Risk-Informed Regulation for Technical Staff *(P-101)*

Gareth Parry & Steve Laur – NRR/DRA
Don Dube – NRO/DSRA

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

Course Objectives

- **At the end of this course, you will be able to:**
  - Define **basic terms** related to risk-informed regulation
  - Identify **how your work fits into** a risk-informed regulatory structure
  - Understand the **basic modeling concepts** in a probabilistic risk assessment
  - Discuss the **benefits** of using risk information
  - **Support and communicate** risk-informed decisions
  - Find **references** for more information in the future

Course Modules

1. **Introduction to Risk-Informed Regulation**
   - What do risk and risk-informed regulation mean?
   - Where do we use risk-informed approaches?
   - How do you fit in to risk-informed regulation?

2. **Use of PRA Models**
   - How do we build PRA models?
   - How do we use PRA in risk-informed regulation?
   - How do we know a licensee’s PRA is adequate?
   - What can we learn from PRA results?

3. **Supporting Risk-Informed Decisions**
   - What guidance do we use?
   - What are some examples?
   - How can risk communication help?

4. **Resources**
   - Where can you get more information?

1. Introduction to Risk-Informed Regulation

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Module 1: Intro to Risk-Informed Regulation

- What do risk and risk-informed regulation mean?
- Where do we use risk-informed approaches?
- How do you fit in to risk-informed regulation?

What do risk and risk-informed regulation mean?

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

What is risk?

- **In everyday usage, "risk" is often used synonymously with the probability of a loss.**
- **In the context of evaluating risk from a nuclear power plant, risk is commonly expressed as the “risk triplet”:**
    1. What can go wrong (accident scenario)?
    2. How likely is it (frequency on a reactor year basis)?
    3. What are the consequences (impact on the plant or on people)?

How do we characterize risk?

- **We characterize risk in terms of its effect on people**

- **What is the likelihood of a nuclear accident:**
  - – Causing near-term death? (prompt fatality)
  - – Causing death from cancer? (latent fatality)

How do we characterize risk?

- **Commission’s SAFETY GOALS* determine how safe is safe enough**
  - Qualitative safety goals
  - Quantitative health objectives
  - Subsidiary objectives

**** Policy statement, 8/21/86 (51 FR 30028)***

How do we characterize risk?

- **Qualitative safety goals**
  - Individual members of the public bear **no significant additional risk to life and health** as a result of nuclear power
  - Societal risk should be **comparable to or less than** risks of other energy generation technologies

How do we characterize risk?

- **Quantitative health objectives**
  - For an average individual living near a plant:
    - ➢ The risk of **accidental death** as a result of a nuclear accident should be **less than one-tenth of a percent (1/1000)** of the total accidental death risk to which the U.S. population is exposed
  - For the population in the area of the plant:
    - ➢ The risk of **death from cancer** as a result of plant operations should be **less than one-tenth of a percent (1/1000)** of the total cancer fatality risk from all other causes

How do we characterize risk?

- **Subsidiary objectives (operating reactors)**
  - Core damage frequency (CDF) no more than about **once every 10,000 years (1E-4/year)** per plant
    - ➢Surrogate for latent cancer fatalities
  - Large early release frequency (LERF) no more than about **once every 100,000 years (1E-5/year)** per plant
    - ➢Surrogate for prompt fatalities

How do we characterize risk?

- **Metrics for new reactors**
  - Core damage frequency (CDF) no more than about **once every 10,000 years (1E-4/year)** per plant
  - Large release frequency (LRF) no more than about **once every 1,000,000 years (1E-6/year)**
  - Conditional containment failure probability (CCFP) less than approximately **0.1**

**** SRM on SECY-90-016, 6/26/90***

What tools are available to evaluate risk?

- **Probabilistic Risk Assessment (PRA) Methods**
  - PRA is a structured, analytical process for identifying potential weaknesses and strengths of a plant design in an **integrated** fashion
  - **One way** of analyzing risk in the nuclear industry
  - PRA provides a framework for explicitly addressing and presenting uncertainties (vs. making conservative assumptions to deal with uncertainty)

- **Alternate methods include:**
  - Qualitative arguments
  - Bounding analyses
  - Screening tools

How is risk addressed in the regulatory framework?

- **Traditional engineering or "design basis" approaches**
  - Implicit consideration of risk (which accidents, systems, etc. are important?)
  - Engineering judgment in determining a set of **"credible" accident categories** that require prevention/mitigation capabilities
    - ➢You'll hear this called **"deterministic"** analysis
  - Reliance on **worst case analyses**, single failure criterion, defense-in-depth, and safety margins

How is risk addressed in the regulatory framework?

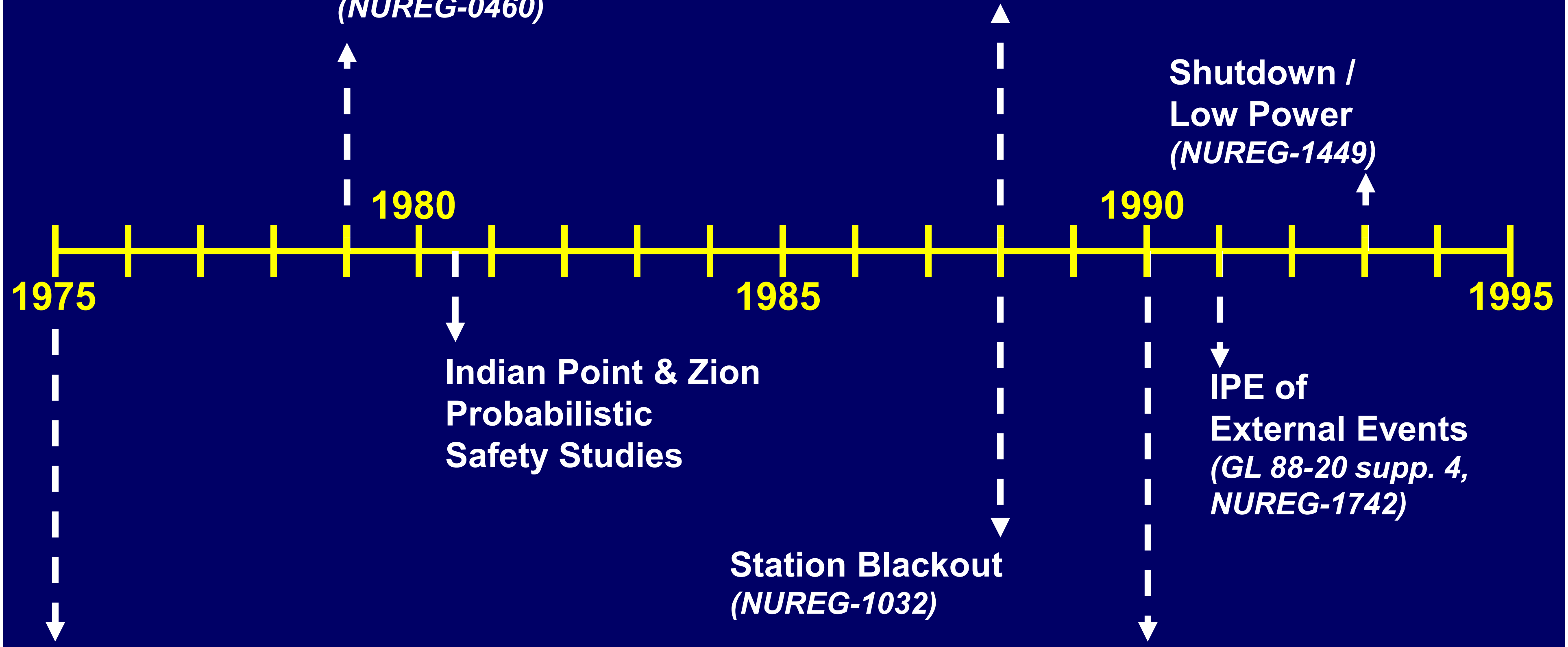
- **Risk-informed approaches**
  - Explicit consideration of risk
  - "Full picture" – scope includes **all potential accident initiators and mitigation failures** (including multiple failures)
  - Address the **possibility of releases** greater than regulatory limits

Why are risk-informed approaches used?

- **Reactor Safety Study (WASH-1400)* assessed reactor risk using PRA**
  - Revealed actual risk significant areas and interactions that were very different from the design basis events
    - Ex: **small loss of coolant accidents (LOCAs)** are significant risk contributors
  - Demonstrated the value of an **integrated** view of risk
- **Other risk studies followed to expand on these early findings**

**** NUREG-75/014, 10/75***

What early risk studies were done?



Reactor Safety Study
(WASH-1400)

ATWS
(NUREG-0460)

Indian Point & Zion Probabilistic Safety Studies

Individual Plant Examinations (IPE) for Severe Accident Vulnerabilities
(GL 88-20, NUREG-1560)

Station Blackout
(NUREG-1032)

Severe Accident Risks
(NUREG-1150)

IPE of External Events
(GL 88-20 supp. 4, NUREG-1742)

Shutdown / Low Power
(NUREG-1449)

Why is risk information used?

- **Commission’s policy statement on the use of PRA* included four main statements:**

1. **Increase use of PRA** to the extent supported by the state-of-the-art and in a way that **complements** traditional engineering approaches
2. Use PRA both to **reduce unnecessary conservatism** in current requirements and to support proposals for **additional regulatory requirements**
3. Be as **realistic** as practicable
4. Consider **uncertainties** appropriately when using the Commission's safety goals and subsidiary numerical objectives

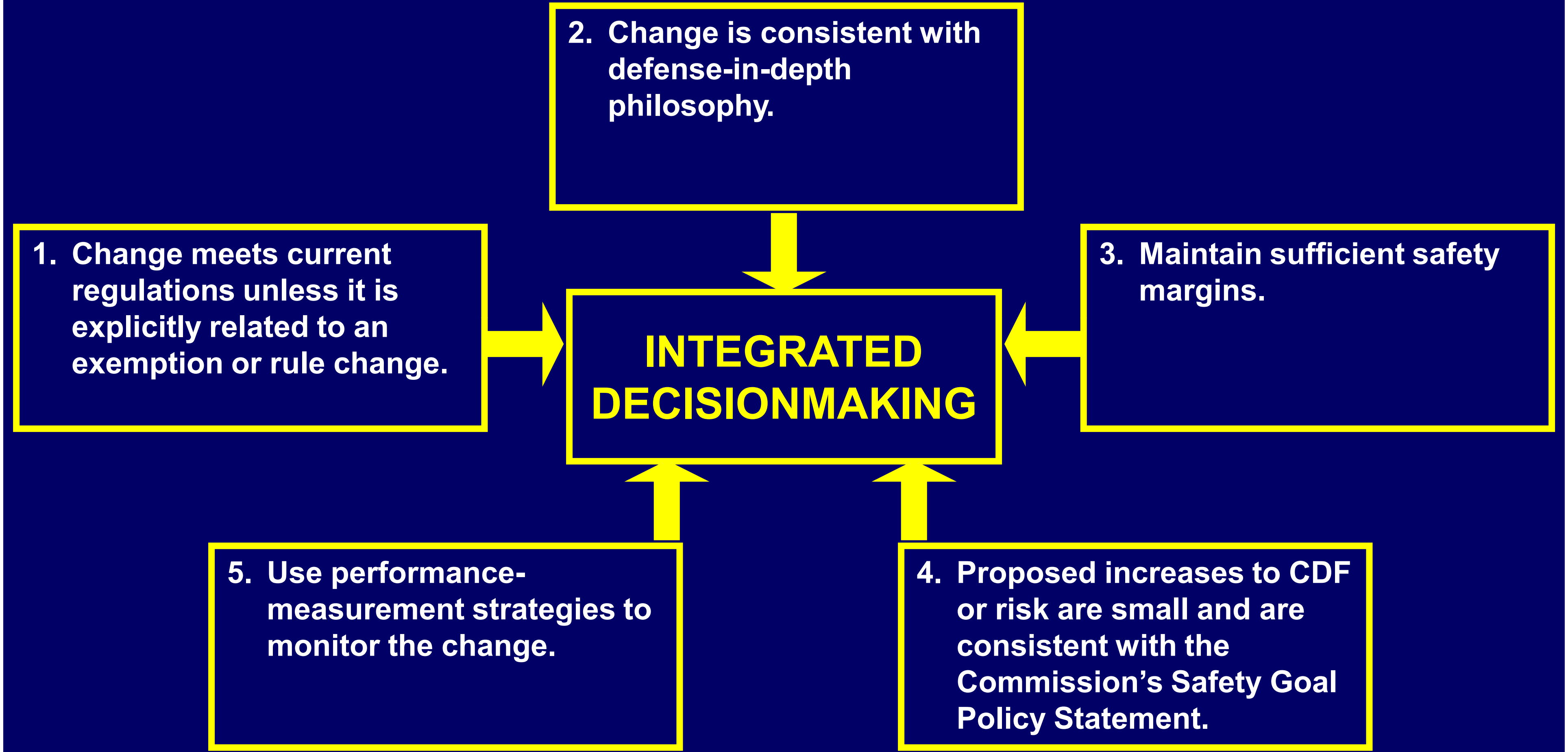
***** 8/16/95***

What is risk-informed regulation?

- A philosophy whereby risk insights are considered **together with other factors** to establish requirements that better focus licensee and regulatory attention on **design and operational issues commensurate with their importance** to health and safety.*

**** SRM on SECY-98-144, 3/1/99***

What are the principles of risk-informed regulation?*



2. Change is consistent with defense-in-depth philosophy.

1. Change meets current regulations unless it is explicitly related to an exemption or rule change.

INTEGRATED DECISIONMAKING

3. Maintain sufficient safety margins.

5. Use performance-measurement strategies to monitor the change.

4. Proposed increases to CDF or risk are small and are consistent with the Commission’s Safety Goal Policy Statement.

RG 1.174, 11/02

Why aren't our decisions risk-based?

- "Risk-based" would mean we decide using **only the numerical results and insights** of a risk assessment – if risk assessments are so helpful, why not?
  - We can't measure risk – we have to evaluate it using models
    - ➢ The models should address all contributors but do so with varying degrees of rigor and realism
    - ➢ Data on many failures or initiating events is sparse
    - ➢ Uncertainties may be large, but in principle we know how to deal with them
  - However, we cannot know everything, and therefore our **models are incomplete**, e.g., there could be previously unknown failure mechanisms.
- **Therefore, we still consider traditional "deterministic" concepts such as defense-in-depth and safety margins, as well as performance monitoring, to accommodate our incomplete knowledge!**

Where do we use risk-informed approaches?

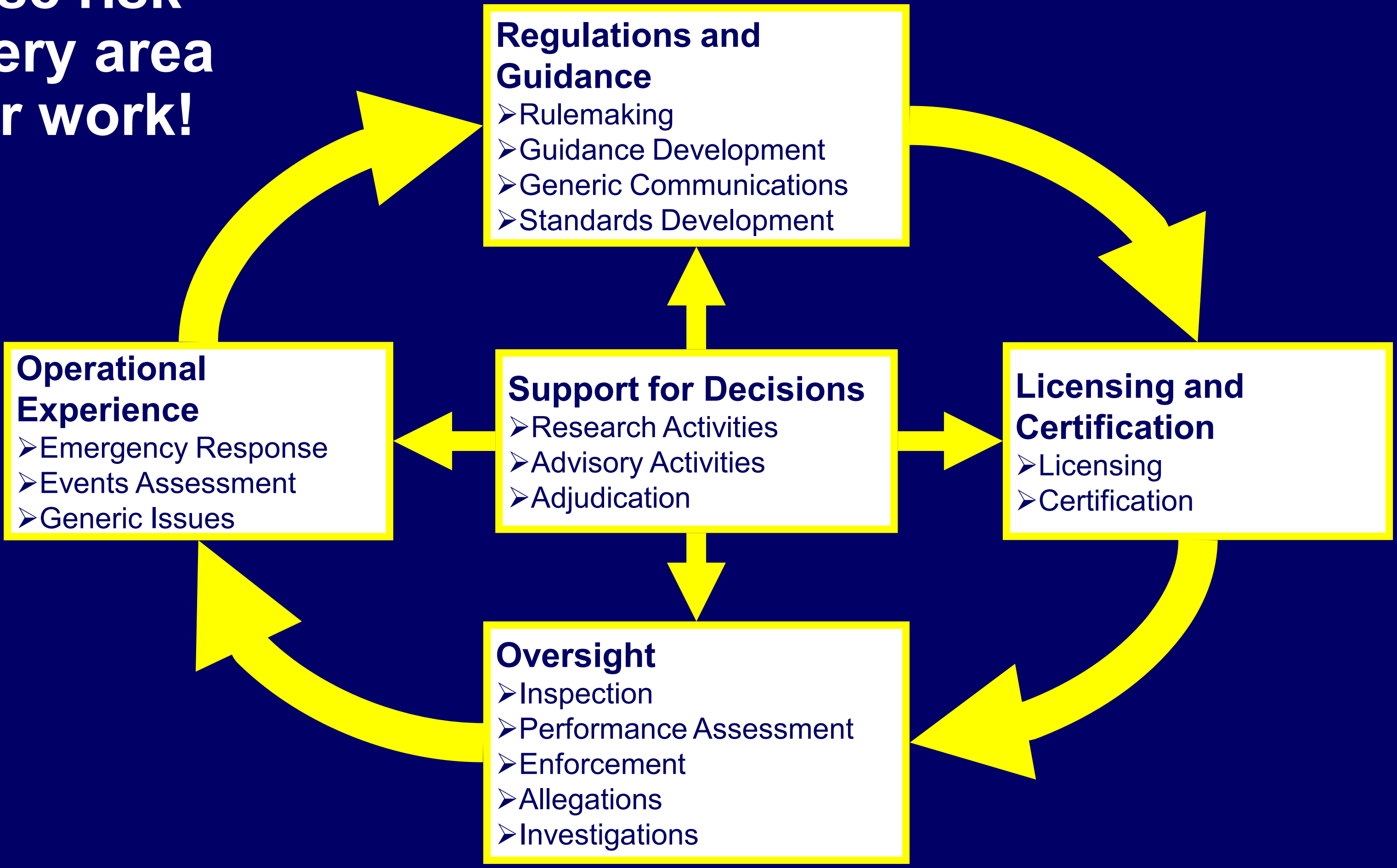
U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Where do we use risk-informed approaches?

- **We use risk in every area of our work!**



Regulations and Guidance

➢Rulemaking
➢Guidance Development
➢Generic Communications
➢Standards Development

Operational Experience

➢Emergency Response
➢Events Assessment
➢Generic Issues

Support for Decisions

➢Research Activities
➢Advisory Activities
➢Adjudication

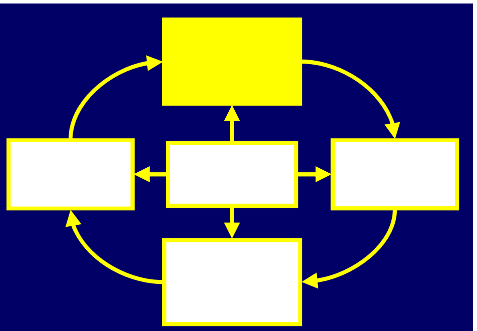
Licensing and Certification

➢Licensing
➢Certification

Oversight

➢Inspection
➢Performance Assessment
➢Enforcement
➢Allegations
➢Investigations

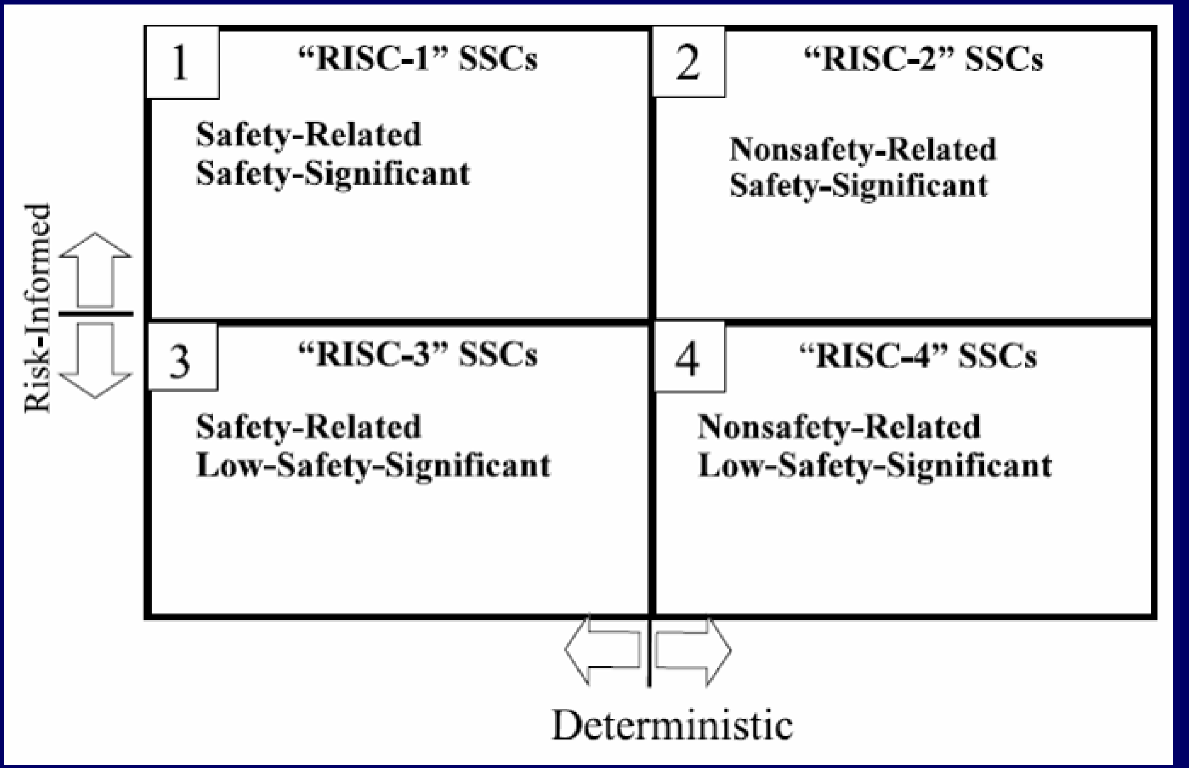
Regulations & Guidance



10 CFR	Subject	Year
50.44	Combustible Gas Control	2003
50.48(c)	Risk-Informed Fire Protection Requirements	2004
50.62	Anticipated Transient Without Scram	1984
50.63	Station Blackout	1988
50.65(a)(4)	Assessment of Maintenance Risk (Maintenance Rule)	1999
50.69	Risk-Informed Special Treatment Requirements	2004
50.71(h), 52.47	PRA Requirements for New Reactors	2007
50.61a	Pressurized Thermal Shock	TBD

Regulations & Guidance

- **Example – 50.69**
  - Risk-informed categorization of systems, structures, and components
  - Reduce (or increase!) testing, procurement requirements, quality assurance, etc.
  - Reduces burden on licensees and focuses on most risk-significant areas



1 "RISC-1" SSCs

Safety-Related
Safety-Significant

2 "RISC-2" SSCs

Nonsafety-Related
Safety-Significant

3 "RISC-3" SSCs

Safety-Related
Low-Safety-Significant

4 "RISC-4" SSCs

Nonsafety-Related
Low-Safety-Significant

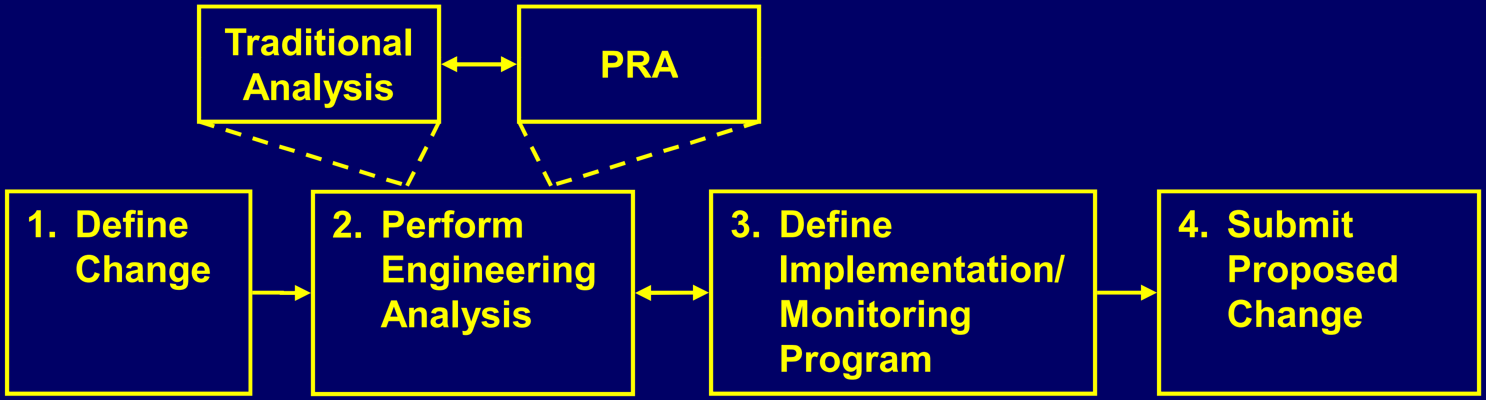
Regulations & Guidance

- **Example – new reactor design certification and combined licenses**
  - NRC reviews a description of the design-specific or plant-specific PRA and its results*
  - PRAs referencing a design certification must account for site information and design changes**
  - Combined license holders must maintain and upgrade their PRAs according to NRC-endorsed standards***

**** 52.47(a)(27) and 52.79(a)(46)***
***** 52.79(d)(1)***
****** 50.71(h)***

Licensing & Certification

- **Voluntary risk-informed licensing basis changes***
  - Risk-informed technical specifications changes – example later!
  - Risk-informed inservice testing (pumps/valves) and inspection (pipes)
  - Risk-informed fire protection


Traditional Analysis

PRA

1. Define Change

2. Perform Engineering Analysis

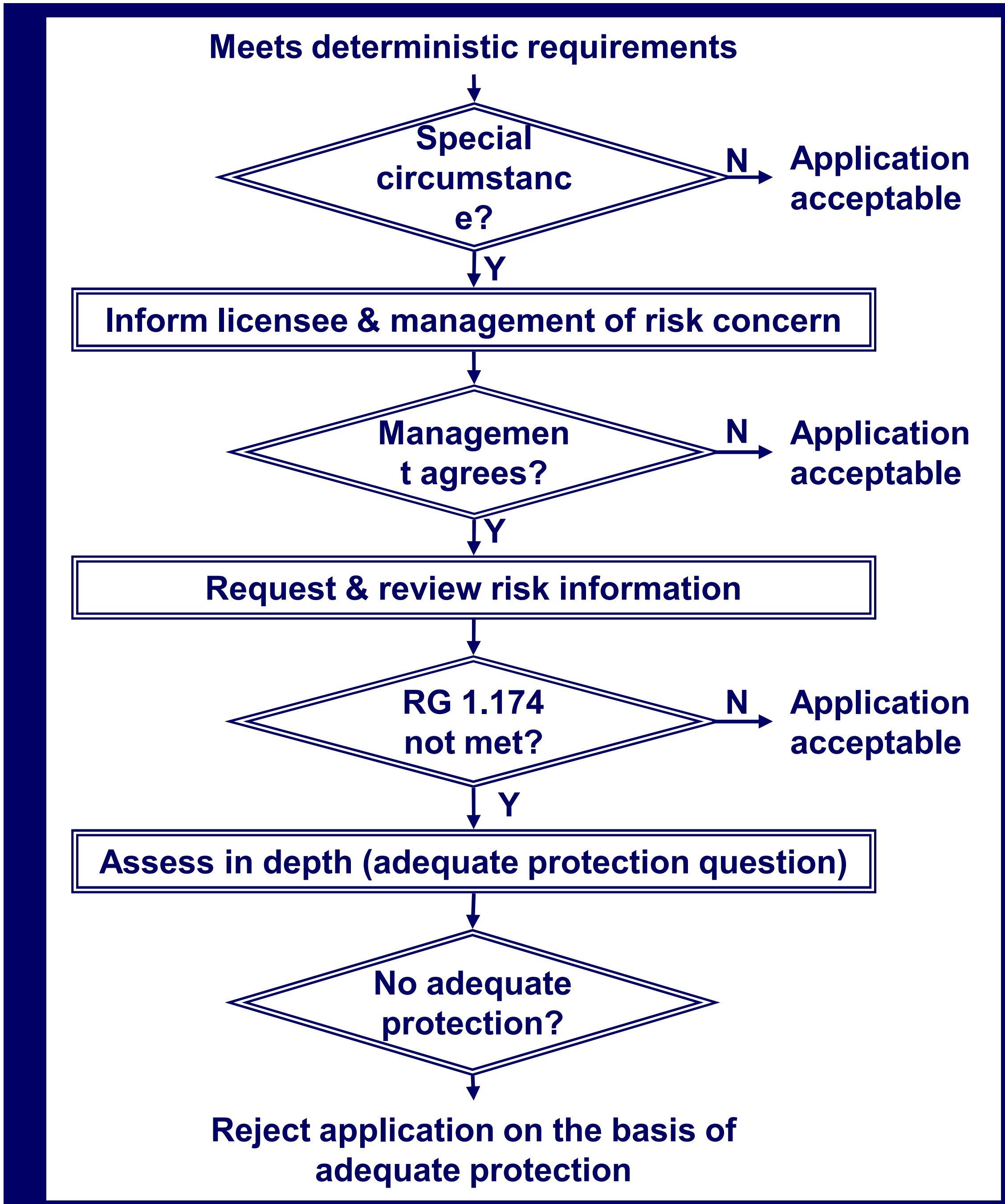
3. Define Implementation/ Monitoring Program

4. Submit Proposed Change

- **NRC staff can request risk information** for non-risk-informed licensing actions in a "special circumstance"**

** RG 1.174, 11/02*

*** SRP 19.2, App. D*



Meets deterministic requirements

Special circumstance?

N → Application acceptable

Y

Inform licensee & management of risk concern

Management agrees?

N → Application acceptable

Y

Request & review risk information

RG 1.174 not met?

N → Application acceptable

Y

Assess in depth (adequate protection question)

No adequate protection?

Reject application on the basis of adequate protection

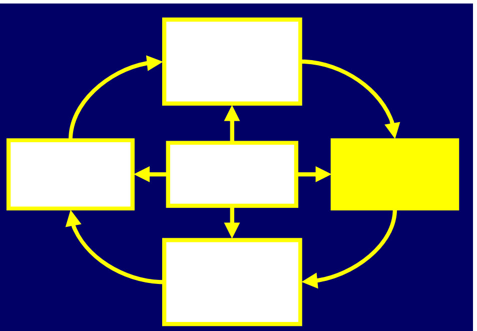
“Special circumstances” may exist if:

1. The situation was not identified or addressed in development of regulations, and could be **important enough to warrant a new regulation** if encountered on a widespread basis.

2. The reviewer has knowledge that the risk impact is not reflected by the licensing basis analysis, and has reason to believe that the risk increase would **warrant denial if the request were evaluated as a risk-informed application**.

**** SRP 19.2, App. D***

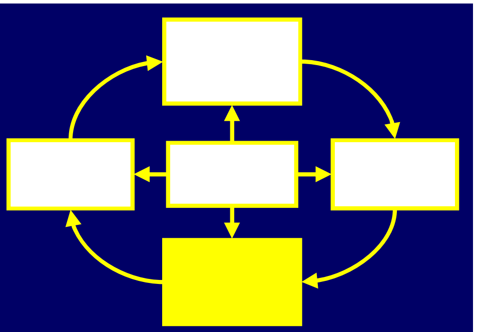
Licensing & Certification



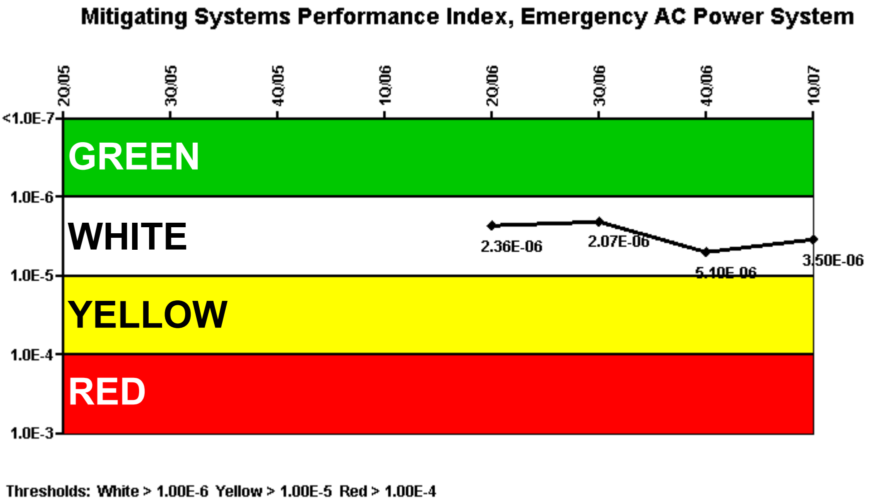
- **Regulatory treatment of non-safety systems (RTNSS)**
  - Used in review of new reactor designs
  - Applies to non-safety-related systems, structures, and components needed to:
    - ➢ Meet NRC performance requirements (ATWS, station blackout)
    - ➢ Ensure safety 72+ hours after an accident or after an earthquake
    - ➢ Meet CDF and LRF guidelines at power and during shutdown
    - ➢ Meet the containment performance goal (CCFP) during severe accidents
    - ➢ Prevent significant adverse system interactions
  - Example: short-term availability controls on hydrogen igniters for AP1000*

***** WCAP-15985, 9/9/03***

Oversight



- **Notice of Enforcement Discretion (NOED)***
  - Non-compliance with a technical specification or license condition
  - Risk argument for avoiding unnecessary plant transient, inappropriate test/inspection, or unjustified delay in startup



- **Reactor Oversight Process**
  - Risk-informed performance indicators
    - ➢ Mitigating System Performance Index (MSPI)**
  - Risk-informed baseline inspections
  - Significance Determination Process for inspection findings

*** Inspection Manual Chapter Part 9900***

**** http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/mspi.html***

Operational Experience

- **Incident response**
  - Follow-up inspections based on event significance*
- **Event assessment**
  - Risk-informed decision-making**
  - Accident Sequence Precursor (ASP) program reported to Congress

<table>
<tr><th colspan="5">Estimated Conditional Core Damage Probability (CCDP)</th></tr>
<tr><th>CCDP &lt; 1E-6</th><th>1E-6 – 1E-5</th><th>1E-5 – 1E-4</th><th>1E-4 – 1E-3</th><th>CCDP &gt; 1E-3</th></tr>
<tr><td colspan="2">No additional inspection</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Special inspection</td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="2">AIT</td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2">IIT</td></tr>
</table>

** Management Directive 8.3*

*** NRR Office Instruction LIC-504*

How do you fit in to risk-informed regulation?

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

How do you fit in?

- Everyone **has a role in risk-informed regulation, because the purpose is general:**
  - Focus on safety
  - Don’t miss things because they’re unlikely or not obvious
  - Don’t spend lots of time on areas that don’t affect safety

- **Your input will depend on your specific job function**

How do you fit in as a PROJECT MANAGER?

- **YOU identify risk-informed licensing actions to ensure they're reviewed by the right groups**
  - ASK YOURSELF: This relief request mentions risk-informed inservice inspection – should the PRA group take a look?
- **YOU hear the plant's current online risk assessment "color" discussed daily on the morning call**
  - ASK YOURSELF: The resident says the risk is "yellow" – what does that mean? Does anyone in headquarters need to know?
- **YOU work with the region on a Notice of Enforcement Discretion for your plant**
  - ASK YOURSELF: Is the risk of staying in the current operating status higher than the thresholds in the guidance?

How do you fit in as a TECHNICAL REVIEWER?

- **YOU may identify a licensing action that <u>could be risk significant</u>, even though it's not risk informed***
  - ASK YOURSELF: Does this change create special circumstances that would be vulnerable to severe accidents even if it is acceptable for design basis accidents?

- **YOU <u>review the deterministic arguments</u> in licensees' risk-informed applications**
  - ASK YOURSELF: Are defense-in-depth and safety-margin requirements still met when this outage time is extended (even if the risk numbers say it's okay)?

- **YOU use risk insights to help <u>focus your review</u>**
  - ASK YOURSELF: Is a less-detailed review of this system warranted based on its low risk significance? Or does it need <u>more</u> attention than was needed at other plants because of some unique risk insight?

**** RIS 2001-02, 1/18/01; SRP 19.2, App. D***

How do you fit in as an INSPECTOR?

- **YOU use risk information to decide which systems or activities to inspect**
  - ASK YOURSELF: Where should I look during my flooding inspection? If I have time to watch one maintenance activity during the outage, which should it be?

- **YOU assess the significance of inspection findings**
  - ASK YOURSELF: How did this deficiency increase the risk at the facility?

- **YOU stay alert for high-risk evolutions**
  - ASK YOURSELF: The plant’s on-line risk monitor says risk will be “yellow” for two hours today – do I need to take any action? How risky is it to have these two pieces of equipment out of service at the same time?

2. Use of PRA Models

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Module 2: Use of PRA Models

- How do we build PRA models?
- How do we use PRA in risk-informed regulation?
- How do we know a licensee’s PRA is adequate?
- What can we learn from PRA results?

How do we build PRA models?

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

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

What are the end states of a PRA?

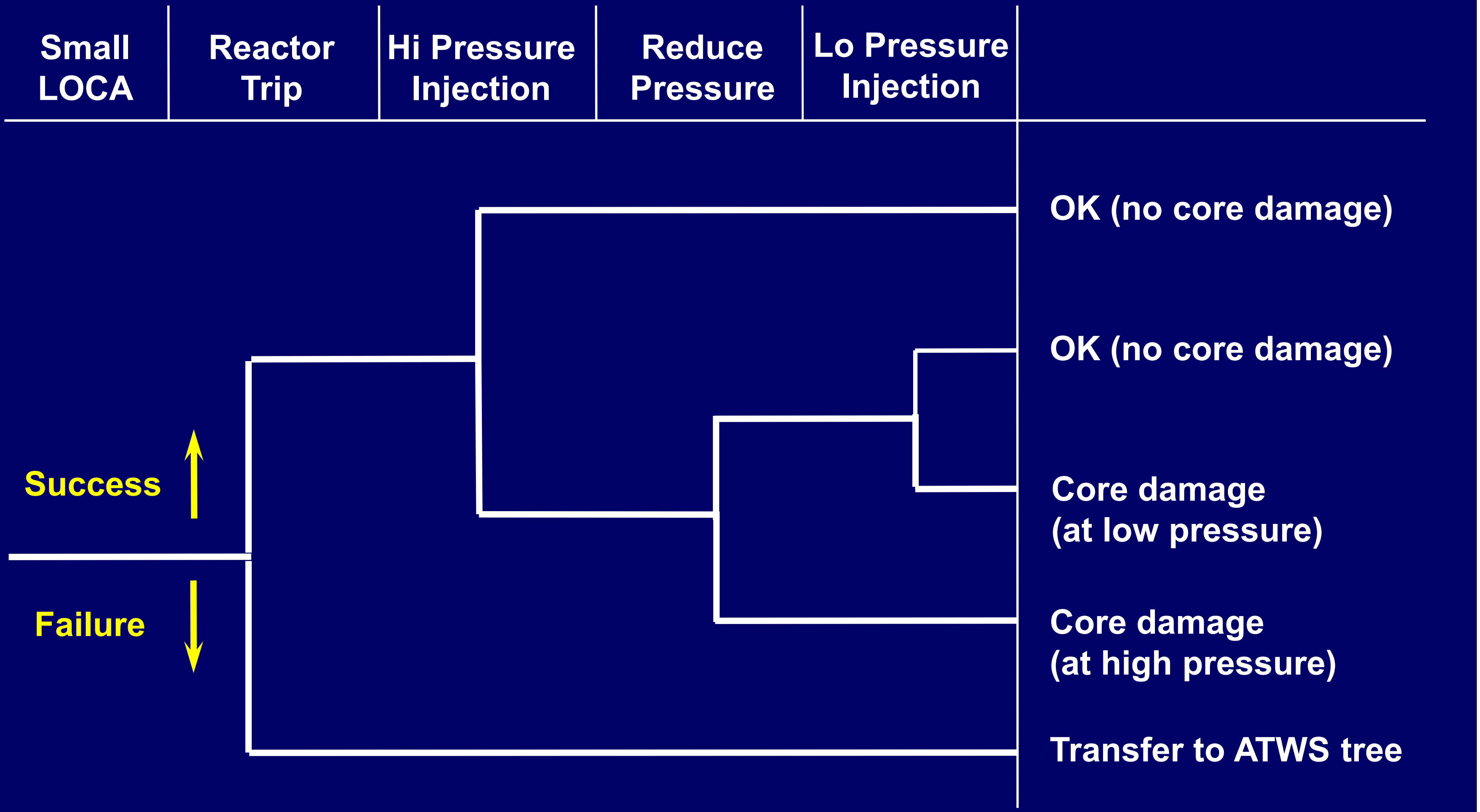
- **Core damage occurs when**
  - **Safety functions** are not met
    - ➢ Such as removal of decay heat, control of reactivity, or control of inventory
  - Engineering models show that core parameters exceed certain pre-determined limits

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

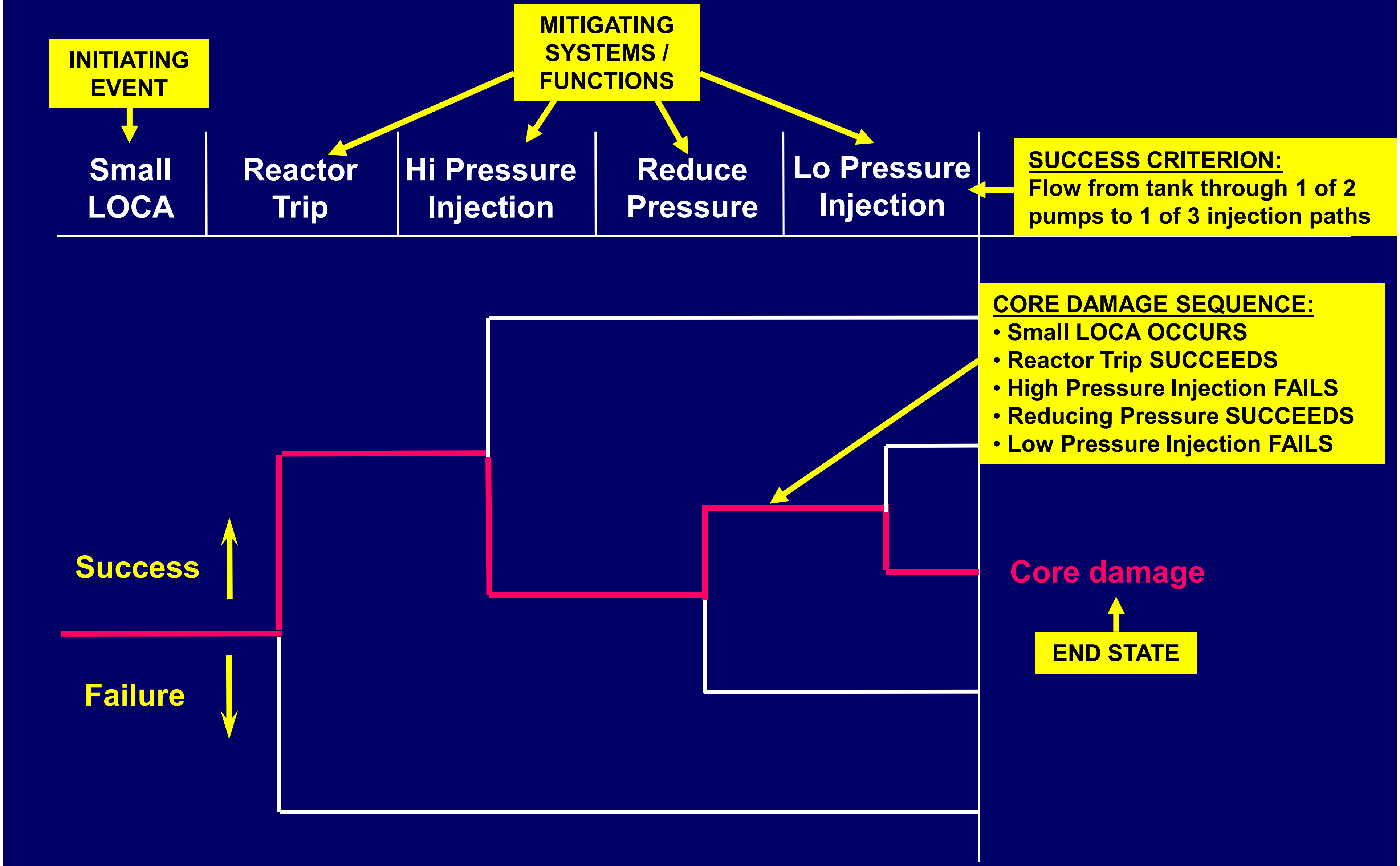
- **A limited Level 2 PRA provides insights related to core damage and large early release.**

What is an event tree?

A graphical depiction of a sequence of events



What is an event tree?



INITIATING EVENT

MITIGATING SYSTEMS / FUNCTIONS

Small LOCA

Reactor Trip

Hi Pressure Injection

Reduce Pressure

Lo Pressure Injection

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

CORE DAMAGE SEQUENCE:

- Small LOCA OCCURS
- Reactor Trip SUCCEEDS
- High Pressure Injection FAILS
- Reducing Pressure SUCCEEDS
- Low Pressure Injection FAILS

Success

Failure

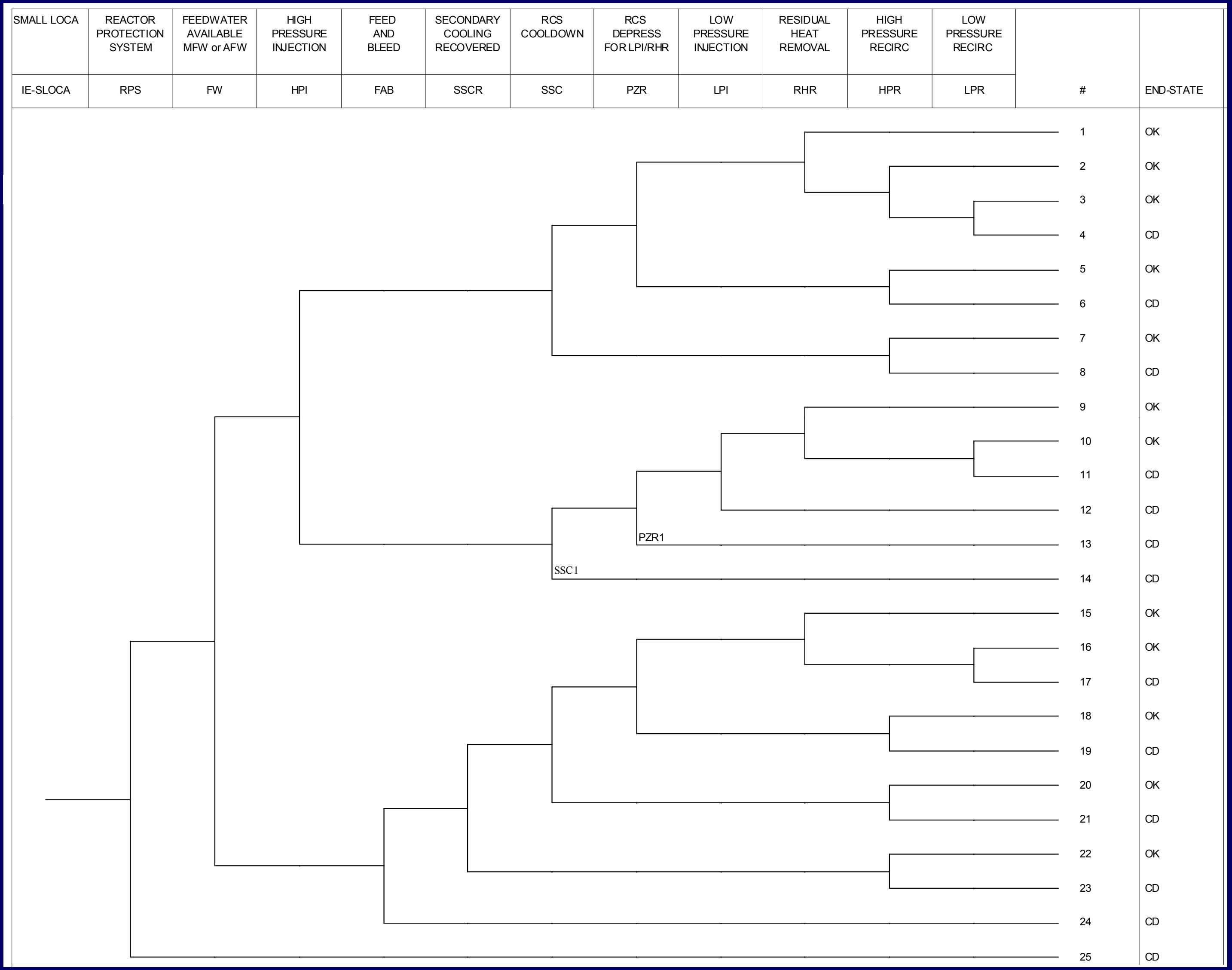
Core damage

END STATE

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

More Complex Event Tree



SMALL LOCA	REACTOR PROTECTION SYSTEM	FEEDWATER AVAILABLE MFW or AFW	HIGH PRESSURE INJECTION	FEED AND BLEED	SECONDARY COOLING RECOVERED	RCS COOLDOWN	RCS DEPRESS FOR LPI/RHR	LOW PRESSURE INJECTION	RESIDUAL HEAT REMOVAL	HIGH PRESSURE RECIRC	LOW PRESSURE RECIRC	#	END-STATE
IE-SLOCA	RPS	FW	HPI	FAB	SSCR	SSC	PZR	LPI	RHR	HPR	LPR		

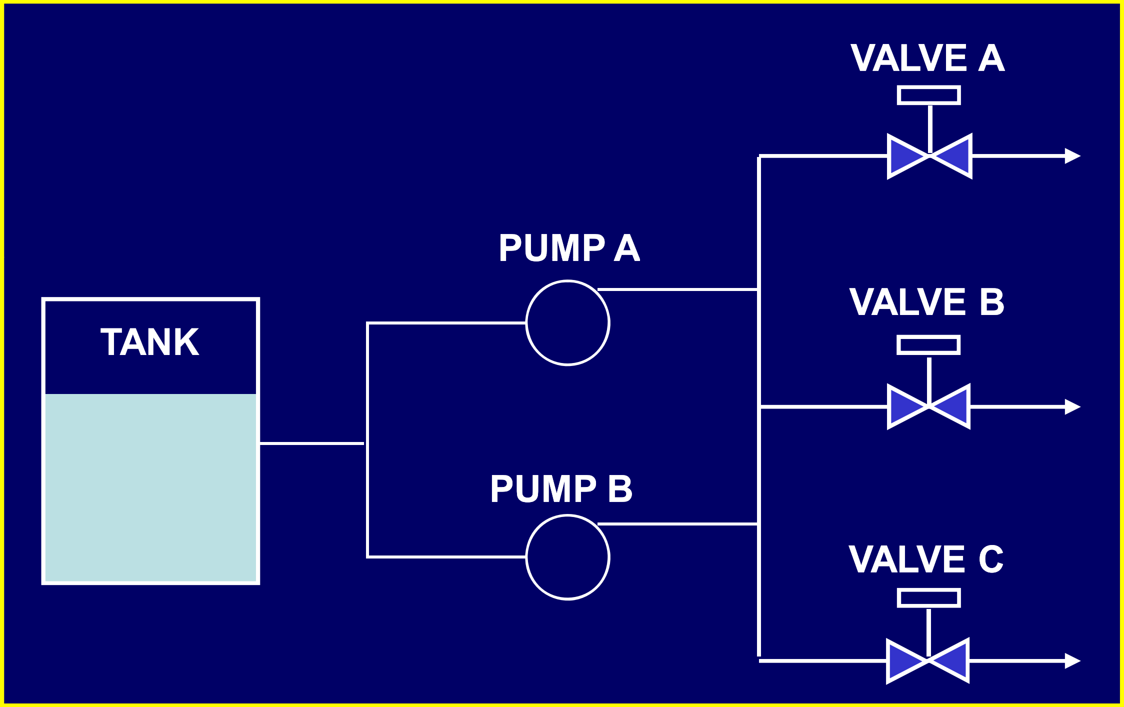
#	END-STATE
1	OK
2	OK
3	OK
4	CD
5	OK
6	CD
7	OK
8	CD
9	OK
10	OK
11	CD
12	CD
13	CD
14	CD
15	OK
16	OK
17	CD
18	OK
19	CD
20	OK
21	CD
22	OK
23	CD
24	CD
25	CD

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

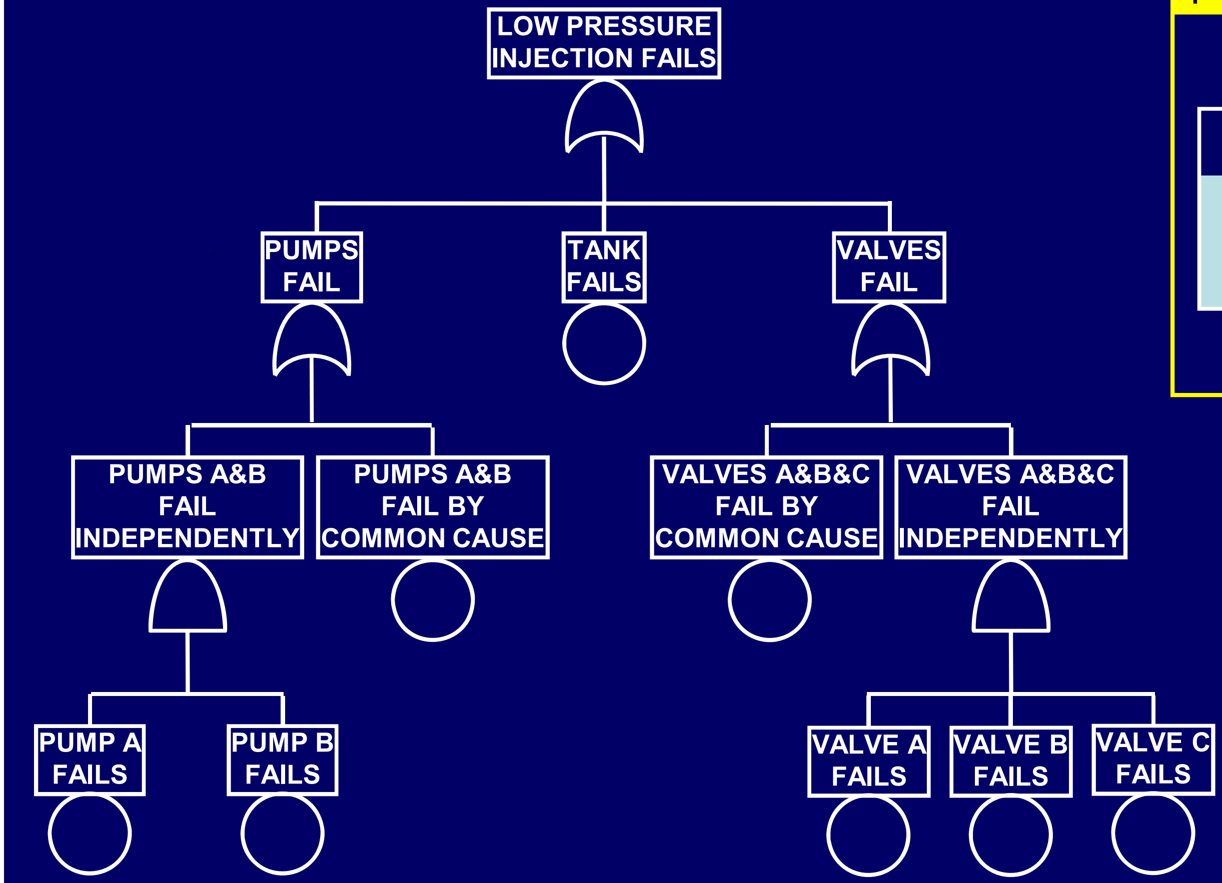
FAILURE OCCURS WHEN:
No flow from tank
OR
No flow from pumps
OR
No flow through injection paths

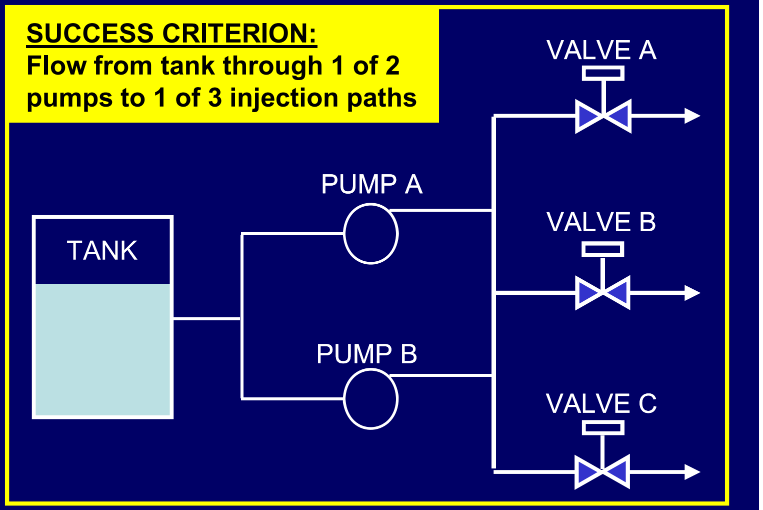


What is a fault tree?

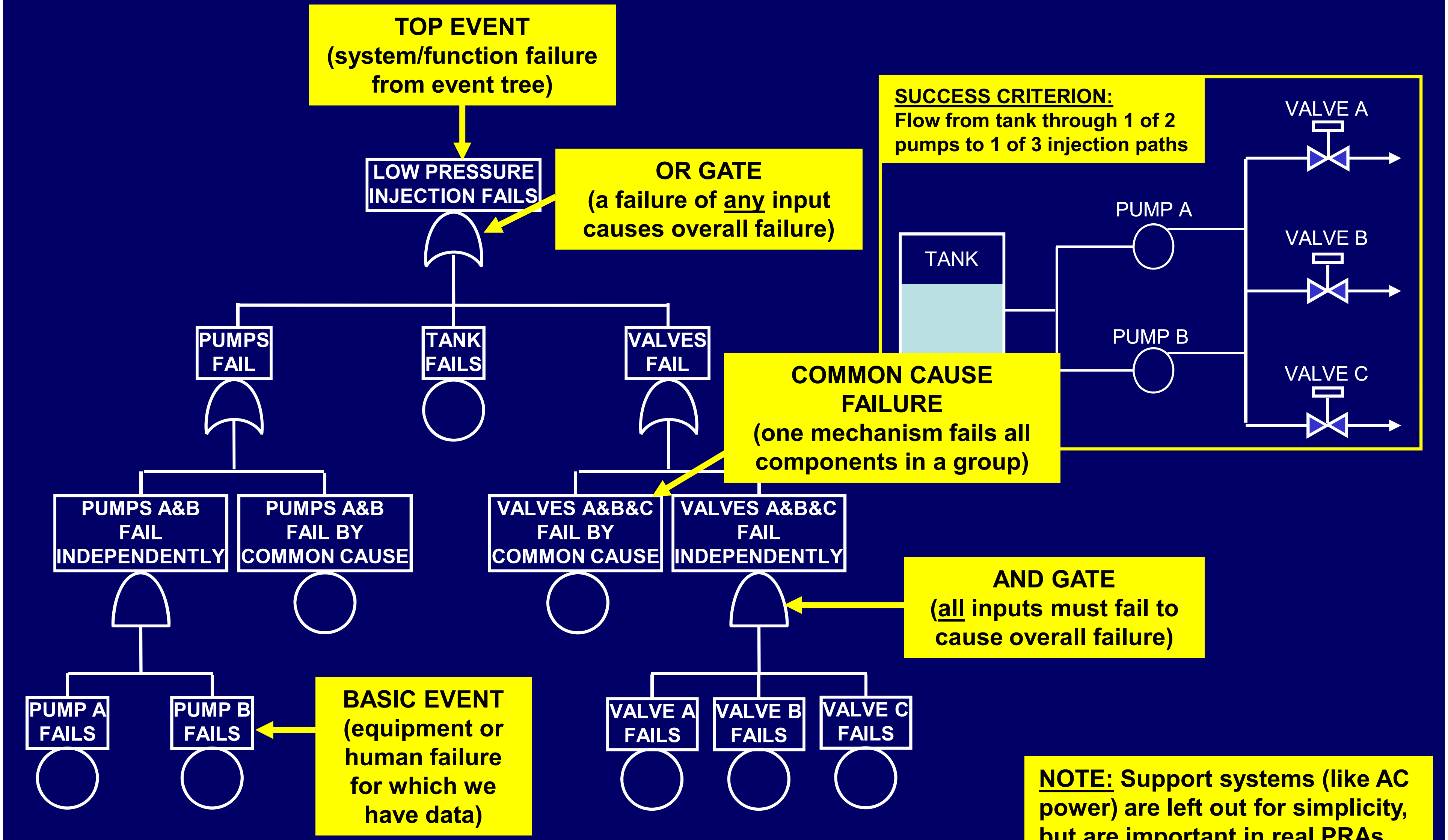
- **Developing fault trees**
  - Need for fault tree usually arises from the event tree
    - What equipment can provide the function?
    - What operator actions must take place?
  - Define **success criteria**, e.g.
    - How much flow is needed to remove decay heat?
    - How much flow is necessary 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?


LOW PRESSURE INJECTION FAILS
PUMPS FAIL
TANK FAILS
VALVES FAIL
PUMPS A&B FAIL INDEPENDENTLY
PUMPS A&B FAIL BY COMMON CAUSE
VALVES A&B&C FAIL BY COMMON CAUSE
VALVES A&B&C FAIL INDEPENDENTLY
PUMP A FAILS
PUMP B FAILS
VALVE A FAILS
VALVE B FAILS
VALVE C FAILS


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

What is a fault tree?


LOW PRESSURE INJECTION FAILS
PUMPS FAIL
TANK FAILS
VALVES FAIL
PUMPS A&B FAIL INDEPENDENTLY
PUMPS A&B FAIL BY COMMON CAUSE
VALVES A&B&C FAIL BY COMMON CAUSE
VALVES A&B&C FAIL INDEPENDENTLY
PUMP A FAILS
PUMP B FAILS
VALVE A FAILS
VALVE B FAILS
VALVE C FAILS
TANK
PUMP A
PUMP B
VALVE A
VALVE B
VALVE C

TOP EVENT
(system/function failure from event tree)

OR GATE
(a failure of <u>any</u> input causes overall failure)

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

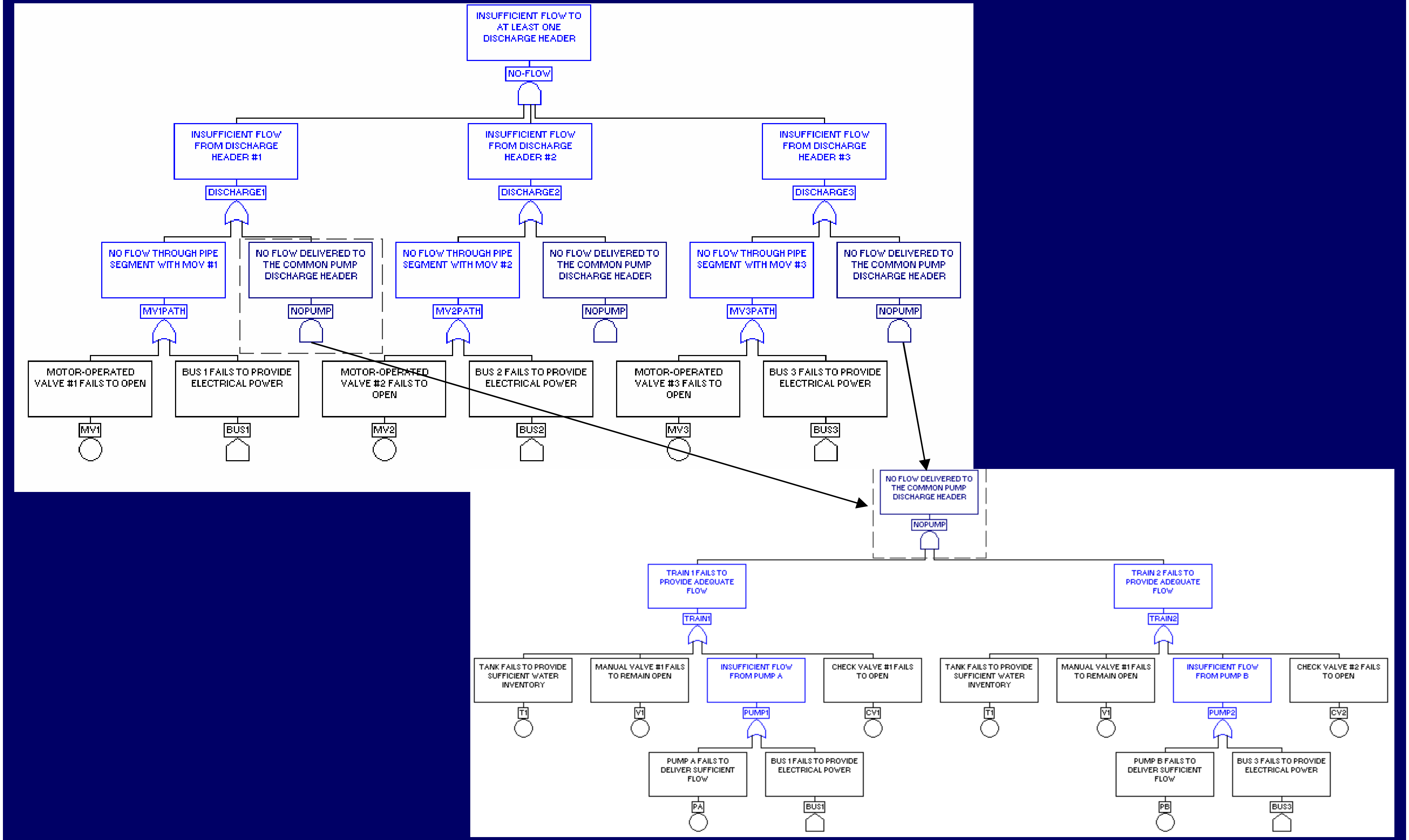
COMMON CAUSE FAILURE
(one mechanism fails all components in a group)

AND GATE
(<u>all</u> inputs must fail to cause overall failure)

BASIC EVENT
(equipment or human failure for which we have data)

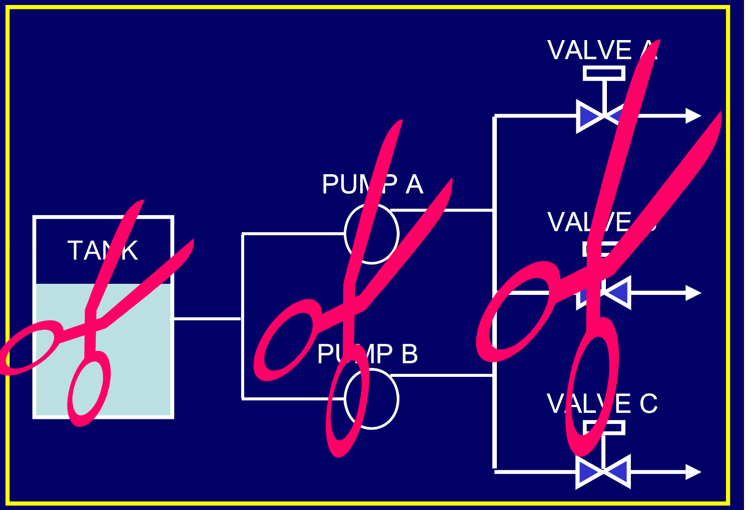
<u>NOTE:</u> Support systems (like AC power) are left out for simplicity, but are important in real PRAs.

More Complex Fault Tree


INSUFFICIENT FLOW TO AT LEAST ONE DISCHARGE HEADER
NO-FLOW
INSUFFICIENT FLOW FROM DISCHARGE HEADER #1
DISCHARGE1
INSUFFICIENT FLOW FROM DISCHARGE HEADER #2
DISCHARGE2
INSUFFICIENT FLOW FROM DISCHARGE HEADER #3
DISCHARGE3
NO FLOW THROUGH PIPE SEGMENT WITH MOV #1
MV1PATH
NO FLOW DELIVERED TO THE COMMON PUMP DISCHARGE HEADER
NOPUMP
NO FLOW THROUGH PIPE SEGMENT WITH MOV #2
MV2PATH
NO FLOW DELIVERED TO THE COMMON PUMP DISCHARGE HEADER
NOPUMP
NO FLOW THROUGH PIPE SEGMENT WITH MOV #3
MV3PATH
NO FLOW DELIVERED TO THE COMMON PUMP DISCHARGE HEADER
NOPUMP
MOTOR-OPERATED VALVE #1 FAILS TO OPEN
MV1
BUS 1 FAILS TO PROVIDE ELECTRICAL POWER
BUS1
MOTOR-OPERATED VALVE #2 FAILS TO OPEN
MV2
BUS 2 FAILS TO PROVIDE ELECTRICAL POWER
BUS2
MOTOR-OPERATED VALVE #3 FAILS TO OPEN
MV3
BUS 3 FAILS TO PROVIDE ELECTRICAL POWER
BUS3
NO FLOW DELIVERED TO THE COMMON PUMP DISCHARGE HEADER
NOPUMP
TRAIN 1 FAILS TO PROVIDE ADEQUATE FLOW
TRAIN1
TRAIN 2 FAILS TO PROVIDE ADEQUATE FLOW
TRAIN2
TANK FAILS TO PROVIDE SUFFICIENT WATER INVENTORY
T1
MANUAL VALVE #1 FAILS TO REMAIN OPEN
V1
INSUFFICIENT FLOW FROM PUMP A
PUMP1
CHECK VALVE #1 FAILS TO OPEN
CV1
TANK FAILS TO PROVIDE SUFFICIENT WATER INVENTORY
T1
MANUAL VALVE #1 FAILS TO REMAIN OPEN
V1
INSUFFICIENT FLOW FROM PUMP B
PUMP2
CHECK VALVE #2 FAILS TO OPEN
CV2
PUMP A FAILS TO DELIVER SUFFICIENT FLOW
PA
BUS 1 FAILS TO PROVIDE ELECTRICAL POWER
BUS1
PUMP B FAILS TO DELIVER SUFFICIENT FLOW
PB
BUS 3 FAILS TO PROVIDE ELECTRICAL POWER
BUS3

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

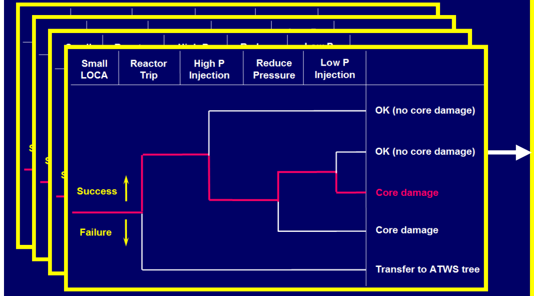


Where do we get the numbers?

- **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)

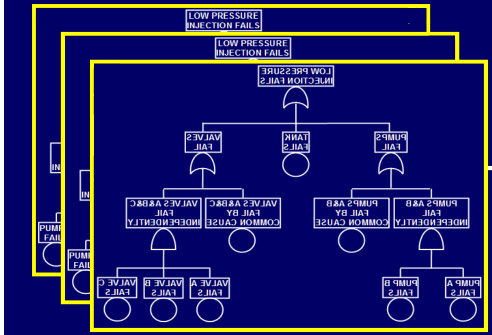
- **Special methods:**
  - **Expert elicitation** for rare events (e.g., large LOCA frequency)
  - **Human reliability analysis** (e.g., operator fails to switch to recirculation)
  - **Common cause failure** modeling

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!)

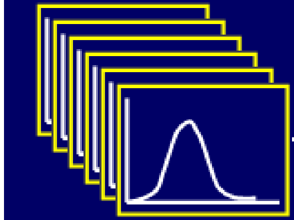


SYSTEM CUTSETS:

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

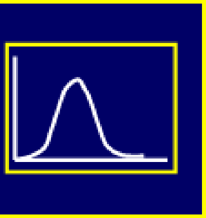
CORE DAMAGE CUTSETS:

- 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

U.S.NRC

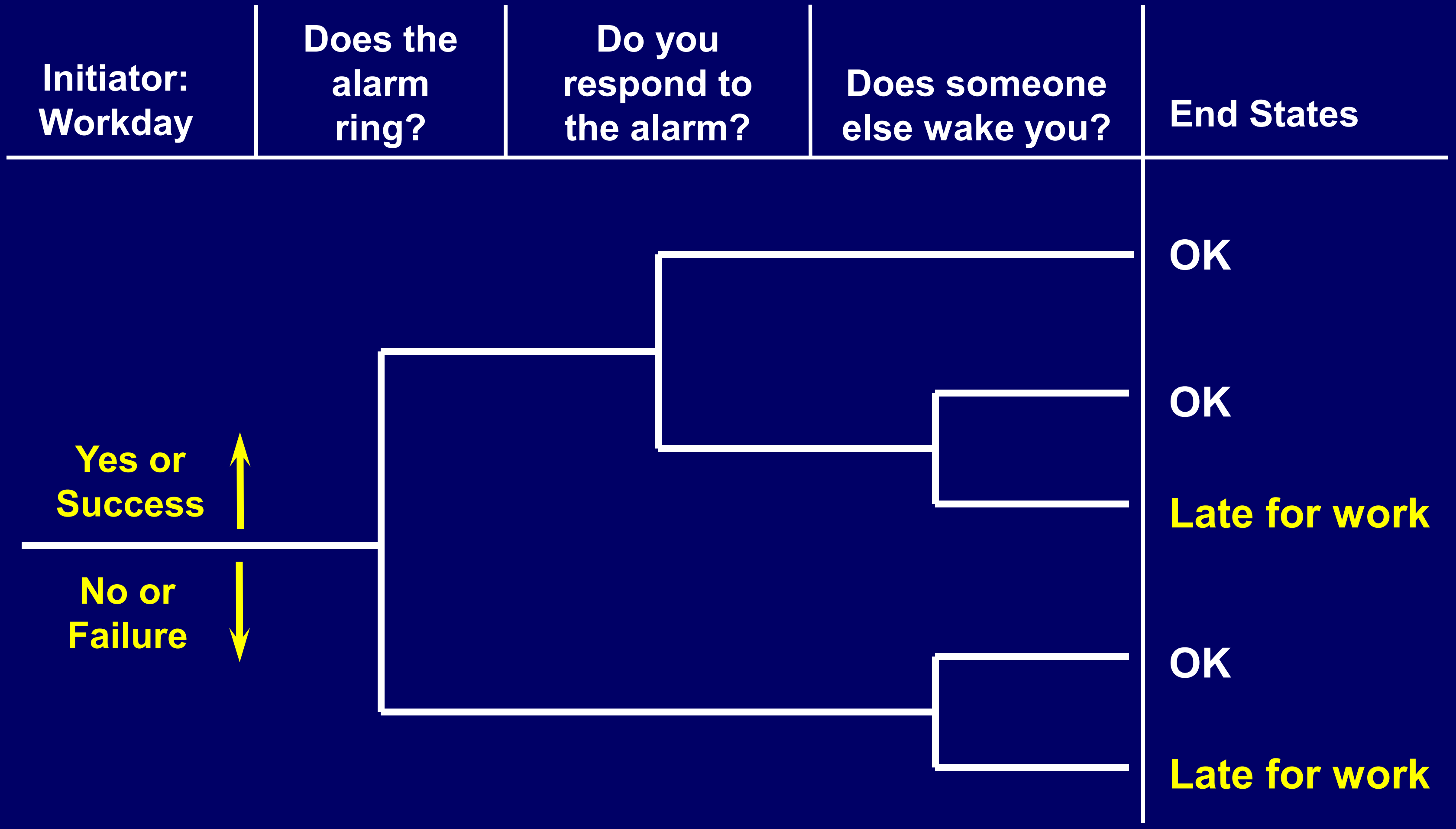
UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

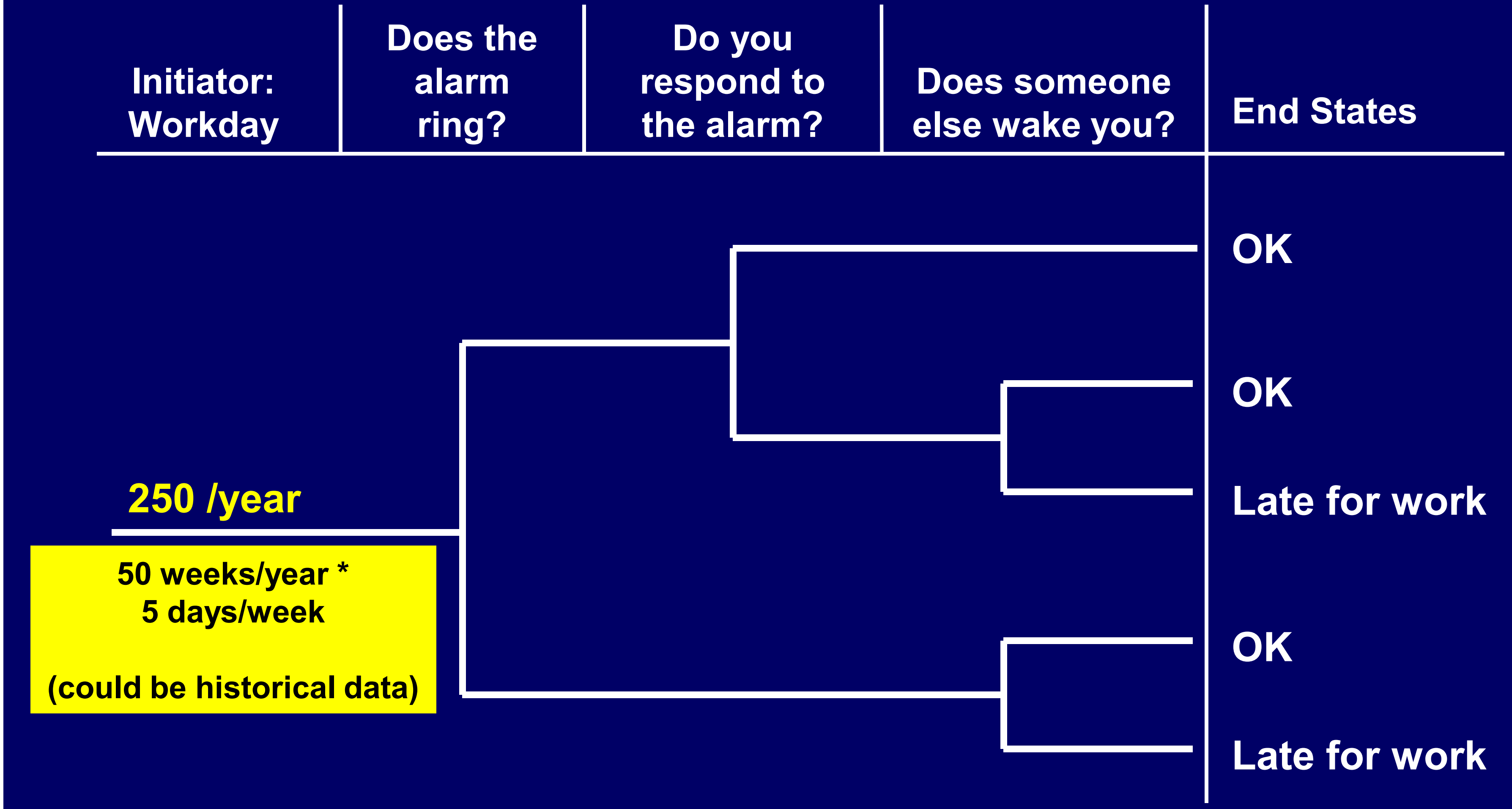
The Scenario

- **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



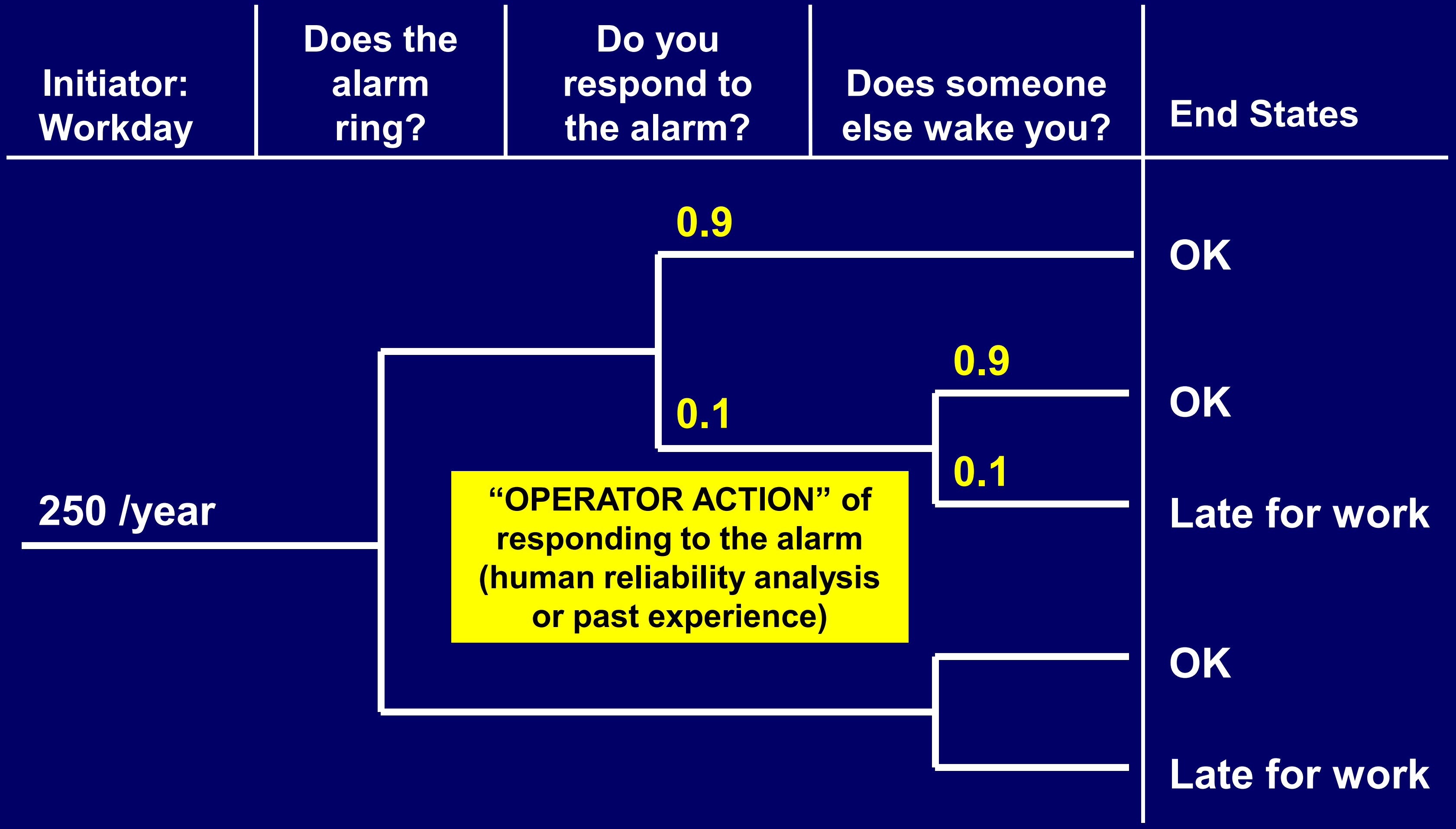
Estimating the Frequency of Oversleeping



50 weeks/year *
5 days/week

(could be historical data)

Estimating the Frequency of Oversleeping



Initiator: Workday

Does the alarm ring?

Do you respond to the alarm?

Does someone else wake you?

End States

250 /year

0.9

0.1

0.9

0.1

OK

OK

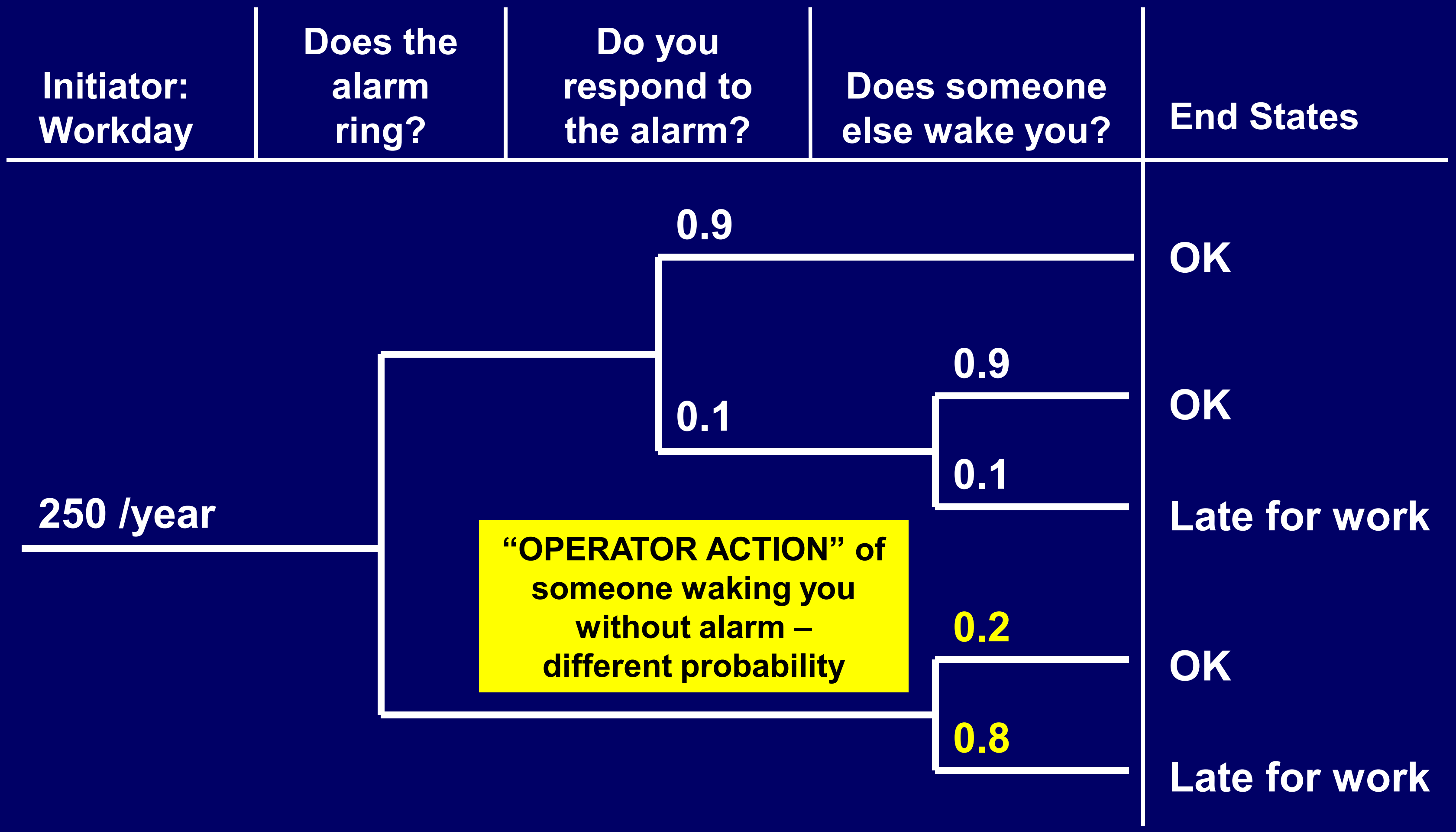
Late for work

OK

Late for work

“OPERATOR ACTION” of responding to the alarm (human reliability analysis or past experience)

Estimating the Frequency of Oversleeping



Initiator: Workday

Does the alarm ring?

Do you respond to the alarm?

Does someone else wake you?

End States

250 /year

0.9

0.1

0.9

0.1

0.2

0.8

OK

OK

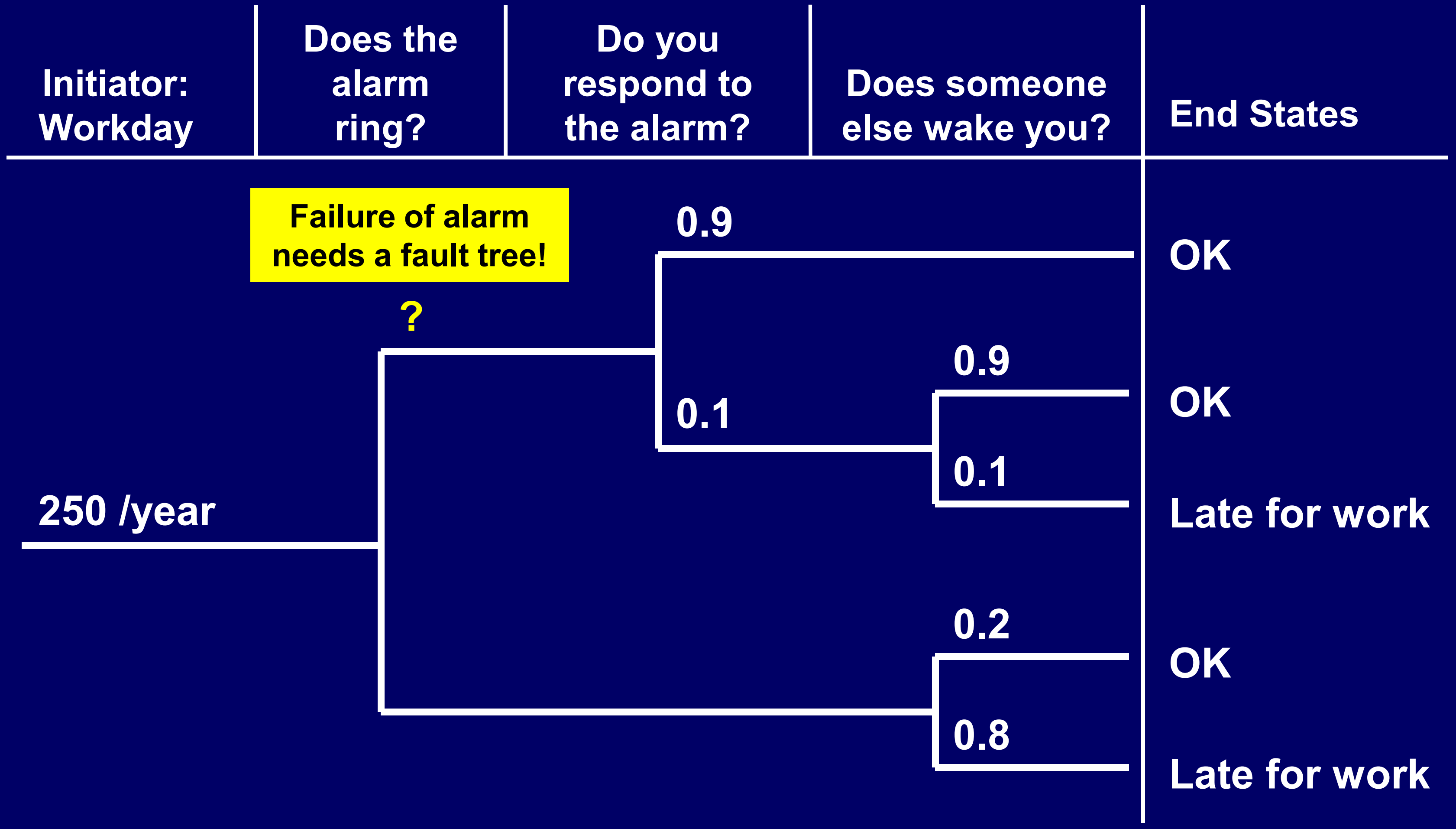
Late for work

OK

Late for work

“OPERATOR ACTION” of someone waking you without alarm – different probability

Estimating the Frequency of Oversleeping



Initiator: Workday

Does the alarm ring?

Do you respond to the alarm?

Does someone else wake you?

End States

Failure of alarm needs a fault tree!

?

0.9

0.1

0.9

0.1

250 /year

0.2

0.8

OK

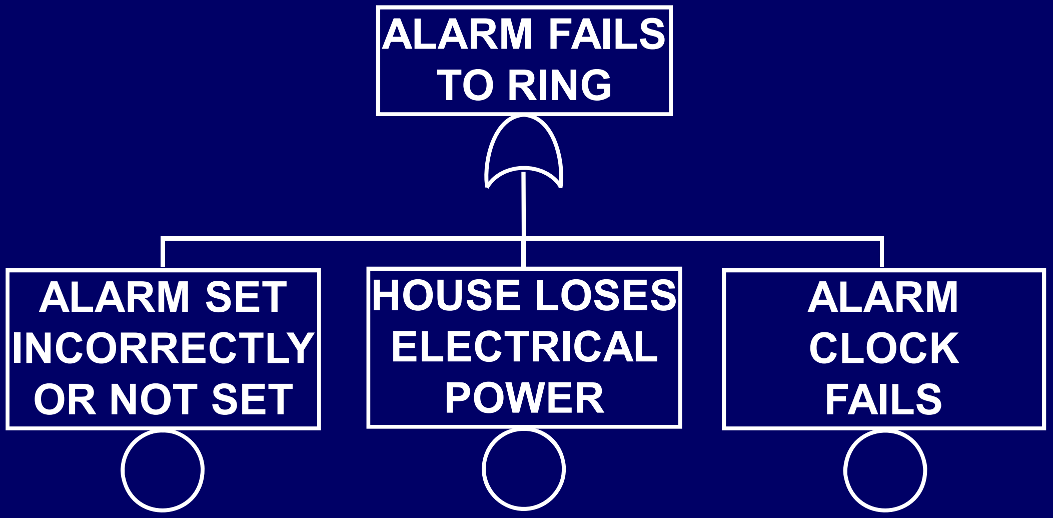
OK

Late for work

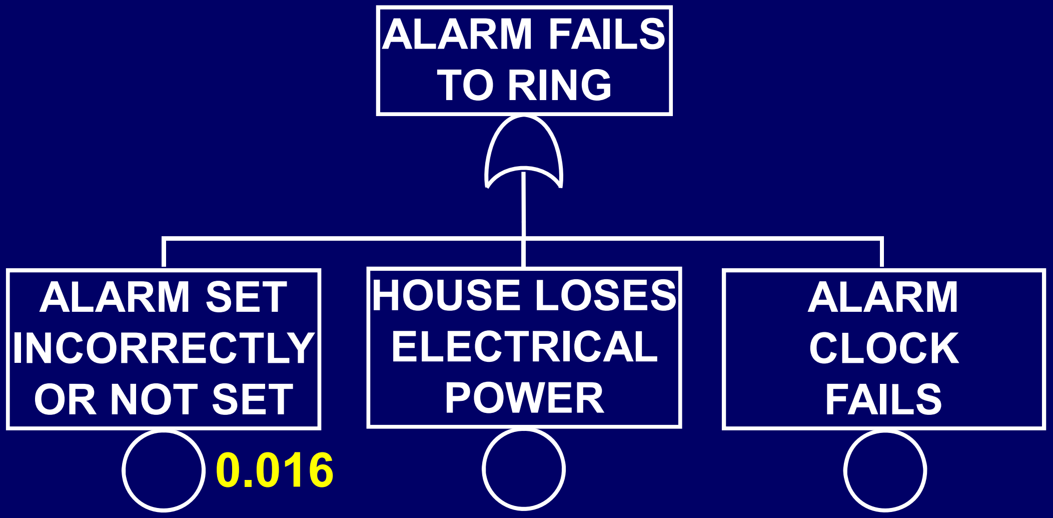
OK

Late for work

Sample Fault Tree for Alarm Failing to Ring


ALARM FAILS TO RING
ALARM SET INCORRECTLY OR NOT SET
HOUSE LOSES ELECTRICAL POWER
ALARM CLOCK FAILS

Estimating the Probability of Alarm Failing to Ring



ALARM FAILS TO RING

ALARM SET INCORRECTLY OR NOT SET

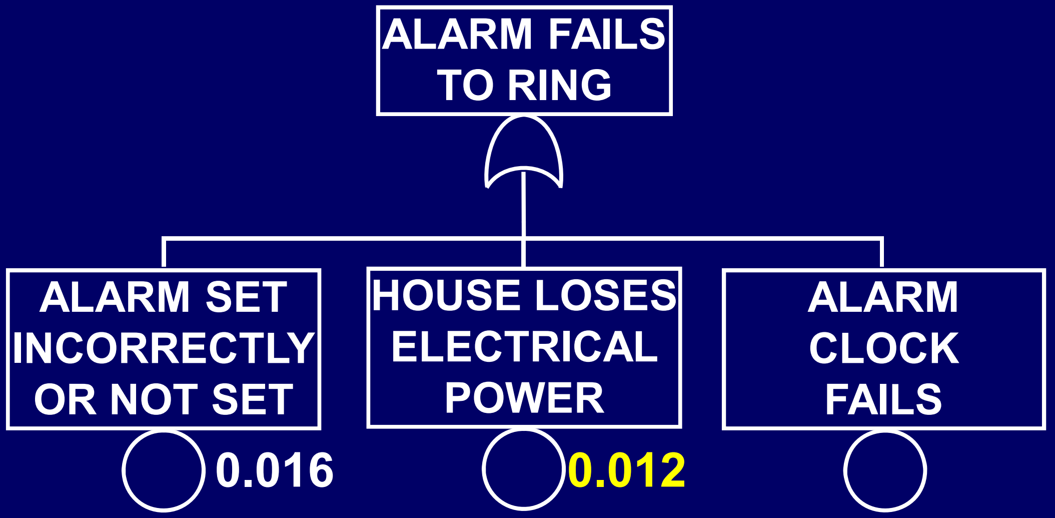
0.016

HOUSE LOSES ELECTRICAL POWER

ALARM CLOCK FAILS

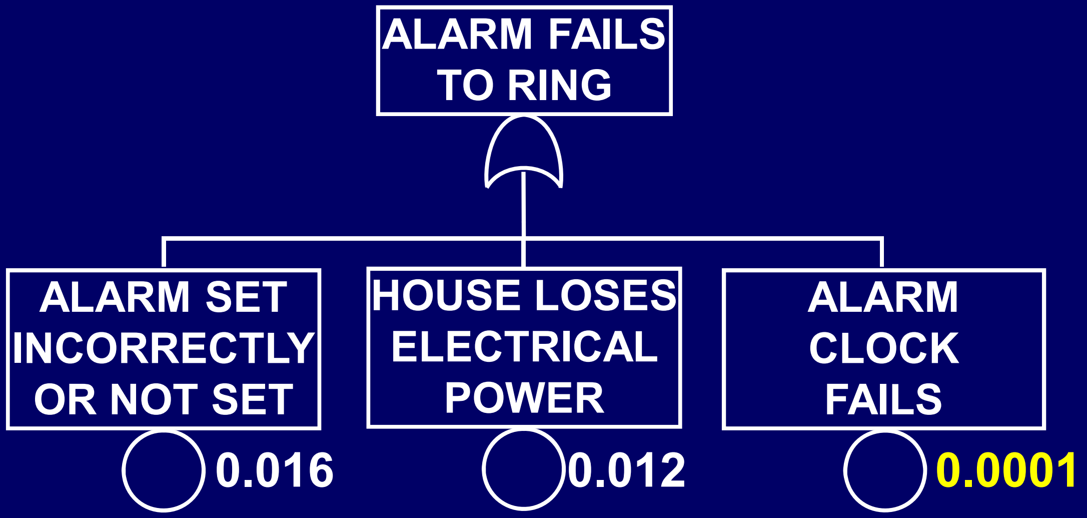
Your experience data:
4 times each work year
4/250 = 0.016

Estimating the Probability of Alarm Failing to Ring


ALARM FAILS TO RING
ALARM SET INCORRECTLY OR NOT SET
HOUSE LOSES ELECTRICAL POWER
ALARM CLOCK FAILS
0.016
0.012

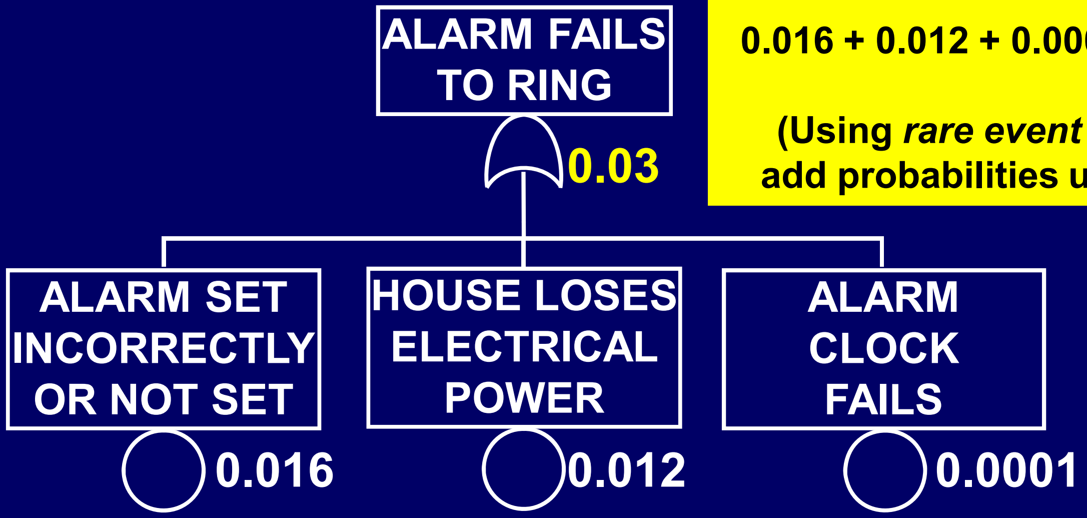
Your experience data:
3 work days per year
3/250 = 0.012

Estimating the Probability of Alarm Failing to Ring


ALARM FAILS TO RING
ALARM SET INCORRECTLY OR NOT SET
HOUSE LOSES ELECTRICAL POWER
ALARM CLOCK FAILS
0.016
0.012
0.0001

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

Estimating the Probability of Alarm Failing to Ring

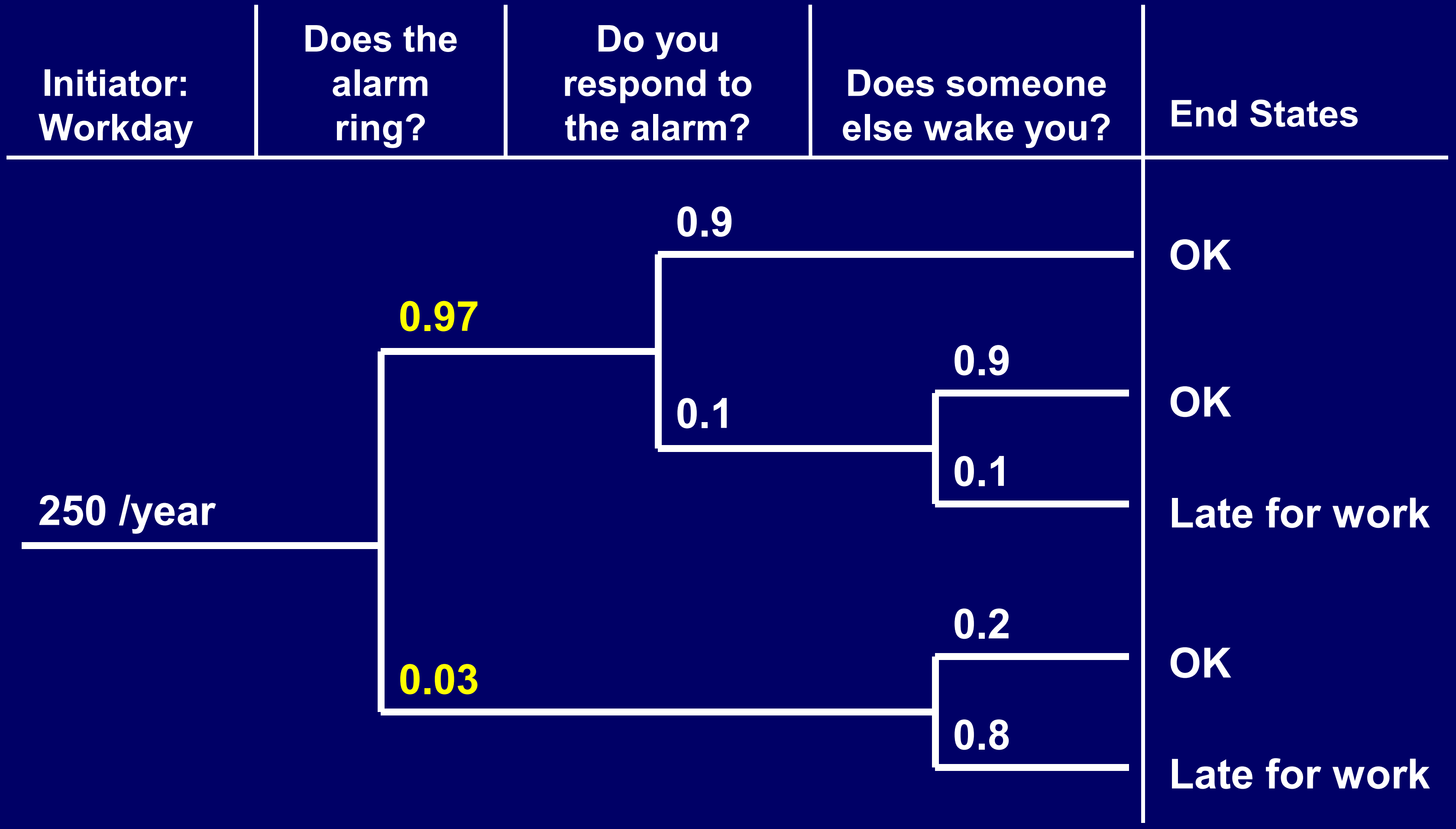

ALARM FAILS TO RING
0.03
ALARM SET INCORRECTLY OR NOT SET
0.016
HOUSE LOSES ELECTRICAL POWER
0.012
ALARM CLOCK FAILS
0.0001

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



Initiator: Workday

Does the alarm ring?

Do you respond to the alarm?

Does someone else wake you?

End States

250 /year

0.97

0.9

OK

0.1

0.9

OK

0.1

Late for work

0.03

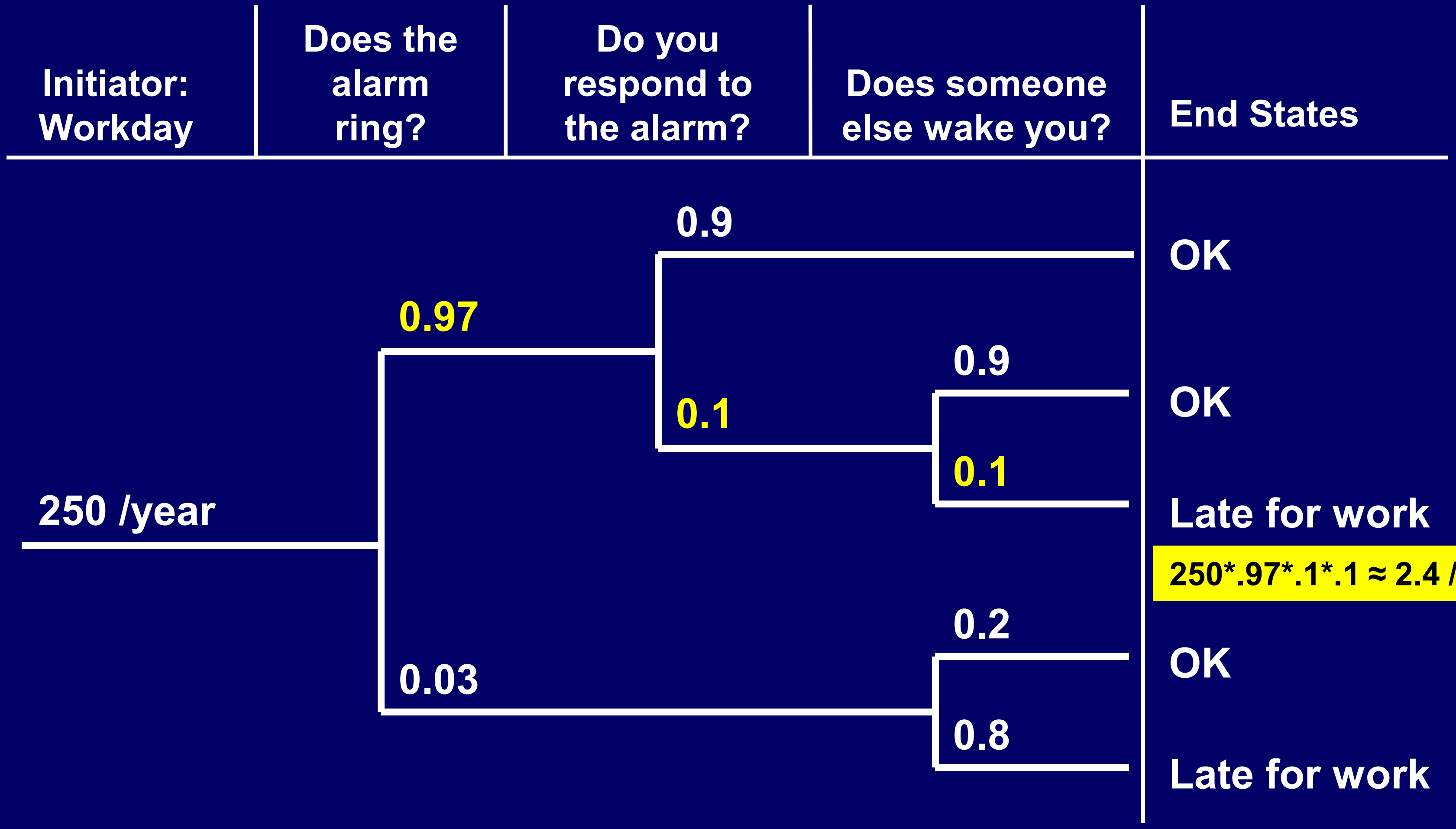
0.2

OK

0.8

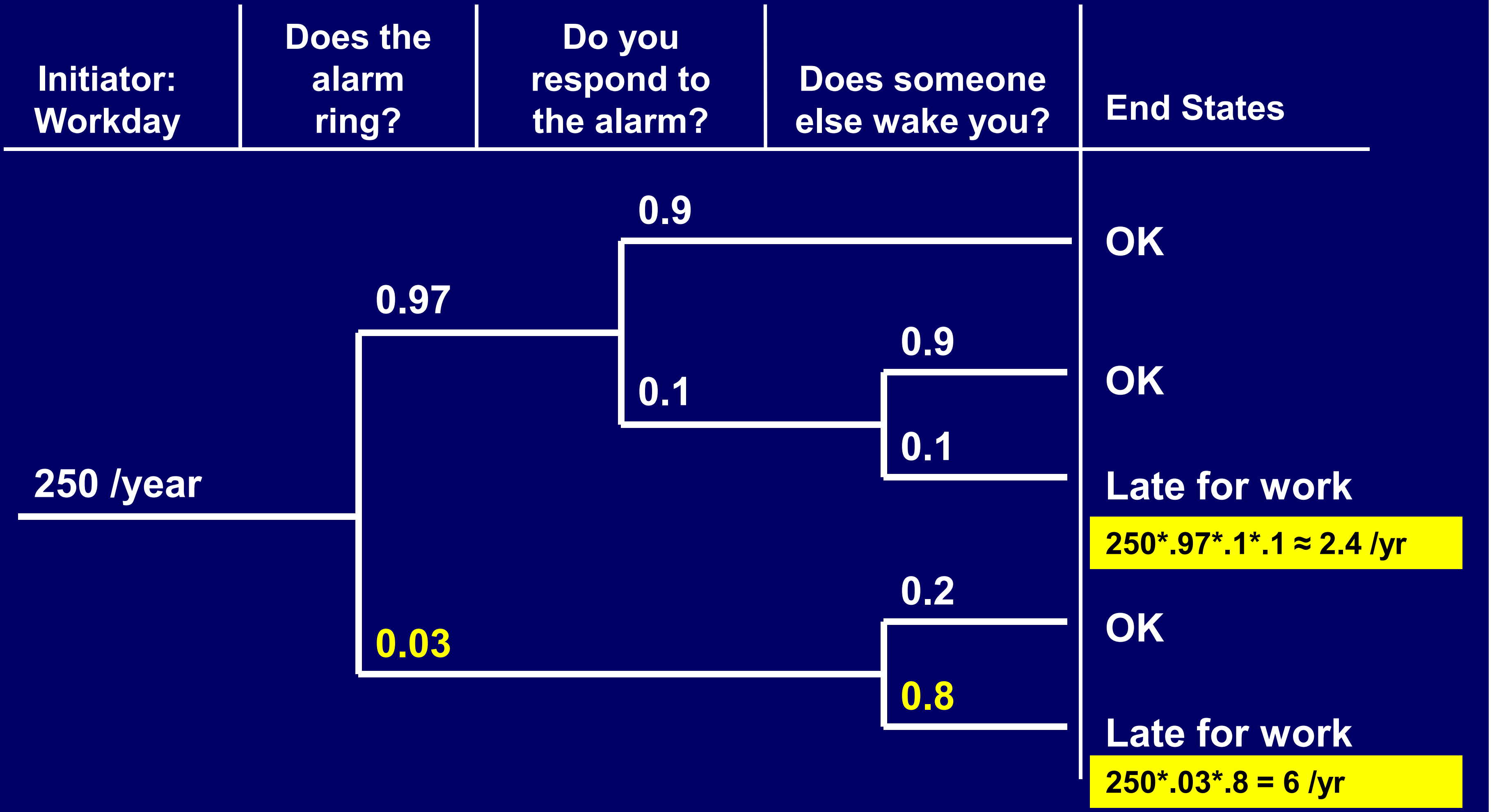
Late for work

Estimating the Frequency of Oversleeping



250*.97*.1*.1 ≈ 2.4 /yr

Estimating the Frequency of Oversleeping



Initiator: Workday

Does the alarm ring?

Do you respond to the alarm?

Does someone else wake you?

End States

250 /year

0.97

0.9

OK

0.1

0.9

OK

0.1

Late for work

250*.97*.1*.1 ≈ 2.4 /yr

0.03

0.2

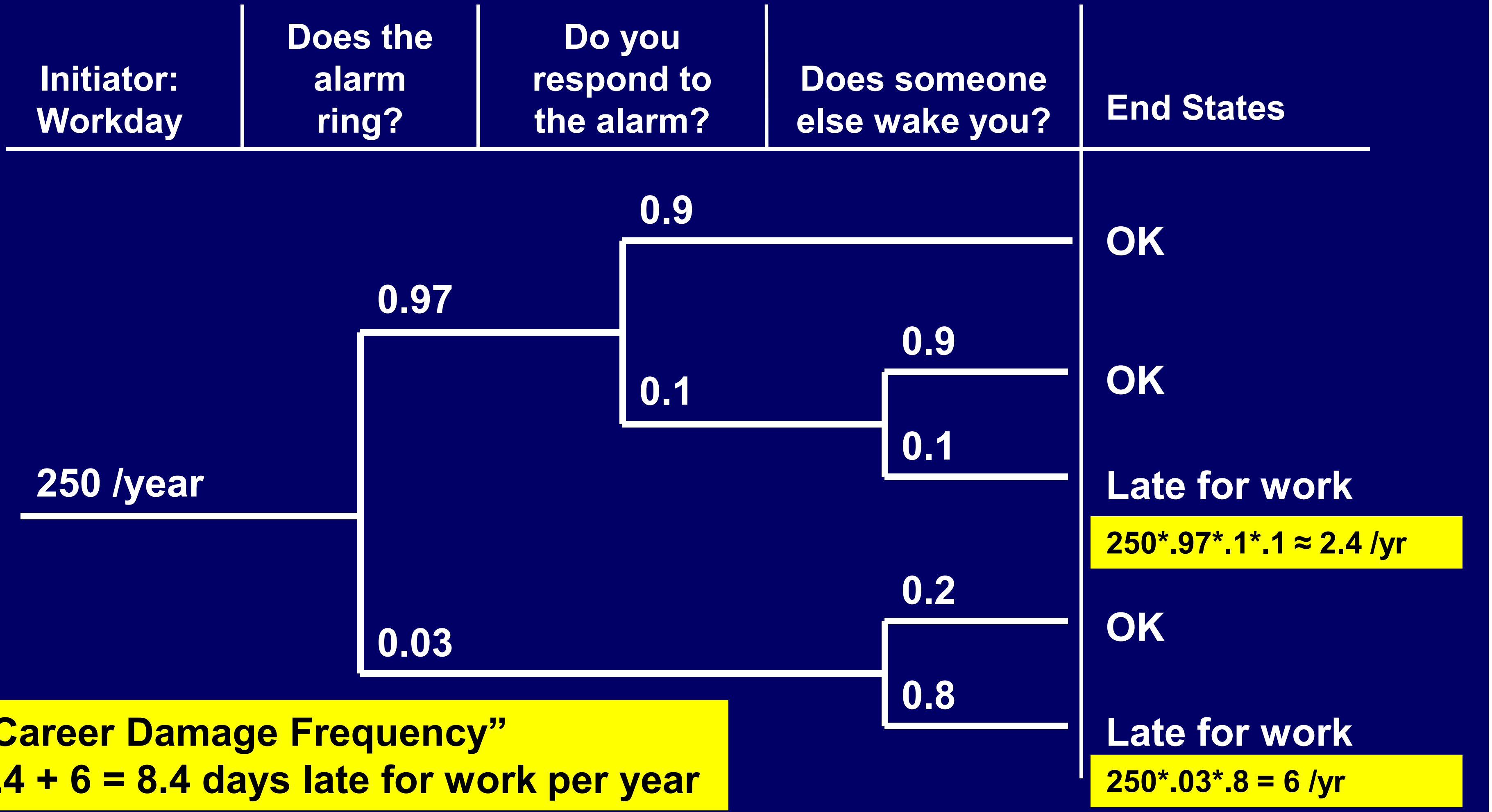
OK

0.8

Late for work

250*.03*.8 = 6 /yr

Estimating the Frequency of Oversleeping



Initiator: Workday

Does the alarm ring?

Do you respond to the alarm?

Does someone else wake you?

End States

250 /year

0.97

0.9

OK

0.1

0.9

OK

0.1

Late for work

250*.97*.1*.1 ≈ 2.4 /yr

0.03

0.2

OK

0.8

Late for work

250*.03*.8 = 6 /yr

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

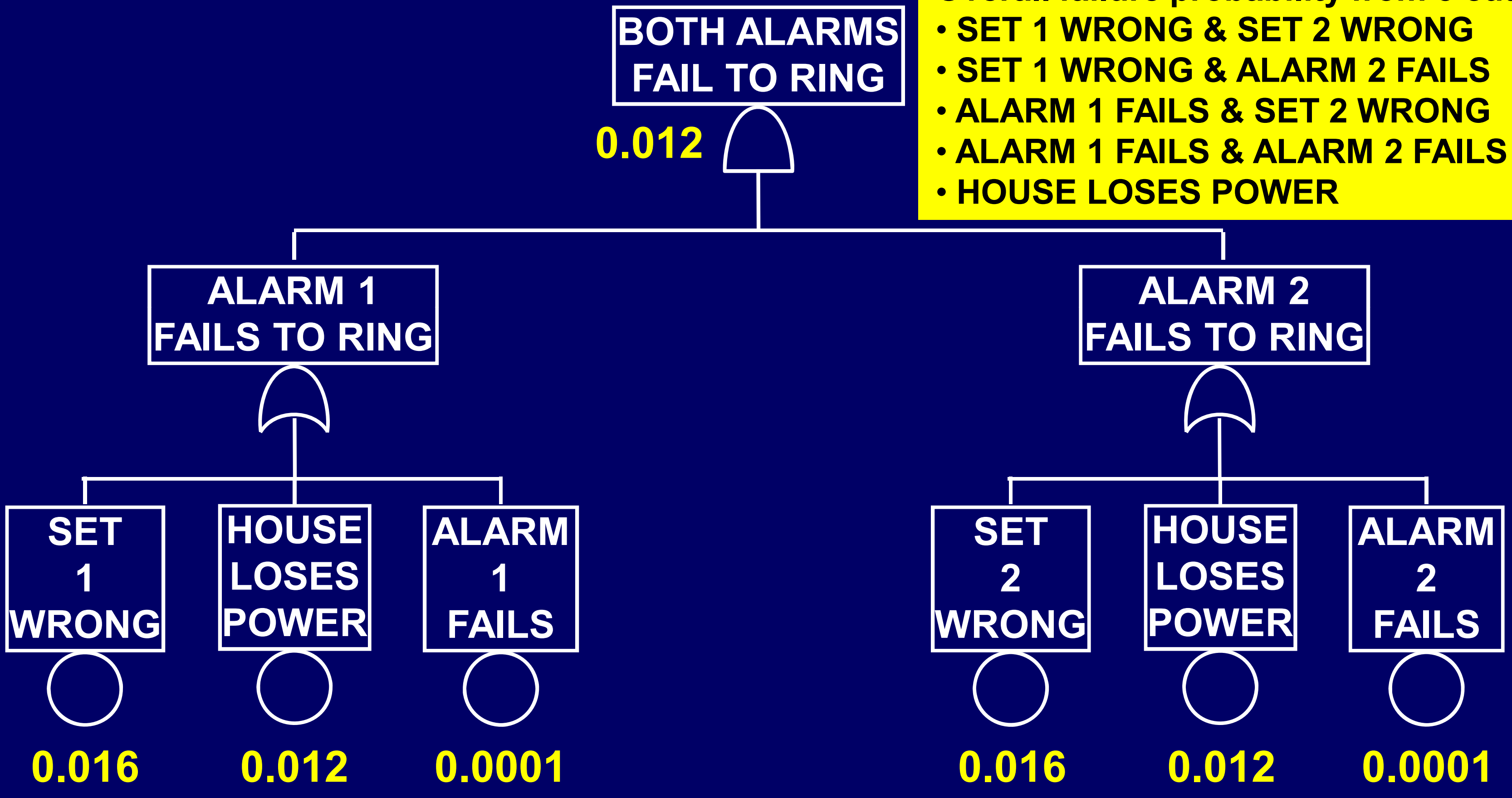
What if we improve the design?

- **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)

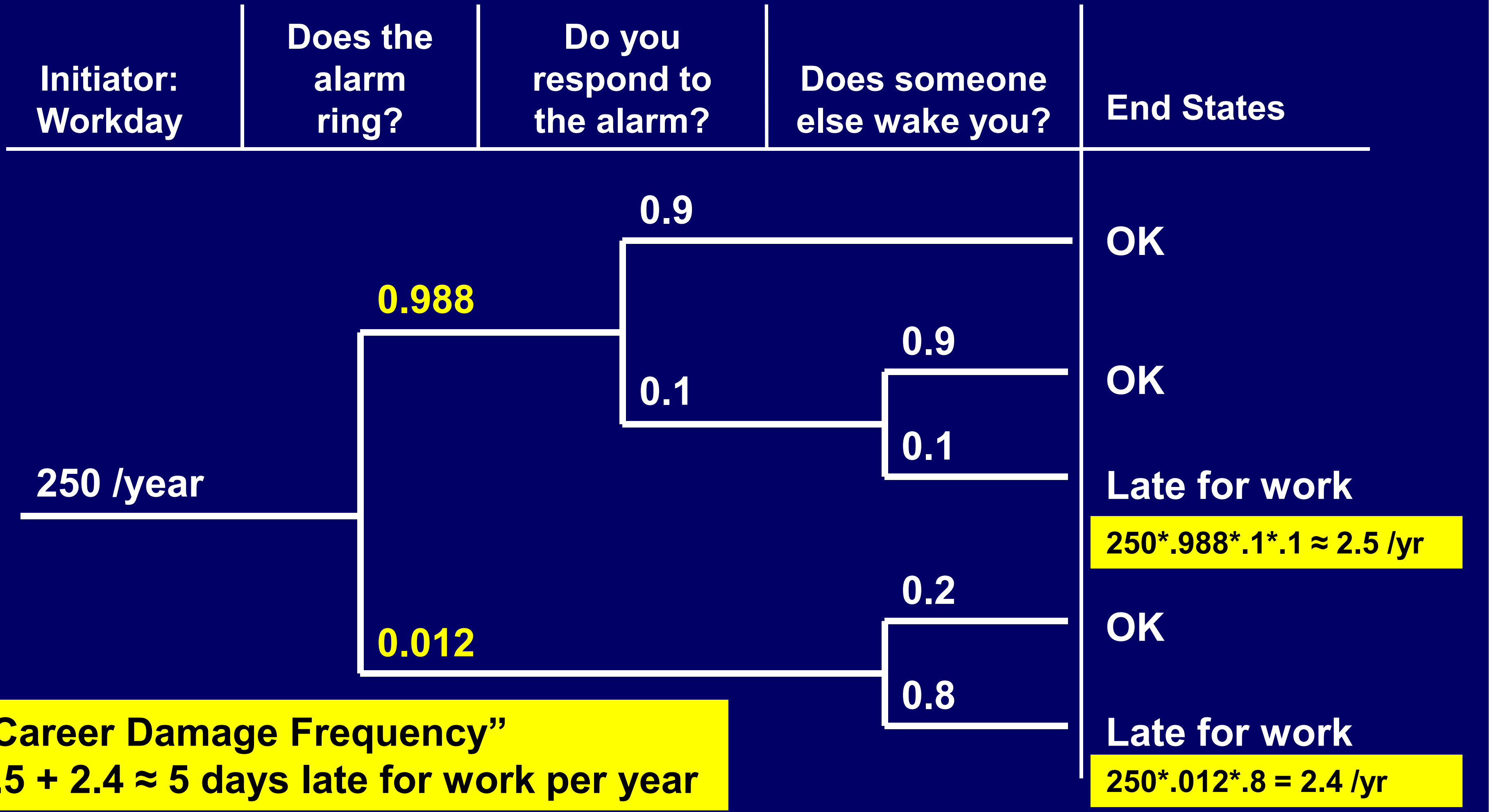
Estimating the Probability of 2 Alarms Failing to Ring

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)



250*.988*.1*.1 ≈ 2.5 /yr

250*.012*.8 = 2.4 /yr

"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!**

How do we use PRA in risk-informed regulation?

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

How do we use PRA in risk-informed regulation?

- The PRA model is used to evaluate the risk implications of the subject of the decision

- Both numerical results and qualitative insights are input to an integrated risk-informed decision

- The numerical risk results are compared against acceptance guidelines or criteria

How do we use PRA in risk-informed regulation?

- **To review new reactor design and license applications:**
  - Ensure that **applicants use PRA effectively** in support of design, construction, licensing and operation of new reactors
  - Ensure **risk from new reactors is reduced** compared to operating reactors
  - Ensure that new reactors meet the **Commission's safety goals**
  - **Identify risk-informed safety insights** for new reactor designs and use them in safety reviews
  - Ensure **technical adequacy of PRAs** for new reactors by requiring the use of consensus PRA standards

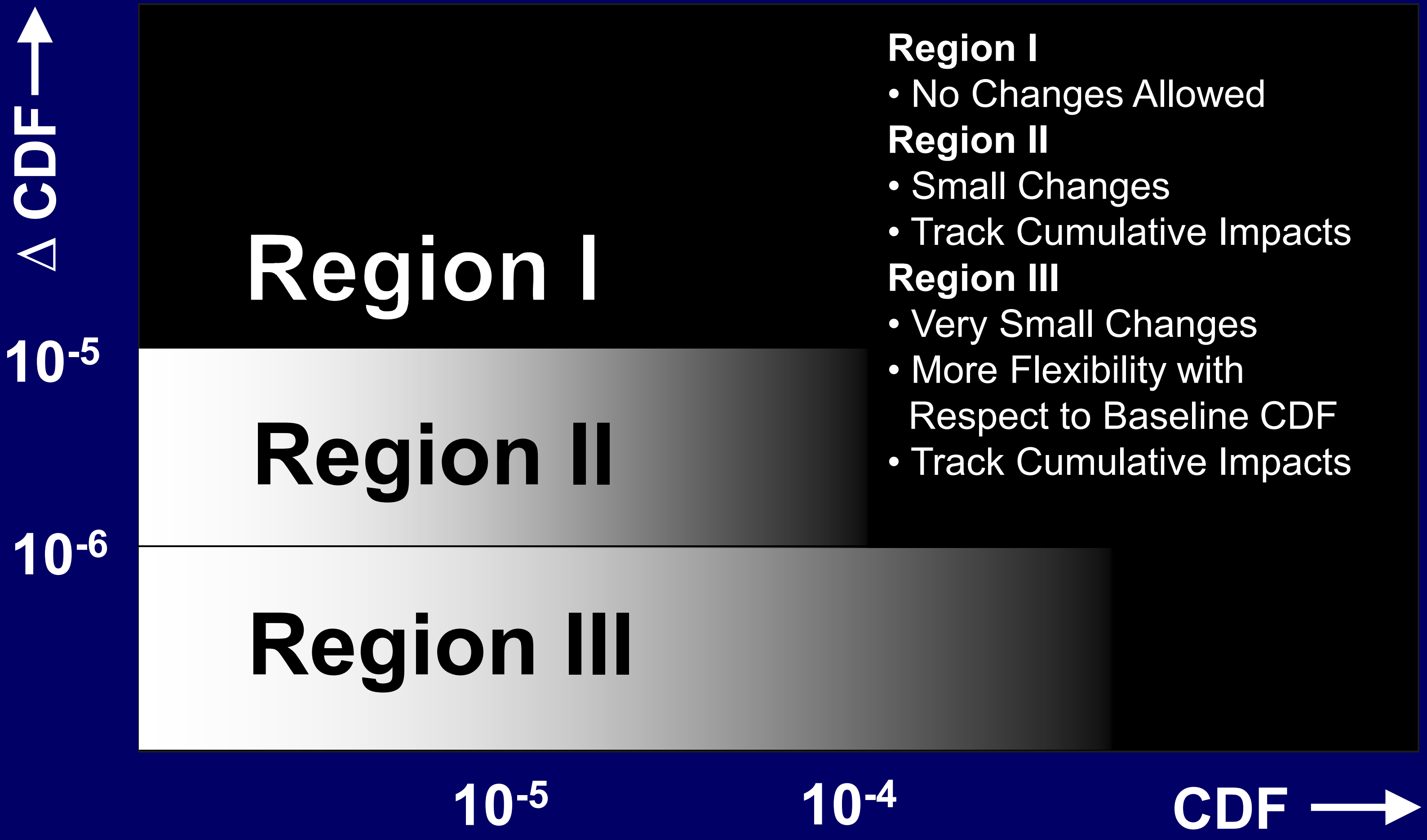
How do we use PRA in risk-informed regulation?

- **To assess the <u>risk significance of an event or condition</u>**
  - ➢ By NRC to determine an appropriate regulatory response
  - ➢ By the licensee to determine an operational response
  - – Metrics used vary depending on the nature of the event or condition
    - ➢ For a plant trip, the PRA can give a measure of the margin to core damage, conditional core damage probability (CCDP)
    - ➢ For a condition, the PRA can give a measure of the increase in CDF (SDP), or the change in core damage probability over the period of the condition
  - – Typically, the values are compared to criteria that delineate regions of risk significance

How do we use PRA in risk-informed regulation?

- **To support a risk-informed license amendment request (LAR)**
  - The risk significance of the subject of the LAR is measured against a set of **acceptance guidelines**
  - The qualitative insights concerning **where the risk is coming from** are also considered in the decision

From RG 1.174



Region I

- No Changes Allowed

Region II

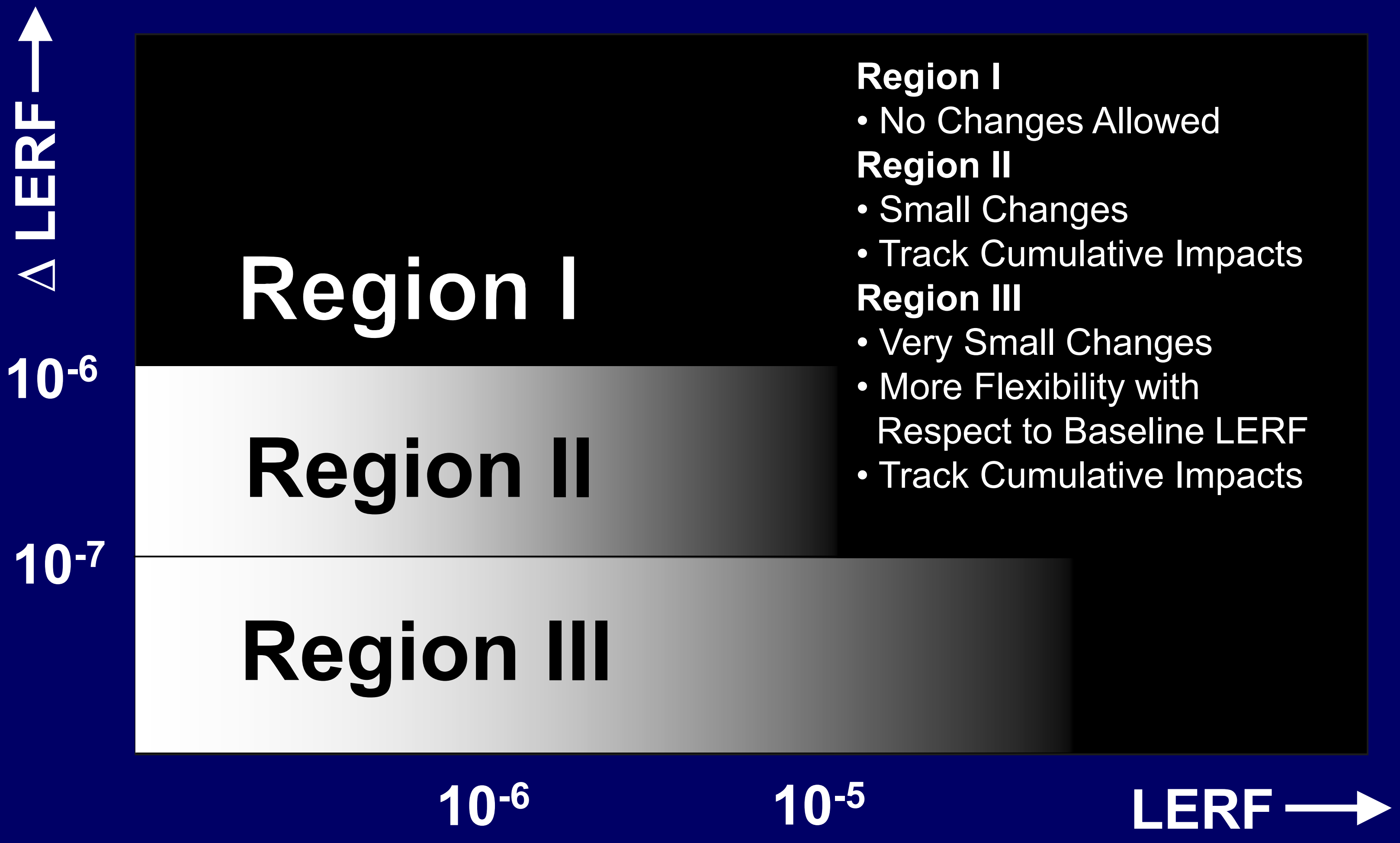
- Small Changes
- Track Cumulative Impacts

Region III

- Very Small Changes
- More Flexibility with Respect to Baseline CDF
- Track Cumulative Impacts

Figure 3. Acceptance Guidelines for Core Damage Frequency (CDF)

From RG 1.174



Region I

- No Changes Allowed

Region II

- Small Changes
- Track Cumulative Impacts

Region III

- Very Small Changes
- More Flexibility with Respect to Baseline LERF
- Track Cumulative Impacts

Figure 4. Acceptance Guidelines for Large Early Release Frequency (LERF)

How do we know a licensee's PRA is adequate?

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

What does PRA quality mean?

- In RG 1.174 and RG 1.200, PRA quality is described in terms of its:

  1. **Scope** (range of risk contributors addressed)
  2. **Technical adequacy**
  3. **Level of detail**

- The PRA must be of sufficient quality to support the application

- When the quality is considered adequate, the analyst can have confidence in the results of the PRA

1: PRA Scope

- **The assessment of risk performed to support a risk-informed application must address the following contributors to risk:**
  - All credible initiating events
    - “Internal” events like reactor trip or loss of feedwater
    - Other events (fires, floods, earthquakes, etc.) that can impact multiple systems
  - Full power, low power, and shutdown modes of operation

- **Ideally, the PRA would address all the relevant scope items**
  - When the PRA does not address the full scope, the missing scope items may be addressed by showing their **impact on the decision is not significant**
  - Another approach to addressing a limited-scope risk assessment is to **limit the applicability** of the risk-informed activity to that addressed by the risk assessment

- **The PRA must provide an assessment of the metrics used to characterize risk:**
  - CDF
  - LERF/LRF

2: PRA Technical Adequacy

- **Those elements of the PRA required for an application must be performed in a technically competent manner consistent with widely-accepted good practices**

- **Consensus Standards**
  - PRA standards and an industry peer review process can be used to demonstrate the technical adequacy of the base PRA
  - RG 1.200, An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-informed Activities, is the **NRC's vehicle for endorsing** the consensus standards
    - ➢ Only the **Level 1/LERF** standard for **internal initiating events at power** is complete and endorsed in RG 1.200
    - ➢ External events and internal fire PRA standards will be endorsed in a future revision to RG 1.200 by **December 31, 2008**

PRA Standards

- **Different in nature from other standards**
- **Two types of requirements:**
  - **Process requirements**
    - PRA maintenance and upgrade
    - Peer review
  - **Technical requirements** for each element of the PRA, e.g., initiating events, systems analysis
    - Specify "**what to do**," but not "how to do"

What does it mean to “meet the PRA standard”?

- **Process requirements must always be met**
- **Technical requirements must be met to the extent needed for the application**
- **There are different ways of meeting the technical requirements**
  - Analyses of the same plant may not be identical
    - ➢Use of different HRA model
    - ➢Different assumptions
  - Addressed through peer review and analysis of uncertainty on the results

3: PRA Level of Detail

- **Different applications require use of different PRA elements and different levels of detail**
  - Some use the complete PRA (e.g., categorization of structures, systems, and components by risk significance)
  - Others require only a portion of the PRA (e.g., a simple tech spec change)
- **If the PRA doesn't model a particular system or component, you can't justify a change to it using the PRA!**

Phased Approach to PRA Quality

- **In December 2003, the Commission issued an SRM* entitled *Stabilizing the PRA Quality Expectations and Requirements***
- **A plan developed by the staff was submitted to the Commission****
  - Defines a phased approach to achieving an appropriate quality of licensee PRAs
  - Benefits from the development of PRA standards
  - Allows **continued practical use of risk insights while progressing towards more complete and technically acceptable PRAs**

**** SRM on COMNJD-03-0002, 12/18/03***

***** SECY-04-0118, 7/13/04***

Phased Approach to PRA Quality (cont.)

- **Once the NRC has endorsed a PRA standard, assessments of the risk contributor covered by the standard must be performed using a PRA if that contributor is significant to the application under consideration**
  - For example, once the fire PRA standard is endorsed, a screening approach is not acceptable if fire risk is important to the application
- **Applications not meeting endorsed standards will be given low priority or not accepted**
  - Acceptance review and prioritization process to be included in NRR Office Instruction LIC-101

Staff Review of PRAs

- **Currently, a review of the base PRA (the entire model) is required when a submittal is based on a PRA that has not been shown to meet the applicable standards**
  - Focus is on those areas of the PRA relevant to the application

- **When the base PRA complies with the standard as endorsed in RG 1.200, no review of the base PRA will be necessary**

- **However, the staff will always examine the modifications to the PRA that are made to support an application**

- **The staff will also confirm that appropriate changes are made to address an emergent issue not included in the original PRA**

What is uncertainty?

- **Aleatory uncertainty**
  - “Randomness,” i.e., nature is unpredictable
  - Such events are modeled as being probabilistic
    - ➢ For example, PRAs model initiating events as a Poisson process with a frequency λ
  - A PRA model is a model of aleatory processes
- **Epistemic uncertainty**
  - “State of knowledge” uncertainty
    - ➢ For example, initiating event frequencies are not known precisely, so PRAs model lack of knowledge about the value of λ by assigning a probability distribution to λ
  - Leads to uncertainty about the results of the PRA model

How do we analyze epistemic uncertainty?

- **Identify sources of uncertainty**
- **Characterize the impact on the PRA model**
  - Parameter uncertainty
    - ➢ Initiating event frequencies
    - ➢ Component failure probabilities
    - ➢ Human error probabilities
  - Model uncertainty, e.g.:
    - ➢ Success criteria
    - ➢ Reactor coolant pump seal LOCA model
  - Completeness
    - ➢ Things not modeled, e.g., operator error of commission
- **Assess the impact of uncertainties on the results**

Examples of Epistemic Uncertainty

- **Parameter uncertainty**
  - Statistical uncertainty associated with parameter estimates based on experience data for active components (pumps, valves) and frequent events (e.g., loss of main feedwater)
  - Uncertainty in estimates of probabilities for rare events (e.g., large loss-of-coolant accident), passive failures (tank collapse), and human errors for which data is sparse or non-existent
- **Model uncertainty (inadequate or incomplete understanding)**
  - Physical processes not fully understood (e.g., chemical effects on containment sump screen clogging)
  - Untested performance (e.g., injection into BWR reactor vessel after containment overpressure)

Examples of Epistemic Uncertainty

- **Completeness**
  - Things knowingly left out of the model
    - Modeling of human errors of commission
    - Exclusion of equipment from model
    - External initiating events
  - Things we don’t know
    - New failure modes (e.g., degradation mechanisms, digital I&C failure mode)
    - Unknown, but potentially important effects
- **Impact of resource constraints (not so much a source of uncertainty, as a source of bias)**
  - Simplifying assumptions in model to save effort
  - Excessive truncation of results during quantification to save time

Treatment of Epistemic Uncertainty

- **Parameter uncertainty can be dealt with analytically**
  - Use **probability distributions** to characterize the level of confidence in the numerical estimates of parameters, e.g., the 95th percentile of the distribution represents a 95% confidence level on the result
  - Uncertainty on input parameters can be propagated to give a probability distribution on the numerical results (e.g., CDF)
  - A range of 10 (5th to 95th percentile) on CDF is typical; LERF uncertainty even greater

- **Model uncertainty is typically addressed by making assumptions**
  - Its impact is analyzed by performing **sensitivity analyses** to assess potential impact of alternate, credible assumptions (e.g., alternate common-cause model or human reliability analysis model)
  - Bounding analyses can be used where overall results are not measurably impacted or skewed

- **Assumptions or approximations can be made for convenience**
  - The impact on the results is assessed, and the PRA model may be refined as necessary to support a specific application

Treatment of Uncertainty (Cont.)

- **Completeness uncertainty cannot be quantitatively assessed**
  - **Known unknowns** dealt with in a number of ways, including:
    - ➢ **Limiting the scope of implementation** of the application
    - ➢ Demonstrating that the missing issues do not affect the application
  - **Unknown unknowns** addressed through the other key principles of risk-informed regulation,
    - ➢ Defense in depth
    - ➢ Safety margins
    - ➢ Performance monitoring
  - Again, we’re not risk-based!

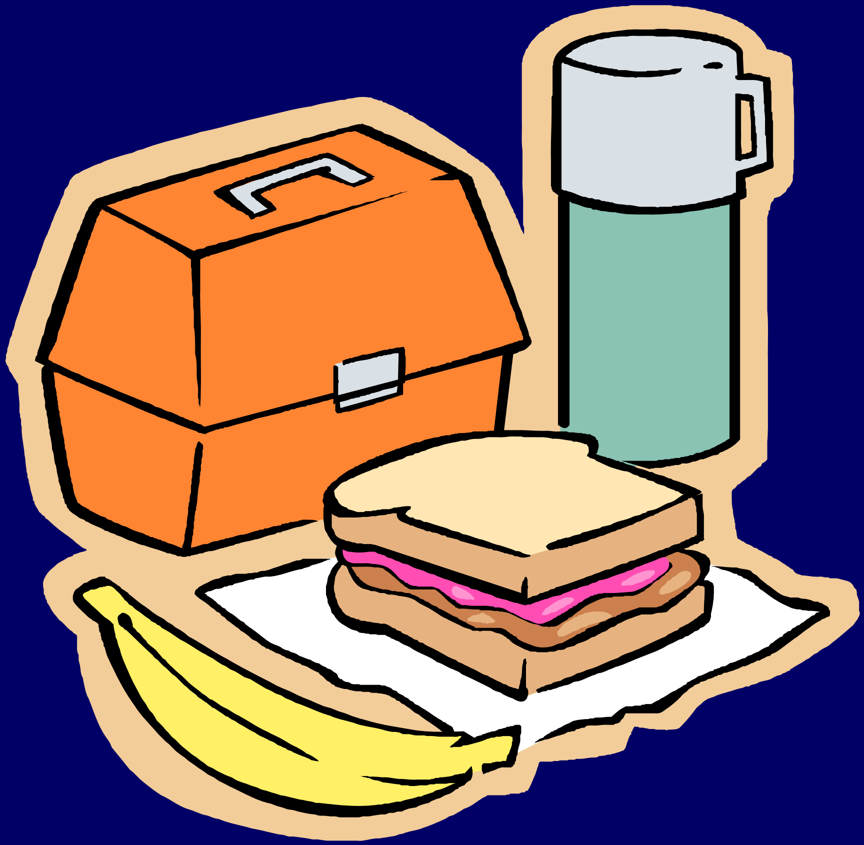
How do we make decisions given the uncertainty?

- **The results obtained from the PRA are compared with acceptance criteria relevant to the application**

- **Acceptability of the risk associated with the application takes into account the uncertainties in the results of the risk analysis**

- **The uncertainty analysis provides the decision-maker with confidence in the assessment of the risk input**

- **Managers should be provided with:**
  - Risk metrics expressed as the mean of a distribution, where possible
  - A discussion of key assumptions and sensitivity studies performed
  - Information on defense in depth, safety margins, and performance monitoring, as applicable



Review & Discussion

- **What did we learn this morning?**
  - Define **basic terms** related to risk-informed regulation
    - ➢ Risk – What can go wrong? How likely is it? What are the consequences
    - ➢ Risk-informed regulation – traditional and risk analyses used together to focus on most safety-significant areas
  - Identify **how your work fits into** a risk-informed regulatory structure
    - ➢ Risk-informed applications in rulemaking, licensing, oversight, and operating experience
  - Understand the **basic modeling concepts** in a probabilistic risk assessment
    - ➢ Logical event trees and fault trees
    - ➢ Based on engineering analyses, plant procedures, etc.

Review & Discussion

- **Thinking of the examples we discussed earlier…**
  - How could risk information **help you** do your job?
  - **Are** any aspects of your current job or reviews “risk-informed”?
  - **Could** any aspects of your current job or reviews be “risk-informed”?

Course Modules

1. **Introduction to Risk-Informed Regulation**
   - What do risk and risk-informed regulation mean?
   - Where do we use risk-informed approaches?
   - How do you fit in to risk-informed regulation?

2. **Use of PRA Models**
   - How do we build PRA models?
   - How do we use PRA in risk-informed regulation?
   - How do we know a licensee’s PRA is adequate?
   - What can we learn from PRA results?

3. **Supporting Risk-Informed Decisions**
   - What guidance do we use?
   - What are some examples?
   - How can risk communication help?

4. **Resources**
   - Where can you get more information?

What can we learn from PRA results?

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

What can we learn from PRA results?

- **A quantitative assessment of risk impact**

- **The significant contributors to the risk measures being used, in terms of, for example:**
  - Accident sequences
  - Cutsets
  - Significant basic events

- **A number of tools are available to extract these results and characterize their significance and the confidence we can have in them:**
  - Importance analyses
  - Uncertainty analysis
  - Sensitivity analyses

- **Qualitative insights about plant vulnerabilities**

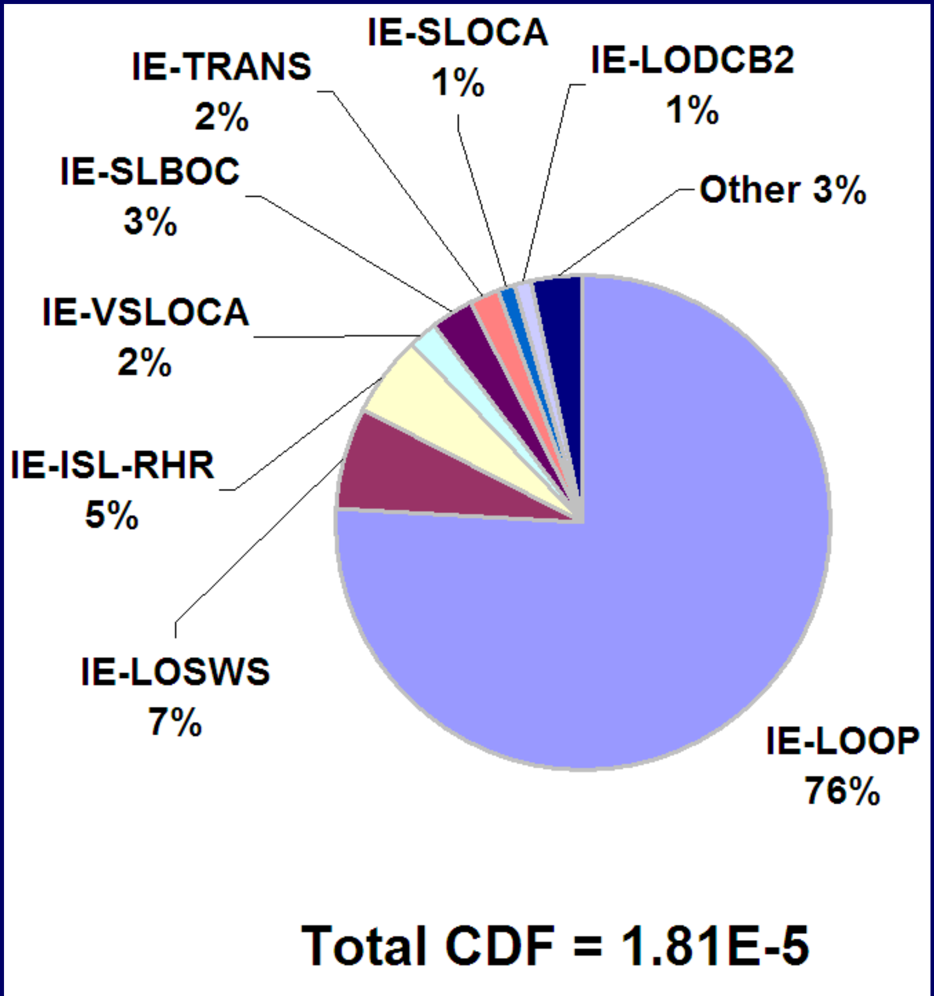
Quantitative PRA Results: Core Damage

- **Core Damage Frequency (CDF)**
  - What is the **frequency** (on a per-year basis) that an **initiating event** and subsequent **mitigating system failures** that lead to **core damage** will occur?
- **Change in CDF (ΔCDF)**
  - Given a component **failure or longer maintenance** time that **increases the probability of a mitigating system failure**, how much does the **overall CDF** increase?
- **Core Damage Probability (CDP)**
  - What is the probability that core damage will occur during a **given period**?
- **Conditional Core Damage Probability (CCDP)**
  - Given that an **initiating event occurs**, what is the probability that a combination of system **failures leading to core damage** will occur?
  - Given a component **failure or maintenance** that lasts a certain duration, what is the probability that **both an initiating event and subsequent mitigating system failures that lead to core damage** will occur during that time period?
- **Incremental Conditional Core Damage Probability (ICCDP)**
  - How much higher is the **CCDP during a component failure or maintenance** compared to the **average CDP** over the same time period?

Quantitative PRA Results: Large Early Release Frequency

- **Large Early Release Frequency (LERF)**
  - What is the **frequency** (on a per-year basis) that a core damage accident with a **large radioactive release before there is time to evacuate** will occur?
- **Change in LERF (ΔLERF)**
  - Given a component **failure or longer maintenance** time that **increases the probability of a mitigating system failure**, how much does the **overall LERF** increase?
- **Large Early Release Probability (LERP)**
  - What is the probability that core damage and large early release will occur during a **given period**?
- **Conditional Large Early Release Probability (CLERP)**
  - Given that an **initiating event occurs**, what is the probability that a combination of system **failures leading to large early release** will occur?
  - Given a component **failure or maintenance** that lasts a certain duration, what is the probability that **an initiating event and subsequent mitigating system failures leading to large early release** will occur during that period?
- **Incremental Conditional Large Early Release Probability (ICLERP)**
  - How much higher is the **CLERP during a component failure or maintenance** compared to the **average CLERP** over the same time period?

Core Damage Contribution by Initiating Event*



LOOP:	Loss of Offsite Power
LOSWS:	Loss of Service Water
ISL-RHR:	Intersystem LOCA - RHR
VSLOCA:	Very Small LOCA
SLBOC:	Steam Line Break
TRANS:	General Transient
SLOCA:	Small LOCA
LODCB2:	Loss of DC Bus 1EB2
Other:	All Other Initiating Events

*** Comanche Peak SPAR version 3.31***

Importance Measures

- **Provide insight into impact of basic events on overall risk**

- **Generally two types:**

  1. Risk decrease measures
     - How much the overall **risk would decrease** if the associated SSC were **less likely to fail**
     - Fussell-Vesely (FV)

  2. Risk increase measures
     - How much the overall **risk would increase** if the associated SSC were **certain to fail**
     - Risk Achievement Worth (RAW)

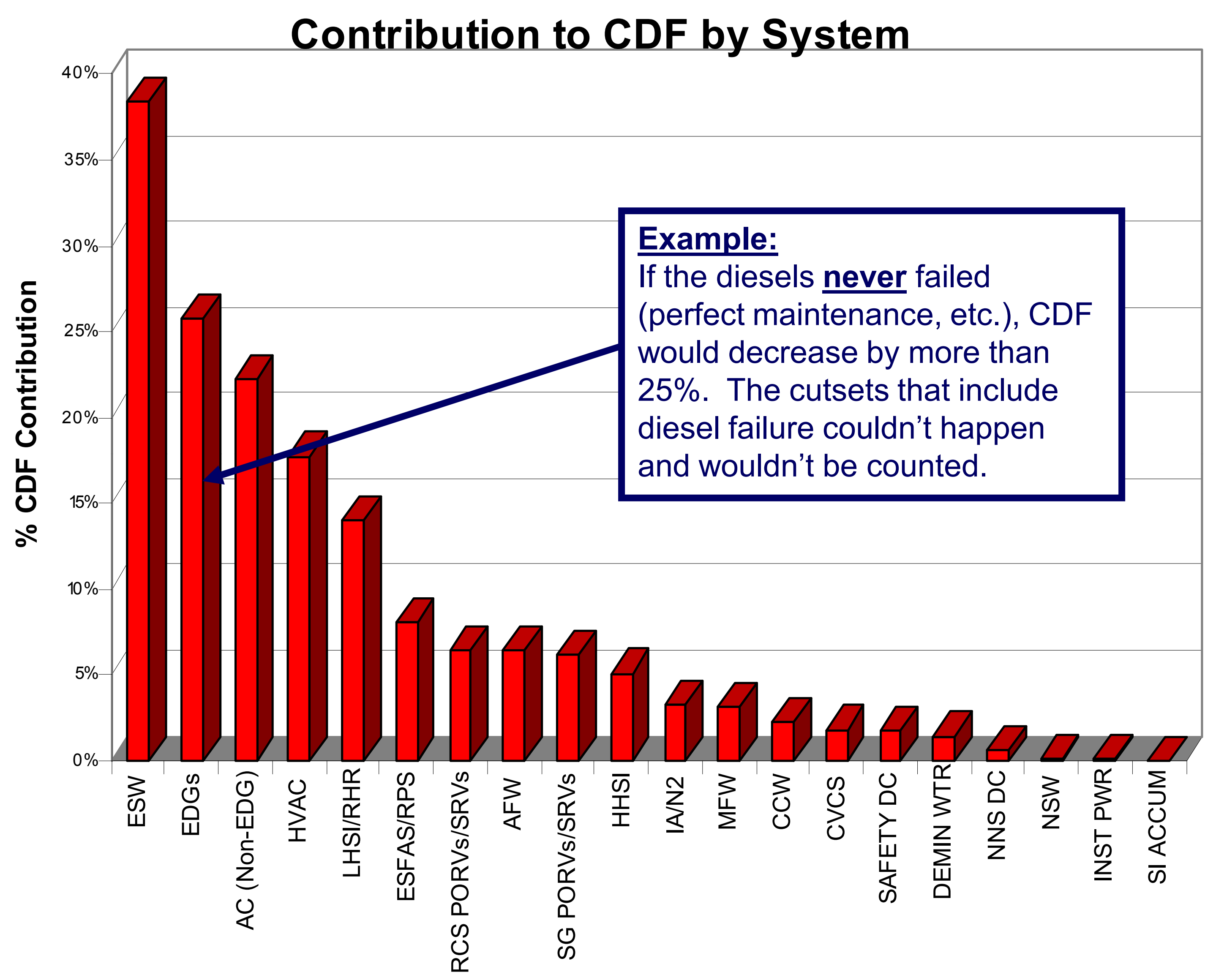
Fussell-Vesely (FV)

- **Answers the questions:**
  - What is driving **current risk**?
  - What **fraction of the total risk comes from cutsets that include a particular component**?
  - If a component were **less likely to fail** (better maintenance, etc.), would that **decrease risk a lot or a little**? (i.e., is it worth the effort?)

- **We use it to:**
  - Focus on **key initiating events, equipment, operator actions, and procedures**
  - Help decide what to inspect

- **A component needs more attention when:**
  - FV is greater than **0.005** (i.e., that event appears in cutsets that contribute to ½% of the risk)

System Contribution to CDF (FV)



Example:
If the diesels **never** failed (perfect maintenance, etc.), CDF would decrease by more than 25%. The cutsets that include diesel failure couldn't happen and wouldn't be counted.

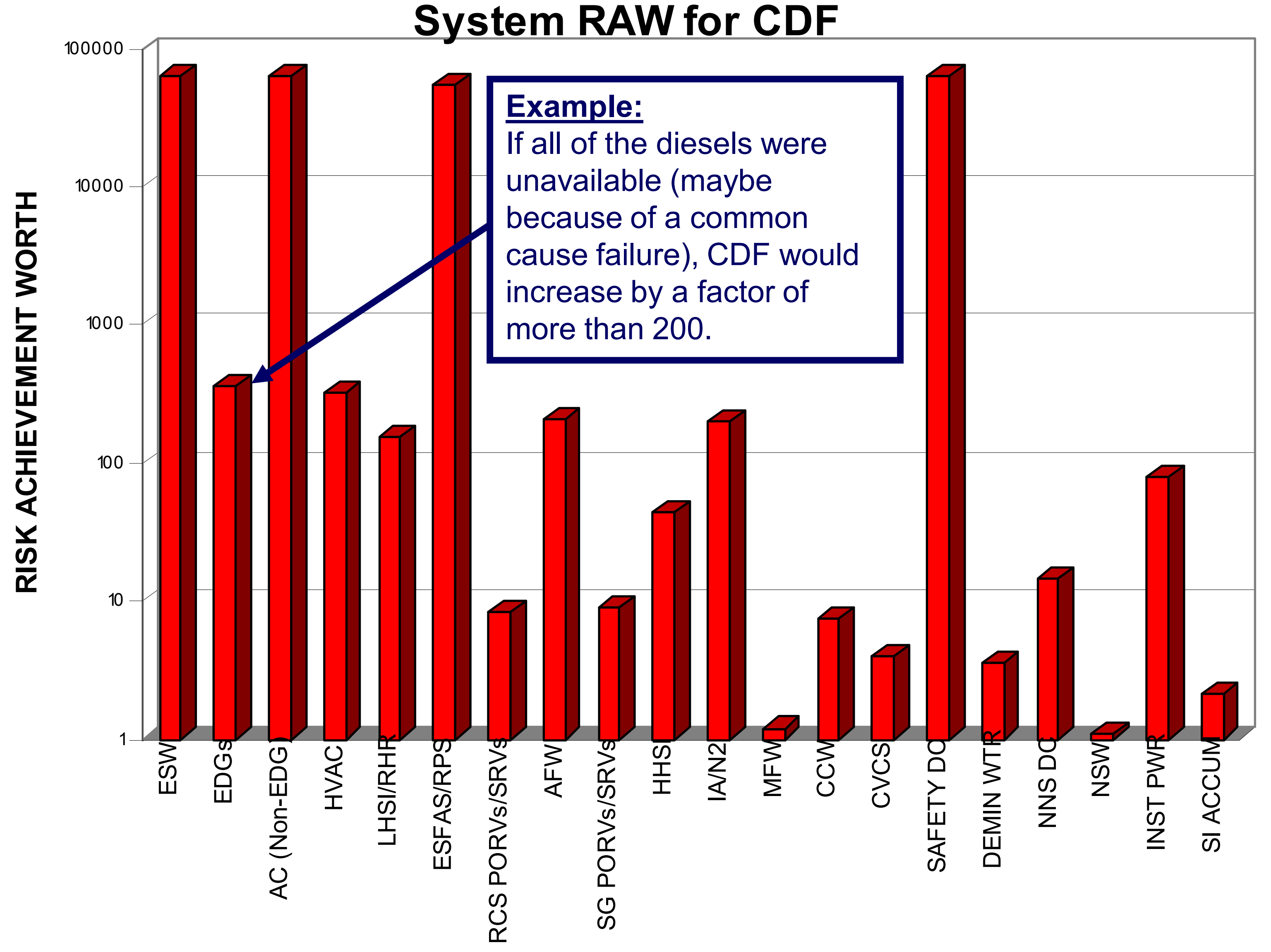
Risk Achievement Worth (RAW)

- **Answers the questions:**
  - If this **component were broken or unavailable**, would that **increase risk a lot or a little**?
  - How important is a component to **maintaining the current level of risk**?

- **We use it to:**
  - Help determine the **significance of inspection findings**
  - **Prioritize systems** to review
  - Identify equipment that needs **special controls** to keep it operational

- **A component is treated differently when:**
  - RAW is greater than **2** (i.e., risk doubles without that component)

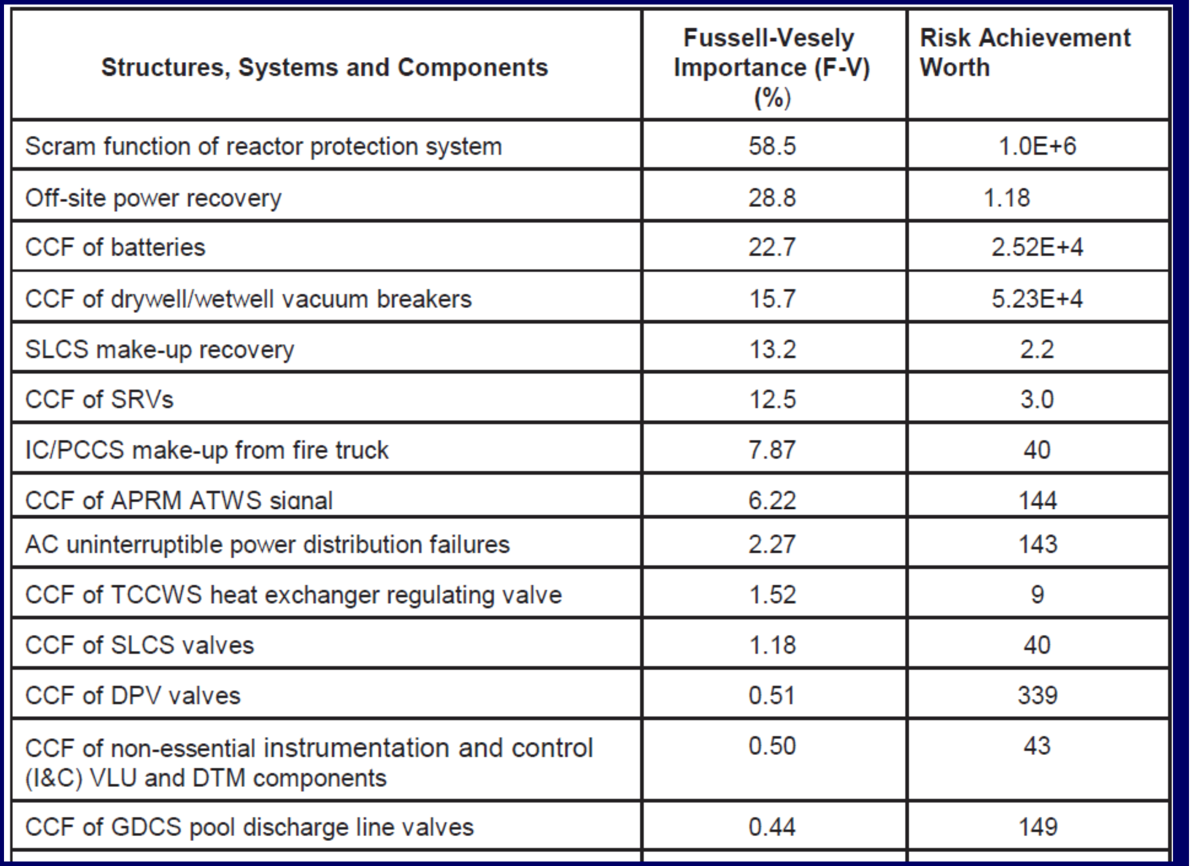
System Importance to CDF (RAW)



Example:
If all of the diesels were unavailable (maybe because of a common cause failure), CDF would increase by a factor of more than 200.

Importance Measures Example: ESBWR

- **Memo from PRA group to ESBWR design certification reviewers***
  - RAW → design features and assumptions that contribute to the “low risk” of the design (may need **extra requirements and maintenance**)
  - FV → areas where design and operational **changes could improve safety**
- **Similar insights to be developed for other new designs****

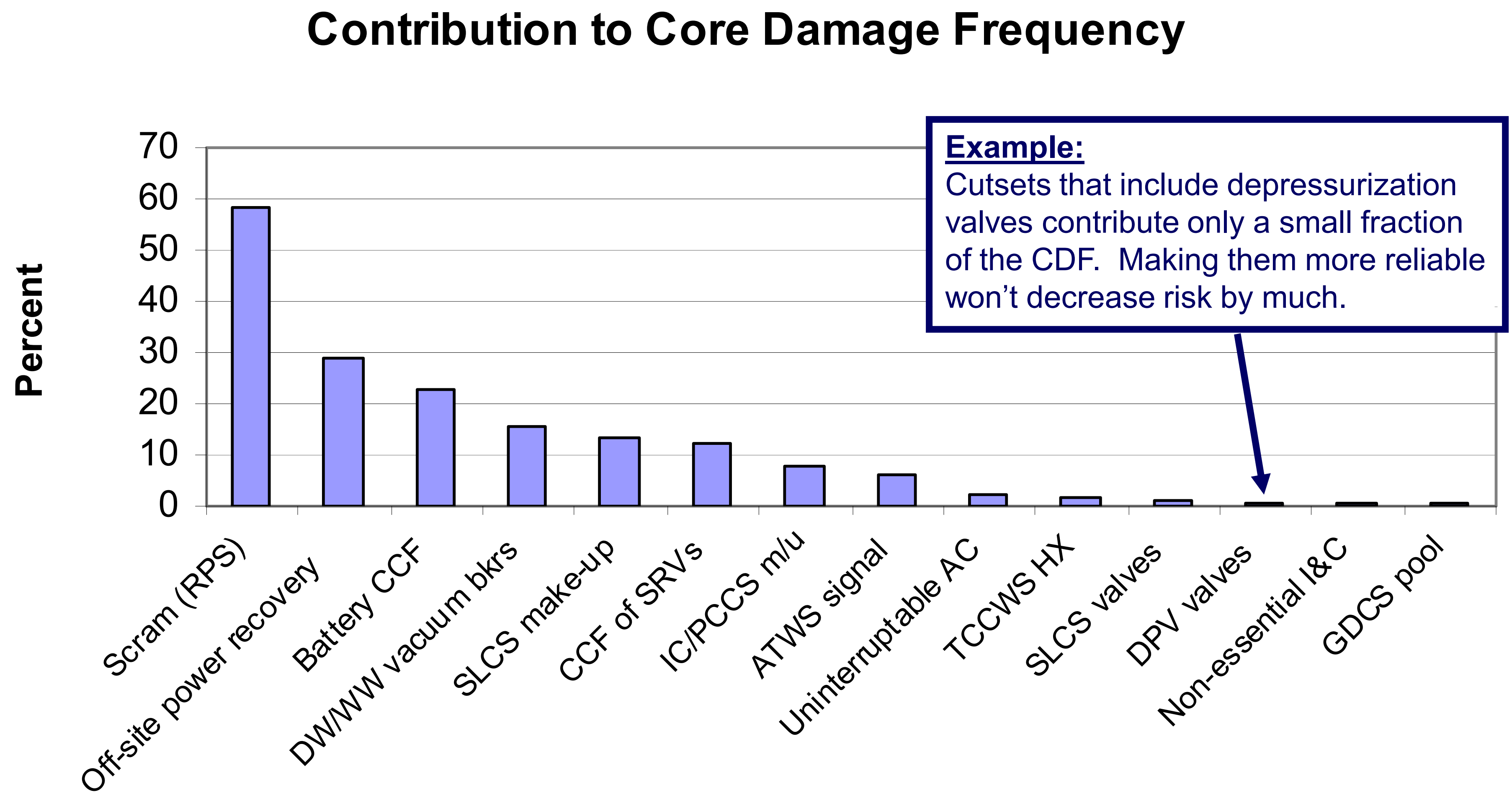


Structures, Systems and Components	Fussell-Vesely Importance (F-V) (%)	Risk Achievement Worth
Scram function of reactor protection system	58.5	1.0E+6
Off-site power recovery	28.8	1.18
CCF of batteries	22.7	2.52E+4
CCF of drywell/wetwell vacuum breakers	15.7	5.23E+4
SLCS make-up recovery	13.2	2.2
CCF of SRVs	12.5	3.0
IC/PCCS make-up from fire truck	7.87	40
CCF of APRM ATWS signal	6.22	144
AC uninterruptible power distribution failures	2.27	143
CCF of TCCWS heat exchanger regulating valve	1.52	9
CCF of SLCS valves	1.18	40
CCF of DPV valves	0.51	339
CCF of non-essential instrumentation and control (I&C) VLU and DTM components	0.50	43
CCF of GDCS pool discharge line valves	0.44	149

*** ML061040127**

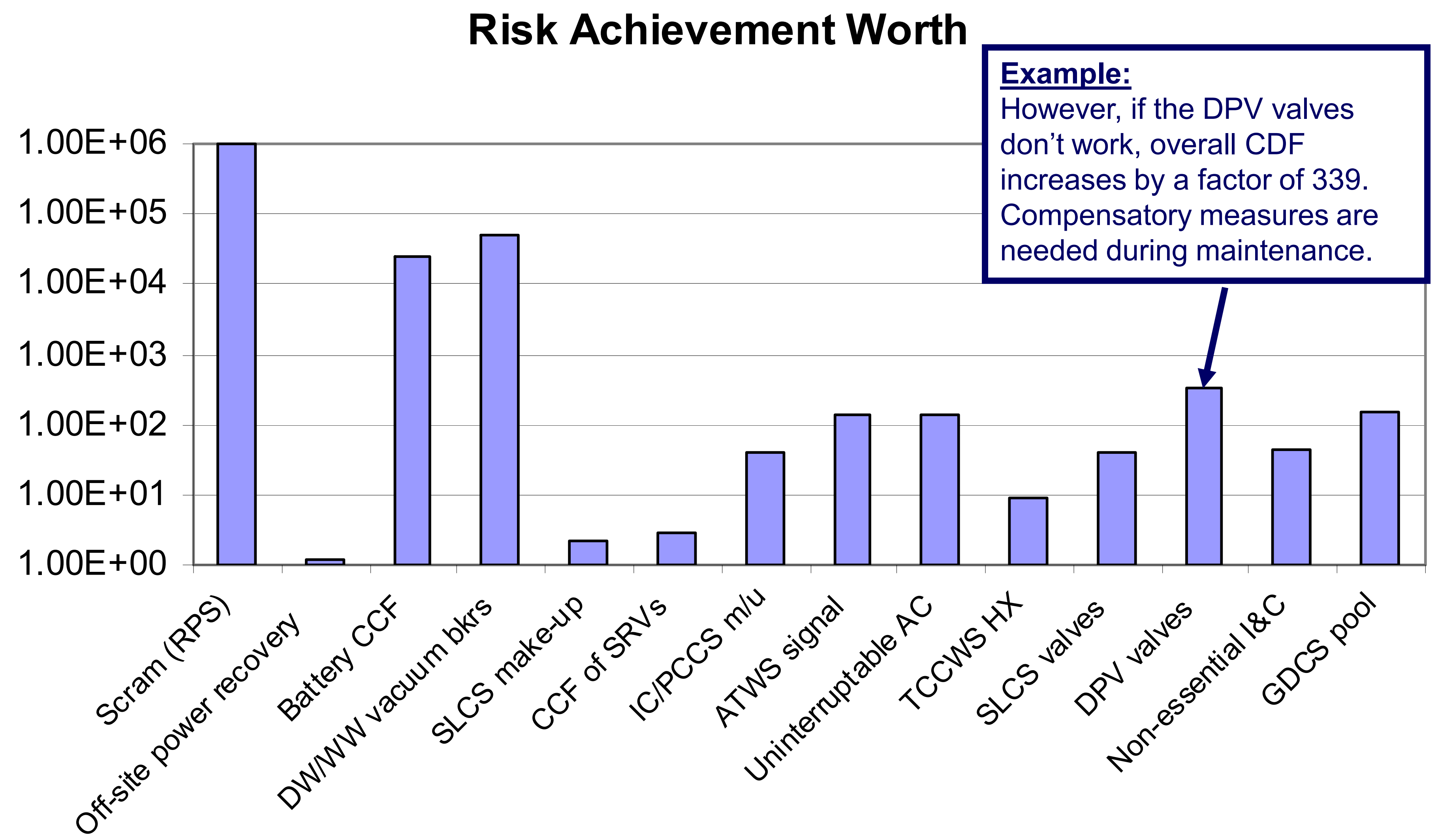
**** ML072040352**

System Contribution to CDF (Fussell-Vesely)



Example:
Cutsets that include depressurization valves contribute only a small fraction of the CDF. Making them more reliable won't decrease risk by much.

System Importance to CDF (RAW)


Risk Achievement Worth

Example:
However, if the DPV valves don’t work, overall CDF increases by a factor of 339. Compensatory measures are needed during maintenance.

Plant Vulnerabilities

- **Key operator action or procedure appearing in many core damage sequences**
- **Safety function that needs a single piece of equipment or support system for success**
- **Degradation that could fail redundant components**
- **Unexpected and adverse system interactions**

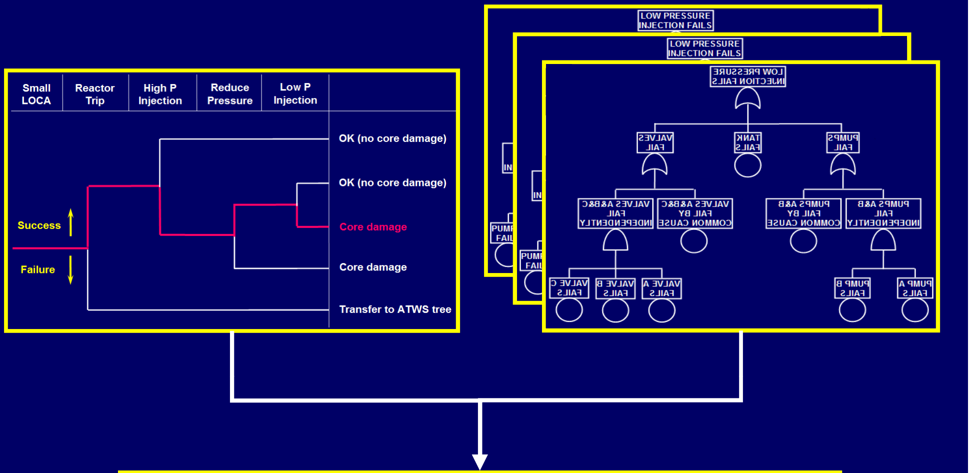
- **Next few slides: some real-life discoveries**
  - Station blackout
  - Individual Plant Examination insights
  - Seismic and fire improvements
  - AP1000 design improvements
  - Shutdown risk
  - Adverse system interactions
  - Small loss-of-coolant accident vulnerability

Cutset Analysis

- Core damage cutsets (as opposed to system cutsets) are the <u>combination of events</u> that result in core damage or large radioactive release

- A <u>measure of design robustness</u>, i.e., number of barriers to core damage or large release

- May indicate plant vulnerability or unexpected reliance on support system



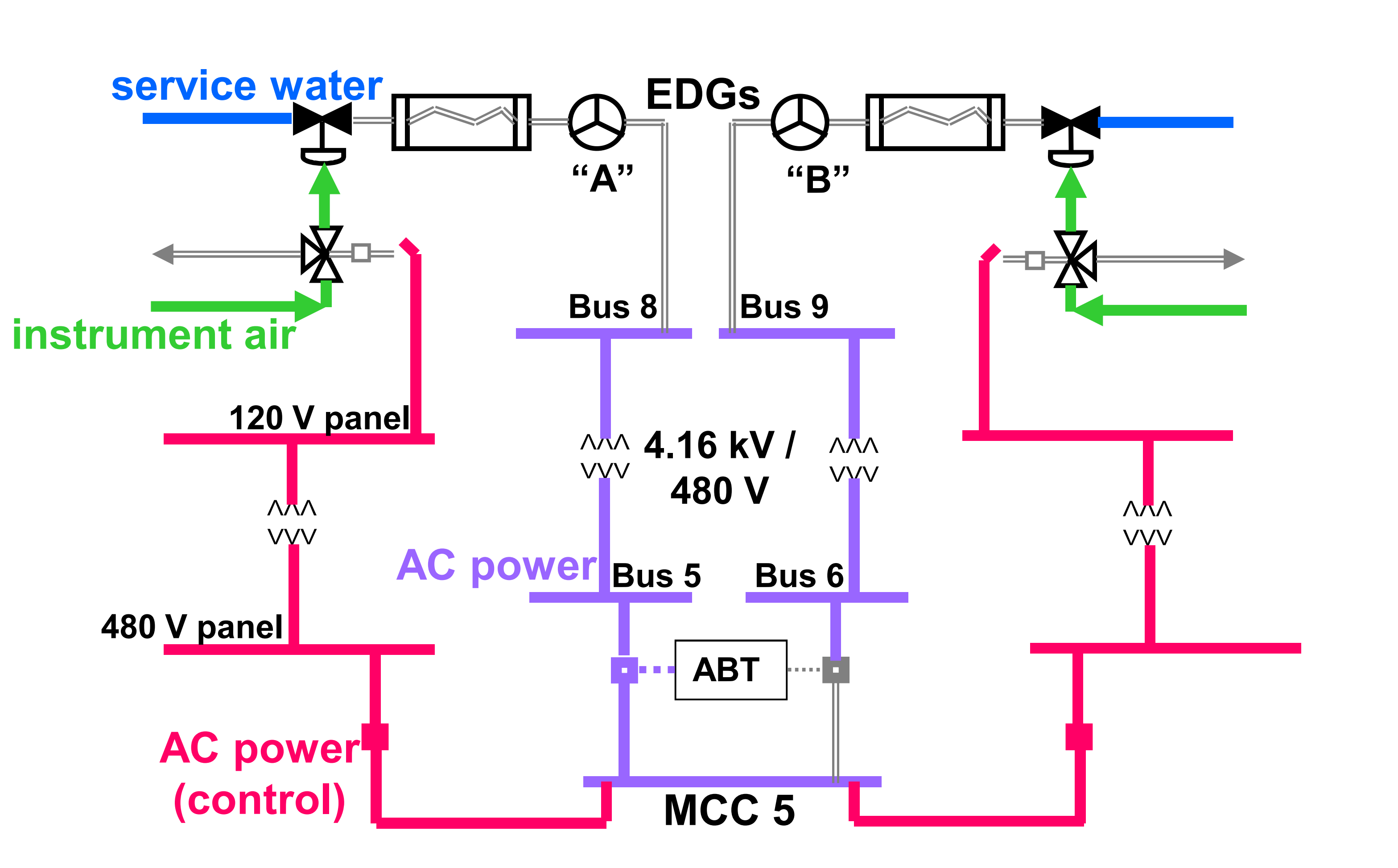
<u>CORE DAMAGE CUTSETS:</u>

- 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

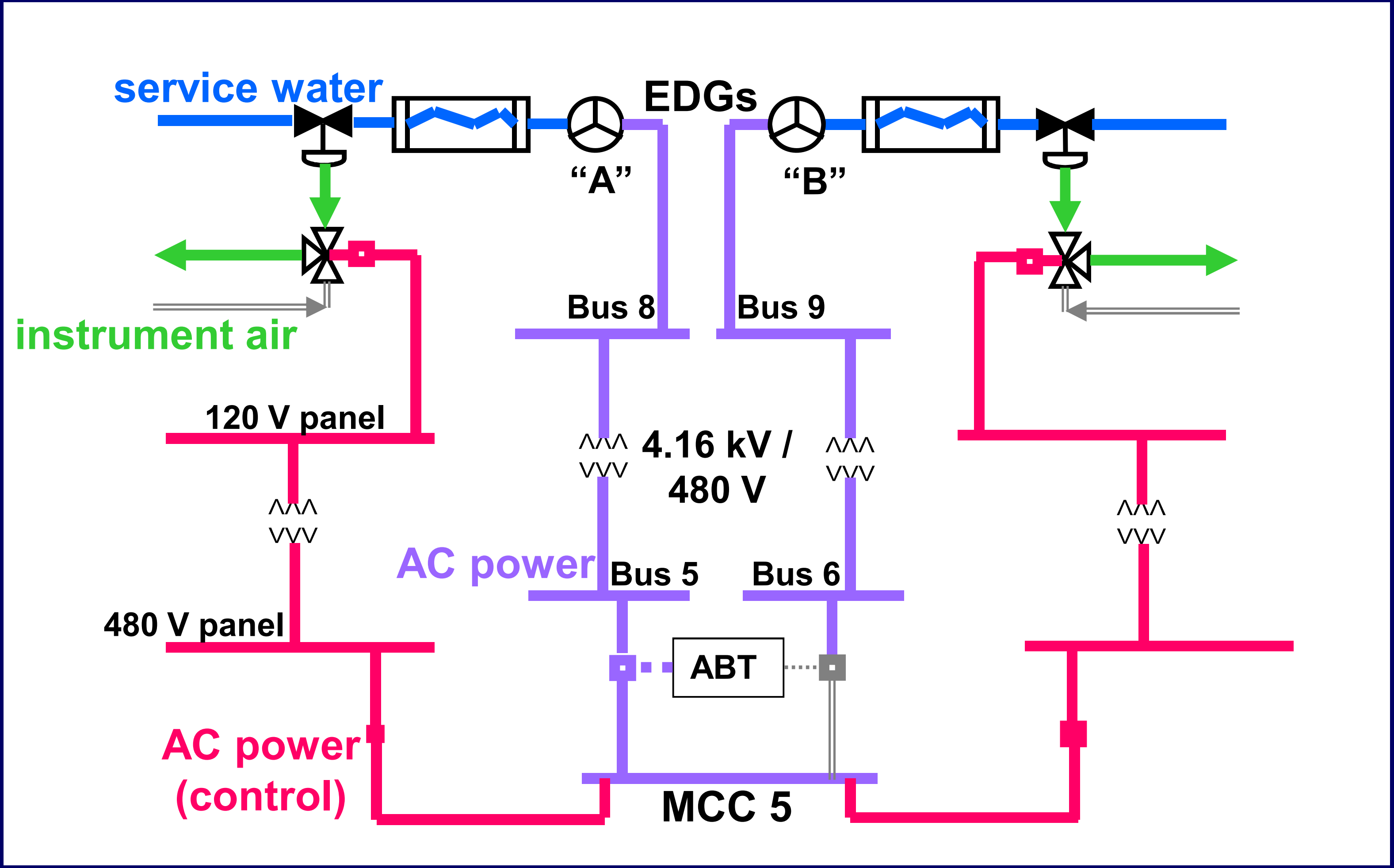
- … (many combinations per sequence!)

1: Plant Vulnerability Discovered in 1980s PRA – Standby State



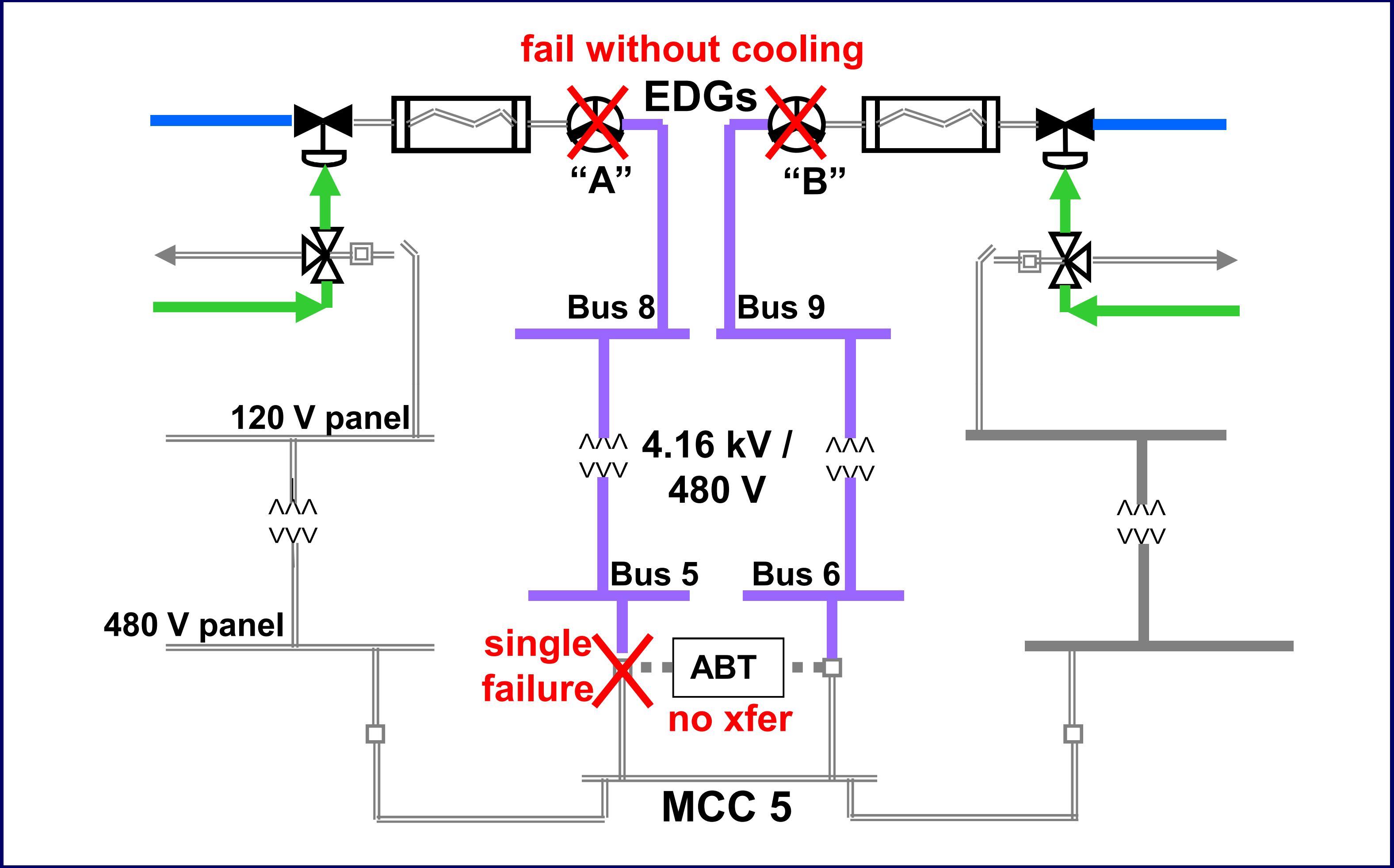
*** LERs 50-213/85-029 and 94-004***

1: Plant Vulnerability Discovered in 1980s PRA – Loss of Offsite Power



** LERs 50-213/85-029 and 94-004*

1: Plant Vulnerability Discovered in 1980s PRA – MCC Supply Breaker Fails



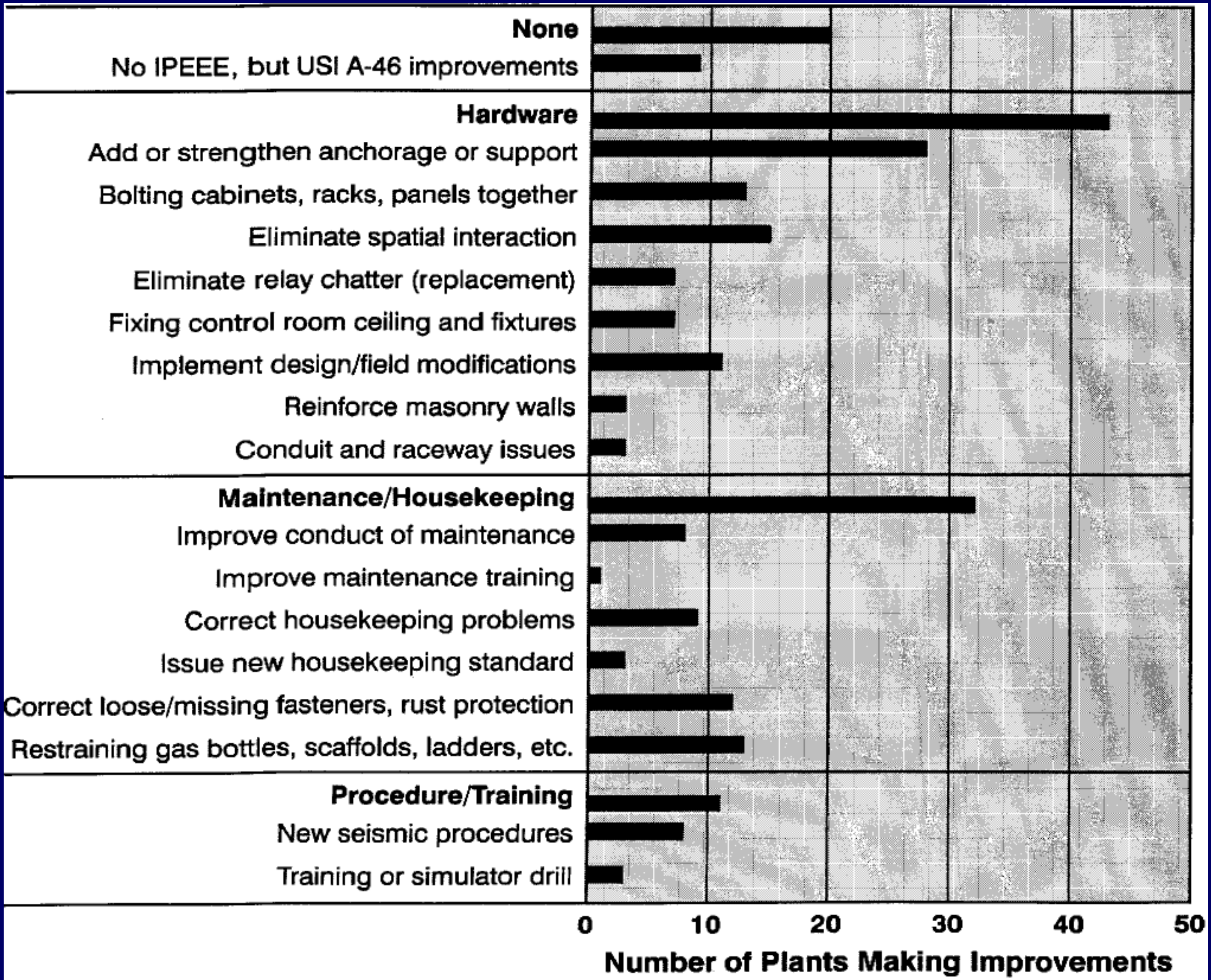
*** LERs 50-213/85-029 and 94-004***

2: Individual Plant Examination Insights*

- **Westinghouse 4-Loop PWRs**
  - **Potential Vulnerability:** Auxiliary feedwater and feed-and-bleed failures in many accident sequences
  - **Resolution:** Prioritize operator training
- **General Electric BWR 3 and 4**
  - **Potential Vulnerability:** Lose 3 of 4 residual heat removal (RHR) loops as a result of failure of either 4.16 kV AC safety bus
  - **Resolution:** Procedures and training for manual alignment of fire water to RHR service water; considering RHR service water cross-tie, portable generator, etc.
- **Other improvements included additional power sources, air-cooled motors, water-tight doors, portable fans, and improved training and procedures.**

**** NUREG-1560, Vol. 1***

3: Improvements from IPEEE Seismic Study*



***** NUREG-1742, Vol. 1**

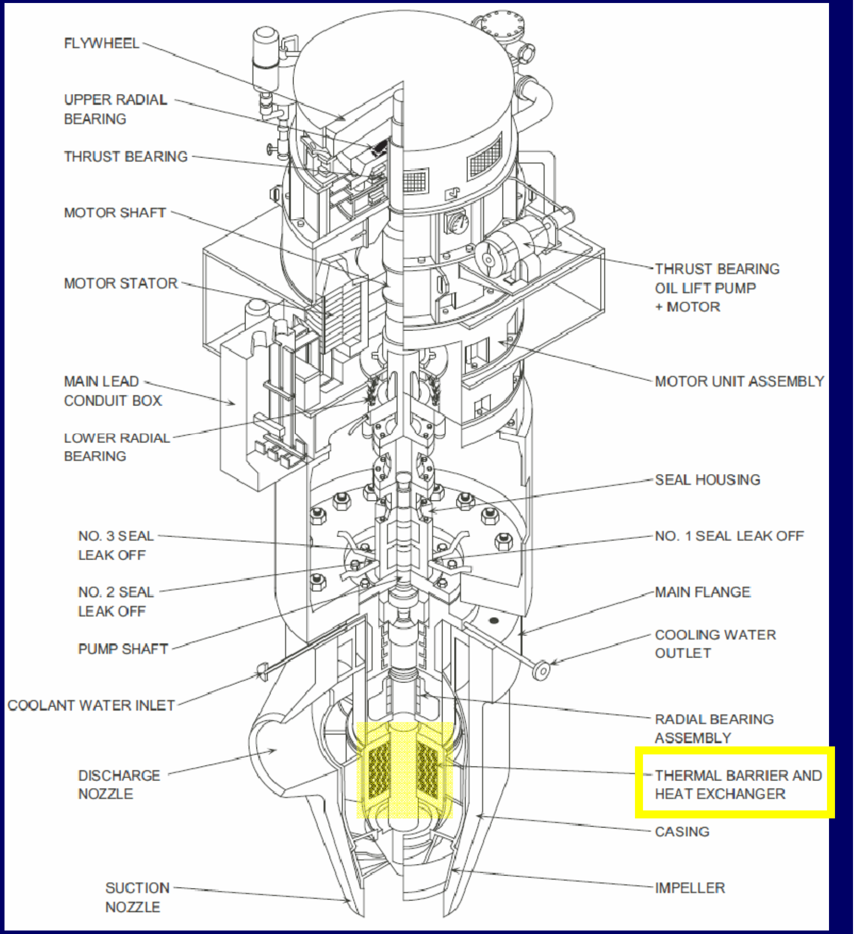
4: Improvements from IPEEE Fire Study*

Improvement Type	#	% of Category	% of Total
Operational Procedures			
Emergency Procedures	71	65	29
Operator Training	17	15	7
Fire Brigade Training	16	15	7
Other	6	5	2
Maintenance Procedures			
General Maintenance Procedures	23	82	10
Other	5	18	2
Physical Design Changes			
General Equipment Modifications	25	24	10
Relocate Equipment/Cables	17	16	7
Fire Protection System Modifications	19	18	8
Barrier Change/Upgrade	19	19	8
Plant System Design Upgrade	19	19	8
Other	5	5	2

NUREG-1742, Vol. 1

5: Interfacing Systems Loss-of-Coolant Accident*

- **Leakage of reactor coolant into another system outside containment**
  - Creates a pathway for **radiation to reach the public** if core damage occurs
  - **"What are the consequences?"** from the risk triplet
- **Surry vulnerability:**
  - Reactor coolant pump **thermal barrier leak** into the component cooling water (CCW) system could **rupture CCW**
  - Unanalyzed **1400 gpm** leak into the auxiliary building**
  - Licensee installed **additional relief capacity** on the CCW lines***



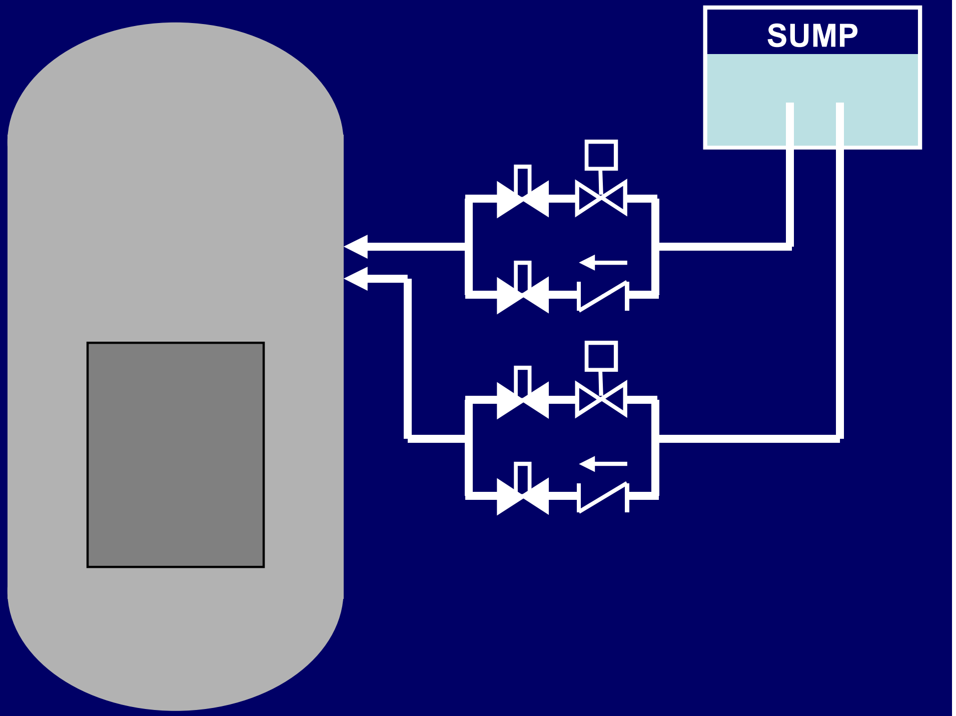
**** NUREG-0933, Issue 105***

***** 50.72 Report, Event #15625***

****** Info. Notice 89-54***

6: AP1000 Design Improvements from PRA*

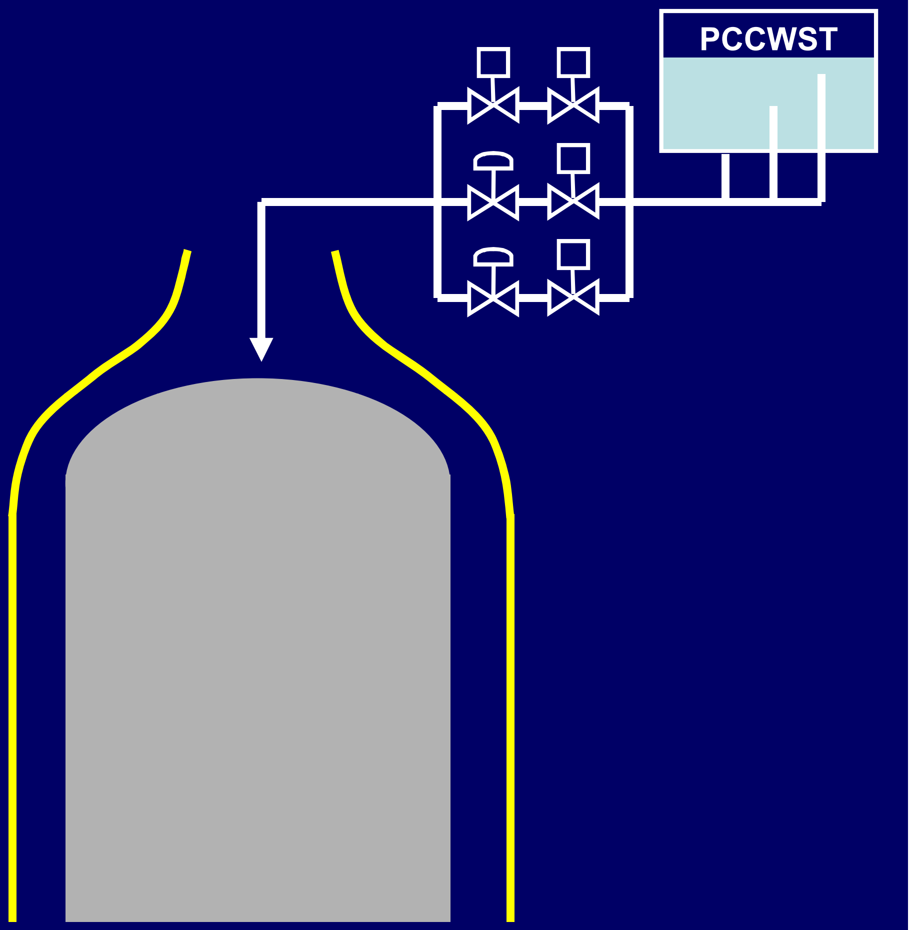
- **Recirculation from Sump to Vessel**
  - **Two** recirculation lines, **each** containing **2 parallel paths**:
    - Motor-operated valve and squib valve in series
    - Check valve and squib valve in series
  - **Diverse squib valves** to resist common-cause failure
  - Motor operated valve **fails open**



**** ML053460410, Section 19.1.6.2***

6: AP1000 Design Improvements from PRA*

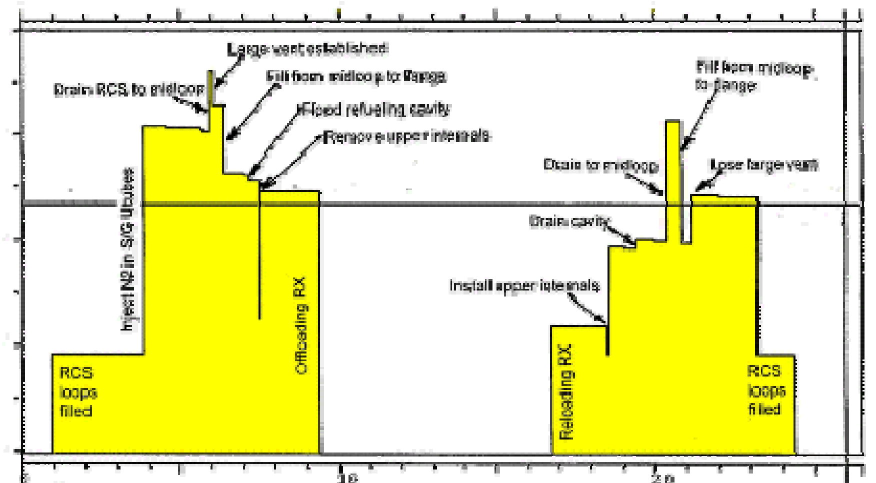
- **Containment Cooling**
  - **Three** parallel supply lines from passive containment cooling water storage tank to containment shell
  - **Diverse actuation** with motor-operated valves in one path



*** ML053460410, Section 19.1.6.2**

7: Shutdown Risk

- **Because of decay heat, risk does not go away when the plant is shut down!**
  - **Maintenance unavailability** and reliance on **manual actuation** increase probability of failure
  - Risk accumulated during shutdown can be **comparable to operational risk** during the rest of the year
- **Example: draining a PWR to mid-loop for steam generator maintenance – could drain too far and draw air into the RHR pumps, possibly failing the system**
- **NRC concern about shutdown risk drove the industry to develop NUMARC 91-06, "Industry Actions to Address Shutdown Management"**



PWR Outage Risk Profile*

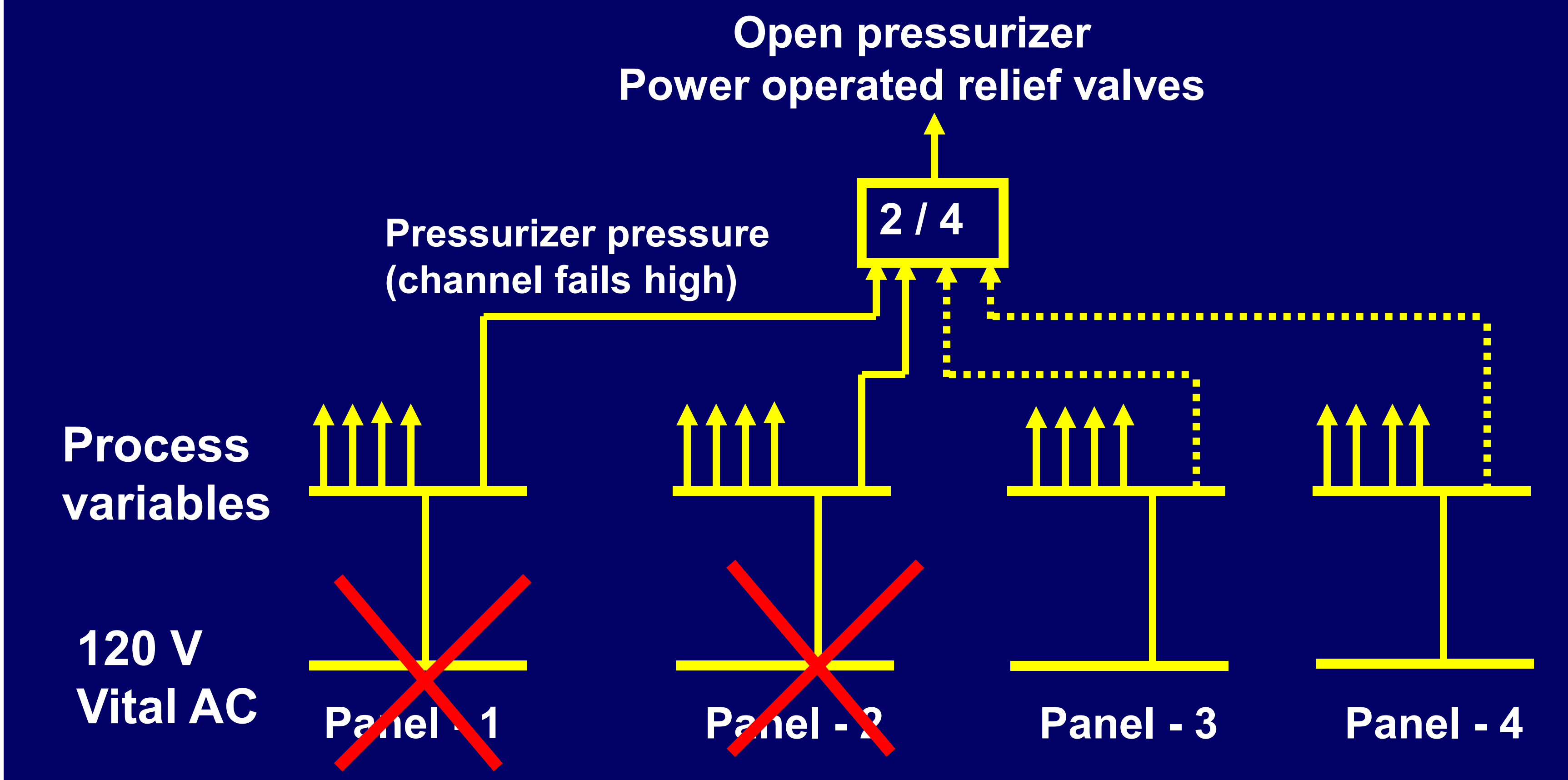
**** Info. Notice 2000-13***

8: Adverse System Interactions

- A number of plants have two-of-four logic for emergency safeguards actuation system (ESAS) supplied by Consolidated Controls Incorporated
- Historically, loss of two-of-four 120 V vital AC buses as an initiator could have resulted in one or both pressurizer PORVs inadvertently opening on false high pressurizer pressure signal, and failure of one or both trains of ESAS
- Potential loss of instrumentation to detect flow through PORV
- Loss of certain combinations of two 120 V vital AC buses during a large LOCA could also cause inadvertent sump recirculation actuation (SRAS):
  - **Tripping of both low pressure safety injection pumps**
  - **One or both containment sump valves opening, back seating the RWST discharge check valve(s) with potential loss of high pressure safety injection pump(s) and containment spray pump(s)**
- Corrective actions: actuation and control logic changes to preclude inadvertent PORV opening and inadvertent SRAS

**** Info. Notice 93-11***

8: Adverse System Interactions



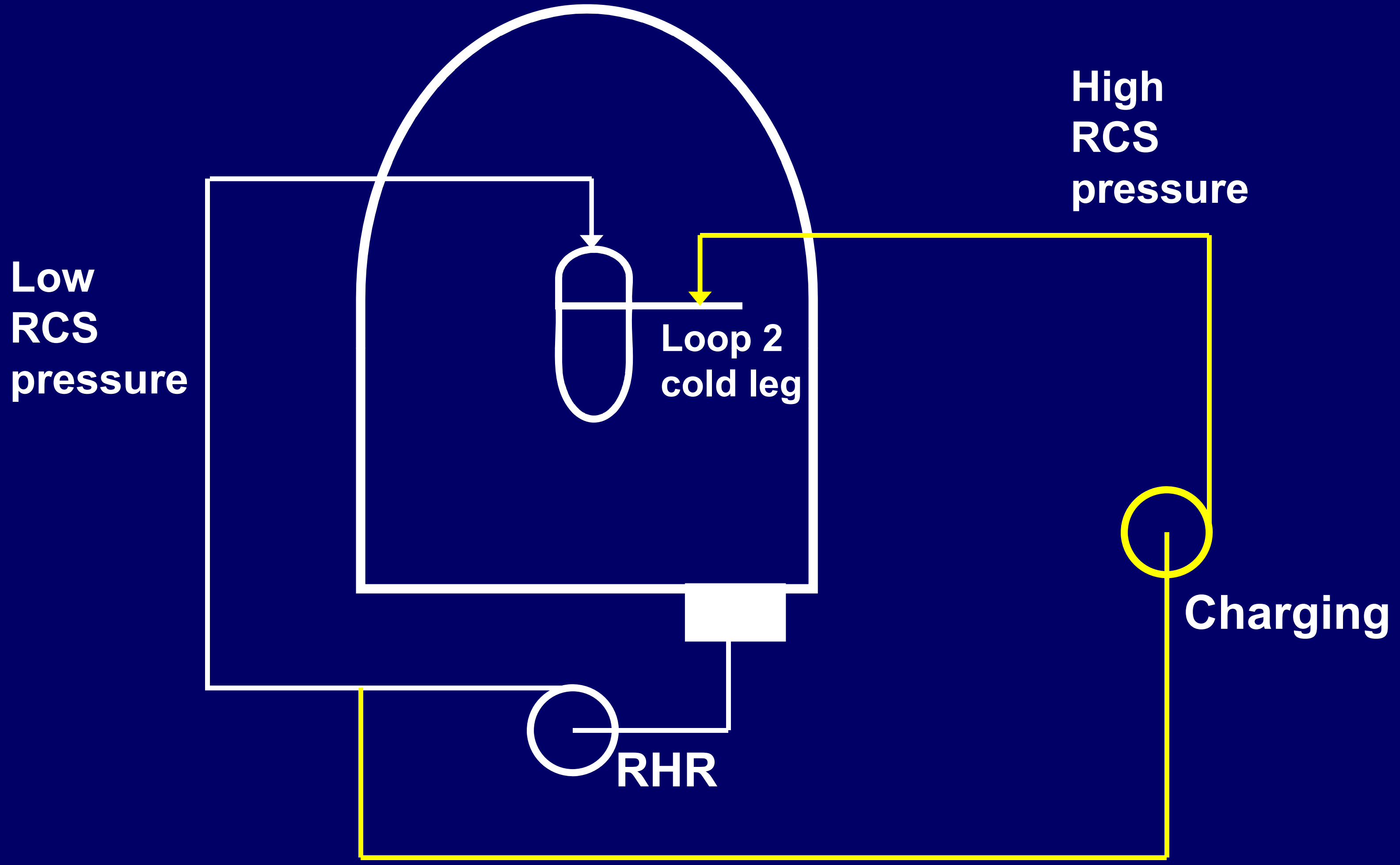
(Similarly, actuate inadvertent Sump Recirculation Actuation Signal.)

9: Small LOCA Vulnerability

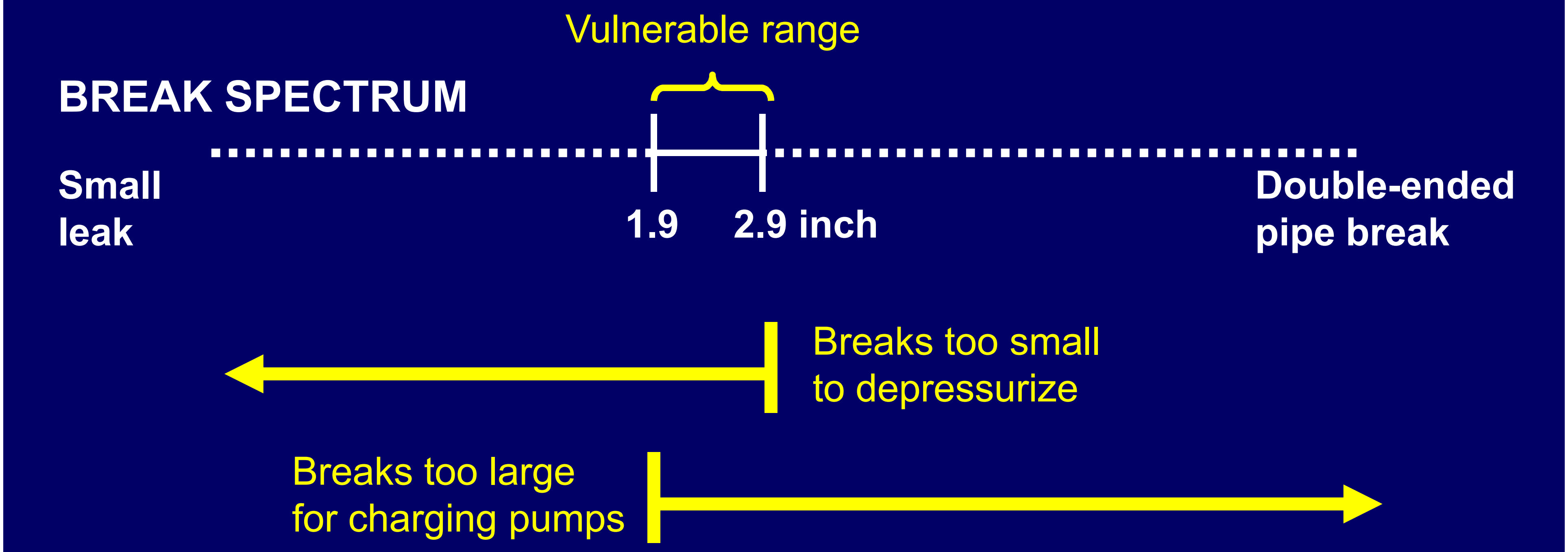
- Similar to other early vintage Westinghouse plants, Haddam Neck plant relied on “piggy-back” mode for high pressure recirculation cooling (sump to RHR pumps to charging pumps)
- However, injection only into loop 2 cold leg via charging line
- Supporting LOCA analyses identified that charging line and loop 2 cold leg breaks between about 1.9 to 2.9 inches equivalent diameter were
  - **Too small to depressurize to low pressure recirculation**
  - **Too large in that safety injection was lost out the break**
- Corrective actions included changes to Emergency Operating Procedures, new piping, use of high pressure safety injection pumps for recirculation, and the addition of throttle valves to control flow

***** LER 50-213/86-013-02***

9: Small LOCA Vulnerability Sump Recirculation



9: Small LOCA Vulnerability RELAP5 Analysis



Vulnerable range

BREAK SPECTRUM

Small leak

1.9

2.9 inch

Double-ended pipe break

Breaks too small to depressurize

Breaks too large for charging pumps

3. Supporting Risk-Informed Decisions

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Module 3: Supporting Risk-Informed Decisions

- What guidance do we use?
- What are some examples?
- How can risk communication help?

What guidance do we use?

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

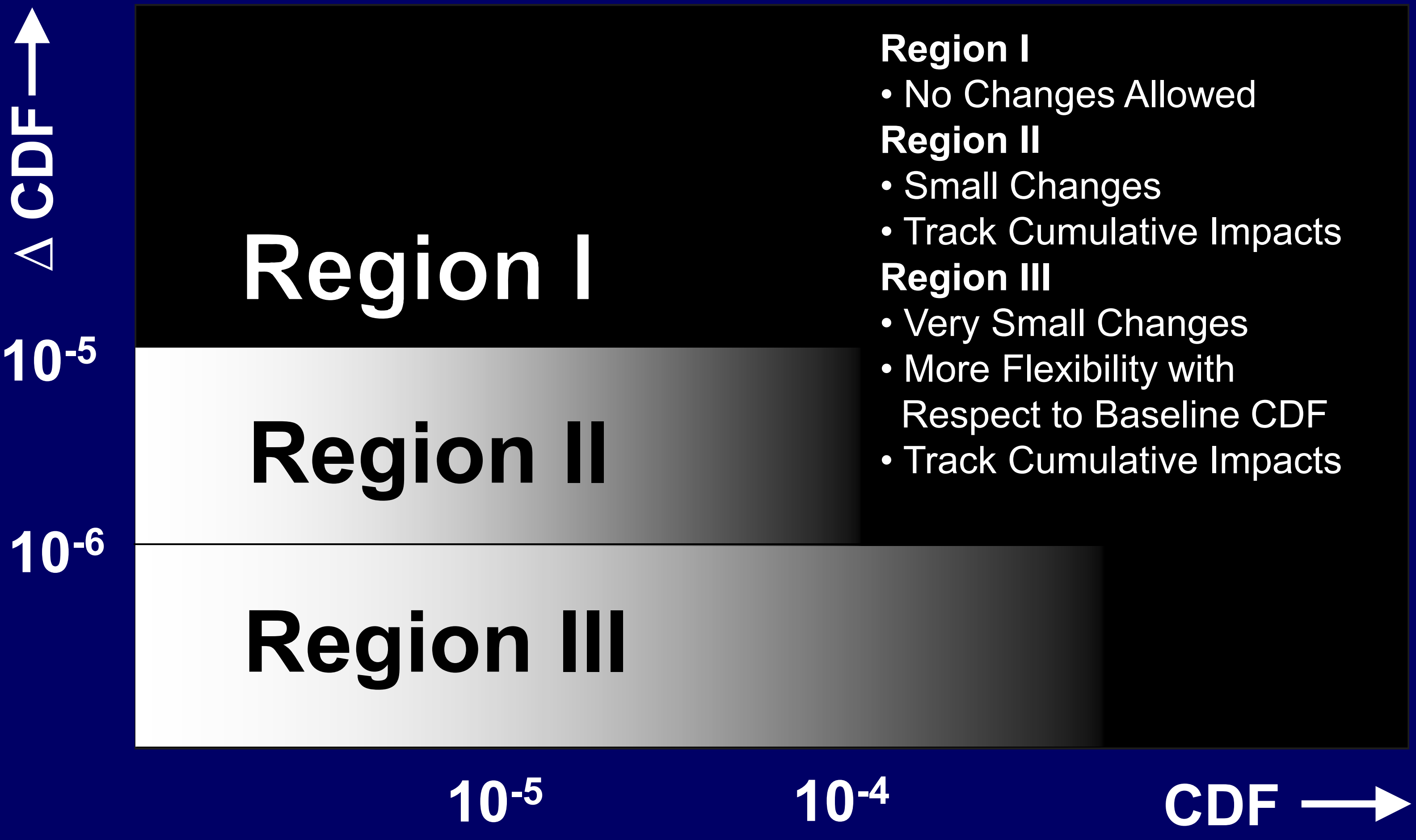
What guidance do we use?

- **For established processes, we have detailed guidance.**
- **When technical reviewers look at licensing action requests…**
  - General guidance:
    - ➢ Regulatory Guide (RG) 1.174, Standard Review Plan (SRP) 19.2
  - Risk-informed technical specifications (TS) changes:
    - ➢ RG 1.177, SRP 16.1
  - Risk-informed inservice testing:
    - ➢ RG 1.175, SRP 3.9.7
  - Risk-informed inservice inspection:
    - ➢ RG 1.178, SRP 3.9.8

What guidance do we use?

- **The RGs and SRPs rely on:**
  - Five principles for making risk-informed decisions
    - ➢ The proposed change:
      1. Meets current **regulations** (presumption of adequate protection)
      2. Is consistent with the **defense-in-depth** philosophy
      3. Maintains sufficient **safety margins**
      4. Results in an increase in CDF or risk that is **small** and consistent with the intent of the Commission’s Safety Goal Policy Statement
      5. Will be monitored using **performance measurement** strategies
  - Acceptance guidelines (not thresholds!) for small increases in risk
    - ➢ RG 1.174: **increase in CDF and LERF**
    - ➢ RG 1.177: **increase in core damage probability** while the plant is in a given condition

From RG 1.174



Region I
- No Changes Allowed

Region II
- Small Changes
- Track Cumulative Impacts

Region III
- Very Small Changes
- More Flexibility with Respect to Baseline CDF
- Track Cumulative Impacts

Figure 3. Acceptance Guidelines for Core Damage Frequency (CDF)

What guidance do we use?

- **When an inspector finds a deficiency at a plant…**
  - Inspection findings:
    - ➢ Significance Determination Process
    - ➢ Inspection Manual Chapter 0609 (and appendices)
  - Significant operational events:
    - ➢ Incident Investigation Program
    - ➢ Management Directive 8.3

<table>
<tr><th colspan="5">Estimated Conditional Core Damage Probability (CCDP)</th></tr>
<tr><th>CCDP &lt; 1E-6</th><th>1E-6 – 1E-5</th><th>1E-5 – 1E-4</th><th>1E-4 – 1E-3</th><th>CCDP &gt; 1E-3</th></tr>
<tr><td colspan="2">No additional inspection</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Special inspection</td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="2">AIT</td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2">IIT</td></tr>
</table>

What guidance do we use?

- **For more complex situations, there's a new procedure.**
- **NRR Office Instruction LIC-504, "Integrated Risk-Informed Decision Making Process for Emergent Issues"**
  - Used for **decisions that are not covered by established processes**
  - Guidelines help determine **whether additional regulatory action is required to place or maintain the plant in a safe condition**:
    - ➢ **Defense in depth** is significantly degraded
    - ➢ There is significant loss of **safety margin**
    - ➢ The **risk impact considering both internal and external events** is high
  - In the face of uncertainties or insufficient information, be conservative
  - Output is the **decision and a documented basis**

What guidance do we use?

- It's likely that you'll provide input to several of these processes over your career!

- For all of these processes, effectively communicating the risk and engineering insights within the agency is required

Example 1:
A License Amendment

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

Example 1: A License Amendment

- **Request: Extend the current Technical Specification (TS) emergency diesel generator (EDG) Allowed Outage Time (AOT) from 3 days to 14 days**
- **Risk-informed license amendment, so the licensee referenced:**
  - RG 1.174, An Approach for using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis
  - RG 1.177, An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications

Licensee Submittal

1. List of applicable regulations and how they would continue to be met
2. Impact of the change on defense in depth
3. Impact of the change on safety margins
4. Risk assessment
5. Performance measurement strategies

Reviewers from NRR/DE look at # 1, 2, 3, 5

Reviewers from NRR/DRA look at # 4, 5

Part 1: Applicable Regulations

- **The licensee confirmed that the changes meets the applicable regulations:**
  - **GDC 17**, Electric Power Systems
    - ➢ Onsite and offsite electric power systems will still provide capacity and capability to assure fuel and RCS design limits are not exceeded and vital functions are maintained
  - **GDC 18**, Inspection and Testing of Electric Power Systems will still be met
  - 10 CFR **50.63** – Station Blackout coping analysis not impacted
  - 10 CFR **50.65** – Will keep current Maintenance Rule reliability and availability goals
- **These regulations should be referenced in the "Regulatory Evaluation" section of our Safety Evaluation.**

Part 2: Defense in Depth

- **The licensee stated that there is no actual impact on defense in depth as a result of the change:**
  - Fission product barriers not impacted
  - Equipment redundancy not impacted
  - Current license allows a period of time when the plant does not meet the single failure criterion
    - ➢Requested change involves **only the duration**
- **NRR/DE will review this information.**

Part 3: Safety Margins

- **RG 1.177 states that sufficient safety margins are maintained when:**
  - Applicable industry **codes and standards** are met
  - **Safety analysis acceptance criteria** in the UFSAR are met
- **The licensee states that extending the EDG AOT:**
  - Does not modify or affect compliance with any industry standards
  - Does not reduce requirements for redundant equipment to be operable during the extended AOT
  - Sufficient redundancy will be maintained to ensure the accident analyses in the UFSAR remain valid
- **NRR/DE will review this information.**

Part 4: Risk Assessment

- **RG 1.177 3-tier approach:**
  1. Assess risk, both average and configuration-specific
  2. Preclude potentially high-risk plant configurations
  3. Have adequate programs/procedures in place to
     - identify risk-significant plant configurations resulting from maintenance or other operational activities
     - take appropriate compensatory measures to avoid such configurations
- **NRR/DRA will review this information.**

Part 4, Tier 1 – Assess Risk

- **Technical adequacy of the PRA for this request**
  - Model scope
  - Industry peer review
  - Conformance to RG 1.200

- **Evaluation of the PRA results and insights for this request**
  - Compare impact on risk to acceptance guidelines of RG 1.174 and, since this is a TS change, RG 1.177

Part 4, Tier 2 – High Risk Configurations

- Licensee identified, up-front, potentially high-risk plant configurations or activities when the proposed AOT is entered

- Licensee imposed appropriate restrictions on these configurations or activities associated with the AOT extension are in place

Part 4, Tier 3 – Risk Management Program

- **The licensee stated that its Maintenance Rule (a)(4) program satisfies the intent of Tier 3 because the licensee:**
  - Assesses and manages risk of equipment removed from service prior to or during the proposed extended AOT period
  - Identifies risk-significant plant configurations resulting from maintenance or other operational activities
  - Takes **appropriate compensatory measures**
- **Reviewers must determine whether the (a)(4) program meets the intent of RG 1.177 Tier 3.**

Part 5: Performance Measurement

- **The licensee should ensure that when equipment does not meet its performance criteria, the evaluation required under the Maintenance Rule (MR) includes prior related TS changes in its scope**

- **Licensee stated that:**
  - The EDGs are monitored under the MR program in accordance with 10 CFR 50.65
  - EDGs are currently designated "category (a)(2) – meeting established reliability and unavailability goals"

Conclusion

- **License amendment issued**
- **Safety Evaluation excerpt:**

  “The NRC staff finds that the licensee's proposed change to revise the TS to permit extending the AOT from 3 days to 14 days for an inoperable EDG is acceptable because the five key principles of risk-informed decisionmaking identified in RG 1.174 and RG 1.177 have been satisfied.”

Example 2:
The LIC-504 Process

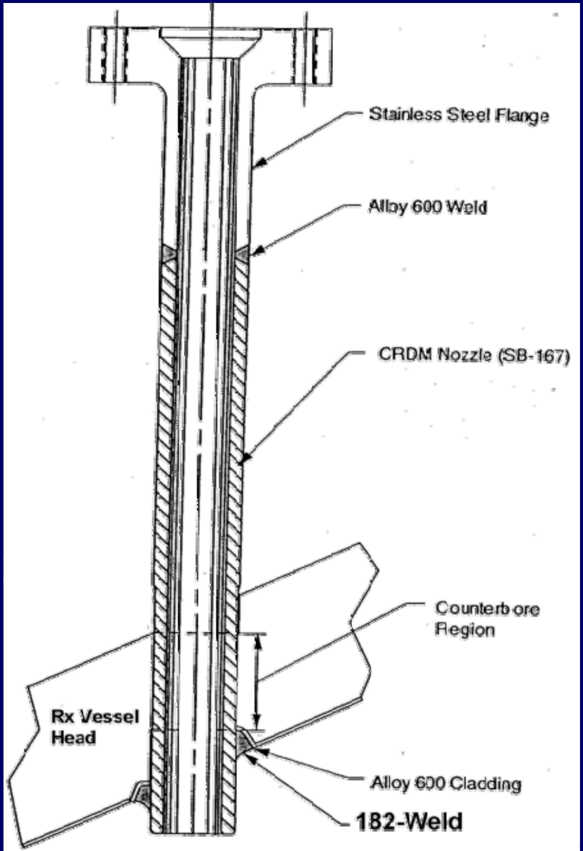
U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Background

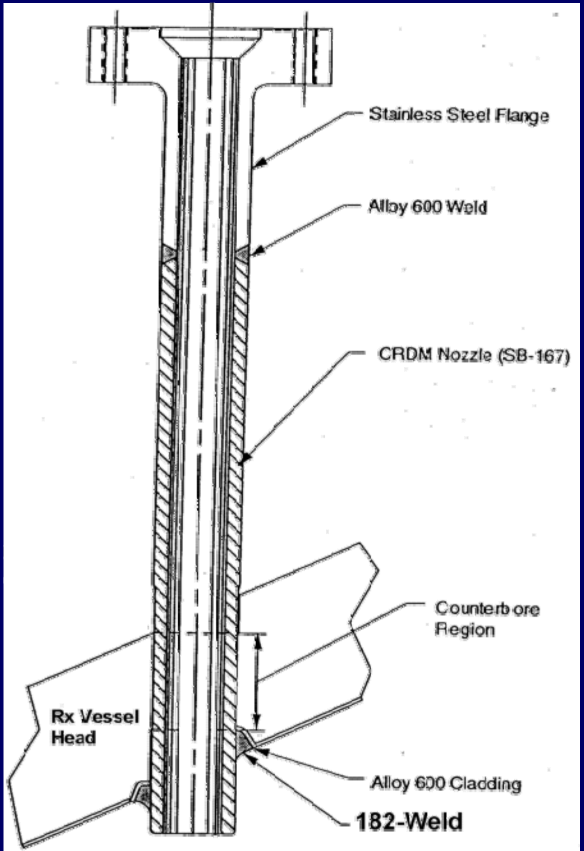
- Control rod drive mechanism (CRDM) weld and nozzle cracks observed in France in ~1990
- U.S. computer models predicted **axial cracks only**
- Nozzle ejection (which would create a **medium LOCA**) not considered credible before the leak would be detected
- U.S. licensees committed to **visual inspections to look for leaks** on the head



NRC Issues

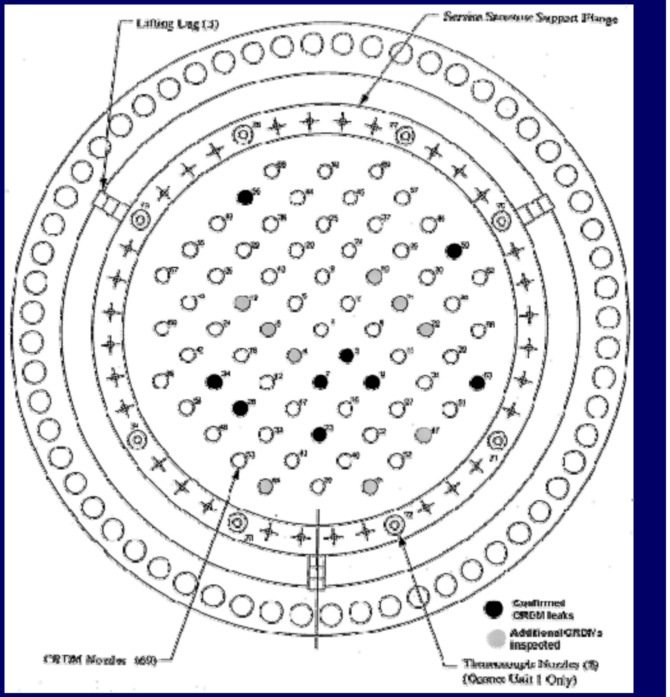
- **Regulatory Considerations**
  - Technical Specifications **prohibit pressure boundary leakage and limit unidentified leakage**
  - 10 CFR 50 Appendix B requires that licensees determine the cause and prevent repetition of **significant conditions adverse to quality** (SCAQs)

- **Risk Concern**
  - If a medium LOCA occurs, there is about a **1/1000 chance of core damage**



Inspection at the Sunny Valley Plant

- **9 leaking nozzles** found in a visual inspection of all 69 nozzles
- Leakage indications much less obvious than expected
- Ultrasonic (UT) exams performed only on 9 visibly leaking nozzles
- **Circumferential cracks** found accidentally in 3 nozzles during repair
- Circumferential cracks began on outside surface; means there was **leakage through axial cracks for years without being discovered by visual inspections**
- Physical exams showed cracks went **almost halfway around the circumference (165°); ejection predicted at 324°**



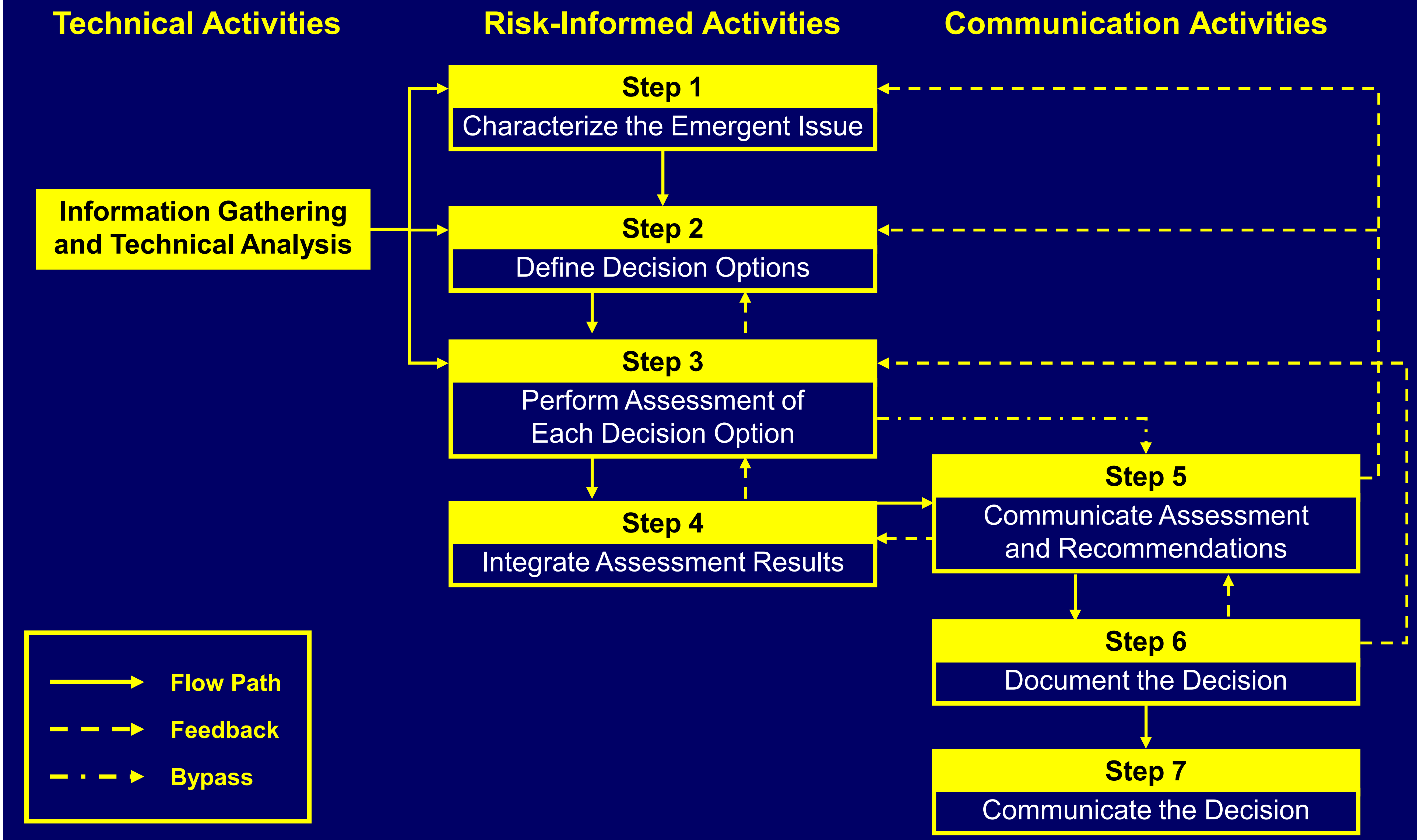
Licensee Response

- **Additional ultrasonic testing (UT) on 9 nozzles that didn’t appear to be leaking (15% of remaining nozzles)**
- **No additional axial or circumferential cracks found**
- **UT was not configured to find circumferential cracks**
  - NRC expert assessment that UT configuration has reasonable probability to **detect at least part of a crack** large enough to become a structural integrity problem within 6 months
- **51 nozzles not inspected by UT**

Our Decision as the Regulator

- Should we allow the plant to start up?
- Should the licensee be required to complete additional testing to provide high confidence that there are no more cracks needing repair in the other 51 nozzles?
- Should we allow the licensee to use the current UT configuration to avoid extending their outage?

Enter the LIC-504 Process…



Technical Activities

Risk-Informed Activities

Communication Activities

Step 1
Characterize the Emergent Issue

Information Gathering and Technical Analysis

Step 2
Define Decision Options

Step 3
Perform Assessment of Each Decision Option

Step 4
Integrate Assessment Results

Step 5
Communicate Assessment and Recommendations

Step 6
Document the Decision

Step 7
Communicate the Decision

Step 2 of LIC-504: Define Options

	Return to Power Before UT?	Additional UT Before Next Outage?	When Next UT?	UT Configuration
1 Require licensee to test all nozzles for circumferential cracks with on-site UT equipment before returning to power.	No	Yes	ASAP	Current
2 Require licensee test all nozzles with proper UT equipment before returning to power.	No	Yes	~1 mo.	Enhanced
3 Allow licensee to restart, but shut down ASAP to test all nozzles with proper UT test equipment.	Yes	Yes	~1 mo.	Enhanced
4 Allow licensee to return to service without additional testing requirements.	Yes	No	~6 mo.	Enhanced

Step 3 of LIC-504: Assess Option 1

UT with **Current** Equipment Before Return to Power			
Driving Factor	**Key Technical Inputs**	**Validity of Input**	**Confidence in Assessment**
Structural safety margin adequate	Assessment that UT configuration has reasonable probability to detect at least part of a crack large enough to become a structural integrity problem within 6 months	Based on UT expert opinion	Greater uncertainty than option 2 due to use of current UT equipment
Compliance with regulations	Not allowed to re-start until UT complete		
Low Risk	Small chance of significant crack being missed; unlikely that an undetected crack could grow to critical size in less than 6 months	Based on UT expert opinion	Greater uncertainty than option 2 due to use of current UT equipment
Licensee burden low	Minimal delay compared to option 2, since can use the on-site UT equipment		

Step 3 of LIC-504: Assess Option 2

UT with **Enhanced** Equipment Before Return to Power			
Driving Factor	**Key Technical Inputs**	**Validity of Input**	**Confidence in Assessment**
Structural safety margin adequate	Use of enhanced UT equipment	Enhanced UT configured to detect subject cracks	High confidence due to enhanced UT equipment
Compliance with regulations	Not allowed to re-start until UT complete		
Risk Low	Very unlikely that a significant crack could be missed	Based on UT expert opinion	Reduced uncertainty compared to option 1 due to enhanced UT equipment
Licensee burden higher than option 1	Larger delay compared to option 1; must wait for enhanced UT equipment (~1 month)		

Step 3 of LIC-504: Assess Option 3

UT with **Enhanced** Equipment when Available (~1 Month)			
Driving Factor	**Key Technical Inputs**	**Validity of Input**	**Confidence in Assessment**
Structural safety margin not demonstrated	Reliance on visual inspections of 51 nozzles for ~1 month		Very low confidence that margin is adequate
Compliance with regulations not demonstrated	Proposed approach does not reliably establish extent of condition		Uncertain whether cracks have been missed
Risk higher than options 1 or 2, although exposure time is short	Some likelihood that a significant crack has been missed		High uncertainty in actual risk
Licensee burden less than options 1 and 2	Restart allowed on schedule; forced outage in ~1 month		

Step 3 of LIC-504: Assess Option 4

UT with **Enhanced** Equipment Next RFO (~6 Months)			
Driving Factor	**Key Technical Inputs**	**Validity of Input**	**Confidence in Assessment**
Structural safety margin not demonstrated	Reliance on visual inspections of 51 nozzles for ~6 months		Very low confidence that margin is adequate
Compliance with regulations not demonstrated	Proposed approach does not reliably establish extent of condition		Uncertain whether cracks have been missed
Higher risk than other options; longer exposure time than option 3	Some likelihood that a significant crack has been missed; more time for cracks to grow		High uncertainty
Minimum Licensee burden	Restart allowed on schedule; perform UT next scheduled outage (~6 months)		

Step 4 of LIC-504: Integrate Results

- **Need to ensure both safety margin and compliance, therefore:**
  - Options 3 and 4 rejected
    - Additional exposure not in compliance with Appendix B (establish extent of condition and prevent recurrence)
    - Uncertain that adequate structural safety margins maintained
    - Inadequate basis to assess risk of these options
  - Option 1 preferred by the staff
    - Adequate assurance based on further inspection with the on-site UT equipment
    - Additional assurance afforded by enhanced UT equipment not judged necessary in this case

Steps 5-7 of LIC-504: Communicate Assessment

- **Example Conclusion**
  - **Option 1** provides full compliance with the regulations, and reasonable assurance of adequate safety margin and low risk.
  - In the absence of UT examination of the remaining nozzles, there would be **no reliable risk information** that could provide a basis for deviation from compliance with Appendix B.
  - The **added assurance of an ASME-qualified inspection technique for circumferential cracks is not required** in this case to provide sufficient assurance that any circumferential cracks present in the nozzles are **not large enough to be of concern** for the near term.
  - The only risk information is the **bounding value from the conditional core damage probability** if a nozzle ejected, which **by itself does not ensure that risk remains within our acceptance guidelines.**

- **For a real example, see ML070990071.**

How can risk communication help?

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

What is risk communication?

- Communicating with our external stakeholders about topics that cause concern about health, safety, security or the environment*
- Communicating amongst ourselves about risk models, risk assessments and risk-informed decisions**

** NUREG/BR-0308, Guideline for External Risk Communication*

*** NUREG/BR-0318, Guideline for Internal Risk Communication*

Why is risk communication important at the NRC?

- **Provides essential links between risk analysts, managers (decision-makers) and internal and external stakeholders.**

- **Facilitates risk-informed decision-making**
  - GAO recommendation: improve communication of risk estimates, uncertainties and assumptions to decision-makers
  - Integrated risk-informed decision-making process developed (Office Instruction LIC-504) which addresses communication

What does effective internal communication require?

- **In short, it requires the background provided by this course:**
  - Common understanding of risk concepts and terminology (among all NRC employees)
  - Common understanding of the strength and limitations of risk analysis
  - An understanding of risk-informed regulation and how it differs from the traditional approach

How are we doing?

- **Let’s see if you can communicate the meaning of these terms:**
  - Risk
  - Success criteria
  - Cutset
  - Core damage frequency

How are we doing?

- **Let’s see if you can communicate the meaning of these terms:**
  - Risk
    - What can go wrong?
    - How likely is it?
    - What are the consequences?
  - Success criteria
    - Systems, components, or actions required for success (often of a function or system) in a given scenario
  - Core damage cutset
    - A set of failures (of basic events) that lead to core damage
  - Core damage frequency
    - The total frequency of all scenarios of initiating events and mitigating system failures that lead to core damage

How are we doing?

- **Let’s see if you can communicate these concepts:**
  - What are some strengths of PRA?
  - What are some limitations of PRA?

How are we doing?

- **Let's see if you can communicate these concepts:**
  - What are some strengths of PRA?
    - ➢Comprehensive safety perspective
    - ➢Provides insights on plant vulnerabilities
    - ➢Explicit treatment of uncertainties
  - What are some limitations of PRA?
    - ➢Modeling limitations
    - ➢Availability of data

What else does internal communication require?

1. Well defined objectives for the communication
2. Clear roles and responsibilities
3. Knowledge of the needs and preferences of your communication partner(s)
4. Technical information provided in understandable language
5. Trust and credibility among staff and managers

1: What are the objectives of internal risk communication?

- Gathering or providing information for a risk determination
- Eliciting or providing peer feedback
- Providing input in support of a decision
- Providing background information
- Conveying a decision
- Supporting communication with external stakeholders
- Developing a new risk-informed regulatory approach

2: How do RISK ANALYSTS participate?

- Seek input from other technical staff early and often during risk assessments
- Summarize assumptions, results and insights for decision-makers in an understandable way
- Explain the uncertainties and limitations of risk assessments
- Be able to explain why risk information is satisfactory for a given application or decision

2: How do OTHER TECHNICAL STAFF participate?

- **Understand risk-informed regulation well enough to communicate effectively with risk analysts**
- **Raise issues that may have some risk impact**
  - Our process allows us to use risk information when warranted for non-risk-informed licensing amendment requests, for example (SRP 19.2 Appendix D)
  - Risk analysts won't know about it unless you go talk to them!
- **Help risk analysts understand how to reflect the issue of concern in the risk model (e.g., pressure boundary cracking, thermal-hydraulic phenomena)**
- **Help determine success criteria or provide data for a PRA model**
- **Characterize safety margins and defense-in-depth**
- **Use PRA insights to focus reviews and assessments**

2: How do PROJECT MANAGERS participate?

- Understand risk-informed regulation well enough to communicate effectively with risk analysts
- Ensure that risk groups are involved in all risk-informed requests
- Arrange meetings between risk analysts and traditional engineering reviewers on risk-informed licensing actions – start the “integrated decision” early

2: How do SUPERVISORS participate?

- **Ensure that decisions are based on an integrated assessment from risk analysts and other technical staff**

- **Understand PRA well enough to assess the quality of risk information presented to them**

- **Communicate the bases for decisions to all stakeholders in an understandable way using a communication plan**

3: What do your communication partners need?

- Decision-makers need information presented in summary format
- Numerical results from PRAs need to be explainable in engineering terms
- Some stakeholders may not want numerical results at all
- Visual aids can be powerful tools for communicating risk information

5: How do we build trust and credibility?

- Involve stakeholders early and often in risk assessments
- Peer review risk information and discuss the reviewer’s perspective
- Discuss the strengths and limitations of risk information and how it should be used
- Explain why risk information is satisfactory for a given application or decision

What resources are available?

- NUREG/BR-0308, NRC Guidelines for External Risk Communication, January 2004
- NUREG/BR-0318, NRC Guidelines for Internal Risk Communication, December 2004
- NRC Risk Communications Web Page:

  http://www.internal.nrc.gov/communications/riskcommunication.html

4. Resources

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

Where can you get more information?

- **Web Resources**
  - NRC Public Website
    - *http://www.nrc.gov/what-we-do/regulatory/rulemaking/risk-informed.html*
  - NRR/DRA Website
    - *http://nrr10.nrc.gov/adt/dssa/spsb/webpages/spsbpage/spsbhomepageindex.html*
    - Huge document archive on risk-informed regulation
  - NRO/DSRA Website
    - *http://nrr10.nrc.gov/NRO/nrooffice/dsrahome/pra-support/index.cfm*
  - @Risk-InformedCommunity Web Forum
    - *http://nrr10.nrc.gov/forum/index.cfm?selectedForum=08*
    - Post questions on anything related to risk-informed regulation

- **NRC Organizations**
  - NRR/DRA
  - NRO/DSRA
  - RES/DRASP
  - Regional Senior Reactor Analysts

- **Training**
  - PRA Basics for Regulatory Applications (P-105, 3 days)
  - PRA Technology and Regulatory Perspectives (P-111, 2 weeks)
  - Advanced P-series courses
  - Model uncertainty course
  - Risk Communication Workshop

Course Objectives

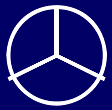
- **At the end of this course, you will be able to:**
  - – Define **basic terms** related to risk-informed regulation
  - – Identify **how your work fits into** a risk-informed regulatory structure
  - – Understand the **basic modeling concepts** in a probabilistic risk assessment
  - – Discuss the **benefits and limitations** of using risk information
  - – **Support and communicate** risk-informed decisions
  - – Find **references** for more information in the future

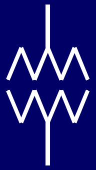
Guide to Abbreviations

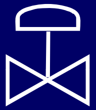
ABT = automatic bus transfer
AC = alternating current
AOT = allowed outage time
ASP = Accident Sequence Precursor program
ASME = American Society of Mechanical Engineers
ATWS = anticipated transient without scram
BWR = boiling water reactor
CCDP = conditional core damage probability
CCFP = conditional containment failure probability
CCW = component cooling water
CDF = core damage frequency
CFR = *Code of Federal Regulations*
CRDM = control rod drive mechanism
CT = completion time
ΔCDF = change in core damage frequency
ΔLERF = change in large early release frequency
EDG = emergency diesel generator
ESAS = engineered safeguards actuation signal
ESBWR = Economic Simplified Boiling Water Reactor
FV = Fussell-Vesely importance
GAO = Government Accountability Office
GDC = General Design Criteria (10 CFR 50 Appendix A)
GL = Generic Letter
GPM = gallons per minute
ICCDP = incremental conditional core damage probability
ICLERP = incremental conditional large early release probability
IPE = Individual Plant Examination (for severe accident vulnerabilities)
IPEEE = Individual Plant Examination of External Events

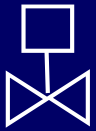
LER = Licensee Event Report
LERF = large early release frequency
LOCA = loss of coolant accident
LRF = large release frequency
MCC = motor control center
MSPI = Mitigating System Performance Index
NOED = Notice of Enforcement Discretion
PORV = power- (or pilot-) operated relief valve
PRA = probabilistic risk assessment
PWR = pressurized water reactor
RAW = risk achievement worth
RFO = refueling outage
RG = Regulatory Guide
RHR = residual heat removal
RIS = Regulatory Issue Summary
RPP = Risk-informed Performance-based Plan (formerly RIRIP, Risk-Informed Regulation Implementation Plan)
RRW = risk reduction worth
RTNSS = regulatory treatment of non-safety systems
SBO = station blackout
SCAQ = significant condition adverse to quality
SRAS = sump recirculation actuation signal
SRM = Staff Requirements Memorandum
SRP = Standard Review Plan (NUREG-0800)
SSC = structure, system, or component
TS = technical specifications
UFSAR = Updated Final Safety Analysis Report
UT = ultrasonic testing

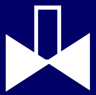
Guide to Symbols

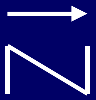

diesel generator

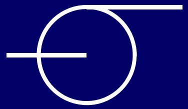

transformer

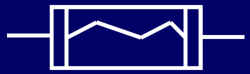

air-operated valve

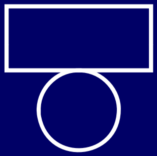

motor-operated valve

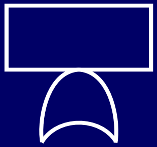

squib (explosive) valve

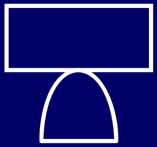

check valve


pump


heat exchanger


basic event


OR gate


AND gate