National Nuclear Security Administration
Environment, Safety and Health

Hazard Analysis (HA) Process-Basic Concepts and Techniques

Bill Schleyer

NNSA-SC

for Integrated Safety Management Conference

Analysis Process- What it Does

- **Hazard analysis is the activity that:**
  - Comprehensively evaluates facility and process hazards
  - Requires a full understanding of facility activities
  - Identifies more important engineered and administrative controls

- **Identifies accidents for further analysis due to a public consequence potential or extreme harm to workers**

Purpose of the Hazard Analysis (HA)

- **Document Safety Controls**
- **The real value in HA performance stems from:**
  - Comprehensive and systematic evaluation of hazards
  - Coverage of a complete spectrum of accidents for both normal and abnormal conditions and events
  - Assessing the effectiveness and adequacy of controls
  - Recommending additional controls as needed
- **Bottom line: A better understanding the spectrum of controls that make any facility or work safe**
  - Construction and processing facilities
  - Environmental restoration activities

Information Derived from HA

- **Independent of the Method, the HA Should:**
  - Identify facility or process hazards
  - Identify potential accident scenarios involving the hazards and initiating events
  - Qualitatively estimate the uncontrolled consequences of potential accident scenarios
  - Qualitatively estimate the frequency that a potential accident scenario may occur
  - Rank the accident scenario according to its relative risk
  - Identify potential preventive and mitigative controls
  - Recommend actions to reduce facility or process risk

Selecting the Hazard Analysis Method

- **Fit the hazard analysis method to the complexity of the operations and magnitude of the hazards**
- **Typical hazard analysis methods include:**
  - Hazard Identification Checklist
  - What-If Analysis
  - Hazard and Operability (HAZOP) Study
  - Process Hazard Analysis (PrHA)
- **Systematic tabular (text) method**

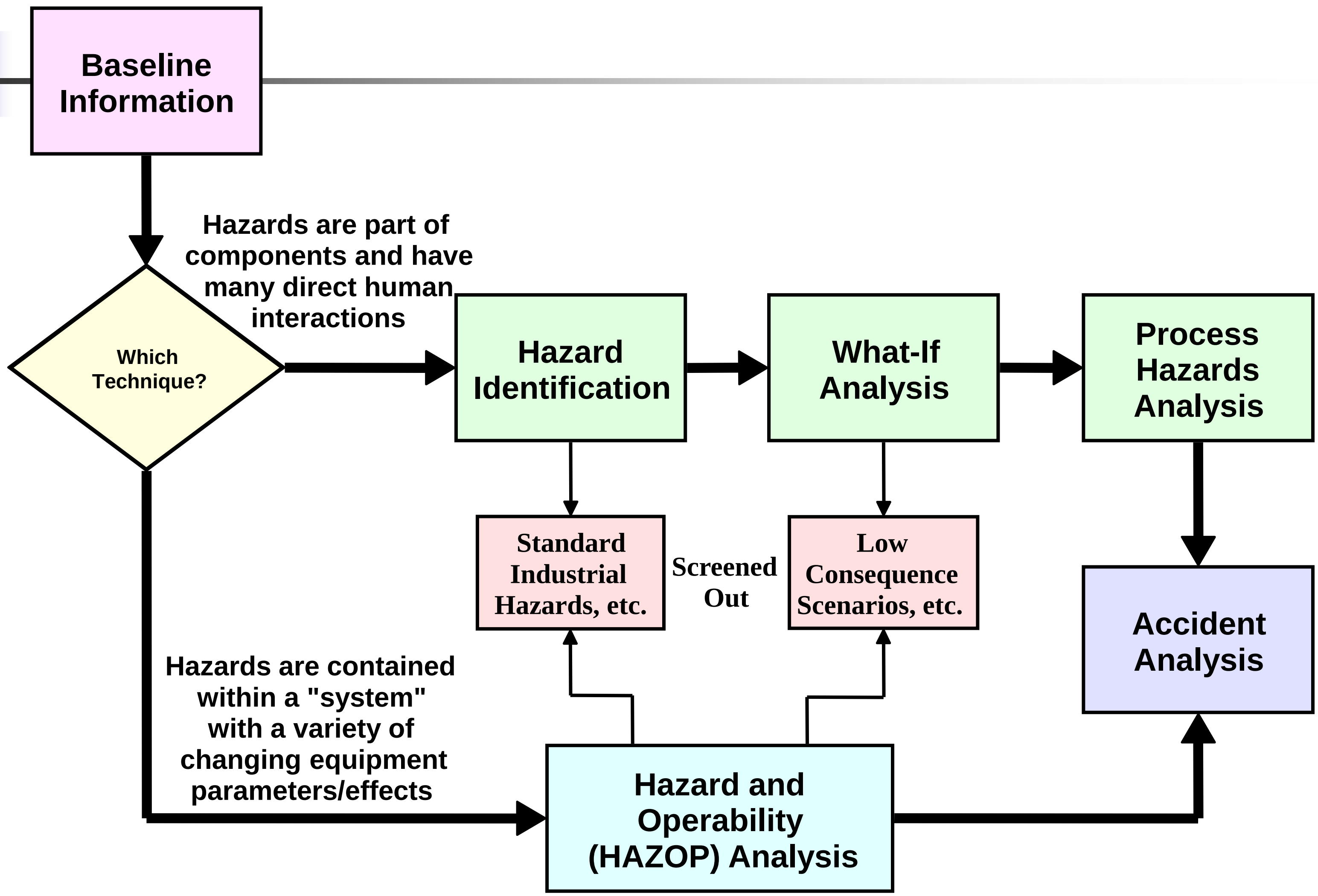
Methods Overview

METHOD	CHARACTERISTICS	ADVANTAGES	DISADVANTAGES
PHA	- Less Rigid and fewer Rules - Less Documentation - Focuses on hazards that have surfaced in the past	- Simple processes - Simple procedures - Shorter meetings; reduced HA effort	- Simplistic process - Requires a very high level of experience-base
What-If	- A defined method with rules - Brainstorming - Focuses on hazards that are unforeseen - More documentation	- Simple to moderately complicated processes or procedures - Very simple method to lead	- Usually used only for collection of information and screening
HAZOP	- Very structured approach using guideword/parameter combinations - Focuses on all deviations from normal operations	- Complicated process or procedures - Complete/thorough - Less reliance on "experts"	- Time consuming - May spend time discussing operability issues rather than safety
FMEA	- Equipment failures	- Complicated systems - Systematic evaluation of component failures	- Single failure modes only - Expert dependent
PrHA	- Organized to develop scenarios from hazards and process/activity - Id controls for each process/accident	- Comprehensive/graded - Presents rational for risk control - Resources moderate for high quality product	- Rigor depends on expected results - Experience necessary

A Recommended Hazard Analysis Approach

- **The Steps to Perform include:**
  - Preparation Activities—Get Ready
  - Hazard Identification & Screening
  - Scenario Analysis
    - What-If Analysis & Screening
    - Process Hazards Analysis

      <u>or</u>
    - HAZOP Study (for system/process parameter analysis)
  - Selection of Major Accidents (for more detailed analysis)


Baseline Information
Hazards are part of components and have many direct human interactions
Which Technique?
Hazard Identification
What-If Analysis
Process Hazards Analysis
Standard Industrial Hazards, etc.
Screened Out
Low Consequence Scenarios, etc.
Accident Analysis
Hazards are contained within a "system" with a variety of changing equipment parameters/effects
Hazard and Operability (HAZOP) Analysis

Benefits of This HA Approach

- **Complex, Diverse Facilities are Too Costly to Comprehensively Analyze Each Hazard/Scenario**
  - Need to Focus on Significant Hazards
  - Need to Screen Out Standard Industrial Hazards and Low Consequence Scenarios
- **This Method Progressively Selects Concerns or Events that Require Additional Analysis, using**
  - Hazard Screening
  - Scenario Screening
  - Bounding Accident Selection (worst feasible)

Benefits of This Approach (continued)

- **Comprehensive coverage of hazards & scenarios**
  - Cost-effective (efficient) analysis of important facility and process safety concerns
- **Methods are "State-of-the-Art"**
  - Can be applied to a variety of facilities/processes
  - Can be tailored to existing, new, or D&D projects

Hazard Analysis
Pre-Start Activities

- **Establish Matrices**
  - for Frequency, Consequences, and Risk
- **Establish Basis for Frequencies**
- **Establish Reductions from Typical Controls**
  - of Frequency and Consequences
- **Establish Use of HA Forms and Terminology**
  - for Consistency

Framework for Consequence, Frequency and Risk

- **Consequences**
  - Level of harm
    - Dose
    - Degree of injury

  To

  - Receptors
    - Immediate Worker
    - Collocated Worker
    - Offsite public (MOI)
    - Environment
- **Frequency**
  - Conservative estimate of HOW OFTEN a scenario may occur
- **Risk**
  - Relative rank based on consequences and frequency of incident
  - Possibility of a loss or injury

HA Frequency Matrix

Frequency Category	Frequency Description	Frequency Range (per yr)
I	**Anticipated** (A) or events that might occur several times during the facility's lifetime	$> 10^{-2}$
II	**Unlikely** (U) or events that are not anticipated to occur during the facility's lifetime (such as a 100-year flood)	$10^{-2} – 10^{-4}$
III	**Extremely Unlikely** (EU) or improbable events that should not occur during the facility's lifetime (such as a design basis accident)	$10^{-4} – 10^{-6}$
IV	**Beyond Extremely Unlikely** (BEU) or incredible events	$< 10^{-6}$

Consequences Matrix

Consequence Category	Consequence Description	
	Public	**Worker**
A	**Potential for immediate or long-term health effects, or exceeding the EPA or DOE exposure/evaluation guidelines** •• Radioactive Material Dispersal (with potential for doses > 25 rem) • Toxic Material Dispersal > ERPG-2	**Potential for immediate and severe health effects, or long-term health effects or disability, or potential for loss of life** • Plutonium Dispersal (mechanical or fire) • Toxic Material Dispersal > IDLH
B	**Minor injuries with no disability or work restrictions** • Radioactive Material Dispersal (with potential for doses between 0.1 and 25 rem) • Toxic Material Dispersal between ERPG-1 and EPRG-2	**Potential for long-term disability or severe injury (non life threatening) from non-standard industrial accidents** • Radioactive Material Dispersal (including tritium< 20 g) • Fire with Toxic Material Dispersal • Toxic Material Dispersal (>TLV-TWA or equivalent)
C	**No significant offsite impact** **(any release is below acceptable limits)** • Radioactive Material Dispersal (but with offsite lifetime doses < 0.1 rem, in accordance with DOE Order 5400.5) • Toxic Material Dispersal < ERPG-1	**Minor injuries with no disability or work restrictions** • Mechanically-caused Toxic Material Dispersal (< TLV-TWA or equivalent)
D	**No Measurable Radiological or Toxic Release**	**No measurable consequences**

HA Risk Matrix

Consequence Category	Frequency Category			
	I	II	III	IV
A	1	1	2	3
B	2	2	3	4
C	3	4	4	4
D	4	4	4	4

1 = High Risk
2 = Moderate
3 = Low Risk
4 = Negligible

Risk # is relative,
not absolute,
to allow ranking.

Basis for HA Frequencies

Accident Initiation Event	Frequency ID (bin)	Frequency Category	Frequency Range (yr)	Comments
Operational Initiators				
Human Error	I	Anticipated (A)	$> 10^{-2}$	
	II	Unlikely (U)	$10^{-2} – 10^{-4}$	Passive features (e.g., shipping container) protect from releases
Operational Fires and/or Explosions	I	Anticipated (A)	$> 10^{-2}$	
etc.				
Natural Event Accident Initiators				
Seismic Events	II	Unlikely (U)	$10^{-2} – 10^{-4}$	Based on PC-3 or PC-4 exceedance probabilities
etc.				
Man-Made External Accident Initiators				
Airplane Crash	IV	Beyond Extremely Unlikely (BEU)	$< 10^{-6}$	Based on analysis of overflights
etc.				

Reductions from Controls

Type of Control	Reduction Factor
Preventive Engineered Features	
Passive structural (e.g., building structural design, permanent shielding)	$1x10^{-4}$
Passive mechanical (e.g., qualified container)	$1x10^{-4}$
Passive electrical (e.g., grounding)	$1x10^{-4}$
Active fail-safe mechanical (e.g., spring loaded valve)	$1x10^{-3}$
Active fail-safe electrical (e.g., fails safe on loss of power)	$1x10^{-3}$
Active mechanical safety-related pedigree (e.g., safety related pump)	$1x10^{-3}$
Active electrical safety-related pedigree (e.g., safety related UPS)	$1x10^{-3}$
etc.	
Preventive Administrative Controls	
Follow procedures that implement specific TSR administrative control elements	$1x10^{-1}$
Certified personnel (e.g., forklift drivers)	$1x10^{-2}$
Follow written procedures for TSR safety controls, with two-person rule	$1x10^{-2}$
Preventive maintenance of safety related equipment	$1x10^{-1}$

Screening

Screening is the decision to remove from evaluation those hazards or scenarios that present a minimal risk or insignificant consequences*

- **Criteria should be Defined prior to the Analysis**
- **Screen at Several Levels**
  - Hazard ID
  - What-If Analysis
- **To Screen or Not to Screen?**
  - when in doubt do not delete a hazard or scenario

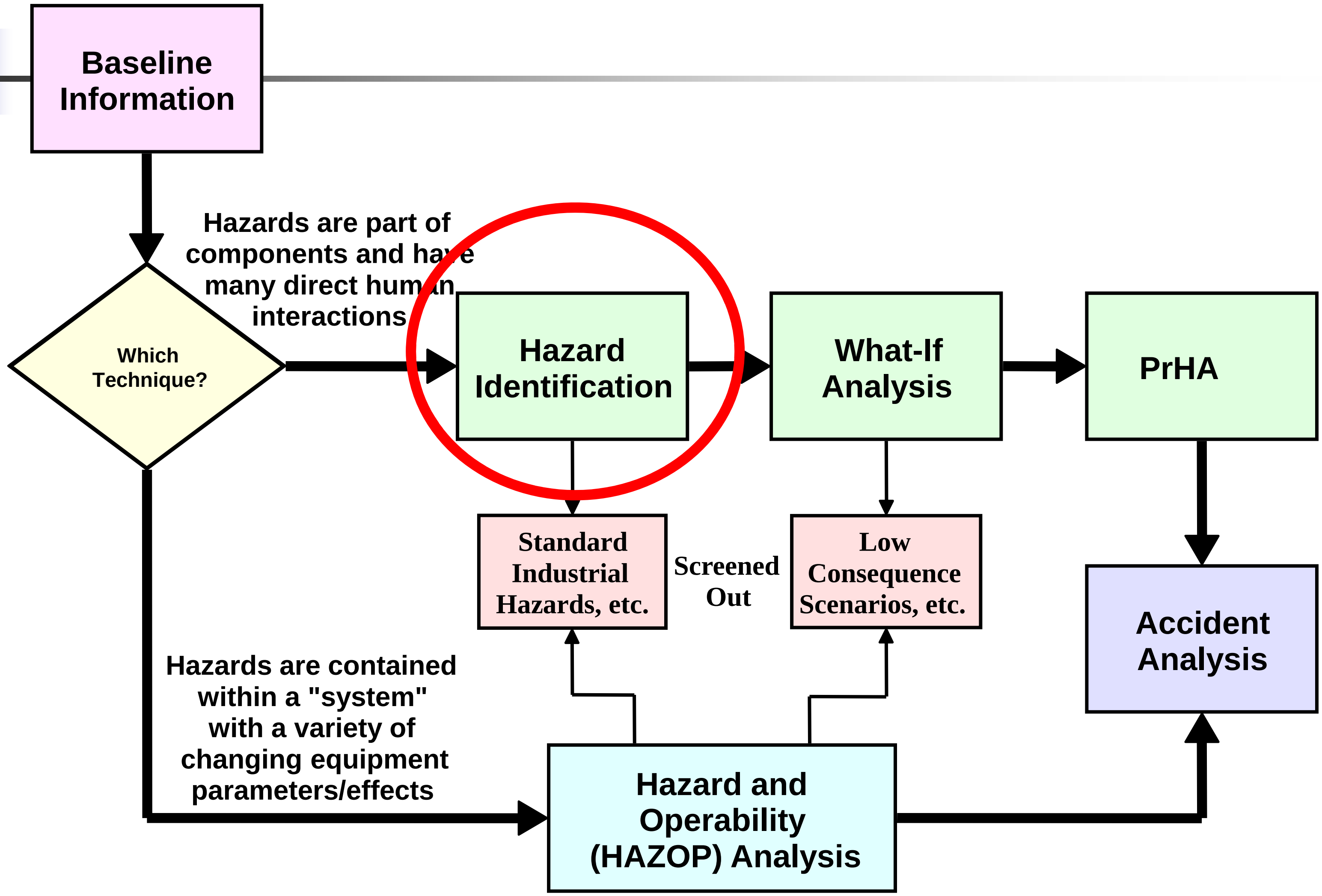
***Screening may impact ability to identify normal/abnormal conditions leading to incidents**

Starting Hazard Analysis

- **Assemble the HA Team**
  - Should be able to discuss operations, design, and safety
  - Should be knowledgeable on hazard analysis methods
- **Establish Analysis Approach**
- **Obtain baseline information**
  - Facility Walk-through
  - Document Review
  - Personnel Interviews
- **Identify the Basic Operations or Areas to Study**

Facility and Process Information

- **Become familiar with baseline information:**
  - Site and location characteristics
  - Facility design information
  - Process/activity information
  - Historical operational information
  - Materials information
  - Safety documents and records
- **A process flow sheet can help understand hazards**


Baseline Information
Hazards are part of components and have many direct human interactions
Which Technique?
Hazard Identification
What-If Analysis
PrHA
Standard Industrial Hazards, etc.
Screened Out
Low Consequence Scenarios, etc.
Accident Analysis
Hazards are contained within a "system" with a variety of changing equipment parameters/effects
Hazard and Operability (HAZOP) Analysis

Hazard Identification and Analysis

- **Hazard Identification**
  - Identifies workforce hazards and activities
  - What are the “energies” and how is each transferred
  - Systematic tabular (text) method
  - Leads into What-If analysis
  - Supports Process Hazards Analysis

Hazard Identification

- **Identify Hazards**
  - Use a Standard, Comprehensive Checklist
  - Use a Separate Checklist for Each Operation/Area
- **Screen Standard Industrial Hazards**
  - Adequate controls covered by OSHA
- **Screen Non-Significant Hazards**
  - If < 25% RQs in 40CFR302/40CFR355
  - If < Criteria you decide (BMP, consensus stds)

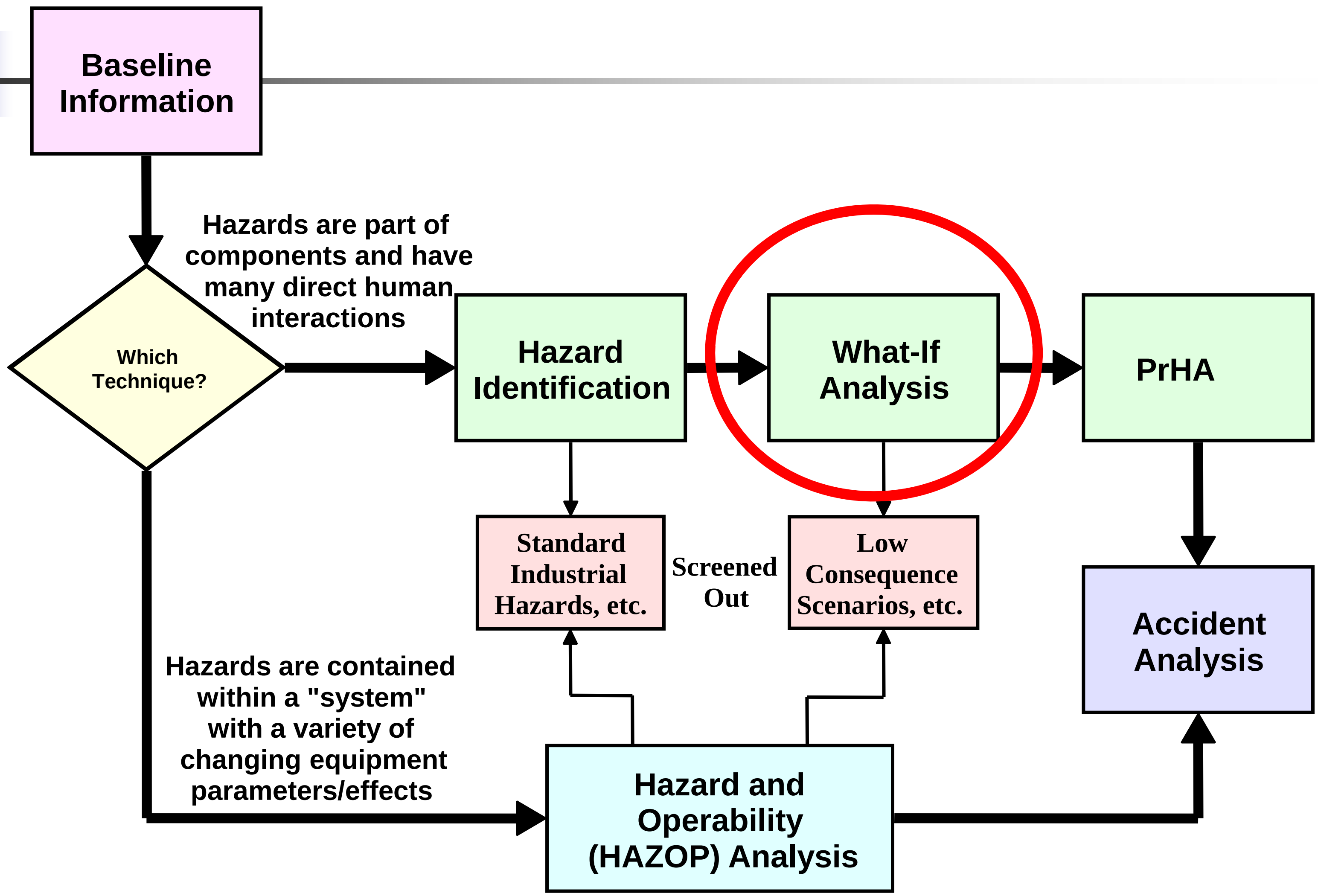
Hazard ID Checklist

Hazard Categories	Hazard Description*	Process or Area	Analysis Status
Acceleration			
Inadvertent motion	Hand Carts of Items	Radiography	A/R
Sloshing of liquids	Photo Chemicals (2 gal - liq - $C_2H_4O_2$)	Photo Lab	SIH and << RQ
etc.			
Deceleration			
Impacts (sudden stops)	Door Shuts on Items	Radiography	A/R
Falling objects	Crane Drops Items (2 ton – 15 ft)	Radiography	A/R
etc.			

* Includes characterization of hazard particulars (quantity, form, location, etc.)

Hazard Identification (continued)

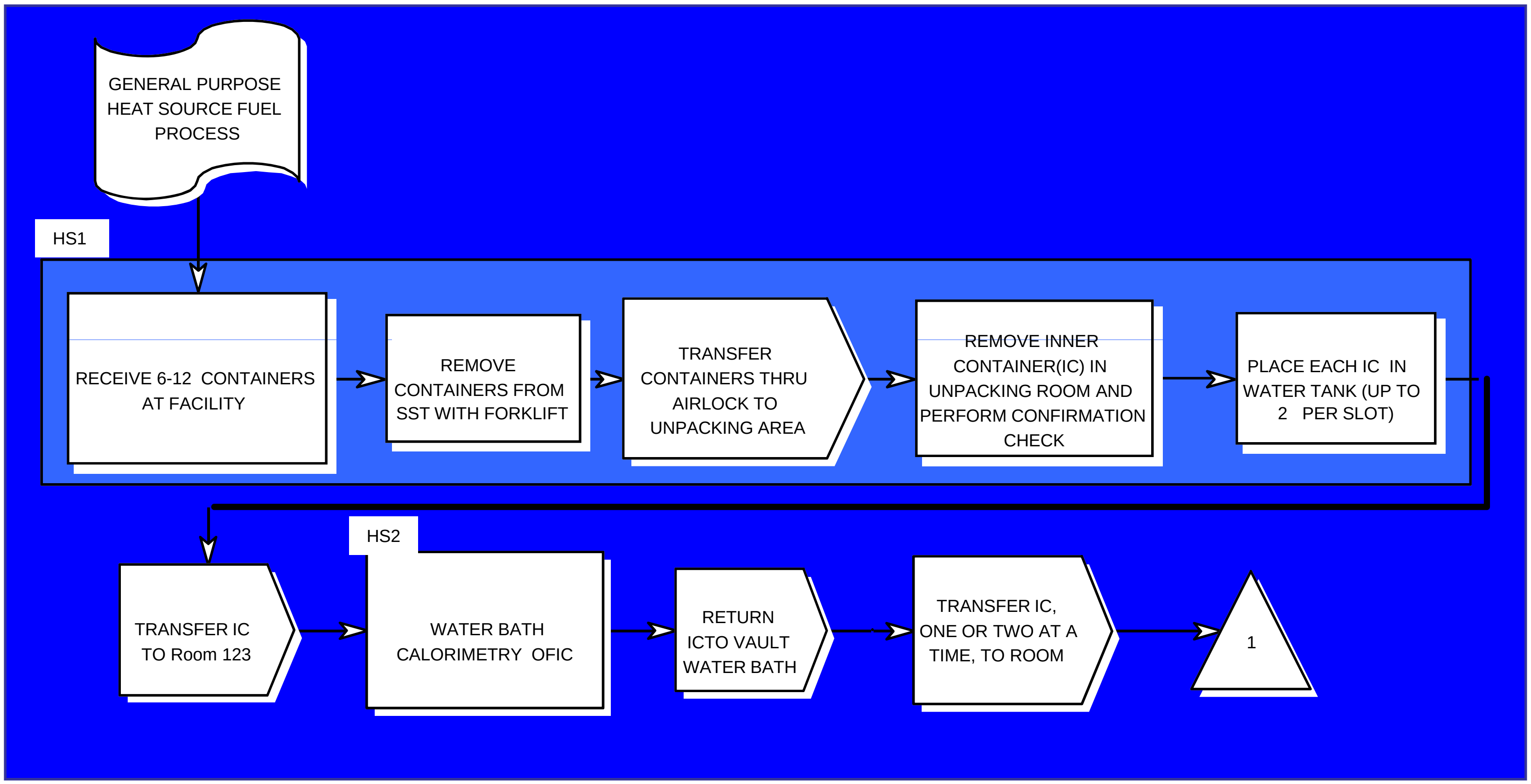
- **Hazards not Screened Out are Evaluated Further**
- **Results can be Summarized and Tabulated**
  - Allows for checking hazards that may be common to several processes or areas


Baseline Information
Which Technique?
Hazards are part of components and have many direct human interactions
Hazard Identification
What-If Analysis
PrHA
Standard Industrial Hazards, etc.
Screened Out
Low Consequence Scenarios, etc.
Accident Analysis
Hazards are contained within a "system" with a variety of changing equipment parameters/effects
Hazard and Operability (HAZOP) Analysis

Preparation for a What-If Analysis

- **Resolve Any Baseline Information Issues**
  - Develop or finalize the process flowchart(s) and description(s) of facility/process operations
- **Identify Hazard Configurations**
  - Physical, Explosives, Toxics
- **Establish General Consequences for Various Insults to Each Configuration**
  - Small release, large release, small fire, large fire
  - Major injury/death, minor injury

Process Flow Chart



Configurations and Consequences

Configuration	Examples	Examples of Bounding Configurations During Assembly Operations	Vulnerabilities	Consequences
Toxic Material	Process inventory chemicals Storage facility	Toxic material containers at process line	Thermal Insults Mechanical Insults Electrical Insults Water Immersion	Vapor Release Spills Fire Chemical Reactions
etc.				

What-If Analysis

- **A Modified What-If Analysis is Performed**
  - Brainstorm Scenarios by Asking “What if…”
  - Goal is to Reduce and Group the Number of Scenarios that Need Additional Analysis
  - Use a Separate Table Used for Each Operation/Area
  - Group Questions by Type of Insult for Each Configuration
  - Screen Out Non-Significant Consequences
    - Equipment Damage Only, Not Physically Possible, Negligible Consequences, etc.

Scenario Development

- **Scenarios are concise, clear, and present a logical description of the factors in an accident chronology.**
  - Typically a scenario describes:
    - Activity or Area of Interest
    - Initiating Event(s) or Cause
    - Type of Accident
    - Resulting Hazard
  - The level of detail will vary
    - Less in What-If Analysis
    - More in the Process Hazard Analysis

Modified What-If Approach

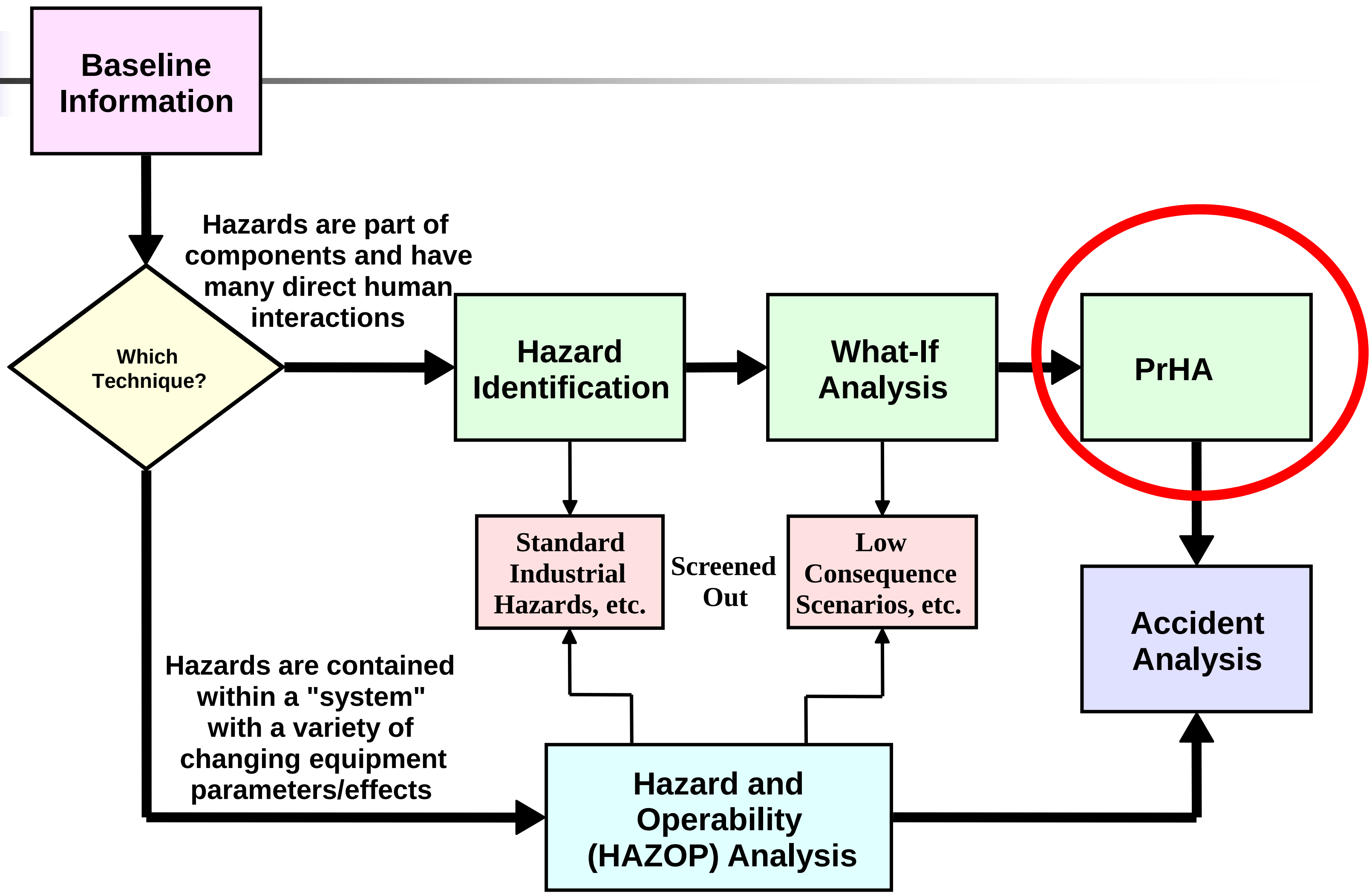
- **AIChE 1992, *Handbook of Chemical Hazard Analysis Procedures*, explains that each What-If scenario should include recommendations**
  - Either a reason for screening or specific controls
- **In this modified approach, can defer control recommendation until bounding accident evaluation**
  - Control the worst case conditions

What-If Analysis Table

ID No.	Area	Configuration	Scenario	Consequence	Action
Mechanical Insults					
nn-nn	Radiography	High Explosives	What if the crane fails?	Explosion	PrHA #
Electrical Insults					
etc.					
Thermal Insults					
etc.	Dryer	Toxic Chemicals	What if the dryer overheats?	Fire	PrHA #
Other Operational Events					
nn-nn	Radiography	Explosives	What if material overexposed?	None	No Action
Natural Phenomena					
etc.					
External Events					
etc.					

AIChE What If Format

What If Analysis Format (AIChE)			
What If?	**Hazard Consequence**	**Safeguards**	**Recommendation**
Plutonium powder inhalation	Drum impacted by truck or punctured by forklift. Radioactive material spill and airborne release.	Truck controls Container Physical barrier Worker/operator training	Controls do not appear adequate. Identify additional engineering controls.
Gasoline, 200 gallon	Gasoline ignited by subcontracted maintenance on electrical system. Fire causing release that causes radiological dose to public.		Can the gas be stored elsewhere and in flammable storage cabinets or similar?
Identify the processes, system and/or component being considered.			


Baseline Information
Which Technique?
Hazards are part of components and have many direct human interactions
Hazard Identification
What-If Analysis
PrHA
Standard Industrial Hazards, etc.
Screened Out
Low Consequence Scenarios, etc.
Accident Analysis
Hazards are contained within a "system" with a variety of changing equipment parameters/effects
Hazard and Operability (HAZOP) Analysis

Process Hazards Analysis Concept

- **An efficient, systematic technique for evaluating and documenting processes/activities of interest**
  - Focuses on those accidents expected to result in more adverse consequences or risk, whether from operations, natural phenomena, or external events
  - Tabulates both uncontrolled and controlled scenarios
    - with and without application of potential controls
  - Highlights potential controls with the most benefit
  - Provides for robust tracking and clear communication of the risk reduction measures resulting from the hazards and potential accident scenarios

PrHA Concept (continued)

- **A Process Hazard Analysis (PrHA) Evaluates Accident Scenarios that were Not Screened Out During the What-If Analysis**
- **Organization**
  - By Process Logic
    - (by operation or activity)
  - By Accident Types (Initiators/Consequences)
    - operational, natural phenomena, and external events
    - (fire, explosion, confinement loss, criticality, rad exposure, earthquake, aircraft crash, etc.)

PrHA Performance

- **The accident scenario description should be specific in identifying the cause (initiating event)**
- **The frequency of occurrence and accident consequences are qualitatively established**
  - **First** – frequencies and consequences are recorded without consideration of existing or possible controls (uncontrolled)
  - **Then** – controls are identified and resulting frequencies and consequences are evaluated
- **Risk matrix tables are used to rank scenarios**

PrHA Performance (continued)

- **Controls that give the most effective reduction of the frequency or consequence category are checked (✓) in the tables**
  - Considered as more Important Controls
  - Safety Management Programs collectively reduce by ½ category (bin)
  - Safety Management Programs adequately protect for scenarios of lower risk
- **Other controls are noted to support safety**

Sample PrHA Table

National Nuclear Security Administration
Environment, Safety and Health

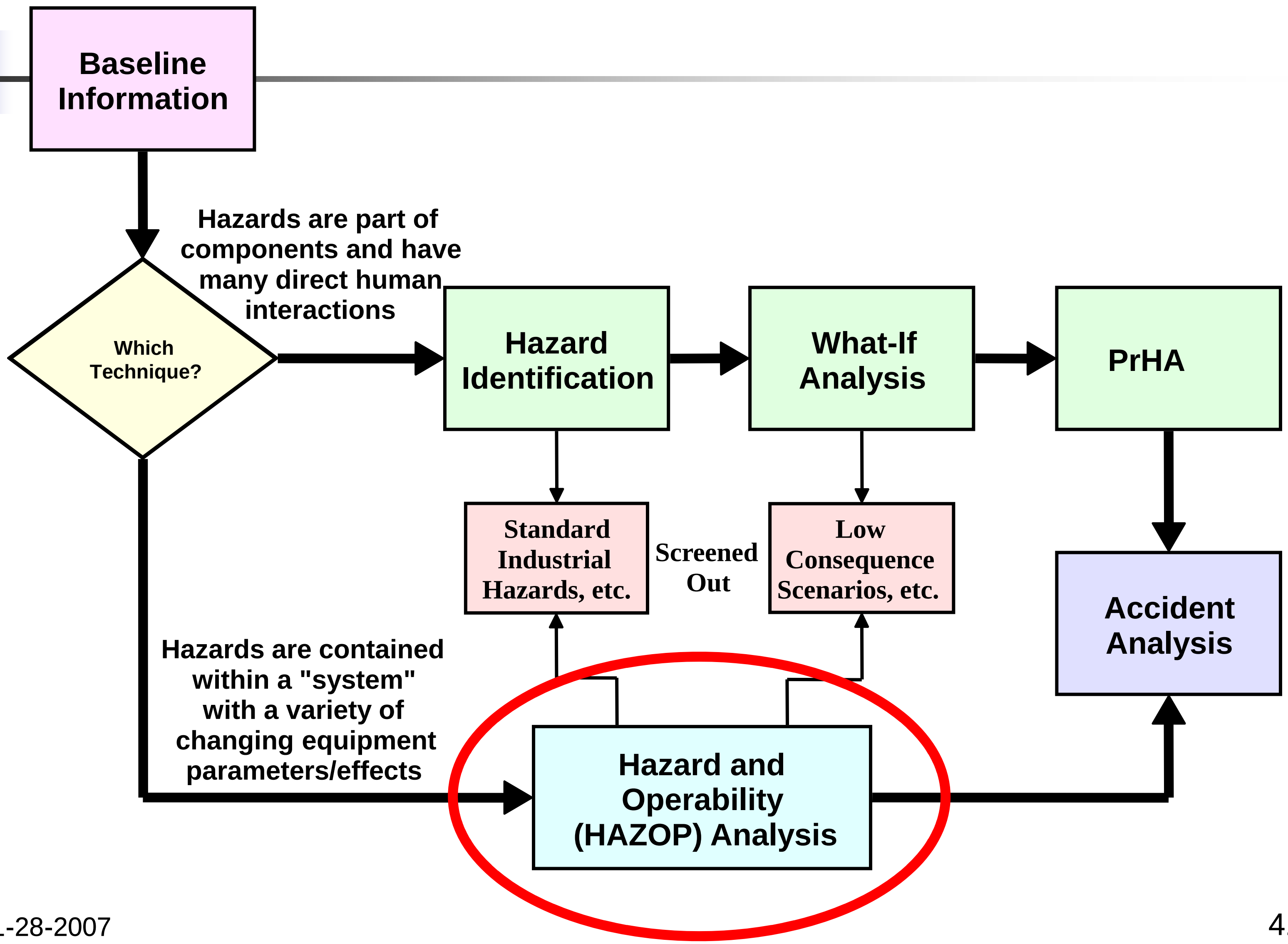
Table 3C-X. Process Hazard Analysis		
Site:	**Facility:**	**Author:**
Process:	**Hazards of Concern:**	**Reviewer:**

{Process/Operations Summary}

ID No.	Accident Type	Cause or Initiating Event	Scenario	Control Description	Ctrl Type	Freq	P = Public W = Worker Conseq P	Conseq W	Risk P	Risk W	Notes (e.g., Assumptions, Material At Risk [MAR])
x-01	xxxx	xxxxxx	xxxxxx	UNCONTROLLED →							
			(1) xxxxxx	(1)							MAR:
			(2) xxxxxx	(2)							MAR:
				Control Description & Type PA = Preventive Administrative; MA = Mitigative Administrative PE = Preventive Engineering; ME = Mitigative Engineering ✓ = Control Gives a Significant Reduction							*[Assumes all Programmatic Administrative controls (e.g., training, procedures), as well as the following, are in place].*
				SMP implementation	P/MA	✓	✓	✓			
				xxxxxx	PE	✓					
				xxxxxx	ME		✓				
				xxxxxx	PA						
				CONTROLLED →							
				(1)							
				(2)							

CONTROLS DEFINED

OMICRON PrHA Format


Baseline Information
Hazards are part of components and have many direct human interactions
Which Technique?
Hazard Identification
What-If Analysis
PrHA
Standard Industrial Hazards, etc.
Screened Out
Low Consequence Scenarios, etc.
Accident Analysis
Hazards are contained within a "system" with a variety of changing equipment parameters/effects
Hazard and Operability (HAZOP) Analysis

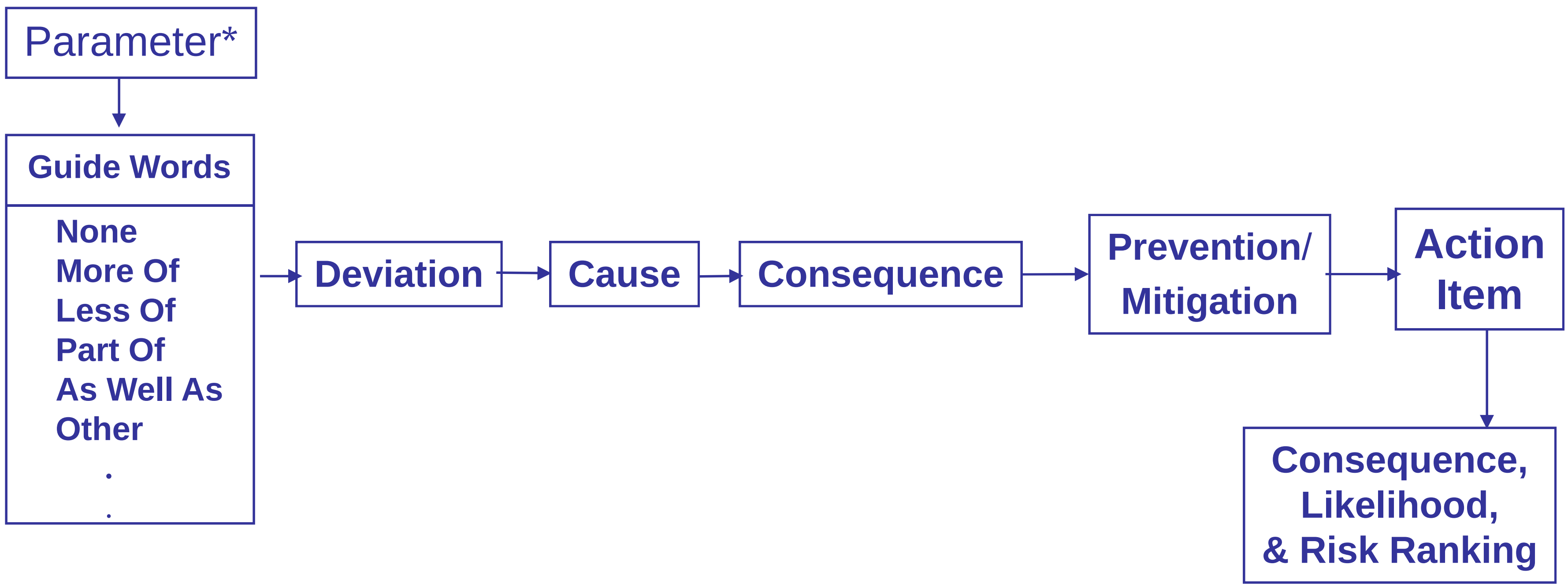
HAZOPS

Assumptions

- Systems work well when operating under design conditions
- Problems arise when deviations from design conditions occur

- **Characteristics**
  - Comprehensive tool to evaluate scenarios and control risk
  - It should be detailed and rigorous
  - System and worker controls defined
- **Complex systems requiring a more methodical approach to ensure completeness**
  - Human/hardware elements involving maintenance/operating procedures

HAZOPS Analysis Process



*Covering every parameter relevant to the system:
flow, pressure, temperature, viscosity, components, etc.

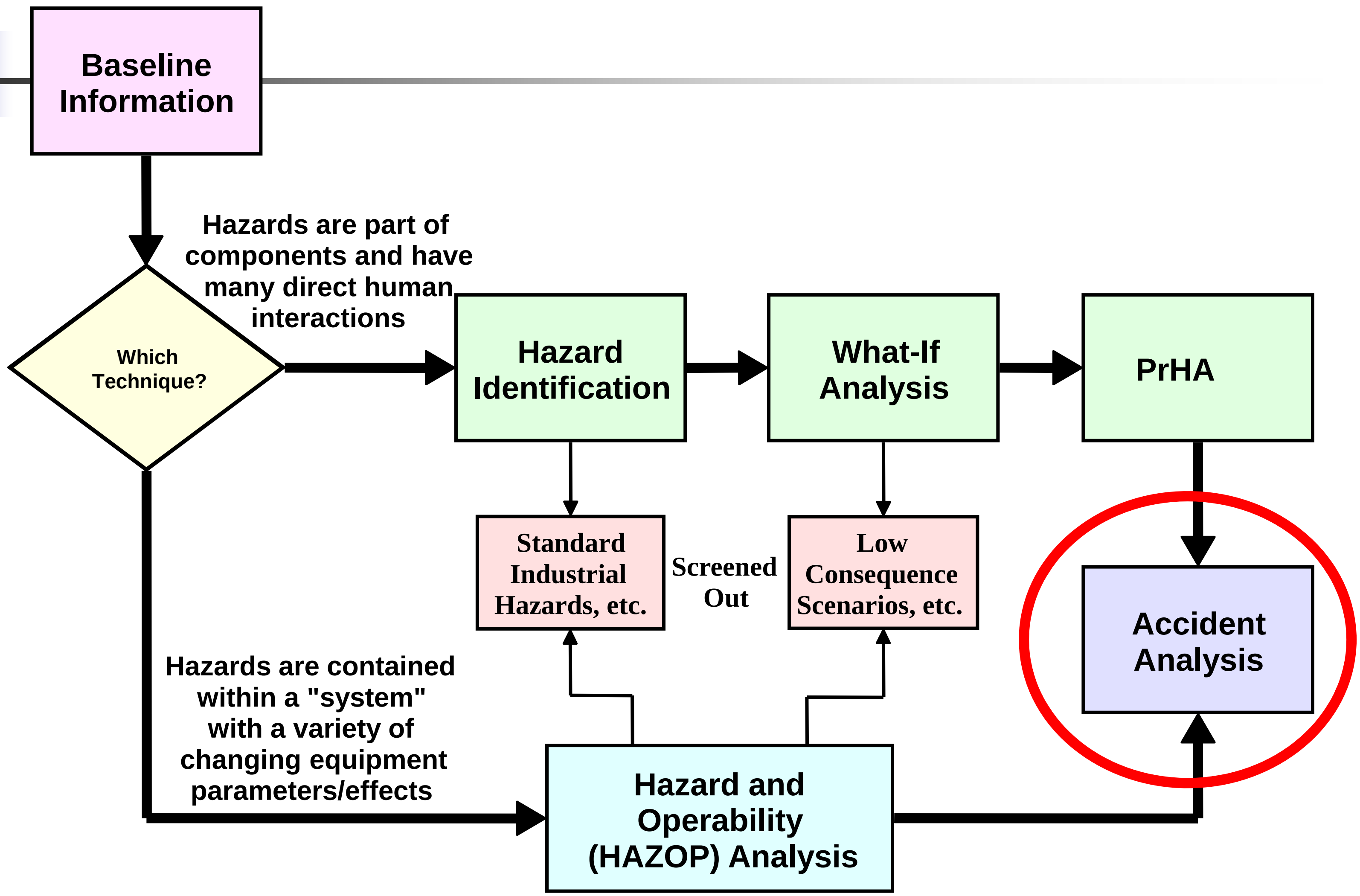
HAZOPS Deviation Matrix

Parameter	None	More Of	Less Of	As Well As	Part Of	Reverse	Other Than
Flow (rate or quantity)	No flow	High flow	Low flow	Contaminants	Wrong concentration	Back flow	Wrong material
Temperature		High temp.	Low temp.				
Pressure		High press.	Low press.				
Time	Misses a step	Too long Too late	Too short Too soon	Extra actions initiated	Some of actions in	Steps backwards	Wrong time

HAZOP Study Example

Plant/Operation: WSTF/Solid Waste to Storage Process **Line/Vessel/Node:** Outdoor truck unloading area - WSTF **Design Intention:** To transfer solid radioactive waste drums from truck to the storage area designated as such without any loss of containment from drums. Storage area capacity is 240 drums.	**Review Date:** 2/1/96 **Drawing No.:** **Review Team:**

Guide Word	Deviation	Cause	Consequences	Protection	Scenario Number	Consequence	Likelihood	Risk Ranking	Action Item/Comments
Other Than	Wrong Building	Solid radioactive waste drums put in cylinder storage building in error	Plutonium inhalation: workers open up drum in error without appropriate PPE.	• Labels on drums • Two-person operation	1.23	High A	Low III	2	Consider a program that requires appropriate radioactive inhalation PPE whenever any drum is opened


Baseline Information
Which Technique?
Hazards are part of components and have many direct human interactions
Hazard Identification
What-If Analysis
PrHA
Standard Industrial Hazards, etc.
Screened Out
Low Consequence Scenarios, etc.
Accident Analysis
Hazards are contained within a "system" with a variety of changing equipment parameters/effects
Hazard and Operability (HAZOP) Analysis

Safety Layers in the Chronology of an Accident or Event

Prevention

- Mechanical integrity
- Predictive and preventive maintenance; inspection; testing
- Operator training
- Human factors
- Impact barriers

- Automatic/manual process control or safety systems
- On-line spares
- Backup systems

- Alarms
- Operator intervention
- Interlocks, trips
- Emergency shutdown
- Last-resort controls
- Relief Valves
- Ignition source control

Mitigation

- Emergency response
- Sprinkler, deluge
- Dike, trench
- Blast wall, barricade
- Water curtain
- Personal protective equipment
- HEPA filters

Hazard → **Cause** → **Deviation** → **Accidents** → **Impact**

Hazard

Material/energy contained and controlled during normal operation

- Toxicity
- Flammability
- Reactivity
- Radioactivity
- Elevated pressure, etc.

Cause

Initiating event of process upset; Start of accident event sequence

- Mechanical failure
- Procedural error
- External force
- Fouling, etc.

Deviation

Excursion beyond design/ operating limits

- No flow
- High temperature
- Low level
- Impurities
- Wrong material
- Step omitted, etc.

Accidents

Loss of containment of process material/energy

- Fire
- Explosion
- Hazardous material release, etc.

Impact

Severity of consequences, losses

- Casualties
- Property damage
- Business interruption
- Environmental damage, etc.

Conclusions

- **Hazards Analysis can use several methods-pick the one that best fits the hazards/conditions.**
- **Plan the analysis**
- **Be consistent**
- **HA Results**
  - Understand the scenario
  - Identify consequences and risk
  - Define controls