Chemical Engineering 612

Reactor Design and Analysis

Lecture 23
Probabilistic Risk Assessment (PRA)*

*Material taken from the nuclear regulatory commission's PRA Primer

Spiritual Thought

"My dear young brothers and sisters, these surely *are* the latter days, and the Lord is hastening His work to gather Israel. That gathering is the most important thing taking place on earth today. Nothing else compares in magnitude, nothing else compares in importance, nothing else compares in majesty. And if you choose to, if you want to, you can be a big part of it. You can be a big part of something big, something grand, something majestic!"

President Russel M. Nelson

Probabilistic Risk Assessment

- Identification and Analysis of:
  - Initiating events
  - Safety functions
  - Accident sequences
- Success response:
  - Plant transitions to stable end-state for a specified period of time.
- PRA model to find frequency and consequence of not having successful response

PRA Model

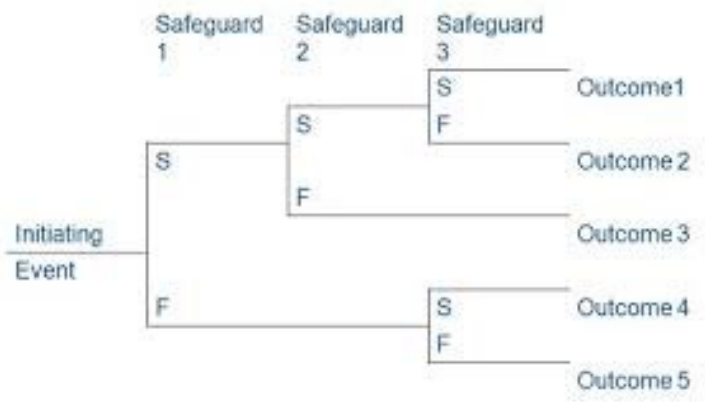
- As-Built, As-Operated Plant
- Highly interdisciplinary: detailed data from:
  - Plant design information
  - Thermal hydraulic analyses of plant response
  - Operating experience data
  - Human Factors data
  - Emergency, abnormal, and system operating procedures
  - Maintenance practices and procedures

PRA Model Basis

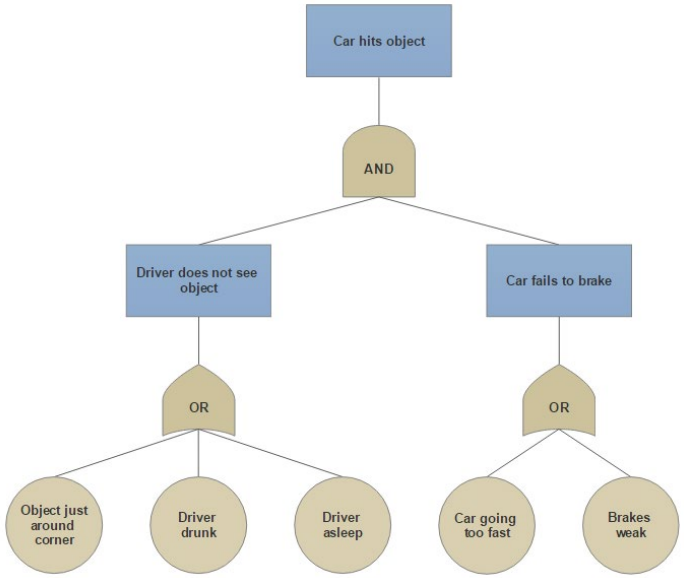
- Model must incorporate:
  - Physical Responses
    - Neutronics
    - Thermal Hydraulics
  - Automatic Responses
    - Reactor trip/Turbine trip
    - Mitigating equipment actuation
  - Operator Responses (per procedures)
    - Manual Reactor Trip
    - Manual Switchover to sump recirculation

PRA Components

- Event Trees



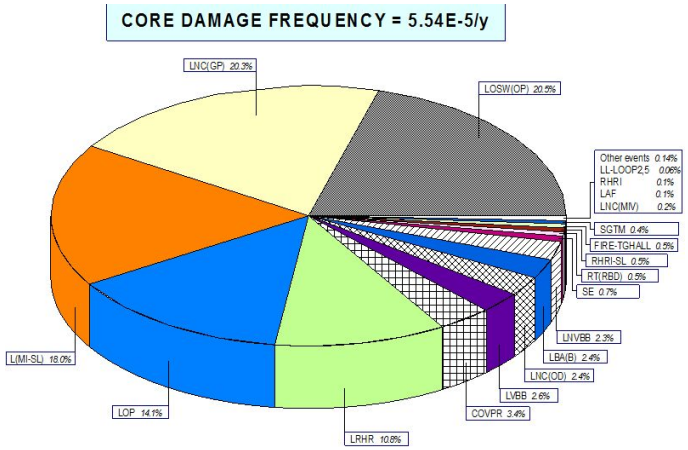
- Faults Trees



- Frequency/Probability Estimates

PRA Outcomes

- Core Damage Frequency
  - Level 1 PRA



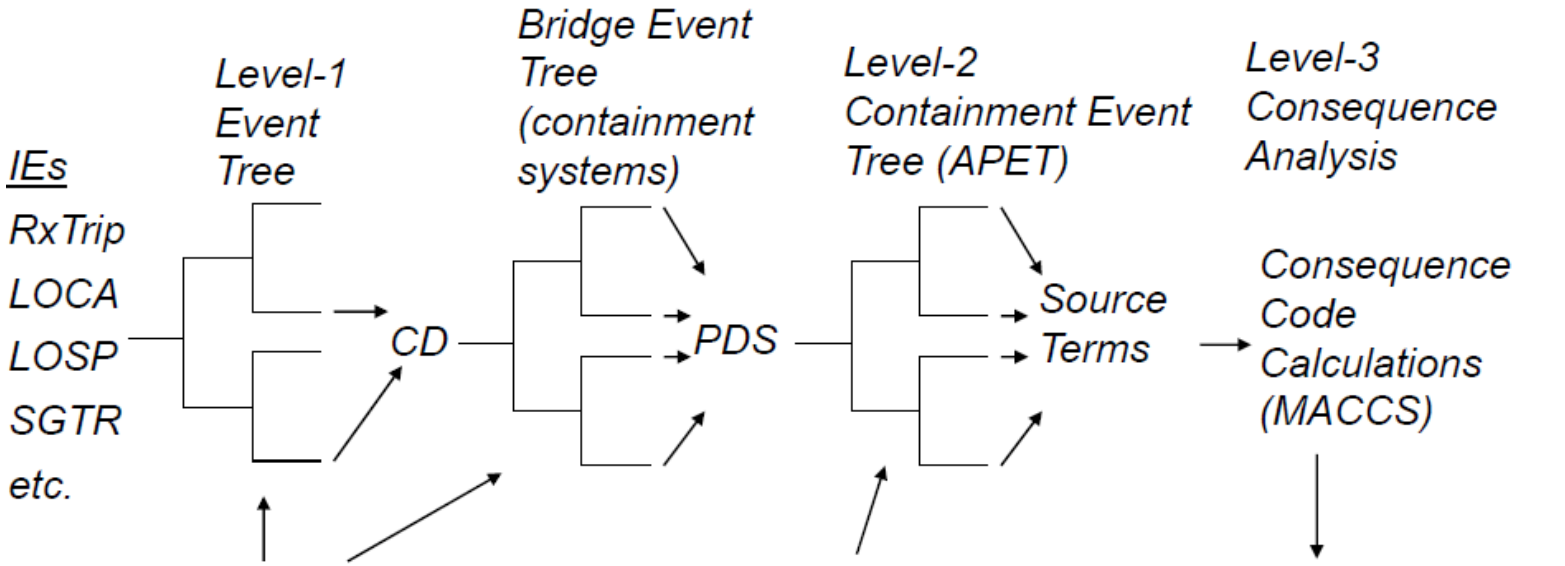
- Radioactive release frequencies
  - Level 2 PRA

- Radiological Consequences
  - Level 3 PRA

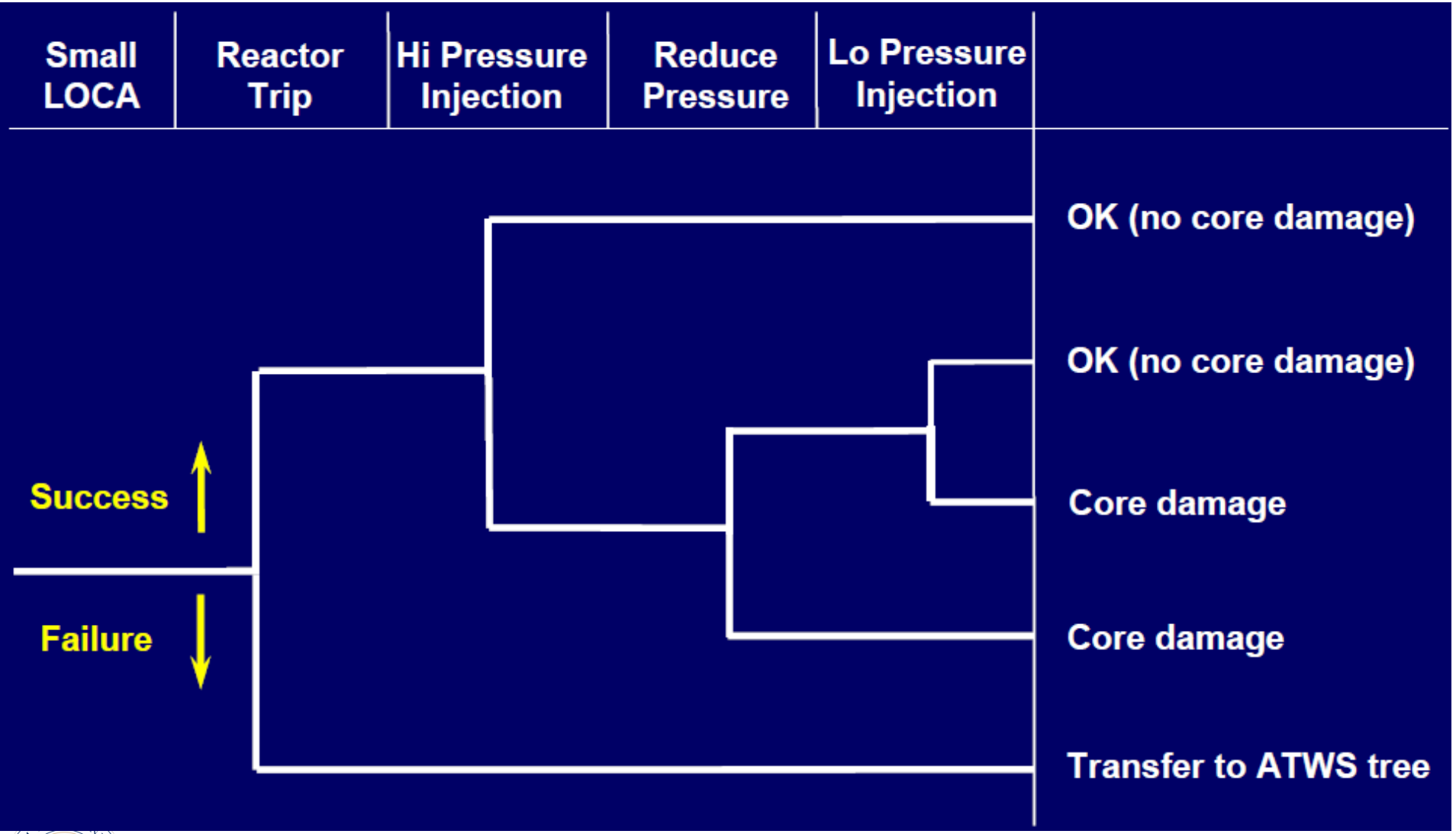
Probability Risk Assessment

$$\text{Risk}\left[\frac{\text{Consequence Magnitude}}{\text{Unit of Time}}\right] =$$

$$\text{Frequency}\left[\frac{\text{Events}}{\text{Unit of Time}}\right] \text{ x Consequences}\left[\frac{\text{Magnitude}}{\text{Event}}\right]$$



Event Tree


Small LOCA
Reactor Trip
Hi Pressure Injection
Reduce Pressure
Lo Pressure Injection
Success
Failure
OK (no core damage)
OK (no core damage)
Core damage
Core damage
Transfer to ATWS tree

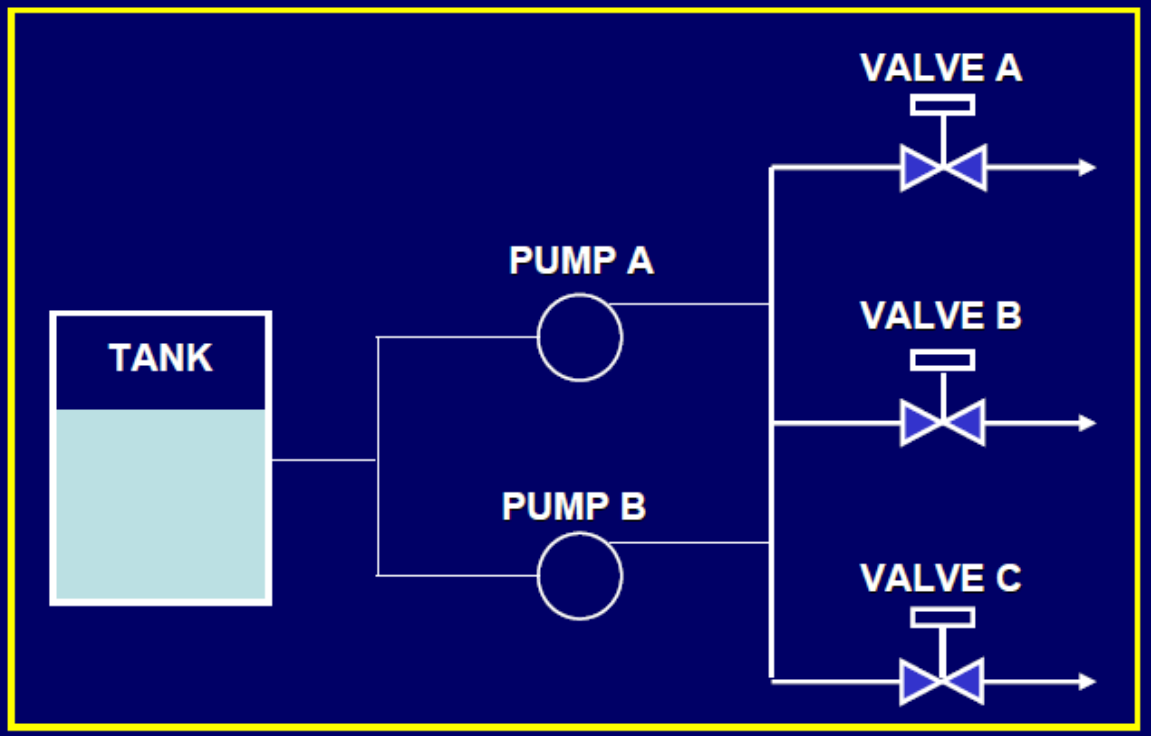
Fault Tree

What is a fault tree?

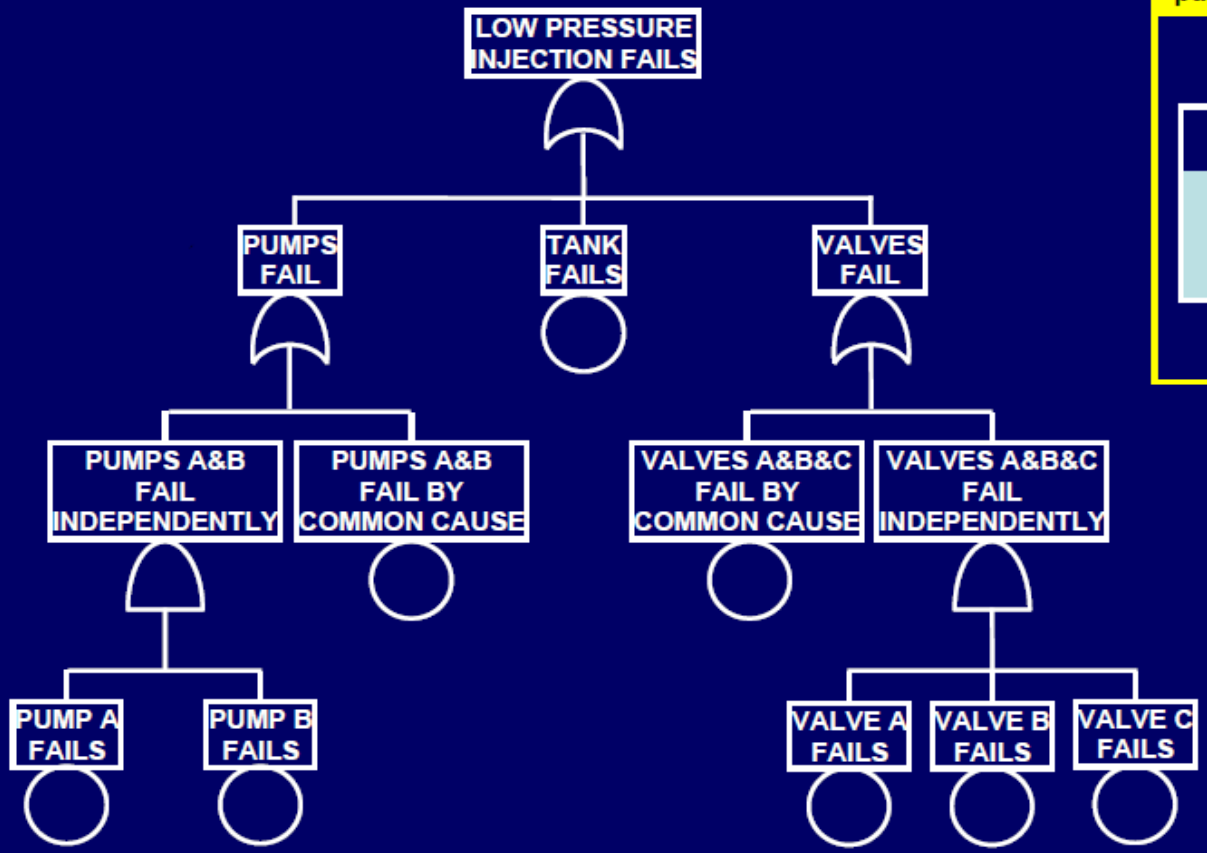
A graphical depiction of how a system can fail

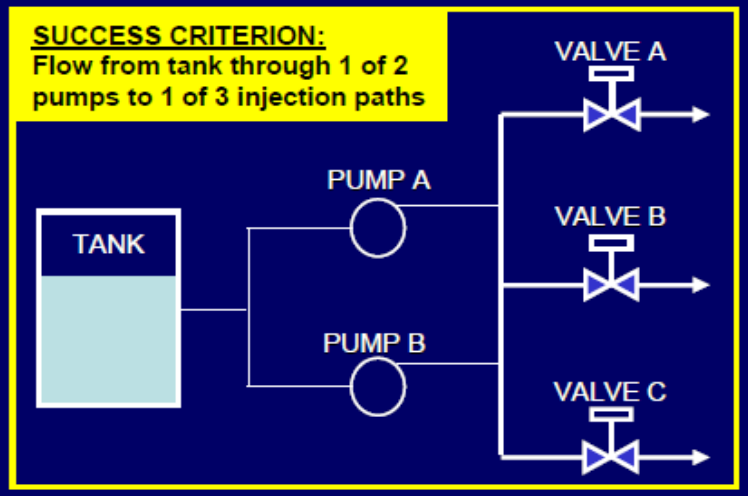
SUCCESS CRITERION:
Flow from tank through 1 of 2 pumps to 1 of 3 injection paths

FAILURE OCCURS WHEN:
No flow from tank
OR
No flow from pumps
OR
No flow through injection paths

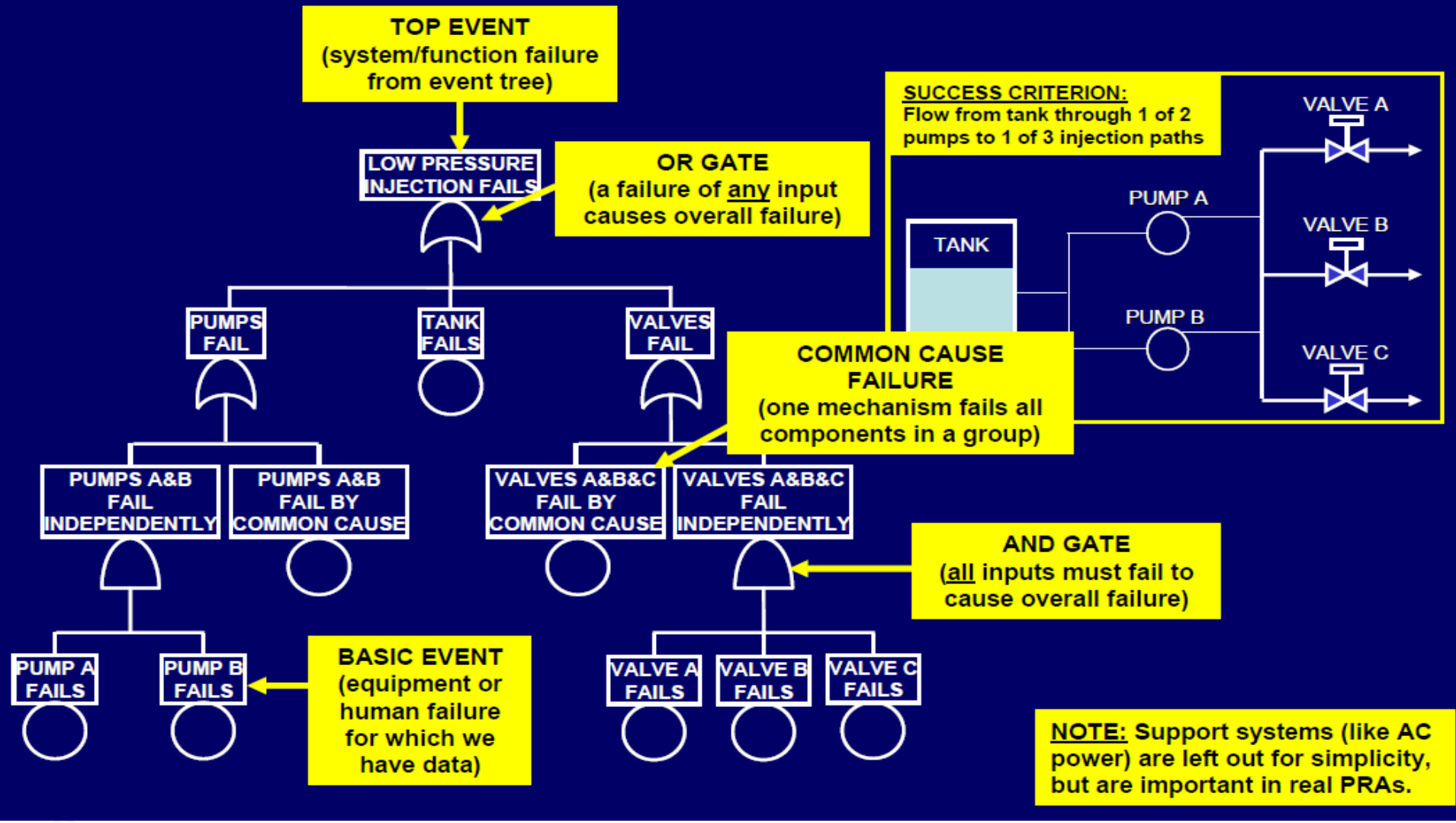


What is a fault tree?

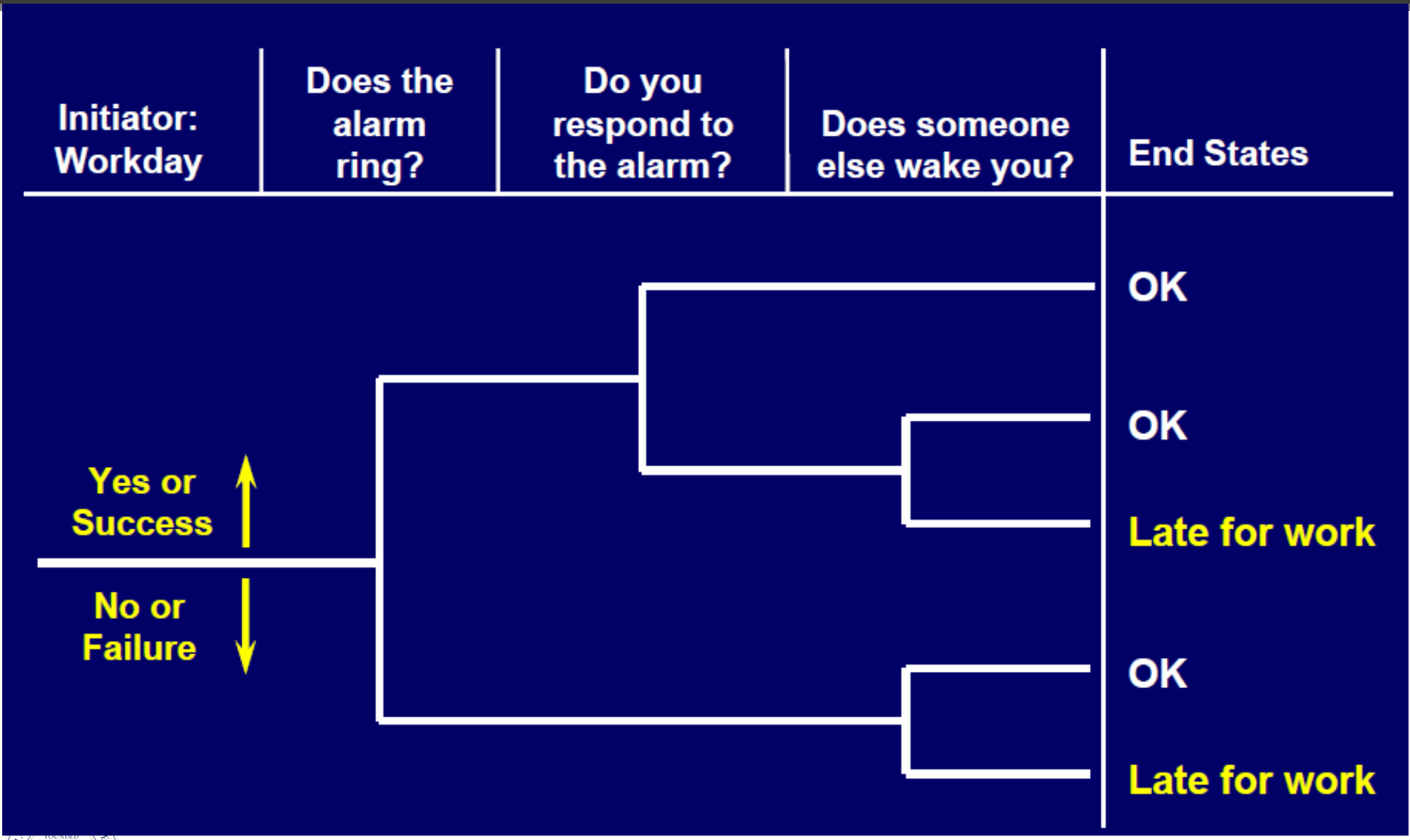




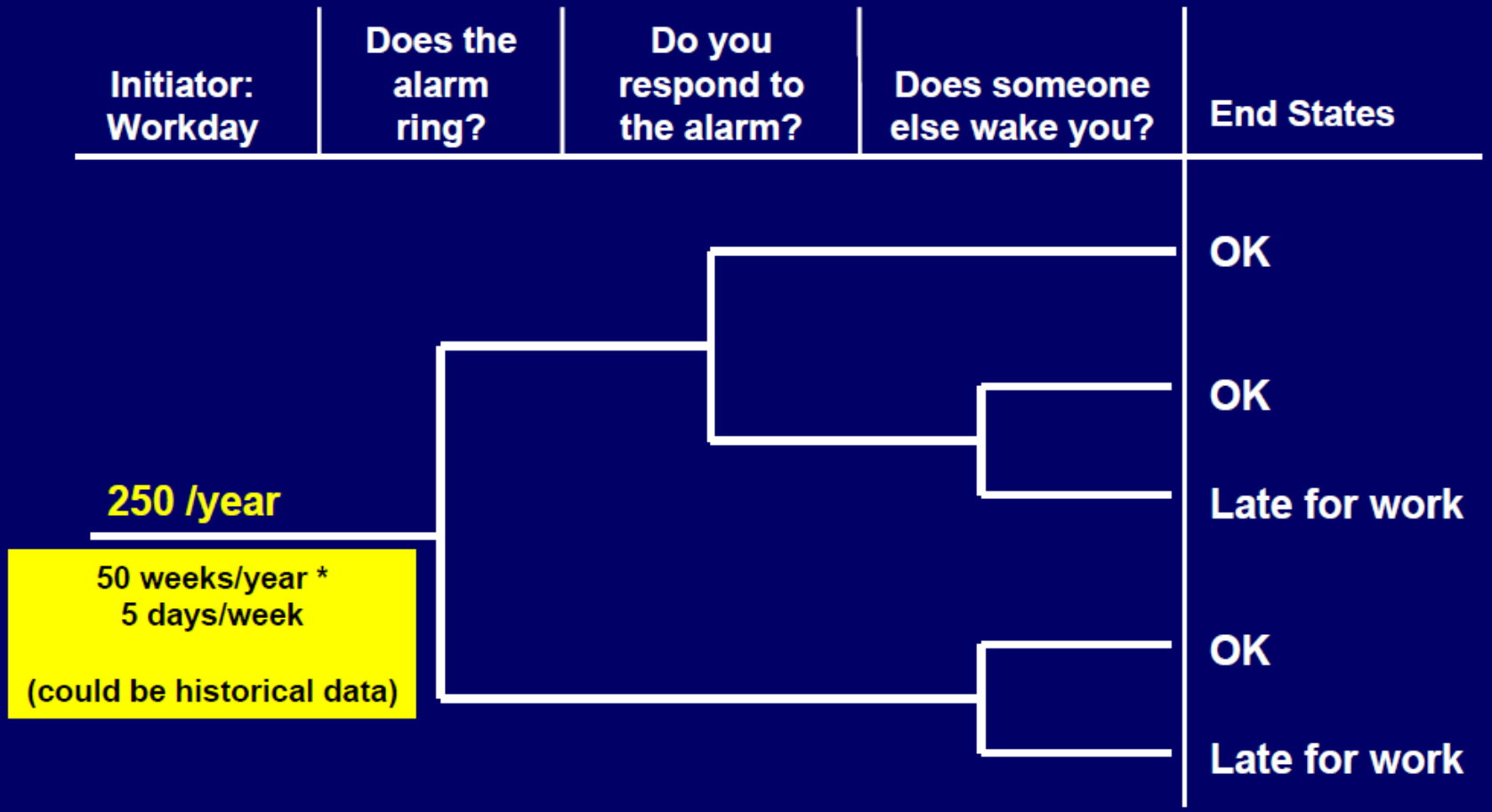
What is a fault tree?



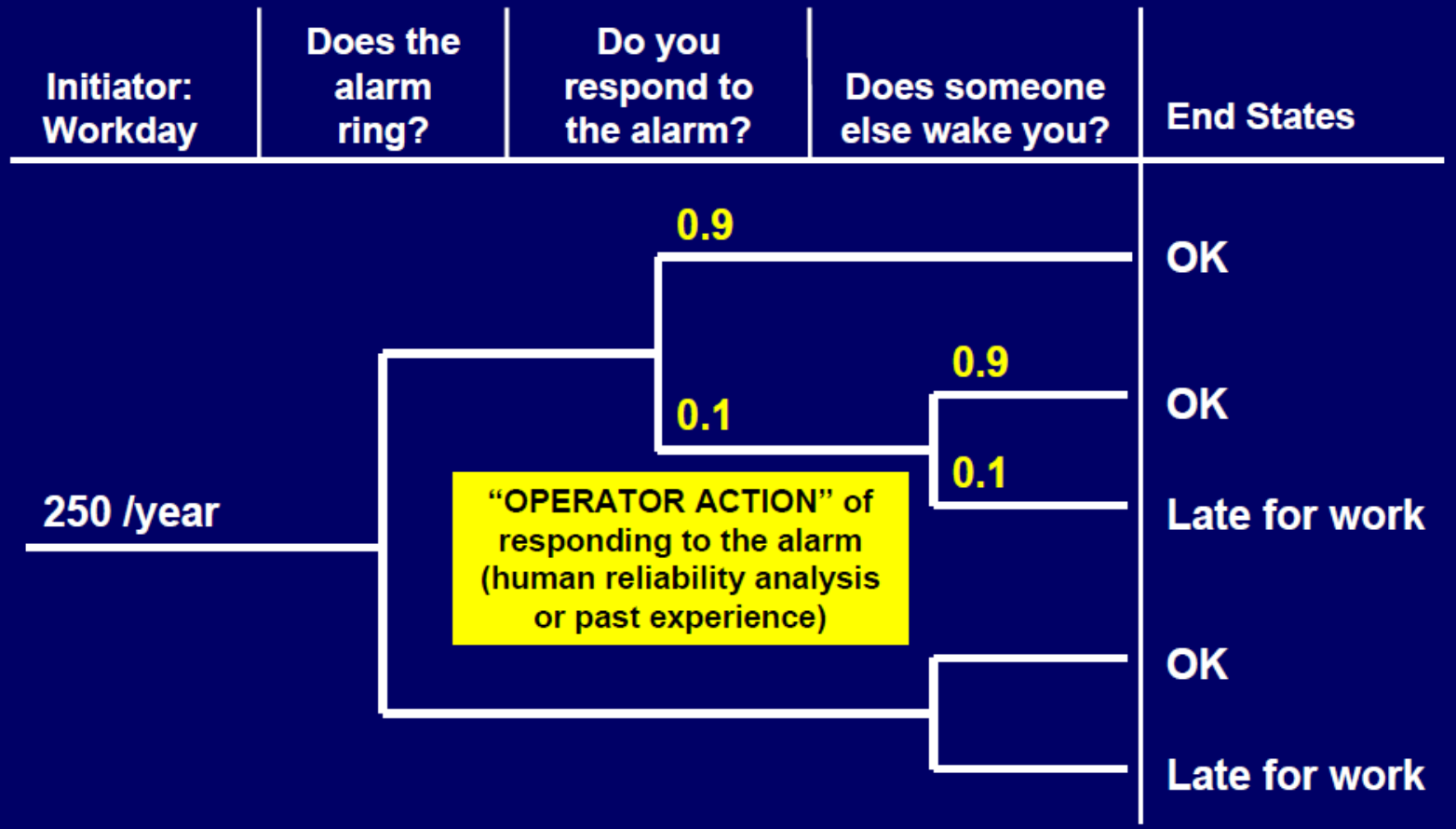
Probabilistic Example



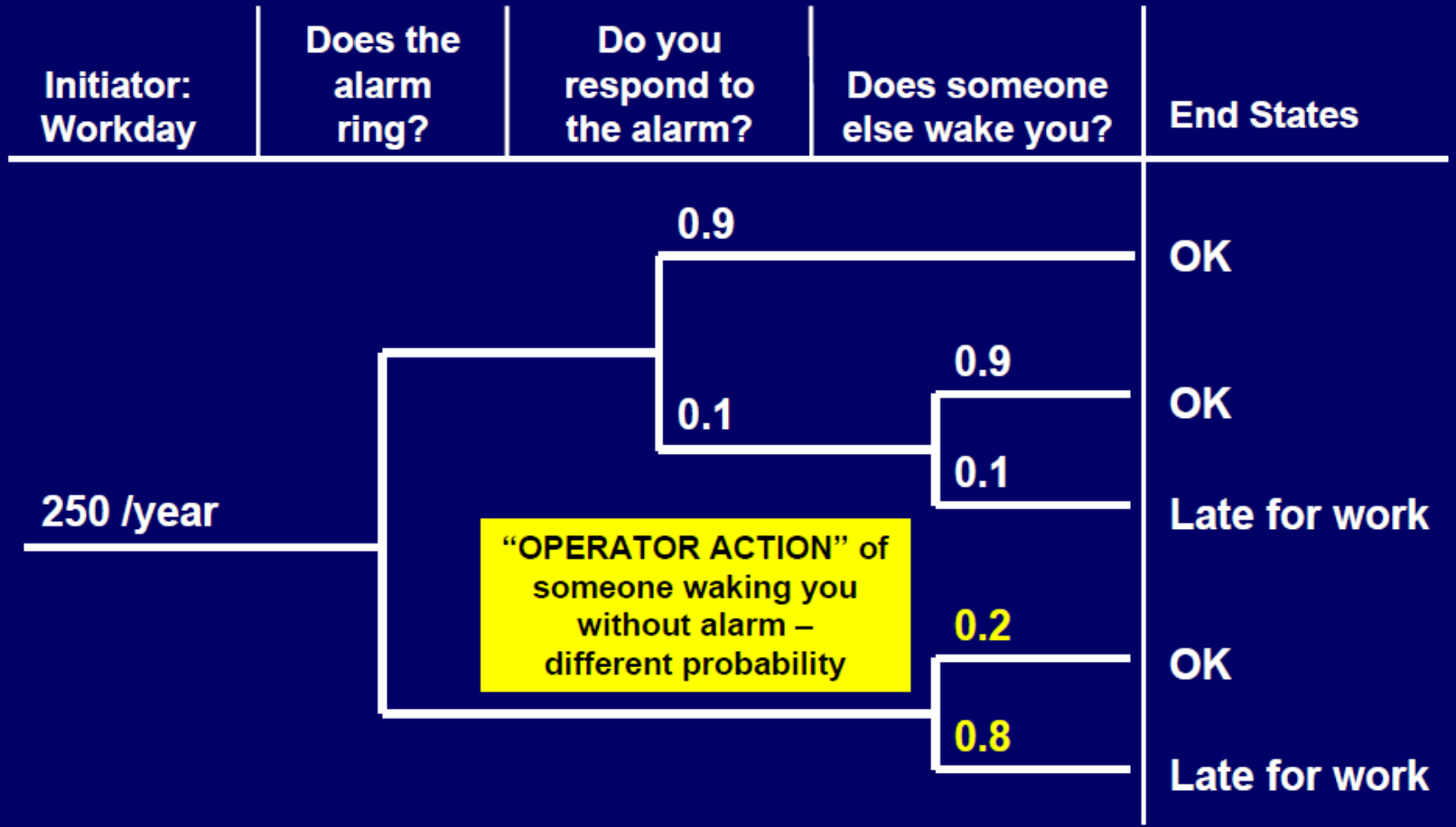
Estimating the Frequency of Oversleeping



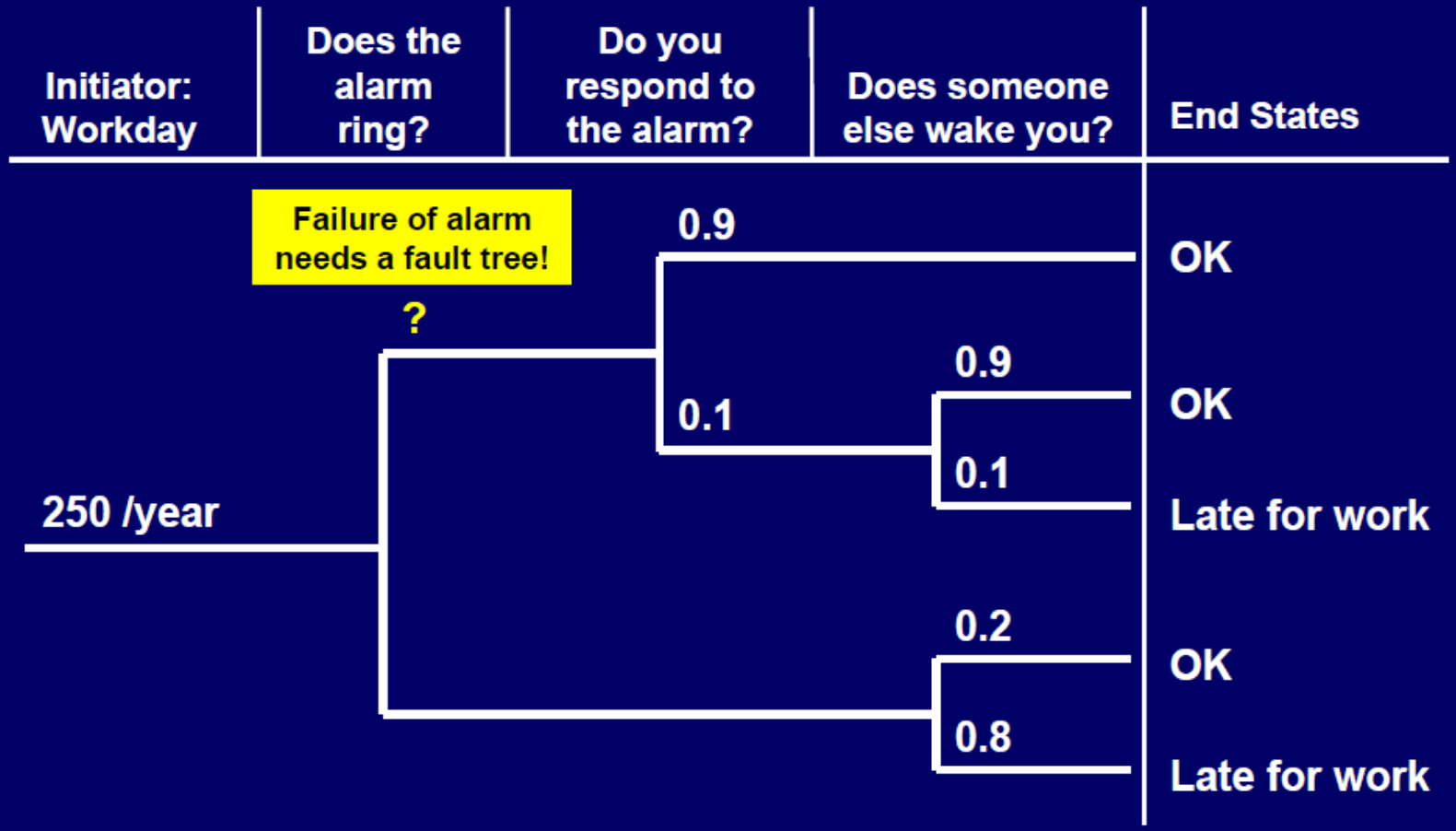
Estimating the Frequency of Oversleeping



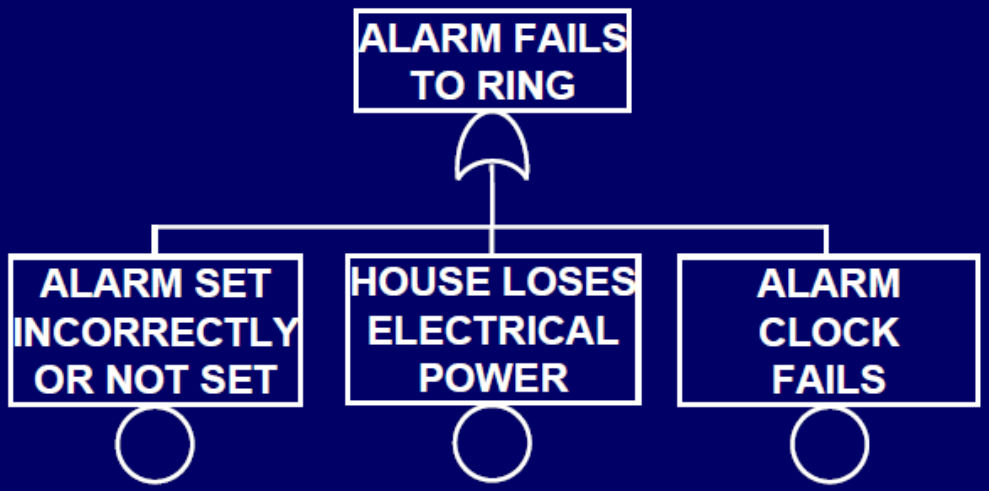
Estimating the Frequency of Oversleeping



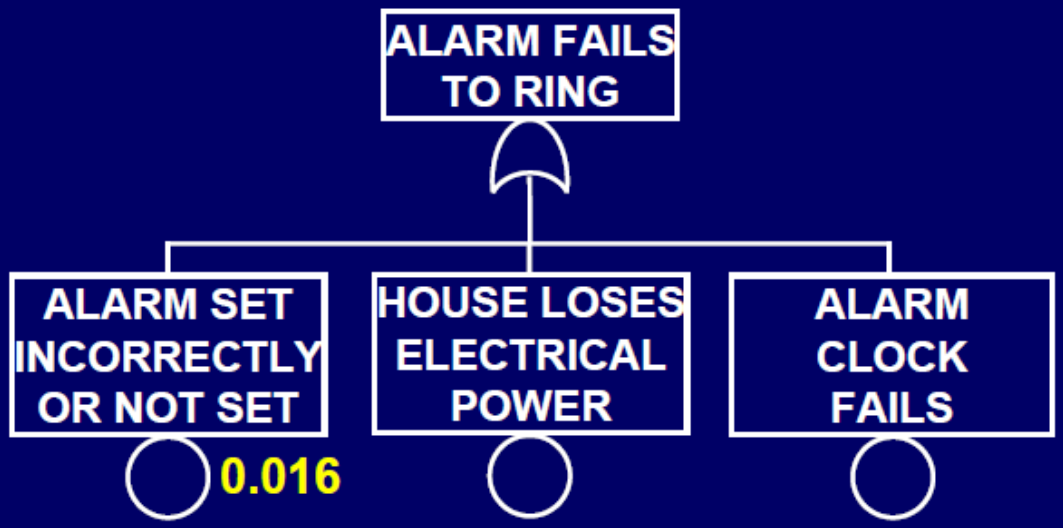
Estimating the Frequency of Oversleeping



Sample Fault Tree for Alarm Failing to Ring

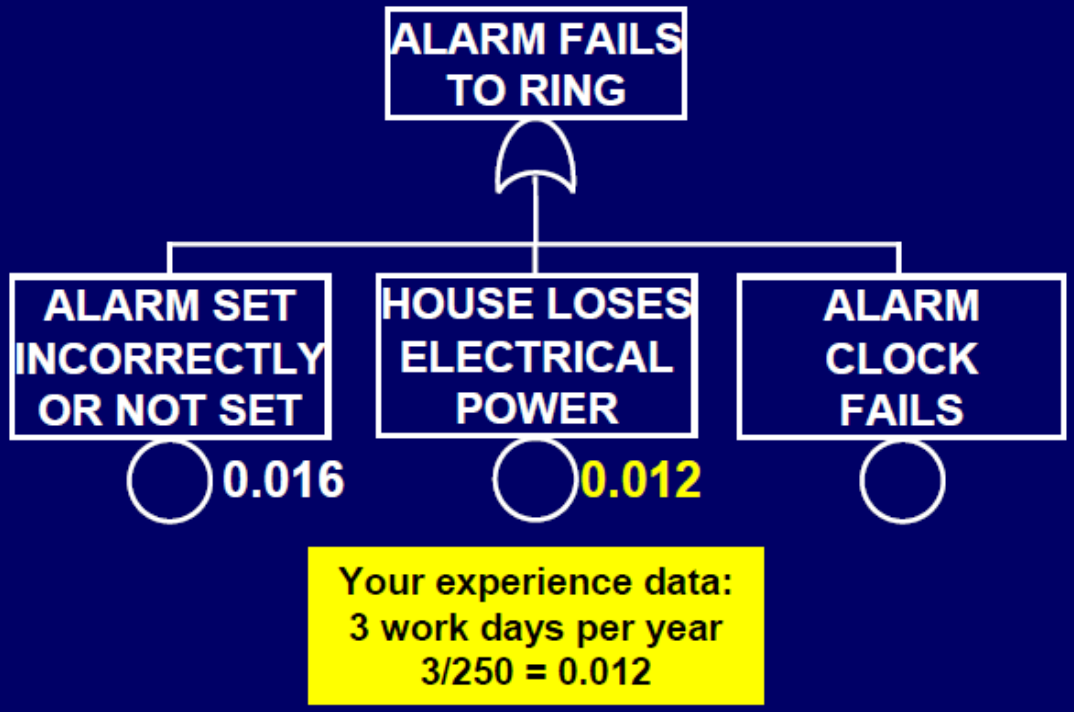


Estimating the Probability of Alarm Failing to Ring

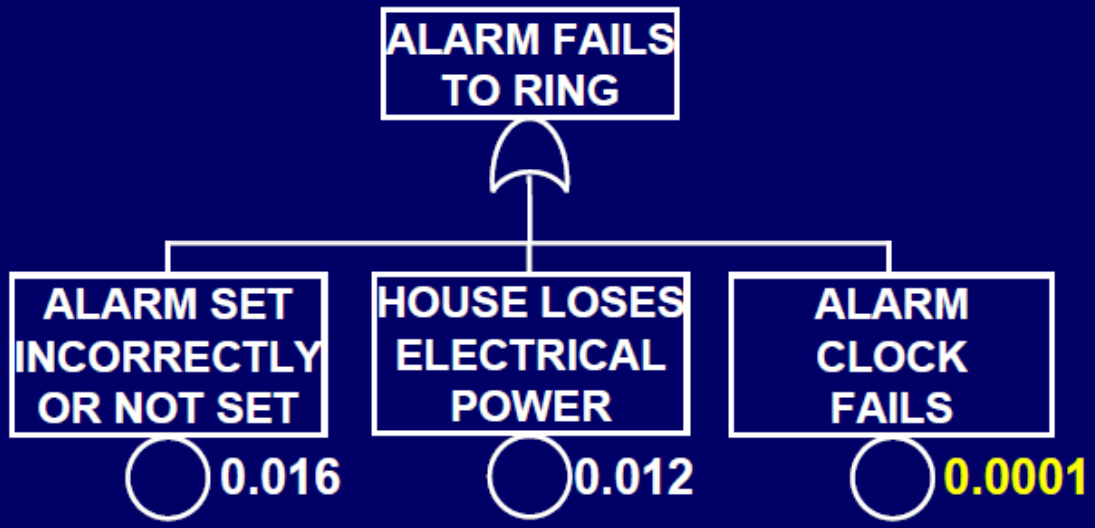


Your experience data:
4 times each work year
4/250 = 0.016

Estimating the Probability of Alarm Failing to Ring

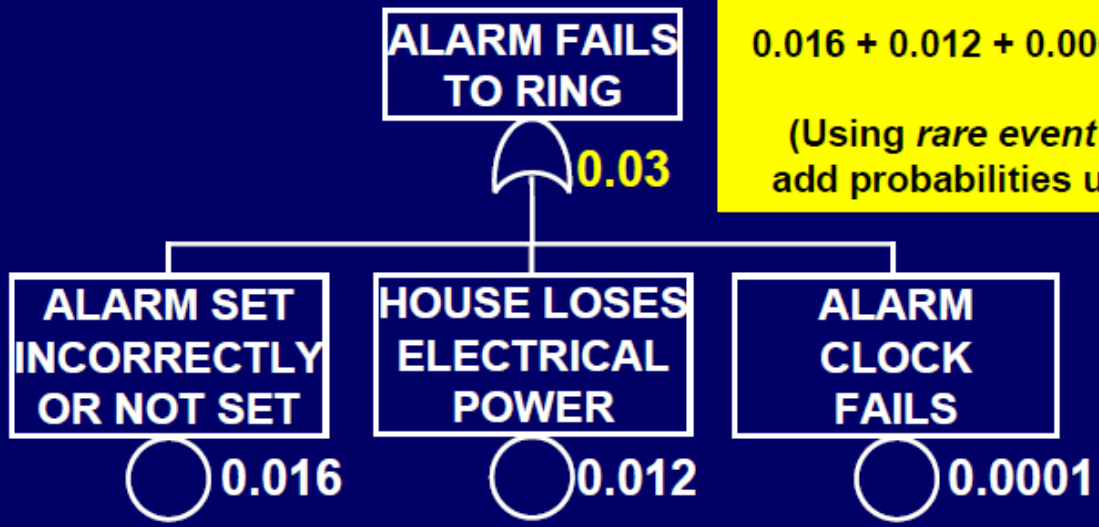


Estimating the Probability of Alarm Failing to Ring



Clock company's experience data:
1 failure in 10,000 demands
1/10000 = 0.0001

Estimating the Probability of Alarm Failing to Ring

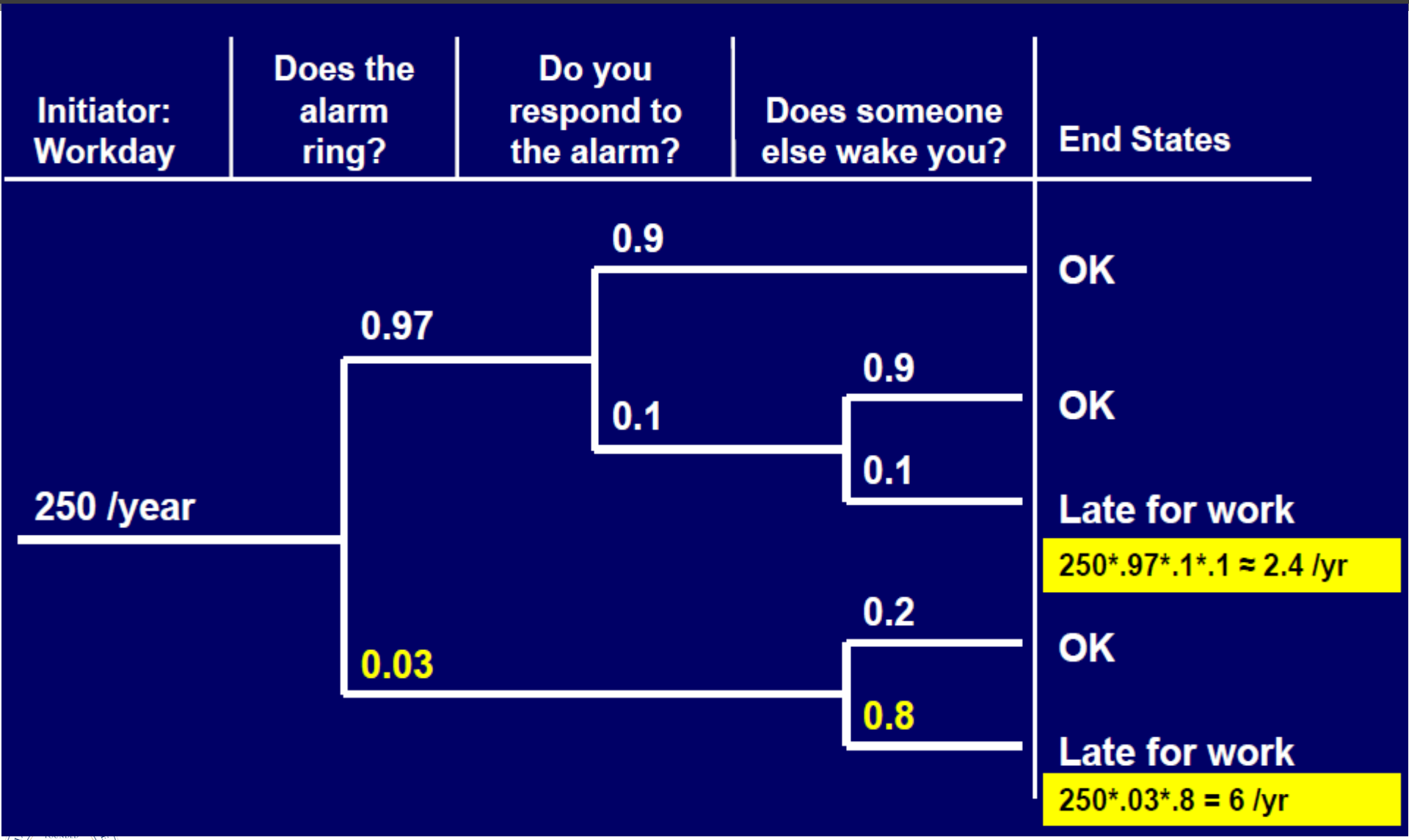


Overall failure probability:

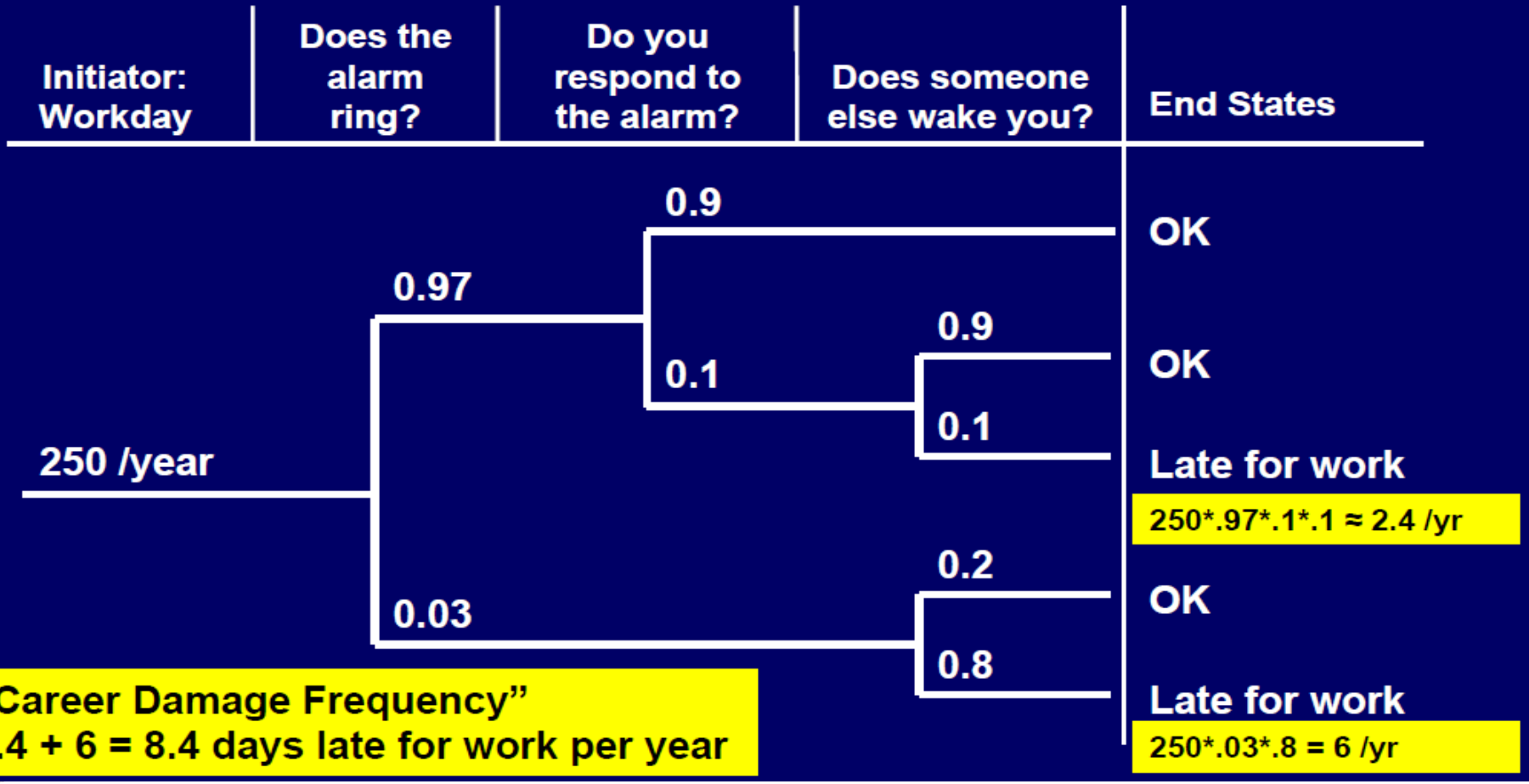
$0.016 + 0.012 + 0.0001 = 0.0281 \approx 0.03$

(Using *rare event approximation*, add probabilities under "OR" gate)

Probabilistic Example

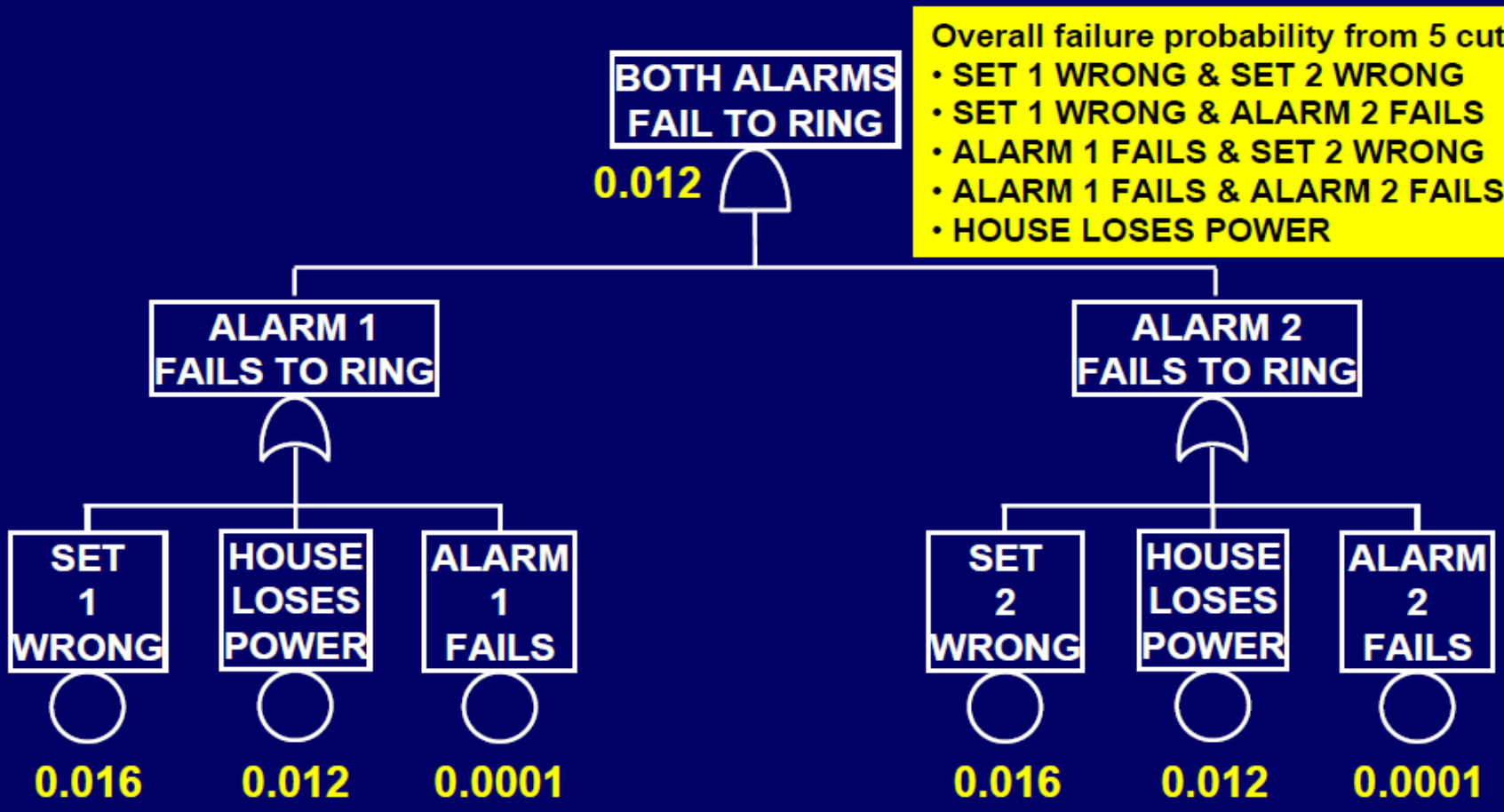


Estimating the Frequency of Oversleeping

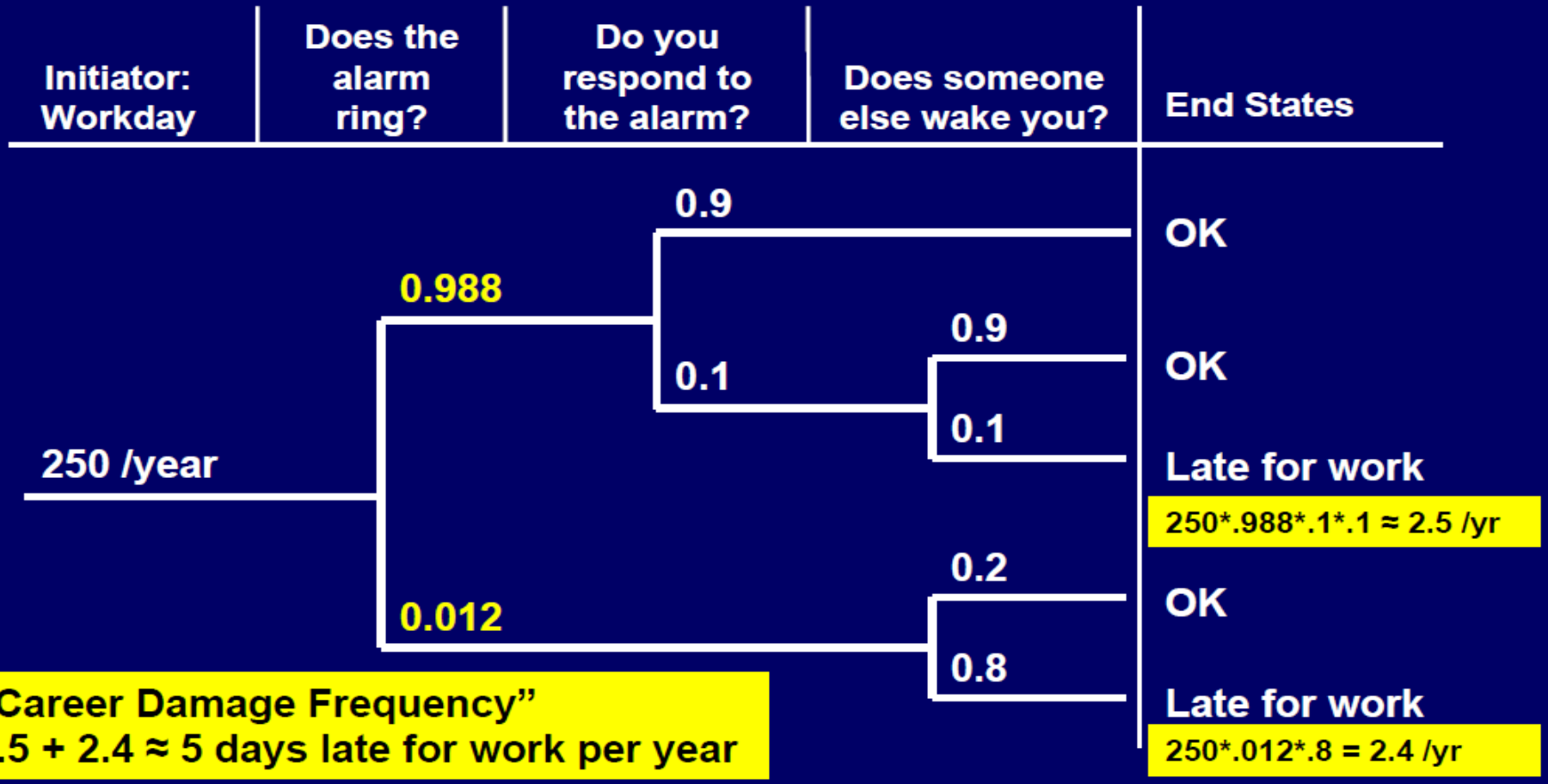


"Career Damage Frequency"
2.4 + 6 = 8.4 days late for work per year

Estimating the Probability of 2 Alarms Failing to Ring



Estimating the Frequency of Oversleeping (2 Alarms)



"Career Damage Frequency"
2.5 + 2.4 ≈ 5 days late for work per year

Notes on the Example

- **Simplified example – not a complete guide to PRA modeling!**
- **A "real" PRA may have:**
  - Dependencies that mean you can't just multiply event tree branch probabilities as we did
  - Common cause failure modeling
  - Ways to remove logically impossible combinations
- **However, we saw that there is a logical way to model events and failures and estimate parameter data.**
- **As a bonus, we saw that redundant equipment helps, but only up to a point!**

Probabilities/Reliability?

- Manufacturer's Information
- Expert Solicitation
- Human Reliability Analysis
- Common Cause Failure
- Operating Experience
- Estimation
- Guess – 95% reliability for most standard equipment (higher for safety grade)

Estimation Parameters

- Mean Time Between Failures (MTBF) - hours
  - $\frac{total\ operating\ time}{\#\ of\ failures}$
- Mean Time to Repair (MTTR) - hours
  - $\frac{Total\ time\ of\ all\ repairs}{\#\ of\ repair\ instances}$
- Availability
  - $\frac{MTBF}{MTTR}$
- Probability of Failure (Reliability)
  - $R(t) = e^{-(\lambda t)}$, $\lambda = \frac{1}{MTBF}$, t is time in hours

Original Safety Strategy

- **Deterministic** Approach
  - Lacked theory & computational input
  - "Empirical" approach to safety
  - Multiple Layers of protection
    - Clad
    - RPV
    - primary system
    - containment
    - etc.
  - Significant effort to mitigate "possibilities" with additional layers of defense
    - Airplane crash ➔ additional containment thickness

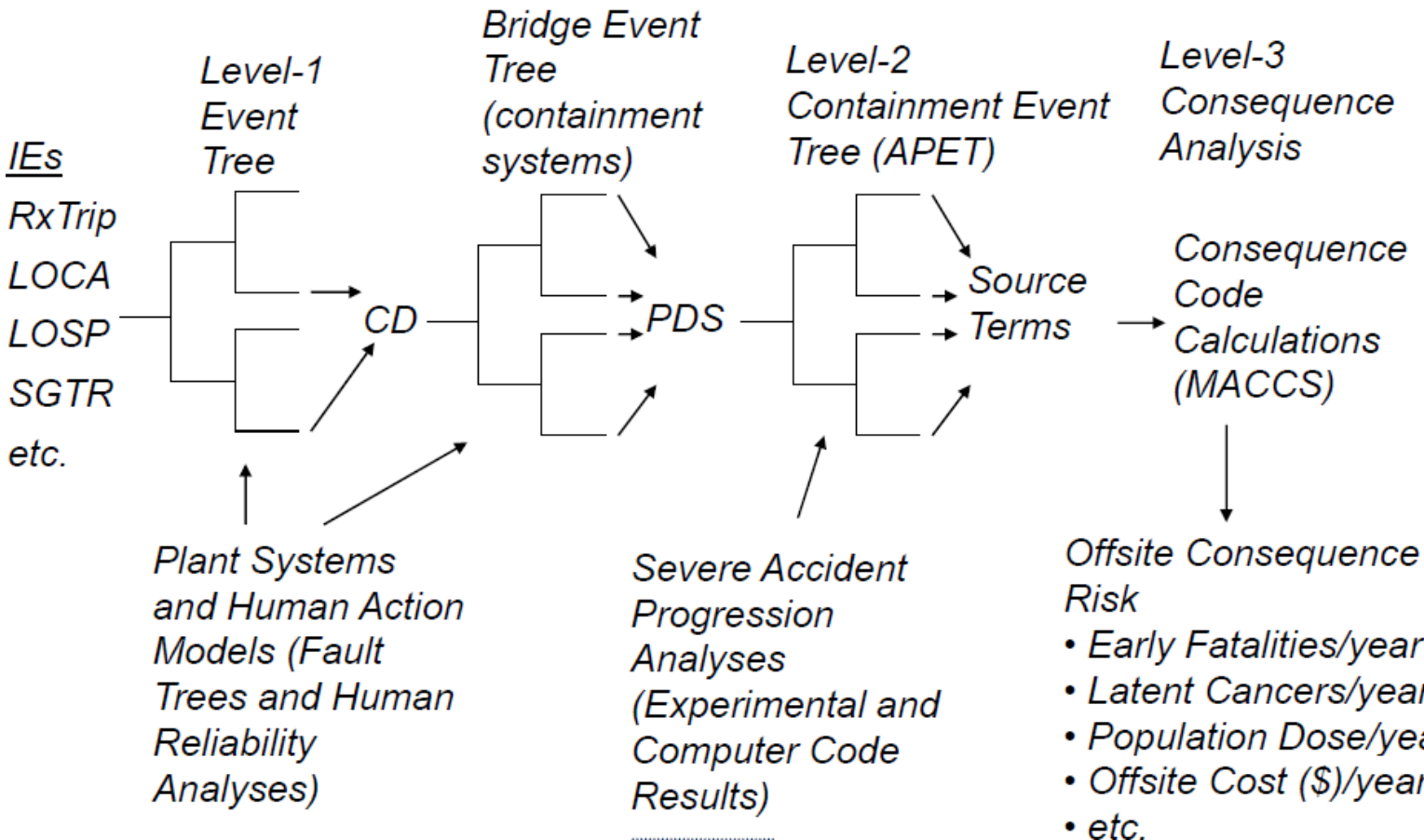
Challenges with Deterministic

- More accident possibilities = more layers
- Expensive, complex and boundless
- Possible to bypass all layers (Fukushima)
- Competing effects for systems
  - Core cooling systems
    - LOHS – Loss of heat sink
    - LOCA – Loss of coolant accident
- EXCESS MARGIN = EXPENSIVE POWER

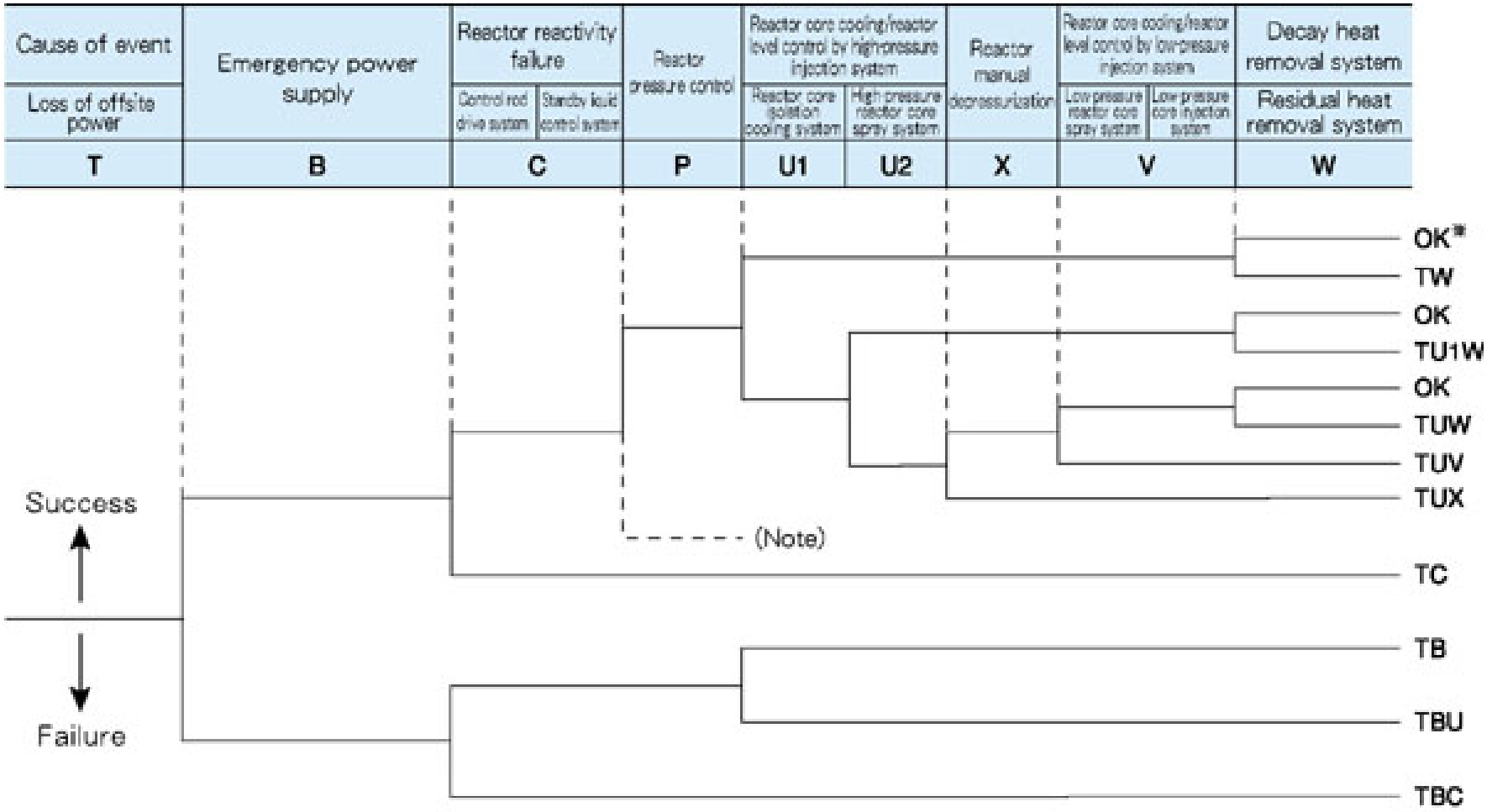
Probability Risk Assessment

$$\text{Risk}\left[\frac{\text{Consequence Magnitude}}{\text{Unit of Time}}\right] =$$

$$\text{Frequency}\left[\frac{\text{Events}}{\text{Unit of Time}}\right] \text{ x Consequences}\left[\frac{\text{Magnitude}}{\text{Event}}\right]$$



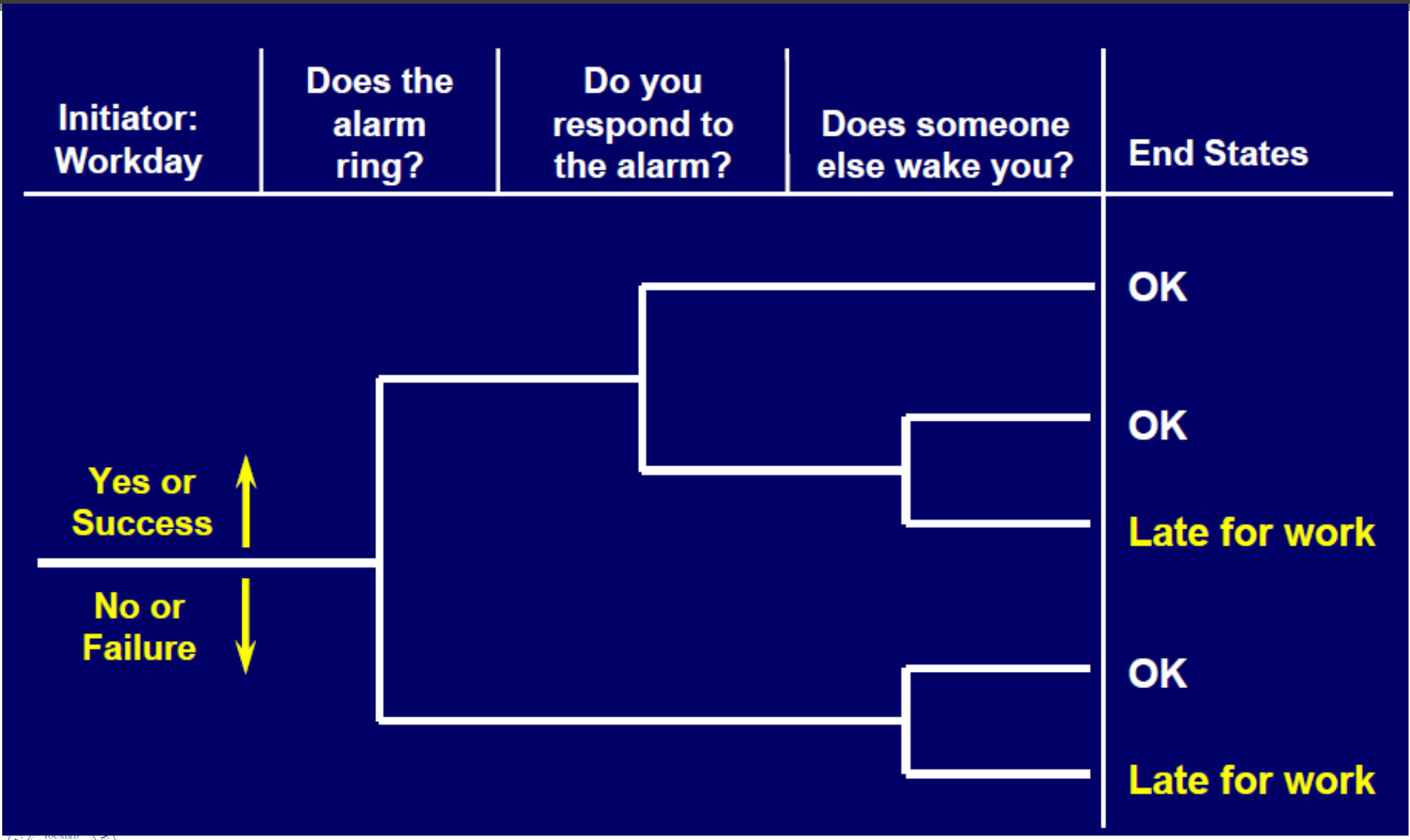
Sample = LOPA



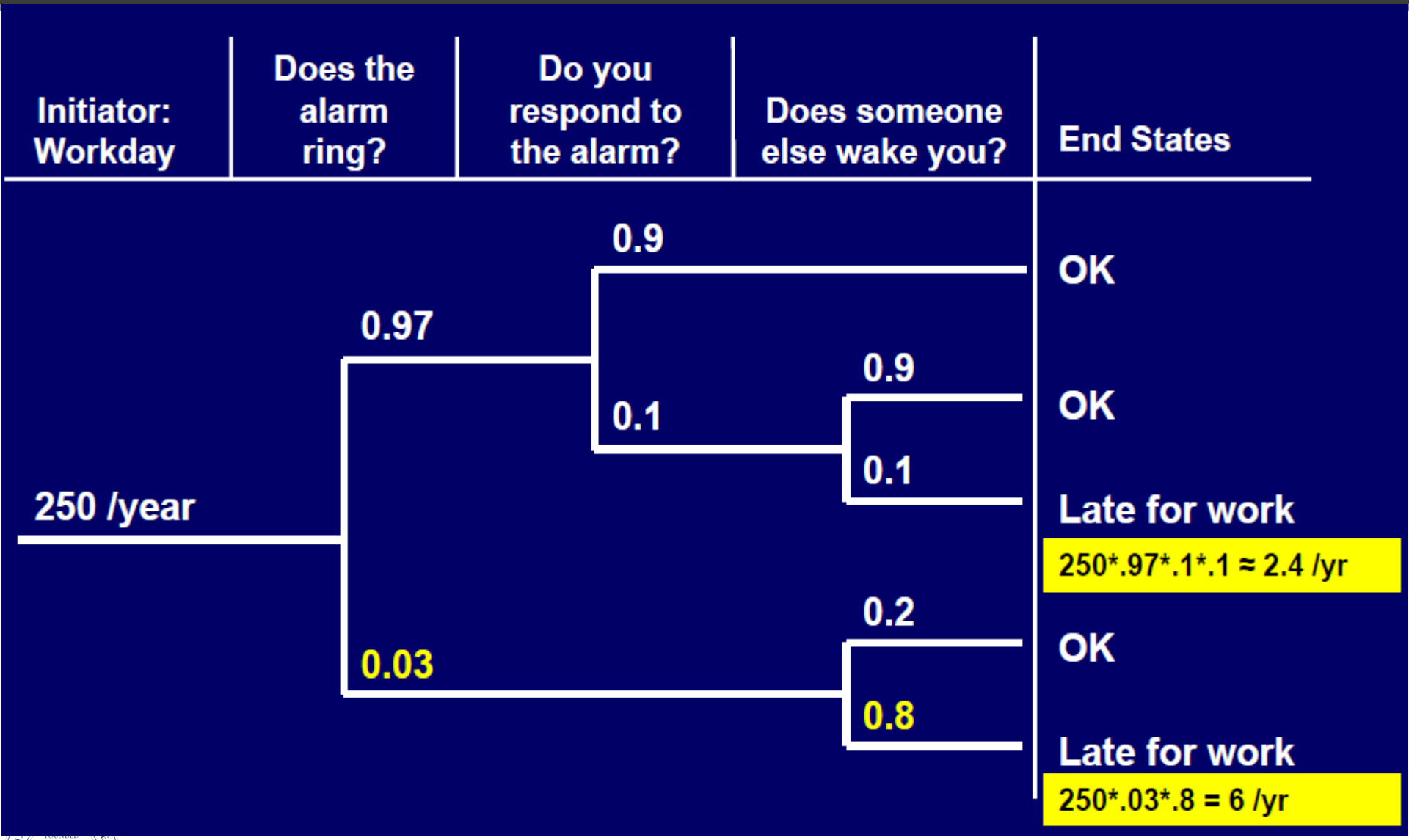
Note: Reactor pressure control by bypass type safety valve assumed successful

※OK: safety secured

Probabilistic Example



Probabilistic Example



Passive Safety Systems

- 4 levels of passivity (IAEA)
  - A. no moving working fluid
  - B. no moving mechanical part
  - C. no signal inputs of “intelligence”
  - D. no external power input or forces
- Do not yet have fully passive systems
- Increase in degree of passivity
- Many systems move to level C passivity
- Last 3-7 days depending on system

Example

You are interested in using a specific reactor coolant pump in your plant. You are friends with a plant manager that currently uses the pump, and he gives you the operational data you need to evaluate the reliability of the pump. In order to use this pump, the reliability must be 97.5% over a single refueling cycle (2 years). Given the following operational data, can this pump be used? If not, how many years must this pump have operated with only two faults in order to be used in your plant?

Operational Time = 48,355.2 hours

Repairs = 2

Repair time = 80 hours