Initiating Events

Lecture 4-1

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

Key Topics

- NPP PRA definition of “initiating event”
- Methods to identify initiating events
- **Fundamental ethos: search for failures**

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

Resources

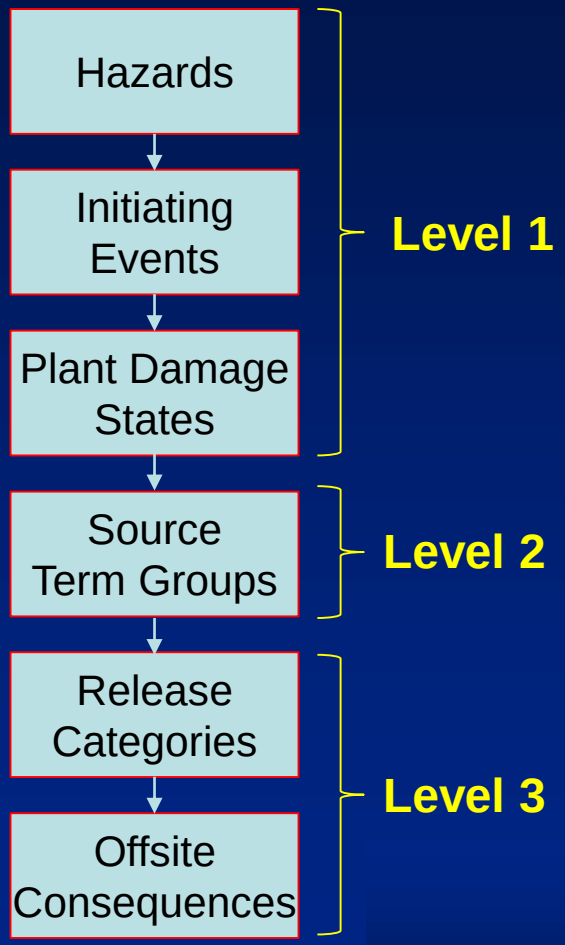
- American Nuclear Society and the Institute of Electrical and Electronics Engineers, “PRA Procedures Guide,” *NUREG/CR-2300*, January 1983
- H. Kumamoto and E.J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists, Second Edition*, IEEE Press, New York, 1996.
- T.A. Kletz, *Improving Chemical Engineering Practices: A New Look at Old Myths of the Chemical Industry, Second Edition*, Hemisphere Publishing, New York, 1990.
- H. Petroski, *To Engineer is Human: The Role of Failure in Successful Design*, Random House, New York, 1992.

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

NPP PRA – The "What"

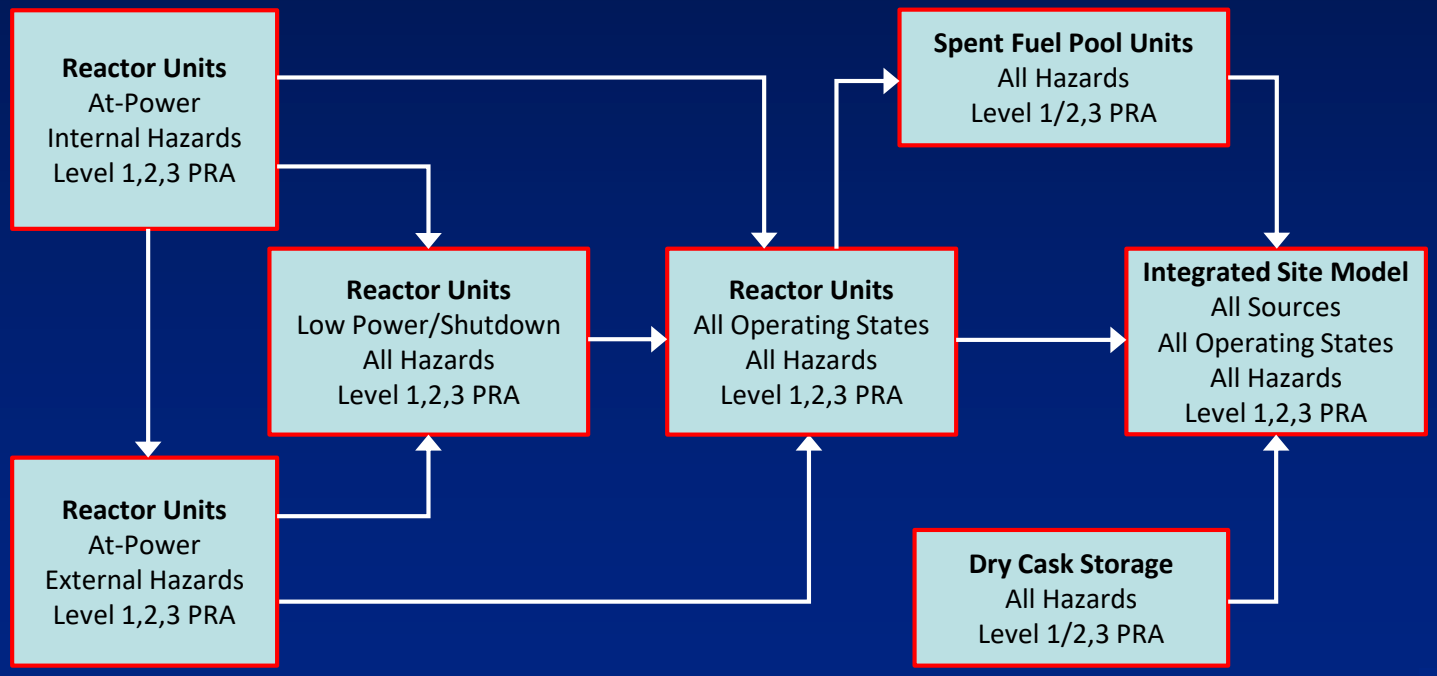
Risk ≡ $\{s_i, C_i, p_i\}$

- Levels
  - Level 1 (core/fuel damage)
  - Level 2 (radioactive release)
  - Level 3 (offsite consequences)
- Hazards
  - Internal events (hardware, human, LOOP)
  - Internal hazards (flood, fire, heavy load drops, …)
  - External hazards (seismic, flood, wind, …)
- Operating Mode
  - At power
  - Low power/shutdown
- Sources
  - Core
  - Spent fuel pool
  - Other (e.g., dry cask storage)



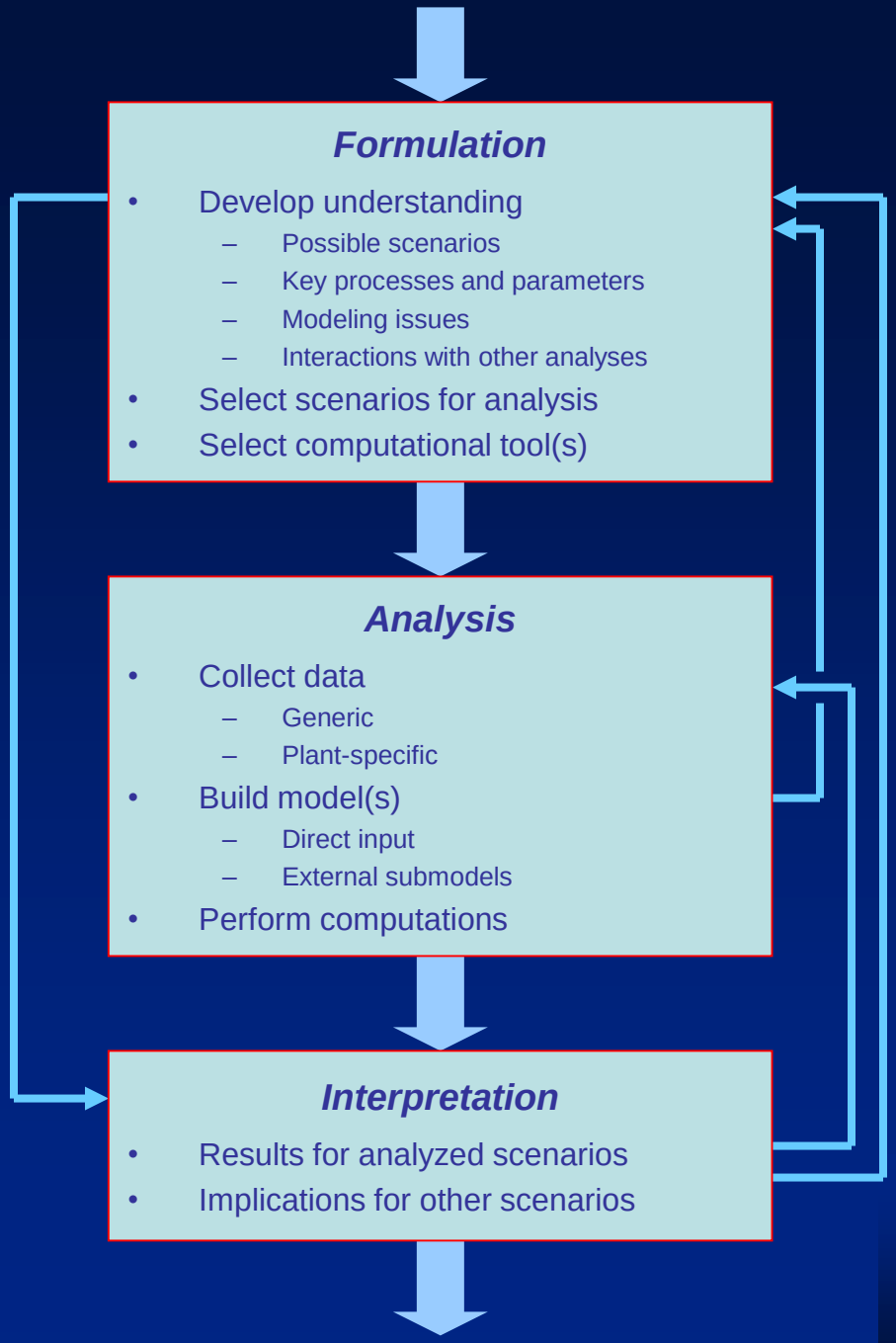
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NPP PRA – The "How" (Big Picture)



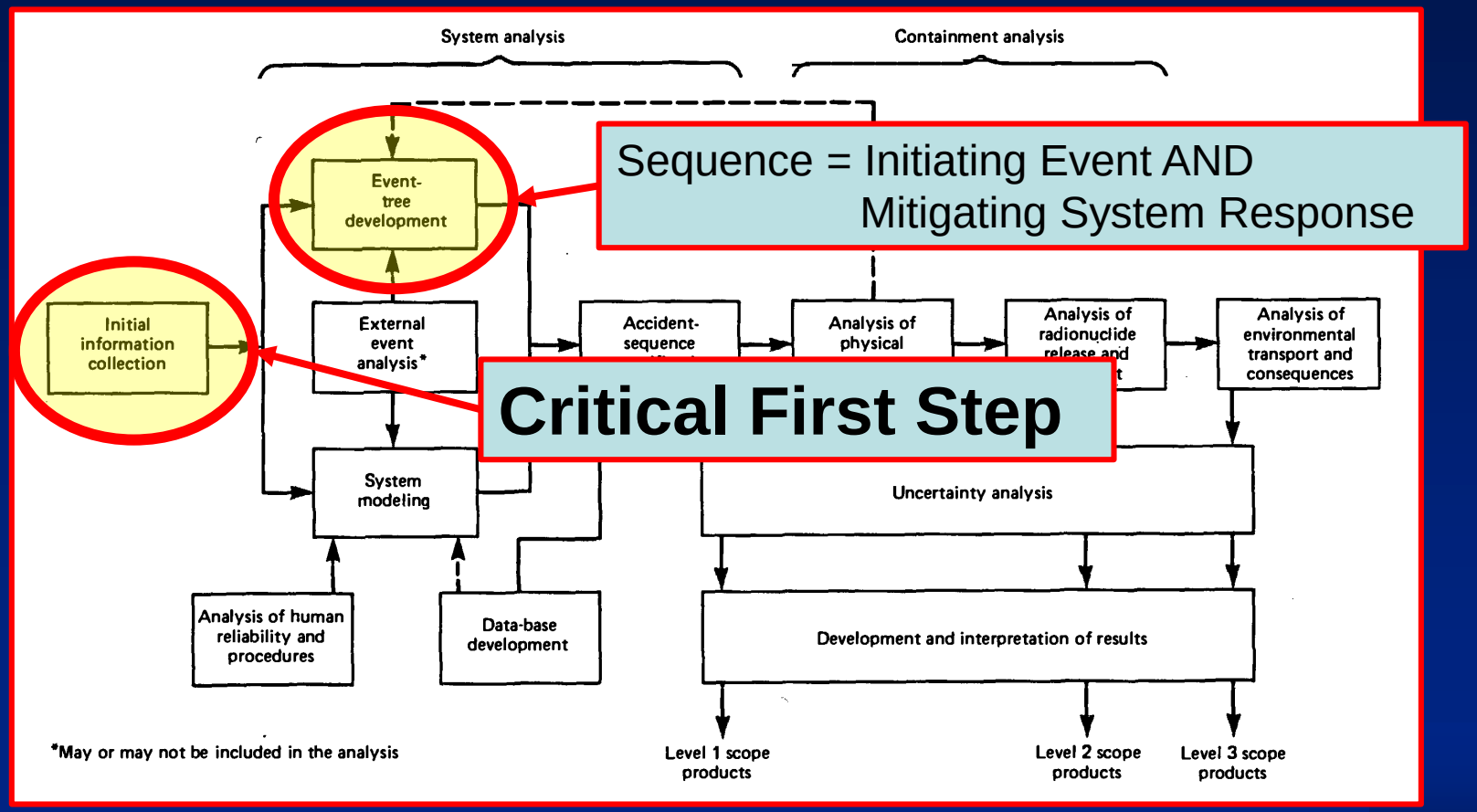
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

The General Modeling Process – One View



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

The Modeling Process – A More Detailed View



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

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

Where to start? Before the storm…*

It's Christmas Eve at the Bunbury Bay Nuclear Power Plant, "Old Reliable" to the crew and local residents, most of whom have friends or family working at the plant.

A severe Nor'easter took down powerlines a month ago, but, as with past blizzards, the plant rode it out, providing needed power to the region. Most of the workers, who had put in long hours to cope with the November storm and its aftermath, are home for a well-deserved rest over the holiday, and Old Reliable is purring along with a nearly minimum crew. (Some unlucky workers are earning overtime working on the plant's newer, air-cooled EDG, which is down for emergency repairs.) A low pressure area, formed in the Atlantic some two days ago, is being tracked but the disturbance is small. Although there are indications of intensification, weather forecasts provide no cause for serious alarm. There's snow on the ground and chestnuts are roasting…

*Thanks to Pierre LeBot (EDF) for parts of this story.

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

Where to start? The storm hits…

At around 3 pm, winds in the region start to rise; blowing snow cuts visibility and trees are swaying. The plant receives a warning that the disturbance had become a storm but its intensity and direction are unclear. Considering the conditions of the roads and crew, past plant performance, and the uncertainty in the weather model predictions, the plant manager decides to alert off-duty senior staff, but not to recall any workers.

At 5 pm, the storm hits the coast. Around 8:30 pm, severe wind gusts take down multiple power lines, disrupting the grid. The plant loses offsite power and trips at 8:32, and the water-cooled EDG starts and loads as designed. At 11:16 pm, wind-driven waves, on top of severe storm surge and an abnormally high tide (a beyond-design basis hazard combination), overtop and damage the protective seawall and start flooding the pump house, endangering service water (normal and emergency). The plant (an old, isolation condenser design) starts preparing to enter SBO conditions. Fortunately, an offsite power line is recovered at 11:34. Recognizing the unreliability of the grid under storm conditions, the plant starts reviewing its procedures to stay at hot shutdown conditions until grid stability can be assured. However, offsite power remains available and the plant achieves cold shutdown early Christmas morning.

Possible Choices

Event	Why?
November storm	Sets up plant workforce, activities, and attitudes, and offsite conditions. Could support risk-informed post-storm operations decisions
Low pressure formation	Natural starting point if using storm simulation modeling. Could support risk-informed early storm preparations.
Storm warning (3 pm)	Deteriorating conditions; warning triggers decision (whether to recall staff). Could support risk-informed response.
Storm hits coast	Natural “event” for storm-oriented analysis.
LOOP	Start of nuclear transient.
Pumphouse flooding	Not a great choice for a literal analysis, but could be “moved up” to coincide with LOOP in a PRA.

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

Convention for "Initiating Event"

Initiating Event, Initiator

An event that perturbs the steady-state operation of the plant and could lead to an undesired plant condition.	In a PRA, an initiating event is an event originating from an internal or external hazard that both challenges normal plant operation and requires successful mitigation. As such, these events represent the beginning of accident sequences modeled in the PRA. Having a reasonably complete set of initiating events is crucial in determining what events could propagate to core damage. Initiating events can arise from the following: • <u>Internal Hazards, which include:</u> — Internal event (*see Internal Event*) — Floods (*see Internal Flood*) — Fires (*see Appendix A for fire terms*) • <u>External Hazards, which include:</u> — Floods (*see External Flood*) — High winds (*see High Winds*) — Seismic events (*see Hazard Analysis*) — Other external hazards These hazards result in different types of initiating events. Examples of initiating events are transients (*see Transient*) and loss-of-coolant accidents (*see Loss-of-Coolant Accident*). The terms initiating event and initiator are both used in a PRA context and generally have the same meaning. In some cases, the term initiator may refer to a class of initiators (e.g., transient), while the term initiating event may refer to the actual event (e.g., loss of a feedwater pump resulting in a transient).

- *Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking*, NUREG-2122, 2013

Identifying Initiating Events

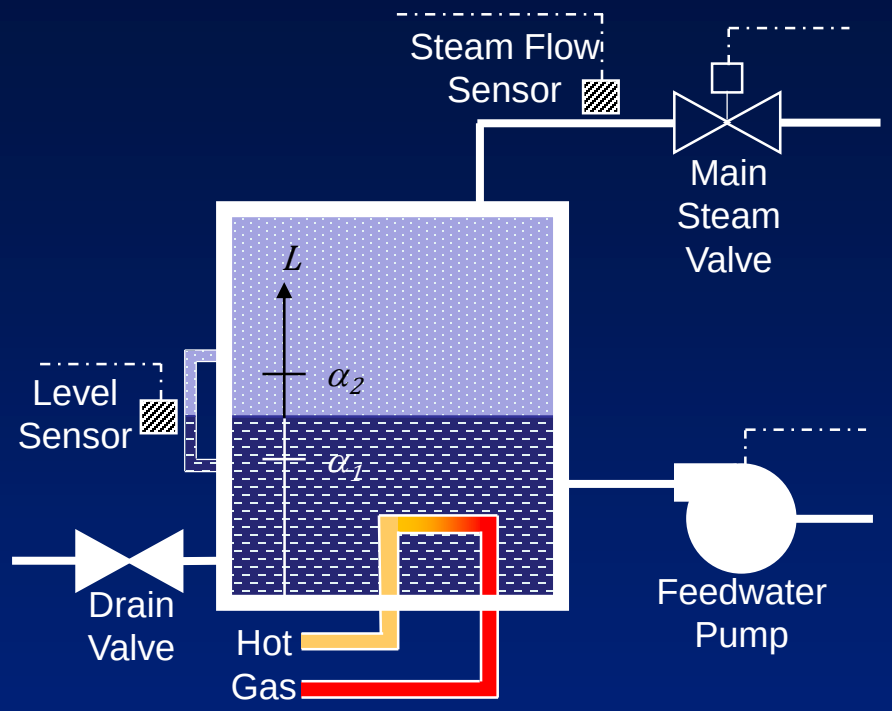
- Tools/approaches include:
  - Failure Modes and Effects Analysis (FMEA)
  - Hazard and Operability Studies (HAZOPS)
  - Master Logic Diagrams (MLD)
  - Heat Balance Fault Trees
  - Review of past events
  - Comparison with other studies
  - Feedback from plant model
- If it's not in the model, it can't be analyzed. "Use your imagination…"

…but

- Frame as a “search” (more active, directed than “imagining”)
- Screen out unimportant events to enable practical solution and avoid distractions
  - Limited analysis resources
  - Risk masking from overly conservative analyses
- Recognize challenges
  - Completeness
  - Data relevance (and “rectifiability”)

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

Example for Demonstrations: A Simple Boiler



		Desired State		
Steam Flow	Liquid Level	MS Valve	FW Pump	Hot Gas
$\dot{M} \leq \dot{m}^*$	$\alpha_1 < L < \alpha_2$	Open	On	On
$\dot{M} \leq \dot{m}^*$	$L \geq \alpha_2$	Open	Off	On
$\dot{M} \leq \dot{m}^*$	$L \leq \alpha_1$	Closed	On	Off
$\dot{M} > \dot{m}^*$	-	Closed	Off	Off

FMEA – Principles

- Inductive approach – postulate failures and determine effects
- Apply to all elements in system
- Uses standardized terms
- FMECA: add "criticality analysis"

TABLE 3.4. Generic Failure Modes

No.	Failure Mode	No.	Failure Mode
1	Structural failure (rupture)	19	Fails to stop
2	Physical binding or jamming	20	Fails to start
3	Vibration	21	Fails to switch
4	Fails to remain (in position)	22	Premature operation
5	Fails to open	23	Delayed operation
6	Fails to close	24	Erroneous input (increased)
7	Fails open	25	Erroneous input (decreased)
8	Fails closed	26	Erroneous output (increased)
9	Internal leakage	27	Erroneous output (decreased)
10	External leakage	28	Loss of input
11	Fails out of tolerance (high)	29	Loss of output
12	Fails out of tolerance (low)	30	Shorted (electrical)
13	Inadvertent operation	31	Open (electrical)
14	Intermittent operation	32	Leakage (electrical)
15	Erratic operation	33	Other unique failure condition as applicable to the system characteristics, requirements and operational constraints
16	Erroneous indication		
17	Restricted flow		
18	False actuation		

TABLE 3.5. Failure Modes and Effects Analysis [14]

Item	Failure Modes	Cause of Failure	Possible Effects	Probability	Criticality	Possible Action to Reduce Failure Rate or Effects
Motor case	Rupture	a. Poor workmanship b. Defective materials c. Transportation damage d. Handling damage e. Overpressurization	Damage by missile	0.0006	Critical	Manufacturing process control for workmanship to meet standards. Quality control of basic materials to eliminate defectives. Inspection and testing of completed cases. Suitable packaging to protect motor during transportation.
Propellant grain	a. Cracking b. Voids c. Bond separation	a. Abnormal stress b. Excessively low temperature c. Aging effects	Excessive burning rate; overpressurization; motor case rupture during operation	0.0001	Critical	Controlled production. Storage and operation only within temperature limits. Formulation to resist effects of aging.
Liner	a. Separation from motor case b. Separation from motor grain or insulation	a. Inadequate cleaning of motor case b. Use of unsuitable bonding material c. Inadequate bonding process control	Case rupture	0.0001	Critical	Strict observance of proper cleaning procedures. Strict inspection after cleaning of motor case to ensure that all contaiminants have been removed.

From H. Kumamoto and E.J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists, Second Edition*, IEEE Press, New York, 1996.

FMEA Partial Example (Boiler Problem)

Component	Failure Mode	Cause(s)	Effects
Pressure Vessel	Rupture	a. Overpressure b. Impact c. Corrosion d. Faulty materials e. Faulty construction f. Faulty installation g. …	a. Stops operation b. Hazards to operators, other components i. Steam ii. Flooding iii. Missile(s) iv. Displacement
Feedwater Pump	Fails to run	a. Mechanical failure (e.g., binding, rotor crack) b. Clogging c. Loss of power d. Incorrect control signal e. Incorrect operator action f. …	a. Stops system operation b. Creates demand for system response
…			

HAZOP – Principles

- Extension of FMEA
- Includes process parameter deviations
- Guide words "to stimulate creative thinking"
- Used extensively in chemical process industry

TABLE 3.6. Process Parameter Deviations for HAZOP

Process Parameter	Deviation
Flow	**No** flow **Reverse** flow **More** flow **Extra** flow **Change** in flow proportions Flow to **wrong place**
Temperature	**Higher** temperature **Lower** temperature
Pressure	**Higher** pressure **Lower** pressure
Volume	**Higher** level (in a tank) **Lower** level (in a tank) Volume rate changes **faster** than expected **Proportion** of volumes is **changed**
Composition	**More** component A **Less** component B **Missing** component C **Composition changed**
pH	**Higher** pH **Lower** pH **Faster** change in pH
Viscosity	**Higher** viscosity **Lower** viscosity
Phase	**Wrong** phase **Extra** phase

From H. Kumamoto and E.J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists, Second Edition*, IEEE Press, New York, 1996.

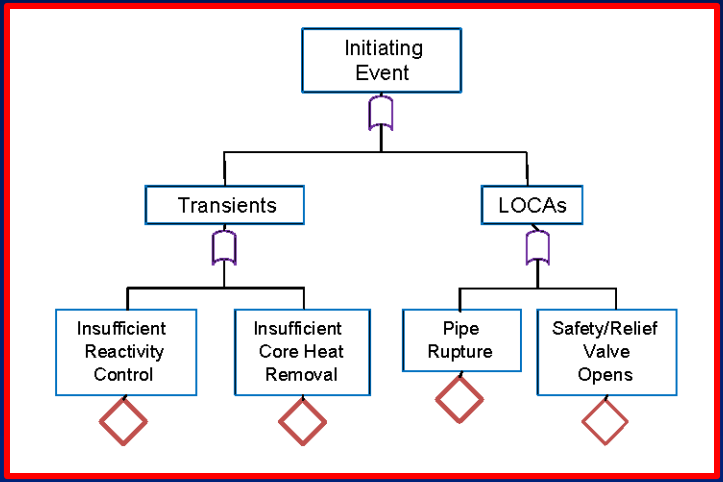
HAZOP Partial Example (Boiler Problem)

Process Parameter	Deviation	Effects
Gas Flow	No Flow	a. Stops operation b. Creates demand for system response (stop feedwater). If response fails, could lead to overfilling and possible flooding elsewhere
Gas Flow	More Flow	a. Increases steam generation rate. Depending on steam flow setpoint, could trigger system shutdown. b. Increases water boiloff rate. If feedwater can't compensate and steam flow setpoint isn't reached, could cause dryout and gas tube rupture.
…		

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

"Master Logic Diagram" – Principles

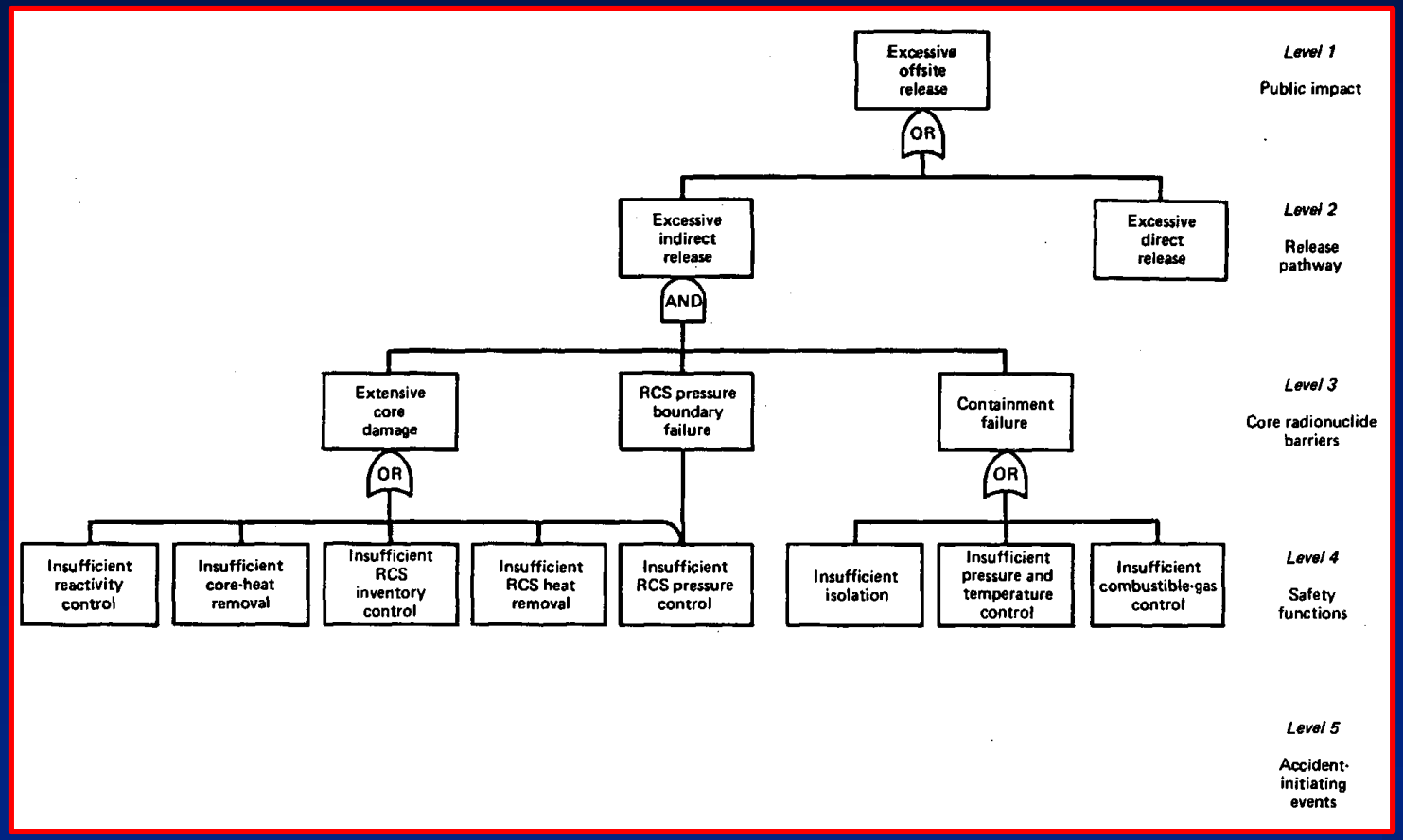
- Deductive approach
- Basically a fault tree; shows how a top event can occur
- "Heat Balance Fault Tree" is similar concept



"Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking," *NUREG-2122*, 2013

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

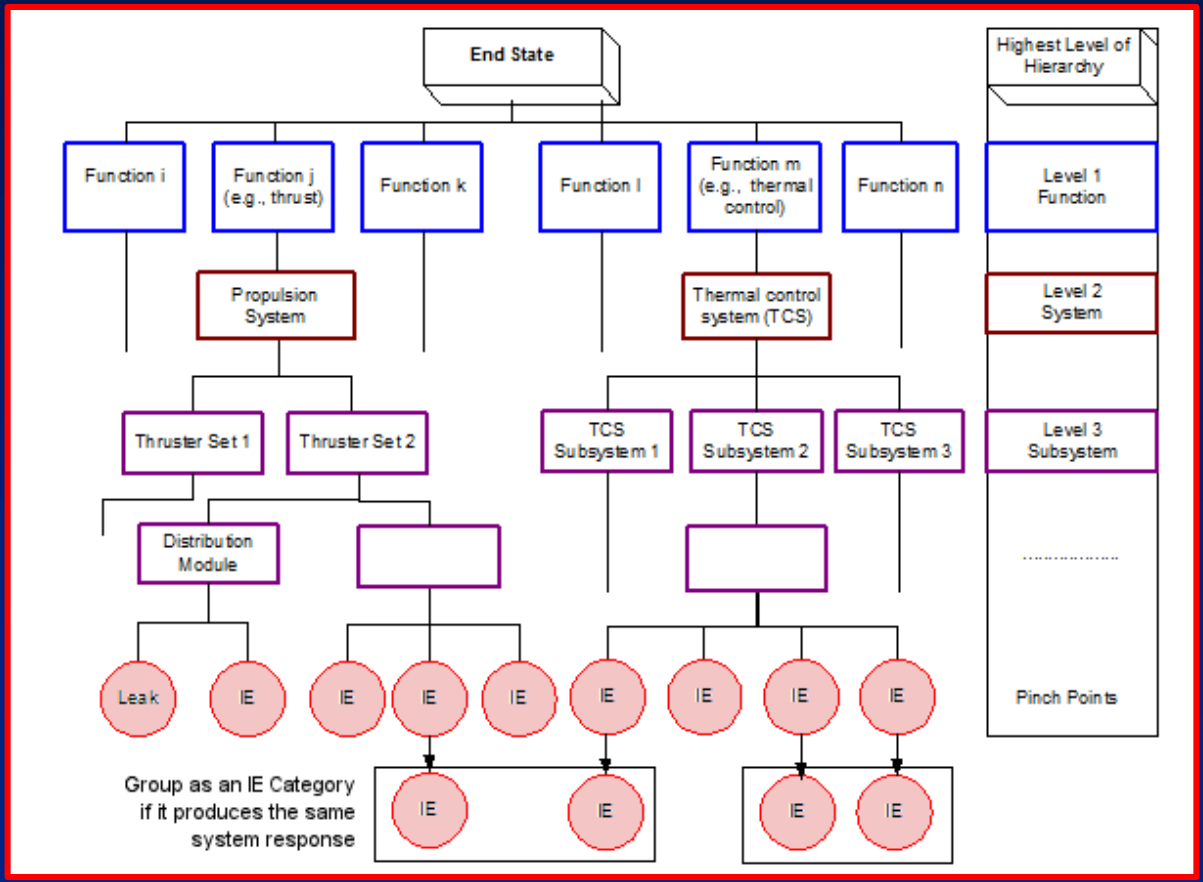
A Classic NPP MLD



"PRA Procedures Guide," *NUREG/CR-2300*, 1983

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

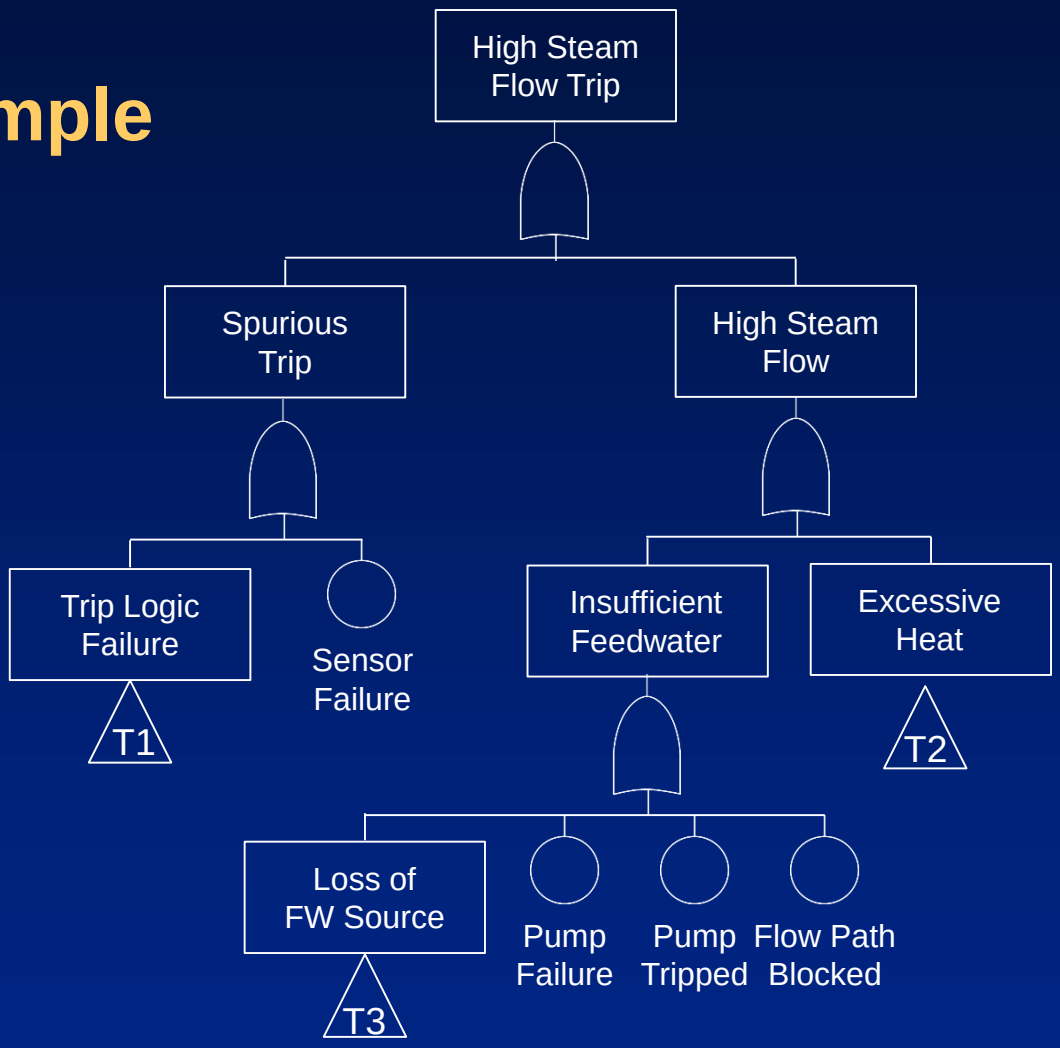
MLD for a Space Application



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

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

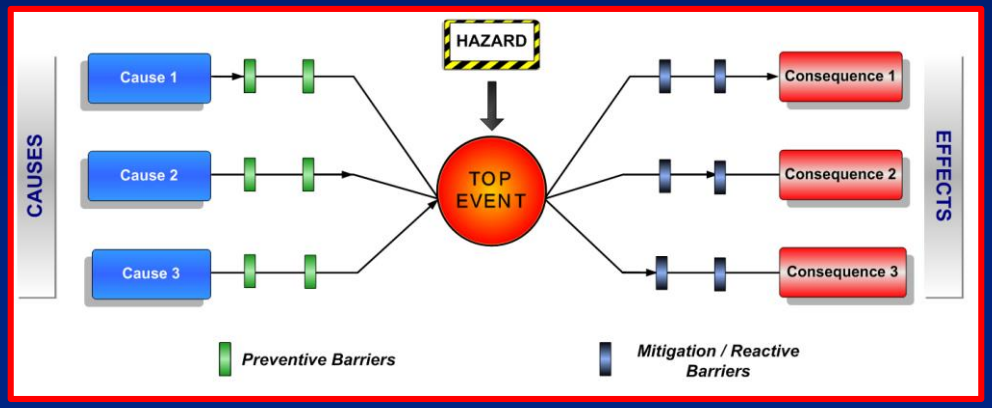
MLD Partial Example (Boiler Problem)



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

Other Frameworks

- Different representations of causality can:
  - Stimulate imagination
  - Facilitate communication with like-minded
- Example: “bowtie diagrams” are advocated for process applications



W. Nelson, “How Things Fail – e.g. Deepwater Horizon and Fukushima – and Occasionally Succeed,” Nov. 2, 2011

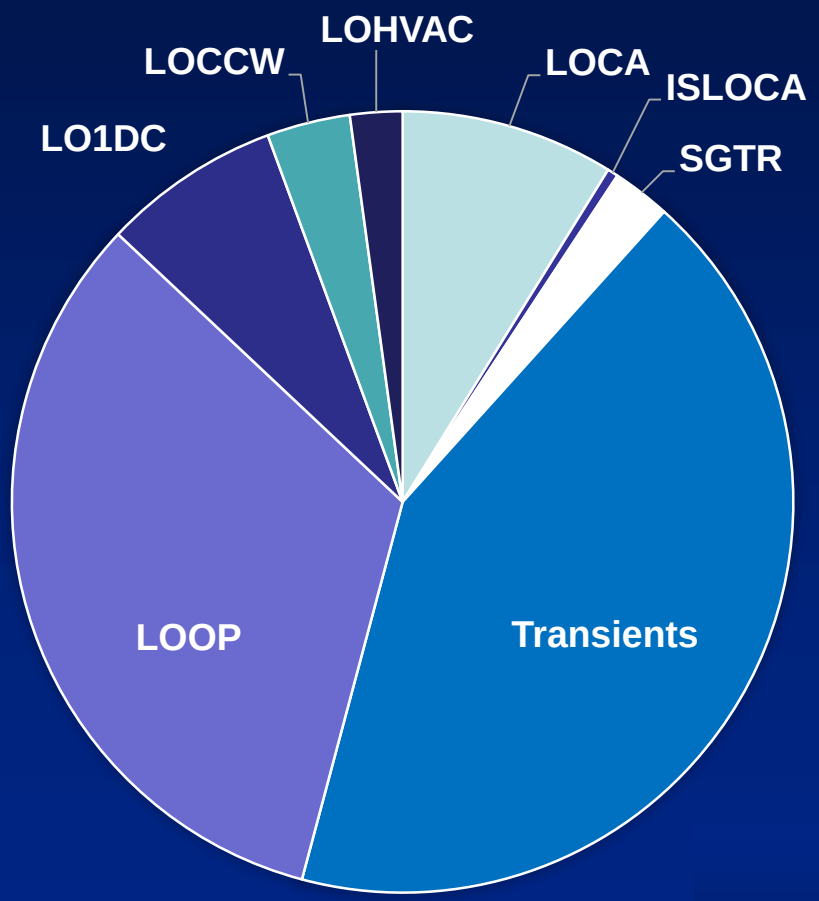
Operational Experience (OpE)

- Illustrates mechanisms and complexities that might otherwise be missed
- Examples
  - Water hammer in fire main causes reactor building flood
  - Lighted candle causes cable fire
  - Boat wake rocks submarine and causes reactivity accident
- OpE also can indicate where imagination might be going too far
- Non-NPP experience is potentially valuable (e.g., see Kletz)

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

Other Studies (NPP)

- Loss of offsite power
  - Plant-centered
  - Switchyard
  - Grid
  - Severe weather
- Loss of safety-related bus
- Loss of instrument or control air
- Loss of safety-related cooling water
- Loss of feedwater
- General transient
- Steam generator tube rupture
- Loss of coolant accident
  - Very small LOCA
  - Small LOCA
  - Medium LOCA
  - Large LOCA
  - Excessive LOCA
  - Interfacing system LOCA
  - Stuck-open relief valve
- High energy line break

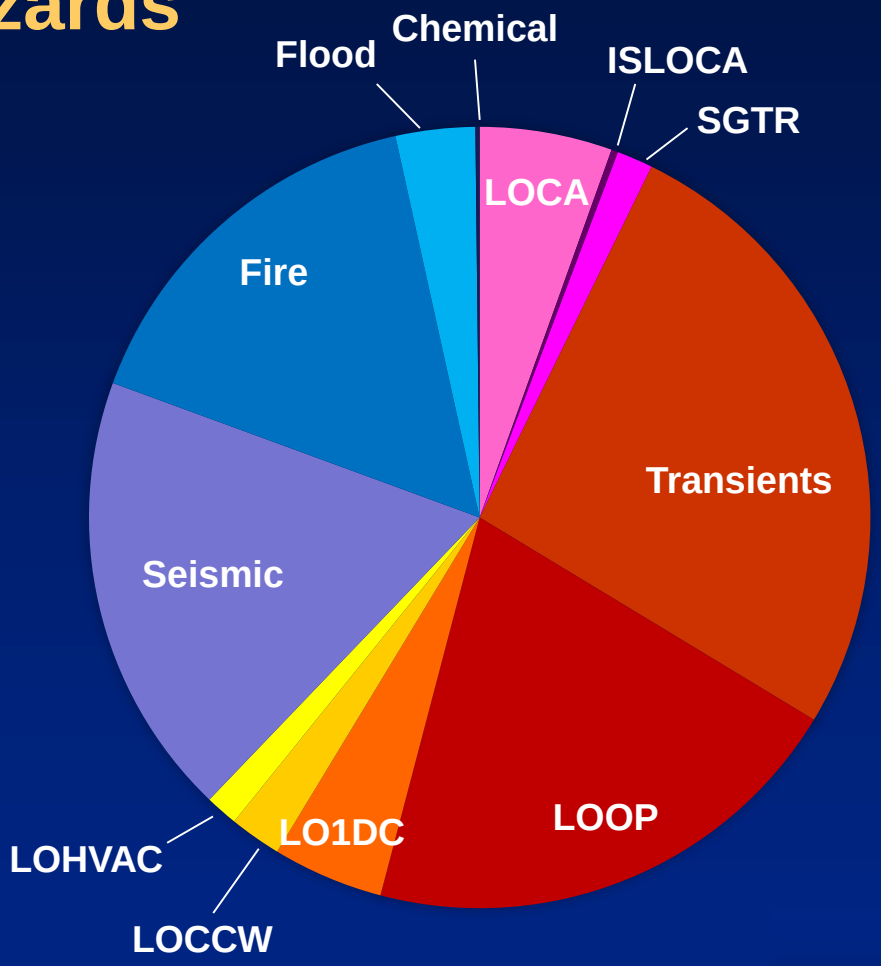


Example CDF Contributions (Internal Events)

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

Including External Hazards

- Internal events
- Internal floods
- Internal fires
- Seismic events
- External floods
- High winds



Further discussion in Lecture 6-2

Comments

- NPP PRA is a systems modeling enterprise => uses “divide and conquer” approach => caution needed at task interfaces (e.g., between initiating event analysis and event sequence analysis)
  - Gaps
  - Mismatches
- Iteration (which “fuzzifies” interfaces) is important. Examples:
  - Initiating event analysis considers “importance” of postulated event; early judgments needed to start other tasks can/should be revisited
  - Internal and external hazards analyses use internal events models (Lecture 6-2); can suggest model modifications based on results and insights

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

Comments (cont.)

- To postulate how things might fail, first need to know how things are supposed to work => **"Initial Information Collection" step (a.k.a. "Plant Familiarization") is critical**
- Checklists (e.g., based on past studies) are useful, but concept of active searching is key, especially for new systems.
- Multiple approaches/tools provide different perspectives and can help ensure completeness.