Tutorial on Probabilistic Risk Assessment (PRA)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

What is a PRA?

- **Risk assessments include identification and analysis of…**
  - Initiating events
    - Circumstances that put a nuclear plant in an **off-normal condition**
  - Safety functions
    - Functions designed to **mitigate the initiating event**
  - Accident sequences
    - Combination of **safety function successes and failures** that describe the accident after an initiator
- **Successful response is that the plant transitions to safe, stable end-state for specified period of time**
- **We use a PRA model to look at the frequency and consequences of NOT achieving a safe, stable end-state**

What is the technical basis for the PRA model?

- **The PRA model is constructed to model the as-built, as-operated plant**
- **Multiple sources of information from the traditional engineering disciplines, including:**
  - Plant design information
  - Thermal hydraulic analyses of plant response
  - System drawings and performance criteria
  - Operating experience data
  - Emergency, abnormal, and system operating procedures
  - Maintenance practices and procedures

What is the technical basis for the PRA model?

- **Understanding the plant perturbation – "initiating event"**
  - Transient (loss of feedwater, condenser vacuum, instrument air, etc.)
  - Loss of offsite power
  - Loss of coolant accident
- **Understanding how the plant responds to the perturbation**
  - **Physical responses**
    - Neutronic
    - Thermal-hydraulic (e.g., vessel and containment pressure, temperature, water level)
  - **Automatic responses**
    - Reactor trip/turbine trip
    - Mitigating equipment actuates
  - **Operator responses** (per procedures)
    - Manual reactor trip
    - Manual switchover to sump recirculation

What is the technical basis for the PRA model?

- **This understanding is used to establish success criteria (based on engineering analyses)**
  - Definition of end states:
    - Establish the acceptance criteria for prevention of core damage, e.g., collapsed level greater than 1/3 core height
    - Establish containment capability
  - Determination of system success criteria for a given scenario:
    - Time at which system is required to prevent damage
    - Required system performance, e.g., two out of three pumps

What are the basic components of a PRA?

- **PRA models use**
  - **Event trees** to model the sequence of events from an initiating event to an end state
  - **Fault trees** to model failure of mitigating functions, including equipment dependencies to function as required
  - **Frequency** and **probability** estimates for model elements (e.g., initiating events, component failures)

- **Outputs may include**
  - **Core damage** frequency ("Level 1" PRA)
  - **Release** frequencies ("Level 2")
  - **Radiological consequences** to public ("Level 3")

What are the end states of a PRA?

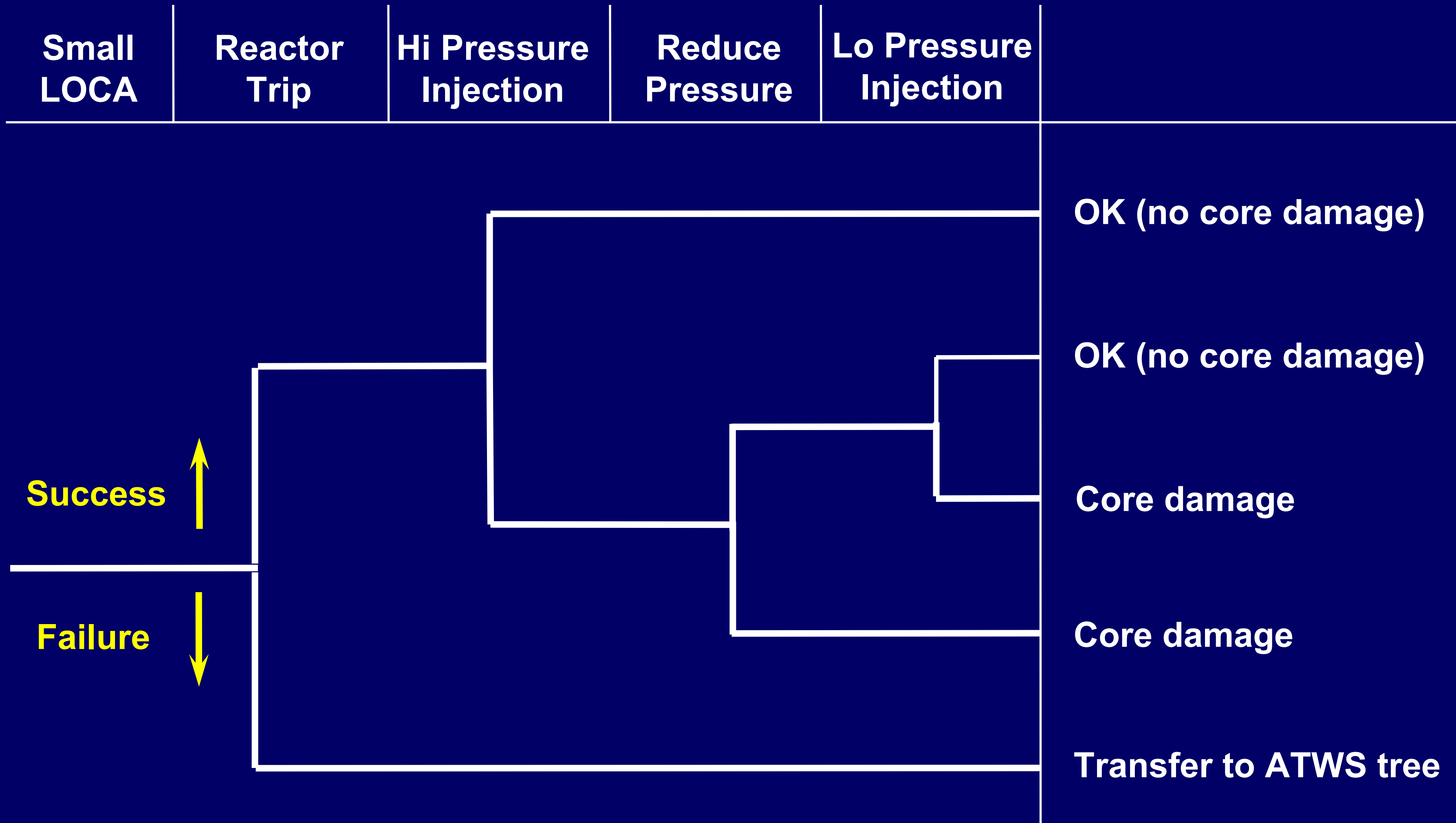
- **Core damage occurs when**
  - **Safety functions** are not met
    - Such as removal of decay heat, control of reactivity, or control of inventory
  - Engineering models show that core parameters exceed certain pre-determined limits

- **Large early release occurs when**
  - Core damage with **containment challenge**, leading to significant, **unmitigated releases prior to effective evacuation** of the close-in population

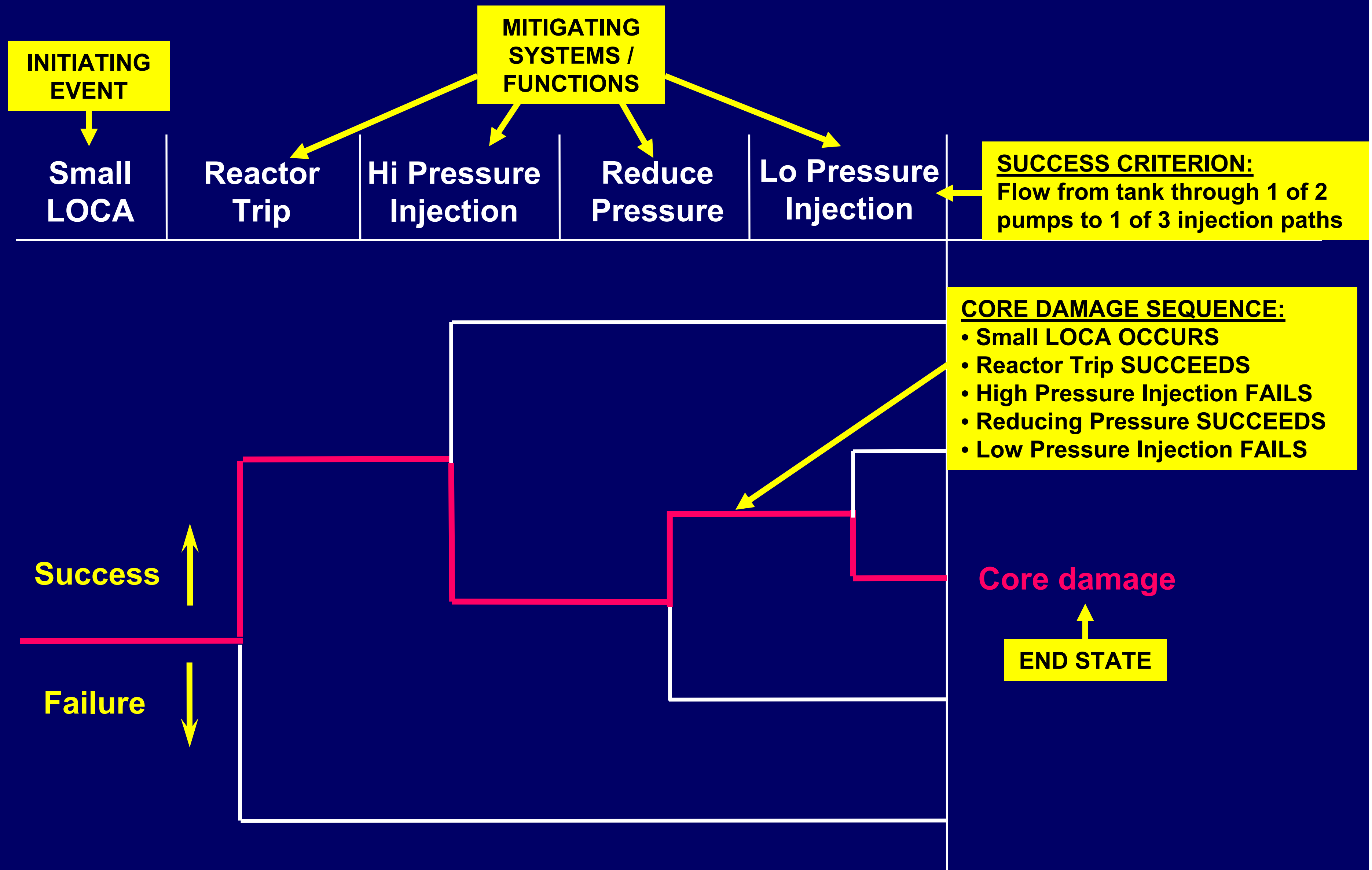
- **A limited Level 2 PRA provides insights related to core damage and large early release.**

What is an event tree?

A graphical depiction of a sequence of events



What is an event tree?



What is an event tree?

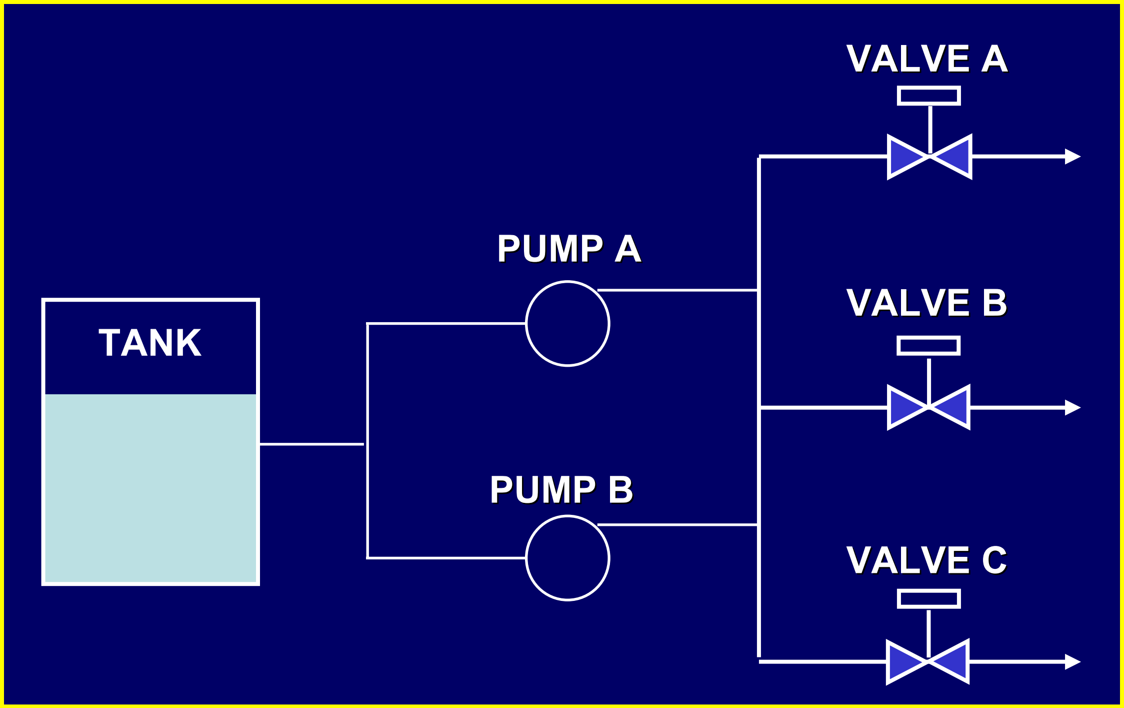
- **Event tree "top events" may represent:**
  - Functions or systems to **mitigate** core damage
  - Key **operator actions**
  - **Containment** support systems
    - Fan coolers, sprays
    - Isolation
- **Event tree also used for Level 2**
  - Use tree to model **core melt and severe accident phenomenology** that challenges containment integrity
  - **LERF is a subset of Level 2** – specific tree end states

What is a fault tree?

<u>A graphical depiction of how a system can fail</u>

<u>SUCCESS CRITERION:</u>
Flow from tank through 1 of 2 pumps to 1 of 3 injection paths

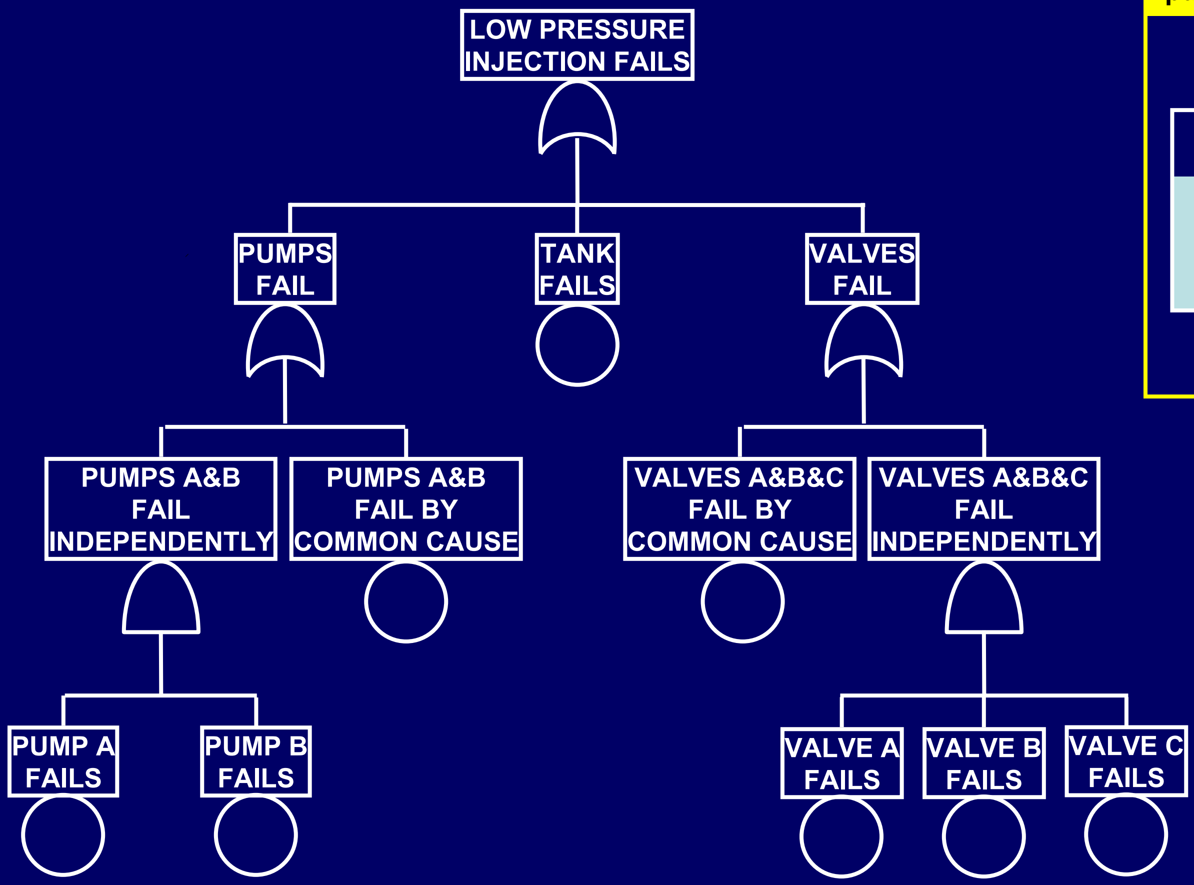
<u>FAILURE OCCURS WHEN:</u>
No flow from tank
OR
No flow from pumps
OR
No flow through injection paths

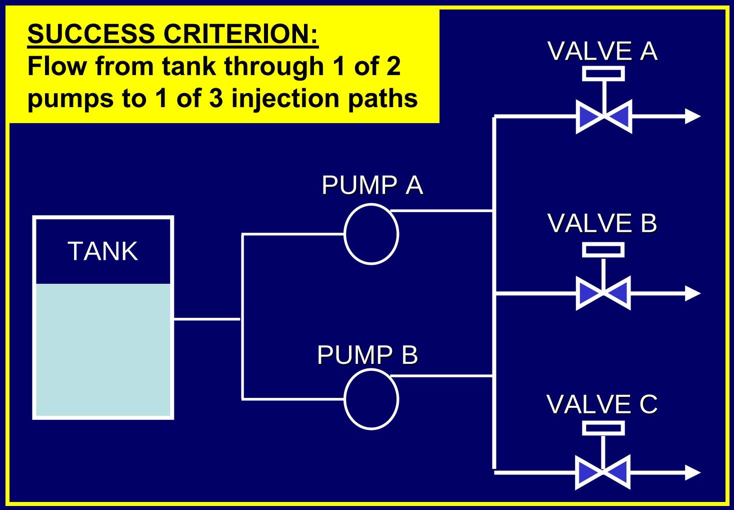


What is a fault tree?

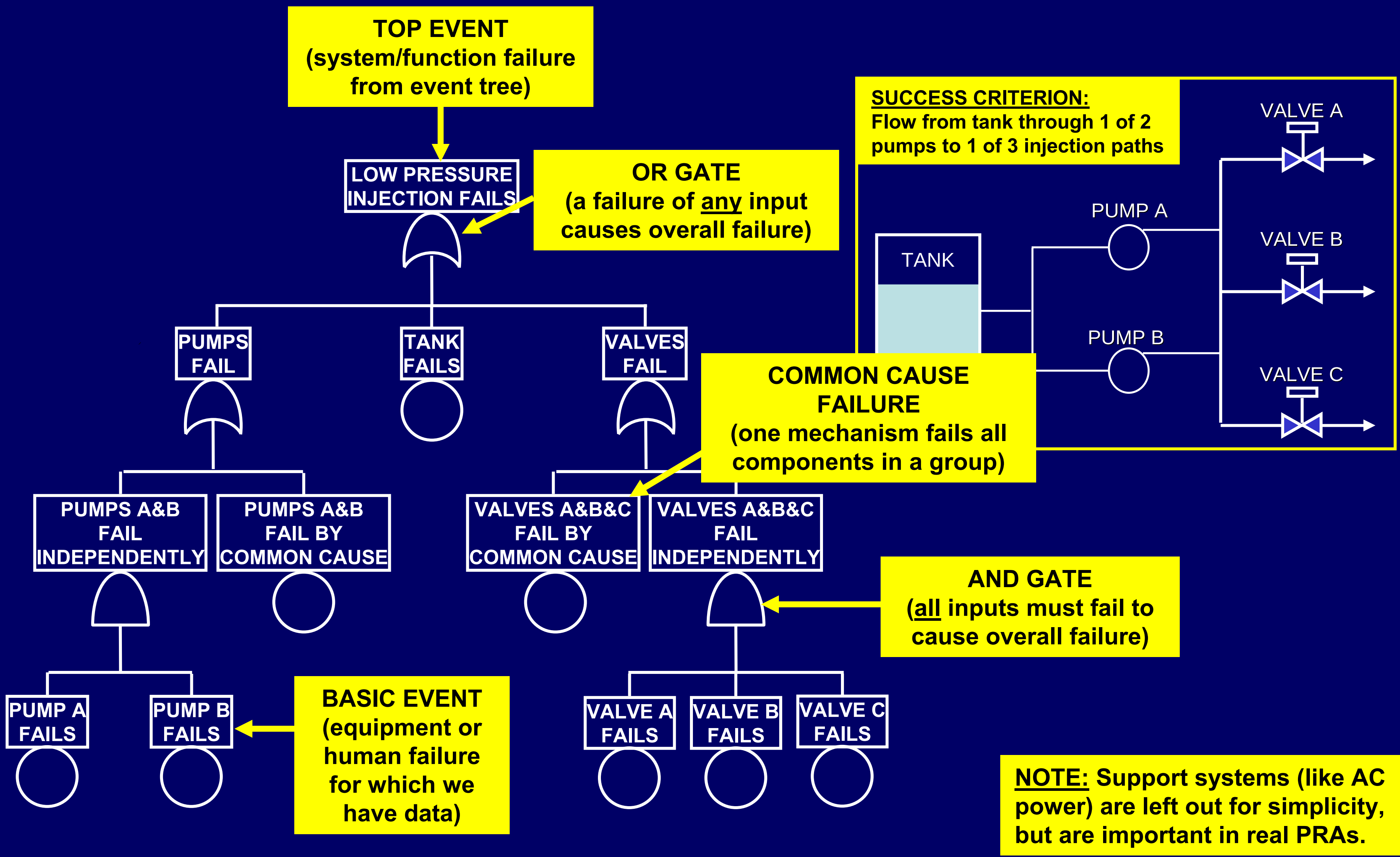
- **Developing fault trees**
  - Need for fault tree usually arises from the event tree
    - What equipment can provide the function?
    - What operator actions must take place?
  - Define **success criteria**, e.g.
    - How much flow is needed to remove decay heat?
    - How much flow is necessary to restore inventory?
    - How many valves must close to isolate containment?
  - Determine the **failure modes** to include in the tree
  - Determine supporting systems; e.g., electric power, room cooling, seal and cooling water, control power, etc.
  - Continue modeling to **basic event level**

What is a fault tree?



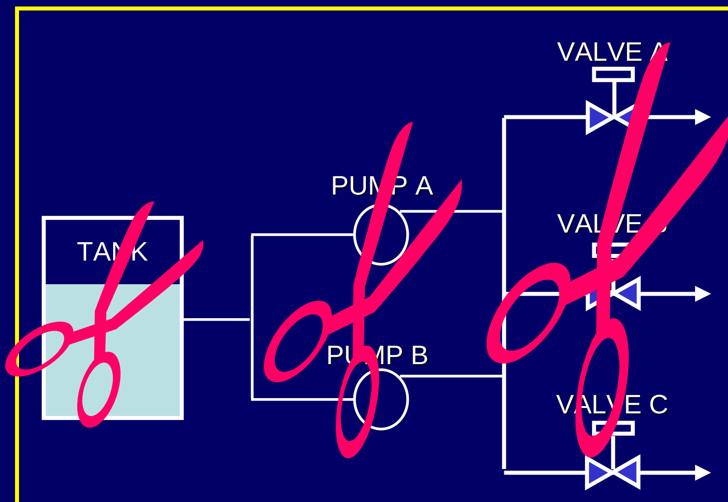


What is a fault tree?



How do we solve fault trees?

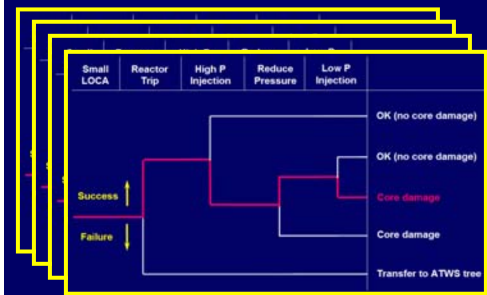
- **Reducing the logic in a fault tree gives:**
  - **Cutsets**, sets of failures that result in overall failure
    - ➢ PUMP A FAILS and PUMP B FAILS
      - Independently or by common cause
    - ➢ VALVE A FAILS and VALVE B FAILS and VALVE C FAILS
      - Independently or by common cause
    - ➢ TANK FAILS
  - **Probability that the function will fail**, derived from the cutsets and the failure probabilities of the basic events therein



Where do we get the numbers?

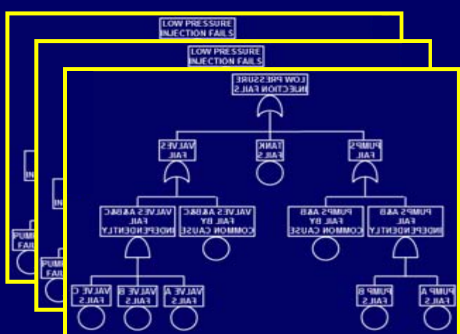
- **Operating experience data for:**
  - Frequency of many initiating events
  - Failure rates of plant equipment
  - Average availability of plant equipment
  - Probabilities of repair and recovery (e.g., restoration of offsite power)
- **Special methods:**
  - **Expert elicitation** for rare events (e.g., large LOCA frequency)
  - **Human reliability analysis** (e.g., operator fails to switch to recirculation)
  - **Common cause failure** modeling

How do we "solve" the PRA model?



CORE DAMAGE SEQUENCES:

- Small LOCA OCCURS &
  Reactor Trip SUCCEEDS &
  High Pressure Injection FAILS &
  Reducing Pressure SUCCEEDS &
  Low Pressure Injection FAILS
- … (may be several on each tree!)

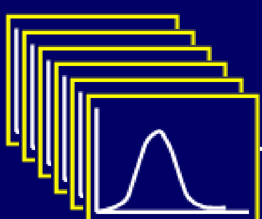


SYSTEM CUTSETS:

- PUMP A FAILS & PUMP B FAILS
- TANK FAILS
- … (may be several for each tree!)

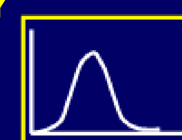
CORE DAMAGE CUTSETS:

- SMALL LOCA &
  HPI TANK FAILS &
  LPI PUMP A FAILS & LPI PUMP B FAILS
- SMALL LOCA &
  HPI PUMP A FAILS & HPI PUMP B FAILS &
  LPI TANK FAILS
- … (many combinations per sequence!)



FAILURE PROBABILITIES &
INITIATING EVENT FREQUENCIES

- CORE DAMAGE FREQUENCY
- UNCERTAINTY ANALYSIS
- IMPORTANCE MEASURES
- SENSITIVITY STUDIES
- RISK INSIGHTS

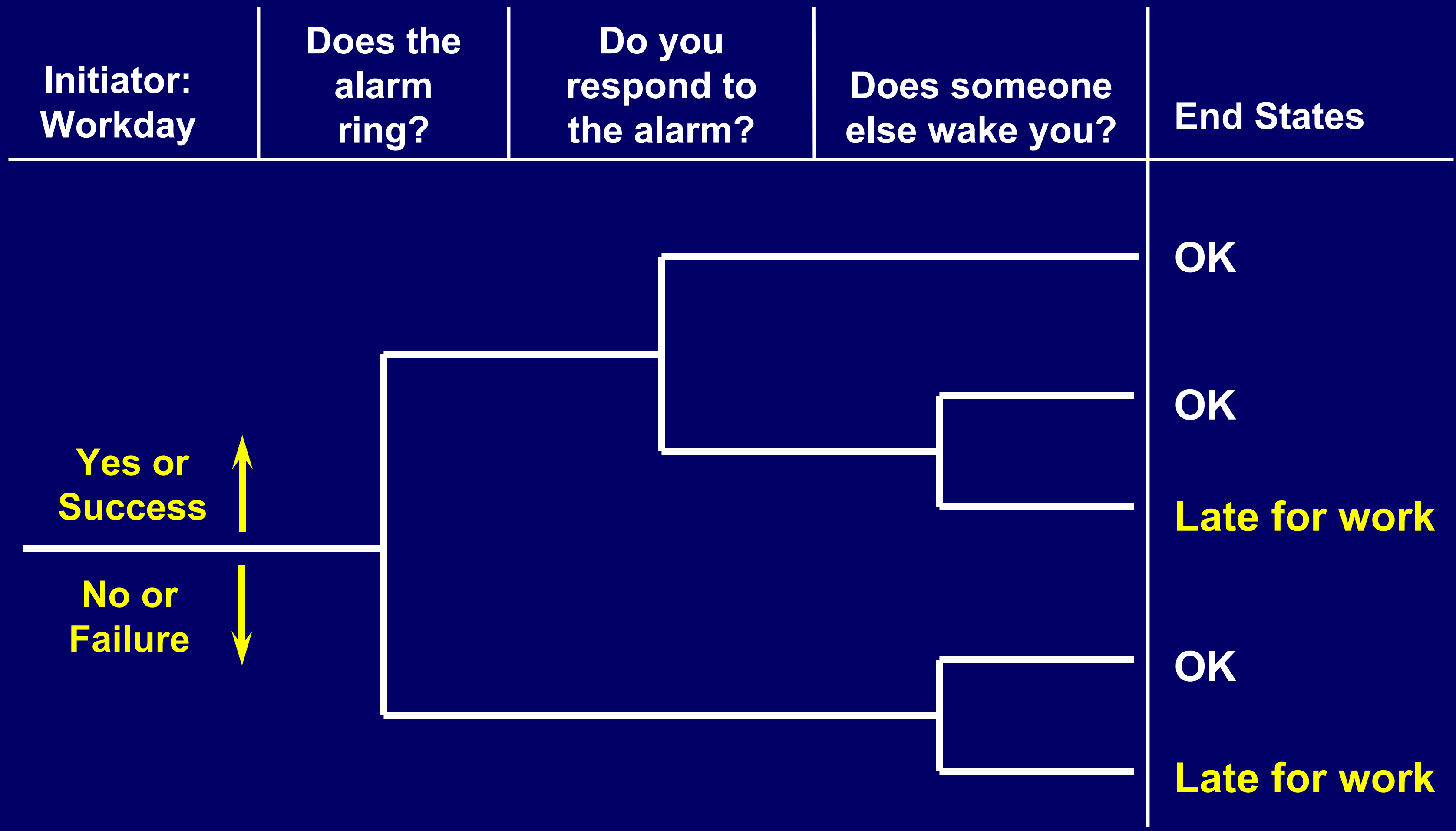


Example: Estimating the Frequency of Oversleeping

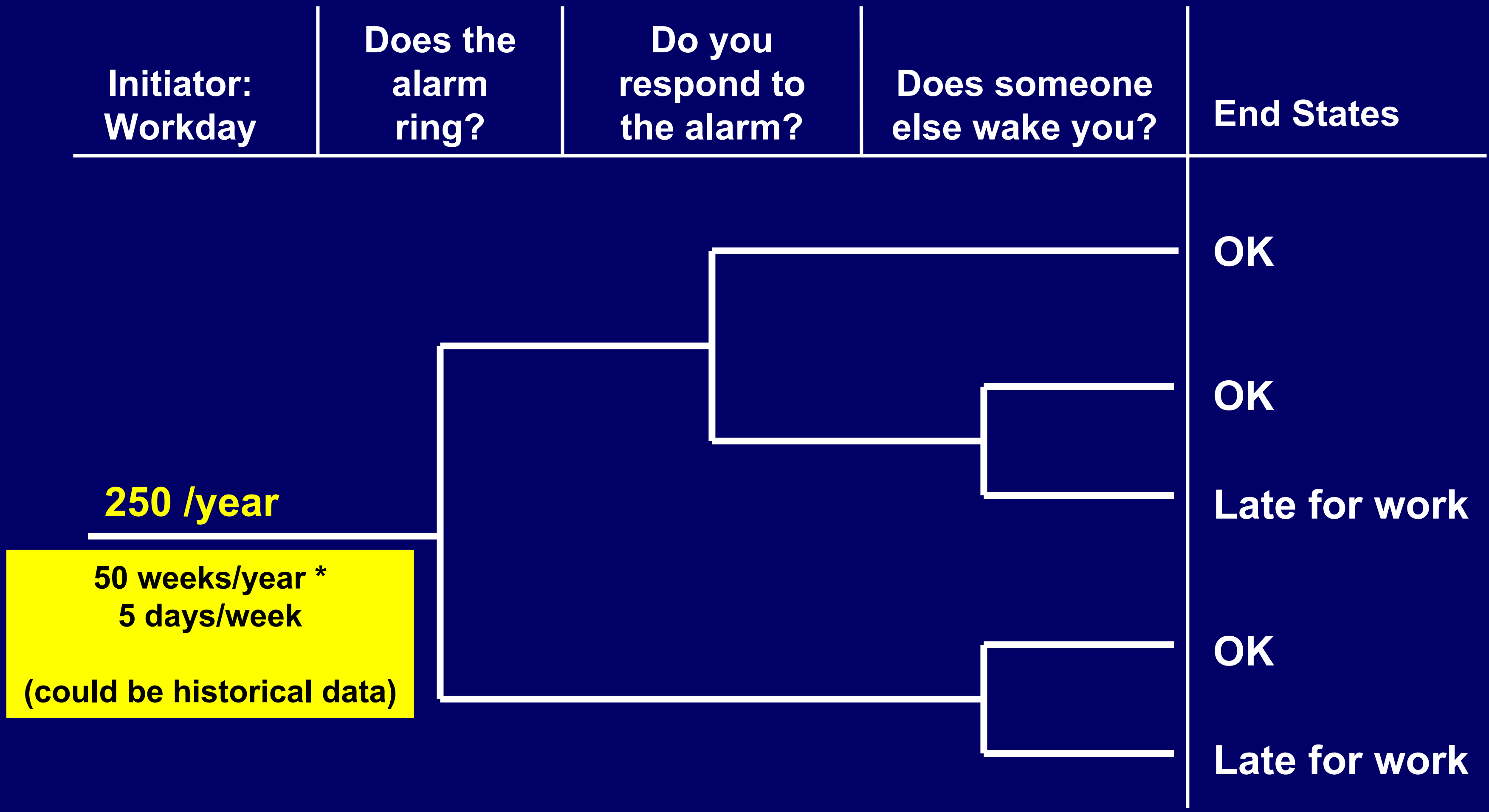
The Scenario

- **You wish to estimate the frequency of being late for work due to oversleeping**
- **After thinking about the problem a bit, you construct a simple event tree model**
  - Initiating event is the fact that it's a work day
  - Mitigating "systems" are an alarm clock and a backup person
- **You "solve" the model to arrive at an estimated "career damage frequency"**
  - Develop initiating event frequency
  - Determine branch probabilities (may need fault trees)
- **You re-analyze the problem to see the impact of adding a redundant alarm clock**

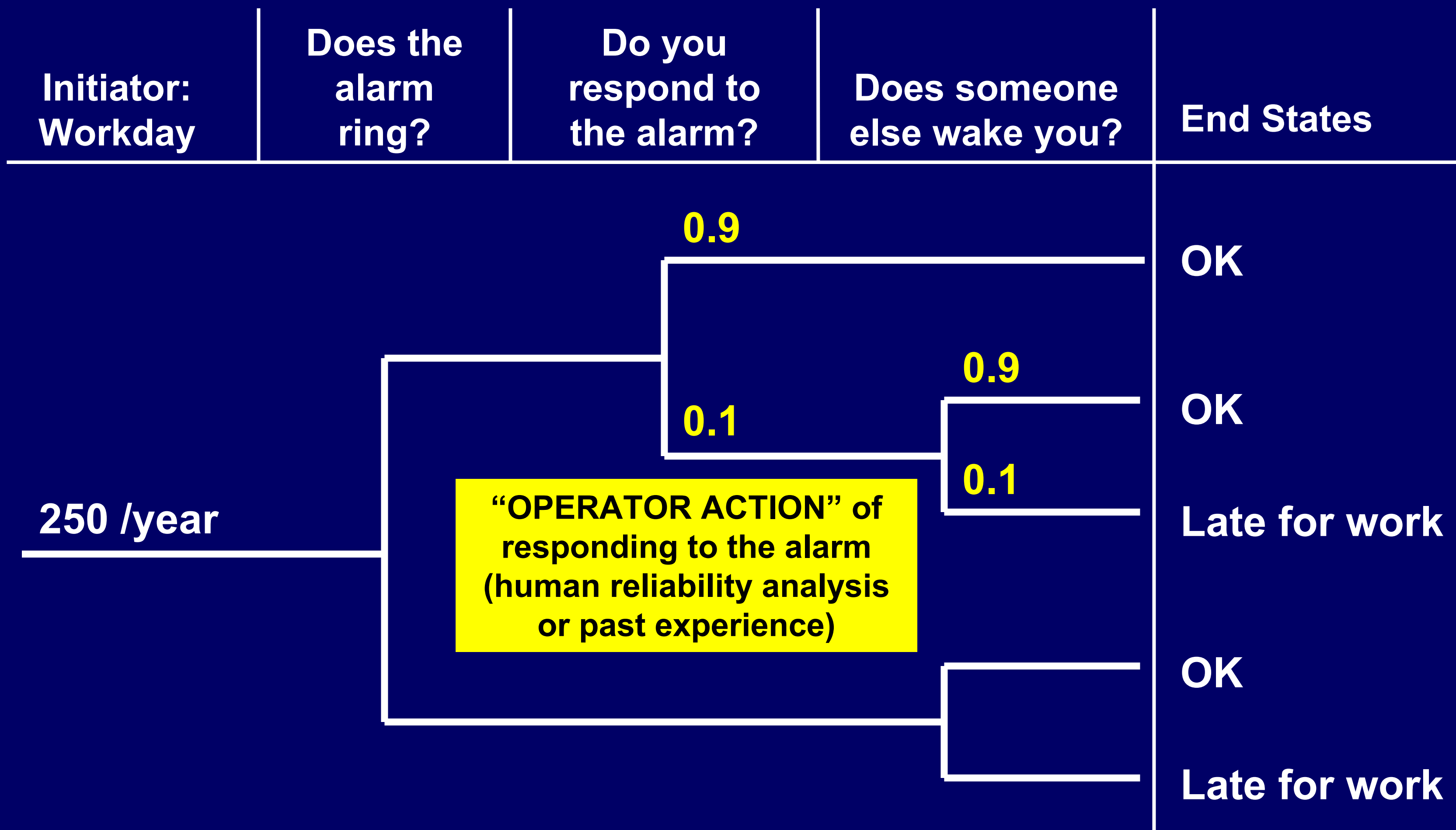
Sample Event Tree for Oversleeping



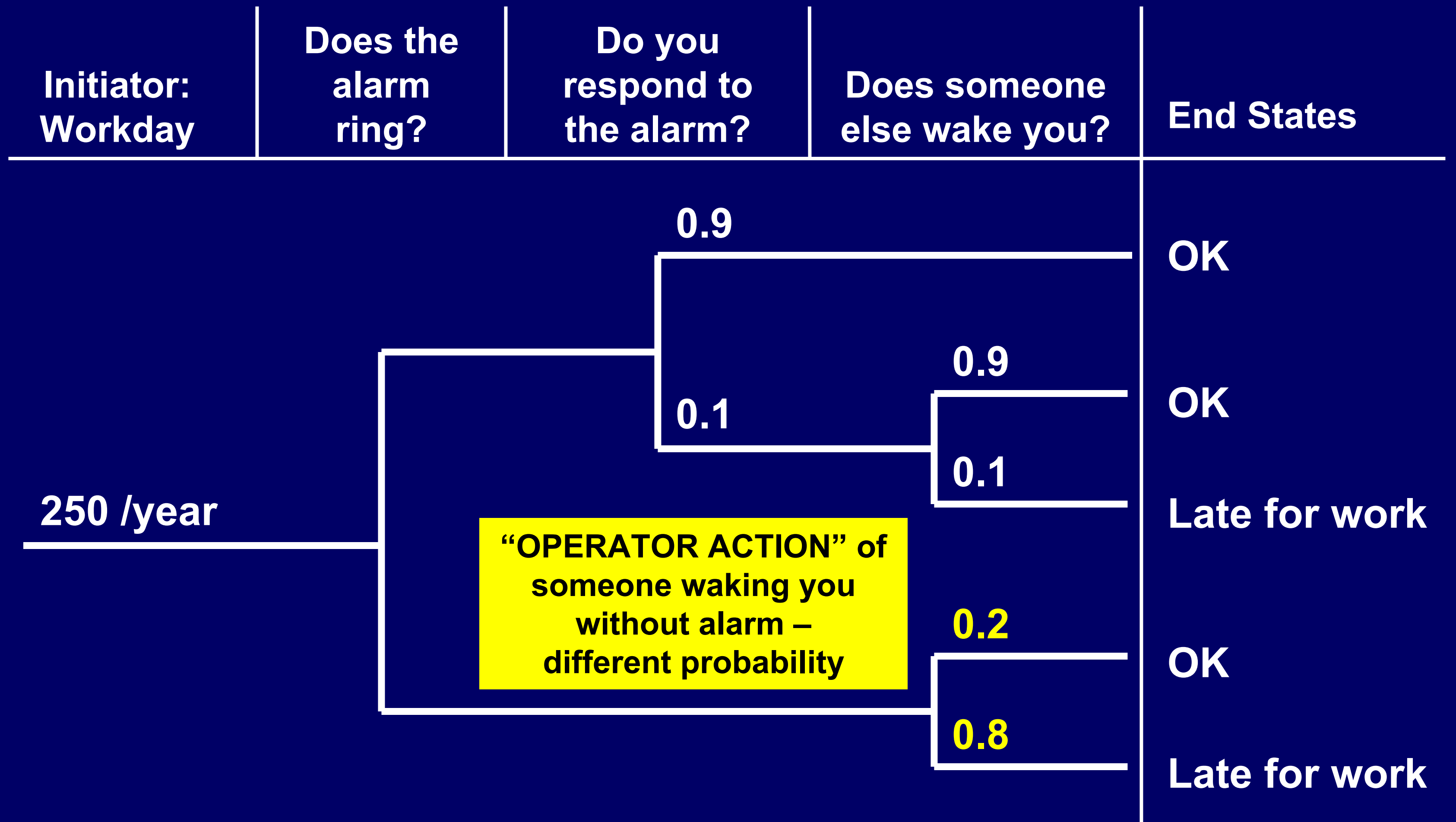
Estimating the Frequency of Oversleeping



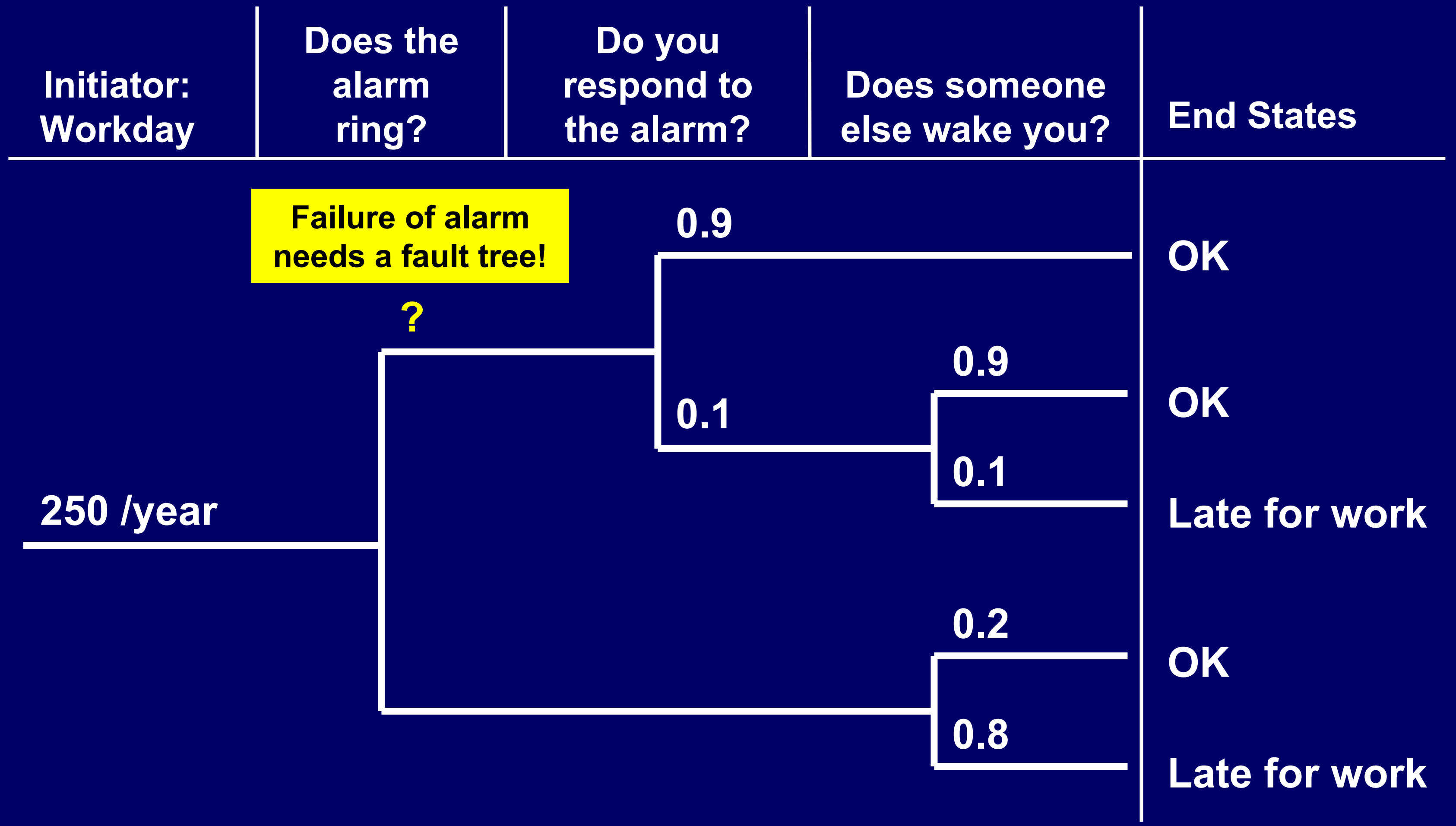
Estimating the Frequency of Oversleeping



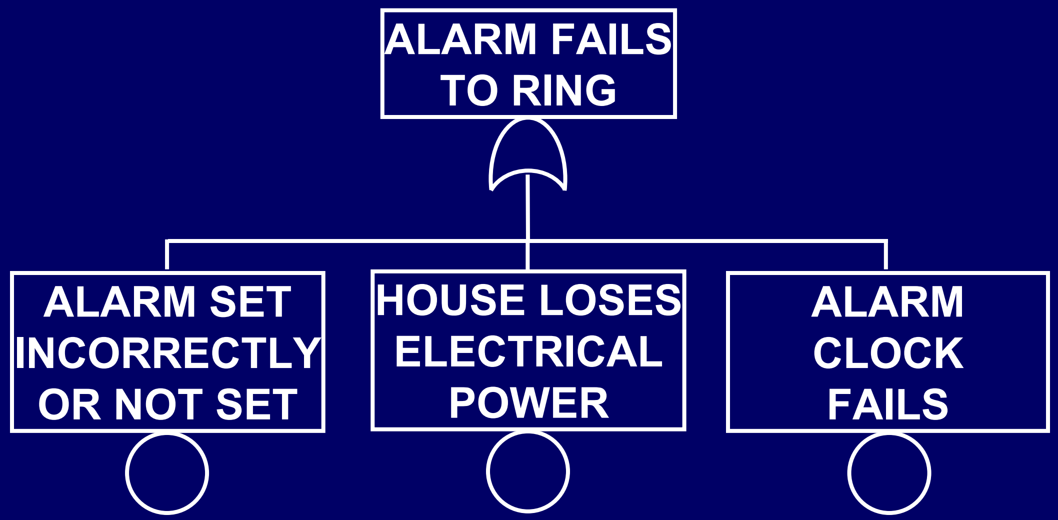
Estimating the Frequency of Oversleeping



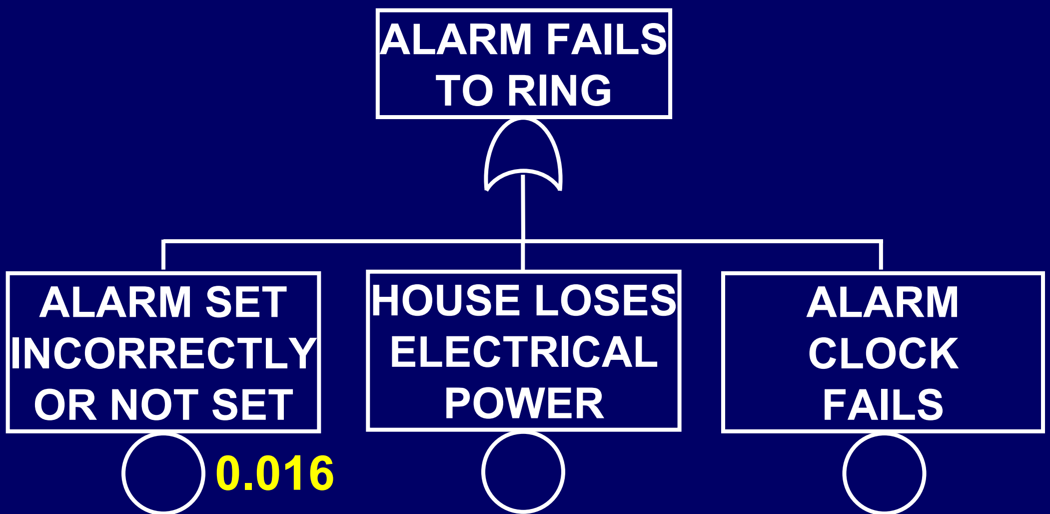
Estimating the Frequency of Oversleeping



Sample Fault Tree for Alarm Failing to Ring

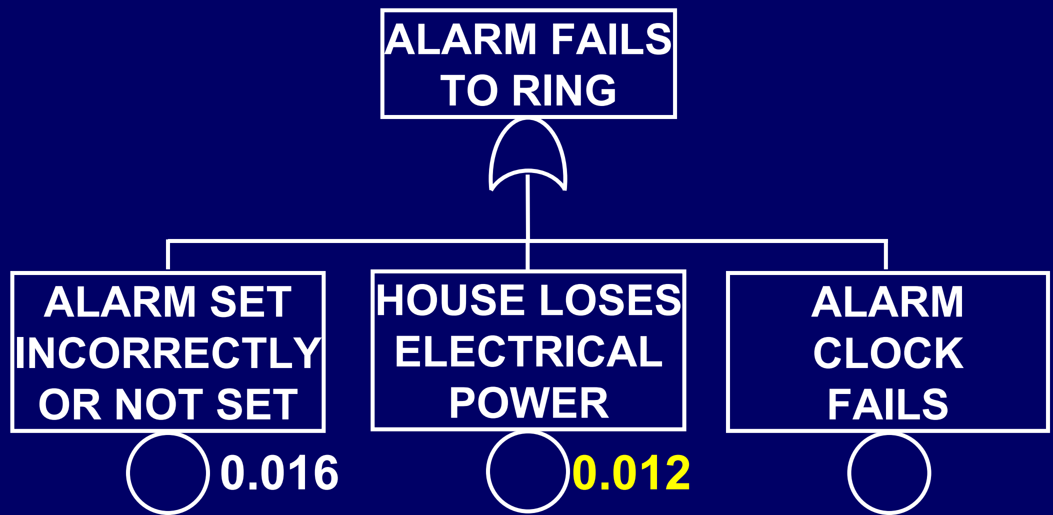


Estimating the Probability of Alarm Failing to Ring



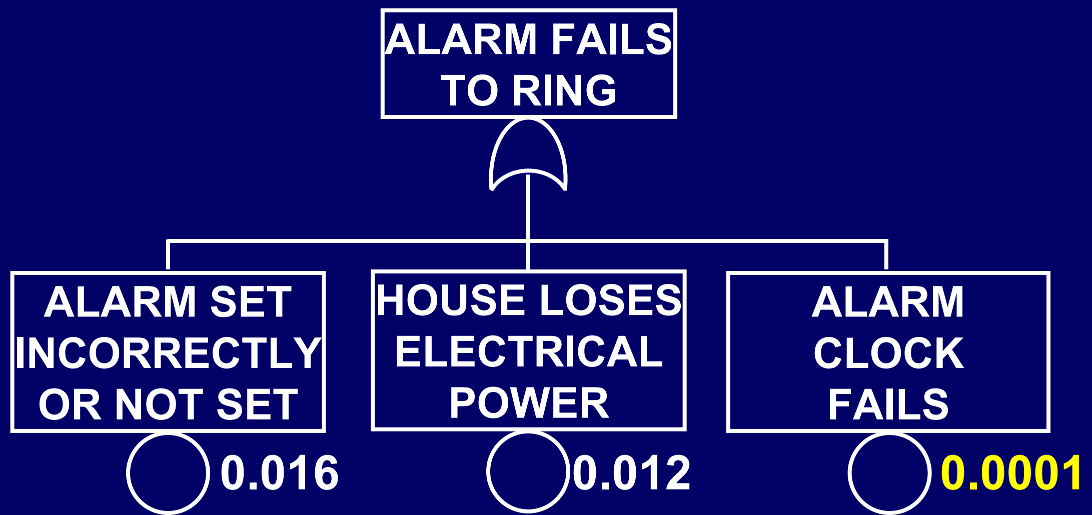
Your experience data:
4 times each work year
4/250 = 0.016

Estimating the Probability of Alarm Failing to Ring



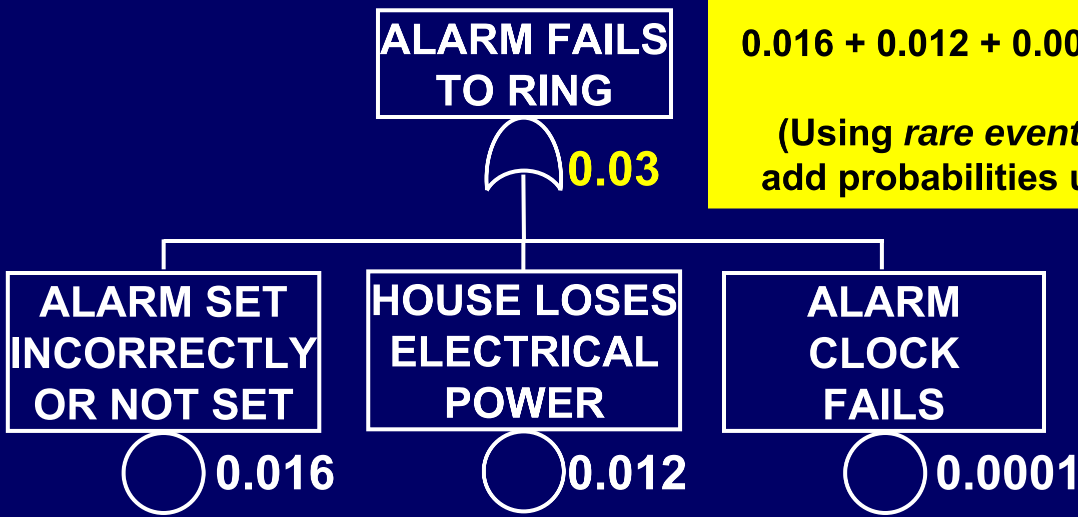
Your experience data:
3 work days per year
3/250 = 0.012

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

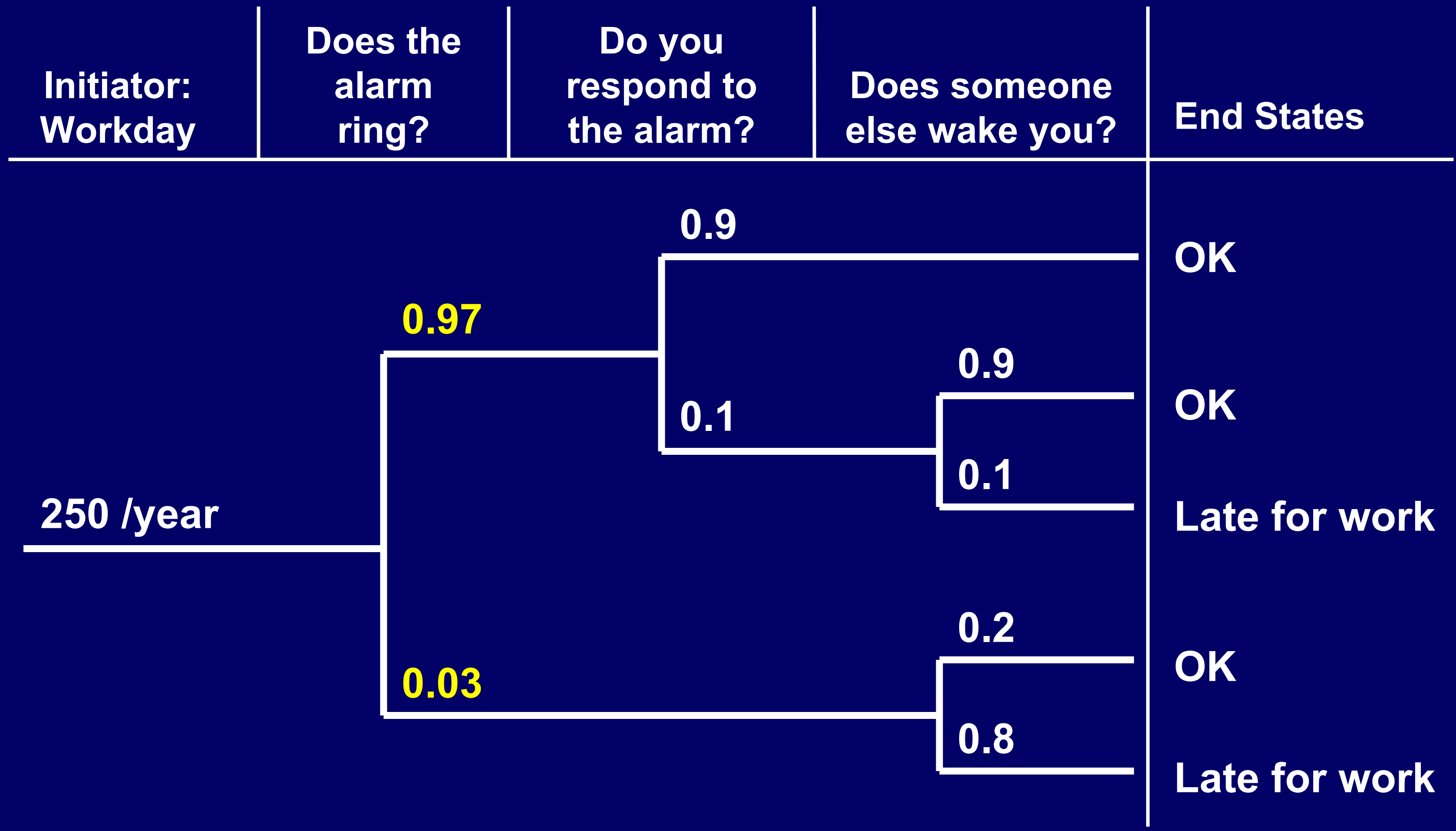


Overall failure probability:

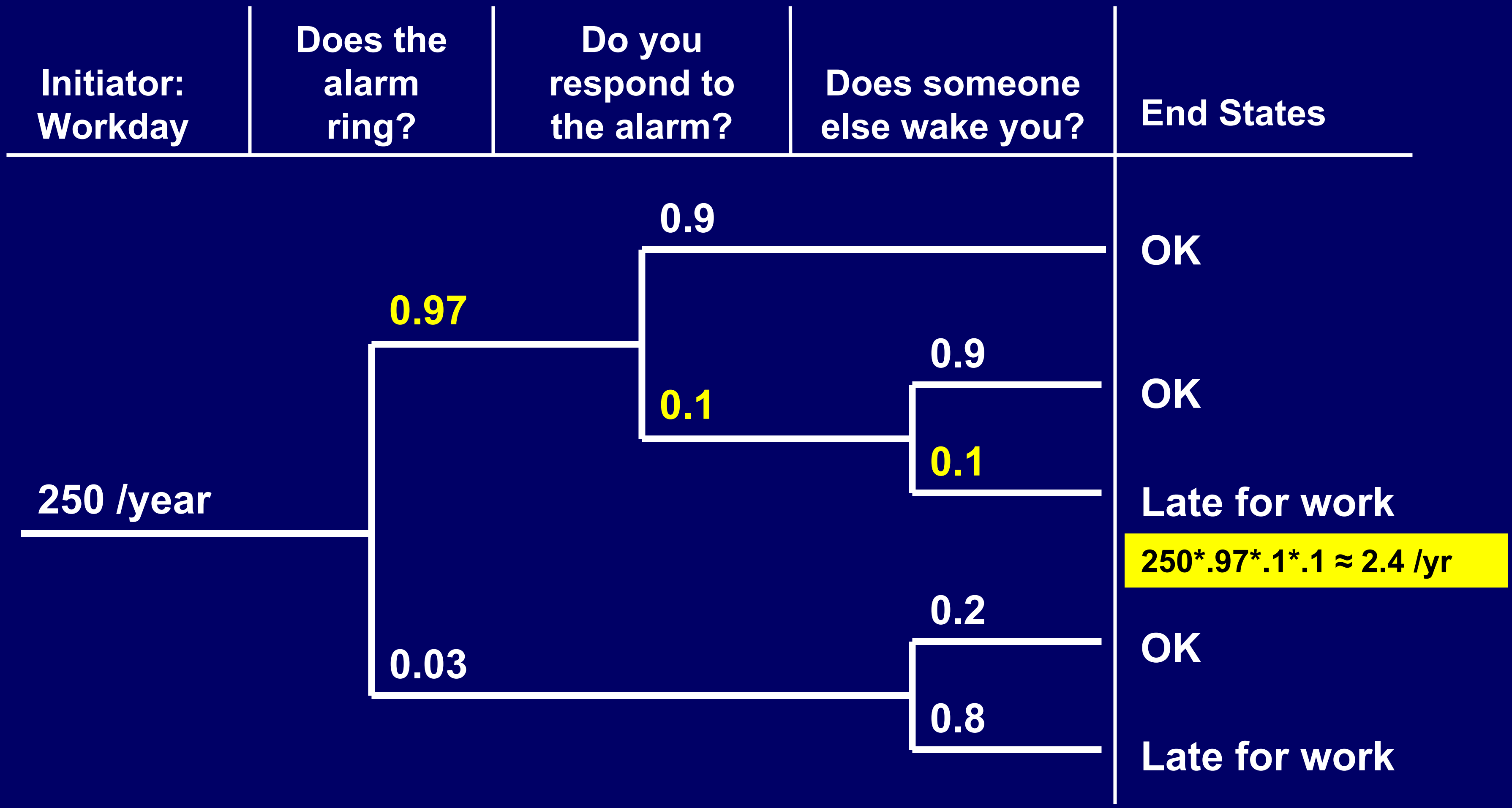
0.016 + 0.012 + 0.0001 = 0.0281 ≈ 0.03

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

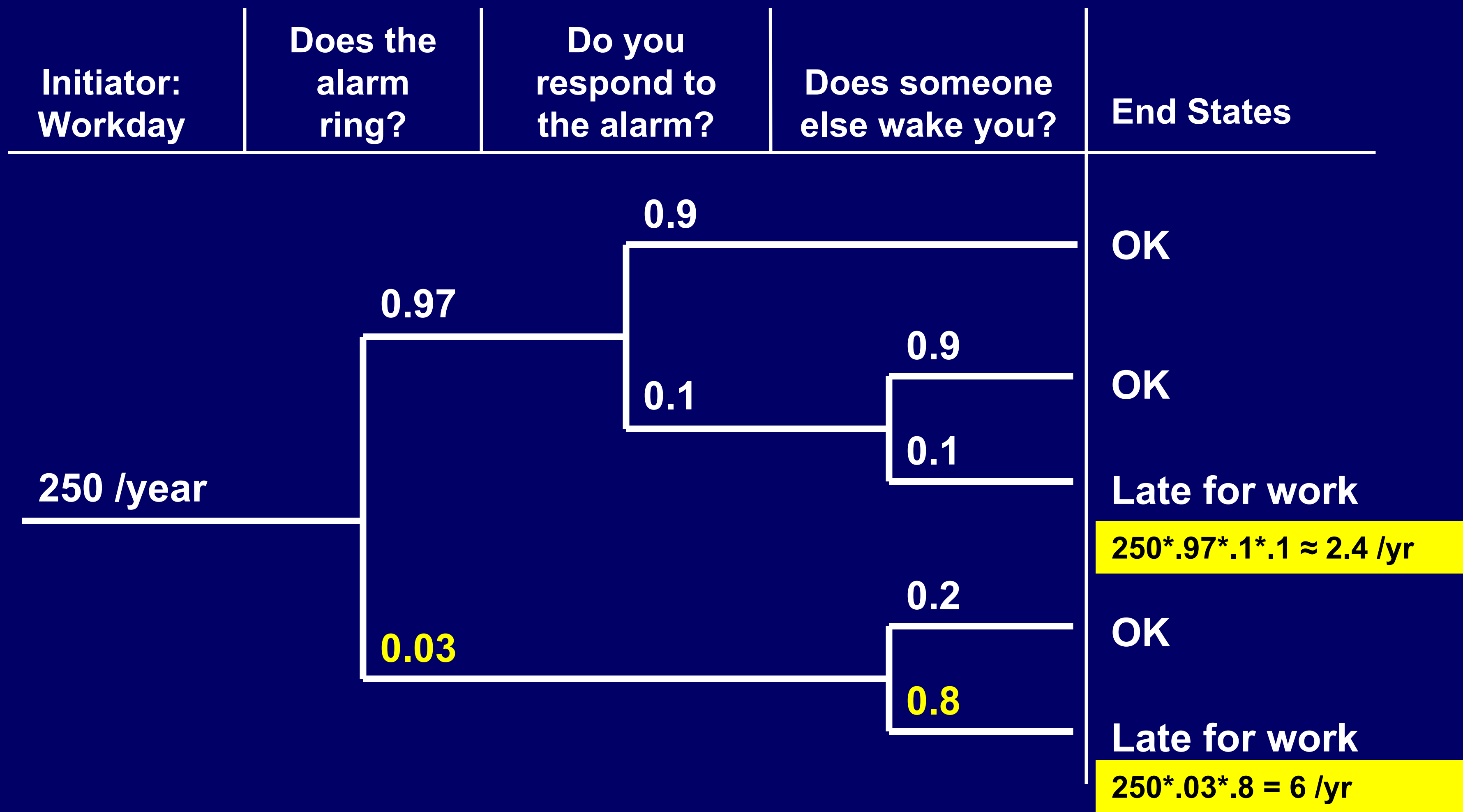
Estimating the Frequency of Oversleeping



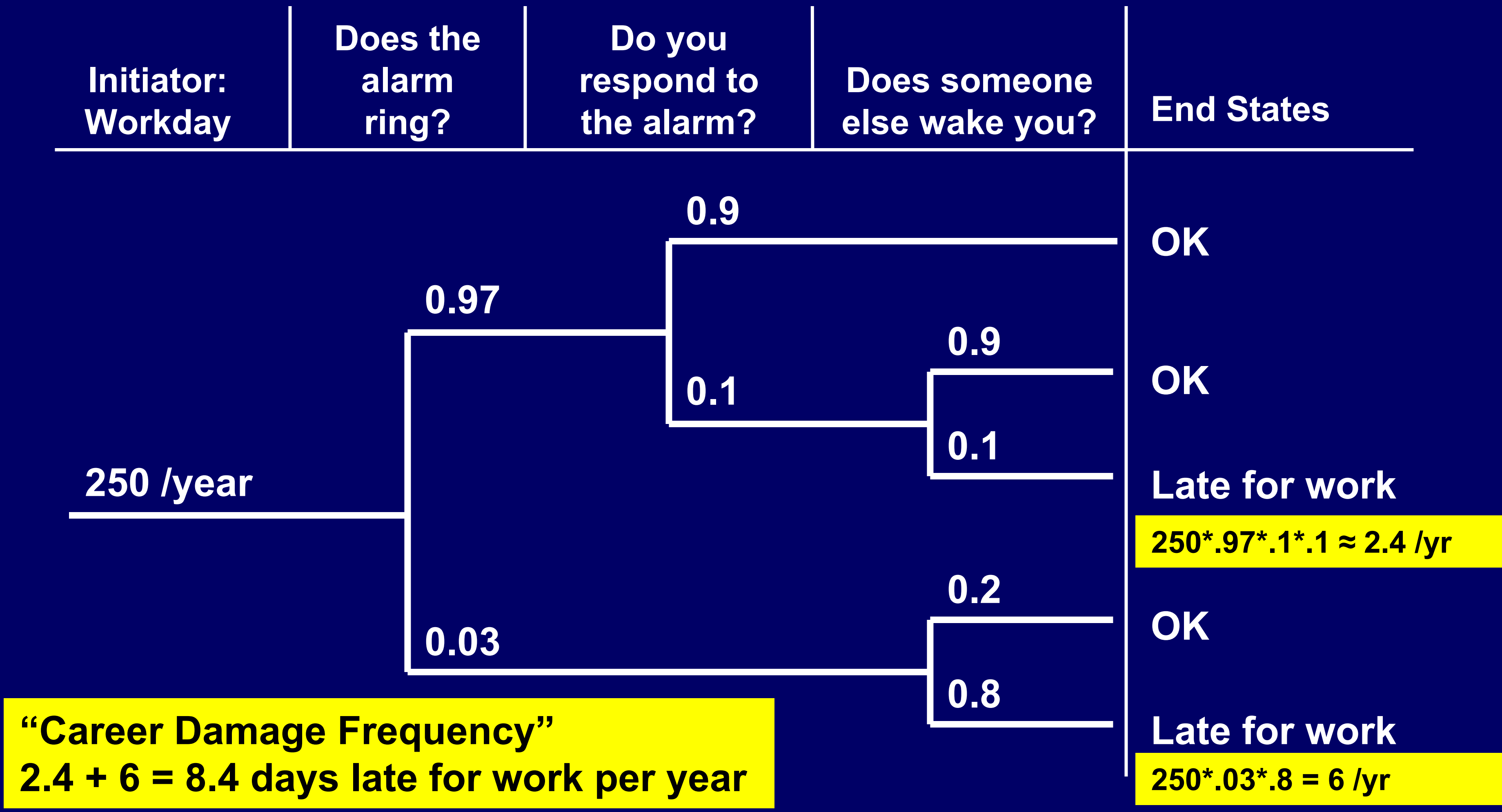
Estimating the Frequency of Oversleeping



Estimating the Frequency of Oversleeping



Estimating the Frequency of Oversleeping

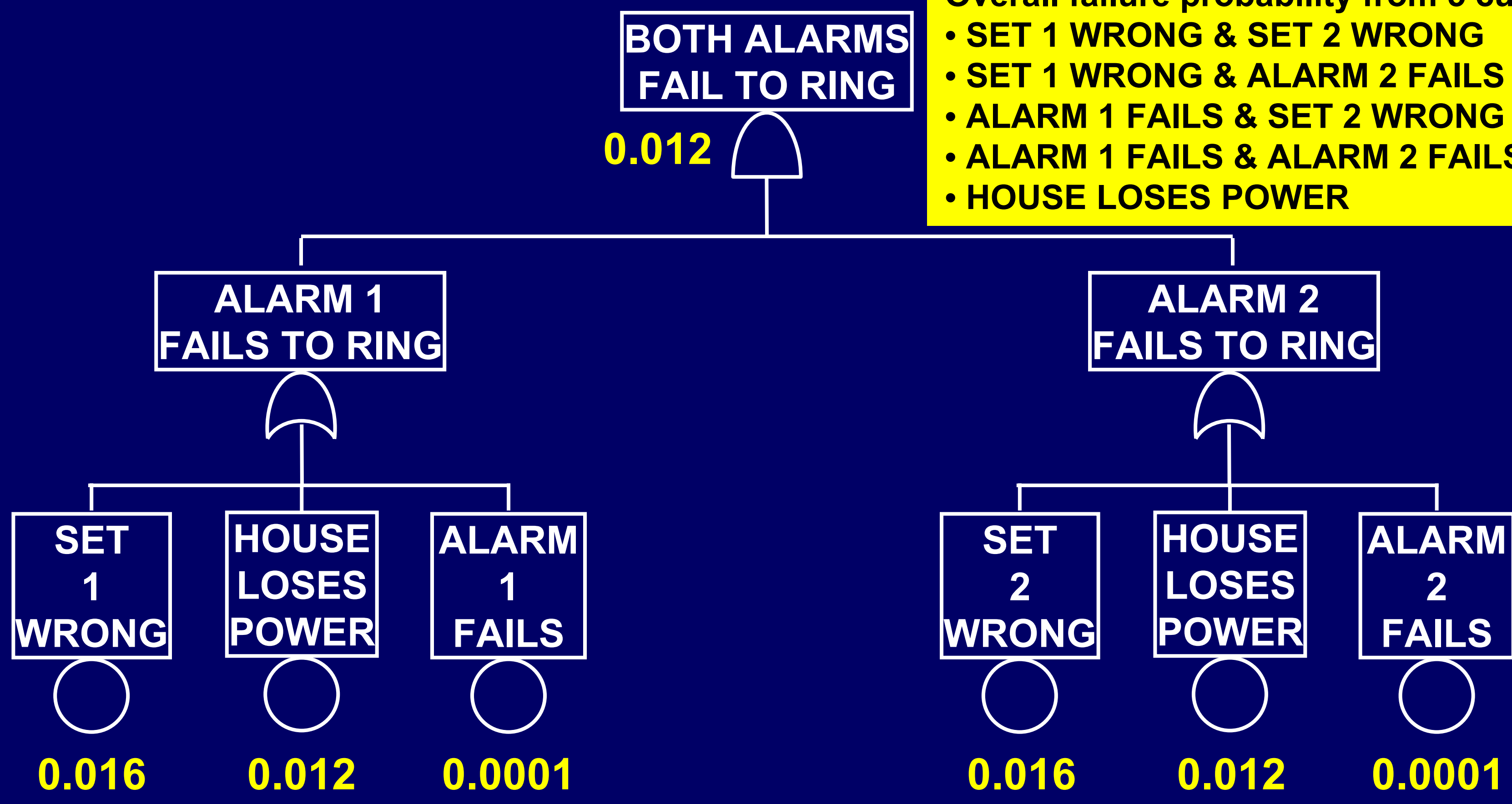


What if we improve the design?

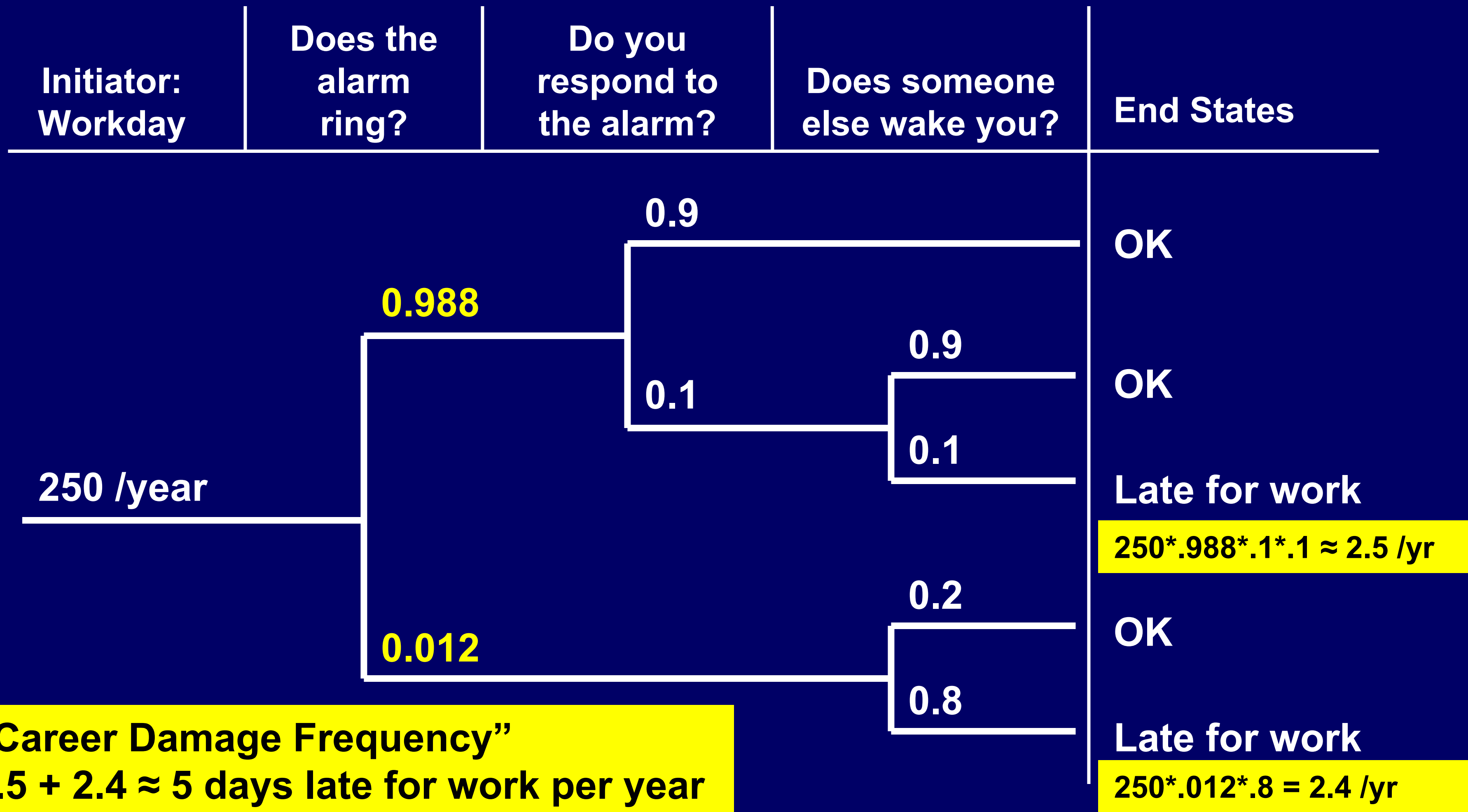
- **What happens if you set two alarms because you have a very important job interview?**
  - Theoretically improves the situation
    - **Both have to fail** for the "alarm fails to ring" event to be satisfied
  - Introduces other complexities
    - If both alarms depend on your home's electrical power, a **power outage makes the redundancy irrelevant**
    - If you set one wrong or forget to set it, the **likelihood of setting the other wrong is affected** (dependency)

Estimating the Probability of 2 Alarms Failing to Ring

Overall failure probability from 5 cutsets:
- SET 1 WRONG & SET 2 WRONG
- SET 1 WRONG & ALARM 2 FAILS
- ALARM 1 FAILS & SET 2 WRONG
- ALARM 1 FAILS & ALARM 2 FAILS
- HOUSE LOSES POWER



Estimating the Frequency of Oversleeping (2 Alarms)



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

Career Damage Frequency Results

- **One alarm clock – ~8** late **days per year**
  - 2.4 days when the alarm rings, you fail to properly respond, and nobody else hears the alarm and wakes you
  - 6 days when the alarm fails, and nobody else wakes you
- **Two alarm clocks – ~5 late days per year**
  - No noticeable change for 1st scenario
    - Alarm reliability almost 1.0 in either case
  - Major impact is on 2nd scenario
    - Failure of two alarms is less likely, but overall alarm failure is dominated by house power – extra plug-in alarms won't help!
- **Results can help you minimize risk of being late**
  - Shows "**where the risk is coming from**" – which sequences
  - May need more than one improvement to reduce overall CDF to an acceptable level

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!**