COMPARISON OF PROCESS HAZARD ANALYSIS (PHA) METHODS

by Primatech Inc.

The hazard and operability (HAZOP) study is the most commonly used process hazard analysis (PHA) method. However, there are many other PHA methods available which may be more suitable depending on the circumstances. This article describes a variety of PHA methods and provides a comparison of their advantages and disadvantages.

Preliminary Hazard Analysis (PrHA)

PrHA identifies the hazards of a process and the hazardous situations they may produce. Possible causes, consequences and recommendations for protective measures are addressed. A criticality ranking may be assigned and used to prioritize protective measures.

Typically, PrHA is used to evaluate and prioritize hazards early in the life of a process as a precursor to more detailed hazard analysis studies. Generally, it is applied during conceptual design or at the R&D stage when there is little information available on design details or operating procedures. Commonly, it is used as a design review tool before a P&ID is developed. It is useful in making site selection decisions and in analyzing large facilities when circumstances prevent other techniques from being used.

The procedure for conducting a PrHA is:

1. Prepare and organize the study
2. Subdivide the process
3. Identify process hazards and hazardous situations
4. List causes
5. Specify consequences
6. Assign criticality ranking
7. Identify any recommendations
8. Document the results
9. Resolve recommendations
10. Follow-up on recommendations

Checklist

A checklist used as a hazard evaluation procedure employs prepared lists of questions relating to process safety to identify concerns and prompt the analysts to determine whether existing safeguards are adequate. Checklists are used to identify common hazards and ensure compliance with procedures, codes of practice, regulations, etc. Checklist questions are based on experience and knowledge of safety issues for the process and applicable codes, standards and regulations.

Checklists can be applied to virtually any aspect of a process such as equipment, materials, procedures, etc. Their application requires knowledge of the process and its procedures and an understanding of the meaning of the checklist questions. Checklists may become outdated and they should be audited and updated regularly.

The procedure for performing a checklist study is:

1. Prepare and organize the study
2. Select or generate the checklist
3. Perform the study
4. Identify any recommendations
5. Document the results
6. Resolve recommendations
7. Follow-up on recommendations

What-If (WI) and What-If Checklist (WIC)

WI studies involve posing questions relating to initiating events to identify hazard scenarios for a process. The PHA team brainstorms questions in a WI study. The team starts with a prepared list of questions in a WIC study, although almost always additional questions are added as a study proceeds. Sometimes PHA teams develop questions based on the HAZOP thought process by thinking through what questions would arise if a HAZOP study were being performed.

WI methods are well-suited to examining the impacts of proposed changes in Management of Change (MOC) PHA studies because the questions can be tailored to the change and the areas affected by it. They can be used to study virtually any aspect of a process such as equipment, procedures, control systems, management practices, etc. Team leaders should be experienced with the technique since it is provides less structure than other PHA methods.

The procedure for conducting a WI or WIC study is:

1. Prepare and organize the study
2. Subdivide the process
3. Develop questions
4. Identify hazards and/or hazard scenarios
5. Specify consequences
6. Identify safeguards
7. Optionally, identify enablers
8. Perform risk ranking
9. Identify any recommendations
10. Document the results
11. Resolve recommendations
12. Follow-up on recommendations

Hazard and Operability (HAZOP) Study

The HAZOP method is used to identify hazard scenarios with impacts on people and the environment as well as operability scenarios where the concern is the capacity of the process to function. Originally, it was developed for fluid processes but it has also been applied to non-fluid systems such as materials handling, drilling operations, aerospace systems, etc. Currently, it is the most commonly used technique in the process industries.

The HAZOP method focuses on investigating *deviations* from design intent such as “no flow” at a location in the process where flow is intended or “high pressure” in a vessel which should not exceed a pressure limit. By definition, deviations are potential problems, e.g., no flow in a transfer line or overpressuring a vessel. Deviations from design intent are generated by applying *guide words* to process *parameters* at different locations (*nodes*) throughout the process, e.g., for an inlet line to a vessel, No + Flow = No Flow, or for a vessel, High + Pressure = High Pressure.

A standard list of seven guide words is used: No, More, Less, As Well As, Part Of, Reverse, and Other Than. The team chooses appropriate parameters for each node, e.g., flow, pressure, temperature, composition, level, addition, cooling, location, etc. The use of guide words with parameters provides the opportunity to explore deviations from design intent in every conceivable way thus helping to ensure completeness of the PHA study.

The procedure for conducting a HAZOP study is:

1. Prepare and organize the study
2. Subdivide the process
3. Select process parameters
4. Specify parameter intention
5. Generate deviations
6. Identify causes of deviations
7. Specify consequences
8. Identify safeguards
9. Optionally, identify enablers
10. Perform risk ranking
11. Identify any recommendations
12. Document the results
13. Resolve recommendations
14. Follow-up on recommendations

Failure Modes and Effects Analysis (FMEA)

FMEA is a hazard evaluation procedure in which failure modes of system components, typically, process equipment, are considered to determine whether existing safeguards are adequate. Failure modes describe how components fail (e.g., open, closed, on, off,

leaks, etc.). The effects of each failure mode are the process responses or incident resulting from the component failures, i.e., hazard scenario consequences. A FMEA becomes a FMECA (Failure Modes and Effects and Criticality Analysis) when a criticality ranking is included for each failure mode and effect. A criticality ranking is the same as a risk ranking.

FMEA is used extensively in the aerospace, nuclear, and defense industries. Typically, it is used in the process industries for special applications such as Reliability Centered Maintenance (RCM) programs and the analysis of control systems.

FMEA can be conducted at different levels of resolution. For PHA purposes, usually it is conducted at the equipment level, e.g., valves, pumps, lines, etc. For RCM purposes, usually it is conducted at the equipment component level, e.g., motor, shaft, impeller, casing, seal, bearings, etc. for a pump.

The procedure for conducting a FMEA is:

1. Prepare and organize the study
2. Subdivide the process
3. List process equipment
4. Identify equipment failure modes
5. Optionally, identify causes of failure modes
6 Specify effects (consequences)
7. Identify safeguards
8. Perform risk ranking
9. Identify any recommendations
10. Document the results
11. Resolve recommendations
12. Follow-up on recommendations

Major Hazard Analysis (MHA) / Direct Hazard Analysis (DHA)

MHA was developed specifically to support process safety studies [A1, A2]. It is used to identify major hazard scenarios involving fires, explosions, toxic releases and reactivity excursions. DHA is an extension of MHA used to address any type of hazard.
MHA employs a structured approach to identify loss of containment scenarios. Causes of loss of containment can be direct, e.g., valves left open or ruptures in lines or vessels, or indirect, e.g., runaway reactions resulting in releases through pressure relief devices or vessel and piping rupture. MHA constrains brainstorming to such scenarios within a structured framework to guide the identification of initiating events using standard checklists. Brainstorming focuses on specific categories of initiating events to focus the team’s brainstorming without narrowing their vision. The checklists provide guidance to the team and help assure completeness. They can be customized for specific facilities or types of processes. The method prompts consideration of items not already in the checklists. MHA uses a process subdivision similar to other PHA methods.

DHA extends MHA to address other hazards such as over-pressurization, entrapment by moving equipment, etc. Each hazard type uses a structured list of categories of initiating events and ways they can occur. Such lists can be developed for any hazard.

The procedure for conducting a MHA or DHA is:

1. Prepare and organize the study
2. Subdivide the process
3. Identify initiating events
4. Specify consequences
5. Identify safeguards
6. Optionally, identify enablers
7. Perform risk ranking
8. Identify any recommendations
9. Document the results
10. Resolve recommendations
11. Follow-up on recommendations

Process Hazard Review (PHR)

PHR was developed for use with operating plants as an alternative to HAZOP [A3]. It addresses major hazards. There are variants that address other types of hazards and environmental releases. It is based on the premise that most major hazard process incidents involve loss of containment. PHR uses prompts covering the range of mechanisms for loss of containment to identify hazard scenarios. The method has been extended to address other hazard types (Operational Hazard Review) and environmental releases (Environmental Hazard Review).

The procedure for conducting a PHR is:

1. Prepare and organize the study
2. Subdivide the process
3. Select prompt / guide word
4. Describe hazardous event scenarios
5. Identify causes of hazardous event scenarios
6. Specify consequences
7. Identify safeguards / existing controls
8. Perform risk ranking
9. Identify any recommendations
10. Document the results
11. Resolve recommendations
12. Follow-up on recommendations

Fault Tree Analysis (FTA)

FTA is not really comparable to standard PHA methods. It does not identify a full set of hazard scenarios for a process. Rather, it is used to identify the causes of a particular incident (called a top event) using deductive reasoning. Often, it is used when other PHA techniques indicate that a particular type of accident is of special concern and a more thorough understanding of its causes is needed. Thus, it is a useful supplement to other PHA techniques. Sometimes FTA is used in the investigation of incidents to deconstruct what happened. FTA is also used to quantify the likelihood of the top event. It is best suited for the analysis of highly redundant systems.

FTA identifies and graphically displays the combinations of equipment failures, human failures and external events that can result in an incident. Computer programs are used to provide graphical representations of fault trees and to calculate top event likelihoods. FTA is not a technique that lends itself to a team-based study. Typically, one or two people construct a fault tree. It requires different training and resources than other PHA techniques.

The procedure for conducting a FTA is:

1. Prepare and organize the study
2. Construct fault tree
3. Analyze fault tree
4. Quantify fault tree
5. Evaluate results
6. Identify any recommendations
7. Document the results
8. Resolve recommendations
9. Follow-up on recommendations

Event Tree Analysis (ETA)

ETA is not really comparable to standard PHA methods. It does not identify a full set of hazard scenarios for a process. Rather it is used to identify the possible outcomes following the success or failure of protective systems after the occurrence of a given starting event and, optionally, to calculate the frequencies of the outcomes. Event trees graphically display the progression of event sequences beginning with a starting event, proceeding to control and safety system responses, and ending with the event sequence consequences.

ETA helps analysts to determine where additional safety functions will be most effective in protecting against the event sequences. Typically, ETA is used to analyze complex processes that have several layers of safety systems or emergency procedures to respond to starting events. ETA is not a technique that lends itself to a team-based study. Typically, one or two people construct an event tree.

The procedure for conducting an ETA is:

1. Prepare and organize the study
2. Identify a starting event
3. Identify controls and safeguards that respond to the event
4. Construct the event tree
5. Describe the event sequence outcomes
6. Optionally, calculate the frequencies of the outcomes
7. Identify any recommendations
8. Document the results
9. Resolve recommendations
10. Follow-up on recommendations

Cause-Consequence Analysis (CCA)

CCA is a blend of fault tree analysis and event tree analysis that produces a CCA diagram combining fault and event trees. It is used to identify causes and consequences of hazard scenarios. The CCA diagram displays the relationships between the incident outcomes (consequences) and their causes and it can depict and evaluate multiple scenario outcomes, including recovery paths where the operator, or system, recovers or mitigates the consequences, as well as the worst consequence path. CCA is commonly used when the failure logic of hazard scenarios is simple.

The procedure for conducting a CCA is:

1. Prepare and organize the study
2. Select an event to be analyzed
3. Identify safety functions that respond to the event
4. Develop the event sequence paths resulting from the event
5. Develop the combinations of basic failures that result in the starting event and safety function failures
6. Evaluate the event sequences
7. Identify any recommendations
8. Document the results
9. Resolve recommendations
10. Follow-up on recommendations

Bow-Tie Analysis (BTA)

BTA is a less formal variation of Cause-Consequence Analysis. It uses a combination of high-level fault and event trees to produce a diagram resembling a bow tie. Hazards and initiating events appear on the pre-event side (left side) and impacts (consequences) appear on the post-event side (right side). The focal point of the diagram is the specific loss event that ties together the initiating events and consequences. There is a time progression from the left to the right of the diagram.

Associated prevention and mitigation safeguards are shown on either side of the loss event and they are viewed as barriers, some of which may apply to more than one cause.

BTA is used for screening hazards of well-understood processes and to perform an initial analysis for existing processes or in the middle stages of process design.

The procedure for conducting a BTA is:

1. Prepare and organize the study
2. Select an event to be analyzed
3. Develop the pre-event side of the diagram
4. Develop the post-event side of the diagram
5. Identify any recommendations
6. Document the results
7. Resolve recommendations
8. Follow-up on recommendations

Comparison of PHA Methods

Method	Advantages	Disadvantages
PrHA	Easy to understand Fast to perform	Requires careful judgment Not a detailed PHA method
Checklist	Easy to use and provides results quickly Level of detail can be varied Communicate information well Effective way to take advantage of lessons learned	Does not help in identifying new, or unrecognized hazards May overlook unusual hazards or novel elements of a process No cause and effect analysis Usually, requires some subjective interpretation Limited to the experience of the author Repetitive nature can lead to errors May not apply to the particular situation Provides a minimum level of hazard evaluation

WI and WIC	Easily understood Flexible Less effort / time Can help to identify scenarios that involve interactions between different parts of the process	Loose structure Results particularly dependent on the skill, experience and thoroughness of users No assurance that the breadth or depth of the questions considered is adequate
HAZOP	Viewed as the most effective of traditional PHA methods Provides assurance that hazard scenarios have been identified Addresses both safety and operability	Difficult to exclude operability scenarios Difficult to consider all aspects of intention in a reasonable time period Effort involved can be significant Focuses on individual nodes and may miss some hazard scenarios that involve interactions between nodes
FMEA	Systematic, element-by-element procedure that helps ensure completeness Easily understood and used by engineers Easily updated for design changes or facility modifications	Not efficient for identifying combinations of equipment failures Human failures are not generally examined although the effects of misoperation can be described by an equipment failure mode or by the causes of a failure External events are not easily addressed
MHA / DHA	Focuses exclusively on hazard scenarios, i.e., does not address operability scenarios Time required is substantially less than traditional methods Structured approach Readily understood by PHA teams All hazard scenarios for a node appear in a single worksheet Current PHA studies can be converted easily into MHA format	Does not address operability scenarios

PHR	Structured method Quickly identifies and assesses major hazard scenarios Operations personnel can share their experience effectively	Focuses more on what team members know, not what they don't know Generates more general recommendations rather than specific ones Proprietary method
FTA	Thorough and systematic	Can be time consuming Binary representation of faults (either success or failure, no partial failures)
ETA	Easy to understand	Can be time consuming Binary representation of failures (either success or failure, no partial failures)
CCA	Provides a detailed graphical depiction of hazard scenarios	CCA diagram can become complex
BTA	Easy to understand	Provides only a simple analysis Does not provide a formal way to identify loss events Can become complex for larger processes