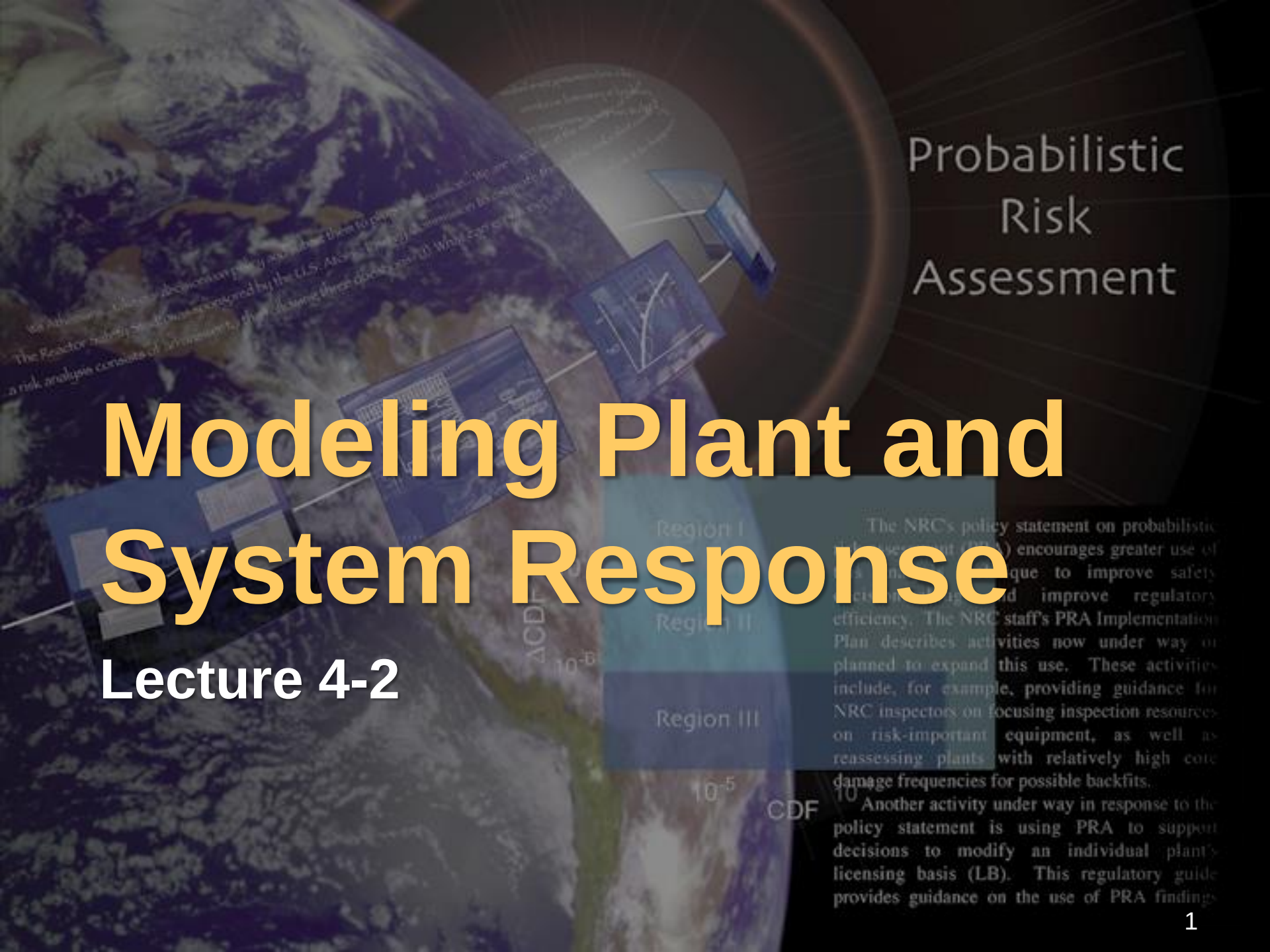


Modeling Plant and System Response

Lecture 4-2

Key Topics

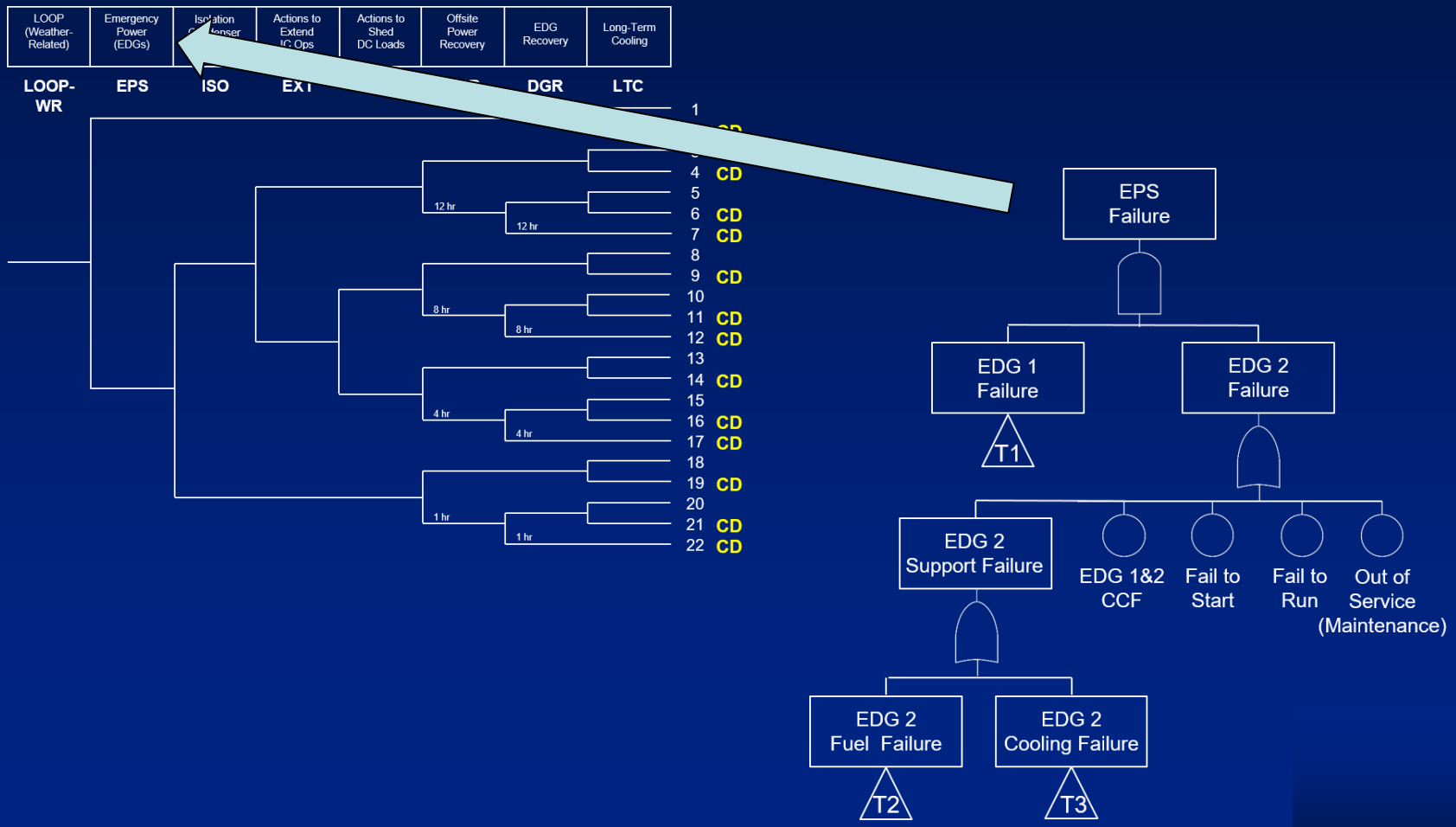
- Considerations in modeling process
- Principal modeling tools
  - Event trees
  - Fault trees
- Methods of analysis
  - Linked fault trees
  - Event trees with boundary conditions
- Useful tools

Resources

- American Nuclear Society and the Institute of Electrical and Electronics Engineers, “PRA Procedures Guide,” NUREG/CR-2300, January 1983.
- W.E. Vesely, et al., “Fault Tree Handbook,” *NUREG-0492*, January 1981.
- R.E. Barlow and F. Proschan, *Statistical Theory of Reliability and Life Testing: Probability Models, Second Edition*, To Begin With, Silver Spring, MD, 1975.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Standard Framework for Plant/System Analysis



Preliminary Remarks

- Greater variability ("art") in modeling post-initiator response than in initiators (at least for operating NPP PRAs)*
- Principal tools (event trees and fault trees) are standard but analysts have modeling choices
  - Analysis scope
  - Level of detail
  - Simplifications
  - Parsing of sequence elements
  - Method of analysis

*There are exceptions (e.g., modeling of LOOP)

Preliminary Remarks (cont.)

- No one "right way," but current processes (e.g., peer reviews, benchmarking, NRC review questions) tend to reduce variability in approaches.
- The act of modeling improves understanding – PRA owners derive maximum benefit if they're involved in the analysis.

*There are exceptions (e.g., modeling of LOOP)

Cautions

- System details can be intimidating to the uninitiated.
  - Need to understand how system works before figuring out how it might fail.
  - Time required to develop understanding can be significant.
- Many attempts to automate model construction, none yet satisfactory. Increasing importance for organizations that “cycle” staff through PRA department.
- Many models already exist.
  - Existing models provide templates for new modeling efforts, also serve as points of comparison
  - Need to be careful of biases from the anchoring and adjustment heuristic (Lecture 2-3)

Example Choices

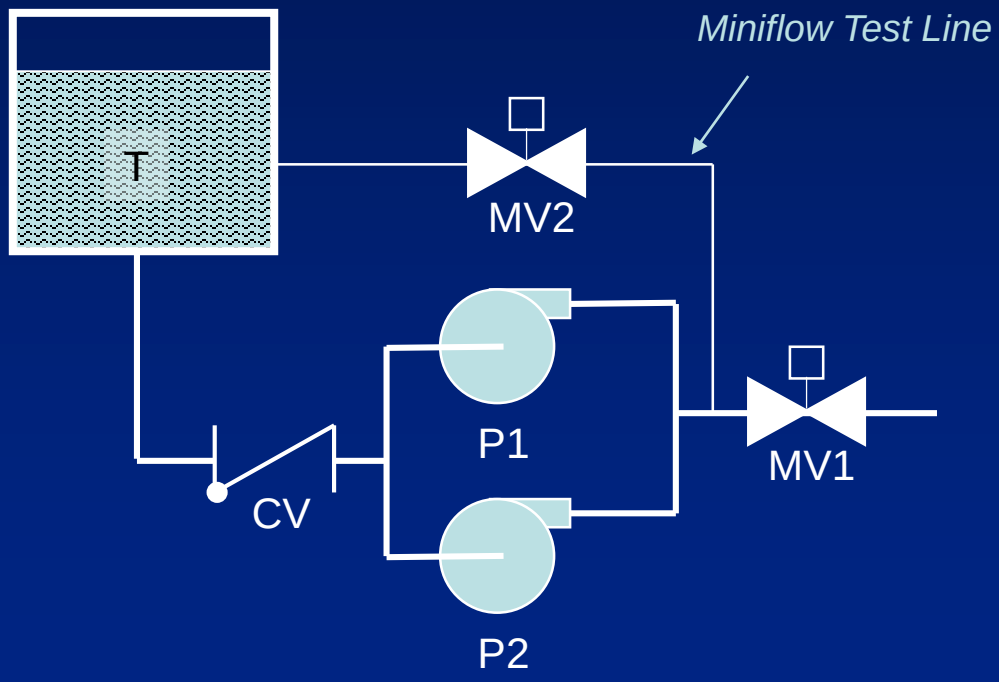
- Analysis scope (given overall project scope)
  - Time (e.g., pre-initiator processes, mission time)
  - Space (e.g., single unit vs. multi-unit, regional hazards)
  - Organization (e.g., plant staff only, offsite organizations)
- Level of detail
  - Piece-part vs. “component” vs. “super-component/module/train”
  - Sub-task vs. task vs. “human failure event” (Lecture 5-2)

Example Choices (cont.)

- Simplifications
  - Unlikely failures and failure combinations (e.g., locked manual valves, multiple instrument line valves)
  - Failures that should have little effect on performance (e.g., non-safety strip chart recorder)
  - Uncredited recovery actions (e.g., untrained, non-proceduralized actions)
  - Independence of events (Lecture 6-1)
  - Treatment of uncertainty (e.g., “Point estimate” vs. full characterization)

Example Choices (cont.)

- Simplifications – Miniflow Test Line Example



Should the miniflow test line (and valve MV2) be included in the fault tree? Why or why not?

Example Choices (cont.)

- Parsing
  - System-based event trees vs. functional event tree vs. no event tree
  - Human failure events in event trees or fault trees
  - Note:
    - Difficulty is conserved
    - Results should be the same, given the same modeling assumptions. However, risk communication can be affected

Guiding Principles in Choosing

- Availability and quality of supporting evidence
- Required degree of realism
  - Key dependencies
  - PRA-user confidence

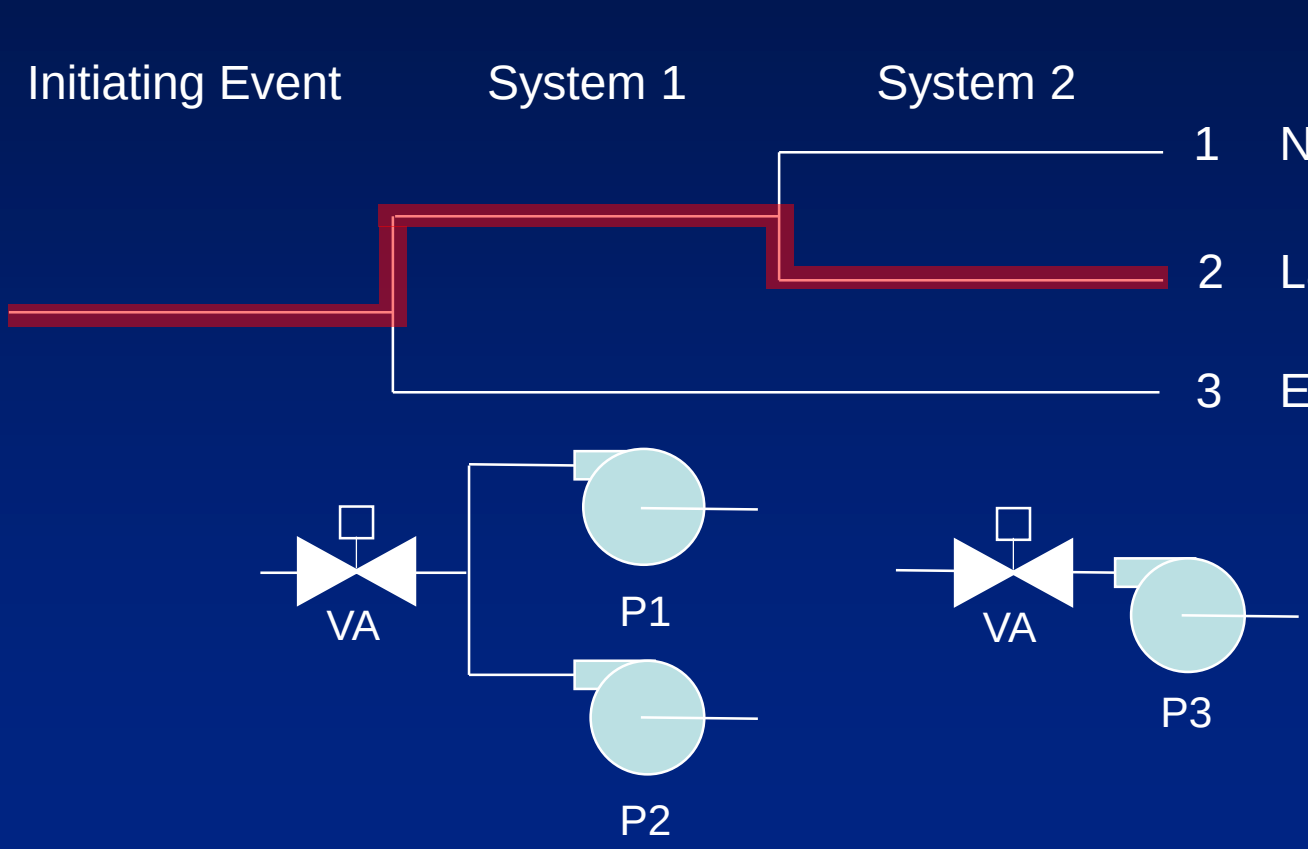
Important: choices => responsibility

- Document understanding and assumptions
- Be able to defend analysis – “take ownership”

Analysis Methods and Models

- Linked fault tree vs event tree with boundary conditions
- Logic modeling vs object-oriented simulation (Lecture 9-3)
- Static vs dynamic (Lecture 9-3)

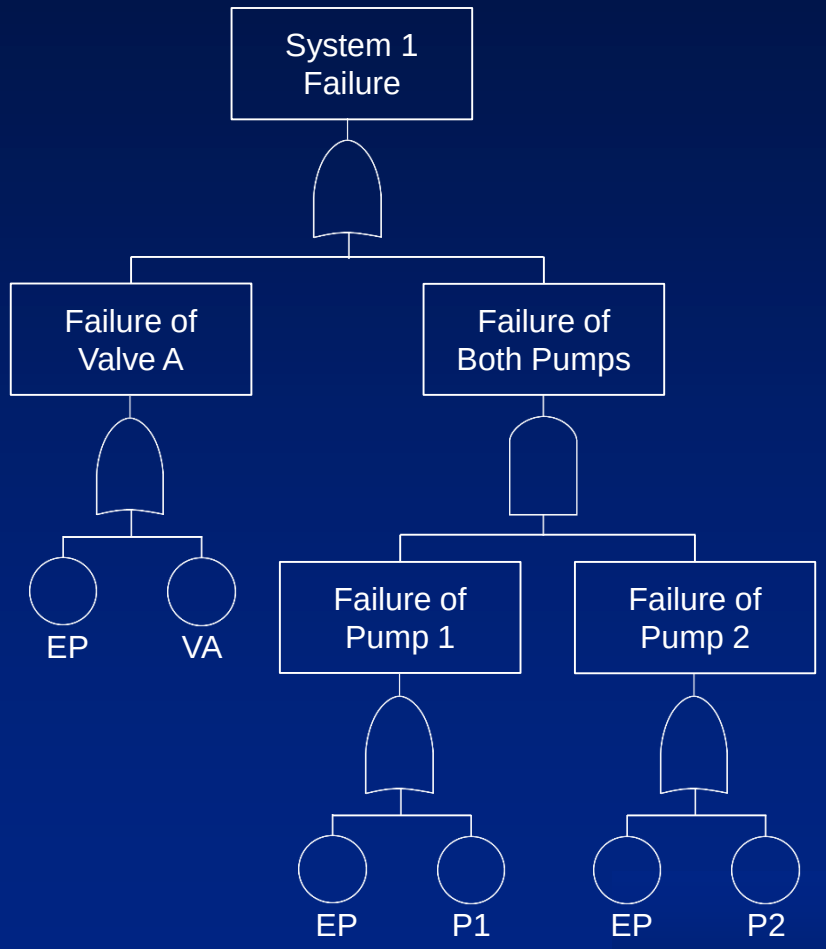
Linked Fault Tree Example



Fault Tree for System 1

Assume

- Each pump can supply the necessary flow (i.e., the pumps are redundant), so system failure requires both pumps to fail
- The pumps and the valve have the same electric power source (EP)



Boolean Operators, Laws, etc

- AND: also ∩ ∧ and multiplication symbols (e.g., ·)
- OR: also ∪ ∨ and addition symbols (e.g., +)
- NOT: also / and overscore

- $A \cup \bar{A} = \text{True}, A \cap \bar{A} = False$
- $A \cup B = B \cup A, A \cap B = B \cap A$
- $(A \cup B) \cup C = A \cup (B \cup C), (A \cap B) \cap C = A \cap (B \cap C)$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C), A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup A = A, A \cap A = A$
- $A \cup (A \cap B) = A$
- $\overline{A \cap B} = \bar{A} \cup \bar{B}, \overline{A \cup B} = \bar{A} \cap \bar{B}$

Application: Fault Tree to Boolean

- System 1 failure:

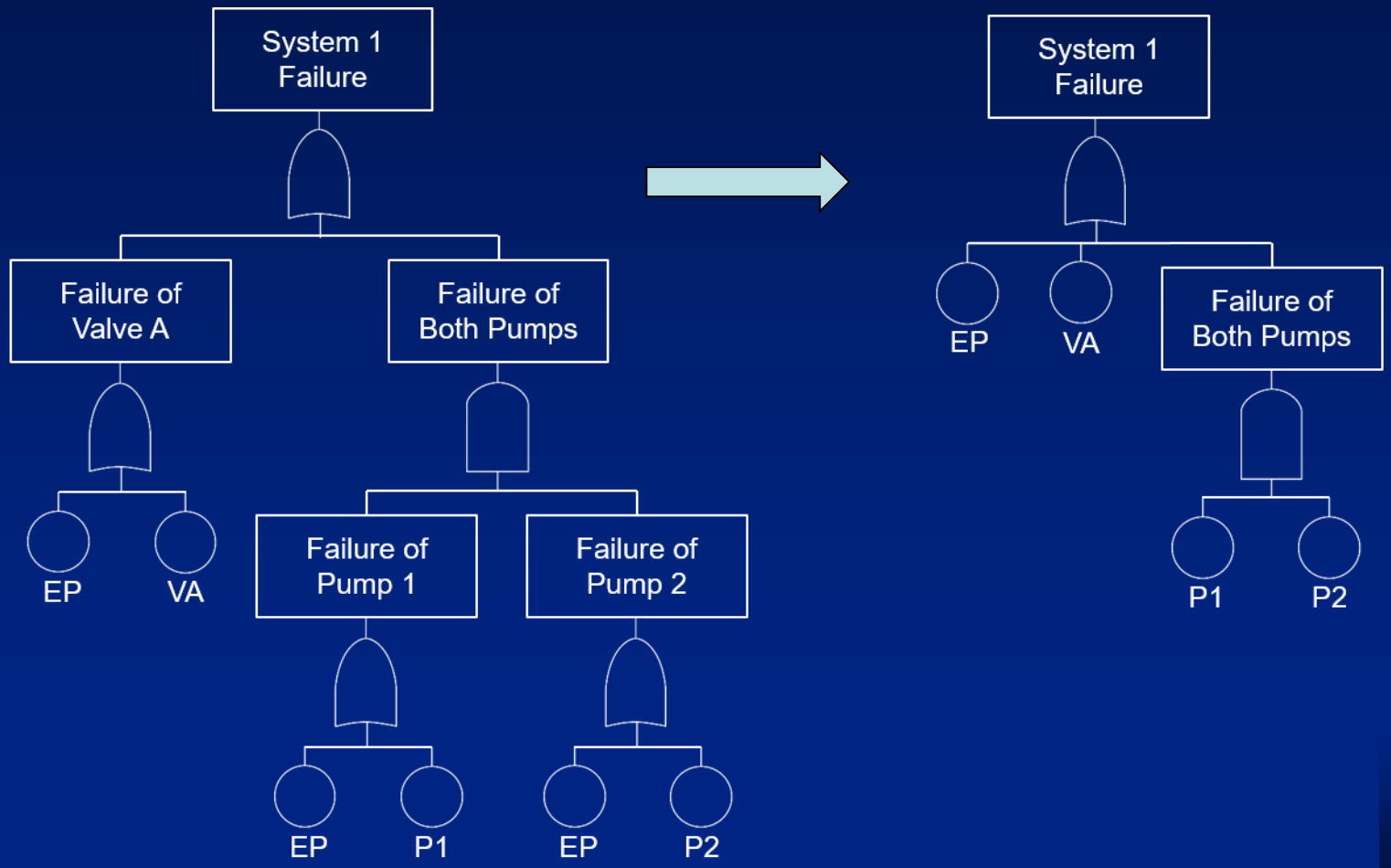
$$S1 = (EP \cup VA) \cup [(EP \cup P1) \cap (EP \cup P2)]$$
$$= (EP \cup VA) \cup [EP \cup (EP \cap P1) \cup (EP \cap P2) \cup (P1 \cap P2)]$$
$$= EP \cup VA \cup (PA \cap PB)$$

- More generally, a fault tree can be drawn as the conjunction/union (OR) of all of the minimal cut sets

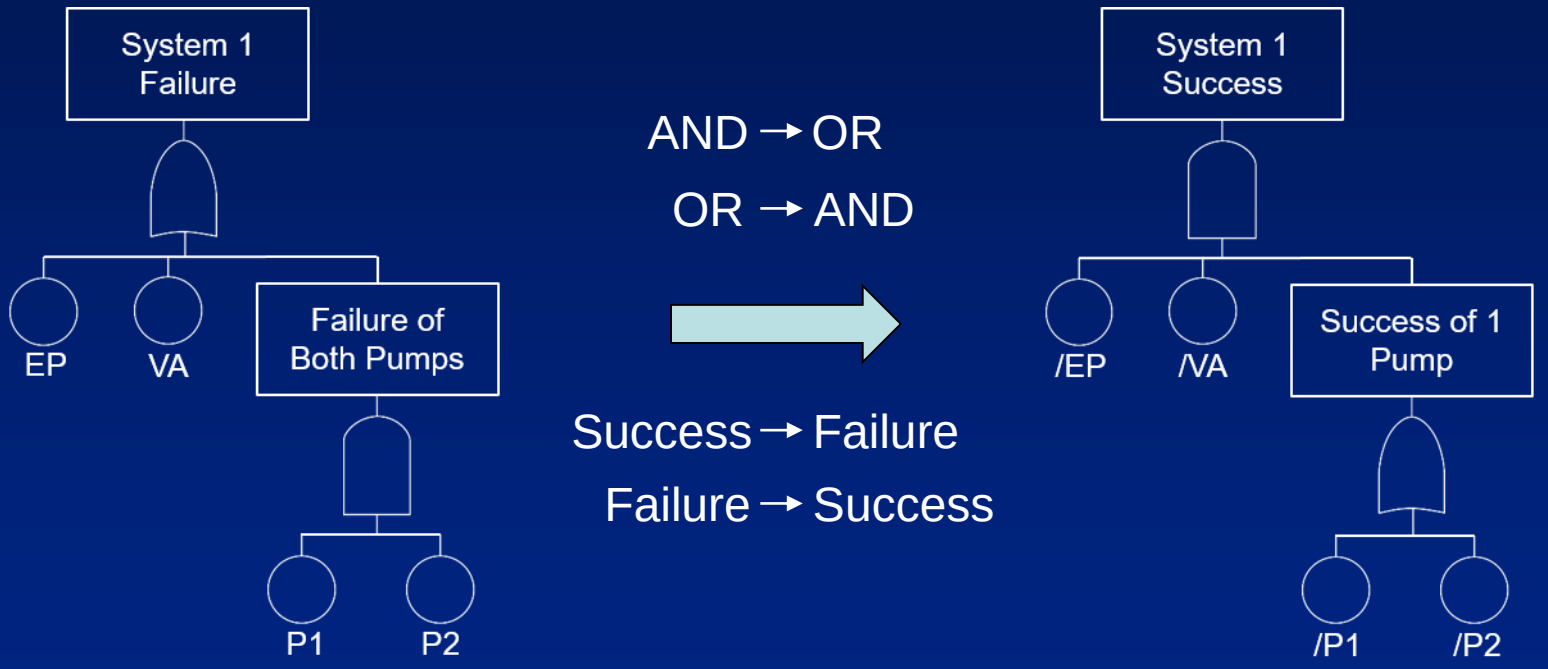
$$Top = \bigcup_{i=1}^{N_{MCS}} MCS_i$$

where MCS_i is the disjunction/intersection (AND) of the basic elements in the MCS

Simplification via Boolean Reduction



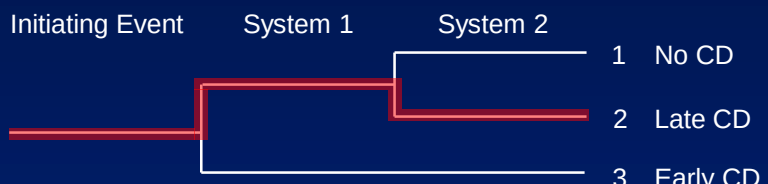
Application: Fault Tree to Success Tree, Minimal Cut Sets to Minimal Path Sets

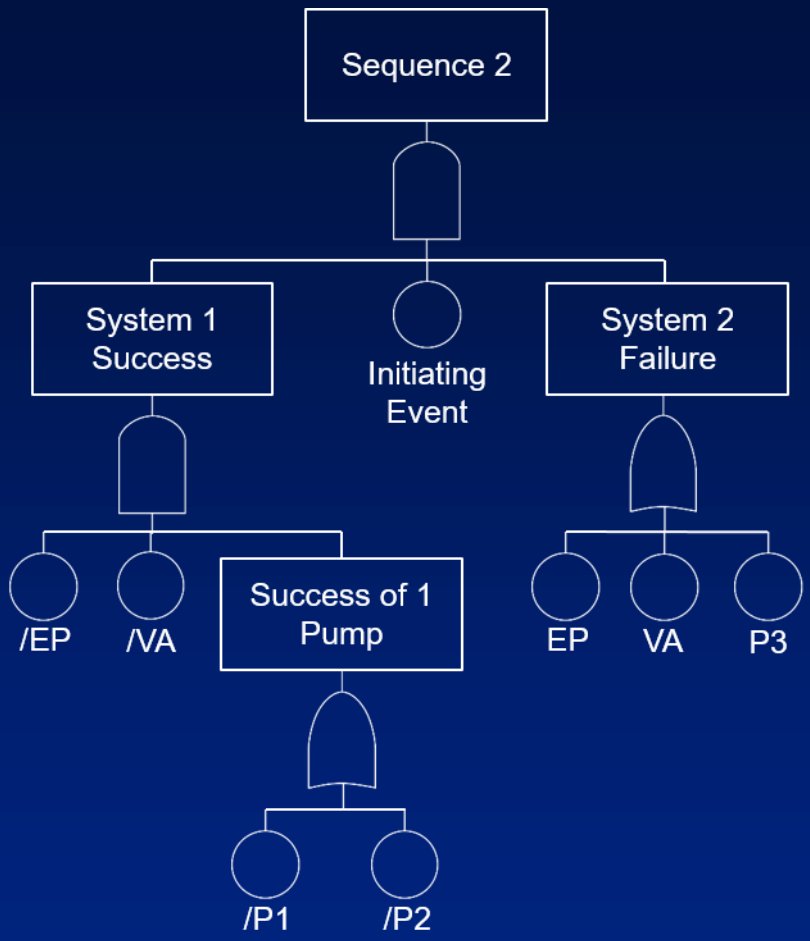


MCS = {EP}, {VA}, {P1, P2}

MPS = {/EP, /VA, /P1}, {/EP, /VA}, /P2}

Linked Fault Tree

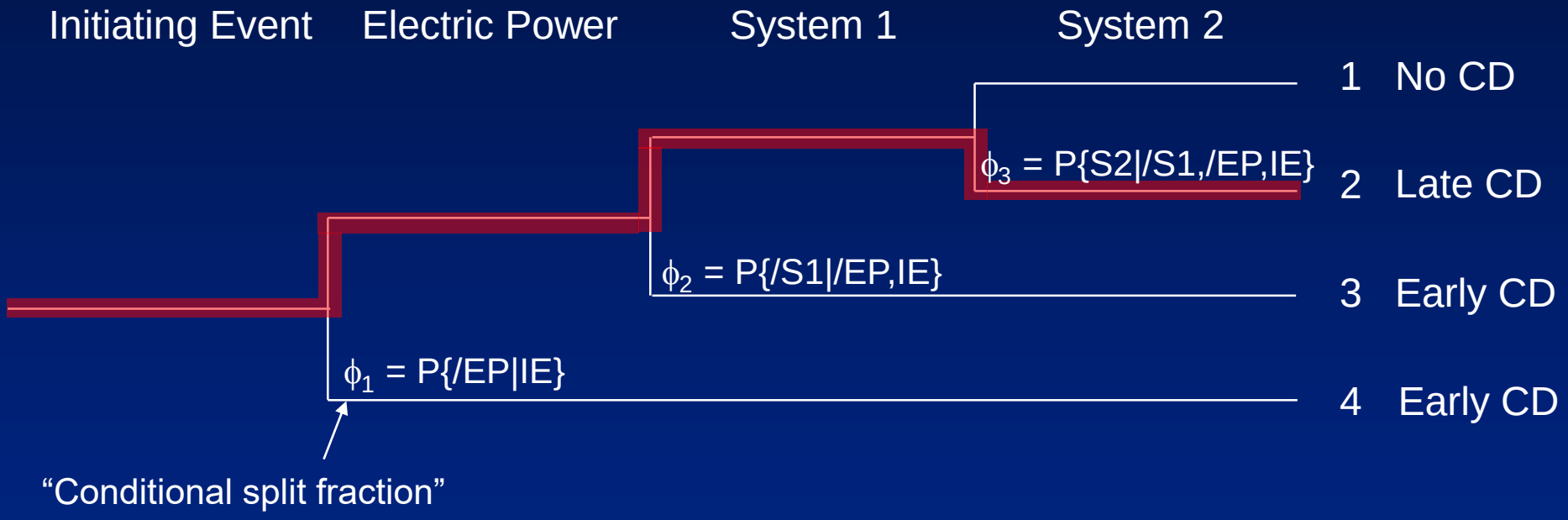




S2 = IE ∩ [{/EP, /VA, P1} U {/EP, /VA}, /P2}] ∩ [{EP} U {VA} U {P3}]
= IE ∩ [{/EP, /VA, P1} U {/EP, /VA}, /P2}] ∩ {P3}

Cut Sets: {IE, /EP, /VA, /P1, P3}, {IE, /EP, /VA, /P2, P3}

Event Tree w/Boundary Conditions Example



$$S_2 = IE \cap \{\overline{EP}|IE\} \cap \{\overline{S1}|\overline{EP}, IE\} \cap \{S2|\overline{S1}, \overline{EP}, IE\}$$

$$= IE \cap /EP \cap /S1 \cap S2 \quad \text{(conditions are understood)}$$

$$\lambda_2 = \lambda_{IE}(1-\phi_1)(1-\phi_2)\phi_3$$

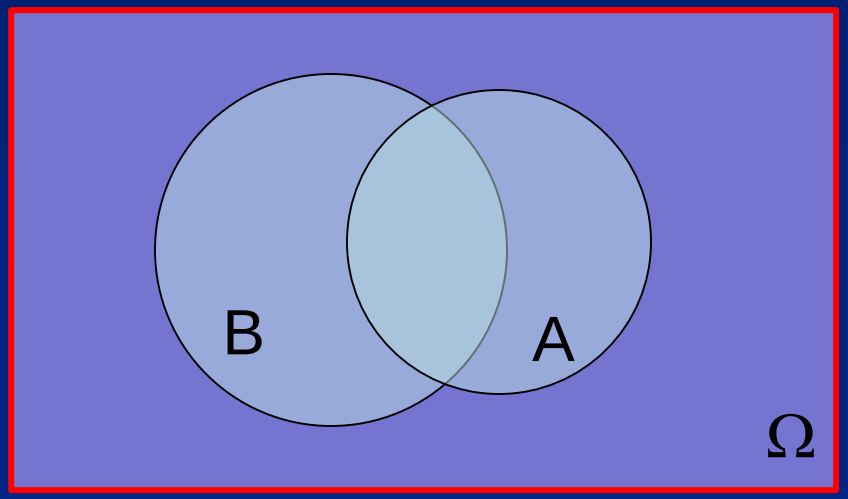
Reminder – Conditional Probability

- Definition

"A given B" => B is assumed to be true

$$P\{A|B\} \equiv \frac{P\{A \cap B\}}{P\{B\}}$$

- Venn Diagram



"A given B" => The universe of possibilities is reduced to B

Linked Fault Trees vs Event Trees w/Boundary Conditions

- Linked fault trees
  - Used by most PRA software
  - Focus on modeling top events; fault tree software deals with logic-based dependencies
  - Special basic event or post-processing rules needed to address other dependencies
  - Qualitative information: sequence cut sets, cut sets
- Event trees with boundary conditions
  - Less used
  - Can be used with reliability block diagrams (discussed later)
  - Focus on conditional probabilities, dependencies
  - Qualitative information: sequences

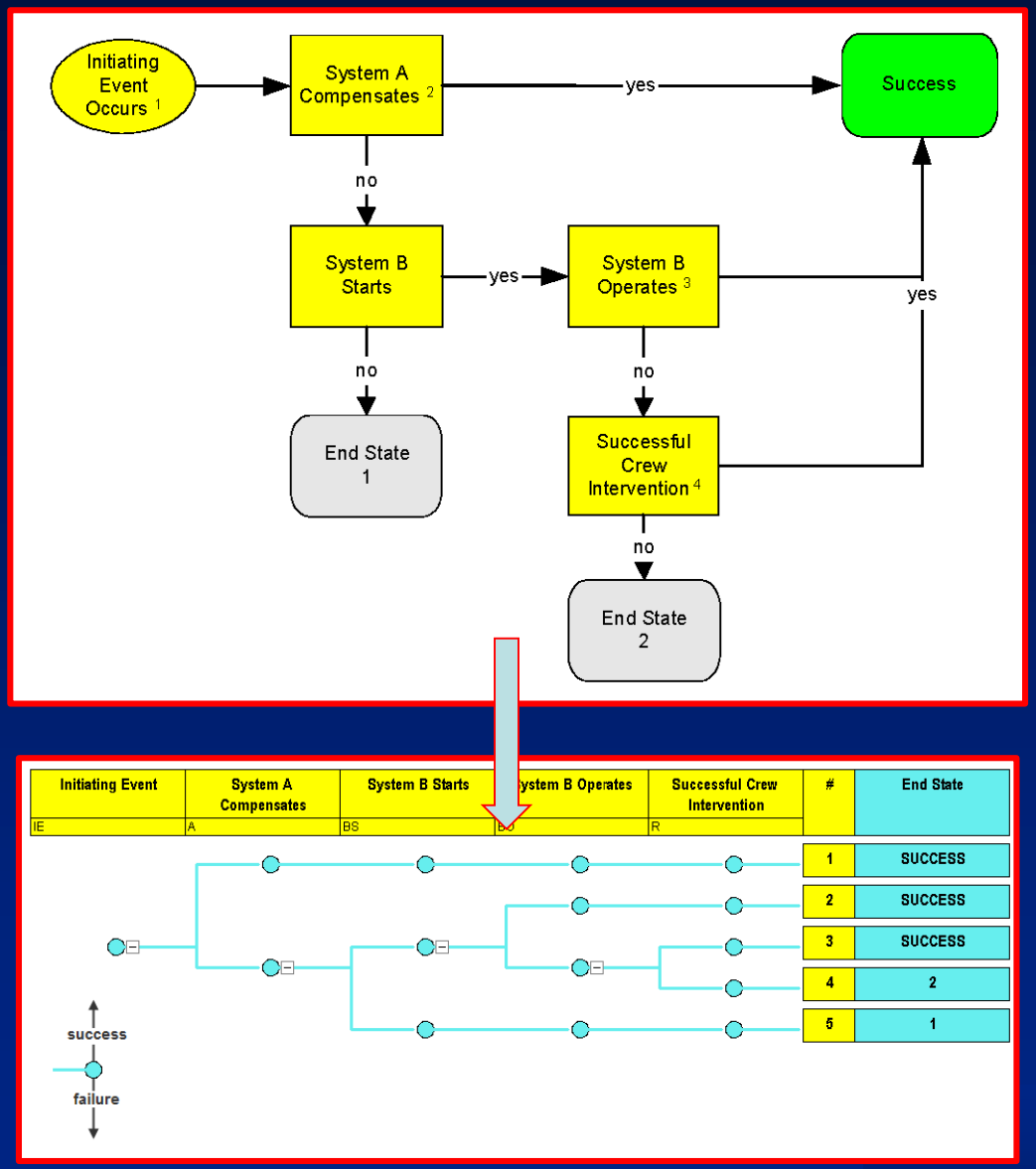
Useful Tools for Plant Modeling

- Event Sequence Diagrams (ESDs)
- Dependency Matrices
- Note: tools are useful for
  - Documenting understanding of system
  - Supporting learning by doing (“active learning”)

Event Sequence Diagrams

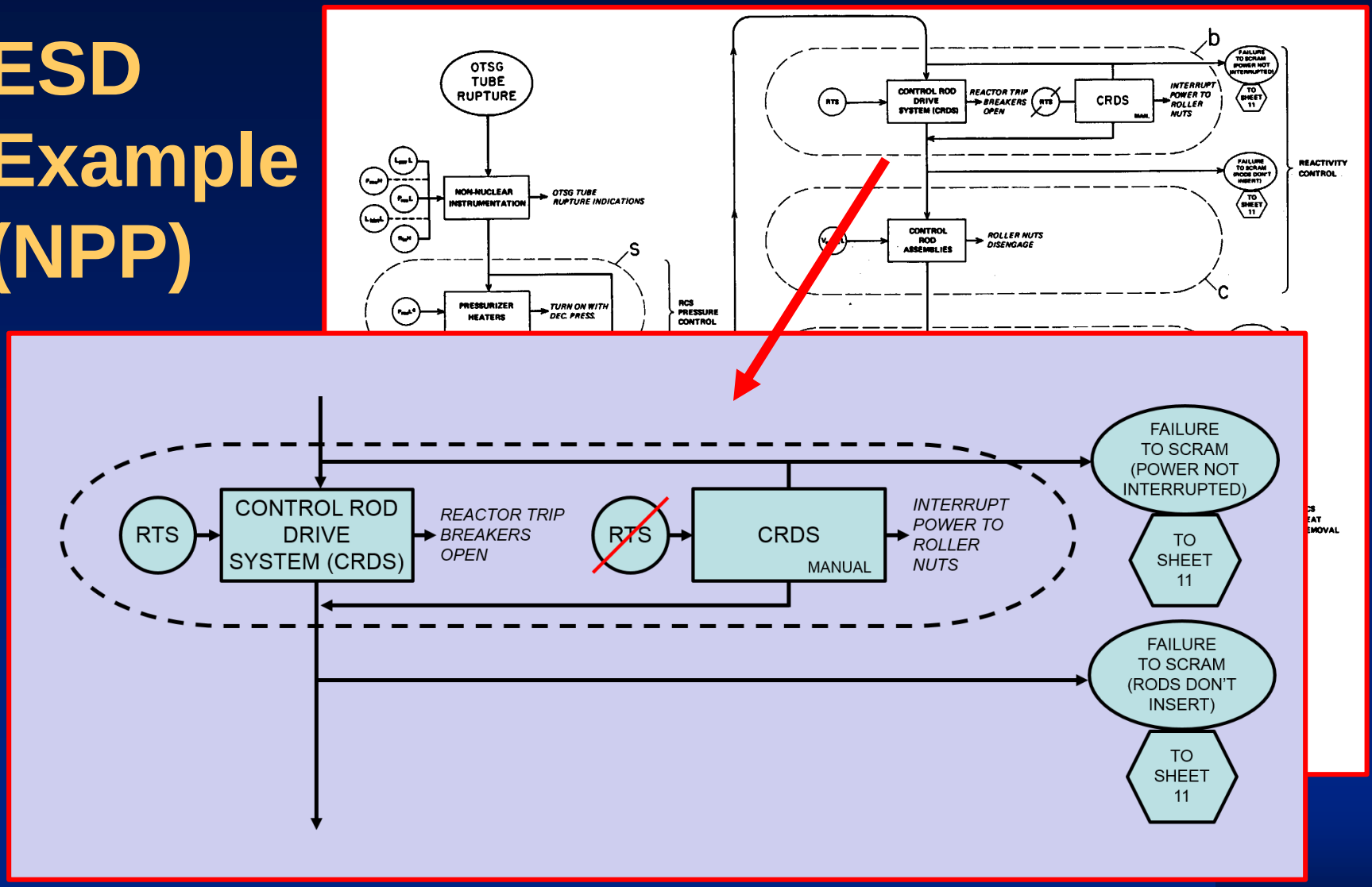
- Flowchart representing potential scenarios
- Not necessary for simple problems but…
  - Helps structure thinking regarding myriad possibilities
  - Can provide a more literal, richer scenario picture ("story") than event trees
    - Key parameters and indications
    - Important trends
    - Loops
    - Modeling assumptions
  - ***Documents understanding***

ESD Concept



Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, *NASA/SP-2011-3421, 2nd ed.*, 2011

ESD Example (NPP)



American Nuclear Society and the Institute of Electrical and Electronics Engineers, "PRA Procedures Guide," *NUREG/CR-2300*, January 1983.

Dependency Matrices

- Tool to help understand and document functional dependencies between systems (and even trains)
- Example:

	Support Systems					Frontline Systems			
	OP	AC-A	AC-B	SW-A	SW-B	LPI-A	LPI-B	LPR-A	LPR-B
OP	X								
AC-A		X		X		X		X	
AC-B			X		X		X		X
SW-A		(1)		X		X		X	
SW-B			(1)		X		X		X

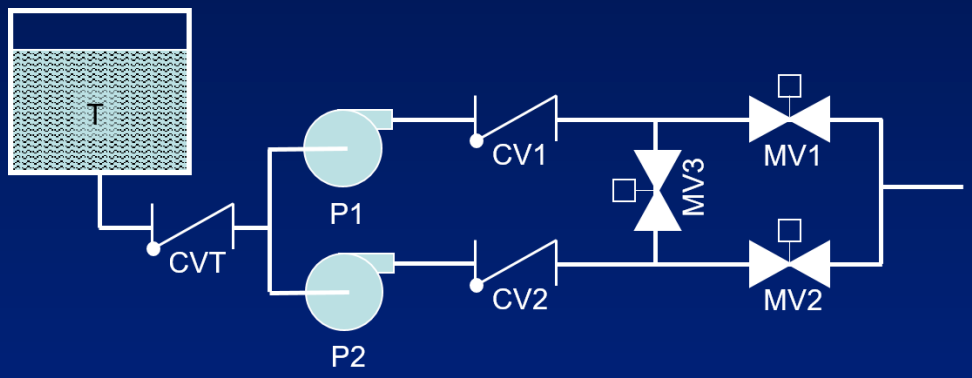
(1) Failure of service water leads to loss of EDG cooling and eventual LOSW (if offsite power is not available).

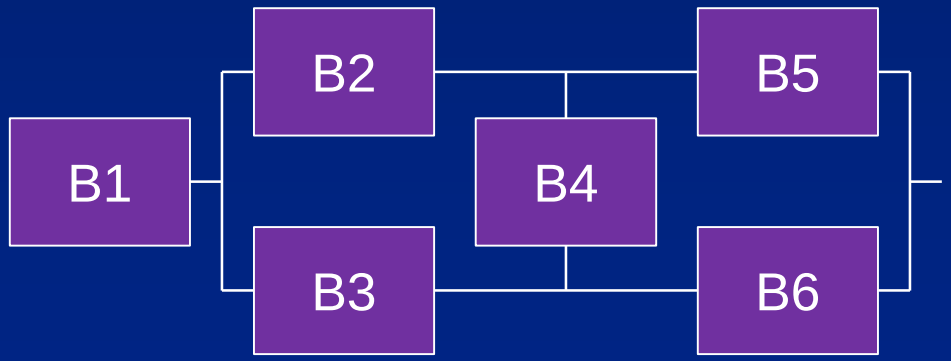
System Modeling Tools

- Fault Trees
- Reliability Block Diagrams
- Object-Oriented Simulation (Lecture 9-3)

Reliability Block Diagrams

Success-oriented, quantitative reliability models





$$P_{B1} \approx P_T + P_{CVT}$$
$$P_{B2} \approx P_{P1} + P_{CV1}$$
$$P_{B3} \approx P_{P2} + P_{CV2}$$
$$P_{B4} = P_{MV3}$$
$$P_{B5} = P_{MV1}$$
$$P_{B6} = P_{MV2}$$

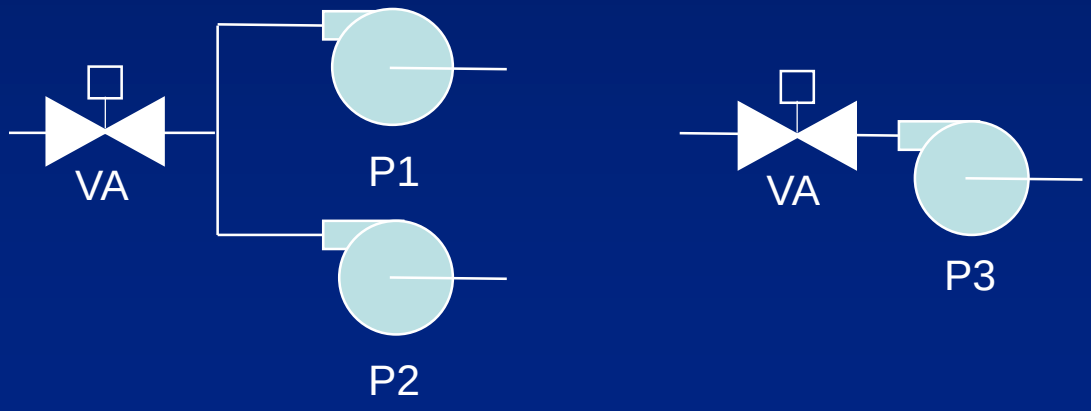
$$P_{MCS1} = P_{B1}$$
$$P_{MCS2} = P_{B2} \cdot P_{B3}$$
$$P_{MCS3} = P_{B5} \cdot P_{B6}$$
$$P_{MCS4} = P_{B2} \cdot P_{B4} \cdot P_{B6}$$
$$P_{MCS4} = P_{B3} \cdot P_{B4} \cdot P_{B5}$$

$$P_{Sys} < \underbrace{\coprod_{i=1}^{5} P_{MCS_i}}_{\text{min cut upper bound}} < \underbrace{\sum_{i=1}^{5} P_{MCS_i}}_{\text{rare event}}$$

where $\coprod_i P_i \equiv 1 - \prod_i (1 - P_i)$

Comment – Details Matter

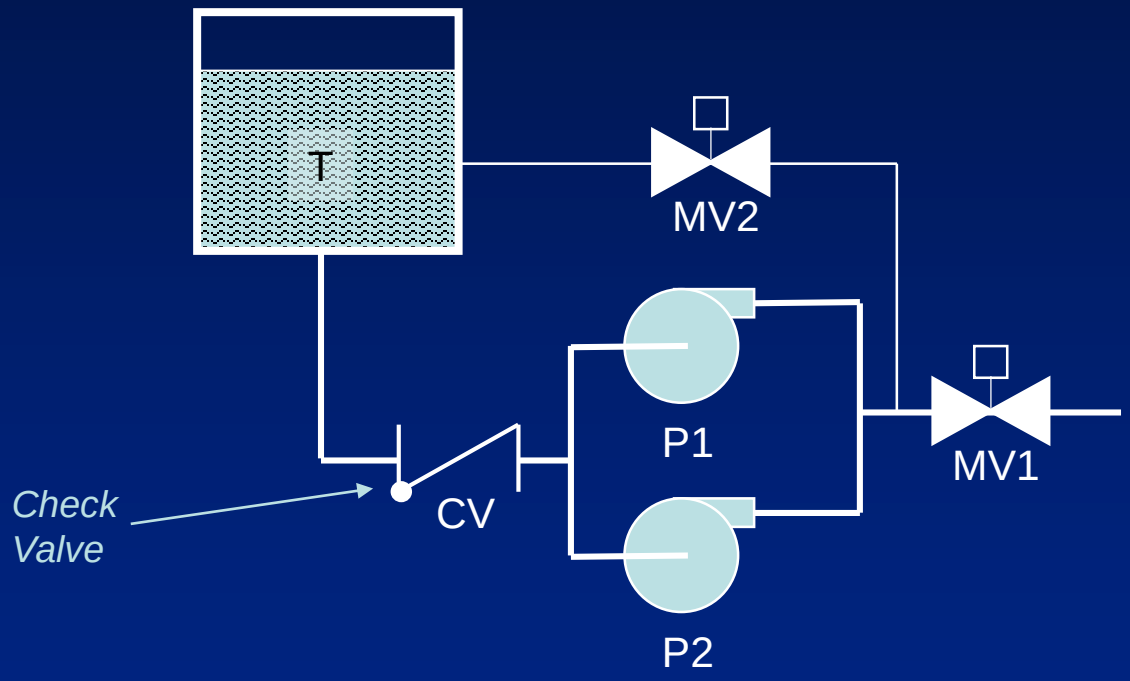
- Including the same component in different system models is OK (software algorithms will do Boolean reduction) but errors in labeling can cause errors in results.
- Example: What happens if the analyst for System 1 labels Valve A as S1-VA and the analyst for System 2 labels that valve as S2-VA?



System 1 System 2

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

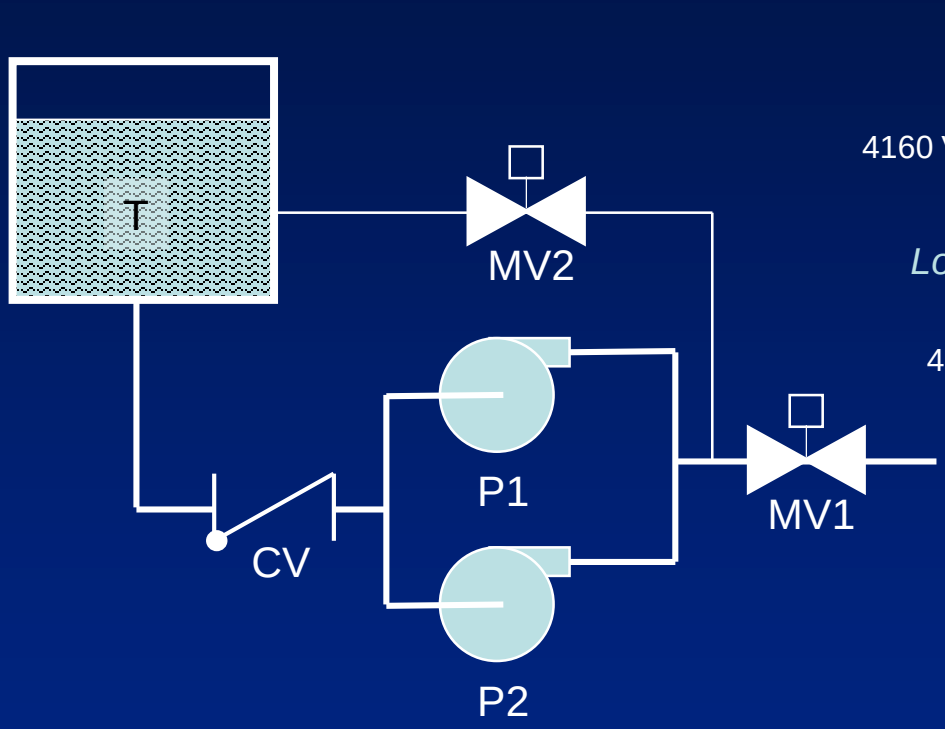
Knowledge Check

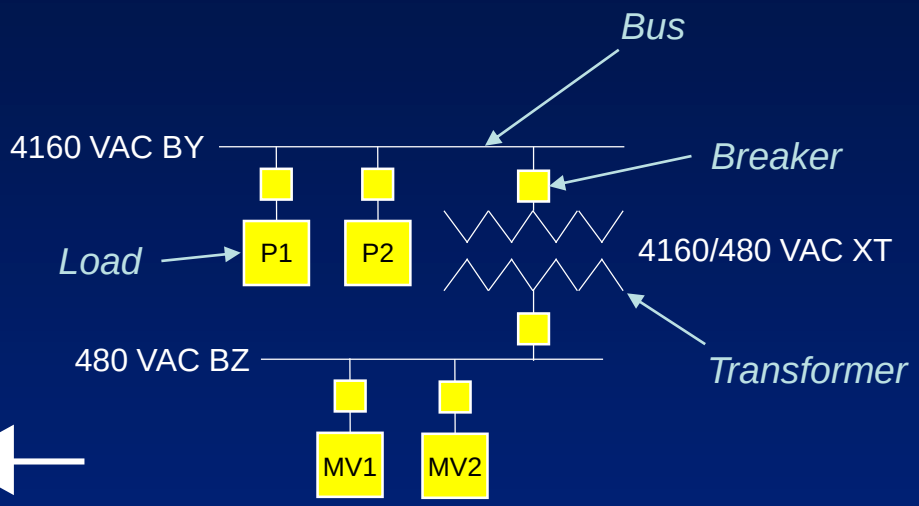


- MCS if each pump can provide 100% flow?
- MCS if each pump can provide 50% flow?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Knowledge Check (cont.)



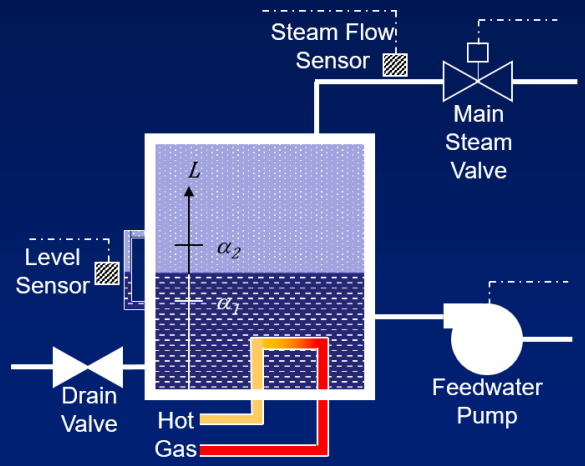


Now what are the minimal cut sets?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Thought Exercise

The plant manager, who's been working at the plant for 40 years, looks at your fault tree for the boiler. He sees that the manual valve at the bottom of the boiler is a "single point failure" (i.e., a single element MCS). He growls at you "Whaddya mean, the valve is going to disappear? And anyways there's no such thing as a random failure!"



What's your response? Hint: There are a number of reasonable choices, but "I'm just doing my job," is probably not one.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Closing Remarks

- Rare events => need to search for potential contributors
- Formal tools (e.g., MLDs, ESDs) can:
  - help the analyst think about the problem, aid the search process, and increase degree of completeness
  - document the analyst's understanding and key modeling assumptions
- Examples from past studies provide useful guidance; beware of treating them as templates