HE Selection Criteria

Lifecycle Based Comparison

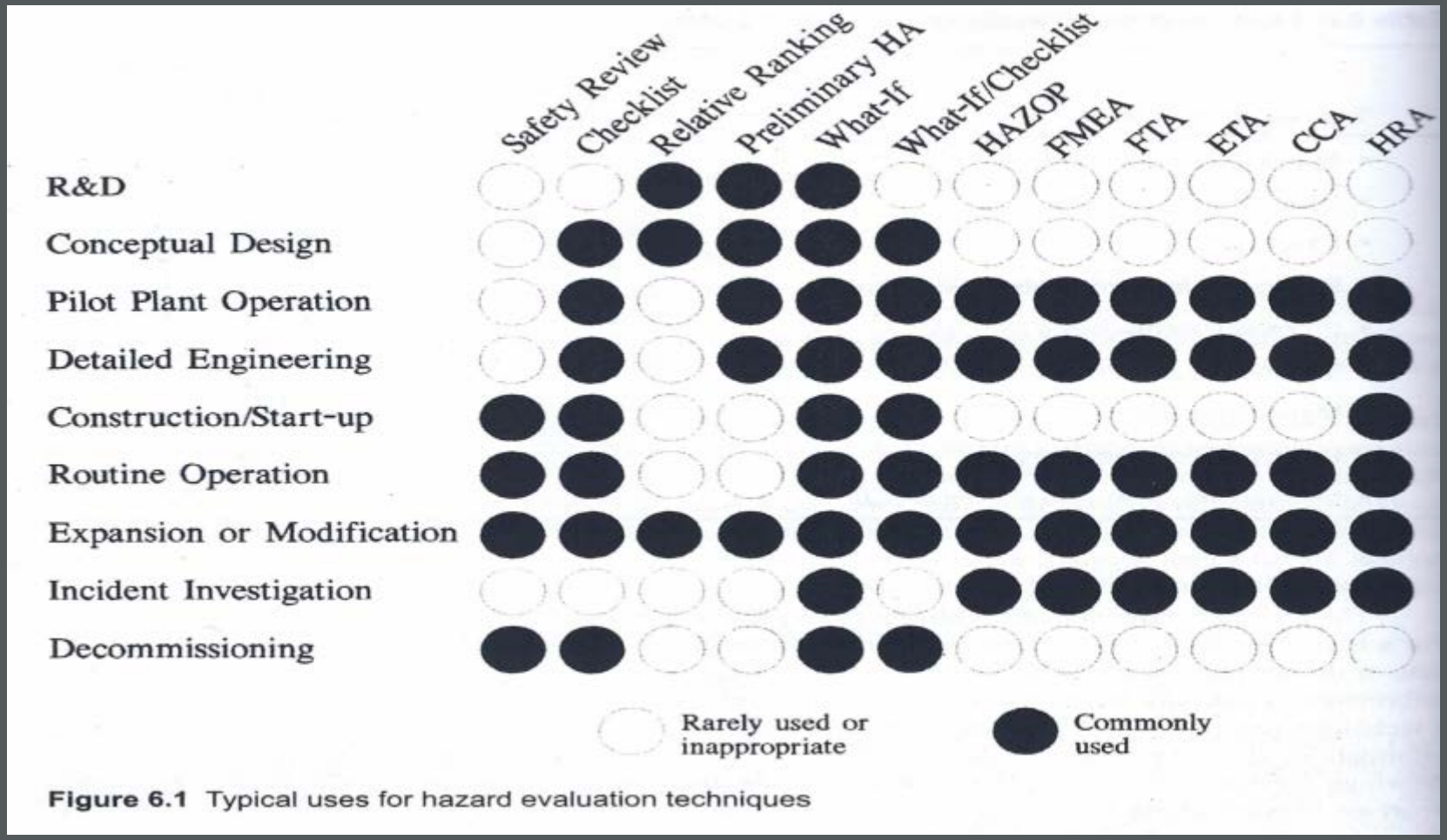

Figure 6.1 Typical uses for hazard evaluation techniques

Guidelines for Hazard Evaluation Procedures 3rd Edition, CCPS ("The Redbook"), pg. 185

Non-Scenario Technique

Preliminary Hazards Analysis

- Purpose:
  - Evaluate Hazards Early in Lifecycle
  - Identify the Basic Risk Control Strategies to be Developed Later in Lifecycle
- Description:
  - Formulates List of Hazards and Generic Hazardous Situations By Considering Process Characteristics Rather Than Specific Process Information
- Type of Results:
  - Qualitative Description of the Hazards With Qualitative Ranking of Hazardous Situations Used to Prioritize Recommendations
- Resource Requirements:
  - Limited Process Information; 1 – 2 Experienced Analyst; 5 – 17 Days Duration
- Analysis Procedure:
  - Collect Information (Typically Limited)
  - Identify Hazards, Safeguards, Causes, & Effects
  - Assign Hazard Category: Negligible, Marginal, Critical, & Catastrophic
  - Identify Potential Controls
- Documenting Results:
  - Typically Recorded in Simple Table Format

Non-Scenario Technique

[Inherent] Safety Review

- Purpose:
  - Ensure Operation & Maintenance Meet Design Intent and/or Standards
  - Performed as a Pre-Startup Safety Review
- Description:
  - Walkthrough Inspection, Design Review, and/or Interviews Against Requirements
- Type of Results:
  - Qualitative Description of the Potential Safety Problems & Suggested Corrective Actions For Identified Deviations & Newly Discovered Safety Items
- Resource Requirements:
  - Detailed Design, Process, and Procedural Information; Small Team of Well Qualified Analyst; 2 – 14 Days Duration
- Analysis Procedure:
  - Collect Detailed Information (Design, Codes/Standards, Equipment Information)
  - Formal Team Meeting(s)
  - Review Hazards & Related Requirements (i.e. Codes, Standards, Procedures)
  - Process Review & Inspection – Walkthroughs, Design Reviews, & Interviews
- Documenting Results:
  - Formal Report with Recommendations for Deviations, Discoveries, & Improvements

Non-Scenario Technique

Relative Ranking

- Purpose:
  - Determine Most Significant Areas of Concern
  - Rank Areas of Concern Before More Intensive Reviews
- Description:
  - Use of Index to Rank Hazards/Hazardous Situations
  - Index Based on 3 Questions ~ What Can Go Wrong? Impact? Likely?
- Type of Results:
  - Ordered List of Processes, Equipment, Operations, or Activities
  - Not Typically Used for Analysis of Safeguards
- Resource Requirements:
  - Basic Physical & Chemical Information; Single Analyst; 1 – 4 Days Duration
- Analysis Procedure:
  - Collect Basic Material/Process Information
  - Assign Relative Ranking Based on 3 Questions (Qualitative vs Quantitative)
  - Rank Hazards/Hazardous Situations
- Documenting Results:
  - Simple List Ranking Hazards/Hazardous Situations
  - Potential Identification of Safety Weaknesses and Corrective Measures

Non-Scenario Technique

Checklist Analysis

- Purpose:
  - Verification of System Status Using Written List of Requirements/Procedural Steps
- Description:
  - List of Known Hazards, Design Deficiencies, and Incidents
  - List of Requirements/Procedural Steps
  - List of Other Parameters (e.g., chemical properties, codes/standards)
- Type of Results:
  - Typically List with “No,” “Yes,” or “Not Applicable” & Associated Corrections
- Resource Requirements:
  - Information to Create Checklist; Single Analyst; 2 – 12 Days Duration
  - Creating Checklist is Intensive Effort
- Analysis Procedure:
  - Select Checklist
  - Perform Walkthrough, Design, Procedure, Codes/Standards Review
- Documenting Results:
  - Qualitative Report (w/ Completed Checklist) & Recommendations
  - Potential for Inherent Safety Review ~ Minimization, Moderation, & Simplification

Scenario Technique

What-If Analysis

- Purpose:
  - Brainstorming Approach to Identify Hazards/Hazardous Situations, or Event Sequences with Potential Undesirable Consequences ~ May Include Cause/Initiating Events
- Description:
  - Use of Facilitator, Scribe, & Team
  - Not Inherently Structured, Requires Skilled Facilitator
  - Ideally Divide Questions Based on Hazards and/or Process Areas
  - What If Can Be Effective & Efficient With Experienced Team/Facilitator
- Type of Results:
  - Random Tabular Listing of Hazardous Situations with Consequences & Safeguards
- Resource Requirements:
  - Supporting Information; Representative Team; 1 – 29 Days Duration
- Analysis Procedure:
  - Collect Chemical Data, Process Description, Drawings, & Operating Procedures
  - Seed Analysis Tables for Workshop Meetings For Team Brainstorming
- Documenting Results:
  - Qualitative Report (w/ Completed What If Analysis Worksheet) & Recommendations
  - Potential for Inherent Safety Review ~ Resolve “What-If Question”
  - May Provide Input into Further More Refine HE Analysis

Scenario Technique

What-If/Checklist Analysis

- Purpose:
  - Systematic Use of Checklist Using Brainstorming Approach to Identify Hazards/Hazardous Situations, or Event Sequences with Potential Undesirable Consequences ~ May Include Cause/Initiating Events
- Description:
  - Use of Facilitator, Scribe, & Team ~ Requires Skilled Facilitator
  - Structured Approach to Identify All Hazards/Hazardous Situations
- Type of Results:
  - Systematic Tabular Listing of Hazardous Situations with Consequences & Safeguards
- Resource Requirements:
  - Supporting Information; Representative Team; 1 – 31 Days Duration
- Analysis Procedure:
  - Collect Chemical Data, Process Description, Drawings, & Operating Procedures
  - Seed Analysis Tables for Workshop Meetings For Team Brainstorming
  - Qualitatively Determine Significant of Effects and Relative Recommendations
- Documenting Results:
  - Qualitative Report (w/ Completed What If Analysis Worksheet) & Recommendations
  - Potential for Inherent Safety Review ~ Resolve “What-If Question”
  - May Provide Input into Further More Refine HE Analysis

Scenario Technique

Hazard and Operability Study

- Purpose:
  - Careful, Systematic Review to Determine Whether Deviations Can Lead to Undesirable Consequences
  - Identification of Causes, Consequences, & Safeguards for Process Nodes
- Description:
  - Use of “Prescribed” Terminology – Guidewords + Parameters = Deviation
  - Use of Facilitator, Scribe, & Team ~ Requires Skilled Facilitator & Trained Team
  - Systematically Identify Hazard & Operability Problems
- Type of Results:
  - Deviations for Each Node Recorded in Table Format With Consequences & Safeguards
- Resource Requirements:
  - Extremely Detailed P&ID; Highly Skilled, Trained Team; 13 – 86 Days Duration
- Analysis Procedure:
  - Explicitly Define Purpose, Scope, & Objectives
  - Collect Supporting Information Prior to Workshop So Team Can Prepare
  - Determine Nodes, Standard Guidelines, Deviations, & Safeguards
  - Complete Node by Node
- Documenting Results:
  - Tabular Format with Separate Action Items

Scenario Technique

Failure Modes and Effects Analysis

- Purpose:
  - Identify Single Component/System Failure Modes, Causes, Effects, & Actions
  - How Can Equipment Fail, What Are Causes, & What Are Effects
- Description:
  - Evaluates How Equipment Can Fail and Effects of Failures on Process
  - Use of Facilitator, Scribe, & Team ~ Requires Skilled Facilitator & Trained Team
  - Systematically Evaluates @ Equipment/Component Level (e.g., pieces & parts)
- Type of Results:
  - Failure Modes, Causes, Effects, & Safeguards for Each Equipment in Table Format
- Resource Requirements:
  - Extremely Detailed P&ID, Equipment Functions; Trained Team; 7 – 42 Days Duration
- Analysis Procedure:
  - Define Problem (Boundaries) & Resolution Level ~ Typically Lowest Level Analysis
  - Detailed Equipment Descriptions & Unique System, Equipment, & Component Identifiers
  - List All Failure Modes with Specific Equipment, Then Analyze Cause/Effect/Actions
- Documenting Results:
  - Systematic & Consistent Tabulation of Effects from Equipment Failure
  - Equipment Identification Allows One-on-Correlation to System

Scenario Technique

Fault Tree Analysis

- Purpose:
  - Deductive Technique Focusing On A Single Incident or System Failure
  - Identify Combinations of Equipment Failures & Human Errors Resulting In Incidents
- Description:
  - Graphical Model That Displays Combinations of Equipment/Human Failures
  - Single Analyst (or Team) with Input & Review by Process Engineers
  - Systematically Evaluates “Top Event” With Specific Logic /Event Symbols & Definitions
- Type of Results:
  - System Failure Models with Boolean (and, or) Logic Gates to Describe Failures
- Resource Requirements:
  - Extreme System Knowledge; Qualified Analyst/Experienced Team; 9 – 100 Days Duration
- Analysis Procedure:
  - Define Problem Via Top Event & Boundary Conditions
  - Construct Fault Tree Model/Analyze Fault Tree Model
- Documenting Results:
  - Formal Report with System Description, Problem Definition, Assumptions, & FTA Models

Scenario Technique

Event Tree Analysis

- Purpose:
  - Inductive Technique Focusing On A Single Incident or System Failure
  - Graphic Representation of Possible Outcomes of Success/Failure of Protective Systems Following Specific Initiating Cause
- Description:
  - Graphical Listing of Incidents That Can Occur ~ Event Sequences
  - Single Analyst or Team for Brainstorming
- Type of Results:
  - Event Tree Models with System Sequence for Failures
- Resource Requirements:
  - Extreme System Knowledge; Trained Analyst; 6 – 80 Days Duration
- Analysis Procedure:
  - Identify Initiating Causes or Loss Events & Safeguards
  - Constructing Event Tree
  - Describing Resulting Event Sequence Outcomes
  - Determining Minimum Cut Sets (Shortest Branch)
- Documenting Results:
  - Formal Report with System Description, Problem Definition, Incident Initiating Cause, Assumptions, & Minimum Cut Sets

Scenario Technique

Cause-Consequence Analysis

- Purpose:
  - Blend of FTA & ETA
  - Graphic Representation to Identify Causes and Consequences of Potential Incidents
- Description:
  - Inductive Features of ETA with Deductive Features of FTA
  - Cause-Consequence Diagram Displays Relationship Between Outcomes & Causes
  - Typically Simple Systems Otherwise Graphically Overwhelming
- Type of Results:
  - Diagrams with Incident Sequences and Qualitative Descriptions of Potential Incident Outcomes
- Resource Requirements:
  - System & Safeguards Knowledge; Trained Analyst; Small Team; 6 – 70 Days Duration
- Analysis Procedure:
  - Selecting Event or Type of Incident & Identifying Safeguards
  - Develop Event Sequence Paths & Intermediate Events With Safeguard Failures
  - Evaluate Event Sequence Minimum Cut Sets
- Documenting Results:
  - Formal Report with System Description, Problem Definition, Incident Initiating Cause, Assumptions, Cause-Consequence Diagrams, & Minimum Cut Sets

What About Risk?

Consequence x Frequency = Risk

- Adequacy of Existing Safeguards
- Risk As Low As Reasonably Practicable
- Qualitative vs. Quantitative Analysis
  - Frequency = Initiating Event x Safeguard Failure
  - Consequence Severity
  - Frequency/Likelihood (Numeric vs. Descriptive)
- Control Analysis
  - Frequency Reduction ~ Preventative
  - Consequence Reduction ~ Mitigative
- Risk Binning
- Layer of Protection Analysis