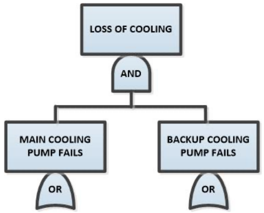
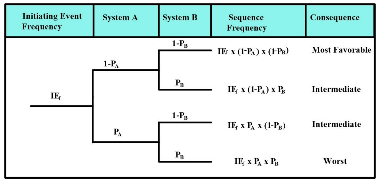
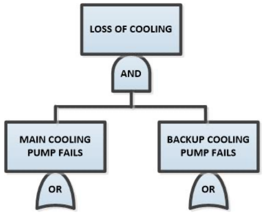


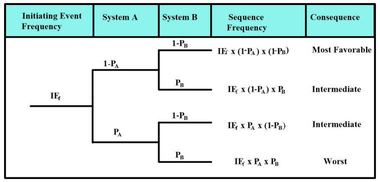
Event Tree/Fault Tree Analysis – Introduction – Session 1 of 4



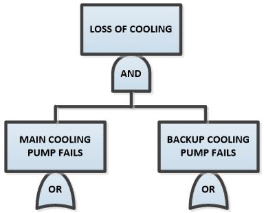
- Overview of the generation and analysis of event tree and fault tree analysis
- Describe supporting analysis
  - System safety analysis
  - Hazard Analysis
  - Failure Modes and Effects Analysis
- Instructor Howard Lambert



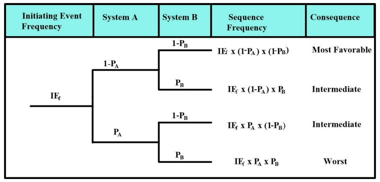
Presentation Goals



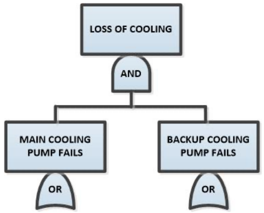
- Motivate audience to the usefulness of event tree and fault tree generation and analysis
- Show how the analysis is used in system safety analysis, reliability and probabilistic risk assessment to generate and analyze undesired events and accident scenarios
- Show how the analysis can recommend safety improvements through hazard reduction, prevention and/or mitigation.
- Discuss historical aspects of system safety analysis, fault tree analysis and probabilistic risk assessment.
- Prerequisite for a training course on event trees and fault trees (for those who want to take the course)
- Numerous examples and case studies of various technologies to illustrate concepts
- What is required for a comprehensive risk analysis?



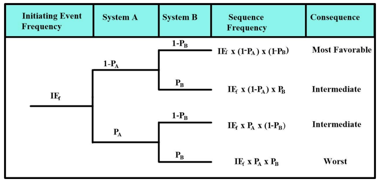
References



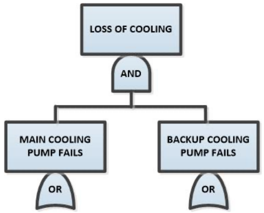
- Methodology
  - EPRI Training Notes
  - PRA procedures guide
  - ASME standard
  - Paper on Initiating and Enabling Events
- Fault Tree Analysis
  - Fault Tree Handbook
  - Vesely FTA
- Human Reliability Assessment
  - Tony Spurgin
  - Dougherty and Fragola
  - Swain and Guttman (First Generation)
  - Second Generation HRA techniques CREAM, SPAR etc



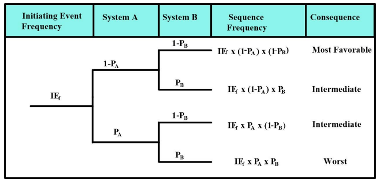
References Continued



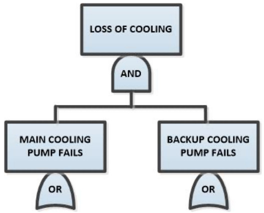
- PRAs
  - Reactor Safety Study
  - Shoreham Nuclear PRA
  - Surry PRA
- Safety and Reliability Studies
  - NIF (LLNL)
  - Criticality Safety (LLNL)
  - Yucca Mountain (DOE)
  - Chlorine Vaporizer (DuPont)
  - Salt Process Cell Study (SRS)
- Computer Codes
  - FTAP
  - IMPORTANCE



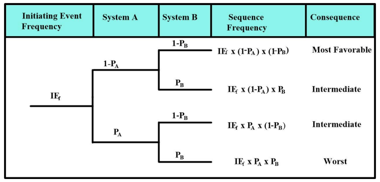
What are Event Trees and Fault Trees?



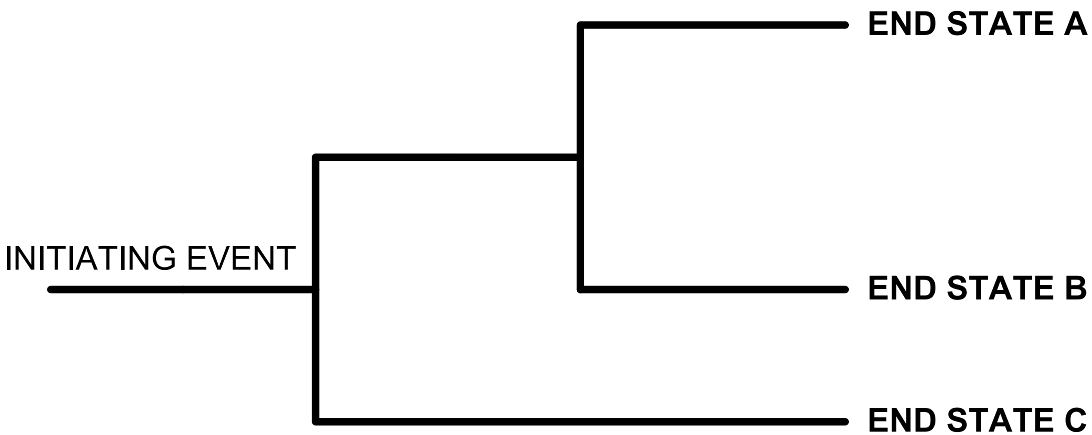
- They are multiple thread logic models that depict the parallel and sequential sequence of events leading to undesired events or accident scenarios
- An **Event Tree** is an inductive logic model starts with an initiating event and depicts branching nodes that can lead to undesired system states and accident scenarios
  - An event tree is an inductive logic model
    - Future thinking
    - Ask the question “what if?”
    - Specific to general

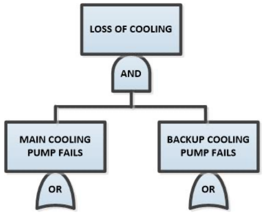


Event Tree Structure

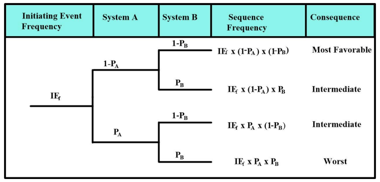


- EVENT TREE
  - Branching tree left to right
  - Starts with initiating event
  - Branch downwards generally indicates failure
  - Branch upwards generally indicate success
  - Define end states and their consequences

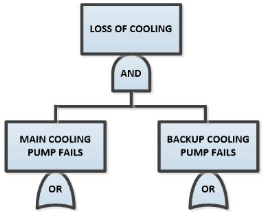




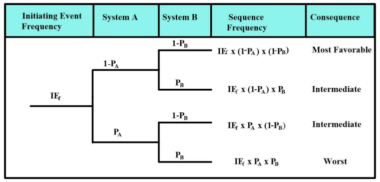
What are Event Trees and Fault Trees?



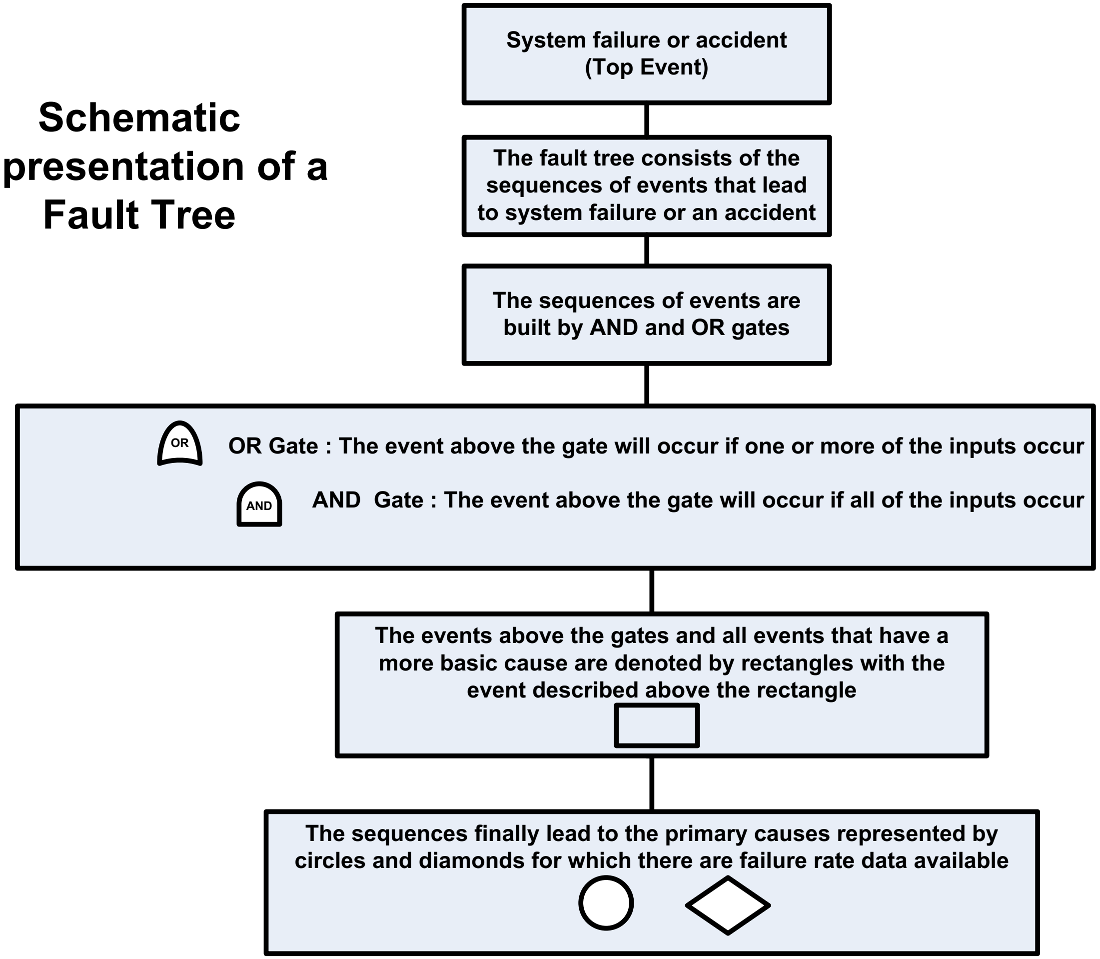
- A **Fault Tree** is a deductive logic model that starts with an undesired top event and depicts the sequential and parallel events leading to the top event with logic gates such as AND, OR and Combination.
  - A fault tree is a deductive logic model
    - Past thinking
    - Ask the question "How can something occur?
    - General to specific

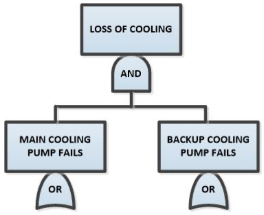


Levels of Fault Tree Development

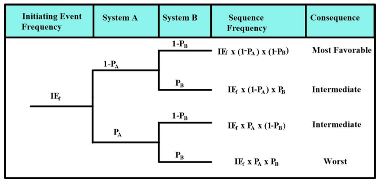


Schematic Representation of a Fault Tree

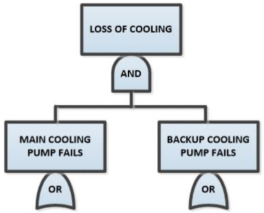




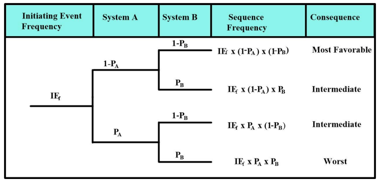
LLNL Programs that use Fault Tree Analysis (FTA) and Event Tree Analysis (ETA)



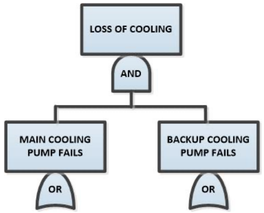
- Nuclear Reactor Safety – USNRC programs
  - Reactor Safety Study (1970's)
  - Material Control Program (mid 1970's)
  - Seismic Safety Research Program (1980's)
  - Control room design reviews (1980's)
  - Reactor Instrumentation studies (1990's to present)
  - Radiation Embrittlement of reactor pressure vessel supports (1993)
  - Portable Reactor Study (2000's)
- AVLIS – 80's
- Weapons Assembly/Disassembly Pantex/DAF
- SARs/Safety Studies – Super block, HWM, NIF, Site 300, HEAF, Test Site, Yucca Mountain
- Space Program -- NASA
  - Space Shuttle



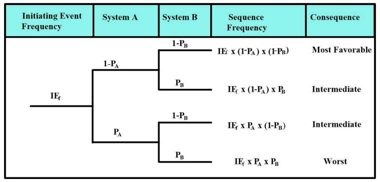
Risk Assessment – Quartet



1. What can go wrong?
2. How can it go wrong? ←
3. How likely is it?
4. What are the consequences?



Risk Definition

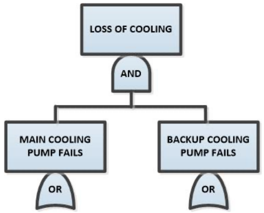


- Risk – the frequency with which a given consequence occurs

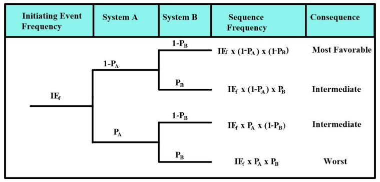
RISK [Consequence Magnitude/unit of time] =

Frequency [events/unit of time]

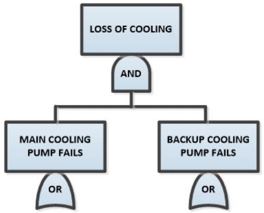
x Consequences [magnitude/event]



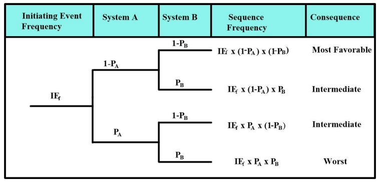
Chinese Fortune Cookie



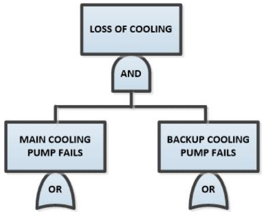
- Keep in mind it's the journey that counts and not the destination that counts
- For safety and risk assessment both the journey and destination counts
- Journey (process) = scope, assumptions, initial conditions, scenario definitions, screening, system understanding, failure mode identification, hazards analysis, model generation
- Destination = min cut sets, probability calculations, consequence analysis, computer analysis, graphs, bar charts etc



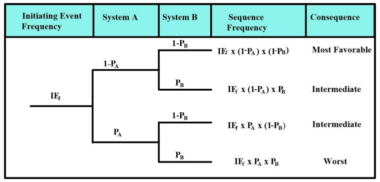
What can go wrong?



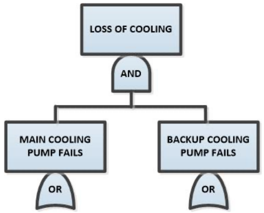
- What are the scenarios that can cause injury or harm?
  - E.g. fire, explosion, radiological or toxicological release
  - **How can these accident scenarios occur?**
  - Risk assessment uses **symbolic logic** trees to generate and analyze these scenarios, e.g.,
    - Event trees
    - Fault trees
    - Other



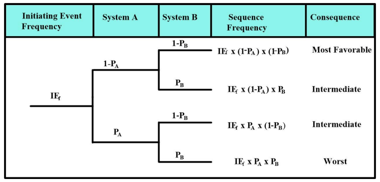
Usefulness of event trees and fault trees



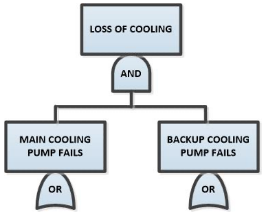
- The **process** of constructing them leads to insights regarding system operation and system failure modes
- They can be qualitatively evaluated – e.g. find the root causes of failure, i.e., human error, hardware failure, software failure, environmental conditions, etc.
- **Identification of Single point failures and common cause failures**
- They can be quantitatively evaluated – e.g., find the probability/frequency of system failure and dominant risk contributors



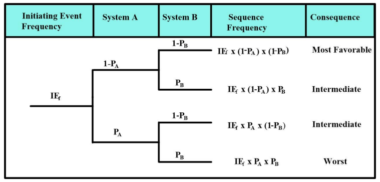
Types of Events/Scenarios Analyzed



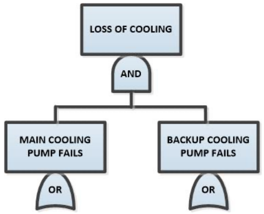
- **Types of undesired events and accident scenarios analyzed**
  - — Reliability
    - Failure to perform required functions or failure to achieve Mission goals
    - Use denial – system is unavailable
  - — Safety –
    - system malfunctions cause injury or harm
  - — Security –
    - Sabotage, Classified information violation, Theft of nuclear material, security system breach
  - — Environmental Protection –
    - release of toxic, biological or radioactive substances



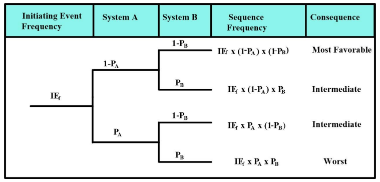
Scope of the Analysis



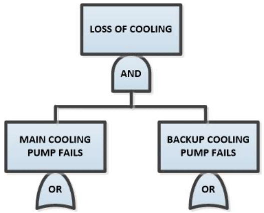
- Goals and Objectives of the Study
- Time Available to conduct the Study
- Information available
- Resources Available
- Temporal and Spatial Bounds
- What analysis techniques (basis) are used to determine if the process is safe and/or reliability?
- Extensiveness of the consequence analysis
- Type of initiating events to be considered
- What is the reliability trial?
- System Mode of Operation startup, steady state, shutdown



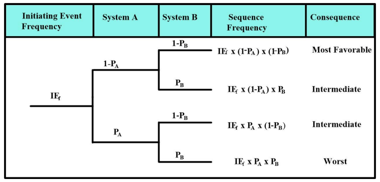
Important topics



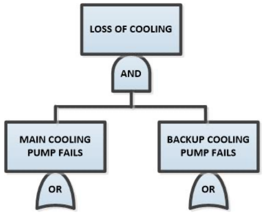
- Reliability trial
  - Assumptions (initial conditions)
  - System Description (Nuclear Industry uses system notebooks)
  - Initiating event identification
    - Internal events
    - External events
  - Data Analysis
  - Models and software used
- Human Reliability Assessment
- Initiating Event Fault tree analysis
  - Two types of failures
  - Initiating and enabling events



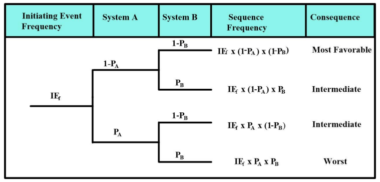
Important topics Continued



- Success Criteria
- Master Logic Diagrams
- Event Sequence Diagrams
- Time Lines
- Directed Graph Analysis
- Safety Goals
- Transparency
- Traceability
- Laws of conditional probability do not hold

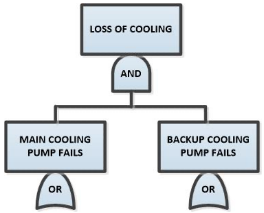


Assumptions (examples)

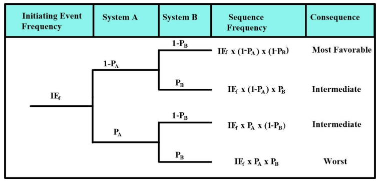


Safety and Reliability

- Existence or non-existence of a feature or condition – may involve success criteria
- Design or Construction Errors
- Operator Recovery
- Flammable Mixtures
  - 30% of the time on aircraft with heated center wing tanks
  - 100% of the time when space shuttle is filled with liquid hydrogen and oxygen
- Flow diversion paths are not considered for pipes that have less than ½'" in diameter
- No pre-existing failures for space shuttle
- Reliability of connectors assumed to be one – e.g., pipes and wires
- Malevolent Acts/sabotage excluded

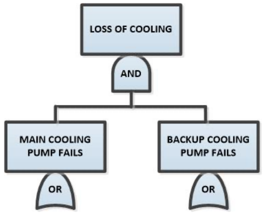


Assumptions Continued

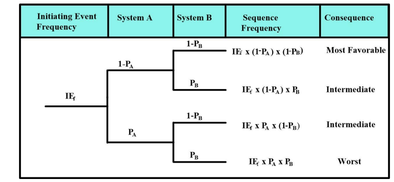


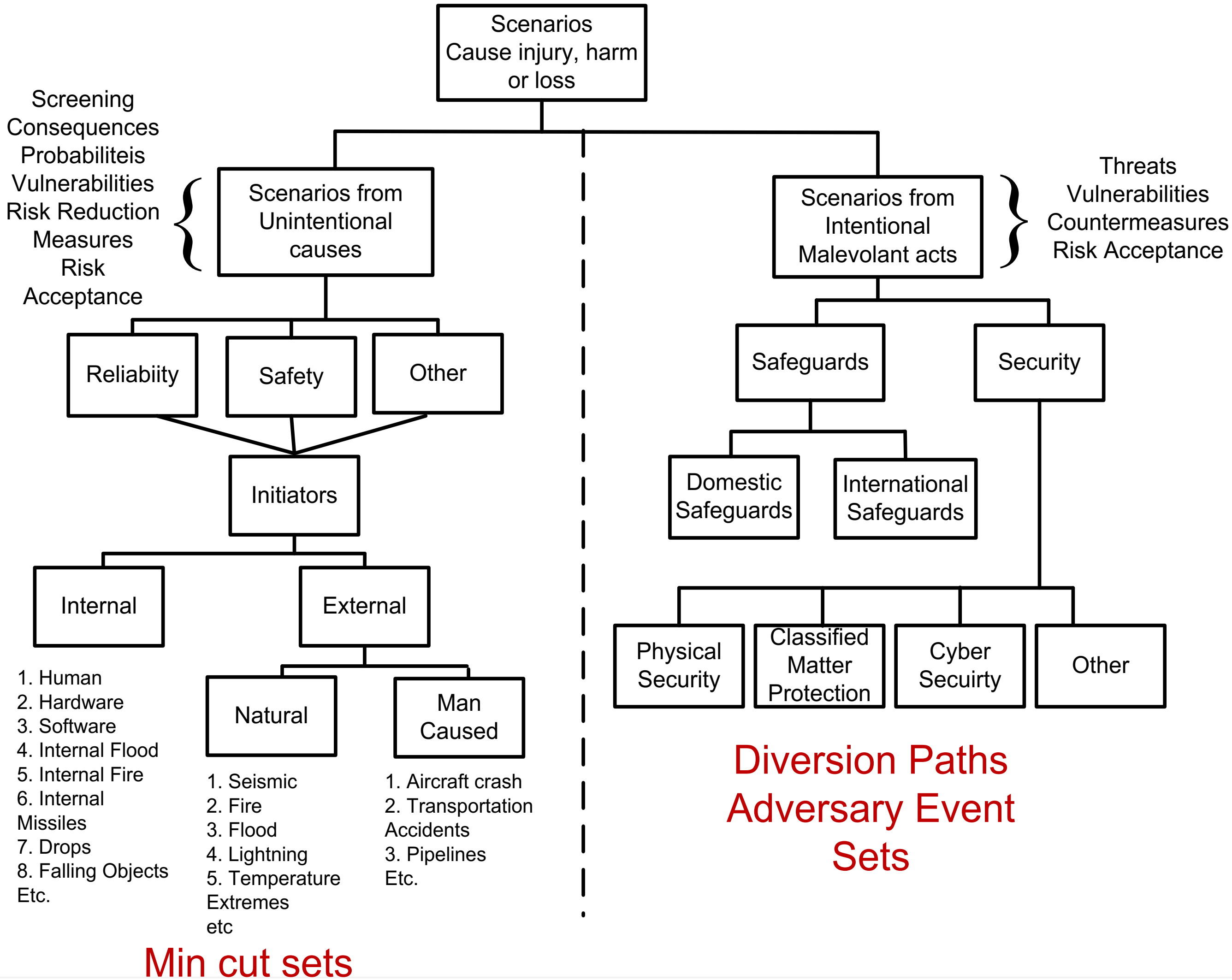
- Safeguards and Security
  - Knowledge of adversary(ies)
  - Types of threats covert, overt, combination, sabotage
  - Resources
  - Collusion

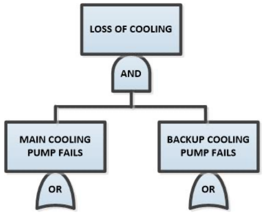
20



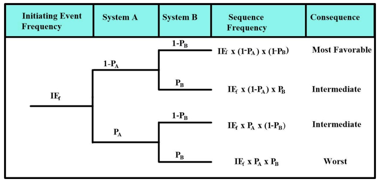
Scenario Breakdown – Scope/Initiating Events



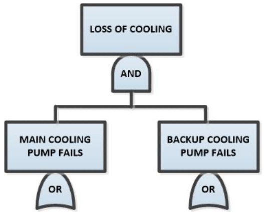




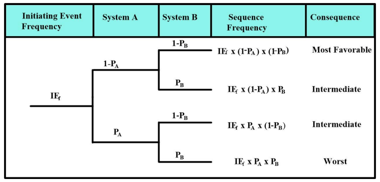
System Safety Analysis



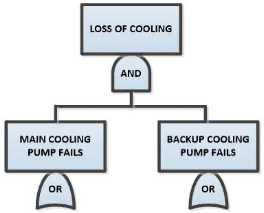
- Use experience both direct and related
- Analysis updated and revised throughout system life cycle, womb to tomb, cradle to grave philosophy
- System familiarization and understanding
- Identification of hazards, undesired events and accident/diversion scenarios



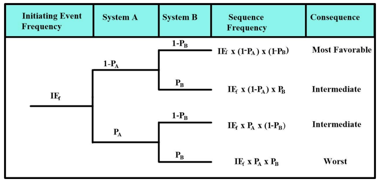
System Safety Analysis -- Continued



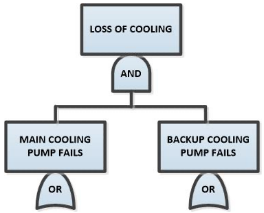
- Modeling and analysis techniques
  - Inductive analysis (what if, bottom-up, future thinking analysis)
  - Deductive (how can something occur, top-down, past thinking analysis)
- Implementation of controls – preventive, mitigation and administrative measures to achieve adequate level of reliability, safety, environmental protection, security etc.
- Tradeoff studies – consider cost, legal and contractual requirements, competing objectives, reliability versus safety versus security, political etc.



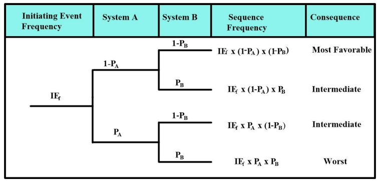
System Safety Analysis Techniques

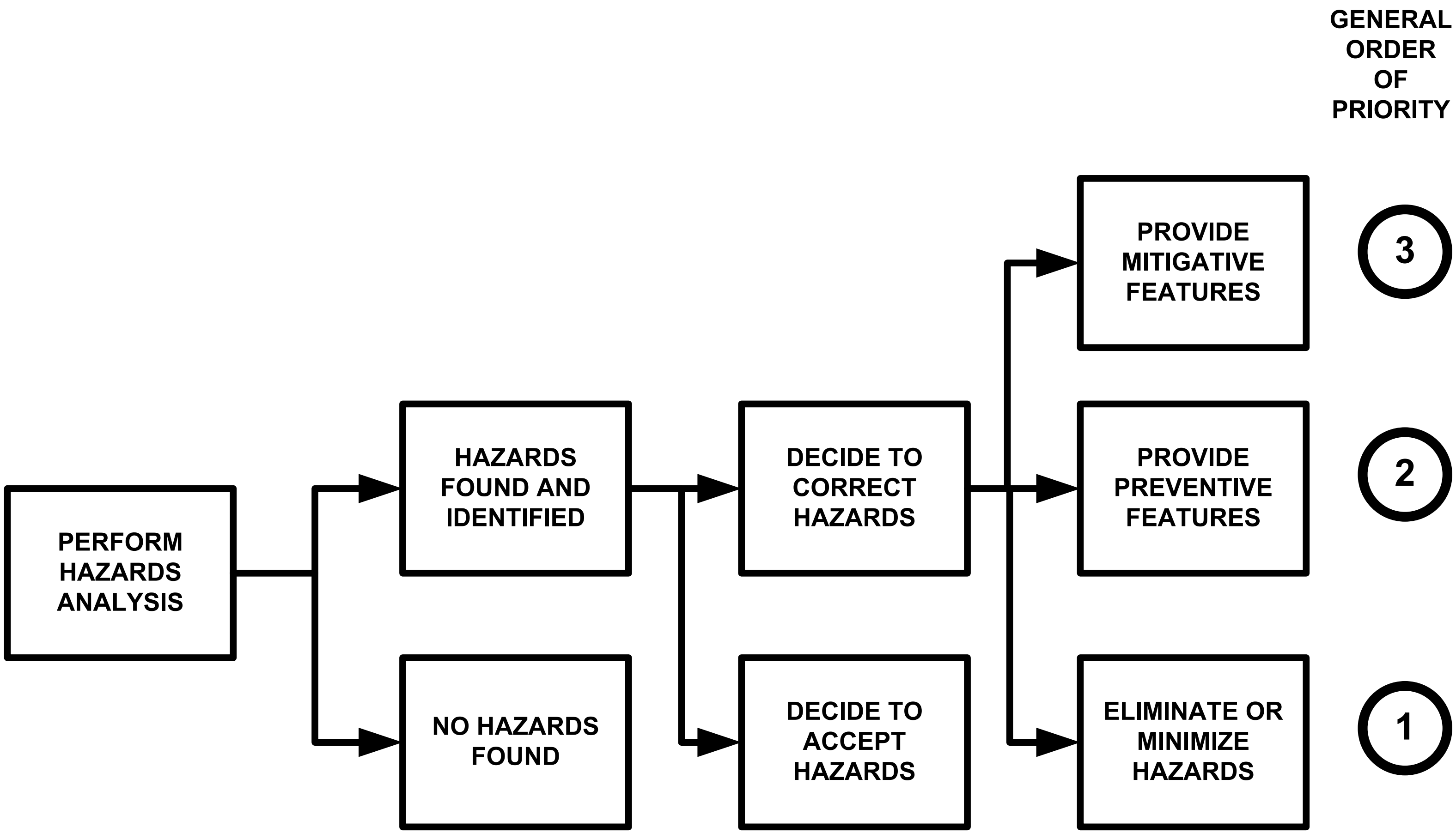


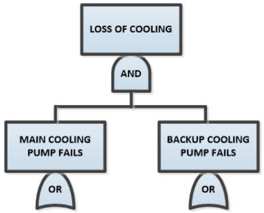
- Inductive analysis techniques
  - — Preliminary hazards analysis
  - — Fault hazard analysis
  - — **Hazards and Operability Study -- HAZOP**
  - — **Failure modes and affects analysis (FMEA)**
  - — **Event Trees**
  - — Markov chains
  - — What if
  - — **Checklists**
- Deductive analysis techniques
  - — **Fault Tree Analysis**
  - — **MORT**
- Cause Consequence Diagrams
- Red indicates techniques used in in-class assignments



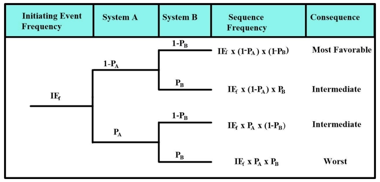
HAZARDS ANALYSIS FLOWCHART

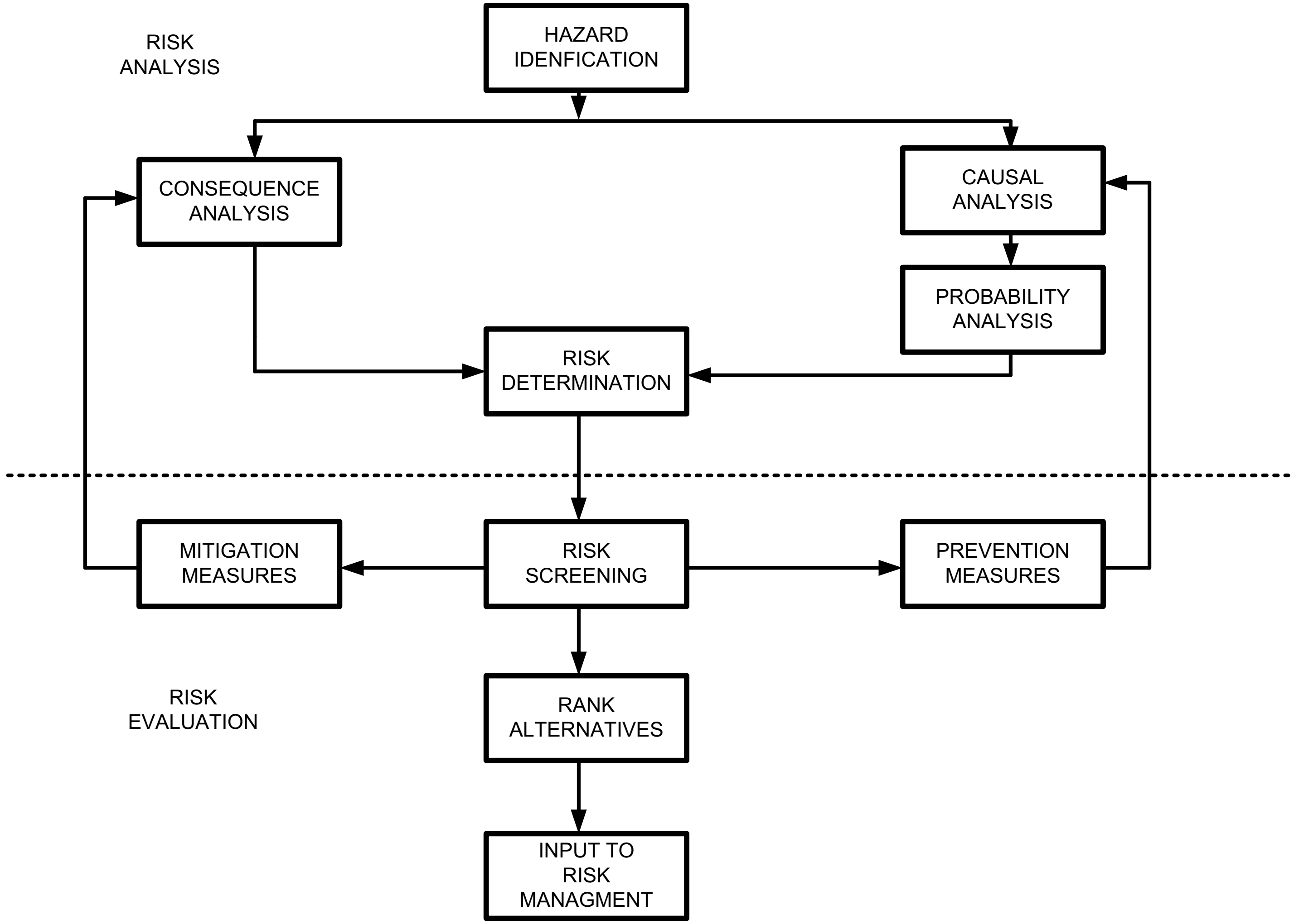


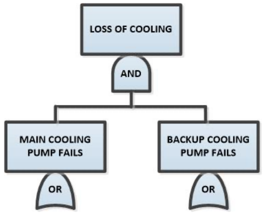




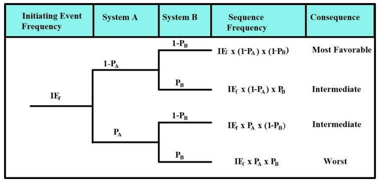
Risk Assessment and Management Flowchart

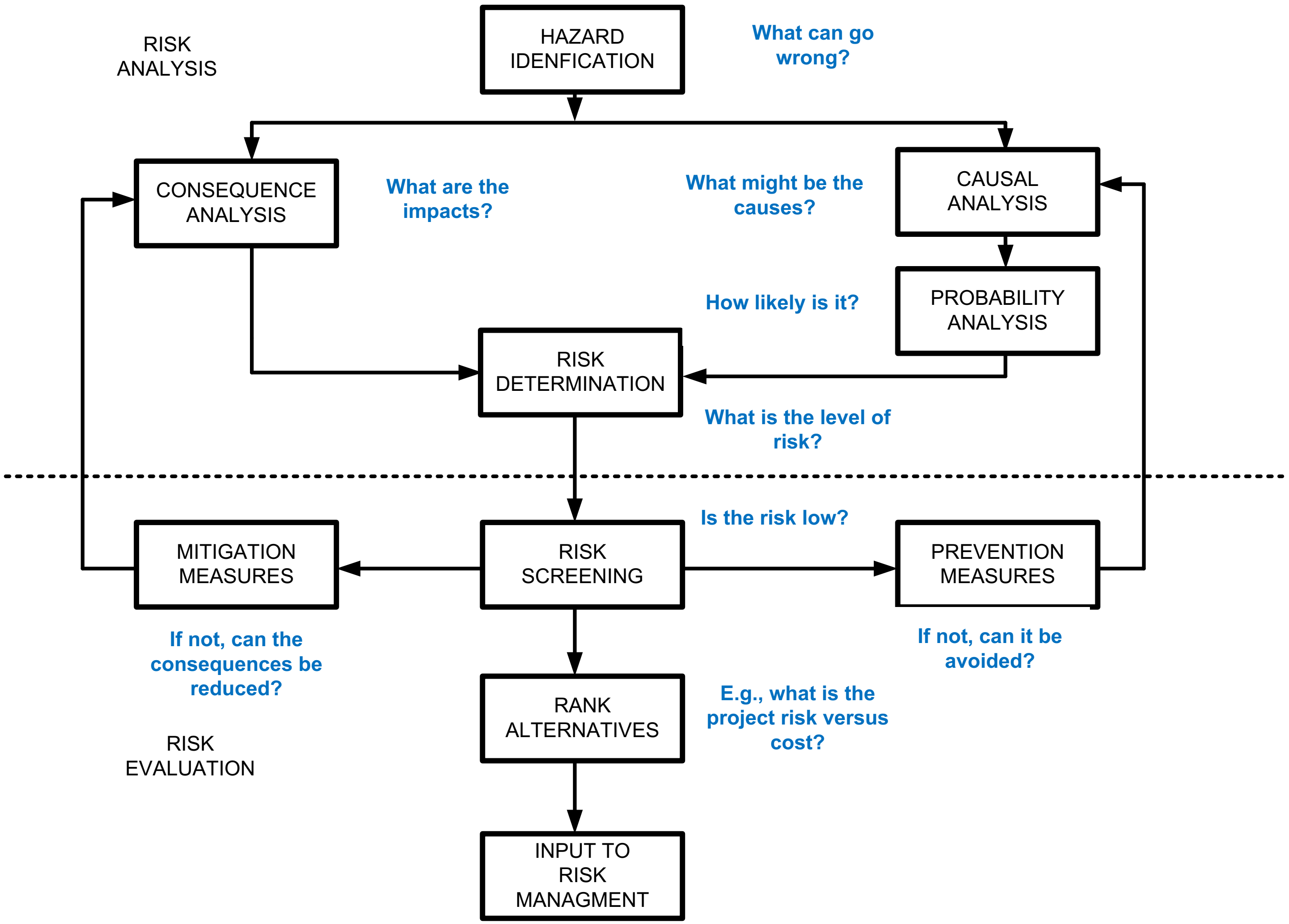


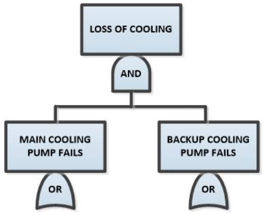




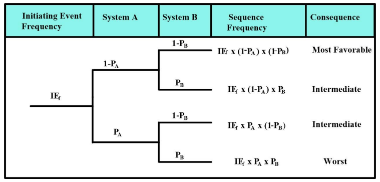
Risk Assessment and Management Flowchart Questions

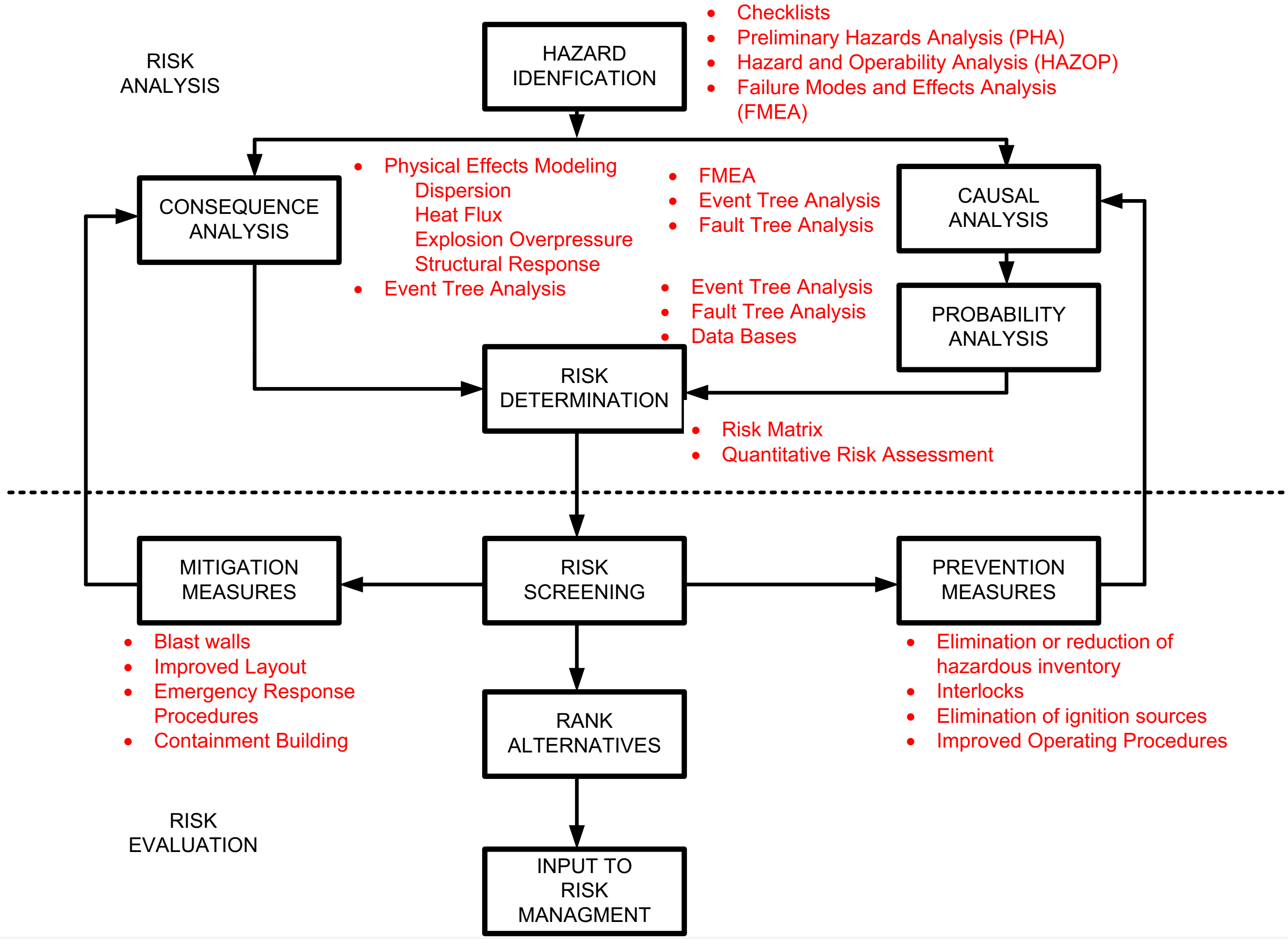


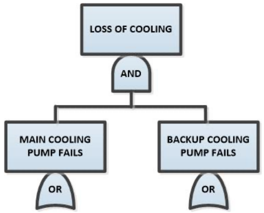




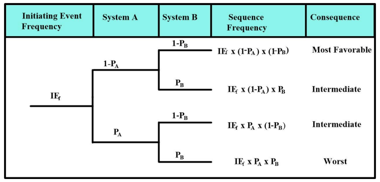
Risk Assessment and Management Flowchart -- Tools







Hazards Checklists



Group	Hazard Energy Source	
Electrical	Battery banks Cable runs Diesel generators Electrical equipment Hot plates Heaters High voltage Locomotive, Electrical Motors	Pumps Power tools Switchgear Service outlets, fittings Transformers Transmission lines Underground wiring Wiring
Thermal	Bunsen burner/ Hot plates Electrical equipment Furnaces Heaters Steam lines Welding torch	Boilers Lasers Electrical wiring Welding surfaces Engine exhaust Exothermic reaction
Kinetic – Linear and Rotational (Friction)	Belts Bearings Fans Gears Motors Presses Grinders Crane Loads (in motion) Power tools	Vehicles Rail cars Fork lifts Carts Dollies Centrifuges Drills Saws Shears
Pyrophoric Material	Pu and U metal	Pu
Spontaneous Combustion	Nitric acid and organics Grease Diesel fuel	Paint solvents Cleaning/Decon solvents Gasoline
Open Flame	Bunsen burners	Welding/cutting flames
Flammables	Flammable gases Flammable liquids Natural Gas Spay paint Gasoline	Compressed flammable gases Propane Paint solvent Cleaning/decon solvents
Combustibles	Combustible materials Plastics	Paper/wood products Petroleum based products
Chemical Reactions	Uncontrolled chemical reactions	
Potential (pressure)	Gas bottles Gas receivers Pressure vessels Steam headers and lines Coiled springs	Boilers Heated surge tanks Autoclaves Furnaces Stressed members
Non-Ionizing Radiation		

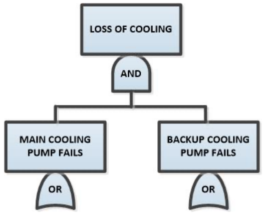
Reference:

HAZARD ANALYSIS METHODOLOGY

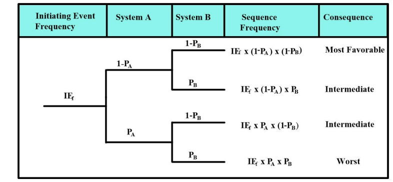
Westinghouse Savannah River Company Projects

Engineering and Construction Division

Aiken, SC



Hazards Checklists Continued



Group	Hazard Energy Source	
Potential (height/mass)	Stairs Lifts Cranes Elevated doors Loading docks Hoists Elevators	Trucks Jacks Scaffolds and Ladders Pits Elevated work Surfaces Mezzanines
Firearm Discharge	Firearm Discharge (puncturing)	
Explosive/Pyrophoric Material	Explosive gases Explosive chemicals Hydrogen Dynamite Sodium Hydrogen (batteries) Primer cord Propane	Dusts Nitrates Peroxides Caps Plutonium/Uranium Potassium Electric squibs Superoxides
Radiological Material	Radiological Material	
Hazardous Material	Alkali Metals Asphyxiants Biologicals Carcinogens Corrosives Acetone Fluorides Lead Oxidizers Asphyxiation Drowning Other toxics	Ammonia and compounds Beryllium and compounds Chlorine and compounds Trichlorethylene Decontamination solutions Dusts and particles Sandblasting particles Metal plating Herbicides Insecticides Bacteria Viruses
Ionizing Radiation Sources	Fissile material Radiography equipment Radioactive material Radioactive sources	Electron beams X-ray machines Critical masses Contamination
Fissile Material	Fissile Material	Fissionable Material
Non-facility Events	Explosion Fire Other	Power Outage Aircraft crash Transportation accident
Vehicles in Motion	Airplane Helicopter Train	Forklifts Truck/Car Heavy construction equipment
Crane	Crane	Crane loads
Natural Phenomena	Straight wind Tornado Earthquake Flood	Lightning Rain/hail Snow, freezing weather

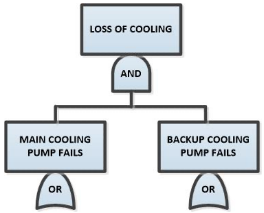
Reference:

HAZARD ANALYSIS METHODOLOGY

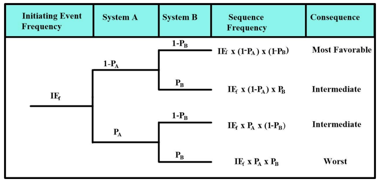
Westinghouse Savannah River Company Projects

Engineering and Construction Division

Aiken, SC



Sample Hazard Identification Checklist – Page 1, Biological and Chemical

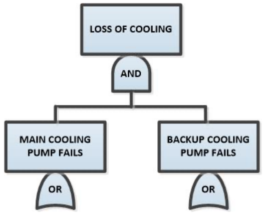


I. Biological Hazards

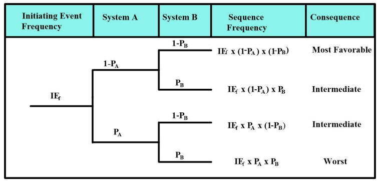
- Non-Select Agents
  - RG1 Agents
  - RG2 Agents
  - RG3 Agents
- Select Agents
  - RG1 Agents
  - RG2 Agents
  - RG3 Agents
- Other Biohazard (e.g., nucleic acid, lab animals, contaminated needles/sharps, animal/human tissues & fluids)
- Materials covered under OSHA Blood borne Pathogens Standard - 29 CFR 1910.1030

II. Chemical Hazards

- Flammable, volatile or fuming
- Toxic materials (acutely toxic, toxic, bio-derived toxin, systemic toxin, toxic gases)
- Corrosives/irritants
- Reactive materials (e.g., air/water sensitive; pyrophoric; thermally, shock, or friction sensitive; perchlorate)
- Carcinogens, mutagens, reproductive hazards
- Pesticides
- Beryllium
- Materials of special concern (e.g., alkali metals, fluorine, asbestos, lead, mercury, PCB)
- Other regulated metals (e.g., chromium, copper, nickel, zinc)
- Other



Sample Hazard Identification Checklist – Page 2, Explosive and Radiological

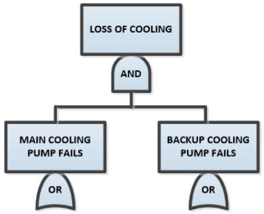


III. Explosive Hazards

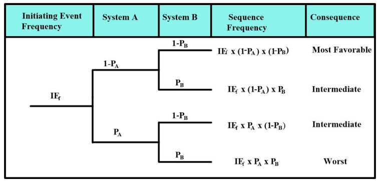
- Primary High Explosives
- Secondary High Explosives
- Propellants/Low Explosives
- Firearms Ammunition
- Fragmentation Hazards (Primary Fragments)
- Group L Explosives

IV. Radiological Hazards

- <1 of Reportable Quantities (RQ) thresholds (40 CFR 302.4 Appendix B)
- >1 of RQ thresholds < Cat. 3 Thresholds (DOE-STD-1027-92, Table A.1)
- >Cat. 3 Thresholds (DOE-STD-1027-92, Table A.1) < Cat. 2 Thresholds (DOE-STD-1027-92, Table A.1)
- Radiation generating devices not covered by DOE O 420.2B (X-rays, Electron Beams, Radiography Equipment)
- Radiation generating devices covered by DOE O 420.2B (Accelerators).
- Exempted materials:
  - Radioactive Certified Sealed Sources
  - Rad. In Type B Containers with current certificates of compliance
  - Either in quantities>Cat. 3 thresholds (DOE-STD-1027-92, Table A.1)



Sample Hazard Identification Checklist – Page 3, Industrial



V. Industrial Hazards

- Electrical

Battery banks, Cable runs, Diesel generators, Electrical equipment, Heaters, High voltage (> 600V), Motors, Power tools, Pumps, Service outlets, Fittings, Switchgear, Transformers, Capacitors, Magnetic fields, Transmission lines, Wiring/underground wiring, Other

- Thermal

Boilers, Bunsen burner/hot plates, Electrical equipment, Electrical wiring, Engine exhaust, Furnaces, Heaters, Lasers, Steam lines, Welding surfaces, Welding torch, Other

- Kinetic

Acceleration/deceleration, Bearings, Belts, Carts/dollies, Centrifuges, Crane loads (in motion), Drills, Fans, Firearm discharge, Fork lifts, Gears, Grinders, Motors, Power tools, Presses/shears, Saws, Vehicles, Airplane, Vibration, Other

- Potential (pressure)

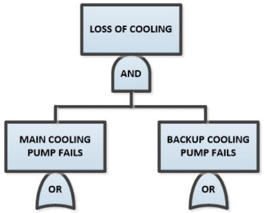
Autoclaves, Boilers, Coiled springs, Furnaces, Gas bottles, Gas receivers, Pressure vessels, Vacuum vessels, Pressurized system (e.g., air), Steam header and lines, Stressed members, Other

- Potential (height/mass)

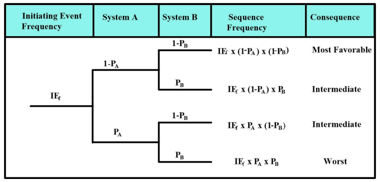
Cranes/hoists, Elevated doors, Elevated work surfaces, Elevators, Lifts, Loading docks, Mezzanines, Floor pits, Scaffolds and ladders, Stacked material, Stairs, Other

- Internal Flooding Sources

Domestic water, Fire suppression piping, Process water, Other



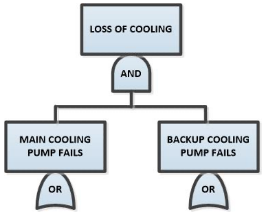
NASA Activities and Identified Hazards



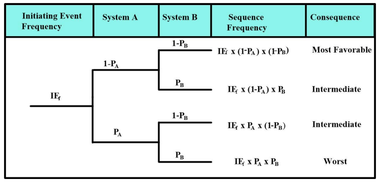
MANNED LAUNCHES
Flight Safety: Hazards to Crew, Passengers, System, Mission, Payload
Range Safety: Hazards to Public and NASA People and Property
- **Debris and Explosive Fragments**
- **Radioactive Fragments and Releases**
- **Blast**
- **Toxic Emissions**
- **Sonic Boom**

UNMANNED LAUNCHES
Flight Safety: Hazards to System, Mission, Payload
Range Safety: Hazards to Public and NASA People and Property
- **Debris and Explosive Fragments**
- **Radioactive Fragments and Releases**
- **Blast**
- **Toxic Emissions**
- **Sonic Boom**

AERONAUTICS (Aircraft, Rockets, Balloons)
Flight Safety: Hazards to Crew, Passengers, System, Mission, Payload
Range Safety: Hazards to Public and NASA People and Property
- **Crash Impact**
- **Fire and Explosion**
- **Sonic Boom**



NASA Activities and Identified Hazards Cont'd



<u>**TRANSPORTATION (All Modes)**</u>

Accidents: Hazards to Public and NASA People and Property

- **Hazardous Materials**
- **Large Objects**

<u>**STORAGE FACILITIES**</u>

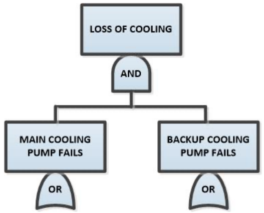
Accidents: Hazards to Public and NASA People and Property

- **Hazardous Materials**
- **Pressures, Vacuums, Temperatures**

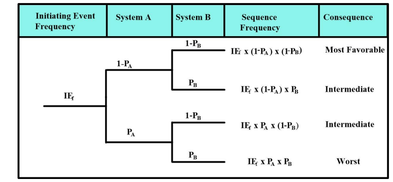
<u>**GR0UND HANDLING OPERATIONS**</u>

Accidents: Hazards to NASA People and Property

- **Hazardous Materials**
- **Pressures, Vacuums, Temperatures**
- **Mechanical Electrical**
- **Noise**



NASA Activities and Identified Hazards Cont’d



<u>WORKPLACE ACTIVITIES</u>

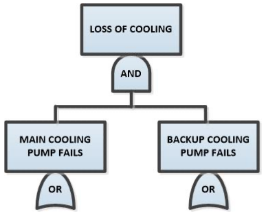
Accidents: Hazards to NASA People and Property

- Fire, Explosion, Electrical, Mechanical, Pressures, Vacuums, Toxics, Cryogens, Suffocates Carcinogens, Mutagens, Noise, Microwave, Laser

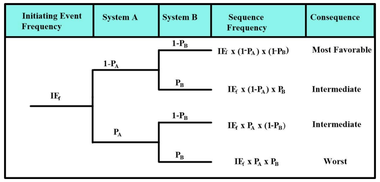
<u>OPERATIONS IN SPACE</u>

Operational Safety: Hazards to Crew, Systems

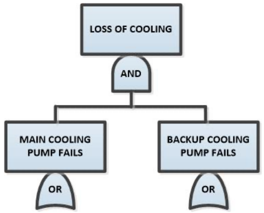
- In-Facilities Hazards
- Extravehicular (EVA) Hazards



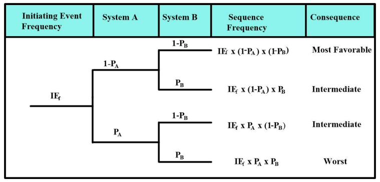
Checklists for Equipment Categories

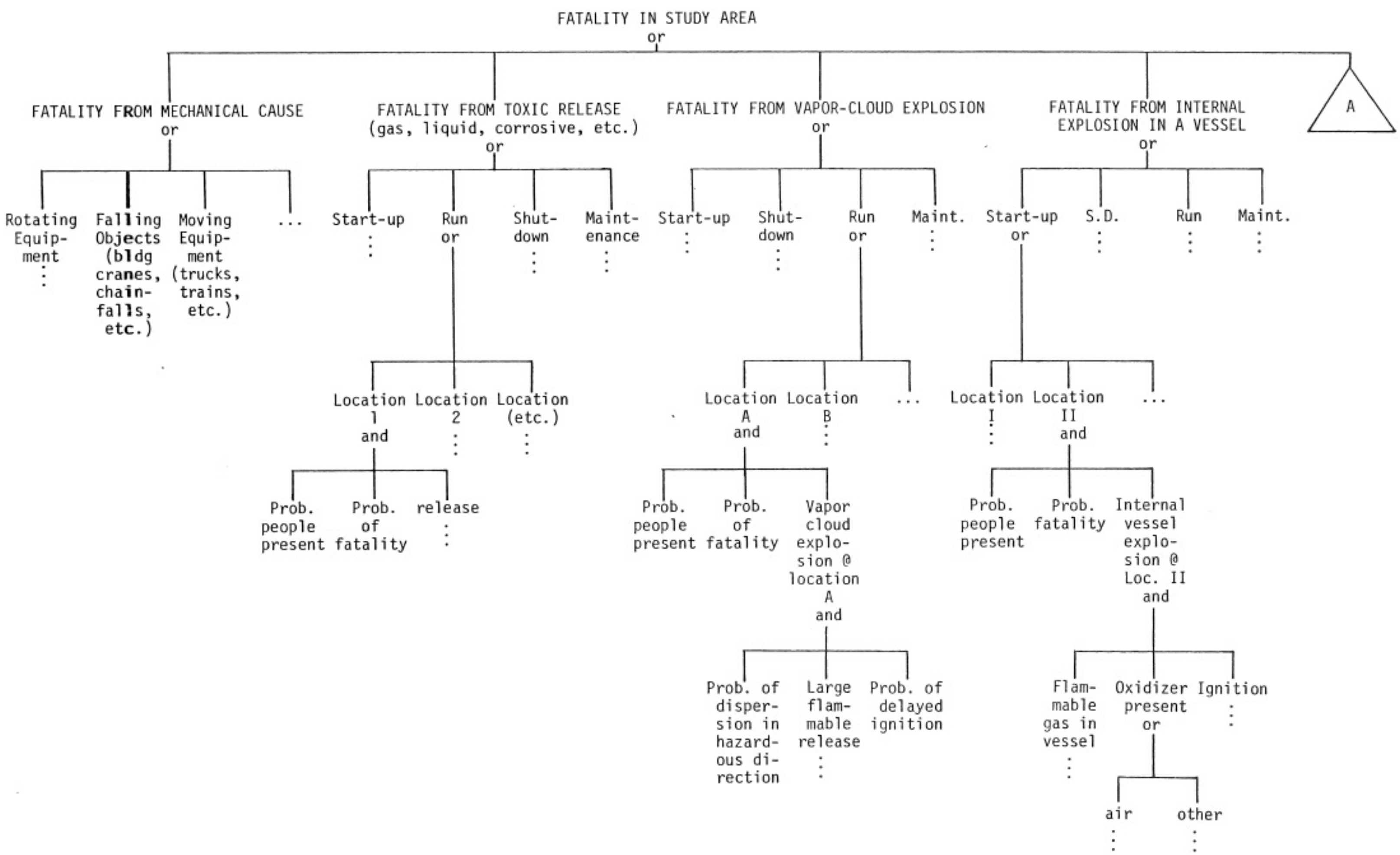


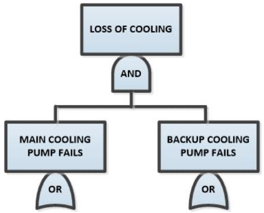
- VARIABLES
  - FLOW, QUANTITY, TEMPERATURE, PRESSURE, pH, SATURATION, ETC.
- SERVICES
  - HEATING, COOLING, ELECTRICITY, WATER, AIR, CONTROL, N2 , ETC.
- SPECIAL STATES
  - MAINTENANCE, STARTUP, SHUT DOWN, CATALYST CHANGE, ETC.
- CHANGES
  - TOO MUCH, TOO LITTLE, NONE, WATER HAMMER, NON MIXING, DEPOSIT, DRIFT, OSCILLATION, PULSE, FIRE, DROP, CRASH, CORROSION, RUPTURE, LEAK, EXPLOSION, WEAR, OPENING BY OPERATOR, OVERRJLL WITH LIQUID
- INSTRUMENT
  - SENSITIVITY, PLACING, RESPONSE TIME



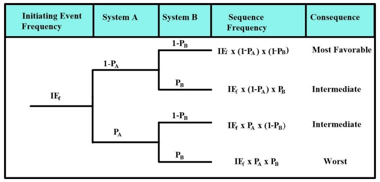
Top Level Fault Tree for Hazards Analysis

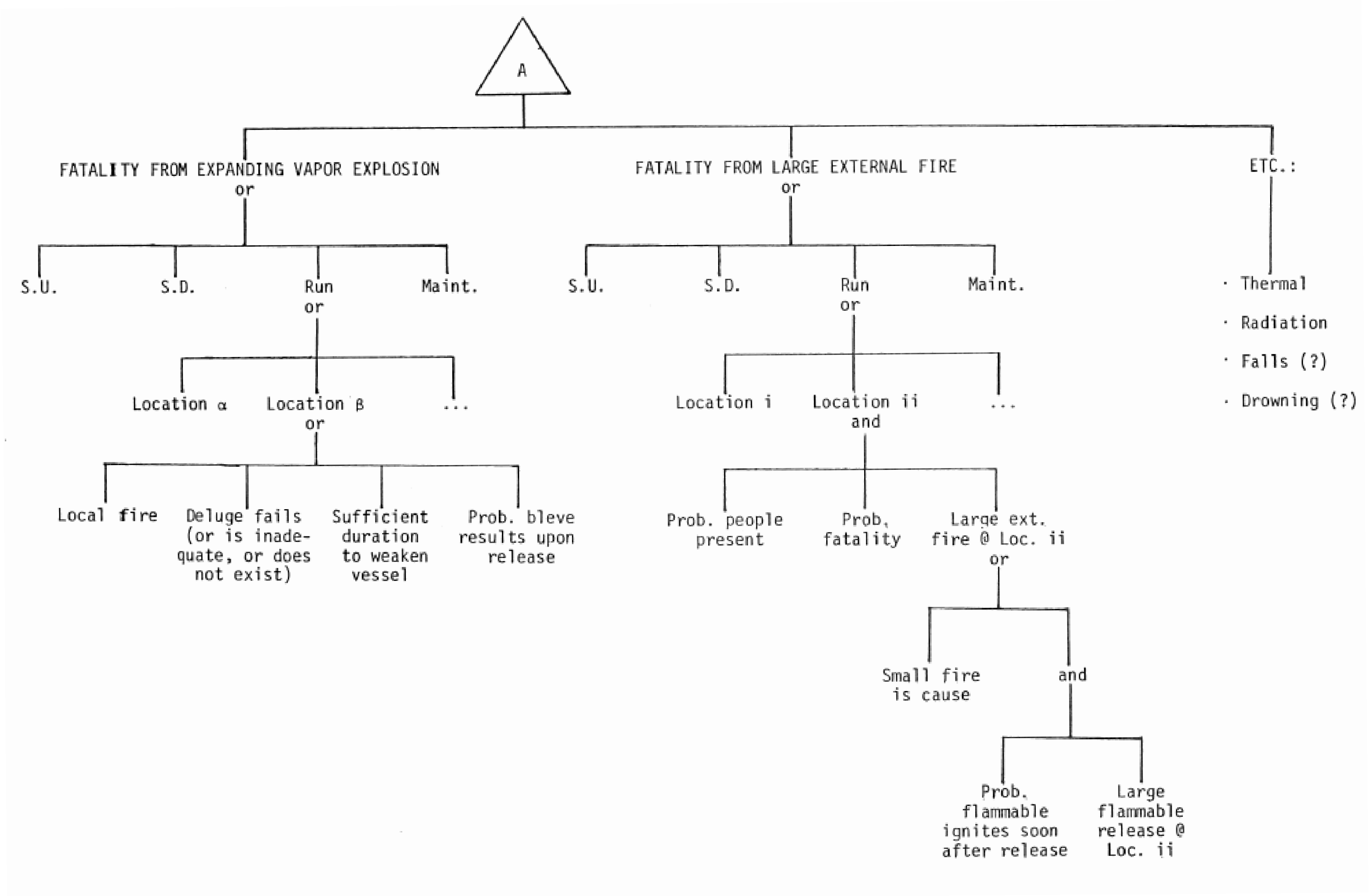


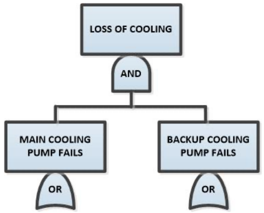




Top Level Fault Tree for Hazards Analysis Cont'd







Example -- What if Analysis – DAP Chemical Reactor

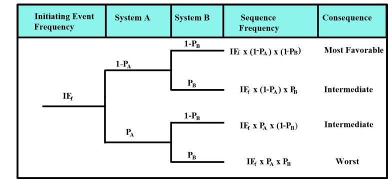


Table 6.9 Sample Page from the What-If Analysis Table for the DAP Process Example

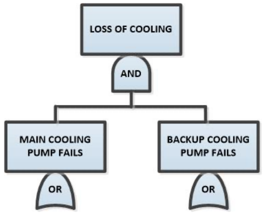
Process: DAP Reactor
Topic Investigated: Toxic Releases

Analysts: Mr. Safety, Ms. Opera, Mr. Design
Date: 05/13/95

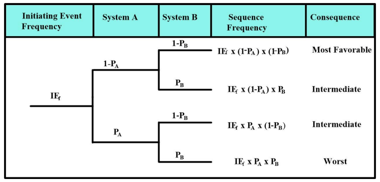
What-If	Consequence/Hazard	Safeguards	Recommendation
the wrong feed material is delivered instead of phosphoric acid?	Potentially hazardous phosphoric acid or ammonia reactions with contaminants, or production of off-specification product	Reliable vendor Plant material handling procedures	Ensure adequate material handling and receiving procedures and labeling exist
the phosphoric acid concentration is too low?	Unreacted ammonia carryover to the DAP storage tank and release to the work area	Reliable vendor Ammonia detector and alarm	Verify phosphoric acid concentration before filling storage tank
the phosphoric acid is contaminated?	Potentially hazardous phosphoric acid or ammonia reactions with contaminants, or production of off-specification product	Reliable vendor Plant material handling procedures	Ensure adequate material handling and receiving procedures and labeling exist
valve B is closed or plugged?	Unreacted ammonia carryover to the DAP storage tank and release to the work area	Periodic maintenance Ammonia detector and alarm Flow indicator in phosphoric acid line	Alarm/shutoff of ammonia (valve A) on low flow through valve B
too high a proportion of ammonia is supplied to the reactor?	Unreacted ammonia carryover to the DAP storage tank and release to the work area	Flow indicator in ammonia solution line Ammonia detector and alarm	Alarm/shutoff of ammonia (valve A) on high flow through valve A

DAP = Diammonium Phosphate

Ref: Guidelines for Hazards Evaluation Procedure Second Edition -- AICHE



Example – Preliminary Hazards Analysis (PHA) – Offshore Oil Platform



									Preventative Measures		
Sub-System or Function	**Item No.**	**Hazardous Element**	**Event Causing Hazard**	**Hazardous Condition**	**Event Causing Accident Potential**	**Potential Accident**	**Effect**	**Hazard Class**	**Hard-ware**	**Proce-dures**	**Person-nel**
Gas metering	M12	Gas pressure	Leak Rupture Equip. damage Inst. failure	Gas released to module	Spark Flame Static electricity	Fire Explosion	Personnel injury Equip. damage	I or II			

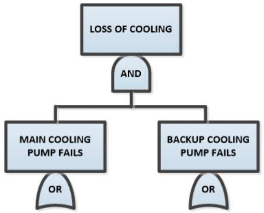
Class I hazards - Catastrophic effects - likely to cause one or more deaths or total plant loss.

Class II hazards - Critical effects - likely to cause severe injury, major property or system damage and total loss of output.

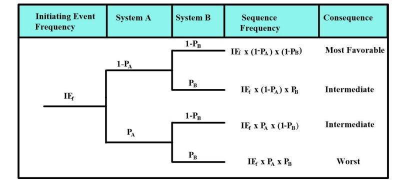
Class III hazards - Marginal effects - likely to cause minor injury, property or system damage with some loss of availability.

Class IV hazards - Negligible effects - unlikely to cause injury, property or system damage.

Ref: Reliability and Risk Assessment, J.D. Andrews and T. R. Moss, Longman Scientific Technical, 1993.

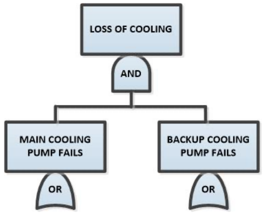


Example – Hazards and Operability Study (HAZOP) – Site 300 – Contained Firing Facility

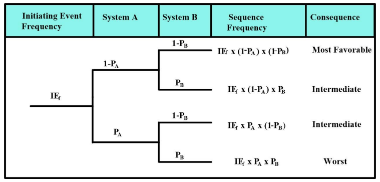


Hazard	Deviation **(Guide words)**	Possible Causes	Methods of Detecting Event	Preventative Features	Possible Consequences	Mitigative Features	Comments
Mobile-lift or forklift. Batteries, hydraulic fluid.	Fire on nearby vehicle creates sufficient heat to detonate HE when personnel are present.	Hydraulic fluid leak with ignition source. Hydrogen leak with ignition source.	Observed by personnel. Heat detector alarms. Sprinkler activation.	Inspection of vehicle hydraulic and electrical systems before first use on a given day. Periodic inspection of vehicle batteries. Approved HE handling equipment. Control of ignition sources. Separation distance between combustible materials and HE.	HE detonation. Personnel death or injury.	Facility emergency response procedures. Operational access controls limit number of exposed personnel. Separated emergency exits in firing chamber. HE limits. Remote location of site. Confinement system.	

Ref. Gary Johnson and Howard Lambert, "Identification of Process Hazards and Accident Scenarios for Site 300, Lawrence Livermore National Laboratory," UCRL-ID-150822, May 4, 2001



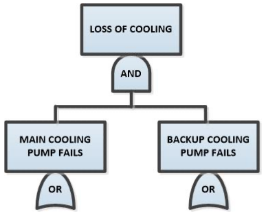
Example – Failure Modes and Effects Analysis (FMEA) -- lubrication system



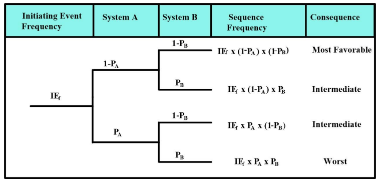
System Reference Description Function	Failure Entry Code	Failure Mode	Possible Causes	System Detected by	Local	On next level	Compensating Provision against Failure	Severity Class	Remarks
Lubrication System	1401	Leakage	Loose connectors. Auxiliary oil pump fault.	Observation - gas in air monitors. Fall of sump level.	Slow leaks have no effect.	Eventual shutdown if uncorrected by loss of oil pressure. Performance loss if air ingress.	2-hourly inspections. Automatic shutdown on low oil pressure.	3	Sump contains 30 liters. A 25% loss should be readily observed, corrected w/o loss of performance.

<u>**Severity Index**</u>	<u>**Consequence**</u>
1 Catastrophic	Complete loss of system.
2 Critical	Severe reduction of functional performance resulting in a change in operational state.
3 Major	Degradation of item functional output.
4 Minor	No effect on performance.

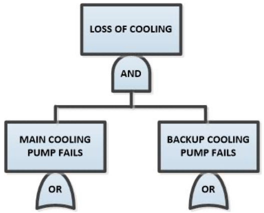
Ref: Reliability and Risk Assessment, J.D. Andrews and T. R. Moss, Longman Scientific Technical, 1993



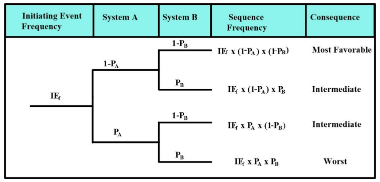
Typical modeled faults Nuclear Power Plants (NPPs)



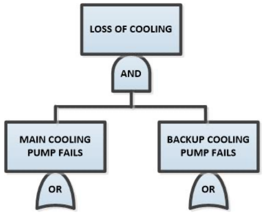
- Failure to Start
- Failure to operate for mission time
- Failure to Open/Close
- Failure to Remain Open/Closed
- Unavailable Due to Test or Maintenance
- Failure to Energize
- Common Cause Failures shared by two or more components or trains
- Human Error
  - Pre-initiator errors rendering the system unavailable at the time of demand
  - Human errors defeating system function during the mission



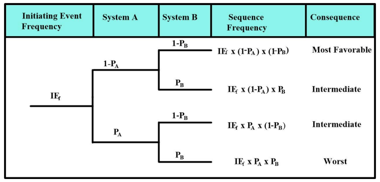
Human Failure Modes (Partial List)



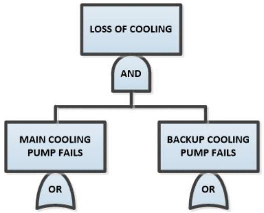
- Failure to perform all or part of the task
- Performance of the task or step incorrectly
- Introduction of some task/step which should not be performed
- Performance of some task/step out of sequence
- Failure to perform the task/step within the allotted time period



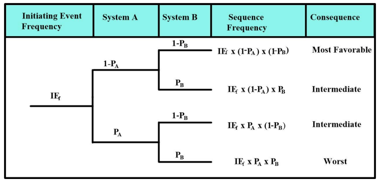
Common Cause Failure Analysis (example cold weather)



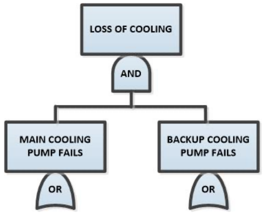
- Car fails to start in cold weather
- Diesel generators fail to start at a nuclear power plant
- Ice storm at nuclear power plant leads to station blackout
  - Loss of offsite power
  - Diesel generators fail to start
- Nuclear Power Plant in Slovenia service water screens freeze
- O-ring failure -- Challenger Space shuttle



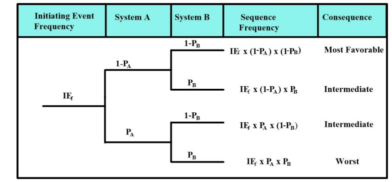
Examples Common Cause Failures



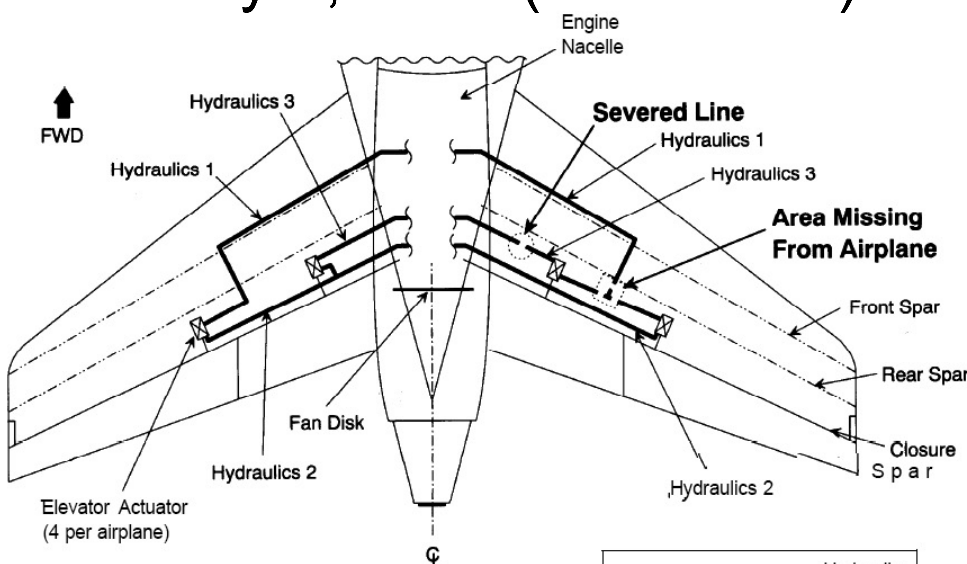
- Three Mile Island Accident (2CCFs) April 1979
  - Redundant AFWS pumps valved out
  - Operator switched off redundant SI pumps
- Salem Unit 1 Feb 1983
  - Both RPS breakers failed to open automatically following valid trip signal on low-low steam generator level
- Gemini Ground Test Fire
- Apollo 13 fuel cell explosion
- Failed Iranian Hostage Mission
- L-1011 flight when all three engines failed
- B-747 engine shutdown from volcanic plume
- Space Shuttle Challenger Accident
- Chernobyl accident
- US Airways Flight 1549
- Lesson: Real accidents seldom if ever result from several independent failures, almost always result from dependent failures



Common Cause Failure Analysis



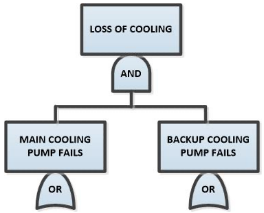
- Space Shuttle – Shields (Hydraulic Systems)
- UA 232 – July 19, 1989 Sioux City Iowa (Fan Casing Ruptures -- damages all three Hydraulic System)
- US Air 1549 – February 2, 2009 (Bird Strike)



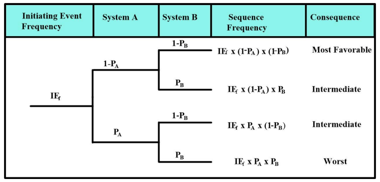
Actuator Position	Hydraulic System
RH Inbd Elev	1 & 3
LH Inbd Elev	2 & 3
RH Outbd Elev	1 & 2
LH Outbd Elev	1 & 2

Not to Scale

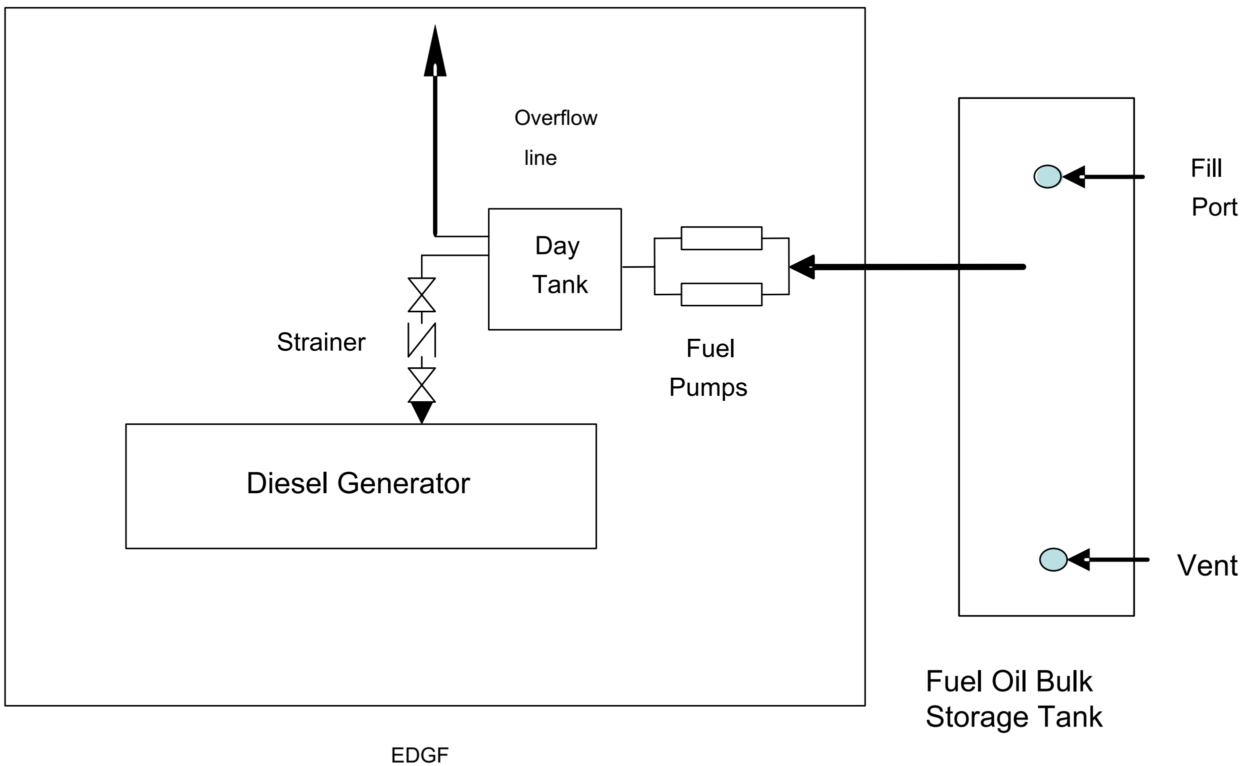
48



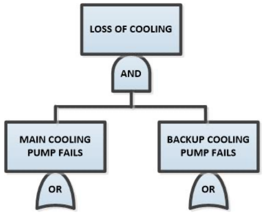
Common Cause Failure Analysis -- Human Error



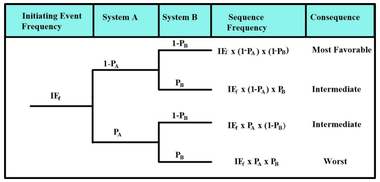
- Georgia Power -- addition of STP to day tanks



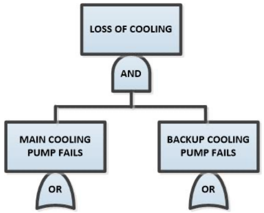
Diesel Generator Fuel Oil System



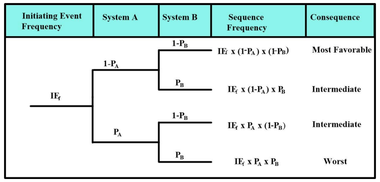
Probabilistic Risk Assessment



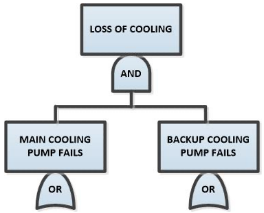
1. Identification of the undesired events/accident scenarios
2. System understanding
3. Logic Model Generation
4. Assumptions and Initial Conditions
5. Qualitative Evaluation of the Logic Model
6. Probabilistic (Quantitative) Evaluation of the Logic Model
7. Sensitivity and Importance Analysis
8. Consequence Analysis
9. Uncertainty Analysis
10. Peer Review



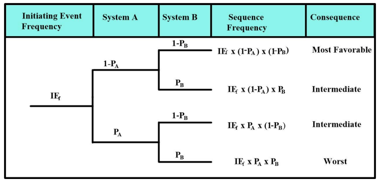
Fields of Expertise for the PCSA (Preclosure safety analysis, Yucca Mountain)



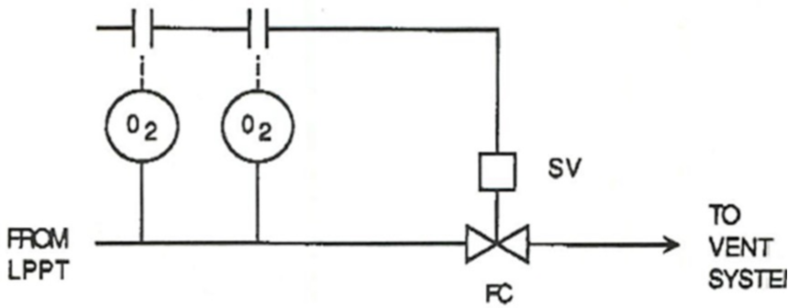
- Structural engineering
- Heat transfer
- Electrical and electronic engineering
- Mechanical engineering
- Fire and explosion analysis
- Dynamics of impact
- Mathematics
- Reliability theory
- Reliability data
- Bayesian statistics
- Seismology
- Seismic equipment and structural analysis
- Atmospheric reentry of meteorites and space debris
- Hazardous material release and transport
- Criticality
- Human factors and human reliability
- Nuclear operations
- Nuclear regulations
- Equipment operation, failure modes and failure causes
- Probabilistic risk assessment
- Hydrology
- Meteorology
- Lightning effects
- Aircraft
- Nuclear materials and source term
- Radiation transport and dose consequences



Type of example addressed in presentation

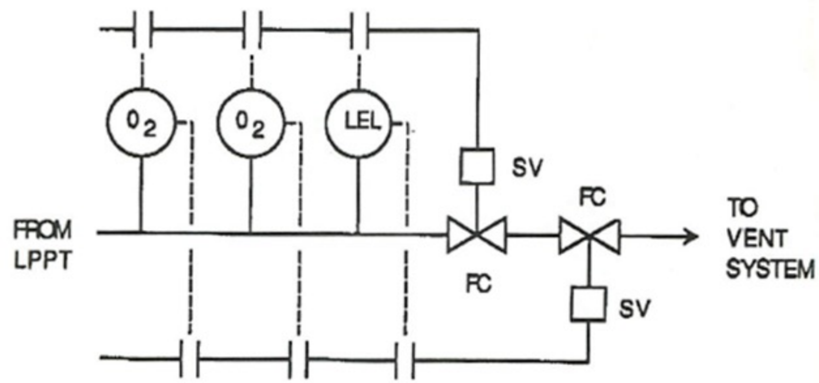


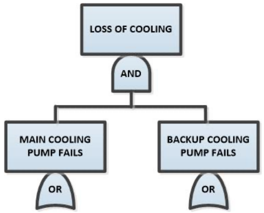
CURRENT BASIS: High O2 reading by either analyser will open circuit to SV, allowing SV to close.



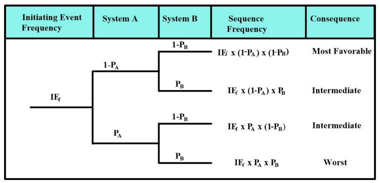
DESIGN B

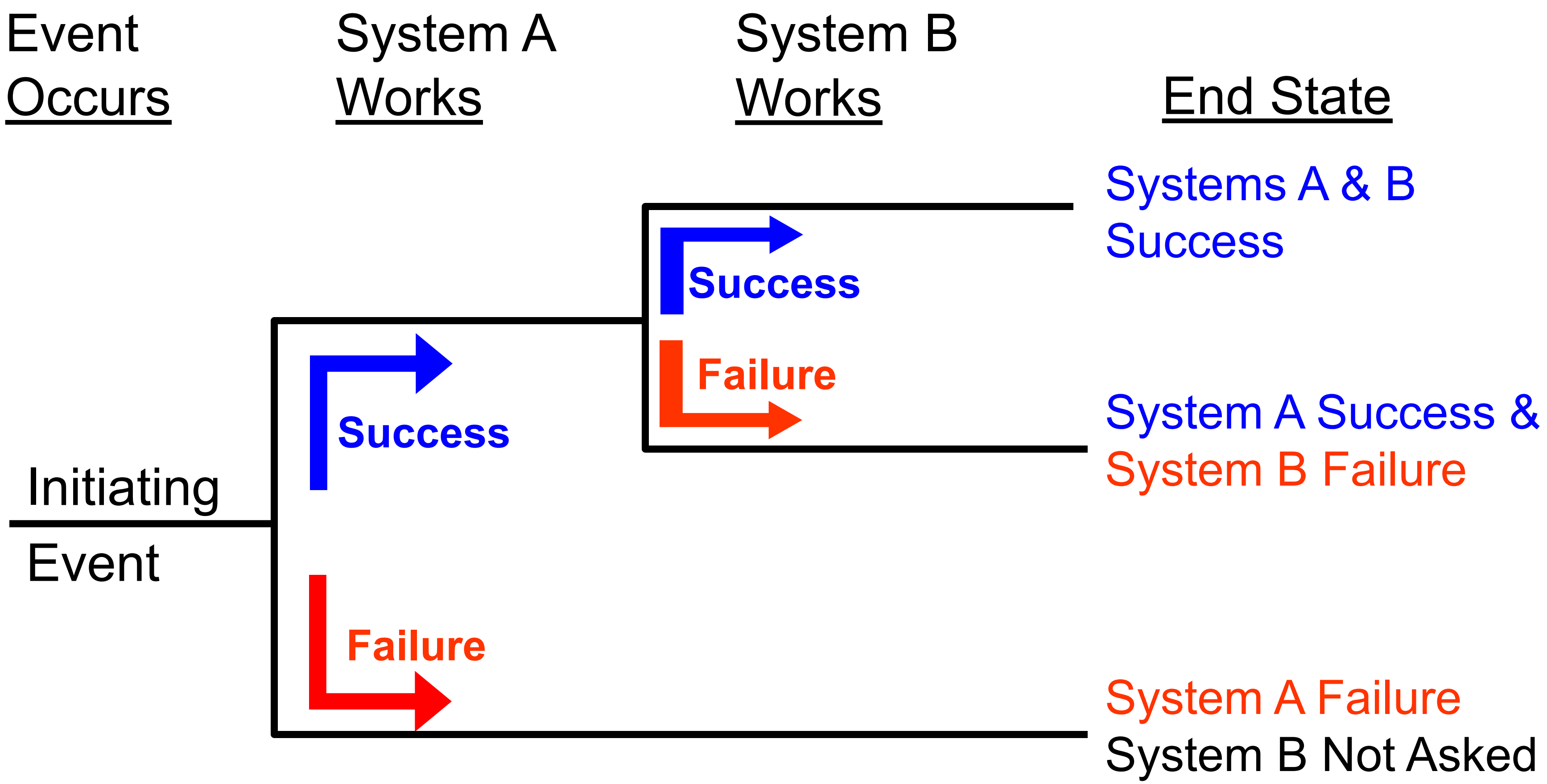
PROPOSED CHANGE: Add an LEL and a series block valve to improve improve reliablity of isolating LPPT from vent system.

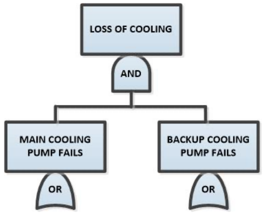




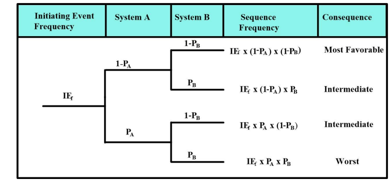
Event Tree Construction

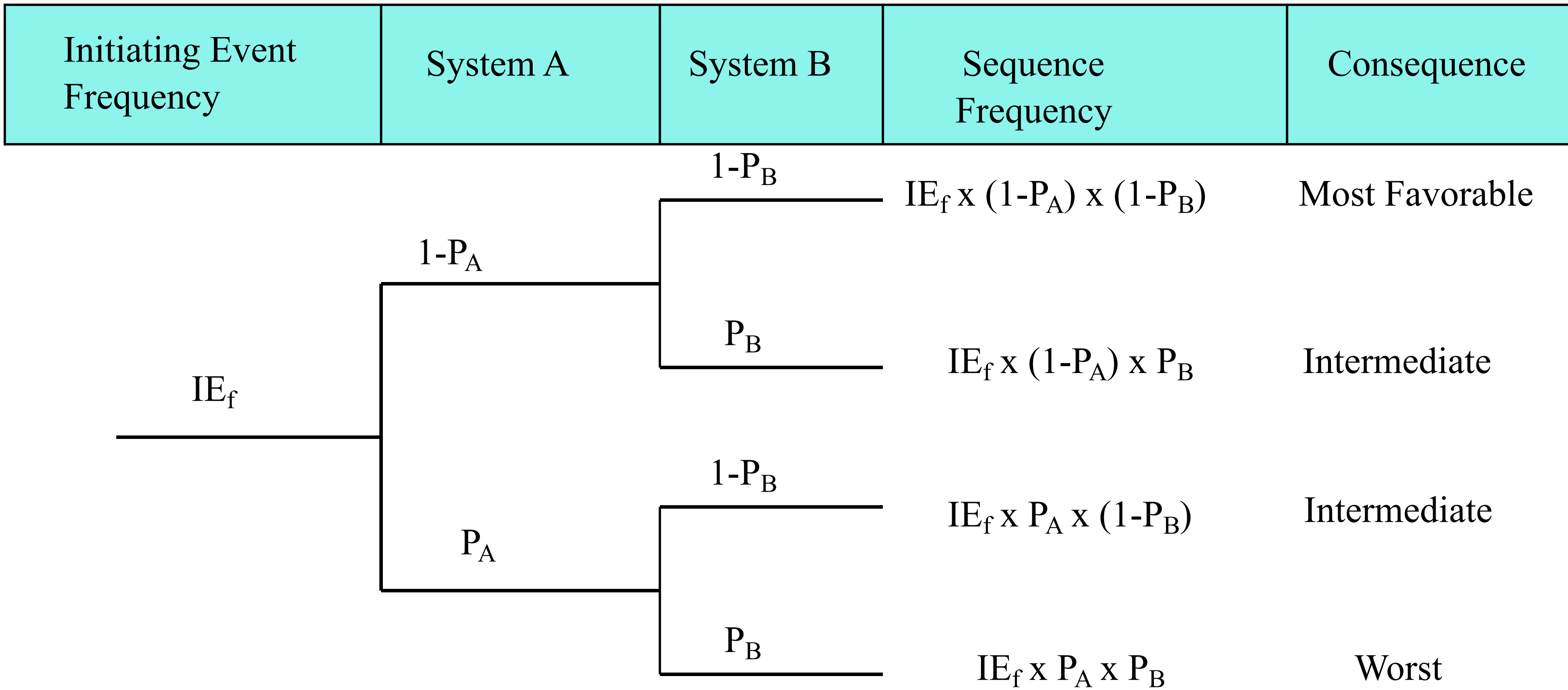


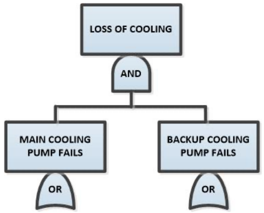




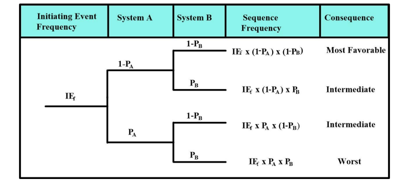
Generic Event Tree

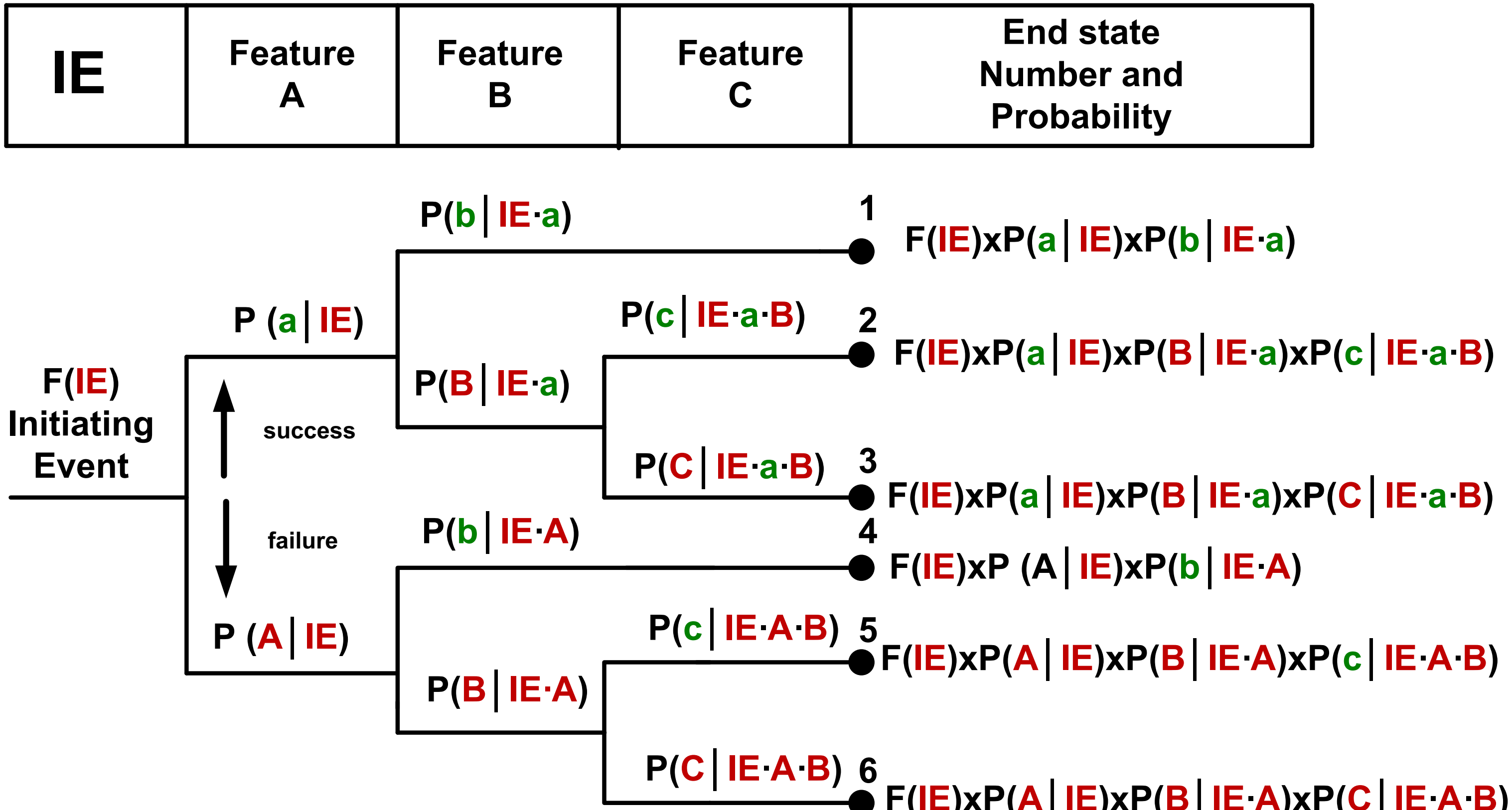






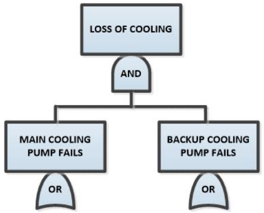
Event Tree Conditional Probabilities



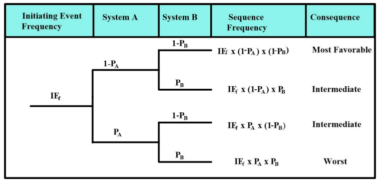


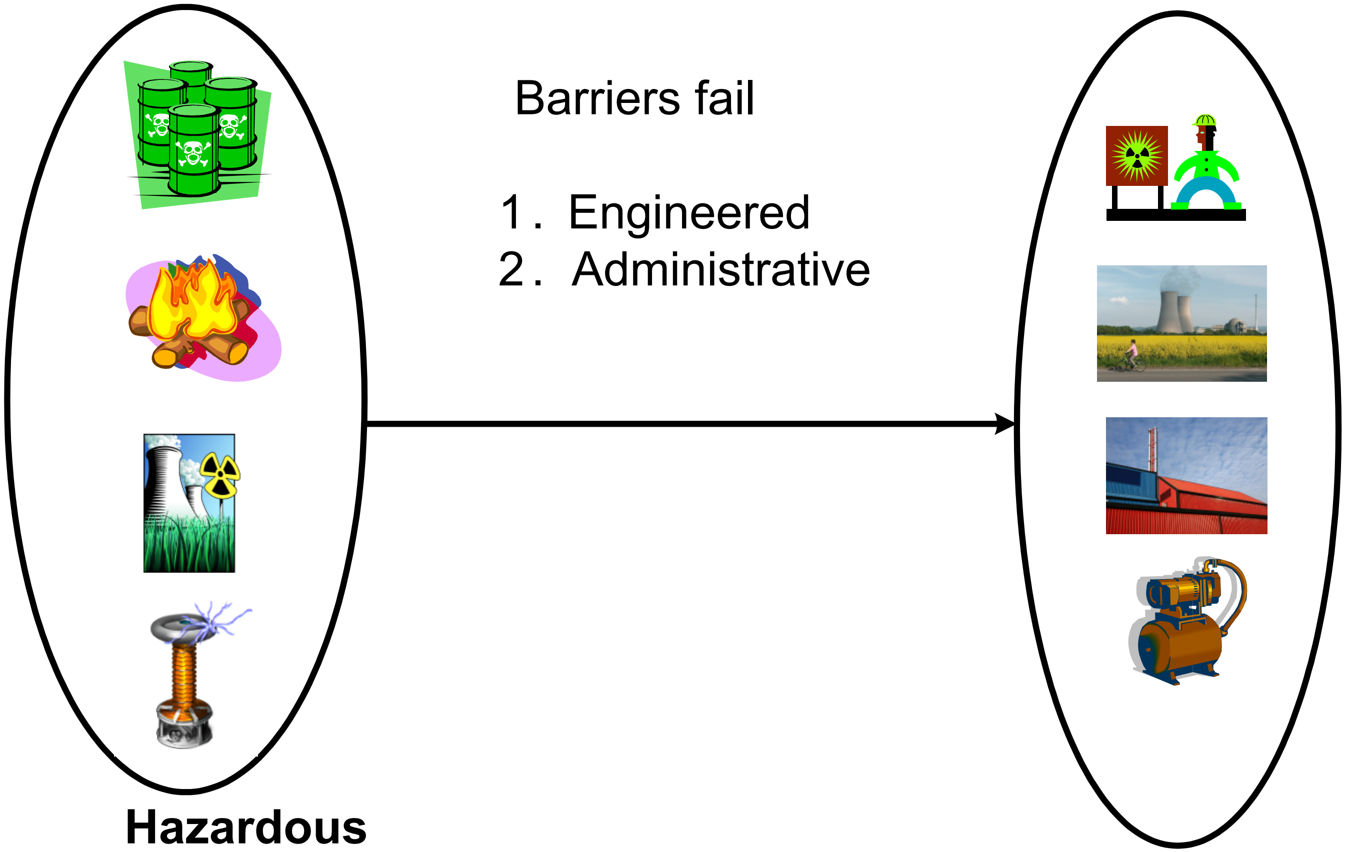
LEGEND
F is frequency (expected rate)
P is probability
| conditional probability
x multiplication

· Means logical intersection AND
Lower case feature success
Upper case feature failure



Barrier Analysis



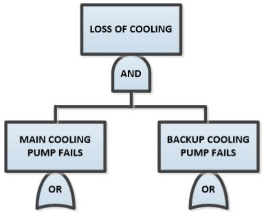


Barriers fail

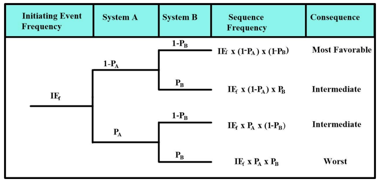
1. Engineered
2. Administrative

Hazardous Material Energy Sources Operations

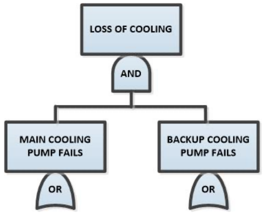
Target



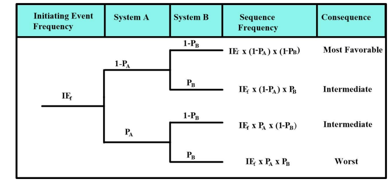
Physical Barriers (Controls)



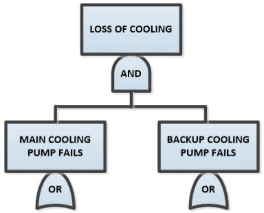
- Engineered safety features
- Safety and relief devices
- Conservative design allowances
- Redundant equipment
- Locked doors and valves
- Ground fault protection devices
- Radiation shielding
- Alarms and annunciators
- Fire barriers and seals
- Containment building
- Blowout walls



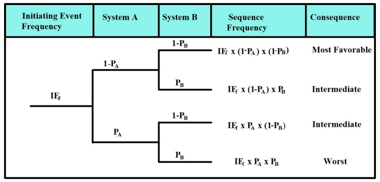
Administrative Barriers (Controls)



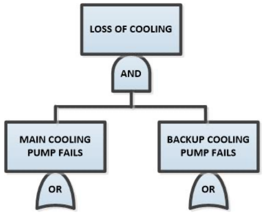
- Operating and maintenance procedures
- Policies and practices
- Training and education
- Maintenance work requests
- Radiation work permits
- Licensing of operators
- Qualifications



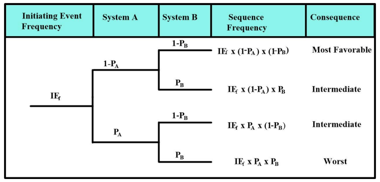
System Representation & Requirements

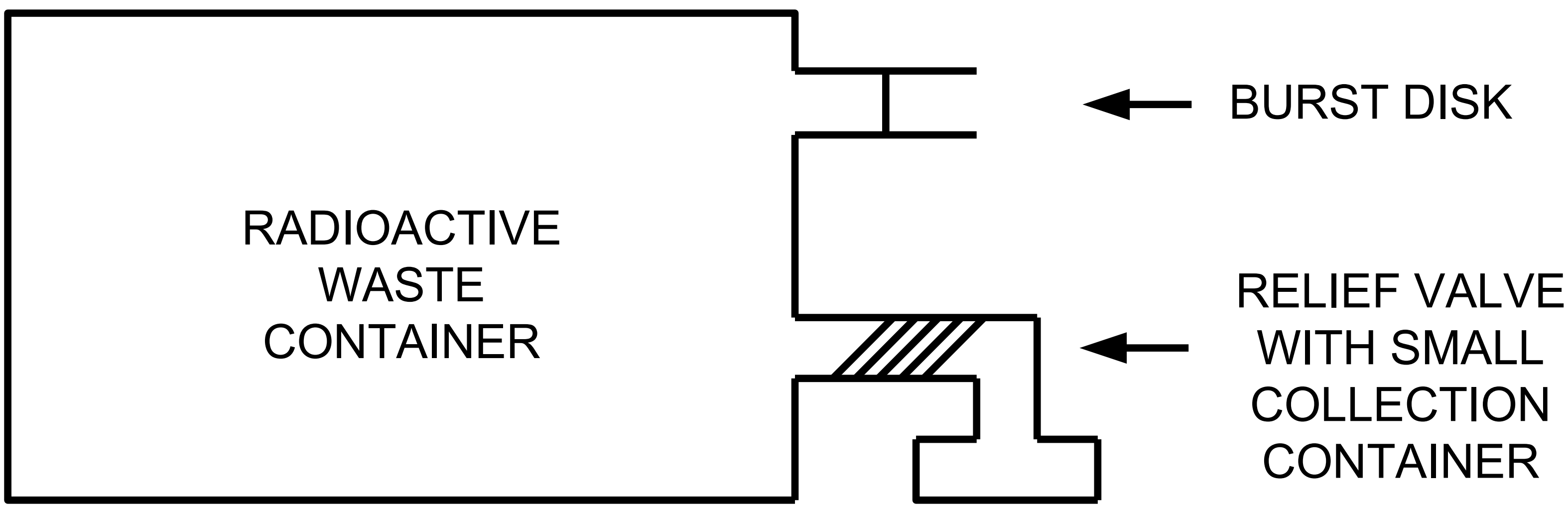


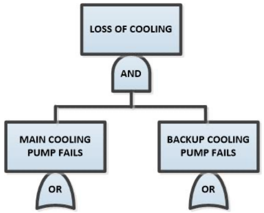
- Principles of operation
- Operating cycles
- Block diagrams
- Systems interaction diagrams
- Piping and instrumentation diagrams
- Interaction diagrams
- Time lines
- Process Control
- Hardwired interlocks
- Softwired interlocks
- Diversity /defense in depth
- Independence
- Operability requirements
- Success criteria
- Reliability, safety and security
- System redundancy (NPP versus space systems)



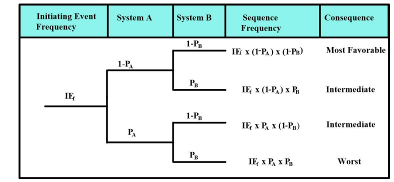
EVENT TREE EXAMPLE





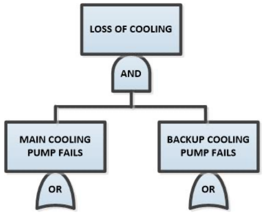


SYSTEM DESCRIPTION

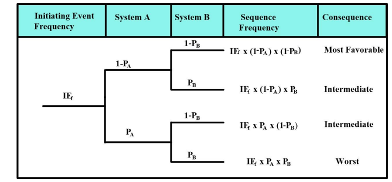


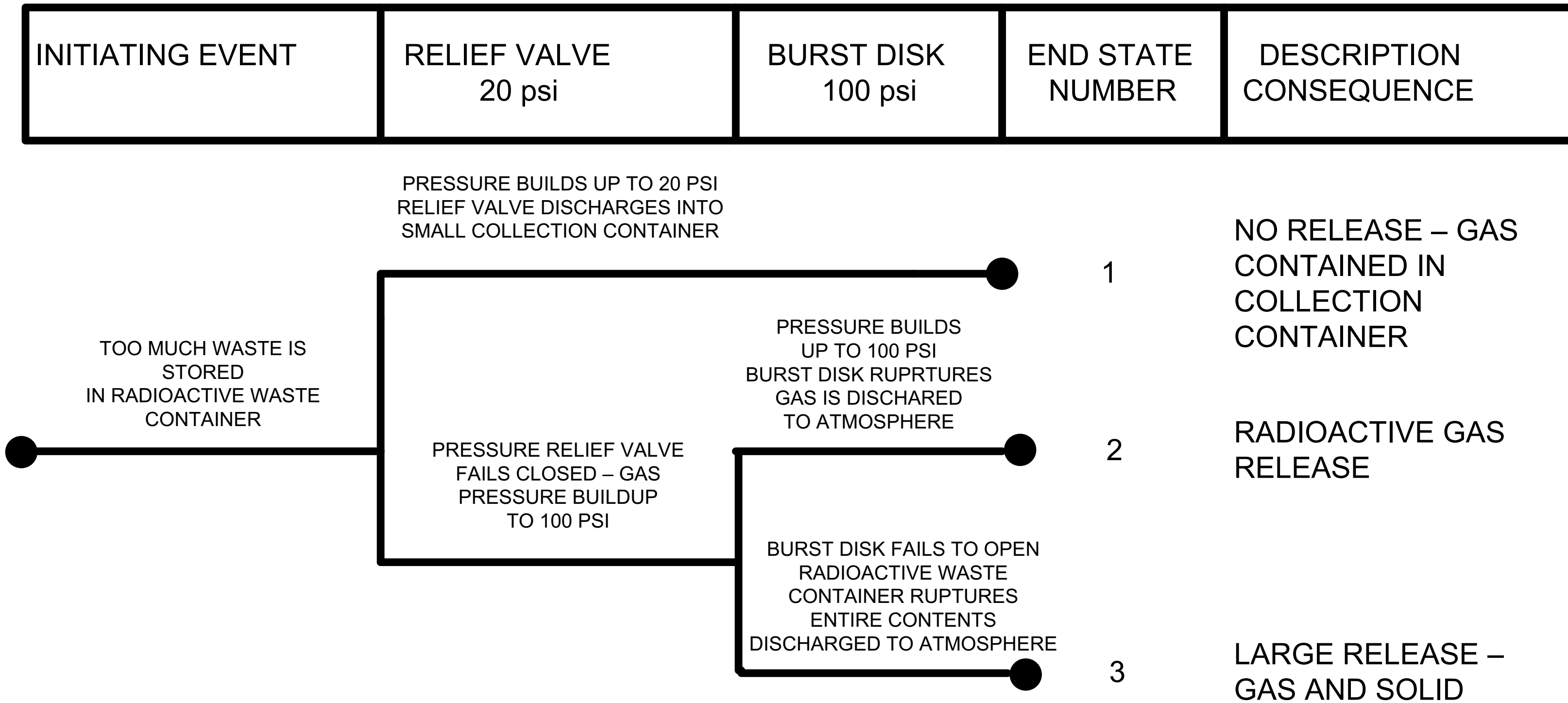
- If too much radioactive waste is stored in the container, there will be a slow buildup of gas pressure.
- The first line of defense if excess pressure builds up is the pressure relief valve that will relieve at 20 psi and the radioactive gas will be contained in the small collection container
- If pressure relief valve fails to open, then the second of defense is that the burst disk will open at 100 psi and the gas will be released to the atmosphere
- If both the pressure relief valve fails and the burst disk fails, then eventually the container will rupture and the largest release of radioactivity will occur

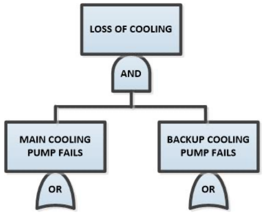
61



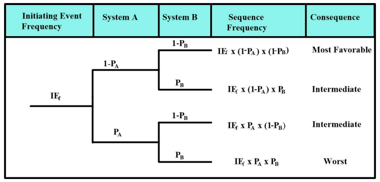
Event tree for radioactive release



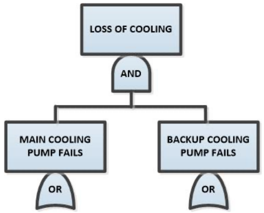




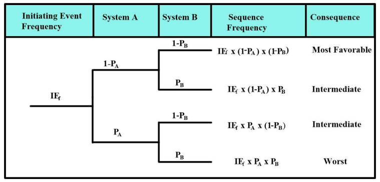
Room/Facility Fire Event Tree



- Facility Layout -- Room with 1 hour fire wall
- Engineered Controls
  - Wet pipe sprinkler system
- Administrative Controls
  - Transient combustibles
  - Fire extinguisher
  - Fire Department
- Undesired Event States
  - Room Fire
  - Full Facility Fire



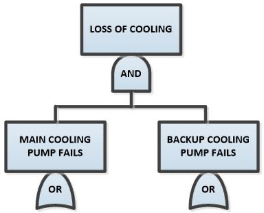
Fire risk methodology includes three basic tasks



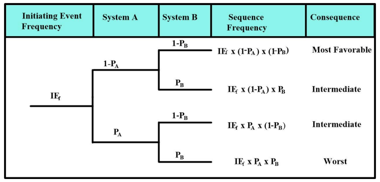
- These include

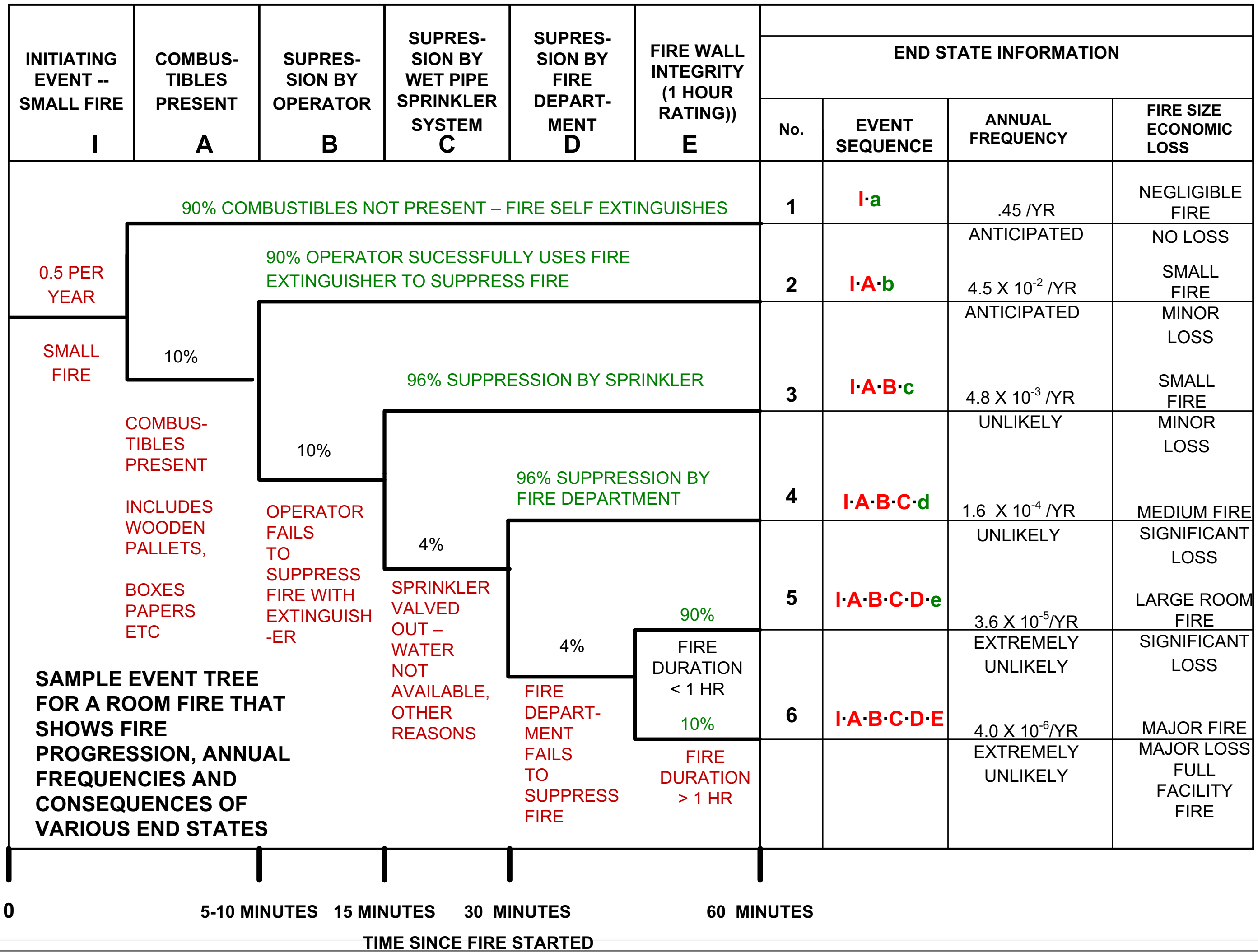
  1. Identify “critical locations and assess the frequency of fires
  2. Estimate fire growth times and compute detection and suppression times
  3. Determine system/plant response

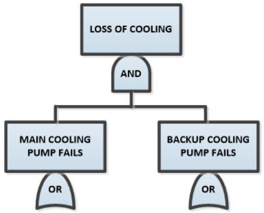
- An event tree that depicts fire ignition and growth is shown in the next slide



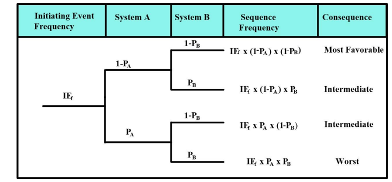
SAMPLE EVENT TREE – ROOM FIRE





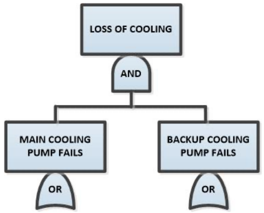


FAULT TREE ANALYSIS

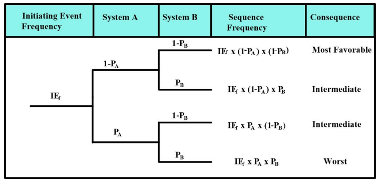


- Define the Top Event
- Types of events in fault tree analysis
- Deductive logic model -- top down approach
- Uses standard OR and AND gates (other) to describe events that have a more basic cause
- Types of AND gates – active versus standby redundancy
- Root causes are basic events represented by
  - Circles
  - Diamonds
- Initiating and Enabling Events
- Min cut sets (System Failure Modes)
- Min path sets (Tie sets, success logic)

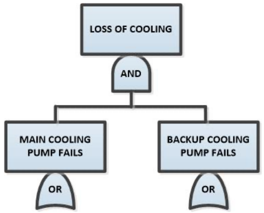
www.ftaassociates.com



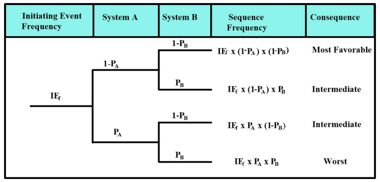
Introduction



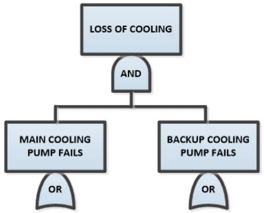
- Types of events in fault tree analysis
  - Normal Events – those that are expected to occur
  - Type 1 – intended function is not achieved
  - Type 2 – unintended function is achieved
- Basic events
  - Initiating events
  - Enabling events
- Human error
  - Latent
  - Dynamic
  - Initiator
  - Error of Omission
  - Error Commission



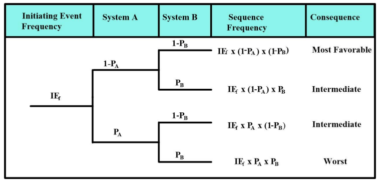
Normal Events



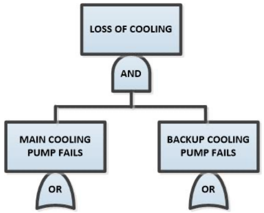
- Describe intrinsic hazards -- expected to occur with no failures examples below
  - Rich Gasoline Mixture during vehicle startup
  - Car has heated surfaces when operated
  - Hot water tank emits flue gases that contain carbon monoxide
  - House power initially available when gas leak occurs



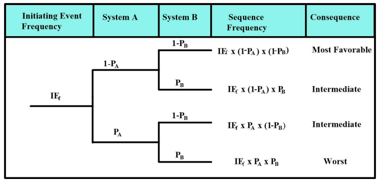
Type 1 events (examples)



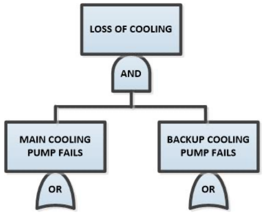
- Type 1 fault events (intended function not achieved)
  - Missile Fails to Launch upon demand
  - Sprinkler system fails to activate in a fire
  - Air bag fail to deploy in an auto accident
  - Fissile material handlers fail to clean out glove box (human error of omission)
  - Alarm Inactive
  - Car Fails to Start



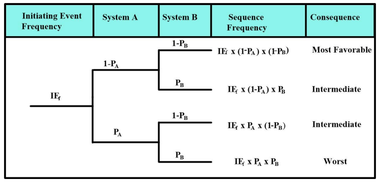
Type 2 Fault Events (examples)



- Type 2 fault events (inadvertent, unwanted function achieved)
  - Inadvertent Launch of a missile
  - Missile blows up on the launch pad
  - Inadvertent sprinkler activation
  - Inadvertent air bag deployment
  - Fissile material handlers move special nuclear material to the wrong glovebox (human error of commission)
  - False Alarm
  - Car Starts in gear



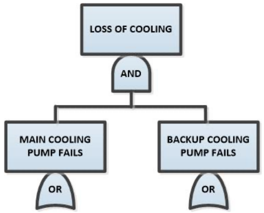
Wet pipe sprinkler system



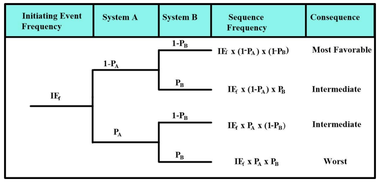
- SPRINKLER HEAD IN WET PIPE SPRINKLER SYSTEM – FUSES OPEN AT 80°F

1. What is the type 1 fault event for the sprinkler head and corresponding undesired event for the system?

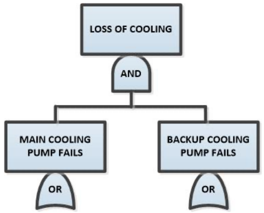
2. What is the type 2 fault event for the sprinkler head and corresponding undesired event for the system?



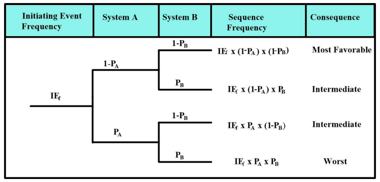
Fault tree construction



- Traditional fault tree construction – evolved from aerospace industry in the 60’s
  - Use immediate cause principle
  - Operator for type 1 fault events
  - Operator for type 2 fault events
- Fault tree analysis of control systems – use of directed graphs
  - Much more complicated to understand
  - Handle control systems with logic loops
    - Feedback
    - Feedforward
    - combination



Light bulb example

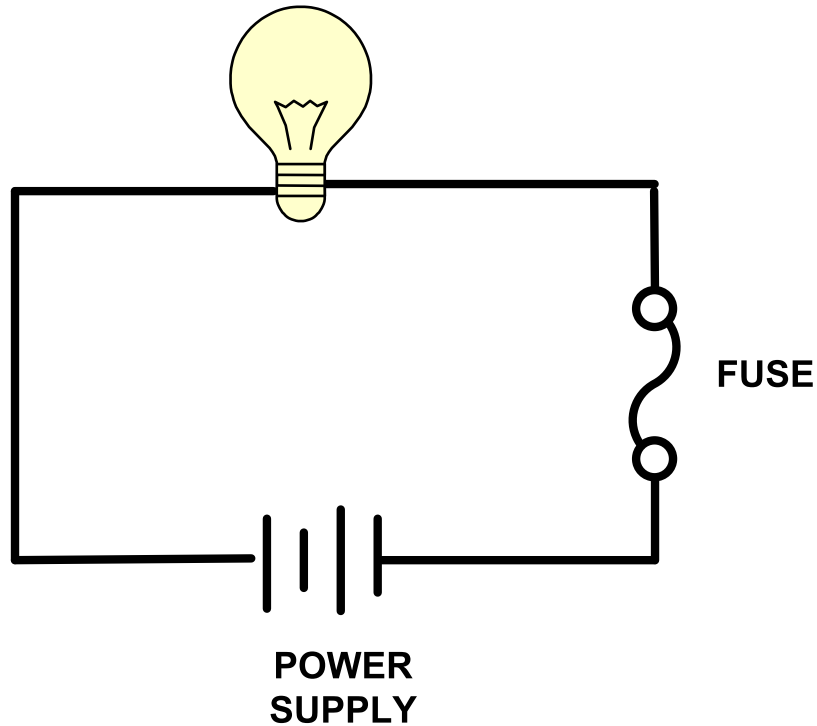


- Simple system that illustrates important concepts in fault tree analysis
  - Series system
  - Redundancy
  - Series parallel system
  - Structuring fault trees
  - Min cut sets (system failure modes)
  - Different top events when considering reliability and safety
  - Consequence analysis
  - Tradeoff analysis

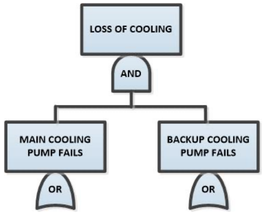
FAULT TREE –LIGHT BULB EXAMPLE

Two top events

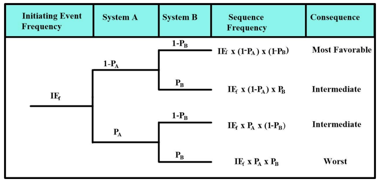
1. No light (reliability)
2. Wire catches fire (safety)



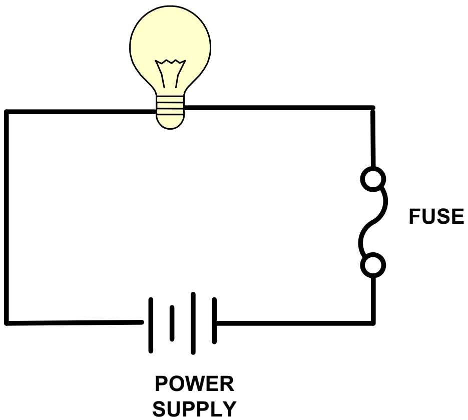
SYSTEM A – SIMPLE SYSTEM



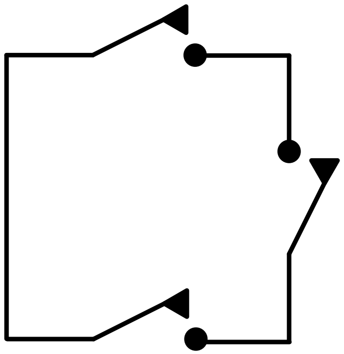
Min Cut Set Analysis



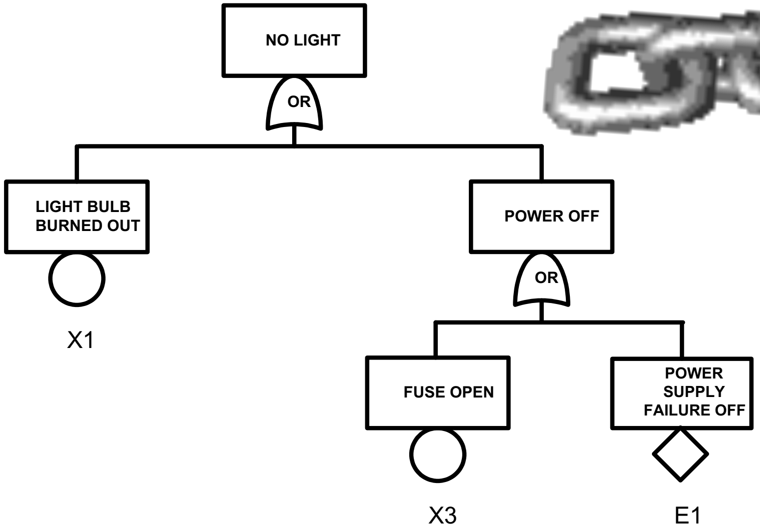
- Reliability fault tree for system A, no light
  - Simple series system
  - Fault tree is all OR gates
  - 3 single point failures
  - 3 min cut sets of order 1
- 3 Min Cut Sets
  1. Light bulb burned out
  2. Fuse open
  3. Power supply failure off

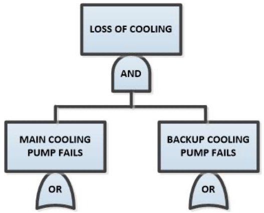


SYSTEM A – SIMPLE SYSTEM

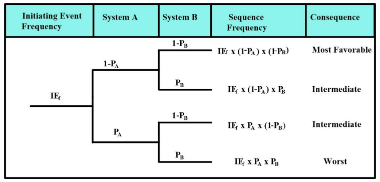


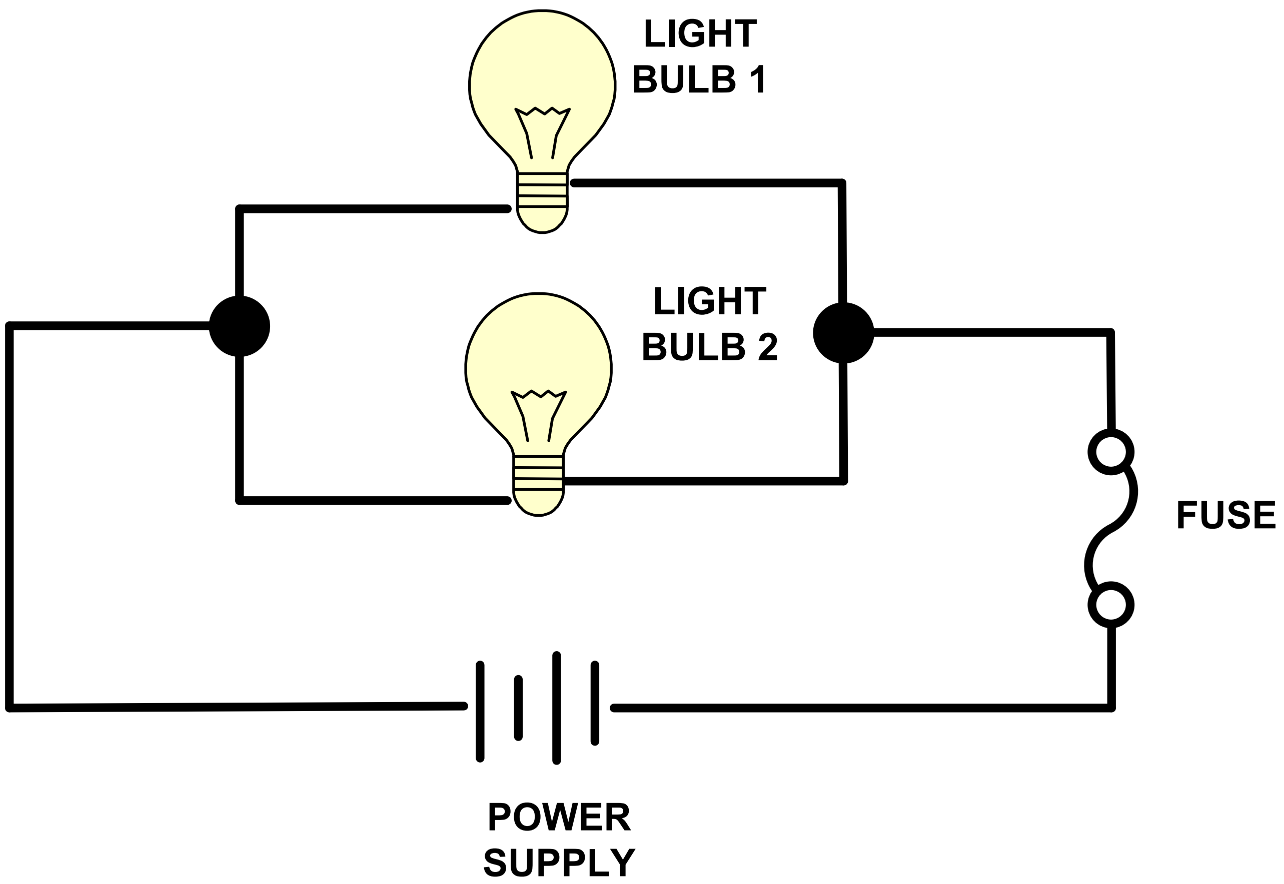
SWITCH ANALOGY

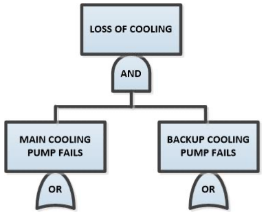




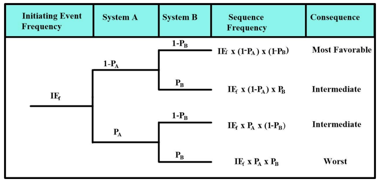
Fault tree –
System B two light bulbs with fuse

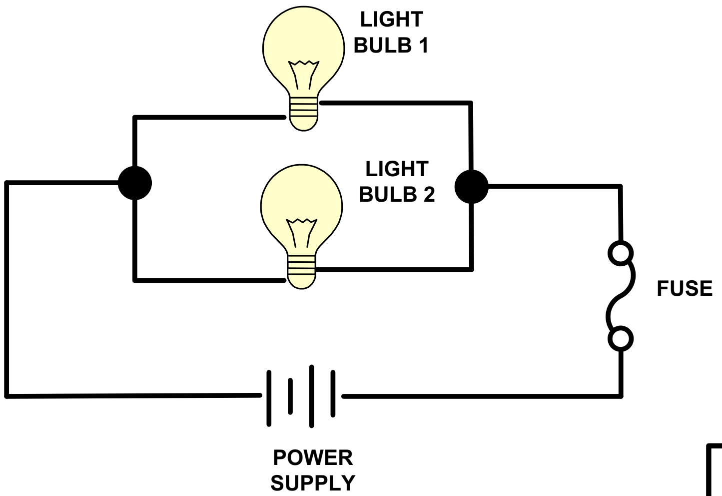


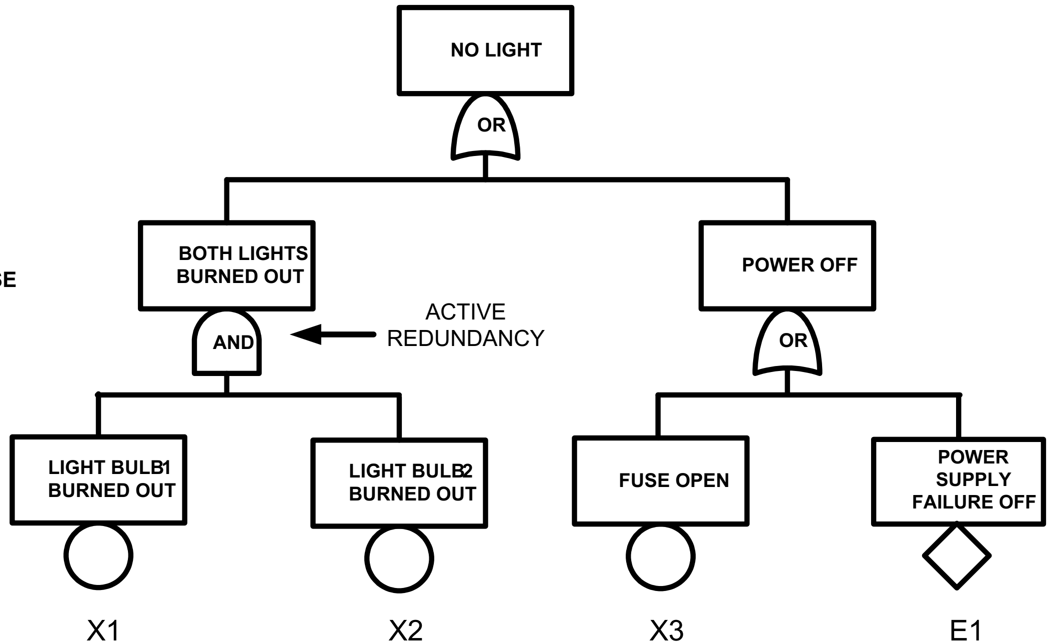




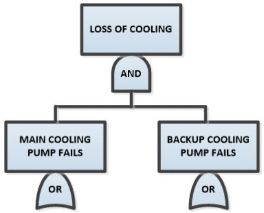
Fault tree – System B



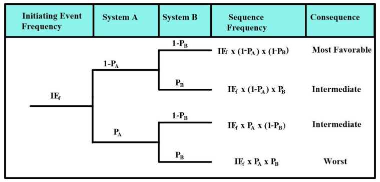


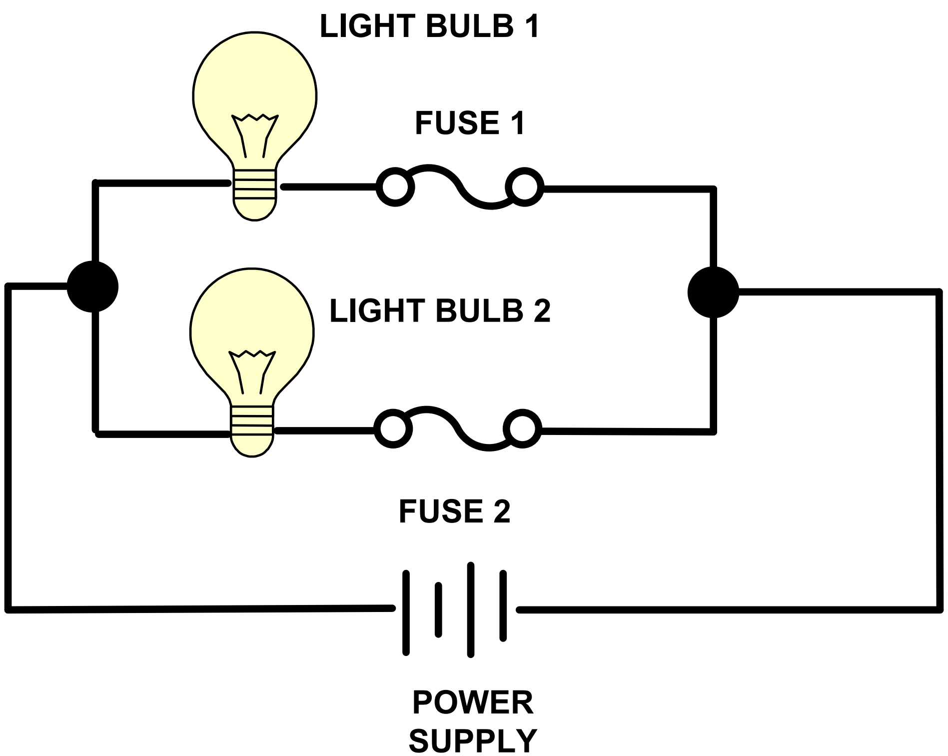


CUT SET NO.	MIN CUT SET	ORDER	DESCRIPTION
1	X3	1	FUSE OPEN
2	E1	1	POWER SUPPLY FAILURE
3	X1, X2	2	LIGHT BULB 1 BURNED OUT LIGHT BULB 2 BURNED OUT

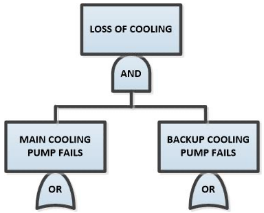


Fault tree – System C two light bulbs and two fuses

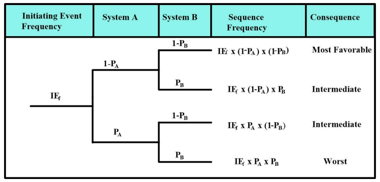




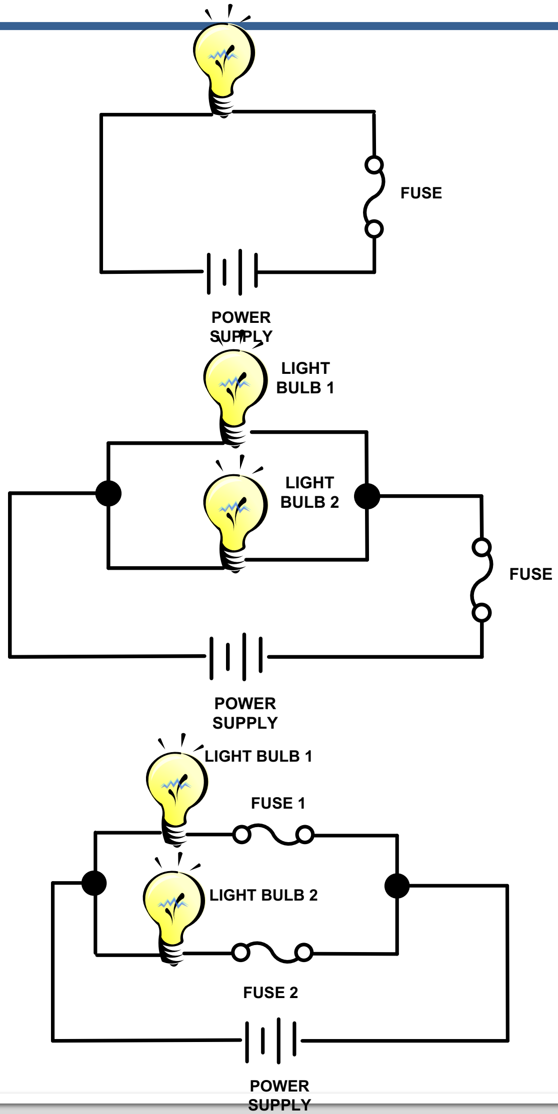
What are the min cut sets??

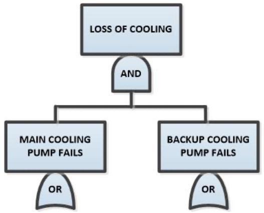


Min Cut Set Analysis – Three systems

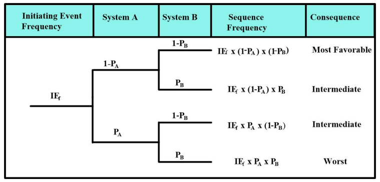


- Min Cut Set Analysis
  - **System A** (3 min cut sets)
    1. Light bulb burned out
    2. Fuse open
    3. Power supply failure off
  - **System B** (3 min cut sets)
    1. Fuse open
    2. Power supply failure off
    3. Light Bulb 1 burned out & light bulb 2 burned out
  - **System C** (5 min cut sets)
    1. Power supply failure off
    2. Light Bulb 1 burned out & light bulb 2 burned out
    3. Fuse 1 open & Fuse 2 open
    4. Light Bulb 1 burned out & Fuse 2 open
    5. Light Bulb 2 burned out & Fuse 1 open

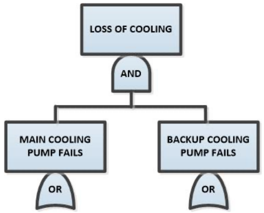




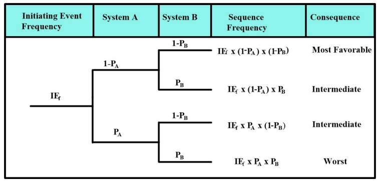
Duality Principle

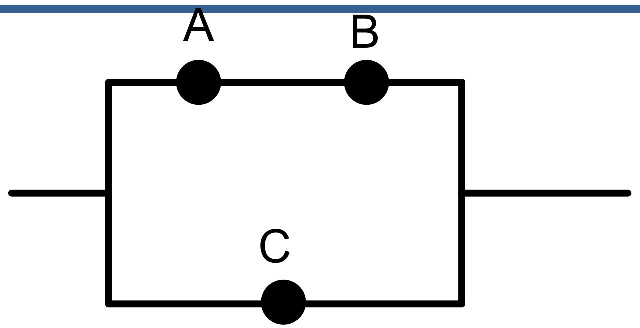


- Important concept
- Start with success criteria
- Use duality principle to define failure logic
- Can reverse process (i.e., failure to success)
- Example
  - System with three pumps A, B and C
  - Pumps A and B have 50% capacity
  - Pump C has 100% capacity



Reliability Network Diagram





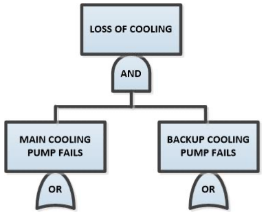
RELIABILITY NETWORK DIAGRAM

SUCCESS PATHS (PATH SETS)

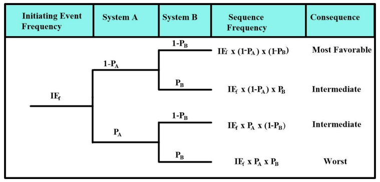
(PUMP A WORKS AND PUMP B WORKS)
OR
PUMP C WORKS
ab, c

MIN CUT SETS

(PUMP A FAILS AND PUMP C FAILS)
(PUMP B FAILS AND PUMP C FAILS)
AC, BC

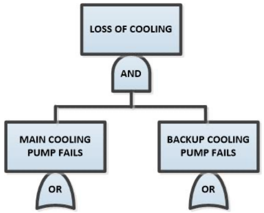


System Analysis: System Success Criteria

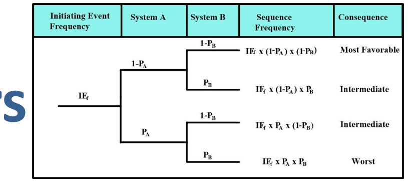


Examples of Success to Failure translation:

- 2 of 4 pumps for success
- 1 of 2 charging pumps OR 2 of 2 Safety Injection pumps for success



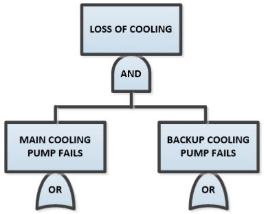
Success Criteria for the mitigating system tabulated as a function of accident initiators



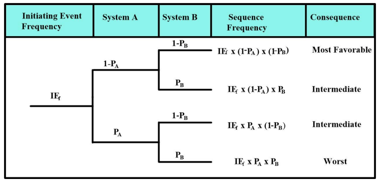
ACCIDENT INITIATOR	SUCCESS CRITERIA*	
	COOLANT INJECTION	CONTAINMENT HEAT REMOVAL
Large LOCA: Steam Break ≥ 0.08 ft^2 Liquid Break ≥ 0.1 ft^2	1 of 4 LPCI Pumps OR 1 of 2 Core Spray Pumps	1 RHR
Medium LOCA: Steam Break 0.016 to 0.08 ft^2 Liquid Break: 0.004 to 0.1 ft^2	HPCI OR 1 of 4 LPCI Pumps OR 1 of 2 CS Pumps } and ADS*	1 RHR
Small LOCA: Steam Break < 0.016 ft^2 Liquid Break < 0.004 ft^2	HPCI OR RCIC OR 1 Feedwater Pump OR 1 of 2 CS Pumps OR 1 of 4 LPCI Pumps OR 1 Condensate Pump } and ADS*	Normal Heat Removal OR 1 RHR OR RCIC in St. Cond. Mode
Transient	Same as Small LOCA	Same as Small LOCA
IORV	Same as Small LOCA	Same as Small LOCA
Transient + SORV	Same as Small LOCA	Same as Small LOCA

Shoreham Nuclear Power Plant

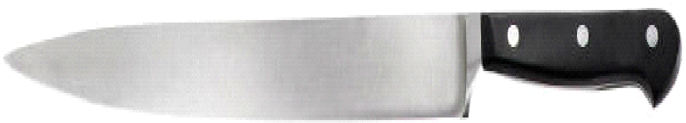
MARK II BWR 4



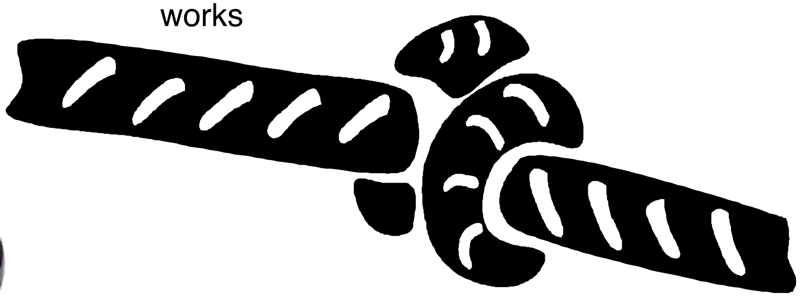
Min Cut Sets versus Min Path Sets

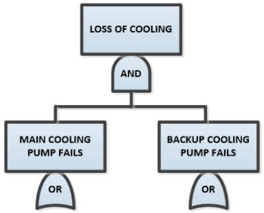


- Min Cut Sets
  - **System A** (3 min cut sets)
    1. Light bulb burned out
    2. Fuse open
    3. Power supply failure off
  - **System B** (3 min cut sets)
    1. Fuse open
    2. Power supply failure off
    3. Light Bulb 1 burned out & light bulb 2 burned out
  - **System C** (5 min cut sets)
    1. Power supply failure off
    2. Light Bulb 1 burned out & light bulb 2 burned out
    3. Fuse 1 open & Fuse 2 open
    4. Light Bulb 1 burned out & Fuse 2 open
    5. Light Bulb 2 burned out & Fuse 1 open

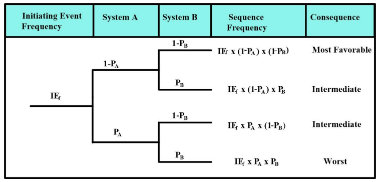


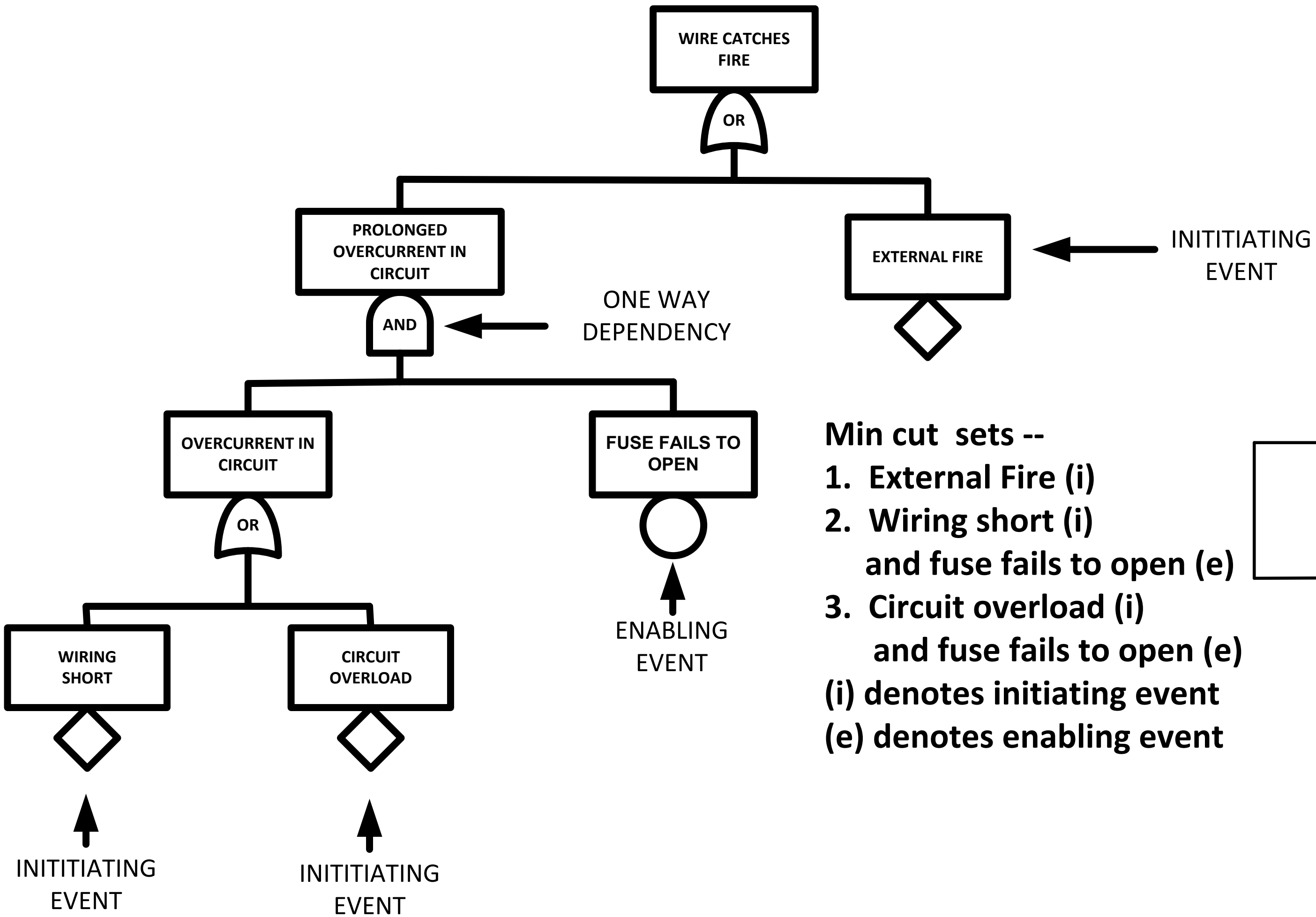
- Min Path (Tie) Sets
  - **System A** (1 min path set)
    1. Light bulb works & fuse works & power supply works
  - **System B** (2 min path sets)
    1. Light bulb 1 works & fuse works & power supply works
    2. Light bulb 2 works & fuse works & power supply works
  - **System C** (2 min path sets)
    1. Light bulb 1 works & fuse1 works & power supply works
    2. Light bulb 2 works & fuse2 works & power supply works





Fault tree for system A or B – wire catches fire



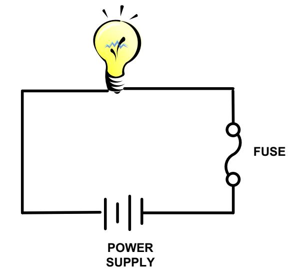


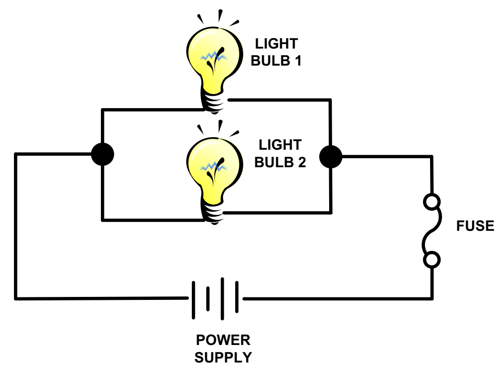
Min cut sets --

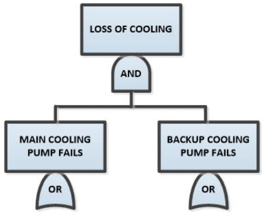
1. External Fire (i)
2. Wiring short (i)
   and fuse fails to open (e)
3. Circuit overload (i)
   and fuse fails to open (e)

(i) denotes initiating event

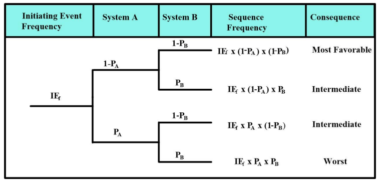
(e) denotes enabling event

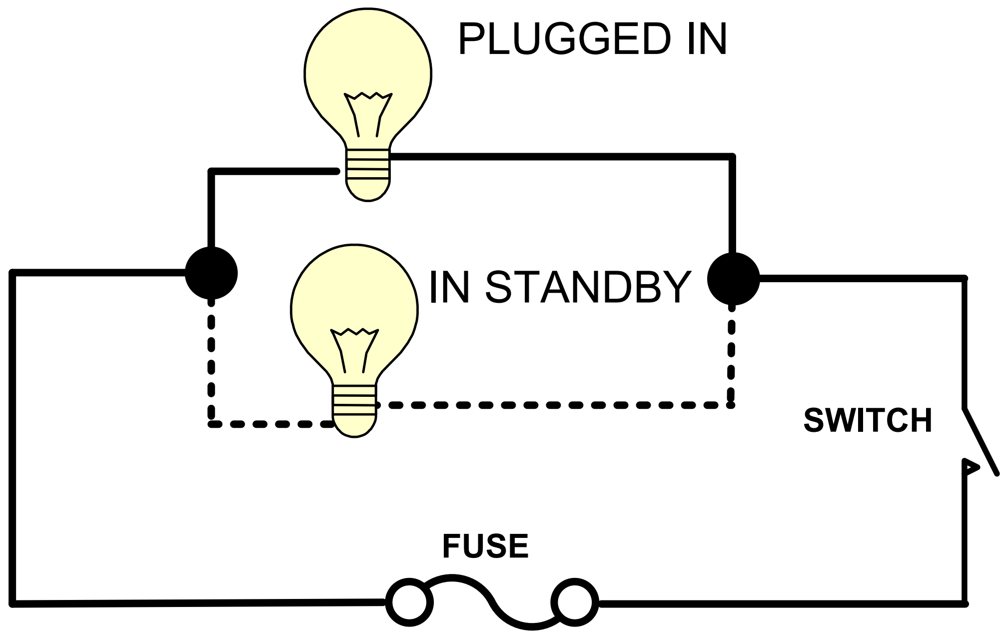


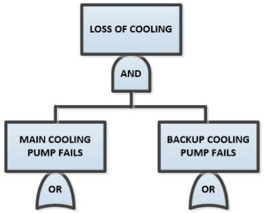




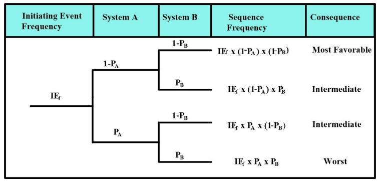
STANDBY REDUNDANCY

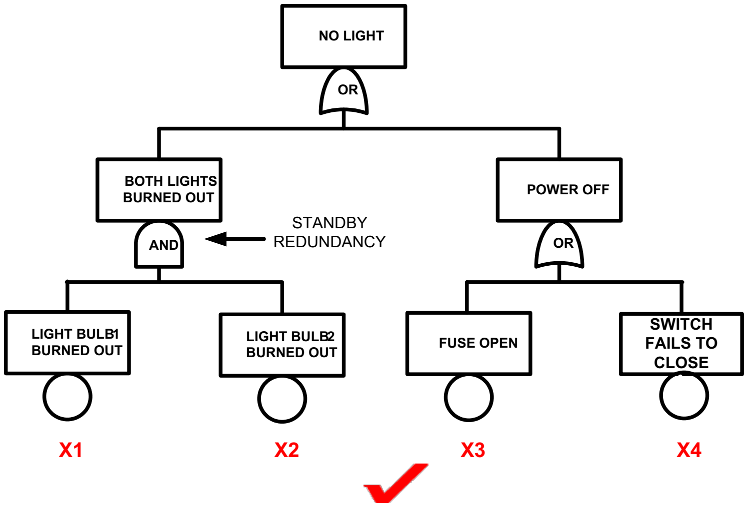


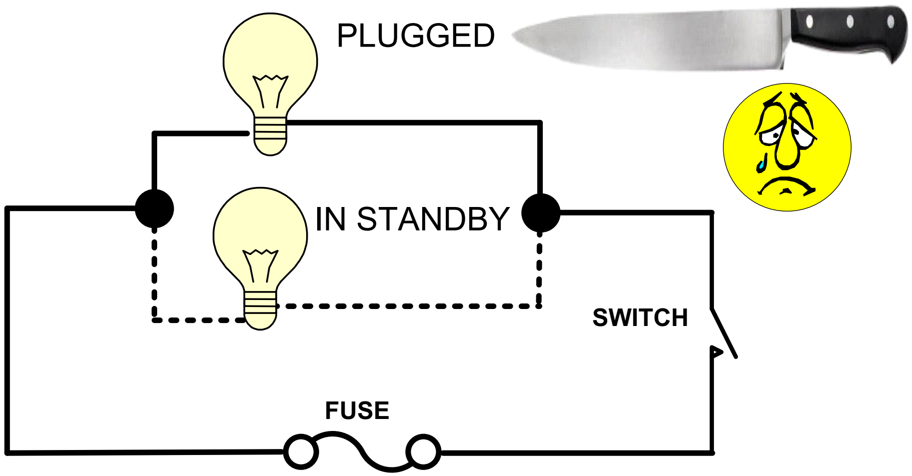




Sample Fault Tree for Standby Redundancy

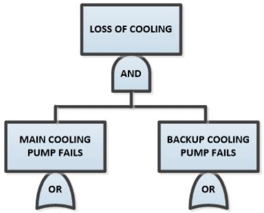




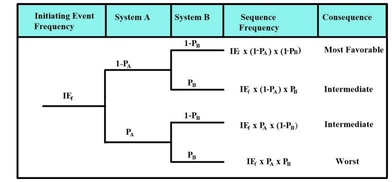


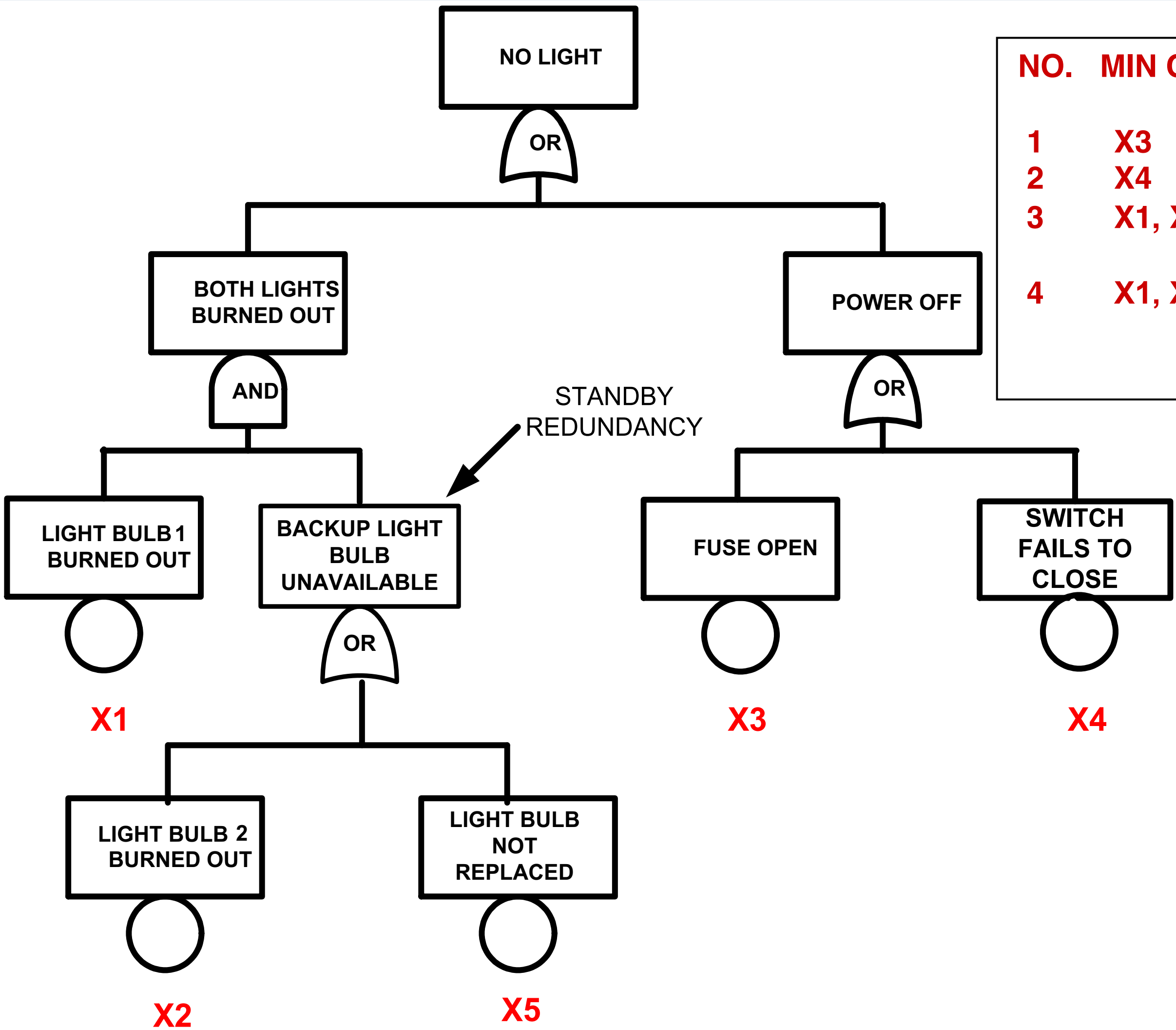
Consider active failures only

CUT SET NO.	MIN CUT SET	ORDER	DESCRIPTION
1	X3	1	FUSE OPEN
2	X4	1	SWITCH FAILS TO CLOSE
3	X1, X2	2	LIGHT BULB 1 BURNED OUT LIGHT BULB 2 BURNED OUT

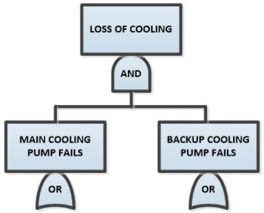


Sample Fault Tree for Standby Redundancy with Replacement Error

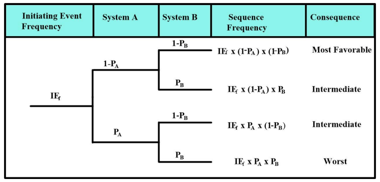




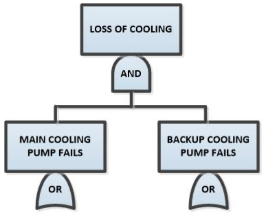
NO.	MIN CUT	ORDER	DESCRIPTION
1	X3	1	FUSE OPEN
2	X4	1	SWITCH FAILS TO CLOSE
3	X1, X2	2	LIGHT BULB 1 BURNED OUT LIGHT BULB 2 BURNED OUT
4	X1, X5	2	LIGHT BULB 1 BURNED OUT BACKUP LIGHT BULB NOT REPLACED



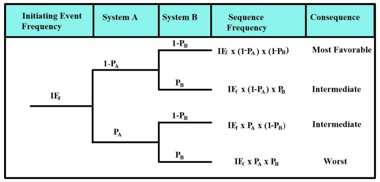
Two Examples LLNL – Event Tree Fault Tree Approach and one fatal criticality incident in Russia



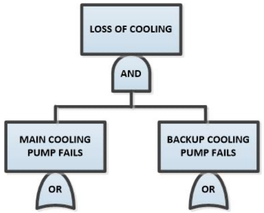
- NIF safety interlock access control system
  - Laser Exposure (NIF National Ignition Facility)
- Fatal Criticality incident in Sarov Russia June 17 1997
- Fissile Material Handling Gloveboxes
  - Criticality



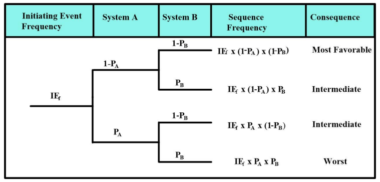
Personnel HAZARDS IN THE NIF

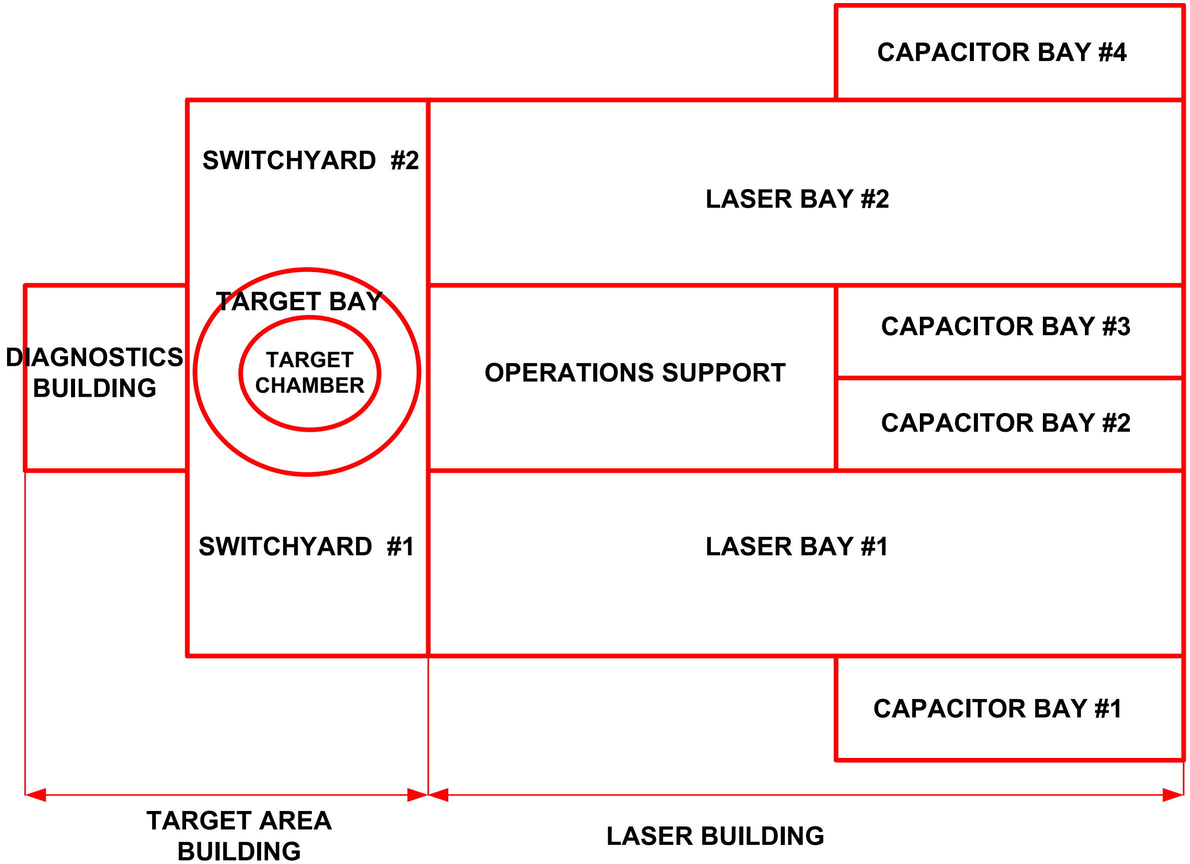


- laser light,
- high voltage
- oxygen deficiency,
- cryogenic materials,
- hazardous chemicals,
- mechanical/moving equipment/lifting,
- falls/falling objects,
- radiation,
- vacuum,
- shrapnel



National Ignition Facility





NIF -- Laser and Target Area Building (LTAB)

NIF Hazards

1. Prompt Radiation from shot –

Target Chamber Controls

i)Access control system

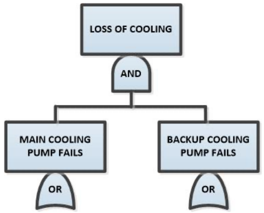
ii) Sweep

2. Electrical hazards –

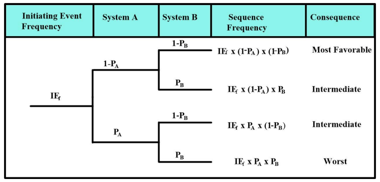
Main Amplifier and power amplifiers – laser bays

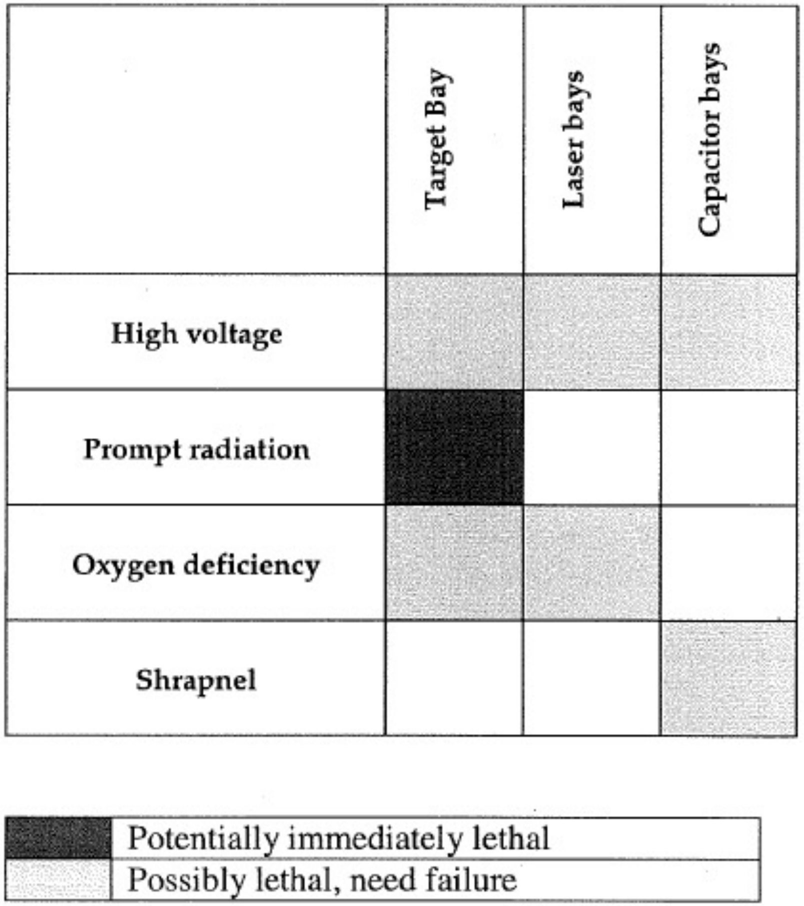
Capacitor Bays

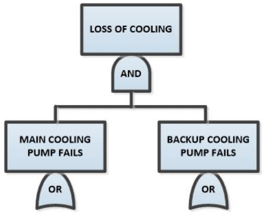
3. Oxygen Deficiency



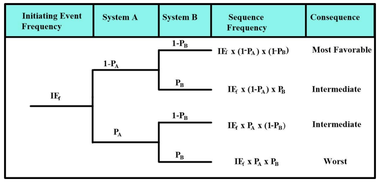
Maximum Hazard Levels in Various NIF Locations during shot sequence

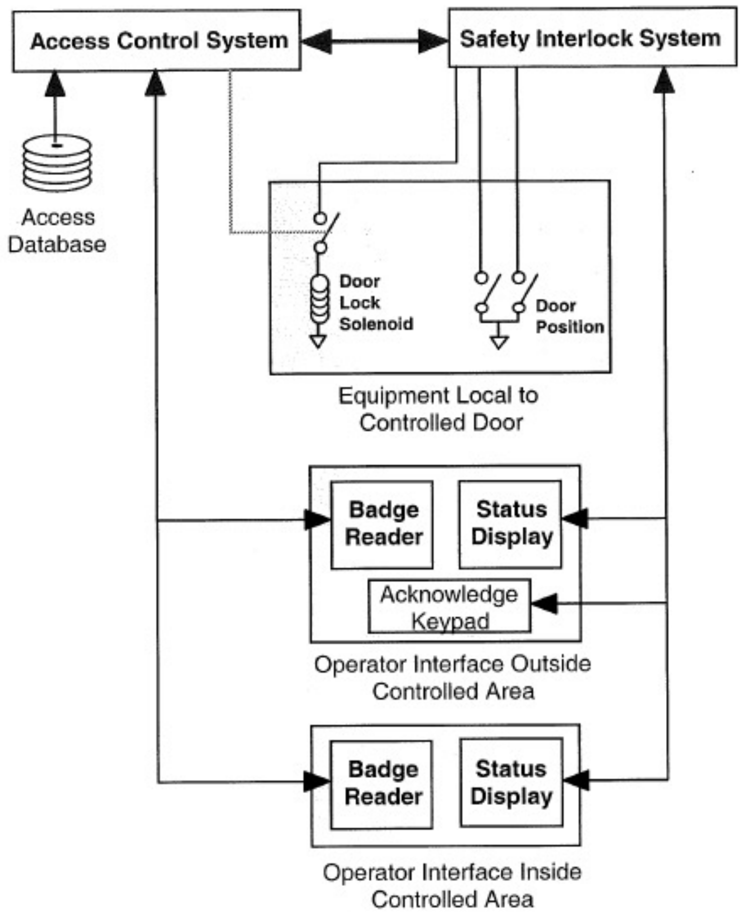


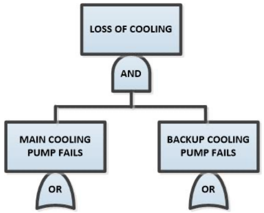




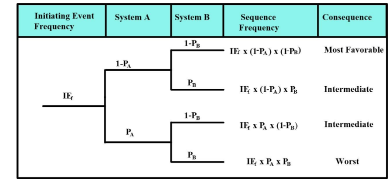
Safety Interlock System interface with Access Control System





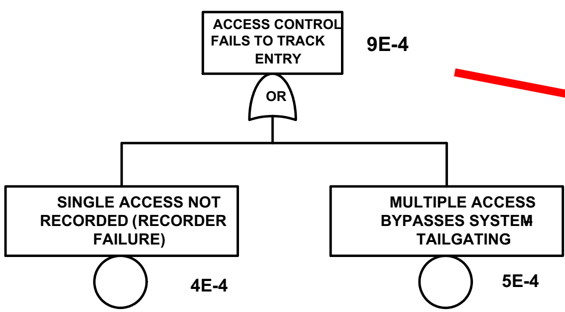


NIF Access Control Event Tree

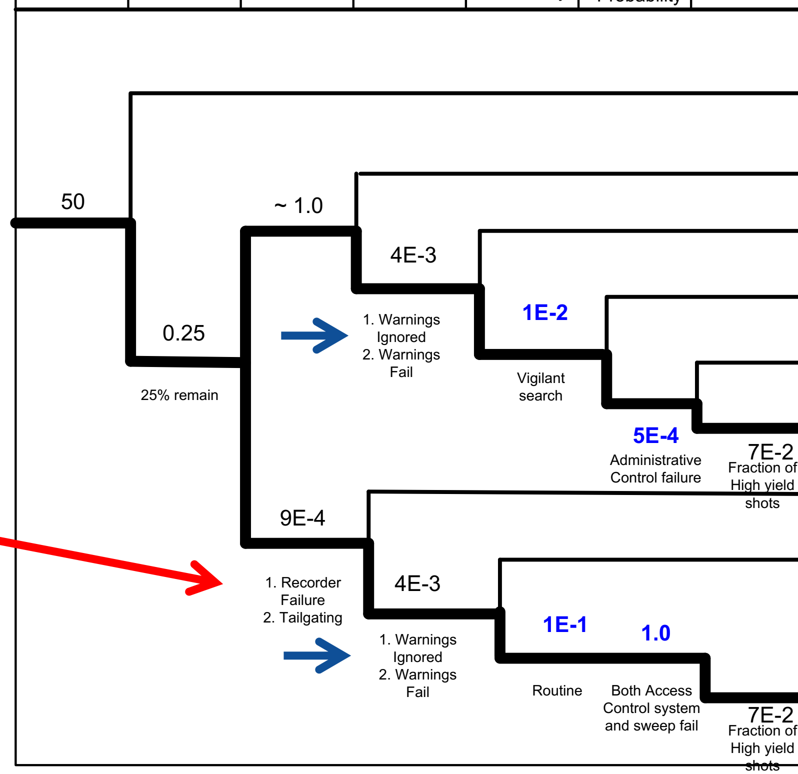


Reference

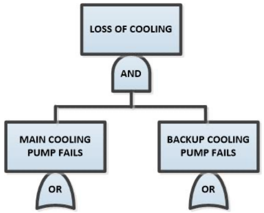
NIF-0065625 -- Personnel Access Control System Evaluations for National Ignition Facility Operations June 2001



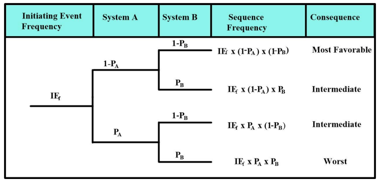
Workers in Target Bay	Job not finished	Access Control System fails to track entry	Persons Fail to Leave	Sweep Fails to remove Person(s)	Shot Sequence Started	Persons Exposed To fatal hazard	END STATE No.	END STATE Probability (Per Shot)	END STATE Description
50	0.25	9E-4	4E-3	Conditional Probability	Conditional Probability	7E-2		Annual Probability (746 shots per year) Importance %	
							1		OK
							2		OK
							3		OK
							4		OK
							5		OK
							6	2E-8 /shot 1.E-5/yr * 6.3%	FATALITY
							7		OK
							8		OK
							9		OK
							10	3E-7/shot 2E-4/yr * 93.8%	FATALITY

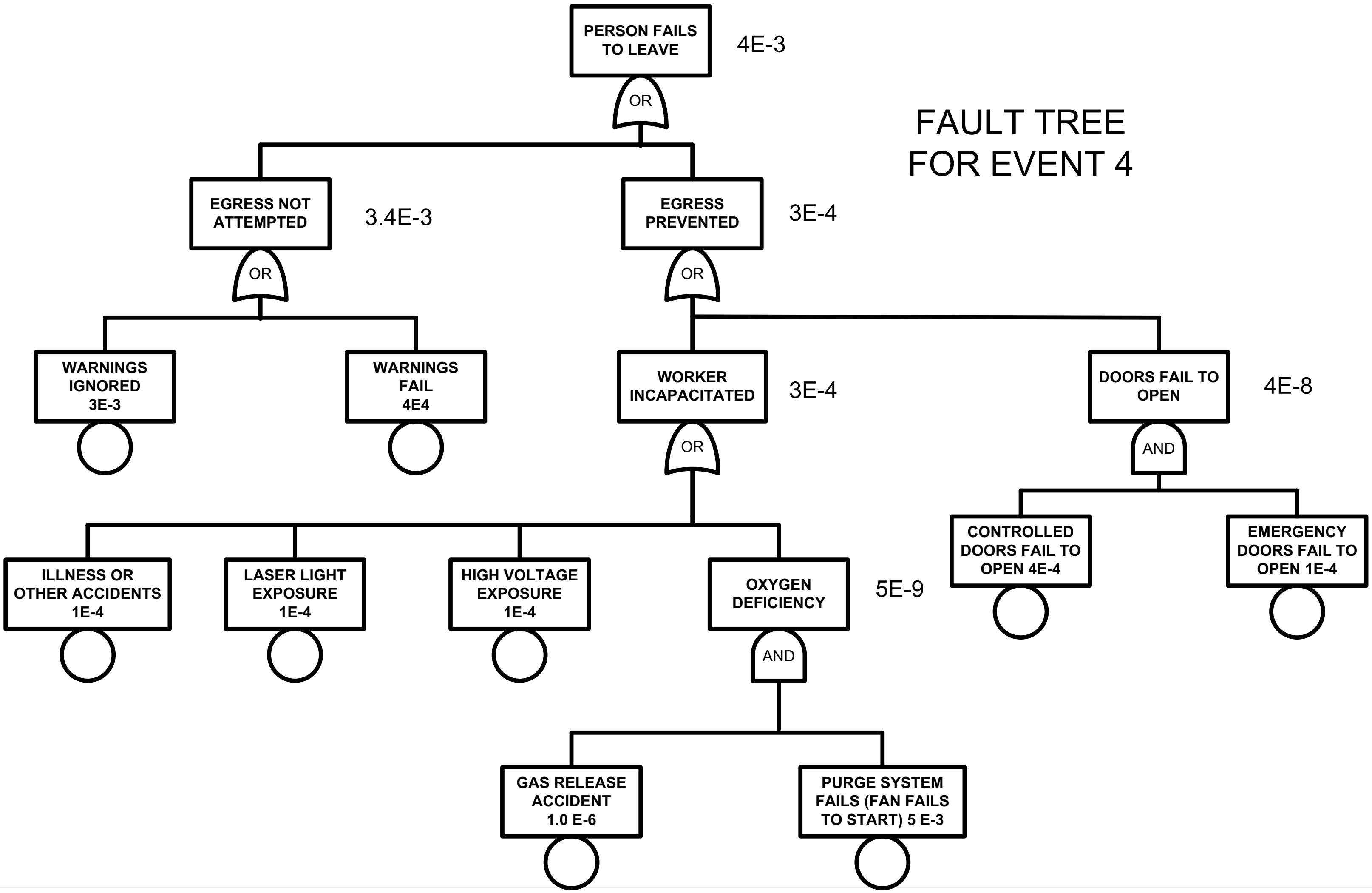


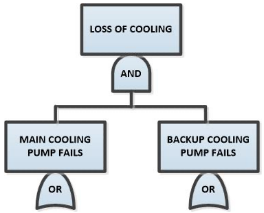
*Total Annual Fatality Rate = 1E-5 + 2E-4 = 2.1E-4 Based on 746 shots per year



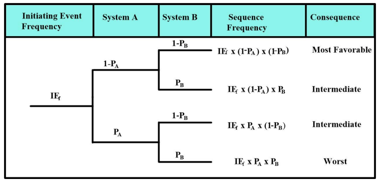
Fault Tree for Persons Failure to Leave





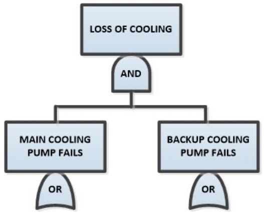


Summary of Event Tree Data

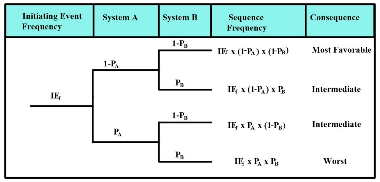


	Target Bay	Laser Bays	Capacitor Bays
Number of entries per shot sequence	50	50	10
Job not finished – workers remain in Bay prior to warnings*	.25	.5	.5
Access control fails to track entry*	$9x10^{-4}$	$9x10^{-4}$	$5x10^{-3}$
Person fails to leave*	$4x10^{-3}$	$4x10^{-3}$	$4x10^{-3}$
Generic sweep fails*	$1x10^{-1}$	$5x10^{-1}$	$1x10^{-1}$
Specific sweep fails*	$1x10^{-2}$	$1x10^{-1}$	$1x10^{-2}$
Human error - shot sequence started*	$5x10^{-4}$	$5x10^{-4}$	$5x10^{-4}$
Person exposed to fatal hazard*	$7x10^{-2}$	$1x10^{-4}$	$9x10^{-5}$
Sum of fatal sequences on event tree per shot	$3x10^{-7}$	$5x10^{-9}$	$9x10^{-10}$
Fatalities per year for 746 shots	$2x10^{-4}$	$4x10^{-6}$	$7x10^{-7}$

* Per shot



Criticality incident in Sarov Russia June 17, 1997 involving a Physicist Zaharov



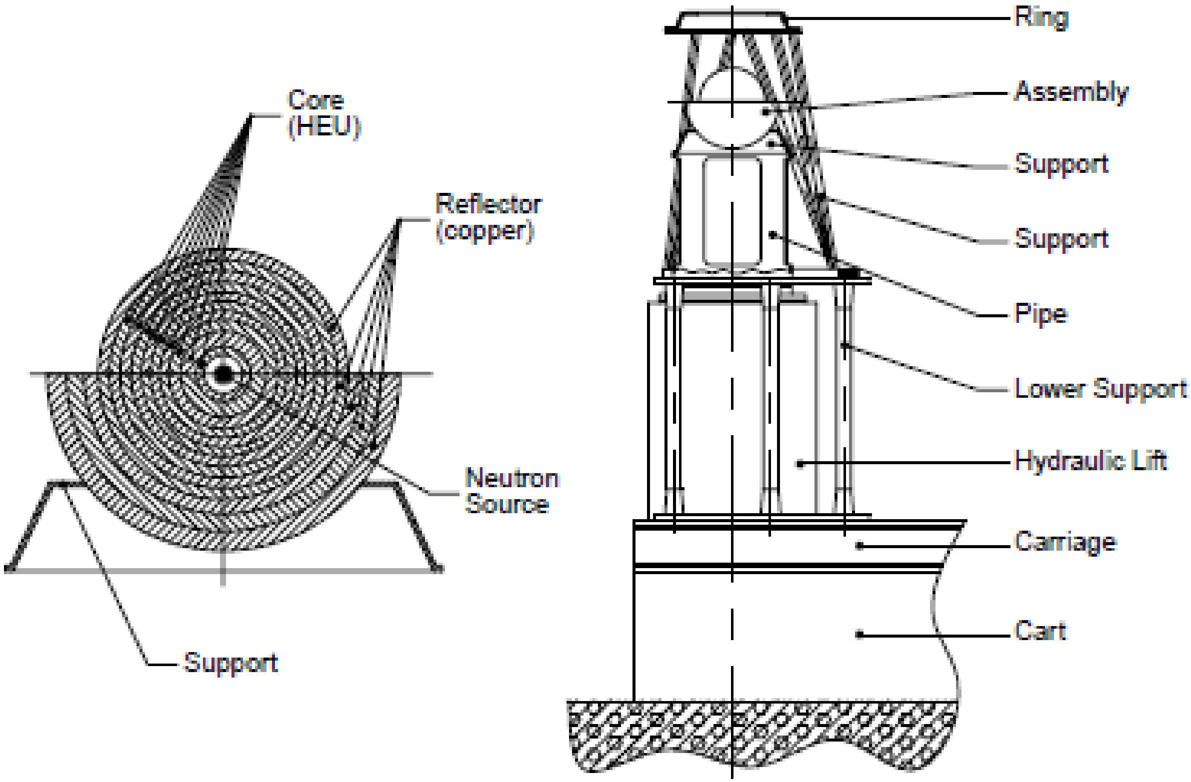
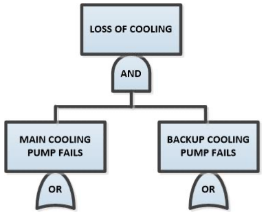


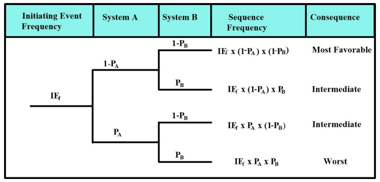
Figure 56. Accident configuration.

1972 logbook inside and outside dimensions copper reflectors (167 and 205mm) copied erroneously as (167 and 265 mm) used lower copper reflector of 258mm

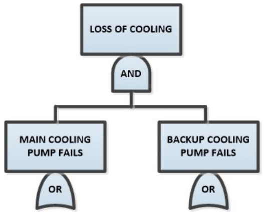
Reference --
Los Alamos Document "A Review of Criticality Accidents," LA-13638



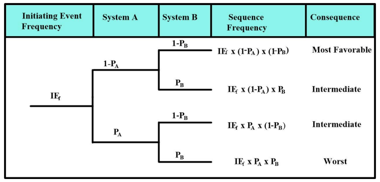
Criticality Accident and Contributing Factors



- Dropped upper copper reflector -- received dose of 4500 Rads (Neutron) and 350 Rads (gamma) died three days later in a Moscow hospital
- Contributing Factors to accidents
  - Arrogance – did not submit proper papers work -- no one checked his dimensions for copper shield
  - working alone – against safety operating procedures
- INTERNATIONAL ATOMIC ENERGY AGENCY publication 2001 recommendations regarding incident (1 of 4)
  - Comprehensive safety assessments enable the probabilities and magnitudes of possible accidents to be determined so that measures can be taken to prevent them or to mitigate their consequences



Double Contingency Principle (DCP) Criticality Safety



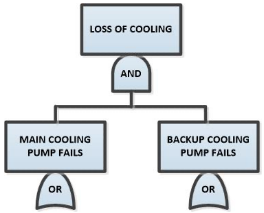
•The DCP defined in ANS 8.1 is a requirement per DOE O 420.1B.

"Process designs should incorporate sufficient factors of safety to require at least <u>two unlikely</u>, <u>independent</u>, and <u>concurrent</u> changes in process conditions before a criticality accident is possible."

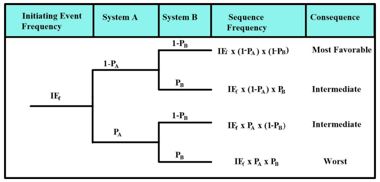
- Operations will be kept sub-critical under both normal and credible abnormal conditions

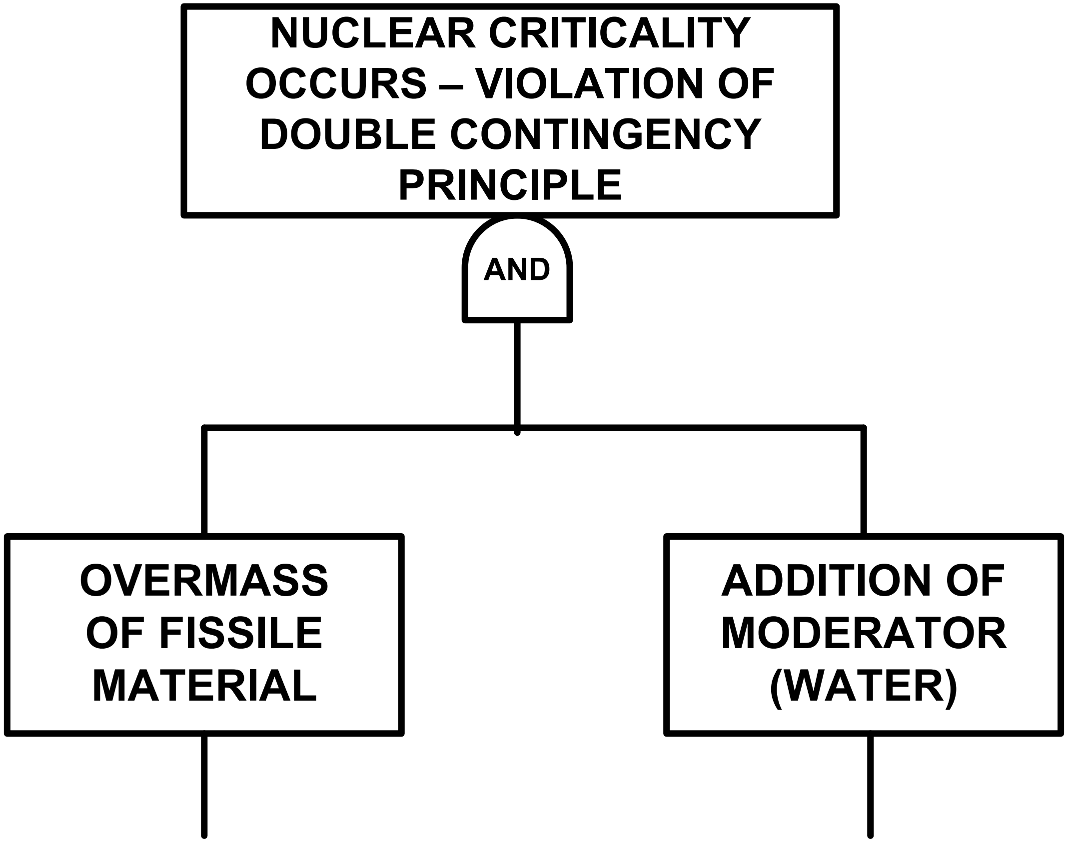
- No Single credible event can result in a criticality

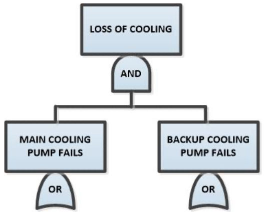
- Controls of multiple process parameters rather than multiple controls of a single parameter



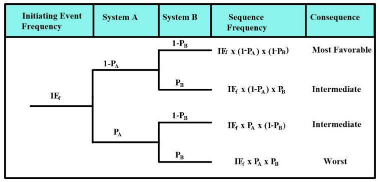
AND GATE – NUCLEAR CRITICALITY



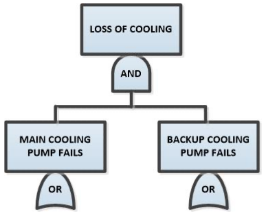




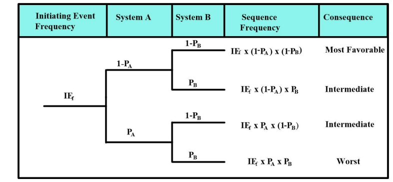
PROCESS PARAMETER Nuclear Criticality



- a physical property whose value affects the nuclear reactivity of a system
  - mass, density, concentration, and isotopic enrichment of fissionable material
  - the geometry, reflection, and interaction conditions of the system
  - the moderation, composition and *neutron absorption characteristics of the fissionable material mixture and other system materials*
- Reference **DOE-STD-3007-2007**



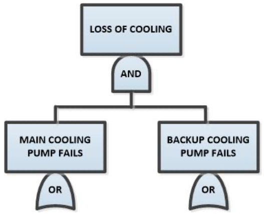
LLNL Procedure CSG-P-004 Process Walkthrough Questions



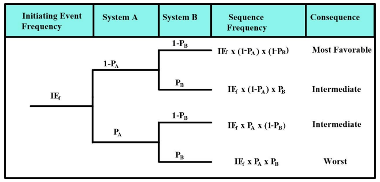
1. What kind of fissionable material operations are intended in the workstation (or the room, etc)?
What is the feed material and does the form or shape of the material change?
Is the material weapons grade or other enrichment? Is it alloyed and what density?
What equipment, fixtures, and specialized containers are used in the process?

2. What are the products of the process? What are the wastes/residues of the process?
Form, shape, intermixed with other materials
How packaged?
Where do they go?
Measurements
Vaults
Other workstations

3. Are liquids used or stored in the workstation?
Coolants, solvents, lubricants
Total volume of the coolant loop
Total volume in bottles or sealed equipment



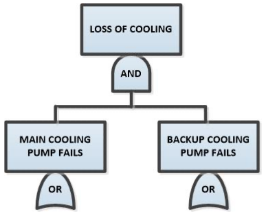
CSG-P-004 Process Walkthrough Questions Cont'd



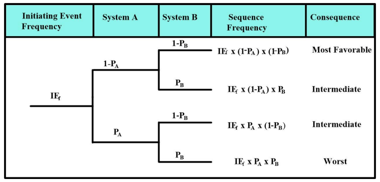
4. What equipment or fixtures are used in the workstation which will provide significant reflection?
Molds, crucibles, specialized containers, heat sinks
Shielding for personnel protection (poly or water walled vessels or wells, Pb lined containers)
Nearby/adjacent concrete walls or other large construction
What materials, size and shape?
Drawings

5. Are there areas in the equipment or glovebox floor where liquids could collect?
Storage wells
Oil collection troughs
Basins in equipment
Containers, pans and trays

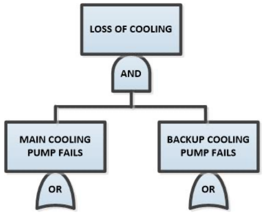
6. What are possible overmass upsets?
What is the maximum credible overmass?
Is automated transfer equipment used which could effect the maximum overmass?
Are there connected gloveboxes which could allow inadvertent transfers?



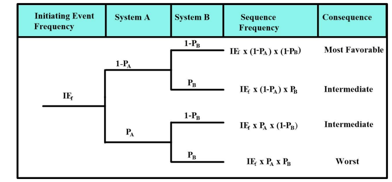
Six specific criticality scenarios were identified for fault tree analysis



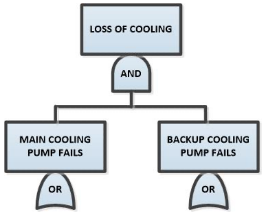
- (1) Inadvertent Criticality in a Metal System in a Workstation
- (2) Criticality in a Powder/Liquid Slurry at a Workstation
- (3) Criticality in an Aqueous System in a Workstation
- (4) Inadvertent Criticality in Storage Vaults
- (5) Criticality During Transportation
- (6) Criticality Due to Earthquake



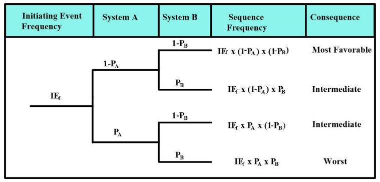
Important procedural errors that could lead to inadvertent criticality



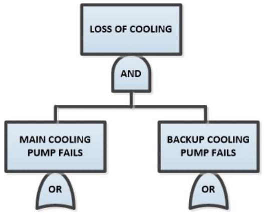
- Overbatch with approved items (handlers are same shipper and receiver, two sets of different handlers)
- Overbatch with unapproved items (handlers are same shipper and receiver, two sets of different handlers)
- Failure to conduct cleanout properly, e.g., leaving moderator in workstation -- unapproved material remains in workstation
- Failure to remove fissile material from workstation -- unapproved fissile material remains in workstation (handlers are same shipper and receiver, two sets of different handlers)
- Movement of incorrect material or equipment into a workstation
- Wrong SCCC (Standard Criticality Control Conditions) posting on workstation



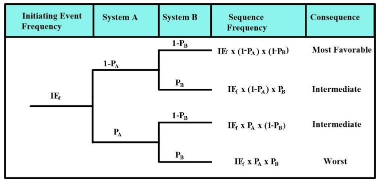
Criticality Hazards Analysis



ID #	Initiating Event	Causes	Event Consequences	Preventive Features	Mitigative Features	Relative Risk Discussion	Fault Tree Identification
Massive Metal							
Metal-01	Overbatch	FMH handling error, COMATS use error, COMATS error, or COMATS non-use (requires repetative procedure violations)	Increased mass at workstation, one overbatch is potentially credible, more than one overbatch is very unlikely. To attain k_{eff}>1, more than one overbatch would be necessary.	Parts handled are designed critically safe when over-batched and optimally water reflected. (Geometry and mass of parts provide the reactivity margin and structural strength of metal maintains the margin). COMATS does not provide permissive if batch limit will be exceeded. Parts are not normally placed together. Large quantity of moderating material is not present at workstation. Without moderator, more than two parts would be required to attain a critical mass.	Should overbatching occur, FMHs would recognize the presence of more than one batch visually during the preparation to transfer stage and initiate corrective action. Even should the material be delivered to the workstation, having the fixture occupied (a part in the way of the new part) would queue FMH to the error before the parts are placed in close proximity.	Requires multiple errors by two or more FMHs that must be repeated to attain at least three parts in a single workstation. This highly unlikely scenario is much less likely than Metal-2 scenario, therefore this scenario was screened out.	--
Metal-02	Overbatch and moderate	FMH handling error, workstation CSSS limit change error, COMATS use error, COMATS error, or COMATS non-use (requires 2 different procedure violations)	Increased mass at workstation, one overbatch is potentially credible. To attain keff>1, one overbatch involving a high reactivity Approved Item would be necessary (which are infrequently handled). Moderator must be added.	Parts handled are designed critically safe when over-batched and optimally water reflected. (Geometry and mass of parts provide the reactivity margin and structural strength of metal maintains the margin). This applies to all except high reactivity Approved Items which are very infrequently handled. COMATS does not provide permissive if batch limit will be exceeded. Parts are not normally placed together. Large quantity of moderating material could remain present after a CSSS change due to FMH error when changing the workstation condition. Without moderator, more than two parts would be required to attain a critical mass.	During the CSSS limit change, visual inspection of the workstation should detect moderator presence. Should overbatching occur, FMHs would recognize the presence of more than one batch visually during the preparation to transfer stage and initiate corrective action. Even should the material be delivered to the workstation, having the fixture occupied (a part in the way of the new part) would queue FMH to the error before the parts are placed in close proximity. Moderator would be in container or in solid form and away from the workstation fixture.	Requires multiple errors by two or more FMHs to deliver two parts to a single workstation, then another FMH error to combine the parts with the moderator. Highly unlikely scenario.	Yes



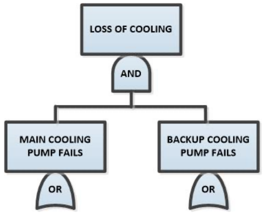
Example Application of the FT/ET Methodology to Criticality Safety



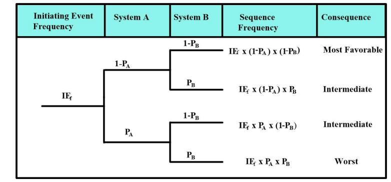
- Goal: Assess criticality accident frequency for a simple fissile operation in a glovebox

- Operation Description: Bring in two metal hemi-shells and assemble them into a spherical unit

- Analysis Method: Event tree with two linked fault trees to develop top event probabilities



Event Tree Example for Fissile Material Movement to Wrong Glovebox



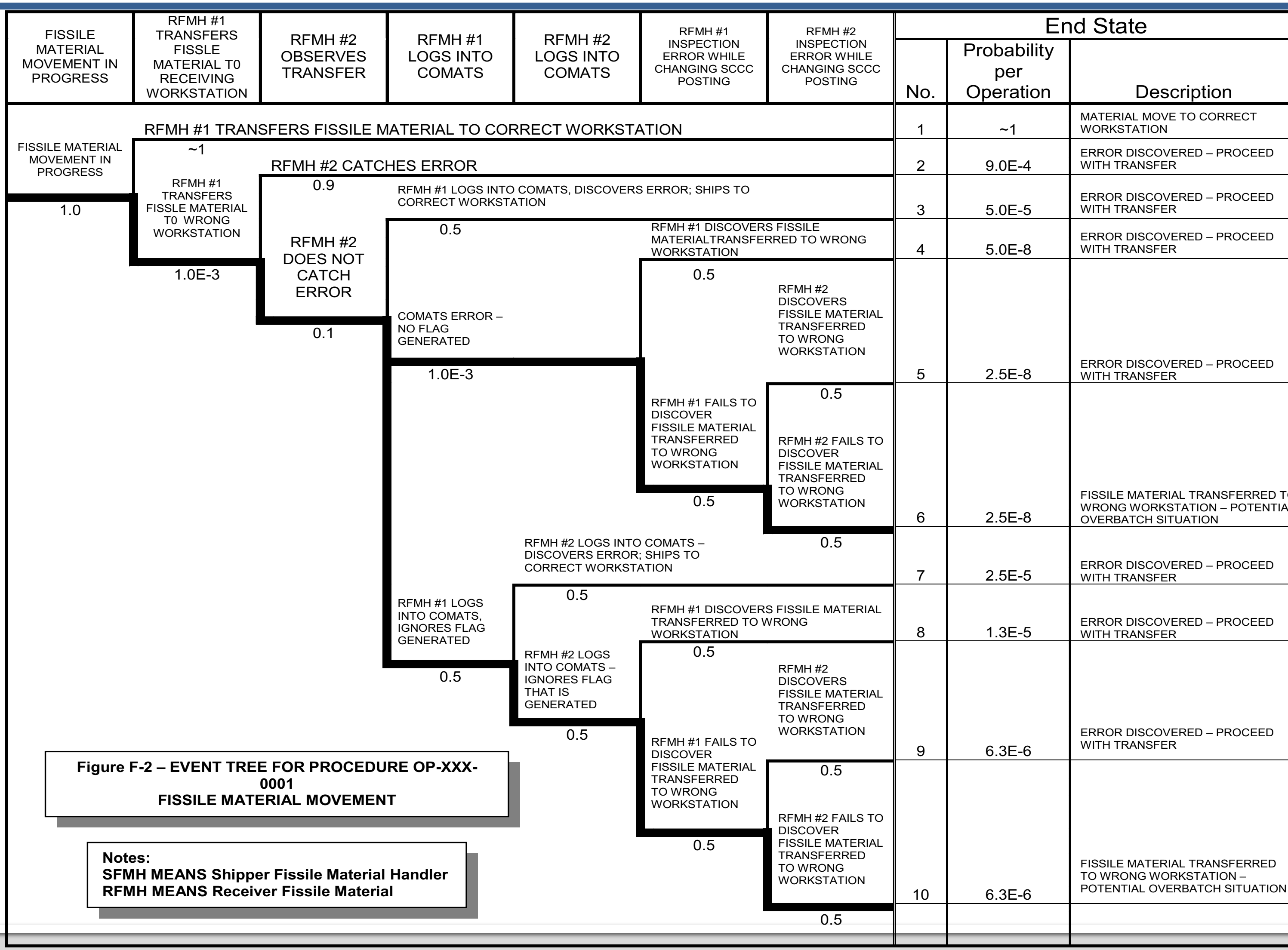
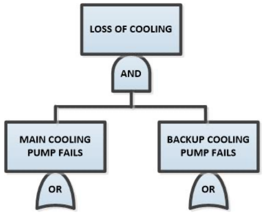
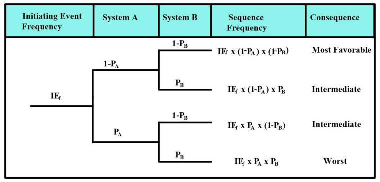


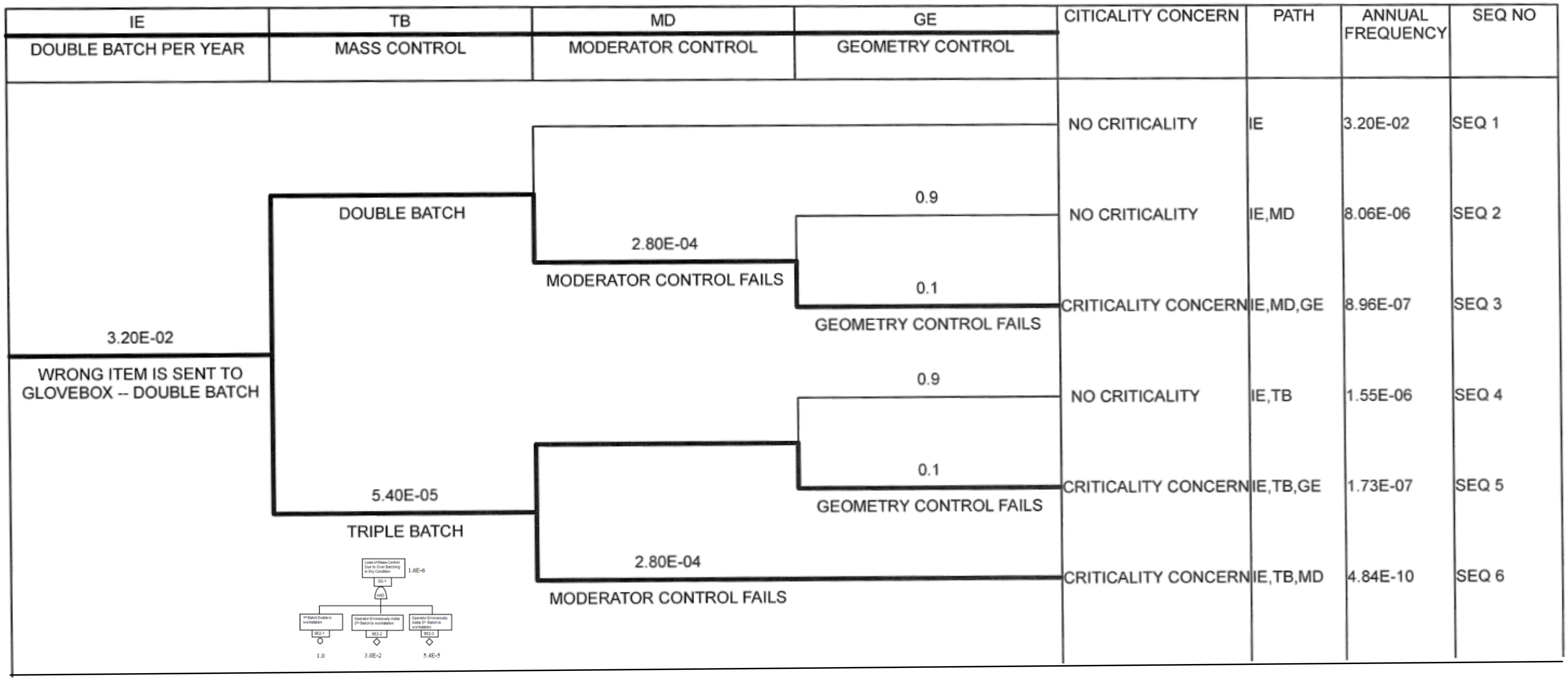
Figure F-2 – EVENT TREE FOR PROCEDURE OP-XXX-0001
FISSILE MATERIAL MOVEMENT

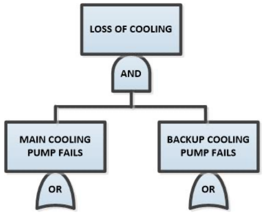
Notes:
SFMH MEANS Shipper Fissile Material Handler
RFMH MEANS Receiver Fissile Material



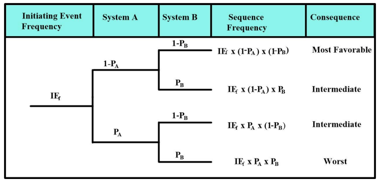
Criticality Event Tree

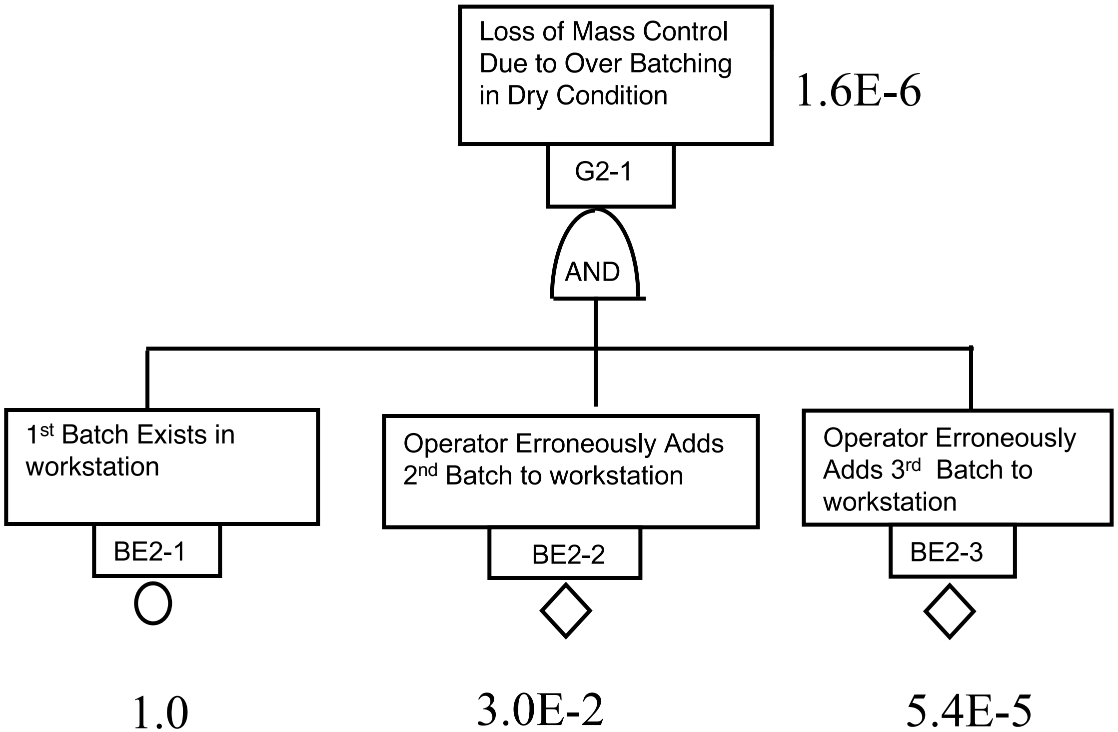


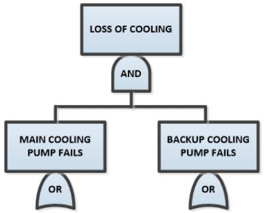




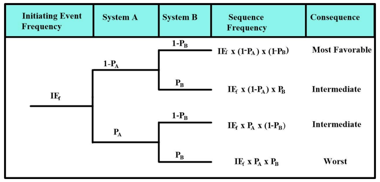
Fault Tree for Loss of Mass Control due to Over Batching in Dry Condition

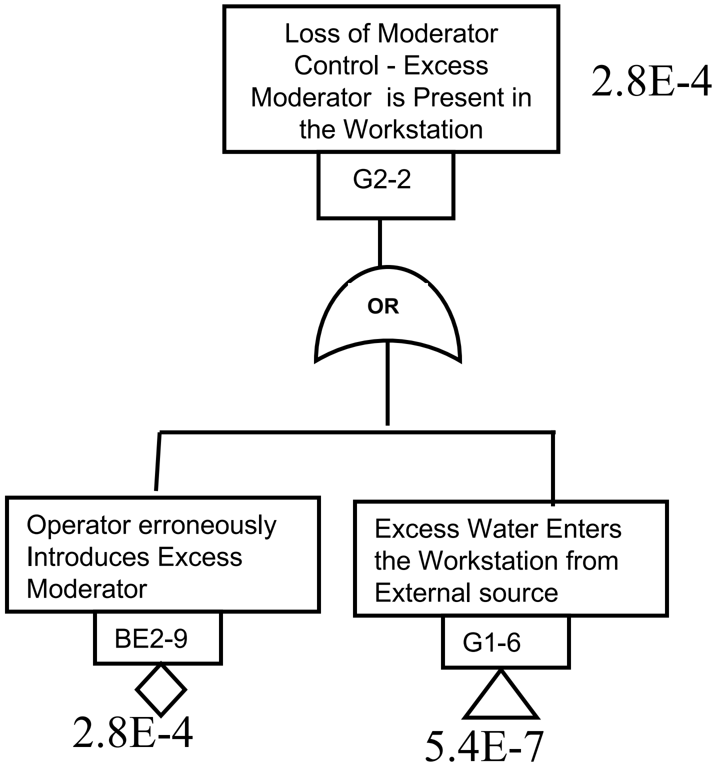


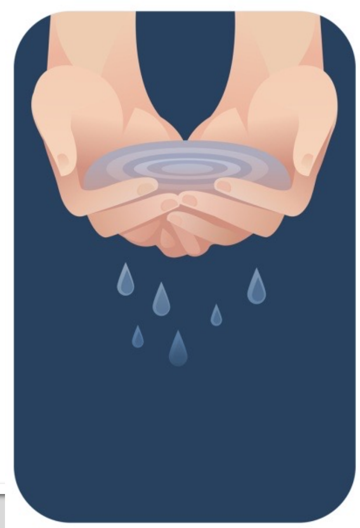


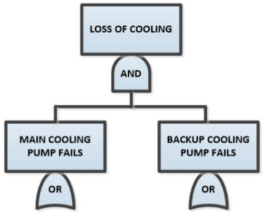


Fault Tree for Loss of Moderator Control

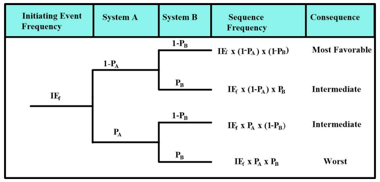


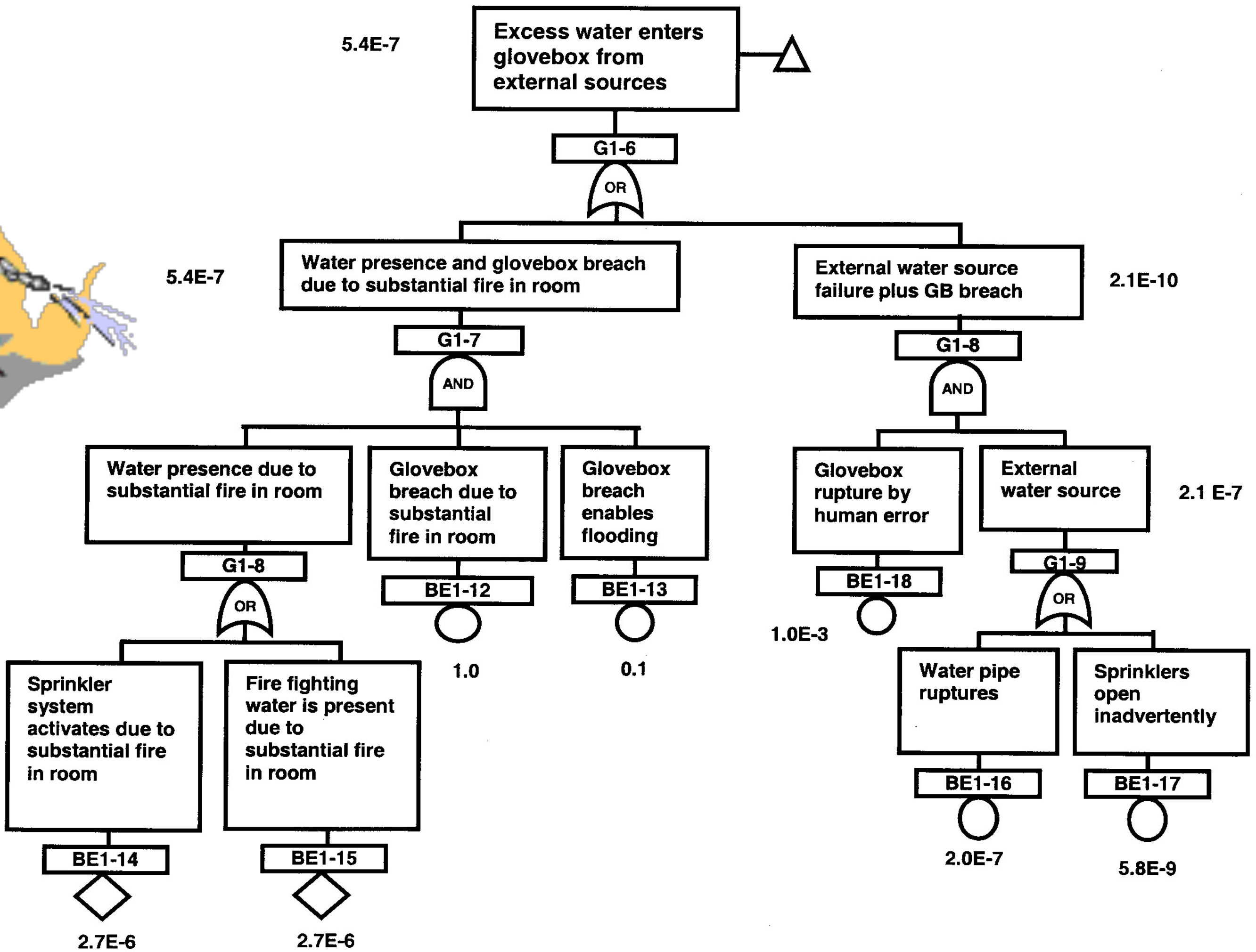


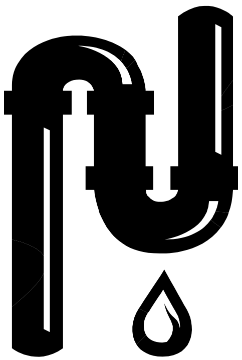


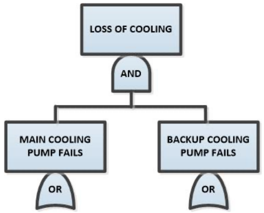


Fire Water System Fault Tree

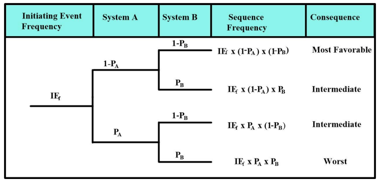






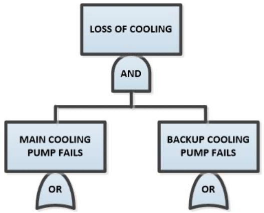


Yucca Mountain Nevada

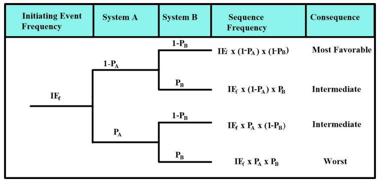


Yucca Mountain Nevada

Entrance Tunnel Yucca Mountain



Geological Repository Operations Area (GROA)



ABBREVIATIONS:

AO = AGING OVERPACK
CSNF = COMMERCIAL SPENT NUCLEAR FUEL
CR = RAIL CAR
DC = HLW AND DOE SNF DISPOSABLE CANISTER
DPC = DUAL PURPOSE CANISTER
GROA = GEOLOGICAL REPOSITORY OPERATIONS AREA
HLW = HIGH LEVEL RADIOACTIVE WASTE CANISTER
NAVAL = NAVAL SNF CANISTER
RC = RAIL CASK/OVERPACK
SNF = SPENT NUCLEAR FUEL
ST = SITE TRANSPORTER
STC = SHIELDED TRANSFER CASK
TAD = TRANSPORTATION, AGING AND DISPOSAL CANISTER
TC = TRUCK CASK/OVERPACK
TEV = TRANSPORT AND EMPLACEMENT VEHICLE
TT = TRUCK TRAILER
WP = WASTE PACKAGE

LEGEND

EMPTY

LOADED

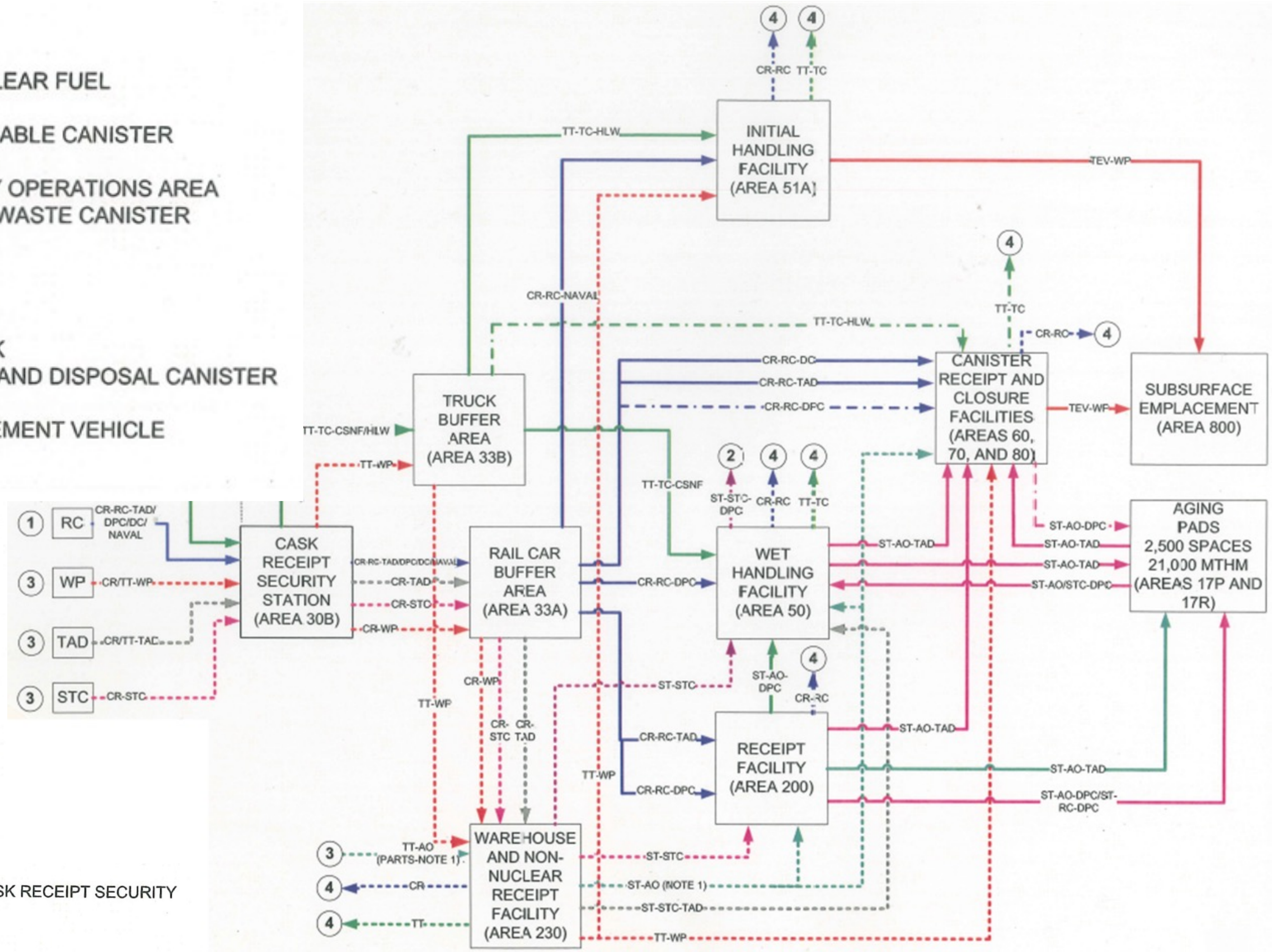
OPTIONAL

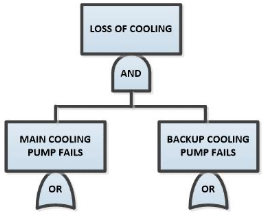
1 FROM NATIONAL TRANSPORTATION

2 TO LOW LEVEL WASTE

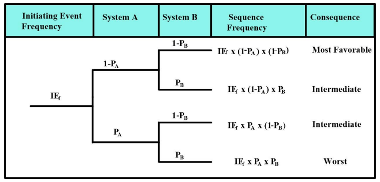
3 FROM SUPPLIER

4 TO NATIONAL TRANSPORTATION VIA CASK RECEIPT SECURITY STATION (AREA 30B)

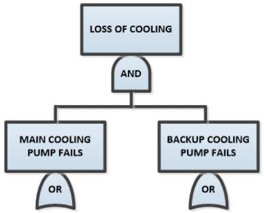




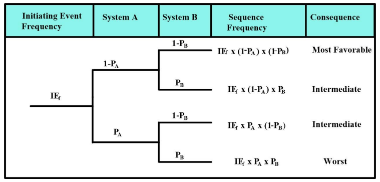
Yucca Mountain Project (YMP)

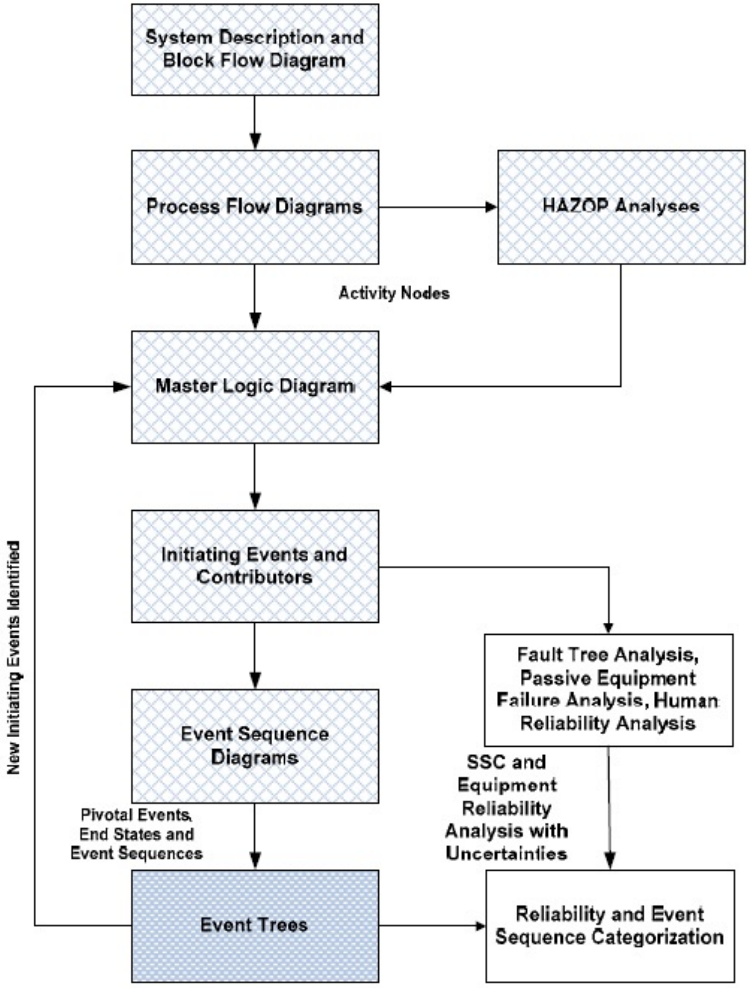


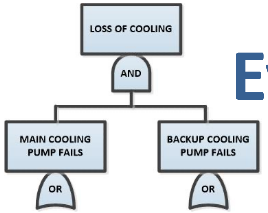
- Preclosure
  - Radionuclide containment (cask, canister or waste package)
  - Confinement (e.g., HVAC)
  - Wet Handling Facility (WHF) pool
- Postclosure – Geologic Barriers



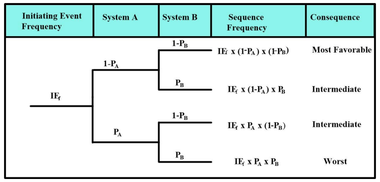
YMP Preclosure Safety Assessment Process

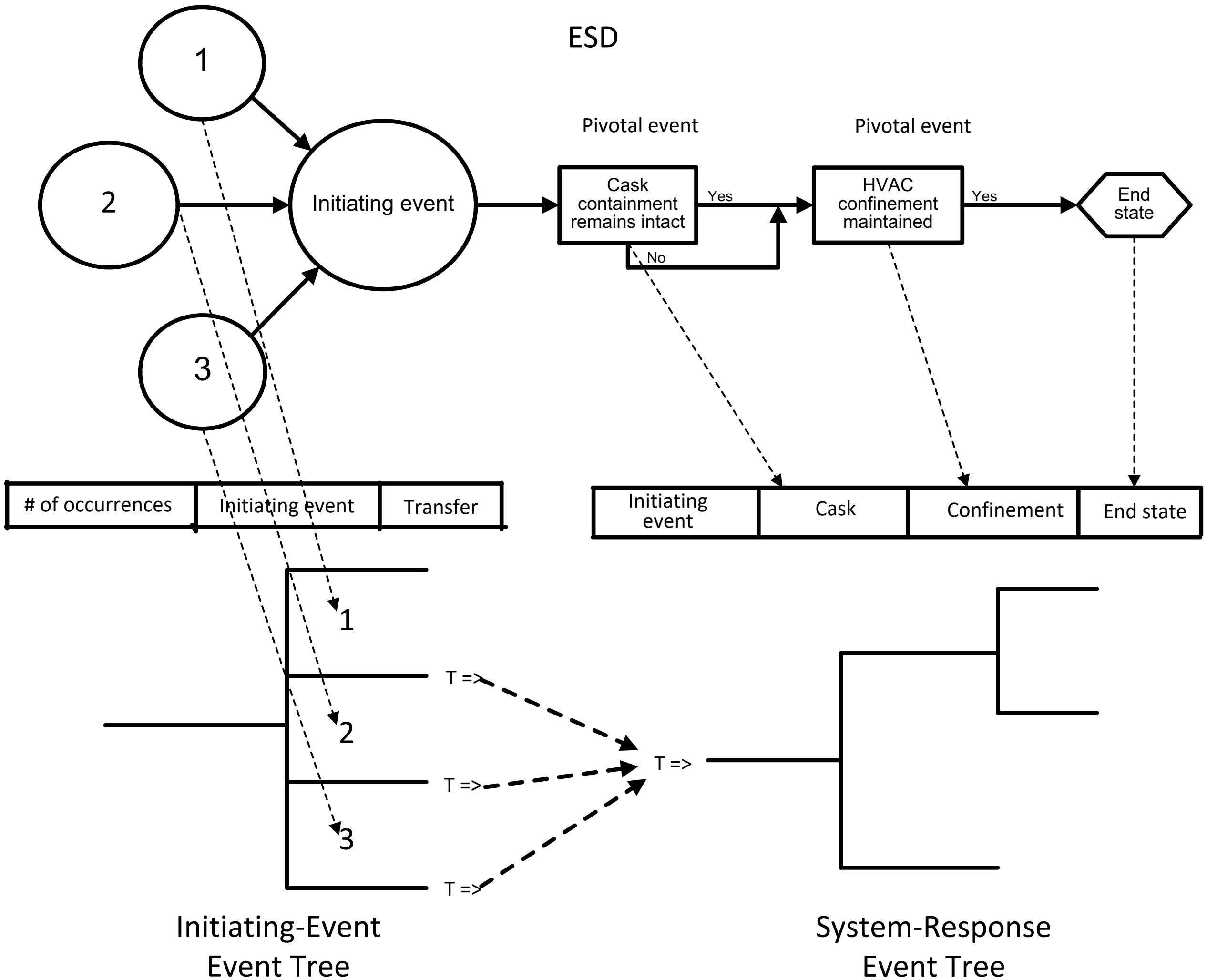


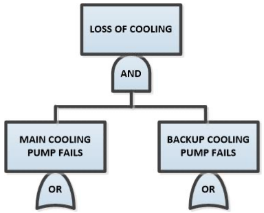




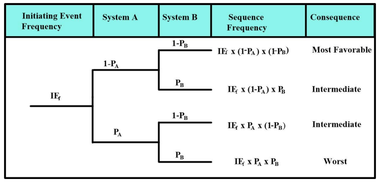
Event sequence diagram (ESD) showing relationship to event trees

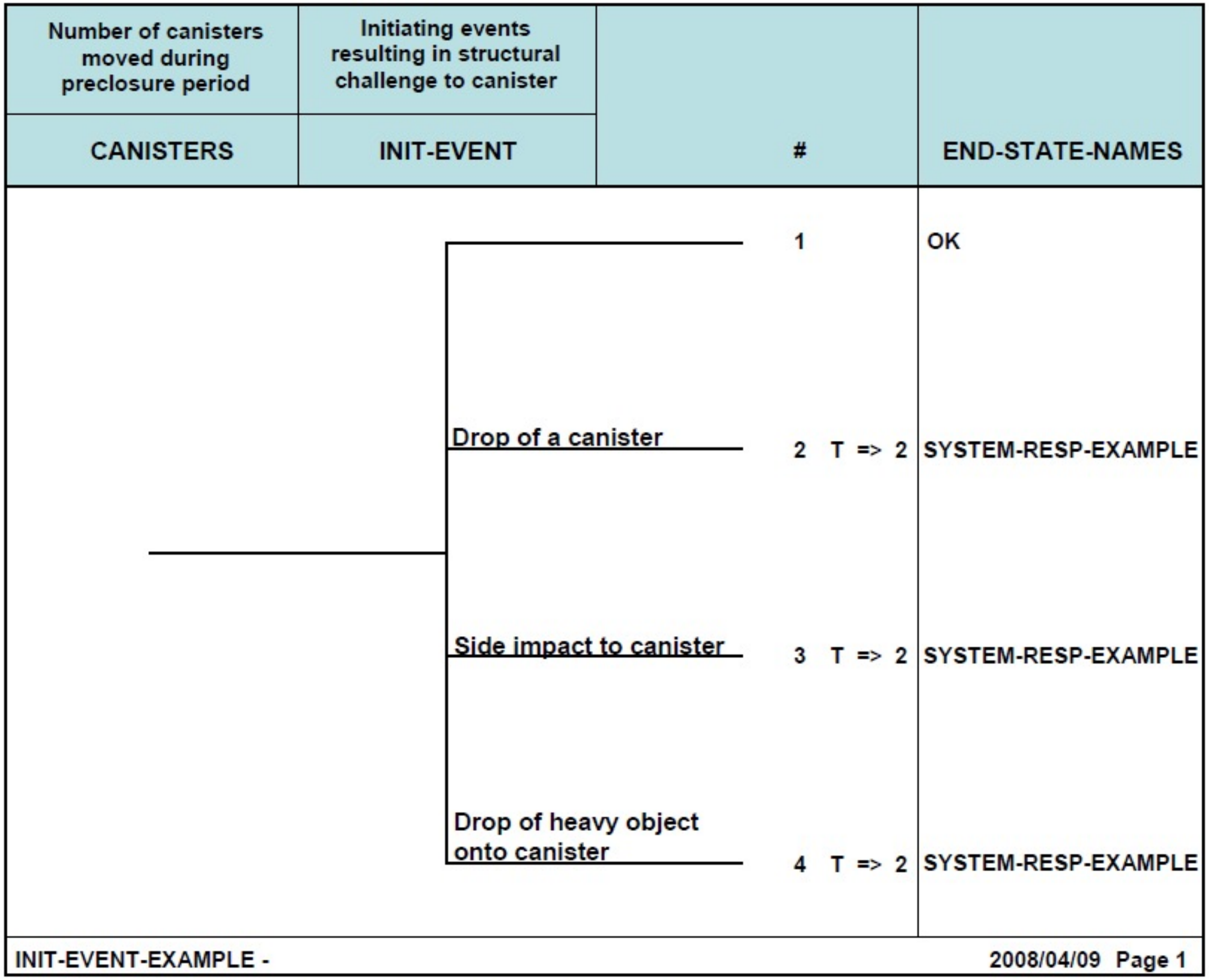


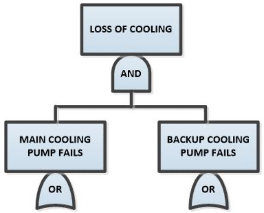




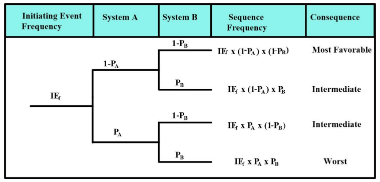
Initiating event tree example



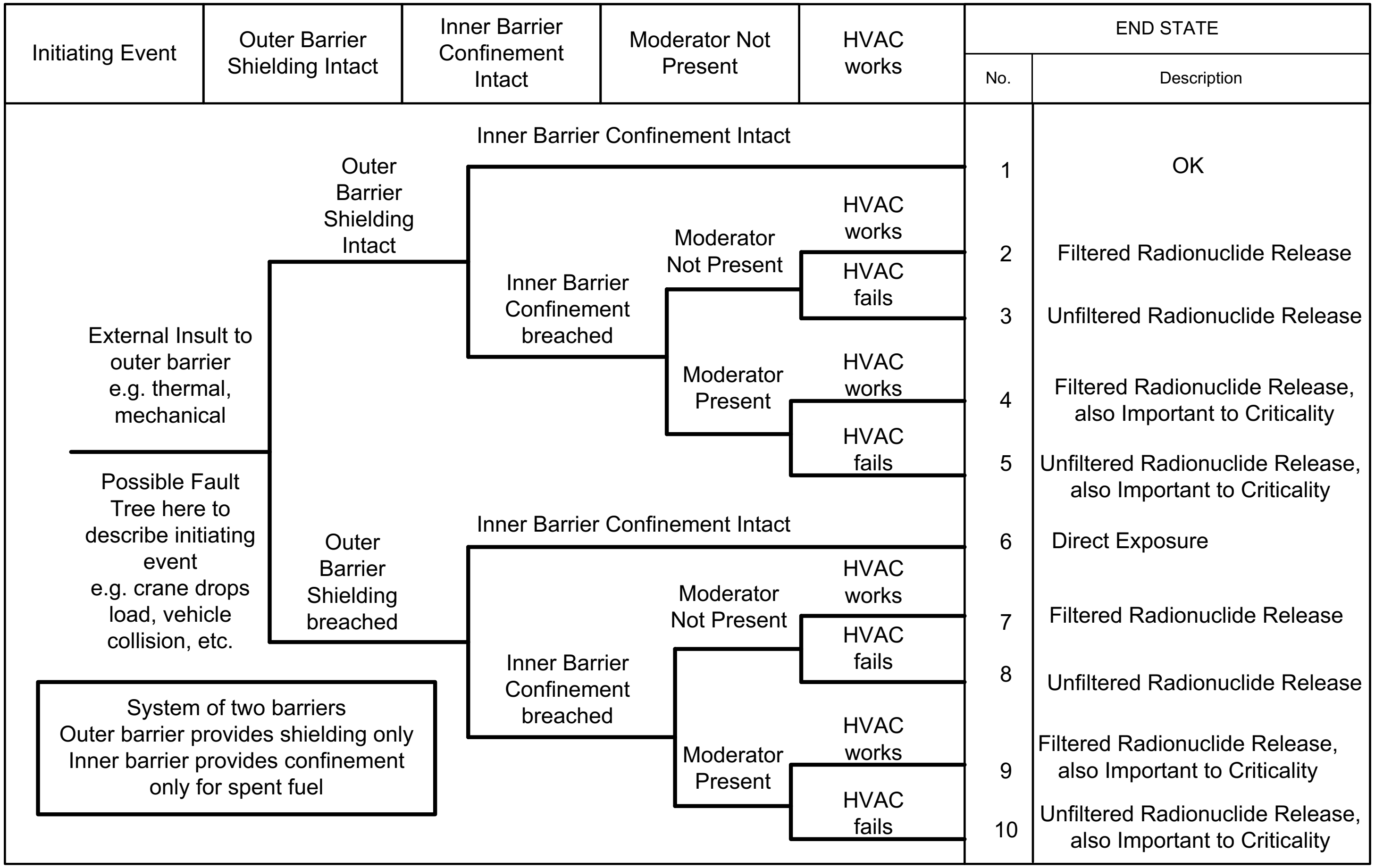


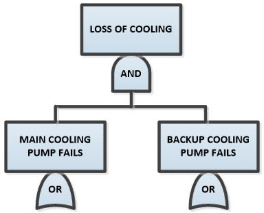


Generic Event Tree for Yucca Mountain Project

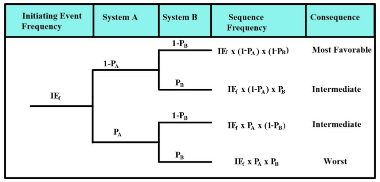


Generic Event Event for a System of Two Barriers with Moderator control and Heating, Ventilation and Air Conditioning (HVAC)

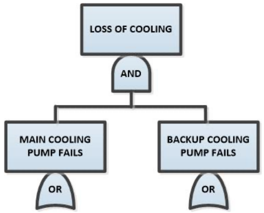




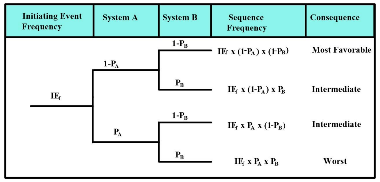
Wet Handling Facility – Preclosure YMP

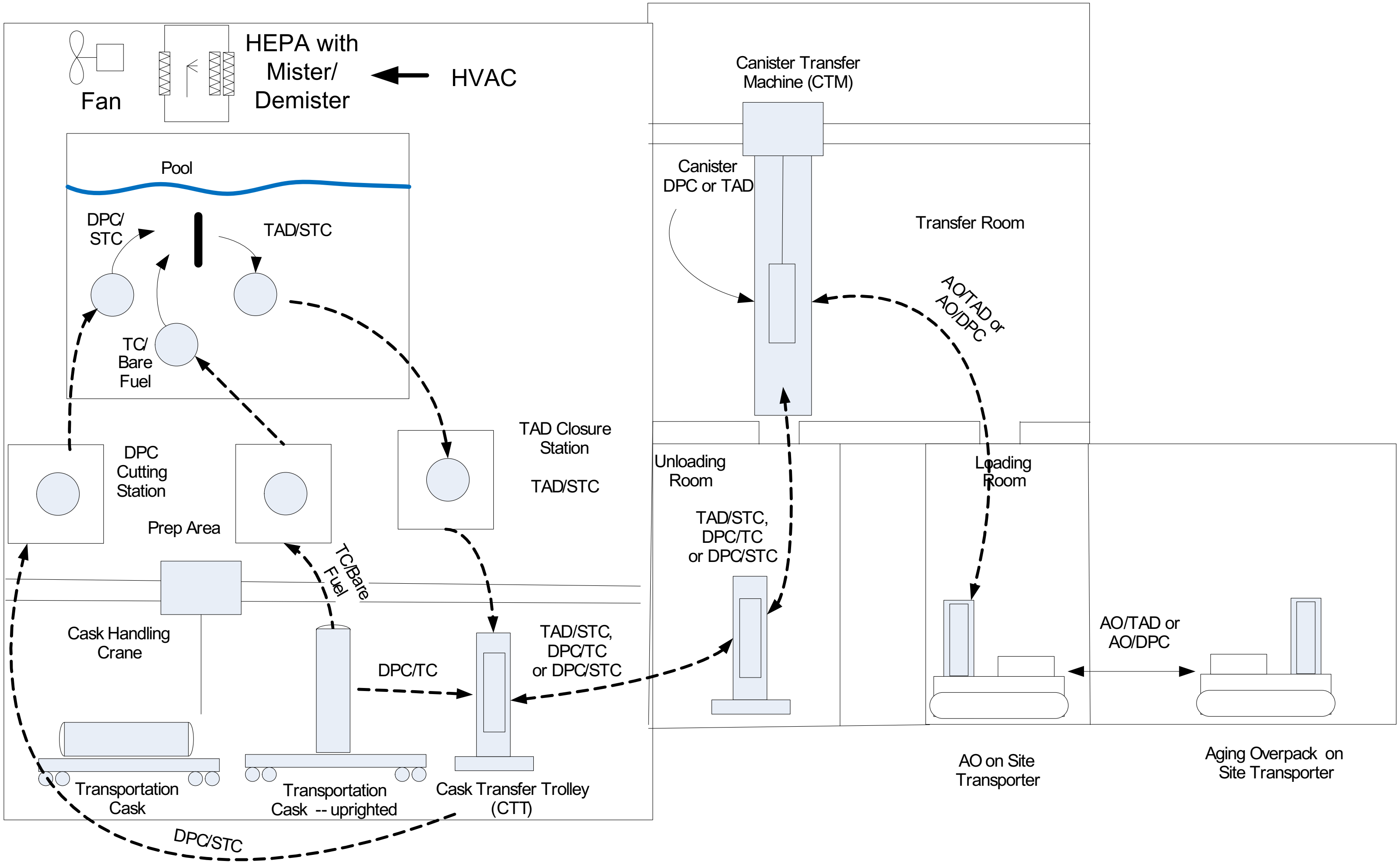


- A small percentage of spent nuclear fuel will not arrive at the repository in canisters called TADs, but will be shipped in transportation casks designed to handle individual assemblies of spent fuel rods.
- The Wet Handling Facility includes a pool of water in which spent fuel rods are removed from transportation casks, placed into TAD canisters and prepared for disposal or aging.

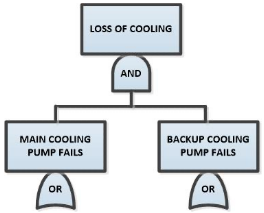


Wet Handling Facility -- Preclosure (YMP)

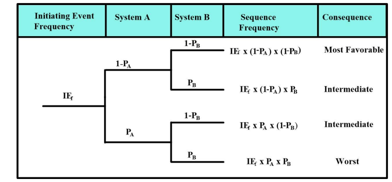


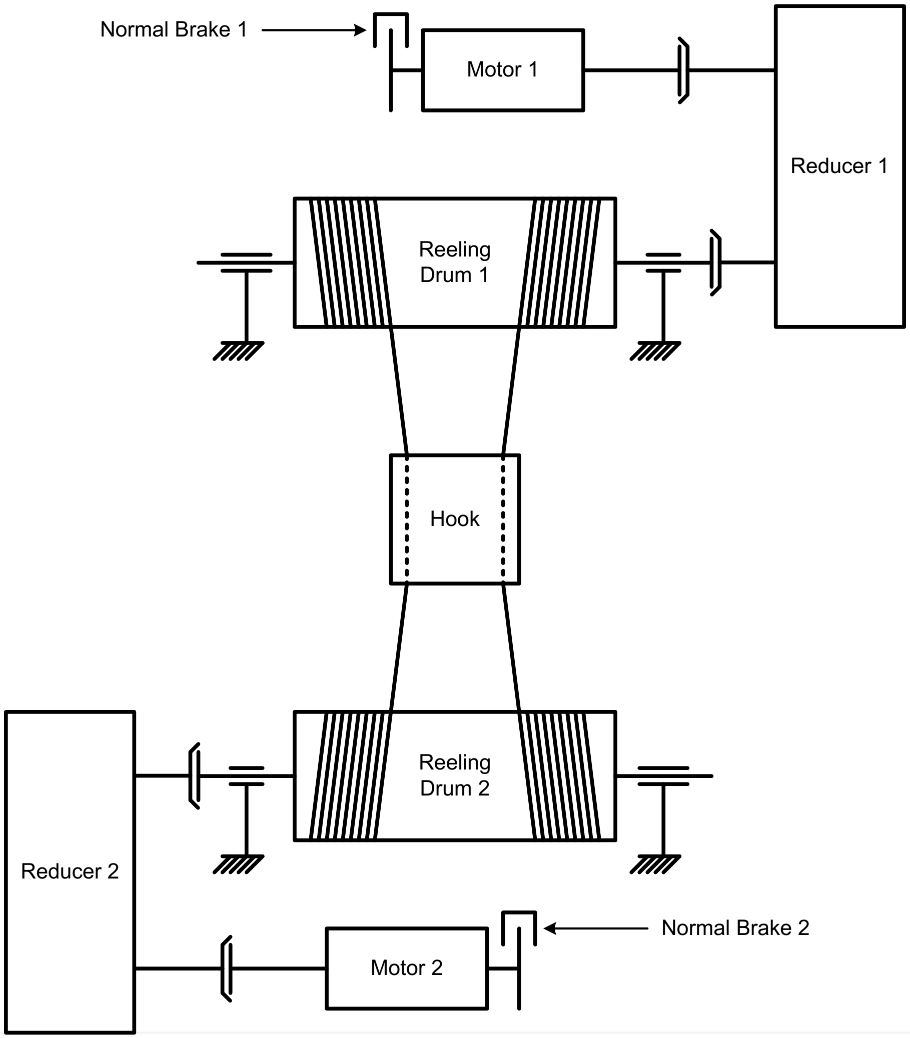


12 1

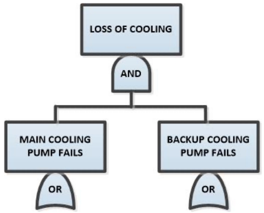


Single Failure Proof Crane

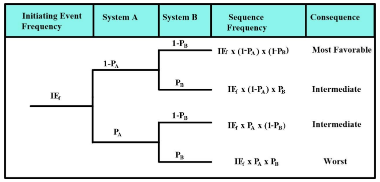


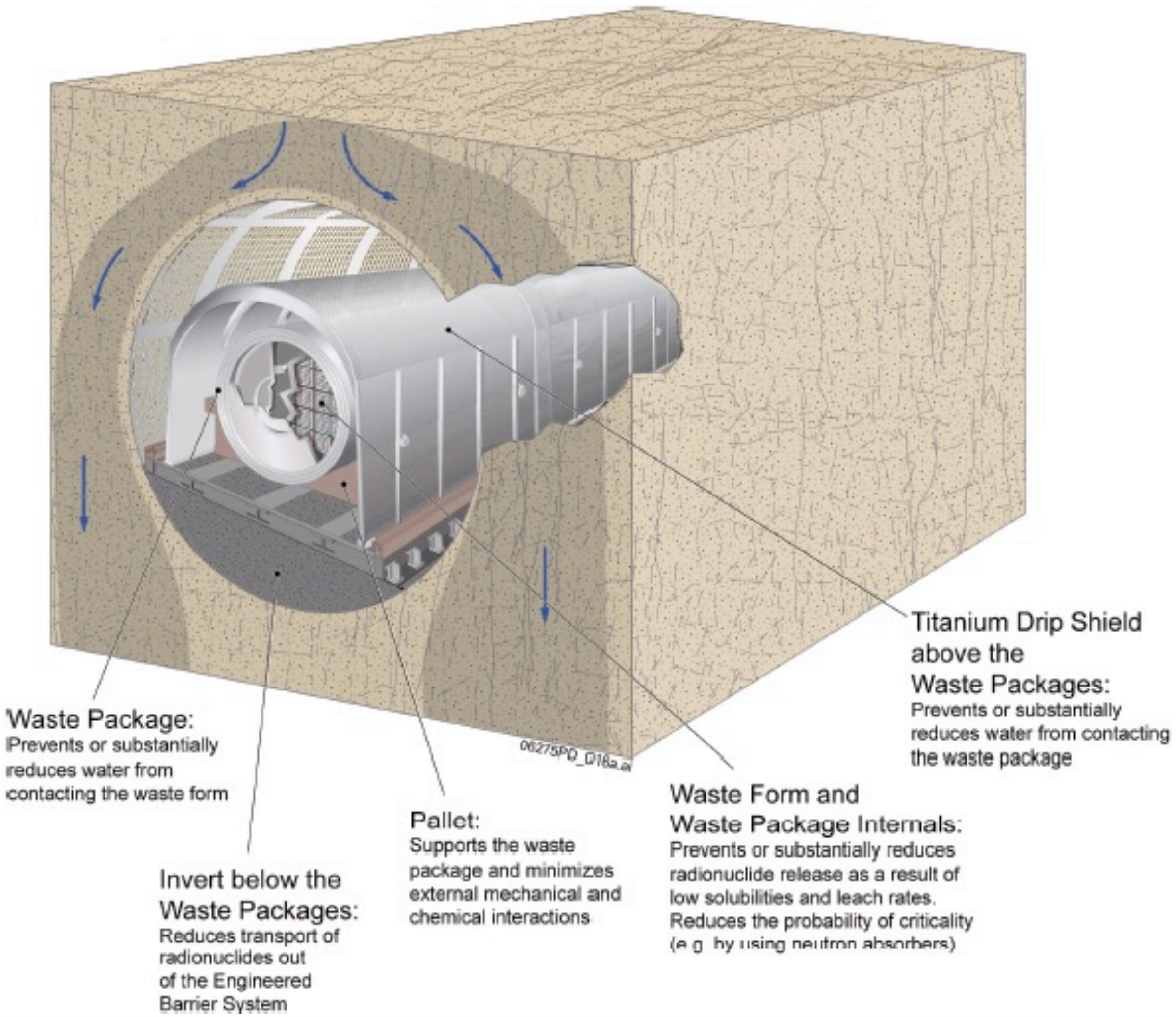


12
2



Postclosure – Engineered Barriers (YMP)





The Features of the Engineered Barrier System that Prevent or Limit the Movement of Water and Prevent or Substantially Reduce the Release of Radionuclides from the waste