LA-UR-10-03701

HAZARD EVALUATION TECHNIQUES

Julie Johnston

Ron Selvage

LANL Safety Basis Academy

Course Objective

Upon completion of this training, participants will possess a working knowledge and skills needed to perform a comprehensive assessment of facility hazards and to provide a qualitative risk perspective to help in decision making for risk reduction. Hazard evaluation techniques covered in this course include:

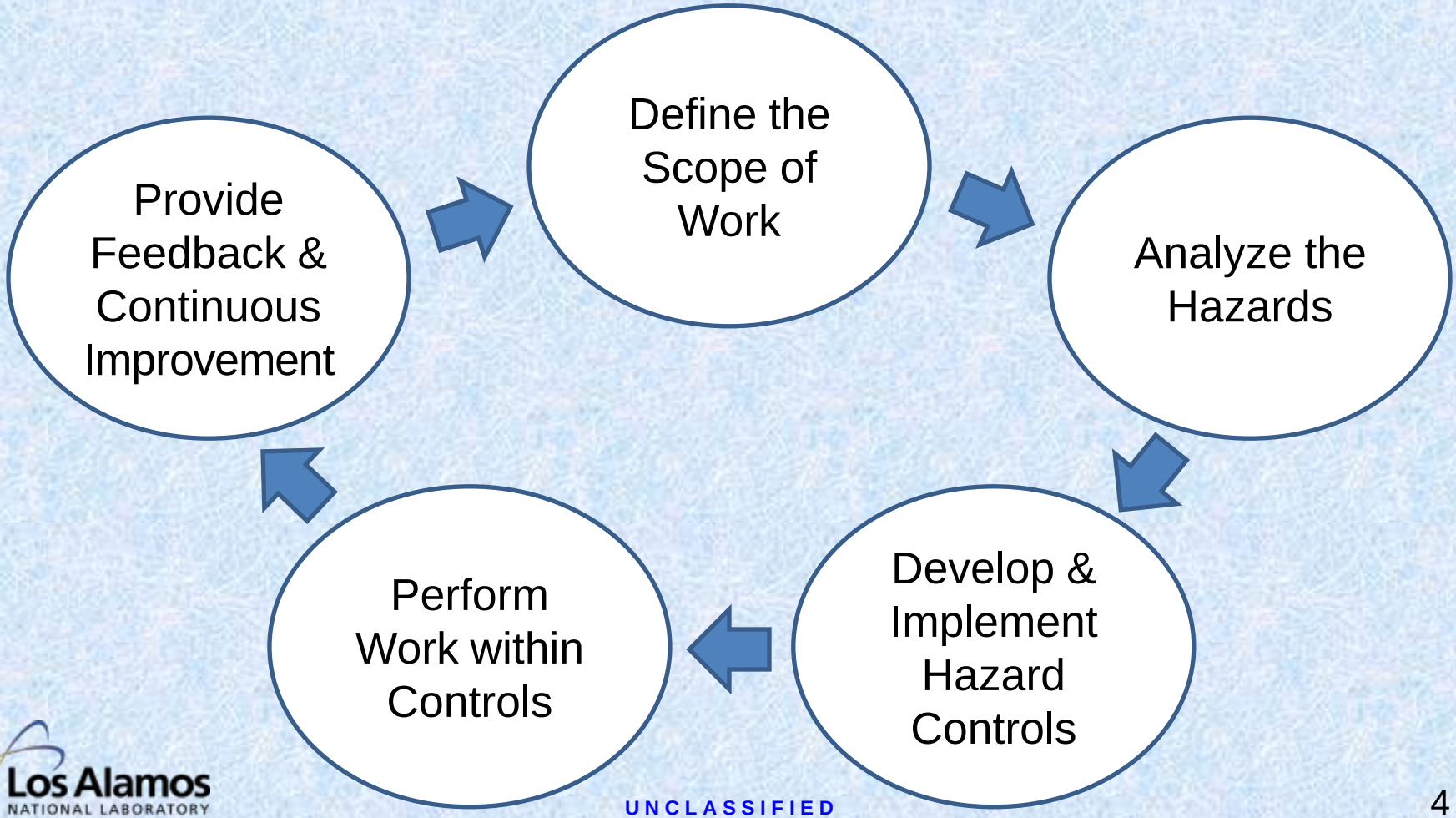
1. Checklist Analysis technique
2. What-If Analysis technique
3. Hazard and Operability (HAZOP) Analysis technique
4. Human Reliability Analysis techniques
5. Fault Tree Analysis technique
6. Event Tree Analysis technique

HAZARD EVALUATION TECHNIQUES

Pre-Start Hazard Evaluation Activities

Purpose and Applicability of HE

- Integrated Safety Management [DOE P 450.4]



Purpose and Applicability of HE

- DOE is committed to protecting workers, the public, and the environment.
- DOE wants reasonable assurance that we can do so.
- DOE is committed to integrated safety management.
- Hazards identification, hazards categorization, and hazards analysis are key components of integrated safety management for nuclear and non-nuclear DOE facilities and activities.
- The techniques presented in this class may be used for a wide variety of hazard analysis needs.

Philosophy of Hazards Evaluation

- Focus: three main activities
  - Hazard Identification
  - Hazard Categorization
  - Hazard Evaluation
- "Hazard means a source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to a person or damage to a facility or to the environment (without regard to the likelihood or credibility of accident scenarios or consequence mitigation)." [10 CFR 830.3]

Philosophy of Hazards Evaluation

- Outcomes
  - Hazard Identification Table(s) ,including hazard form, type, location & total quantity
  - Hazard Categorization, including results & basis
  - Hazard Evaluation, including hazard scenarios, frequency, consequence, & potential controls

Philosophy of Hazards Evaluation

- Hazard scenario development
  - How could an identified hazard cause harm to workers, the public, or the environment?
  - What could cause this sequence of events to happen?
  - Without prevention, what is the likelihood that this sequence of events could happen? (What is the scenario frequency?) This should be largely qualitative.
  - Without mitigation, what harm (consequences) could come to workers, the public, and the environment? This should be largely qualitative.
  - What controls might prevent (reduce the likelihood or probability of) this scenario from occurring?

Hazards Evaluation Pre-Start Activities

- Assemble the hazards evaluation team.
  - Team leader is key
  - Scribe
  - Include appropriate disciplines and organizations
    - Safety basis
    - Engineering (construction, systems, others)
    - Operations (both management and workers)
    - Safety disciplines (industrial safety, industrial hygiene, radiation safety, explosive safety, fire protection, criticality safety, etc.)
    - Other subject matter experts
  - Define roles and responsibilities

Hazards Evaluation Pre-Start Activities

- Gather baseline information and ensure that the information is under configuration control.
  - Facility location, surroundings
  - Facility design, configuration
  - Operational processes
  - Interfaces with other facilities or operations
  - Local conditions (geography, demography, meteorology, climatology, geology, hydrology, seismology, etc.)

Hazards Evaluation Pre-Start Activities

- Determine appropriate hazard analysis techniques.
  - Identify applicable requirements and objectives
  - Identify required outputs
  - Choose appropriate techniques
- Define frequency, consequence, & risk matrices
  - Need to cover normal operations, abnormal operations, & accident conditions
  - Need to be consistent with applicable requirements, desired outputs, and intended hazard evaluation techniques

Hazards Evaluation Pre-Start Activities

- Document project plan
  - Identify objectives and requirements
  - Identify project team
  - Define analysis scope
  - Define analysis methodology & structure
  - Define review process
  - Develop project schedule
  - Obtain approvals from appropriate parties

Frequency, Consequence, & Risk

- Typical frequency bins

Bin Name	Annual Likelihood of Occurrence (f)	Description
Frequent	$f \geq 10^{0}$	Incidents that are expected to occur frequently with normal operations
Anticipated	$10^{0} > f \geq 10^{-2}$	Incidents that may occur several times during the life of the facility
Unlikely	$10^{-2} > f \geq 10^{-4}$	Accidents that are not anticipated to occur during the life of the facility
Extremely Unlikely	$10^{-4} > f \geq 10^{-6}$	Accidents that are unlikely to occur during the life of the facility
Beyond Extremely Unlikely	$10^{-6} > f$	All other accidents

Frequency, Consequence, & Risk

- Typical radiation dose consequence bins

Bin Name	Public[1]	Collocated Worker[2]	Immediate Worker[3]
High	≥ 25 rem TEDE[4]	≥ 100 rem TEDE	Prompt death
Moderate	≥ 0.5 rem TEDE	≥ 5 rem TEDE	Serious injury
Low	< 0.5 rem TEDE	< 5 rem TEDE	< Serious injury

1. Public is represented by the maximally-exposed off-site individual (MEOI) or maximum offsite individual (MOI).
2. Collocated worker or non-involved worker is ≥ 100 m from the release.
3. Immediate worker is sometimes called the involved worker.
4. TEDE is the Total Effective Dose Equivalent (50-year).

Frequency, Consequence, & Risk

Likelihood ↑	Low	Moderate	High
Frequent	10	13	15
Anticipated	7	11	14
Unlikely	4	8	12
Extremely Unlikely	2	5	9
Beyond Extremely Unlikely	1	3	6

Worker Consequence →

Low Risk | Moderate Risk | High Risk

Hazard Scenario Risk

- Hazard scenarios should reflect qualitative frequency, consequence, and risk estimates without credit for prevention or mitigation.
- Aids in identifying the relative risk of each scenario.
- Aids in selecting bounding hazard scenarios for further analysis in accident scenarios.

Information Obtained in HE Process

- Facility
  - Site information
  - Buildings, structures, systems, components, design
  - Process design
  - Regulatory information
  - Other
- Hazards
  - Material hazards
  - Energy hazards
  - Process hazards
  - External man-made hazards
  - Natural phenomena hazards

Hazard Evaluation Team

- Three basic positions
  - Leader (project manager, experienced hazard analyst)
  - Scribe (document discussions, manage information)
  - Subject matter expert(s) (SMEs in design, construction, operation, & safety of the facility/operation)
- Minimum team is one person, but that's problematic.
- All hazard evaluation techniques are more thorough & effective when performed by team.
- Team with 3-8 members is usually best.
- Very large teams are problematic. Better to have a smaller core team, then consult with other SMEs.

Basic Hazard Evaluation Process

- Define scope
- Gather information
- Identify hazards
- Determine hazard category
- Evaluate hazards
  - Postulate hazard scenarios
  - Estimate likelihood of occurrence
  - Evaluate potential consequences
  - Identify controls to prevent or mitigate
  - Determine whether detailed accident analysis is needed
- Document results

Outputs of Hazard Evaluation Process

- Defense-in-Depth Controls
  - Structures, systems, and components
    - Barriers to contain uncontrolled hazardous material or energy release.
    - Preventive feature to protect the barriers
    - Systems to mitigate uncontrolled hazardous material or energy release upon barrier failure (e.g., ventilation zone confinement).
  - Specific administrative controls
    - Procedural restrictions or limits imposed.
    - Manual monitoring of critical parameters.
    - Responses or actions counted on to limit abnormal conditions, accident progression, or potential exposures.
  - Safety management programs
    - Preventive and mitigative programs

Elements of Hazard Analysis

- Identification of hazardous material and energy sources present by type, quantity, form and location
  - Foundation of all hazard and accident analysis.
  - Incomplete or inaccurate hazard identification will result in incomplete or inaccurate hazard and accident analysis, questionable controls, and will undermine confidence that the facility or activity can be conducted safely.

Elements of Hazard Analysis

- Identification of the spectrum of potential accidents at the facility in terms of qualitative consequence and frequency estimates
  - Identification of planned design and operational safety improvements
  - Defense in depth controls and safety structures, systems and components
  - Design and operational features that reduce the potential for large material releases to the environment
  - Identification of the limited set of unique and representative accidents
  - Identification and documentation of assumptions and initial conditions that are carried into accident analysis and formalized as controls

Include in Hazard Evaluation

- Facility processes and activities, both present and planned
  - Identify hazardous materials and energy sources for each step in each process and activity.
- Natural phenomena events (e.g., earthquakes, tornadoes, straight-winds, lightning strikes)
  - Identify hazard scenarios for each hazardous material and energy source for each step in each process and activity.
- Man-made external events (e.g., aircraft and vehicular impact)
  - Identify hazard scenarios for each hazardous material and energy source for each step in each process and activity.

Control Selection Process

- Explain the process used for selecting hazard controls to reduce/prevent the risk associated with facility accidents.
  - Preventive over mitigative
  - Engineered controls over administrative controls
  - Passive engineered controls (design features) over active engineered controls
  - Controls nearer the source are usually better than controls far from the source
  - Controls must be implementable
  - Controls should be practical

Plant/Facility Features

- Engineered features
  - Structures, systems, and components (e.g., buildings, walls, berms, fire alarm systems, fire suppression systems, HEPA-filtered exhaust systems, emergency generators).
- Administrative features
  - Specific administrative controls credited for preventing or mitigating a hazard or accident scenario (e.g., MAR controls, specific human action requirements).
  - Programmatic administrative controls not specifically credited with preventing or mitigating a hazard or accident scenario, but may provide defense-in-depth.

Plant/Facility Features

- Mitigating features
  - Reduce the consequences of an accident (e.g., containment structures, HEPA filtration, fire suppression, MAR limits).
- Preventive features
  - Reduce the likelihood (probability of occurrence) of a hazard or accident scenario (e.g., ignition source controls, combustible controls, inert atmosphere, criticality limits, lightning protection systems).

Differentiate

- Defense-in-depth
  - Layers of protection from the release of hazardous material so that no one layer, no matter how good, is completely relied upon.
  - Structures, Systems, and Components (SSCs) that provide a significant contribution to defense-in-depth for the public are designated as safety significant.
  - SSCs that provide a significant contribution to defense-in-depth for workers are not designated as safety significant, but they may be other (important to safety) controls not in the technical safety requirements.
  - Defense-in-depth may be provided by SSCs or Specific Administrative Controls (SACs), but SACs are not designated as safety significant, even though they may provide a significant contribution to defense-in-depth for the public.

HAZARD EVALUATION TECHNIQUES

Checklist Analysis Technique

Checklist Analysis: Description

- Uses a written list of items or procedural steps to verify the status of a system.
- Frequently used to verify compliance with standards and practices.
- Easy to use.
- Can be applied at any stage in a process's lifetime.
- Once developed, can be used by inexperienced personnel to familiarize themselves with a process.
- Provides a common basis for management review of the analyst's assessments of a process or operation.

Checklist Analysis: Description

- Generic hazard checklists are often combined with other hazard evaluation techniques to evaluate hazardous situations.
- Checklists are limited by their authors' experiences.
- They should be developed by authors with varied backgrounds who have extensive experience in the systems they are analyzing.
- Traditional checklists are used primarily to ensure compliance with standard practices.

Checklist Analysis: Purpose

- Checklists may be used as a means of hazard identification.
- Analysts may use a more general checklist in combination with another hazards evaluation technique (e.g., what-if/checklist) to discover common hazards that the checklist alone might miss.

Checklist Analysis: Results

- Standard checklists contain a series of questions that can be answered “yes”, “no”, “not applicable”, or “need more information”.
- Used to verify compliance with standard procedures.
- Used to identify deficient items needing maintenance, repair, replacement, or upgrade.
- May be used to identify hazards.

Checklist Analysis: Use

- Technical Approach
  - Traditional checklist analysis uses a list of specific items to identify known types of hazards, design deficiencies, and potential accident situations associated with common process equipment and operations.
  - Checklist analysis can be used to evaluate materials, equipment, or procedures.
  - Checklists are most often used with a design or process with which there is lots of experience.
  - Checklists may be used during the development of new designs or processes to identify or eliminate hazards like those found in similar designs or processes with which there is lots of experience.

Checklist Analysis: Use

- Technical Approach (continued)
  - Checklist generally confirms that a piece of equipment conforms with accepted standards.
  - Best if checklist is customized for a particular piece of equipment or process.
  - Analysis usually includes touring the process area and comparing equipment or process parameters against the checklist.
  - For equipment or processes not yet built, experienced personnel compare design documentation against checklist.

Checklist Analysis: Example 1

HAZARDS IDENTIFICATION CHECKLIST

Site: DOE Site XX **Building/Facility:** Building 1234 **Room:** 567 **Operations:** Part Fabrication

Hazard Type	Equipment/ Condition	Material Form	Quantity	Hazard Description	Standard Industrial Hazard (Y/N)	Potential to contribute to DSA accidents
Asphyxiant	Ar bottle, valve, hose, glovebox	Gas	90 CF	Equipment leaks, fill room with Ar	Y	
Mechanical	Ar hose/ coupling	Gas	NA	Hose whip if hose/coupling breaks	Y	
Flammable	Ar hose/ coupling	Solid	? amount of combustion products	Loss of inert glovebox; potential fire as part oxidizes with air	N	✓
Pressure	Ar bottle	Gas	2150 psi	Potential missile if Ar bottle valve breaks off; possible glovebox rupture	N	✓
Work Environment	Lathe metal shavings	Solid	NA	Cut hazard	Y	
Thermal	Lathe part		NA	Inadvertently touch part that is “hot” from machining (causing glove to burn or operator to rip glove)	Y	✓

Checklist Analysis: Example 1

HAZARDS IDENTIFICATION CHECKLIST

Site: DOE Site XX **Building/Facility:** Building 1234 **Room:** 567 **Operations:** Part Fabrication

Hazard Type	Equipment/ Condition	Material Form	Quantity	Hazard Description	Standard Industrial Hazard (Y/N)	Potential to contribute to DSA accidents
Flammable	Lathe/ cleaner	Liquid	0.5 L	Cleaner put on hot part / lathe and catches on fire	Y	✓
Electrical	Lathe power cord		110 V	Frayed cord creates shock hazard	Y	
Pressure	Hydraulic control hose		NA	Hose whip if hose/coupling fails	Y	
Flammable	Hydraulic fluid	Liquid	4 L	Hydraulic fluid peaks and contacts hot part	Y	✓
Toxic	Machining	Solid	? amount of combustion products	Loss of inert atmosphere during operation. Chips ignite releasing toxic combustion products exposing operators.	N	✓
Toxic	Material handling	Solid	400g	Chips removed from glovebox are dropped, exposing operator to process material	N	✓
Criticality	Glovebox	Solid	> 400g	Overload the glovebox with excess Special Nuclear Material	N	✓

HAZARD EVALUATION TECHNIQUES

What-If Analysis Technique

What-If: Description

- What-If analysis technique is a **creative brainstorming** approach to hazards evaluation.
- Group of experienced people familiar with the subject process ask questions or voice concerns about possible undesired events.
- Not highly structured like HAZOP analysis or FMEA.
- Leader needs to guide group to ensure thorough coverage of the required scope.
- Frequently used with good results.
- Powerful technique if HE team is experienced; otherwise, results are likely to be incomplete.

What-If: Description

- HE team thinks of questions that begin with “What-If.” However, any process safety concern can be voiced, even if it is not phrased as a question.
- May address any normal, abnormal, or accident condition.
- Scribe records all of the questions and concerns on a chart pad, marking board, or word processor.
- Questions are divided into logical groups based on subject matter, discipline, or consequence.
- Each question is addressed by a team of one or more subject matter experts.
- Suggest alternatives for risk reduction.

What-If: Purpose

- What-If analysis identifies hazards, hazardous situations, and accident events that could produce undesirable consequences.
- Can examine deviation from the design, construction, modification, or operating intent.
- Simple technique — can be performed more quickly than most other hazard evaluation techniques.
- Can be performed at any stage in the life of a facility or process.

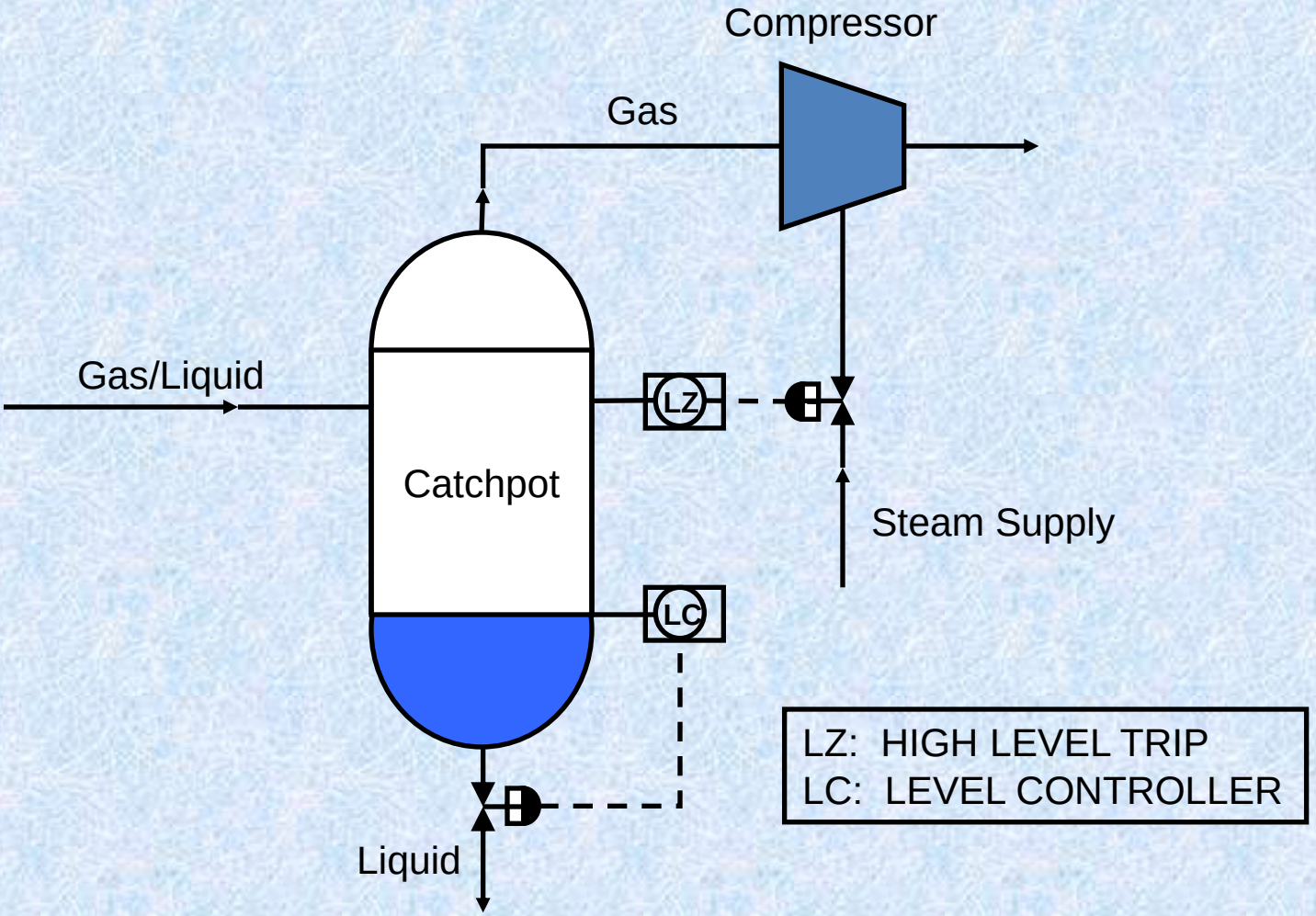
What-If: Results

- Generates a list of questions and answers.
- May also produce a list of hazardous situations, their consequences, potential controls, and recommendations.
- No frequency, consequence, or risk estimates or ranking.

What-If: Use

- Performing the review
  - Meeting should begin with explanation of the scope and methodology.
  - Facility or process SME should explain the process, including safety precautions, safety equipment, and health control procedures.
  - Facility or process is reviewed and HE team members ask “What-If” questions or raise concerns about things that could go wrong or cause a bad result.
  - Issues are recorded on a chart pad, on a marking board, or a computer (preferably connected to a projector so everyone can see).

What-If: Exercise



HAZARD EVALUATION TECHNIQUES

Failure Modes and Effects Analysis (FMEA) Technique

FMEA: Description

- Failure Modes and Effects Analysis (FMEA) tabulates failure modes of equipment (including improper operation) and their effects on a system or plant.
- Failure mode describes how the equipment fails (open, closed, on, off, leaks, ruptures, sticks, etc.).
- FMEA identifies single failure modes that directly result in or significantly contribute to an accident.
- FMEA is not efficient for identifying an exhaustive list of combinations of equipment failures that lead to accidents.
- Human operator errors are usually not directly evaluated with FMEA, but may result in equipment failure.

FMEA: Purpose

- Identifies single equipment and system failure modes and the effect of failure on the system or plant.
- Provides recommendations for increasing equipment reliability, thus improving process safety.

FMEA: Results

- Table identifying each piece of equipment or system, failure modes, failure effects, qualitative estimate of worst-case consequences, and recommended changes to improve reliability and/or safety.

FMEA: Resource Requirements

- Need equipment list or P&ID, knowledge of equipment functions and failure modes, knowledge of system or plant function and response to equipment failures.
- FMEA can be performed by single analyst, but results should be reviewed by others to ensure accuracy and completeness.
- Staff requirements vary with the size and complexity of equipment being analyzed.

FMEA: Use

- Technical approach
  - FMEA evaluates the ways equipment can fail (or be improperly operated) and the effects these failures can have on a process or a facility.
  - Each individual failure is usually considered as an independent occurrence with no relation to other failures in the systems, except for subsequent effects that it may produce.
  - Common cause failures are sometimes considered.
  - Usually a qualitative technique, but it can be used to rank failure consequence severity.

HAZARD EVALUATION TECHNIQUES

Preliminary Hazards Analysis (PHA) Technique

PHA: Description

- Preliminary Hazard Analysis (PHA) was derived from U.S. Military Standard, *System Safety Program Requirements* [MIL-STD-882B].
- PHA formulates a list of hazards and hazard scenarios by considering:
  - Hazardous materials and energy sources, including raw materials, intermediate and final products, and their properties;
  - Facility layout and plant equipment;
  - Operating environment;
  - Operating activities, including testing, maintenance, etc.; and
  - Safety-related interfaces among elements of the system.

PHA: Description

- Each hazard scenario is qualitatively evaluated for likelihood and consequences to develop a qualitative risk ranking.
- Controls to prevent or mitigate each hazard scenario are proposed.
- Qualitative risk ranking is used to prioritize any recommendations for improving safety that emerge from the analysis.

PHA: Purpose

- Often used in the conceptual or preliminary design phase of a facility or process to aid in site selection and to make facility and process design decisions at a time when the cost and schedule impacts of safety improvements is minimized.
- Can also be used on an existing facility or process to identify and rank hazards and hazard scenarios and prioritize safety improvements when a more sophisticated technique is not warranted or possible.
- Useful in situations where experience provides little or no insight into potential safety problems.

PHA: Purpose

- Does not preclude the need for further hazards analysis.
- Often a precursor to further (more detailed) hazard and accident analysis.

PHA: Use

- Technical approach
  - Identify hazards. May screen insignificant hazards.
  - Create hazard scenarios.
  - Qualitatively evaluate hazard scenario likelihood (without prevention, consequences (without mitigation), and resulting risk.
  - Identify controls to prevent or mitigate each hazard scenario.
  - Document the results.
  - Review and approval.

HAZARD EVALUATION TECHNIQUES

Hazard and Operability (HAZOP) Analysis Technique

HAZOP: Description

- HAZOP technique was developed by Imperial Chemical Industries (ICI) to identify and evaluate safety hazards in a chemical process plant and to identify operability problems that could hinder plant productivity.
- Originally intended for technology for which there was little experience, but it also works well with existing operations.
- Requires detailed source of information about the design and operation of a process, so it is not useful until after the detailed design stage.
- Creative systematic approach to identify hazard and operability problems resulting from deviations from the process design intent.

HAZOP: Description

- HAZOP leader systematically guides an interdisciplinary team through the plant design using “guide words” applied to “process parameters” at “study nodes” resulting in deviations.
  - Guide words: no, less, more, part of, as well as, reverse, other than.
  - Process parameters: flow, time, frequency, mixing, pressure, composition, viscosity, addition, temperature, pH, voltage, separation, level, speed, information, reaction.
  - Study nodes: points throughout the process.
  - Examples: No + Flow = No Flow; Less + Flow = Less Flow.
- Team agrees on possible causes for the deviation, consequences, controls, and recommendations.

HAZOP: Purpose

- HAZOP carefully reviews a process or operation in a systematic fashion to determine whether process deviations can lead to undesirable consequences.
- HAZOP can be applied to continuous or batch processes.
- HAZOP can be adapted to evaluate written procedures.
- When HAZOP team determines that inadequate controls exist for a credible deviation, it usually recommends actions to reduce the risk.

HAZOP: Use

- Technical approach
  - HAZOP uses a prescribed protocol to methodically evaluate the significance of deviations from the normal design intention.
  - HAZOP is based on the principle that several experts with different backgrounds can interact in a creative, systematic fashion, and identify more problems when working together than when working separately and combining their results.
  - This same principle is beneficial to other HE techniques as well, but it is at the core of HAZOP.
  - This is why HAZOP cannot be performed by a single individual.

HAZOP: Use

- Performing the review
  - Select a “study node” (a process section or operating step).
  - Explain the design intention of the study node.
  - Select a process variable or task in the study node.
  - Apply guide word to process variable or task to develop a meaningful deviation. (Discard non-meaningful deviations.)
  - Examine consequences associated with the deviation (assuming controls fail).
  - List all possible causes of the deviation.
  - Identify existing controls to prevent the deviation.
  - Assess the acceptability of the risk based on the consequences, causes and controls.

HAZOP: Use

- Performing the review (continued)
  - Identify action items improving safety or productivity.
  - Repeat for all guide words on that process variable or task.
  - Repeat for all process variables or tasks in that study node.
  - Repeat for all study nodes.
  - HAZOP team probably needs to meet again to review report.

HAZOP: Example

- The following table was used to evaluate parameter variations to determine which variations needed to be developed into nuclear criticality scenarios.

HAZOP: Example

Parameter/ Guide Word	Mass	Enrich.	Chem. Form	Phys. Form	Moderation	Geometry	Spacing	Config.	Poisons	Reflection
None…	NC	NC	NC	NC	NC	NC	Sca	NA	NC	NC
More of…	SCb	SCc	NA	NA	SCd	NA	NC	NA	NC	Sce
Less of…	NC	SCf	NA	NA	NC	NC	SCh	NA	NA	NC
Part of…	NP	NP	NP	NP	NA	NA	NA	NP	NA	NA
As well as…	NP	NP	NP	NP	NP	NP	SCbb	NP	NC	NA
Reverse…	NA	NA	NA	NC	NA	NA	NA	NA	NA	NA
Other than…	NA	NA	SCw	SCx	SCy	SCz	NC	NC	NC	NA

SC#: Scenario Number

NC: No Nuclear Criticality Safety Concern

NP: Normal Procedure

NA: Not Applicable

HAZARD EVALUATION TECHNIQUES

Human Reliability Analysis Technique

Human Reliability Analysis: Description

- Human reliability analysis (HRA) is a general term for methods by which the probability of human errors is estimated for any aspect of research, design, construction, operations, maintenance, management, etc.
- HRA may be qualitative or quantitative. A useful HRA technique will yield qualitative information that can be used as the basis for recommending safety or operability improvements, regardless of whether any quantitative analysis is performed. If quantification is required, a useful technique should yield valid and consistent estimates of human performance characteristics necessary for quantitative risk assessment, such as response times, human error probabilities, and uncertainties.

Human Reliability Analysis: Description

- The reliability of human performance is influenced by many factors. These are called performance shaping factors (PSFs).
- Human reliability analysis is used to identify and improve PSFs to reduce the likelihood of human errors.
- In most cases, HRA is performed in conjunction with or following a hazards analysis of an entire system, and focuses on areas identified by that hazards analysis where human errors can initiate or exacerbate an accident.

Human Reliability Analysis: Description

- Major limitations of HRA
  - **Completeness**: There can never be a guarantee that all human errors, extraneous acts, and recovery factors have been considered, nor that everything affecting human behavior has been considered.
  - **Validity/Specificity**: Probabilistic failure models cannot be completely verified. Human behaviors are observed in experiments and used in model correlations, but models are, at best, approximations of specific circumstances. Some HRA models are based on debatable assumptions about human behavior. The HRA may not provide a good representation of specific plant tasks and PSFs.

Human Reliability Analysis: Description

- Major limitations of HRA (continued)
  - **Accuracy/Uncertainty**: The lack of specific data on human error probabilities, PSFs, and accident diagnosis models severely limits accuracy and can produce large uncertainties, especially for prediction of very low-probability human behavior.
  - **Reproducibility/Bias**: Various aspects of HRAs are highly subjective — the results are very sensitive to the analyst's assumptions. The same problem, using identical data and models, may generate widely varying answers when analyzed by different experts, or by the same expert at different times.
  - **Traceability/Scrutability**: Attempting to understand all of the detailed documentation of an analyses that led to the HRA results can be an overwhelming, tedious task.

Human Reliability Analysis: Purpose

- The potential human errors associated with specific tasks and their effects must be identified so appropriate preventive measures and/or recovery factors can be identified and implemented.
- Estimates of human error probabilities are needed as input for cost/benefit studies of alternative designs, procedures, or policies.
- Estimates of human error probabilities are needed as input for quantitative risk assessments.

Human Reliability Analysis: Results

- List of errors likely to be encountered during normal or emergency operations and their consequences.
- Factors contributing to such errors.
- Proposed system modifications to reduce the likelihood of such errors.
- May include a ranking of errors based on probability of occurrence, consequence, or risk.
- Results may be qualitative or quantitative.

Human Reliability Analysis: Resources

- HRA is typically performed by one or two analysts skilled in HRA.
- Need access to plant layout, function, control panel layout, alarm panel layout, procedures, etc.
- Also need access to plant workers. Analysts will probably interview workers to find out how work is really performed.
- Time and resources required for HRA depends on scope and level of detail desired.

Human Reliability Analysis: Use

- Technical Approach
  - Technical approach is determined by the project team after the study objectives and scope have been defined.
  - A variety of HRA techniques are available and the selection of the appropriate technique(s) depends on the objectives of the study, the scope of the study, and the sources of data available for the study.
  - Depending on the study objectives, the HRA will involve one or more of the following basic steps:
    - Human factors engineering evaluation;
    - Task analysis;
    - Quantification; and
    - Sensitivity and uncertainty analysis.

Human Reliability Analysis: Use

- Analysis Procedure
  - Preparing for the review
    - Gather the information and resources identified in the HRA charter.
  - Performing the Review
    - Human factors engineering evaluation (collecting data, inspecting the facility, and evaluating the general PSFs that will influence the workers);
    - Task analysis (dissect worker tasks to identify specific potential errors of omission or commission);
    - Quantification (e.g., constructing event trees and assigning human error probabilities for each potential error); and
    - Sensitivity and uncertainty analysis (show how assumptions or boundary conditions would alter the HRA results).

HAZARD EVALUATION TECHNIQUES

Fault Tree Analysis Technique

Fault Tree Analysis: Description

- Fault tree analysis is a deductive technique that focuses on one particular accident or main system failure (called the top event) and provides a method for determining causes of that event.
- The fault tree is a graphical model that displays the various combination of equipment failures and human errors that can result in the main system failure of interest.
- It is a **qualitative** tool that allows the hazard analyst to focus preventive controls on the significant basic causes to reduce the likelihood of an accident.
- Fault tree analysis can be used **quantitatively** as a part of probabilistic risk analysis.

Fault Tree Analysis: Purpose

- The purpose of a fault tree analysis to identify combinations of equipment failures, human errors, and other events that can result in an accident.
- Often used when another HE technique has pinpointed an important accident of interest that requires more detailed analysis to determine causes and preventive controls.
- Well suited to complex, highly redundant systems, and systems vulnerable to **multiple failures**.
- For systems particularly vulnerable to a single failure that can lead to accidents, single-failure techniques (FEMA, HAZOP) may be used.

Fault Tree Analysis: Results

- Fault tree analysis produces failure logic models that use Boolean logic gates (e.g., AND, OR) to describe how equipment failures and human errors can combine to cause a main system failure.
- Fault tree models may be simple or very large and complex.
- The fault tree analyst usually solves the logic model to generate a list of failures, called minimal cut sets, that can result in the top event.
- Qualitatively, cut sets containing more failures are generally less likely than those containing fewer failures.

Fault Tree Analysis: Results

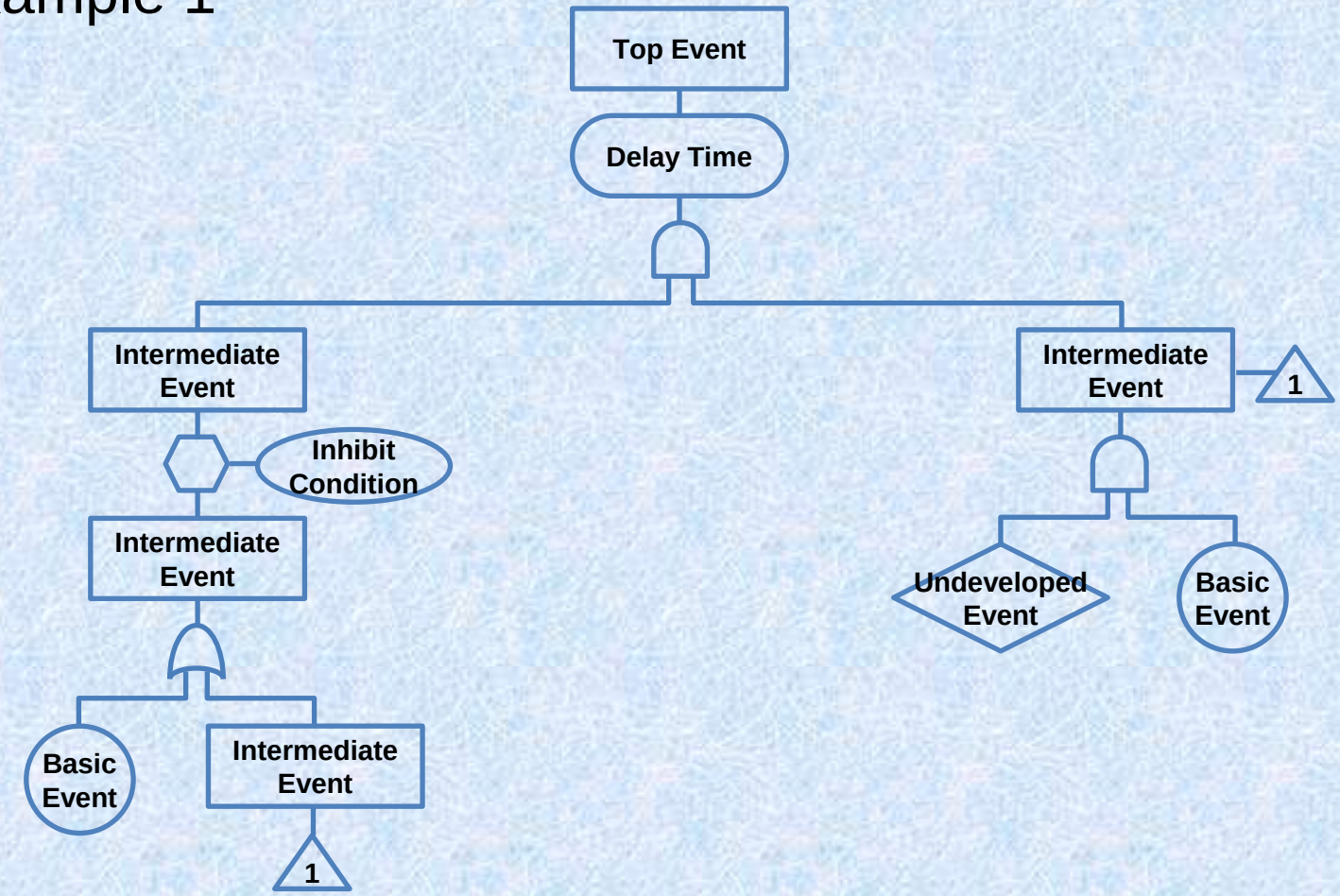
- Can associate frequencies with initiating events and calculate the frequency of the top event. This is one form of probabilistic risk analysis.

Fault Tree Analysis: Resources

- Fault tree analysis requires a detailed understanding of how the plant or system functions, detailed process drawings and procedures, and knowledge of component failure modes and their effects.
- Fault trees can be created by a single analyst who understands the system to be analyzed, but a team approach helps to ensure a broader understanding to achieve completeness.
- Time and cost of a fault tree analysis depends on the scope and complexity of the system being analyzed.

Fault Tree Analysis: Use

- Example 1



Fault Tree Analysis: Use

- Analysis Procedure
  - Define the scope to be analyzed.
    - Define the top event
    - Define boundary conditions for the analysis. These boundary conditions include:
      - System physical bounds
      - Level of resolution
      - Initial conditions
      - Not allowed events
      - Existing conditions
      - Other assumptions

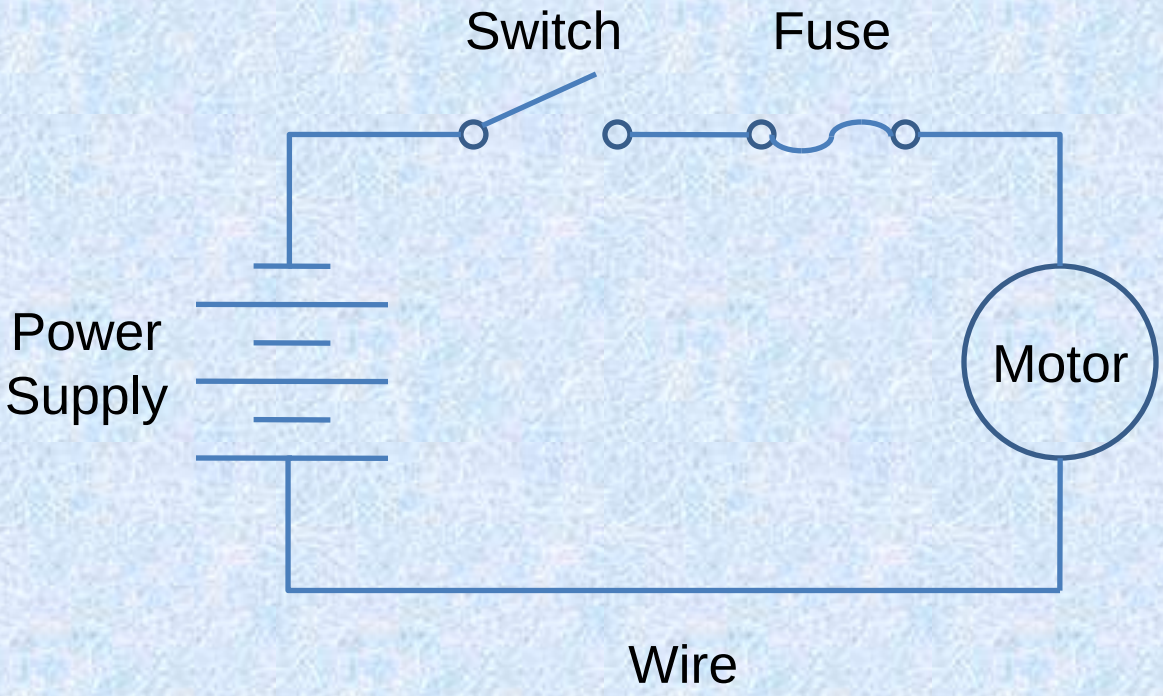
Fault Tree Analysis: Use

- Analysis Procedure
  - Construct the fault tree.
    - Start at the top event
    - Proceed down each branch through logic gates and intermediate events until you reach the basic events or the defined system boundary.
    - Follow rules for constructing fault trees.

Fault Tree Analysis: Use

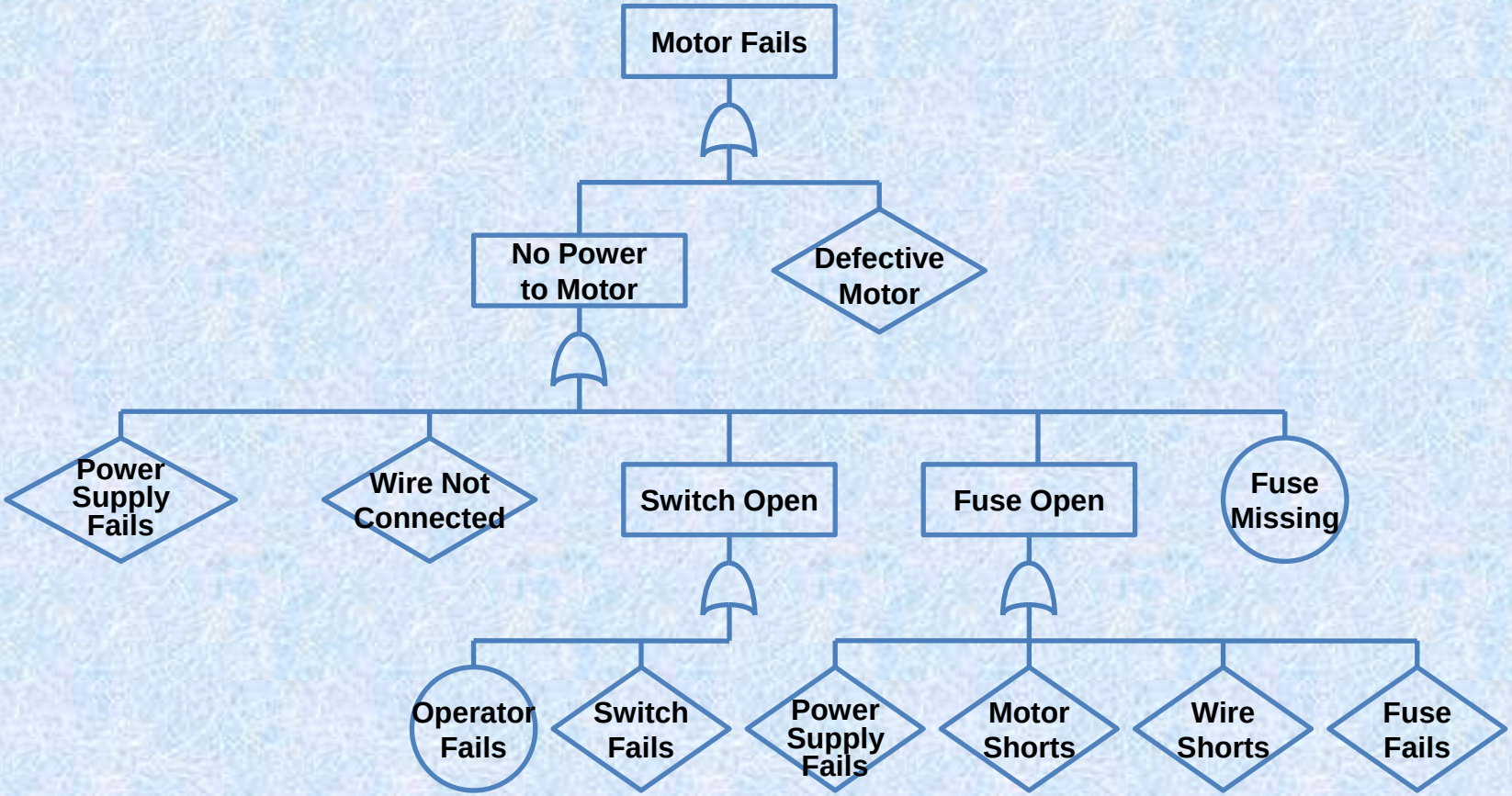
- Analysis Procedure
  - Document the results.
    - Describe the system analyzed.
    - Discuss the problem definition.
    - List assumptions
    - Identify fault tree model(s) developed.
    - List the minimal cut sets.
    - Discuss the significance of the cut sets
    - Identify any recommendations.

Exercise 1.1 – Motor Failure Fault Tree



- Top Event: Motor fails to operate
- Create a fault tree to explore why.

Exercise 1.1 – Potential Answer



HAZARD EVALUATION TECHNIQUES

Event Tree Analysis Technique

Event Tree Analysis: Description

- Event tree analysis is a inductive technique that starts with one initiating event (e.g., a specific equipment failure or human failure) and develops the possible sequences from that initiating event that could result in an accident.
- The event tree is a graphical model that evaluates both failures and successes of preventive and mitigative controls when determining the accident's potential outcomes.
- Event tree analysis can be used quantitatively as a part of probabilistic risk analysis.

Event Tree Analysis: Purpose

- Event trees are used to identify the various accident outcomes that can occur in a complex process.
- After these accident sequences are identified, the specific combinations of failures that can lead to the accidents can be determined using Fault Tree Analysis.
- Frequency, consequence, and risk can be calculated for each branch of the event tree.

Event Tree Analysis: Results

- Event tree analysis produces the event tree model and the safety system successes or failures that lead to each outcome.
- Accident sequences from the event tree can be input to a fault tree model for further analysis.
- The results help to identify design and procedural weaknesses and form the basis for recommendations for reducing the likelihood and/or consequence of the potential accident scenarios.

Event Tree Analysis: Results

- Can associate frequencies with initiating events and conditional probabilities with each safety function to calculate the frequency of the accident sequence. This is one form of probabilistic risk analysis.

Event Tree Analysis: Resources

- Event tree analysis requires a knowledge of potential initiating events and an understanding of safety system functions and emergency procedures that might mitigate the effects of each initiating event.
- Event trees can be created by a single analyst who understands the system to be analyzed, but a team approach helps to ensure a broader understanding to achieve completeness.
- Time and cost of a event tree analysis depends on the scope and complexity of the system being analyzed.

Event Tree Analysis: Use

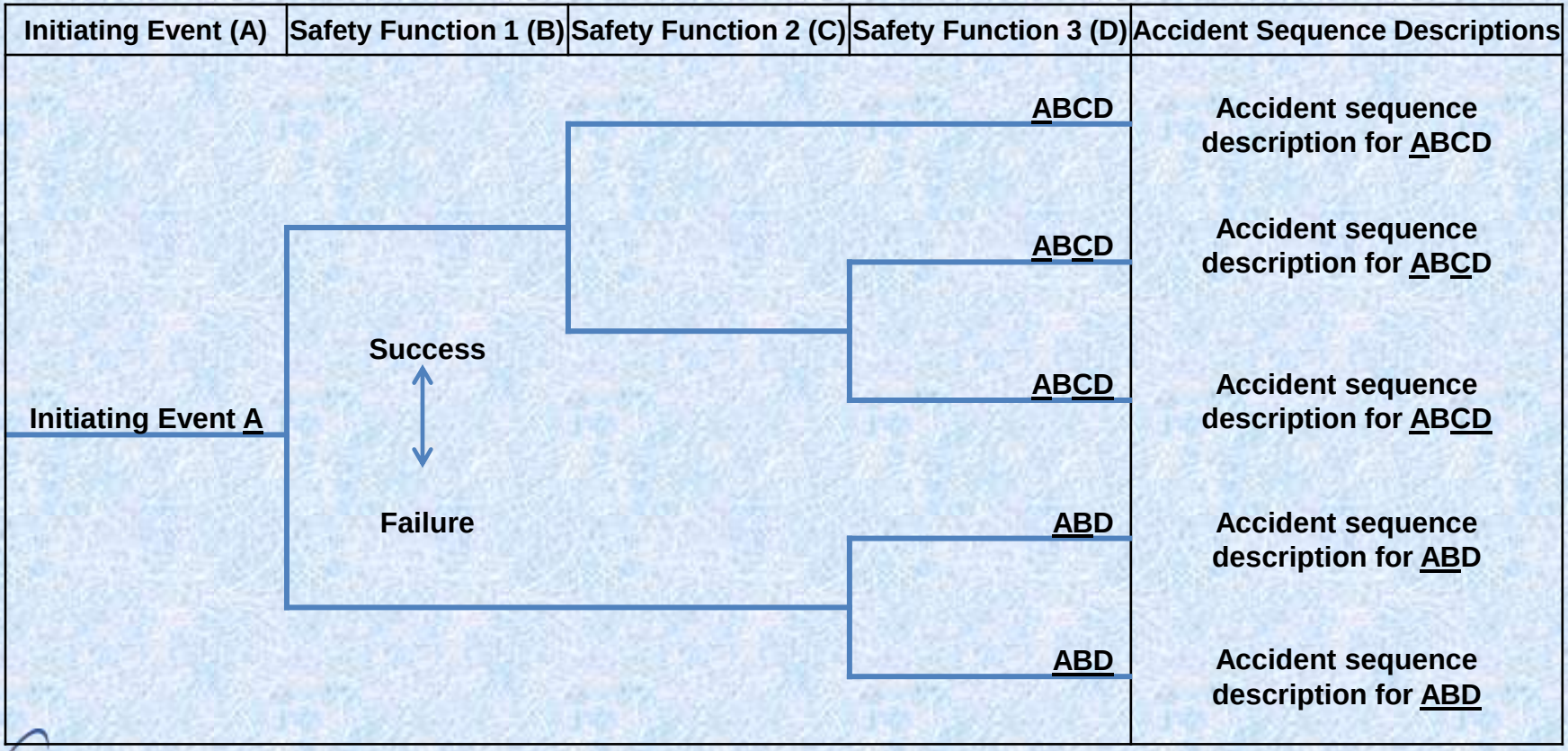
- Technical Approach
  - Start from an initiating event, then identify controls that could mitigate the consequences of that initiating event.
  - Evaluate the consequences of the success or failure of each successive control.
  - Each branch of the event tree represents a separate accident sequence.
  - Event trees are well-suited for analyzing initiating events that could result in a variety of outcomes.

Event Tree Analysis: Use

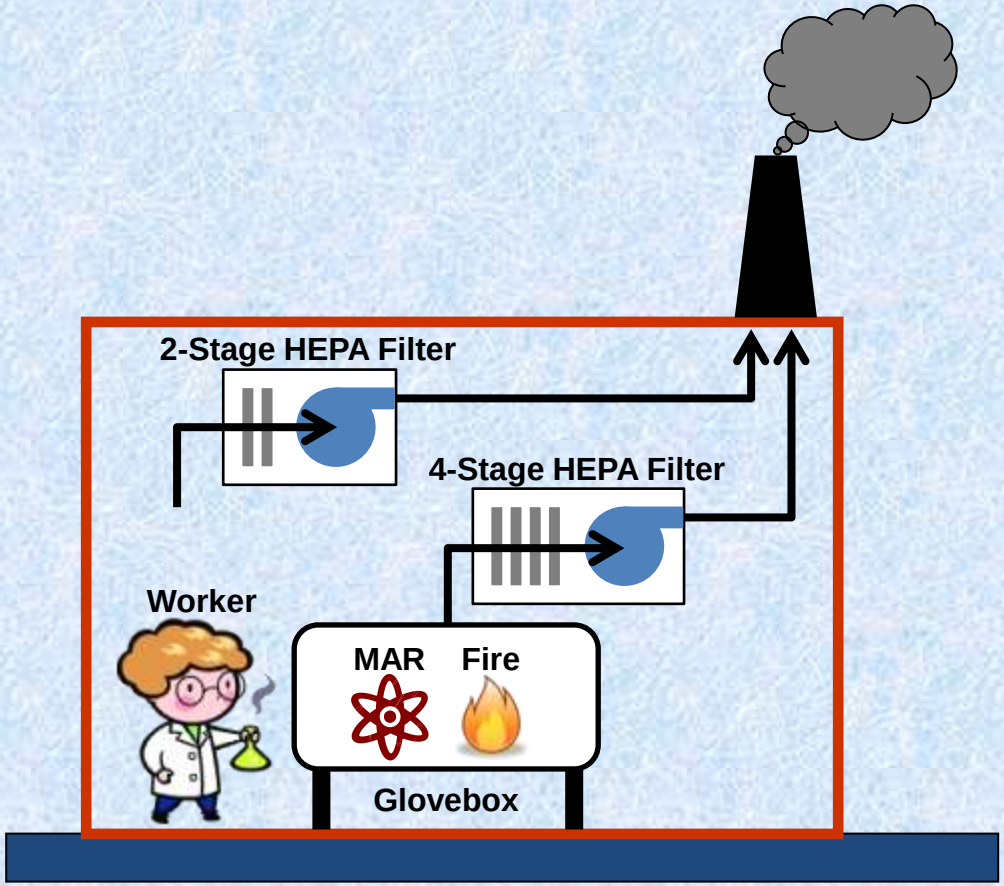
- Analysis Procedure
  - Identify the initiating events of interest that can result in the type of accident of concern.
    - May be a system or equipment failure, human error, or process upset that could lead to the consequences of interest.
    - The initiating event is usually something that is expected. The plant design, includes systems, barriers, or procedures that are intended to respond to and mitigate the effects of the initiating event.
    - If an initiating event directly results in the consequence of interest, a fault tree may be more suitable for analyzing the accident.

Event Tree Analysis: Use

- Analysis Procedure
  - Construct an event tree for each initiating event (continued).



Example – GB Fire Event Tree

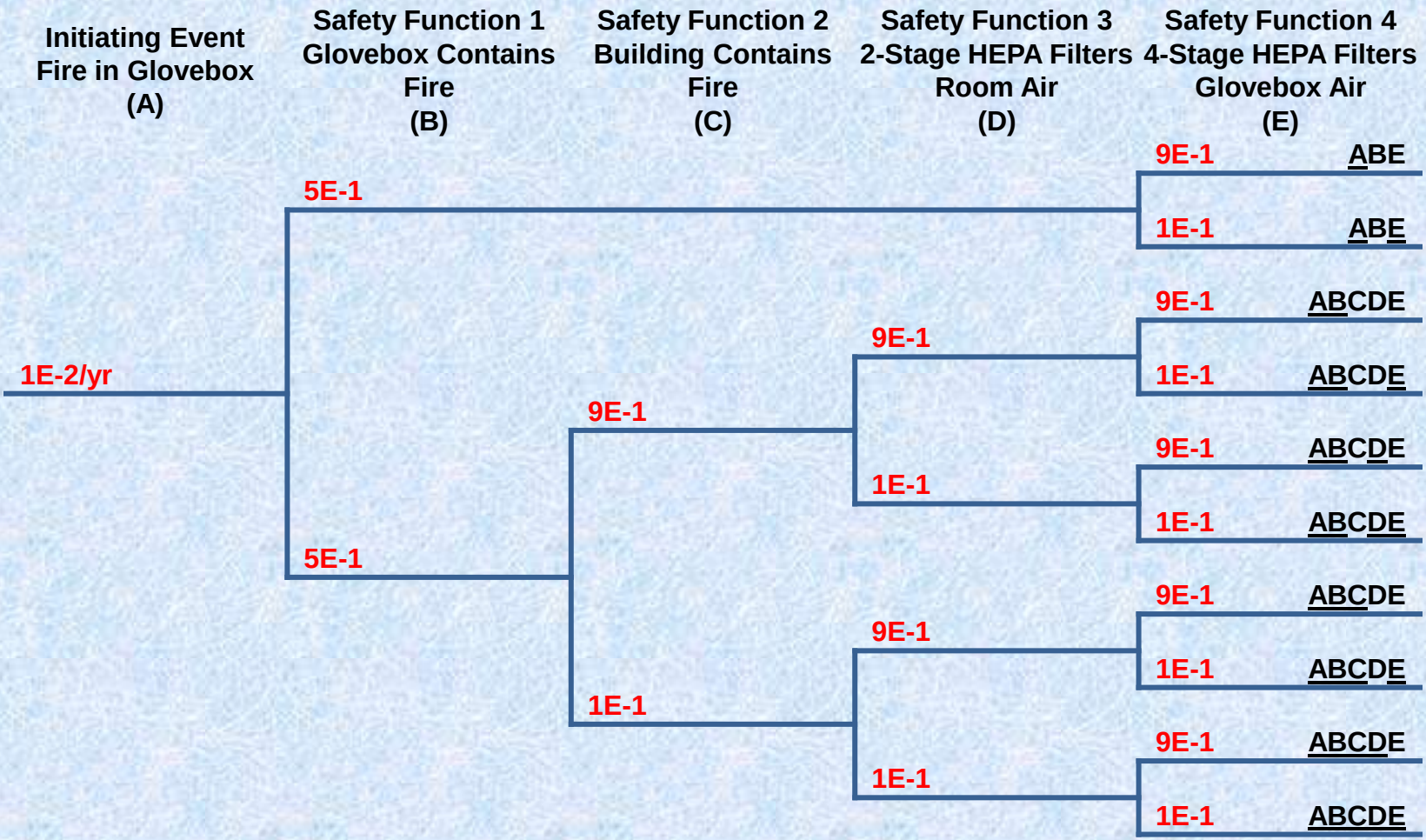


Example – GB Fire Event Tree

Initiating Event: Fire in glovebox.

- Safety Function 1: Glovebox contains fire.
- Safety Function 2: Building contains fire.
- Safety Function 3: 2-Stage HEPA filter plenum filters room air exhaust. (Room air pressure is less than atmospheric pressure.)
- Safety Function 4: 4-Stage HEPA filter plenum filters glovebox air exhaust. (Glovebox air pressure is less than room air pressure.)

Example – GB Fire Event Tree



Example – GB Fire Event Tree