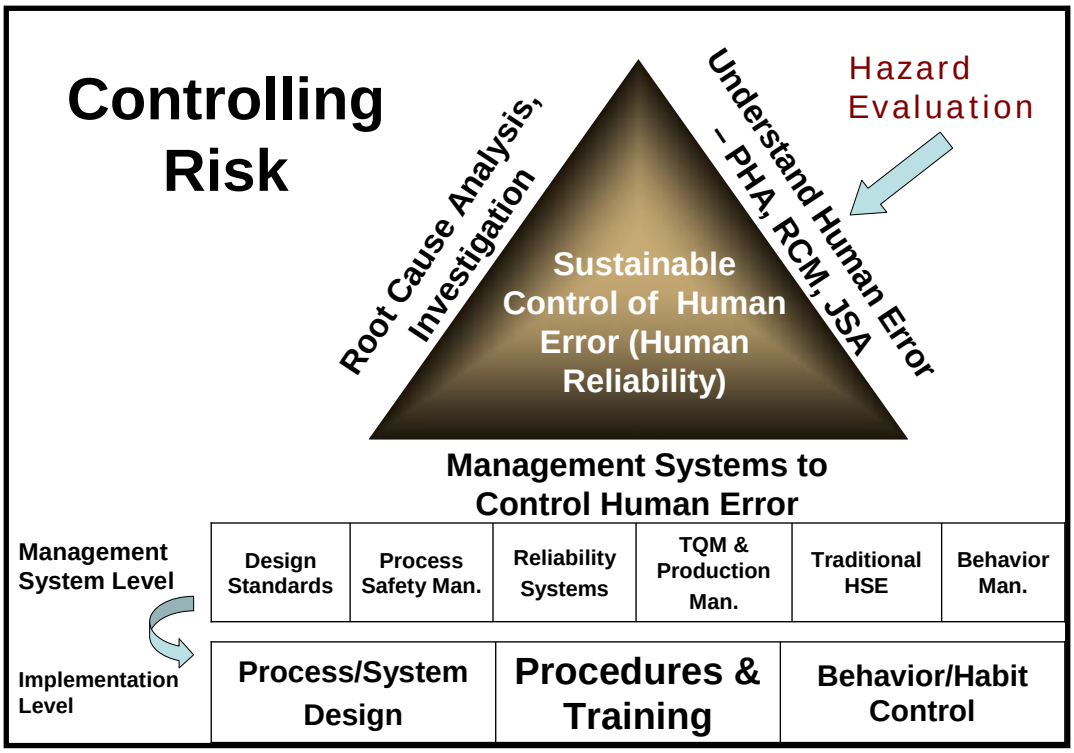
Selection of Hazard Evaluation Techniques

William Bridges
Process Improvement Institute, Inc. (PII)
1938 Riversound Drive
Knoxville, TN 37922 USA
+1-865-675-3458
wbridges@p-i-i-i.com
www.p-i-i-i.com

The ability to ensure process safety at a facility is influenced by many things: for example, employing appropriate technology in design and construction, anticipating the effects of external circumstances, understanding and dealing with human behavior, getting high reporting of near misses to learn from incidents, and having effective management systems. However, all of these efforts depend on a successful hazard evaluation program; without these evaluations, the company will not know what layers of protection are needed.



A successful hazard evaluation program requires tangible management support; sufficient, technically competent people (some of whom must be trained to use hazard evaluation techniques); adequate, up-to-date information and drawings; and selection of the techniques (matched to the complexity and hazard of the process). Fortunately, a variety of flexible hazard evaluation techniques exist. Below is a simple listing of generally accepted techniques:

Qualitative Techniques: These methods help a multi-disciplinary team (1) identify potential accident scenarios and (2) evaluate the scenario in sufficient detail to make a reasonable judgment of risk. If the team is confused on the risk, a scenario identified in a qualitative hazard review may be further analyzed using one or more of the quantitative techniques.

Preliminary Hazard Analysis (PreHA): A technique that is derived from the U.S. Military Standard System Safety Program Requirements. The Preliminary Hazard Analysis is often used to evaluate hazards early in the life of a process. A Preliminary Hazard Analysis is generally applied during the conceptual design or R&D phase of a process plant and can be very useful when making site selection decisions. It is also commonly used as a design review tool before a process P&ID is developed

Checklist (traditional)*:* A detailed list of desired system attributes or steps for a system or operator to perform. Usually written from experience and used to assess the acceptability or status of the system or operation compared to established norms.

What-If Analysis: A brainstorming approach in which a group of experienced people familiar with the subject process ask questions or voice concerns about possible undesired events. The method does not use guide words to help in the brainstorming.

What-If/Checklist Analysis: A brainstorming approach in which a group of experienced people familiar with the subject process ask questions or voice concerns about possible undesired events. The method is similar to What-if alone, with the difference being that broad categories of types of concerns are used to structure the analysis.

2 Guide Word Analysis*:* A systematic method in which potential operating problems are identified by asking what would happen is a step in a procedure were (1) skipped or (2) performed incorrectly. This method is applicable to any procedure (startup, shutdown, online maintenance, or normal batch operations), but does not apply to continuous operating mode.

Hazard and Operability (HAZOP) Analysis*:* A systematic method in which potential operating problems are identified using a series of guide words to investigate process deviations. Can be applied to any mode of operation of a flow process and can also be applied to any procedure or flowchart.

Failure Modes and Effects Analysis (FMEA)*:* A systematic, tabular method for evaluating and documenting the effects of known types of component failures. Applies to electrical/mechanical systems. Can also be applied to flow systems where very high reliability factors are needed (such as fire-fighting water supply systems).

Quantitative Techniques: These do not identify possible accident scenarios, but they instead aid in risk judgment by provide more detailed, statistical evaluations of the risk of a specific scenario.

Layer of Protection Analysis (LOPA)*:* A method that uses pre-defined values for initiating events, independent protection layers, and consequences to provide an order-of-magnitude estimate of risk. LOPA applies to a single cause-consequence pair. Scenarios are identified elsewhere (typically in a qualitative hazard evaluation).

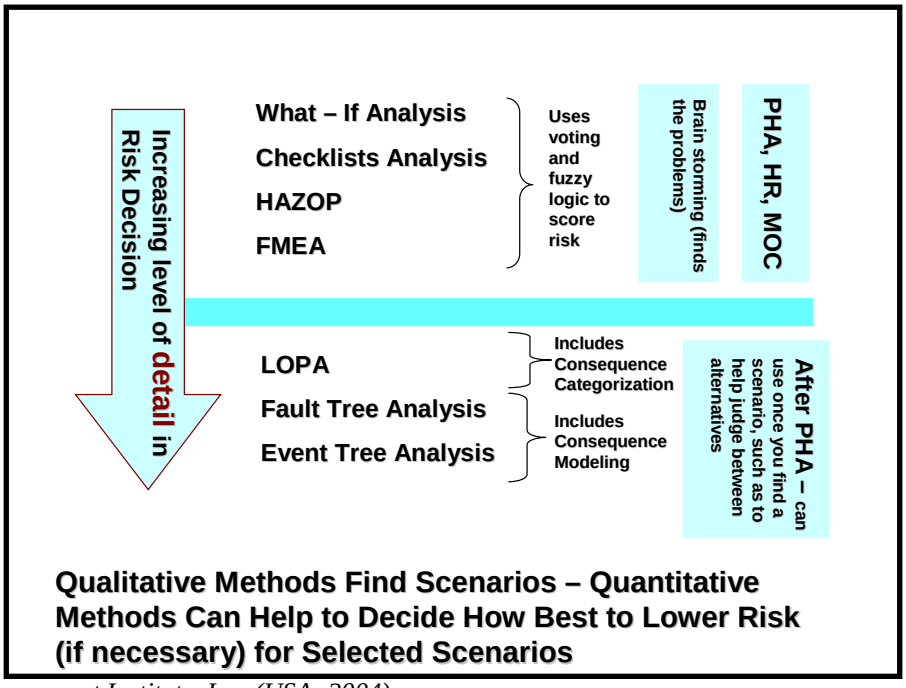
Dow Fire and Explosion Index (F&EI)*:* A method, developed by Dow Chemical Company, for ranking the relative potential fire and explosion risk effect radius and property damage/business interruption impacts associated with a process. Analysts calculate various hazard and exposure indexes using material characteristics and process data.

Dow Chemical Exposure Index (CEI): Address five types of factors that can influence the effects of release of the material: (1) acute toxicity, (2) volatile portion of material which could be released, (3) distance to areas of concern, (4) molecular weight of the substance, and (5) various process parameters such as temperature, pressure, reactivity, and so forth. The CEI is the product of values assigned for each of the factors of concern using arbitrarily defined numerical scales.

Fault Tree Analysis (FTA): A logic model that graphically portrays the combinations of failures that can lead to a specific main failure or incident of interest (Top event). This method using Boolean Logic (And & Or logic gates). Assigning statistical values to each end point on a branch allows the calculation of risk.

Event Tree Analysis (ETA)*:* A logic model that graphically portrays the combinations of events and circumstances in an incident sequence. Assigning statistical values to each branch point (failure or condition) allows the calculation of composite risk starting from a defined initiating event.

Human Reliability Analysis (HRA) event tree*:* A graphical model of sequential events in which the tree limbs designate human actions and other events as well as different conditions or influences upon these events. Assigning statistical values to each branch point (correct or incorrect performance of a step) allows the calculation of composite risk starting from a defined first step.



Each technique presented in this paper has been applied in the chemical process industry and is appropriate for use in a wide variety of situations. In an effective hazard evaluation program, excellent

performance is based on successfully executing individual hazard evaluations. A successful hazard evaluation can be defined as one in which (1) the need for risk information has been met, (2) the results are of high quality and are easy for decision makers to use, and (3) the study has been performed with the minimum resources needed to get the job done. Obviously, the technique selected has a great bearing on each hazard evaluation's success.

Who should decide which hazard evaluation technique to use?

It is appropriate and necessary that management define the basic charter for a hazard evaluation: the main objective of the study, the type of decision making information (results) needed, and the initial resources and deadlines for performing the work. But the hazard evaluation team leader should select the most appropriate hazard evaluation method to fulfill the study's charter.

Many organizations develop policies that specify that analysts use certain types of hazard evaluation techniques. Usually, providing this guidance does not present a problem as long as the hazard analyst can use an alternate hazard evaluation method if it can better satisfy the study's charter. For example, suppose a corporate safety group has decided that facilities under their jurisdiction must use the HAZOP analysis technique to perform the majority of hazard evaluations. The hazard evaluation team leader for a major process modification project is requested to perform an analysis procedure for startup of a compressor. In this case the team leader believes, based on his experience, that the HAZOP approach is not the most efficient method to investigate the ways humans can make mistakes, he believes the 7 Guide Words of HAZOP of procedures will overwork the analysis. Instead, the leader wants to use the 2 Guide Word (this pre-dates the HAZOP method) technique, which, for this type of analysis problem, he has seen work more efficiently than HAZOP. Management listens to the leader's recommendation and allows him to use the 2 Guide Word technique. The same leader might also choose the FMEA method for evaluating the extruder portion of the system.

Hazard evaluation specialists should be allowed significant freedom to select the proper method(s) for a hazard evaluation.

Since selecting an appropriate hazard evaluation technique is more an art than a science, there may be no "best" method for a particular application. This paper discusses a strategy for selecting a method that is likely to contribute to the success of a study. *The approach below is similar to the approach in the Guidelines for Hazard Evaluation Procedures, 2nd Ed, 1992, CCPS/AIChE.*

Factors Influencing the Selection of Hazard Evaluation Techniques

Each hazard evaluation technique has its unique strengths and weaknesses. Understanding these attributes is prerequisite to selecting an appropriate hazard evaluation technique. The process of selecting an appropriate hazard evaluation technique may be a difficult one for the inexperienced practitioner because the "best" technique may not be apparent. As hazard analysts gain experience with the various hazard evaluation methods, the task of choosing an appropriate technique becomes easier and somewhat instinctive. The thought process behind selecting hazard evaluation techniques is complex, and a variety of factors can influence the decision-making process. The table below lists six categories of factors that analysts should consider when selecting a hazard evaluation technique for a specific application. The importance that each of these categories has on the selection process may vary from facility to facility, company to company, and industry to industry. However, the following general observations about the relative significance of these factors should be true for nearly every situation.

Categories of factors that could influence the selection of hazard evaluation techniques

- Motivation for the study
- Type of results needed
- Type of information available to perform the study
- Characteristics of the analysis problem
- Perceived risk associated with the subject process or activity
- Resource availability and analyst/management preference

The following sections discuss each category and provide examples of factors that analysts should consider when selecting an appropriate hazard evaluation technique.

Motivation for the Hazard Evaluation

This category of factors should be the most important to every hazard analyst. Performing a hazard evaluation without understanding its motivation and without having a well-defined purpose is likely to waste safety improvement resources. A number of issues can shape the purpose of a given study. For example, what is the impetus for doing the study in the first place? Is the study being chartered as part of a policy for performing hazard evaluations of new processes? Are insights needed to make risk management decisions concerning the improvement of a mature, existing process? Or is the study being done to satisfy a regulatory or legal requirement?

Hazard analysts responsible for selecting the most appropriate technique and assembling the necessary human, technical, and physical resources must be provided a well-defined, written purpose so that they can efficiently execute the study's charter.

Type of Results Needed

Depending on the motivation for a hazard evaluation, a variety of results could be needed to satisfy the study's charter. Defining the specific type of information needed to satisfy the objective of the hazard evaluation is an important part of selecting the most appropriate hazard evaluation technique. The following are five categories of information that can be produced from hazard evaluations:

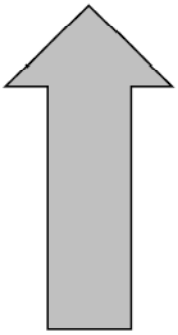
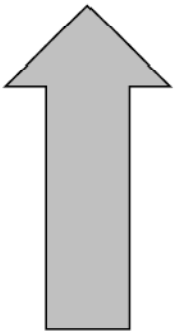
- List of hazards
- List of potential incident situations
- List of alternatives for reducing risk or areas needing further study
- Prioritization of results
- Input for a quantitative risk analysis

Some hazard evaluation techniques can be used solely to identify the hazards associated with a process or activity. If that is the only purpose of the study, then a technique can be selected that will provide a list or a "screening" of areas of the process or operation that possess a particular hazardous characteristic. Nearly all hazard evaluation techniques can provide lists of potential incident situations and possible risk reduction alternatives (i.e., recommendations); a few of the hazard evaluation techniques can also be used to prioritize the recommendations based on the team's perception of the level of risk associated with the situation that the recommendation addresses. If an organization can anticipate that their need for risk management information is not likely to be satisfied by a qualitative analysis, then a hazard analyst may elect to use a hazard evaluation technique that provides more definitive input as a basis for performing a LOPA, FTA, ETA, in the event that such an analysis is needed.

Type of Information Available to Perform the Study

There are two conditions that define what information is available to the hazard evaluation team: (1) the stage of life the process or activity is in when the study needs to be performed and (2) the quality and currentness of the available documentation. The first condition is fixed for any hazard evaluation, and the analyst cannot do anything to change it. The table below shows what information becomes available through the plant's evolution.

Typical information available to hazard analysts

Type of information	Increasing level of detail	Time when information becomes available from project inception
▪ Specific operating experience ▪ Operating procedures ▪ Existing equipment ▪ Piping and instrumentation diagrams (P&IDs) ▪ Process flow diagrams (PFDs) ▪ Experience with similar processes ▪ Material inventories ▪ Basic process chemistry ▪ Material, physical, and chemical data		

CCPS/AIChE, Guidelines for Hazard Evaluation Procedures

The stage of life of the process establishes the practical limit of detailed information available to the hazard evaluation team. For example, if a hazard evaluation is to be performed on the conceptual design of a process, it is highly unlikely that an organization will have already produced a P&ID for the proposed process. Thus, if the analyst must choose between HAZOP and What-If Analysis, then this "phase-of-life" factor would dictate that the What-If Analysis method should be used, since there is not enough information to perform an adequate HAZOP analysis. (The techniques which are commonly used for hazard evaluations at various phases of a new project are discussed later in this paper). ***Ultimately, if the analysts believe that, because of the lack of information, the objectives of the study cannot be met using an appropriate hazard evaluation technique, they should recommend to management that their objectives be reexamined or the study be delayed until sufficient information becomes available.***

The second condition deals with the quality and currentness of the documentation that does exist. For a hazard evaluation of an existing process, hazard analysts may find that the P&IDs are not up-to-date or do not exist in a suitable form. Using any hazard evaluation technique on out-of-date process information is not only futile, it is a waste of time and resources (and it is also dangerous since the results may falsely be considered valid). Thus, if all other factors point to using a technique (e.g., the HAZOP analysis technique) for the proposed hazard evaluation that requires such information, then the analysts should ask management to have the necessary, up-to-date process drawings and operating procedures created. ***An important part of an overall hazard evaluation program is establishing a foundation to support hazard evaluations. Good planning in the creation of this information (drawings, operating procedures, online maintenance procedures) can help avoid delays in the performance of hazard evaluations.***

Characteristics of the Analysis Problem

To choose a hazard evaluation technique, an analyst should look at certain characteristics of the plant or process being studied. These characteristics can be divided into five areas: (1) the complexity and size of the problem, (2) the type of process, (3) the type of operation(s) included in the process, (4) the nature of the inherent hazards, and (5) the incidents or situations of concern.

The ***complexity and size*** of the problem are important because some hazard evaluation techniques can get bogged down when used to analyze extremely complicated problems. The complexity depends of factors such as chemistry, reaction rates, operating conditions far from ambient, the number and types of hazards and effects being analyzed (e.g., toxic, fire, explosion, economic, or environmental), and number of interactions between humans and machine. The size of a problem is a function of the number of processes or systems being analyzed, the number of pieces of equipment in each process or system, and the number of operating steps. It is particularly important that hazard analysts select a level of resolution that is compatible with the purpose of the study. For example, if a large facility is to be analyzed, a prudent hazard evaluation team leader should divide the facility into as many smaller pieces as necessary for analysis. Different techniques may be used to analyze each part of the process, depending upon the characteristics of each analysis problem. However, if the purpose of the hazard evaluation is primarily to screen hazards (e.g., develop emergency response plans), analysts should choose a level of resolution that looks at systems rather than individual components. For emergency planning purposes, an analyst might use a What-If Analysis or PreHA to identify general types of incident sequences that can have an impact on the plant population.

For many hazard evaluation techniques, considering a larger number of equipment items or operating steps will increase the time and effort needed to perform a study. For example, using the FMEA technique will generally take 3 to 4 times more effort for a process containing 100 equipment items than for a process containing 20 items. The HAZOP meeting time for analyzing a batch reactor system consisting of 50 operating steps will take about 60 to 70% longer as for a batch process with 25 steps. Thus, the types and number of hazards and effects being evaluated increases (slightly non-linear) to the size of the system under review.

The ***type of process*** also affects the selection of a hazard evaluation technique. Individual processes can be composed of one or more of these process types. However, certain hazard evaluation techniques are better suited for particular processes than others. For example, the FMEA approach has a well-deserved reputation for efficiently analyzing the hazards associated with electronic and computer systems, whereas the HAZOP Study approach may not work as well for these types of systems

The ***type of operations*** included in the subject process also influences the selection of hazard evaluation techniques. Whether an operation is (1) a fixed facility or a transportation system; (2) permanent or transient; and (3) continuous, semi-batch, or batch can affect the selection of techniques. All of the techniques mentioned here can be used for analyzing fixed facilities or for transportation operations.

Because potential incidents involving transportation systems typically involve single, discrete events (e.g., vehicle failures due to impact), single-failure analysis methods such as FMEA, What-If Analysis, or What-If/Checklist Analysis are used more often than FTA. However, sometimes ETA is used to consider the combination of circumstances surrounding a spill from a transport vehicle.

The permanency of the process can affect the selection decision in the following way: if all other factors are equal, analysts may use a more detailed, exhaustive approach if they know that the subject process will operate continuously over a long period of time. For example, a HAZOP table listing the detailed evaluation of types of upsets, causes, consequences, safeguards, etc., could be used in an operator training program. However, analysts are cautioned to recognize that a temporary operation can present significant hazards and could justify the use of a more detailed hazard evaluation technique.

Finally, some methods such as What-If Analysis, What-If/Checklist Analysis, HAZOP Analysis, ETA, and HRA are better able to analyze batch processes than others (e.g., FTA, FMEA, PreHA) because the latter methods cannot easily deal with the need to evaluate the time-dependent nature of batch operations.

The ***nature of the hazards*** associated with the process has a minor influence on the selection of a hazard evaluation technique. Toxicity, fire, explosion, and reactivity hazards can all be analyzed with any of the hazard evaluation techniques.

The charter of a hazard evaluation may address a variety of ***types of failures, events, or situations of concern***. Whether a study focuses on (1) single failures versus multiple failures; (2) simple loss of containment events; (3) loss of function events; (4) process upsets; or (5) hardware, procedure, software, or human failures can affect the technique selection decision. The biggest influence in this category of factors is whether the analysis is directed at evaluating complex, multiple failure situations. FTA, ETA, and HRA techniques are primarily used for these situations. Single-failure-oriented methods such as HAZOP Analysis and FMEA are not normally used for this purpose, although they can be extended to evaluate a few simple incident situations involving more than one event. On the other hand, HAZOP, What-if, and FMEA will need to be done to help build the list of accident scenarios before starting a FTA or ETA. The remaining factors in this category have a relatively minor impact on the selection process.

Perceived Risk of the Subject Process or Activity

If all hazard evaluations were perfect, then it would not matter which hazard evaluation technique is used or who performs the analysis. But, unfortunately, neither the techniques, analysts, teams, nor studies can ever be perfect. Neither a hazard evaluation technique nor an analyst can guarantee that all possible incident situations involving a process have been identified. Organizations deal with the limitation of completeness in two main ways. First, they use interdisciplinary teams to perform the analysis, capitalizing on the team members' combined experience. This "many heads are better than one" strategy is the key to performing high-quality hazard evaluations when using certain techniques (e.g., HAZOP Analysis, What-If/Checklist Analysis). Second, organizations tend to use more systematic techniques for those processes that they believe pose higher risk (or, at least, for situations in which incidents are expected to have severe consequences). Thus, the greater the perceived risk of the process, the more important it is to use hazard evaluation techniques that minimize the chance of missing an important incident situation.

The most important experience factor is the length of time over which the experience is gained. Has the process been operating for over 30 years, and are there many such processes operating within the organization and the industry? Or is the process relatively new? For a new process involving first-of-its kind technology that is still in the design phase, an organization may have absolutely no experience with the subject process. Sometimes, there may be some similar company or industry experience that members of an organization can draw upon to derive their understanding of risk. The next experience factor deals with the actual operating record of the process. Have there been frequent, high-consequence incidents? Or have there only been a few minor incidents and near misses? Sometimes a process will have operated for many years and never have experienced a major incident, even though the potential has always existed. The last experience factor deals with the current relevance of the experience base to the subject process. There may have been many changes to the process that invalidated the operating experience as a current indicator of process risk. Or there may have been only a few minor changes over the years that have been adequately dealt with by the organization's management of change policy. Typically, when (1) the subject process has operated relatively free of incidents over a long time and the potential for a high-consequence incident is perceived to be low, and (2) there have been few changes to the process that would invalidate this experience base, then organizations will tend to select less exhaustive, less systematic, more experience-based hazard evaluation techniques, such as Checklist Analysis. When the opposite is

perceived, more rigorous, predictive techniques are generally preferred, such as HAZOP Analysis, What-If/Checklist Analysis, and LOPA.

Resource Availability and Preference

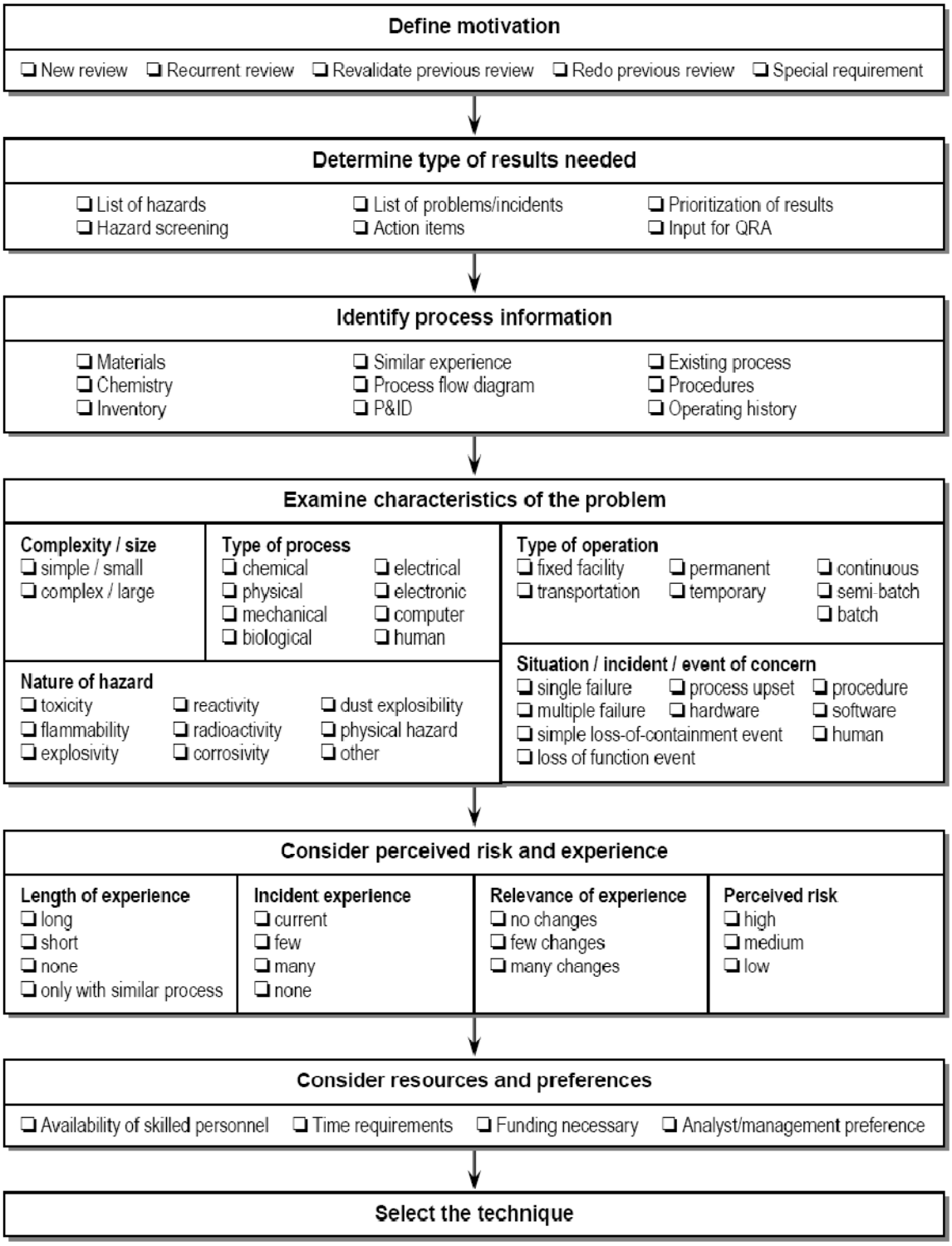
A variety of other factors can influence the selection of hazard evaluation techniques. Some factors that customarily affect technique selection are: (1) availability of skilled and knowledgeable personnel, (2) target dates by which to perform the study, (3) financial resources, (4) preference of the hazard analysts, and (5) preference of the manager(s) that charters the hazard evaluation. Generally, two types of personnel must be available for the hazard evaluation: skilled leaders and practitioners of the particular hazard evaluation technique chosen and people knowledgeable in the process or activity being analyzed. Many hazard evaluation techniques require the creative interaction of participants on a team. Team meetings can typically last for days, weeks, or months, depending upon the complexity of the subject process. Other techniques (e.g., FTA) may be performed primarily by individuals working alone. However, these detailed, single-analyst approaches require a "gestation period" to enable the analyst to create realistic models of the causes of potential incidents. Team situations may not be as helpful when using these techniques; however, these models may be constructed based on information derived from a team meeting or may efficiently be reviewed in a team meeting environment. Altogether, schedule constraints should take a back seat to other technical concerns.

Hazard evaluations done on a shoestring budget, marginally staffed, and under tight schedule constraints are usually not destined for success. ***The quality of the results from a hazard evaluation is inevitably a strong function of the quality of the team's effort.*** If adequate in-house personnel are unavailable to lead hazard evaluations, then an organization should acquire training for its prospective hazard analysts. Under tighter schedule constraints, outside consultants can be used to lead and document hazard evaluations.

Decision-Making Process for Selecting Hazard Evaluation Techniques

Each hazard evaluation technique has unique strengths and weaknesses. Moreover, each industry, organization, facility, and process/activity will have unique objectives and needs when it comes to performing hazard evaluations. The six categories of factors discussed earlier may have varying degrees of importance, depending upon the circumstances for each particular application of hazard evaluation techniques. Thus, it is difficult to construct a universal decision-making flowchart that would be correct for every organization and facility. However, it is possible to suggest a logical order for considering the factors. Certainly, the factors involving motivation and type of results should be most important to every organization; these factors provide the basic definition for satisfying the need for greater risk understanding, which likely precipitated the charter for a hazard evaluation. The information available, characteristics of the problem, and perceived risk may have varying degrees of importance placed upon them, depending upon the culture of the sponsoring organization and facility.

The flowchart on the next page provides a framework for getting the input to decide on which techniques to use for a hazard evaluation. The table that follows provides a side-by-side comparison of factors to help the analyst decide which hazard evaluation best fits the input factors.



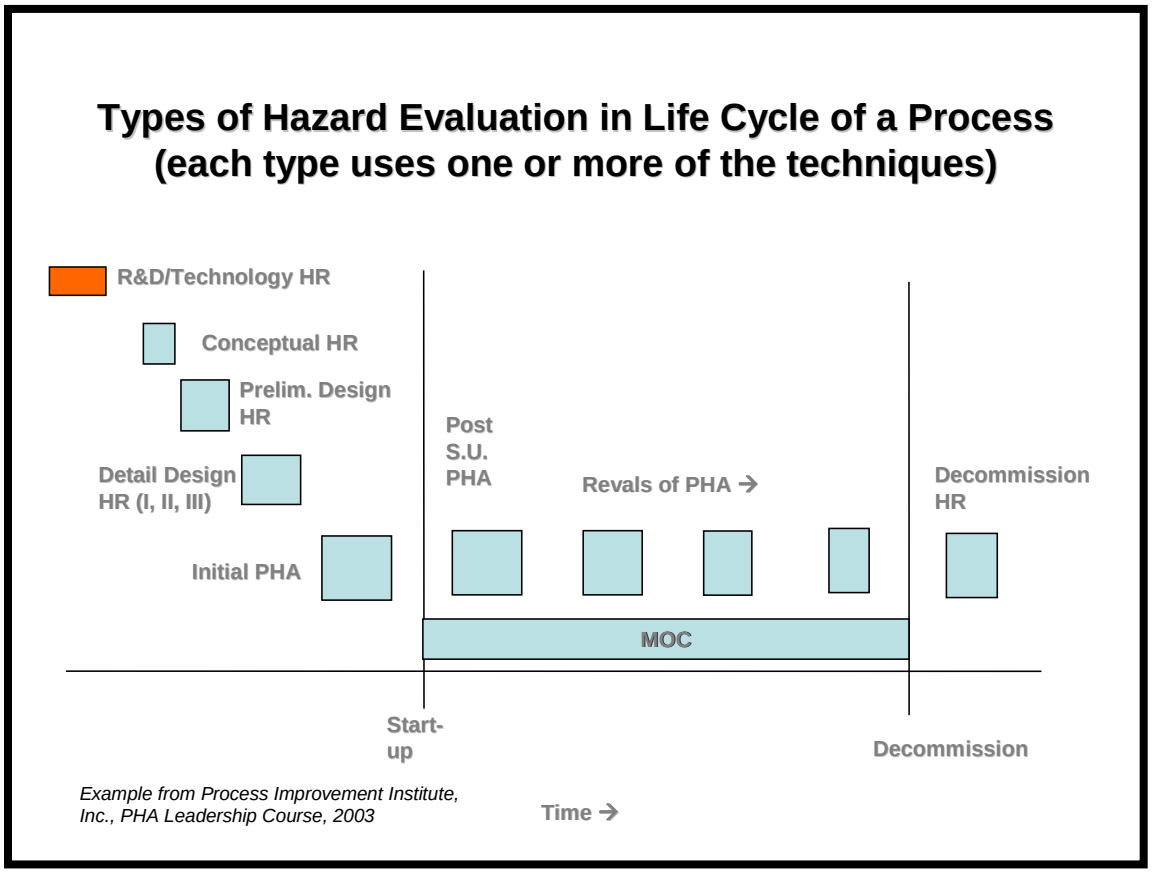
CCPS/AIChE, Guidelines for Hazard Evaluation Procedures

Comparison of Hazard Evaluation and Risk Assessment Methods

METHOD	APPLICABILITY														
	Operating Mode		Hazard level		Process or Task Complexity		Number of Scenarios Found		Process Type		Experience with Process or Task		Details Available for Process		
	Continuous	Batch, Startup, Shutdown, online maintenance	Low	High	Low	High	Low	High	Flow	Mechanical, Electrical	Low	High	Low (i.e., conceptual design)	Medium (i.e., detailed design)	High (i.e., pre-startup or operating unit)
QUALITATIVE – Identify and evaluate hazards and judge risk by voting of multi-disciplinary team															
Checklist	X	X	X		X		X		X	X	X	X	X		
Preliminary Hazard Review	X	X		X		X	X		X	X	X		X		
What-If	X	X	X		X		X		X	X	X	X	X	X	X
What-If/Checklist	X	X	X		X		X		X	X	X	X	X	X	X
2 Guide Word		X		X	X			X	X	X		X			X
HAZOP (full set of guide words)	X	X		X		X		X	X		X	X		X	X
FMEA	X			X		X		X		X	X	X		X	X
QUANTITATIVE – Numerically estimate the risk to aid in judgment of a scenario that is already identified; typically not a team															
Fire/Explosion Index	X	X		X	X	X	NA	NA	X			X		X	X
Toxicity Index	X	X		X	X	X	NA	NA	X			X		X	X
LOPA	X	X		X	X	X	NA	NA	X	X		X		X	X
Fault Tree Analysis	X	X		X		X	NA	NA	X	X		X		X	X
Event Tree Analysis	X	X		X		X	NA	NA	X	X		X		X	X
Human Reliability Analysis		X		X		X	NA	NA	X	X	X	X		X	X

Hazard Evaluation at Different Plant Lifetime Stages

Process hazards exist from the onset of a project through its end or assimilation into another project. The message to take from this section is that hazard evaluation must be used in all phases of a unit life cycle to ensure safe operations.



The following plant lifetime stages will be used in this section:

- Process development (perhaps several hazard evaluations during lab and pilot phases)
- Detailed design (1-3 hazard evaluation phases)
- Construction and start-up (and the initial and post-startup PHA)
- Operating lifetime (revalidations and MOC risk reviews)
- Extended shutdowns
- Decommissioning

Process Development

Research and development. A project starts somewhere with a need or opportunity identified. It is not important how or where the project starts, but it is important that environmental, health and safety effects be considered early in the benefit/risk justification. It is at this stage that an initial hazard evaluation is performed. Relatively few hazard evaluation techniques are applicable primarily due to the preliminary nature of the project. However, as reviews of the hazards and refinements are made to the concept through lab and literature work, options become available to consider an inherently safer design, operation, and procedures for the project. This can include exploring alternative chemistry or processes.

At some point in the process development stage, a process flow diagram is created to establish an event sequence, material balance, heat balance, and the like. A hazard evaluation update is essential, as critical reaction or process information was likely not available at an earlier hazard evaluation or has since been refined. There is also an opportunity to revisit inherently safer (IS) design options. As the process flow becomes more defined, the safety system development needs to be formalized with initial set points, allowable and safe deviations, and an initial statement of overall health, safety, and environmental risk tolerance.

Pilot plant operations act as segue to the implementation phase. Here the earlier hazard assessments are confirmed and refined. Previous heat management scenarios are played out under plant-like operating conditions. The added benefit is the exposure of the process to a range of start-up, shutdown, and upset conditions. The expected range for the materials of construction can be tested in a controlled manner for effects on the process and associated impact on process safety.

Commercialization Project Initiation

In a likely parallel effort with the pilot plant work, the front-end engineering would have begun with process, equipment, and instrument specifications as the P&IDs are developed from the process flow diagrams and control strategies. A PreHA, Checklist, or What-if analysis is appropriate at this stage. The results will form the basis for the implementation of a safety system consisting of passive and active safeguards. At this point in the front-end engineering process, a LOPA may be applied to quantify the health and safety risk and assess the need for further safeguards. Reference would be made to the initial statement of overall health, safety, and environmental risk tolerance created earlier in the process development stage. If the LOPA indicates that process risk is unacceptable, then additional safeguard(s) would need to be incorporated. The recognition for the need of additional safeguards could lead to functional specification of items such as a safety instrumented system (SIS). The operating procedures created and used in the pilot plant work would form the framework of the initial operating procedures. Batch operations may require few modifications for full-scale operation. However, the transition of operating procedures for continuous operations from pilot plant to full scale will likely require a complete rewrite. Administrative safeguards, such as preventive verifications and protective responses to upset conditions, can begin to be built into the operating procedures at this stage.

Detailed Design

When the commitment is made to launch the detailed design, major elements of the process are “locked” subject to minor changes. This would imply that the hazards are also “locked”. It is appropriate and desirable that a full hazard evaluation be completed as soon as the process P&IDs and major equipment specifications are well-established. It is critical that the hazard evaluation be done before heavy construction is started and major equipment is ordered. This gives the opportunity to adjust, at a minimal cost, to any critical health and safety flaws discovered in the review of the process design and/or procedures, including facility siting considerations. HAZOP, FMEA, and What-if/Checklist are appropriate for this phase.

Construction and Start-up

Any project manager will recognize the need to control field change orders during construction. The primary driver is construction cost control. Change orders can also have an impact on the safety systems design and integrity. All changes that occur following the full hazard evaluation must be documented and noted on safety documents. Near the end of construction and prior to start-up, the hazard evaluation is may need to be revalidated to incorporate any changes to the process and/or procedures. The initial PHA of the unit will need to be completed before startup and perhaps redone or update shortly after startup. HAZOP or 2 Guide Word analysis of procedures may be needed in these phases to complete the unit PHA.

The table below provides an example of the risk reviews that may be necessary during a large project:

PROCESS SAFETY MANAGEMENT APPLIED TO PROJECTS

PSR STAGE	DESCRIPTION	APPROPRIATE PHA	APPROPRIATE OSHA 29 CFR 1910.119 ELEMENT	PROJECT PROGRAM	IMPORTANT DOCUMENTATION
1	Conceptual design/project study	Checklist "What-if" QRA	ix) Management of change i) Process safety info. ii) PHA x) Incident investigation (lessons learned)	Statement of requirements/ Design proposal	Process description Hazardous materials Codes and standards Specialist equipment data
2	Design proposal/plant specifications	"What-if" FMEA	i) Process safety info. ii) PHA vii) Mechanical integrity xi) Emergency planning and response	F.E.E.D. study PSR-2 to report before Class II estimate finalized	Layout drawings Process flow drawings Specifications Ops, Maint. philosophy HSEQ philosophy
3	Detailed design	HAZOP QRA	i) Process safety info. ii) PHA vii) Mechanical integrity iii) Operating procedures	P&ID's "frozen" Mechanical design complete Fabrication started	P&ID's Electrical classification HAZOP report Inst./electrical drawings Mechanical drawings
4	Construction	HAZOP for field/late modifications	v) Contractors vii) Mechanical integrity viii) Work permits iv) Training	Site construction Field changes Pre-commissioning begins	Mechanical certificates Test certificates Contractor safety policy QA/QC reports Training program
5	Pre-commissioning	**HAZOP/WI of SOPs** **HF & FS Checklists**	vi) Pre-start-up safety review iii) Operating procedures iv) Training vii) Mechanical integrity viii) Work permits	Pre-commissioning complete Documentation complete Training and procedures complete	Operating procedures Training records Pre-commissioning report Emergency response plan
6	Post-commissioning	Appropriate PHA for post-commissioning changes	x) Incident investigation xi) Compliance auditing vii) Work permits iv) Training iii) Operating procedures	**3-6 months after startup**	Commissioning report Modification job files and HAZOP reports Operating reports

Operating Lifetime

Production operations. Following the initial start-up, production units are restarted following:

- a normal shutdown
- an emergency (abnormal) shutdown
- a “turnaround” or maintenance phase.

Each has safety issues associated which could be unique to the shutdown event. Start-up from a normal or scheduled shutdown (without maintenance action) should already have been addressed as a procedure-based hazard evaluation (HAZOP, What-if, or 2 Guide Word technique) of non-routine operations. Less likely to have had an established safety review is the start-up from an emergency or abnormal shutdown, since not all possible emergency scenarios would have been predicted. These are frequently considered to be operated like a normal start-up once the system has reached a safe state. A careful restart review (usually 2 Guide Word or What-if) is advised, since by the (hopefully) unique nature of the emergency, experience with the specific type of restart is limited.

Cyclic Reviews (Revalidations). Even as process changes never end during the life of a facility, there will always be the necessity to continue hazard evaluations. Periodic updating or revalidation of the hazard study to incorporate facility changes is the method used to maintain adequate safeguards. The timing of these cyclic reviews depends on factors such as regulations, the rate of process changes, and the

nature of those changes. A significant change outside the fence line can also trigger the need for a hazard review. Examples of such changes are:

- Population changes such as new residential housing nearby
- Land/water/air traffic pattern changes
- Necessary community emergency and security adjustments
- New buildings such as schools or commercial establishments
- Demolished buildings.
-

Management of Change. Change is an inevitable and necessary feature for all organizations. When changes occur in an operation that contains hazards of any sort, it is necessary that the change process be managed to understand and control those hazards. Most organizations have some "Management of Change" (MOC) policies and procedures in place to address the wide range of issues related to changes. Regardless of the type of change, the risk of change must be analyzed. All of the hazard evaluation methods are applicable to MOC risk reviews and the criteria for selecting the appropriate technique is the same as for other risk reviews. However, one nuance is that the choice of technique may depend also on how the unit hazard evaluation will be revalidated (updated). For instance, if the unit hazard evaluation (called a Process Hazard Analysis in the US) was accomplished using primarily HAZOP, then long-term it might be best if the risk review of the "change" also be documented in HAZOP format; this will make rolling-up the data into the next revalidation that much easier for the company.

Extended Shutdowns. Mothballing a plant or a unit within a plant site goes beyond the steps taken to shutdown a process to an established safe state. Tanks, lines, and valves must all be drained and any residual reactive materials neutralized. Most of these operations will likely be performed only once during the lifetime of the operation, and hence will have no history to help guide the safe implementation of the mothballing effort. A potentially riskier activity is a restart from an extended shutdown. In that event, the condition and intended operation of all equipment and instruments must be checked. In particular, the safety systems must be re-verified and validated. The restart of a mothballed unit within and perhaps attached to an active production site should include a review of the hazard evaluation for the connected active units.

Decommissioning. An active plant or unit that is slated for decommissioning would go through the stages of a normal shutdown, then cleanout in preparation for mothballing, followed by disassembly. In the refining industry as well as in other process industries, a hazard review is conducted before decommissioning. Health, safety, and environmental issues would be related to uncontrolled pressure releases, workers potentially exposed to noxious or toxic vapors, and spills during line separation. A plant or unit that has been previously mothballed would have all the issues associated with the decommissioning of an active plant or unit, with the added potential hazard associated with corrosion products. Over a period of time, residues can change such that these new compounds may be unknown and have unknown health and environmental effects or thermal decomposition sensitivities.

Example of When to Use Each Technique to Complete a Process Hazard Analysis of a Complete Process Unit

The best approach for completing a PHA if you have good documentation and especially if you have good procedures (SOPs):

Continuous Mode	Discontinuous Mode (batch, startup, shutdown, major maintenance, emergency shutdowns)
HAZOP of Parameters FMEA of Continuous Mode What-if of Simple Sub-systems	HAZOP of Steps • 8 guideword • 2-3 guideword • What-if of procedure module What-if of Simple Tasks
Note: Do this first for a continuous process; don't do this at all for a Batch process	Note: Do this second for a Continuous process; do this as the only steps for a Batch process

Next Best: If you do NOT have good procedures (SOPs) or if you do not intend to analyze the procedures regardless, then the best approach is:

Continuous Mode	Discontinuous Mode (batch, startup, shutdown, major maintenance, emergency shutdowns)
HAZOP of Parameters FMEA of Continuous Mode What-if of Simple Sub-systems	Use HAZOP or FMEA but ask about issues of each deviation (or failure mode) for each Mode of Operation
Note: Do these simultaneously	