1

Introduction to the Guidelines

A *hazard* is a physical or chemical condition that has the potential for causing harm to people, property, or the environment. A *hazard evaluation* is an organized effort to identify and analyze the significance of hazardous situations associated with a process or activity. Specifically, hazard evaluations are used to pinpoint weaknesses in the design and operation of facilities that could lead to hazardous material releases, fires, or explosions. These studies provide organizations with information to help them improve the safety and manage the risk of their operations.

Hazard evaluations usually focus on process safety issues, like the acute effects of unplanned chemical releases on plant personnel or the public. These studies complement more traditional industrial health and safety activities, such as protection against slips or falls, use of personal protective equipment, monitoring for employee exposure to industrial chemicals, and so forth. Many hazard evaluation techniques can also be used to help satisfy related needs (e.g., operability, economic, and environmental concerns). Although hazard evaluations typically analyze potential equipment failures and human errors that can lead to incidents, the studies can also highlight gaps in the management systems of an organization's process safety program. For example, a hazard evaluation of an existing process may reveal gaps in the facility's management of change program or deficiencies in its maintenance practices.

From its inception, the Center for Chemical Process Safety (CCPS) has recognized the importance of hazard evaluations; in fact, the first book in CCPS' series of guidelines dealt with hazard evaluation procedures.[1] Because of the ongoing and increased emphasis on performing hazard evaluations, CCPS commissioned the development of the *Guidelines for Hazard Evaluation Procedures, Third Edition.* The purpose of *Part I — Hazard Evaluation Procedures* is to provide users with a basic understanding of the concepts of hazard evaluation, as well as information about specific techniques so they will be able to perform high quality hazard evaluations within a reasonable amount of time. Several chapters on new topics, including preparing for studies, identifying hazards, and following up after completed analyses are included in the *Guidelines.*

In addition, because of the ongoing need to train a large number of competent hazard evaluation practitioners, this document includes the companion, *Part II — Worked Examples.* The *Worked Examples* give detailed illustrations of how the various hazard evaluation techniques can be used throughout the lifetime of a process as a part of a company's process safety management (PSM) program. People responsible for hazard evaluation training in their organizations will find both the *Hazard Evaluation Procedures* and the *Worked Examples* to be valuable resources.

The remainder of the Introduction explains some basic terminology and concepts of hazard evaluation and its relationship to risk management. It outlines various incident prevention and risk management strategies and discusses how hazard evaluation can provide important information to organizations who are striving for incident-free operation. This section also discusses how hazard evaluations can be performed throughout the life of a process as part of a PSM program. Finally, some limitations that should influence the interpretation and use of hazard evaluation results are presented.

1.1 Background

Formal hazard evaluations have been performed in the chemical process industry (CPI) for more than thirty years. Other less systematic reviews have been performed for even longer. Over the years, hazard evaluations have been called by different names. At one time or another, all of the terms listed in Table 1.1 have been used as synonyms for hazard evaluation, with some of the terms having different shades of meaning depending on the context and usage.

An important prerequisite or starting point for performing a hazard evaluation is the identification of process hazards, since hazards that are not identified cannot be further studied. Chapter 3 describes frequently used hazard identification methods and discusses their use in hazard evaluation efforts. An efficient and systematic hazard evaluation, preceded by a thorough hazard identification effort, can increase managers' confidence in their ability to manage risk at their facilities.

Hazard evaluations usually focus on the potential causes and consequences of episodic events, such as fires, explosions, and unplanned releases of hazardous materials, instead of the potential effects of conditions that may routinely exist such as a pollutant emitted from a registered emission point. Also, hazard evaluations usually do not consider situations involving occupational health and safety issues, although any new issues identified during the course of a hazard evaluation are not ignored and are generally forwarded to the appropriate responsible person. Historically, these issues have been handled by good engineering design and operating practices. In contrast, hazard evaluations also focus on ways that equipment failures, software problems, human errors, and external factors (e.g., weather) can lead to fires, explosions, and releases of toxic material or energy.

Hazard evaluations can occasionally be performed by a single person, depending upon the specific need for the analysis, the technique selected, the perceived hazard of the situation being analyzed, and the resources available. However, ***most high-quality hazard evaluations require the combined efforts of a multidisciplinary team.*** The hazard evaluation team uses the combined experience and judgment of its members along with available data to determine whether the identified problems are serious enough to warrant change. If so, they may recommend a particular solution or suggest that further studies be performed. Sometimes a hazard evaluation cannot give decision makers all the information they need, so more detailed methods may need to be used such as Layer of Protection Analysis (LOPA) or Chemical Process Quantitative Risk Analysis (CPQRA).

The purpose of these *Guidelines* is to provide practitioners and potential users of the results of hazard evaluations with information about identifying hazards, selecting a hazard evaluation technique appropriate for a particular need, using a particular method, and following up on the results. This document is designed to be useful to the veteran hazard analyst as well as the novice. It also provides some guidance to those faced with using, reviewing, or critiquing the results of hazard evaluations so they will know what to reasonably expect from them. Special emphasis is placed on the theoretical and practical limitations of the various hazard evaluation techniques presented.

Table 1.1 Hazard evaluation synonyms

▪ Process hazard(s) analysis	▪ Predictive hazard evaluation	▪ Hazard and risk analysis
▪ Process hazard(s) review	▪ Hazard assessment	▪ Hazard identification and risk analysis
▪ Process safety review	▪ Process risk survey	
▪ Process risk review	▪ Hazard study	

1.2 Relationship of Hazard Evaluation to Risk Management Strategies

Over the past few years, remarkable progress has been made toward institutionalizing formal process safety management (PSM) programs within chemical process industry companies. This crescendo of activity was sparked by a variety of factors including (1) the occurrence of major industrial incidents, (2) aggressive legislative and regulatory process safety initiatives reflecting a reduced public risk tolerance, and (3) the evolution and publication of model PSM programs by several industrial organizations.[2-9] Perhaps even more significant was the increased awareness and the enlightened self-interest of companies that realized, in the long run, operating a safer plant leads to more profitable business performance and better relationships with communities and regulatory agencies.

In 1989, CCPS published its *Guidelines for Technical Management of Chemical Process Safety*, which outlined a twelve-element strategy for organizations to consider when adopting management systems to ensure process safety in their facilities.[10] This strategy has been more recently updated and expanded to reflect an emphasis on risk-based process safety, as reflected in the twenty elements listed in Table 1.2.[16] Two of the elements in this table address the identification of hazards, assessment of risk, and selection of risk control alternatives throughout the operating lifetime of a facility. Other elements such as management of change, incident investigation, and asset integrity and reliability can also involve the use of hazard evaluation techniques.

Implementing a PSM program can help an organization manage the risk of a facility throughout its lifetime. Managers must, at various times, be able to develop and improve their understanding of the things that contribute to the risk of the facility's operation.[11-13] Developing this understanding of risk requires addressing three specific questions (also shown in Figure 1.1):

- ***What can go wrong?***
- ***What is the potential impact*** *(i.e., how severe are the potential loss event consequences)?*
- ***How likely is the loss event to occur?***

Table 1.2 CCPS elements of risk-based process safety

Commit to process safety	**Manage risk**	**Learn from experience**
▪ Process safety culture	▪ Operating procedures	▪ Incident investigation
▪ Compliance with standards	▪ Safe work practices	▪ Measurement and metrics
▪ Process safety competency	▪ Asset integrity and reliability	▪ Auditing
▪ Workforce involvement	▪ Contractor management	▪ Management review and continuous improvement
▪ Stakeholder outreach	▪ Training and performance assurance	
Understand hazards and risk	▪ Management of change	
▪ Process knowledge management	▪ Operational readiness	
▪ Hazard identification and risk analysis	▪ Conduct of operations	
	▪ Emergency management	

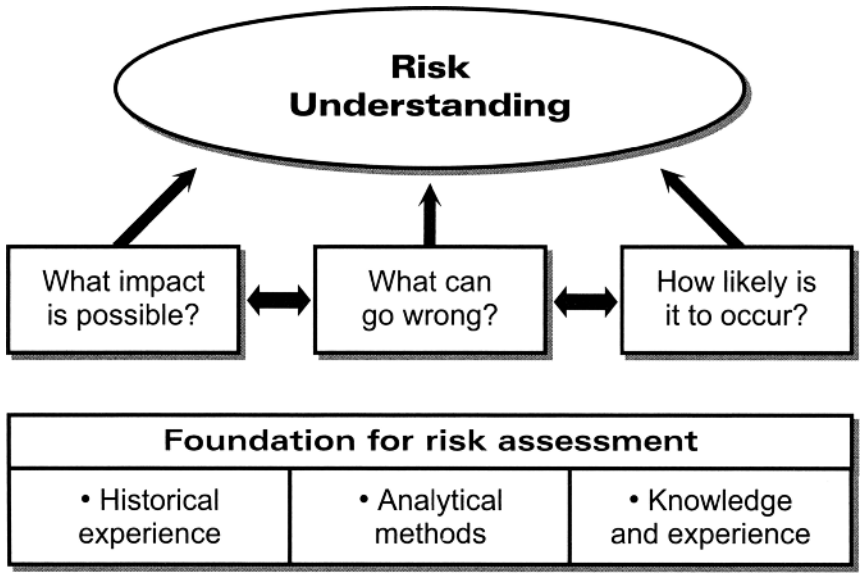

Figure 1.1 Aspects of understanding risk

The effort needed to develop this understanding of risk will depend upon (1) how much information the organization possesses concerning potential incidents and (2) the specific circumstance that defines the organization's need for better risk information. In any case, managers should first use their experience and knowledge to understand the risk their organizations face in operating a facility. If the organization has a great deal of pertinent, closely related experience with the subject process or operation, then little formal analysis may be needed. In these situations, experienced-based hazard evaluation tools (e.g., checklists) are commonly used to manage risk.

On the other hand, if there is not a relevant or adequate experience base, an organization may have to rely on analytical techniques for developing "answers" to the three risk questions to satisfactorily meet the organization's risk management needs. In these situations, organizations typically use predictive hazard evaluation techniques to creatively evaluate the significance of potential incidents.

Using hazard evaluation techniques is one way to increase a company's understanding of the risk associated with a planned or existing process or activity so that appropriate risk management decisions can be made.

1.3 Anatomy of a Process Incident

One definition of process safety is the sustained absence of process incidents at a facility. To prevent these process incidents, one must understand how they can occur. Using hazard evaluation methods can help organizations better understand the risks associated with a process and how to reduce the frequency and severity of potential incidents. Section 1.2 showed how hazard evaluation procedures fit into an

overall strategy for risk management. The purpose of Sections 1.3 and 1.4 is to discuss some of the salient features of process incidents by presenting the "anatomy" of typical process incidents.[14]

A process hazard represents a threat to people, property and the environment. Examples of process hazards are given in Table 1.3. Process hazards are always present whenever hazardous materials and hazardous process conditions are present. Under normal conditions, these hazards are all contained and controlled.

An ***incident*** is defined as an unplanned event or sequence of events that either resulted in or had the potential to result in adverse impacts. Thus, an ***incident sequence*** is a series of events that can transform the threat posed by a process hazard into an actual occurrence.

Table 1.3 Elements of process incidents

Process hazards	Initiating causes	Incident outcomes
Significant inventories of:	Containment failures	Loss events
Flammable materials	Pipes, ducts, tanks, vessels, containers, flexible hoses, sight glasses, gaskets/seals	Discharges or releases
Combustible materials		Fires
Unstable materials	Equipment malfunctions	Pool fires
Corrosive materials	Pumps, compressors, agitators, valves, instruments, sensors, control failures	Jet fires
Asphyxiants		Flash fires
Shock-sensitive materials	Spurious trips, vents, reliefs	Fireballs
Highly reactive materials		Explosions
Toxic materials	Loss of utilities	Confined explosions
Inert gases	Electricity, nitrogen, water, refrigeration, air, heat transfer fluids, steam, ventilation	Unconfined vapor cloud explosions
Combustible dusts		Vessel rupture explosions
Pyrophoric materials	Human errors	BLEVEs
Physical conditions	Operations	Dust explosions
High temperatures	Maintenance	Detonations
Cryogenic temperatures	External events	Condensed-phase detonations
High pressures	Vehicle impact	Impacts
Vacuum	Extreme weather conditions	Toxic, corrosive, thermal, overpressure, missile, and other effects on:
Pressure cycling	Earthquake	Community
Temperature cycling	Nearby incident impacts	Workforce
Vibration/liquid hammering	Vandalism/sabotage	Environment
Ionizing radiation		Company assets
High voltage/current		Production
Mass storage		
Material movement		
Liquefied gases		

The first event in an incident sequence is called the ***initiating cause***, also termed the ***initiating event*** or, in the context of most hazard evaluation procedures, just the ***cause***. The types of events that can initiate incident sequences are generally equipment or software failures, human errors, and external events. Table 1.3 gives some examples.

The initiating cause can be understood by considering the anatomy of an incident from an operations perspective, as presented in Figure 1.2. In the **Normal** operations mode, all process hazards are contained and controlled, and the facility is operating within established limits and according to established operating procedures. The operational goals during normal operation can be summarized as optimizing production and keeping the facility within the bounds of the normal operating procedures and limits. Key systems involved in keeping the facility operating normally include the primary containment system typically consisting of piping and vessels, the basic process control system (BPCS) including sensors and final control elements, functional process equipment such as pumps and distillation columns, and the execution of operational tasks according to established operating procedures. These key systems are supported by activities such as inspections, functional testing, preventive maintenance, operator training, management of change, and facility access control.

An ***initiating cause*** has as its result a shift from a **Normal** to an **Abnormal** operations mode, as soon as the operation departs from its established operating procedures or safe operating limits. In the context of hazard evaluation procedures, this abnormal mode is termed a ***deviation***. For example, loss of cooling water supply to an exothermic reaction system can be an initiating cause for a runaway reaction incident sequence. As soon as the cooling water supply (pressure and/or flow rate) drops below the minimum established limit, it can be considered an initiating cause, and the plant is in an "abnormal situation." The plant operational goal changes when an abnormal situation is detected. Instead of the goal of keeping the plant operating within normal limits, the operational goal becomes returning the plant to normal operation if possible; and, if this is not possible, bringing it to a safe state such as shutting down the unit before a loss event can occur.

If the situation in this example is allowed to continue uncorrected, a runaway reaction may result, with possible outcomes of an emergency relief discharge to the atmosphere (if the system is so configured) or a vessel rupture due to overpressurization. At this point, the operating mode transitions from an abnormal situation—which may be able to be corrected and brought back under control—to an **Emergency** situation. (The term "emergency" in this context refers to the emergency operations mode after a loss event occurs. Emergency procedures may actually be activated even before the relief discharge or vessel rupture event.) The operational goal again changes in an emergency situation, with the objective now being to minimize injuries and losses (*mitigate* the loss event impacts).

Key Concept: the Loss Event

In the anatomy of an incident, the beginning of an **Emergency** situation is termed the ***loss event*** (Figure 1.3), since some degree of loss or harm is likely to ensue once a loss event has occurred. The loss event is the point of time in an incident sequence when an ***irreversible physical event*** occurs that has the potential for loss and harm impacts. Examples include opening of a non-reclosing emergency relief device such as a rupture disk, release of a hazardous material to the environment, ignition of flammable vapors or an ignitable dust cloud, and overpressurization rupture of a tank or vessel. Other examples are given in Table 1.3. Note that an incident might involve more than one loss event, such as a flammable liquid spill (first loss event) followed by ignition of a flash fire and pool fire (second loss event) that heats up an adjacent vessel and its contents to the point of rupture (third loss event).

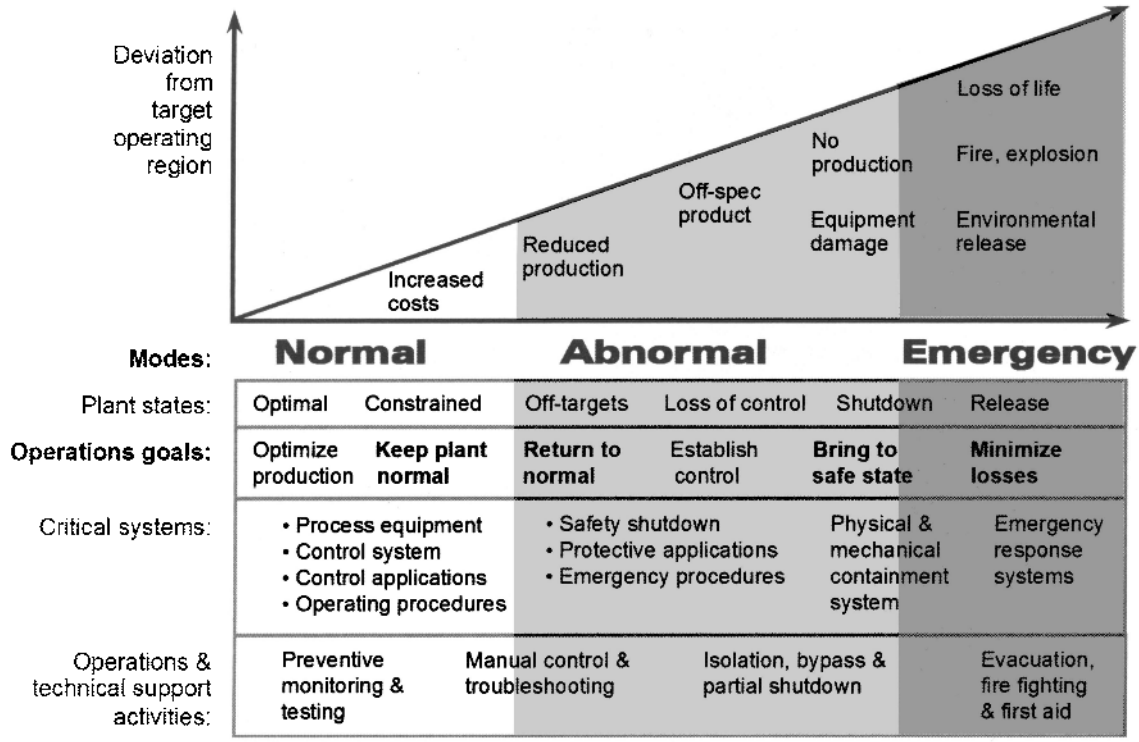

Figure 1.2 Anatomy of a catastrophic incident, from Reference 17

(Note: This Figure is included only to help understand initiating causes and loss events in relation to Normal, Abnormal, and Emergency operational modes and highlighted key operational goals)

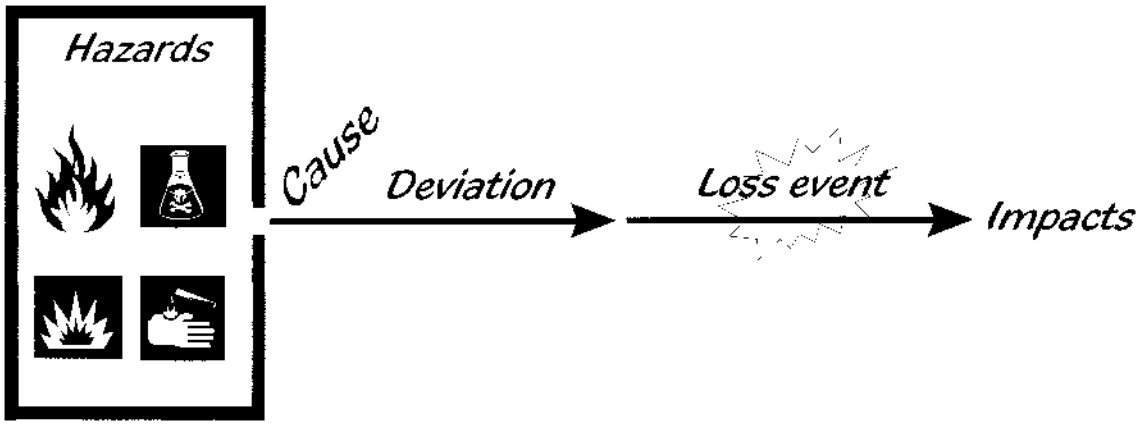

Figure 1.3 Basic incident sequence without safeguards

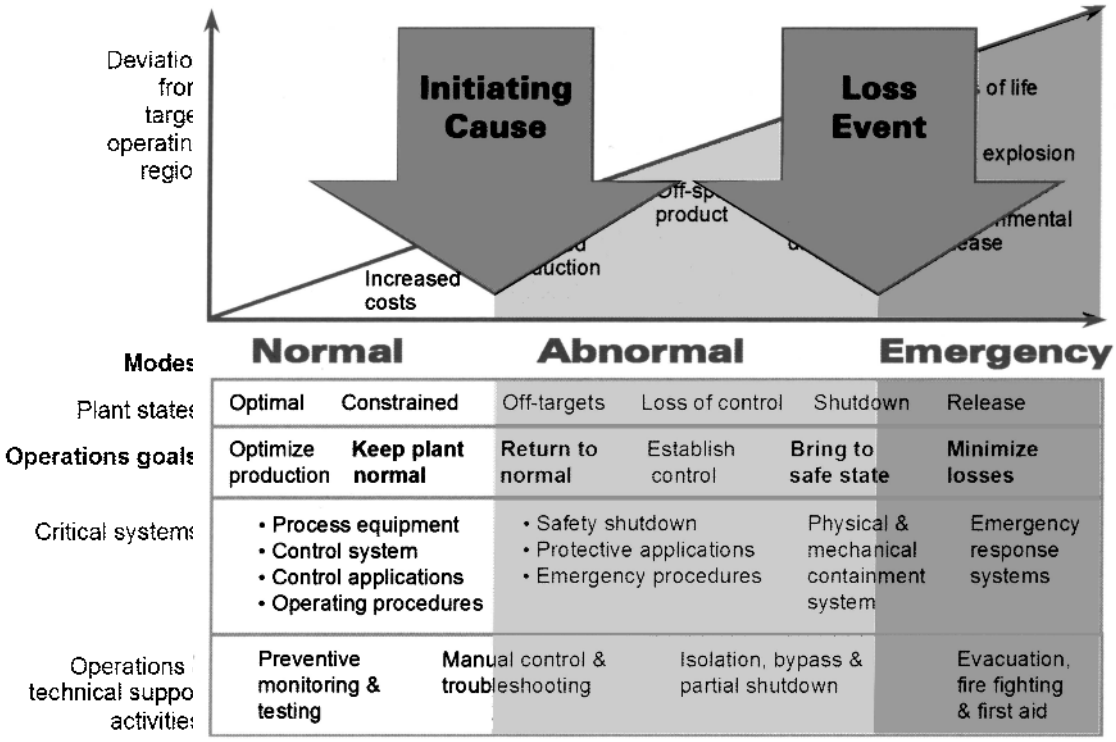

Figure 1.4 Identifying the initiating cause and the loss event in an incident scenario

Figure 1.4 might be helpful in identifying the initiating cause and loss event in an incident sequence. The initiating cause is at the transition from the **Normal** to the **Abnormal** mode of operation, and the loss event is at the transition from the **Abnormal** to the **Emergency** mode of operation.

The ***initiating cause*** may proceed directly to the ***loss event*** if there are no intervening safeguards or if the initiating cause is so severe that the design basis for the safeguards is violated. An example would be sufficient vehicle movement to cause mechanical failure of a simple unloading hose while transferring a hazardous material. As soon as the vehicle-movement initiating cause occurs, the irreversible physical event (unloading hose failure with release of hazardous material to the surroundings) would be realized. More often, there is a series of intermediate events that link an initiating cause to the loss event, due to the presence of preventive safeguards as described in Section 1.4.

The severity of consequences of the loss event is termed the ***impact*** (see Figure 1.3). The impact is a measure of the ultimate loss and harm of a loss event. It may be expressed in terms of numbers of injuries and/or fatalities, extent of environmental damage, and/or magnitude of losses such as property damage, material loss, lost production, market share loss, and recovery costs.

The full description of a possible incident sequence is a ***scenario***. A scenario is an unplanned event or incident sequence that results in a loss event and its associated impacts, including the success or

failure of safeguards involved in the incident sequence (see Section 1.4 regarding the role of safeguards). Thus, each scenario starts with an initiating cause as previously described, and terminates with one or more incident outcomes. The outcomes may involve various physical or chemical phenomena, which can be evaluated using ***consequence analysis*** methodologies, to determine the loss event impacts.

Hazard evaluation methods can help users understand the significance of potential incident sequences associated with a process or activity. This understanding leads to identification of ways to reduce the frequency and severity of potential incidents, thus improving the safety of process operations.

1.4 The Role of Safeguards

In the context of hazard evaluation procedures, any device, system or action that would likely interrupt the chain of events following an initiating cause is known as a ***safeguard***.[18] Different safeguards can have very different functions, depending on where in an incident sequence they are intended to act to reduce risks, as illustrated in an event-tree format in Figure 1.5.

One way of characterizing safeguards that is useful in hazard evaluations is to view the safeguards in relation to the loss event. A ***preventive safeguard*** intervenes after an initiating cause occurs and prevents the loss event from ensuing. A ***mitigative safeguard*** acts after the loss event has occurred and reduces the loss event impacts. Thus, preventive safeguards affect the likelihood of occurrence of the loss event, whereas mitigative safeguards lessen the severity of consequences of the loss event. As will be discussed later, more than one loss event is possible for a given initiating cause, depending on the success or failure of safeguards. Figure 1.6, which is a "bow-tie" diagram as further described in Section 5.7, provides another illustration of how preventive and mitigative safeguards relate to hazards, initiating causes, loss events, and impacts.

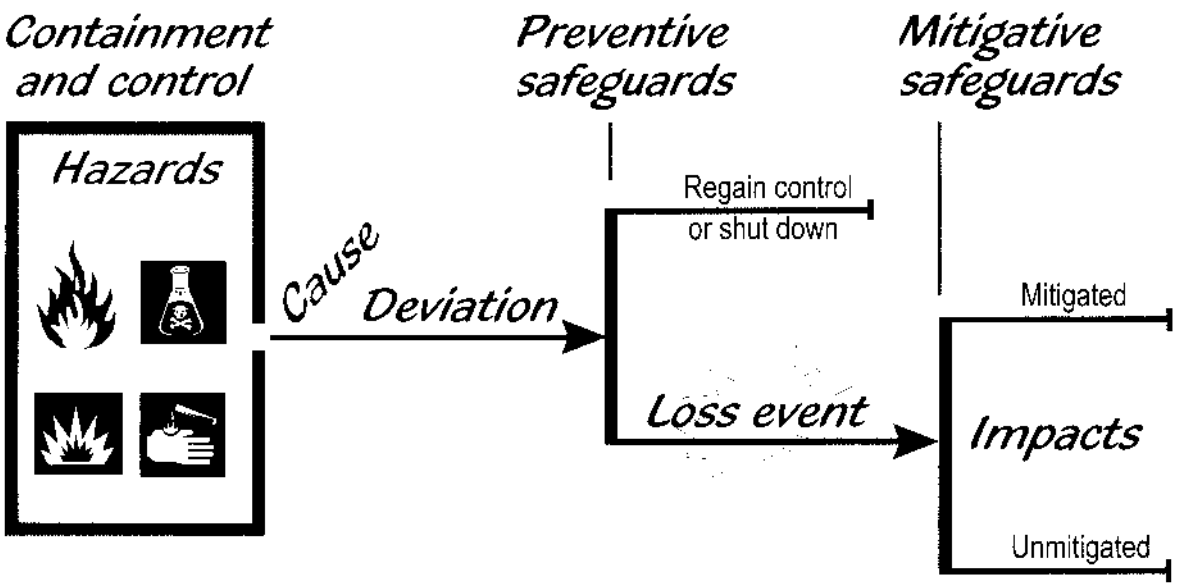

Figure 1.5 Preventive and mitigative safeguards function after an initiating cause has occurred

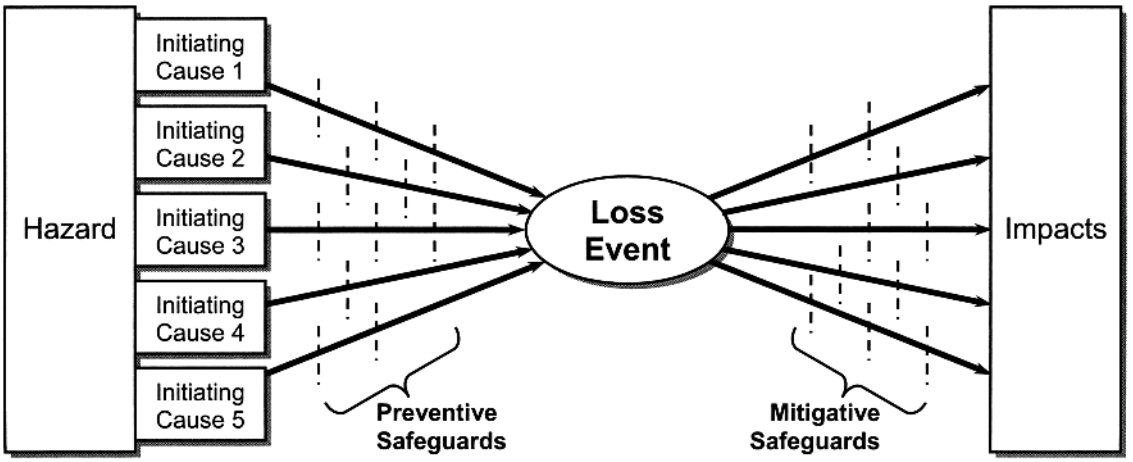

Figure 1.6 Generic "bow-tie" diagram showing relation of safeguards to loss event

Contain and Control

Although not considered to be safeguards as defined above, the containment and control of process hazards serve critical functions in avoiding or reducing the likelihood of initiating causes and ensuing incident scenarios. Note that, in this context, "containment" refers to the primary containment system consisting of piping, vessels and other process equipment designed to keep hazardous materials and energies contained within the process. Secondary containment systems such as diked areas and berms are mitigative safeguards.

Typical ***contain and control*** measures include:

- Proper design and installation of the primary containment system, along with inspections, testing, and maintenance to ensure the ongoing mechanical integrity of the primary containment system
- Guards and barriers to reduce the likelihood of an external force such as maintenance activities or vehicular traffic impacting process piping or equipment
- Basic process control system (BPCS) design, installation, management, and maintenance to ensure successful control system response to anticipated changes and trends such as variations in feed compositions, fluctuations in utility parameters such as steam pressure and cooling water temperature, ambient condition changes, gradual heat exchanger fouling, etc.
- Operator training to reduce the likelihood of a procedure being improperly performed

- Segregation, dedicated equipment, and other provisions to reduce the likelihood of incompatible materials coming into contact with each other
- Management of change with respect to materials, equipment, procedures, personnel, and technology.

The objectives of ***contain and control*** are to keep process material confined within its primary containment system and to keep the process within safe design and operating limits, thus avoiding abnormal situations and loss of containment events that could lead to loss, damage and injury impacts. Containment and control measures, such as those listed above, affect the frequency of initiating causes.

It should be noted that many practitioners consider containment and control measures to also be "safeguards." However, they do not meet the definition of a safeguard given earlier as "any device, system, or action that would likely interrupt the chain of events following an initiating cause." Most of these measures apply not only to individual scenarios but to the entire process or facility, so the repeated listing of measures such as "Operator training" and "Mechanical integrity program" in the Safeguards column on hazard evaluation worksheets only makes it more difficult for the review team to assess the overall effectiveness of the preventive and mitigative safeguards in interrupting the chain of events following the initiating cause. If the desire is to give credit for having these general measures in place, they can be listed in a separate "Primary Containment and Control of Process Hazards" or similar section in a hazard evaluation report, rather than be included throughout the hazard evaluation worksheets.

Preventive Safeguards

Preventive safeguards intervene after an initiating cause has occurred and process conditions are abnormal or out of control. They act to regain control or achieve a safe state when an abnormal process condition is detected, thus interrupting the propagation of the incident sequence and avoiding the loss event (irreversible physical event with potential for loss and harm impacts, such as a hazardous material release, fire, or explosion). Preventive safeguards do not affect the likelihood of initiating causes, but do affect the probability that a loss event will result, given that an initiating cause occurs. Preventive safeguards thus affect the overall scenario frequency. Typical preventive safeguards include:

- Operator response to bring an upset condition back within safe operating limits
- Operator response to a safety alarm or upset condition to manually shut down the process before a loss event can occur
- Instrumented protective system designed and implemented to automatically bring the system to a safe state upon detection of a specified abnormal condition
- Ignition source control implemented to reduce the probability of ignition given the presence of an ignitable mixture, thus preventing the loss event of a fire, dust explosion, confined vapor explosion or vapor cloud explosion
- Emergency relief system acting to relieve vessel overpressurization and prevent the loss event of a bursting vessel explosion
- Other last-resort preventive safety systems such as manual dump or quench systems.

The objective of preventive safeguards is to avoid a loss event or a more severe loss event, given the occurrence of an initiating cause. An example of avoiding a more severe loss event is if mechanical failure of a piping system immediately results in loss of containment of a flammable liquid (which is both an initiating cause and a loss event, since no preventive safeguards intervene), ignition source control can avoid a different, more severe loss event of a fire or vapor cloud explosion.

Preventive safeguards should be considered as systems that must be designed, maintained, inspected, tested, and operated to ensure they are effective against particular incident scenarios. For safety instrumented systems, this is termed the safety integrity level (SIL). CCPS[19] provides guidance on the life cycle management of instrumentation and control systems to achieve a specified level of integrity.

Both qualitative and quantitative methodologies can be used to identify and classify safeguards. Layer of Protection Analysis (LOPA), an order-of-magnitude method that builds on traditional hazard evaluation results to determine the required integrity of safeguards, is summarized in Section 7.6.

The following example illustrates how operator response to a safety alarm can be considered as a preventive safeguard "system" having several essential parts. Figure 1.7 shows the example reaction process used to illustrate Fault Tree Analysis in Section 5.5. The process consists of a reactor for a highly unstable process that is sensitive to small increases in temperature. It is equipped with a deluge for emergency cooling to protect against an uncontrolled reaction. To prevent a runaway reaction during an increase in temperature, the inlet flow of process material to the reactor must be stopped or the deluge must be activated. The reactor temperature is monitored by a sensor (T1) that automatically activates the deluge by opening the deluge water supply valve when a temperature rise is detected. At the same time, sensor T1 sounds an alarm in the control room to alert the operator of the temperature rise. When the alarm sounds, standard operating procedure calls for the operator to push the inlet valve close button to shut the inlet valve and stop inlet flow to the reactor and to push the deluge open button in the control room if the deluge is not activated by sensor T1. If the inlet valve closes or the deluge is activated, system damage due to an uncontrolled reaction is averted. (Note that the example process is described in this manner for illustrative purposes only; this would not likely be the best way to arrange a reactive process of this nature.)

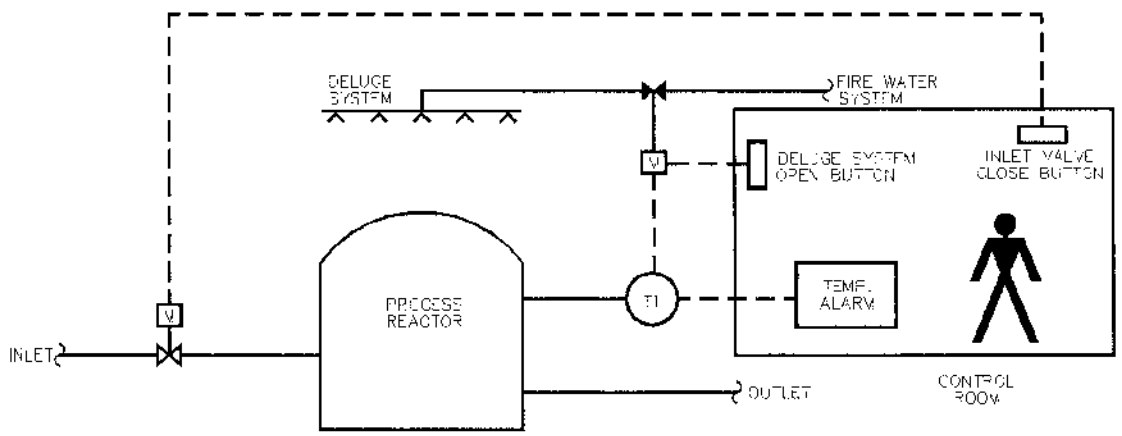

Figure 1.7 Emergency cooling system schematic

The operator response preventive safeguard system would require all of the following to occur in order to successfully protect against the consequence of concern:

1. The temperature sensor is at the right location and responds with inconsequential time delay, giving a correct output signal corresponding to the increase in reactor temperature.

2. A relay or other device successfully operates at the proper safety limit setting to send a signal to the alarm module.

3. The high temperature alarm functions to annunciate the proper audible and/or visual warning in the control room.

4. The operator is present in the control room at the time the alarm sounds.

5. The ambient noise level and distractions are sufficiently minimal such that the operator is alerted by the alarm signal.

6. The operator decides to respond to the alarm and not just acknowledge it.

7. The operator makes the correct diagnosis as to the meaning of the alarm based on the operator's training, experience, and preconceptions of the state of the process.

8. The operator responds to the alarm in time to avert the loss event.

9. The operator actuates the correct push buttons to stop the inlet flow and/or activate the deluge.

10. The inlet flow is stopped in time by successful functioning of the inlet valve close button and the inlet valve; or, the deluge is activated in time by successful functioning of the deluge push button, deluge valve, and deluge piping and nozzles, and an adequate supply of fire water is available.

It should be noted that, for this example, the operator response to the alarm to actuate the deluge system is not independent of the automatic deluge system, since they share a common temperature sensor and a common final control element (deluge water supply valve). Likewise, the operator-actuated inlet flow isolation system and the deluge system are not independent of each other, since they share a common temperature sensor. Thus, a hazard evaluation team would need to evaluate the effectiveness of the overtemperature safeguards by examining both the operator responses and the automatic safety systems together rather than as independent protective systems. This assessment of the independence of preventive safeguards is an important part of a hazard evaluation, regardless of whether the evaluation is performed using a qualitative or a quantitative technique.

Mitigative Safeguards

A *mitigative safeguard* acts to reduce the severity of consequences of a loss event; i.e., the sum total of safety, business, community, and environmental impacts resulting from a fire, explosion, toxic release, or other irreversible physical event. Typical mitigative safeguards include:

- Reclosing emergency relief devices such as safety relief valves, acting to reduce the duration of a hazardous material release loss event if the emergency relief discharges to the atmosphere
- Secondary containment (e.g., double-walled system, secondary enclosure)
- Explosion blast and missile containment structures / barricades
- Fire/release detection and warning systems
- Automatic or remotely actuated isolation valves
- Fire extinguishers, sprinkler systems, and fire water monitors
- Deluge, foam, and vapor mitigation systems
- Fire-resistant supports and structural steel
- Storage tank thermal insulation
- Blast-resistant construction of occupied buildings
- Loss-event-specific personal protective equipment (e.g., splash goggles, flame-retardant clothing, escape respirators)
- Emergency response and emergency management planning.

The objective of mitigative safeguards is to detect and respond to emergency situations in such a way as to reduce the impacts of loss events as compared to the unmitigated impacts without the safeguards.

When performing detailed, scenario-based hazard evaluations, a useful distinction can be drawn between those mitigative safeguards designed to act after the loss event occurs and affect the *source term* (i.e., the release parameters of magnitude, rate, duration, orientation, temperature, etc. that are the initial conditions for determining the consequences of the loss event) and those mitigative safeguards designed to reduce the impacts of the released material or energy on people, property and the environment. Examples of the first category of mitigative safeguards (which could be called *source-mitigative safeguards*) include excess flow valves, dry-break connections on unloading hoses, automatic release detection and isolation systems, and engineered vapor release mitigation systems such as deluges and water curtains. Examples of the second category of mitigative safeguards (which could be called *receptor-mitigative safeguards* and are sometimes termed *response* rather than *mitigation*) include the buffer distance to surrounding populations, occupied building blast resistance, fire-resistant construction, specialized personal protective equipment evacuation or shelter-in-place procedures, and other emergency response actions including firefighting. Section 7.2 includes a discussion of how these different types of safeguards are evaluated when assessing scenario risk.

1.5 Hazard Evaluation Throughout a Plant Lifetime

Many organizations have published model programs for process safety management (PSM). All of these PSM approaches embrace a consistent theme: *Hazard evaluations should be performed throughout the life of a facility.* As an integral part of its PSM program, an organization can use the results of hazard evaluations to help manage the risk of each phase of process activity. Hazard evaluations can be done efficiently from the earliest stages of R&D, in detailed design and construction, during commissioning and start-up, periodically throughout the operating lifetime, and until the process is decommissioned and dismantled.[10,15] A more complete discussion of hazard evaluation at different plant life cycle stages, including as part of managing changes, can be found in Chapter 6, Sections 6.4 and 6.6. Two aspects of hazard evaluation throughout a plant lifetime warrant particular emphasis:

- Using this life cycle approach in association with other PSM activities can efficiently reveal deficiencies in design and operation before a unit is sited, built or operated, thus making the most effective use of resources devoted to ensuring the safe and productive life of a facility.
- Regardless of the technique used for conducting hazard evaluations throughout the operating lifetime of a facility, each study, along with its documented information and assumptions, should be updated or revalidated on a periodic basis.

An important part of performing hazard evaluations throughout a plant lifetime is knowing which technique is the best one for the study. Chapter 5 discusses many factors that influence this decision and provides the logic behind choosing an appropriate technique. One of the most important factors that influences which hazard evaluation technique an analyst chooses is how much information is available to perform the work. Some hazard evaluation methods may be inappropriate or impossible to perform at a particular life cycle stage because of inadequate process information.

1.6 Hazard Evaluation and Regulations

Although most companies in the chemical processing industries conduct hazard evaluations voluntarily because they believe they are necessary to control hazards and to manage risk at an acceptable level, many companies in the world also conduct hazard evaluations because they are required by regulation. For example, in the United States, the U.S. OSHA regulation 29 CFR 1910.119 (Process Safety Management Standard) requires a hazard evaluation to be performed for covered processes in these elements:

- The Process Hazard Analysis element requires a hazard evaluation that meets certain criteria every five years.
- The Management of Change element includes a requirement to assure the safety and health impact is addressed prior to any change being made.

The techniques discussed in this book can be used in part to fulfill the hazard evaluation requirements for this and other international regulations. When hazard evaluations are required by regulation, specific documentation of the study and the follow-up of recommendations may be mandatory so that regulators can be shown that proper hazard evaluations have been completed. Table 1.4 gives a partial list of international regulations requiring some form of hazard identification and evaluation. Many other countries have hazard evaluation requirements that are based on U.S. or European requirements. This list is not comprehensive; companies need to contact government authorities having jurisdiction to determine what regulations apply to them and what hazard evaluation procedures can be used.

1.7 Limitations of Hazard Evaluation

Hazard evaluation, whether one uses experience-based or predictive methods, is subject to a number of theoretical and practical limitations.[11,14] Managers should realize that the quality of any risk management decisions they base on hazard evaluation results will be directly related to their appreciation of the limitations of such studies. Table 1.5 lists five limitations of hazard evaluations discussed in this section. Some of these may be relatively unimportant for a specific study, depending upon its objectives, while others may be minimized through care in execution and by limiting expectations about the applicability of the results. However, both practitioners and users of these studies must respect these limitations when chartering, executing, and using the results of a hazard evaluation.

Table 1.4 Governmental regulations related to identifying and evaluating process hazards

Country or region	Regulation
Australia	National Standard for Control of Major Hazard Facilities [NOHSC:1014 (1996)]
European Union	Seveso II Directive 2003/105/EC
	ATEX 137 Workplace Directive 1999/92/EC
Mexico	NOM-028-STPS-2004, Occupational organization – Safety in the Processes of Chemical Substances
Singapore	National Environment Agency (one-time QRA Report for new chemical plants)
South Korea	Industrial Safety and Health Act — Article 20, Preparation of Safety and Health Management Regulations
United Arab Emirates	Federal Law No 8 of 1980 Regulations of Labour Relations
	Federal Law No 24 of 1999 for the protection and development of the environment
United Kingdom	U.K. Health & Safety Executive, Control of Major Hazards (COMAH) regulations
United States	29 CFR 1910.119, U.S. Occupational Safety and Health Administration (OSHA) Process Safety Management of Highly Hazardous Chemicals
	40 CFR 68, U.S. Environmental Protection Agency (EPA) Risk Management Program for Chemical Accident Release Prevention

Table 1.5 Classical limitations of hazard evaluations

Issue	Description
Completeness	There can never be a guarantee that all incident situations, causes, and effects have been considered
Reproducibility	Various aspects of hazard evaluations are sensitive to analyst assumptions; different experts, using identical information, may generate different results when analyzing the same problem
Inscrutability	The inherent nature of some hazard evaluation techniques makes the results difficult to understand and use
Relevance of experience	A hazard evaluation team may not have an appropriate base of experience from which to assess the significance of potential incidents
Subjectivity	Hazard analysts must use their judgment when extrapolating from their experience to determine whether a problem is important

Completeness

The issue of completeness affects a hazard evaluation in two ways. First, it arises in the hazard identification step — an analyst can never be certain that all hazardous conditions or potential incident scenarios have been identified. Second, for those hazards that have been identified, a hazard analyst can never guarantee that all possible causes and effects of potential incidents have been considered. It is impossible for a hazard analyst to identify and assess the significance of all possible things that can go wrong even for a very limited, well-defined set of circumstances. But one can reasonably expect trained and experienced practitioners, using systematic hazard evaluation techniques and relevant experience, to identify the most important incidents, causes, and effects.

Moreover, a hazard evaluation is a "snapshot in time" evaluation of a process. Any changes in design, procedures, operation or maintenance (however small) may have a significant impact on the safety of the facility.

Reproducibility

Probably the least appreciated limitation of hazard evaluation techniques is that the results of a hazard evaluation, because of their highly subjective nature, are difficult to duplicate by independent experts. Even with the variety of experience-based and predictive methods available for use in a hazard evaluation, the performance of a high quality hazard evaluation is still largely dependent on good judgment. The subtle assumptions that hazard analysts and process experts necessarily make while performing hazard evaluations can often be the driving force behind the results. Analysts should always highlight their known assumptions when documenting their work so future users can identify the places where additional research is necessary for better hazard information or data. As organizations gain experience in using these approaches, they will appreciate that the assumptions made during a study are as important as any of the results.

Inscrutability

Hazard evaluations can generate hundreds of pages of tables, minutes of review team meetings, models such as fault trees and event trees, and other information. Attempting to assimilate all of the details of a hazard evaluation, depending upon the method chosen and the size of the problem, can be an overwhelming task. Combined with hazard analysts' tendencies to use copious amounts of jargon, reviewers can find themselves wondering what to do with all this information. Fortunately, not all hazard evaluations result in this much paperwork; instead, effective hazard evaluation analysts produce a summary of potential improvements or areas for additional study that management should consider pursuing to improve the safety of the process. These lists, by themselves, are usually straightforward; however, depending upon the technique used to perform the hazard evaluation, the underlying technical bases of the problems and the potential effectiveness of the solutions may be difficult to understand.

Relevance of Experience Base

Some hazard evaluation methods depend solely on the analysts' experience with similar operations (e.g., the Checklist Analysis technique). Other hazard evaluation techniques involve analysts predicting the causes and effects of potential incidents based on their creativity and judgment. All of the techniques hope to capitalize, to some extent, on an organization's experience with a hazardous process. In cases where the experience base is limited, not very relevant, or nonexistent, hazard analysts should use more predictive, systematic techniques such as HAZOP Study or Fault Tree Analysis. Even then, users of the results of these studies must be cautious, since the foundation of knowledge on which the study is based may not justify the use of a sophisticated hazard evaluation technique. Use of a detailed analysis technique does not guarantee better risk understanding; the relevance of the experience base that underlies the analysis is more important than the use of a particular hazard evaluation method.

Reliance on Subjective Judgment

Hazard evaluations use qualitative techniques to determine the significance of potential incident situations. Inherently, the conclusions of such a study are based on the collective knowledge and experience of the hazard evaluation team. Because many of the events considered by the team may never have happened before, the team must use their creativity and judgment to decide whether the potential causes and effects of the incident pose a significant risk. The subjective nature of these deliberations may trouble some people who use the results of these studies, as this subjectivity can create a lack of confidence in the results. Some people incorrectly believe that if an analyst uses quantitative methods to express the significance of a problem, then the limitation of subjectivity will simply fade away. However, this is not the case. Although quantifying the risk parameters can reduce some of the subjectivity in estimating likelihoods and impact, the apparent numerical precision of a chemical process quantitative risk analysis can mask (1) a great deal of the judgment that influenced the identification of incident scenarios and the selection of incident models and (2) large uncertainties associated with the data used to estimate risk. In fact, the quality of hazard evaluation and CPQRA studies alike depend upon having performed an exhaustive search for what can go wrong. In the end, the user must have confidence in both the team and the technique selected for performing the hazard evaluation.

The limitations discussed above should not be reasons for rejecting the use of hazard evaluation techniques. Learning from experience alone may be adequate when the consequences of an incident are small. However, the consequences of potential incidents are not always small, and gaining an empirical perspective of risk through experiencing high-consequence incidents is not acceptable. Hazard evaluation techniques can help analysts find ways to reduce both the frequency and severity of life-threatening loss events. In this way, hazard evaluation techniques can form the basis for a sound and cost-effective risk management program.

Chapter 1 References

1. Center for Chemical Process Safety, *Guidelines for Hazard Evaluation Procedures*, American Institute of Chemical Engineers, New York, 1985.
2. Recommended Practice RP-750, "Management of Process Hazards," American Petroleum Institute, Washington, DC, January 1990, reaffirmed May 1995.
3. Organization Resources Counselors, Inc., *Process Hazards Management of Substances with Catastrophic Potential*, Process Hazard Management Task Force. Washington, DC, 1988.
4. *Responsible Care Management System® Guidance and Interpretations (RCMS 102)*, American Chemistry Council, Arlington, Virginia, 2004.
5. 29 CFR 1910.119, *Process Safety Management of Highly Hazardous Chemicals*, Occupational Safety and Health Administration, Washington, DC, 1992.
6. 40 CFR Part 355, "Extremely Hazardous Substances List," U.S. Environmental Protection Agency, Washington, DC, 1987.
7. N.J.A.C. 7:31, Toxic Catastrophe Prevention Act of 1987, New Jersey Department of Environmental Protection, Trenton, 1987.
8. State of California Health and Safety Code, *Risk Management and Prevention Program*, Chapter 8.95 of Division 20, Sacramento, 1987.
9. Extremely Hazardous Substances Risk Management Act of 1989, Delaware Department of Natural Resources and Environmental Control, Wilmington, DE, 1989.
10. Center for Chemical Process Safety, *Guidelines for Technical Management of Chemical Process Safety*, American Institute of Chemical Engineers, New York, 1989.
11. Arendt, J. S. et al., *Evaluating Process Safety in the Chemical Industry—A Manager's Guide to Quantitative Risk Assessment*, American Chemistry Council, Arlington, Virginia, 1989.
12. V. L. Grose, *Managing Risk—Systematic Loss Prevention for Executives*, Prentice Hall, Englewood Cliffs, New Jersey, 1987.
13. G. L. Head, *The Risk Management Process*, Risk and Insurance Management Society, Inc., New York, 1978.
14. Center for Chemical Process Safety, *Guidelines for Chemical Process Quantitative Risk Analysis, 2nd Ed.*, American Institute of Chemical Engineers, New York, 1999.
15. J. Stephenson, *System Safety 2000—A Practical Guide for Planning, Managing, and Conducting System Safety Programs*, ISBN 0-0442-23840-1, Van Nostrand Reinhold, New York, 1991.
16. Center for Chemical Process Safety, *Guidelines for Risk Based Process Safety*, American Institute of Chemical Engineers, New York, 2007.
17. Abnormal Situation Management® Consortium, "Anatomy of a Catastrophic Incident," www.asmconsortium.com. Figure 1.3 is based on original concepts created by K. Emigholz of ExxonMobil, I. Nimmo of UCDS LLC and J. Errington of NOVA Chemicals. Earlier version published in I. Nimmo, "Adequately Address Abnormal Operations," *Chemical Engineering Progress 91*(9), 36-45, September 1995.
18. Center for Chemical Process Safety, *Layer of Protection Analysis: Simplified Process Risk Assessment*, ISBN 0-8169-0811-7, American Institute of Chemical Engineers, New York, 2001.
19. Center for Chemical Process Safety, *Guidelines for Safe and Reliable Instrumented Protective Systems*, ISBN 978-0-471-97940-1, American Institute of Chemical Engineers, New York, 2007.