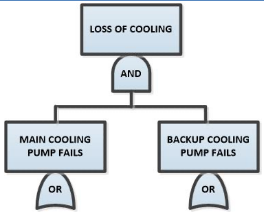
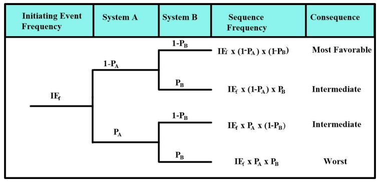


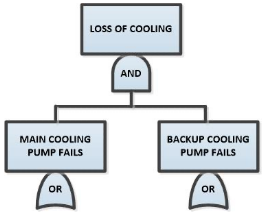
Event Tree session 3 of 4



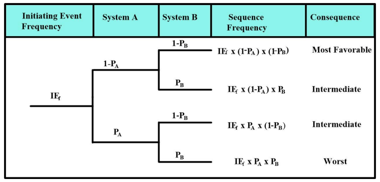
Present event tree analysis basics

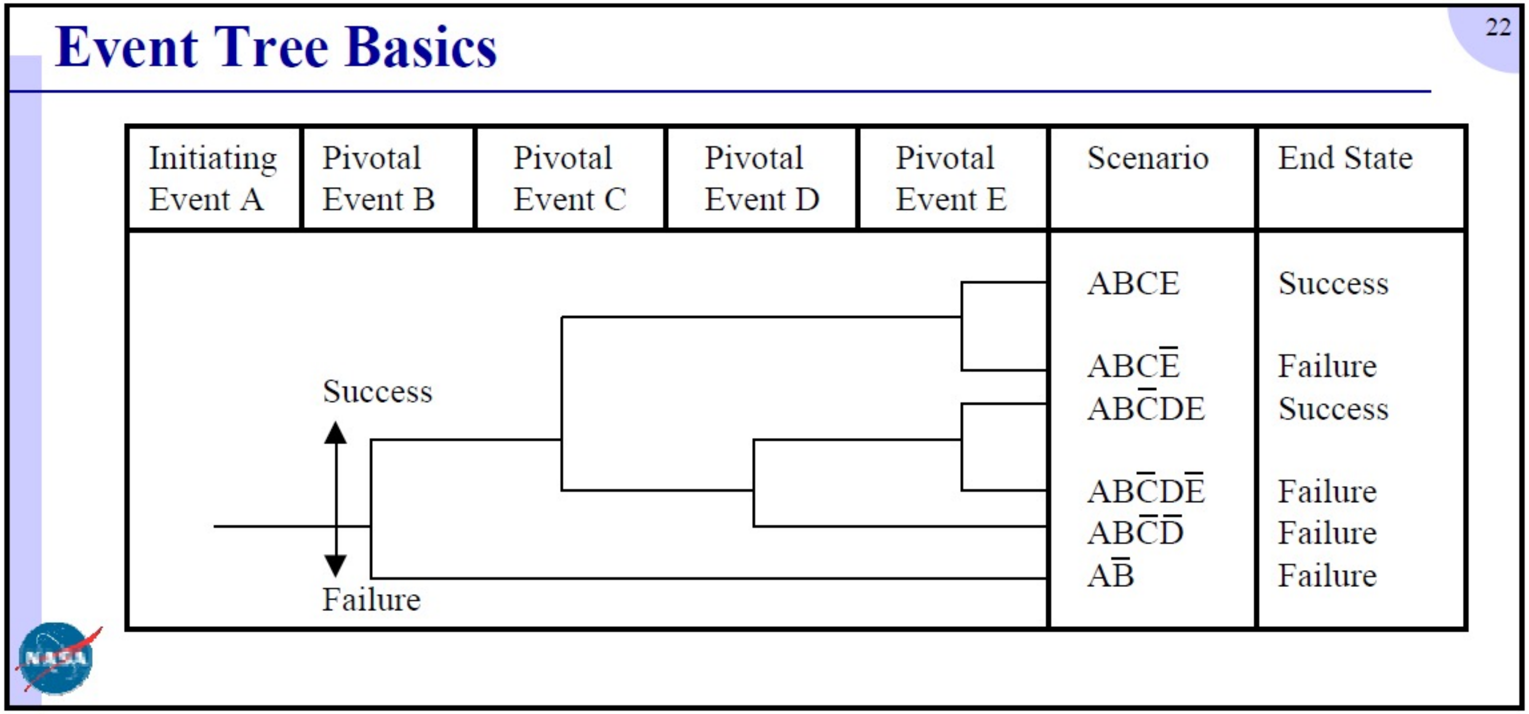
with examples and case studies

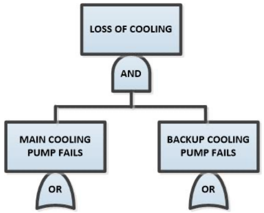
Howard Lambert
FTA Associates
2022



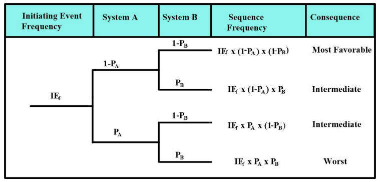
Event Tree Basics – Pivotal Events



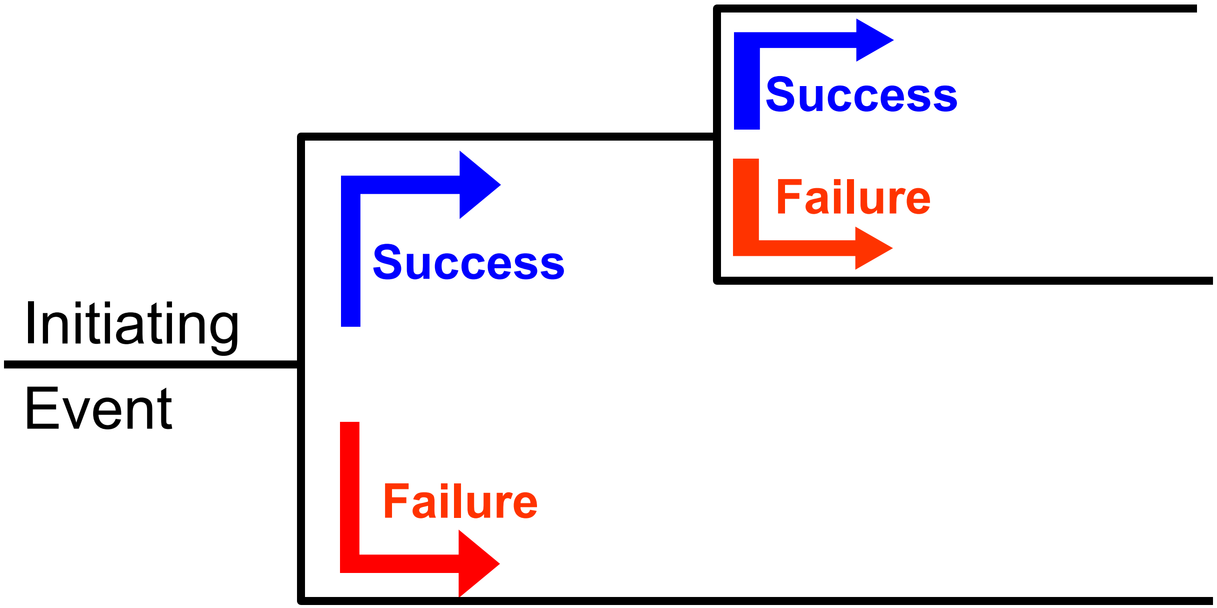




Event Tree Construction



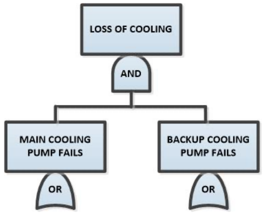
Event Occurs	System A Works	System B Works	End State



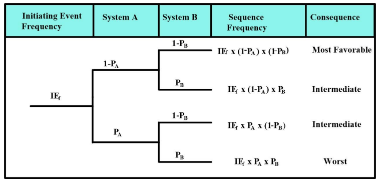
Systems A & B Success

System A Success & System B Failure

System A Failure
System B Not Asked



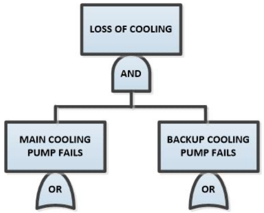
Event Tree Construction Methods



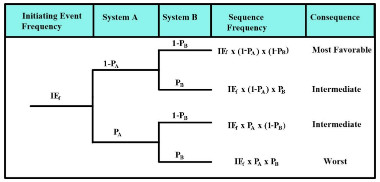
- There are no prescribed methods to include headings on the event tree such as failure of systems, controls, etc and subsequent ordering that are to be incorporated in event tree construction

- Construction of the event tree depends upon the discretion of the analyst
  - For example, including support systems on the heading or including them in the fault trees for the front-line systems
  - The analyst must determine the level of detail to be presented either in event trees or in the fault trees or a combination

- Parallel sequences require separate event trees



Simplified Low Pressure Injection System



Piping to primary coolant system

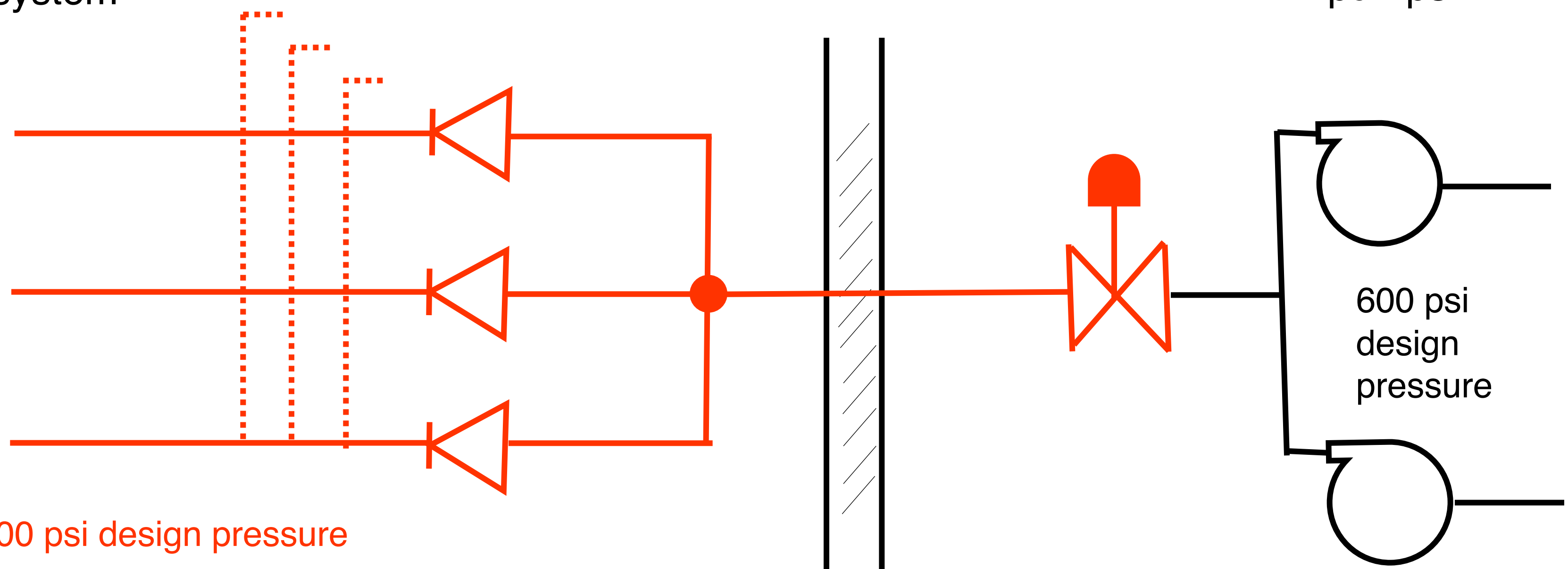
High Pressure Injection lines

Check Valves

Containment Building

Manual Valve Locked Open

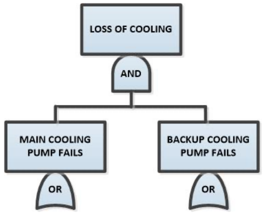
Low Pressure Injection pumps



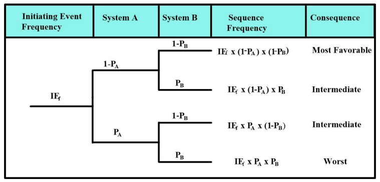
2500 psi design pressure

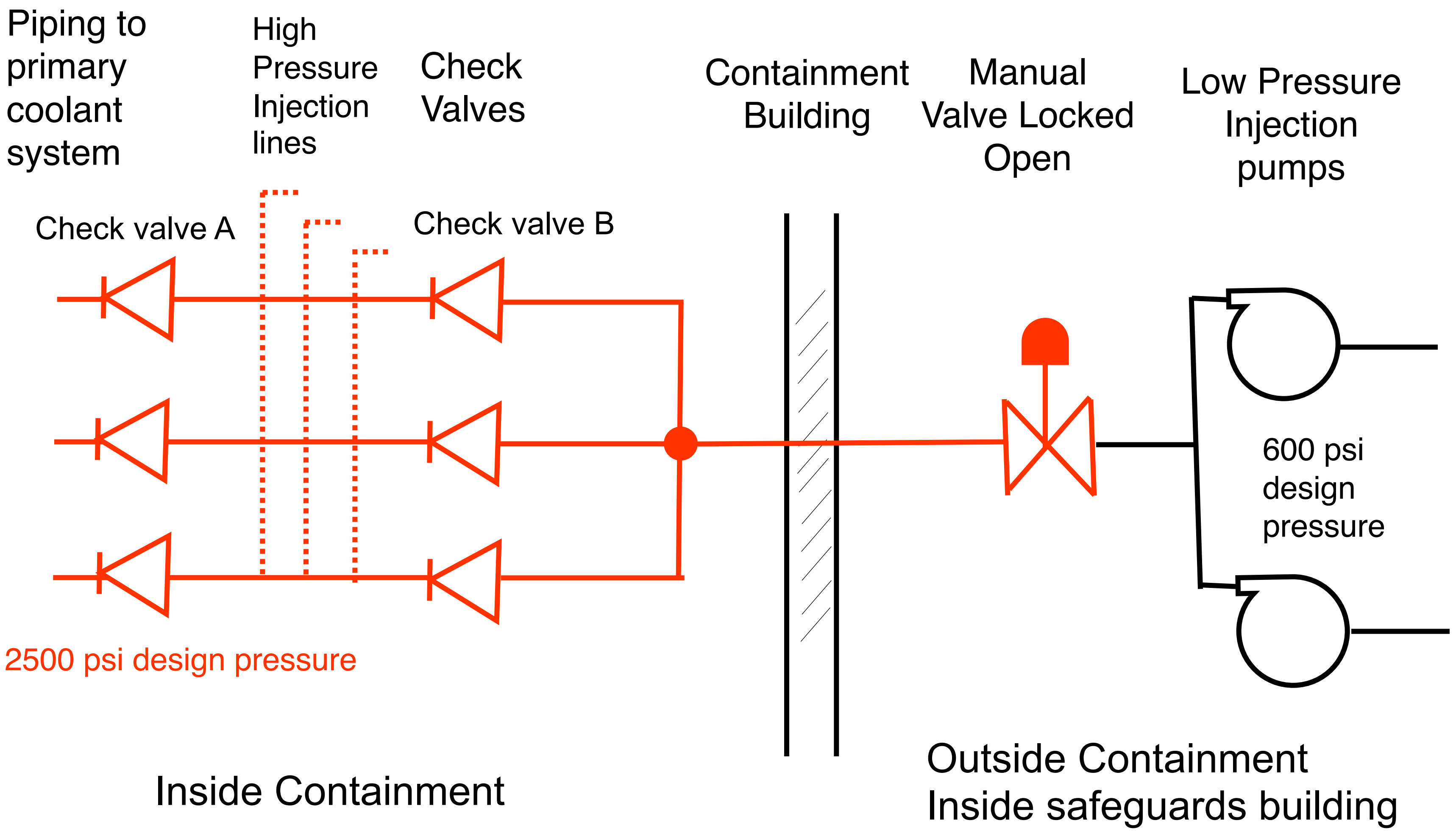
Inside Containment

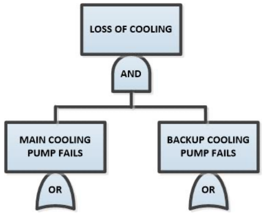
Outside Containment
Inside safeguards building



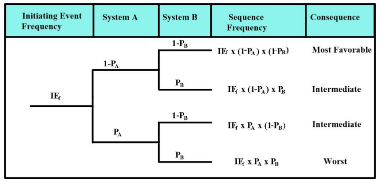
LPIS Fix – Two Check Valves in Series



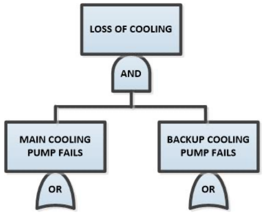




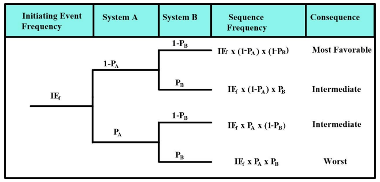
Notation

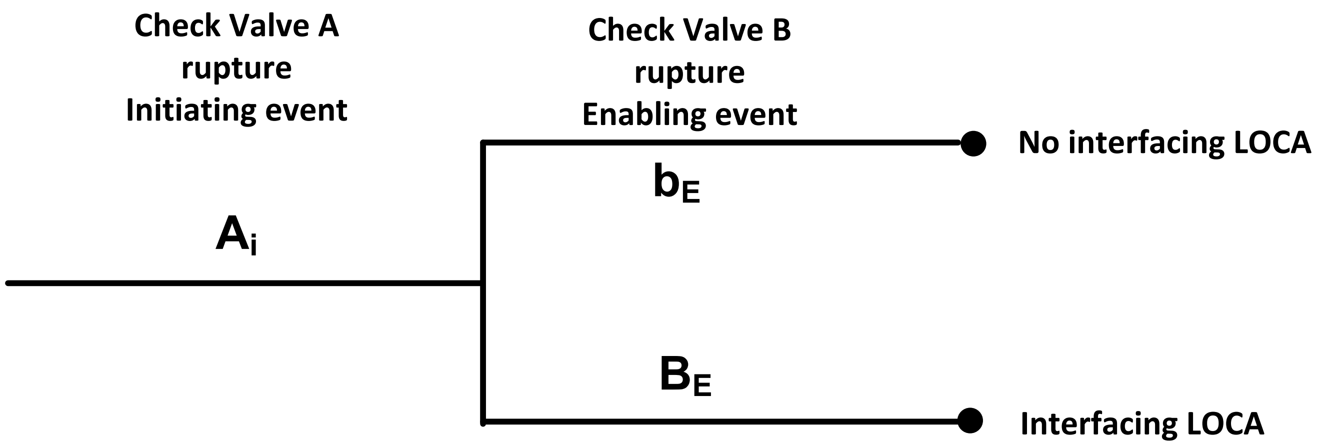


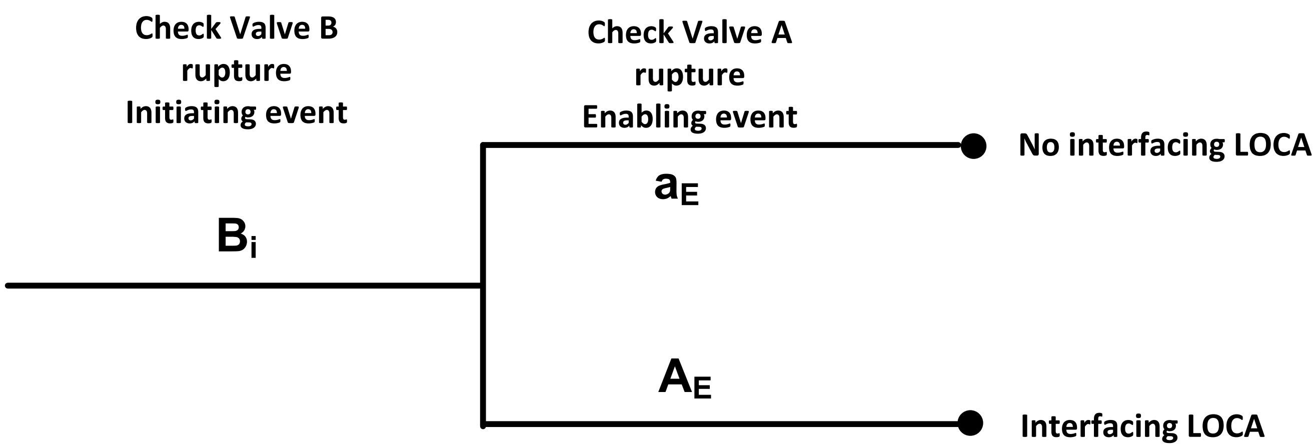
- Check valve failure is a gross internal rupture of the check valve
- For a two check valve system, the check valve that fails first is the enabling event
- The check valve that fails second is the initiating event that causes the interfacing LOCA
- Two parallel sequences



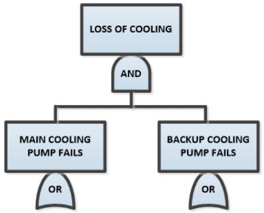
Interfacing LOCA event trees



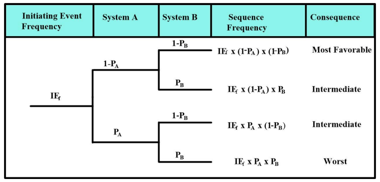




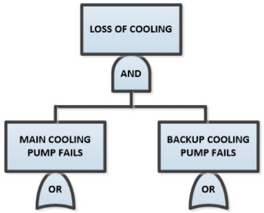
$P(B_i)P(A_e | B_i) > P(A_i)P(B_e | A_i)$ Law of Conditional Probability does not hold!!



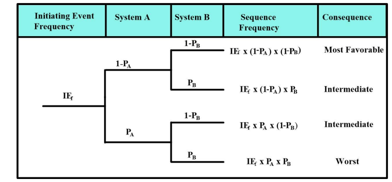
Interfacing LOCA Insights

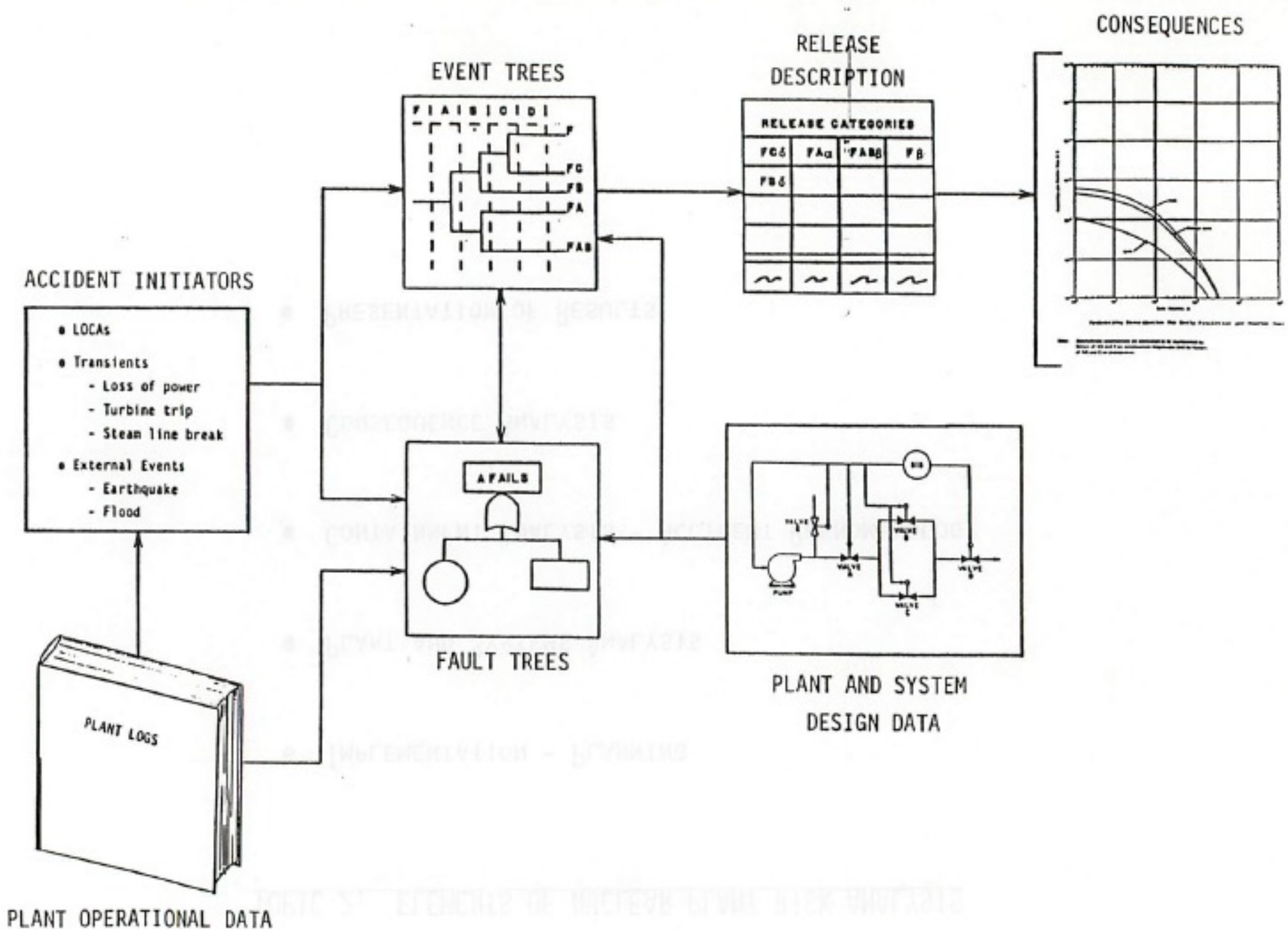


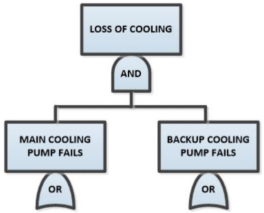
- Interfacing LOCA results in releases that bypass containment and render coolant makeup and core heat removal systems ineffective (called event V in nuclear power plant PRAs)
- Single check valve failure was a single point failure for Surry – double check valves were placed in series – Important finding and recommendation of the Reactor Safety Study that was not publicized
- Two interfacing LOCA event trees were not equivalent – Laws of Conditional Probability does not hold.
- If the high-pressure check valve A fails first (enabling event) this puts additional stress on the low-pressure check valve B – the reverse is not true, if the low-pressure check valve B fails first it does not put additional stress on the high-pressure check valve A.
- If the ordering of event headings on the event tree result in different conditional probabilities, then separate event trees need to be generated as shown for the interfacing LOCA example – another finding of the Reactor Safety Study



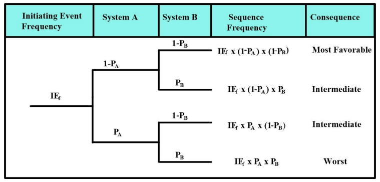
Nuclear Power Plant PRAs

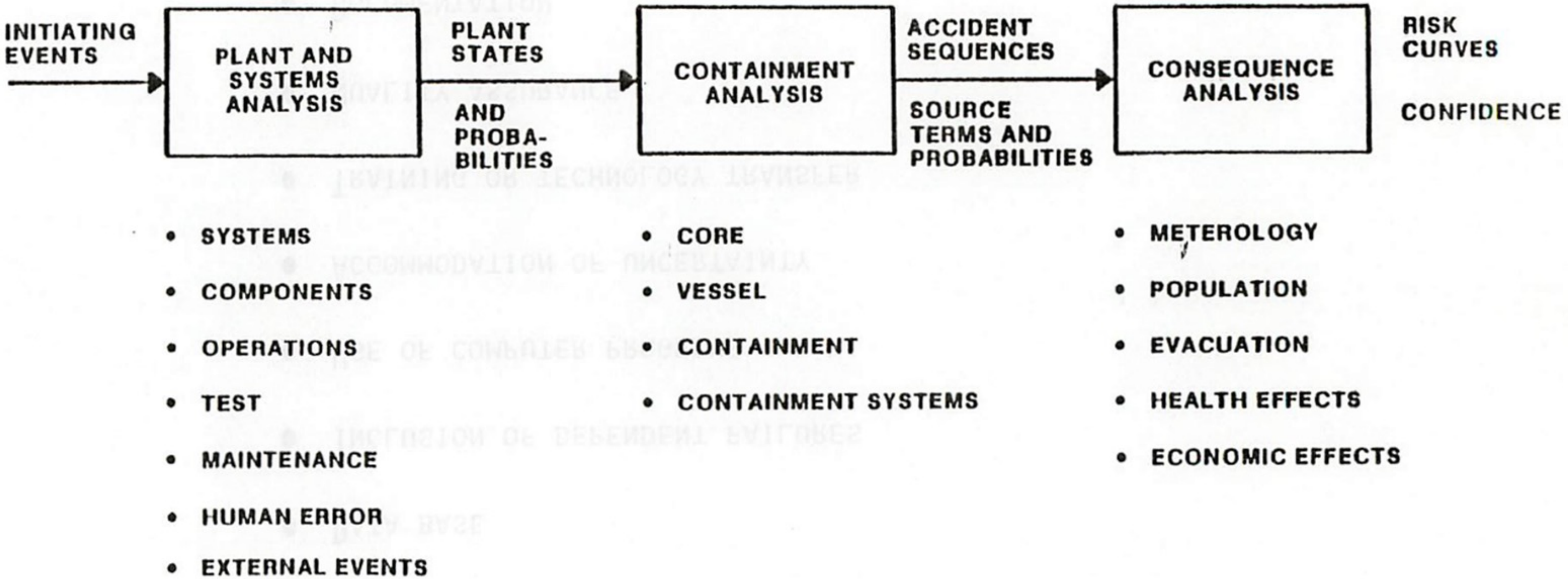


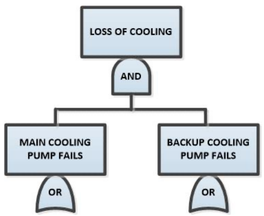




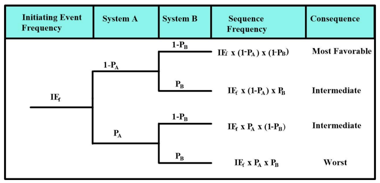
PRA Flowchart





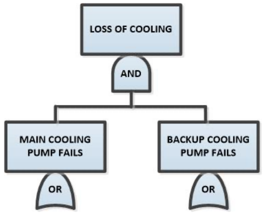


Overview of Level-1/2/3 PRA

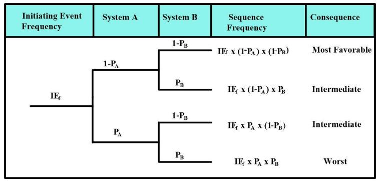


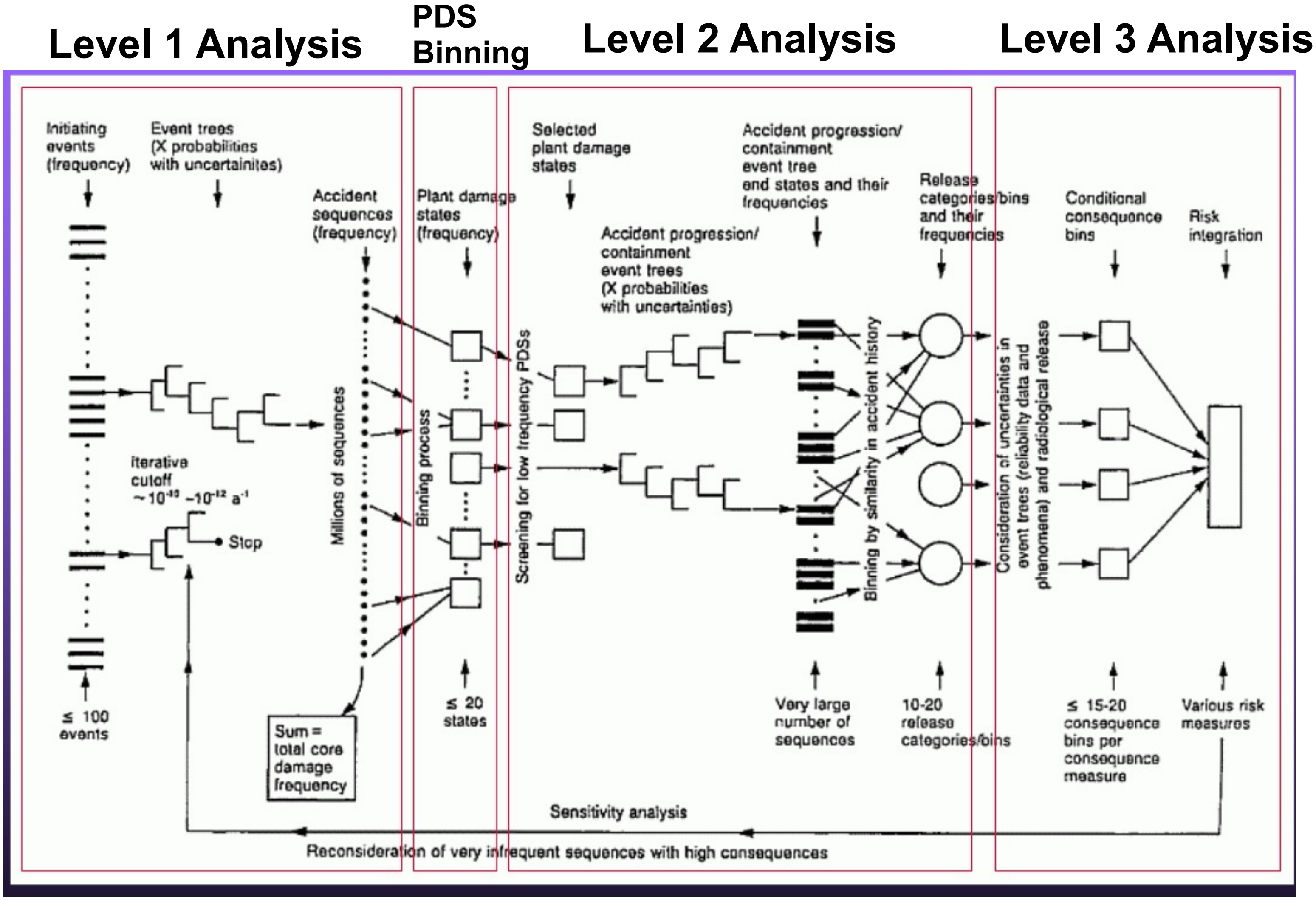
CDF – Core Damage Frequency

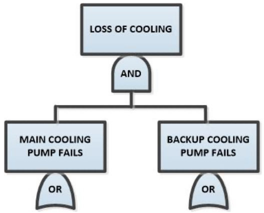
Input	Analysis	Results
	Level 1 PRA:	
Initiating events	System Failures	**CDF Sequences**
	Level 2 PRA:	
CDF Sequences	Plant Damage States Containment Failure	**Source Term**
	Level 3 PRA:	
Source Term	Radiation transport Consequence Analysis	Early fatalities Latent cancers Population dose



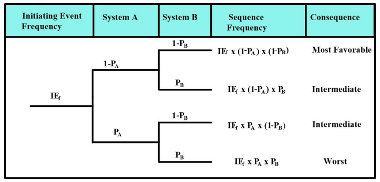
PRA Framework – three levels





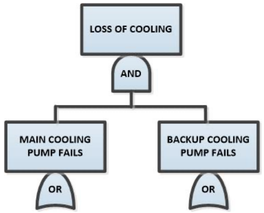


Introduction & Overview – Basic Definitions

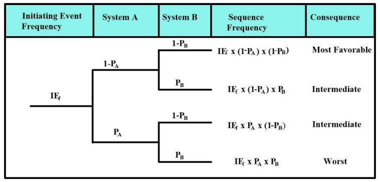


- **Front Line System**: A front line system is a system that is directly used to provide a mitigating function in response to an initiating event. Generally, front line systems are modeled as functions in an accident sequence or event tree model.

- Examples of Front Line Systems:
  - Reactor Protection System (PWR, BWR)
  - Main Feedwater (PWR, BWR)
  - Auxiliary/Emergency Feedwater (PWR)
  - HPCI, RCIC, HPCS (BWR)
  - Residual Heat Removal (PWR, BWR)
  - Suppression Pool Cooling (BWR)

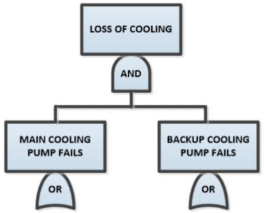


Introduction & Overview – Basic Definitions

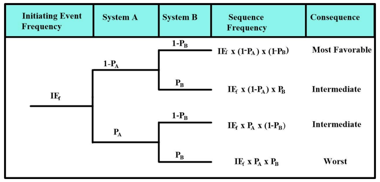


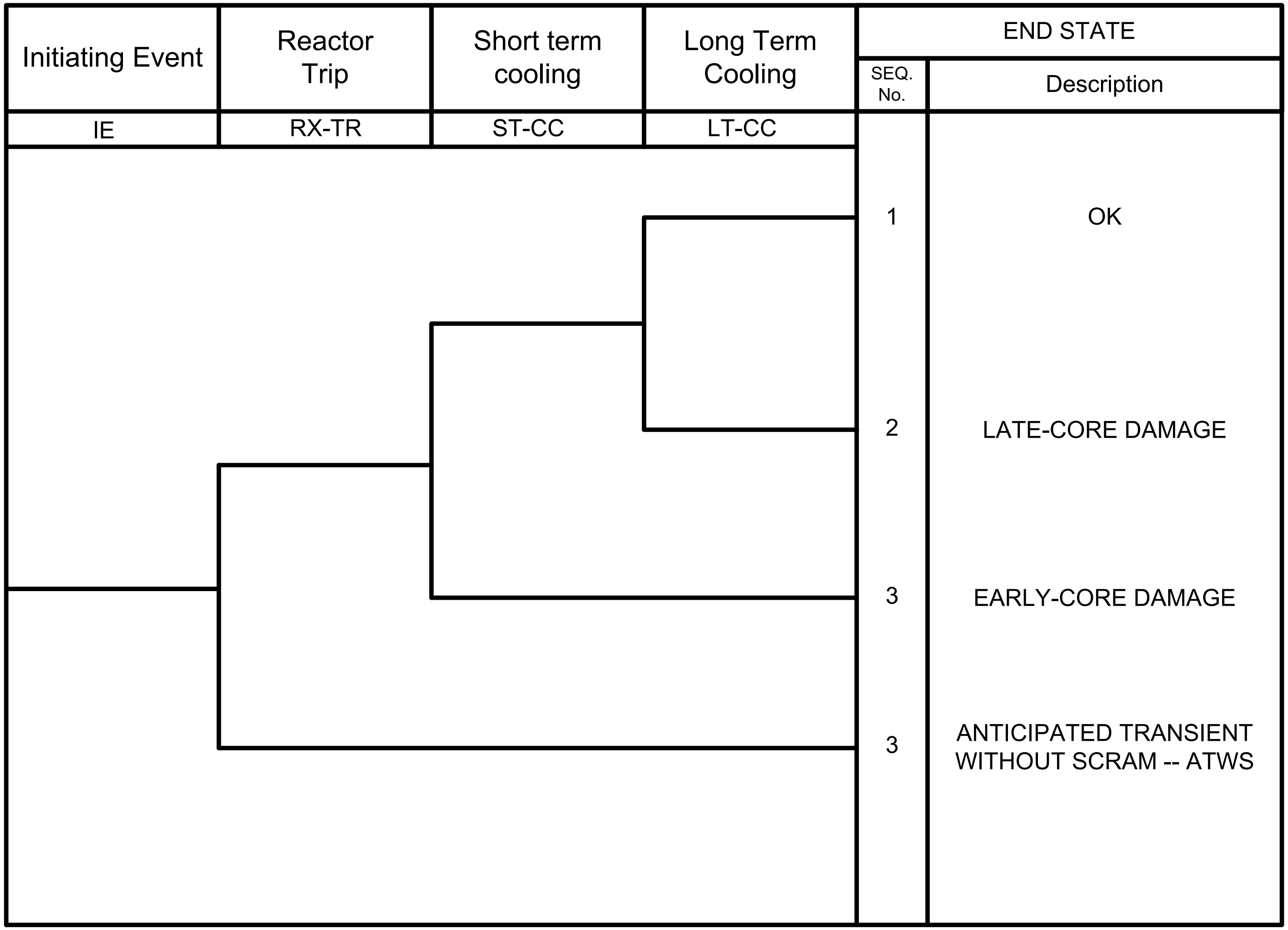
- **Support System**: A support system is any system that is required for the operation of a front-line system but which, by itself, does not provide any mitigating function in response to an initiating event. Generally, support systems are modeled as internal transfers to the various front line system fault tree models.

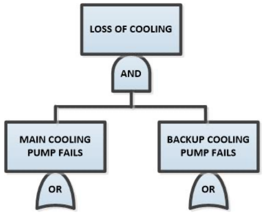
- Examples of Support Systems:
  - AC, DC Electric Power (PWR, BWR)
  - Service Water (PWR, BWR)
  - RBCCW, TBCCW Reactor Building, Turbine Building, component cooling water system (BWR)
  - Component Cooling Water (PWR)
  - Instrument Air, Station Air (PWR, BWR)



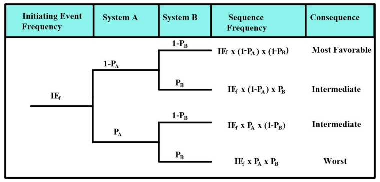
Generic Level 1 Event Tree



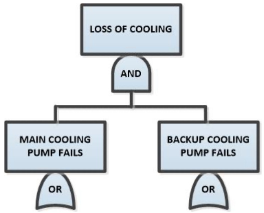




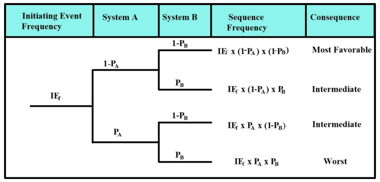
Success Criteria

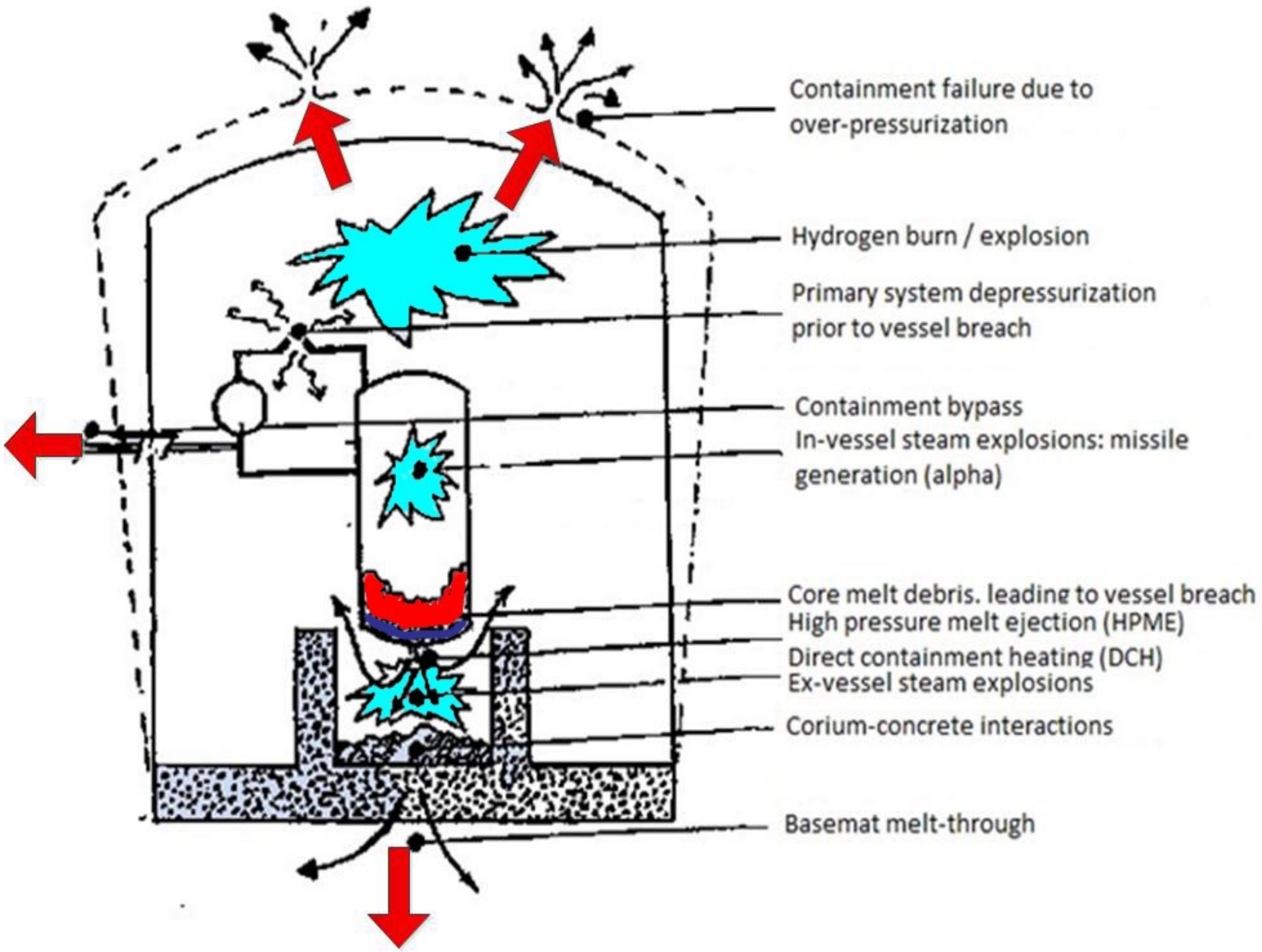


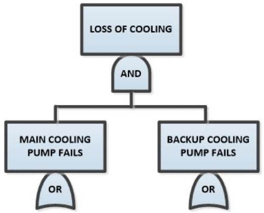
IE	*Reactor Trip*	*Short-Term Core Cooling*	*Long-Term Core Cooling*
Transient	*Auto Rx Trip or Man. Rx Trip*	*PCS or 1 of 3 AFW or 1 of 2 PORVs & 1 of 2 ECI*	*PCS or 1 of 3 AFW or 1 of 2 PORVs & 1 of 2 ECR*
Loss of Coolant (LOCA)	*Auto Rx Trip or Man. Rx Trip*	*1 of 2 ECI*	*1 of 2 ECR*



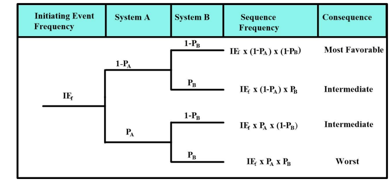
Severe Accident Phenomena in Containment

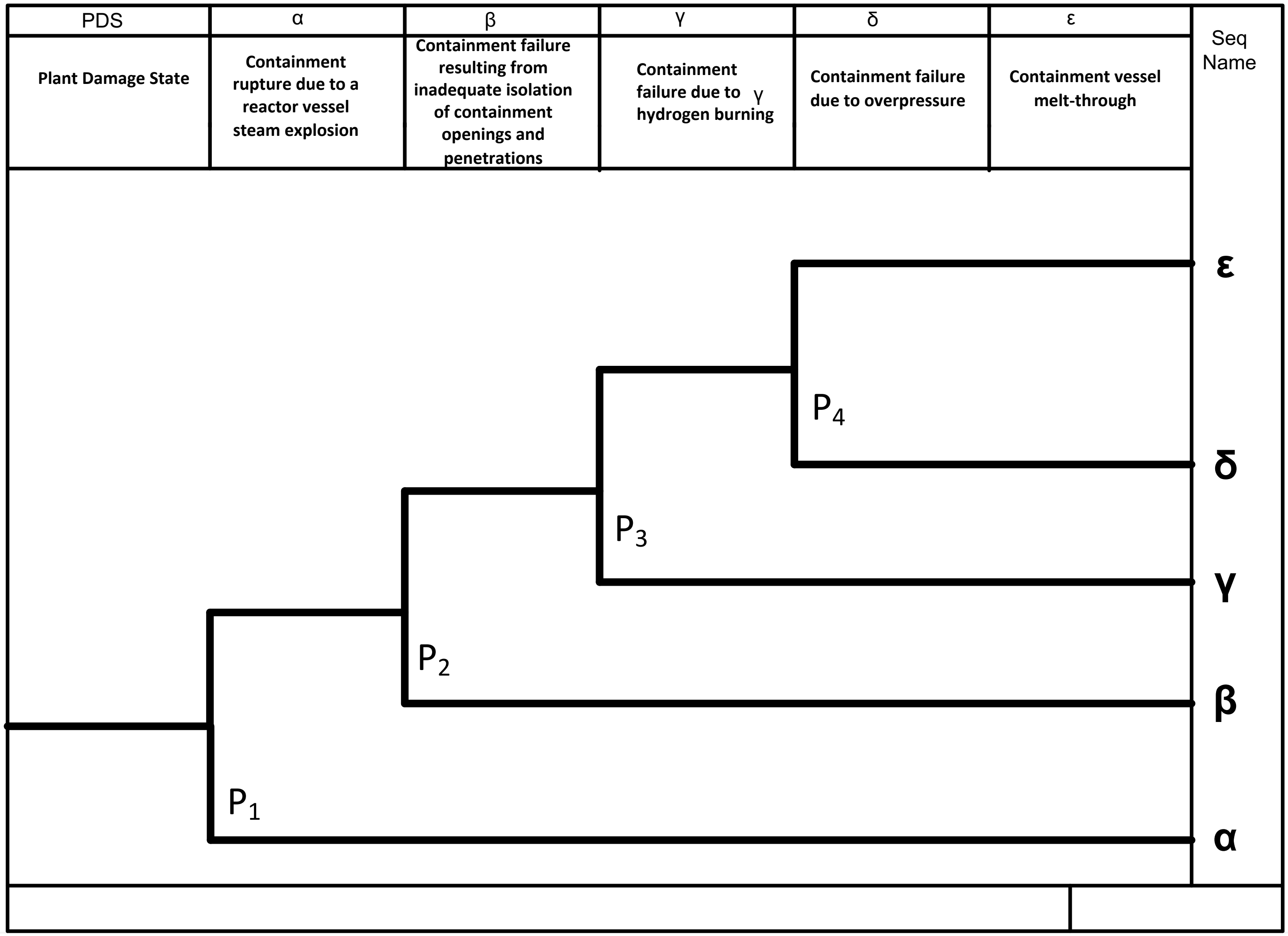






Containment Event Tree with end state probabilities – Reactor Safety Study





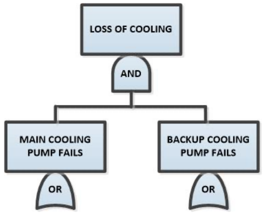
$P_\varepsilon = (1 - P_1)(1 - P_2)(1 - P_3)(1 - P_4)$

$P_\delta = (1 - P_1)(1 - P_2)(1 - P_3)P_4$

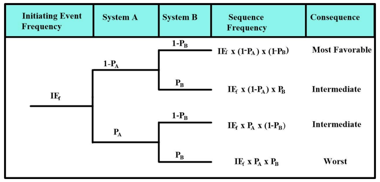
$P_\gamma = (1 - P_1)(1 - P_2)P_3$

$P_\beta = (1 - P_1)P_2$

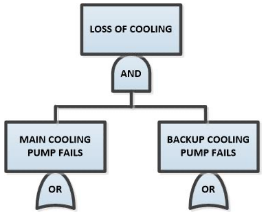
$P_\alpha = P_1$



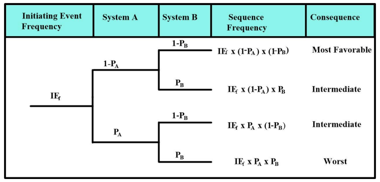
Plant Functions vs Front Line Systems Matrix



	Reactor Protection System	Power Conversion System	High Pressure Injection System	Low Pressure Injection System	Accumulator System	Auxiliary Feedwater System	Recirculation System	Quench Spray System	Primary SRV System	Secondary SRV System	Reactor Coolant Pump Seal
Reactor Sub criticality	X		X								
Normal Cooldown		X									
Emergency Core Cooling (Early)			X	X	X	X			X	X	X
Emergency Core Cooling (Late)			X				X				
Containment Heat Removal							X				
Containment Overpressure Protection (Early)								X			
Containment Overpressure Protection (Late)							X				

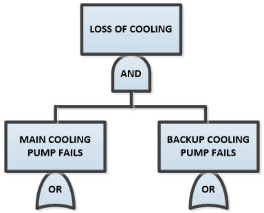


Front Line Systems vs Support Systems Matrix

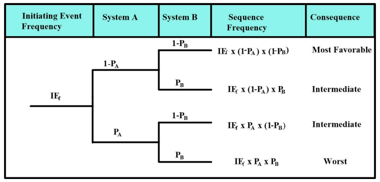


	Eng. Safety Fact. Act. System	AC Power System	DC Power System	Charging Pump Cooling System	Safety Injection Pump Cooling System	Reactor Pump Comp. Coolant Water	Turbine Pump Comp. Coolant Water	Circulating Water System	Service Water System
Reactor Protection System	X		X						
Power Conversion System		*	X				X	X	
High Pressure Injection System	X	X	X	X	X				
Low Pressure Injection System	X	X	X						
Accumulator System									
Auxiliary Feedwater System	X	X	X						
Recirculation System	X	X	X						X
Quench Spray System	X	X	X						
Primary SRV System			X						
Secondary SRV System			X						
RCP Seal Cooling System							X		

*requires offsite power



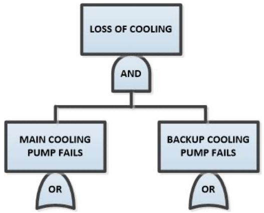
Support Systems vs Support Systems Matrix



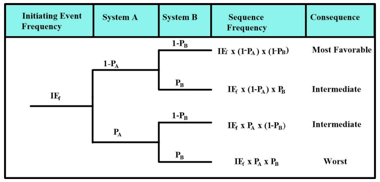
	Eng. Safety Feat. Act	AC Power System	DC Power System	Service Water System
Engineered Safety Features Actuation	**		X	
AC Power System	X	**	X	X
DC Power System			**	
Charging Pump Cooling System	X	X	X	X
Safety Injection Pump Cooling System	X	X	X	X
Reactor Plant Component Cooling Water System		X	X	X
Turbine Plant Water System		X	X	X
Circulating Water System		*	X	
Service Water System	X	X	X	**

* Requires offsite power

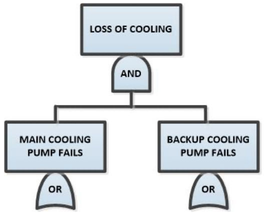
** Not Applicable



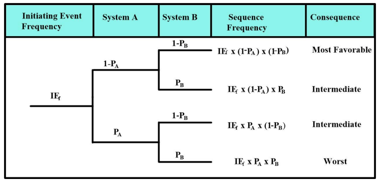
Identify Systems Capable of Fulfilling Functions



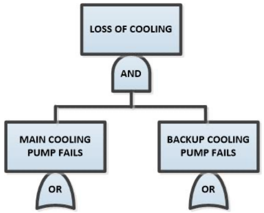
- For each initiating event (IE) identified
  - Which systems are capable of providing:
    Reactor subcritical
    Early core cooling (injection mode)
    Late core cooling (recirculation mode)
- Specific success criteria need to be defined for each system



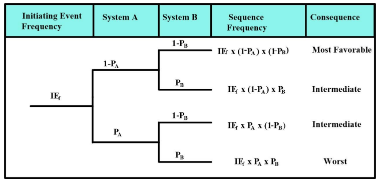
Success Criteria



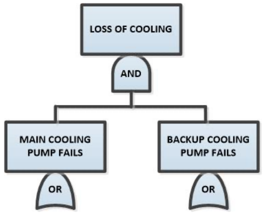
- 3/4 accumulators injecting,
- 1/2 SI (safety injection) pumps injecting into 2/4 cold legs,
- and 1/4 containment fan coolers or 1/2 containment spray trains.



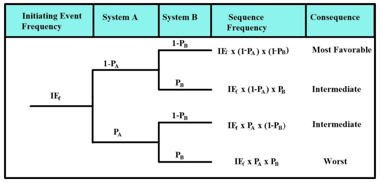
Event Tree Quantification Example – Station Blackout



- Station Blackout occurs when there is no motive AC power available
- Assume the nuclear power plant has three sources of motive AC power
  - Offsite power (preferred source)
  - Emergency Diesel Generator 1
  - Emergency Diesel Generator 2
- Compute annual frequency for three scenarios
  - Station blackout occurs and exceeds 4 hours, 8 hours and 24 hours

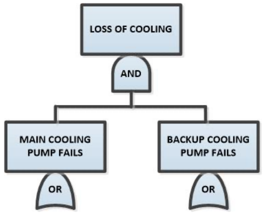


Loss of offsite power categories and frequencies

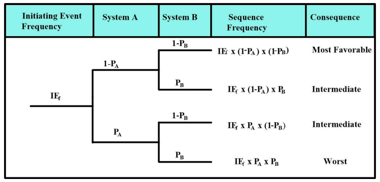


- Loss of offsite power (LOOP) is broken down into four categories for loss of offsite power annual frequency shown the table below from actual plant data (NUREG/CR-6890 VOL 2)

LOOP Power Category	LOOP offsite mean frequency	Probability non LOOP Recovery 4 hours	Probability non LOOP Recovery 8 hours	Probability non LOOP Recovery 24 hours
Plant centered	2.07E-03	4.77E-02	1.37 E-02	1.11E-03
Switchyard Centered	1.04E-02	7.86E-02	2.46E-02	2.25E-03
Grid Related	1.86E-03	1.54E-01	4.73E-02	3.42E-03
Weather Related	4.83E-03	3.82E-01	2.58E-01	1.14E-01
All	3.59E-02	1.57E-01	6.72E-02	1.79E-02



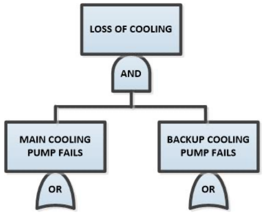
Emergency Diesel Generator Failure Data



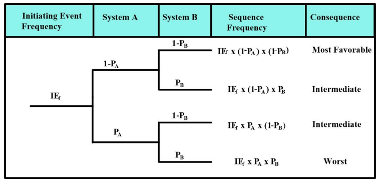
- Probability EDG fails to start or run > 1 hour 8.0E-3 (NUREG/CR-6928)
- Probability of repair given that the EDG fails to start or run (NUREG/CR-6890 VOL 2)

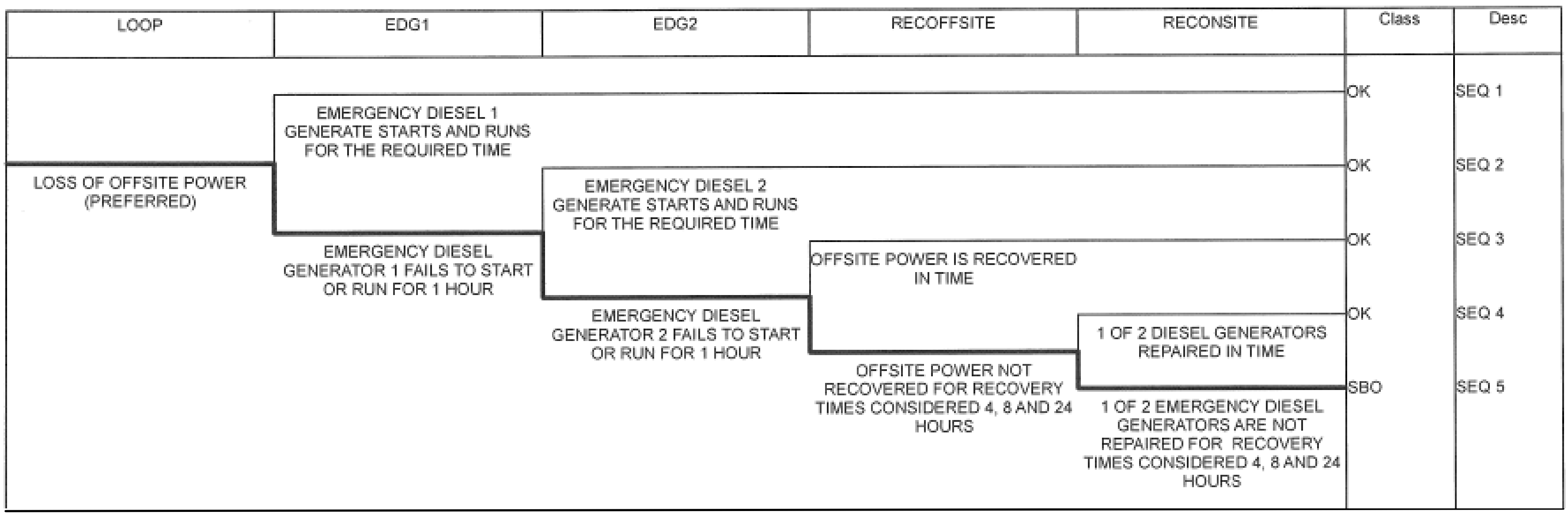
Duration hr	Probability of no diesel generator repair*
4	0.483
8	0.296
24	0.063

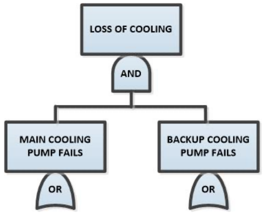
*Repair of one of two EDGs that is easiest to repair



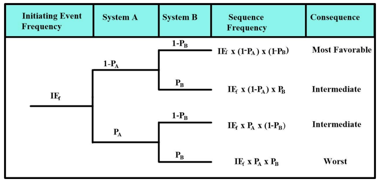
Generic Station Blackout (SBO) Event Tree – Recovery times 4, 8 and 24 hours



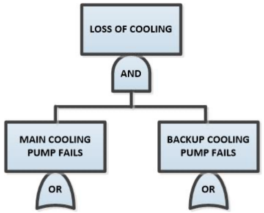




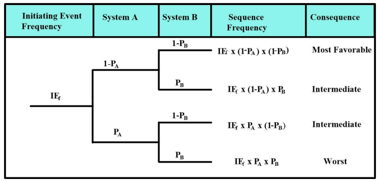
Sequence 5 min cut set



1. Loss of offsite power (preferred)
2. Emergency diesel generator 1 fails to start or run for 1 hour
3. Emergency diesel generator 2 fails to start or run for 1 hour
4. Offsite power not recovered for recovery times considered 4, 8 and 24 hours
5. 1 of 2 emergency diesel generators are not repaired for recovery times considered 4, 8 and 24 hours



Sequence 5 min cut set quantification example



- Example – plant centered LOOP , duration time 4 hours
- Annual LOOP frequency -- 2.07×10^{-3}
- Both EDGs fail (alpha = 0.05)
  - $(8 \times 10^{-3} \times .95)^2 + 8 \times 10^{-3} \times .05$
  - $= 4.6 \times 10^{-4}$
- Probability of Failure to recover LOOP within 4 hours
- $= 4.77 \times 10^{-2}$
- Probability of failure to repair either EDG within 4 hours = 0.483
- Annual Frequency that LOOP occurs and exceeds 4 hours for a plant centered LOOP
- $= 2.07 \times 10^{-3} \times 4.6 \times 10^{-4} \times 4.77 \times 10^{-2} \times 0.483 = 2.2 \times 10^{-8}$

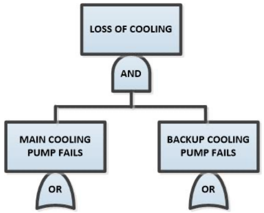
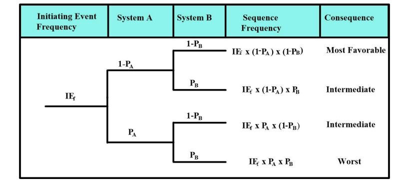
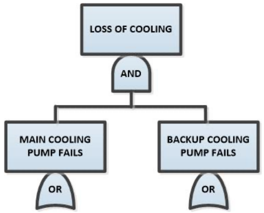


Table of Final Results for SBO Annual Frequency

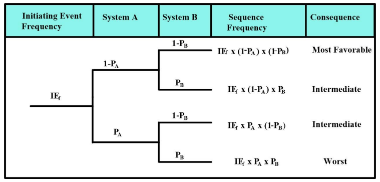


LOOP Power Category	4 HOUR DURATION	IMPORTANCE	8 HOUR DURATION	IMPORTANCE	24 HOUR DURATON	IMPORTANCE
Weather Related	4.10E-07	60.54%	1.70E-07	77.00%	8.82E-09	90.47%
Switchyard Centered	1.82E-07	26.82%	3.48E-08	15.81%	6.78E-10	6.96%
Grid Related	6.36E-08	9.40%	1.20E-08	5.44%	1.84E-10	1.89%
Plant centered	2.19E-08	3.24%	3.86E-09	1.75%	6.66E-11	0.68%
All	6.77E-07	100.00%	2.20E-07	100.00%	9.75E-09	100.00%

Weather related LOOP dominates probabilistically



Human Reliability Analysis – THERP (first generation analysis)



THERP – Technique for Human Error Rate Prediction – from "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278

FAMILIARIZATION

- Information gathering
- Plant visit
- Review of procedures and information from system analysts

↓

QUALITATIVE ASSESSMENT

- Determine performance requirements
- Evaluate performance situation
- Specify performance objectives
- Identify potential human errors
- Model human performance

↓

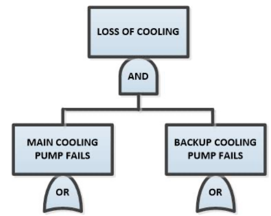
QUANTITATIVE ASSESSMENT

- Determine probabilities of human errors
- Identify factors and interactions affecting human performance
- Quantify effects of factors and interactions
- Account for probabilities of recovery from errors
- Calculate human-error contribution to probability of system failure

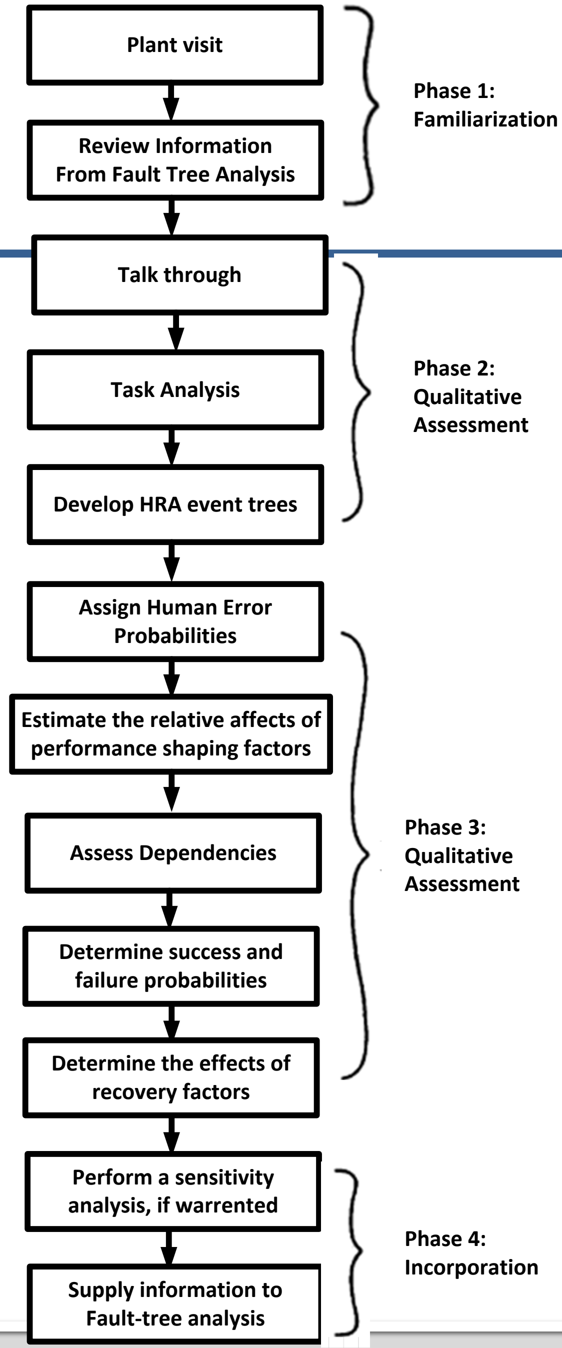
↓

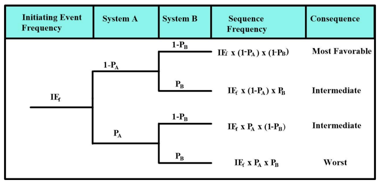
INCORPORATION

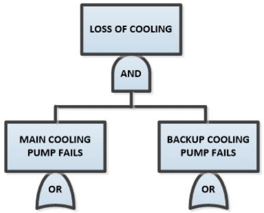
- Perform sensitivity analysis
- Input results to system analysis



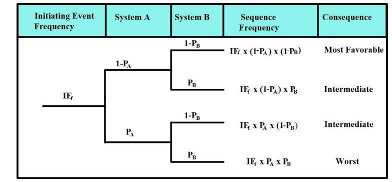
THERP Flowchart

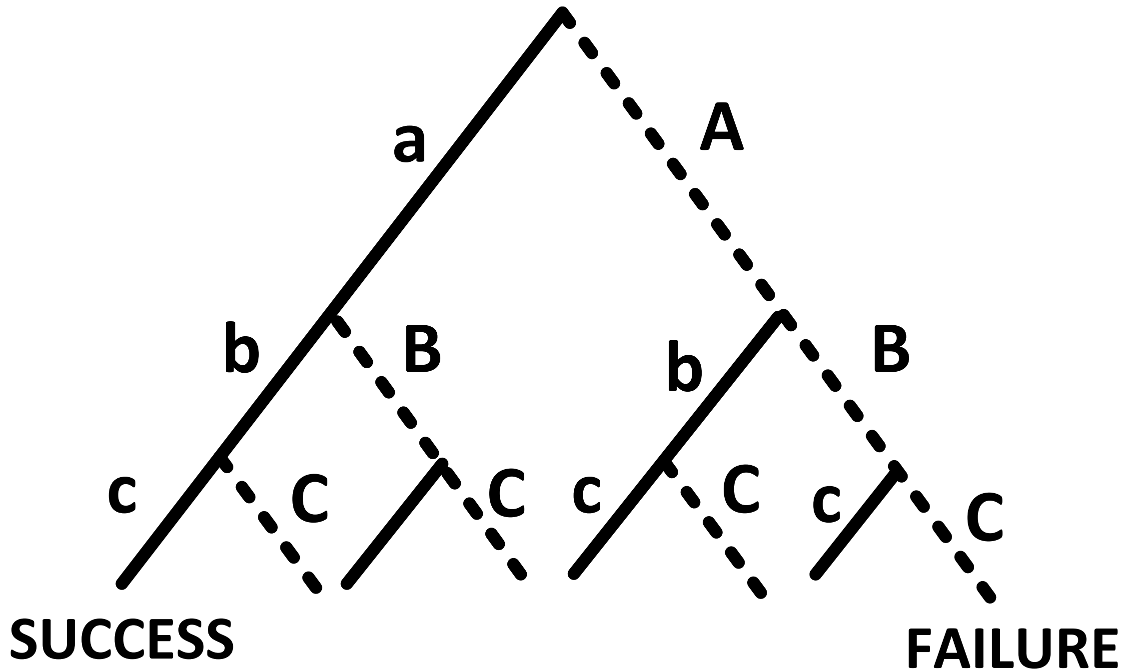




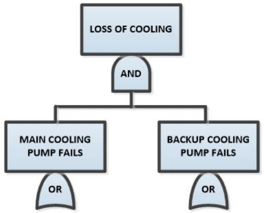


THERP event tree

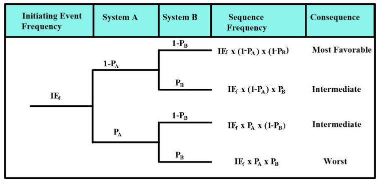


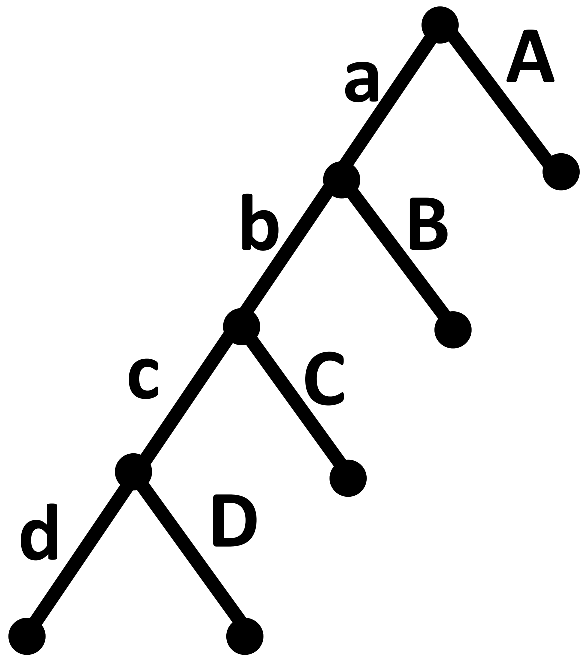


Scheme for the construction of an HRA-THERP event tree: Each node in the tree is related to an action, the sequence of which is shown from the top downwards. Originating from each node are two branches: The branch to the left, marked with a lowercase letter, indicates the success; the other, to the right and marked with the capital letter, indicates the failure.



THERP event tree example





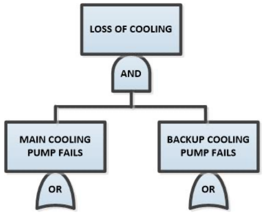
<u>Event</u>

A= Control-room operator omits ordering the following tasks

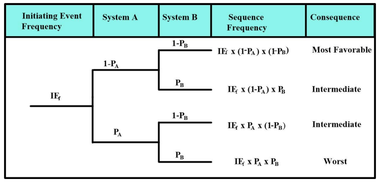
B= Operator omits verifying the position of MU-13

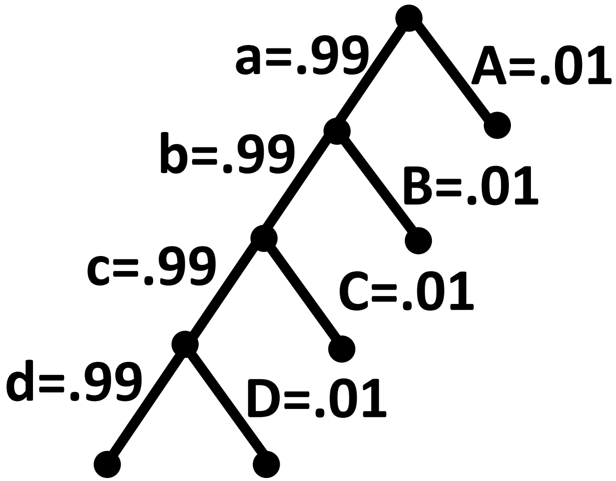
C= Operator omits verifying/opening the OH valves

D= Operator omits isolating the DH pump rooms



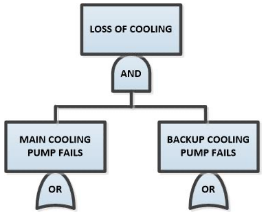
THERP event tree example



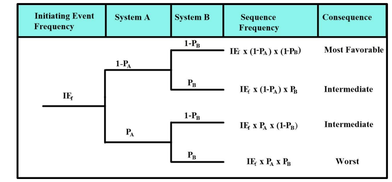


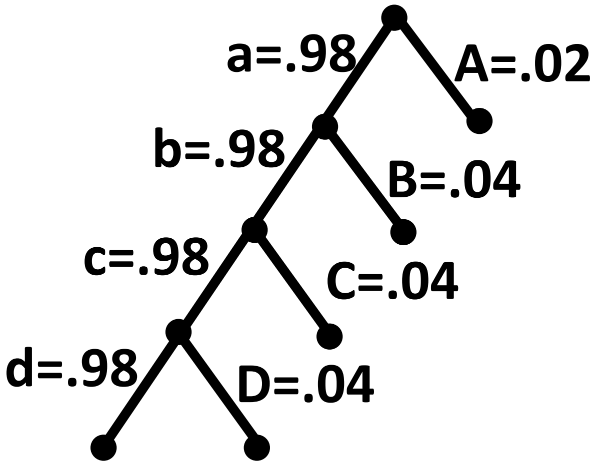
EVENT	HEP	SOURCE
A = Control-room operator omits ordering the following tasks	.01(.005 to .05)	Table 20-22. item 1 (p. 20-31)
B = Operator omits verifying the position of MU-13	.01(.005 to .05)	Table 20-18, item 3 (p. 20-28)
C = Operator omits verifying/opening the DH valves	01(.005 to .05)	Table 20-18, item 3 (p. 20-28)
D = Operator omits isolating the DH pump rooms	.01(.005 to .05)	Table 20-18, item 3 (p. 20-28)

HRA event tree for actions performed outside the control room, with estimates of nominal human-error probabilities



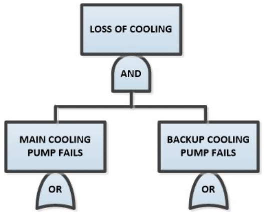
THERP event tree example to incorporate dependencies



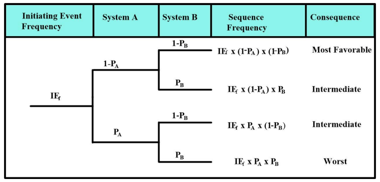


EVENT	HEP	SOURCE
A = Control-room operator omits ordering the following tasks	.02(.01 to .1)	Table 20-22. item 1 (p. 20-31)
B = Operator omits verifying the position of MU-13	.04(.02 to .2)	Table 20-18, item 3 (p. 20-28)
C = Operator omits verifying/opening the DH valves	04(.02 to .2)	Table 20-18, item 3 (p. 20-28)
D = Operator omits isolating the DH pump rooms	04(.02 to .2)	Table 20-18, item 3 (p. 20-28)

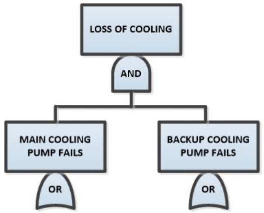
HRA event tree for actions performed outside the control room, with estimates of nominal human-error probabilities to reflect Performance Shaping Factors (PSFs). The HEP for event A has been modified to reflect the effects of moderately high stress and dependence; the HEPs for events B,C and D have been modified to reflect the effects of moderately high stress and protective clothing.



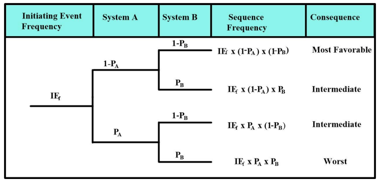
Human Failure Events



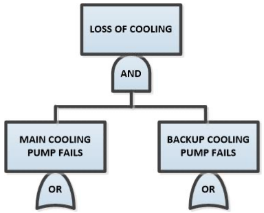
- Human Reliability Analysis identifies human Interactions that are incorporated as Human Failure Events in a PRA
- HFEs address deficiencies, e.g.,
  - deficiencies in control indications
  - inadequacy of procedural guidance for the particular scenario of concern
  - lack of time to diagnose a situation and act reliably
  - other factors that can affect operator performance
- Two Parts of the Each Human Failure Event (HFE)
  - Operator must recognize the need/demand for the action**(cognition)** AND
  - Operator must take steps **(execution)** to complete the actions



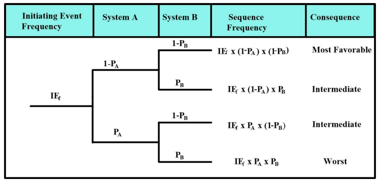
Human Failure Events

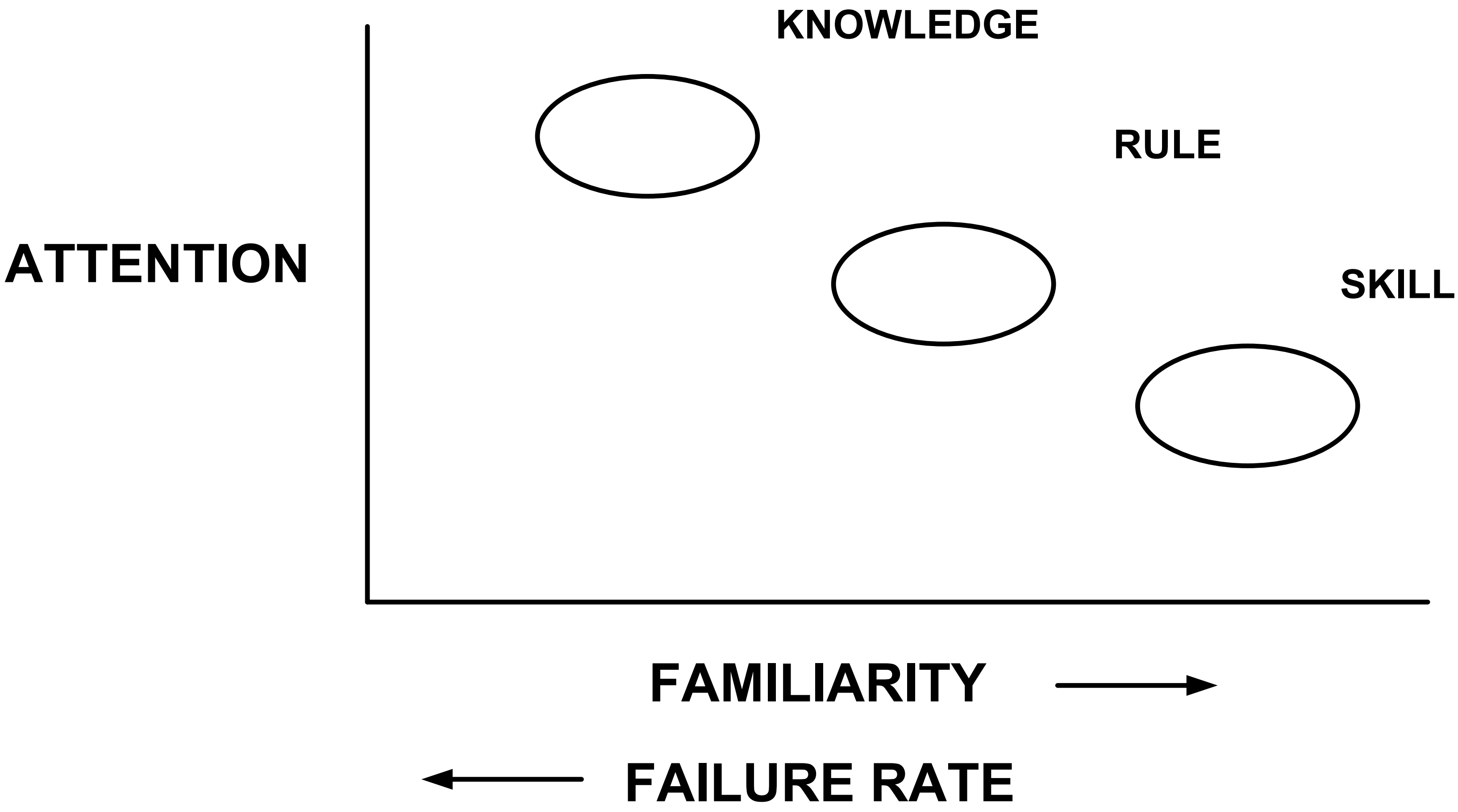


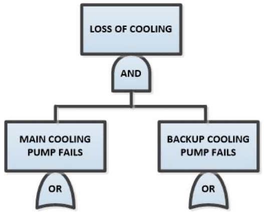
- Post-initiator operator actions consist of:
  - **Qualitative Analysis** defines Context and Performance Shaping Factors
    - Operator action must be feasible (for example, sufficient time, sufficient staff, sufficient cues, access to the area)
  - Then **Quantitative assessment (using an HRA method)**
    - Includes dependency evaluation



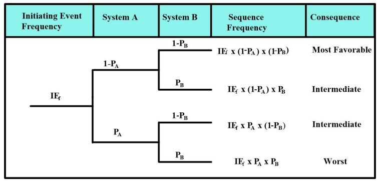
Recovery Post-Initiator Action

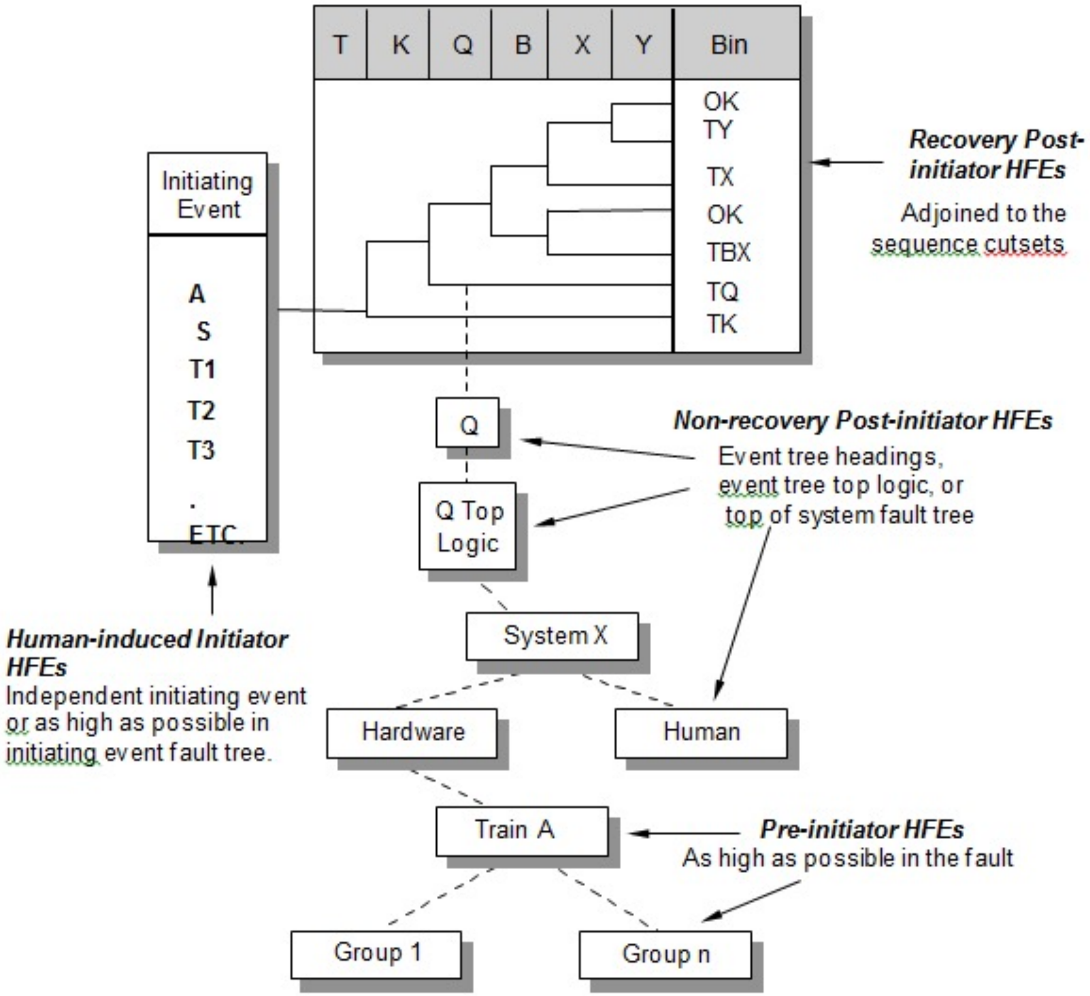




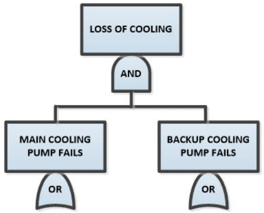


Time Phases of Human Failure Events (HFEs)

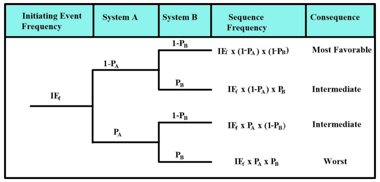




- Pre-initiator HFE
- Initiator HFE
- Post-initiator HFE
  - Non-recovery post-initiator HFE
  - Recovery post-initiator HFE (not identified at this time)

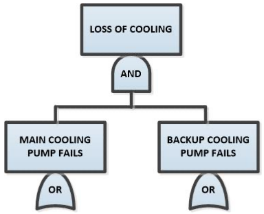


System Analysis: Human Interactions

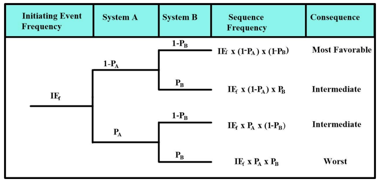


There are three types of Human Interactions (HIs) that are typically modeled:

- Type A: Latent HIs occurring before an initiating event (e.g., incorrect component restoration after maintenance) – included in FTs.
- Type B: HIs associated with the initiating event (typically captured in the initiating event data) – not included in FTs. **(don't agree)**
- Type C: Dynamic or Recovery HIs in response to the initiating event (e.g., actions in response procedures) – included in FTs.



Examples type A human interactions

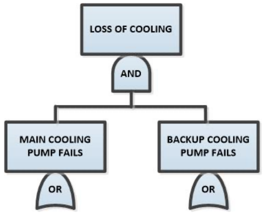


1. Failing to re-open an isolation valve following test or maintenance activities;

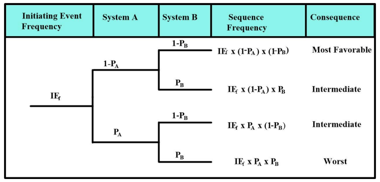
2. Failing to re-close a valve that isolates a test recirculation line after pump testing is complete, such that flow would be diverted from its intended load;

3. Failing to rack a breaker back in when returning a pump to service;

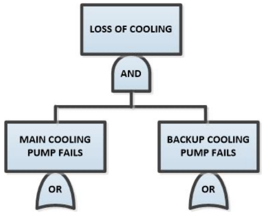
4. Miscalibrating one or more instrument channels or otherwise leaving them in an unavailable state (for example, by leaving closed an instrument root valve) such that a portion of a standby system could fail to actuate when needed.



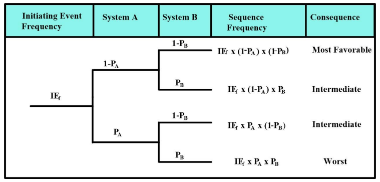
Examples type B human interactions



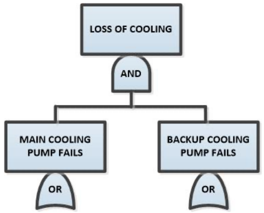
- Internal Flooding – operator opens isolation valve that causes internal flooding
- Operator actions that trip the plant
- Inadvertent operation of a safety system (e.g., safety injection)



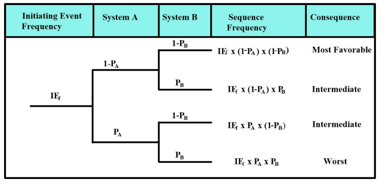
Post initiator



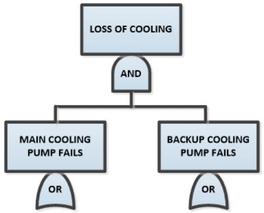
Post-initiator human interactions occur after an initiating event and consist of a cognitive element and an execution element. **The cognitive element includes detection, diagnosis and decision-making, while the execution element consists of manipulation tasks.** Post-initiator human interactions occur in response to some cue; the cue may be the initiating event itself, an alarm, a procedural step or an observation. In contrast to pre-initiator human interactions, post-initiator human interactions are **dynamic and subject to time constraints.** This is assumed to increase the level of dependency between members of the crew, which increases the probability of failure. Some performance shaping factors may mitigate the stress level thus decreasing the probability of failure, while other performance shaping factors may aggravate the stress level thus increasing the probability of failure. Post-initiator human interactions are analyzed in a cue-response time framework.



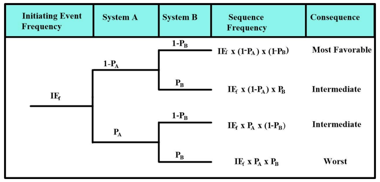
Two types of C human interactions



- Non-recovery post-initiator HFE (in sequence fault trees) C_P
  - Failure to accomplish procedurized actions
    - The failure to change the mode of a system under the appropriate conditions
    - The failure to initiate the function of a system that normally requires manual actuation or to align a backup system.
- Recovery post-initiator HFE (recovery actions added to min cut sets) C_R
  - Non-Procedurized actions -- knowledge based
  - Several failures occur
  - Actions are not guided by explicitly by procedures

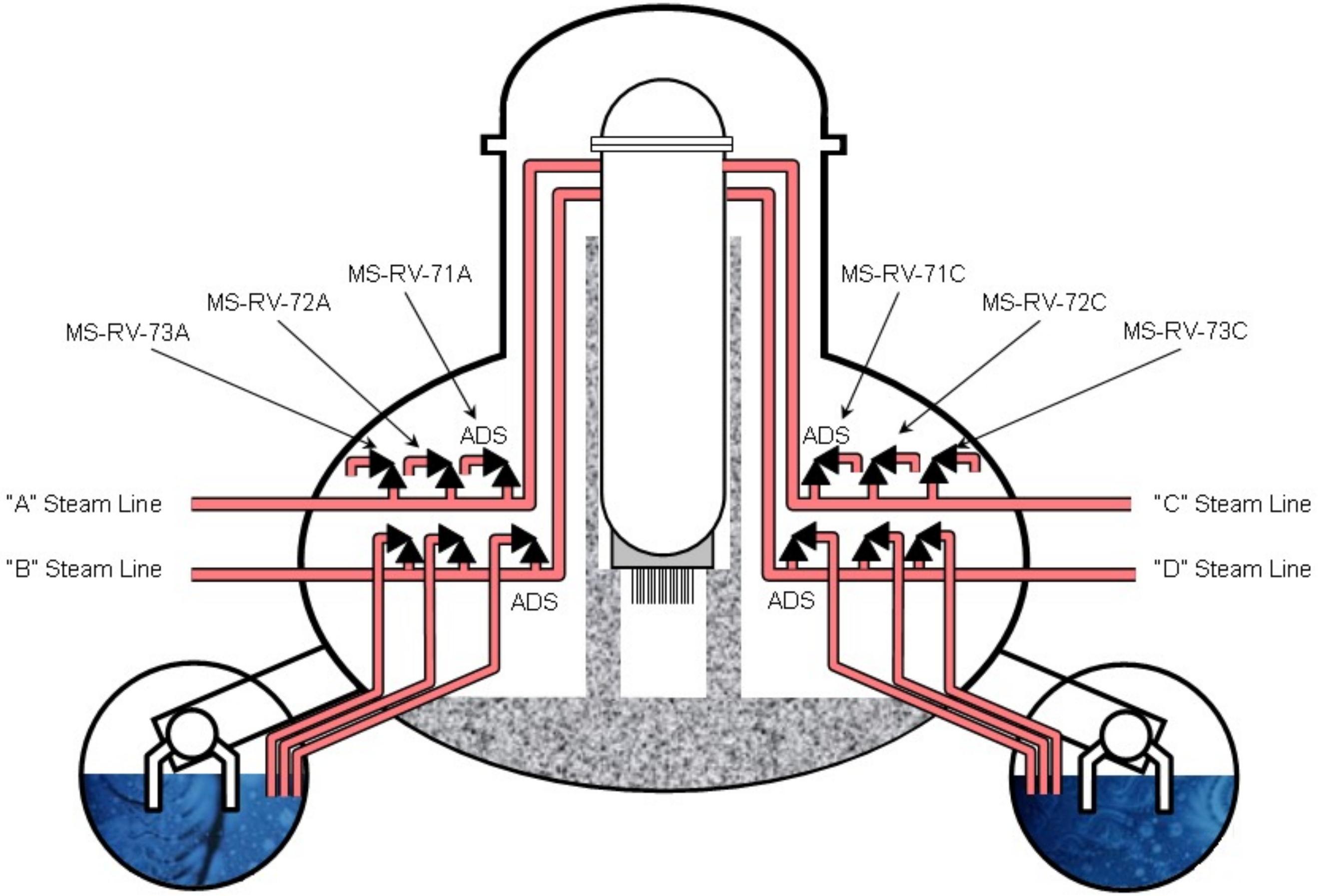


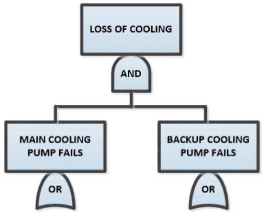
Manual Actuation of ADS valves (example of C_P Interaction)



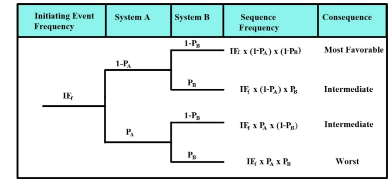
RV Relief Valves

ADS Automatic Depressurization System

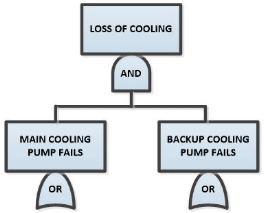




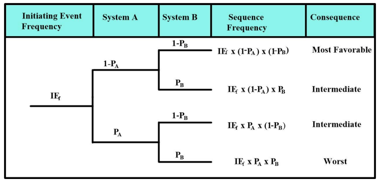
Examples of Human Error Probabilities



CREAM Nominal Values and Uncertainty Bounds for Cognitive Failures				
Cognitive Function	**Generic Failure Type**	**5% Lower Bound**	**Median**	**95% Upper Bound**
Observation	Wrong object observed	3.0E-04	1.0E-03	3.0E-03
	Wrong Identification	1.0E-03*	3.0E-03*	9.0E-03*
	Observation Not Made	1.0E-03*	3.0E-03*	9.0E-03*
Interpretation	Faulty diagnosis	9.0E-02	2.0E-01	6.0E-01
	Decision error	1.0E-03	1.0E-02	1.0E-01
	Delayed interpretation	1.0E-03	1.0E-02	1.0E-01
Planning	Priority error	1.0E-03	1.0E-02	1.0E-01
	Inadequate plan	1.0E-03	1.0E-02	1.0E-01
Execution	Action of Wrong Type	1.0E-03	3.0E-03	9.0E-03
	Action at wrong time	1.0E-03	3.0E-03	9.0E-03
	Action on wrong object	5.0E-05	5.0E-04	5.0E-03
	Action out of sequence	1.0E-03	3.0E-03	9.0E-03
	Missed action	2.5E-02	3.0E-02	4.0E-02

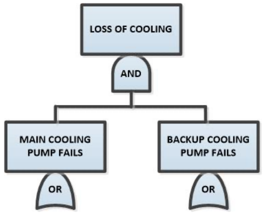


Performance Shaping Factors for human error probabilities (CREAM)

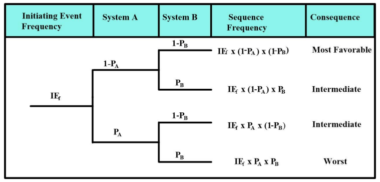


CREAM Performance Factors

Factor	Level	Cognitive Function			
		Observation	Interpretation	Planning	Execution
Adequacy of Organization	Very efficient	1.0	1.0	0.8	0.8
	Efficient	1.0	1.0	1.0	1.0
	Inefficient	1.0	1.0	1.2	1.2
	Deficient	1.0	1.0	2.0	2.0
Working Conditions	Advantageous	0.8	0.8	1.0	0.8
	Compatible	1.0	1.0	1.0	1.0
	Incompatible	2.0	2.0	1.0	2.0
Adequacy of Man Machine Interface	Supportive	0.5	1.0	1.0	0.5
	Adequate	1.0	1.0	1.0	1.0
	Tolerable	1.0	1.0	1.0	1.0
	Inappropriate	5.0	1.0	1.0	5.0
Availability of Procedures	Appropriate	0.8	1.0	0.5	0.8
	Acceptable	1.0	1.0	1.0	1.0
	Inappropriate	2.0	1.0	5.0	2.0
Number of *Simultaneous Goals*	Fewer than capacity	1.0	1.0	1.0	1.0
	Matching capacity More	1.0	1.0	1.0	1.0
	than capacity	2.0	2.0	5.0	2.0
Available Time	Adequate	0.5	0.5	0.5	0.5
	Temporarily inadequate	1.0	1.0	1.0	1.0
	Continuously inadequate	5.0	5.0	5.0	5.0
Time of day	Day-time	1.0	1.0	1.0	1.0
	Night-time	1.2	1.2	1.2	1.2
Adequacy of Training/Preparation	Adequate, high experience	0.8	0.5	0.5	0.8
	Adequate, low experience	1.0	1.0	1.0	1.0
	inadequate	2.0	5.0	5.0	2.0
Crew Collaboration Quality	Very efficient	0.5	0.5	0.5	0.5
	Efficient	1.0	1.0	1.0	1.0
	Inefficient	1.0	1.0	1.0	1.0
	Deficient	2.0	2.0	2.0	5.0



Time reliability correlations operator action – log normal distribution



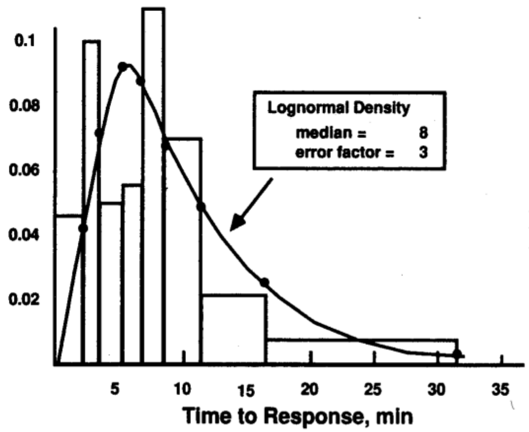


Figure 4-3. Density for the data of Table 4-1.

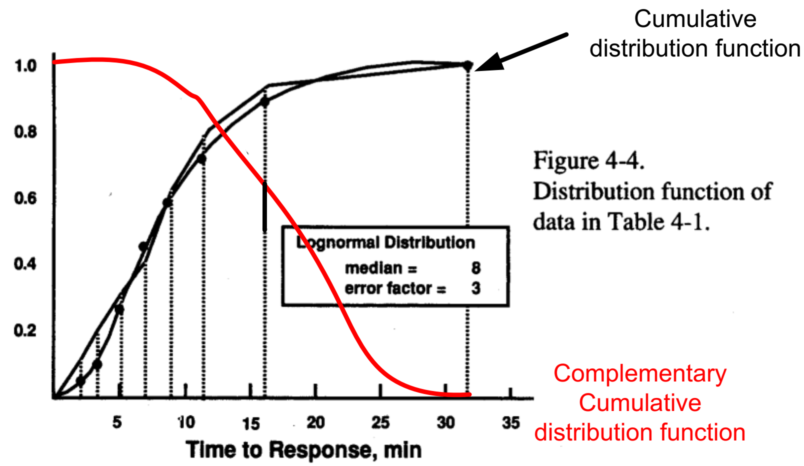
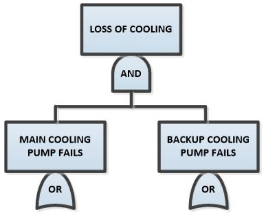
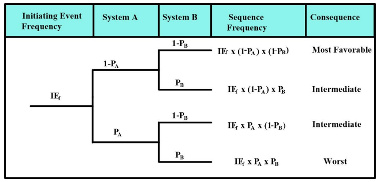
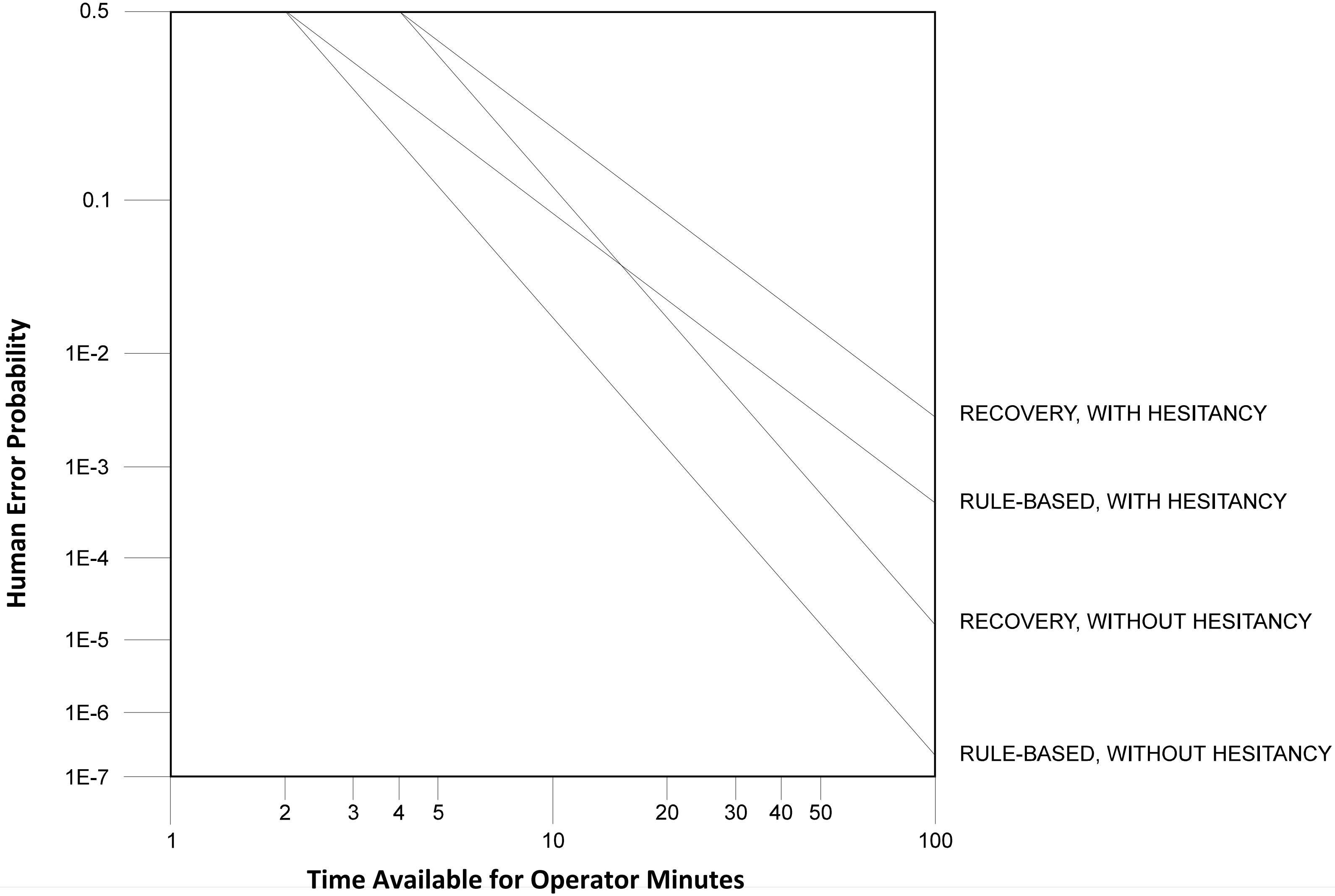


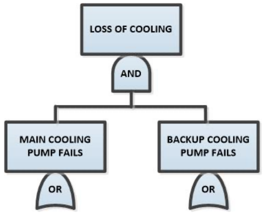
Figure 4-4. Distribution function of data in Table 4-1.



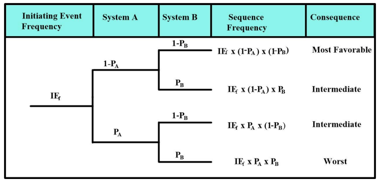
TIME RELIABILITY CORRELATION OPERATOR RESPONSE





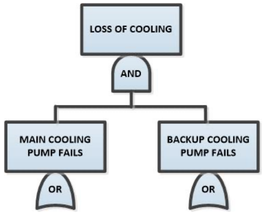


Human Performance Limiting Values

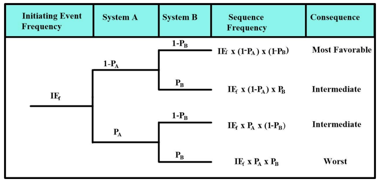


Actions	HPLV
Actions taken by a single team.	1E−5/d
Actions taken by more than one team either when the significance of the goal is well understood and the time is adequate or when extended time is available.	1E−6/d
Actions taken by more than one team when the significance of the goal is well understood and a fundamental part of training. Extended time must also be available so that inaction would have to persist for several hours if no further attempts were made to achieve the desired goal.	1E−7/d

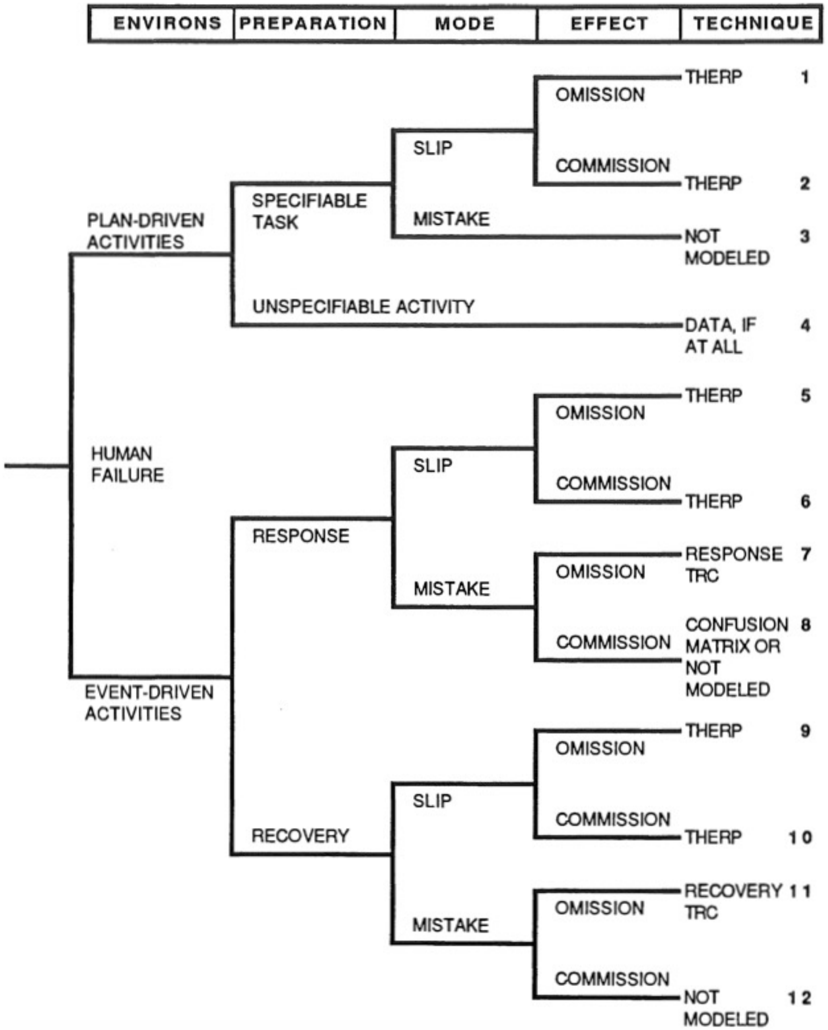
NOTE: d = demand; HPLV = human performance limiting values.
Source: Modified from *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique*



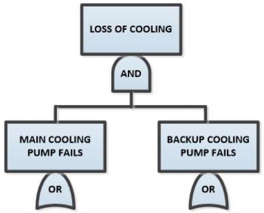
Classification System for Human Failure Events



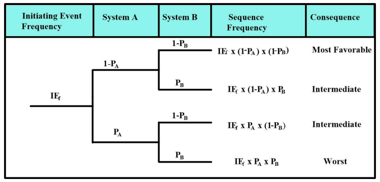
Reference:
Human Reliability Analysis,
E.M.Dougherty, Jr.
J.R.Fragola, John Wiley and Sons, 1988



“slips” are mechanistic failures in carrying out routine, often prescribed procedures versus “mistakes” are errors in the cognitive processes of interpretation and decision making especially pertinent to contingency actions.

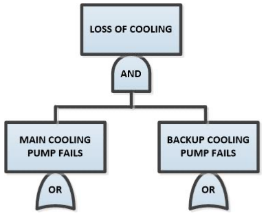


Fire Risk Evaluation

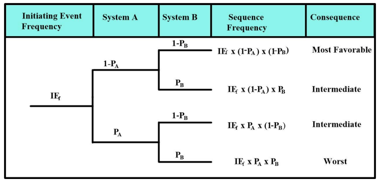


- Objective: To quantify fire-induced Core Damage Frequency
- Tasks

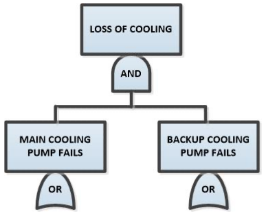
1. Ignition frequency
2. Scenario-specific equipment and cable damage
3. Equipment failure modes and likelihoods
4. Credit for fire mitigation (detection and suppression)
5. Fire-specific HEPs
6. Quantification of the FPRA plant response model



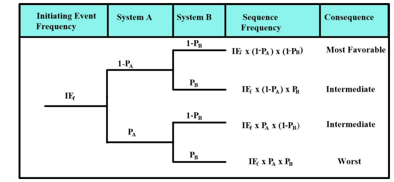
Fire PRA Plant Response Model



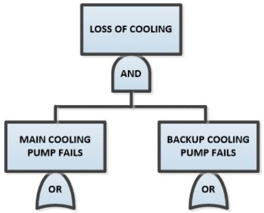
- *fire PRA plant response model:* a representation of a combination of equipment, cable, circuit, system, function, and operator failures or successes, of an accident that when combined with a fire-induced initiating event can lead to undesired consequences, with a specified end state (e.g., core damage or large early release).



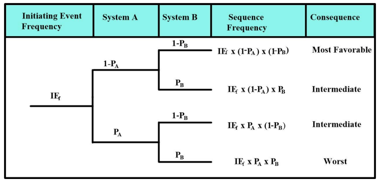
High Level Requirements HLRs per PRA standard

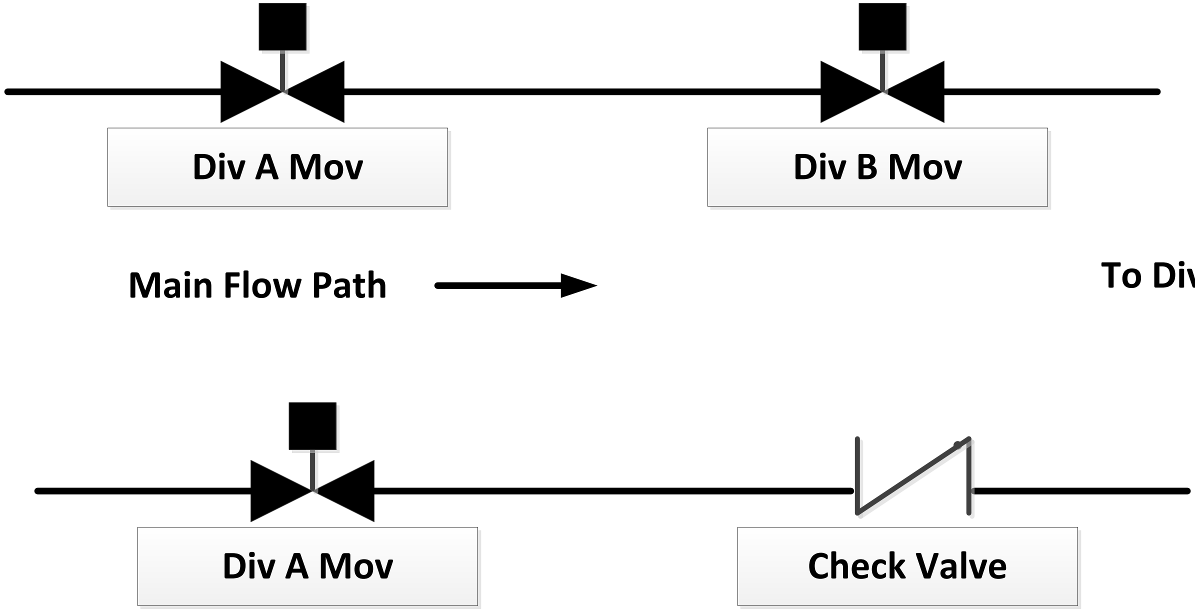


- HLR-ES-A: The Fire PRA shall identify equipment whose failure caused by an initiating fire including spurious operation will contribute to or otherwise cause an initiating event (6 supporting requirements SRs)
- HLR-ES-B: The Fire PRA shall identify equipment whose failure including spurious operation would adversely affect the operability/functionality of that portion of the plant design to be credited in the Fire PRA (5 SRs)
- HLR-ES-C: The Fire PRA shall identify instrumentation whose failure including spurious operation would impact the reliability of operator actions associated with that portion of the plant design to be credited in the Fire PRA (2 SRs)
- HLR-ES-D: The Fire PRA shall document the fire PRA equipment selection, including that information about the equipment necessary to support the other fire PRA tasks (e.g. equipment identification, equipment type, normal, desired, failed states of equipment) in a manner that facilitates fire PRA applications, upgrades, and peer review (1 SR)



Fire PRA Component Selection
Flow Diversion Path Example





To Diversion path

Takes two spurious hot shorts to open diversion path -- included in model

Takes 1 spurious hot short and failure of the check valve to open

Screened from model if not potential high Consequence event