Application of Hazard Evaluation Techniques To The Design of Potentially Hazardous Industrial Chemical Processes

NIOSH Instructional Module

SHAPE

Safety/Health Awareness for Preventive Engineering

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Public Health Service
Centers for Disease Control
National Institute for Occupational Safety and Health

CDC

CENTERS FOR DISEASE CONTROL

APPLICATION OF HAZARD EVALUATION TECHNIQUES TO THE DESIGN OF POTENTIALLY HAZARDOUS INDUSTRIAL CHEMICAL PROCESSES

Authors
H.R. Kavianian
J.K. Rao
G.V. Brown
California State University, Long Beach

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Public Health Service
Centers for Disease Control
National Institute for Occupational Safety and Health
Division of Training and Manpower Development
Cincinnati, Ohio
March 1992

ACKNOWLEDGEMENTS

We wish to thank the following personnel for their review of this document: John Etherton, NIOSH; Michael G. Gressel, NIOSH; Laurence D. Reed, NIOSH; and Robert M. Rosen, BASF. The report was edited by Marion G. Curry. Layout and typesetting were provided by Pauline J. Elliott.

This report was prepared in support of NIOSH Project SHAPE (Safety and Health Awareness for Preventive Engineering). Project SHAPE is designed to enhance the education of engineers in the safety and health field.

DISCLAIMER

The opinions, findings, and conclusions expressed are not necessarily those of the National Institute for Occupational Safety and Health, nor does mention of company names or products constitute endorsement by the National Institute for Occupational Safety and Health.

NIOSH Project Officer
John T. Talty, P.E.

NIOSH Order No. 88-79897

PREFACE

The field of occupational and environmental safety has grown rapidly making it difficult for technology transfer to keep pace with changes in engineering and science, laws and regulatory demands, and the attitude of workers and the public.

This module is addressed to college-level faculty in schools of engineering. In addition, managers and technical personnel should find it a useful reference in dealing with this complex field.

Employees in the workplace have a growing need to be more knowledgable about the hazards of their work environment. It is imperative that individuals and governments work together to better inform and protect these workers from the varied and complex exposure of potentially hazardous situations. Additionally, community relations and the general public play an ever increasing role in management and operation of facilities. The public has a right to know and better understand the potential hazards of such operating facilities within or near their communities to better anticipate problems that may arise.

The more management understands about potential hazards and the implementation of measures to either eliminate or reduce the risk connected with these hazards, the better will be the relationship among the operating facility, the workers, and the community.

Historically, many aspects of safety have been delegated to people lacking the engineering and scientific knowledge to readily understand the principles behind hazards in the work environment. The result has been that engineers have often not participated in decisions related to occupational and environmental safety. It is imperative that engineers should become more involved in both engineering and management decisions regarding safety. We hope this module will provide additional insight and direction to allow this to happen. Unless safety management and engineering is approached as a science with defined goals and objectives, it would boil down to "lip service" and "slogans."

H.R. Kavianian
J.K. Rao

ABSTRACT

Occupational safety and environmental health issues are of increasingly vital concern both to society and to technological organizations. In designing and operating potentially hazardous facilities, technologies, or processes engineers must consider occupational and environmental hazards as well as their responsibilities for the safety of the surrounding community.

The case studies presented in this module highlight the importance of applying system safety techniques to the design and operation of potentially hazardous processes. These techniques, when applied properly, can identify and rectify the hidden system failure modes that would otherwise contribute to accidents.

Seven different techniques for analyzing hazards (preliminary hazard analysis, "What If" analysis, failure modes effects and criticality analysis, hazard and operability study, fault tree analysis, event tree analysis, and cause-consequence analysis) are described. Several of these evaluation techniques are applied to the preliminary design of five potentially hazardous processes (metal organic chemical vapor deposition, an ethylene production plant, an alkylation process, a high pressure/low density polyethylene plant, and the batch process of industrial and military explosive production).

Emphasis has also been placed on the importance of including hazard evaluation procedures in the senior level capstone design courses of all engineering disciplines. This would equip the graduating engineer with the tools necessary to apply the scientific laws of nature to the design and operation of hazardous processes in an occupationally and environmentally safe manner.

CONTENTS

UNIT V—PRELIMINARY DESIGN OF AN ALKYLATION PROCESS

UNIT VI—PRELIMINARY DESIGN OF A HIGH PRESSURE/LOW DENSITY POLYETHYLENE PLANT

UNIT VII—THE BATCH PROCESS OF INDUSTRIAL AND MILITARY EXPLOSIVE PRODUCTION

UNIT VIII—INSTRUCTOR'S GUIDELINES

List of Figures

List of Figures (cont'd)

List of Tables

Unit I

SYSTEM SAFETY ENGINEERING

PURPOSE:

To introduce students to the importance of system safety in the design process

OBJECTIVE:

To acquaint the student with:

1. System safety engineering
2. The need for incorporation of system safety in the design process
3. Concept of risk evaluation

SPECIAL TERMS:

1. System safety engineering
2. Hazardous technology
3. Occupational safety and environmental laws
4. Acceptable versus unacceptable risk
5. Probability and severity

INSTRUCTOR MATERIALS:

1. Lesson plan
2. Chalkboard

TRAINEE MATERIALS:

1. Participant outlines made by instructor
2. Supplementary materials

INTRODUCTION TO SYSTEM SAFETY

System safety provides a thorough and systematic approach with which to address workplace hazards. Formal hazard evaluation techniques are the result of increasing demands for more precise hazard assessment; the complexity of production, construction, and processes makes it impossible to informally assess risk.

The methods used in system safety engineering are among the most effective and advanced methods to prevent system failures that result in accidents. The system safety approach identifies the hazards associated with a system as a result of process, equipment, or human interactions. This approach must be applied from the earliest stages of development of a process through to shipment of products and disposal of wastes.

Accident causes

Although system safety engineering is a relatively new field, it has been used extensively by the military and the aerospace and nuclear industries to improve the safety of highly complex systems. This approach is based on the concept that: (a) accidents within a system are the result of a number of interacting causes, (b) each cause for an accident can be identified and analyzed in a logical manner, (c) control measures for the cause of each accident can be developed in terms of equipment, instrumentation, and/or standard operating procedures. Through logical application of system safety engineering concepts, an optimum degree of safety can be achieved throughout a system's life cycle. These techniques provide not only a unique opportunity for analysis of all safety aspects of a problem but a valuable tool for communicating safety information to management for designing and operating existing and new facilities.[1]

Optimum safety

System safety concepts are based on the idea that an optimum degree of safety can be achieved within the constraints of system effectiveness. This optimum is attained through a logical reasoning process. Accidents, or potential accidents, are considered to be the result of a number of interacting causes within the system. From a deliberate analysis of the system, each accident cause and interaction is logically identified and evaluated. Work may then be performed to eliminate or otherwise control these accident causes.[1]

System safety definition

The system safety approach begins by defining a system and focusing on how accidents can occur within that system as a result of equipment failure, human error, environmental conditions, or a combination of these. The preventive measures to mitigate the hazards include design of equipment, development of procedural safeguards, or development of procedural safeguards. Early identification, analysis, control, or elimination of the hazards in a process can eliminate the need for major design changes later in the project. Also, early detection of hazards in a process and the associated cost of their elimination or control must be included in the overall economic feasibility of a process. This is especially true in commercialization of new and extremely hazardous technology. The cost of equipment and/or design changes to control or eliminate hazards could change the overall economic picture of the project.[2,3]

NEED TO INCORPORATE SYSTEM SAFETY INTO THE DESIGN PROCESS

Moral and legal responsibilities of engineering profession

As the exact definitions of the moral and legal responsibilities of the "engineer" towards health and safety are under debate, the public will put more and more pressure on industry to enhance the quality of life through advancing technology safely without interfering with their valuable human and natural resources. In recent years, this pressure has been transmitted to industry through strict occupational safety and environmental health laws and regulations.

Today's engineer must accept his/her legal and moral responsibilities along with the technical responsibilities to the public. Many technological organizations have also come to realize that safe work practices and policies will dramatically translate themselves into profit by eliminating or reducing the number of accidents.

Engineering schools and safety

Today's engineer must be equipped with appropriate tools to apply the scientific laws of nature to the design and operation of hazardous technologies safely and with minimum interference with the environment. True, the public has pressured industry; however, this pressure has not been proportionately transmitted to the engineering schools, which

are responsible for the basic education of engineers. If the public's expectations from engineers are to be fulfilled, "Safety" must be regarded as a science, and safety topics must be incorporated into the regular curriculum of engineering schools. Also, the culture of the "system safety" approach must be incorporated into all phases of development of hazardous technologies from the concept to design, pilot plant, and commercial operation.[4,5]

IMPORTANCE OF INCORPORATING SYSTEM SAFETY TOPICS INTO THE SENIOR LEVEL DESIGN PROJECTS

Thousands of accidents occur throughout the United States everyday. Most are caused by the failure of people, equipment, supplies, or surroundings to behave or react as expected. Data published by the National Safety Council reveal that 98 percent of all industrial accidents are caused by unsafe conditions and unsafe acts.[6] Natural disasters have been responsible for 2 percent of industrial accidents. Lack of attention to safety topics at the design stage of a process undoubtedly creates inherent unsafe conditions in the process that lead to disastrous accidents.

As technology mobilizes itself to respond to the ever increasing demands by society to improve the quality of life through advancing technology, new dimensions must be added to the role of the design engineer to accomplish this task in an occupationally and environmentally safe manner.

Public reaction

Public reaction towards unsafe design and operation of our industrial processes has manifested itself in the form of strict occupational and environmental laws in recent years. Traditionally, engineering schools have done a superb job of training engineering students on the fundamental laws of nature governing their fields and on applying these laws to engineering problems. They may have been less successful, however, in conveying to students the importance of occupational and environmental safety in the design process and the criticality of legal as well as moral responsibilities of the engineer towards society.

Engineering student training

It is not uncommon for a senior-level graduating engineer to think only in terms of the technical aspects of the profession, giving little or no emphasis on the real issues of safety and environment in the design process. This graduating engineer is rudely awakened when he or she joins the industry and finds out that safety and environmental issues are real problems that must be dealt with and with little or no training in these areas. Although some companies are commited to train newly hired engineers on occupational safety and environmental problems, not all engineers are lucky enough to work for these companies. Many work for a company with a poor safety record and with no training in these areas; these beginners must learn about safety and environmental problems through trial and error and through unnecessary, senseless accidents.

Engineering schools must take a more responsible position in regard to occupational safety and environmental health problems. Unless safety is regarded as a science and is incorporated into the engineering curriculum in a systematic manner, it can easily turn into "lip service" with no meaningful results.

Design project and system safety

The senior level design project can be the perfect introduction to system safety. Hazard evaluation techniques should be discussed. Students can apply one or more of these techniques to portions of their design project. Students can then appreciate the time and effort that go into such analyses, and can also recognize the cost-saving factors of identifying, reducing, or eliminating hazards at the design stage rather than after implementation. Students in design courses have enough core knowledge of processes to understand, at least fundamentally, the repercussion of system safety. For these reasons hazard evaluation techniques and system safety topics should be addressed in all senior level design projects.

Technical, economic, and safety aspects of design

By incorporating system safety topics into the senior level design courses, the graduating engineer will: (a) realize (maybe for the first time) that, to make a process both economical and operable, safety and environmental issues must go hand in hand with the technical aspects of the project; (b) develop an appreciation of the legal as well as moral respon-

sibilities of the engineering profession; (c) have the minimum tools needed to apply the scientific laws of nature to design and operation of hazardous technologies in an occupationally and environmentally safe manner.

RISK EVALUATION

Hazard Identification

The system safety approach to safe design and operation of potentially hazardous processes can be viewed as a system that allows for equipment, human, and environmental interactions (Figure I-1 a.). The next step is to identify hazards that could result from equipment failure, human error, environmental conditions or a combination of these effects. Hazards generally fall into one of four categories: physical, chemical, biological, and human factors (Figure I-1 b.).

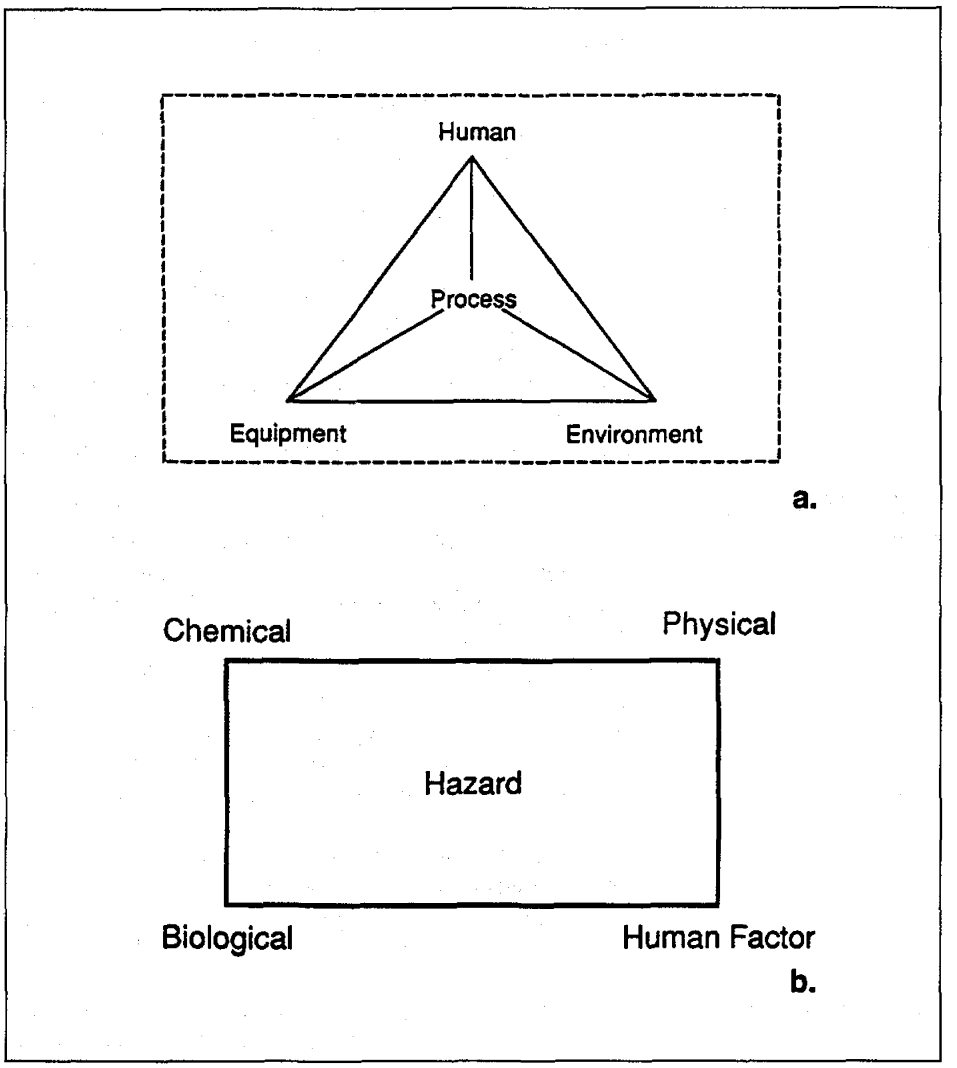


Figure I-1. System interactions for use in hazard evaluation procedures.

Hazard probability and severity

When hazards are identified within the system, the next step is to determine whether the risks associated with the hazards are acceptable, and if not (such as loss of human life), at what cost could the risks be eliminated or reduced. In determining the risks associated with the hazards, the severity of the hazard and its probability of occurrence should be taken into account. For example, the release of a highly toxic chemical from a storage facility has such an adverse effect on the surrounding community that it would be considered unacceptable even though the probability of such a release might be very low.[2]

Once the system components and their failure modes have been identified, the acceptability of risks taken as a result of such failures must be determined. The risk assessment process yields more comprehensive and better results when reliable statistical and probability data are available. In the absence of such data, the results are a strong function of the engineering judgment of the design team. The important issue is that both the severity and probability (frequency) of the accident must be taken into account.

Risk assessment

Table I-1 summarizes one method of probability and severity assessment that can be applied to a system component failure. Both probability and severity have been ranked on a scale of 0 to 1 with table entries being the sum of probability and severity. The acceptability of risk is a major decision and can be described by dividing the situations presented by Table I-1 into unacceptable, marginally acceptable, and acceptable regions. Figure I-1 graphically represents the risk data.[2,7]

Table I-1
Risk Data Summary

	Severity†									
Probability*	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	1.1
0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	1.1	1.2
0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	1.1	1.2	1.3
0.4	0.5	0.6	0.7	0.8	0.9	1.0	1.1	1.2	1.3	1.4
0.5	0.6	0.7	0.8	0.9	1.0	1.1	1.2	1.3	1.4	1.5
0.6	0.7	0.8	0.9	1.0	1.1	1.2	1.3	1.4	1.5	1.6
0.7	0.8	0.9	1.0	1.1	1.2	1.3	1.4	1.5	1.6	1.7
0.8	0.9	1.0	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8
0.9	1.0	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9
1.0	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	2.0

* Corresponds to ordinate in Figure I-2.
† Corresponds to abscissa in Figure I-2.

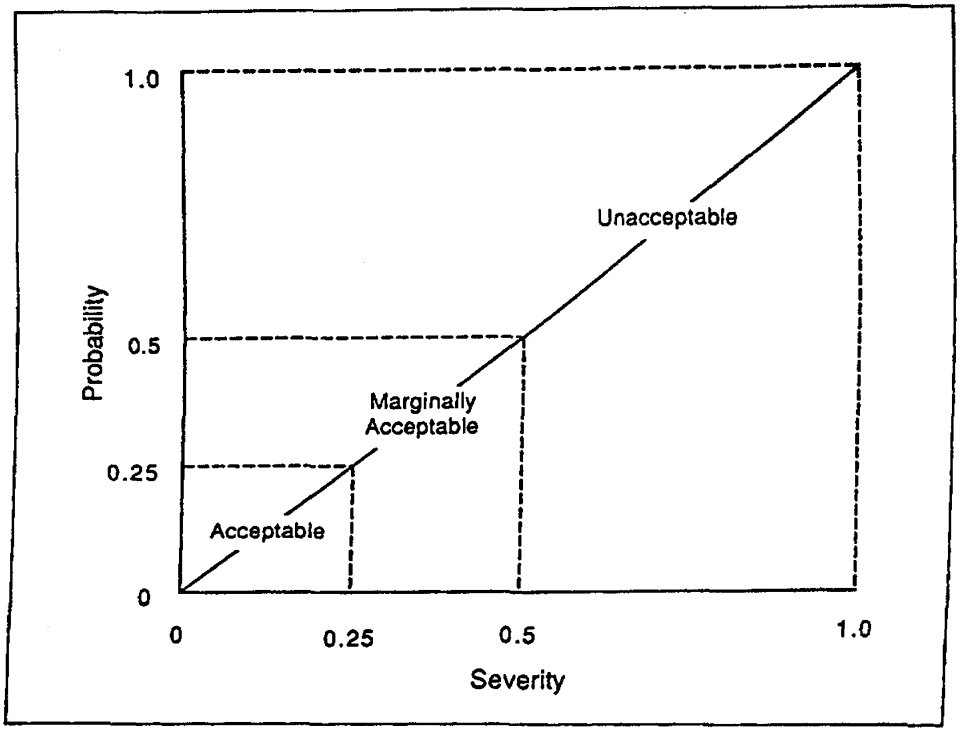


Figure I-2. Graphic representation of risk data.

REFERENCES

1. U.S. Department of Labor, System Safety Engineering, Safety Manual No. 15, Mine Safety and Health Administration, U.S. Department of Labor, Washington, DC (1986).
2. Slote, L.: Handbook of Occupational Safety and Health, John Wiley & Sons, New York, NY (1987).
3, Kavianian, H.R., J.K. Rao, and G.V. Brown: Toxic Gas Hazard Management in Microelectronics and Optoelectronics Industries, Proc. HAZMACON 88, April 5-7, 1988, Anaheim, CA (1988).
4. Kavianian, H.R., and J.K. Rao: Should Engineering Schools Address Environmental and Occupational Health Issues? Discussion Paper, J. Professional Issues in Engineering, 115(1):91-93, (Nov. 12, 1987).
5. Cowan, P.A., and J.K. Rao: Disaster Abatement and Control in the Chemical Process Industry Through Comprehensive Safety Systems Engineering and Emergency Management, Lessons from Flixborough and Bhopal, Proc. World Conf. on Chemical Accidents, Institute Supervisor di Sainta, Rome (July 7-10, 1987).
6. McElroy, F.E., ed.: Accident Prevention Manual for Industrial Operations, 8th ed., National Safety Council, Chicago, IL (1981).
7. Henley, E.J., and H. Kumamoto: Reliability Engineering and Risk Assessment, 1st ed., Prentice Hall, New York, NY (1981).

Unit II

SYSTEM SAFETY TECHNIQUES

PURPOSE:

To familiarize students with system safety techniques

OBJECTIVE:

To acquaint the student with:

1. System safety techniques
2. Checklist of hazards in the design process
3. System definition
4. System interactions

SPECIAL TERMS:

1. Relative ranking
2. Preliminary hazard analysis (PHA)
3. What if analysis
4. Failure mode effect criticality analysis (FMECA)
5. Hazard and operability study (HAZOP)
6. Fault tree analysis (FTA)
7. Event tree analysis (ETA)
8. Cause-consequence analysis

INSTRUCTOR MATERIALS:

1. Lesson plan
2. Chalkboard

TRAINEE MATERIALS:

Supplementary materials supplied by instructor

INTRODUCING HAZARD EVALUATION TECHNIQUES

Role of design team

Several hazard evaluation techniques have been developed; when applied properly to a given system, hidden system failure modes can be identified and techniques for their rectification can be recommended. Many occupational and environmental safety problems are recognized as the result of an emergency, and in many of these situations, once the emergency is over, the problem is considered resolved. Although solving safety problems once they have occurred is the domain of the design engineer, the true role of the design team must be to prevent accidents from occurring in the first place. The hazard evaluation techniques, when integrated with engineering design, provide the design engineer with the necessary tools to identify and modify those components of the system that have the potential to cause an accident. [1,2]

System definition

To properly apply the system safety techniques to the design and operation of potentially hazardous technologies, the design engineer must have a clear understanding of the system and be able to prepare a written response to questions such as:

1. What is the intended function of the system?
2. What are the raw materials, intermediates, and final products and byproducts?
3. What steps are taken to convert the raw materials to final products? (e.g., chemical reactions, physical operations, etc.)
4. How does the system interact with the environment? (e.g., hazardous waste streams, toxic releases, etc.)
5. How does the system interact with personnel? (e.g., the need for personal protective equipment.)
6. What sources of energy does the system use and how is this energy supplied to the system?
7. What are the maintenance requirements of the system?
8. How does the system interact with other systems within the plant?

The above list is illustrative only and must be tailored to the particular system design at hand.

Hazard type

Proper application of the hazard evaluation technique also requires a sound knowledge of the types of hazards involved within the system. The design engineer must develop a checklist summarizing the types of hazards that warrant further evaluation within the system. This checklist should take the following hazards into account:

- Toxic chemical
- Fire
- Explosion
- Runaway chemical reaction
- Temperature extreme
- Radiation
- Equipment/instrumentation malfunction that can be a factor in the appearance of a hazard
- System moving part
- Electrical
- Hazardous noise and vibration
- Mechanical
- Biological
- Environmental pollution
- Pressure

Hazard minimization

After the system has been defined, the hazard evaluation techniques can be used to identify different types of hazards within the system components and to propose possible solutions to eliminate the hazards. These procedures are extremely useful in identifying system modes and failures that can contribute to the occurrence of accidents; they should be an integral part of different phases of process development from conceptual design to installation, operation, and maintenance.[3,4] The hazard evaluation techniques that are

useful in the preliminary and detailed stages of the design process include relative ranking techniques (DOW and MOND Hazard Indices), the preliminary hazard analysis (PHA), the "What If" analysis, hazard and operability (HAZOP) study, failure modes effects criticality analysis (FMECA), fault tree analysis (FTA), event tree analysis (ETA), and cause-consequence analysis (C-CA).[5]

RELATIVE RANKING TECHNIQUES–DOW AND MOND HAZARD INDICES

The DOW and MOND methods provide a quick and simple way of estimating risks in process plants. The procedure employed assigns penalties for those processes or operations that can contribute to an accident and assigns credits to the safety features of the plant that can mitigate the effects of an accident. The penalties and credits are combined into an index that indicates the relative ranking of the plant risk.[1,6]

Although both DOW and MOND methods can be used to evaluate risks associated with different processing units, the MOND method considers material toxicity in addition to reactivity and flammability. The relative ranking techniques consist of seven general steps.

1. Processing units that pose the highest risk must be identified.

Material factor

2. A material factor (MF) is assigned to each processing unit. MFs take into account the degree of flammability, toxicity, and/or reactivity of materials used in each unit. Each MF is denoted by a number between 1 and 40.

General and special process hazards

3. When the contributing factors of toxic effects, fire, and explosion are considered, the hazard factors (HFs) must be evaluated. The HFs fall into two broad categories: "general process hazards" and "special process hazards." General process hazards are classified as those whose major adverse contributing effect is an increase in the intensity of an accident. Special process hazards are categorized as those that can increase the probability of occurrence of an accident. Examples of the first category are inadequate storage facilities or improper plant layout; examples of the second category include high or low pressure vessels and equipment operating under extremes of temperature. A description of the actual assignment of HFs is beyond the scope of this study, and the reader is referred to AIChE "Guidelines for Hazard Evaluation Procedures"[1] and the DOW guide.[7]

Unit hazard factors and damage factors

4. Based on the information obtained in steps 1 through 3, the unit hazard factor (UHF) as well as damage factor (DF) can be calculated for each processing unit.[1]

Fire and explosion index

5. The fire and explosion index (FEI) as well as the area of exposure (AE) for each unit can be calculated at this point. The FEI, which is a measure of the damage which may result, can be calculated by multiplying the UHF and the MF. The AE is defined as a circular area around the processing unit.

Maximum probable property damage

6. The base and actual maximum probable property damage (MPPD) can be calculated at this juncture. The base MPPD is defined as the cost of replacing the equipment within the AE. The actual MPPD, on the other hand, can be obtained by applying loss control credit factors (LCCFs) to the base MPPD. The LCCFs account for the effectiveness of safety design features of the plant.[1]

Maximum probable days outage

7. Finally, maximum probable days outage (MPDO) and business interruption (BI) costs can be calculated by considering the cost of repairing or replacing equipment and the cost of loss in production.

PRELIMINARY HAZARD ANALYSIS (PHA)

A PHA is a general, qualitative study that yields a rough assessment of the potential hazards and means of their rectification within a system. It is called "preliminary" because it is usually refined through additional studies. PHA, which is part of the U.S. Military Standard System Safety Program, contains a brief description of potential hazards in system development, operation, or disposal. This method focuses special attention on sources of energy for the system and on hazardous materials that might adversely affect the system or environment.

Resources necessary to conduct a PHA include plant design criteria, equipment, and material specifications.

Hazard table and logic diagram

The results of a PHA study can be summarized in the form of a table (such as could be developed from Table II-1) or a logic diagram (such as could be illustrated by completing Figure II-1). In either format, potential hazards that pose a high risk along with their cause and major effects are identified. In addition, for each hazard identified, preliminary means of control are also prescribed in the analysis. Thus, a PHA is not performed only to develop a list of possible hazards; it also is used to identify those hazardous features of a system that can result in unacceptable risks and to assist in developing preventive measures in the form of engineering or administrative controls or use of personal protective equipment.[1,2,8,9]

Table II-1
Summary Table to be Completed for Preliminary Hazard Analysis (PHA)

Hazard	Cause	Major Effects	Corrective/Preventive Measures
.....	....	.....	.....
.....	....	....	.....
.....	....	.....	.....
.....	....	.....	.....
.....	....	.....	.....

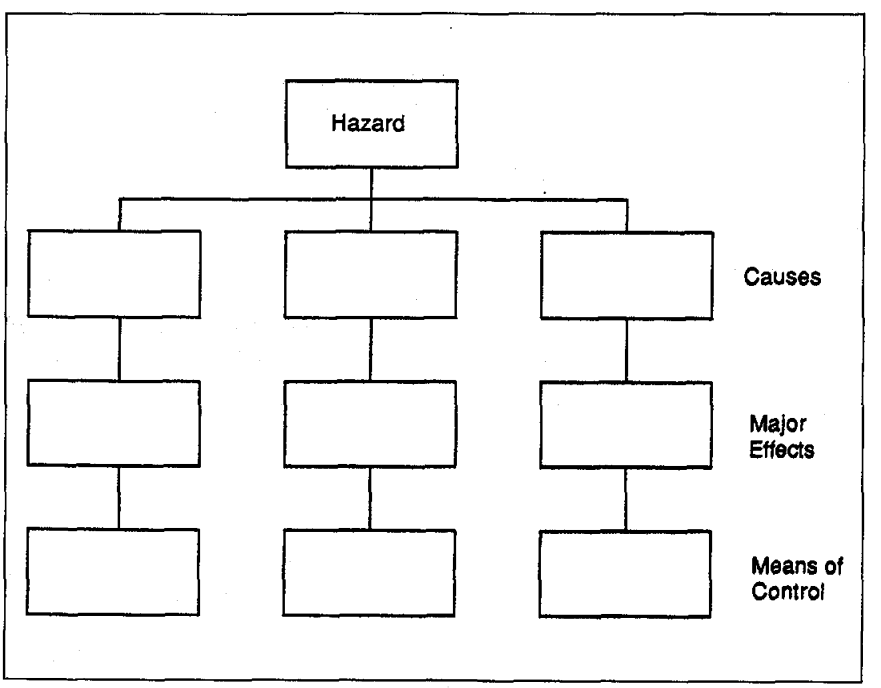


Figure II-1. Logic diagram to complete for preliminary hazard analysis (PHA).

"WHAT IF" ANALYSIS

The main purpose of the "What If" method is to identify the hazards associated with a process by asking questions that start with "What if. . . ." This method can be extremely useful if the design team conducting the examination is experienced and knowledgeable about the operation; if not, the results are incomplete. The examination usually starts at the point of input and follows according to the flow of the process.[1,10]

Study boundaries

The first step of "What If" analysis is to define the study boundaries. There are two types of study boundaries to be considered: the consequence category boundary, which includes public risk, employee risk, and economic risk, and the physical boundary, which addresses the section of the plant that should be considered for analysis.

Process information

The second step is to obtain all the information about the process that will be needed for a thorough evaluation including but not limited to: the process materials used and their physical properties, the chemistry and thermodynamics of the process, a plant layout, and a description of all the equipment used including controls and instrumentation. The last part of the information gathering step is the preliminary formation of the "What If" questions.

Review team

The third step is to select a review team. The team is usually composed of two or three members that have combined experience in the process to be studied, knowledge in the consequence category, and experience in general hazard evaluation. If the team is inexperienced, results may be incomplete or incorrect.

Hazard consequences

Once the team has been established, the review is conducted. Typically, the review begins with the process inputs and follows through to the outputs. Each of the "What If" questions is addressed by identifying the hazard and it's consequence and then recommending solutions or alternatives to alleviate the risk.[1]

Reporting

The final step in the "What If" analysis is reporting the results in a systematic and easily understood format. An example of a common format can be seen in Table II-2, which includes the questions, their consequences, and recommendations. The ethylene polymerization process (which will be explained later), is used to demonstrate the format for a "What If" analysis.

Table II-2

"What If" Analysis on the Ethylene Polymerization Reactor

What if...	Consequence/Hazard	Recommendation
1. Cooling water pump breaks down	Runaway reaction/explosion/fire	Stand-by pump/alarm system
2. Too much oxygen fed into reactor	Runaway reaction/explosion/fire/ debris flying	Alarm system/feed flow control/ initiator flow control
3. Wrong initiator	None likely	----------
4. Valve after reactor gets clogged	Pressure buildup/explosion/fire/ debris flying	Feed flow control/initiator flow control/alarm system
5. Compressor breaks down	None likely	----------
6. Trauma to cooling jacket	Runaway reaction/explosion/fire/ debris flying	Temperature alarm/feed flow control

FAILURE MODES EFFECTS AND CRITICALITY ANALYSIS (FMECA)

FMECA, also known as failure modes and effect analysis (FMEA), is a systematic method by which equipment and system failures and the resulting effects of these failures are determined.[11] FMECA is an inductive analysis; that is, possible events are studied, but not the reasons for their occurrences. FMECA has some disadvantages: human error is not considered and the study concentrates on system components, not the system linkages that often account for system failures.[12] FMECA provides an easily updated systematic reference listing of failure modes and effects that can be used in generating recommen-

dations for equipment design improvement. Generally, this analysis is first performed on a qualitative basis; quantitative data can later be applied to establish a criticality ranking that is often expressed as probabilities of system failures.

Five steps are required for a thorough analysis: the level of resolution of the study must be determined; a format must be developed; problem and boundary conditions are then defined; the FMECA table is completed; and, finally, the study results are reported.[1,4]

Level of resolution

The first step in FMECA is to determine a level of resolution. If a system-level hazard is to be addressed, equipment in the system must be studied; for a plant-level hazard, individual systems within the plant must be examined.

Format

Once the level of resolution has been determined, a format must be developed—one to be used consistently throughout the study. A minimal format should include each item, its description, failure modes, effects, and criticality ranking.

Defining the problem and boundary/criticality ranking

Defining problem and boundary conditions includes identifying the plant or systems that are to be analyzed and establishing physical system boundaries. In addition, reference information on the equipment and its function within the system must be obtained. This can be found in piping and instrumentation design drawings as well as in literature on individual components or equipment. The final step in the problem definition step is to provide a consistent criticality ranking definition. In a quantitative study, probabilities are often the method used for ranking. If the study is being conducted on a qualitative basis, relative scales (Table II–3) are usually used as ranking methods. Table II–3 summarizes the hazard classes used in the aerospace industry that may be used as a relative scale.[11] If this type of scale is used, however, "negligible, marginal, critical, and catastrophic" should be defined more clearly. Another more specific criticality ranking scale (summarized in Table II–4) is suggested by the American Institute of Chemical Engineers.

Table II–3

Suggested Criticality Rankings Based on Aerospace Hazard Classification[2]

Criticality Ranking	Effects on System and Surroundings
I	Negligible effects
II	Marginal effects
III	Critical effects
IV	Catastrophic effects

Table II–4

Suggested Scale for Criticality Ranking for a Qualitative Failure Modes Effects and Criticality Analysis (FMECA)[1]

Criticality Ranking	Effects on System and Surroundings
1	None
2	Minor system upset Minor hazard to facilities Minor hazard to personnel Orderly process shutdown necessary
3	Major system upset Major hazard to facilities Major hazard to personnel Orderly process shutdown necessary
4	Immediate hazard to facilities Immediate hazard to personnel Emergency shutdown necessary

Table preparation/ failure modes

The FMECA table should be concise, complete, and well organized. This table should identify equipment and relate it to a system drawing or location. This is to prevent confusion when similar equipment is used in different locations. One of the limitations of FMECA is that the table must include *ALL* failure modes for each piece of equipment and effects of each failure along with the associated criticality ranking. Table II-5 shows a sample chart that can be completed for the FMECA table.

Report

The final step in conducting a FMECA is to report the results. If the prepared table (Table II-5) is complete, that may be sufficient. Often, however, a report of suggested design changes or alterations should also be included.

Table II-5

Sample Chart that Can Be Completed for a Failure Modes Effects and Criticality Analysis (FMECA)

		Effects on			
Equipment	Failure Mode	Other Systems	System	Relative Ranking	Remarks

HAZARD AND OPERABILITY STUDY (HAZOP)

Deviations of plant operation

The purpose of a HAZOP study is to identify (a) problems associated with potential hazards and (b) deviations of plant operation from design specifications. This is carried out by a multidisciplinary team following a structure that includes a series of guide words. The results of this study depend on the quality of information on the process or plant and the experience of the team members.

Purpose

A thorough HAZOP study can be done in five steps. The first step is to define the scope and purpose of the study. The scope includes the specific areas of the process to be studied as well as what type of hazard consequences will be considered. The purpose, as stated above, is to identify potential hazards and operation deviations; the object of the study is included within the "purpose."

Select a team

The second step in a classic HAZOP study is to select a team to carry out the study. Ideally, this team has five to seven members from different areas within the operation.[1,8] A team leader is chosen; this person should have a good general knowledge of the process being studied as well as experience in conducting HAZOP studies. It should be noted that more than just design engineers are needed on the team; e.g., plant workers and foremen can provide valuable information on how procedures in the plant are really carried out.

Information gathering

Once the team has been formed, information gathering begins. The quality of the study depends on the source of information. Suggested materials include piping and instrumentation diagrams, flow diagrams, layouts, and any equipment information that may be available. As the data are being collected, the team leader should determine the sequence of study, or study nodes. Each study node is a specific portion of the design that will be studied individually. The leader should also compose a list of guide words such as the ones summarized in Table II-6.

Process review

The team will then review the process, examining each study node individually and applying all guide words to each of its components. The flow diagram in Figure II-2 suggests a typical sequence to follow when carrying out this study. Each member of the team should contribute equally to the hazard analysis and tabulated final report.

Final report

The final report for a HAZOP study should have all information in table format. Each table should include the guidewords used, the deviation from expected operation, the causes of that deviation, any consequences, and suggested actions to alleviate or eliminate the problem. For example, a HAZOP study on a tank where sulfuric acid is fed and removed on a continuous basis can provide the preliminary design information summarized

Scope of study

in Table II-7. Because the main purpose of HAZOP studies is to find problems, not solve them, only obvious solutions need be suggested. Each parameter should be addressed in an individual table. These tables may be accompanied by a report that includes the scope of the study and any suggestions or general recommendations. It should be emphasized that HAZOP can be used to evaluate both the hazards posed by the plant design as well as hazards posed by the operating procedures.

Table II-6

Guide Words for a Hazard and Operability (HAZOP) Study[1]

General parameters	no; more; part of; less; as well as; other than; reverse
Time parameters	sooner; later; other than
Position, source parameters	where else; other than
Temperature, pressure parameters	higher; lower; more; less

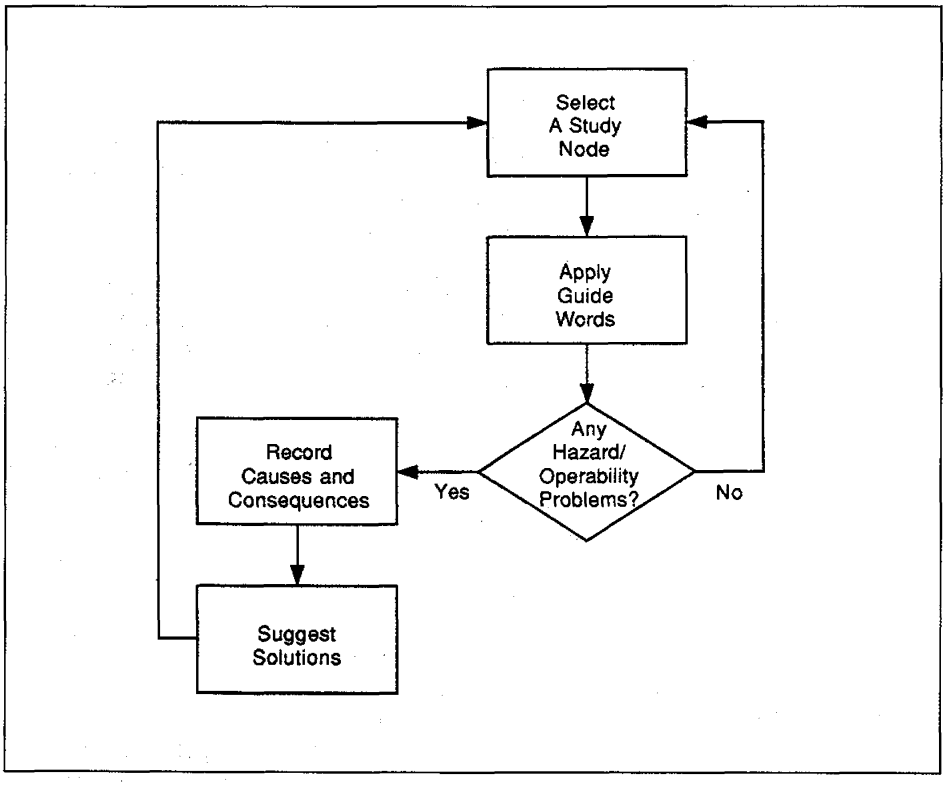


Figure II-2. Flow diagram for a hazard and operability (HAZOP) study.

FAULT TREE ANALYSIS (FTA)

TOP event

FTA was developed in 1961 by H.A. Watson of Bell Telephone Laboratories.[2] This method of hazard evaluation visually demonstrates the interrelationship between equipment failure, human error, and environmental factors that can result in an accident.[5] FTA is a "backward" analysis: a system hazard, or TOP event (e.g., the hazardous event placed at the top of the fault tree), is the starting point, and the study traces backwards to find the possible causes of the hazard. Analysis is restricted to identifying system elements and events that lead to the specified failure or accident. FTA employs Boolean logic; this requires that any statement, condition, act, or process be described as only one of the two possible states, such as on/off, fully open/not fully open, etc. FTA can be computerized, and, by using the probabilistic risk assessment technique, probabilities of events occurring can be calculated using minimum cut sets.

A cut set is any group of contributing elements which, if all occur, will cause the TOP event to occur. A minimum cut set is a least group of contributing elements which, if all occur, will cause the TOP event to occur.

Table II-7

Sample Hazard and Operability (HAZOP) Worksheet for Design of a Sulfuric Acid Intermediate Tank

Guide Word	Deviation	Consequences	Causes	Recommended Action
No	No flow	Overflow of acid, contamination of area, potential personnel exposure to a corrosive material.	Outlet valve malfunctions	• Provide automatic flow through control on inlet valve with flow sensors on outlet line • Install level control in the tank with signal to flow control on the inlet valve • Provide bypass line on the outlet line with response from level control inside the tank

TOP event and system analysis

Three steps are needed to conduct a FTA thoroughly and accurately. First, the undesired event, or TOP event, is defined. It should be noted that one of the limitations of Fault Tree is the required knowledge about the TOP events. The second step is to develop a thorough understanding of the system to be analyzed by studying design drawings, equipment specifications, literature, and operation procedures, as well as other source information that may be available. The third step is to construct the fault tree. The symbols used in FTA are displayed in Figure II-3. The fault tree will begin with the TOP event and will address any possible equipment failure, human error, or environmental factors that could result in the TOP event. "AND" gates are used when the existence of all conditions or events indicated must occur for the TOP event to occur. "OR" gates indicate that any one of the conditions or events indicated leads to the TOP event. Undeveloped events are occurrences that are not further addressed, either because of lack of necessary information or for other reasons such as the particular event goes beyond the scope of the study. Basic faults are the primary cause of the TOP event. Basic faults represent a malfunction of equipment that occurs in the environment in which the equipment was intended to operate. Each branch of the fault tree should eventually end up in either a basic fault or perhaps an undeveloped event. The triangles are used for transfer of the fault tree to another location or another page. Figure II-4 is an example of FTA applied to a flammable storage area fire.

Gates

EVENT TREE ANALYSIS (ETA)

Safety functions

ETA is a forward analysis beginning with an initiating event and proceeding forward to find possible consequences resulting from that event.[2,13] The course of events is determined by the success or failure of various safety functions as the accident progresses.

Initiating event

A complete ETA can be done in four steps: the initiating event is identified; relevant safety functions are determined; the event tree is constructed; and the resulting accident event sequences are described.[1,14,15]

The initiating event should be a system or equipment failure, a human error, or a process upset. The process upset can be caused by numerous factors, including environmental factors.

Safety functions

The second step is to identify all the safety functions designed to deal with the initiating event. These safety functions should include any automatically responding safety systems, such as automatic shutdown. Alarms and warning systems, operator actions, and containment methods or barriers must also be considered.

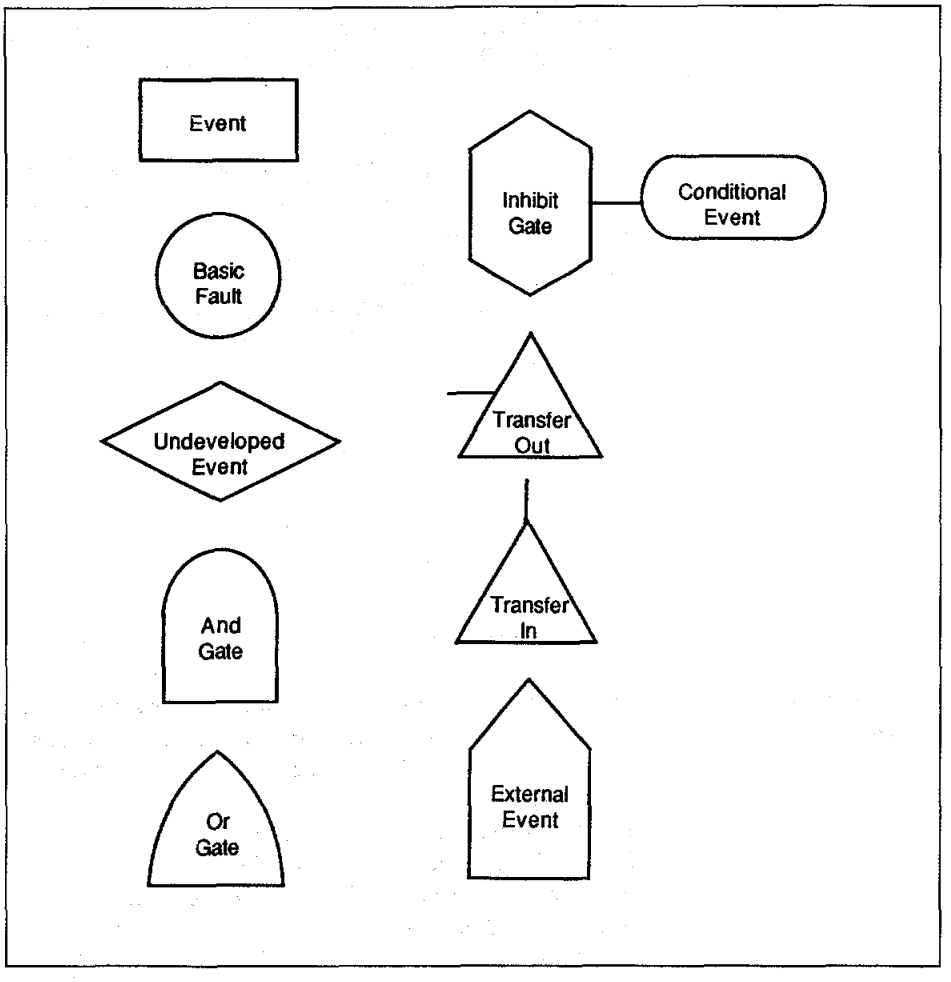


Figure II-3. Fault tree analysis (FTA) symbols.

Event tree construction

The construction of the event tree begins by placing the initiating event on the left side of the diagram, and placing each of the safety functions being considered at the top of the page. Since the event tree will display a chronological development of accidents, the placement of safety functions should be accurate in this respect. The event tree will show branches at a safety function if, and only if, the success or failure of that function affects the course of the accident. If this is not the case, there will be no branching at that safety function. Upward branching indicates success of the safety function, and downward branching indicates failure. Figure II-5 shows a representative event tree structure with the letters representing safety functions. The series of letters at the end of each branch indicate all the safety functions that have failed in that particular path. The end of each branch should contain notation as to the condition of the system, such as safe, unsafe, unstable, etc.

Contribution to accidents

The final step in this analysis is to describe each of the sequences contributing to an accident. An accurate description of the expected outcome for each branch must be supplied in the final report. Although the results of this study are qualitative, they can be quantified with the use of minimal cut sets and probabilistic data. It should be pointed out that the major limitation of the ETA is that it cannot handle multiple initiating events well. This is one of the strong points of FTA.

CAUSE-CONSEQUENCE ANALYSIS (C-CA)

C-CA, developed at RISO Laboratories in Denmark,[2] combines the forward thinking features of ETA with the reverse thinking features of FTA. The result of this analysis is a cause-consequence diagram that displays the relationships between accident sequences and their basic causes.

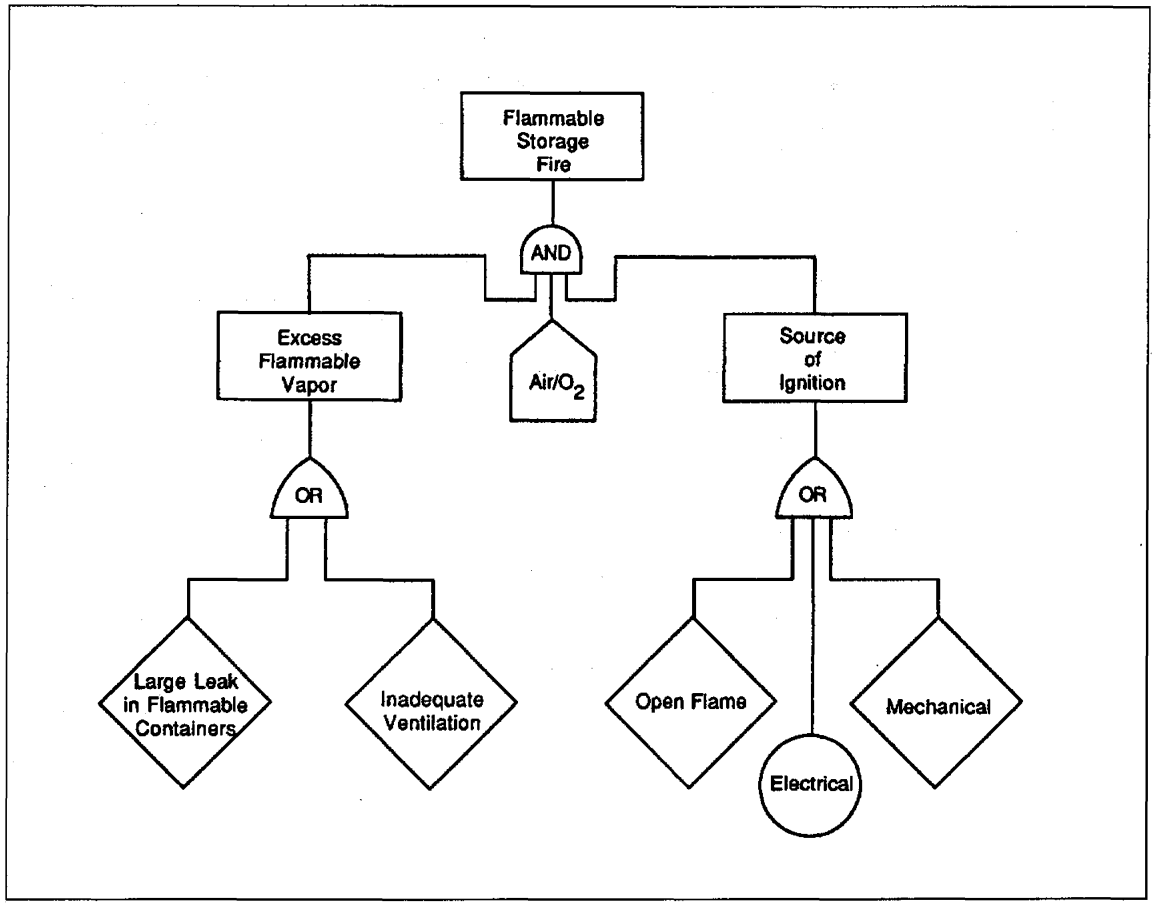


Figure II-4 Fault tree analysis (FTA) for a flammable storage area fire.

Simultaneous fault tree and event tree

Four basic steps are involved in the completion of C-CA. The first step is to select an event for analysis. The event should be either a TOP event, as in FTA, or an initiating event, as in ETA. If a TOP event is chosen, the second step is to develop a fault tree for that event; if an initiating event is chosen, an event tree diagram should be developed. The third step is to either complete a fault tree for each resulting accident on the event tree formed in step 2; or complete an event tree for each of the safety functions found in the fault tree developed in step 2. Essentially what is being done is a simultaneous FTA and ETA, which combines top-down and bottom-up studies. Once steps 2 and 3 are completed, the information obtained must be assembled into one coherent flow diagram. The symbols used for the event tree portion of the study can be found in Figure II-6. Although the results of this study are qualitative, they are quite accurate, and minimum cut sets can be used to quantify the results.

Minimum cut sets

SYSTEM CHECKLISTS

Compliance problems

A system checklist is useful to identify compliance problems and also those areas of the system that require further hazard evaluation. The method is easy to use and can be applied to any component of a given system such as equipment, instrumentation, materials, and procedures. This method, which produces qualitative results, must be prepared by an engineer thoroughly experienced with the system; once the checklist is prepared, however, it can be used by engineers or managers who may have less technical experience with the system.[1]

Project life cycle

The method of checklists can be applied to any phase of a project's life cycle from preliminary design to shipment of products and disposal of wastes. Since the safety requirements of a system are a strong function of the nature of the process, preparing a standard "checklist" format applicable to all systems may be difficult; therefore, the

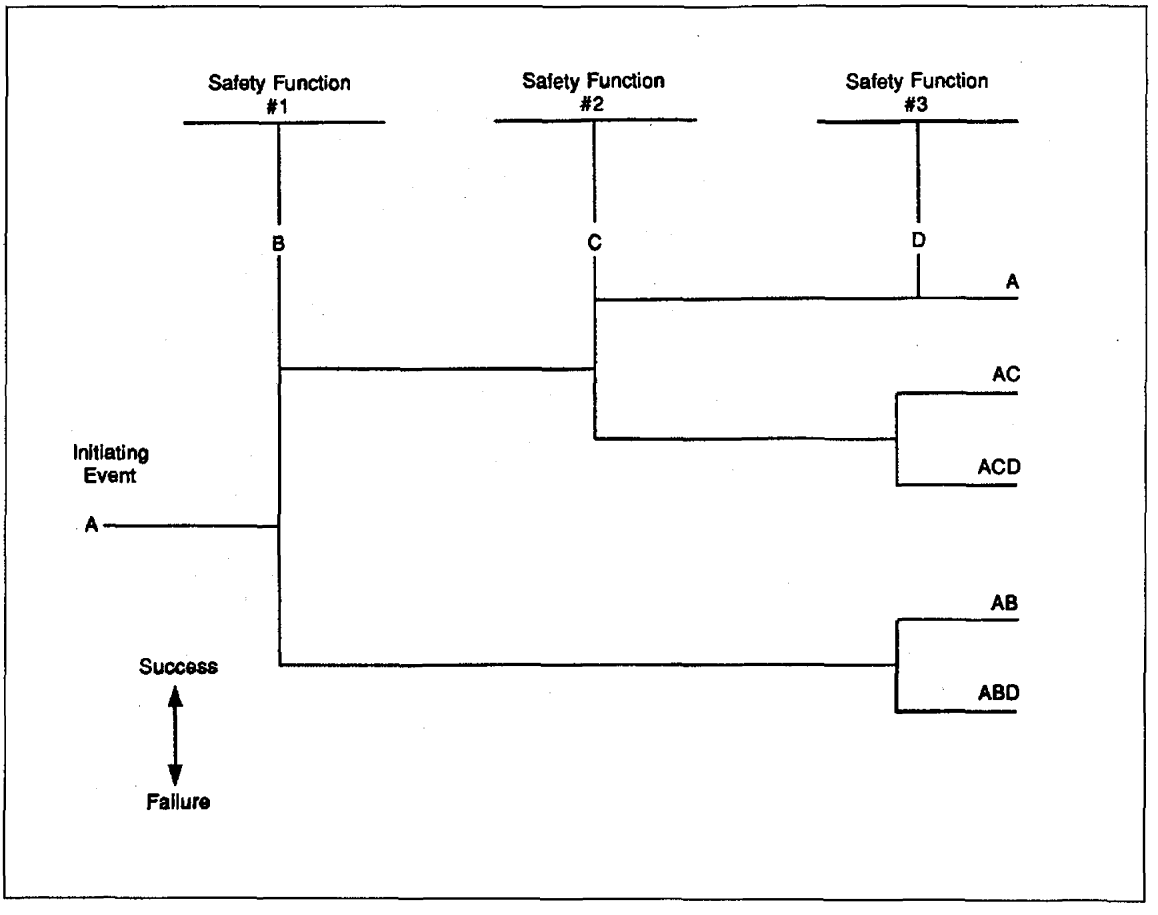


Figure II-5. Typical event tree analysis (ETA) structure.

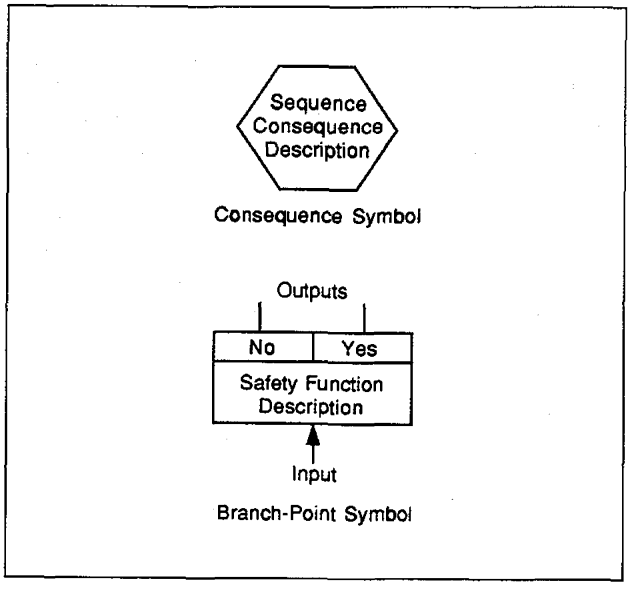


Figure II-6. Symbols used in cause-consequence analysis (C-CA).

checklist must be tailored to the specific problem at hand. For example, in a preliminary plant design, the design engineer might prepare a checklist to cover the following areas:

- Raw materials
- Products
- Intermediate products
- Equipment
- Instrumentation
- Plant layout
- Start-up
- Shut down
- Emergency shutdown
- Personal protective equipment (PPE)
- Contingency planning (both personnel and community)
- Waste disposal

Each specific area mentioned above can be further expanded to provide more details for hazard evaluation. For example, the design engineer might prepare the following checklist to gain more insight into the hazards posed by the raw materials:

- Flammability:
  - What is the flash point?
  - What are the upper and lower flammability limits?
  - What is the autoignition temperature?
  - What is the fire point temperature?
  - What are the products of combustion?
  - What is the evaporation rate?
  - What is the proper fire extinguishing agent?
  - What is the vapor pressure?
  - Does the material undergo hazardous polymerization?
  - Is the material pyrophoric? (i.e., can it catch fire upon contact with air?)
- Toxicity:
  - What are the exposure limits for the material? e.g., threshold limit values (TLV), permissible exposure limit (PEL), recommended exposure limit (REL)
  - Is the material classified as "highly toxic" or "toxic" based upon the results of tests on laboratory animals? e.g., LD_{50} or LC_{50} data. NOTE: LD_{50} and LC_{50} are referred to as the dose of a chemical that is lethal to 50 percent of laboratory test animals.
- Storage:
  - What materials are incompatible with the raw material?
  - What monitoring devices are needed for the storage area? e.g., combustible gas meter, organic vapor analyzer, etc.
  - How should a spill of this material be cleaned up?
  - Based on the flammability data, does the storage area require ignition proof equipment?
  - Can the material undergo hazardous polymerization or decomposition under storage conditions?
  - Do containers of this meterial need grounding and/or bonding to protect against electrostatic hazards?
- Reactivity:
  - Is the material stable under storage conditions?
  - Is the material water reactive? (A water reactive material can violently react with water to produce a toxic or flammable gas).

A similar checklist can be prepared for the other areas of interest mentioned above. The results of a checklist study are qualitative. These results, however, can be used to identify design areas that require further hazard evaluation and to communicate the safety needs of the plant to the management.

REFERENCES

1. Battelle Columbus Division, Guidelines for Hazard Evaluation Procedures, The Center for Chemical Process Safety, AIChE, New York, NY (1985).
2. Henley, E.J., and H. Kamamoto: Reliability Engineering and Risk Assessment, 1st ed., Prentice Hall, Englewood Cliffs, NJ (1981).
3. Hanes, N.B., and A.M. Rossignol: Comprehensive Occupational Safety and Health Engineering Academic Program Development Strategy, U.S. Department of Health and Human Services. Springfield, VA: Nat. Tech. Info. PB 86-226453 (1984).
4. Roland, H.E., and B. Moriarty: System Safety Engineering and Management, 1st ed., John Wiley & Sons, New York, NY (1983).
5. Kavianian, H.R., C.A. Wentz, R.W. Peters, and L.E. Martino: Total Concepts in Safety Systems Management for Hazardous Materials Handling and Design of Hazardous Processes, Annual Loss Prevention Symp., AIChE Spring 1989 National Meeting, Houston. AIChE, New York, NY (1989).
6. Shreve, R.N., and J.A. Brink: Chemical Process Industries, 4th ed., McGraw Hill, New York, NY (1977).
7. Dow Chemical Company, Fire and Explosion Index, Hazard Classification Guide, 5th ed., Midland, MI (1981).
8. Page, G.A.: Hazard Evaluation Procedures, American Society of Safety Engineers, Professional Development Conference and Exposition, Las Vegas, NV (1988). American Society of Safety Engineers, Des Plaines, IL.
9. Kavianian, H.R., R. Orr, R. Arbuckle, and A. Edwards: Hazard Analysis and Safety Management of a Radioactive Gas Handling Process,* School of Engineering, California State University, Long Beach, CA (1988).
10. Dollah-Kanan, M., Z.H. Mustaffa, and Z. Abidin: Safety System Management for Design of Hazardous Technologies,* School of Engineering, California State University, Long Beach, CA (1988).
11. U.S. Department of Labor, System Safety Engineering, Safety Manual No. 15, Mine Safety and Health Administration, U.S. Department of Labor, Washington, DC (1986).
12. Firenze, R.J.: The Process of Hazard Control, 1st ed., Kendall/Hurt Publishing Co., Dubuque, IA (1978).
13. Green, A.E.: Safety Systems Reliability, Wiley & Sons, New York, NY (1983).
14. Kavianian, H.R., G.V. Brown, and J.K. Rao: Safety Systems Management for Design of Hazardous Technologies, American Society of Safety Engineers, Des Plaines, IL (1988).
15. Kavianian, H.R., L.J. McIntyre, E. Shanahan, and L. Tami: Application of Hazard Evaluation Procedures to the Design of a Hazardous Industry,* School of Engineering, California State University, Long Beach, CA (1988).

*Available upon written request to the author.

Unit III

PRELIMINARY DESIGN OF METAL ORGANIC CHEMICAL VAPOR DEPOSITION (MOCVD)

PURPOSE:

To examine the application of system safety techniques to the MOCVD process

OBJECTIVE:

To acquaint the student with:

1. How system safety techniques can be applied to the design process
2. The effects of raw materials and product hazardous properties on process design

SPECIAL TERMS:

1. Metal organic chemical vapor deposition (MOCVD)
2. Toxicity; LD_{50}; LC_{50}
3. Permissible exposure limit (PEL)
4. Unsafe condition

INSTRUCTOR MATERIALS:

1. Student supplementary materials
2. Lesson plan
3. Chalkboard

TRAINEE MATERIALS:

1. Supplementary materials supplied by instructor from the list of references

DESCRIPTION OF THE MOCVD PROCESS

Metal organic vapor deposition (MOCVD) is a process whereby electronic photovoltaic thin films are produced. These films are used in semiconductors, photocathodes, and laser diodes, as well as in other applications where photovoltaic cells are needed. Thin film technology is based almost entirely on deposition from the gas phase; chemical deposition is favored for epitaxial growth on single crystal substrates. In epitaxial growth, the formed crystals follow the crystal pattern of the substrate, or base crystal; this allows for the formation of a product that is consistent and predictable in performance.

A basic understanding of the MOCVD process is necessary to be aware of the hazards involved in this process. The reactants involved are typically alkyls of group II metals and hydrides of group V elements. The alkyls are stored in stainless steel bubblers in the liquid phase; these bubblers are maintained in carefully controlled refrigerated baths to maintain a stable vapor pressure. The gaseous hydride sources are often contained at or near room temperature in dilute mixtures with hydrogen.

Dilute vapors of these alkyd and hydride reactants are transported at near room temperature to a common manifold. The alkyls and hydrides remain separated until introduced into the reactor containing a heated susceptor where pyrolysis and deposition occur. The carrier gas is normally purified hydrogen, and the storage and flow systems are typically assembled from stainless steel tubing. Figure III–1 shows a simplified schematic diagram of the gas handling system used in MOCVD.[1,2]

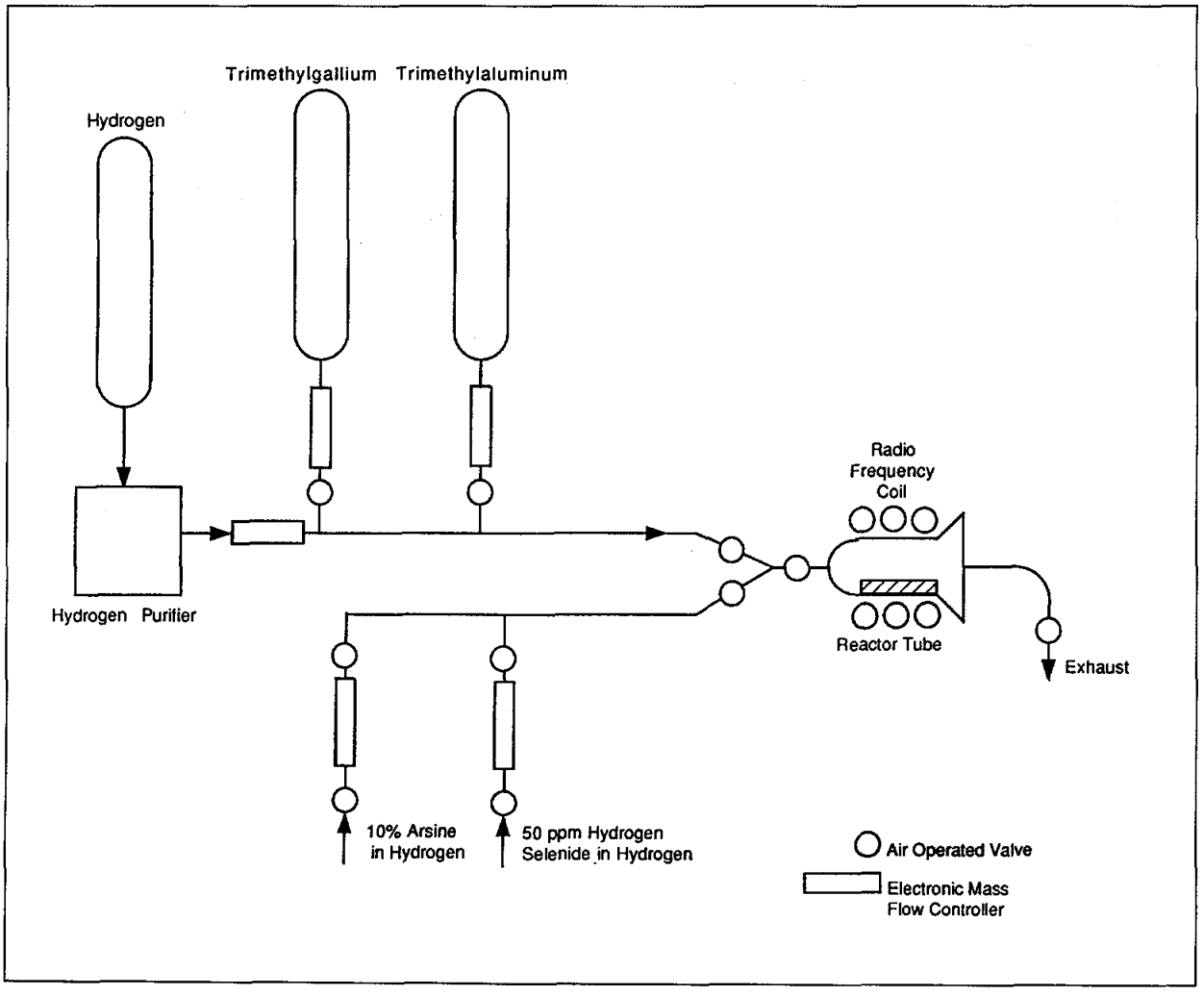


Figure III–1. Simplified schematic diagram of metal organic chemical vapor deposition (MOCVD).

HAZARDS OF GASES USED IN MOCVD AND THEIR EFFECTS ON WORKERS AND PUBLIC SAFETY

Physical properties

The physical properties and hazardous characteristics of the gases used in MOCVD are critical factors in design of this process. Fire and explosion hazards are based on flash points, i.e., the lowest temperature at which the air/vapor mixture formed above the surface of a liquid will ignite in the presence of a source of ignition. Liquids with flash points below 100°F are classified as "flammable liquids" because they pose a severe fire hazard at room temperature. Liquids with flash points between 100°F and 200°F are classified as "combustible liquids," and they are less of a fire hazard than are flammable liquids.[3] In Table III-1, fire hazards of source gases are classified into "dangerous" and "moderate." Dangerous refers to flash points below 100°F, and moderate refers to flash points between 100°F and 200°F.

Table III-1

Hazardous Properties of Source Gases[4]

Source Gases	Health Hazard	Fire and Explosion
Arsine	Extremely toxic	Moderate
Hydrogen selenide	Extremely toxic	Dangerous
*Trimethylaluminum	Highly toxic	Dangerous
*Triethylaluminum	Highly toxic	Dangerous
*Triethylgallium	Toxic	Dangerous
*Trimethylindium	Toxic	Dangerous
*Triethylantimony	Toxic	Dangerous
*Dimethylmercury	Toxic	Dangerous

*Pyrophoric gases.

Health hazards

As can be noted from Table III-1, the source gases used in the MOCVD process also pose severe health hazards. One measure of the degree of health hazard posed by a chemical is its toxicity. Although all chemicals may be toxic if the dose administered is high enough, toxic chemicals are divided into three groups: extremely toxic, highly toxic, and toxic. Most toxicity data are obtained by conducting experiments on laboratory animals. The lethal dose that brings fatality to half of the test animals when administered orally is called "Lethal Dose 50" or LD_{50}. An extremely toxic chemical, by definition, has an oral LD_{50} of less than 1 mg/kg (milligrams of chemical per kilogram of body weight). A highly toxic chemical, on the other hand, is defined as one that has an LD_{50} greater than 1 mg/kg but less than 50 mg/kg. A toxic chemical has an LD_{50} between 50 mg/kg and 500 mg/kg.[4]

Arsine

A typical hydride gas source used in MOCVD is arsine, which is extremely toxic and dangerously reactive under certain conditions. The primary hazard posed by arsine is exposure through inhalation. This gas is a carcinogen that can also affect red blood cells, the gastrointestinal system, and the central nervous system. The permissible exposure limit (PEL) set by OSHA for this gas is 0.05 part per million (ppm). In addition, arsine poses **severe fire/explosion hazards** in the presence of an ignition source or oxidizers such as chlorine and nitric acid. In addition, arsine is flammable when exposed to flame and **explosive** when exposed to chlorine, nitric acid, or open flame. When this gas is heated to decomposition, it emits highly toxic fumes. Personnel who might be exposed to arsine must wear protective gear and self-contained breathing apparatus. When arsine is used in a MOCVD process, the primary threat to the surrounding community is the accidental release of large quantities of gas.

Alkyls

Alkyls used in the MOCVD process are all pyrophoric; that is, they explode on contact with oxygen in air. Because of this high reactivity, they must be stored under an inert atmosphere. These compounds are also irritating to mucus membranes and the skin; personnel must wear the appropriate personal protective equipment (PPE) when working with these compounds. Although toxicity is not a primary concern for the surrounding

community since the gases are generally stored as dilute mixtures with hydrogen, disaster hazard is high because of their highly flammable and explosive nature. Employee awareness and safety procedures are essential to the safe handling of alkyls.

Some other chemicals involved indirectly in MOCVD also pose physical and health hazards. Acetone, methanol, and chloroform are used in cleaning the substrates before deposition. Chloroform, for example, is a carcinogen. Methanol and acetone present severe fire hazards. Personnel exposed to these substances should wear the appropriate protective gear and work in well-ventilated areas.

APPLICATION OF PHA TO THE MOCVD PROCESS

Toxic and pyrophoric properties

The greatest risk to personnel and the surrounding community in the MOCVD process is the toxic and pyrophoric properties of the reactant gases. Table III-2 is the result of concentrating on these two characteristics in the first step of preliminary hazard analysis (PHA). To complete a thorough PHA on this process, similar studies would include hazards resulting from the operating environment, operations, facility, and safety equipment. The study of each area would result in a table similar to that completed for toxic gas release and fire/explosion hazards.[5]

APPLICATION OF FTA TO THE MOCVD PROCESS

Basically, fault tree analysis (FTA) employs a logic diagram to analyze an undesired event. All causes that can lead to the undesired event are cataloged and broken down further. This analysis is continued to determine all of the events and combinations of events that can lead to the undesired event.

Logic diagram

The first step in constructing a fault tree is selecting the undesired event. A fault tree can be constructed for virtually any event that can occur within a system. Since only one event is analyzed in a single fault tree, the undesired event is usually an accident or potential accident that is sufficiently important to warrant the study. The undesired event may be a catastrophe such as release of toxic gases into a community or it may be an accident with less serious results such as one that produces a minor injury.

Backward reasoning

Next, it is necessary to reason backward from the undesired event by asking "How could this happen?" In answering this question, the primary causes and how they interact to produce the undesired event are identified. The same question is then asked for each of the primary causes. In turn, they are broken down into events that lead to them, and so on. This logic process is continued until all potential causes have been identified.

Tree diagram

Throughout the process, a tree diagram is used to record the events as they are identified. The undesired event is shown at the top of the tree. The primary causes are shown immediately below the undesired event. The events that lead to the primary causes are shown at the next lower level, etc. The tree branches are terminated when all events that could eventually lead to the undesired event are shown.

Release of toxic gases

The TOP event for the illustrated MOCVD process is selected to be the release of toxic gases from the reactor tube during normal operation. Before the analysis can begin, the existing event, unallowed events, and system boundary (reactor), must be defined, and equipment configuration must be identified as shown in Figure III-2. The causes for the TOP event can be overheat damage to reactor tube, damage to reactor tube, or pressure build up within the reactor. Figure III-3 summarizes the sequence of events that could lead to the TOP event.

APPLICATION OF FMECA TO THE MOCVD PROCESS

The major objective of the failure modes effects and criticality analysis (FMECA) is to identify the location of failures within the system and the effect of such failures. In the usual procedure, each item used in the system is listed on a FMECA chart. Such items include equipment, materials, machine parts, and environmental elements necessary for system operations. The exact manner or mode in which each item can fail is then determined.

Location of failures

Table III-3 summarizes the results of applying FMECA to the MOCVD process. It should be noted that the criticality rankings used are somewhat subjective and depend to a large

Table III-2

Application of Preliminary Hazard Analysis (PHA) to the Design of Metal Organic Chemical Vapor Deposition (MOCVD)

Hazard	Cause	Major Effects	Corrective/Preventative Measures
Toxic gas release	Leak in storage cylinder	Potential for injury/fatalities from large release	• Provide warning system • Minimize on-site storage • Develop procedure for tank inspection and maintenance • Develop purge system to remove gas to another tank • Develop emergency response system
"	Reactor heater failure	Potential for injury/fatalities from large release	• Provide temperature control inside reactor with automatic shutdown of gas flow to the reactor • Design collection system to remove and purify/recycle or discard unreacted gases • Design control system to detect excess gases in exhaust and shut down gas flow
"	Pressure buildup due to high temperatures in storage cylinders due to refrigeration system failure	Potential for injury/fatalities from large release	• Provide control system to detect extreme temperature variations and activate backup cooling system • Backup cooling system
"	Rupture in storage tanks	Potential for injury/fatalities from large release	• Locate gas storage away from unnecessary plant traffic • Install warning system for personnel in the area such as signs, lights, etc. • Training employees in the area
"	Leakage in process lines	Potential for injury/fatalities from large release	• Provide accurate gas monitoring system on-site • Provide emergency response system • Design control system to detect leakage and divert flow to a secondary system
"	Damage to reactor tube due to high temperature	Potential for injury/fatalities from large release	• Provide a warning system for temperature fluctuation • Divert flow to temporary storage tank
"	Compressor failure	Potential for injury/fatalities from large release	• Provide spare compressor with automatic switch-off control • Develop emergency response system
"	Reactor outlet becomes plugged	Potential for injury/fatalities from large release	• Provide relief valve on reactor with outlet to a temporary storage tank
Explosion, fire	Spark	Potential for fatalities due to toxic release and fire Potential for injuries/fatalities due to flying debris	• Design process to maintain spark-inducing equipment at a safe distance from gas-handling equipment • Ground possible static producing equipment • Develop emergency fire response system • Train personnel
"	Reaction with oxygen, water, oxidizing agents	Potential for fatalities due to toxic release and fire Potential for injuries/fatalities due to flying debris	• Maintain inert carrier gases or vacuum in all phases • Install warning system to monitor presence of water or air • Design plumbing (water pipes) to be a safe distance from gas-handling equipment • Provide maintenance and inspection to maintain safe operation of all parts of system
"	Overheat in reactor tube	Potential for fatalities due to toxic release and fire Potential for injuries/fatalities due to flying debris	• Provide warning system for temperature fluctuation • Evacuate reaction tube • Shut off input valves • Activate cooling system • Design control system to detect overheat and disconnect heater
"	Leak in reactor	Potential for fatalities due to toxic release and fire Potential for injuries/fatalities due to flying debris	• Connect all reactor inlet and outlet lines to a common inert tank • Activate the connecting line in emergency • Provide automatic unit shut down as a result of above activation

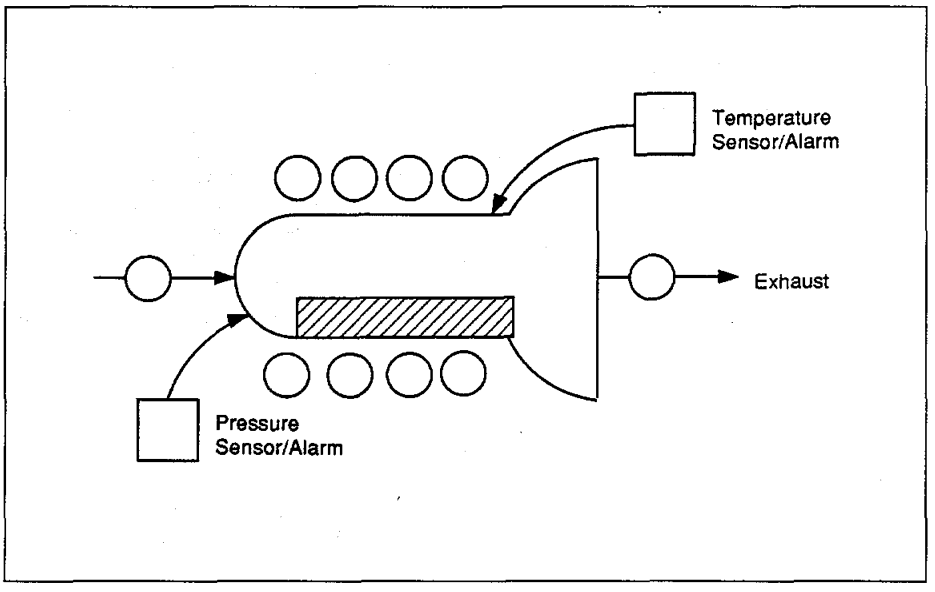


Figure III-2. Fault tree analysis for metal organic chemical vapor deposition (MOCVD) process, preliminary steps.

Table III-3
Results of Failure Modes Effects and Criticality Analysis (FMECA) to the Metal Organic Chemical Vapor Deposition (MOCVD) Process

Item	Failure Mode	Effects	Criticality Ranking
Reactor tube	Rupture	Release of pyrophoric gases causing fire Release of toxic gases	III IV
Air operated valve on storage cylinder	Rupture	Release of pyrophoric gases Release of toxic gases	III IV
	Failure to close	Excess gas in reactor tube can cause increase in pressure and rupture of reactor tube	IV
Air operated exhaust valve	Failure to open	Pressure buildup in reactor; possible rupture, release of pyrophoric and toxic gases	IV
	Rupture	Release of pyrophoric and toxic gases	IV
Control on reactor heater	Sensor fails Inadequate response Control system fails	Reactor over heating beyond design specification	II
Pump from storage to reactor	Malfunction: electrical mechanical	Overheat reactor tube	II
Transfer line fittings	Loose, not properly installed	Leakage of pyrophoric and toxic gases	II
Refrigeration equipment	Failure to operate	Increase in vapor pressure; cylinder rupture	IV

degree on the judgment and experience of the design engineer. This, however, can become an important factor for using and prioritizing hazard mitigation in the process design.

APPLICATION OF HAZOP STUDIES TO THE MOCVD PROCESS

System deviations

The major objective of hazard and operability (HAZOP) studies is to determine the possibilities of a system deviating from its design intent. Table III–4 presents a HAZOP study on two parameters of the MOCVD process: flow of trimethylaluminum (TMAl) and temperature of the TMAl storage tank. Although both of these areas are quite important, it must be emphasized that many more parameters such as the reactor tube should be considered in a similar manner. The guide words are chosen from Table II–6; more specific guidewords may be considered for different types of processes.

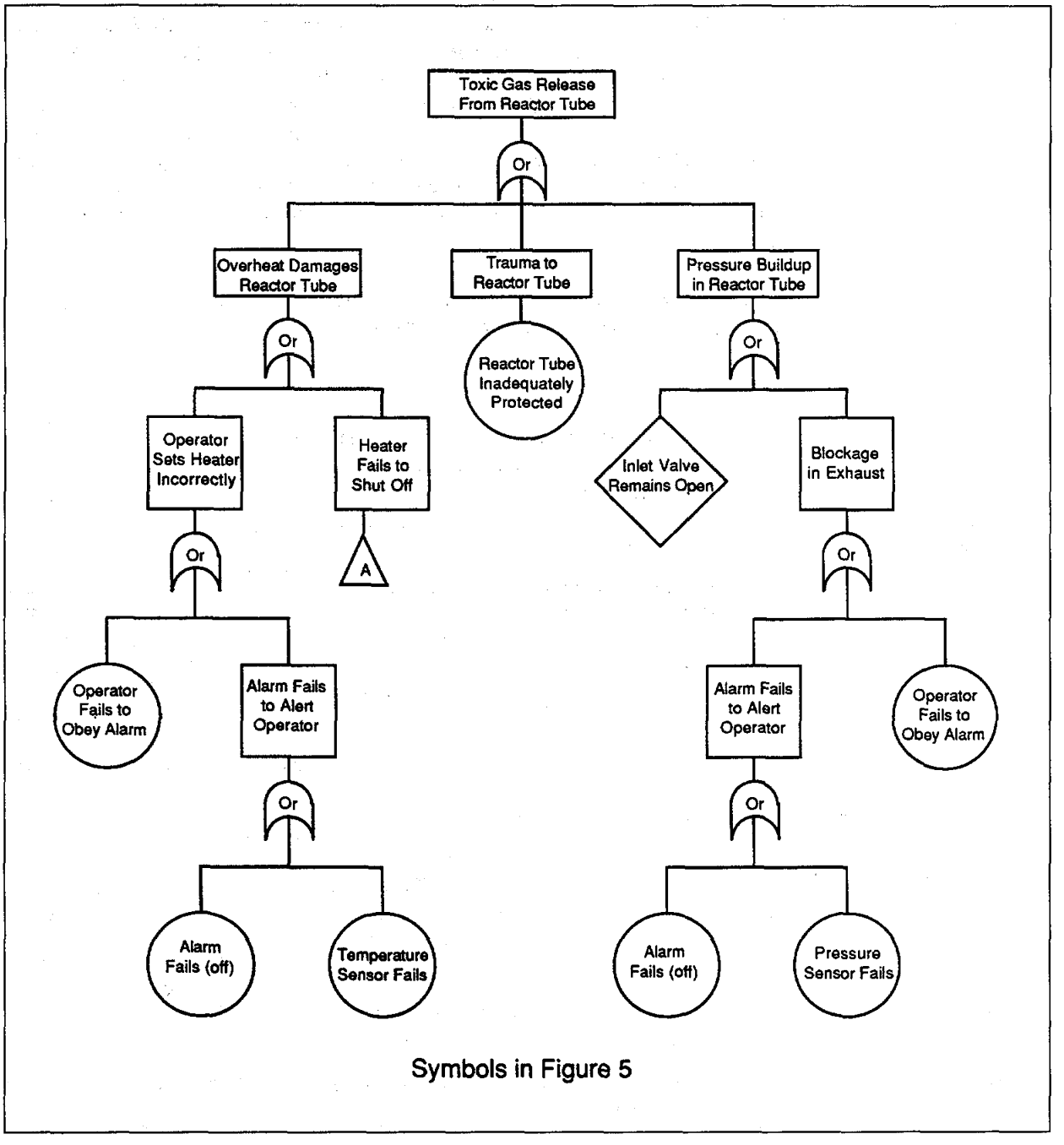


Figure III–3. Fault tree analysis (FTA) flow chart for the metal organic chemical vapor deposition (MOCVD). The symbols used here are described in Figure II–3.

APPLICATION OF ETA TO THE MOCVD PROCESS

Accident outcomes

Event tree analysis (ETA) focuses on the outcomes of the accident that may result following an equipment failure within the system. ETA, which is a forward thinking process, starts with an initiating event and analyzes the consequences both in terms of success and failure.

Reactor heater failure

Figure III–4 represents an ETA for a reactor heater failure in the MOCVD process. This method demonstrates the possible outcomes of various equipment failure combinations. This information can be used to determine if unsafe conditions exist. The event tree is straightforward and concise and can be used for analyzing initiating effects that could lead to unacceptable risks.

DISCUSSION OF RESULTS FOR THE MOCVD PROCESS

Each method used to analyze the MOCVD process results in important design information. HAZOP and PHA both include recommended corrective actions in the final report. PHA begins with a hazard and then explores cause and effects. HAZOP, on the other hand, begins with a particular equipment malfunction and studies the cause. FTA begins with a TOP event and traces it down to all possible basic faults that cause the undesired event. On the other hand, ETA starts with an initiating event and explores the effects of different combinations of failure modes. The final report from a FMECA is in tabular form; one individual failure mode and its effects and criticality on the system are studied. Because of the broad scope of results obtained from different types of analyses, the most beneficial hazard evaluation to the design process should include several evaluation methods.[6,7]

It should be pointed out that these procedures are invaluable tools in safe design and operation of any potentially hazardous process.

Table III–4
Application of Hazard Operability (HAZOP) Studies to the Metal Organic Chemical Vapor Deposition (MOCVD) Process Parameter: Flow of Trimethylaluminum (TMAl)

Guide word	Deviation	Consequences	Causes	Recommended Action
no	No flow of TMAl	TMAl not released to reaction chamber; no reaction occurs; possible unreacted toxic gas in exhaust	Faulty valve	Pressure-regulated automatic shutdown (at storage tank)
			Faulty mass flow	Pressure-regulated automatic shutdown (at storage tank)
			Empty storage tank	Monitor tank levels regularly, automatic level, pressure control
more	More flow of TMAl	Possible rupture to reaction chamber or valves; release of toxic, pyrophoric gas	Faulty mass flow controller	Pressure-regulated automatic shutdown (before reactor)
part of	Normal flow of lower concentration TMAl	Possible unreacted toxic gas released in exhaust	Operator error in flow rate ratios of gases or faulty mass flow controller at storage tank for TMAl or other gases	Monitor exhaust with shutdown if unreacted gases detected
less	Less flow of TMAl	Unreacted toxic gas may be released with exhaust	Faulty mass flow controller, operator error in choice of flow rates	Pressure regulated automatic shutdown warning to operator if flow rates of all gases not in a ratio within limits
higher	Higher temperature in storage tank	Increased pressure; possibility of leakage of toxic, pyrophoric gas	Faulty cooling unit	Backup cooling unit activated by temperature sensor
lower	Lower temperature in storage tank	Decreased pressure may result in lack of flow of gas resulting in unreacted toxic gases in exhaust	Faulty cooling system	Backup cooling unit activated by temperature sensor
			Faulty thermostat	Regular monitoring and maintenance of all aspects of cooling unit

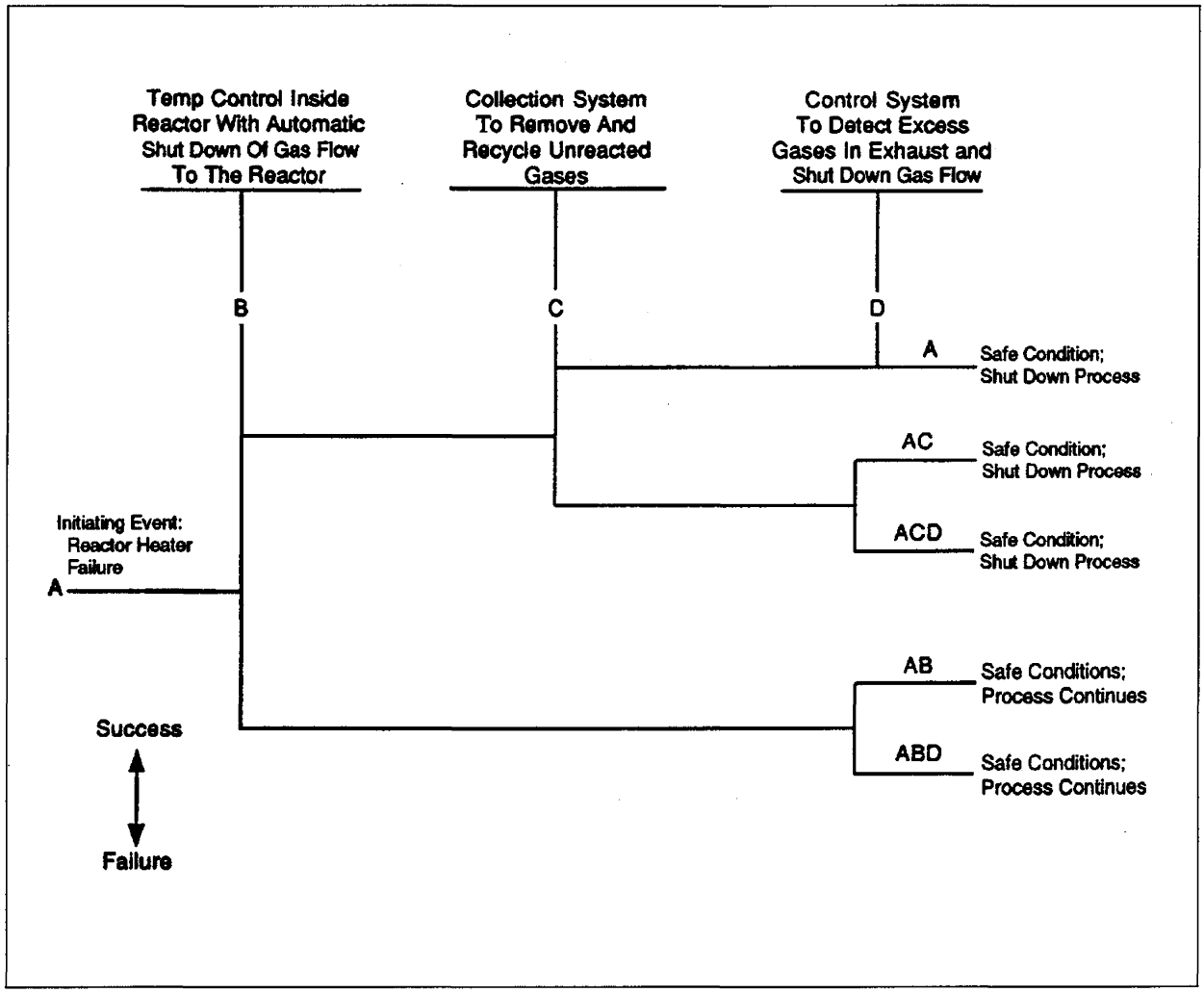


Figure III–4. Application of event tree analysis (ETA) to the reactor tube in the metal organic chemical vapor deposition (MOCVD) process.

REFERENCES

1. Kavianian, H.R., C.A. Wentz, R.W. Peters, and L.E. Martino: Total Concepts in Safety Systems Management for Hazardous Materials Handling and Design of Hazardous Processes, Annual Loss Prevention Symp., AIChE Spring 1989 National Meeting, Houston AIChE, New York, NY (1989).
2. Kavianian, H.R., G.V. Brown, and J.K. Rao: Safety Systems Management for Design of Hazardous Technologies, American Society of Safety Engineers, Des Plaines, IL (1988).
3. National Fire Protection Association, Fire Protection Handbook, 5th ed., NFPA, Quincy, MA (1976).
4. Plunkett, E.R.: Handbook of Industrial Toxicology, 3rd ed., Chemical Publishing Co., Inc., New York, NY (1987).
5. Jaafar, S., F. Rajab, and N. Saaidin: Preliminary Hazard Evaluation for Hydrogen Plant,* School of Engineering, California State University, Long Beach, CA (1988).
6. Battelle Columbus Division, Guidelines for Hazard Evaluation Procedures, The Center for Chemical Process Safety, AIChE, New York, NY (1985).
7. Hazardous Materials Information Center, Hazard Classification Systems, Inter/Face Associates, Inc., Middletown, CT (1986).

*Available upon written request to the author.

Unit IV

PRELIMINARY DESIGN OF AN ETHYLENE PRODUCTION PLANT

PURPOSE:

To examine the application of system safety techniques to the design of an ethylene production plant

OBJECTIVE:

To acquaint the student with:

1. The ethylene production process
2. Application of system safety techniques to design of an ethylene production plant

SPECIAL TERMS:

1. Pyrolysis
2. Waste heat recovery
3. Selectivity
4. Residence time

INSTRUCTOR MATERIALS:

1. Chalkboard
2. Student supplementary materials

TRAINEE MATERIALS:

1. Supplementary materials provided by the instructor

ETHYLENE PLANT PROCESS DESCRIPTION

Steam pyrolysis

Ethylene is the major feedstock used by the petrochemical industry for producing a variety of synthetic polymers. Ethylene is produced by steam cracking hydrocarbons such as ethane, propane, naptha, and gas oil. Steam pyrolysis of hydrocarbons produces ethylene along with a wide range of byproducts such as hydrogen, methane, propylene, and butadiene. Since ethylene purity is a critical factor in polymerization units, the mixture of gases obtained as a result of steam cracking must be purified. Therefore, ethylene plants are composed of a pyrolysis section in which the feedstock is cracked in pyrolysis furnaces to produce ethylene and other gases and in a purification section in which the pyrolysis products are separated and recovered.[1,2,3]

Ethylene production

Ethylene production involves high temperatures (1500°F) in the pyrolysis section and cryogenic temperatures in the purification section. The feedstocks, products, and byproducts of pyrolysis are flammable and pose severe fire hazards. Benzene, which is produced in small amounts as a byproduct, is a known carcinogen. Table IV-1 summarizes some of the properties of ethane (feedstock) and product gases.

Table IV-1
Hazardous Properties of Materials in Ethylene Production[4]

Feedstock	Toxicity	Fire Hazard	Explosion Hazard
Ethane	Low	Very dangerous	Moderate
Hydrogen	None	Dangerous	Dangerous
Acetylene	Moderate	Very dangerous	Moderate
Methane	Low	Very dangerous	Dangerous
Ethylene	Low	Very dangerous	Moderate
Carbon dioxide	Low	None	None

Figure IV-1 shows a simplified schematic diagram of the pyrolysis and waste heat recovery section of an ethylene plant.

Process

The feedstock is mixed with steam before entering the pyrolysis reactors. Steam reduces the hydrocarbon partial pressure, acts as a heat transfer media, and reduces coke laydown inside the reactor tubes. The tubular reactors are heated to reaction temperatures (1100°F to 1700°F) by means of direct fired heaters. The flow of steam and feedstock to the reactors can be adjusted to provide an optimum residence time, which is a function of the feedstock used.

After completing the cracking reactions in the tubular reactors, the gaseous mixture flows to a quench tower where the gas temperature is lowered enough to stop the cracking reactions. Oil or water can be used as the cooling media. Transfer line heat exchangers can be used to recover the heat contained in the product gas, and this energy can be used to produce high pressure steam.

The cooled gaseous products are dried using molecular sieves and compressed to about 500 psig by a multistage compressor. The compressed gas is then sent to an acetylene converter where acetylene is selectively hydrogenated to ethane. The gaseous mixture then flows to the purification section of the plant where each component of the gas is recovered by means of cryogenic distillation.

APPLICATION OF PHA TO THE PYROLYSIS AND WASTE HEAT RECOVERY SECTION

Table IV-2 summarizes the results of application of a preliminary hazard analysis (PHA) to the pyrolysis section of an ethylene plant. The major hazard to the personnel and plant is the fire or explosion hazard of the gases used or produced in the process.

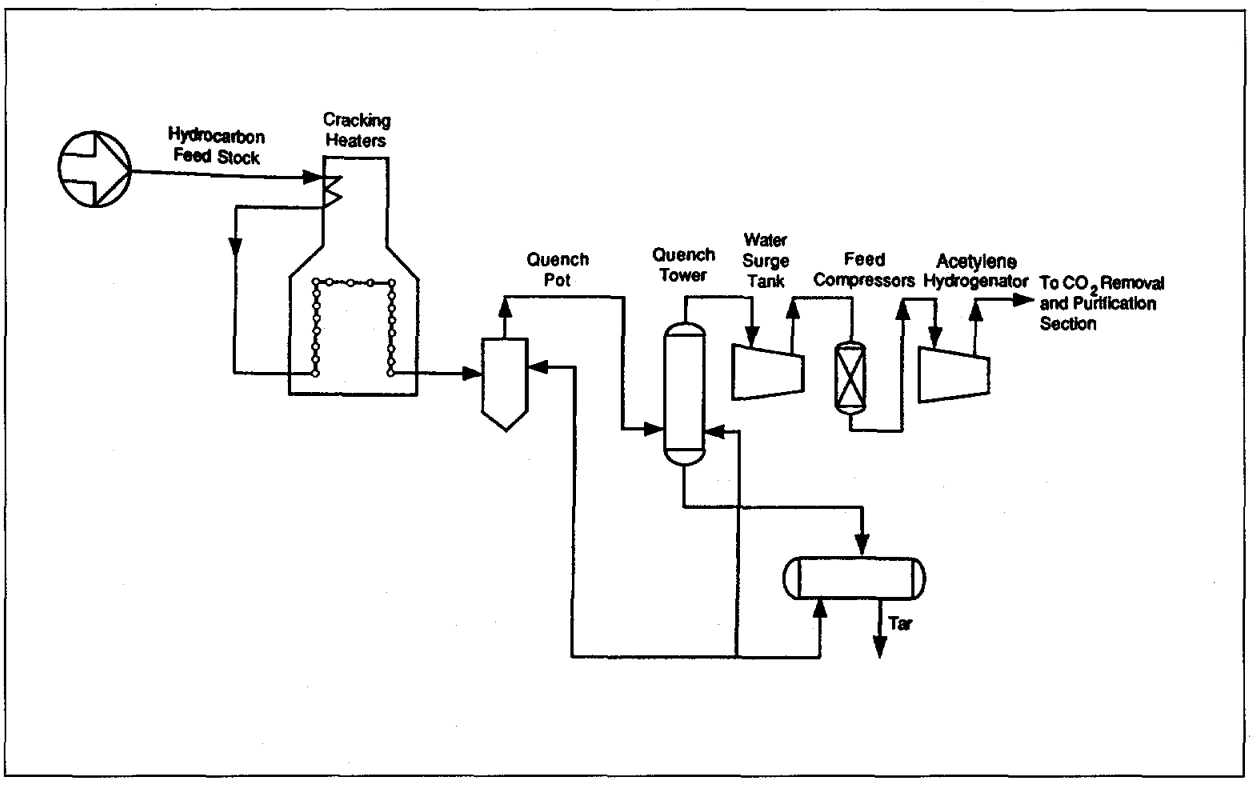


Figure IV-1. Pyrolysis and waste heat recovery section of an ethylene production plant.

APPLICATION OF FTA TO THE PYROLYSIS FURNACE OF AN ETHYLENE PLANT

Figure IV-2 demonstrates the preliminary steps for a fault tree analysis (FTA); in addition, the TOP event, bounds, configurations, and unallowed events are specified, and the level of resolution is shown. Once all the limits have been determined, the fault tree is constructed (as in Figure IV-3). Note that every branch of the fault tree ends in a basic fault or cause leading to the TOP event.

As can be noted in Figure IV-2, steam and ethane are mixed before entering the reactor tubes where pyrolysis reactions take place. All feed and product lines must be equipped with appropriate control devices to ensure safe operation.[5]

DISCUSSION OF RESULTS

FTA results in a flow chart that breaks down a TOP event (see description of fault tree in Unit II) into all possible basic causes. Although, this method is more structured than PHA, it addresses only one individual event at a time. To use FTA for a complete hazard analysis, all possible TOP events must be identified and investigated; this would be extremely time consuming and perhaps unnecessary in a preliminary design. As can be noted from the analysis of the ethylene plant, one of the major disadvantages of the FTA is lack of recommendations for preventative and corrective measures. FTA, however, has the advantage of pinpointing the sequence of events that could lead to an undesired TOP event. Once these causes have been identified, an experienced design team can recommend solutions in the form of design alternatives and/or instrumentation. In recommending solutions, the probability, severity, and economics of each case must be taken into account. For example, the problem of temperature control failure in the reactor tubes as a result of disruption in ethane flow can also be solved by installing flow controls on the lines. Although flow controls on feed and steam lines are installed for the purpose of controlling the residence time in the reactor and product distribution, the flow controllers also contribute to temperature control in the reactor. These interactions are important and their effects must be taken into account as a conceptual design develops into a flow diagram and finally into a piping and instrumentation diagram.

Table IV–2

Example of Applying Preliminary Hazard Analysis (PHA) to an Ethylene Plant

Hazard	Cause	Major Effects	Corrective/Preventative Measures
Damage to feed reactor tubes	Feed compressor failure (no endothermic reactions in reactor)	Capital loss, downtime	• Provide spare compressor with automatic switch-off control
		Damage to the furnace coils due to high temperature	• Develop emergency response system
Explosion, fire	Pressure buildup in the reactor due to plug in transfer lines	Fatalities, injuries	• Provide pressure relief valve on the reactor tubes • Provide warning system for pressure fluctuations (high-pressure alarm) • Provide auxiliary lines with automatic switch off
" "	Violent reaction of H_2 to acetylene converter with air in presence of ignition source	Potential for injuries and fatalities due to fire or explosion	• Provide warning system (hydrogen analyzer) • Eliminate all sources of ignition near hydrogen gas storage area • Develop emergency fire response • Automatically shut off the H_2 feed • Provide fire fighting equipment
Flammable gas release	Ethane storage tank ruptures	Potential for injuries and fatalities due to fire or explosion	• Provide warning control system (pressure control) • Minimize on-site storage • Develop procedure for tank inspection • Develop emergency response system • Provide gas monitoring system
Flammable gas release	CH_4 Storage tank (line) leak/rupture (fuel for the furnace)	Potential for injuries and fatalities due to fire or explosion	• Provide warning system • Minimize on-site storage • Develop procedure for tank inspection • Develop emergency response system • Provide gas monitoring system
Flammable gas release	Radiant tube rupture in the furnace	Potential for injuries and fatalities due to fire	• Improve reactor materials of construction • Monitor design vs. operating reactor temperature • Provide temperature control instrument
Employee exposure to benzene (carcinogen)	Leak in knock-out pots or during handling benzene	Chronic health hazard	• Install warning signs in the area • Provide appropriate PPE • Develop safety procedures for handling and cleanup • Monitor concentration of benzene in area to meet TLV requirements
Fire/explosion in acetylene converter	Runaway reaction (exothermic)	Fatality, injury, or loss of capital	• Install temperature control on converter • Install pressure relief on reactor responding to temperature control
Flammable atmosphere	Leak in transfer lines	Fire/explosion	• Install combustible gas meter in sensitive areas • Provide adequate fire fighting equipment • Provide for emergency shutdown • Educate and train personnel on emergency procedures

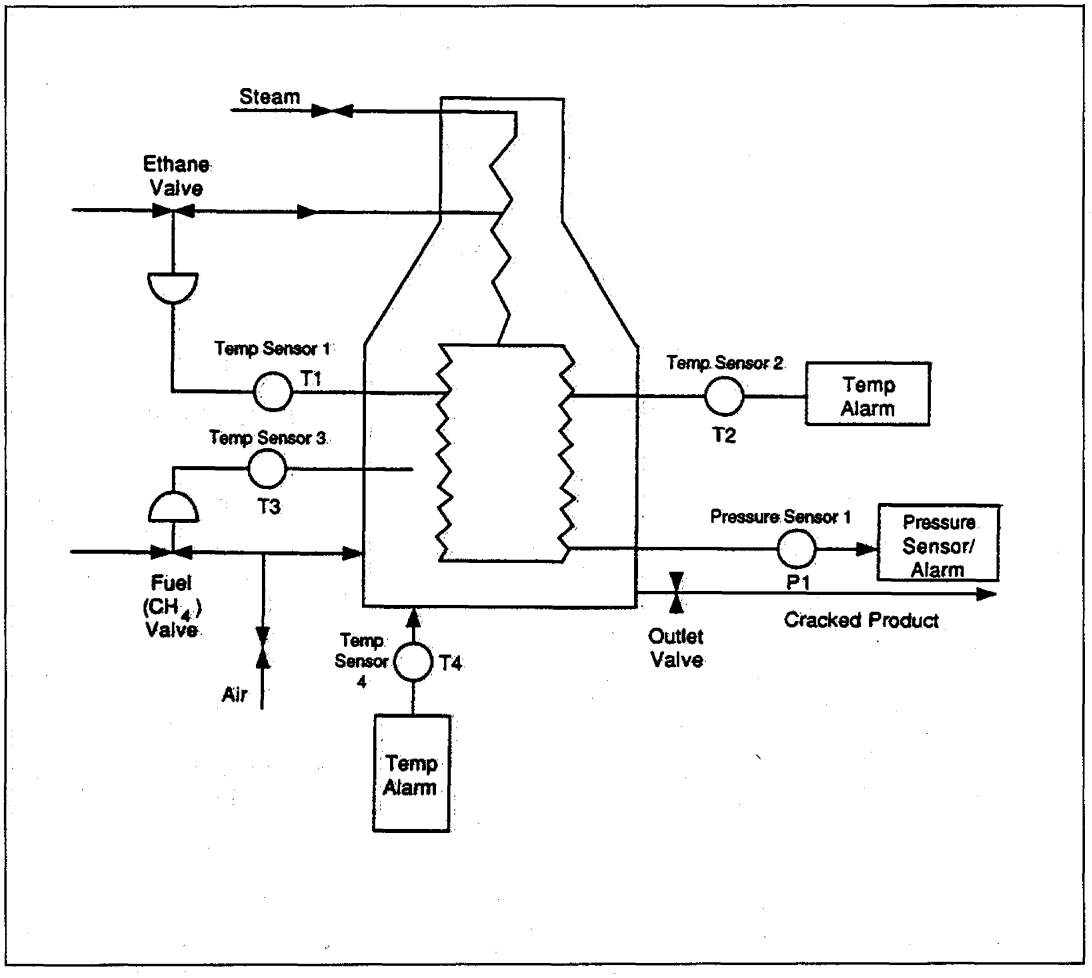


Figure IV–2. Fault tree analysis (FTA) preliminary steps, ethylene plant.

The earlier analysis of PHA indicates that PHA is not only capable of identifying major hazards in the process, but it also recommends corrective measures at the very early stages of design. This is extremely important in developing new technologies and in feasibility studies. The overall economic picture of a process can change drastically as a result of instrumentation and/or procedures to minimize risk or to bring the plant into compliance with regulations.

REFERENCES

1. Paustenbach, D.J.: Should Engineering Schools Address Environmental and Occupational Health Issues? J. Professional Issues in Engineering, 113(2):93-111, ASCE (April 1987).
2. Meyers, R.A.: Handbook of Petroleum Refining Processes, McGraw-Hill, New York, NY (1986).
3. Kniel, L., O. Winter, and K. Stork: Ethylene, Keystone to the Petrochemical Industry, Marcel Dekker Inc., New York, NY (1980).
4. Plunkett, E.R.: Handbook of Industrial Toxicology, 3rd ed., Chemical Publishing Co., Inc., New York, NY (1987).
5. Abdulmalik, M., E. Firoszabadi, H. Kavianian, and S. Panahshashi: Safety and Hazard Assessment for Preliminary Design of Ethylene Plant,* School of Engineering, California State University, Long Beach, CA (1988).

*Available upon written request to the author.

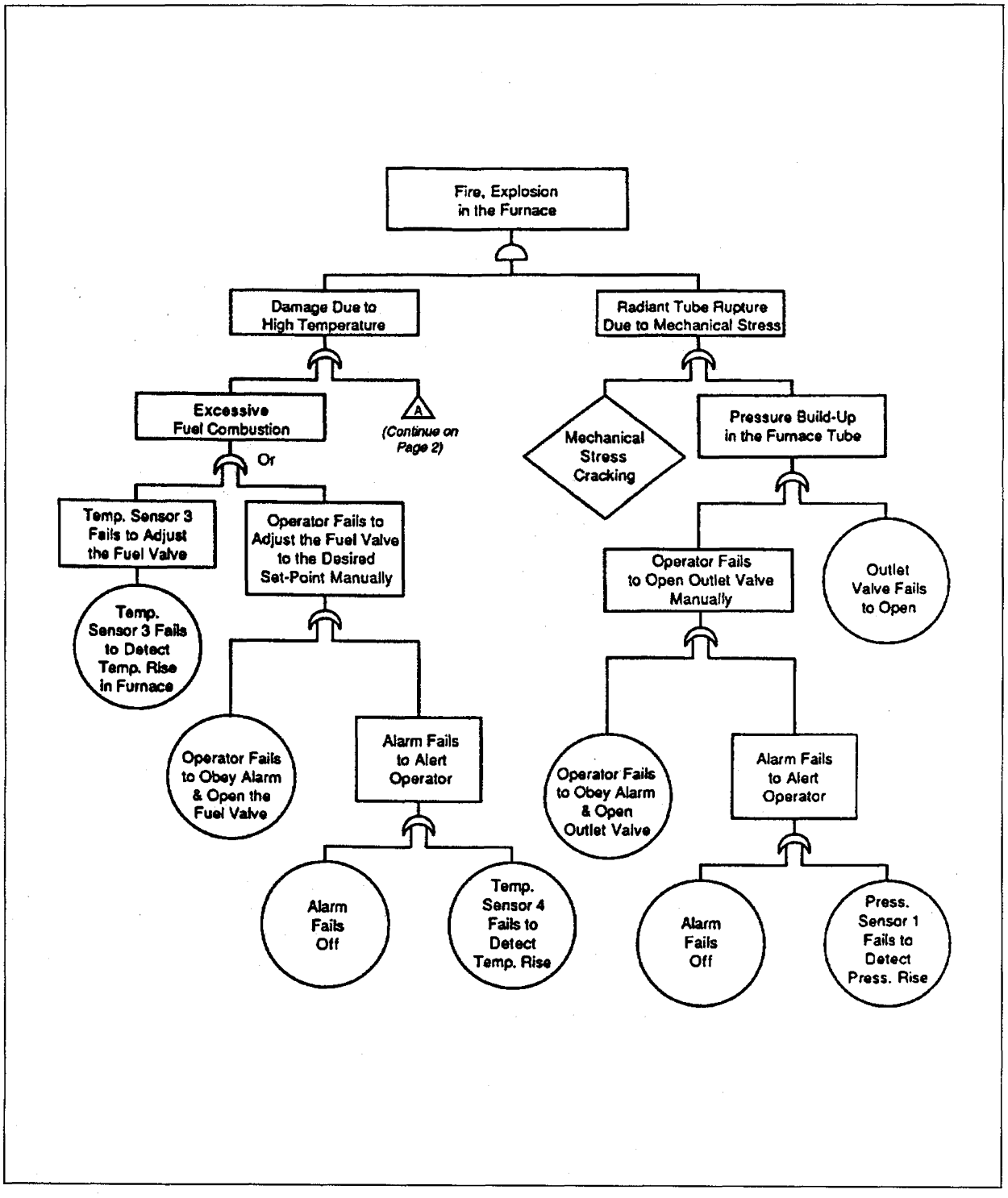


Figure IV-3. Fault tree analysis (FTA) for an ethylene plant design. The symbols used here are described in Figure II-3. (sheet 1 of 2)

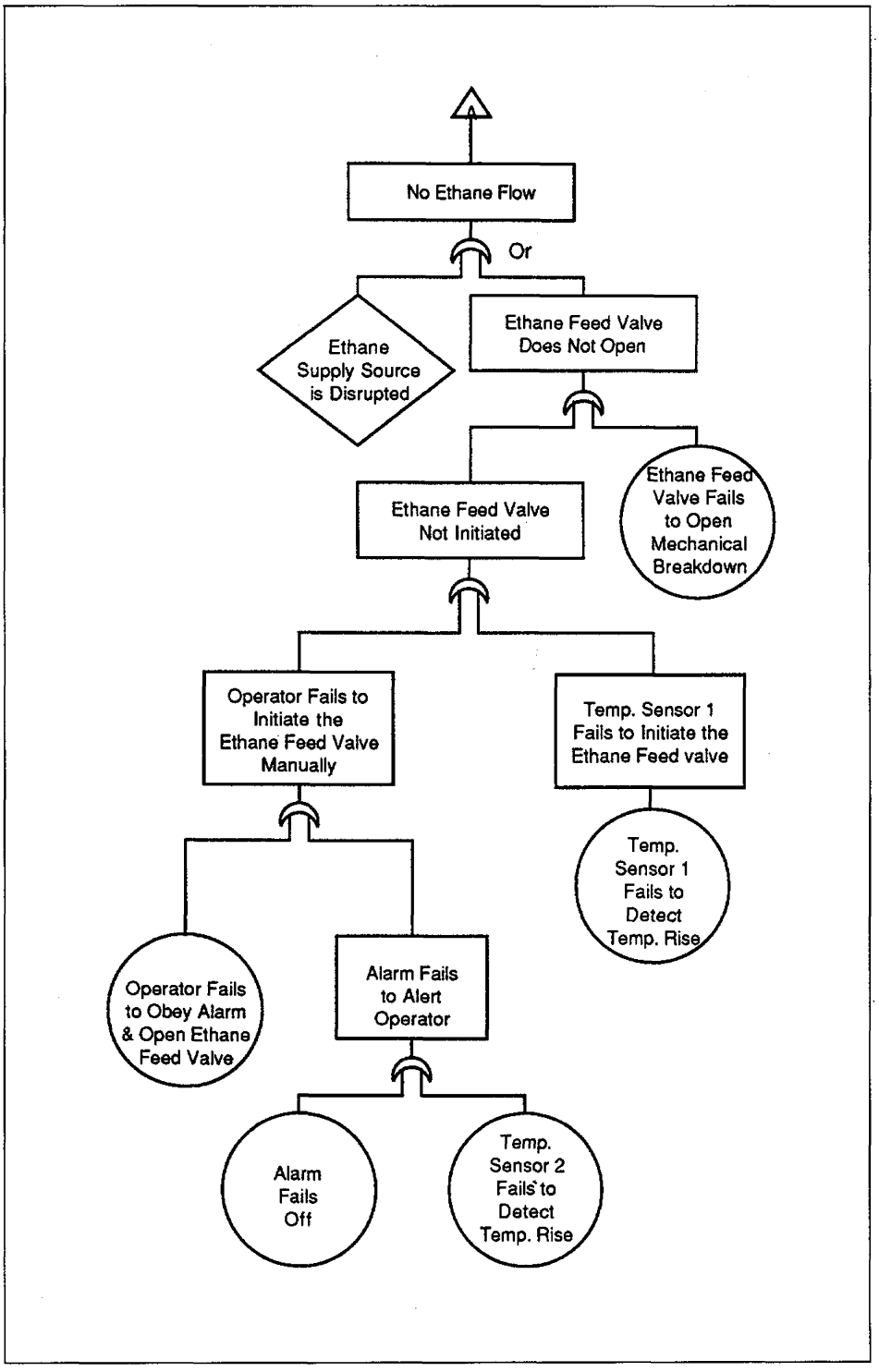


Figure IV-3. Fault tree analysis (FTA) for an ethylene plant design. The symbols used here are described in Figure II-3. (sheet 2 of 2)

Unit V

PRELIMINARY DESIGN OF AN ALKYLATION PROCESS

PURPOSE:

To examine the application of system safety techniques to the design of an alkylation process

OBJECTIVE:

To acquaint the student with:

1. The alkylation process
2. The application of system safety techniques to the preliminary design process

SPECIAL TERMS:

1. Alkylation
2. Catalyst
3. Reactor/settler

INSTRUCTOR MATERIALS:

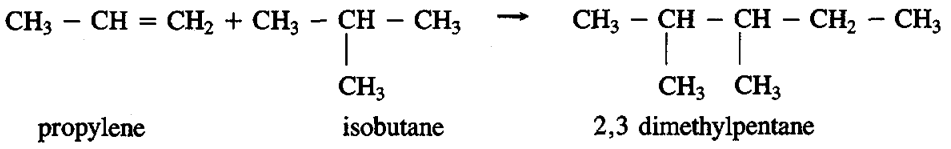
1. Chalkboard
2. Student supplementary materials

TRAINEE MATERIALS:

1. Supplementary materials provided by the instructor

ALKYLATION PROCESS DESCRIPTION

Alkylation is used widely in the petroleum industry to produce high octane gasoline. It involves the reaction between a low molecular weight olefin and an isoparaffin in the presence of an acid catalyst. For example, propylene and isobutane can react according to the following reaction to produce gasoline:



Although the reactions taking place in an alkylation reactor are numerous and relatively complex, the major reactions always involve combination of a low molecular weight olefin and an isoparaffin as demonstrated above.

Alkylation processes

The acid catalysts used in the alkylation process include mainly hydrofluoric acid and sulfuric acid. Most alkylation processes in operation today use hydrofluoric acid as the catalyst because of the operating temperature flexibility. The hydrofluoric acid process developed by Phillips Petroleum Company is among the most widely used alkylation processes and, therefore, our process description will focus on the Phillips process. Table V–1 summarizes some of the hazardous properties of materials used in an alkylation process. It should be noted that hydrofluoric acid which has a permissible exposure limit of 3 ppm, can cause severe health hazards ranging from skin burns to death as a result of overexposure. This acid, because of hazardous properties, requires implementation of special handling and storage procedures as well as the use of proper protective equipment.

Table V–1

Hazardous Properties of Materials Commonly Used in Alkylation[1]

Alkylation Materials	Toxicity	TLV*	Fire Hazard	Explosion Hazard
Butene	Low	---	Very dangerous	Moderate
Propene	Low	---	Very dangerous	Moderate
Butane	Moderate	800 ppm	Very dangerous	Dangerous
Propane	Moderate	1000 ppm	Very dangerous	Very dangerous
Hydrofluoric acid	Dangerous	3 ppm	---	---

*TLV = threshold limit value.

Process

Figure V–1 shows a simplified schematic flow diagram of the Phillips alkylation process. In this process, isobutane is catalytically alkylated with oelfins, which exist in refinery of gases, in presence of liquid hydrofluoric acid. Recycled isobutane from the fractionating tower is mixed with olefin and isobutane feed before entering the alkylation reactor. The feed must be passed through dryers to remove any moisture before its entry into the alkylation reactor.

The alkylation reactor/settler, which is designed exclusively by Phillips Petroleum Company (see Figure V–2), has no moving parts and contains a moving bed of hydrofluoric acid; this bed provides high dispersion of feed into the catalyst and almost instantaneous conversion of feed to alkylate product.

The operating conditions in the reactor are mild. The temperature can range from 25°C to 45°C, and the operating pressure is selected to maintain fluids in their liquid states.

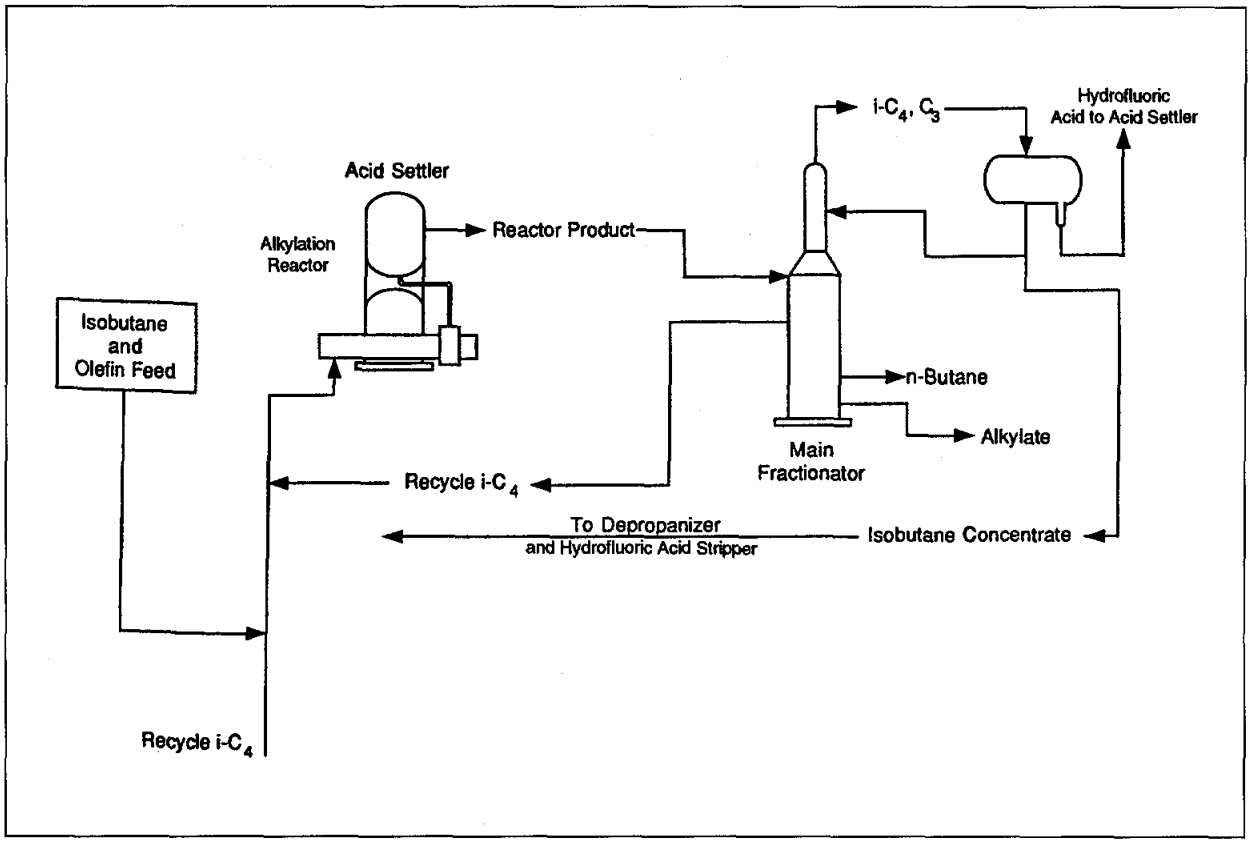


Figure V–1. Adapted from flow diagram of the Phillips Alkylation Process.[2]

After completion of the alkylation reactions, the mixture of catalyst, alkylate, and unreacted reactants flow upward to an acid settler (see Figure V–2) where acid hydrocarbon phase separation takes place. The hydrocarbon phase has a lower density than hydrofluoric acid, and because the two phases have very little solubility, the acid settles at the bottom of the settler.[2]

The hydrocarbon phase, which contains the alkylate product, is withdrawn from the top of the settler and is sent to the main fractionator where the alkylate is separated from hydrocarbon gases. The acid is withdrawn from the bottom of the settler and sent through a water cooled heat exchanger before being recycled back to the reactor.

APPLICATION OF ETA TO THE ALKYLATION REACTOR

The major hazards in the alkylation process are the flammability of gaseous and liquid hydrocarbons and health hazards posed by hydrofluoric acid. Figure V–3 shows an event tree analysis (ETA) focusing on the possibility of an acid leak from the lines carrying the acid into and out of the water-cooled acid cooler. It should be emphasized that ETA provides an opportunity to study the combination of scenarios that result from an undesired initiating event. Figure V–4 shows a similar analysis for the reactor tube failure. It can be seen that safety issues such as these can be identified and dealt with properly even in the very preliminary and early stages of design.

APPLICATION OF C-CA TO THE ACID CONTAINMENT UNIT OF ALKYLATION REACTOR

Figure V–5 demonstrates the application of cause-consequence analysis (C-CA). The starting point for this analysis is the event tree in Figure V–4. In Figure V–5, the acid containment unit has been isolated for study. The consequences and reasons for the success or failure of the containment unit are highlighted. It should be noted that C-CA combines the backward-thinking scheme of the ETA for initiating events, with FTA being somewhat more readable and easier to use in the design process. It should be emphasized that although C-CA can become very complex and involved in a short period

of time, it is a valuable tool for identifying possible accident scenarios and their consequences.

REFERENCES

1. Plunkett, E.R.: Handbook of Industrial Toxicology, 3rd ed., Chemical Publishing Co., Inc., New York, NY (1987).
2. Meyers, R.A.: Handbook of Petroleum Refining Processes, McGraw-Hill, New York, NY (1986).

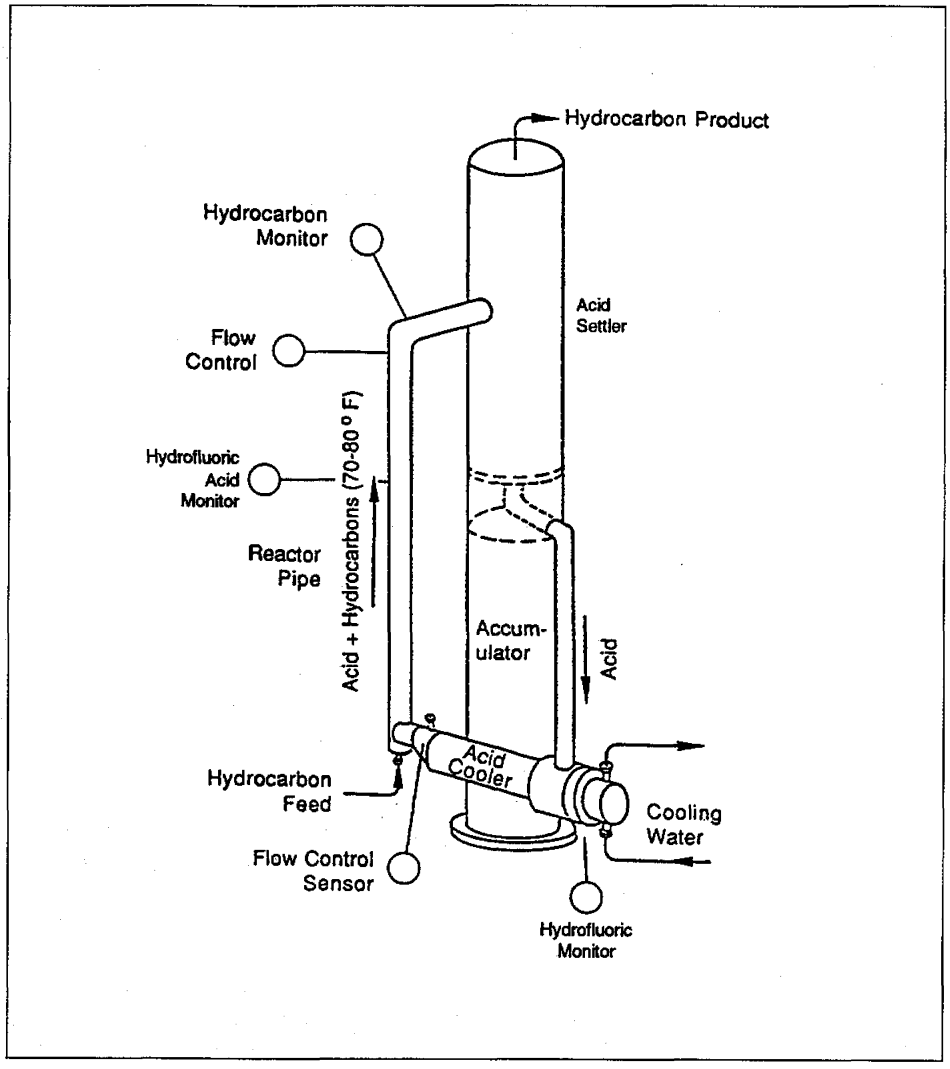


Figure V-2. Diagram of an alkylation reactor.[2]

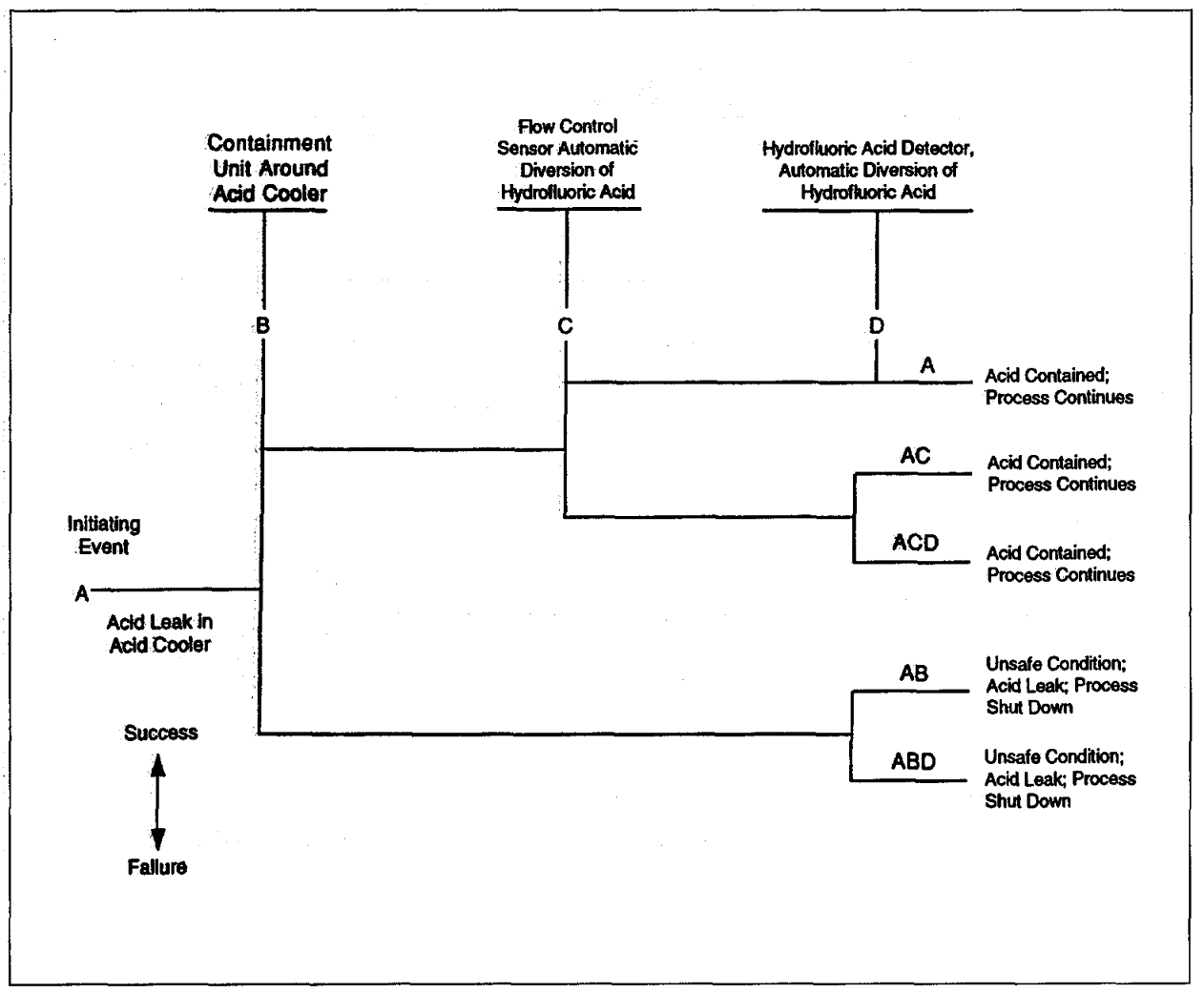


Figure V-3. Event tree analysis (ETA) for an acid leak around acid cooler of an alkylation reactor.

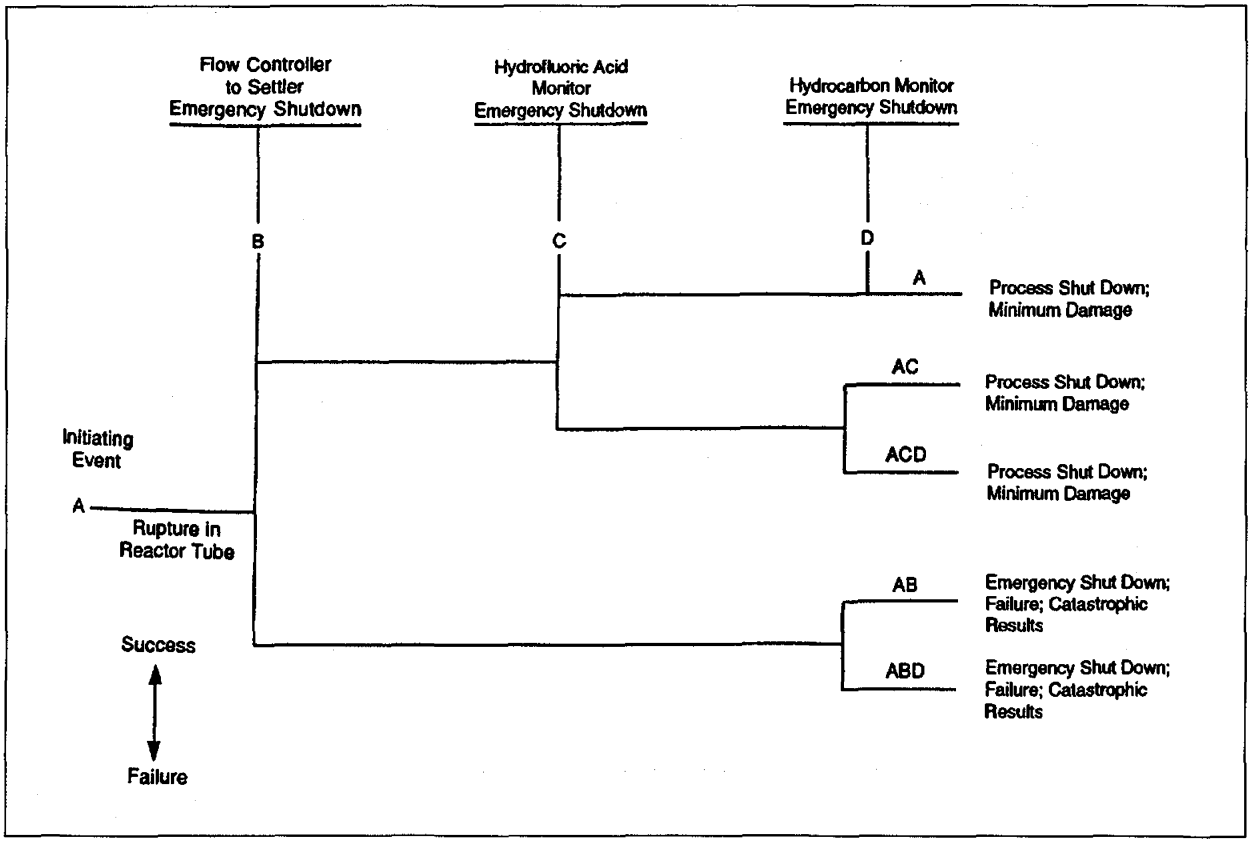


Figure V–4. Event tree analysis (ETA) for acid leak as a result of reactor failure.

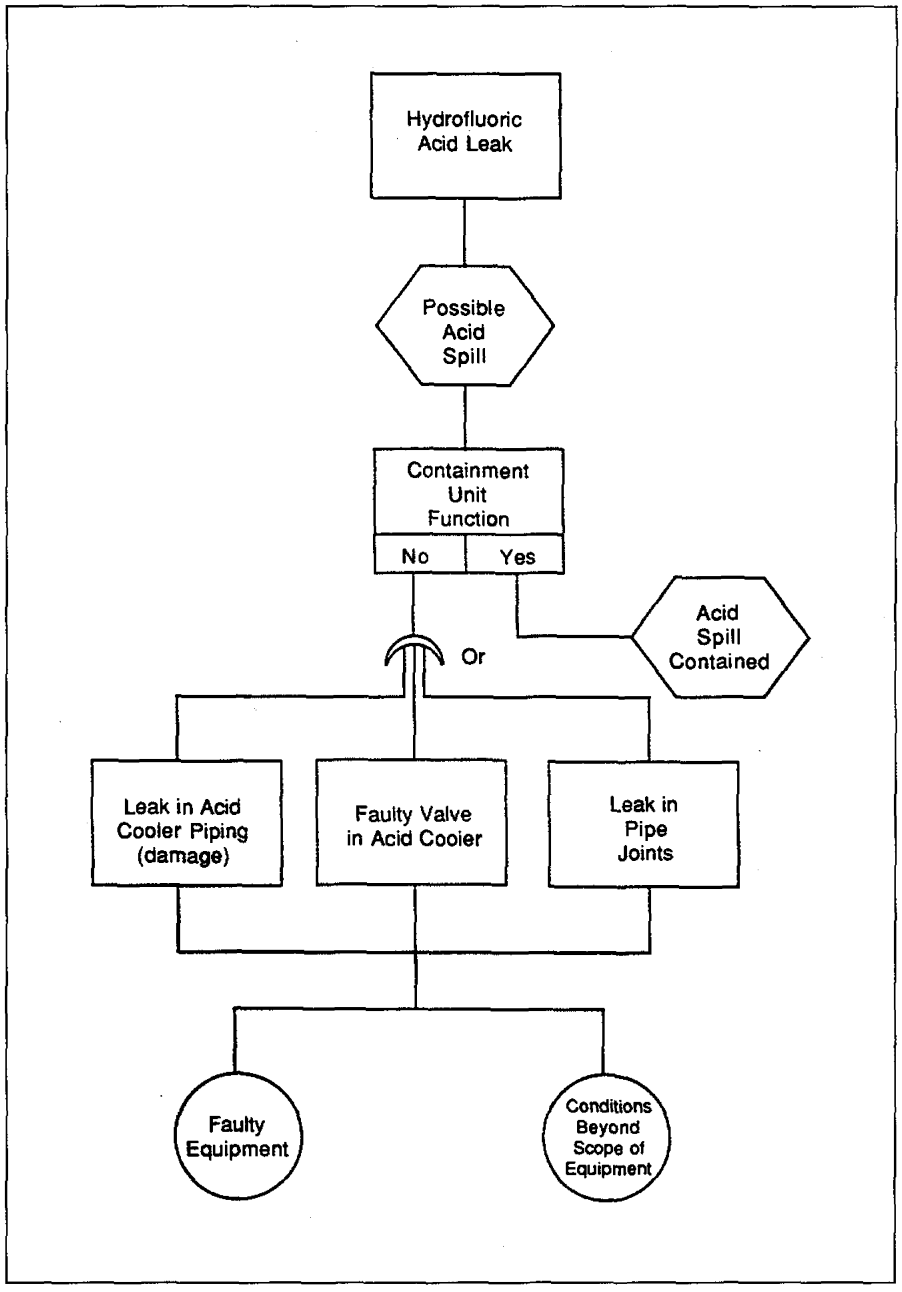


Figure V–5. Cause-consequence analysis (C-CA) for an acid leak in alkylation process.

Unit VI

PRELIMINARY DESIGN OF A HIGH PRESSURE/LOW DENSITY POLYETHYLENE PLANT

PURPOSE:

To examine the application of system safety techniques to the design of a high pressure/low density polyethylene plant

OBJECTIVE:

To acquaint the student with:

1. The high pressure/low density polyethylene process
2. The application of system safety techniques to the preliminary design process

SPECIAL TERMS:

1. High pressure/low density polyethylene process
2. Multistage reciprocating compressor
3. Exothermic reaction
4. Conversion

INSTRUCTOR MATERIALS:

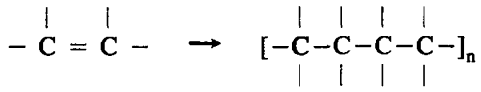
1. Chalkboard
2. Student supplementary materials

TRAINEE MATERIALS:

1. Supplementary materials provided by the instructor

PROCESS DESCRIPTION

Polyethylene, which is one of the most widely used thermoplastics, can be obtained by polymerization of ethylene:



Low pressure process

The polymerization process can be carried out either at low or high pressures depending on the intended use of the final product. Polyethylene obtained by the low pressure process has a higher degree of crystallinity and, as a result, a higher density when compared with the polyethylene obtained via the high pressure process. Polyethylene has found widespread use in packaging, construction, agriculture, household items, and the rubber industry.[1,2]

High pressure process

Figure VI–1 shows a simplified schematic flow diagram of a high pressure/low density polyethylene plant. Polymerization grade ethylene (99.5% pure) is compressed to about 1500 atmospheres using a multistage reciprocating compressor (make-up compressor) and heated to a temperature of about 350°F. The molecular weight of the polymer is directly proportional to the reactor pressure. After the addition of small amounts of initiator, which acts as a catalyst for the polymerization reactions, the mixture of ethylene and initiator enter the polymerization reactor—a tube with length-to-diameter ratio to facilitate removing the heat generated by polymerization. Because of the large exothermic heat of polymerization and difficulty of removing this heat, the conversion of ethylene per pass is kept in the range of 15 to 25 percent. Some reactors use a cooling jacket with a suitable heat transfer fluid to remove the heat of polymerization. Removing the heat generated within the reactor is critical because of the possibility for a "runaway" reaction. A runaway reaction is defined as a self-accelerating reaction that, if not controlled, can lead to a disaster. If the heat generated within the polymerization reactor is not removed, the reactor temperature would rise; this would then increase the rate of polymerization reactions, generate more heat, and increase the reactor temperature further.

The mixture of polymer and unreacted ethylene are removed from the reactor by means of a melt pump and are sent to a high pressure separator to recover the bulk of the unreacted ethylene. The ethylene recovered from the high pressure separator is fed to the suction port of the recycle gas compressor and is then fed back to the polymerization reactor. The polymer, which contains some unreacted ethylene, is pumped out of the high pressure separator using a melt pump and is sent to a low pressure separator for the recovery of the remainder of the unreacted ethylene. The overhead from the low pressure separator is sent to a recycle gas compressor and is fed back to the reactor. The polymer is pumped out of the low pressure separator by a melt pump and is sent through water tanks to a pelletizer. The pelletized product is devolatilized and purged to remove any residual monomer before it is sent to packaging.

APPLICATION OF "WHAT IF" ANALYSIS TO A LOW DENSITY POLYETHYLENE PLANT

Table VI–1 summarizes the results of preliminary "What if" analysis to high pressure/low density polyethylene production. This information is compiled in tabular form, and recommendations are provided. The success of a "What if" analysis depends upon the analyst's familiarity with the process and experience with this type of hazard evaluation. For example, the possibility of a runaway reaction may not seem obvious to someone unfamiliar with the polymerization process.[3]

APPLICATION OF HAZOP TO A LOW DENSITY POLYETHYLENE PLANT

As mentioned before, a hazard and operability (HAZOP) study focuses on how certain parameters of a plant can deviate from their design value. Although during the course of a HAZOP study the solution to certain problems might become evident, it should be emphasized that the main objective is to identify design problems.

Table VI–2 is an example of a HAZOP study for two parameters in a high pressure/low density polyethylene process. Since the reaction temperature and the flow rate of ethylene

Table VI-1

"What If" Analysis Applied to High Pressure/Low Density Polyethylene Production (simplified diagram)

What If	Consequence/Hazard	Recommendations
Coolant pump to reactor fails	Runaway condition in reactor causing explosion/fatality	• Provide accurate temperature monitoring in reactor • Employ backup pump/high temperature alarm • Relieve reactor pressure in reactor through automatic control to stop reactions • Provide automatic shut off of ethylene flow
Coolant temperature to jacket is high	Eventual runaway condition in reactor	• Provide adequate temperature control on coolant line • Use heat exchanger flow control to adjust inlet temperature
Runaway condition in reactor	Explosion; fire/fatality	• Provide adequate temperature control on coolant line • Use heat exchanger flow control to adjust inlet temperature • Install rupture disk/relief valve to relieve pressure to stop reactions • Emergency shut down procedure
Recycle gas compressor 1 or 2 fails	None likely	• Provide spare compressor or shutdown procedure
Melt pump fails	High level in reactor causing more polymerization: runaway reaction eventually exceeds design pressure	• Provide level and flow control schemes to activate spare pump or shut the flow of monomer • Shut down procedure if no spare pump
Leak at suction or discharge of compressors	Fire; explosion	• Use monitoring devices to ensure no flammable gas is released
Ethylene leaks out of process lines	Fire; explosion	• Provide adequate flammable gas monitoring devices
Monomer/initiator ratio out of control	Eventual runaway reaction causing fire and explosion	• Provide flow control on the initiator and monomer lines

Table VI-2

A Hazard and Operability (HAZOP) Study on a Polyethylene Plant

Guide Work	Deviation	Consequences	Causes	Recommended Action
Parameter: Reactor temperature				
Higher	Higher reactor temperature	Runaway reaction in reactor	Coolant pump to reactor fails	• Provide temperature control • Provide high temperature sensor/alarm • Provide pressure relief valve with automatic feed from temperature control system • Provide spare coolant pump
			Coolant temperature high	• Use heat exchanger temperature control to adjust inlet cooler temperature
Lower	Lower reactor temperature	Poor or no reaction; poor quality product	Coolant temperature low	• Provide temperature monitoring in reactor • Use heat exchanger to adjust inlet coolant temperature
Parameter: Flow rate of ethylene, polyethylene, and initiator				
No (polyethylene)	No flow	Level buildup in reactor	Melt pump 1 fails	• Provide level control in reactor with automatic flow through a spare pump
Less (ethylene)	Less flow	System upset; product quality affected; system shutdown	Make up or recycle compressor failure	• Provide a spare compressor with automatic switch from the failed compressor
More (initiator)	More flow	More polymerizatiion; possibility of runaway conditions; product quality off specification	Initiator pump malfunction	• Provide adequate flow controls on both initiator and monomer lines to maintain the desired initiator to monomer ratio
Less (initiator)	Less flow	Less polymerization; reactor temperature imbalance affects downstream equipment such as heat exchangers	Make up and recycle gas compressor failure	• Provide flow controllers on ethylene and initiator lines

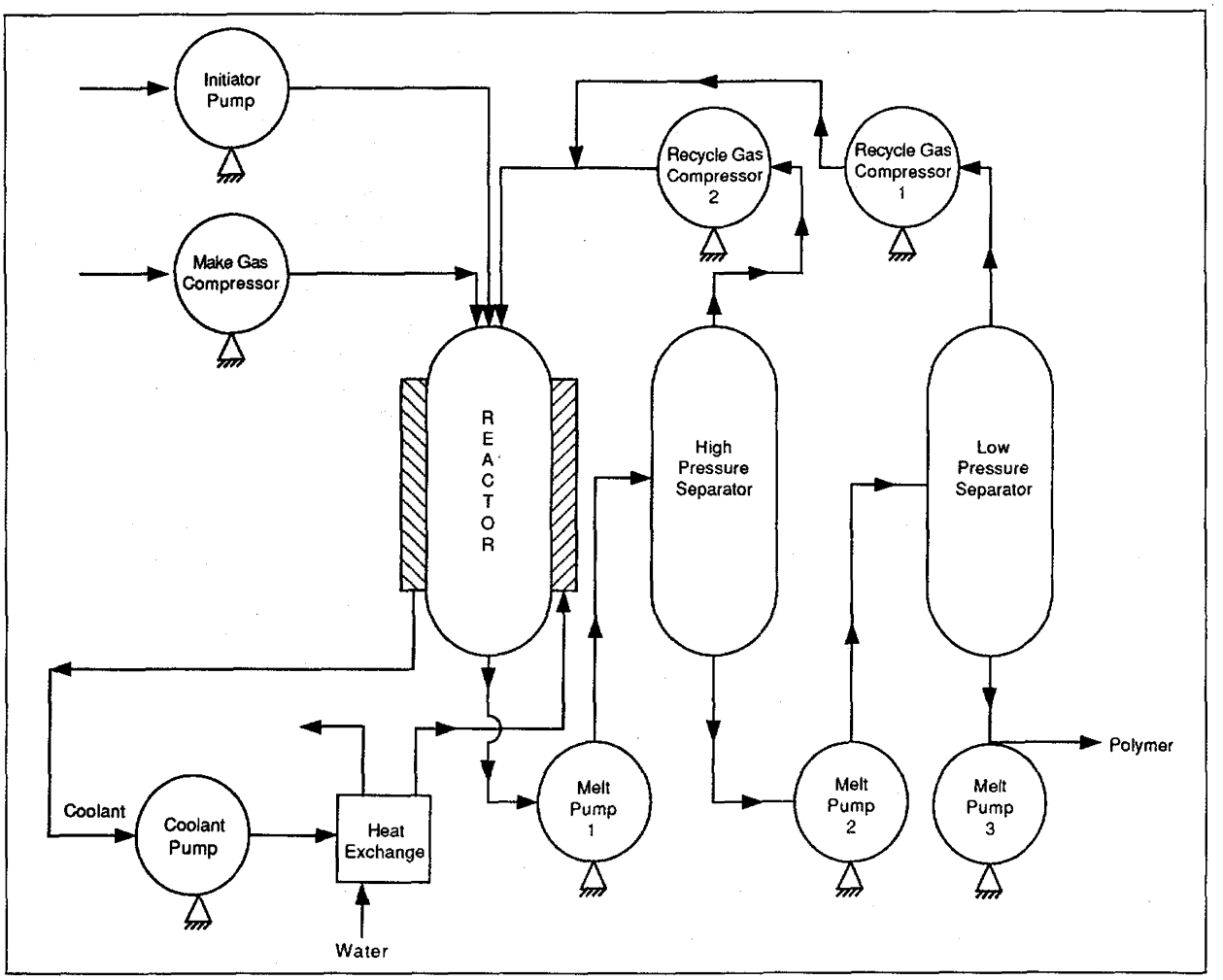


Figure VI-1. High pressure/low density polyethylene production.

are important both for quality and quantity of product as well as for safety considerations, these two areas are good candidates for study. A complete HAZOP will also contain studies of temperature in the preheat and cooling stages, the flow rate of the initiator, and the integrity of all equipment.[4]

DISCUSSION OF RESULTS

As can be noted from the case studies on polyethylene plant, both "What if" and HAZOP provide valuable insight for the safe design of a process at the preliminary stages. Although both techniques provide recommendations for a safe design, HAZOP is somewhat more organized in terms of guidelines. The analyst needs only choose all desired parameters and then apply the appropriate guide words. "What if" analysis, on the other hand, does not follow any specific guidelines and its success depends largely on the experience of the design team conducting the study.

REFERENCES

1. Moore, G.R.: Properties and Processing of Polymers, 1st ed., Prentice Hall, Englewood Cliffs, NJ (1984).
2. Rosen, S.L.: Principles of Polymeric Materials, 1st ed., John Wiley and Sons, New York, NY (1982).
3. Norsham, K., M. Kamaluddin, and D.N. Nguyen: Preliminary Hazard Evaluation of Polyethylene Plant,* School of Engineering, California State University, Long Beach, CA (1988).
4. Renshaw, L., B. Brand, and A. Roubanis: Hazard Evaluation of a Low Density Polyethylene Reactor,* School of Engineering, California State University, Long Beach, CA (1988).

*Available upon written request to the author.

Unit VII

THE BATCH PROCESS OF INDUSTRIAL AND MILITARY EXPLOSIVE PRODUCTION

PURPOSE:

To apply system safety techniques to the design of a batch process

OBJECTIVE:

To acquaint the student with the application of system safety techniques to the preliminary design of industrial and military explosive production

SPECIAL TERMS:

1. Nitrocellulose
2. Molecular weight
3. Explosion temperature
4. Velocity of wave

INSTRUCTOR MATERIALS:

1. Chalkboard
2. Student supplementary materials

TRAINEE MATERIALS:

1. Supplementary materials provided by the instructor

INTRODUCTION

Many people view explosives as chemical products used solely by the military. Although chemical explosives have been used extensively by the military for destructive purposes, many engineering projects such as constructing dams and roads and underground mining would have been impossible without their use.

Although commercial production and sales of explosives is a 20th century phenomenon, explosive mixtures, such as black powder, were known to the Chinese many centuries ago. The discovery of nitroglycerin, nitrocellulose, and dynamites in the mid-19th century formed the cornerstone for the development and use of a variety of more sophisticated and powerful explosives.

Unstable chemical compounds

Explosives are defined as unstable chemical compounds that can decompose as a result of thermal or mechanical shock. The decomposition reactions normally generate large quantities of heat and gases. When confined, the gases can exert a large amount of force on the walls of their container.[1] Table VII-1 summarizes the properties and decomposition products of some common explosive compounds.

Table VII-1
Properties of Some Commonly Used Explosives[1]

Identity	Formula	Decomposition Products	Heat Released, cal/kg	Explosion Temperature, °C	Pressure, kg/cm^2	Velocity of Wave, m/s
TNT	$C_7H_5(NO_2)_3$	H_2, CO, C, N_2	656	2,200	8,386	6,800
Trinitroglycerine	$C_3H_5(NO_3)_3$	H_2O, O_2, N_2	384	1,100	5,100	4,100
Picric acid	$C_6H_2(OH)(NO_2)_3$	CO, H_2O, H_2, N_2	847	2,717	9,960	7,000
Ammonium nitrate	NH_4NO_3	H_2, O_2, N_2	384	1,100	5,100	4,100
Nitrocellulose	$C_{24}H_{29}O_9(NO_3)_{11}$	CO, CO_2, H_2O, N_2	1,250	2,800	10,000	6,100
Gun powder	2 KNO_3 + 3C + S	N_2, CO_2, K_2S	501	2,090	2,970	NA

MANUFACTURE OF EXPLOSIVES

Chemical explosives are manufactured by a variety of processes depending on their intended use. Because of the unstable nature of these compounds, most manufacturing processes pose both physical and health hazards. In the following section, manufacture of nitrocellulose will be discussed and the preliminary hazard analysis (PHA) and "What if" analysis will be applied to a preliminary design of this process.

MANUFACTURE OF NITROCELLULOSE

The explosive properties of nitrated cotton have been known for a long time. The major problem with the use and commercialization of this compound has been its inherent instability and its rapidity of explosion. With the relatively recent discovery of stabilizing compounds and techniques to prolong its storage life, nitrocellulose has found widespread use as a military propellant.

The empirical formula for cellulose is $[C_6H_7O_2(OH)_3]_n$. Cellulose is a rather complex molecule with an average molecular weight in the neighborhood of 300,000 and a wide range of molecular weight distribution. The fundamental cellulose molecule contains three hydroxy groups that can be esterified with nitric acid according to the following reaction:

$$C_6H_7O_2(OH)_3 + 3HNO_3 + H_2SO_4 \rightarrow C_6H_7O_2[ONO_2]_3 + 3H_2O + H_2SO_4$$

In addition to nitrate esters, some sulfate esters are also formed as a result of the presence of sulfuric acid. The sulfate esters are extremely unstable compounds that could generate a dangerous acid condition in the powder storage area if not properly removed. Preventing acidic conditions in the finished nitrocellulose product is critically important because

such conditions would greatly catalyze and enhance the decomposition reactions and could lead to disastrous explosions. Normally a stabilizer, which is a compound with basic properties such as diphenylamine, is added to the finished product to neutralize any excess sulfuric or nitric acid.

THE PROCESS

Figure VII–1 shows a simplified schematic diagram of a nitrocellulose manufacturing process.

Cellulose-containing compounds such as wood, cotton liners, or pulp are boiled in a caustic solution in process vessels called kiers. The product of kiers flows into another vessel where bleaching is accomplished by compounds such as sodium hypochlorite or calcium chlorite. After bleaching, the cellulose is dried in dryers at about 105°C. The product of the dryer is fluffed and weighed; it is then fed into a nitrator where proper amount of nitric and sulfuric acids is added to the charge to carry out the nitration reactions. Normally, one nitrator charge contains 32 pounds of cellulose mixed and agitated with 1500 pounds of acid at 30°C for approximately 30 minutes.

After completion of the nitration reactions, the nitrator charge is dropped into a centrifuge where nitrated cellulose and mixed acid are separated. The spent acid is partially recovered for reuse in the nitrator and the nitrocellulose is washed with boiling water and washed again in a beater.

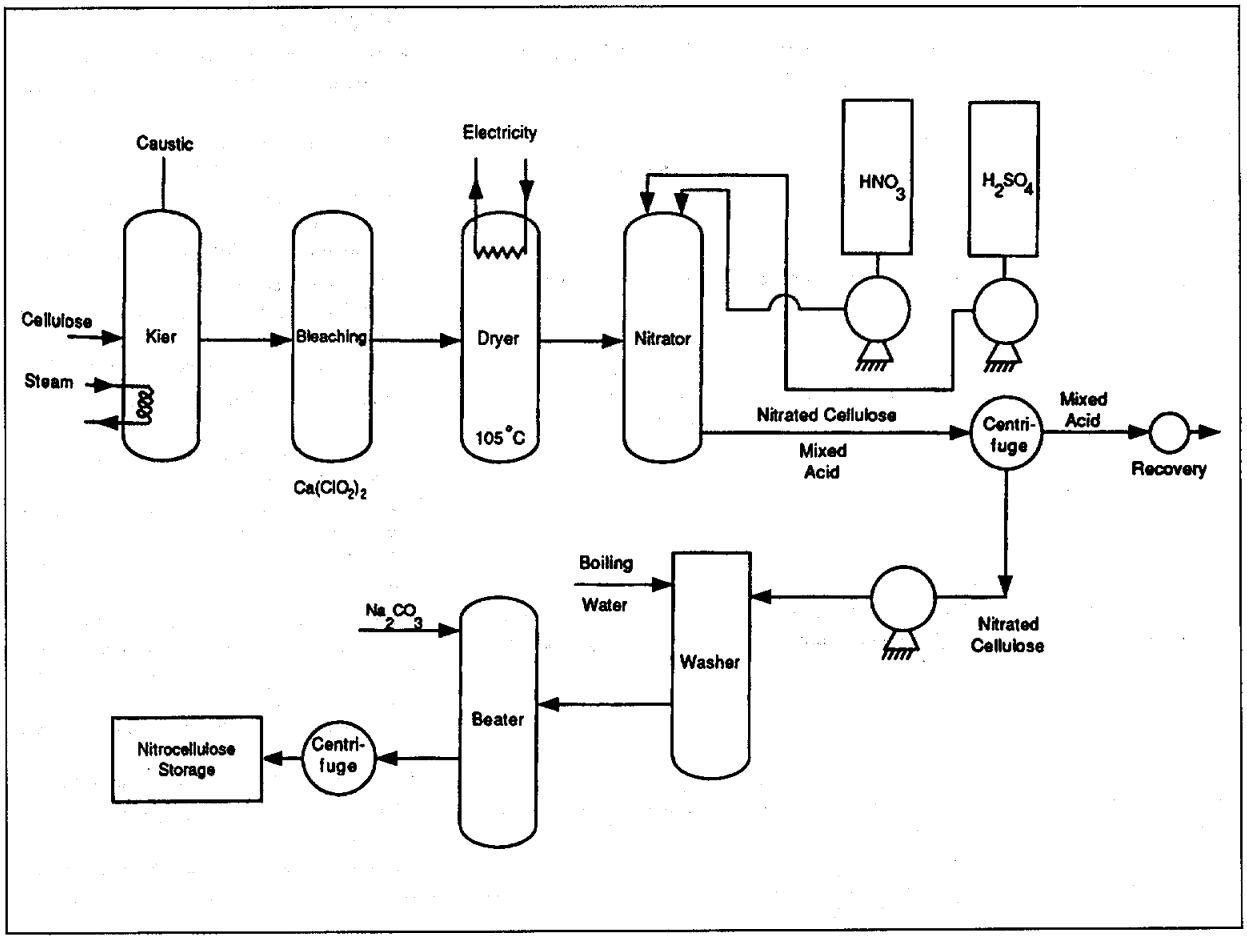


Figure VII–1. Nitrocellulose production.[1]

To neutralize the residual ester sulfates and acids, the nitrocellulose product is washed with boiling water and sodium carbonate solution. The water is then removed by a centrifuge, and the product is stored.

HAZARD ANALYSIS

Tables VII-2 and VII-3 summarize the results of a PHA and "What if" analysis of the nitrocellulose manufacturing process. As can be noted from these tables, hazard evaluation techniques can identify and mitigate the process hazards by recommending safety procedures and/or instrumentation.

REFERENCE

1. Shreve, R.N., and J.A. Brink, Chemical Process Industries, 4th ed., McGraw Hill, New York, NY (1977).

Table VII-2
Preliminary Hazard Analysis (PHA) Applied to Nitrocellulose Production

Hazard	Cause(s)	Major Effects	Preventive Measures
Explosion in storage area	Acid condition in finished product	Potential for fatality, injury	• Install sulfate and acid analyzing instrument after centrifuge • Divert flow to temporary storage with subsequent flow to centrifuge inlet
Explosion in nitrator as a result of excess acid and high temperature	Malfunction of pumps; malfunction of nitrator heater	Explosion, fatality, fire	• Install adequate flow controllers on sulfuric and nitric acid lines • Install temperature control on nitrator with a high-temperature alarm
Explosion in or downstream of the nitrator	Dryer heater malfunction resulting in high temperatures	Fire, fatality, injury	• Install temperature control on dryer with automatic shut off and high temperature alarm
Nitrated cellulose and mixed acid spill	Centrifuge	Employee exposure to hazarodous substances	• Develop procedures for using personal protective equipment (PPE) • Develop emergency and spill cleanup procedures • Install instrumentation for emergency shut off
Nitrated cellulose spill	Malfunction of centrifuge	Possible explosion, fatality, fire	• Use appropriate PPE • Develop emergency and spill response procedures • Install instruments for automatic shutoff
Acid spill from storage tanks	Leak in storage or acid lines	Employee exposure to corrosives	• Require appropriate PPE to match potential hazards • Develop procedures for storage tanks and lines inspection • Install acid monitoring devices in area; compare with PEL or TLV* • Develop procedures for general safe acid handling
Caustic spill while transferred to kiers	Pump malfunction or employee mishandling	Employee exposure to corrosives (health hazard)	• If pump used, install instrumentation to stop flow in case of pump malfunction or leak • Develop caustic handling standard operating procedure (SOP) • Develop emergency and spill response procedures • Determine appropriate PPE to be used
Nitrated cellulose spill	Pump malfunction or mishandling from centrifuge	Explosion, fire, fatality	• Install instrumentation to detect, alert, and correct malfunction • Develop SOPs for handling and spill response

*PEL = permissible exposure limit; TLV = threshold limit value.

Table VII–3

"What if" Analysis Applied to Nitrocellulose Production

"What If"	Consequence/Hazard	Recommendation
There is excess sulfate and acid in finished product?	Explosion; fire; fatality	• Analyze for excess sulfate and acid before storage • Install flow controllers on acid lines or develop proper acid handling procedures • Develop emergency response procedures
Pump malfunctions or acid is handled improperly?	Acid condition in product; personnel exposure to health hazards	• Install flow controllers on acid lines, or develop adequate acid handling and charging procedures • Develop emergency and spill response procedures
Centrifuge malfunctions?	Nitrocellulose spill/explosion; fire; fatality	• Install appropriate instruments to shut off equipment in case of a malfunction • Develop emergency and spill response procedures in case of a malfunction and spill
The acid storage tanks leak?	Personnel exposure to health hazards	• Develop procedures for acid storage tank inspection • Install acid monitoring instruments • Develop spill clean up procedures
The caustic line leaks or pump to kiers malfunctions?	Caustic spill; personnel exposure to a corrosive health hazard	• Install instrumentation to detect/alert caustic leaks and stop the flow of caustic to kiers • If caustic handled manually, determine appropriate personal protective equipment and develop handling procedures • Develop emergency and spill response procedures

Unit VIII

INSTRUCTOR'S GUIDELINES

IMPORTANCE OF INCORPORATING SYSTEM SAFETY TOPICS INTO SENIOR LEVEL DESIGN PROJECTS

Unsafe conditions and acts

Thousands of industrial injuries occur throughout the United States everyday. Most are caused by the failure of people, equipment, supplies, or surroundings to behave or react as expected. Data published by the National Safety Council reveal that 98 percent of all industrial accidents are caused by unsafe conditions and unsafe acts. Natural disasters have been responsible for 2 percent of industrial accidents. Lack of attention to safety topics at the design stage of a process would undoubtedly create inherent unsafe conditions in the process—conditions that can lead to disastrous accidents.

Role of design engineer

As technology is mobilized to respond to society's ever-increasing demands to improve the quality of life, new dimensions must be added to the role of the design engineer to accomplish this task in an occupationally and environmentally safe manner.

Occupational and environmental laws

The public's reaction to unsafe design and operation of industrial processes has manifested itself in the form of strict occupational and environmental laws in recent years. Although the public has pressured industry to ensure that their interests are incorporated into design, operation, and waste disposal of industrial processes, this pressure has not been transmitted proportionately to the engineering schools responsible for educating future engineers and, in part, for the continuing education of practicing engineers.

Engineering schools

Traditionally, engineering schools have done a superb job of educating their students on the fundamental laws of nature governing their fields and on the application of these laws to engineering problems. They have been less successful, however, in conveying to the students the importance of occupational and environmental safety in the design process and the criticality of legal as well as moral responsibilities of the engineer to society.

Student training

It is not uncommon for senior-level graduating engineers to think only in terms of the technical aspects of the profession with little or no thought given to the issues of safety and environment in the design process. When these graduating engineers join industry do they find out that safety and environmental issues are real problems to be dealt with and that they have little or no training in these areas. Although some companies have made a commitment to train their young engineers in the occupational safety and health and environmental problems, not all young engineers are lucky enough to work for those companies; many end up working for companies which have a rather poor safety record and, with no academic training in these areas, end up learning about safety and environmental problems through trial and error and unnecessary, senseless accidents.

It can be seen that it is unreasonable to attempt to convey any safety or environmental training to the graduating engineer when food and beverages are allowed in chemical laboratories and when, due to lack of a system, dangerous chemicals are poured down a laboratory sink.

It is time for our engineering schools to take a more responsible position in regard to occupational safety and environmental health problems. Unless safety and health is regarded as a science and is incorporated into the engineering curriculum in a systematic manner, it can easily turn into "lip service" with no meaningful results.

Senior level design project

The senior level design project is the perfect opportunity to introduce system safety. Hazard evaluation procedures should be discussed. The students can apply one or more of these methods to portions of their design project. This will also give the student the appreciation for the time and effort that go into such analyses. In addition, students should recognize the cost-saving factors for identifying, reducing or eliminating hazards at the design stage rather than after implementation. Students in design courses have enough core knowledge of processes to understand, at least fundamentally, the repercussions of system safety. For these reasons hazard evaluation procedures and system safety topics should be addressed in all senior level design projects.

EDUCATIONAL OBJECTIVES

System safety in design project

Incorporation of system safety topics into the senior level design courses can accomplish several goals. The graduating engineer realizes (maybe for the first time) that in order to make a process both economical and operable, safety and environmental issues must go hand in hand with the technical aspects of the project. The student also can develop an appreciation of legal as well as moral responsibilities of the engineering profession. Incorporation of system safety topics into the preliminary design projects can also give the student the minimum tools required to apply the scientific laws of nature to design and operation of hazardous technologies in an occupationally and environmentally safe manner.

Systematic approach to workplace hazards

System safety provides a thorough systematic approach with which to address workplace hazards. Due to complexity of production, construction, and processes, informal hazard evaluations are no longer sufficient; a systematic approach is more economical and results in more complete analyses. A thorough assessment of risks inherent to a process can minimize losses due to down time and worker injury. In addition public intolerance of dangerous failures and accidents is a reality. Stricter requirements are more likely to be met by utilizing a systematic hazard evaluation approach.

System definition

The system safety approach begins with defining the system to be studied; allowing for human, equipment, and environmental interactions. The scope and depth of the study are determined; the prime factors in this determination include the projected cost of analysis, schedule deadlines, and available human resources. Safety hazards are then identified; these hazards can be the result of equipment failure, human error, environmental conditions, or any combination of these.[1] After identification of hazards, decisions must be made as to whether or not the related risks are acceptable. If the risks are not acceptable, plans to reduce or eliminate those risks are identified and analyzed for efficiency, cost, and workability.

SYSTEM SAFETY AS AN INTEGRAL PART OF DESIGN PROCESS

The techniques of system safety can be applied to design and risk assessment of any process and/or operation. These procedures are independent of the nature or type of process or operation and can easily be applied to minimize risks.

Risk assessment

Identifying hazards at design stage

The first risk assessment effort must be made at the design stage. Risk reduction is far less costly before equipment is in operation. Once the process is in operation, hazard abatement may be carried out through safety devices or isolation of the hazard; however, addressing the hazard at the design stage could make it possible to entirely eliminate the risk before the plant is built. Identifying and presenting hazards at the design stage saves time and money by reducing the need for equipment modification, down time, and litigation costs. The design engineer for any process must recognize his moral as well as legal responsibility and his obligation to incorporate systematic hazard evaluation into the design process.

ABET requirements

The Accreditation Board for Engineering and Technology (ABET) requires that engineering graduates understand the engineer's responsibility to protect both occupational and public health and safety. For example, release of a toxic gas from a highly toxic hazard material storage tank can pose a severe environmental problem. The system safety techniques can easily be applied to design a storage tank that would minimize the risk of toxic gas release.

Table VIII-1 summarizes the application of PHA to a highly toxic hazardous material (HTHM) storage facility. This analysis identifies the hazard, its cause, and consequences. Additionally, possible preventative and corrective measures are suggested.[2]

Table VIII-1

Application of Preliminary Hazard Analysis (PHA) to a Highly Toxic Hazardous Material (HTHM) Storage Tank

Hazard	Cause	Major Effects	Corrective/Preventive Measures
Release of toxic gas	Rupture in storage tank	Fatalities; injuries	• Improve tank materials of construction
Release of toxic gas	Fire in tank farm; explosion of storage tank	High release of gas into the community; fatality	• Prepare community • Develop fire prevention techniques, and install fire control equipment in tank farm
Release of toxic gas	Collapse of tank foundation due to earthquake	High release of gas into the community	• Site down wind • Improve structural design of foundation
Release of toxic gas	Rupture in main transfer line	High release of gas into the community	• Install gas analyzer with automatic diversion of flow • Minimize piping
Release of toxic gas	Leak in line or from tank	High release of gas into the community	• Install toxic gas analyzer

REFERENCES

1. Kavianian, H.R., C.A. Wentz, R.W. Peters, and L.E. Martino: Total Concepts in Safety Systems Management for Hazardous Materials Handling and Design of Hazardous Processes, Annual Loss Prevention Symp., AIChE Spring 1989 National Meeting, Houston, AIChE, New York, NY (1989).
2. Little, A.D., and R. Levine: Guidelines for Safe Storage and Handling of High Toxic Hazard Materials, Center for Chemical Process Safety, AIChE, New York, NY (1988).

EXERCISES

1. A flammable liquid storage facility contains one-hundred 55-gallon drums of gasoline with a flash point of −40°F. Assuming that all electrical devices are of the approved type, construct a fault tree diagram depicting all the possible scenarios that can lead to a fire in the storage area.
2. In a hazardous waste site, the cleanup crew uses highest level of protection with self contained breathing apparatus (SCBA). Perform a preliminary hazard analysis (PHA) to identify the failure modes for the SCBA and recommend procedures, equipment, and/or instrumentation for preventive measures.
3. As part of a feasibility study for commercialization of the metal organic chemical vapor deposition (MOCVD) process, it is necessary to determine the system failure modes and their effects on personnel, community, and equipment safety. Perform a hazard and operability (HAZOP) analysis using the reactor temperature as the selected parameter.
4. A high pressure/low density polyethylene plant is operating under 1500 atmospheres and 300°F. Perform a fault tree and event tree analysis (FTA and ETA) for the possibility of a runaway reaction in the polymerization reactor. Combine the FTA and ETA into a cause-consequence diagram.
5. You are the process engineer in charge of operating an HF alkylation unit in a petroleum refinery. The acid catalyst is stored in a 5000-gallon tank from which the catalyst is pumped to the unit for use as make-up catalyst. Perform a "What If" analysis on the acid storage tank; concentrate on the different ways that an acid leak can occur. Discuss the occupational safety and environmental health effects of such a leak, and recommend procedures, equipment, and/or instrumentation to minimize risks.
6. In a chemical laboratory, which is located on the fourth floor of a heavily populated building, several bottles of chemicals are stored in wooden cabinets. The 25- by 25- by 15-foot laboratory is used by 18 students at a time to perform their chemistry experiments. During a recent inspection, it was discovered that nitric acid (an oxidizer and corrosive), methyl ethyl ketone (an organic peroxide), and a petroleum derivative with a flash point of −25°F are stored together in one of the cabinets. Perform a preliminary hazard analysis (PHA) to identify the possible accidents that can occur. Discuss the effects of each accident, and recommend procedures, equipment, and/or instrumentation to minimize risks.
7. In an industrial operation, two workers are responsible for running parts through a caustic tank that generates corrosive vapors at concentrations much above the threshold limit value (TLV). Perform a preliminary hazard analysis (PHA) to identify the physical and health hazards associated with this operation. Your analysis should result in recommendations for engineering controls to reduce the concentration of corrosive vapors to below the TLV value and appropriate personal protective equipment for worker safety.
8. In an ethylene plant, ethane is used as feedstock in pyrolysis reactors located inside a furnace operating at 1500°F. Perform a preliminary hazard analysis (PHA) and a failure mode effect and criticality analysis (FMECA) on the reactor tubes and furnace assembly. Your analysis should identify any safety instrumentation devices (such as flow controllers, temperature controllers, etc.) that might be needed for the safe operation of the heaters. Draw a simplified diagram of the heater assembly (with reactors inside), and mark any instrumentation required on the diagram.

GLOSSARY OF TERMS

ALKYLATION: the chemical reaction between a low molecular weight olefin and isobutane to produce gasoline.

CAUSE-CONSEQUENCE ANALYSIS: a system safety technique which combines fault tree and event tree analysis.

EVENT TREE ANALYSIS: a system safety technique that concentrates on an initiating event and proceeds forward to find possible consequences.

EXOTHERMIC REACTION: a chemical reaction that results in generation of heat.

FAILURE MODES EFFECTS AND CRITICALITY ANALYSIS: a system safety technique that concentrates on equipment and system failures and their effects.

FAULT TREE ANALYSIS: a system safety technique that visually demonstrates how an undesired event can take place.

HAZARD AND OPERABILITY: a system safety technique that concentrates on hazards created as a result of deviation of plant parameters from their intended design value.

LC_{50}: the dose of a chemical that has lethal effect on 50 percent of test animals when administered through inhalation.

LD_{50}: the dose of a chemical that has lethal effect on 50 percent of test animals when administered orally or on the skin.

METAL ORGANIC CHEMICAL VAPOR DEPOSITION: a process for production of photovoltaic thin films.

PEL: permissible exposure limit for air contaminant as set by OSHA.

POLYMERIZATION: the combining of relatively low molecular weight molecules into a high molecular weight compound.

PRELIMINARY HAZARD ANALYSIS: a system safety technique concentrating on cause, effect and means of control of a hazard.

PYROLYSIS: break down of a molecule by thermal energy.

PYROPHORIC GAS: a gas that can catch fire on contact with air in the absence of a source of ignition at temperatures below 130°F.

REL: recommended exposure limit for air contaminant as developed by NIOSH.

RELATIVE RANKING PROCEDURE: a procedure for assessment of risks in processing plants by assigning credits and penalties to different features of a plant.

RISK EVALUATION: a determination of the amount of risk using probability and severity of an accident.

RUNAWAY REACTION: an exothermic reaction continuously accelerated by the reaction heat effects.

SAFETY FUNCTION: a feature built into a process for safety purposes, e.g., a relief valve.

TLV: threshold limit value recommended by American Conference of Governmental Industrial Hygienists (ACGIH).

TOXIC CHEMICAL: a chemical that can result in adverse health effects in humans at relatively small doses.

"WHAT IF" ANALYSIS: a system safety technique which addresses hazards by asking questions which start with "what if. . . ."

SELECTED BIBLIOGRAPHY

American Chemical Society Committee on Chemical Safety, *Safety in Academic Chemistry Laboratories,* Washington, DC (1990).

Bretherick, L., *Handbook of Reactive Chemical Hazards,* Butterworth's, London-Boston (1979).

Brown, D., *Systems Analysis and Design for Safety,* Prentice Hall, Inc., Englewood Cliffs, NJ (1976).

Crone, H., *Chemicals and Society,* Cambridge University Press, London, England (1986).

Engineering Control Technology Workshop Panel, *Engineering Control of Occupational Safety and Health Hazards,* U.S. DHHS (NIOSH) Publ. No. 84-102 (1984).

Ferry, T.S., *Safety Program Administration for Engineers and Managers,* Charles C. Thomas, Publisher, Springfield, IL (1984).

International Labour Office, (ILO), *Occupational Exposure Limits for Airborne Toxic Substances,* Geneva (1980).

Lewis, R.J., *Hazardous Chemical Desk Reference,* Van Nostrand Reinhold Co., New York, NY (1990).

Mendeloff, J., *Regulating Safety: An Economic and Political Analysis of Occupational Safety and Health Policy,* MIT Press, Cambridge, MA (1979).

Nouhi, A., and R. Stirn, *Heteroepitaxial Growth of Cdrx Mnx Te on Ga As by Metal Organic Chemical Vapor Deposition,* Journal of Solar Cells, 21:225-232 (1987).

O'Riordan, T., and W. Sewell, *Project Appraisal and Policy Review,* John Wiley & Sons, New York, NY (1981).

Sax, N., and R. Lewis, *Dangerous Properties of Industrial Materials,* Van Nostrand Reinhold Co., New York, NY (1988).

☆U.S. GOVERNMENT PRINTING OFFICE: 1992-648-004/40828