HAZARD ANALYSIS AND RISK ASSESSMENT

1. Introduction

The hazards associated with any facility that produces or uses chemicals can be quite numerous, perhaps in the hundreds or thousands for larger facilities. These hazards are the result of the physical properties of the materials, the operating conditions, the procedures, or the design, to name a few. Most of the hazards are continually present in a facility.

Without proper control of hazards, a sequence of events (scenario) occurs that results in an accident. A hazard is defined as anything that could result in an accident, ie, an unplanned sequence of events which results in injury or loss of life, damage to the environment, loss of capital equipment, or loss of production or inventory.

Risk consists of two components: the probability of the accident and the consequence. It is not possible to completely characterize risk without both of these components. Thus, a hazard could have low probability of accident but high consequence or vice versa. The result for both cases may be moderate risk.

The purpose of hazard analysis and risk assessment in the chemical process industry is to (*1*) characterize the hazards associated with a chemical facility; (*2*) determine how these hazards can result in an accident, and (*3*) determine the risk, ie, the probability and the consequence of these hazards. The complete procedure is shown in Figure 1 (see also INDUSTRIAL HYGIENE; PLANT SAFETY).

Most of the techniques for estimating risk or identifying hazards that are discussed herein require analysis by committee. The committee must be formed from individuals having specific and relevent experience to the chemical process under consideration. Furthermore, the management of this committee is paramount to the success of the hazards analysis. Members must focus on the problem at hand and continue to make satisfactory progress.

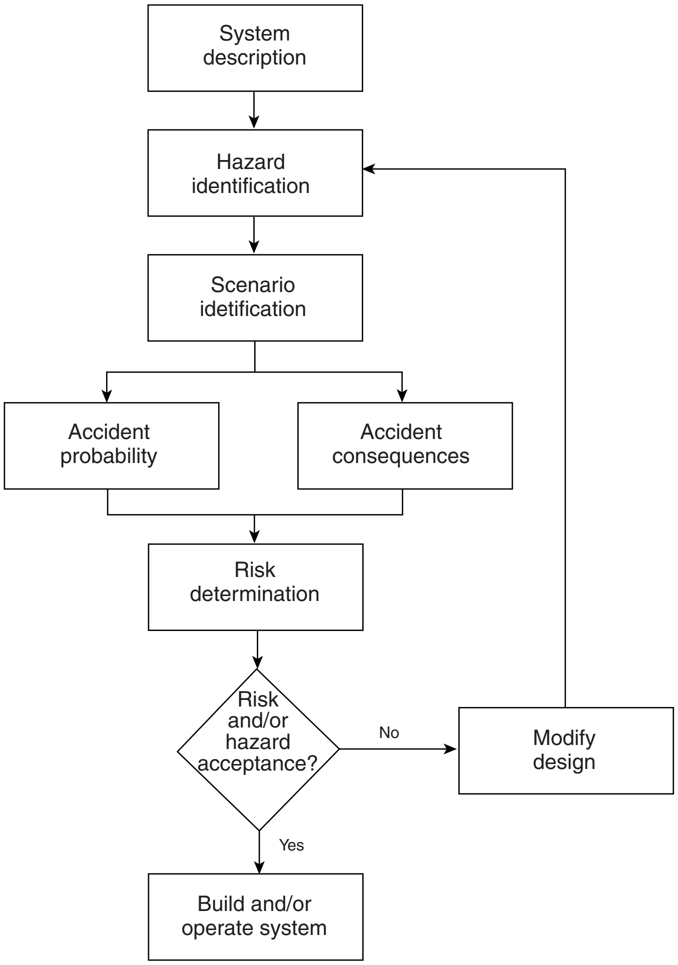

Fig. 1. Flow chart representing the complete hazard identification and risk assessment procedure.

The first step is to have a complete and detailed description of the system, process, or procedure under consideration. This step must include physical properties of the materials, operating temperatures and pressures, detailed flow sheets, instrument diagrams of the process, materials of construction, other detailed design specifications, etc. The more detailed and up-to-date this information is, the better the result of the analysis.

The next step is to identify the hazards, which is done using a number of established procedures. It is not unusual for several hundred hazards to be identified for a reasonably complex process.

The subsequent step is to identify the various scenarios which could cause loss of control of the hazard and result in an accident. This is perhaps the most difficult step in the procedure. Improper characterization of the accident scenarios may result in inadequate or improper handling of the hazards, resulting in an accident. For a reasonably complex chemical process, there might exist dozens, or even hundreds, of scenarios for each hazard. The essential part of the analysis is to select the scenarios which are deemed credible and worst case.

The next part of the procedure involves risk assessment, which includes a determination of the accident probability and the consequence of the accident and is done for each of the scenarios identified in the previous step. The probability is determined using a number of statistical models generally used to represent failures. The consequence is determined using mostly fundamentally based models, called source models, to describe how material is ejected from process equipment. These source models are coupled with a suitable dispersion model and/or an explosion model to estimate the area affected and predict the damage. The consequence is thus determined.

The final part of the procedure is to decide if the risk is acceptable. If it is not, then a change must be made and the entire procedure restarted. If the risks and/or hazards are acceptable, then the process and/or procedure are approved for implementation.

The hazard analysis and risk assessment procedure can be applied at any stage in the lifetime of a process or procedure including research and development, initial conceptual design (see PLANT LAYOUT; PLANT LOCATION), pilot-plant operation (see PILOT PLANTS AND MICROPLANTS), construction and start-up, operation, maintenance, plant expansion, and final plant decommissioning. For economic reasons, it is best to begin this procedure during the very initial stages when changes are easier and less costly.

There are a large number of standard methods suitable for each stage in the hazard analysis and risk assessment procedure. The selection of the proper method depends on several factors. Some of these are the type of process, the stage in the lifetime of the process, the experience and capabilities of the participants, and the step in the procedure that is being examined. Information regarding the selection of the proper procedure is available in an excellent and comprehensive reference (1).

Hazard analysis does have limitations. First, there can never be a guarantee that the method has identified all of the hazards, accident scenarios, and consequences. Second, the method is very sensitive to the assumptions made by the analysts prior to beginning the procedure. A different set of analysts might well lead to a different result. Third, the procedure is sensitive to the experience of the participants. Finally, the results are sometimes difficult to interpret and manage.

For chemical facilities in the United States, hazard analysis is not an option if inventories of hazardous chemicals are maintained in amounts greater than the threshold quantities specified by the Occupational Safety and Health Administration (OSHA) regulation 1910.119. Many facilities are finding that hazard analysis has many benefits. The process or procedure often works better, the quality of the product is improved, the process experiences less down time, and the employees feel more comfortable in the work environment after a hazard analysis has been completed.

2. Hazard Identification Procedures

Methods for performing hazard analysis and risk assessment include safety review, checklists, Dow Fire and Explosion Index, Dow Chemical Exposure Index, what-if analysis, hazard and operability analysis (HAZOP), failure modes and effects analysis (FMEA), fault tree analysis, and event tree analysis. Other methods are also available, but those given are used most often.

2.1. Safety Review.

The safety review procedure begins by the preparation of a detailed safety review report. The purpose of this report is to provide the relevant safety information regarding the process or operation. This report is generally prepared by the process engineer. A typical outline for this report follows:

Introduction
Process summary
Reactions and stoichiometry
Engineering data
Raw materials and products (refers to hazards and special handling requirements)
Equipment set-up, including a process flow diagram (PFD) and process and instrumentation diagram (P&ID)
Equipment description
Equipment specifications
Procedures
Normal operating procedures
Safety procedures
Emergency shutdown
Fail-safe procedures, including safety instrumented systems
Major release procedures
Waste disposal procedures
Clean-up procedures
Safety checklists
Chemical hazard sheets (MSDS)

The next step in the procedure is to form a committee comprised of people with expertise specific to the process and chemistry involved. The committee could also include a process safety specialist, an industrial hygienist, an environmental expert, the process operators, a consultant, and others. The committee should not contain more than a dozen individuals.

The safety review report is distributed to the committee which meets to work its way through the report, section by section, discussing safety concerns and potential improvements to the process or procedure. An individual must be designated to take minutes at the meeting and record suggested modifications. If the review covers an existing process, the committee should perform a site visit to examine the actual equipment.

At the completion of the review of the report, an action plan is formulated and changes agreed upon by the committee are implemented. A final check must be made by management to ensure that these changes are actually completed.

The safety review technique is also useful for small laboratory operations and small changes in existing processes. In these cases, the committee often consists of two or three people and any changes are often less formally recommended.

2.2. Checklists. A checklist is simply a detailed list of safety considerations. The purpose of this list is to provide a reminder to safety issues such as chemical reactivity, fire and explosion hazards, toxicity, etc. This type of checklist is used to determine hazards, and differs from a procedure checklist which is used to ensure that the correct procedure is followed.

The hazards checklist usually has three columns next to each item on the list. Items can number in the hundreds or even the thousands. The first check is marked if the issue has been considered and complete. The second check is marked if additional consideration or work is required, and the last check is marked if the item does not apply. An example of a detailed checklist can be found in the literature (2).

2.3. Dow Fire and Explosion Index. The Dow Fire and Explosion Index (3) is a procedure useful for determining the relative degree of hazard related to flammable and explosive materials. This Index form works essentially the same way as an income tax form. Penalties are provided for inventory, extended temperatures and pressures, reactivity, etc, and credits are applied for fire protection systems, process control, and material isolation. The complete procedure is capable of estimating a dollar amount for the maximum probable property damage and the business interruption loss based on an empirical correlation provided with the Index.

The procedure begins by using a material factor that is a function only of the physical properties of the chemical in use. The more hazardous the material, the higher the material factor. A table containing factors for common materials is provided with the Index. Additionally, a procedure is detailed for determining the material factor for unlisted materials.

The next step is to apply penalties for general process hazards such as exothermic or endothermic reactions, material handling and transfer, enclosed or indoor units, access, drainage, and for special process hazards, eg, toxic materials, low or high pressure, flammable dusts, low or high temperature, leakage, rotating equipment, quantity of material. Correlations are provided to assist in determining reasonable penalties for these items.

Finally, the penalties are factored into the original material factor to result in a fire and explosion index value. The higher this value, the higher the degree of hazard.

The next step is to apply a number of loss control credit factors such as process control (emergency power, cooling, explosion control, emergency shutdown, computer control, inert gas, operating procedures, reactive chemical reviews), material isolation (remote control valves, blowdown, drainage, interlocks) and fire protection (leak detection, buried tanks, fire water supply, sprinkler systems, water curtains, foam, cable protection). The credit factors are combined and applied to the fire and explosion index value to result in a net index.

The net index is used with correlations provided to determine the maximum probable property damage and business interruption loss in the event of an accident.

The Dow Fire and Explosion Index is a useful method for obtaining an estimate of the relative fire and explosion hazards associated with flammable and combustible chemicals. However, the method does not provide any information on toxicity, environmental or other types of hazards. The technique is very procedure oriented, and there is the danger of the user becoming more involved with the procedure than the intent.

2.4. Dow Chemical Exposure Index. The Dow Chemical Exposure Index (4) is a procedure for rating the relative acute health hazard potential for people in neighboring plants or communities due to possible chemical releases of toxic materials. This index works essentially the same as the Dow Fire and Explosion Index, using a number of forms to organize the procedure. This index estimates the hazard distance for chemical exposure, based on the emergency response planning guideline (ERPG) values for the particular material released.

The procedure begins with a definition of possible release incidents. This includes releases from pipes, hoses, pressure relief devices relieving directly to the atmosphere, vessels, and tank overflows and spills. The Index Guide has detailed guidelines for these incidents. The incidents are used with a number of simplified source models provided to estimate the release rate of material. The ERPGs are then used with a simplified dispersion model to determine the hazard distance resulting from the release.

2.5. What-if Analysis. The what-if analysis is simply a brainstorming technique that asks a variety of questions related to situations that can occur. For instance, in regards to a pump, the question What if the pump stops running? might be asked. An analysis of this situation then follows. The answer should provide a description of the resulting consequence. Recommendations then follow, if required, on the measures taken to prevent or control the hazard.

A what-if form, consisting of columns assigned to identify the item under consideration, lists the question, describes the potential consequence/hazard, and lists the recommendations. Additionally, columns can be employed to assign work and to indicate completion.

The what-if analysis approach is useful throughout the entire lifetime of a process and is frequently used in conjunction with the checklist approach. However, the approach is very unstructured and depends heavily on the experience of the analysts.

2.6. Hazard and Operability Analysis. The hazard and operability analysis (HAZOP) procedure is quite popular because of its ease of use, the ability to organize and structure the information, reduced dependence on the experience of the analysts, and the high level of results. Furthermore, the approach is capable of finding hazards associated with the operation of a facility, hence the incorporation of the word operability in the name.

HAZOP is an organized way to draw out the team experience and knowledge to identify hazards. But, if the knowledge does not exist in the team, HAZOP will not identify the hazards. HAZOP helps to ask the right questions, but does not guarantee the right answers.

The HAZOP procedure, performed by committee, is mostly an organizational one. There is little technology associated with the process. The HAZOP approach is capable of identifying hundreds of items for a reasonably complex process. This information must be organized and managed properly.

The HAZOP committee must be composed of people with specific experience related to the process at hand. The chair, or facilitator, responsible for managing the committee should be highly familiar with the HAZOP procedure and should have excellent committee management skills. This person must ensure that the discussion is focused and productive, and then oversee the paperwork and progress of the work.

The first step in the procedure is to define the purpose, objectives, and scope of the study. The more precisely this is done, the more focused and relevant the committee discussions can be. The next step is to collect all relevant information on the process under consideration. This includes flow diagrams, process equipment specifications, nominal flows, etc. The procedure is highly dependent on the reliability of this information. Efforts expended here are worthwhile. Many committees use the flow sheet as the central structure to organize their discussions.

After the first two steps are completed, the committee conducts the review. The facilitator divides the flow sheet into a number of sections containing one principal equipment piece and auxiliaries. A section is chosen and the following procedural steps performed (5): (*1*) a study node, ie, vessel, line, operating instruction is chosen; (*2*) the node's design intention, ie, flow, cooling, etc, is described; (*3*) a process parameter such as temperature, pressure, pH, component, viscosity, etc, is chosen; (*4*) a guide word (Table 1) to determine a possible deviation is applied; (*5*) if the deviation is applicable, the possible causes are determined and any protective systems noted; (*6*) the consequences of the deviation are evaluated; (*7*) specific action is recommended by spelling out what, when, and by whom; and (*8*) all information is recorded on HAZOP forms. Steps 4–8 are repeated until all guide words have been applied to the chosen process parameter. Steps 3–9 are repeated until all applicable process parameters have been considered for the given study node. Finally, steps 1–10 are repeated until all study nodes have been completed in a given section. Then the next section is examined. The guide words provided in Table 1 represent a standard set.

Table 1. **List of Guide Words for HAZOP Procedure**[a]

Guide word	Meaning	Comments	Example
no, not, none	the complete negation of	no part of the design intention is achieved, but nothing else happens	no flow
more, higher, greater	quantitative increase	applies to quantities such as flow rate and temperature as well as activities like heat and reaction	more flow
less, lower	quantitative decrease	same as above	less flow
as well as	qualitative increase	all the design and operating intentions are achieved along with some additional activity, such as contamination of process streams	something else with the flow
part of	qualitative decrease	only some of the design intentions are achieved, some are not	partial flow
reverse	the logical opposite of	most applicable to activities such as flow or chemical reaction; also applicable to substances	reverse flow
other than	complete substitution	no part of the original intention is achieved; the original intention is replaced by something else	something else flows
sooner than	too early or in wrong order	applies to process steps or actions	flow started early
later than	too late or in wrong order	applies to process steps or actions	flow started late
where else	in additional locations	applies to process locations or locations in operating procedures	flow goes some other place

[a] Ref. 5.

Most companies customize their sets of guide words and many companies use different sets based on the type of unit operation being examined.

The committee must carefully regulate its time to ensure that the participants do not experience HAZOP burnout. Many meetings might be required over a period of months to complete a particularly large process, but meetings should be limited to not more than three hours every other day.

A reactor system is shown in Figure 2 to which the HAZOP procedure can be applied. This reaction is exothermic, and a cooling system is provided to remove the excess energy of reaction. If the cooling flow is interrupted, the reactor temperature increases, leading to an increase in the reaction rate and the heat generation rate. The result could be a runaway reaction with a subsequent increase in the vessel pressure possibly leading to a rupture of the vessel.

Performing a HAZOP on this process with the assigned task of considering runaway reaction episodes would lead to a completed form, part of which is shown in Figure 3. The process is already small enough to be considered a single section. Four study nodes are cooling water line, stirring motor, monomer feed line, and reactor vessel. Figure 3 shows the HAZOP form completed for the cooling water and stirring motor study nodes.

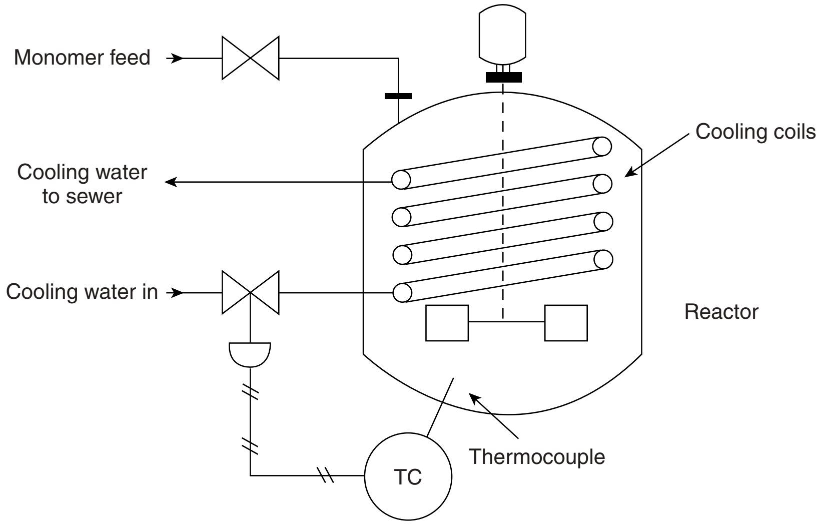

Fig. 2. Reactor systems used for HAZOP example (6). (Courtesy of Prentice Hall.)

This example HAZOP analysis reveals the following potential process modifications: (*1*) installation of a cooling water flow meter and low flow alarm to provide an immediate indication of cooling loss; (*2*) installation of a high temperature alarm to alert the operator in the event of cooling function loss; (*3*) installation of a check valve in the cooling line to prevent reverse flow of cooling water; (*4*) periodic inspections and maintenance of the cooling coil; and (*5*) evaluation of the cooling water source to consider any possible interruption and contamination of the supply. Once the recommendations are completed, it is the job of management to rate the recommendations with respect to importance and then to ensure that the recommendations are implemented.

2.7. Failure Mode and Effects Analysis. Failure mode and effects analysis (FMEA) is applied only to equipment. It is used to determine how equipment could fail, the effect of the failure, and the likelihood of failure. There are three steps in an FMEA (5): (*1*) define the purpose, objectives, and scope. Large processes are broken down into smaller systems such as feed or cooling. At first, the failures are only considered to affect the system. In a more general study, the effects on a plant-wide basis can be considered. (*2*) Define the problem and boundary conditions. This includes identifying the system to be studied, establishing the physical boundaries, and labeling the equipment with a unique identifier for use in the FMEA procedure. (*3*) Complete the FMEA table (5) by beginning at the system boundary and evaluating the equipment items in the order these appear in the process.

An FMEA table contains a series of columns for the equipment reference number, the name of the piece of equipment, a description of the equipment type, configuration, service characteristics, etc, which may impact the failure

Project name: Example 1	Date: 1/1/93	Page 1 of 2	Completed:
Process: Reactor shown in Figure 2			No action:
Section: Reactor shown in Figure 2	Reference drawing: Figure 2		Reply date:

Item	Study node	Process parameters	Deviations (Guide words)	Possible causes	Possible consequences	Action required	Assigned to:			
1A	Cooling water	Flow	No	1. Control valve fails closed	1. Loss of cooling, possible runaway	1. Select valve to fail open	DAC	1/93		
				2. Plugged cooling coils	2. Same	2. Install filter with maintenance procedure Install cooling water flow meter and low flow alarm Install high temperature alarm to alert operator	DAC DAC DAC	1/93 2/93 2/93		
				3. Cooling water service failure	3. Same	3. Check and monitor reliability of water service	DAC	2/93		
				4. Controller fails and closes valve	4. Same	4. Place controller on critical instrumentation list	DAC	1/93		
				5. Air pressure fails, closing valve	5. Same	5. See 1A.1				
1B			High	1. Control valve fails open	1. Reactor cools, reactant conc builds, possible runaway on heating	1. Instruct operators and update procedures	JFL	1/93		
				2. Controller fails and opens valve	2. Same	2. See 1A.4 above				
1C			Low	1. Partially plugged cooling line	1. Diminished cooling, possible runaway	1. See 1A.2 above				
				2. Partial water source failure	2. Same	2. See 1A.2 above				
				3. Control valve fails to respond	3. Same	3. Place valve on critical instrumentation list	JFL	1/93		
1D			As well as	1. Contamination of water supply	1. Not possible here	4. None			X	
1E			part of	1. Covered under 1C					X	
1F			reverse	1. Failure of water source resulting in backflow	1. Loss of cooling, possible runaway	1. Sec 1A.2				
				2. Backflow due to high backpressure	2. Same	2. Install check valve	JFL	2/93		
1G			Other than	1. Not considered possible					X	
1H			Sooner than	1. Cooling normally started early	1. None				X	
11			Later than	2. Operator error	1. Temperature rises, possible runaway	1. Interlock between cooling flow and reactor feed	JEH	1/93		
1J			Where else	1. Not considered possible					X	

Fig. 3. Hazards and operability (HAZOP) analysis example.

Table 2. **Failure Modes for Process Equipment**[a]

Equipment type	Failure modes
valve, normally open	fails to open (or fails to close when required) closes unexpectedly leaks to external environment valve body rupture
pump, normally operating	fails on (fails to stop when required) stops unexpectedly seal leak/rupture pump casing leak/rupture
heat exchanger, high pressure on tube side	leak/rupture, tube side to shell side leak/rupture, shell side to external environment tube side plugged shell side plugged

[a] Ref. 5.

modes and/or effects, and a list of the failure modes. Table 2 provides a list of representative failure modes for valves, pumps, and heat exchangers. The last column of the FMEA table is reserved for a description of the immediate and ultimate effects of each of the failure modes on other equipment and the system.

2.8. Fault Tree Analysis.

Fault trees represent a deductive approach to determining the causes contributing to a designated failure. The approach begins with the definition of a top or undesired event, and branches backward through intermediate events until the top event is defined in terms of basic events. A basic event is an event for which further development would not be useful for the purpose at hand. For example, for a quantitative fault tree, if a frequency or probability for a failure can be estimated without further development of the failure logic, then there is no point to further development, and the event is regarded as basic.

Figure 4 shows a fault tree for a flat tire on an automobile. The top event, the flat tire, is broken down into two immediate contributing events, road debris and tire failure. The contributing event, road debris, is a basic event. This event, which cannot be broken down into other events unless additional information is provided, is enclosed in a circle to denote it as a basic event. The other event, tire failure, is enclosed in a rectangle to denote it as an intermediate event.

These two events are related to each other through an OR gate, ie, the top event can occur if either road debris or tire failure occurs. Another type of gate is the AND gate, where the output occurs if and only if both inputs occur. OR gates are much more common in fault trees than AND gates, ie, most failures are related in OR gate fashion.

The next step is to define the intermediate event, tire failure. There are two events which could contribute: a worn tire or a tire that is defective owing to a manufacturing problem. These are both basic events because additional information is needed for any further definition.

An important part of fault tree analysis is the initial problem definition. Failure to adequately define the problem can produce unclear results. The top

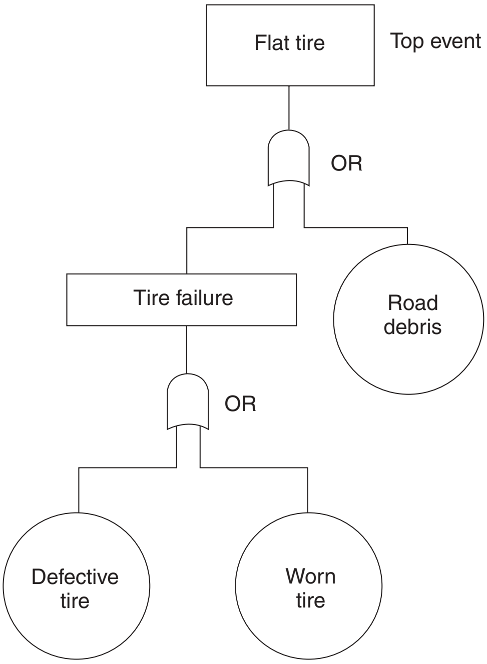

Fig. 4. Fault tree analysis for a flat tire (7). (Courtesy of Prentice Hall.)

event must be precisely defined. Events such as FIRE IN PLANT, or EXPLOSION OF EXTRACTOR, are too vague and general. Likewise, top events such as LEAK IN VALVE V24 are too specific. Appropriate events would include RUNAWAY REACTION IN REACTOR R1, HIGH PRESSURE IN VESSEL V1, HIGH LEVEL IN VESSEL V2, etc. The analysis boundary conditions, ie, all of the equipment under consideration, and the state of this equipment must also be defined; the open valves, the material flowing, etc, must be designated. Then the level of resolution must be defined; eg, the valve itself or the positioner on the valve must be designated. Additionally, any unallowed events (which are outside the scope of the project) such as wiring failures, lighting, etc, should be defined along with any assumptions made in the analysis.

Other considerations for fault tree construction are (*1*) assume that faults propagate through normally operating equipment. Never assume that a fault is stopped by the miraculous failure of another piece of equipment. (*2*) Gates are connected through labeled fault events. The output from one gate is never connected directly into another.

It is important in fault tree analysis to consider only the nearest contributing event. There is always a tendency to jump immediately to the details, skipping all of the intermediate events. Some practice is required to gain experience in this technique.

The principal problem in using fault trees is that for reasonably complicated processes the analysis is most likely to produce a huge fault tree. Fault

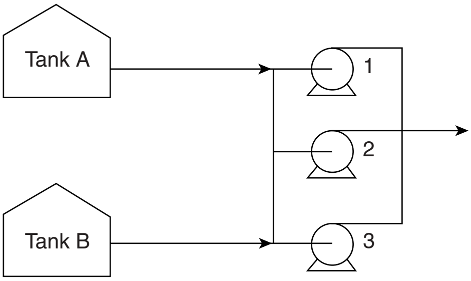

Fig. 5. Schematic of a pumped storage facility.

trees involving hundreds or even thousands of intermediate events are not uncommon. The effort involved in fault tree development can also be substantial.

Another problem for fault trees is the uniqueness of the result. Fault trees produced by two different teams of analysts most often show a different structure. However, this problem is reduced as the detail in the problem definition increases.

A pumped storage facility having two tanks and three pumps is shown schematically in Figure 5. Any one tank can be connected to any of the pumps to provide raw material. The first step in the fault tree analysis procedure is to define the problem. If the top event is defined as the failure to pump raw material from pumped storage, then the analysis boundary conditions and equipment state are: the equipment is configured as shown in Figure 5; both tanks contain the same raw material; any one pump can be connected to either of the two tanks to provide raw material. The level of resolution is the equipment configuration shown in Figure 5. Unallowed events include wiring failures, electrical failures, lighting, tornadoes, etc.

The resulting fault tree is shown in Figure 6, in which the top event is defined in terms of two intermediate events: failure of the tank system or failure of the pumping system. Failure in either system would contribute to the overall system failure. The intermediate events are then further defined in terms of basic events. All of the basic events are related by AND gates because the overall system failure requires the failure of all of the individual components. Failures of the tanks and pumps are basic events because, without additional information, these events cannot be resolved any further.

2.9. Event Trees.

Event trees use an inductive logic approach to consider the effects of safety systems on an initiating event. The initiating event is propagated through the various safety functions. Branching is dependent on the success or failure of the safety function.

Consider again, eg, the case of the flat tire on an automobile. The initiating event in this case is the flat tire. There are two safety functions that can be defined: a spare tire and an emergency road patrol. Other safety functions might be included depending on the particular situation.

The event tree is drawn by first identifying the initiating event, on the left-hand side of the drawing sheet, as shown in Figure 7. The two safety functions

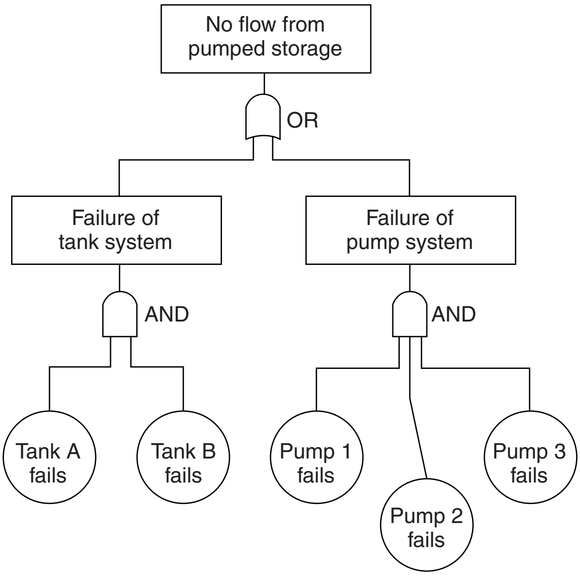

Fig. 6. A fault tree for the pumped storage example of Figure 5. For a real system the tank and pump failures would be more precisely defined, or set as intermediate events having further definition by subsequent basic events and more detailed failure modes.

are identified on the top of the sheet. A line is drawn from the initiating event to a position immediately below the first safety function, in this case the spare tire. At this point the line branches, the upper branch representing the success of the safety function and the lower branch representing the failure of this safety function. The lines are continued in this fashion so that branching occurs below each safety function.

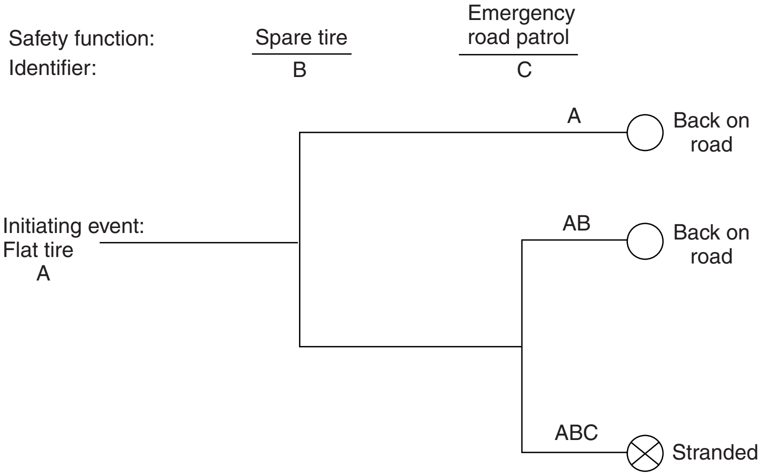

Fig. 7. Event tree for a flat tire.

In some cases the safety function is meaningless. For the example provided, if the spare tire is successfully mounted, then the safety function for the emergency road patrol is meaningless. In this case the line is drawn directly through the safety function.

The branching is continued until all of the safety functions are considered. At this point a conclusion is reached about the result. For the flat tire example, only two results are possible: the driver is either stranded or back on the road. The circle used to terminate the stranded result is given an X to denote it as an unfavorable outcome.

The initiating event is given a unique letter designation. In Figure 7 it is assigned the letter A. Each safety function is also assigned a unique letter designation, different from the letter used for the initiating event. These letters are used to identify each line on the event tree. Thus, letter sequence AB identifies initiating event A, followed by the failure of safety function B.

It is not coincidental that the top event of the fault tree is the initiating event for the event tree. The fault tree shows how an event is decomposed into basic events whereas an event tree demonstrates the effect of the various safety functions. The disadvantage of event trees is that the outcomes are difficult to predict. Thus the outcome of interest might not arise from the analysis.

Fault trees and event trees can also be used to provide quantitative information, such as overall failure rates and frequencies (2).

3. Scenario Identification

An important part of hazard analysis and risk assessment is the identification of the scenario, or design basis by which hazards result in accidents. Hazards are constantly present in any chemical facility. It is the scenario, or sequence of initiating and propagating events, which makes the hazard result in an accident. Many accidents have been the result of an improper identification of the scenario.

Most hazard identification procedures have the capability of providing information related to the scenario. This includes the safety review, what-if analysis, HAZOP, failure modes and FMEA, and fault tree analysis. Using these procedures is the best approach to identifying these scenarios.

4. Source Modeling and Consequence Modeling

Once the scenario has been identified, a source model is used to determine the quantitative effect of an accident. This includes either the release rate of material, if it is a continuous release, or the total amount of material released, if it is an instantaneous release. For example, if the scenario is the rupture of a 10-cm pipe, the source model would describe the rate of flow of material from the broken pipe.

Once the source modeling is complete, the quantitative result is used in a consequence analysis to determine the impact of the release. This typically includes dispersion modeling to describe the movement of materials through the air, or a fire and explosion model to describe the consequences of a fire or explosion. Other consequence models are available to describe the spread of material through rivers and lakes, groundwater, and other media.

The dispersion model is typically used to determine the downwind concentrations of released materials and the total area affected. Two models are available: the plume and the puff. The plume describes continuous releases; the puff describes instantaneous releases.

An explosion model is used to predict the overpressure resulting from the explosion of a given mass of material. The overpressure is the pressure wave emanating from an explosion. The pressure wave creates most of the damage. One way to estimate the overpressure is the TNT equivalency method. The result is dependent on the mass of material and the distance away from the explosion. Suitable correlations are available (2). A detailed discussion of source and consequence models may be found in References 2,8–10.

5. Probability

In order to complete an assessment of risk, a probability must be determined. The easiest method for representing failure probability of a device is an exponential distribution (2).

$$R(t) = e^{\mu t} \tag{1}$$

where $R(t)$ is the reliability, μ is the failure rate in faults per time, and t is the time.

There are other distributions available to represent equipment failures (11), but these require more detailed information on the device and a more detailed analysis. For most situations the exponential distribution suffices.

Once the reliability is defined, the failure probability, $P(t)$, follows.

$$P(t) = 1 - R(t) = 1 - e^{-\mu t} \tag{2}$$

Figure 8 compares the failure probability and reliability functions for an exponential distribution. Whereas the reliability of the device is initially unity, it falls off exponentially with time and asymptotically approaches zero. The failure probability, on the other hand, does the reverse. Thus new devices start life with high reliability and end with a high failure probability.

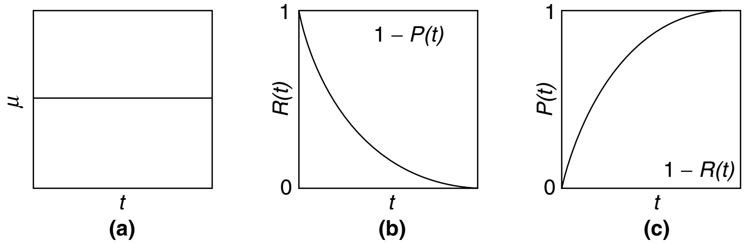

Fig. 8. (**a**) Failure rate, (**b**) reliability, and (**c**) failure probability.

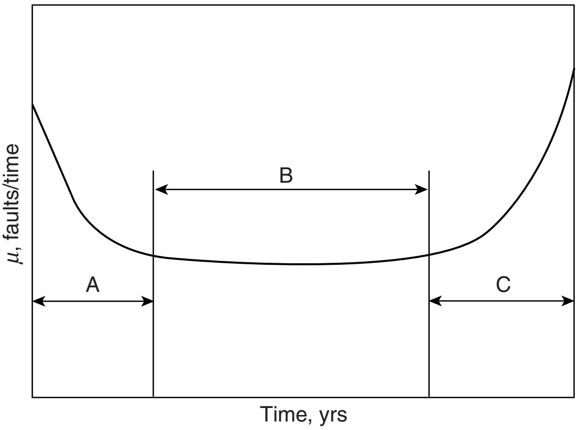

Fig. 9. Failure rate curve for real components. A, infant mortality; B, period of approximately constant μ; and C, old age.

A considerable assumption in the exponential distribution is the assumption of a constant failure rate. Many real devices demonstrate a failure rate curve more like that shown in Figure 9. For a new device, the failure rate is initially high owing to manufacturing defects, material defects, etc. This period is called infant mortality. Following this is a period of relatively constant failure rate. This is the period during which the exponential distribution is most applicable. Finally, as the device ages, the failure rate eventually increases.

Table 3 lists typical failure rate data for a variety of types of process equipment. Large variations between these numbers and specific equipment can be expected. However, this table demonstrates a very fundamental principle: The more complicated the device, the higher the failure rate. Thus switches and thermocouples have low failure rates; gas–liquid chromatographs have high failure rates.

The next step is to develop a method to determine the overall reliability and failure probability for systems constructed of a variety of individual components. This requires an understanding of how components are linked. Components are linked either in series or in parallel. For series linkages, overall failure results from the failure of any of the components. For parallel linkages, all of the components must fail. An example of a series linkage is an automobile. The car is disabled if a flat occurs in any one of the four tires. This situation is linked in parallel to the spare tire. The car is completely disabled only if a flat occurs and the spare tire is flat.

The computational technique for the two linkages is shown in Figure 10. For series linkages (Fig. 10**a**), the reliabilities of the individual components are multiplied together. For parallel linkages (Fig. 10**b**) the failure probabilities are multiplied together. This method for combining the distributions assumes that the failures of the individual devices are independent of each other, and that the failure of one device does not strain an adjacent device causing it, too, to fail. It also assumes that devices fail hard, that is, the device is obviously failed and not in a partially failed state.

Table 3. **Failure Rate Data for Process Hardware**[a]

Instrument	Failure rate, faults/year
controller	0.29
control valve	0.60
flow measurement	
fluids	1.14
solids	3.75
flow switch	1.12
gas–liquid chromatograph	30.6
hand valve	0.13
indicator lamp	0.044
level measurement	
liquids level measurement	1.70
solids level measurement	6.86
oxygen analyzer	5.65
pH meter	5.88
pressure measurement	1.41
pressure relief valve	0.022
pressure switch	0.14
solenoid valve	0.42
stepper motor	0.044
strip chart recorder	0.22
thermocouple temperature measurement	0.52
thermometer temperature measurement	0.027
valve positioner	0.44

[a] Ref. 9.

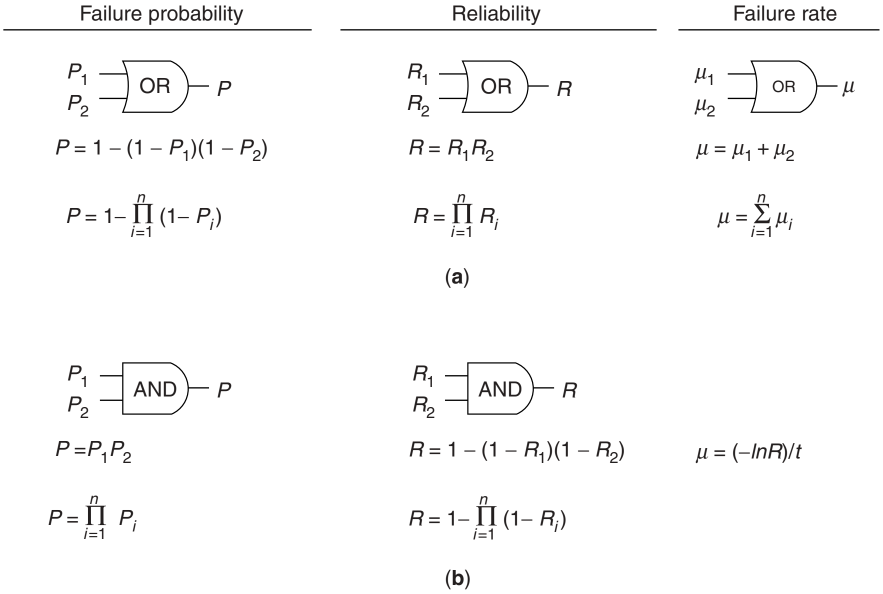
Failure probability
Reliability
Failure rate
P_1
P_2
OR
P
R_1
R_2
OR
R
μ_1
μ_2
OR
μ
$P = 1 - (1 - P_1)(1 - P_2)$
$R = R_1 R_2$
$\mu = \mu_1 + \mu_2$
$P = 1 - \prod_{i=1}^{n} (1 - P_i)$
$R = \prod_{i=1}^{n} R_i$
$\mu = \sum_{i=1}^{n} \mu_i$
(a)
P_1
P_2
AND
P
R_1
R_2
AND
R
$P = P_1 P_2$
$R = 1 - (1 - R_1)(1 - R_2)$
$\mu = (-lnR)/t$
$P = \prod_{i=1}^{n} P_i$
$R = 1 - \prod_{i=1}^{n} (1 - R_i)$
(b)

Fig. 10. Reliability and failure probability computations for components in (**a**) series linkages where the failure of either component adds to the total system failure, and (**b**) parallel linkages where failure of the system requires the failure of both components. There is no convenient way to combine the failure rate (12). (Courtesy of Prentice Hall.)

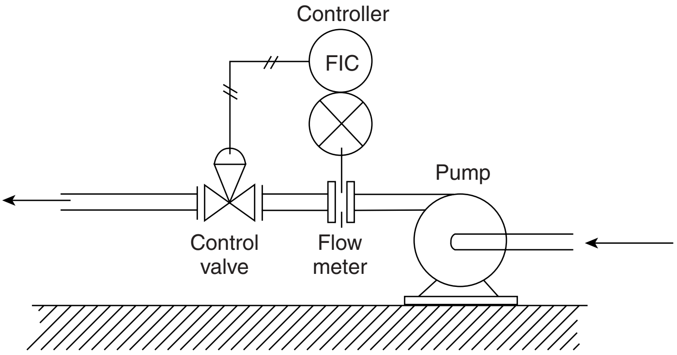

Fig. 11. Flow control system (13). Flow indicator controller = FIC. (Courtesy of Prentice Hall.)

Another problem with this approach is common mode failures. A common mode failure is a single event which could lead to the simultaneous failure of several components at the same time. An excellent example of this is a power failure, which could lead to many simultaneous failures. Frequently, the common mode failure has a higher probability than the failure of the individual components, and can drastically decrease the resulting reliability.

The results computed using this approach are only as good as the failure rate data for the specific equipment. Frequently, failure rate data are difficult to acquire. For this case, the numbers computed only have relative value, that is, they are useful for determining which configuration shows increased reliability.

Figure 11 shows a system for controlling the water flow to a chemical reactor. The flow is measured by a differential pressure (DP) device. The controller decides on an appropriate control strategy and the control valve manipulates the flow of coolant. The procedure to determine the overall failure rate, the failure probability, and the reliability of the system, assuming a one-year operating period, is outlined herein.

These process components are related in series, thus if any one of the components fails, the entire system fails. The failure rates for the various components are given in Table 3. The reliability and failure probability are computed for each individual component using equations 1 and 2 and assuming a one-year period of operation. The results are shown in Table 4.

Table 4. **Risk Assessment of Flow Control System**[a]

Component	Failure rate, μ, faults/year	Reliability, $R = e^{-\mu t}$	Failure probability, $P = 1 - R$
control valve	0.60	0.55	0.45
controller	0.29	0.75	0.25
DP cell	1.41	0.24	0.76

The overall reliability for components in series is computed using the appropriate equation in Figure 10. The result is

$$R = \prod_{i=1}^{3} R_i = (0.55)\,(0.75)\,(0.24) = 0.10$$

The failure probability is computed from equation 2.

$$P = 1 - R = 1 - 0.10 = 0.90/\text{year}$$

The overall failure rate is computed using the definition of the reliability, equation 1.

$$\mu = -\ln(0.10) = 2.30 \text{ failures/year}$$

6. Hazard Acceptance and Inherent Safety

The remaining step in the hazard identification and risk assessment procedure shown in Figure 1 is to decide on risk acceptance. For this step, few resources are available and analysts are left basically by themselves. Some companies have formal risk acceptance criteria. Most companies, however, use the results on a relative basis. That is, the results are compared to another process or processes where hazards and risks are well characterized.

If the hazards and/or risk are unacceptable, then something must be done to change them. The process can be modified, the raw materials changed, and/or the process relocated, for example. In extreme cases, the process might be abandoned as too hazardous.

A more recent concept which could have significant impact on future designs is that of inherently safer design (14,15). This basic principle states that what is not there cannot be blown up or leak into the environment. Thus, the idea is to avoid the hazard in the first place.

Inherently safer design is performed by three techniques. First, there is substitution. This means substituting a less hazardous material for the material in use and asking whether that flammable solvent is really necessary. Or is that toxic chemical the only possible reaction pathway? The second method for inherently safer design is attenuation, ie, operating the process at lower temperatures and pressures. The last inherently safer design technique is intensification. This means using much smaller inventories of hazardous raw and intermediate materials, and reducing process hold-up and inventories. These inventories are readily reducible if the management practices associated with the resources are improved.

Details on the technical management requirements for a successful hazards analysis and risk assessment program are provided elsewhere (16).

BIBLIOGRAPHY

"Hazard Analysis and Risk Assessment," in *ECT* 4th ed., Vol. 12, pp. 930–949, by Daniel A. Crowl, Michigan Technological University; "Hazard Analysis and Risk Assessment" in

ECT (online), posting date: December 4, 2000, by Daniel A. Crowl, Michigan Technological University.

CITED PUBLICATIONS

1. *Guidelines for Hazards Evaluation Procedures: Second Edition with Worked Examples*, American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 1992.
2. D. A. Crowl and J. F. Louvar, *Chemical Process Safety: Fundamentals with Applications*, 2nd ed., Prentice-Hall, Englewood Cliffs, N.J., 2002.
3. *Dow's Fire and Explosion Index Hazard Classification Guide*, 7th ed., American Institute of Chemical Engineers, New York, 1994.
4. *Dow's Chemical Exposure Index Guide*, American Institute of Chemical Engineers, New York, 1994.
5. G. A. Page, *Hazard Evaluation Manual*, American Cyanamid, Wayne, N.J., 1990.
6. Ref. 2, p. 452.
7. Ref. 2, p. 492.
8. *Guidelines for Chemical Process Quantitative Risk Analysis*, 2nd ed., American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 2000.
9. F. P. Lees, *Loss Prevention in the Process Industries*, 2nd ed., Butterworths, London, 1996.
10. *Guidelines for Consequence Analysis of Chemical Releases*, American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 1999.
11. K. C. Kapur and L. R. Lamberson, *Reliability in Engineering Design*, John Wiley & Sons, Inc., New York, 1977.
12. Ref. 2, p. 476.
13. Ref. 2, p. 477.
14. T. Kletz, *Plant Design for Safety, A User Friendly Approach*, Hemisphere Publishing, New York, 1991.
15. R. E. Bollinger and co-workers, *Inherently Safer Chemical Processes, A Life Cycle Approach*, American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 1996.
16. *Guidelines for Technical Management of Chemical Process, Safety*, American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 1989.

GENERAL REFERENCES

1. S. R. Hanna and P. J. Drivas, *Guidelines for Use of Vapor Cloud Dispersion Models*, 2nd ed., American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 1996.

Daniel A. Crowl
Michigan Technological University