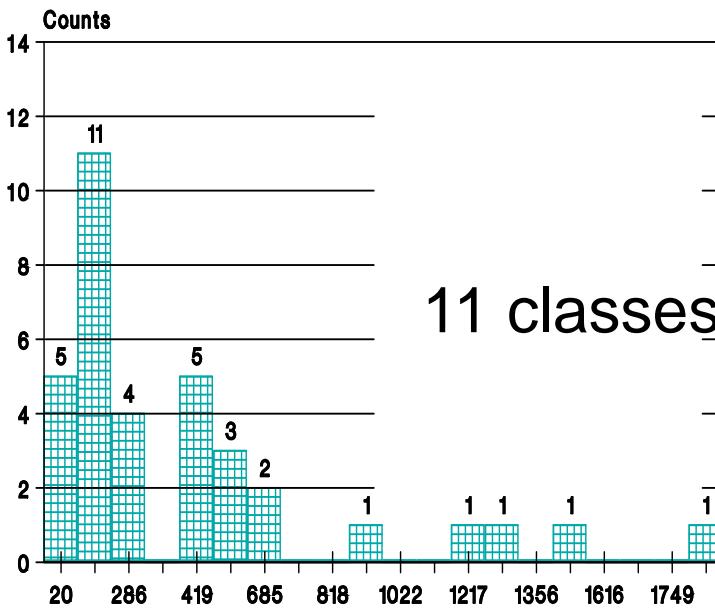
8

FREQUENCY DISTRIBUTION
OF OBSERVED VALUES



Too few classes

FREQUENCY DISTRIBUTION
OF OBSERVED VALUES

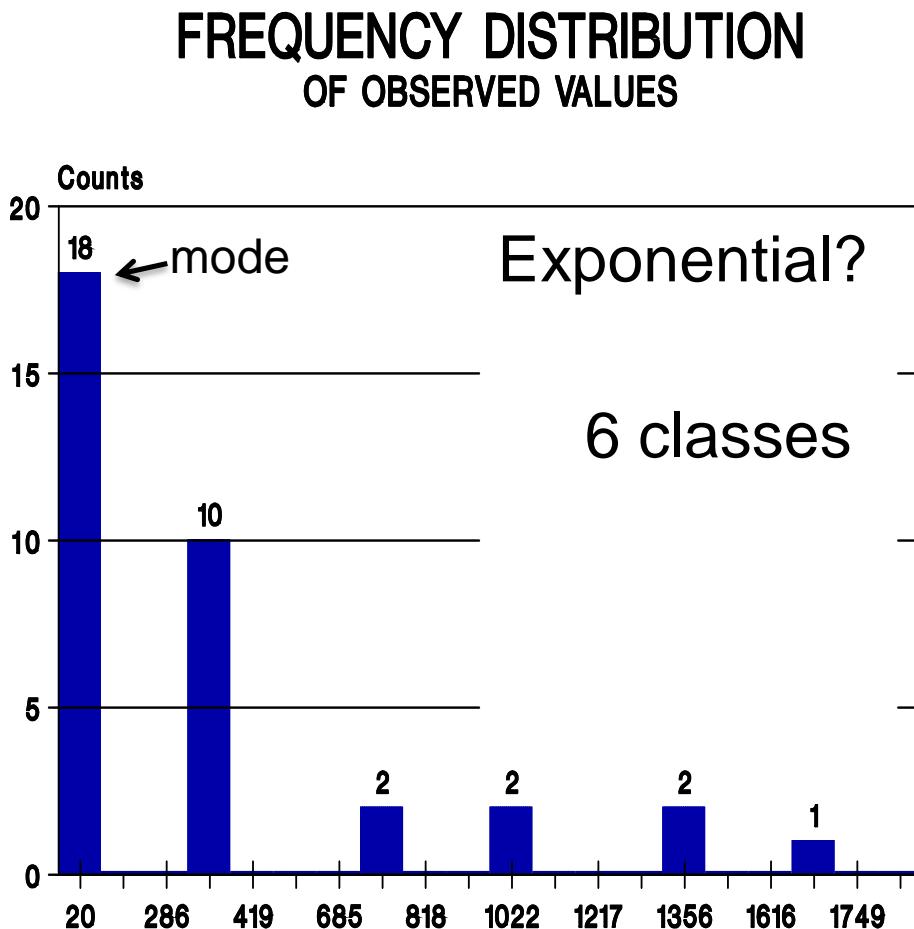


Too many classes

If the classes are too few or too many, the underlying distribution is harder to view and identify.

Ex. 15.1: Histogram Following Sturges' Rule

9



Depending on the sample size, the number of classes resulting from Sturges' Rule is 5 to 20 classes.

9

Descriptive Statistics

- Use Descriptive Statistics to rule out some distributions or to identify one or more candidate distributions.
- Mean and median values are nearly equal if the failure times are from a **symmetric**:
 - Normal pdf or nearly symmetric distribution, such as Weibull pdf with $\beta = 3$ to 4, or Lognormal pdf for $s \leq 0.1$ (Estimate the median in empirical data from the middle failure value if $n = \text{odd}$ or the average of the two middle failure values if $n = \text{even}$)
- If the pdf **mean and std dev** is about equal
 - Exponential
- If the mean is significantly larger than the median with the distribution being **skewed** with a tail to high values of t
 - Exponential pdf, Lognormal pdf for $s > 0.1$, or Weibull pdf with $\beta < 3$.
- If the conditional failure rate, $\lambda(t)$ is
 - roughly constant: Exponential
 - decreasing: Weibull $\beta < 1$
 - increasing: Weibull $\beta > 1$, Normal (symmetric), or Lognormal with $s > 0.1$ (skewed).

Ex. 15.2: Descriptive Statistics

11

Same n = 35 failure empirical data values now rank ordered:

Rank ordered data: 35, odd, so median = 300 hr

20	31	36	47	98
157	182	185	210	210
214	221	246	247	279
284	289	300	400	401
428	438	442	467	499
552	553	597	767	796
1024	1297	1476	1563	2025

Empirical estimates:

$$\hat{t}_{\text{med}} = 300 \text{ hr}$$

$$\hat{\text{MTTF}} = \hat{a} = \frac{\sum t_i}{n} = 485 \text{ hr}$$

supports Exponential

$$s^2 = \frac{\sum_{i=1}^n t_i^2 - n \hat{\text{MTTF}}^2}{n-1}$$

Empirical sample variance, s^2 , std dev, s

$$s^2 = (20^2 + 31^2 + \dots + 2025^2 - 35 \times 485.2^2)/34 = 220,712. \text{ So, } s=470 \text{ hr}$$

Because the Exponential is skewed to higher values, median < mean.
 Also, for Exponential, $\text{MTTF} = 1/\lambda = \sigma$

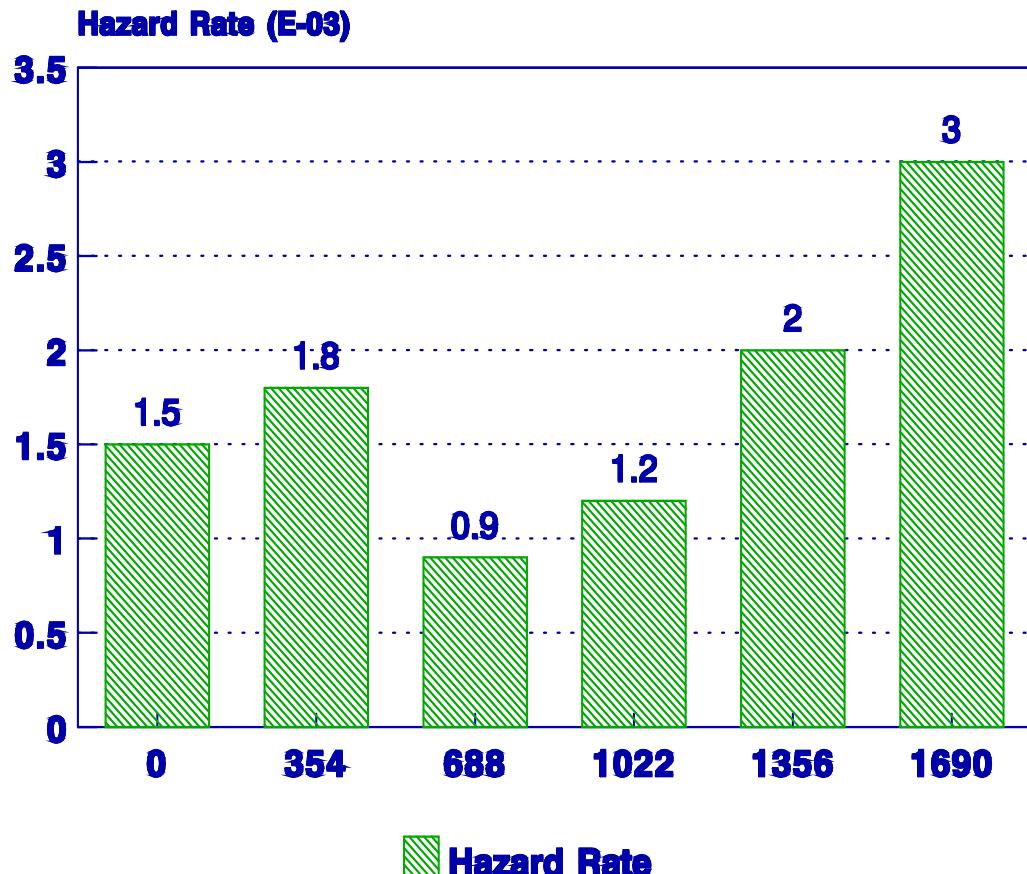
11

Ex. 15.2: Empirical Conditional Failure Rate Curve

Is $\lambda(t)$ from DFR, CFR, IFR, or inconclusive?

From the same 35 failure data values that for the empirical $f(t)$ supported Exponential, the empirical $\lambda(t)$ here is not monotonic, so the Exponential model is less supported but cannot be ruled out by the $\lambda(t)$ figure. So, inconclusive.

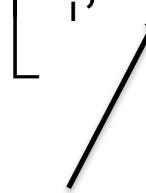
Empirical view of $\lambda(t)$ from data



Step 2: Probability Plot of $t_i, \hat{F}(t_i)$

13

Plot a straight line on graph paper prepared for a particular distribution: $y = a + b x$

$$\left[t_i, \hat{F}(t_i) \right], i = 1, 2, \dots, n$$


Plotting position $\hat{F}(t)$ given by:

$$\text{Mean, } \frac{i}{n+1} \text{ or Median, } \frac{(i - 0.3)}{(n + 0.4)}$$

low bias

The plot will be an approximate straight line if the data came from the distribution corresponding to the graph paper design, such as Weibull or Lognormal.

13

Exponential Plots using a Linear Expression

14

$$F(t) = 1 - e^{-\lambda t} \quad \text{Linearize!}$$

$$\ln [1 - F(t)] = -\lambda t \quad \text{or}$$

$$-\ln [1 - F(t)] = \ln [1/(1 - F(t))] = \lambda t$$

$$\left. \begin{array}{l} Y = \text{Vertical scale: } \hat{F}(t) \rightarrow \ln \left[\frac{1}{1 - \hat{F}(t)} \right] \\ X = \text{Horizontal scale: } \lambda t \end{array} \right\} \text{Slope} = \lambda$$

Probability plots for the Exponential are based upon the above linearizing transformation, which will create a linear graph if the data follow the Exponential distribution.

14

Methods to find failure rate

- A. Use all data (lower uncertainty) to estimate slope, λ from graph
- B. LSF Method to estimate λ : For a more accurate result, use least-squares to fit a line passing through the data and the origin for $t = 0$, and estimate the slope

Least Squares expression $\hat{\lambda} = b = \frac{\sum_{i=1}^n x_i y_i}{\sum_{i=1}^n x_i^2}$

where $y_i = \ln \{1/[1-F(t)]\}$, and $x_i = t_i$

Ex. 15.4 Least Squares Fit



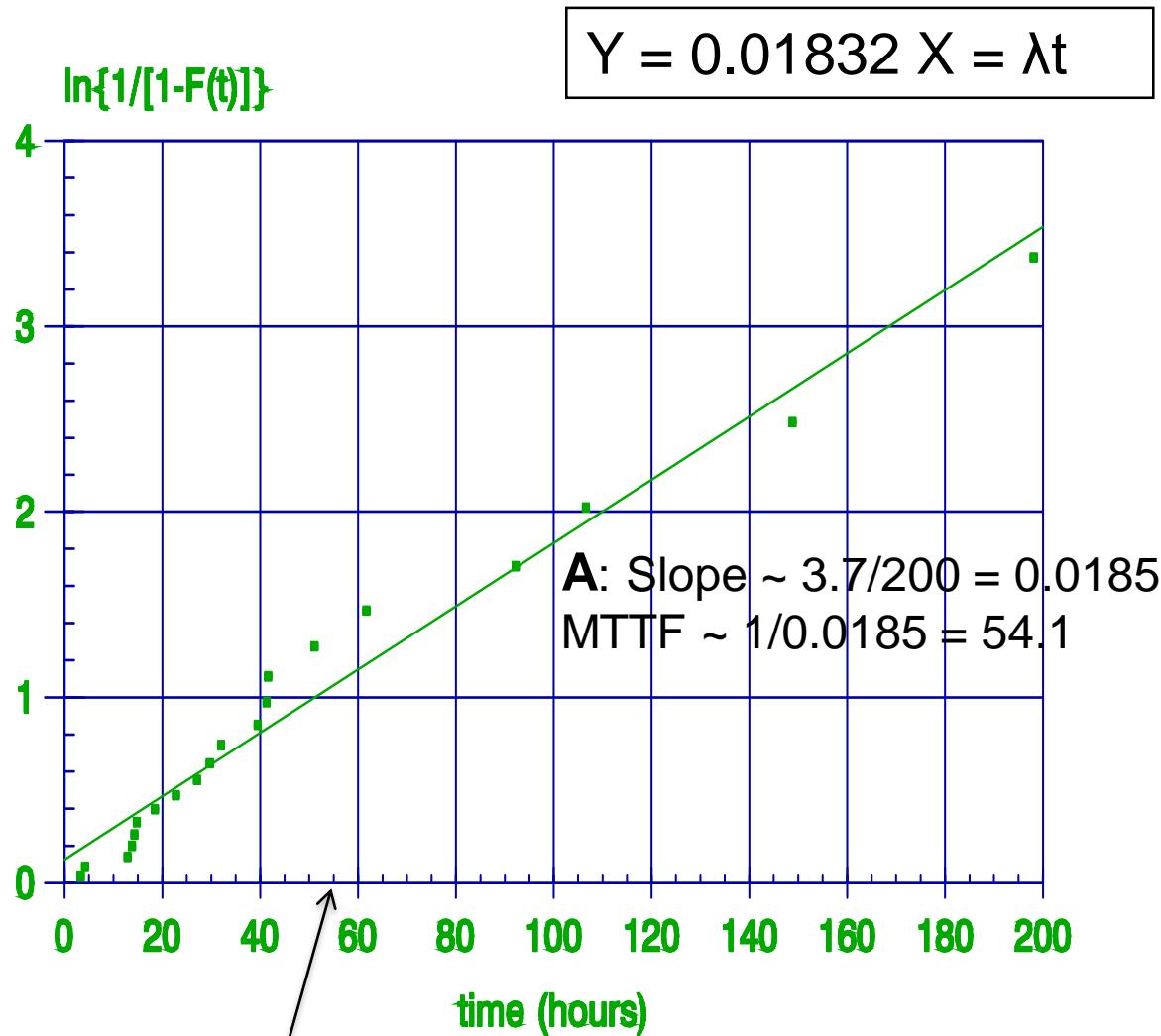
Data	Median	Linear Expression	
FAILURE TIME (x_i)	$F(t_i) = (i-0.3)/(n+0.4)$	$y_i = \ln [1/(1-F(t_i))] = \lambda_i t$	
3.3	3.431373E-02	3.491616E-02	
4.2	8.333334E-02	8.701131E-02	
12.9	0.132353	0.1419703	
13.8	0.1813726	0.2001262	
14.3	0.2303922	0.2618741	SLOPE: $0.01832 = \hat{\lambda}$
14.8	0.2794118	0.3276874	
18.5	0.3284314	0.398139	
22.8	0.377451	0.4739329	
27.1	0.4264706	0.5559461	
29.7	0.4754902	0.6452911	
32	0.5245098	0.743409	
39.5	0.5735295	0.8522118	
41.3	0.622549	0.9743145	
41.6	0.6715686	1.113427	
51.1	0.7205883	1.275069	
61.7	0.7696078	1.467972	
92.2	0.8186275	1.707202	
106.6	0.8676471	2.022284	
148.8	0.9166668	2.484908	
198.1	0.9656863	3.372211	

Median plotting position is used for $F(t_i)$ but other plotting positions also can be used.

Sample mean = 48.7 hr

Ex. 15.4 – Exponential Plot of Data: LSF

17



$$R(t) = e^{-0.01832t}$$

Weibull Plots by Linearization

18

$$F(t) = 1 - e^{-\left(\frac{t}{q}\right)^b} \rightarrow \ln \left[\frac{1}{(1-F(t))} \right] = \left(\frac{t}{q}\right)^b$$

$$Y = bX + a$$

$$\ln \left[\frac{1}{(1-F(t))} \right] = b \ln t - b \ln q$$

Slope = β

Plot: $\left(\ln t_i, \ln \left[\frac{1}{(1-\hat{F}(t_i))} \right] \right)$

Probability plots for the Weibull are based upon the above transformation, which will create a linear graph if the data are from the Weibull distribution.

Weibull, Least-Squares Approach

Through least-squares fitting, the slope, b , and intercept, a , can be estimated more accurately and tested by the Index of Fit value rather than by plotting the data.

$$Y = \ln \ln \left[\frac{1}{(1 - F(t))} \right] = b \ln t - b \ln q$$

slope intercept

$$x_i = \ln t_i \quad \text{and} \quad y_i = \ln \ln \left[\frac{1}{1 - F(t_i)} \right]$$

Least Squares Expressions:

$$\text{Slope: } b = \frac{\sum_{i=1}^n x_i y_i - \bar{x} \sum_{i=1}^n y_i}{\sum_{i=1}^n x_i^2 - n \bar{x}^2}$$

$$\text{Intercept: } a = \bar{y} - b \bar{x} = -\beta \ln \theta$$

$$\hat{b} = b \quad \text{Shape parameter}$$

$$\hat{q} = e^{-a/b} \quad \text{Scale parameter}$$

Example 15.5 (continued)

X <u>FAILURE TIME</u>	$F(t_i) = (i-0.3)/(n+0.4)$	Y $\ln \ln[1/(1-F(t_i))] = b\ln t - a$
32	0.1296296	-1.974459
51	0.3148148	-0.9726862
74	0.5	-0.3665129
90	0.6851852	0.1447674
120	0.8703704	0.7144555

INTERCEPT, a	-8.9516
SLOPE, b	2.0156
ESTIMATED β	$2.016 = b$
ESTIMATED θ	$84.89 = e^{-a/b}$
Index-of-Fit (R)	0.9986 Excellent fit

$$R(t) = e^{-\left(\frac{t}{84.89}\right)^{2.0156}}$$

Ex. 15.6, Weibull Curve Fit to Complete Failure Data

21

i	t _i	$\hat{F}(t_i) = \frac{i - 0.3}{15 + 0.4}$
1	25.1	0.0455
2	73.9	0.1104
3	75.5	0.1753
4	88.5	0.2403
5	95.5	0.3052
6	112.2	0.3701
7	113.6	0.4351
8	138.5	0.5000
9	139.8	0.5649
10	150.3	0.6299
11	151.9	0.6948
12	156.8	0.7597
13	164.5	0.8247
14	218.0	0.8896
15	403.1	0.9545

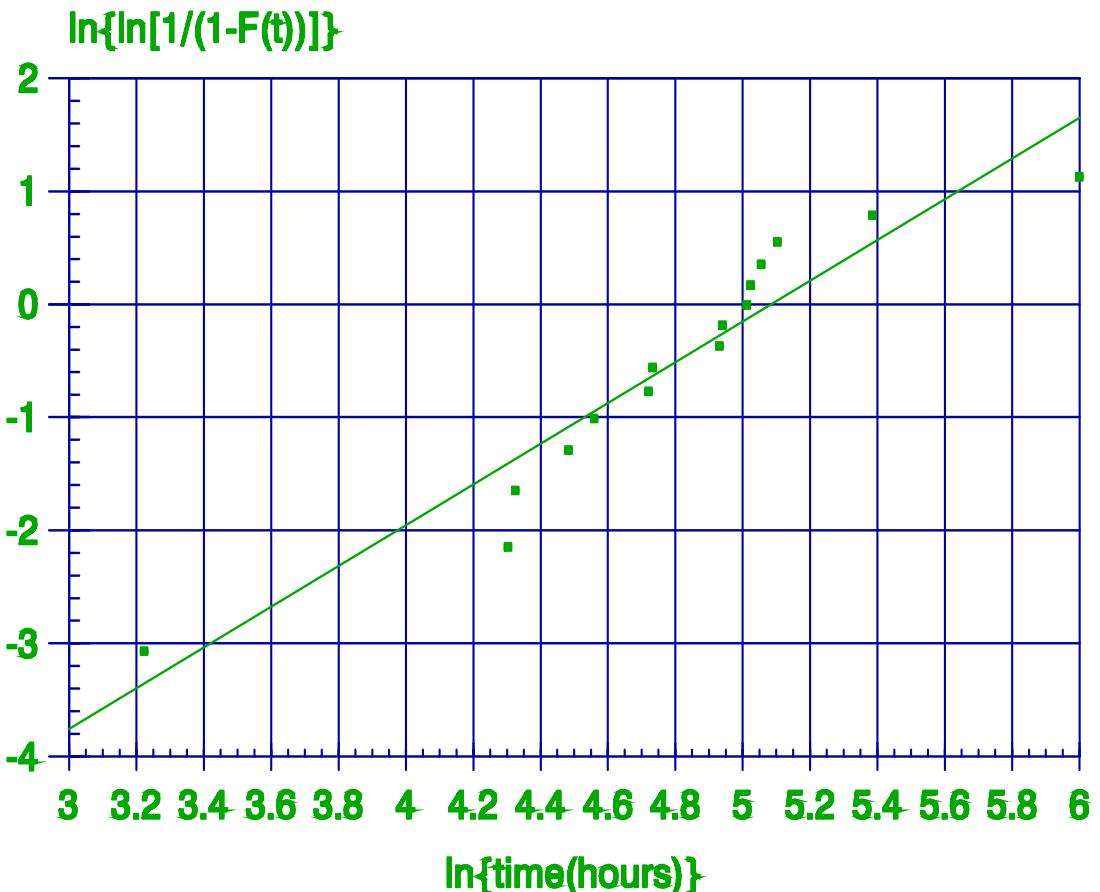
$$y_i = \ln \ln [1/(1-F(t_i))]$$

-3.067874
 -2.145824
 -1.646281
 -1.291789
 -1.010262
 -0.7716678
 -0.5602884
 -0.3665131
 -0.1836104
 -6.117305E-03
 0.1712648
 0.3548976
 0.5545261
 0.7901556
 1.128508

Ex. 15.6

22

Weibull Failure Data



INTERCEPT - a	-9.1649
SLOPE - b	1.8027
Est. BETA (β)	1.8027
Est. THETA (θ)	161.41
Index of Fit	0.9545

Index of Fit value shows a good fit.

$$R(t) = e^{-\left(\frac{t}{161.4}\right)^{1.803}}$$

Normal Distribution Plots

Linearization converts the estimate of the cumulative probability to the corresponding Z value. Failure time t and z are then linearly related. The parameters μ and σ can thereby be estimated.

$$F(t) = \Phi\left(\frac{t - \mu}{\sigma}\right) = \Phi(z)$$

slope = $1/\sigma$

Z is linearly related to failure time t:

$$z_i = \Phi^{-1}[F(t_i)] = \frac{t_i - \mu}{\sigma} = \frac{t_i}{\sigma} - \frac{\mu}{\sigma} = bt_i + a$$

intercept

set: $x_i = t_i$ and $y_i = z_i$ and apply the L-S formulas

$$\hat{\sigma} = \frac{1}{b} \quad \text{and} \quad \hat{\mu} = -a \hat{\sigma} = -\frac{a}{b} \quad = \text{intercept divided by slope}$$

Ex. 15.7: Wearout of Ball Bearings Data

24

I	$x_i = t$	$F(t_i)$	$y_i = z_i$
1	68.0	0.0343	-1.8211
2	69.6	0.0833	-1.3832
3	71.1	0.1324	-1.1151
4	71.4	0.1814	-0.9100
5	74.3	0.2304	-0.7375
6	74.6	0.2794	-0.5846
7	75.5	0.3284	-0.4443
8	77.6	0.3775	-0.3121
9	77.8	0.4265	-0.1853
10	78.0	0.4755	-0.0615
11	78.2	0.5245	0.0615
12	80.2	0.5735	0.1853
13	80.3	0.6225	0.3121
14	81.9	0.6716	0.4443
15	83.0	0.7206	0.5846
16	85.6	0.7696	0.7375
17	87.4	0.8186	0.9100
18	87.7	0.8676	1.1151
19	88.4	0.9167	1.3832
20	98.3	0.9657	1.8211

Median plotting position

$$F(t_i) = (i - 0.3) / (20 + 0.4)$$

Normal Table: Find Z_i from $F(t_i)$

$$\text{INTERCEPT} - a = -9.81565$$

$$\text{SLOPE} - b = 0.123553$$

$$\text{Est. } \sigma (s) = 1/b = 8.0937$$

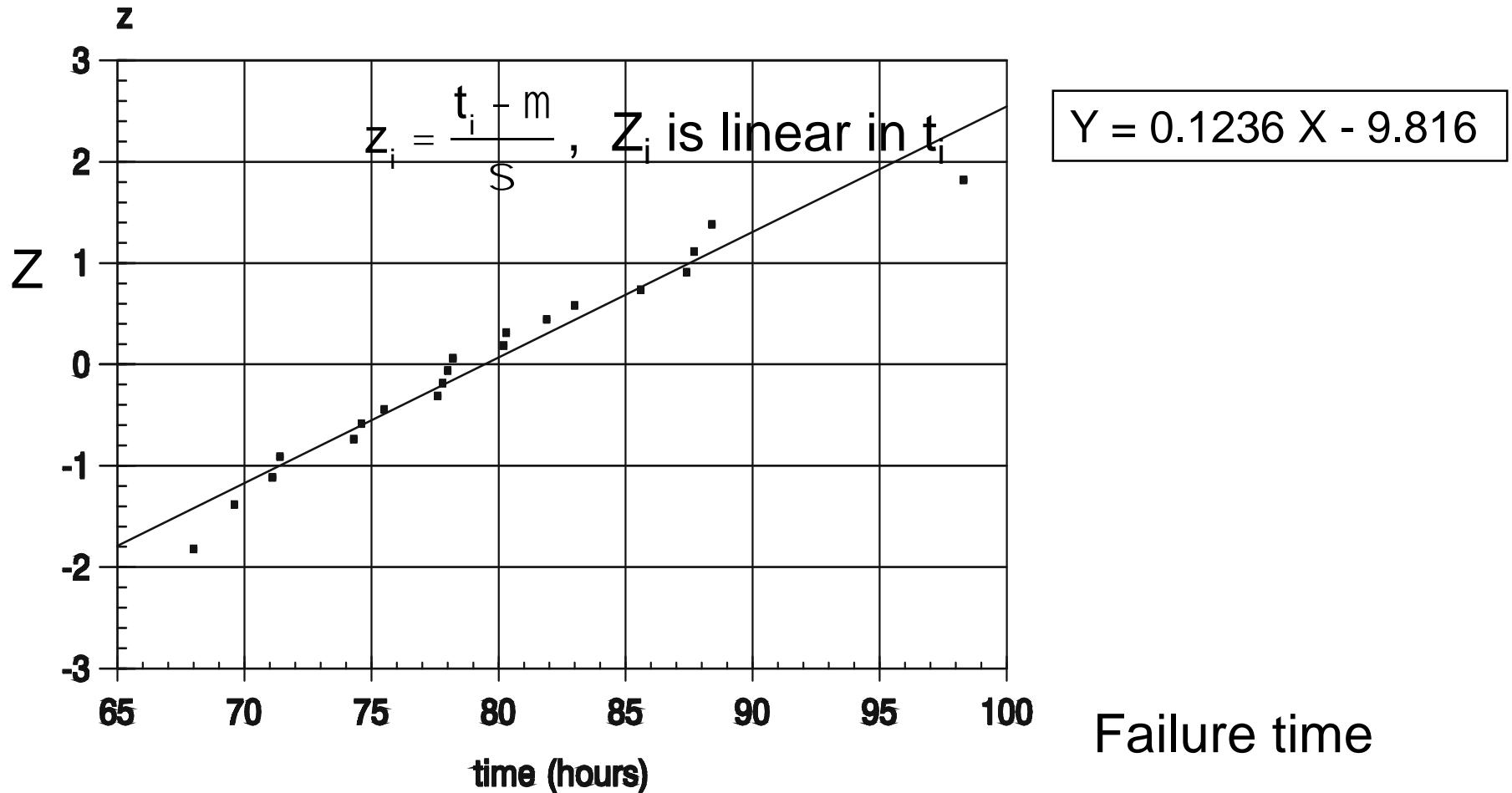
$$\text{Est. } \mu = -a/b = 79.445$$

$$\text{Index of Fit} = R = 0.979$$

$$R(t) = 1 - F\left(\frac{t - m}{s}\right) = 1 - F\left(\frac{t - 79.445}{8.0937}\right)$$

Normal Least-Squares Probability Plot

25



Failure time

25

Lognormal Plots

Lognormal is similar to the Normal except z is linear in the log of the failure times.

$$F(t) = F\left(\frac{1}{s} \ln \frac{t}{t_{\text{med}}}\right) = F(z)$$

slope = $1/s$

$$z = F^{-1}[F(t_i)] = \frac{1}{s} \ln t_i - \frac{1}{s} \ln t_{\text{med}} = b \ln t_i + a$$

intercept

set: $x_i = \ln t_i$ **and** $y_i = z_i$ and apply the L-S formulas

$$\hat{s} = \frac{1}{b} \quad \text{and} \quad \hat{t}_{\text{med}} = e^{-a/b}$$

$$\ln t_{\text{med}} = -a/b$$

Ex: Repair Times of a Mechanical Pump

27

Repair times (in min) of a mechanical pump are believed to follow a Lognormal distribution.

i	t _i	F(t _i)	z _i
1	44.0	0.0276	-1.9173
2	47.1	0.0669	-1.4993
3	53.4	0.1063	-1.2465
4	59.8	0.1457	-1.0551
5	61.5	0.1850	-0.8965
6	77.0	0.2244	-0.7574
7	78.7	0.2638	-0.6317
8	84.8	0.3031	-0.5155
9	99.6	0.3425	-0.4057
10	100.8	0.3819	-0.3005
11	102.4	0.4213	-0.1986
12	104.6	0.4606	-0.0989
13	112.	0.5000	0.0000
14	122.1	0.5394	0.0990
15	122.5	0.5787	0.1986

i	t _i	F(t _i)	z _i
16	138.8	0.6181	0.3005
17	151.3	0.6575	0.4057
18	151.3	0.6969	0.5155
19	151.9	0.7362	0.6317
20	186.2	0.7756	0.7574
21	213.5	0.8150	0.8965
22	218.2	0.8543	1.0551
23	222.8	0.8937	1.2461
24	230.1	0.9331	1.4993
25	498.4	0.9724	1.9173

Median Plotting Position

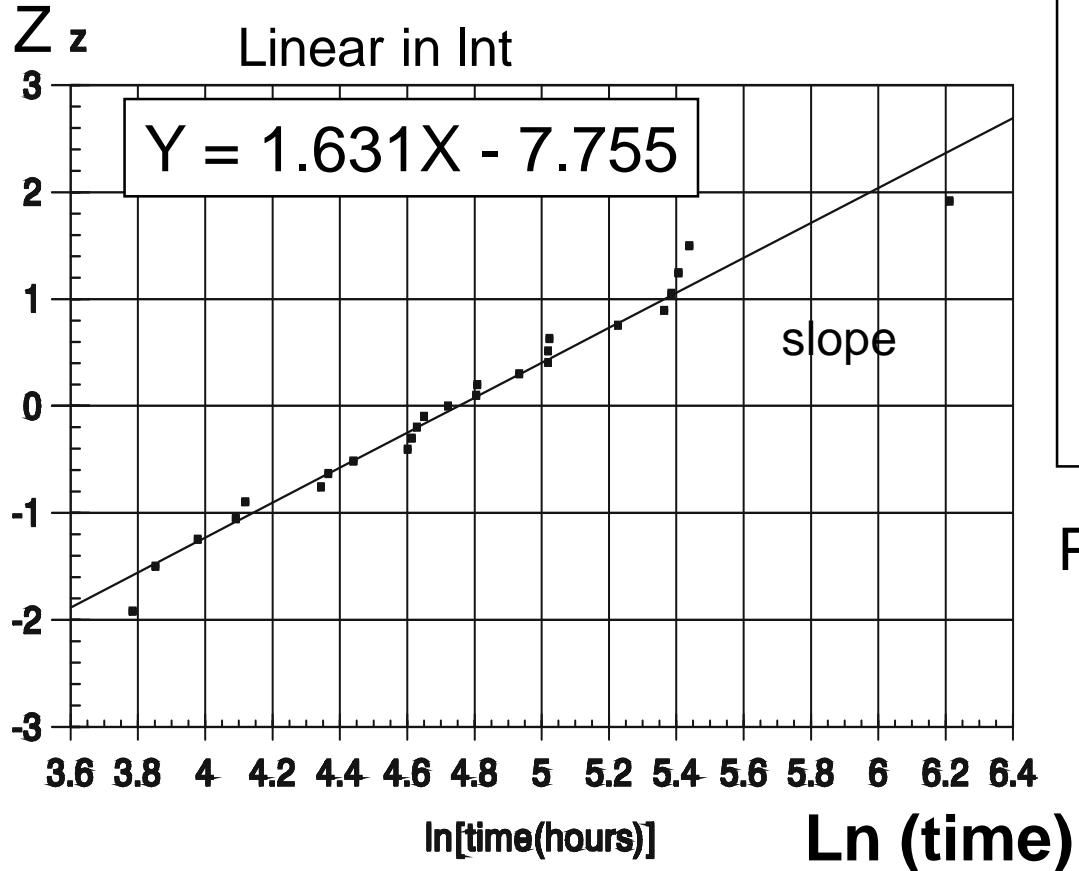
$$F(t_i) = (i - 0.3) / (25 + 0.4)$$

Normal Tables: find z_i from F(t_i)



Lognormal Least-Squares Repair Times

28



INTERCEPT - $a = -7.755$
 SLOPE - $b = 1.631$
 Est. $s = 1/b = 0.613$
 Est. $T_{MED} = e^{-sa} = 116.0$
 Index of Fit = 0.986

Pr of repair completed by $T = t$:

$$P(T \leq t) = H(t) = F\left(\frac{1}{0.613} \ln \frac{t}{116}\right)$$

Empirical Histogram Analysis & Modeling

Procedure for data collection, analysis, and use:

1. Collection of observed time to failure data
2. Analysis of all data for quality (outliers).
3. **Parameter Estimation** using plotting or, Maximum Likelihood Estimate (MLE))
4. Compare observed times with **expected** times using the model with estimated parameters
5. Perform **Goodness-of-Fit** tests: Are the sample data represented adequately by the selected distribution model? (use Chi-Square, A-D, K-S methods etc.). If so, use the data to estimate the parameters of the reliability model.
6. Test the model and update given new data.

Maximum Likelihood (ML) Method

- Used widely in engineering estimation
- For a continuous random variable, X , in the pdf $f(X, \theta)$, with parameters represented by θ .
- For a sample, $x_1, x_2, \dots, x_n = \{x_i\}$
- The ML approach is to provide an optimum estimate of the value of a parameter θ that results in the greatest probability/likelihood of observing the particular sample set, $\{x_i\}$.
- The likelihood function is $L(x_1, x_2, \dots, x_n; \theta) = \prod_{i=1}^n f(x_i, \theta)$ and is the joint pdf of n events considered independent, $\{x_i\}$.
- Method to obtain $q = \hat{q}_0$ (maximum value of the joint pdf):

$$\frac{\frac{\partial L(x_1, x_2, \dots, x_n; q_0)}{\partial q_0}}{\frac{\partial q_0}{\partial q_0}} = 0 \quad \text{or} \quad \frac{\frac{\partial \ln L(x_1, x_2, \dots, x_n; q_0)}{\partial q_0}}{\frac{\partial q_0}{\partial q_0}} = 0$$

Easier to perform

Parameter Estimation: Exponential Distribution



- Units of a component with n empirically observed failures recorded at $t_1 < t_2 < \dots < t_n < t_0$, where t_n is the observed time for n independently observed failures (t_0 is the total time of the test during which the failures were observed).
- If failure times follow the Exponential distribution with constant scale parameter λ , the likelihood function (i.e. the likelihood of λ given the data set of time t) is:

$$\begin{aligned} L(t_1, t_2, \dots; \lambda) &= \prod_{i=1}^n f(t_i; \lambda) = \prod_{i=1}^n \lambda \exp(-\lambda / t_i) = \lambda^n \exp\left(\sum_{i=1}^n -\lambda / t_i\right) \\ &= \lambda^n \exp(-\lambda / t_0) \quad t_0 = \sum_{i=1}^n t_i \end{aligned}$$

λ , parameter; t_0 , total unit time on test

Maximum Likelihood for Estimation of λ

32

- To determine value of λ from a given dataset of t , find the derivative of the Maximum Likelihood (ML)

$$L(t_1, t_2, \dots; \lambda) = /^n \exp(-\lambda / t_0)$$

Finding the ML with $\ln L$ is generally easier than with L

$$\ln L = n(\ln \lambda) - \lambda \sum_{i=1}^n t_i \rightarrow \frac{\partial \ln L}{\partial \lambda} = \frac{n}{\lambda} - \sum_{i=1}^n t_i = 0$$

So, the **Maximum Likelihood Estimate of λ :**

$$\hat{\lambda} = \frac{n}{\sum_{i=1}^n t_i} = \frac{n}{t_0}$$

(n = no of observed failures within t_0)

Recall for $n = 1$ observed failure within t_0 , $MTTF = 1/\lambda$
A similar analysis is applied for any distribution behavior.

4. Determining Expected Values:

Example



- The time to failure data for an electronic unit are shown in the table. Test the hypothesis that the failure data can be modeled acceptably by an Exponential distribution with ROCOF $\lambda = 0.005/\text{hr}$.

TABLE 2.3
Frequency Table

Class Interval	Observed Frequency
Time, hr	# failures
0–100	35
100–200	26
200–300	11
300–400	12
400–500	6
500–600	3
600–700	4
700–800	2
800–900	0
900–1000	1

Number of units in test $N = 100$

N = 100

Exponential Model for Unit Failure

- Using the Exponential model, calculate the expected failure frequencies predicted by the model and compare with the observed frequencies.
- Ex., cumulative failure Pr for interval $0 < T < 100$ hr assuming Exponential model behavior:

$$P(0 < T < 100) = F(100) = \int_0^{100} e^{-\lambda t} dt = [1 - e^{-0.005t}]_0^{100} = 0.393$$

- So number of units expected to fail between $0 < t < 100$ is $0.393 * 100 = 39.3$

4. Observed and Expected Values:

35

TABLE 2.3
Frequency Table

Class Interval Time, hr	Observed Frequency # failures	Expected Frequency # failures
0–100	35	39.3 ← $N \cdot Pr = 100 (0.393)$
100–200	26	23.8 ← $N \cdot Pr = 100 (0.238)$
200–300	11	14.5
300–400	12	8.8
400–500	6	5.3
500–600	3	3.2
600–700	4	2.0
700–800	2	1.2
800–900	0	0.7
900–1000	1	0.4

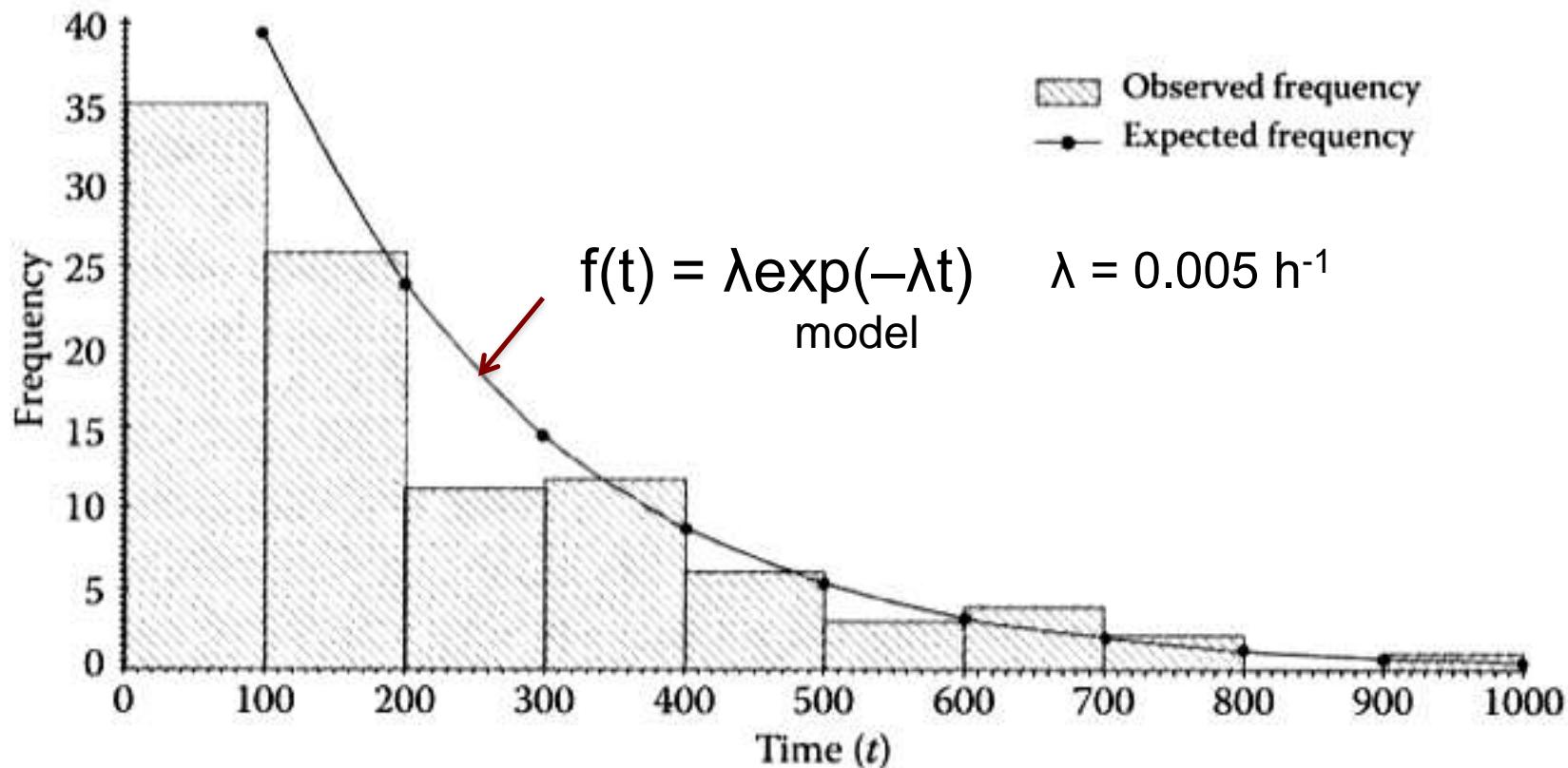
Number of units in test $N = 100$

Pr over t interval

$$N[\int \lambda e^{-\lambda t} dt]$$

Observed and Expected Frequencies for Time to Failure of Electronic Unit

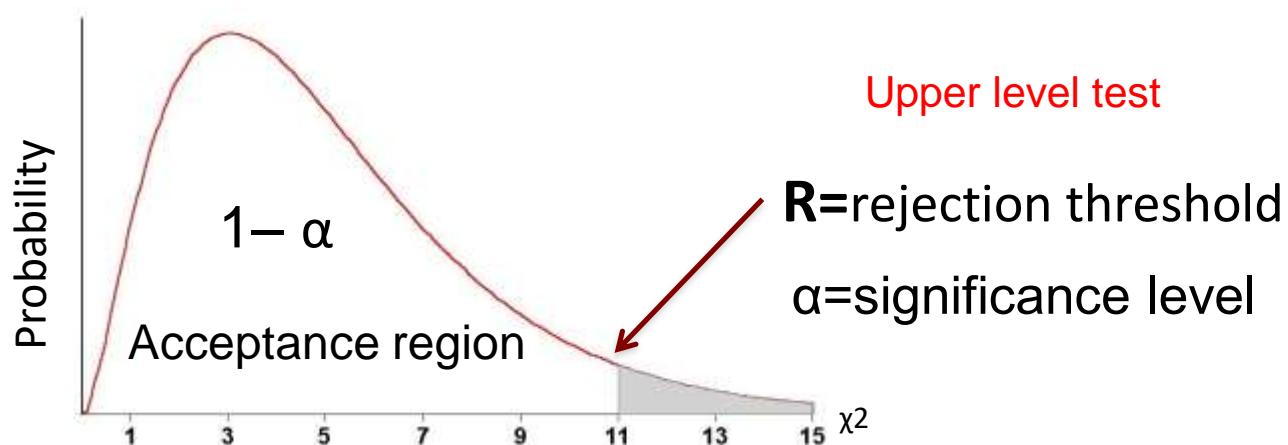
Are the data represented adequately by the Exponential model?
Can we judge the model by only looking at this figure?



How to assess the quality of model fit to the data?

5. Goodness of Fit Test: Chi-Square Distribution

- **Chi-Square Test:** a test applied to frequency data using the χ^2 distribution. χ^2 statistic approximately follows a the χ^2 distribution
- It is a Gamma distribution with shape parameter $\beta = 2$, scale parameter $\alpha = n/2$, where n = degrees of freedom (df), which is the number of independent variables that are free to vary. So for each df, there is a separate χ^2 distribution.
- $df = (\text{number of intervals, } k) - (\text{number of parameters, } m) - 1$



If $W > R$ (χ^2_c), reject the hypothesized distribution.

Chi-Square Distribution

- **Decision rule for upper test:** Reject null hypothesis H_0 if $\chi^2 > \chi^2_c$,
 c = critical value based on α for an upper test
- **Goodness-of-fit procedure:** Determine whether an obtained distribution fits a hypothesized distribution model

$$W = \chi^2 = \sum_{i=1}^k \frac{(\text{observed} - \text{expected})_i^2}{\text{expected}_i}$$

- **W is the value of the χ^2 statistic:** If the observed values differ considerably from the expected values, W will be large and the fit will be considered poor.
- **If $W > R$ (where $R = \chi^2_c$), reject the hypothesized distribution.**
- Otherwise do not reject (chances are the observed data matches the hypothesized distribution)

Degrees of Freedom	Area to the Right of Critical Value									
	0.995	0.99	0.975	0.95	0.90	0.10	0.05	0.025	0.01	0.005
1	—	—	0.001	0.004	0.016	2.706	3.841	5.024	6.635	7.879
2	0.010	0.020	0.051	0.103	0.211	4.605	5.991	7.378	9.210	10.597
3	0.072	0.115	0.216	0.352	0.584	6.251	7.815	9.348	11.345	12.838
4	0.207	0.297	0.484	0.711	1.064	7.779	9.488	11.143	13.277	14.860
5	0.412	0.554	0.831	1.145	1.610	9.236	11.071	12.833	15.086	16.750
6	0.676	0.872	1.237	1.635	2.204	10.645	12.592	14.449	16.812	18.548
7	0.989	1.239	1.690	2.167	2.833	12.017	14.067	16.013	18.475	20.278
8	1.344	1.646	2.180	2.733	3.490	13.362	15.507	17.535	20.090	21.955
9	1.735	2.088	2.700	3.225	4.168	14.684	16.919	19.023	21.666	23.589
10	2.156	2.558	3.247	3.940	4.865	15.987	18.307	20.483	23.209	25.188
11	2.603	3.051	3.816	4.575	5.578	17.275	19.675	21.920	24.725	26.757
12	3.074	3.571	4.404	5.226	6.304	18.549	21.026	23.337	26.217	28.299
13	3.565	4.107	5.009	5.892	7.042	19.812	22.362	24.736	27.688	29.819
14	4.075	4.660	5.629	6.571	7.790	21.064	23.685	26.119	29.141	31.319
15	4.601	5.229	6.262	7.261	8.547	22.307	24.996	27.488	30.578	32.801
16	5.142	5.812	6.908	7.962	9.312	23.542	26.296	28.845	32.000	34.267
17	5.697	6.408	7.564	8.672	10.085	24.769	27.587	30.191	33.409	35.718
18	6.265	7.015	8.231	9.390	10.865	25.989	28.869	31.526	34.805	37.156
19	6.844	7.633	8.907	10.117	11.651	27.204	30.144	32.852	36.191	38.582
20	7.434	8.260	9.591	10.851	12.443	28.412	31.410	34.170	37.566	39.997
21	8.034	8.897	10.283	11.591	13.240	29.615	32.671	35.479	38.932	41.401
22	8.643	9.542	10.982	12.338	14.042	30.813	33.924	36.781	40.289	42.796
23	9.260	10.196	11.689	13.091	14.848	32.007	35.172	38.076	41.638	44.181
24	9.886	10.856	12.401	13.848	15.659	33.196	36.415	39.364	42.980	45.559
25	10.520	11.524	13.120	14.611	16.473	34.382	37.652	40.646	44.314	46.928
26	11.160	12.198	13.844	15.379	17.292	35.563	38.885	41.923	45.642	48.290
27	11.808	12.879	14.573	16.151	18.114	36.741	40.113	43.194	46.963	49.645
28	12.461	13.565	15.308	16.928	18.939	37.916	41.337	44.461	48.278	50.993
29	13.121	14.257	16.047	17.708	19.768	39.087	42.557	45.722	49.588	52.336
30	13.787	14.954	16.791	18.493	20.599	40.256	43.773	46.979	50.892	53.672
40	20.707	22.164	24.433	26.509	29.051	51.805	55.758	59.342	63.691	66.766
50	27.991	29.707	32.357	34.764	37.689	63.167	67.505	71.420	76.154	79.490
60	35.534	37.485	40.482	43.188	46.459	74.397	79.082	83.298	88.379	91.952
70	43.275	45.442	48.758	51.739	55.329	85.527	90.531	95.023	100.425	104.215
80	51.172	53.540	57.153	60.391	64.278	96.578	101.879	106.629	112.329	116.321
90	59.196	61.754	65.647	69.126	73.291	107.565	113.145	118.136	124.116	128.299
100	67.328	70.065	74.222	77.929	82.358	118.498	124.342	129.561	135.807	140.169

Get the value of R from this table using values corresponding to α and df

Summary: Chi-Square Test Steps



df, degrees of freedom = k-m-1

- 1. Hypothesize a distribution H_0 to represent the data.
- 2. Set the significance level of the test = α . Select an upper test or an upper and lower test.
- 3. For an upper test, state the rejection region threshold $R > \chi^2_{1-\alpha}(k-m-1)$, where k = no. of intervals, m = no. of parameters calculated from the sample, $(k-m-1)$ = degrees of freedom (df) for the specific $\chi^2_{1-\alpha}(df)$ distribution. (IRME, Tab A.3, p. 521)
- 4. Calculate $\chi^2_{1-\alpha}(df) = W = C^2 = \sum_{i=1}^k \frac{(O_i - E_i)^2}{E_i}$
- If $W > R$, reject H_0 ; otherwise do not reject H_0 (H_0 is the hypothesized distribution).

χ^2 Example 1: Poisson model goodness-of-fit

41

The number of parts ordered per week by a maintenance department in a manufacturing plant is believed to follow a Poisson distribution. Use a χ^2 goodness-of-fit test to determine the adequacy of the Poisson distribution. Use the data found in the following table:

Number of Parts per Week (x)	Observed Frequency (o_i)	Expected Frequency (e_i)	χ^2 Statistic $((o_i - e_i)^2/e_i)$
0	18	15.783	0.311
1	18	18.818	0.036
2	8	11.219	0.923
3	5	4.459	0.066
4	2	1.329	0.339
5	1	0.317	1.472
Total	52	52	3.147 ← W

↑
Number of spare parts ordered in a week (x)

Number of weeks when x number of spare parts were ordered

$$\text{Total number of spare parts ordered over 52 weeks} = (18 \times 0) + (18 \times 1) + (8 \times 2) + (5 \times 3) + (2 \times 4) + (1 \times 5) = 62$$

How to calculate expected frequency (e_i)

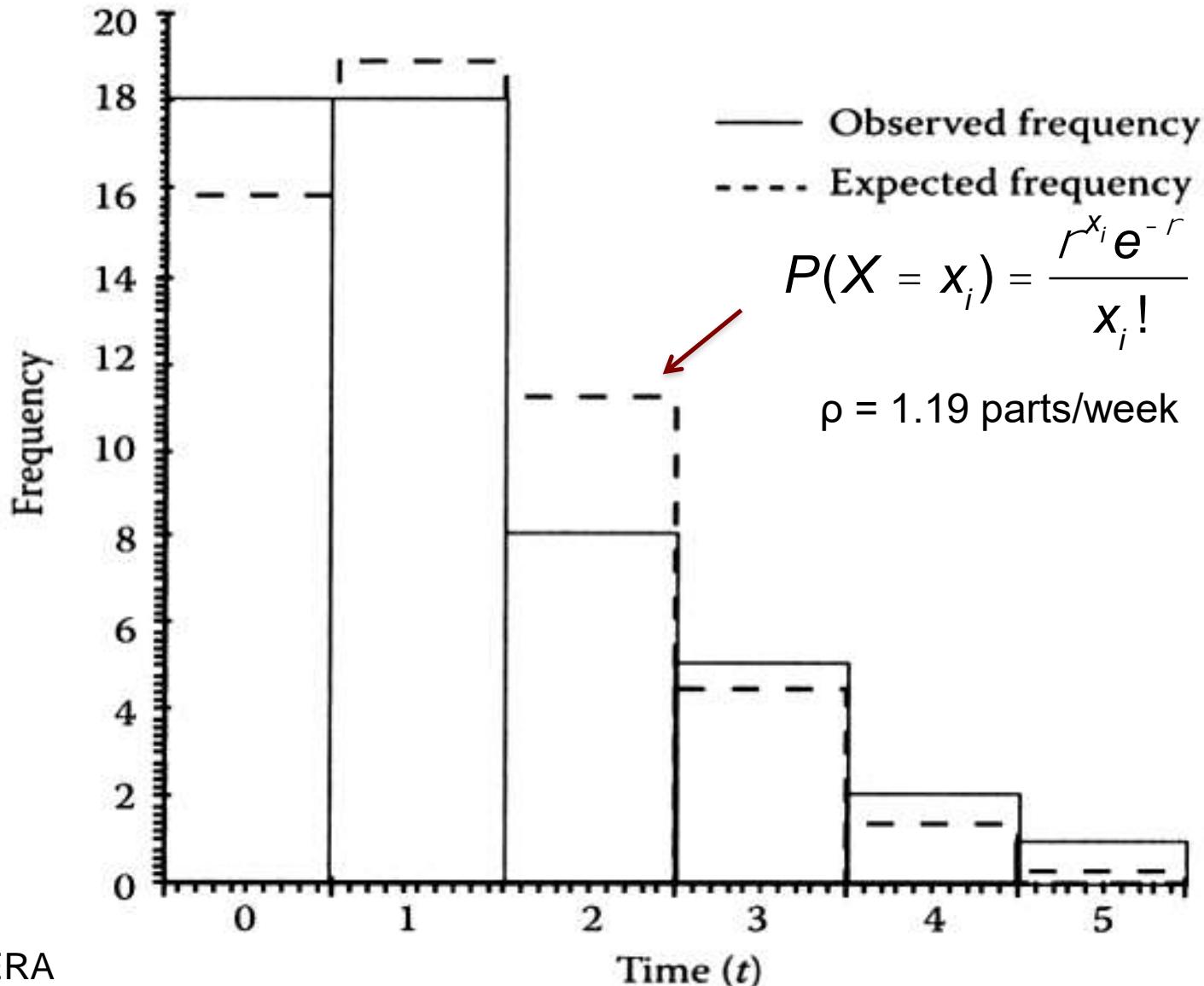
42

- Total number of parts ordered over 52 weeks= 62.
So, $\lambda=62 \text{ parts}/52 \text{ weeks}$
- Poisson parameter, $\rho = \lambda t = (62 \text{ parts}/52 \text{ weeks}) * 1 \text{ year} = 1.19$
- Calculate $P(n = x) = \frac{r^x e^{-r}}{x!}$ for each value of x.
 - *For example:* $P(X = 0) = P(0) = e^{-1.19} = 0.304$
- Expected Frequency (e_i)= $N * P$, where $N= 52 \text{ weeks}$.
 - *For example:* for $X = 0$, $e_i = 52 * e^{-1.19} = 52 * 0.304 = 15.783 \text{ weeks}$
- Other frequencies are predicted identically

Observed and Expected Parts Frequencies

Use the chi-square test to judge the Poisson model.

43



Reject/Do Not Reject Hypothesis

- One parameter (ρ) was estimated ($m = 1$). Poisson is a single parameter distribution.
- 6 intervals/sets of data (0,1,2,3,4,5) were used ($k=6$)
- $df = k-m-1 = 6-1-1 = 4$
- With significance level of $\alpha = 0.05$, $R = \chi^2_{0.95}(4) = 9.49$
- $W=3.147$ (Slide 15)
- Thus, $R > W$. So at the 0.05 significance level, **do not reject** the Poisson as an acceptable model to represent the data.

χ^2 Example 2:

Car Mileage to Test Normal Distribution, H_0

45

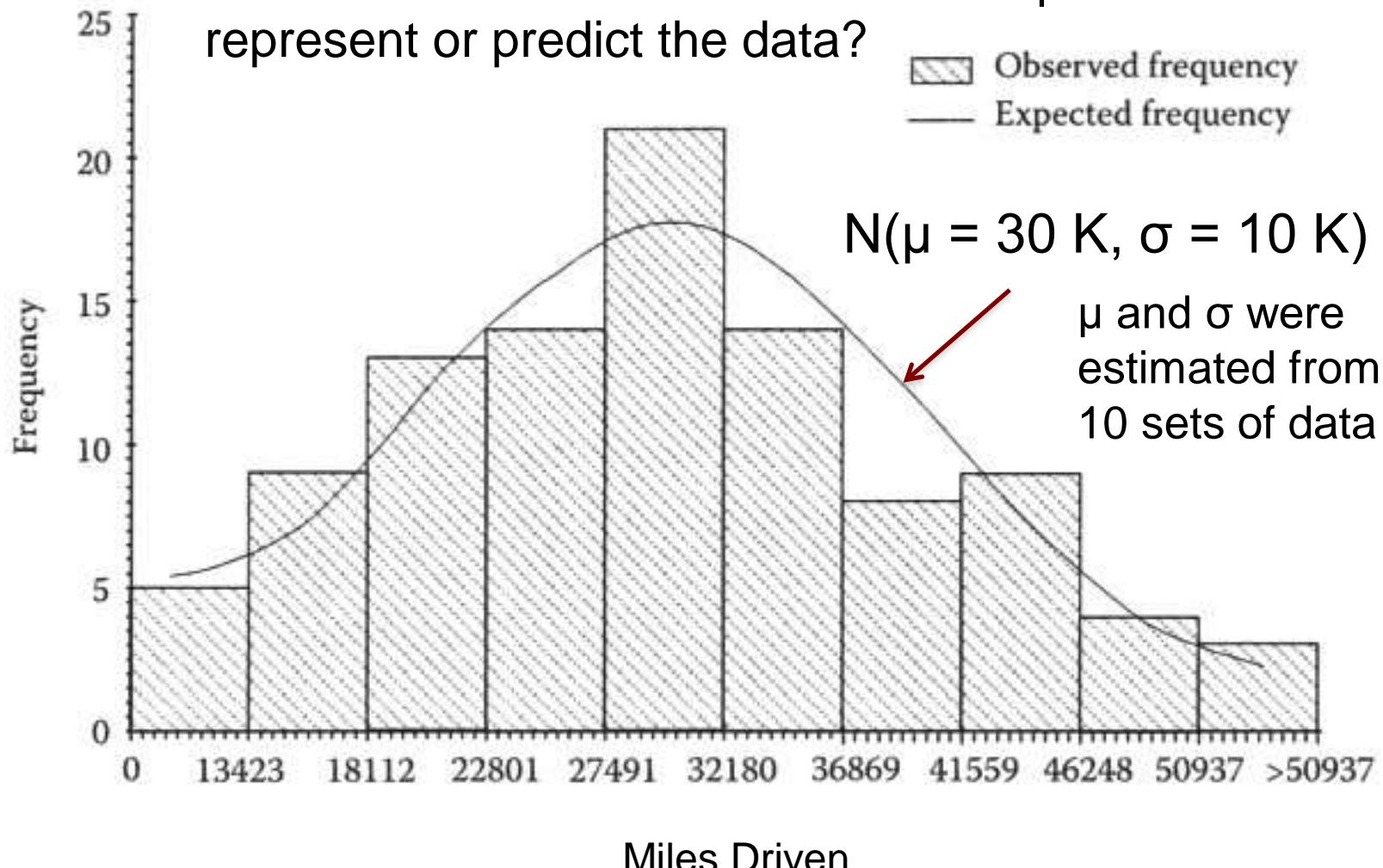
- Data for the accumulated mileage of 100 automobiles after 2 years in service are collected and grouped. The mileage pattern is believed to follow a normal distribution with $\mu = 30 \text{ K}$, $\sigma = 10 \text{ K}$. Use the χ^2 test to check the hypothesis at the 0.05 significance level.

Grouped Data		Frequency (o_i)	Expected Frequency (e_i)	χ^2 Statistic $((o_i - e_i)^2/e_i)$
Interval Start	End			
0	13,417	5	5.7	0.0368
13,417	18,104	9	7.1245	0.4937
18,104	22,791	13	11.7500	0.1330
22,791	27,478	14	15.9143	0.2303
27,478	32,165	20	17.7014	0.2985
32,165	36,852	15	16.1699	0.0846
36,852	41,539	8	12.1305	1.4064
41,539	46,226	9	7.4733	0.3119
46,226	>46,226	7	6.2882	0.0806
Total		100	100.0000	W= 3.0758

Observed and Expected Car Mileage Frequencies

46

Is the Normal distribution model acceptable to represent or predict the data?



Our senses are biased (eyeballing the curve)

Car Miles Test of Normal Distribution Summary

- (Normal distribution parameters μ and σ can also be estimated from the provided data: $\mu = 30,011$ miles; $\sigma = 10,472$ miles)
- Using $z = \frac{x - \bar{m}}{s}$, expected frequencies were predicted as $100 * \Phi(z)$.
- Degrees of freedom: Normal distribution has two parameters (μ, σ), so, $m = 2$. There were 9 data sets, so, $k = 9$. Thus $df = k-m-1 = 9-2-1 = 6$
- For significance level $\alpha = 0.05$, the rejection threshold, $R = \chi^2_{0.95}(6) = 12.59 > 3.08 = W$
- So accept H_0 at the 0.05 significance level that the Normal distribution is not rejected as an acceptable model for these data.

χ^2 Example 3: System Failure Poisson Model Test

- Perform an upper test at the $1 - \alpha = 0.95$ confidence level of the Poisson distribution model to represent data for the number of system failures during 50 days.
- Poisson parameter $\rho = 45 \text{ failures}/50 \text{ days} = 0.9 = \text{mean}$

Expected frequency = (50 day) [Pr(x failures/day)]

$$= 50 \frac{r^x e^{-r}}{x!}, \quad x = 0, 1, 2, 3, 4$$

x	Observed failures	Pr(x) failures/day	Expected failures/day	Error: $\frac{(o_i - e_i)^2}{e_i}$	$W = \sum_{i=1}^k \frac{(o_i - e_i)^2}{e_i}$
0	21	0.41	20.33	0.022	
1	18	0.37	18.30	0.0049	
2	7	0.16	8.23	0.184	
3	3	0.05	2.47	0.114	
4	1	0.01	0.56	0.346	
Total = 50 days			Total = 0.6709	= W<R?	48

System Failure Poisson Model Test

49

$$W = C^2 = \sum_{i=1}^5 \frac{(obs - exp)_i^2}{expected_i} = 0.671$$

Note that ρ is obtained from the 5 data sets, so $m = 1$, and $k = 5$.

- $\chi^2_{1-\alpha}(k-m-1) = \chi^2_{0.95}(5-1-1) = \chi^2_{0.95}(3) = 7.81$
- $W \sim 0.67 < 7.81 = R$, rejection threshold, so the Poisson distribution as the H_0 model is **not rejected**.

- The K-S Test works with data from individual components rather than clustering the components into discrete intervals.
- Similar to the χ^2 test, an empirical distribution, $S(t)$, (here cdf in contrast to the pdf used in χ^2) is compared to a hypothesized cdf, $F(t)$, to test whether the data are sufficiently well represented by $F(t)$.
- χ^2 sometimes lacks sufficient data in each interval. This is not a problem with **K-S** by working with all data together in a cumulative distribution.

Kolmogorov-Smirnov (K–S) Test

- An empirical cdf, $S(t)$, is defined for an ordered sample, $t_1 < t_2 < \dots < t_n$

$$S_n(t) = \begin{cases} 0, & -\infty < t < t_1 \\ \frac{i}{n}, & t_i \leq t \leq t_{i+1} \\ 1, & t_n \leq t \leq \infty \end{cases}$$

- The K–S Statistic is a measure of the **maximum difference** between the empirical data $S_n(t)$ and $F(t)$, which is the proposed cdf model:

$$K - S = \max_i [|F(t_i) - S_n(t_i)|, |F(t_i) - S_n(t_{i-1})|]$$

$n \setminus \alpha$	0.001	0.01	0.02	0.05	0.1	0.15	0.2
1		0.99500	0.99000	0.97500	0.95000	0.92500	0.90000
2	0.97764	0.92930	0.90000	0.84189	0.77639	0.72614	0.68377
3	0.92063	0.82900	0.78456	0.70760	0.63604	0.59582	0.56481
4	0.85046	0.73421	0.68887	0.62394	0.56522	0.52476	0.49265
5	0.78137	0.66855	0.62718	0.56327	0.50945	0.47439	0.44697
6	0.72479	0.61660	0.57741	0.51926	0.46799	0.43526	0.41035
7	0.67930	0.57580	0.53844	0.48343	0.43607	0.40497	0.38145
8	0.64098	0.54180	0.50654	0.45427	0.40962	0.38062	0.35828
9	0.60846	0.51330	0.47960	0.43001	0.38746	0.36006	0.33907
10	0.58042	0.48895	0.45662	0.40925	0.36866	0.34250	0.32257
11	0.55588	0.46770	0.43670	0.39122	0.35242	0.32734	0.30826
12	0.53422	0.44905	0.41918	0.37543	0.33815	0.31408	0.29573
13	0.51490	0.43246	0.40362	0.36143	0.32548	0.30233	0.28466
14	0.49753	0.41760	0.38970	0.34890	0.31417	0.29181	0.27477
15	0.48182	0.40420	0.37713	0.33760	0.30397	0.28233	0.26585
16	0.46750	0.39200	0.36571	0.32733	0.29471	0.27372	0.25774
17	0.45440	0.38085	0.35528	0.31796	0.28627	0.26587	0.25035
18	0.44234	0.37063	0.34569	0.30936	0.27851	0.25867	0.24356
19	0.43119	0.36116	0.33685	0.30142	0.27135	0.25202	0.23731
20	0.42085	0.35240	0.32866	0.29407	0.26473	0.24587	0.23152
25	0.37843	0.31656	0.30349	0.26404	0.23767	0.22074	0.20786
30	0.34672	0.28988	0.27704	0.24170	0.21756	0.20207	0.19029
35	0.32187	0.26898	0.25649	0.22424	0.20184	0.18748	0.17655
40	0.30169	0.25188	0.23993	0.21017	0.18939	0.17610	0.16601
45	0.28482	0.23780	0.22621	0.19842	0.17881	0.16626	0.15673
50	0.27051	0.22585	0.21460	0.18845	0.16982	0.15790	0.14886
OVER 50	1.94947	1.62762	1.51743	1.35810	1.22385	1.13795	1.07275
	\sqrt{n}						

Get the K-S statistics value from this table using values corresponding to α and df D

Kolmogorov-Smirnov (K–S) Test



- Steps to apply the K–S model are:
 - 1. Select a hypothesized cdf, $F(t)$ to represent the sample data.
 - 2. Select a specific significance level, α , for the test.
 - 3. Calculate the K–S statistic
 - 4. For the particular distribution model, find the rejection region (critical value), $R > D_n(\alpha)$, where $n =$ number of trials, from Tab A.4 in Modarres RERA.
 - 5. If K–S statistic $> D_n(\alpha)$, reject the hypothesized distribution that does not acceptably represent the observed data. Otherwise do not reject the hypothesized model.

Exponential Failure of Electronic Device

- Time to failure of an electronic device is measured in a life test. The failure times are 254, 586, 809, 862, 1381, 1923, 2542, and 4211 h. Is the exponential distribution with $\lambda = 5 \times 10^{-4}$ an adequate representation of this sample?

For an exponential distribution with $\lambda = 5 \times 10^{-4}$, we obtain $F_n(t) = 1 - \exp(-5 \times 10^{-4}t)$. For $\alpha = 0.05$, $D_8(0.05) = 0.457$. Thus, the rejection area is $R > 0.457$.

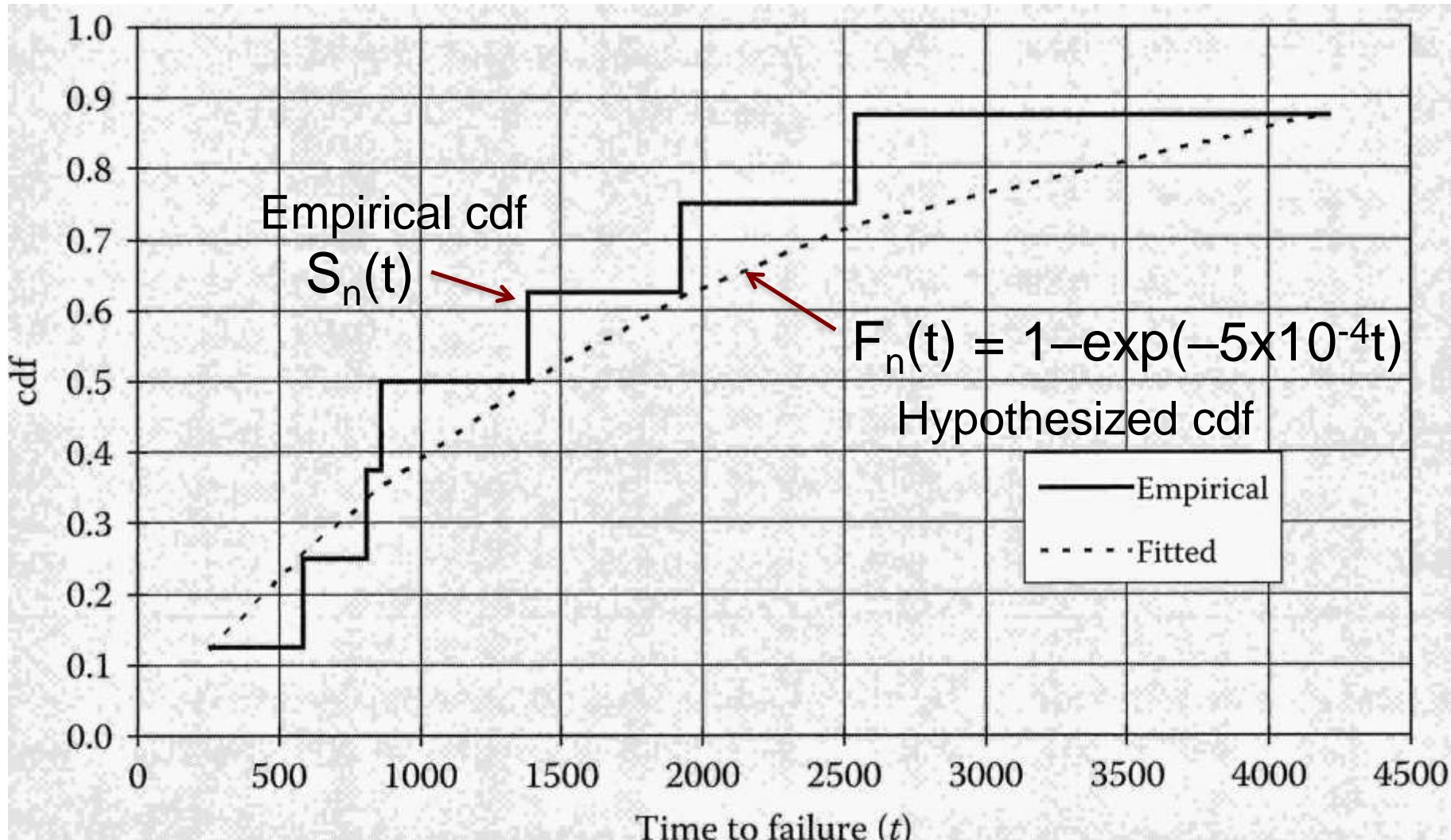
Time to Failure (t)	i	Empirical cdf		$(F_n(t_i))$	$K - S$ Statistic	
		$S_n(t_i)$	$S_n(t_{i-1})$		$ F_n(t_i) - S_n(t_i) $	$ F_n(t_i) - S_n(t_{i-1}) $
254	1	0.125	0.000	0.119	0.006	0.119
586	2	0.250	0.125	0.254	0.004	0.129
809	3	0.375	0.250	0.333	0.042	0.083
862	4	0.500	0.375	0.350	0.150	0.025
1381	5	0.625	0.500	0.499	0.126	0.001
1923	6	0.750	0.625	0.618	0.132	0.007
2542	7	0.875	0.750	0.719	0.156	0.031
4211	8	1.000	0.875	0.878	0.122	0.003

Max.

Since $K - S = 0.156 < 0.454$, we should not reject the hypothesized exponential distribution model (Figure 2.15).

K-S Test of Electronic Unit Data

55



Anderson-Darling (A-D) Test

- CDFs are relatively flat at the tails, so the maximum deviation in the K-S test will rarely occur in the tails. Also in a Chi-Square test, the frequencies in the tails must be grouped together.
- So neither the K-S, or the Chi-Square test will reveal discrepancies between the empirical and theoretical frequencies in the tails of a proposed distribution.
- The A-D test statistic is expressed in terms of the **logarithm of the probabilities**, so it is much more **sensitive to data within the tails of a distribution**.

Maintainability of Repairable Components

Unit 16

Spring 2022

References

- Ebeling, C.E., An Introduction to Reliability and Maintainability Engineering, 3rd ed., Waveland Press, 2019 (Ebeling, IRME), Chapter 9, Maintainability;
- M. Modarres, M. Kaminskiy, and V. Krivtsov, *Reliability Engineering and Risk Analysis*, 2nd ed, Taylor & Francis, 2010 (Modarres, RERA)
- Modarres, M., *Risk Analysis in Engineering*, Taylor&Francis, 2006 (Modarres, RAE)
- Modarres, M., *Reliability Engineering and Risk Analysis in Engineering*, Marcel Dekker, 1999 (Modarres, RE)
- Sivia, D.S., *Data Analysis A Bayesian Tutorial*, Oxford, 1996
- Tweeddale, M., *Managing Risk and Reliability of Process Plants*, Elsevier Science, 2003 (Tweeddale, 2003)

Maintainability: Maintenance Types

- Common methods:
 - Corrective (reactive/run-to-failure) maintenance
 - Preventive (scheduled) maintenance
 - Predictive (condition-based) Maintenance
 - Reliability-Centered Maintenance

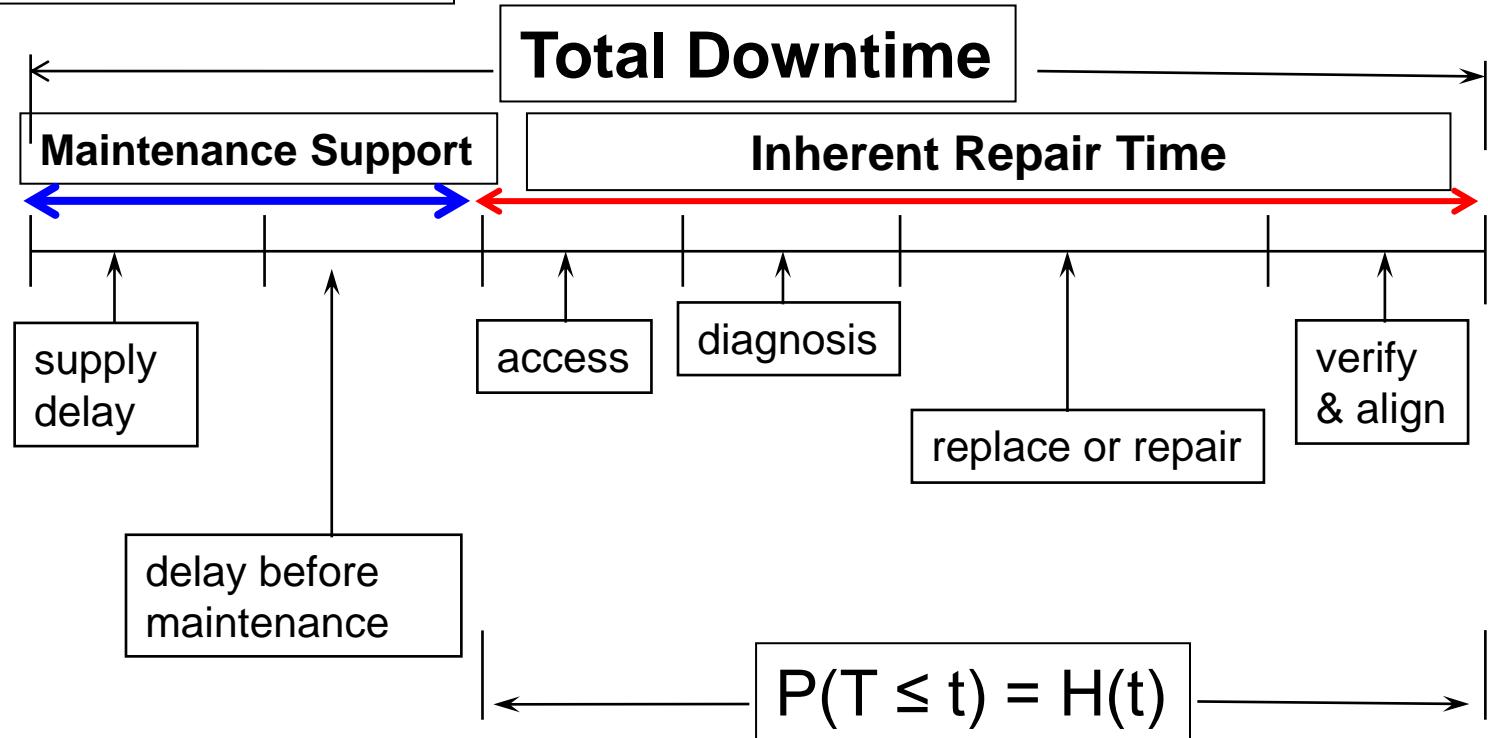
Maintainability: Repairability

- Failed components are either Replaced by new components or they are Repaired.
- **Non-Repairable** components are those that must be Replaced following failure.
- For **Repairable** component in a failed state, it has to be restored to an operating condition. The analysis of its downtime is needed for Maintenance Decision Making.
- The time required to Restore or Repair a failed component is a measure of its Maintainability.
- **Renewal Process**: Systems or components restored to “as good as new” condition
- **Minimal Repair** : System or component undergoes partial restoration to a condition that is below Renewal (as good as old, same as old)
- **Imperfect Repair**: System restored to condition that is between ‘as-good-as-new’ and ‘as-good-as-old’

Downtime of Repairable Components

Organizational Factors:

resources, training, SAD delays



Maintainability is measured by the Repair distribution pdf, $h(t)$, repair rate, and $H(t)$ cdf, which represents the cumulative Pr that a repair will be completed by time $T = t$. The Mean Time to Repair (MTTR) is the mean of the Maintainability distribution.

Repairable Components

- Once a failure of a repairable component occurs, then the repair downtime of the component consists of the activities shown in the previous slide.
- Usually the times of excessive delays for repair resources (maintenance delay) and replacement parts (supply delay) are not considered part of **the *Inherent Repair Time*** of the component. They are, however, influenced by Human and Organizational Factors, and they are measures of Organizational Resilience. In a High Resilience Organization, excessive Supply and Administrative Delays (SAD) are near zero.
- Lesser time for maintenance, repair and SAD is desired to ensure the equipment is more available to perform its function.

Downtime: Organization and Human Factors

- **Supply and Administrative Delays, SAD:** Excessive delay to obtain spare parts (administrative delay time, production time, procurement lead time, transportation time). With effective management and ample stored parts, excessive delay can be near 0
- **Maintenance delays:** time for maintenance resources (personnel, test equipment, tools, manuals, technical information), personnel training or facilities (repair station, test stand) to get ready for repair. Influenced by Human & Organizational factors.
- **Repair time:** access to unit, diagnosis, replacement, repair, verification, alignment. Requires training/retraining, procedures, human reliability
- **Downtime \bar{M}** = Mean or Expected Downtime following failure,

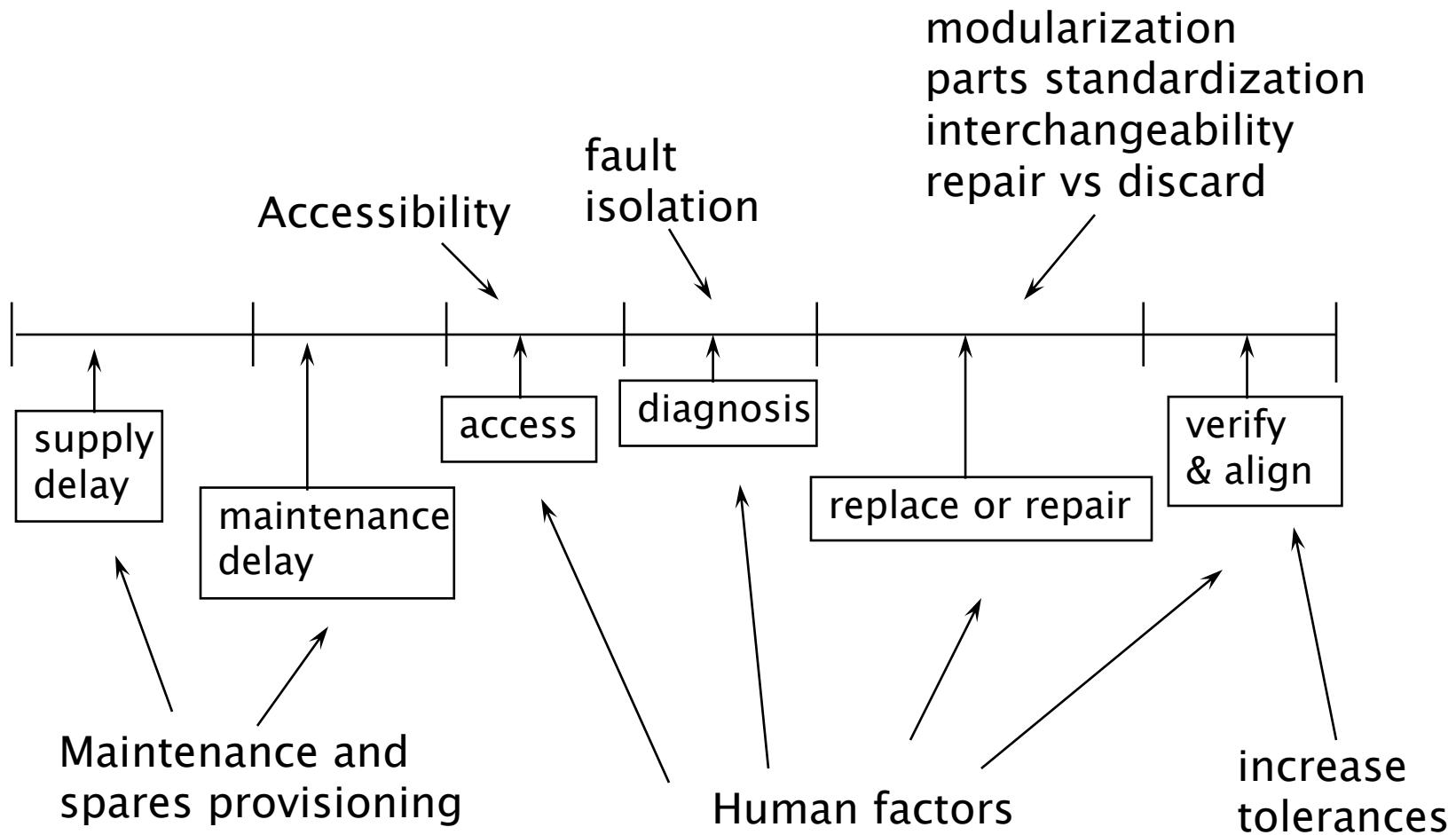
$$\bar{M} = MTTR + SAD$$

- **Unavailability Q_m** : Failure Pr due to \bar{M} .

$$Q_m = \frac{\bar{M}}{t_m}$$

where Q_m is Unavailability due to maintenance and t_m is sum of all contributions to mission time.

Design Methods to Reduce Down Time



Normal vs. Excessive Delays, SAD

Design for Maintainability

Human Factor Considerations:

- Controls
 - Displays
 - Tool and Equipment Design
 - Workplace
 - Environment
 - Organizational Climate
 - Universal Human Ethic
- } Operator Equipment Interface



The Coffee is terrible.
I can't work here!

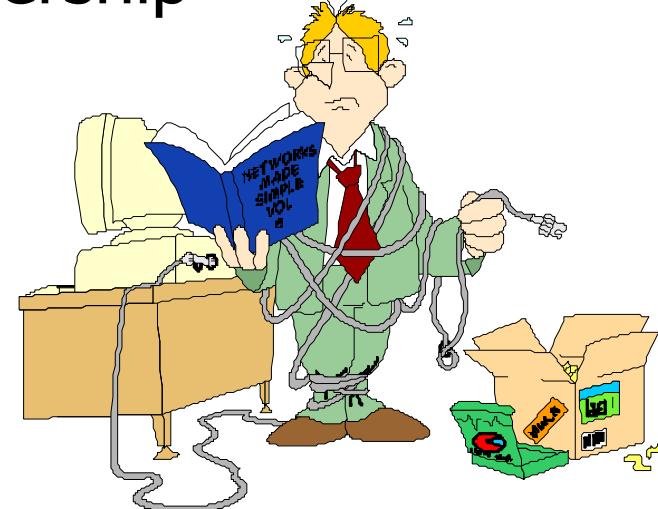
Working Environment: Work Conditions, Performance Shaping Factors, PSF

- Noise
 - OSHA limit of 85 db; pain at 130 db
- Illumination
 - 50 foot-candles for dials, gauges, and meters
- Vibration
 - Exposure limits depends on frequency, amplitude, and duration
- Ambient Air
 - Temperature (55^0 to 75^0 F.)
 - Humidity



Causes of Excessive Human Error

- Poor training and low skill levels
- Inadequate maintenance procedures
- Inadequate supervision and leadership
- Poor working environment
- Improper or lack of motivation



Human Reliability

Human Reliability:

$$R_h = 1 - e/n$$

n = number of tasks

e = number of unsuccessful completions

<u>Task</u>	<u>Relative Frequency, e/n</u>	
read 5 letter word incorrectly	.0003	
read digital display wrongly	.001	
leave light on	.003	
select wrong switch among similar	.005	
read 10 digit number incorrectly	.006	
mate a connector wrongly	.01	
wrong selection –vending machine	.02	
dial 10 digits incorrectly	.06	
fail to check hardware unless specified	.1	
fail to notice wrong position of valves	.5	

Example
frequencies are
highly
dependent on
conditions

The Repair-Time Distribution

Let T = time to repair a failed unit.

Then the CDF (the cumulative probability) that the repair is completed in time $T \leq t$, is expressed by:

$$P(T \leq t) = H(t) = \int_0^t h(t) dt$$

$\sim F(t) \quad t \sim f(t)$

} Probability that repair is completed within time t

$$MTTR = \int_0^\infty t h(t) dt = \int_0^\infty [1 - H(t)] dt$$

where MTTR is the mean of the repair distribution, $h(t)$.

$1 - H(t) = P(T > t)$ is the probability that the repair is completed for $T > t$

$$\text{Variance for repair completion: } s^2 = \int_0^\infty (t - MTTR)^2 h(t) dt$$

Repair Distribution Example

Given $h(t) = 0.083 t$, defined for the interval $1 \leq t \leq 5$ hr, the probability that the repair is completed within a required time interval t is:

$$H(t) = \int_1^t 0.083t dt = 0.04167t^2 - 0.04167$$

Example: $P\{T \leq 3\} = H(3) = 0.04167 \times 9 - 0.04167 = 0.33$.

This is the Pr that the repair is completed in $T \leq 3$ hr or within 3 hours.

Then, $P\{T > 3\} = 1 - 0.33 = 0.67$ is probability that repair takes more than 3 hours.

The mean time to repair is:

$$MTTR = \int_1^5 t h(t) dt = \int_1^5 0.08333t^2 dt = \frac{0.08333t^3}{3} \Big|_1^5 = 3.44 \text{ hrs}$$

over all applicable t

Review: Exponential Repair Behavior, λ , r Constant

Failure: $f(t) = \lambda e^{-\lambda t} = \frac{1}{MTTF} e^{-t/MTTF}$, pdf of failure rate, λ

Repair: $h(t) = r e^{-rt} = \frac{1}{MTTR} e^{-t/MTTR}$, pdf of repair rate, r

$$H(t) = \int_0^t \frac{e^{-\frac{t'}{MTTR}}}{MTTR} dt' = 1 - e^{-\frac{t}{MTTR}}$$

cdf for repair

Let $r = 1/MTTR$, the constant rate of occurrence of repair, then

$$H(t) = \int_0^t r e^{-rt'} dt' = 1 - e^{-rt}$$

r is the constant
repair rate

Student Exercise: Exponential Repair Times

A component can be repaired at the constant rate of 10 units per 8 hour day ($r=10/8\text{hr} = 1.25/\text{hr}$). Calculate first the MTTR using the single parameter of the repair distribution expected to follow Exponential behavior. What is the probability of a single repair exceeding one hour?

Solution:

$$\text{MTTR} = 8 \text{ hr}/(10 \text{ units}) = 0.8 \text{ hr} = 1/r = 1/(1.25/\text{hr}).$$

$P(T \leq 1) = H(t = 1)$, the cumulative Pr of repair within 1 hr

$$\text{So, } P(T > 1) = 1 - H(1) = 1 - (1 - e^{-1/0.8}) = e^{-1.25} = 0.29$$

Note the Exponential used as a Repair Distribution:

$$r = 1/\text{MTTR} \text{ and } \lambda = 1/\text{MTTF}.$$

Lognormal Repair Times

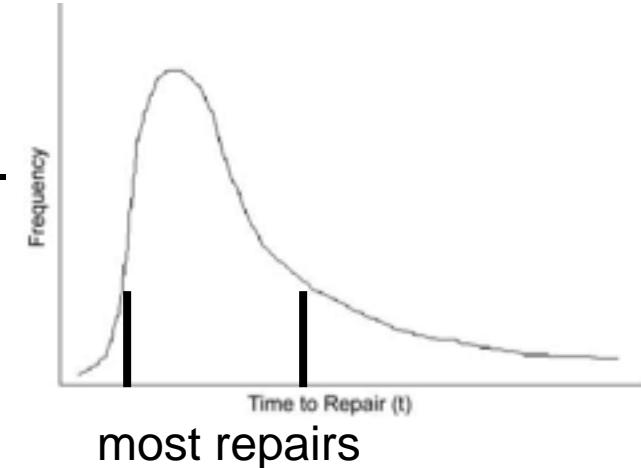
$$h(t) = \frac{1}{\sqrt{2\pi} t s} e^{-\frac{1}{2} \left(\ln \frac{t}{t_{\text{med}}} \right)^2}, \quad t \geq 0$$

Repair within t : Z_t

$$P\{T \leq t\} = H(t) = F\left(\frac{\ln t - \ln t_{\text{med}}}{s}\right) = F\left(\frac{1}{s} \ln \frac{t}{t_{\text{med}}}\right).$$

$$\text{MTTR} = t_{\text{med}} e^{\frac{1}{2}s^2}$$

$$\text{Variance: } t_{\text{med}}^2 e^{s^2} [e^{s^2} - 1]$$



Lognormal repair times are often observed in practice, because the long tail for increasingly higher repair rates at decreasing probabilities results in skewing the distribution to lower repair rates with a tail to long repair times. Analyzing Lognormal repair times makes use of the underlying Normal distribution in the same manner as in analyzing Lognormal failure times.

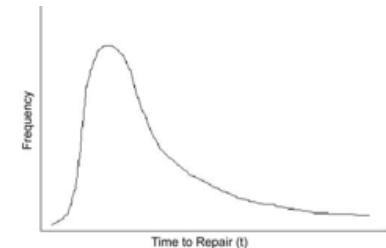
Lognormal Repair Times

A requirement exists for customer's engine fuel pump to be repaired (or replaced) within $t = 3$ hours 90% of the time. If the repair distribution is Lognormal with shape parameter $s = 0.45$, what MTTR must be achieved to meet this goal?

$$Z_t = \Phi\left(\frac{1}{0.45} \ln \frac{3}{t_{\text{med}}}\right) = 0.90$$

$$\frac{1}{0.45} \ln \frac{3}{t_{\text{med}}} = F^{-1}(0.90) = 1.28$$

$$t_{\text{med}} = \frac{3}{e^{1.28(0.45)}} = 1.686 \text{ hr}$$



$$\text{MTTR} = t_{\text{med}} e^{s^2/2} = 1.686 e^{(0.45)^2/2} = 1.87 \text{ hr}$$

$$t_{\text{MODE}} = \frac{t_{\text{med}}}{e^{s^2}} = \frac{1.686}{e^{(0.45)^2}} = 1.38 \text{ hr}$$

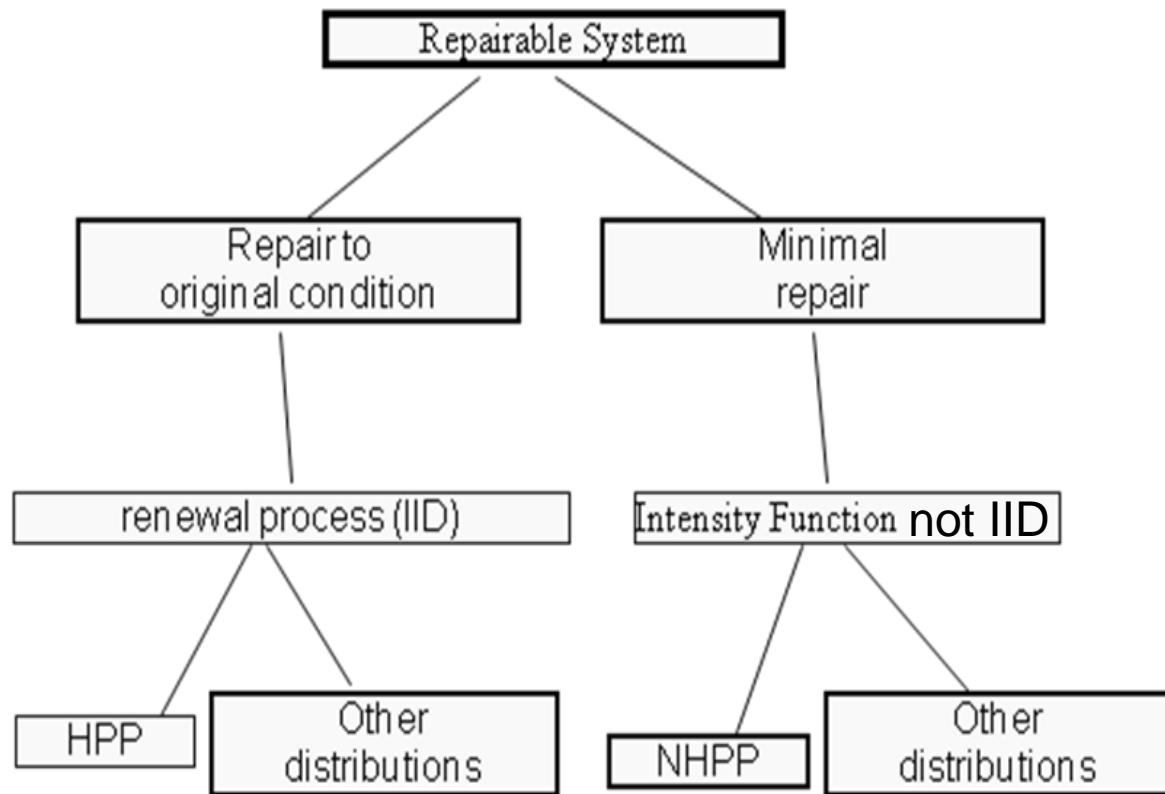
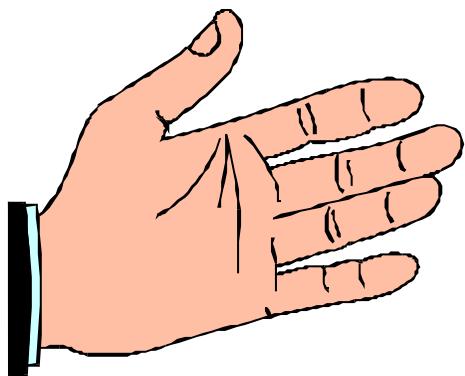
Note: $t_{\text{mode}} < t_{\text{med}} < t_{\text{mean}}$
because of skew

Renewal Process and Minimal Repair Process

Stochastic Point Process

- Stochastic process: Random events occurring at instants distributed over a given time
- From an operation perspective, Mean-time-between-failures (MTBF) is an important parameter.
- We can assume repair/restoration times to be negligible and consider reliability of system operating over a given time T during which k failures occur
- For a renewal repair process, the system or component may be replaced or restored back to ‘as-good-as-new’ condition
- At the other extreme, a system may be repaired such that it reverts to the ‘same-as-old’ condition (condition it was just before it failed)
- Anything in between is an imperfect repair

Stochastic Point Processes



To test whether the Renewal Process applies, values of MTBF should be examined for trends different from expected behavior, such as a time dependent ρ or λ , which if found, a NHPP (Non-Homogeneous Poisson Process) model is required.

Renewal Process: Repair to New Condition

For a Renewal Process, X_i (the time between failures) are *independent and identically distributed* (IID), i.e. the distribution of the time between Poisson failures is the same. For time to the k^{th} failure, T_k :

$$T_k = \sum_{i=1}^k X_i = kE(X_1) = k\mu_1 \quad \mu_1 = \text{mean time to 1st failure}$$

$$\text{Var}(T_k) = k\text{Var}(X_1) = k\sigma_1^2 \quad \sigma_1 = \sigma \text{ of 1st failure at } T_1$$

Repair results in “as good as new,” because after each repair, the expected time to the next failure, or time between failures, MTBF, is the same as the expected time to the first failure, MTTF. If repaired to a different condition, it will have a different distribution and not be IID.

For large k ($k > 30$), the **probability of time to the k^{th} failure being within time t** approaches Normal behavior:

$$\Pr\{T_k \leq t\} \approx F\left(\frac{t - k\mu_1}{\sigma_1\sqrt{k}}\right)$$

Variance of time to k failures = $k(\sigma_1)^2$

Renewal Process Example, MTTF = MTBF

A cutting tool has a time-to-failure distribution which is Normal with a mean of 5 operating hr. and std dev = 1 hr. Nine replacement tools are available with which to complete a 40 hr production run. Find R(40) [i.e. P(failure > 40 hr)], given the 9 cutting tools.

The Pr that failure of the 9th tool $T_9 \geq 40$ hr is:

$$\Pr\{T_9 \geq 40\} = 1 - F\left(\frac{40 - 45}{\sqrt{9}}\right) = 1 - F(-1.67) = 0.952$$

↑
9(MTBF)
↑
 $(\sigma_1 = 1)$

The Normal distribution is used as an approximation for the sum of k variables regardless of the underlying distribution. This is a Renewal Process, because the part is replaced and is expected to be “restored to as good as new” upon failure.

Homogeneous Poisson Process (HPP), Constant $\rho = \lambda t$

A important example of a renewal process occurs when the time between failures is Exponential (failure rate is constant).

If the time between failures follows the Exponential with parameter λ ; then the **Pr of the N^{th} failure or N number of failures occurring in time t , $N(t)$** , is Poisson and is given by:

$$\Pr\{N(t) = j\} = \frac{(l t)^j e^{-l t}}{j!}$$

$\rho = \lambda t$ = Poisson parameter, mean & variance of Poisson distribution.

$N(t)$ has a Poisson distribution with $E\{N(t)\} = \rho = \lambda t$. This distribution with constant ρ for a given t is designated the Homogeneous Poisson Process, HPP

Renewal Function: $m(t)$

For a renewal process, the **expected number of failures in time interval $(0,t)$ is given by $m(t)$** , the *Renewal Function*:

of failures: $m(t) = E[N(t)] = \sum_{j=1}^{\infty} j \Pr\{N(t) = j\}$

= Poisson
given
Exponential t

For large t :

$$\lim_{t \rightarrow \infty} \frac{m(t)}{t} = \frac{1}{m}$$

$\mu = \text{MTBF} = \text{MTTF}$,
assuming negligible
repair time for t large

$$m(t) = T / \text{MTBF}$$

For any time period T , if the system is in steady-state, the expected number of failures is given by $m(t)$

Renewal Exercise, Weibull t

A motor has a 1st time to failure distribution, which is Weibull with scale parameter, $\theta = 2,400$ hr, and shape parameter $\beta = 1.8$. Determine reliability at $T = 500$ hours if the motor failed at 200 hr and is restored to as “good as new” condition (Renewal Process). Motor reliability at $T = 500$ hr is $R(300)$, or 300 hours after restoration to new condition:

$$R(300) = e^{-\left(\frac{300}{2400}\right)^{1.8}} = 0.977$$

Assuming steady state condition, how many failures are expected in the first 10,000 hours of use? Use $m(t)$, the Renewal Function:

Weibull mean

$MTTF = MTBF = 2,400 \times (1 + 1/1.8) = 2,135$ hours, so the expected number of failures, $m(t)$, is $\sim T / MTBF = 10,000 / 2,135 = 4.7$.

(assumes negligible repair/replacement times compared to MTBF)

Minimal Repair Processes

- Repair processes range from renewal processes to minimal repair.
- Many repairs are minimal to fix or replace one or more single parts with the rest of the system remains unchanged, at the same age as before repair, and continuing to change with t .
- Unlike the Renewal Process, distributions of the time between failures for minimal repair are not independent and not identical (so **not IID**).
- To model Minimal Repair, an intensity function is defined to be the rate of change of the expected number of failures in time t with respect to t and the expected number of failures in the interval from t to $t + \Delta t$ divided by Δt . By integrating the intensity function from 0 to t , the expected, time-dependent number of failures in time t is obtained.

Minimal Repair of Parts of a Component or Components of a System

Define Intensity Function: **Let $\rho(t)$ = failure rate at time t** (also called rate of occurrence of failure, ROCOF)
If $N(t)$ = number of failures in $(0,t)$:

$$r(t) \approx \frac{N(t + Dt) - N(t)}{Dt} \quad \text{ROCOF at } t$$

$$r(t)Dt \approx E[N(t)] \quad \text{expected no. of failures in } \Delta t$$

Expected number of failures in $[0,t]$ is:

$$E[N(t)] = \int_0^t r(t') dt'$$

Because of Minimal Repair (in which all parts of a component or system is not repaired or replaced), times between repairs are not independent.

Minimal Repair within $[t_2 - t_1]$

Given failures in $[t_1, t_2]$, the expected failures in $[0, t]$ is

$$E[N(t)] = \int_0^t r(t') dt' = m(t)$$

$$MTBF(t) = \frac{1}{r(t)} \quad \text{Instantaneous MTBF at } t$$

$$MTBF(t_1, t_2) = \frac{t_2 - t_1}{m(t_1, t_2)} \quad \text{MTBF for } [t_1, t_2] \text{ interval}$$

where $m(t_1, t_2)$ is the expected number of failures in $[t_1, t_2]$ and predicted from

$$m(t_1, t_2) = E[N(t_2) - N(t_1)] = \int_{t_1}^{t_2} r(t) dt$$

Example 9.9

A manufacturing machine has an intensity function given by $\rho(t) = \exp(-6.5 + 0.0002t)$ with t measured in operating hours.

After 1 year of operation (3000 hours), $\rho(3000) = 0.00274$ and the instantaneous MTBF = $1/\rho(3000) = 1/0.00274 = 364.9 \sim 365$ hours.

The expected number of failures over the second year is found by integrating the intensity function from t_1 to t_2 .

$$m(3000, 6000) = \int_{3000}^{6000} e^{-6.5 + 0.0002t} dt = 11.26 \sim 11.3$$

NonHomogeneous Poisson Process (NHPP)

If the number of failures in a time interval follows a Poisson distribution with a mean that is dependent on time or the time interval, $\rho(t)$, the distribution is called a NHPP. Probability of j failures between time t_1 and t_2 is:

$$\text{NHPP: } \Pr\{N(t_2) - N(t_1) = j\} = \frac{m(t_1, t_2)^j e^{-m(t_1, t_2)}}{j!}$$

where $m(t_1, t_2) = \int_{t_1}^{t_2} r(t) dt$

For NHPP, the mean of the Poisson distribution is a function of time: $\rho(t)$ whereas for the HPP, the Poisson mean is constant, ρ .

$$R(t) = \Pr\{N(t) = 0\} = e^{-m(0,t)}$$

$$R(t | T) = \Pr\{N(T + t) - N(T) = 0\} = e^{-m(T,T+t)}$$

Power Law Process & Weibull $\lambda(t)$

$$\rho(t) = a b t^{b-1}, a, b > 0$$

Note that the functional form of the intensity function $\rho(t)$ is the same as the Weibull $\lambda(t)$ with $b = \beta$ and $a = \theta^{-\beta}$; $\theta = (1/a)^{1/b}$

$$\lambda(t) = \frac{b}{q} \left(\frac{t}{q} \right)^{b-1} \quad \text{Recall expression for } R(T) = e^{- \int_{t_1}^{t_2} \lambda(t) dt}$$

A six year old regional transit bus experiences minimal repair upon failure. It was found to have an intensity function given by $\rho(t) = 0.0464 t^{2.1}$ with t measured in years.

1. MTBF (instantaneous) = $1/\rho(t = 6) = 1 / [(0.0464)(6)^{2.1}] = 0.5$ yr
2. The expected number of failures during the 7th year is:

$$m(6,7) = \int_6^7 0.0464 t^{2.1} dt = 2.37 \sim 2.4$$

Power Law Process: Transit Bus, cont.

3. $P\{\text{exactly one failure in the 7th year}\}, j = 1 \quad m(6,7) = 2.37$

$$= P\{N(7) - N(6) = 1\} = \frac{m(6,7)^{j=1} e^{-m(6,7)}}{1!} = 2.37 e^{-2.37} = 0.222$$

4. The reliability for the 7th year, (i.e. $j = 0$), given the Pr it has survived through the 6th year:

$$R(1|6) = P\{N(7) - N(6) = 0\} = \frac{m(6,7)^{j=0} e^{-m(6,7)}}{0!} = e^{-2.37} = 0.093$$

5. Reliability expression:

$$R(t) = e^{-\int_0^t r(t)dt} = \exp[-\int_0^t 0.0464y^{2.1}dt] = e^{-0.0149677t^{3.1}}$$

Note: This behavior is Weibull with $\beta = 3.1$ and $\theta = 3.88$, which applies only for the first failure due to Minimal Repair.

Student Example

- A system under minimal repair has the intensity function
 $r(t) = 0.002(1 - e^{-0.001t})$ where t is measured in days
- The system has been operating for 2 years (730 days). Its instantaneous MTBF is
$$1/r(730) = \left[0.002(1 - e^{-0.001(730)}) \right]^{-1} = 965 \text{ days}$$
- Its reliability over the next year is,
$$R(t) = \exp \left[- \int_{730}^{1095} 0.002(1 - e^{-0.001t}) dt \right] = e^{-0.4353} = 0.647$$
- By the tenth year, the number of failures is predicted to be:

$$m(10) = \int_0^{3650} 0.002(1 - e^{-0.001t}) dt = 5.35$$

Renewal and Minimal Repair

Repair “as good as new”

$$\text{MTBF} = \text{MTTF}$$

$$E[N(t_2) - N(t_1)] = m(t_1, t_2)$$

$$= \frac{t_2 - t_1}{\text{MTBF}}$$

HPP (CFR):

$$\Pr\{N(t) = j\} = \frac{(\lambda t)^j e^{-\lambda t}}{j!}$$

$$R(t) = e^{-\lambda t}$$

$$m(t) = \frac{t}{\text{MTBF}}$$

$$\text{MTBF} = \left(\sum_{i=1}^n \frac{1}{\text{MTBF}_i} \right)^{-1}$$

Minimal Repair

$$\text{MTBF} = (t_2 - t_1) / m(t_1, t_2)$$

$$E[N(t_2) - N(t_1)] = m(t_1, t_2) = \int_{t_1}^{t_2} r(t) dt$$

NHPP:

$$\Pr\{N(t) = j\} = \frac{m(t_1, t_2)^j e^{-m(t_1, t_2)}}{j!}$$

$$R(t) = e^{-m(0, t)}$$

Power law Process:

$$r(t) = abt^{b-1}; m(t) = \int_0^t abt^{b-1} dt = at^b$$

(Ebeling, IRME)

Availability of Repairable and Non-Repairable Components

Repairable Components

- Failure categories of repairable components:
 - 1. Failure can be detected at the time of failure (**Revealed Fault**).
 - 2. Failure (**Latent Failure**) discovered following lack of response to a system demand
 - 3. Failure is detected also upon inspection, routine testing, or maintenance.

Availability Definition

Definition: *Availability is the probability that a system or component is available to respond to system demand by performing its required function at a given point in time or over conditions during a stated period of time when operated and maintained in a prescribed manner. It differs from Reliability by including more failure types in addition to random failure.*

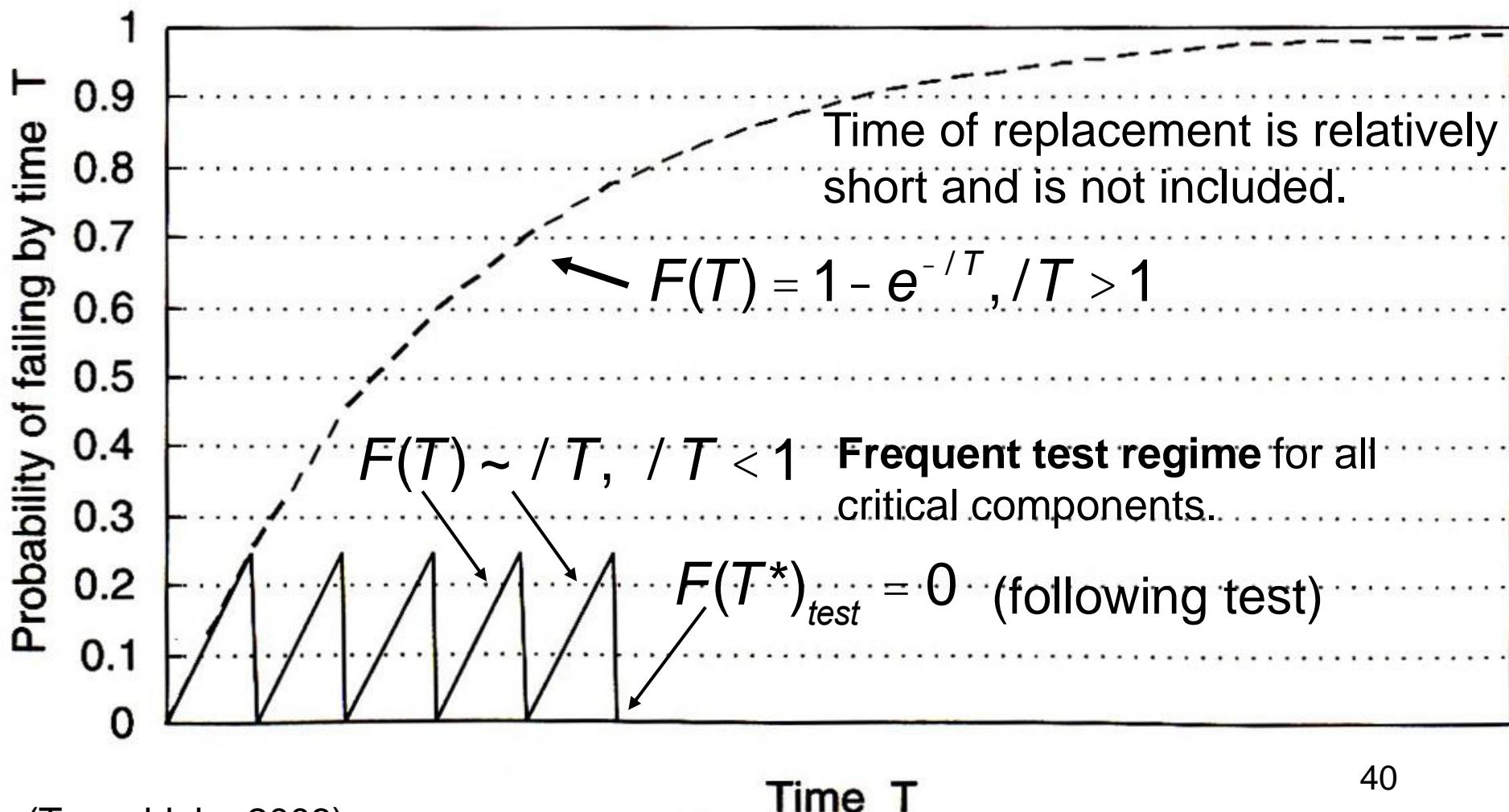
Therefore, the Availability distribution includes Reliability, probability of functioning or not failing between tests, and Maintainability (access, diagnose, repair or replace, and verify), probability of maintaining through repair, replacement, and sufficient spare parts and components with SAD ~ 0, so the Availability is sufficiently high to support Management of Risk within acceptable ranges.

$$Availability = \frac{uptime}{uptime + downtime}$$

Availability Summary

- **Reliability, $R(t)$:** Pr that a component or hazard barrier will *function at time t without failure when not being tested or under Maintenance.*
- **Availability, $a(t)$:** Probability that a repairable item *will respond and function at time t* when called upon by a demand of the system. It is the fraction of time a unit is online and can respond to system demand
- **Unavailability, $q(t) = 1 - a(t)$,** is the probability that a repairable item *will not respond and function at time t* due to:
 - Random failure (Type 1 failure), unscheduled test or maintenance (Type 2 failure), or excessive supply and administrative (SAD) delays (Type 3 failure)
 - Scheduled Preventive Maintenance or Replacement

$P(\text{fail})$ for Frequently Tested Sensitive Components, for $\lambda \sim \text{constant}$, Weibull, $\beta = 1$



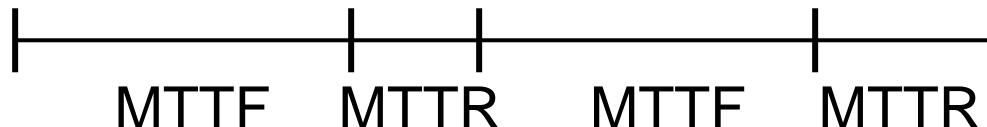
Preface: Availability Definitions

1. $A(t) =$ the availability at time t , also referred to as the **Point Availability**
2. $A(T) = \frac{1}{T} \int_0^T A(t) dt$ is the **Average Availability** over $[0, T]$

$$A_{t_2-t_1} = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t) dt \quad \text{Average Availability over, } [t_1, t_2]$$

$$3. A_{inh} = \lim_{T \rightarrow \infty} A(T) = \frac{\text{Time between failures}}{\text{Time between failures} + \text{time of repair}} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

= **Steady-State Availability or Inherent Availability**



Achieved Availability

Steady-state availability includes the following:

1. Inherent Availability $A_{inh} = \lim_{T \rightarrow \infty} A(T) = \frac{MTBF}{MTBF + MTTR} = \frac{\text{Up time}}{\text{Total time}}$

2. Achieved Availability

$$A_a = \frac{MTBM}{MTBM + \bar{M}}$$

Mean time between maintenance, MTBM includes unscheduled maintenance and preventive maintenance downtime.

\bar{M} = mean system downtime (includes SAD)

Inherent Availability Example

A machine has a time-between failure distribution that is Lognormal with a shape parameter $s = 0.86$ and a scale parameter $t_{\text{med}} = 40$ operating hours.

The Renewal repair distribution is Normal with a mean of 3.5 hr and a std dev of 1.8 hr. Calculate the inherent availability, A_{inh} . What is needed to calculate A_{inh} ?

MTBF = MTTF for a Renewal Process

$$\text{MTBF} = t_{\text{med}} e^{(s)^2/2} = 40 e^{(0.86)^2/2} = 57.9 \text{ hours}$$

$$A_{\text{inh}} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} = \frac{\text{Working Time}}{\text{Total Time}} = \frac{57.9}{57.9 + 3.5} = 0.943$$

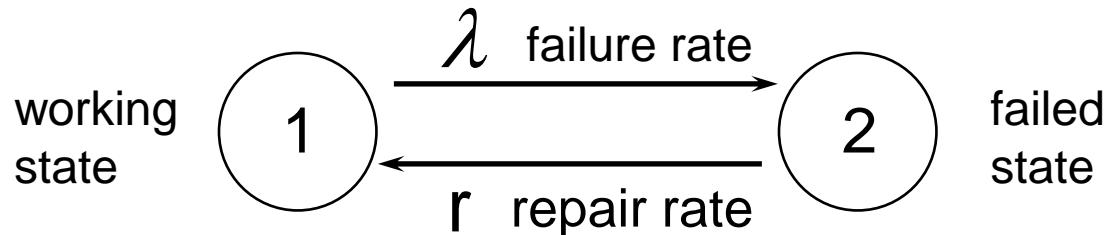


Markov Process

- The Markov model is based on the Markov property (process) in which the distribution of the variable that changes with time depends only on the distribution of the previous state (Markov, 1st Order) of the variable. Recall similarly that a Bayesian network variable is directly dependent, by cause and effect, only on its parent variables.
- The Markov model is useful for analyzing systems with multiple states, such as success/failure, failure/repair, or in a standby state.
- Markov model transitions between adjacent states are assumed to have constant transition rates, ρ_{ij} .
- For a system with n mutually exclusive and exhaustive (MEE) discrete states, the probability = $P_i(t)$ that the system is in state i at time t: $P_i(t)$; $\sum_{j=1}^n P_j(t) = 1$ By Pr Axiom 2

Exponential Model

The Exponential failure and repair distributions are the simplest that can be used in computing the measures of availability.



λ , constant failure rate; $r = \text{constant repair rate}$.

For a single CFR component having a constant repair rate, r , two states are defined: an up-state (1) with probability $P(1)$ and a down-state (2) with probability $P(2)$.

$$\frac{dP_1(t)}{dt} = -\lambda P_1(t) + r P_2(t)$$

$$P_1(t) + P_2(t) = 1$$

Transition Definitions

- Rate of transition of an item from working (up) to failure (down) = $\lambda(t)$, which is for Exponential the constant rate of occurrence of failure, ROCOF.
- Rate of transition of an item from failure (down) to working (up) is the rate of repair or Maintenance = $\mu(t)$, which is designated by r when the rate of maintenance is constant.

Markov Transitions for $a(t)$ and $q(t)$

- For a Markov process, the probability that an item is in the *up* state, $a(t)$, or in the *down* state, $q(t)$, from:

$$\frac{\Delta \text{ upstate}}{dt} = -\lambda(t)a(t) + m(t)q(t) \quad a(t) = \frac{\mu}{\lambda + \mu} + \frac{1}{\lambda + \mu} \exp[-(\lambda + \mu)t]$$

failure to down repair to up

$$\frac{\Delta \text{ downstate}}{dt} = \lambda(t)a(t) - m(t)q(t) \quad q(t) = \frac{1}{\lambda + \mu} - \frac{1}{\lambda + \mu} \exp[-(\lambda + \mu)t]$$

solve

- where the transition rate expressions are $\lambda(t)$, down rate, and the up rate of repair or maintenance = $\mu(t)$
Now assume λ and μ ~ constant.

- $\mu = r = 1/\text{MTTR} = 1/(\text{mean time to repair or maintain})$
- .
- $\text{MTTF} = 1/\lambda; \text{MTBF} = 1/\lambda$ for a renewed component

Exponential Model - Interval Availability

An Exponential Interval Availability is derived by integrating the Point Availability from t_1 to t_2 .

$$\begin{aligned} A_{t_2-t_1} &= \frac{1}{t_2-t_1} \int_{t_1}^{t_2} \left(\frac{r}{r+\lambda} + \frac{\lambda}{r+\lambda} e^{-(\lambda+r)t} \right) dt \\ &= \frac{r}{r+\lambda} + \frac{\lambda}{(r+\lambda)^2(t_2-t_1)} \left[e^{-(\lambda+r)t_1} - e^{-(\lambda+r)t_2} \right] \end{aligned}$$

$$\text{For } t_1 = 0 \quad A_t = \frac{r}{r+\lambda} + \frac{\lambda}{(r+\lambda)^2} t \xrightarrow{t_2} t_2 \left[1 - e^{-(\lambda+r)t} \right]$$

Then taking the limit, a steady-state or Inherent Availability, A_{inh} , is obtained. Because Exponential, λ and r are constant

$$A_{inh} = \lim_{t \rightarrow \infty} A_{t-0} = \frac{r}{r+\lambda} = \frac{1/\text{MTTR}}{1/\text{MTTR} + 1/\text{MTBF}} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

Availability Calculation Expressions

EXAMPLE 11.3. A component has MTBF = 200 hr and MTTR = 10 hr with both the failure and repair distributions exponential. Then $r = 1 \text{ repair}/10\text{hr} = 0.1$; $\lambda = 1/200$

$$A(t) = \frac{r}{r+1} + \frac{1}{r+1} e^{-(\lambda+r)t}$$
$$A(t) = \frac{0.1}{0.1 + 0.005} + \frac{0.005}{0.1 + 0.005} e^{-0.105t}$$

Point availability, $A(t)$: $= 0.952 + 0.048e^{-0.105t}$

For a specific point in time, $A(10) = 0.952 + 0.048e^{-0.105(10)} = 0.969$.

The interval availability for the first 10 time units is

$$A_{10-0} = 0.952 + \frac{0.005}{(0.105)^2(10)} \left[1 - e^{-0.105(10)} \right] = 0.981$$

Ave. Availability over [0,10]

The graph of $A(t)$ for this example, shown in Fig. 11.3, approaches the steady-state availability of $A = 0.952$.

$$\frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

↑
Slide 21

Interval Availability, $[0,t]$: $A_t = \frac{r}{r+1} + \frac{1}{(r+1)^2 t} \left[1 - e^{-(\lambda+r)t} \right]$

Human Reliability Analysis

Unit 16

Spring 2022

References

- Modarres, M., M. Kaminskiy, and V. Krivtsov, *Reliability Engineering and Risk Analysis*, 2nd ed, Taylor&Francis, 2010 (Modarres, RERA)
- Modarres, M., *Risk Analysis in Engineering*, Taylor & Francis, 2006
- Calixto, E., G.B.A. Lima, and P.R.A. Firmino, Comparing SLIM, SPAR-H, and Bayesian Network, *Open J. of Safety Science and Technology*, 2013, 3, 31-41 (Calixto, 2013)
- Boring, R.L. ad D.I. Gertman Human Error and Available Time in SPAR-H, Idaho National Engineering and Environmental Laboratory (INEEL/Con-04-01630), (Boring, 2004)
- Kumamoto, H. and Henley, Ernest, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2nd ed, IEEE Press, 1996 (Kumamoto, 1996)
- Groth, K.M. and A. Mosleh, "Deriving causal Bayesian networks from human reliability analysis data: A methodology and example model," *J. Risk and Reliability* o(o), pp. 1–19, 2012 (Groth, 2012)
- Jordaan, Ian, *Decisions Under Uncertainty— Probabilistic Analysis for Engineering Decisions*, Cambridge University Press, 2005 (Jordaan, 2005)
- The SPAR-H Human Reliability Analysis Method, Idaho National Laboratory, National Regulatory Commission (NRC), NUREG/CR-6883, 2004 (NUREG, 2004)
- Le Coze, J.C., "Reflecting on Jens Rasmussen's legacy. A strong program for a hard probem, Safety Science, 71 (2015, 123-141 (Le Coze, 2015)
- Laux, Liala and C. Plott, Using Operator Workload Data fo Inform Human Reliability Analysis, 2007 (Laux, 2007)
- Fullwood, R.R., *Probabilistic Safety Assessment in the Chemical and Nuclear Industries*, Butterworth, 2000
- Cameron, I. and Raman, R, *Process Systems Risk Management*, Elsevier, 2005
- Leveson, Nancy G., *Engineering a Safer World, Systems Thinking Applied to Safety*, MIT Press, Fall, 2011 (Leveson, 2011)

Human Errors - History

- 1950s: Efforts to quantify human elements through Reliability Engineering. Most activities were within Aerospace and Nuclear Engineering industries.
- 1962: Prototype of Human Reliability databank formed (THERP)
- 1979: Three Mile Island Accident
 - Partial nuclear reactor meltdown, release of radiation in Pennsylvania
 - Led to an increased interest in human error, especially in the Nuclear Industry.

Chernobyl Nuclear Reactor, 1986

- Nuclear runaway and meltdown: 56 immediate fatalities, 336,000 people relocated, wide ranging radioactive fallout and severe exposure to the community
- Reactor design flaws
- Safety systems offline
- Operator errors showed poor training, leadership
- Numerous simultaneous alarms (alarm flooding) confused operators in this incident (similar to the Three Mile Island accident)
- Dysfunctional safety culture

Introduction

- Human Error:
 - Unwanted human actions or inactions that arise from problems in sequencing, timing, knowledge, interfaces, or procedures and that result in deviations from expected standards or norms and place people, equipment, and systems at risk.
- Human Reliability
- Human Factors

Learning from Human Error

- Should the operator be blamed? We can blame the operator for an “error” **or**
- We can investigate causes and influences underlying the immediate cause and finally to root causes that lead to management, and to the underlying Safety Culture.
- Thereby, we can learn from the “error”, causes, and conditions under which the error and upset event occurred.

Human Failure Rates due to Task and Conditions

Activity	Rate Examples ⁷
Error of omission / items embedded in procedure	3×10^{-3}
Simple arithmetic error with self-checking	3×10^{-2}
Inspector oversight of operator error	1×10^{-1}
General rate/ high stress / life threatening situation	0.2 – 0.3
Error of omission / 10-item check list	1×10^{-3}
Carry out plant policy / no check on operator	5×10^{-2}
Select wrong control / identical, labeled controls	3×10^{-3}

Wash -1400 (NUREG)-75/014); “Reactor Safety Study – An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants.”, 1975

NUREG/CR-1278; “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.” 1989

Human Reliability Depends Greatly on Conditions and on Feedback



Examples of Conditions:

- $P(\text{Error}) \sim 0.5$: Not trained, or under excessive stress, or fatigued, or with insufficient time
- $P(\text{Error}) \sim 0.01$: Trained, under normal (not excessive) stress, not fatigued, with sufficient time to perform a task
- $P(\text{Error}) \sim 0.001$: Trained, under normal (not excessive) stress, not fatigued, with sufficient time, and with feedback (indicator for confirmation)
- Conclusion: By adjusting conditions, Human Reliability can be greatly influenced, and available time to perform a task is a sensitive variable!

BP Texas City Disaster, 2005: Failure of Feedback System: Need Confirmation

- Operation of a Raffinate Splitter Tower within acceptable risk limits was not sufficiently understood or executed
- Startup procedures not followed correctly
- Material fed to column but did not exit due to a valve not opened during startup
- Level exceeded safe limits, level device failed but not recognized
- Level instrumentation in blow-down tank failed but was not repaired and was not checked
- **Consequences:** Blow-down tank overflowed, material reached an ignition source, and a vapor cloud explosion occurred under partial confinement

BP Texas City Explosion / Fire



March 23, 2005

10



15 fatalities; > 180 injuries

Feedback control systems can detect errors/deviations to alert operators and enable recovery of normal operations.

Feedback Examples

- Bell or buzzer to alert operator when something was undone or done incorrectly. Example is beeping bell when keys left in ignition.
- Control system requires confirmation that the entered amounts are correct or the controls are entered correctly, such as open or closed valves.
- A human checking system is useful but not sufficiently reliable by itself, so a nonhuman feedback system is often also needed. But the feedback system must be tested and maintained and not just trusted!
- Human Expectancy bias is that if someone else checked, they will often depend on or “trust” that someone without checking it themselves!

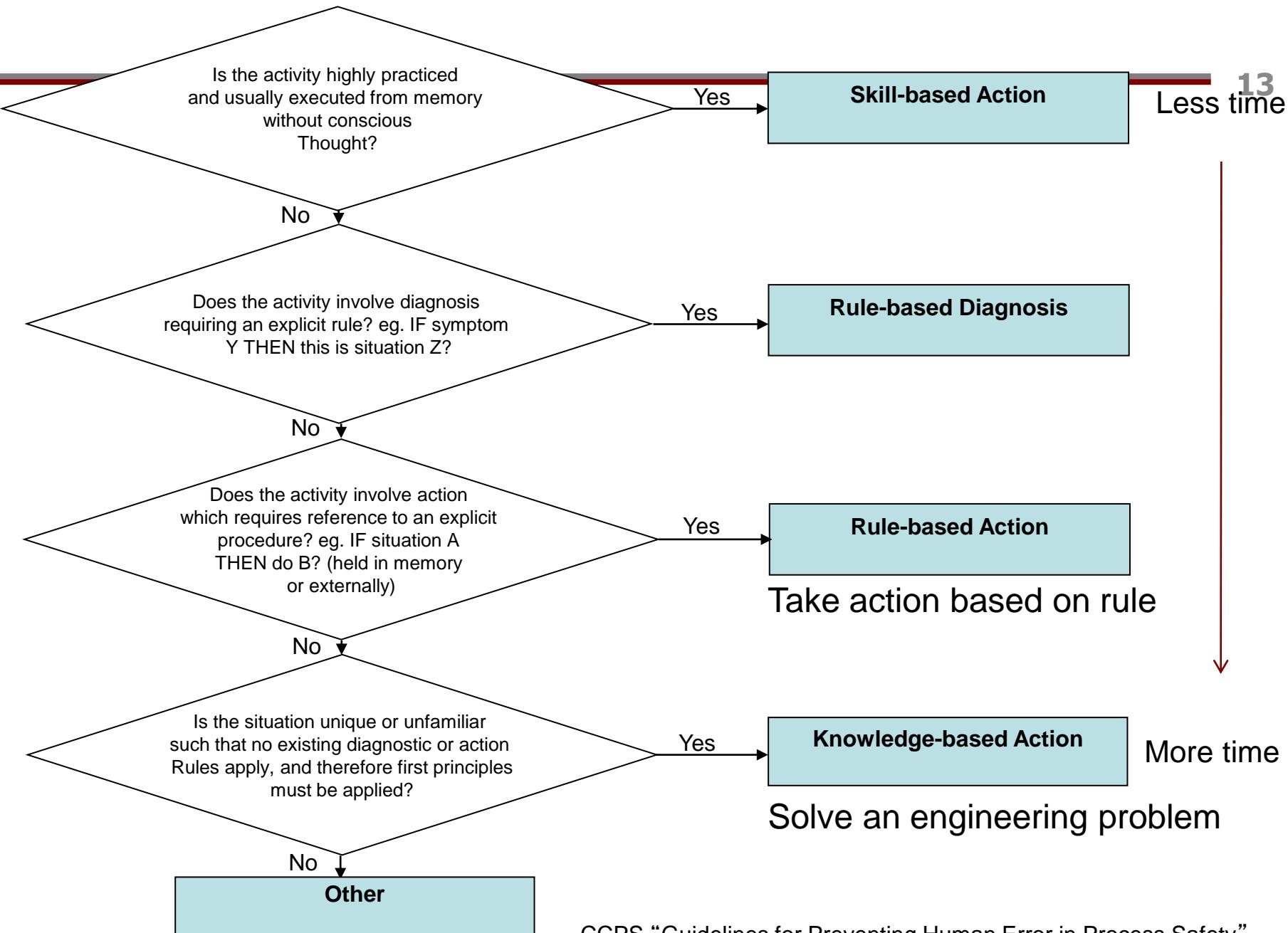
SRK Classification of Human Error

12

Skill-, Rule-, Knowledge-Based Tasks

- Distinguishes among three types of human error according to the types of information processing done by personnel performing industrial tasks and the relative amount of time needed for tasks in each category.
- Provides a useful framework to identify types of error more likely to occur in operational situations.

Flow Chart for Classifying Skill-, Rule-, Knowledge (SRK)-based Processing



Workload Assessment

- Operators are the best judges of their stress
- Monitoring, Questionnaires, and Interviews of operators to identify ways to improve the work environment.
- Rating scales to quantify task loading
- Workload questionnaires to provide information from operators
- Various assessment techniques are used, including the NASA Task Load Index

NASA Task Load: Extension of SRK

Influences

Rating Scale Definitions		
Title	Endpoints	Descriptions
MENTAL DEMAND	Low/High	How much mental and perceptual activity was required (e.g. thinking, deciding, calculating, remembering, looking, searching, etc.)? Was the task easy or demanding, simple or complex, exacting or forgiving?
PHYSICAL DEMAND	Low/High	How much physical activity was required (e.g. pushing, pulling, turning, controlling, activating, etc.)? Was the task easy or demanding, slow or brisk, slack or strenuous, restful or laborious?
TEMPORAL DEMAND	Low/High	How much time pressure did you feel due to the rate or pace at which the tasks or task elements occurred? Was the pace slow and leisurely or rapid and frantic?
EFFORT	Low/High	How hard did you have to work (mentally and physically) to accomplish your level of performance?
PERFORMANCE	Good/Poor	How successful do you think you were in accomplishing the goals of the task set by the experimenter (or yourself)? How satisfied were you with your performance in accomplishing these goals?
FRUSTRATION LEVEL	Low/High	How insecure, discouraged, irritated, stressed and annoyed versus secure, gratified, content, relaxed and complacent did you feel during the task?

Human Error Probabilities, HEP

- Probability estimations must include realistic HEP values to include interactions and dependencies under the conditions of operation.
- Challenges of Human Reliability Analysis (HRA):
 - More interdependent and more difficult to quantify human failure compared to hardware failure
 - Binary success and failure states usually unrealistic, because human actions depend on conditions
 - Insufficient data to quantify human behavior for extreme conditions, e.g., responding to multiple alarms
 - But we know that we can influence Human Reliability

Human Reliability Analysis, SHARP

Systematic Human Action Reliability Procedure (SHARP):
7 steps to provide a framework for HRA

1) Definition of all types of human interactions through activity categories:

- Operator can restore safeguard functions during tests and maintenance
- Operator can cause system to deviate
- Can recover systems to normal operation
- Can fail to terminate challenge to system
- Can restore initially failed equipment

2) Screening: focus on main human interactions that challenge the system safety

Human Reliability Analysis, SHARP

3) Qualitative analysis of key human actions:

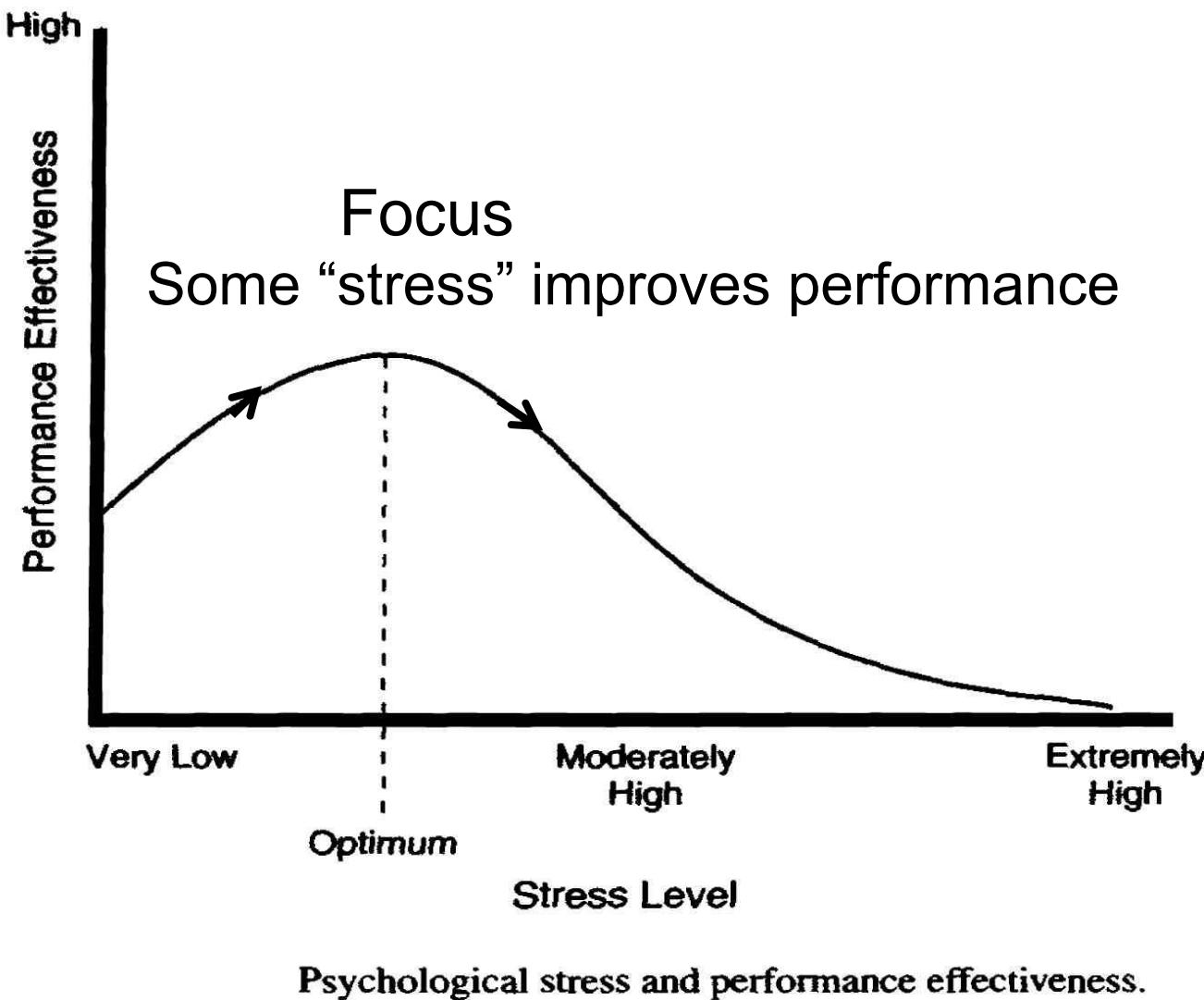
- Predict operator thinking and actions based on effects of **performance shaping factors (PSFs)** that influence reliability
- Predict how operator performance can initiate a challenge or modify a challenge to the system
- Predict operator performance & error modes

Performance Shaping Factors (PSFs)

- Internal PSFs:
 - Physiological, physical, pathological
 - Psychological, cognitive (skill, rule, knowledge, SRK task categories)
- External PSFs or PIFs (Performance Influencing Factors)
 - Situational work conditions: work hours, breaks, environmental design, organizational issues
 - Task and equipment characteristics
 - human-machine interface, control display relationships, complexity,...

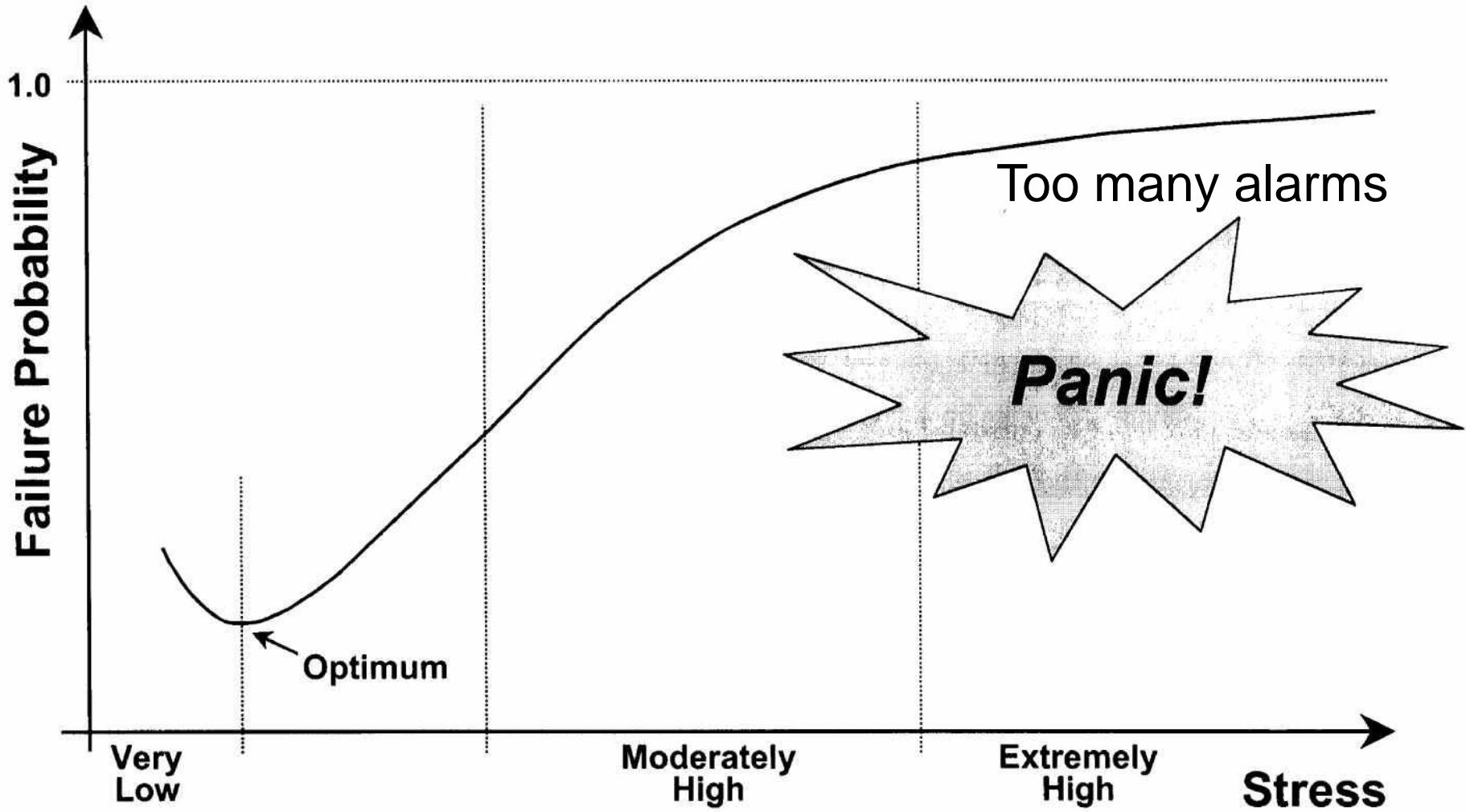
Effectiveness Related to Stress

20



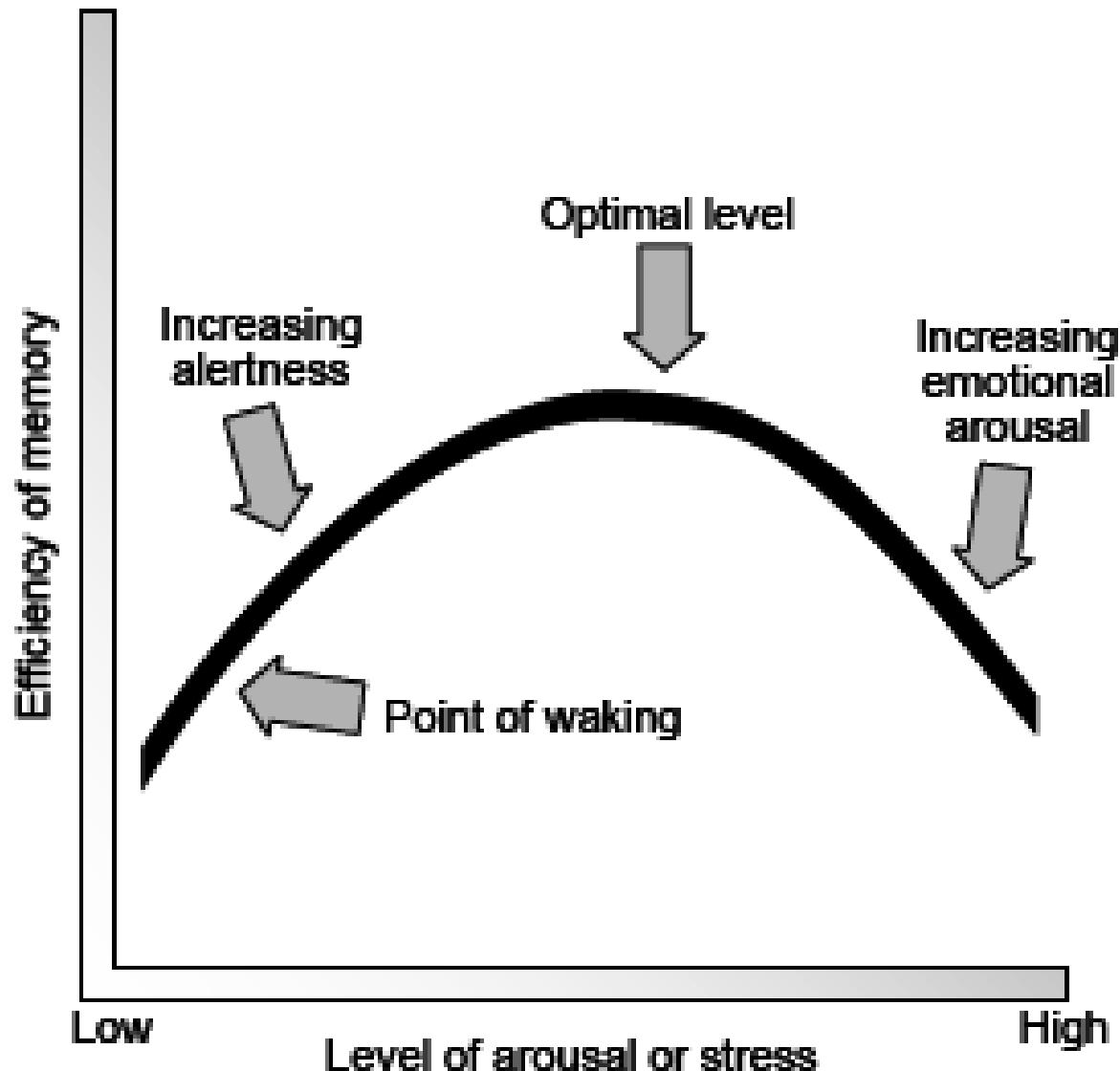
Effect of Stress on Failure Probability

21



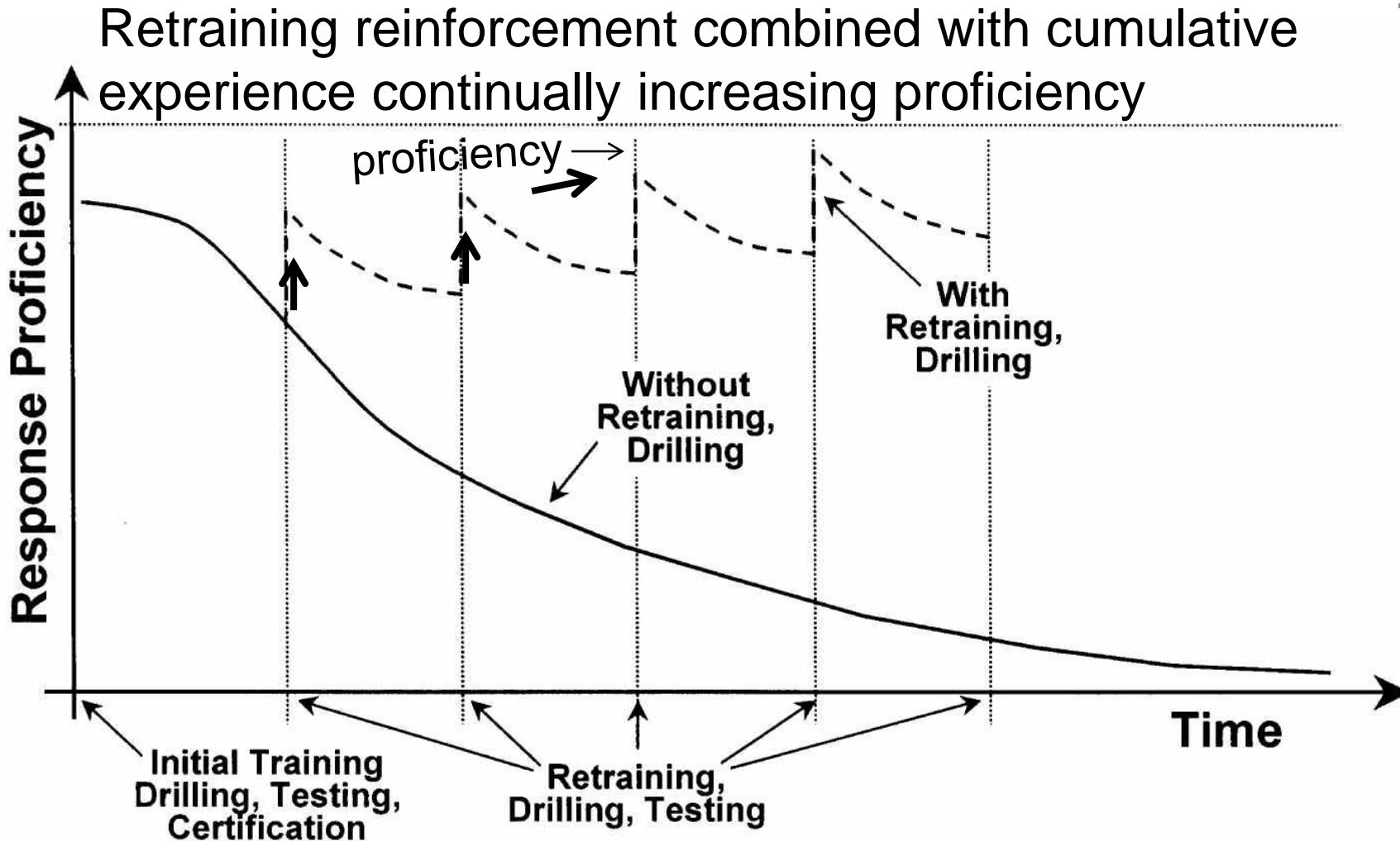
Effect of Stress on Memory

22



Influence of Training, Retraining, and Drills

23

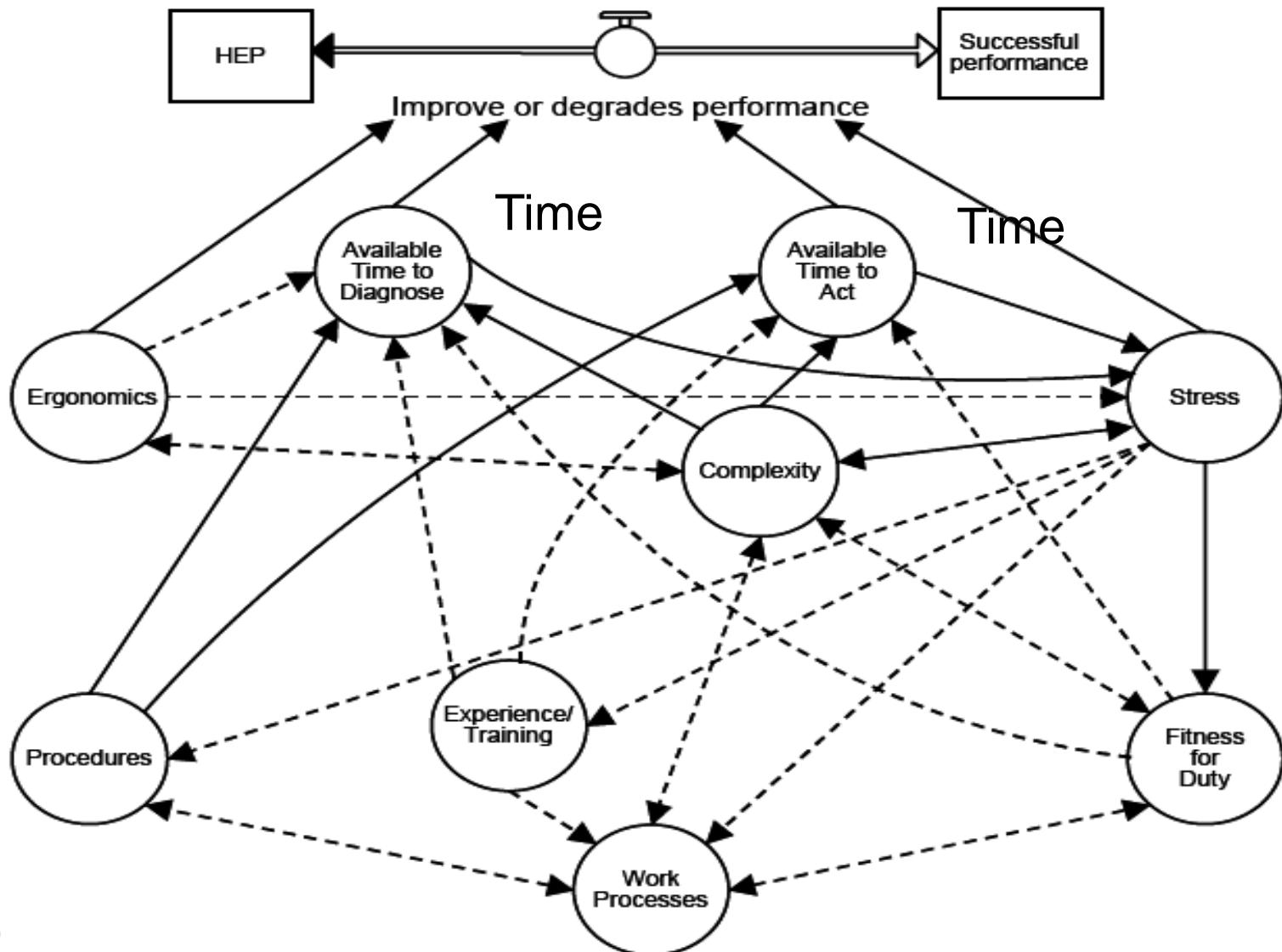


Interrelated PSFs, Effect on Available Time or Time Needed to Act

1. Experience, E, and Training/Retraining, T: More E and T means less time needed for decisions and actions
2. Available Time to detect, diagnose, & perform task: less time makes tasks more complex, stressful
3. Stress and stressors, environmental effects: less time for action can increase stress
4. Complexity of task: time to understand and act
5. Ergonomics, human-machine interface and time
6. Procedures: Are they clearly written? Time needed
7. Fitness for Duty at work and effect on time needed
8. Work Processes that affect independent operation of equipment or of another operator and available time

High (solid) or Low (dashed) Degree of Influence Among 8 Primary PSFs: Time to Detect, Diagnose, & Act

25



(Boring, 2004)

(NUREG, 2004)

Available Time > Required Time

Human Reliability Analysis, SHARP

4) Representation: Qualitative Action Analysis:

Representation of modes of human error to combine HRA with system reliability models developed for system components

- Operator action event tree

5) Impact assessment: evaluate impact of key human actions, represented in 4), on the system using fault trees, event trees, Bayesian networks

- First, use screening to assess impacts
- Incorporate human interactions that are challenges to system in the fault trees, event trees, and Bayesian networks.
- Include estimated or modeled outcome and consequence ranges and distributions

HRA, Operator Action Tree:

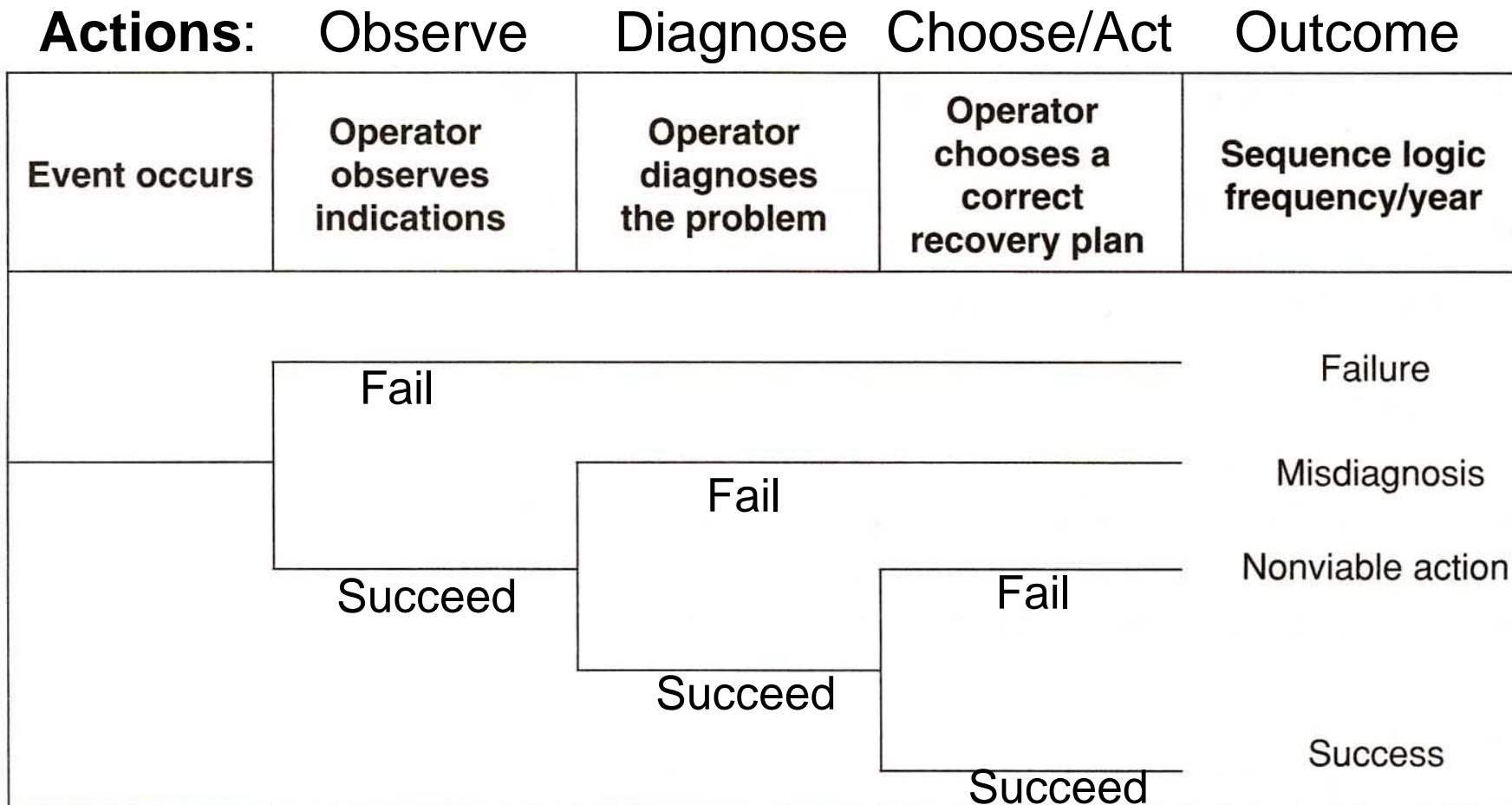


FIGURE 4.14 Operator action tree.

Figure 6.7, RERA Quantify event tree in SHARP. Step 5, impact assessment and probabilities in Step 6

Human Reliability Analysis, SHARP

6) Probability Quantification: Calculate and assess probabilities of success and failure for each key human activity identified in previous steps

- Selection of quantitative models to use within the SHARP procedure to calculate human failure probabilities are based on characteristics of the analyzed human interactions under the observed conditions
 - Data; time-reliability distributions of human reliability, as with system components
 - Expert judgment needed when applicable observed data are not sufficient or available

Human Reliability Analysis, SHARP

7) Documentation of analysis: traceable description of the process used in the previous steps to develop a quantitative assessment of key human interactions to guide decision making and future analysis

- Assumptions
- Data sources
- Models used
- Criteria for screening to eliminate less important or unimportant human interactions

SHARP Procedure

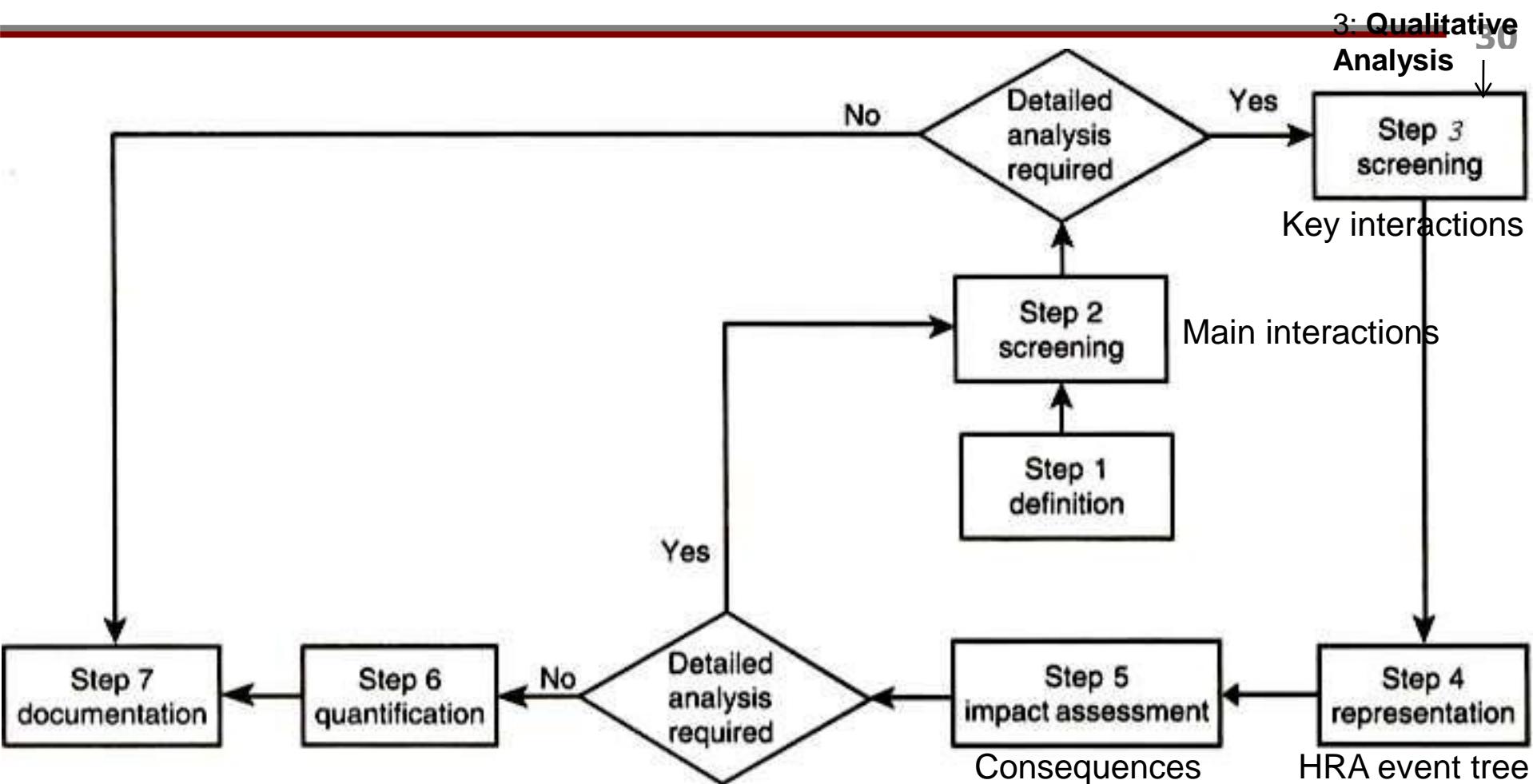


FIGURE 4.13 Systematic human action reliability procedure, Hannaman and Spurgin [45].

Figure 6.6, RERA

Use in SHARP Step 6 (Probability Quantification)

31

- THERP (Technique for Human Error Rate Prediction):
 - Based on system reliability analysis for equipment.
- Procedure:
 - 1) Define system failures from human interaction points, task characteristics, and impacts on the system
 - 2) Use HRA event trees to estimate probability of error for each key task

Analytical Methods, SPAR-H: Use in SHARP Step 6 (Probability Quantification)

32

- Standardized Plant Analysis Risk Model-Human (SPAR-H) to estimate human error probability (HEP) from diagnosis and human action failures.
- Uses the 8 primary PSFs for error context
- Assign positive and negative influences of PSFs
- Accounts for dependencies among PSFs

Analytical Methods, SPAR-H[^]

- HEP model: $P_e = \frac{P_{eb} PSF_c}{P_{eb}(PSF_c - 1) + 1}$
- P_{eb} is base Pr of human error
- PSF_c : composite of 8 PSFs: $PSF_c = \tilde{\bigcirc}_{i=1}^8 PSF_i$
- PSF levels and values:
 - Time available < time required for task: >1
 - Time available = nominal time required: 1
 - Time available $\geq 5 \times$ time required: 0.1
 - Time available $\geq 50 \times$ time required: 0.01

P(failure) reduced given more time

SPAR-H Application

- Consider similar tasks for which PSF values are affected the same way by the PSFs and therefore estimated using the same values.
- Nominal PSF values are set = 1 in this model when conditions are acceptable, and the PSFs have low influence on human failure.
- Use PSF data and $HEP1 = P_b$ for the 4 tasks to calculate HEP2 for each task (that considers PSF) and a total HEP

Table 6. PSFs composite (before improvement).

PSFs	Task 1	Task 2	Task 3	Task 4
Available time	1	1	1	1
Stress	1	1	1	1
Complexity	1	1	1	1
Experience/Training	1	1	1	1
Procedures	5	5	5	5
Ergonomics	1	1	1	1
Fitness for duty	1	1	1	1
Work proess	1	1	1	1
Total	5	5	5	5

	HEP2	HEP1
Open Vapor Valve—Task 1	0.357143	$0.1 = P_b$
Open Suction Valve—Task 2	0.0005	0.0001
Close Suction Valve—Task 3	0.208333	0.05
Open Vapor Valve—Task 4	0.0005	0.0001
Total	0.566476	

$$\text{Task 1 HEP2} = \frac{P_{eb} \times \text{PSF}_c}{P_{eb} (\text{PSF}_c - 1) + 1} = \frac{0.1(5)}{0.1(4) + 1} = 0.357$$

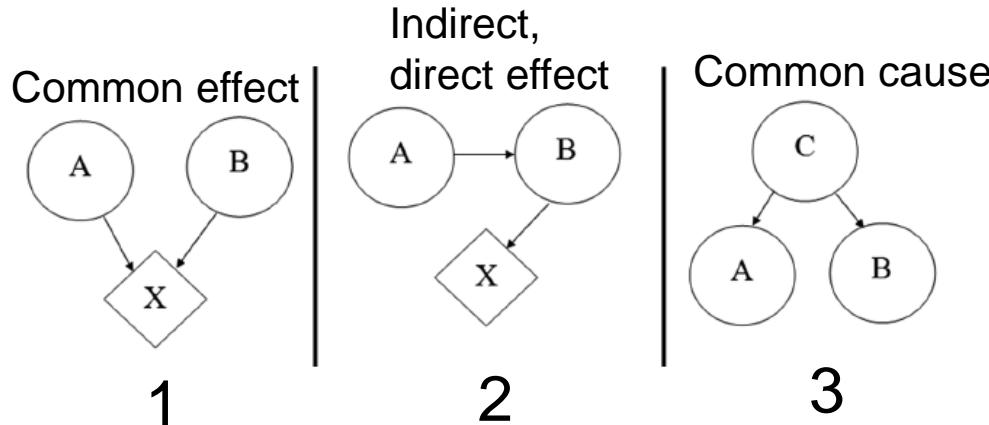
$$\text{PSF}_c = \tilde{\bigcirc}_{i=1}^8 \text{PSF}_i = 5$$

Human Error Causal Model

- HRA research (e.g. Groth, 2012) has shown progress in using available data to identify and characterize main influences of human performance and to develop a predictive model of Human Reliability based on Bayesian Networks.
- Causal relationships among PSFs can be incorporated in a **Causal HRA** model to predict different types of human errors in real-time engineering environment under observed conditions and, given the probable causes or influences, to reduce the probability for human error and thereby reduce system risk.

Types of Causal Relationships

36



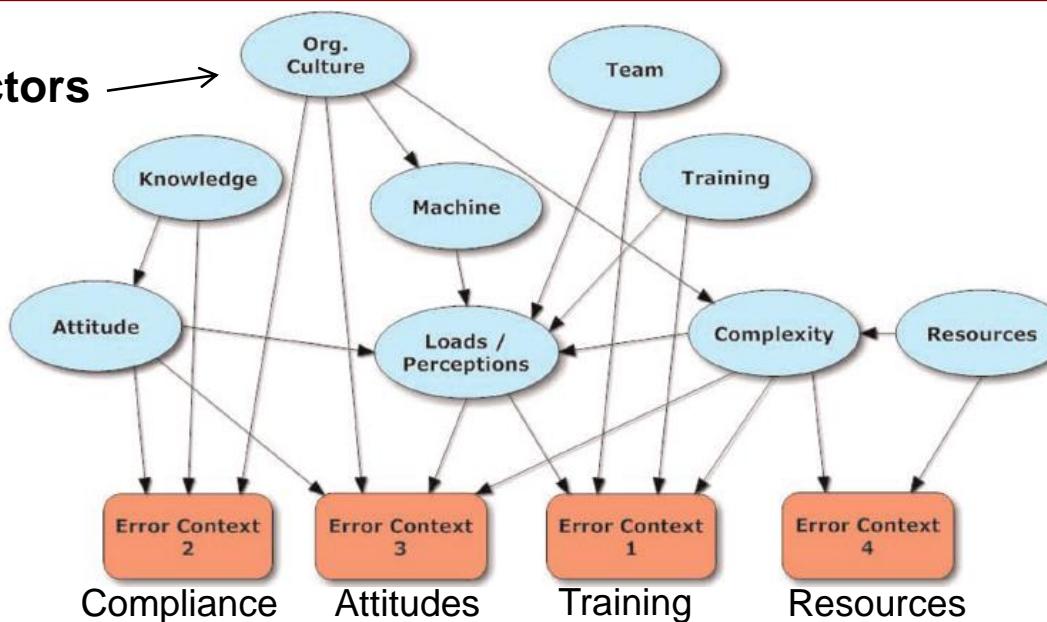
- 1. For error context X, PSF A is independent of PSF B (X not instantiated). PSFs A, B directly influence common effect error context X
- 2. PSF A influences PSF B, which directly influences X
- 3. PSF C is a direct common cause influence on PSF A and on B, each of which may influence one or more error contexts X₁, X₂, ...

Human Reliability Model with Error Contexts (EC_i)

37

Organizational Factors

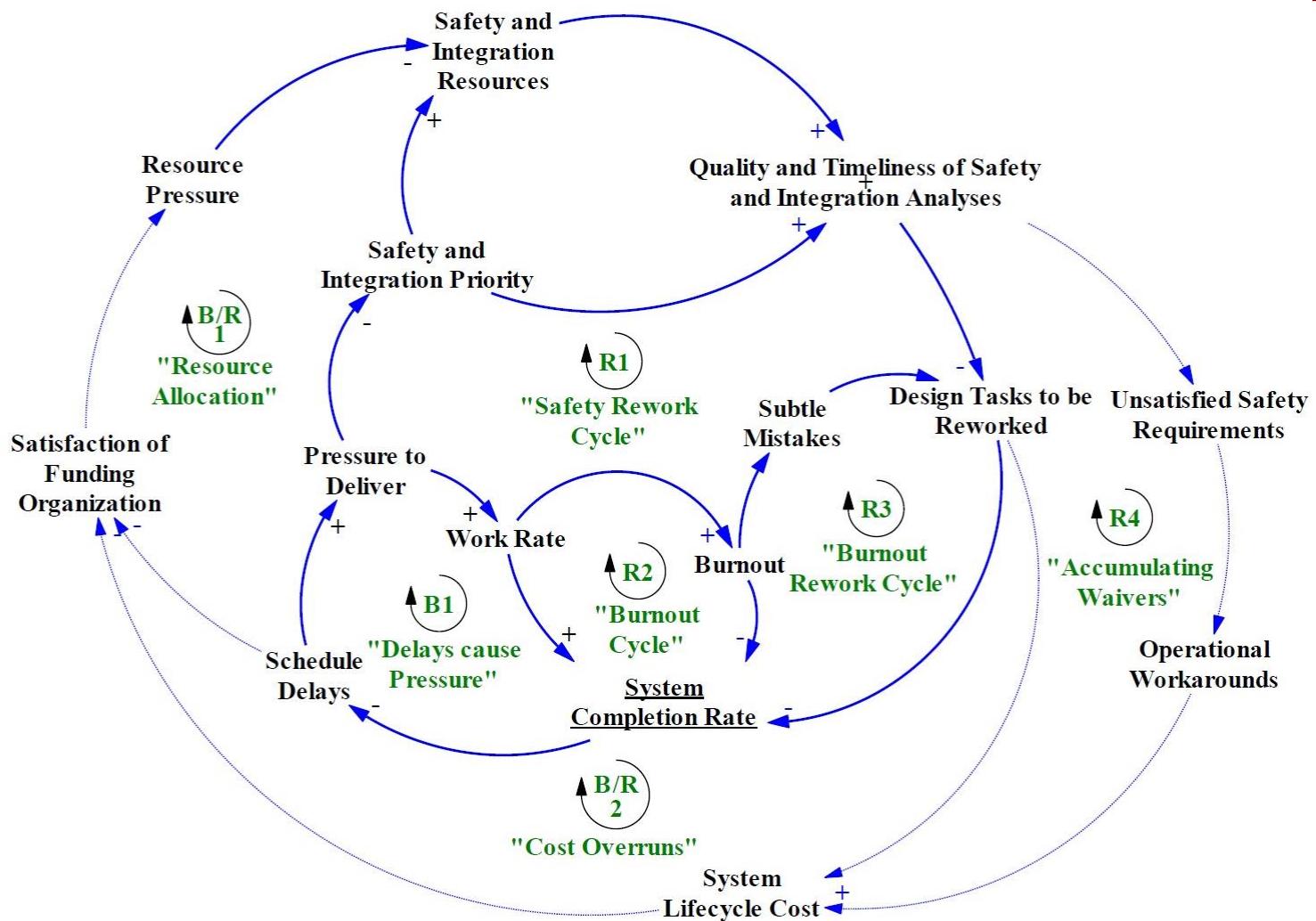
Extend this model by including BN node variables with values calculated from indicator aggregation



- EC1: teamwork and training insufficient to respond to a complex, dynamic scenario of events and conditions.
- EC2: insufficient compliance with recognized best practices at the individual or organization levels
- EC3: poor work attitudes due to complex situations requiring judgment and problem solving
- EC4: complex situations that exceed scope of available resources (procedures, tools, needed information)

Example Model Loops: Influences of Human Reliability

38



(Leveson, 2011)

Table 1. First generation. Source: Calixto, 2011.

Human Reliability Analysis Methods		
<i>First Generation</i>		
	Name	Objetive
THERP	<i>Technique for human error rate prediction</i>	Assess failure in task or action sequence. It is applied in maintenance, operational or incident analysis with complex graphic representation. (1975)
OAT	<i>Operator action trees</i>	Assess failure in task or action sequence. It is applied in maintenance, operational or incident analysis with simple graphic representation. (1982)
SLIM	<i>Success likelihood Index Methodology</i>	Assess failure in task or action sequence and is applied in maintenance, operational or incident analysis and regards human factors performance based in specialist opinion. (1984)
SHARP	<i>Systematic Human Action Reliability Procedure</i>	Assess cognitive human process of failure (detection, understanding, decision and action), being applied in maintenance, operational or incident analysis. (1984)
STAHR	<i>Social-Technical Assessment of Human Reliability</i>	Assess failure in task or action sequence and is applied in maintenance, operational or incident analysis. Such method regards human factors performance based in specialist opinion. (1983)

Table 2. Second generation. Source: Calixto, 2011.

Human Reliability Analysis Methods		
<i>Second Generation</i>		
	Name	Objective
ATHEANA	<i>A Technique for Human Error Analysis</i>	Assess cognitive human process of failure (detection, understanding, decision and action), being applied in maintenance, operational or incident analysis. (1996)
CREAM	Cognitive Reliability and Error Analysis Method	Assess cognitive human process of failure (detection, understanding, decision and action), being applied in maintenance, operational or incident analysis. (1998)
<i>Third Generation</i>		
	Name	Objective
Redes Bayesianas	Assess failure in task or action sequence and is applied in maintenance, operational or incident analysis and regards human factors performance based in specialist opinion. In addition such methods regards human factors performance dependency.(2005)	

Human Reliability Data Sources

40

- Plant specific data. These are limited. In some cases, reporting of human errors can lead to penalties. Reporting of errors and near misses should be rewarded because of the valuable information gained to track the system and direct actions to reduce system risk.
- Bayesian Network model of STS organization by aggregation of lagging and leading indicators updated frequently or continuously to reveal probabilities of hidden states influencing Human Reliability within the STS organization
- Human action simulation data
- Expert judgment, which is especially important due to scarcity of HRA data.
- Literature: Numerous HRA articles with models and data are available online.

Risk Measures

Unit 17

Spring 2022

References

- Modarres, M., *Risk Analysis in Engineering*, Taylor & Francis, 2006, Chap 8 on website (Modarres, RAE)
- Modarres, M., M. Kaminskiy, and Vasiliy Krivtsov, *Reliability Engineering and Risk Analysis*, Taylor & Francis, 2010 (Modarres, RERA)
- Fischhoff, Baruch and J. Kadvany, *Risk, A Very Short Introduction*, Oxford, 2011 (Fischhoff, 2011)
- Jordaan, Ian, *Decisions Under Uncertainty—Probabilistic Analysis for Engineering Decisions*, Cambridge University Press, 2005 (Jordaan, 2005)
- *Making Acute Risk Decisions with Chemical Process Safety Applications*, CCPS, AIChE, 1995 (AIChE, 1995)
- Ang, A. H-S. and W.H. Tang, *Probability Concepts in Engineering Planning and Design, Vol 2*, Wiley, Decision, Risk, and Reliability, 1990 (Ang, PCEPD)
- Korb, K.B. and A.E. Nicholson, *Bayesian Artificial Intelligence*, CRC Press, 2004 (Korb, 2004)

Risk Decisions

- Categories of risk decisions
 - Risk **Acceptability**: compare risk to an absolute risk acceptance level or preferably a Risk Acceptability Range.
 - Risk **Alternatives**: select best overall alternative using multiple criteria that include, risk, performance, and cost.
 - Risk **Actions**: select one or more coordinated actions to reduce frequencies, consequences, or both, cost effectively to bring specific and overall risk to within tolerable ranges.

Benefit-Cost Analysis Model, B-CA

- Monetary values placed on benefits and costs (direct and indirect) of risk control measures.
- Easily understood by Stakeholders and by the Public
- Disadvantage of B-CA: Requires conversion of risk values (frequencies/consequences) to monetary values; introduces bias depending on risk attitudes.
- Conversion of risk values to money is sometimes difficult and highly subjective (e.g., value of a statistical life), but utility functions can be used to reduce bias.

Benefit-Cost Benefits

- Example: Installing a scrubber as a barrier to reduce emissions
- **Direct effects:**
 - Benefit: reduced pollution levels
 - Cost: capital expenditure to install
- **Indirect effects:**
 - Benefits: lower overall costs of production, enhanced reputation, good will of community
 - Costs: maintenance, training of operators

Benefit-Cost Ratio

- The benefit-cost ratio metric compares the effectiveness of risk control measures.
- Monetary or utility values can be used.

$$R_{b/c} = B / C$$

B = benefit (direct, indirect, or total)

C = cost (direct, indirect, or total)

Decision Criteria Based on Direct and Indirect Costs

TABLE 8.1
Decision Criteria in Benefit–Cost Analysis

Case	Direct Balance	Indirect Balance	Decision
1	$C_D < B_D$	$C_I < B_I$	Acceptable
2	$C_D > B_D$	$C_I > B_I$	Unacceptable
3	$C_D < B_D$	$C_I > B_I$	Unacceptable (unless allowed by regulation)
4	$C_D > B_D$	$C_I < B_I$	Unacceptable (unless subsidized)

(Modarres, RAE)

Risk decisions are generally made based on market and non-market benefits such as environmental and public health benefits (good will). In all cases, an analysis of costs and benefits and a cost/gain balance are required.

Example: Transportation Risk Reduction

- Truck fuel tank's side impacts lead to fires.
Manufacture fuel tank with modified side design
to reduce fuel tank fires with following options:
 - 1. Steel plate, \$14: Fires reduced ~ 100%
 - 2. Lexan plate, \$4: Fires reduced 95%
 - 3. Plastic tank lining, \$2: Fires reduced 85%

TRR Risk and Cost Data

- Number of trucks involved: 6,000,000
- Projected fatalities from trucks: 180
 - Cost/fatality: \$500,000
- Expected injuries: 200
 - Cost/injury: \$70,000
- Expected trucks damaged: 3,000
 - Cost to repair: \$1,200/truck

TRR Benefit Cost Analysis

- Option 1, 100% reduction: Steel plate for 6x10⁶ trucks
 - Cost = \$84,000,000
 - Benefits = $180(\$5 \times 10^5)$ fatalities + $200(\$7 \times 10^4)$ injuries + $3,000(\$1200)$ damages
= \$107,600,000 (upper limit)
 - B/C = $107.6/84 = 1.3$ for ~ 100% reduction
- Option 2, Lexan plate, 95% reduction: B/C = $[107.6 \times 10^6 \times 0.95]/[\$4 \times 6 \times 10^6] = 4.3$
- Option 3, Plastic lining, 85% reduction: B/C = 7.6
- What is best alternative? Other costs to consider?

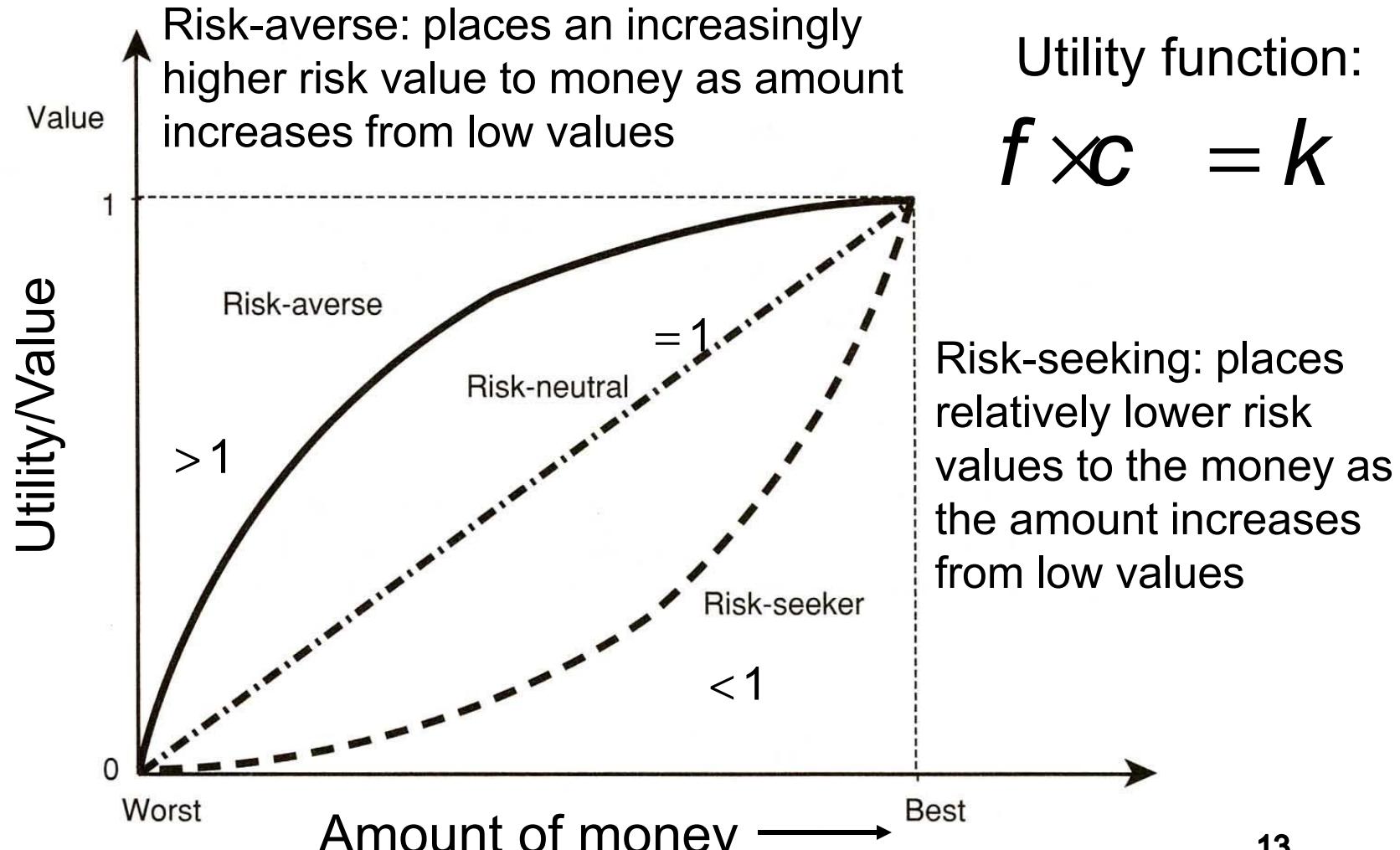
Transportation Risk Reduction Decision

- Option 3 yields the highest benefit-cost ratio (based on given benefits and costs)
- Decision should be based on these direct costs and on additional information:
 - Indirect costs: Reliability and Maintainability over suitable time, performance and resilience of hazard guards tested under conditions of use, possible litigation charges, law suit
 - Benefits to manufacturer reputation, Environmental and public health benefits
 - More analysis of probabilities of occurrences
 - Willingness to accept risk; risk aversion

Value of Money

- Difficult to estimate actual \$ amounts of costs and benefits (such as effects on company reputation); so ranges can be estimated.
- Monetary estimates can be converted to utilities for costs and benefits.
- Because of indirect and direct factors that affect risk perception and risk aversion, the value of money to the risk taker is often not linear with the risk level
- A project with known cost is preferred by a risk-averse person (or facility) to a similar project with an uncertain cost.

Review: Risk Value a Function of the Monetary Value:



Value of Money Example for Stakeholders and Public

- Engineering project with **known cost** of \$ 5×10^5 compared to a similar project with **uncertain cost** with equal probability within \$ 3 to 7×10^5 (expected/average cost = \$ 5×10^5).
- Risk neutral: no prior preference
- Risk averse: prefer 1st project (certain cost)
- Risk seeking: prefer 2nd project (additional risk accepted for potentially greater profit)

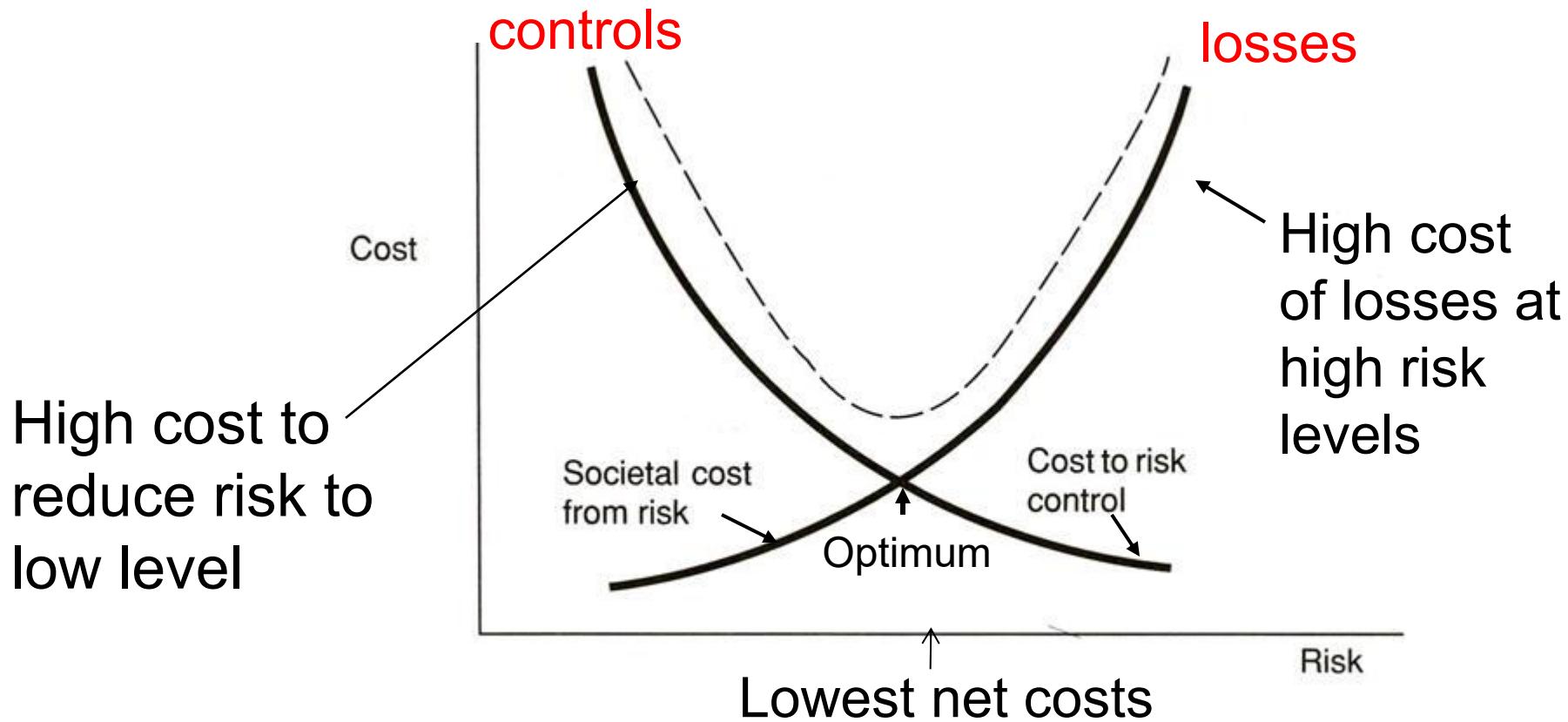
Fallacy of Zero Risk: Regulators, Stakeholders

- Some regulators on moral grounds have opposed economic risk models by arguing that cost should not be a significant factor of risk management.
- High-cost, low-benefit safety decisions to obtain near zero risk, however, can result in
 - challenges to business sustainability
 - reduced levels of organization safety and performance and
 - risk transferred elsewhere with a similar or greater overall risk.

Cost-Effectiveness Balance

- Decisions based on the comparison between the cost for **taking** the risk and the cost for **controlling** the risk.
- Assumption of cost-effectiveness: the residual risk level (following risk reductions) is acceptable.
- Cost of risk control decreases as willingness to accept risk increases.
- Find choices for optimum risk control to balance costs to Plant and costs to Society.

Costs vs. Risk: Costs of Risk and Control

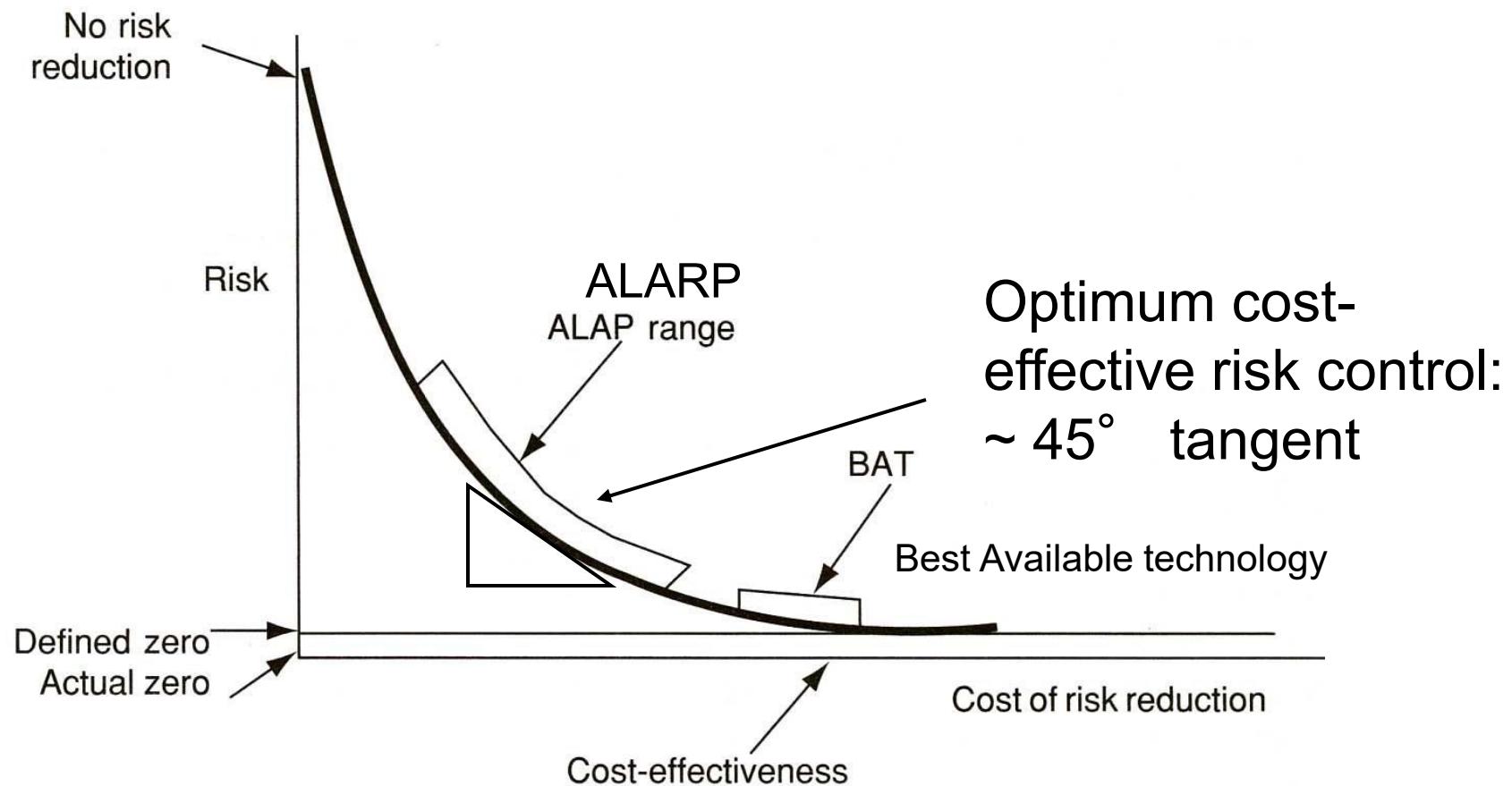


Obtain an optimum **working range** near this optimum region of control costs and loss risks.

Cost of Risk Control

- Optimum control: *most cost-effective region* is near a 45° tangent line on the risk vs. cost curve
- ALARP, *as-low-as-reasonably-practicable* region of acceptability from risk reduction actions
- BAT, *best available technology* region uses the most sophisticated equipment and often at exorbitant prices to drive a portion of the overall risk as close as possible to zero.

Risk vs. Cost Regions for Cost of Risk Control



ALARP Region Incremental Reduction Targets

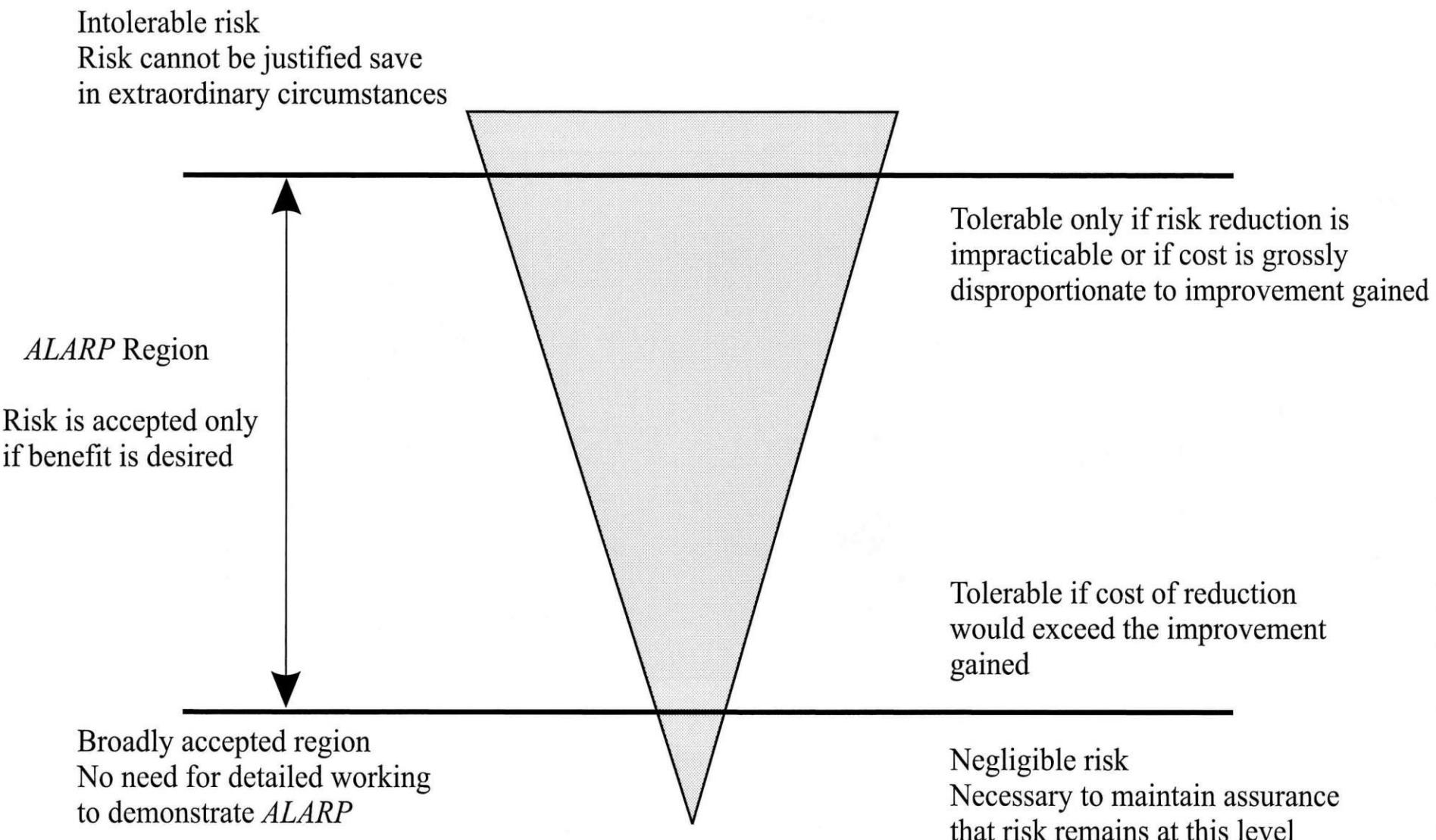


Figure 10.21 *ALARP* principle (as low as reasonably practicable)

(Jordaan, 2005)

Cost-Benefit Curves and Tolerable Risk

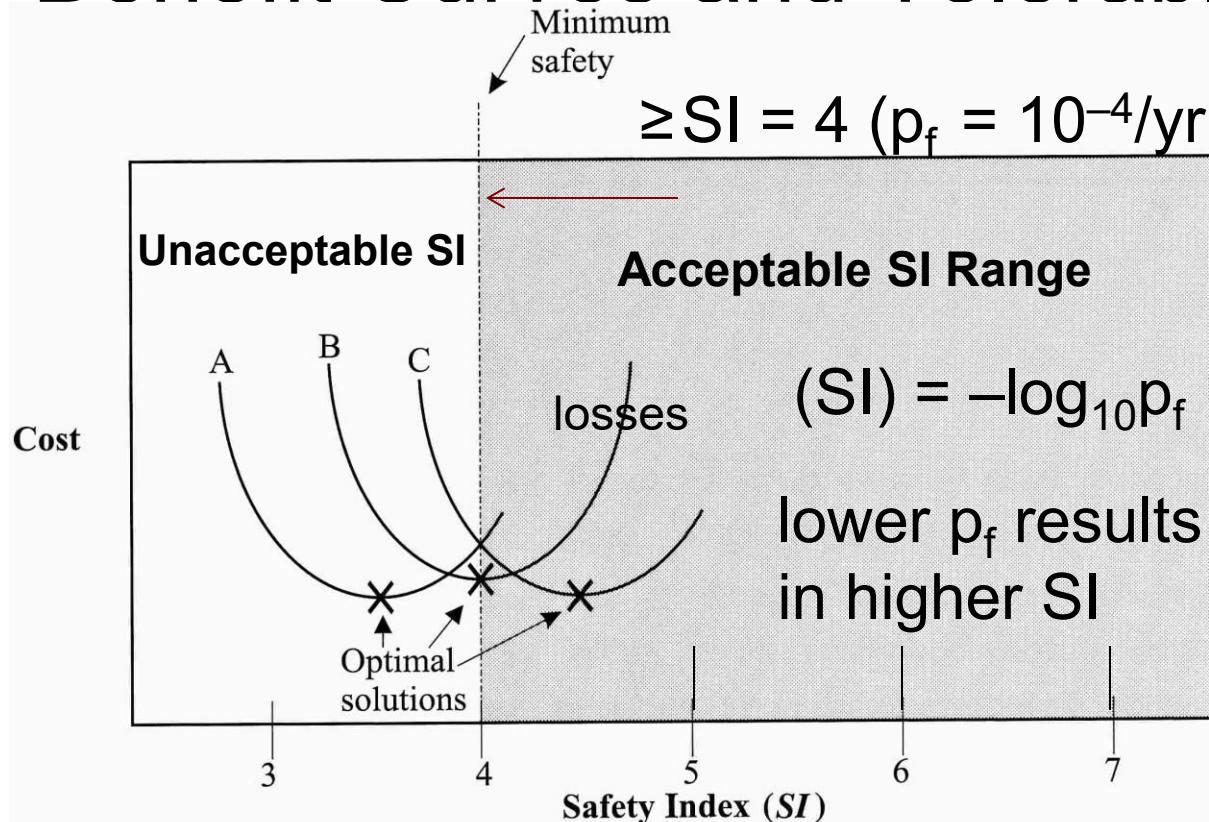


Figure 10.20 Tradeoff between optimal cost and safety: $SI = -\log_{10} p_f$

(Jordaan, 2005)

Cost benefit alternative ranges must be consistent with the tolerable or **Acceptable Risk Range** set for the application and type of risk within the estimated conditions and uncertainties.

Safety Index (SI) = $-\log_{10} p_f$, where p_f is probability of fatality or failure, so the smaller the p_f , the greater the SI.

Risk-Effectiveness Analysis, R-EA

Without converting Risk to Monetary Value

- Measure the risk reduction ability of plant actions (or of regulations), e.g., per life saved

$$RE = \frac{S}{\sum_{i=1}^n F_i C_i} = \frac{\text{Cost}}{\text{Risk}}$$

Risk prior Risk following

RE = risk reduction effectiveness

S = cost of a risk reduction

F_i = freq of scenario i ; C_i = consequence of i

F'_i , C'_i = freq, conseq. of scenario i following S

Risk-Effectiveness Example

- Addition of a prevention measure S costs US\$ 1.5 million/yr.
 - S reduces the fatality frequency ($1 \times 10^{-5}/\text{yr}$) by a factor of 10.
 - S reduces # fatalities from 1500 to 100/yr
 - Calculate the RE of S.

$$RE = \frac{US\$1.5 \times 10^6}{(1 \times 10^{-5} \times 1500) \times (1 \times 10^{-6} \times 100)} \quad 1 \times 10^8 \text{ US\$ / life saved}$$

- $1/RE : (\text{life saved})/(\text{cost of S})$
 - Decision can involve additional issues, e.g., public perception of the value placed on a statistical life.

Risk Acceptance Criteria

- Criteria for acceptance have been based on relative comparisons:
 - Compare calculated risk, frequency, or exposure to a hazard with historical levels of same or similar hazards
 - Compare risk levels of observed events with previously estimated risk levels of exposure to the same hazard
 - Compare a risk and risk acceptance with more familiar risks in society and daily life (e.g. individual fatality risk observed to be 10^{-4} /person-yr for volunteer sports)

Individual Risk Criteria

- Tolerable (or acceptable) risk criteria have been proposed for an individual, a facility, and for society.
- A tolerable level of individual risk is historically founded on the familiar risk of natural hazards and risk of disease.
- **Individual fatality risk is tolerably low if it is \leq fatality risk of natural hazards $\sim 10^{-6}$ yr $^{-1}$ (SI = 6).**
- **Individual risk is unacceptably high if it is $>$ fatality risk of disease $\sim 10^{-3}$ yr $^{-1}$ (SI = 3).**

Safety Index (SI) = $-\log_{10}p_f$, where p_f is probability of fatality.
SI is used as a measure of safety in risk management

Everyday Risk Levels

- Higher risk levels are generally more acceptable for familiar events than for unfamiliar events.
- Voluntary Risk: Accidental risk of 10^{-4} fatality/yr (SI = 4) for 10-14 year old (young, healthy) age group is the basis for this risk criterion for voluntary activities (such as working in a plant)
- NRC (Nuclear Regulatory Commission) assigns maximum voluntary risk level as having a death rate of $10^{-4}/\text{yr}$. This is broadly accepted

Risk Measure for an Individual or Facility, or a Group of People or Facilities

- **Individual risks** –probability of exposure of a person, system, or plant to a hazard or a particular level of the hazard. Ex.: risk of injury or fatality for an individual performing work in a plant.
Fatality $\leq 10^{-4}$ yr $^{-1}$, (Voluntary standard)
- **Societal risks** –cumulative frequency or probability of outcome for a number of people (or facilities) affected, by a specified consequence level from exposure to specified hazards.
Fatality $\leq 10^{-6}$ yr $^{-1}$, SI = 6, (Involuntary standard)
- So Fatality $\leq 10^{-4} - 10^{-6}$ yr $^{-1}$, (SI $\geq 4-6$) is used to determine effective distances of people and communities from a plant based on risk analysis consequence and risk contours

Risk Acceptance Criteria: Review

TABLE 7.1
Considerations in Establishing Involuntary Individual Risk Acceptance Limits

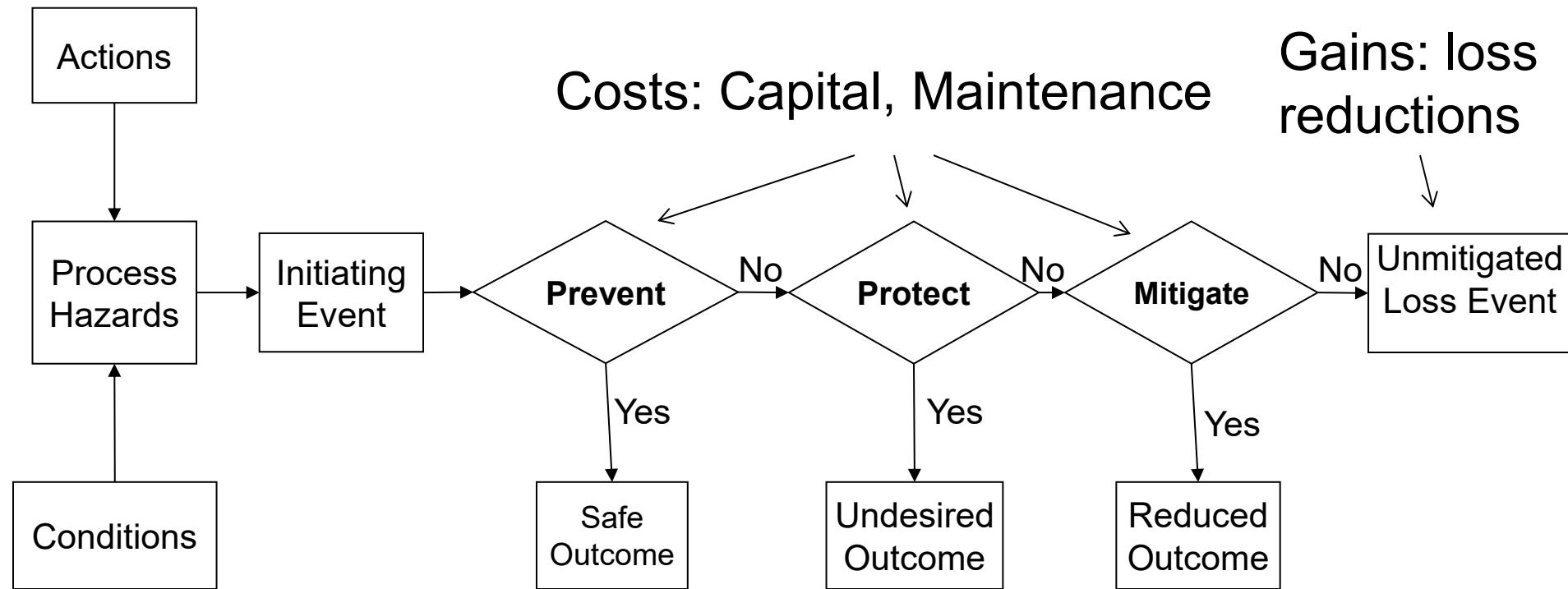
Fatality Risk Level per Year	Considerations
10^{-3} Fatality rate (illnesses)	This level is unacceptable to everyone. Accidents exposing hazards at this level are difficult to find. When risk approaches this level, immediate action is taken to reduce the hazard.
10^{-4} voluntary	This level is acceptable; however, individuals would like to see that public money is spent to control a hazard exposure at this level (e.g., placing traffic signs).
10^{-5} air travel	While acceptable, the individuals in public recognize this level of risk, but generally feel comfortable about it. At this level, individuals may accept inconveniences to avoid this level of risk, such as avoiding air travel.
10^{-6} involuntary (natural hazards)	Generally acceptable with no great concern. Individuals may be aware of the risks at this level, but feel that they cannot happen to them. They view this level of risk as “an act of God.”
Less than 10^{-6}	Acceptable. Individuals are not generally aware of this level of risk.

Risk Control

- Risk control, management strategies
 - internal
 - Reduce frequency, e.g., reduce concentration of a corrosive agent in pipe.
 - Add hazard barriers to contain toxicants
 - Test for hazard barrier dependencies and act to reduce dependencies
 - external
 - Facility pay externality tax equal to cost of losses due to hazardous events, such as a significant release levels of a toxic gas

Process Incident Scenario Development

Economic balance of costs/gains:



LOPA to reduce Risk: _____
Pr of failure, and Consequences

Flammable Release in a Tunnel: Event Tree

Example of Data for a Cost/Gain Balance

Spill of flammable material	Flammable concentration of gases	Automatic ventilation fails	Automatic alarm fails	Fire Ignition	Automatic sprinklers fail	Outcome (consequences)
E_0						
						O_1 : fire/explosion, casualties
				yes, E_4	p_{f5}	O_2 : extinguishing, injuries
				no	$1-p_{f5}$	O_3 : intoxication casualties/injuries
			yes, E_3	p_{f4}	yes, E_5	O_4 : fire/explosion, no casualties
			no	$1-p_{f4}$	no	O_5 : extinguishing, no injuries
				yes, E_4	p_{f5}	O_6 : gasified environment, no intoxication
				no	$1-p_{f5}$	O_7 : exhaustion of gas
				yes, E_5		O_8 : intoxication casualties/injuries
				no		O_9 : gas-filled environment, no intoxication
			no			O_{10} : exhaustion of gas
		yes, E_1	p_{f2}			
		no	$1-p_{f2}$			
			yes, E_2			
			no			
				yes, E_3		
				no		
					yes, E_4	
					no	

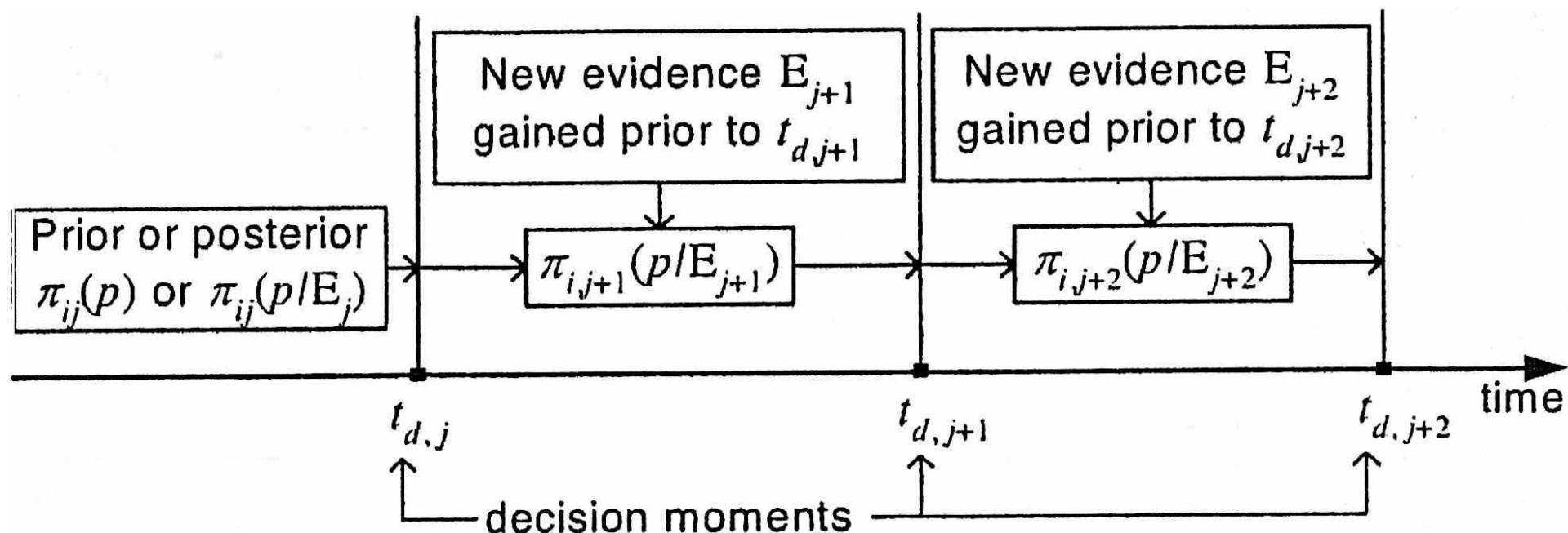
Figure 1. Scenarios of an accident initiated by a spill of flammable material in a tunnel
(Zavadskas, 2008)

Decision Making Under Uncertainty

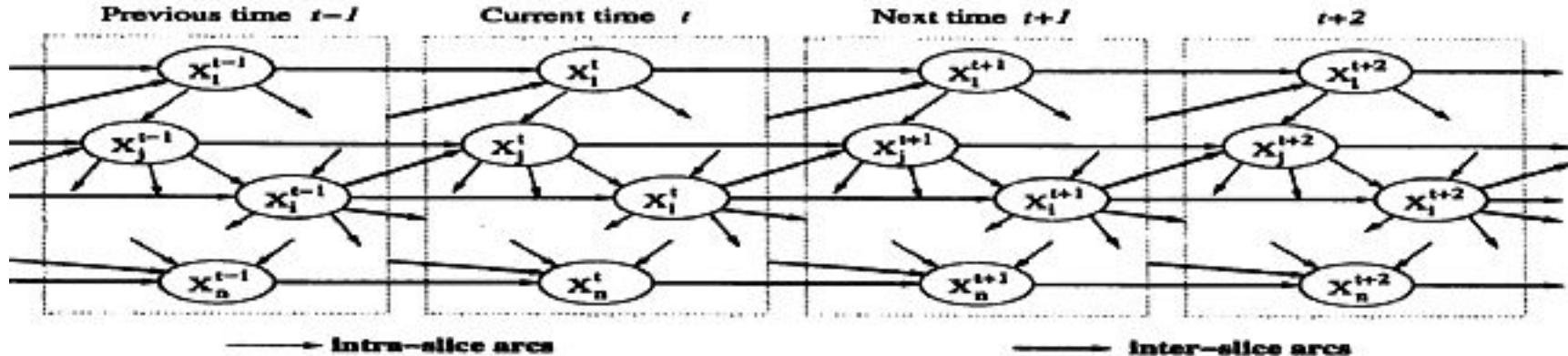
- Decision making, about uncertain events and using uncertain information, begins with search for data and information from all categories: generic, expert judgment, and current system specific.
- New decisions can be made based on updated information from time to time as new data becomes available (using Bayesian analysis) to facilitate a Dynamic Risk Assessment and Risk Management

Information and Updates for Risk Decision Making, e.g., Cost Effective Hazard Guards

Dynamic Decision Making at time $j, j+1, j+2, \dots$ is based on all available information at each decision time by continual Bayesian updating of hazard guard failure distributions resulting in uncertainty reductions to support optimum decision-making at each successive time increment.

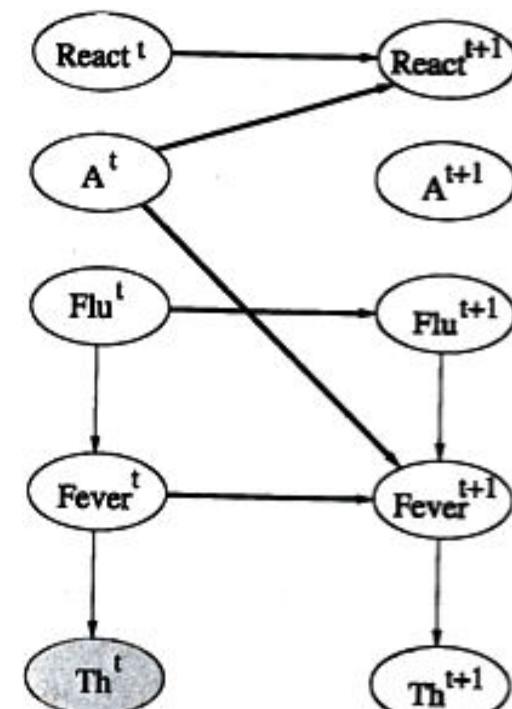


Time Slice Dynamic Bayesian Network, DBN



DBNs model temporal relationship of a variable by including additional variables at future or past times in time slices.

For this example, a patient's Flu changes over time by taking an aspirin at the current time t , A^t , to result in a reaction at the next time step, React^{t+1} and it may reduce fever in Fever^{t+1} , which also depends on fever at time t , Fever^t , as measured by thermometer, Th^{t+1} , and at later time slices, $t+2, t+3, \dots$



Given the evidence, updating the entire DBN at all time slices for a probabilistic projection.

Risk Communication and Risk Management

Unit 18

Spring 2022

References

- Modarres, M., *Risk Analysis in Engineering*, Taylor&Francis, 2006 (Modarres, RAE)
- Fischhoff, Baruch and Kadvany, J., *Risk – a Very Short Introduction*, Oxford University Press, 2011 (Fischhoff, 2011)
- Cameron, I and Raman, R., *Process Systems Risk Management*, Elsevier, 2005 (Cameron, PSRM)
- Siegrist, M., Earl, T.C., and Gutscher, H., *Trust in Risk Management: Uncertainty and Scepticism in the Public Mind*, Routledge, 2012 (Siegrist, 2010)
- National Research Council, *Science and Judgment in Risk Assessment*, National Academy Press, 1994 (NRC, 1994)
- Modarres, M., M. Kaminskiy, and Vasiliy Krivtsov, *Reliability Engineering and Risk Analysis*, Taylor & Francis, 2010 (Modarres, RERA)
- Jordaan, Ian, *Decisions Under Uncertainty– Probabilistic Analysis for Engineering Decisions*, Cambridge University Press, 2005 (Jordaan, 2005)
- Fullwood, R., *Probabilistic Safety Assessment in the Chemical and Nuclear Industries*, Butterworth-Heinemann, 1999 (Fullwood, PSA)
- Lundren, R. and McMakin, A., *Risk Communication*, 3rd ed, Battelle Press, 2004 (Lundren, RC)
- NASA, *Probabilistic Safety Assessment Procedures Guide*, Office of Safety and Mission Assurance, 2002 (NASA, PSAPG)
- NRC (National Research Council), *Improving Risk Communication*, National Academy Press, 1989 (NRC, IRC)

Risk Communication

Technical problem announcement



Technical problem explanation



FIGURE 2-10 THE FLIGHT OR FRIGHT? (BY PERMISSION OF JESPER DELEURAN)

Risk Communication

Can be defined as:

- An interactive learning and partnering process of risk information and opinion exchange among individuals, groups, plant personnel, stakeholders, and institutions, including the media.
- Interaction example:
 - The media influences public perception and therefore influences public opinion. Based on responses the media receives from the public, the media responds back to the public within interactive feedback loops.

Risk Stakeholders

- Personnel at organization (engineers, managers, staff)
- Industrial societies, disciplines
- Information media
- Policy decision makers, regulators
- Public
- Experts

Objectives of Risk Communication

- To inform all Stakeholders and Decision Makers about potential risk scenarios and consequences of risk management options and important decisions.
 - **Partner** with stakeholders, **Learn**, and **Share information and responsibility** for decision making and communication.
 - **Reduce Bias**, settle misunderstandings by stakeholders and the public about hazards, uncertainty, and risk
 - **Educate & Prepare** for potential adverse events and their consequences. **Inform** what to do in an emergency. Prepare the LEPC, Local Emergency Planning Committees

Risk Perception Cases

Contrast risk perception for these cases:

- Three Mile Island, 1979
 - Release of radiation, but no fatalities
 - But this incident fundamentally altered the public attitude toward nuclear power
- US traffic losses
 - 42,000 fatalities per year (approximates to catastrophic since it equates to a total of 280 airline failures/yr, 150 fatalities/failure)
 - Yet auto accidents have not resulted in fundamental changes in people's preference to driving cars

Risk Perception Cases

- Perception differences in the two cases
- Nuclear power
 - The public perceives a lack of control
 - Need for this power source is not clear to public
 - Concern about potential for catastrophic events
- Motor vehicles
 - People perceive more control with a more familiar technology
 - Need for vehicles and the benefits are clearer and direct
 - Risks of numerous accidents are more accepted

Ranking by public

TABLE 9.2
Rankings of Perceived Risks for 30 Activities and Technologies

LWV Ranking	Activity or Technology	Expert's Ranking
1	Nuclear power	20
2	Motor vehicles	1
3	Handguns	4
4	Smoking	2
5	Motorcycles	6
6	Alcoholic beverages	3
7	Private aviation	12
8	Police work	17
9	Pesticides	8
10	Surgery	5
11	Firefighting	18
12	Large construction	13
13	Hunting	23
14	Spray cans	26
15	Mountain climbing	29
16	Bicycles	15
17	Commercial aviation	16
18	Electric power (nonnuclear)	9
19	Swimming	10
20	Contraceptives	11
21	Skiing	30
22	X-rays	7
23	High school and college football	27
24	Railroads	19
25	Food preservatives	14
26	Food coloring	21
27	Power mowers	28
28	Prescription antibiotics	24
29	Home appliances	22
30	Vaccinations	25

Ranking by experts

Communication of Benefits

Transform Fear to Understanding:

- Expected benefits of accepting risk (given that it is appropriately managed): products, profits, reduced losses
- Direct beneficiaries (person, stakeholders, society) of the risk.
- Explain balance and range between risks and benefits, e.g., ALARP cost effectiveness balance or risk effectiveness ($RE = Cost/\Delta R$). Show how target ranges were calculated.
- Use decision tools: B/C , $RE = C/\Delta R$, such as risk reductions within ALARP consistent with acceptable risk criteria regions.
- Show the magnitude and importance of the benefits of profits and reduced costs through demonstrated fewer upsets at your plant

Risk Management

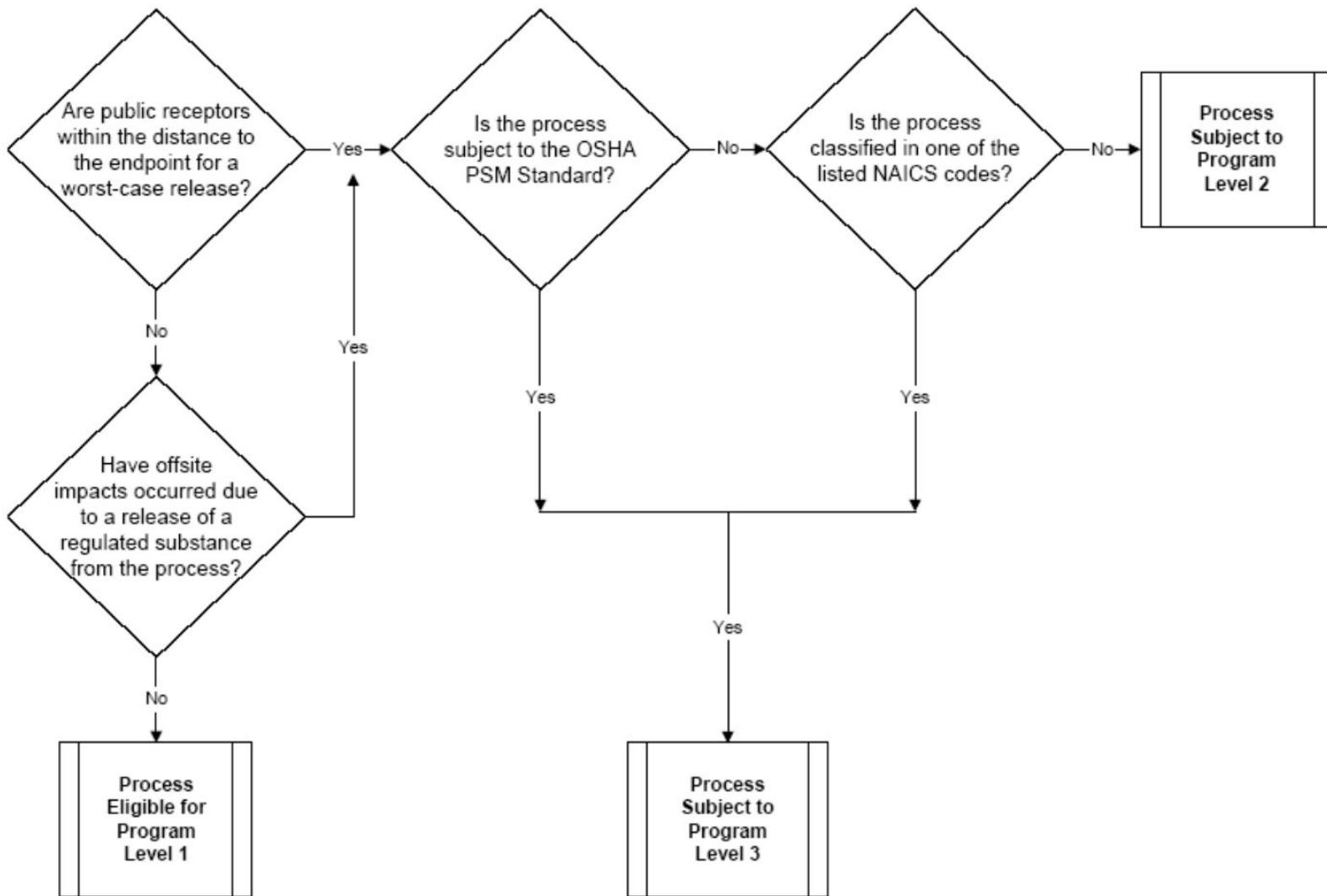
What Types of Risk? And for Whom a Risk?

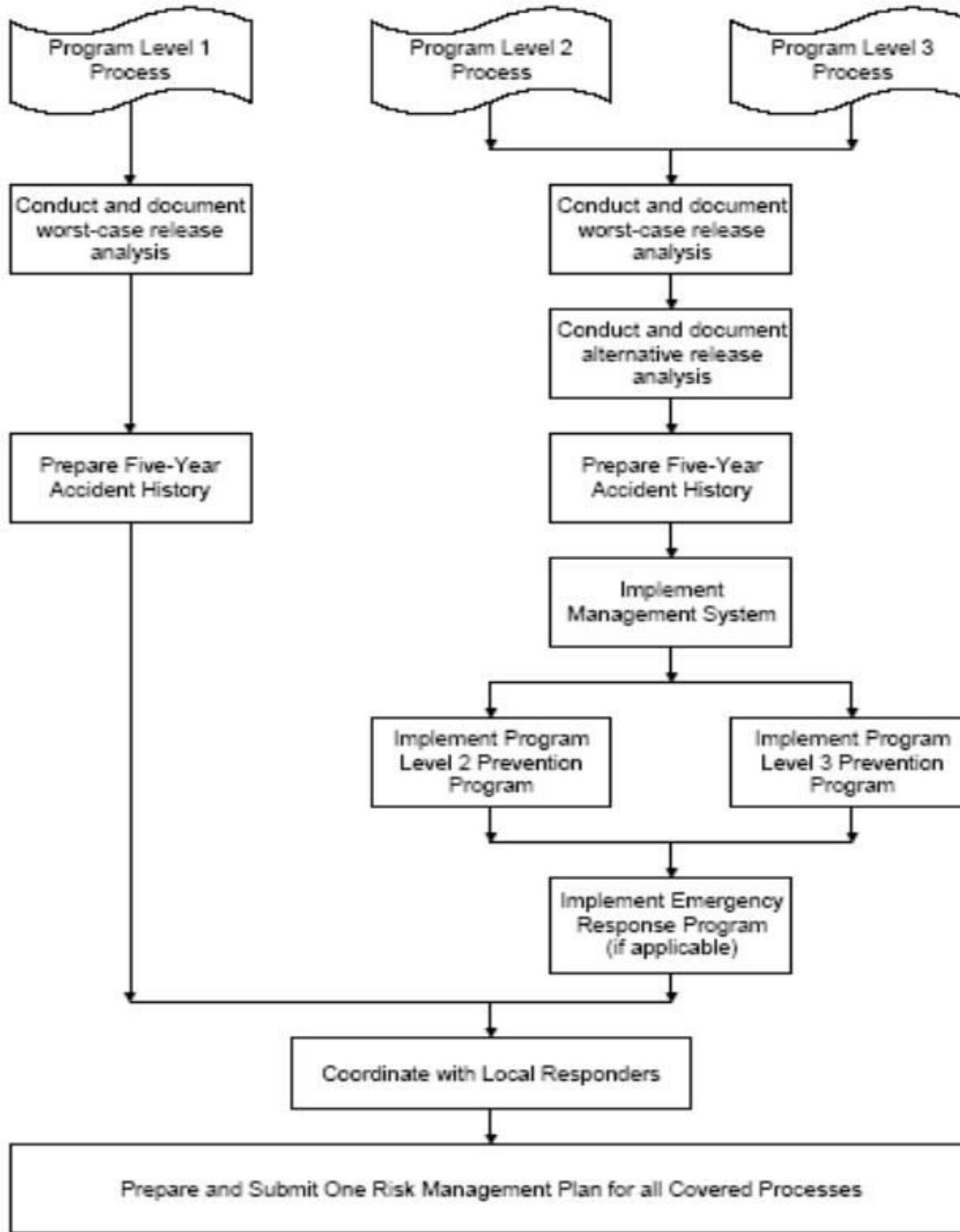
- Large variety of risks, as discussed in class:
 - Economic risks, political risks
 - Financial/trade risks,
 - Insurance risks,
 - Cyber risks,
 - Project risks (delivery time – money – quality),
 - Environmental risks,
 - Safety risks: Personal Safety and Process Safety risks
- Risk for Society, for the Company, and for you personally can be different
- Risk can be subjective: '*What I feel as a risk, doesn't bother you*'.
- Risk Analysis is relative (= comparing) risk

OSHA* Process Safety Management (PSM) Standard

- Process Safety Mgmt of Highly Hazardous Chemicals (PSM), 1992
 - general requirements for managing hazardous substances; with focus to protect on-site people
- 14 elements to manage chemicals, prevent major incidents, and protect the safety of the workplace:
 - Employee Participation
 - Process Hazard Analysis (PHA)
 - Training
 - Pre-startup Safety Review (PSSR)
 - Hot Work Permit
 - Incident Investigation
 - Compliance Audit
 - Process Safety Information (PSI)
 - Operating Procedures
 - Contractors
 - Mechanical Integrity
 - Management of Change (MOC)
 - Emergency Planning
 - Trade Secrets

EPA's Risk Management Plan (RMP)





CCPS* Guidelines for Risk Based Process Safety (RBPS)

Describes components of a Risk Based Process Safety Program

1. COMMIT to PROCESS SAFETY

Process Safety Culture

Compliance with Standards

Process Safety Competency

Workforce Involvement

Stakeholder Outreach

Asset Integrity and Reliability
Contractor Management
Training & Performance Insurance
Management of Change
Operational Readiness
Conduct of Operations
Emergency Management

2. UNDERSTAND HAZARDS AND RISK

Process Knowledge Management

Hazard Identification, Risk Analysis

3. MANAGE RISKS

Operating Procedures

Safe Work Practices

4. LEARN FROM EXPERIENCE

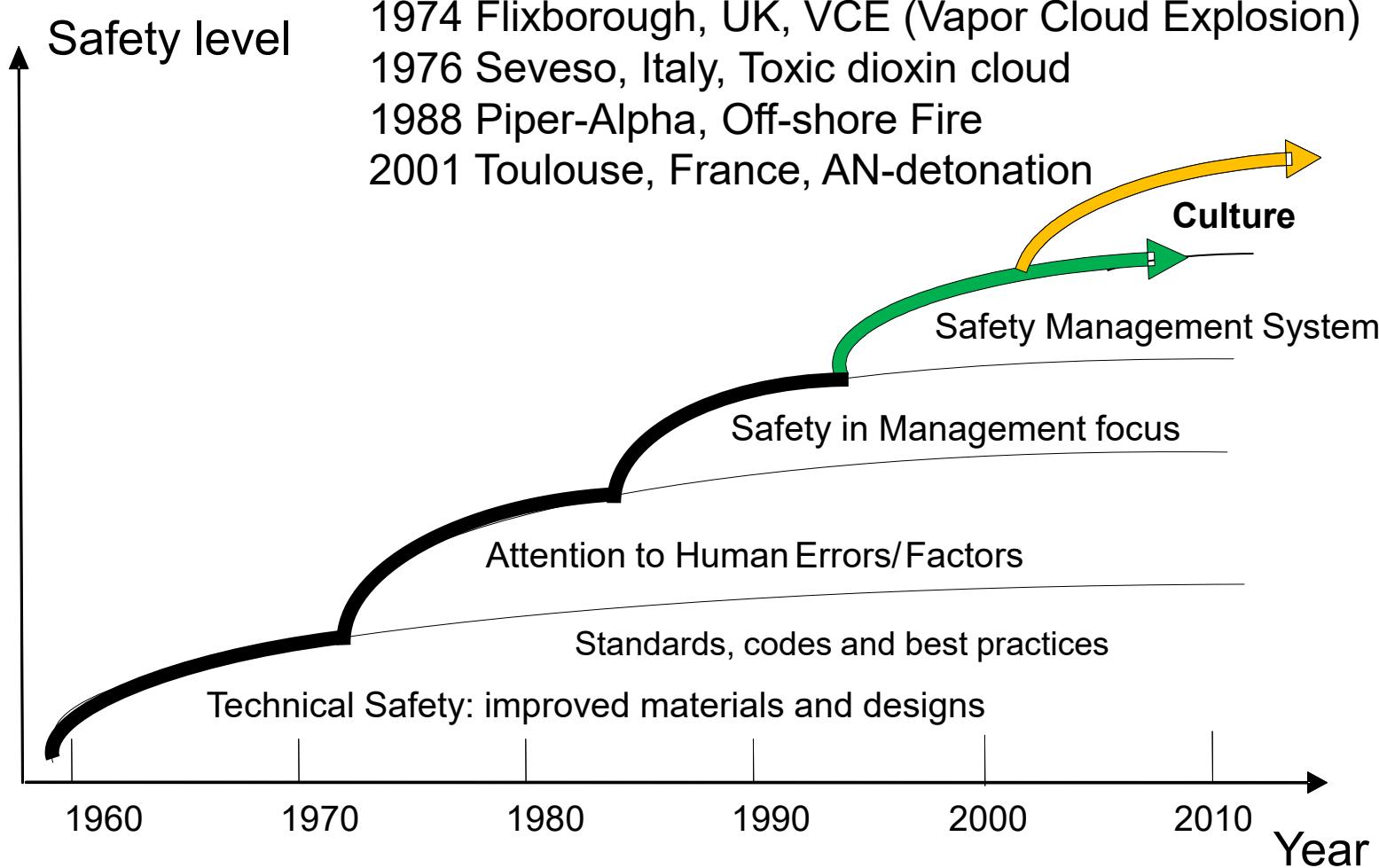
Incident Investigation

Measurement and Metrics

Auditing

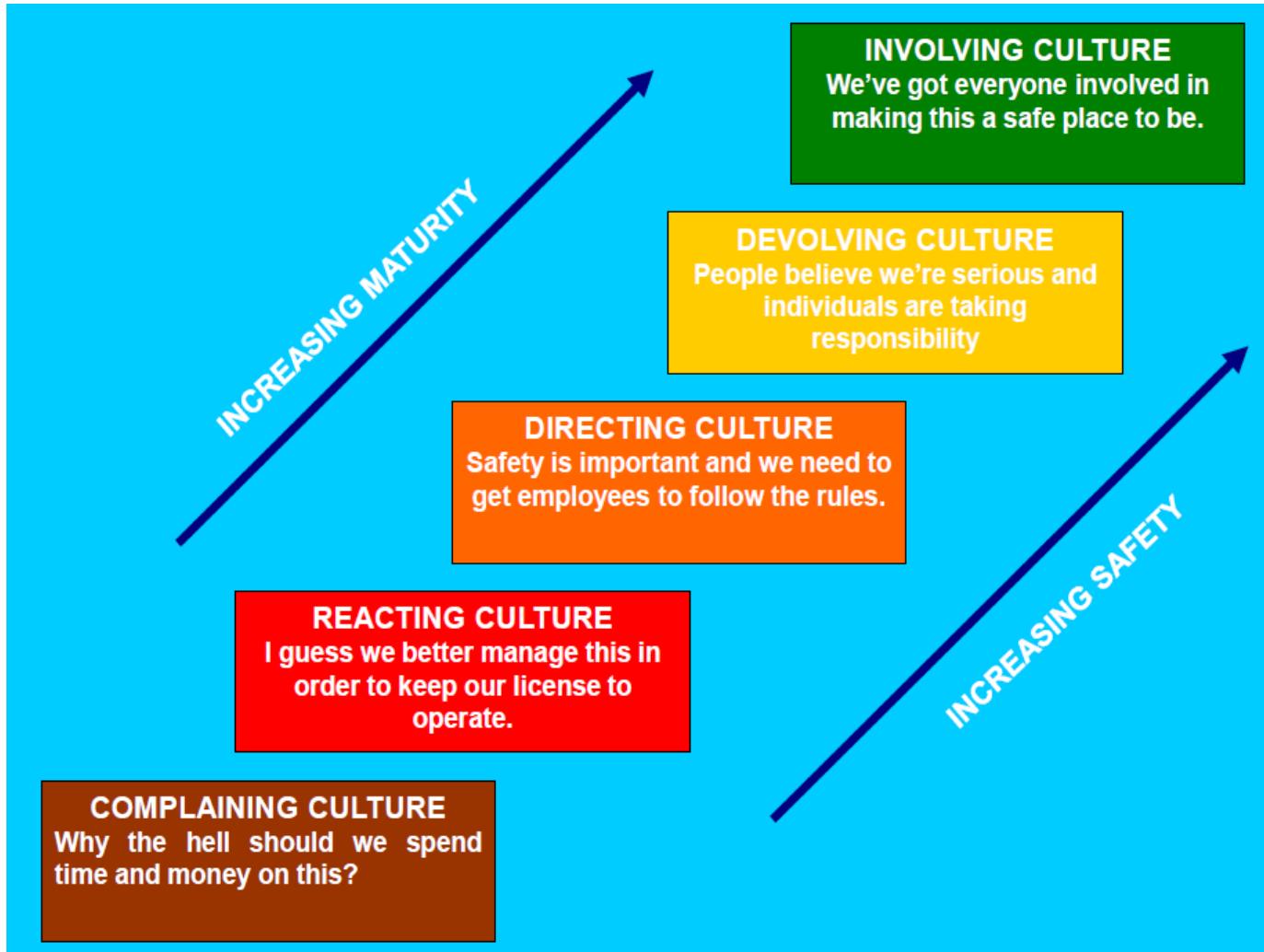
Management Review and
Continuous Improvement

History Process and Plant Safety; Contributing Factors



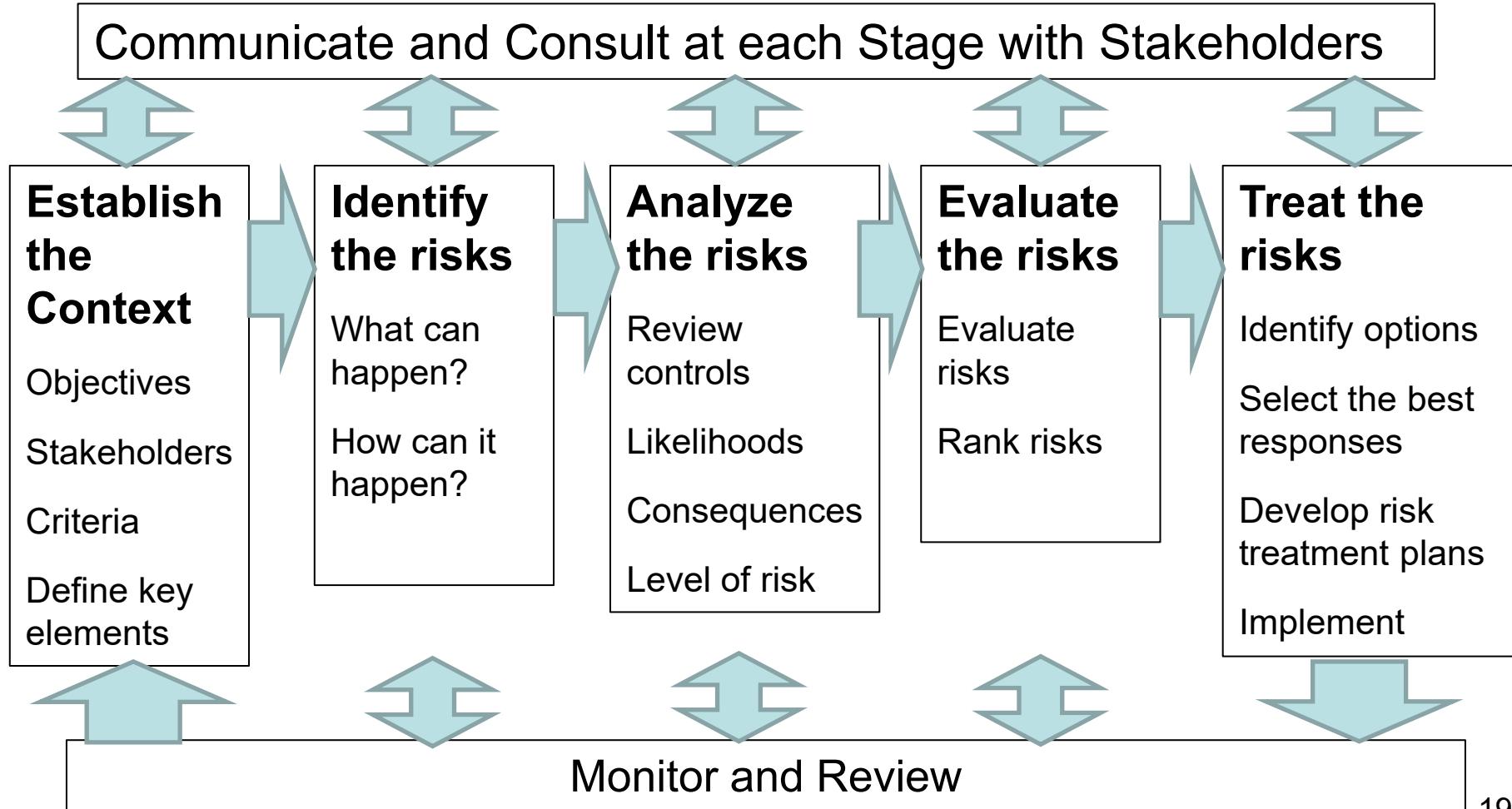
Problem of Risk Assessment: it often misses scenarios of real accidents!
We must focus on monitoring and updating as systems evolve in time.

HSE Safety Culture Maturity Model



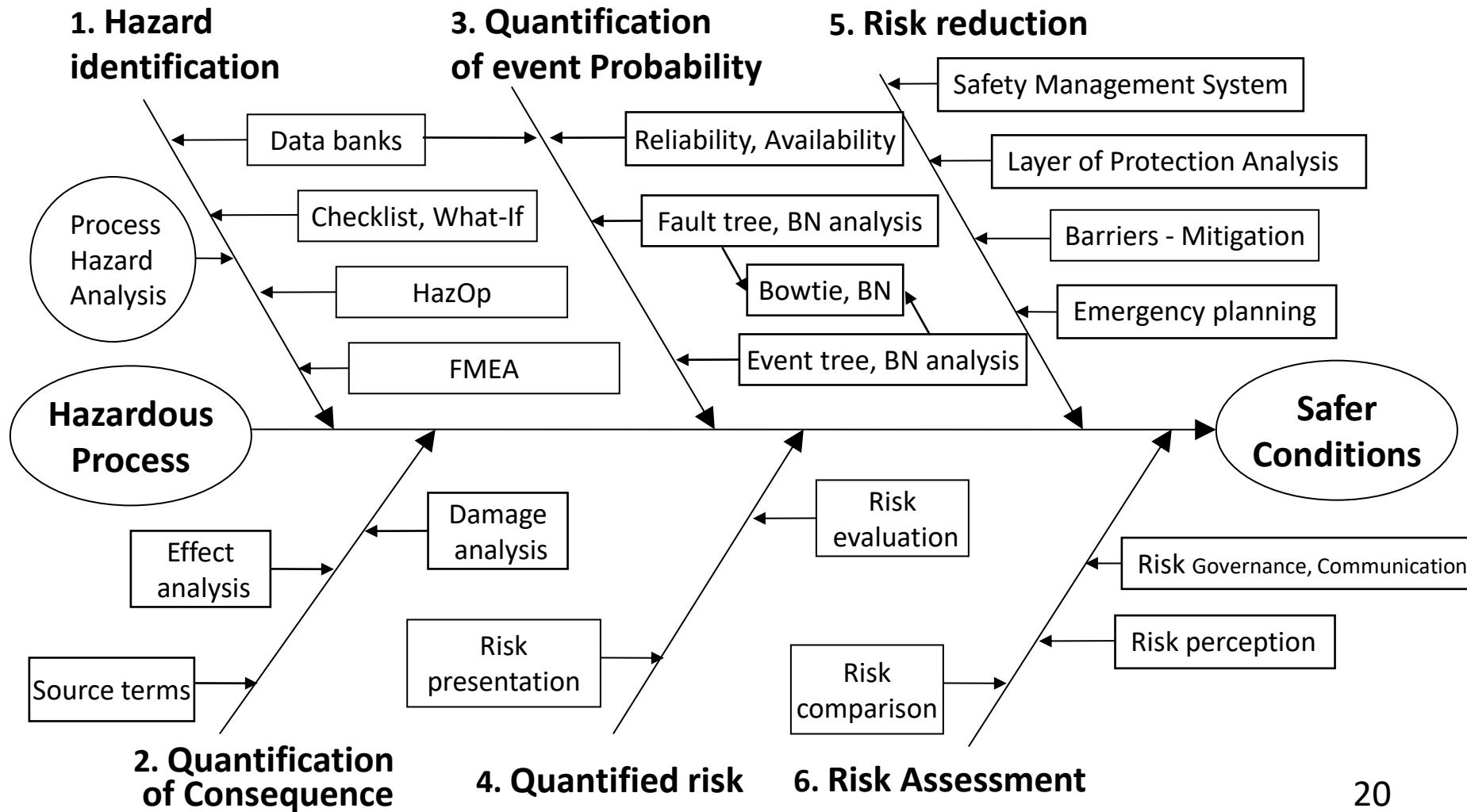
Risk Management

Cooper, D., Grey, S., Raymond, G., Walker, Ph., Project Risk Management Guidelines, Managing Risks in Large Projects and Complex Procurements, John Wiley & Sons, 2005, ISBN 0-470-02281-7

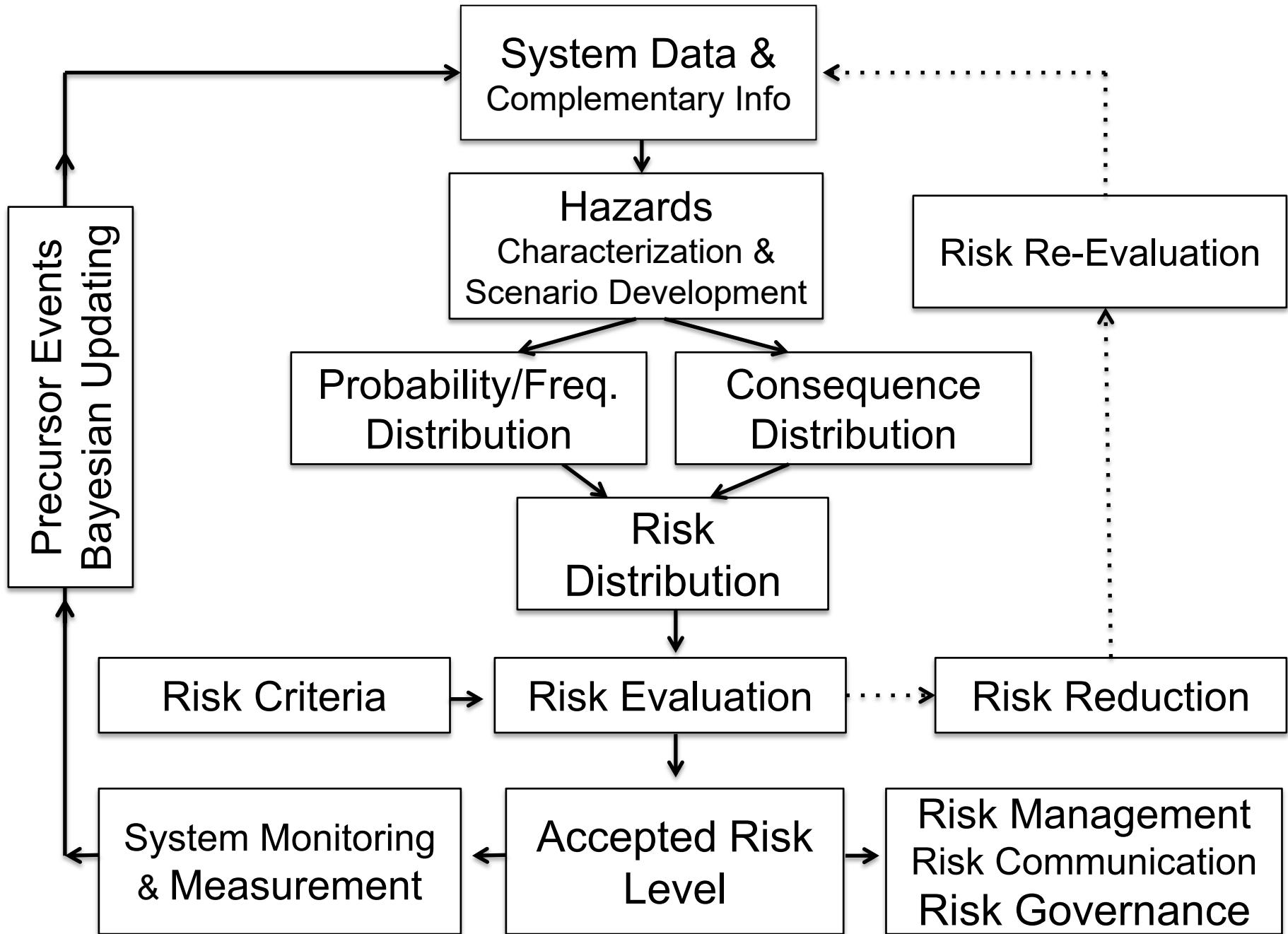


Process/Plant Risk Assessment Tools: RA

Six step Quantified Risk Analysis Sequence



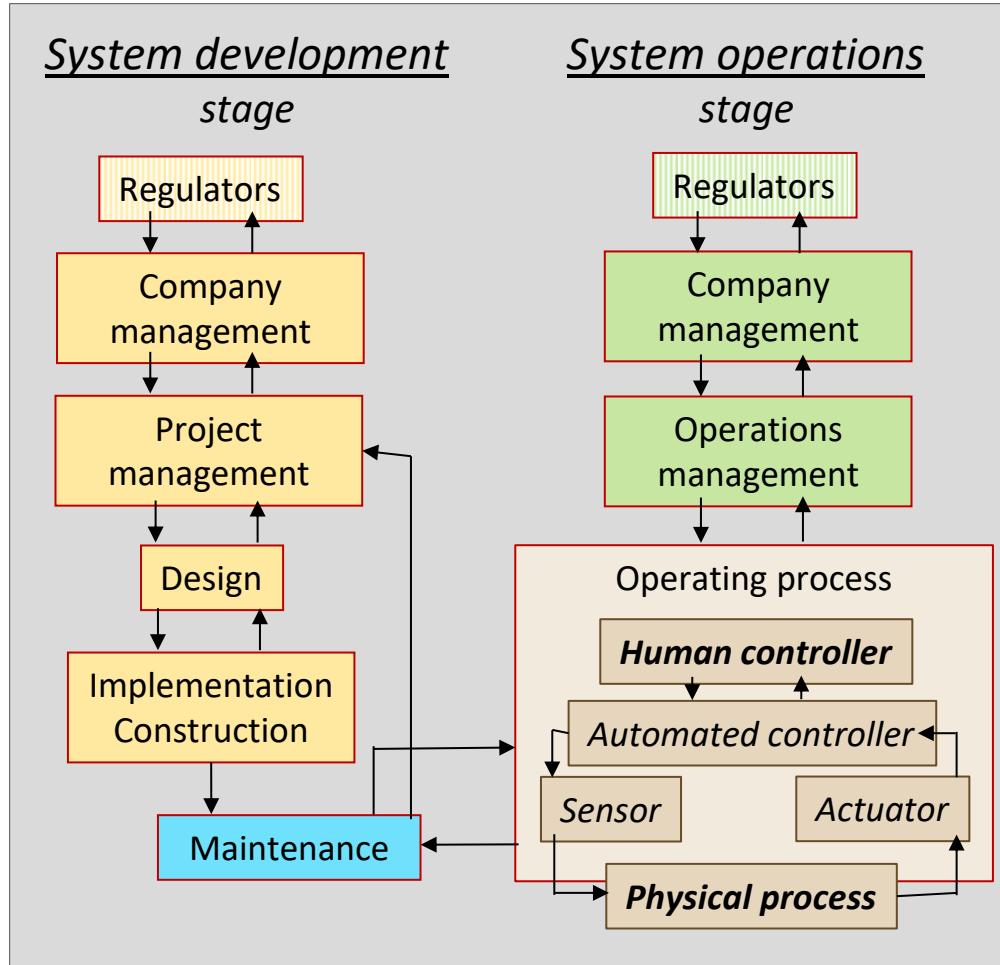
Risk Analysis Map



Complex Engineered Systems Safety:

Concepts of Jens Rasmussen and Nancy Leveson

Safety as a Control Problem



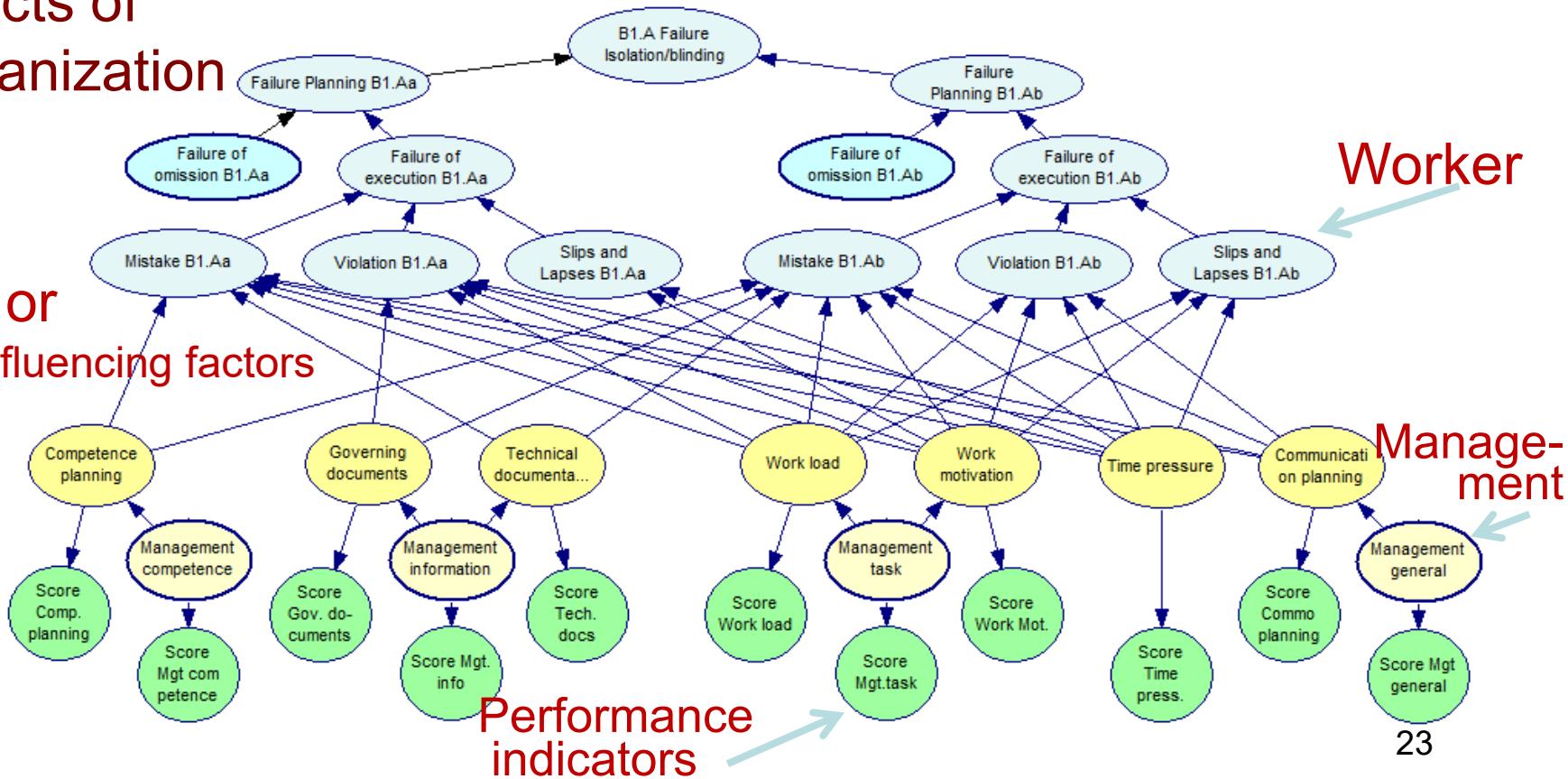
- System is more than the sum of parts
- Complex system: hierarchy of organizational levels.
- Complexity as an **emergent system hazard** that can be modeled and estimated

Socio-Technical Modeling of Human and Organizational Factors

- Vinnem et al. used Bayesian Network to show how Human error + Risk Influencing Factors (RIF) from Management influence failure in offshore operations

Effects of Organization

RIFs or
Risk Influencing factors



PDCA in Risk Management

- Risk management should have involvement from all levels of the organization (from the CEO to the frontline operator)
- Each level should actively implement the PDCA cycle:

Plan – Do – Check – Act



**Deming cycle
Management**

Indicators

If you can detect it, you can control it

- If a factor or influence under conditions affects your system, that factor or influence can be detected.
- Because the factor can be detected, it can be measured.
- Because it can be measured, it can be controlled to an extent to benefit your system.
- A simple measurement with a few data or even an estimate may be sufficient and therefore cost effective to lower uncertainty for more optimal decision making.

Companies Define Their Own Meaningful Performance Measures

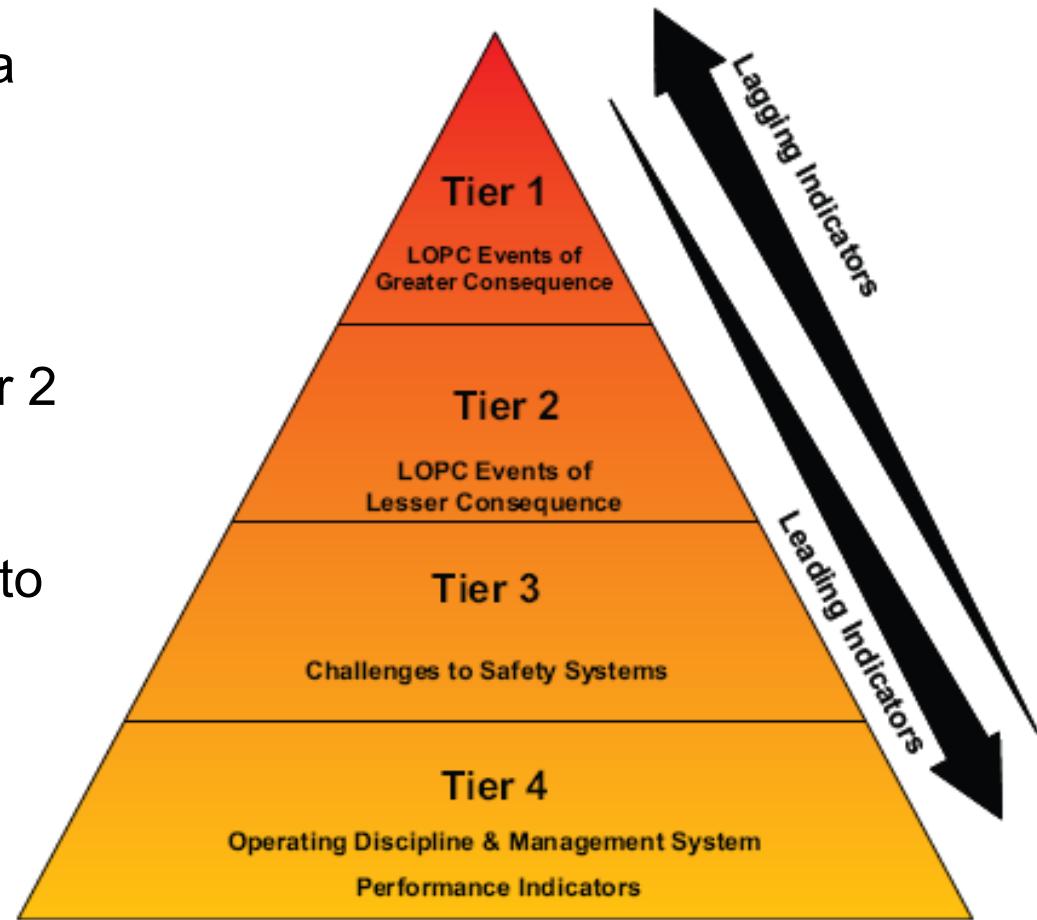
Safety performance measurement using indicators

Indicator ≡ Observed Variable

- Indicators become valuable when measured over a period of time or as a trend, and at multiple operations / sites
- Trend analysis looks at an indicator over a period of time to determine if there is a general sustained increase, decrease, or no discernible pattern

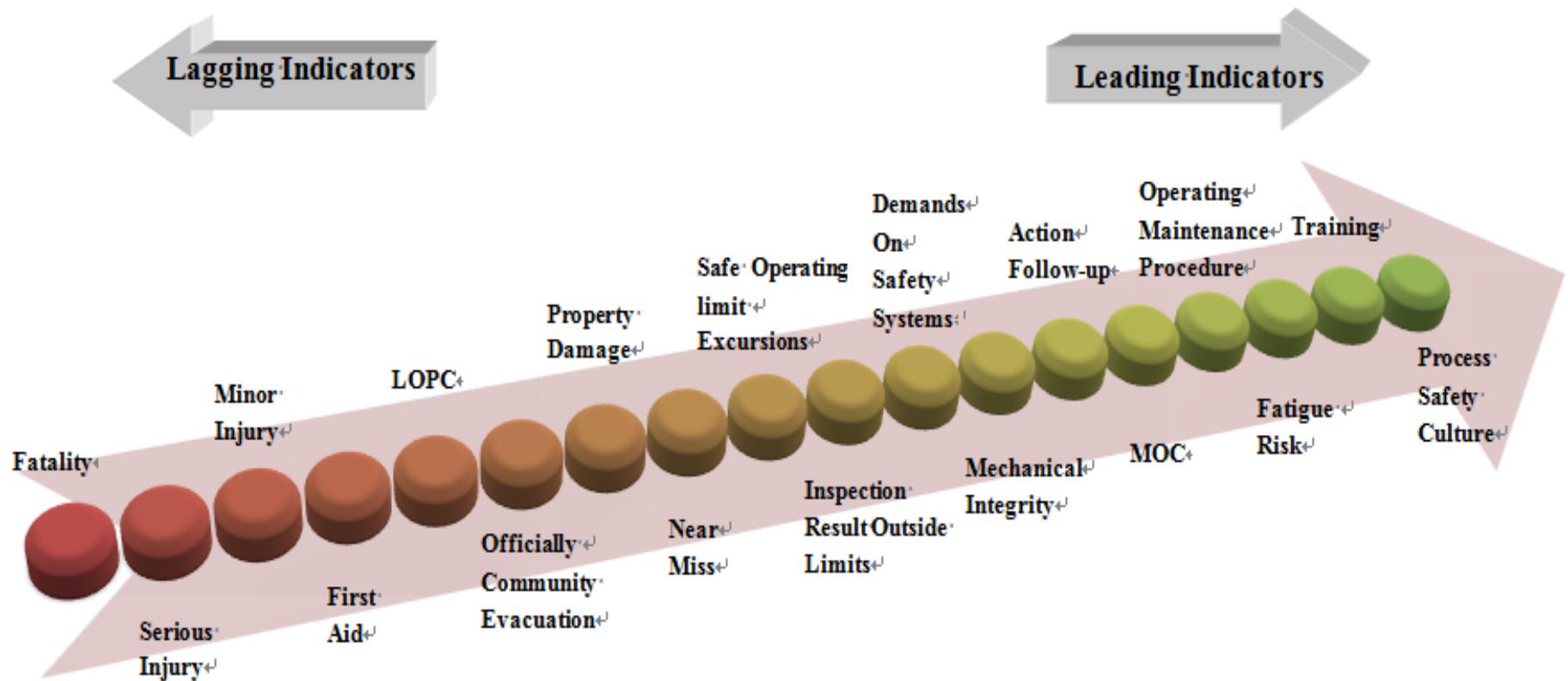
Process Safety Performance Indicators for the Refining and Petrochemical Industries

- Tiers of the pyramid represent a continuum of leading and lagging process safety indicators
- Loss of primary containment (LOPC) event results in a Tier 1 or 2
- Important to adopt appropriate indicators to measure challenges to the barrier system in Tier 3
- Precursor events and barrier system weaknesses in Tier 4



ANSI/API Recommended Practice 754, "Process Safety Performance Indicators for the Refining and Petrochemical Industries," First Edition, 2010.

Spectrum of Process Safety Indicators: Lagging vs. Leading Indicators



Process Safety Lagging and Leading Indicator Synthesis Scale

Trailing or Lagging Indicators

- Measurement of incidents; with intent to analyze and take steps to reduce risk and hazards
- Most safety indicators historically tend to be lagging
- Limited usefulness since they apply after the incident
- Also, one obtains fewer data for use in improving safety performance as safety improves
- Examples of lagging indicators:
 - ***Number of safety related on-the-job-incidents***
 - ***Trend in process safety incidents – loss of containment, fires, \$\$ damage, vapor releases, etc***

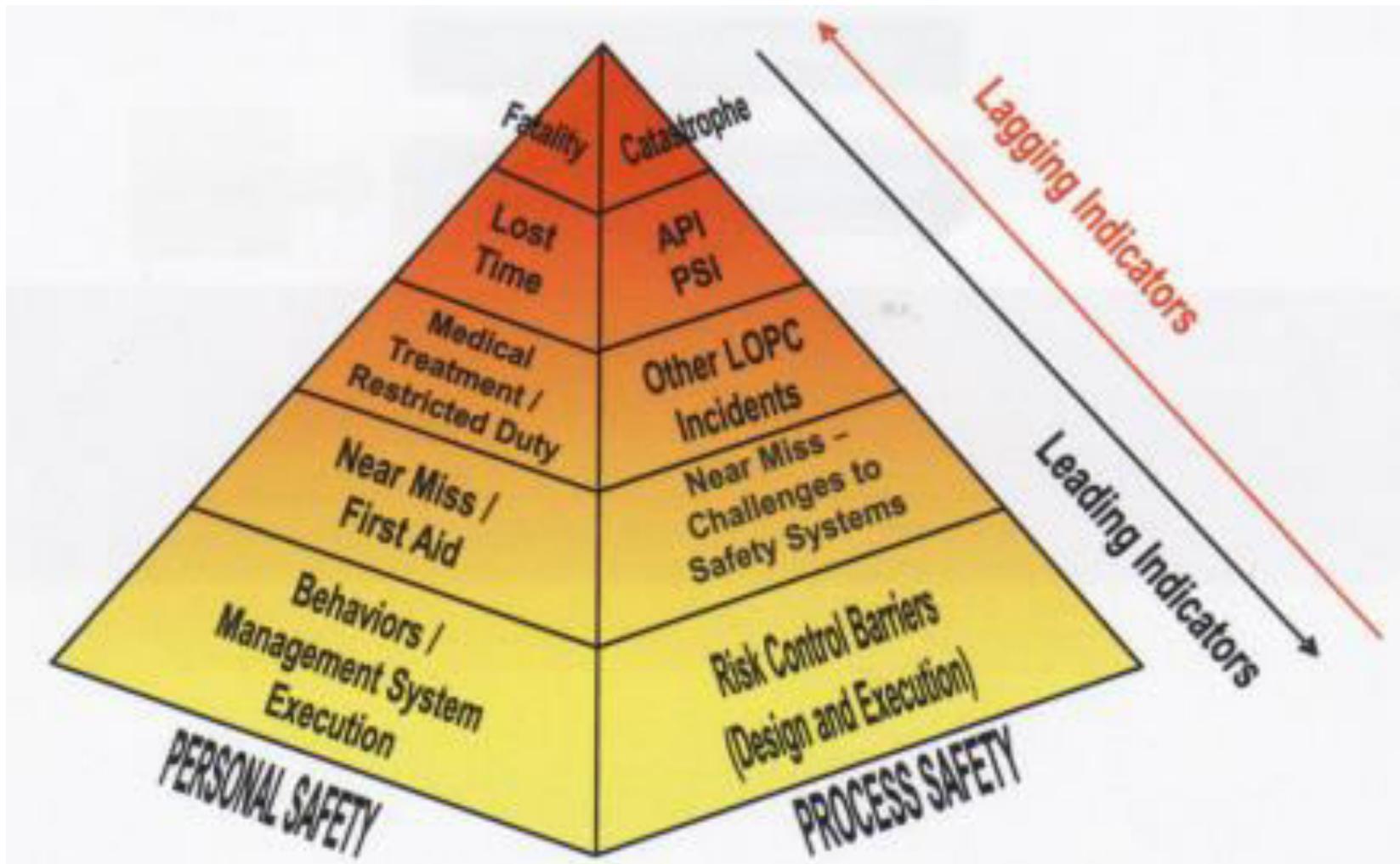
Leading Indicators

- A measure of activities to reduce risk prior to occurrence of an incident
- Unfortunately, not as widely used as lagging indicators
- Examples of leading indicators:
 - Number of near misses reported
 - Trend in implementation of prevention programs, employee safety training, etc.
 - Follow-up on items identified from risk assessments (%)
 - Deferred maintenance, % of items
 - Faults detected by inspections and testing

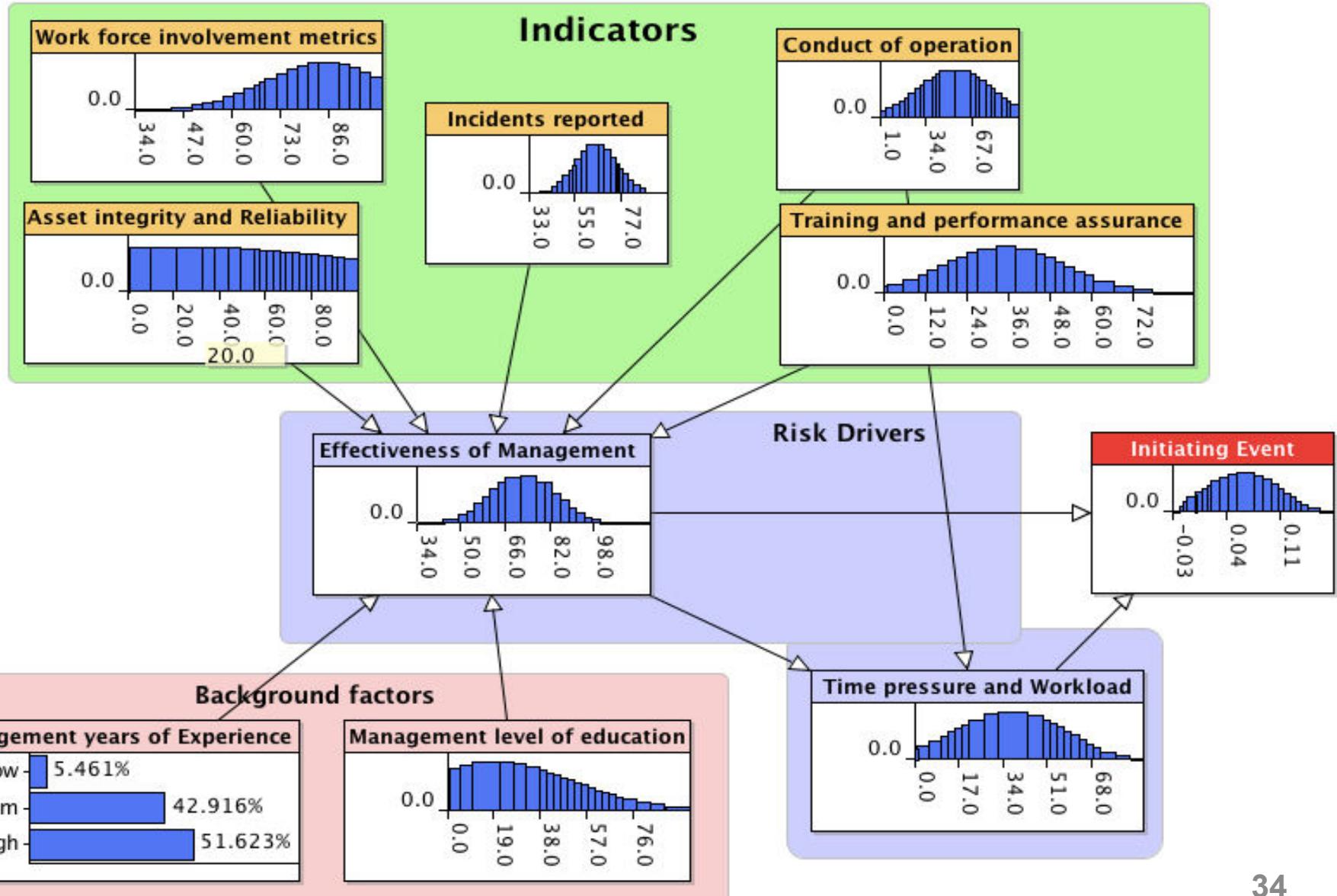
Process vs. Personnel Safety Metrics

- Personnel Safety
 - # injuries, illnesses & fatalities and their rates
 - Processes well developed for lagging indicators; evolved over last decade for leading indicators
- Process Safety
 - Businesses have historically measured volume of oil spilled, chemical releases, fires, hazard loss \$\$, etc
 - Industry standardization with API RP 754 ‘Process Safety Performance Indicators’
 - Tiers 1 & 2 primarily provide lagging indicators; measure loss of primary containment resulting in serious injuries, significant fire / explosion, community evacuation, etc
 - Tiers 3 & 4 leading indicators; % completion of process safety audit followup, training, work permit compliance, etc

Safety Incidents - Chevron



Model Management Effectiveness and Prediction of Consequences



Parameter Learning in BN

NOT included in FINAL EXAM

Parameter Learning: Classical Approach, Case 1

A school education department publishes data of the exam pass fractions or p values for 9 district schools. The data are aggregated to obtain an average pass fraction of 0.664 (or, 66.4%), to show the chances of a prospective student to pass/fail an exam.

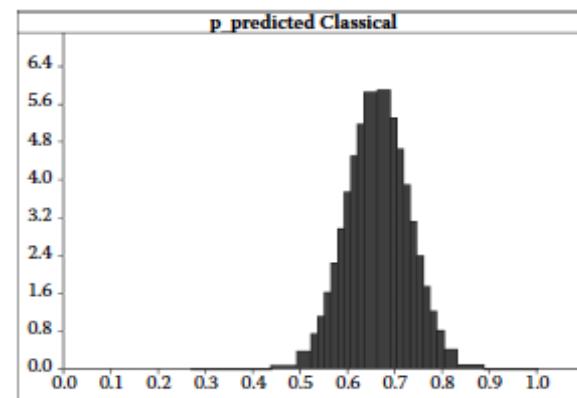
This pass fraction point value includes, however, no information about the variance of the exam score data for each school, and the sample weight or n_i for each school is not part of the published information.

The Classical Statistical approach is to fit data with the Normal distribution, as shown in the distribution figure and find the resulting Mean and Variance of the school p values as a prediction for a randomly selected school among these 9 schools.

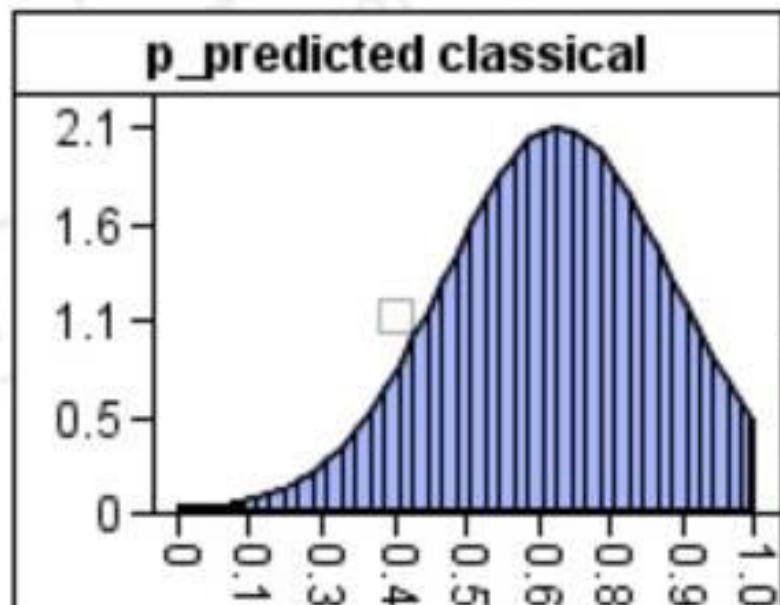
$$\hat{\mu}_p = \bar{p} = \frac{\sum_{i=1}^n p_i}{n} = 0.664$$

$$\hat{\sigma}_p^2 = \frac{\sum_{i=1}^n (p_i - \bar{p})^2}{n} = 0.0344$$

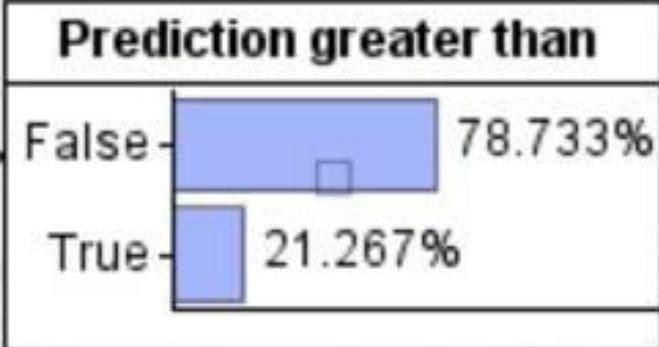
School i	Exam Pass Rate per School $p_i = x_i/n_i$
1	0.88
2	0.40
3	0.69
4	0.53
5	0.36
6	0.78
7	0.90
8	0.78
9	0.67



Classical Approach

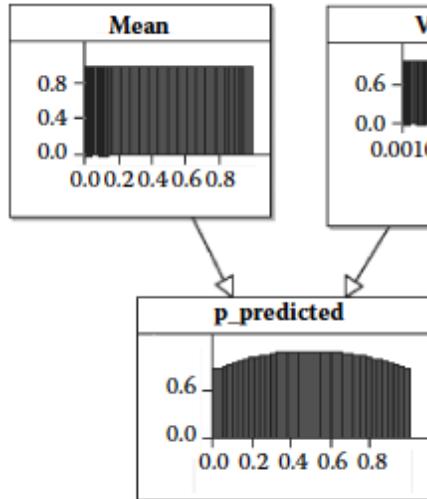


Mean = 0.664 and
Variance= 0.0391



```
if(p_predicted_classical>0.5,  
"False","True")
```

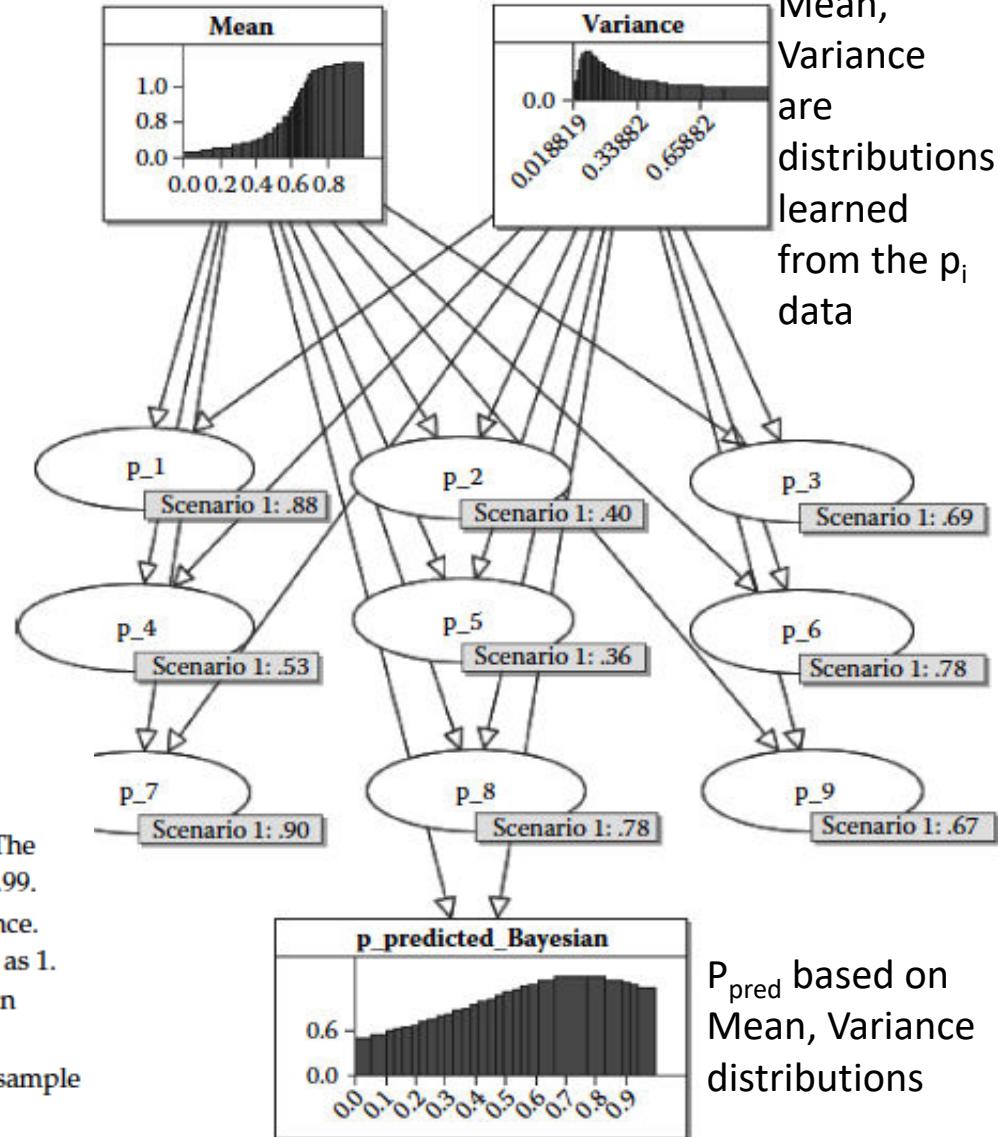
Bayes Model of p for 9 Schools, Case 2



Prior values of the parameters and a prior predicted p exam success fraction.

Table 9.3
NPTs for Parameter Learning Model

Node	NPT	Justification
mean	Uniform(0,1)	This assumes total prior ignorance. The mean is just as likely to be 0.01 as 0.99.
variance	Uniform(0,1)	This assumes a form of prior ignorance. The variance is just as likely to be 0 as 1.
$p_{predictedBayesian}$	TNormal (mean, variance, 0, 1)	This is the prediction for an unknown school.
p_1	TNormal (mean, variance, 0, 1)	This was the assumption about any sample distribution.
p_2	TNormal (mean, variance, 0, 1)	This was the assumption about any sample distribution.
etc.



Posterior p with mean = 0.57

Mean, Variance are distributions learned from the p_i data

P_{pred} based on Mean, Variance distributions

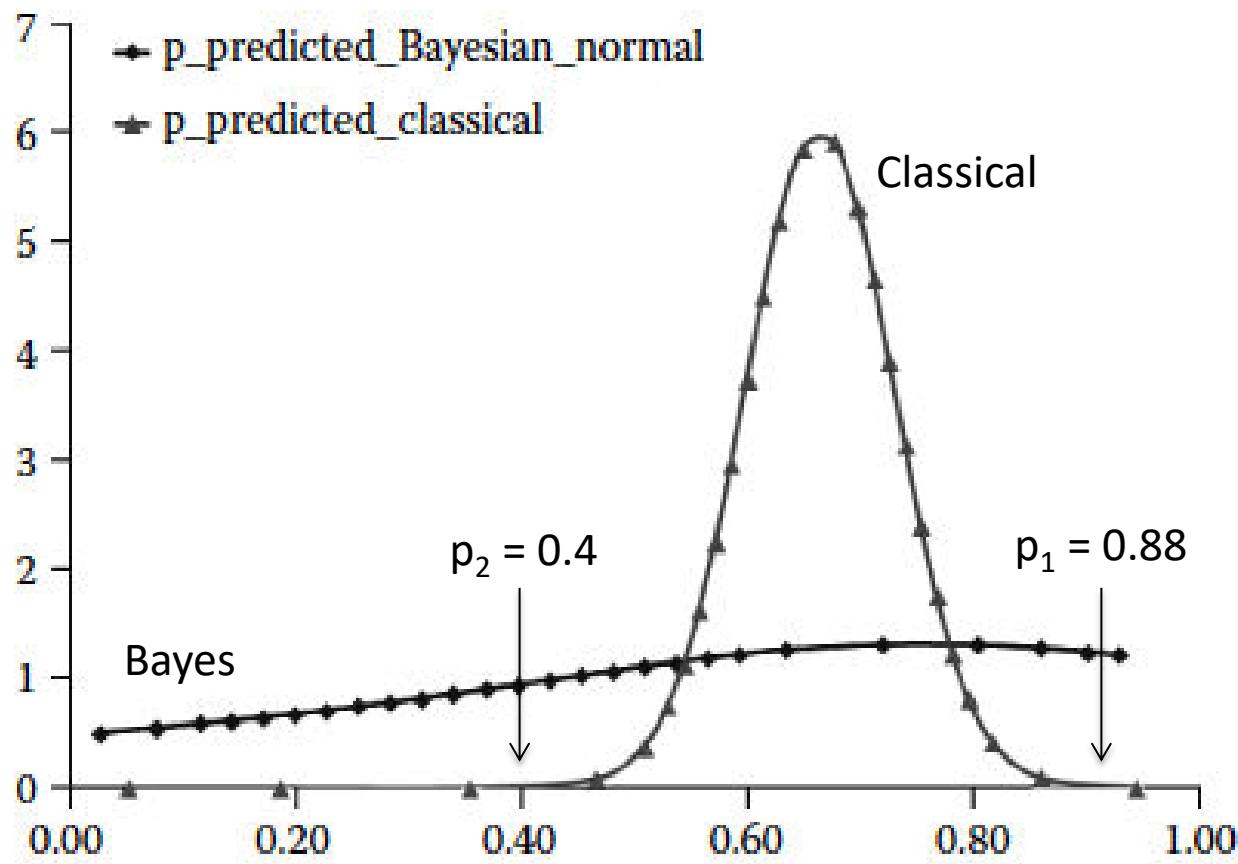
Parameter Learning using Bayes, Case 2

- Using the Bayes model, we can learn the distribution parameters from all of the data including the p_i and the n_i .
- For these p_i data from 0 to 1, a distribution from 0 to 1, such as the TNormal, is a convenient choice.
- To model the 9 sets of data, we can construct a BN with numeric nodes in the range 0 to 1 with a mean = (unknown) population mean and variance = (unknown) population variance.
- Because for this case we will learn the distribution parameters from the observed data, the Prior distributions for mean and for variance will be the uniform distribution, $U(0,1)$ with equal probability of any value within 0 to 1.

Induction Idiom: Parameter Learning using Bayes, Case 2

- Because the Likelihood distribution is TNormal and the Prior distribution is uniform, the Posterior distribution based on the intersection (joint distribution) of Prior and Likelihood is a TNormal distribution.
- The calculated model results in Posterior distributions for the mean and variance from which a predicted p value mean of 0.57 with a predicted variance of 0.07 is calculated from the Bayes model.
- From the mean and variance distributions is calculated a Posterior predictive distribution for p , the Exam Success Rate, based on the listed data from the 9 schools.

Bayes Mean = 0.57, variance = 0.07 learned from p data of 9 schools



Parameter Learning: Classical, Case 1, vs. Bayes, Case 2

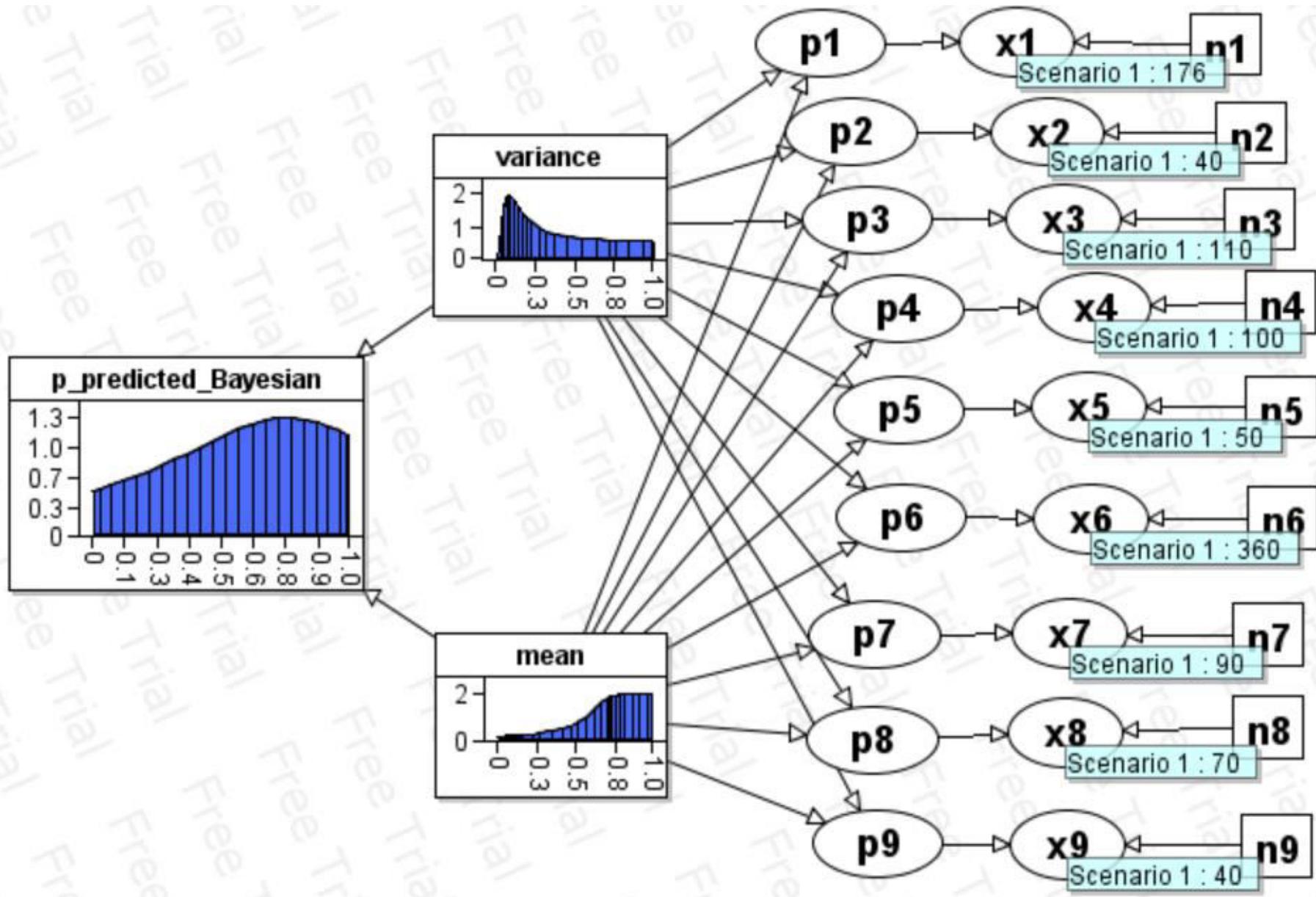
- Comparing the Classical statistical approach with the Bayes approach, the Bayes result shows a larger and much more realistic variance. Note that schools 1, 2, 7 with p values of 0.88, 0.4, and 0.9 would be predicted with very low probability in the tail regions of the Classical model distribution but now, using the Bayes posterior distribution, schools 1, 2, 7 are represented by much more realistic probabilities.
- A weakness of this calculation is that only the p_i data and **not** the p_i together with the n_i (number of students taking the test in a school) data are explicitly modeled. Therefore, the variance is for the range of p values among the schools and does not include the size of the data for each of the individual schools.

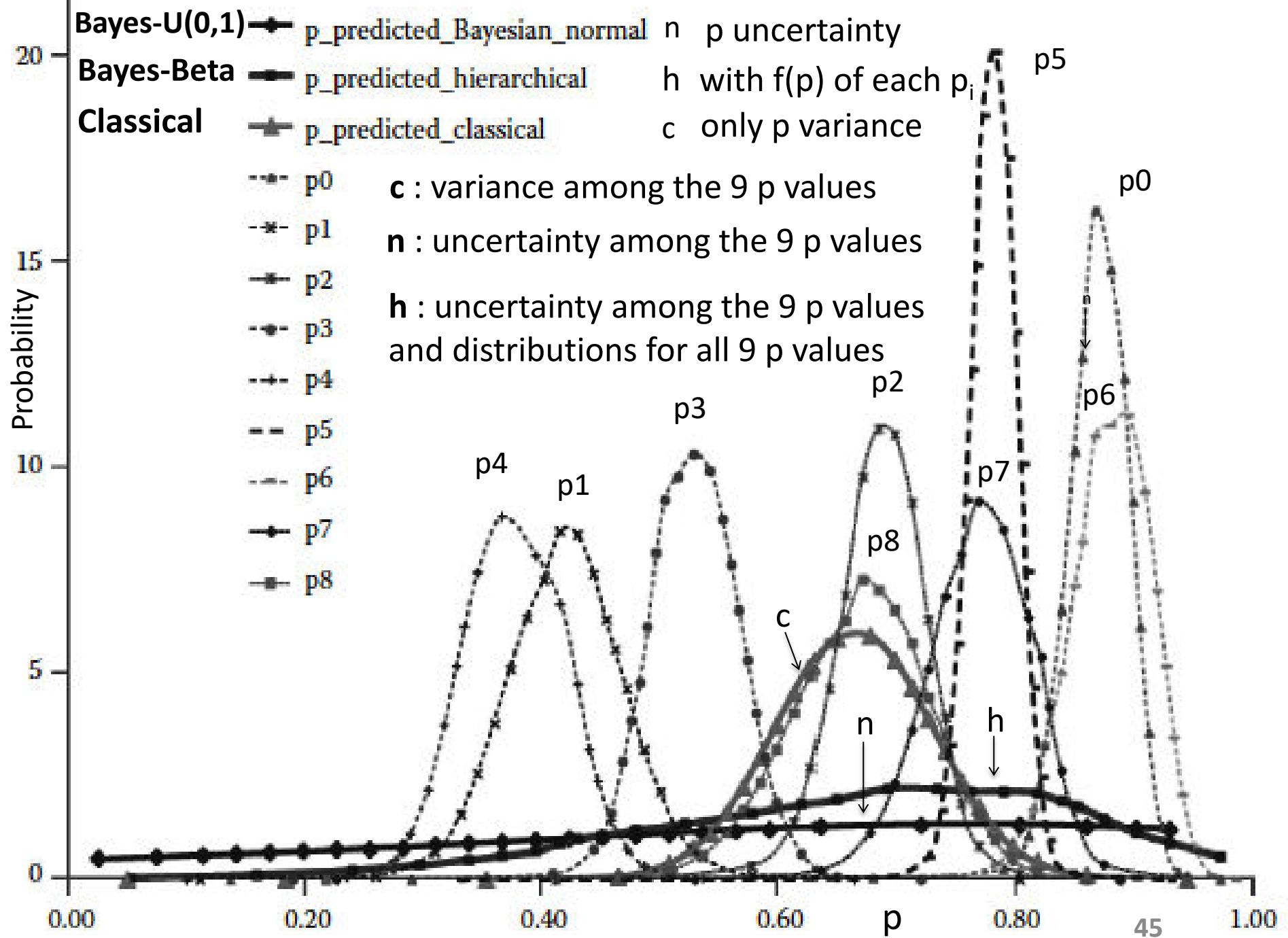
Hierarchical Bayesian Modelling

- Needed is a 3rd model that results in a p distribution showing uncertainty due to sample weight n_i for each school, so that the 9 schools can be directly compared each with its own distribution and uncertainty. This third model is constructed using Bayesian Hierarchical (multilevel) Modeling with the Beta (Prior/Posterior) and Binomial (Likelihood for exam data) distributions.

Exam Pass Rate per School

School i	n_i	x_i	$p_i = x_i/n_i$
1	200	176	0.88
2	100	40	0.40
3	160	110	0.69
4	190	100	0.53
5	140	50	0.36
6	460	360	0.78
7	100	90	0.90
8	90	70	0.78
9	60	40	0.67

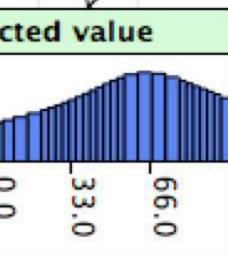
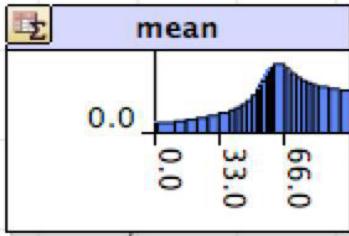




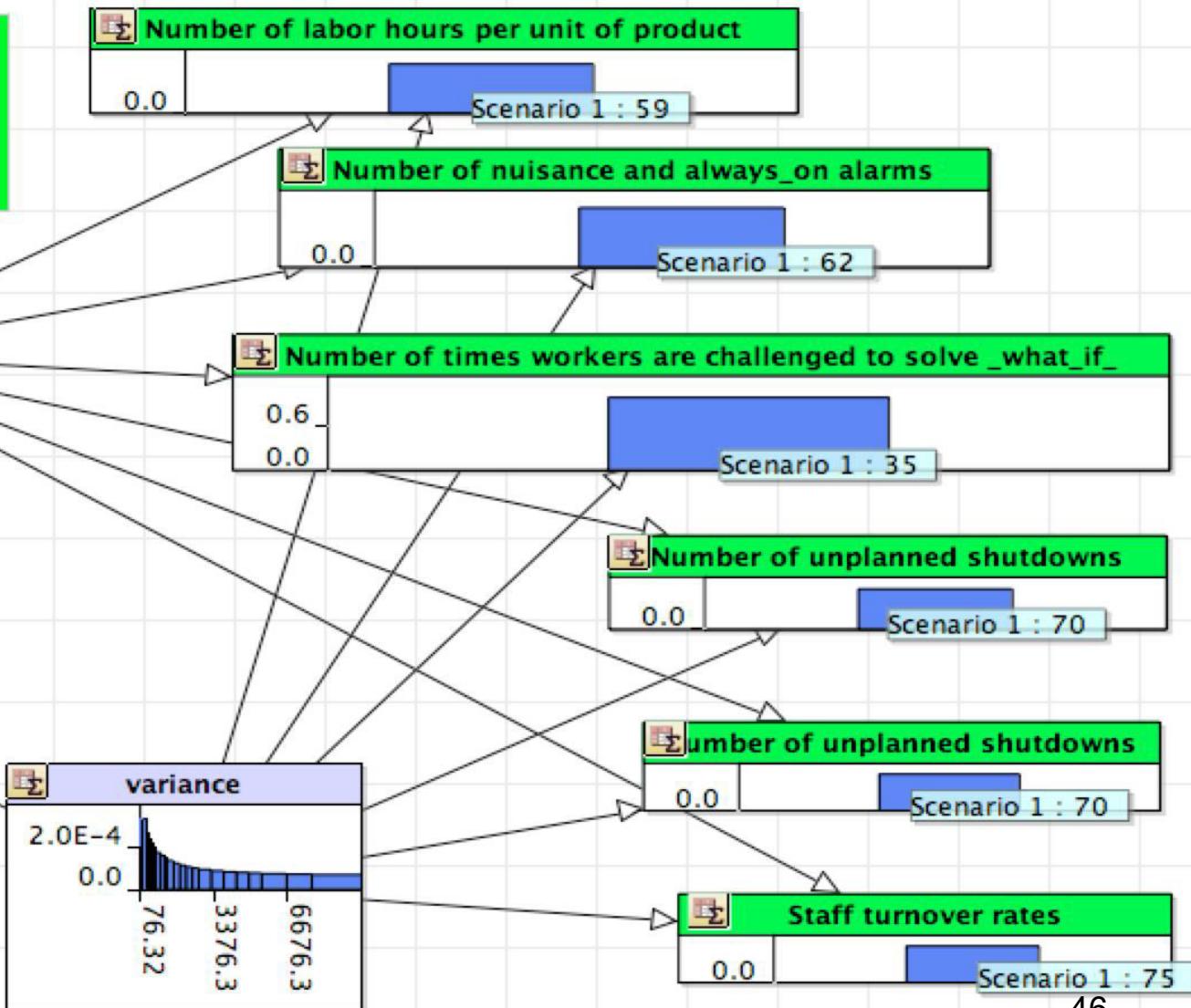
Learning Population Model Parameters from STS Indicators

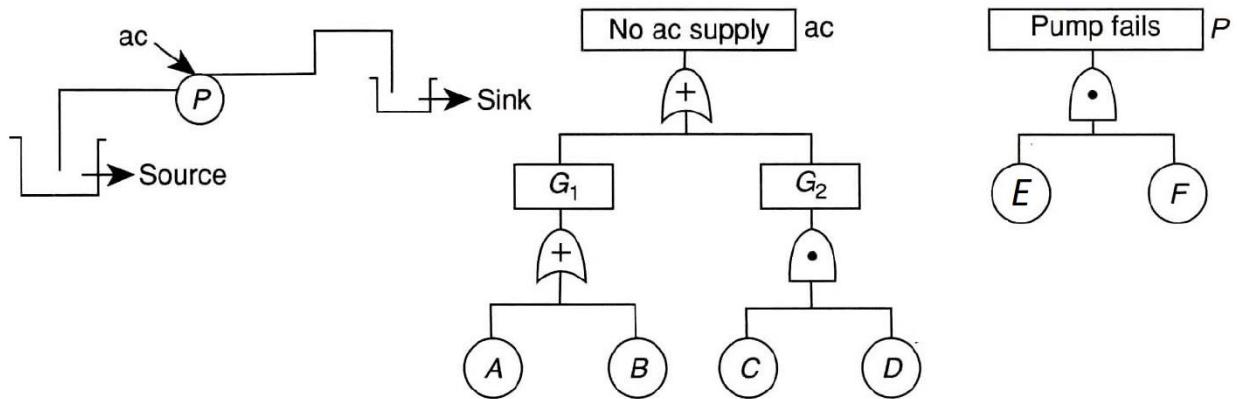
Normal Distribution Parameter Fitting

Indicator Conduct of Operation



Predicted Conduct of Operation Distribution





The pumping system shown above allows water to be transferred from the source to the sink. The pumping system requires both the AC supply AND the Pump P to work for the water to be transferred.

The fault trees for ‘no ac supply’ and ‘pump fails’ are shown.

Assuming A, B, C, D, E and F are all independent and rare events, on a given year, the probability of each event is 0.1 [that is $P(A)=P(B)=P(C)=P(D)=P(E)=P(F)=0.1$].

Calculate the following:

Probability of ‘no ac supply’: $P(A)+P(B)+[P(C).P(D)]=0.1+0.1+(0.1*0.1)=0.21$

Probability of ‘pump fails’: $P(E).P(F)=0.01$

Probability of the pump system to be working = $[1-\Pr(\text{‘no ac supply’})].[1-\Pr(\text{‘pump fails’})]$

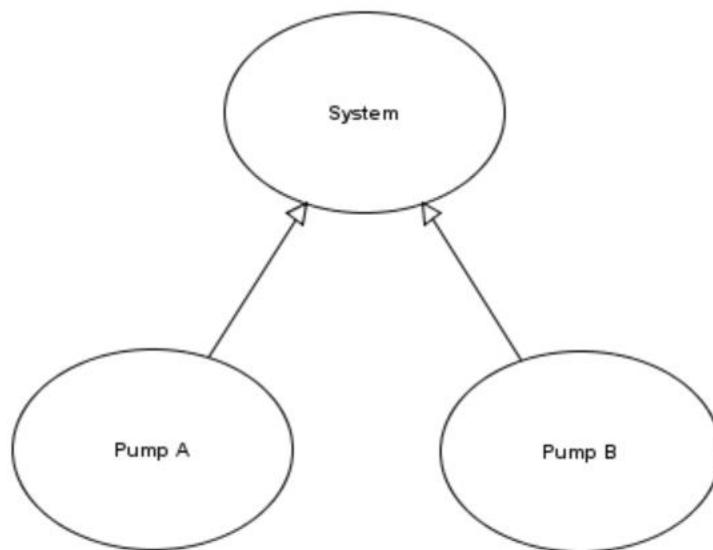
$$=[(1-0.21)*(1-0.01)]=0.78$$

Quiz 4

Question 1:

For a system that has two redundant pumps (Pump A and Pump B), a fault tree drawn for the System will connect Pump A and Pump B through an And- gate.

A Bayesian Network drawn for such a ‘System’ is shown below, where nodes ‘Pump A’ and ‘Pump B’ are connected to the ‘System’ node and the Node Probability Table of the ‘System’ node is an AND-gate. **Fill up the Node Probability Table of the ‘System’ node below:** (60 points)



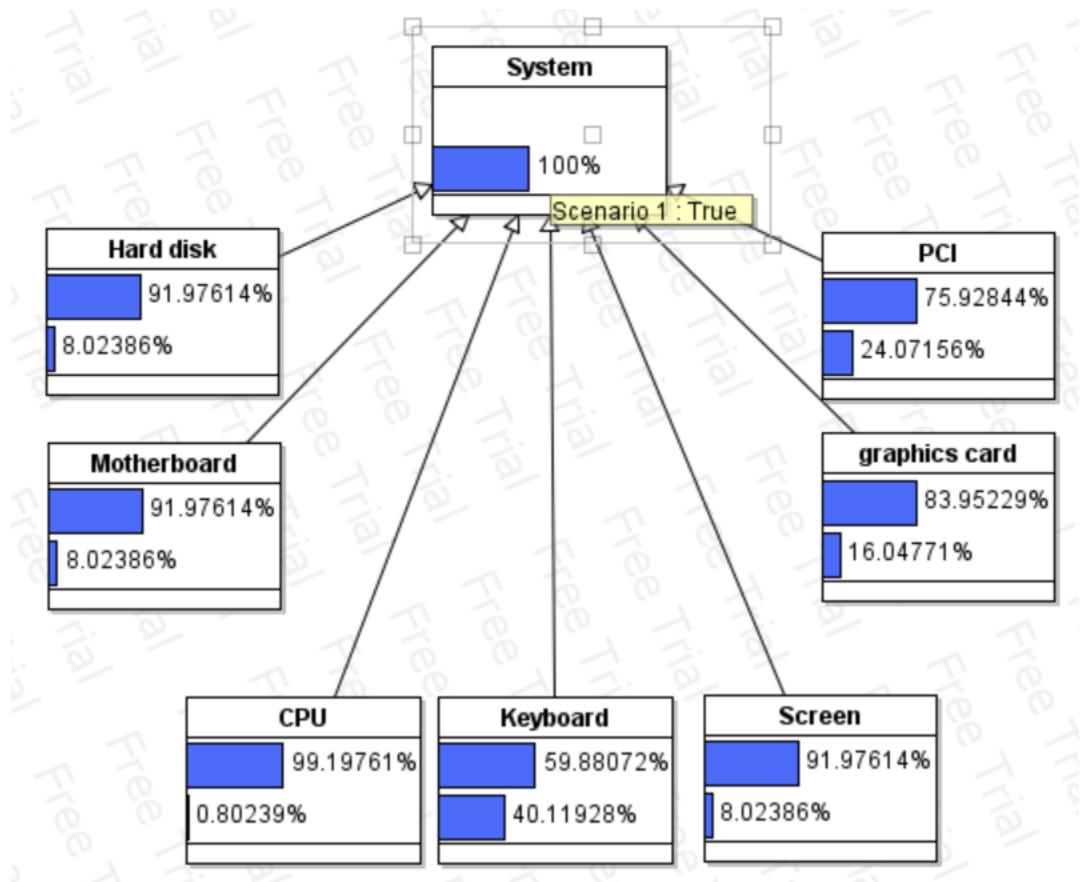
Node Probability Table of ‘System’ Node:

Pump A	Fails		Does not Fail	
Pump B	Fails	Does not Fail	Fails	Does not Fail
Fails	1	0	0	0
Does not Fail	0	1	1	1

Question 2:

The Bayesian Network in the next page shows how failure of the various components of the System can lead to its failure. The System fails if any one of the components fail. For each node, the top bar represents the probability of the components being in a working state and the bottom bar represents the probability of the components’ failure.

It is observed that the System fails ('System' node observed to be 'True'). **Given the updated Bayesian Network shown in the figure, which component do you think should be checked first to bring the System back to working condition? (40 points)**



ANSWER: Keyboard has the highest probability of not being in the working state, so it should be checked first.

QUIZ 5

A die forge press operates an average of 300 days/yr. Under a minimal repair concept, machine failures generated a nonhomogenous Poisson process having the following intensity function with t measured in operating hours: $\rho(t) = 5 \times 10^{-6}t^2$.

- a. Calculate the number of expected failures of the press during a mission time of 300 days, $m(300)$.

Answer: 45

- b. Calculate the MTBF (mean time between failures) for the mission time of 1 yr = 300days.

Answer: 6.67

- c. When the machine has failed, the repair time follows a normal distribution with mean=1day and standard deviation of 0.01 day. Calculate the average inherent, steady state, Availability, A_{inh} of the mission time of 1 yr operating life of the press (to 2 decimal places)

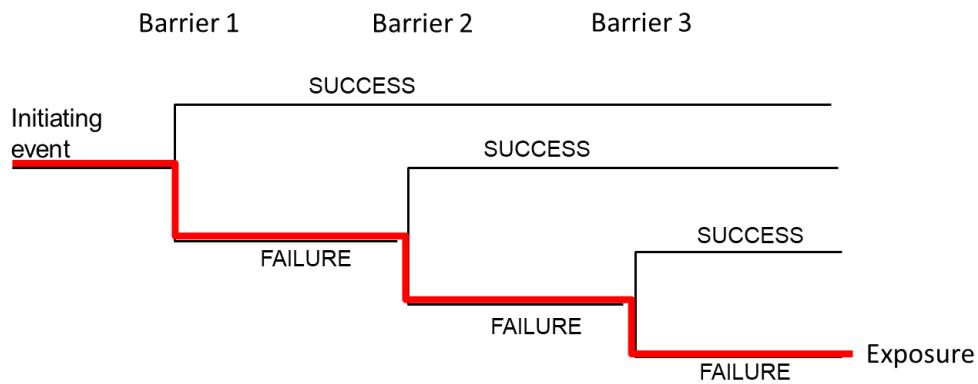
Answer: 0.87

CHEN/SENG 460/660

HW 5

Due: 04/07/2022 (11:59 PM)

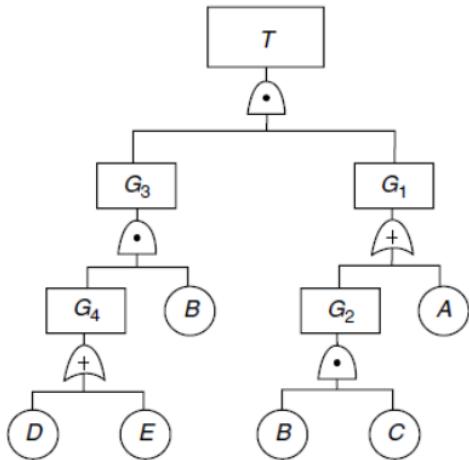
1. The hazard of exposure to radioactive chemicals is mitigated with 3 independent barriers. If only 1 barrier works, the exposure is prevented. The probability of each barrier to fail is 0.001 and the consequence of hazard exposure is 3000 cancer-deaths per year. Develop an event tree showing all branches and outcome. What is the probability of exposure. What is the risk (probability x consequence) due to the hazard?



$$\text{Probability of exposure} = 0.001 \times 0.001 \times 0.001 = 1 \times 10^{-9}$$

$$\text{Risk} = P \times C = 1 \times 10^{-9} \times 3000 \text{ cancer-deaths} = 3 \times 10^{-6} \text{ deaths}$$

2. RAE 3.4: The top event T for a tank rupture scenario is shown in the fault tree below:



Find the following:

- Minimal cut sets
- Minimal path sets
- Probability of the top event if the following probabilities apply:

$$\Pr(A) = \Pr(C) = \Pr(E) = 0.01$$

$$\Pr(B) = \Pr(D) = 0.0092$$

Solution:

a) Tank Ruptures Failure Tree

$$T = [(D + E) \cdot B] \cdot [(B \cdot C) + A]$$

$$T = (BD + BE) \cdot [(B \cdot C) + A]$$

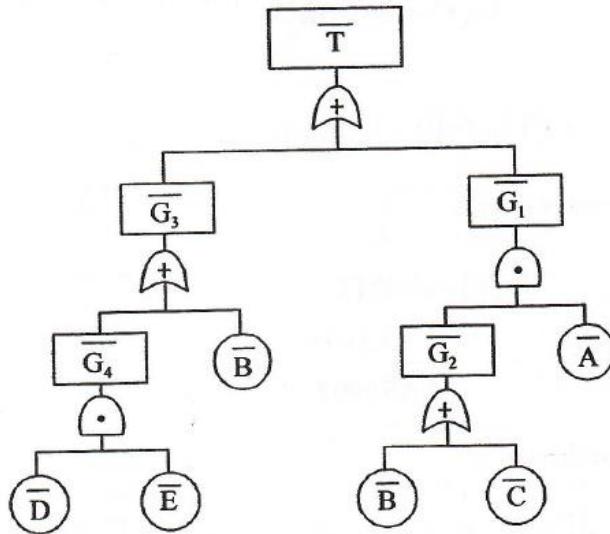
$$T = BCD + BCE + ABD + ABE$$

The minimal cut-sets of the top event are thus

$$C_1 = \{B, C, D\} \quad C_3 = \{A, B, D\}$$

$$C_2 = \{B, C, E\} \quad C_4 = \{A, B, E\}$$

b) Tank Ruptures Success Tree



$$\overline{T} = [(\overline{D} \cdot \overline{E}) + \overline{B}] + [(\overline{B} + \overline{C}) \cdot \overline{A}]$$

$$\overline{T} = \overline{D} \cdot \overline{E} + \overline{B} + \overline{A} \cdot \overline{B} + \overline{A} \cdot \overline{C}$$

$$\overline{T} = \overline{D} \cdot \overline{E} + \overline{B} + \overline{A} \cdot \overline{C}$$

The minimal path-sets of the top event are thus

$$\begin{aligned} P_1 &= \{\overline{B}\} & P_2 &= \{\overline{A}, \overline{C}\} \\ P_3 &= \{\overline{D}, \overline{E}\} \end{aligned}$$

c) Assume independence

$$T = BCD + BCE + ABD + ABE$$

$$Pr(T) = Pr(BCD + BCE + ABD + ABE)$$

$$Pr(T) = 1 - [1 - Pr(B) \cdot Pr(C) \cdot Pr(D)] \cdot [1 - Pr(B) \cdot Pr(C) \cdot Pr(E)] \cdot [1 - Pr(A) \cdot Pr(B) \cdot Pr(D)] \cdot [1 - Pr(A) \cdot Pr(B) \cdot Pr(E)]$$

$$Pr(T) = 1 - [1 - (0.0092)^2 (0.01)]^2 \cdot [1 - (0.0092)(0.01)^2]^2$$

$$Pr(T) = 3.5328 \times 10^{-6}$$

The probability of the top event is

$$\Pr(T) = 3.5 \times 10^{-6}$$

For the success tree

$$\Pr(\bar{T}) = \Pr(\bar{B} + \bar{A} \cdot \bar{C} + \bar{D} \cdot \bar{E})$$

The probability of the top event is then

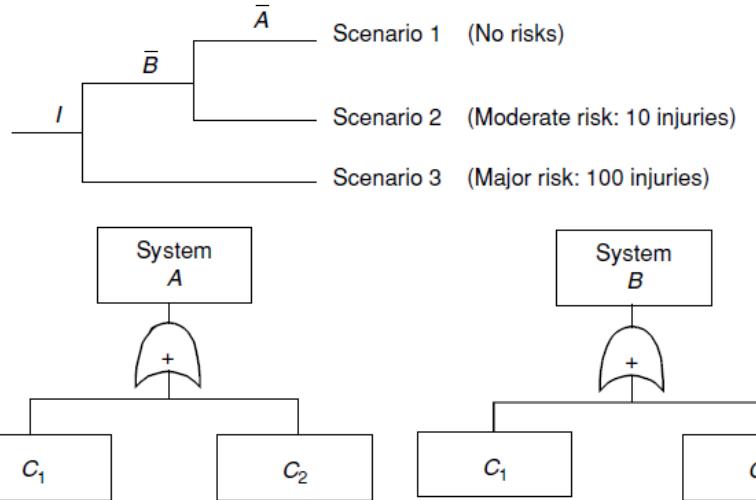
$$\begin{aligned}\Pr(\bar{T}) &= 1 - \Pr(T) \\ &= 1 - 3.5 \times 10^{-6} \\ &= 0.999997\end{aligned}$$

Or versus Rare Event Approximate

$$\begin{aligned}\Pr(T) &= 2[(0.0092)^2(0.01) + (0.0092)(0.01)^2] \\ &= 3.5 \times 10^{-6}\end{aligned}$$

$$\begin{aligned}\Pr(\bar{T}) &= 1 - \Pr(T) \\ &= 1 - 3.5 \times 10^{-6} \\ &= 0.999997\end{aligned}$$

3. Consider the event tree and the fault trees below:



- (a) Determine a Boolean equation representing each of the event tree scenarios in terms of the fault tree basic events (C_1 , C_2 , and C_3).
- (b) If the frequency of the initiating event I is $10^{-3}/\text{year}$, and $\Pr(C_1)=0.001$, $\Pr(C_2)=0.008$, and $\Pr(C_3)=0.005$, calculate the risk (injuries per year).
- (c) Plot the risk profile curve (Farmer's curve) for this problem.

Recall that a risk profile curve (Farmer's curve) is a plot of frequency vs. consequence (injuries in this case).

Solution:

- a) The Boolean equation representing of each of the event tree scenarios in terms of the fault tree basic events (C_1 , C_2 , and C_3) are:

Scenario 1:

$$\begin{aligned}
 & I \cdot \bar{B} \cdot \bar{A} \\
 & I \cdot (\overline{C_1 + C_3}) \cdot (\overline{C_1 + C_2}) \\
 & I \cdot \overline{C_1} \cdot \overline{C_3} \cdot \overline{C_1} \cdot \overline{C_2} \\
 & I \cdot \overline{C_1} \cdot \overline{C_2} \cdot \overline{C_3}
 \end{aligned}$$

Scenario 2:

$$\begin{aligned}
 & I \cdot \overline{B} \cdot A \\
 & I \cdot (\overline{C_1 + C_3}) \cdot (C_1 + C_2) \\
 & I \cdot \overline{C_1} \cdot \overline{C_3} \cdot (C_1 + C_2) \\
 & I \cdot C_1 \cdot \overline{C_1} \cdot \overline{C_3} + I \cdot \overline{C_1} \cdot C_2 \cdot \overline{C_3} \\
 & I \cdot \overline{C_1} \cdot C_2 \cdot \overline{C_3}
 \end{aligned}$$

Scenario 3:

$$\begin{aligned}
 & I \cdot B \\
 & I \cdot (C_1 + C_3) \\
 & I \cdot C_1 + I \cdot C_3
 \end{aligned}$$

- b) Since I is $10^{-3}/\text{year}$, and $\Pr(C_1) = 0.001$, $\Pr(C_2) = 0.008$, and $\Pr(C_3) = 0.005$, then the frequency are

$$\text{Frequency Scenario 1} = \Pr(I \cdot \overline{C_1} \cdot \overline{C_2} \cdot \overline{C_3})$$

$$\text{Frequency Scenario 1} = 1 \times 10^{-3} (0.999)(0.992)(0.995)$$

$$\text{Frequency Scenario 1} = 9.86 \times 10^{-6} / \text{year}$$

$$\text{Frequency Scenario 2} = \Pr(I \cdot \overline{C_1} \cdot C_2 \cdot \overline{C_3})$$

$$\text{Frequency Scenario 2} = 1 \times 10^{-3} (0.999)(8 \times 10^{-3})(0.995)$$

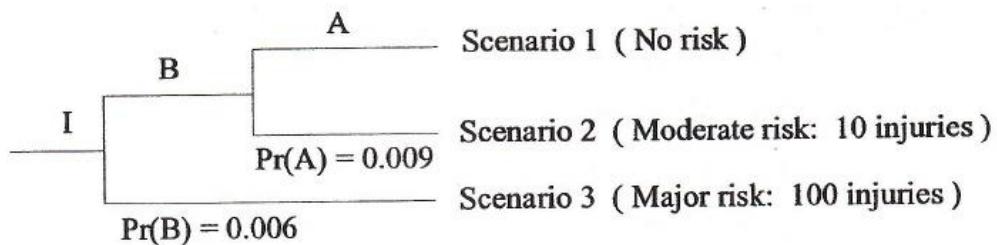
$$\text{Frequency Scenario 2} = 7.95 \times 10^{-6} / \text{year}$$

$$\text{Frequency Scenario 3} = \Pr(I \cdot C_1) + \Pr(I \cdot C_3)$$

$$\text{Frequency Scenario 3} = 1 \times 10^{-3} (0.001) + 10^{-3} (0.005)$$

$$\text{Frequency Scenario 3} = 6.00 \times 10^{-6} / \text{year}$$

therefore, from the event tree, we get



Scenario 1 Consequence $\emptyset \rightarrow$ Risk = frequency \times consequence

$$\text{Risk} = 0$$

$$\text{Scenario 2 Risk} = 7.95 \times 10^{-6} (10) = 7.95 \times 10^{-5} \text{ injuries per year}$$

$$\text{Scenario 3 Risk} = 6.00 \times 10^{-6} (100) = 6.00 \times 10^{-4} \text{ injuries per year}$$

$$\text{Total Risk} = 7.95 \times 10^{-5} + 6.00 \times 10^{-4} = 6.80 \times 10^{-4} \text{ injuries per year}$$

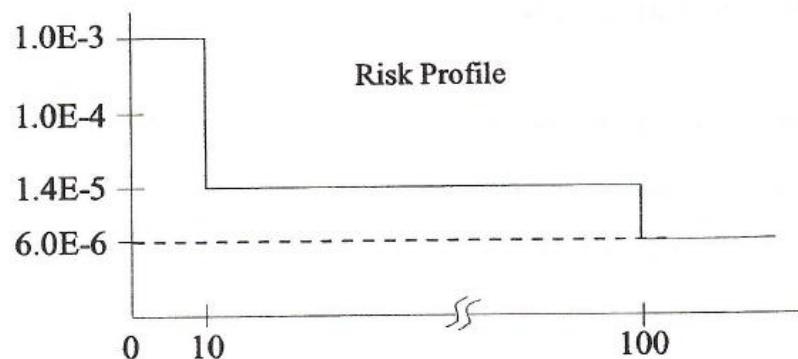
$$\text{Risk} = \sum_{n=1}^3 \text{Pr}_n C_n$$

$$\text{Pr}(x \geq 0) = \sum \text{Frequency of all scenario} = 1.0 \times 10^{-3} / \text{year}$$

$$\text{Pr}(x \geq 10) = \sum \text{Scenarios 2 and 3} = 1.4 \times 10^{-5} / \text{year}$$

$$\text{Pr}(x \geq 100) = \sum \text{Scenario 3} = 6.0 \times 10^{-6} / \text{year}$$

c) A plot of the risk-profile curve (Farmer Curve) is shown below



Students are not required to do (c)

4. Using a typical frequency value for the initiating event and PFD values provided in class lectures, estimate the mishap or consequence frequency for a cooling water failure if the system to be cooled is provided with the following IPLs: (1) Personnel action with a 10 min response time, and (2) A basic process control system (BPCS).

Solution:

Frequency of a cooling water failure from Table 11-3, $f_1^I = 10^{-1}/\text{yr}$

PDF values are estimated from Table 11-5 (Active IPLs and Human Actions):

Human response, action within 10 min: PDF = 10^{-1}

Basic process control system (BPCS): PDF = 10^{-1} to 10^{-2}

Consequence frequency:

$$f_1^C = f_1^I \times \prod_{j=1}^2 PDF_{1j} \quad \text{with a conservative value for the BPCS}$$

$$= 10^{-1}/\text{yr} \times (10^{-1})(10^{-1}) = 10^{-3} \text{ failure/yr}$$

5. For a system designed with three IPLs, provide a conservative estimate for the consequence frequency of a regulator failure. (When the SIL level is not known, use SIL1, where PFD = 10^{-2} is generally used.)

Solution:

From Table, regulator failure frequency is $10^{-1}/\text{yr}$

$$f_1^C = f_1^I \times \prod_{j=1}^3 PDF_{1j}$$

$$= 10^{-1}/\text{yr} \times (10^{-2})(10^{-2})(10^{-2}) = 10^{-7} \text{ failure/yr}$$

Conservative approach: $\frac{1}{\text{yr}} \times (10^{-2})(10^{-2})(10^{-2}) = (10^{-6})/\text{yr}$

6. Determine the expected failure rates, λ , and mean time to failures (MTTF), calculated as $1/\lambda$, for control systems with SIL1, SIL2, and SIL3 ratings with PFDs of 10^{-2} , 10^{-3} , and 10^{-4} , respectively.
 (PFD= Probability of Failure on Demand= 1- Reliability)

$$P(t) = 1 - e^{-\lambda t}$$

$$R(t) = 1 - P(t) = e^{-\lambda t}$$

For $P = 10^{-2} = 0.01$; $R = 0.99$

For $t = 1$ year:

$$R = e^{-\lambda}; \lambda = -\ln R = -\ln(0.99) = 0.01 \text{ failure/yr}$$

So, MTTF = $1/\lambda = \sim 100$ years

SIL	P	R	λ, yr^{-1}	MTBF, yr
1	0.01	0.99	0.01	100
2	0.001	0.999	0.001	1000
3	0.0001	0.9999	0.0001	10000

HW 6

Due: 04/19/2022, 11:59 PM

1. Review the Hot Oil Heating System and convert the reduced fault tree to a Bayesian Network in AgenaRisk.

- a. For the node probability tables use the PFD (probability of failure on demand) probabilities as calculated in class for the components as shown in Unit 10B, Slide 25. For the BN, use Boolean nodes, which is the default case. Begin at the bottom of the FT and use OR1, OR2, OR3 as identifiers for the OR gates, AND1, AND2 identifiers for the AND gates.

- b. As stated, frequencies can be converted into probabilities of occurrence over any time interval.

For the pump with failure frequency of 1.5/yr, assume a constant λ and convert the failure frequency to a cumulative failure probability for $t = 1$ year using the Exponential failure distribution $F(t) = 1 - \exp(-\lambda t)$.

As stated, frequencies can be converted into probabilities of occurrence over any time interval. For the pump with failure frequency of 1.5/yr, assume a constant λ and **convert the failure frequency to a cumulative failure probability for $t = 1$ year** using the Exponential failure distribution $F(t) = 1 - \exp(-\lambda t)$.

$$F(T=1\text{yr}) = 1 - \exp(-1.5) = 1 - 0.2231 = 0.777$$

- c. Check that the BN variable values agree with the probability values calculated for the FT. Check that your top event probability calculated using the probability of pump failure during 1 year is consistent with the top event frequency calculated in class using the frequency of pump failure.

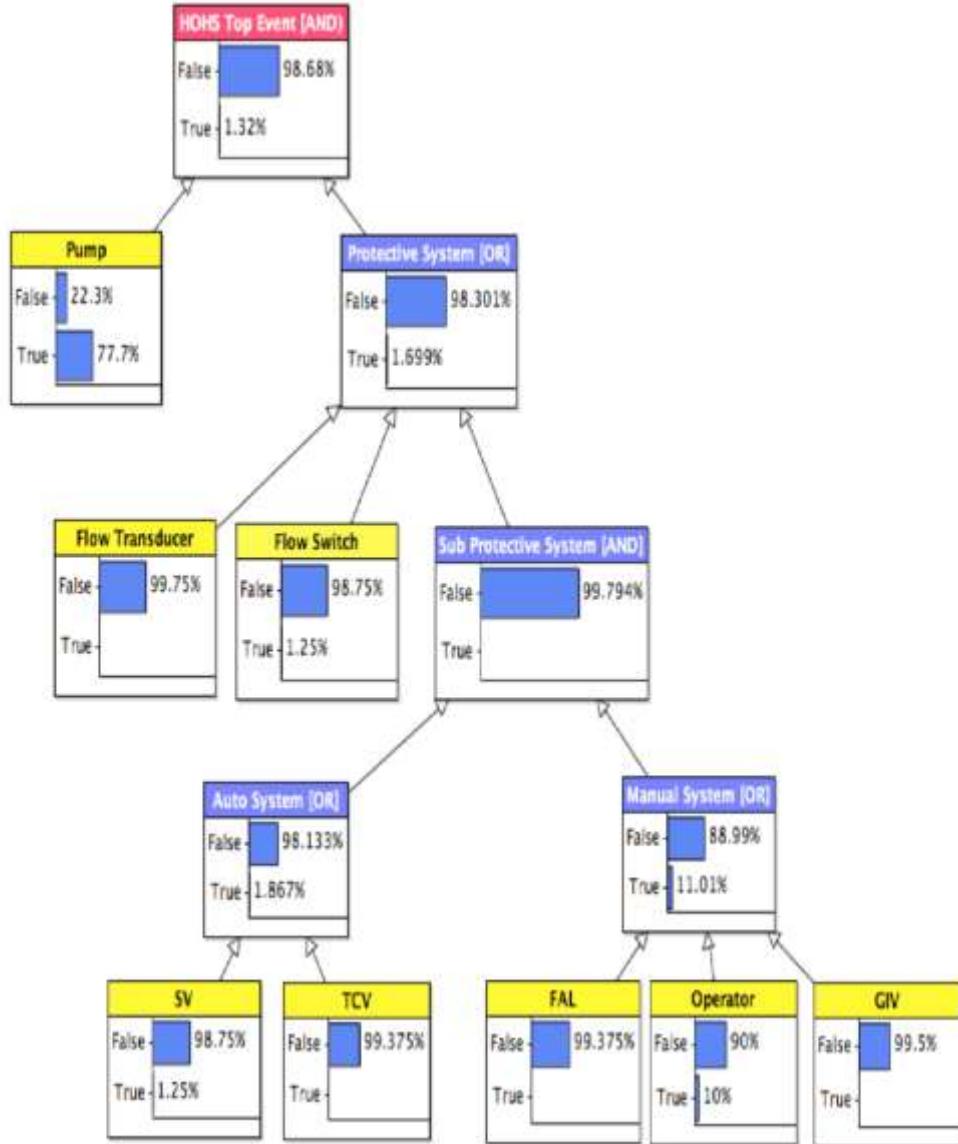
For the BN, use Boolean nodes, which is the default case. Begin at the bottom of the FT and use OR1, OR2, OR3 as identifiers for the OR gates, AND1, AND2 identifiers for the AND gates.

For the NPT of an OR operator, use Expression = noisyand, e.g.,
if(FAL=="True"||Operator=="True"||GIV=="True", "True", "False").

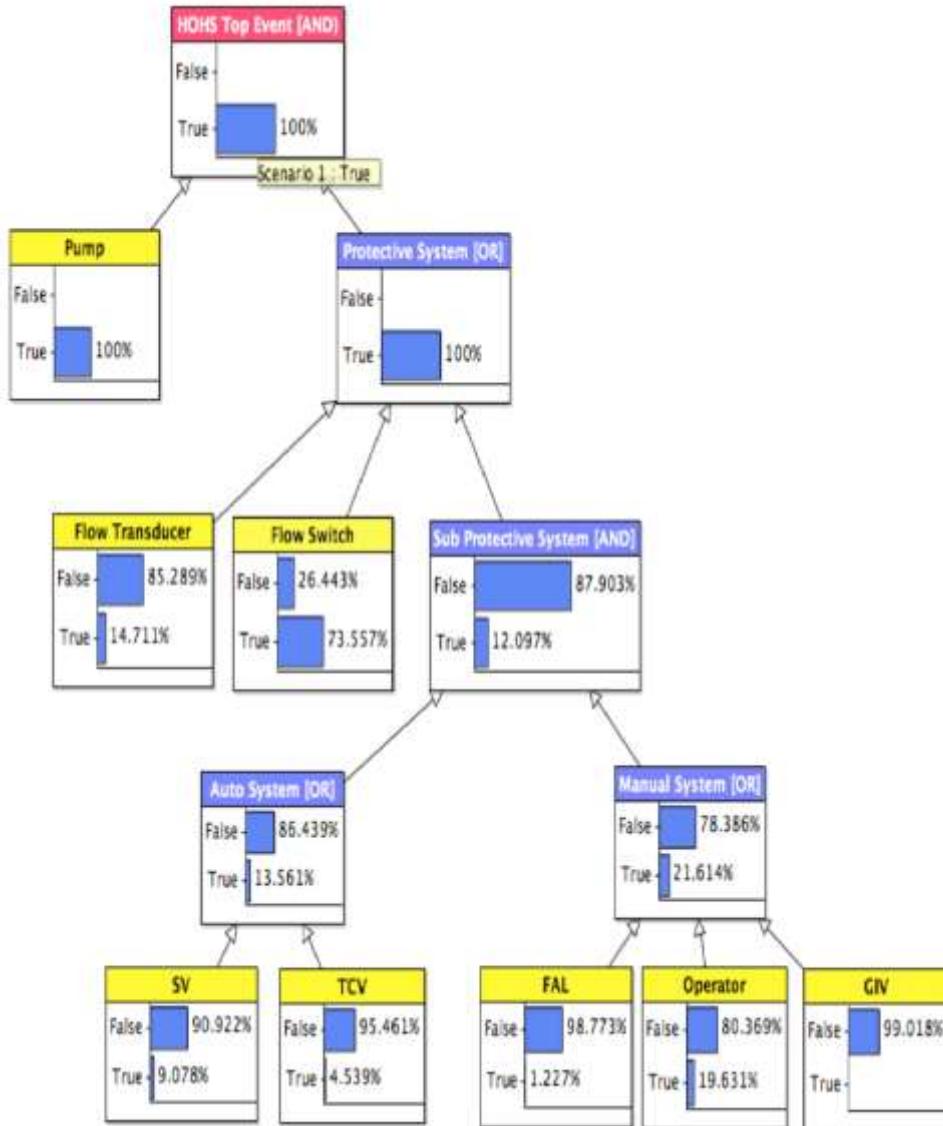
For the NPT of an AND operation, use Expression = noisyand, e.g.,
if(Auto_System=="True"&&Manual_System=="True", "True", "False")

Alternately, NPT for Boolean AND and OR-gates can be developed.

- d. View the nodes as bar charts (double click on the node) and include a screen capture of the Hot Oil Heating System BN in your homework.



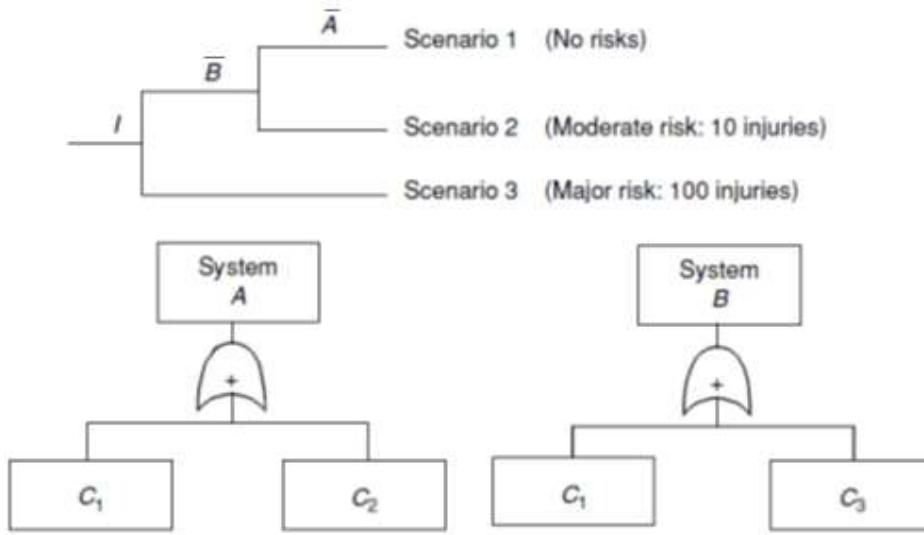
- e. Even though only binary states (success/fail) are used in the BN for this problem, you can practice diagnostic and predictive reasoning or “what if” calculations and MLE (most likely explanation) to explore the effect of system modifications on system risk and analyze where risk originates within the system. Practice diagnostic reasoning: Instantiate the Fault Tree top event BN to “True” indicating that the top event has occurred, recalculate the BN, and identify, and state in your answer, the MLE (most likely explanation) component within the Protective System for the top event system failure.



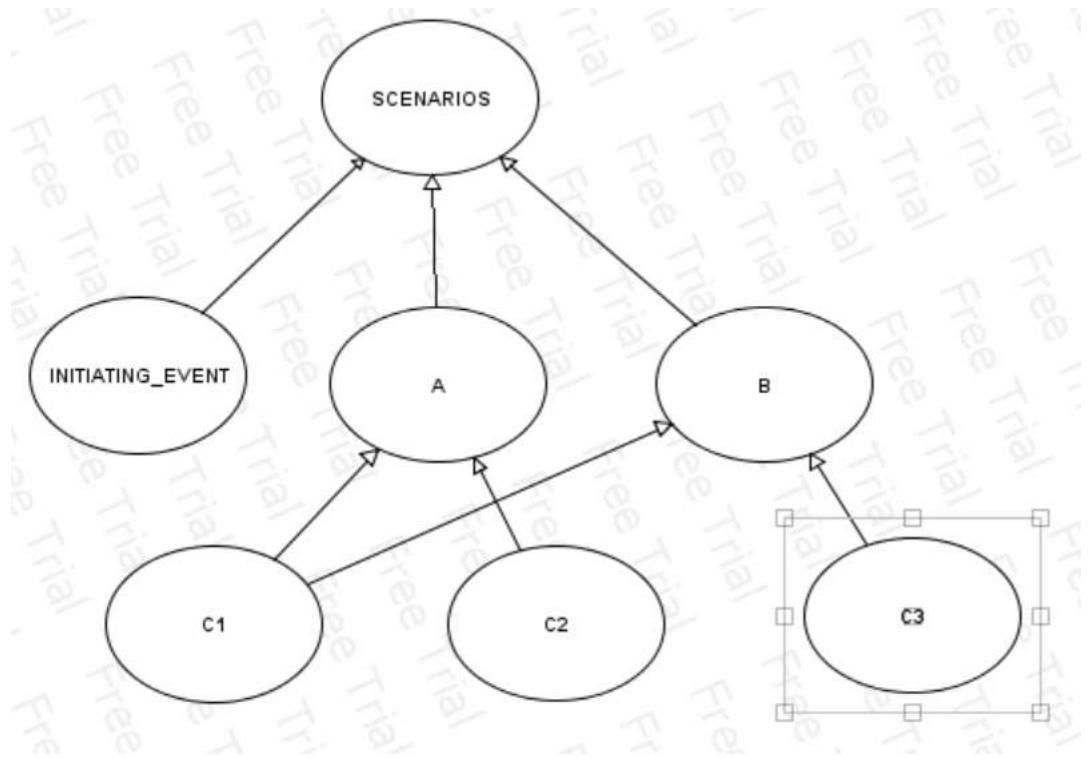
- f. For the MLE component and function, state an action to lower the probability of this particular function and its contribution to the Top Event occurrence. State how this altered function for the MLE component can be included in the BN.

An action to lower risk due to the MLE component, Flow Switch, FS, is to add a second FS in parallel to measure flow as part of the protective system if the temperature rises, which indicates that the first FS in the process control circuit has failed. This modification is then modeled in the BN by including a duplicate Flow Switch with the redundancy captured by an AND node like the AND node for the Sub Protective System.

2. Recall the problem you solved in HW5 as shown in the figure below. Develop a BN for the problem to determine the probabilities of each of the Scenarios. View the nodes as bar charts and include a screen capture of the Hot Oil Heating System BN in your homework.

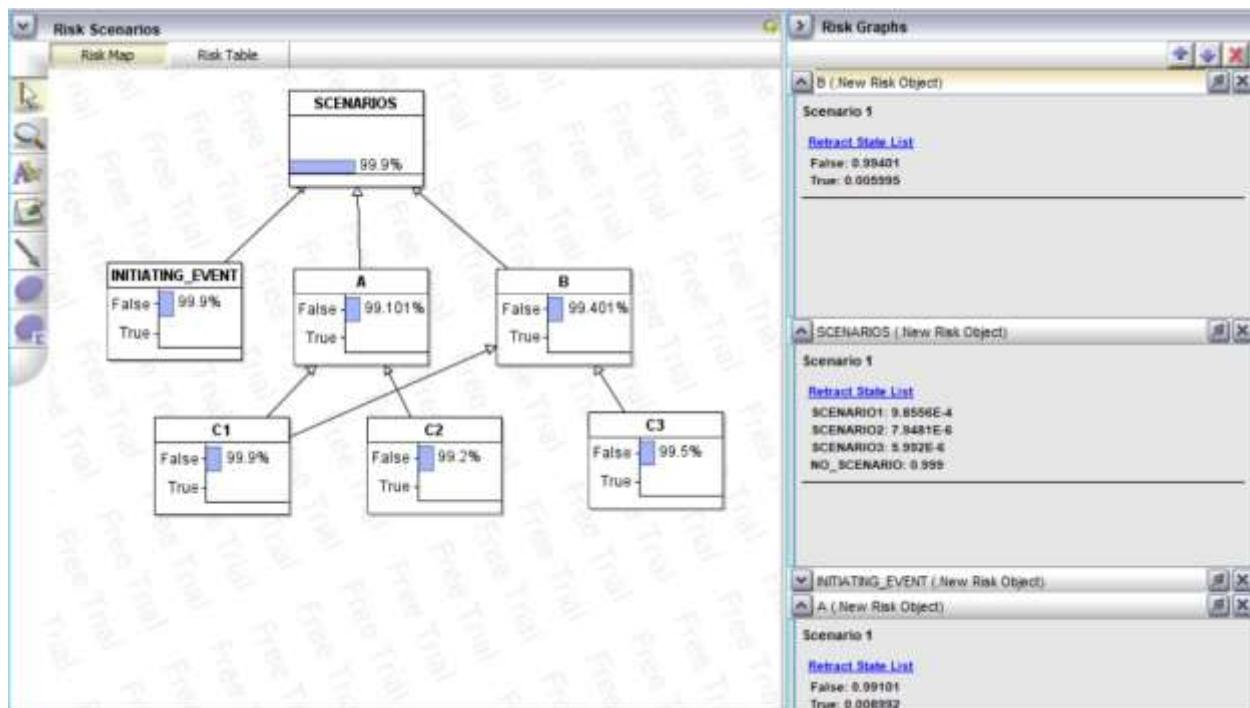


Frequency of initiating event I is $10^{-3}/\text{year}$ and failure probabilities are $\Pr(C_1)=0.001$, $\Pr(C_2)=0.008$ and $\Pr(C_3)=0.005$. Are the values different from the ones you obtained in the calculations in HW5? If so, state the reason.



The NPT for the Scenarios node is shown below. This is a labelled node. The label 'No_Scenario' is used to consider the condition when the initiating event does not occur.

A		False				True			
		False		True		False		True	
B	INITIATING...	False	True	False	True	False	True	False	True
SCENARIO1		0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0
SCENARIO2		0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0
SCENARIO3		0.0	0.0	0.0	1.0	0.0	0.0	0.0	1.0
NO_SCENARIO		1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0



3. Ungrouped failure data with 10 failure (or repair) times in hour units are given: 38.7, 45.4, 52.0, 63.6, 70.0, 43.1, 79.5, 18.3, 58.8, 49.0

- a) Order the data by time of failure (first failure to last failure) in a table with the following columns: Time; Reliability, R(t); Failure, F(t) with each to be estimated using the associated empirical expression and the calculated values placed in the table. Use the median plotting position for F(t). Calculate the mean time to failure, MTTF, of the 10 failure times. Estimate the median failure time by selecting the middle value (Since the number of failures are even, you will take the mean of the two middle points.) Calculate and report the empirical variance and the standard deviation of the data.

i	t	F(ti)	R(ti)
	0		
1	18.3	0.067308	0.932692
2	38.7	0.163462	0.836538
3	43.1	0.259615	0.740385
4	45.4	0.355769	0.644231
5	49	0.451923	0.548077
6	52	0.548077	0.451923
7	58.8	0.644231	0.355769
8	63.6	0.740385	0.259615
9	70	0.836538	0.163462
10	79.5	0.932692	0.067308

Mean: Sum of all times divided by 10 = 51.84

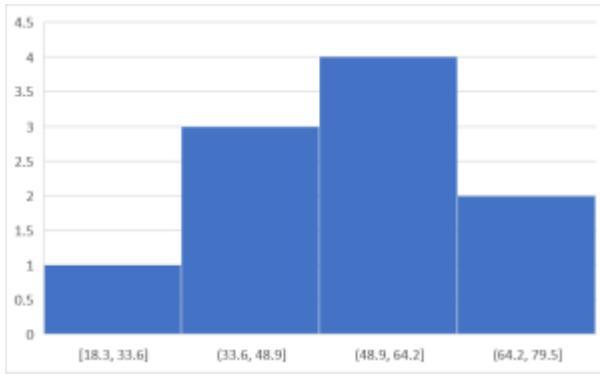
Median: (49+52)/2=50.5

$$\text{Variance} = s^2 = \frac{\sum_{i=1}^n t_i^2 - n\widehat{MTTF}^2}{n-1} = \frac{29579 - 10(51.84)^2}{9} = 300,$$

Standard Deviation s=17.3

- b) Use Sturges' Rule to determine the number of bins/classes/groups the data should be divided into. Use your result to sketch a histogram using the time data (Right click the x-axis of your histogram to go to the axis option. Set the number of bins in your histogram in excel equal to the number you found from Sturges' Rule).

$$\text{Sturges' Rule} = 1 + 3.3 \cdot \log(10) = 4.3 \sim 4$$



- c) Apply your knowledge of descriptive statistics to answer the following and identify population model candidates:

- Compare the MTTF with the median time to failure you calculated in a and state what this suggests concerning potential population model candidates and state three distributions that are consistent in behavior with this information.

Because the mean and median are very close in value, a symmetric pmf of failure, $f(t)$, represents these data. Therefore, candidate models are Normal, Weibull ($\beta = 3$ to 4), Lognormal ($s \leq 0.1$).

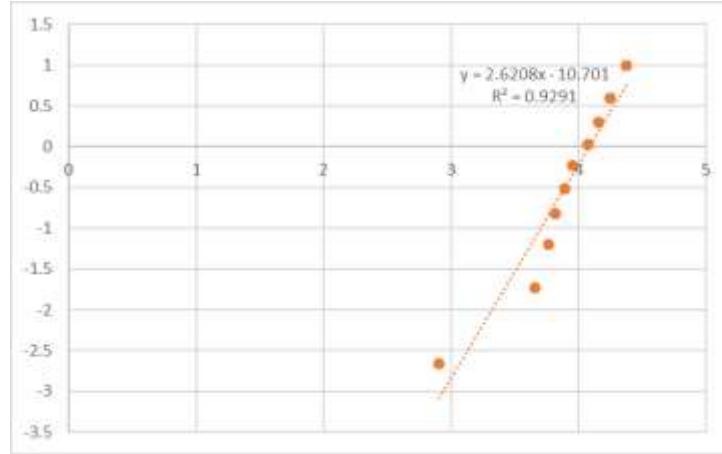
- Comment on your histogram with regard to symmetry of the pmf (probability mass function), $f(t)$, to make suggestions about the model. Provide a list of at least two potential models and state why. Also, state what you expect the failure rate behavior to be, i.e., which region of the bathtub curve: DFR, CFR, or IFR?

A histogram is expected to be roughly symmetrical indicating normal or Weibull ($\beta = 3$ to 4), and a histogram of the failure rate $\lambda(t)$ is expected to be increasing with time. $\lambda(t)$ is expected to show IFR (increasing failure rate).

Candidate distributions based on the data are Normal, Weibull, Lognormal, or Gamma, which can each represent IFR.

- d) Perform a Weibull least-squares fit of the data and report the Intercept, a ; Slope, and the scale and shape parameter of the Weibull distribution. Report also the R-squared value from the least squares

fit. Comment on your obtained value of the shape parameter (does it match your guess from the descriptive statistics?)



$$\text{Shape parameter } \beta = \text{slope} = 2.62$$

$$\text{Scale Parameter } \theta = e^{-\text{intercept}/\text{slope}} = e^{10.7/2.62} = 59.3 \text{ hrs}$$

- e) From your calculation of the empirical MTTF, variance and std. dev. calculated in a), report the empirical upper and lower $1-\alpha$ confidence interval, $\alpha/2 = 0.05$, (90% confidence interval), for MTTF using the t distribution for $n-1 = 9$ degrees of freedom.

$$\widehat{MTTF} \pm t_{\frac{\alpha}{2}, n-1} \frac{s}{\sqrt{n}} = 51.84 \pm t_{0.05, 9} \frac{56.8}{\sqrt{10}} = 51.84 \pm \left(1.833 \times \frac{56.8}{\sqrt{10}} \right)$$

4. A set of 40 high-efficiency pumps is tested. All of the pumps fail ($F=40$) after 400 pump hours of operation ($T=400$). It is believed that the time to failure of the pumps follows an exponential distribution. Using the following table and the Chi-Square Goodness-of-Fit method, determine if the exponential distribution is a good choice.

Time Interval (hrs)	Number of observed failures
0-2	6
2-6	12
6-10	7

10-15	6
15-25	7
25-100	2
	Total=40

Prepare a table with columns from left to right of the following:

Time Interval (hrs), L – U (where L = lower and U = upper value in each Time Interval);

Observed Failures, O_i ;

Expected Failures, E_i ;

$(O_i - E_i)$;

$(O_i - E_i)^2 / E_i$

Use the following exponential expression to calculate the expected number of failures in each cell, E_i ,

$$\text{where: } E_i = n[e^{-\hat{\lambda}L_i} - e^{-\hat{\lambda}U_i}]$$

a) From the chi-squared table (RERA(Modarres), Table A.3), choose Significance $\alpha = 0.05$, ($1 - \alpha = 0.95$) confidence parameter, and find the critical value of χ^2 with 4 degrees of freedom (df) to compare with the Chi-Square statistic W.

b) Select the null hypothesis that the pump failure behavior can be represented at an acceptable level by the exponential distribution (behavior is exponentially distributed) if $\chi^2(0.05,4) \leq \chi^2(\text{critical})$. From your analysis, state whether the exponential distribution is a satisfactory model for these failure data.

Solution:

2.27 Computation of Chi-Squared Method for a Goodness of fit to a Exponential Distribution.

The problem is to verify that the exponential distribution is a good choice.

Steps:

1. H_0 : Null hypothesis: the distribution is $\text{Exp}(\hat{\lambda})$.
2. H_1 : Alternate hypothesis: the distribution is not $\text{Exp}(\hat{\lambda})$.
3. An $\alpha = 0.05$ require a value of $\chi^2(0.05, 4) = 9.49$
4. If $\chi^2(\text{obs}) > \chi^2(\text{crit})$, reject H_0 . That is, conclude that the data do not come from the hypothesized distribution. Otherwise, do not reject H_0 .
5. Using the sample results, the value of χ^2 is computed in the table below.

Since

$$\hat{\lambda} = \frac{n}{\sum_{i=1}^n t_i} = \frac{40}{400} = 0.10$$

and the expected number of observation in each cell is

$$e_i = n \left[e^{-\hat{\lambda} L_i} - e^{-\hat{\lambda} U_i} \right]$$

Computation of Chi-squared Method for a Goodness-of-fit to a Exponential Distribution

No i	Time Interval (hrs) $L_i - U_i$	No. of Observed Failures o_i	No. of Expected Failures e_i	$(o_i - e_i)$	$(o_i - e_i)^2$	$\sum \frac{(o_i - e_i)^2}{e_i}$
1	0 - 2	6	7.25	- 1.25	1.56	0.2155
2	2 - 6	12	10.80	1.20	1.44	0.1333
3	6 - 10	7	7.24	- 0.24	0.06	0.0080
4	10 - 15	6	5.79	0.21	0.04	0.0076
5	15 - 25	7	5.64	1.36	1.85	0.3279
6	25 - 100	2	3.28	- 1.28	1.64	0.4995
$n = 6$	100	40	40.00			1.1918

$$e_1 = 40 [e^{-0.1(0)} - e^{-0.1(2)}] \\ = 40 [1 - 0.8187] = 7.25$$

$$e_2 = 40 [e^{-0.1(2)} - e^{-0.1(6)}] \\ = 40 [0.8187 - 0.5488] = 10.80$$

$$e_3 = 40 [e^{-0.1(6)} - e^{-0.1(10)}] \\ = 40 [0.5488 - 0.3679] = 7.24$$

$$e_4 = 40 [e^{-0.1(10)} - e^{-0.1(15)}] \\ = 40 [0.3679 - 0.2231] = 5.79$$

$$e_5 = 40 [e^{-0.1(15)} - e^{-0.1(25)}] \\ = 40 [0.2231 - 0.0821] = 5.64$$

$$e_6 = 40 [e^{-0.1(25)} - e^{-0.1(100)}] \\ = 40 [0.0821 - 4.54E-5] = 3.28$$

5. The time to repair a power generator is best described by the following probability density function:

$$h(t) = \frac{t^2}{333} \quad 1 \leq t \leq 10 \text{ hr}$$

Determine the probability that a repair will be completed in 6 hour. What is the MTTR? What is the median time to repair?

Solution

$$H(t) = \int_1^t \frac{t'^2}{333} dt' = \left[\frac{t'^3}{3(333)} \right]_1^t = \frac{t^3 - 1}{999} \rightarrow H(6) = \frac{6^3 - 1}{999} = .215$$

$$MTTR = \int_1^{10} t \cdot h(t) dt = \int_1^{10} \frac{t^3}{333} dt = \left[\frac{t^4}{4(333)} \right]_1^{10} = \frac{10^4 - 1}{1332} = 7.507 \text{ hrs}$$

$$H(t_{med}) = .5 = \frac{t_{med}^3 - 1}{999} \rightarrow t_{med} = (999(.5) + 1)^{1/3} = 7.940 \text{ hrs}$$

6. Maintainability for a Subsystem: Your team is charged with developing a subsystem that has a 90% probability of operating for 5 years.

- a) If the subsystem failure times are Lognormal with a shape parameter of $s = 0.7$, predict the MTTF consistent with the subsystem requirement.
- b) If the subsystem fails, it must be repaired within 4 hr or the system of which the subsystem is a part would more likely fail and increase the System Risk to an unacceptable level. If the repair time is Lognormal with a MTTR = 2 hr and with a shape parameter of 1, calculate the probability that the subsystem will be repaired within the required time.
- c) Find the Most Probable Repair Time, i.e., the mode of the repair time distribution. The mode of a repair distribution is an important point value representative of the distribution in which the majority of repairs are distributed in the region of the mode with relatively few short repairs and even fewer very long repairs that appear in the long tail to higher t values.

Solution:

a)

$$R(t) = 1 - \Phi\left(\frac{1}{s} \ln \frac{t}{t_{med}}\right) = 1 - \Phi\left(\frac{1}{.7} \ln \frac{5}{t_{med}}\right) = .90 \rightarrow \Phi\left(\frac{1}{.7} \ln \frac{5}{t_{med}}\right) = .10$$

$$\frac{1}{.7} \ln \frac{5}{t_{med}} = -1.28 \rightarrow t_{med} = \frac{5}{e^{.7(-1.28)}} = 12.249 \text{ yrs}$$

$$MTTF = t_{med} e^{s^2/2} = 12.249 e^{.7^2/2} = 15.650 \text{ yrs}$$

b)

$$t_{med} = \frac{MTTR}{e^{s^2/2}} = \frac{2}{e^{.7^2/2}} = 1.213 \text{ hrs} \rightarrow H(4) = \Phi\left(\frac{1}{s} \ln \frac{4}{t_{med}}\right) = \Phi\left(\ln \frac{4}{1.213}\right) = .883$$

c)

$$t_{mode} = \frac{t_{med}}{e^{s^2}} = \frac{1.213}{e^1} = .446 \text{ hrs}$$