Fault Tree Synthesis for Chemical Processes

This paper outlines the concepts for a systematic approach to the safety analysis of chemical processing systems. A procedure for automatically generating fault trees is presented. The fault trees describe nearly all the failure modes for the system under analysis. The fault tree generation procedure uses information on (1) the description of the system (detailed flowsheet), (2) physical and chemical properties of materials in and around the system, and (3) unit models which describe the behavior of the units within the system and which are assembled to describe the behavior of the complete system. The unit models are connected to form an information flow structure for the complete processing system. Unit failure models are also defined for common chemical units. By systematically defining hazard states and searching the information flow structure for the system, it is possible to generate fault trees for the complete process. An analysis of the fault trees can reveal the important failure modes for the process.

GARY J. POWERS
and
FREDERICK C. TOMPKINS, JR.

Department of Chemical Engineering
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

SCOPE

The safety of chemical processing plants is becoming increasingly important as they become larger and more complex. The chemical industry has had an admirable safety record over the past 20 years. This record has been achieved by concerned designers, plant managers, and operators who made safety an integral part of their professional activities. Within the last ten years several trends have been set which severely test our current methods for insuring the safety of chemical plants. The primary thrust of these trends is to build large, single-train plants with integrated energy recovery networks and rather complex centralized control systems. In addition, these plants are often located closer to population centers. The added complexity of these modern plants requires more rigorous techniques for assessing their safety and reliability. In this paper we present several systems safety techniques developed in the aerospace industry and indicate how they might be applied in the chemical process industries. The most used analysis methods are Failure Modes and Effects Analysis (FMEA) and Fault Tree analysis. The FMEA technique is a formalized system for asking "what if?" questions related to the safety of the process. Component failures such as valves leaking, pump failure, power failure, and operator error are hypothesized and the possible adverse effects on the system are determined by investigating how the system responds to each failure and failure combination. The Fault Tree method takes a different approach to determining the safety of a system. The most undesirable events (such as explosion, fire, etc.) which could occur within a system are defined and the system is then searched for failures that could lead to these events.

Both of these methods have been successfully applied to aerospace and electronics problems. Their application to chemical plants has been less frequent. The main reasons for the chemical industry not adopting these methods are:

1. Until recently our systems were not complex enough to warrant these approaches. Informal techniques were able to discover most of the hazardous failure modes.
2. Chemical processing systems are remarkably robust. Even when several unit failures have occurred the total process does not fail completely.
3. The consequences of failure often mean that the plant is shut down and may be restarted. In aerospace applications the systems appear to be more inherently sensitive to failure and the consequences of failure more spetacular.
4. The inherent hazards in most of the chemical industry are due to the reactivity of the chemicals being processed. The prediction of the behavior of these chemicals under a wide range of conditions is difficult. Hence, a great deal of uncertainty surrounds the definition of hazards.
5. The behavior of chemical processing systems is not easily predicted. Current chemical process models are time-consuming to formulate and often times difficult to solve. The models are usually formulated for one operating condition and do not predict aberrant behavior under extreme conditions.
6. It takes a long time, months and often times years, to generate high quality FMEA's or Fault Trees for chemical plants.

These six reasons have contributed to the lack of use of more rigorous methods for the safety analysis of chemical plants. The trends of increased plant complexity and larger process size have partially negated the first three reasons given above. With this new challenge it is desirable to develop techniques to overcome the last three problems.

In this paper we focus on the last two problems: (1) describing the behavior of chemical plants with simple models suited to safety analysis and (2) developing rapid means for performing high quality safety analyses of complex chemical processing systems.

CONCLUSIONS AND SIGNIFICANCE

It is possible, using information flow models, to describe simply the behavior of chemical processing systems so that rapid safety analysis of these systems can be performed. A procedure for carrying out the fault tree analysis of a

general chemical process has been developed and programmed for testing on a digital computer. The analysis asks for information pertinent to the chemical plant under analysis. Information is required to:

1. **Describe the chemical process, that is, a detailed flowsheet,**
2. **Determine the properties of the chemical species in and around the process, so that hazards can be identified,**
3. **Assess the probabilities of occurrence of certain primal events, that is, valve failure, pump failure, operator error, etc.**

Given this information the procedure uses information flow models developed for common processing units such as reactors, separators, pumps, heat exchangers, etc. to trace out failure pathways which lead to hazardous events. Failure models for each process unit predict ways that the units must fail in order that the final hazard is achieved.

The system is currently being tested on several existing chemical plants and has successfully revealed significant failure modes undetected by current safety review methods.

The significance of this work is that a systems approach to chemical plant safety analysis appears to be feasible. The analysis procedures, if programmed for digital computers, can be performed very accurately, completely, and quickly. This analysis capability allows the system designer or plant superintendent to screen quickly a wide range of possible process failure modes to determine which are significant. The fault trees generated via this technique are also an effective way of documenting and communicating the safety related behavior of a process. Finally, this approach portends a more rigorous approach to safety problems which may allow educators to teach safety and reliability analysis methods more effectively.

Several trends have been set in the past decade that indicate the need for more rigorous methods for safety analysis of chemical plants. These trends are:

1. Increasing preponderance of single train installations
2. Larger processing units
3. More complete process integration for energy recovery and waste recycling
4. Reduction of intermediate storage capacity
5 Centralization of control
6. Growth of computer based operations
7. Multiplexing of equipment
8. Location of plants closer to population centers.

Implicit in these trends is the increased profitability associated with economies of scale, tighter control of plant operations, and reduced transportation costs.

Also implicit in these trends are the use of complex, integrated control strategies designed for more economic operation near inherent process constraints; increased demands on operator competence; on-stream maintenance policies to avoid costly process shut-down; and increased frequency of computer based, on-line process optimization studies.

The total capital investment per plant has greatly increased in line with economies of scale; however, this has been accompanied by an increased potential for large losses if a serious process failure should occur.

The implications of process failure have a wider ranging impact than economic losses to a particular plant. With increases in plant size and complexity, there is a concomitant increase in the potential for pollution in the event of process failure. The growing evidence of environmental degraduation has resulted in stiffer pollution control regulations and general concern that preventative measures be implemented. Another aspect of the above trends is the increased likelihood of injury to both workers and the public in the event of major failures, and public awareness of this fact (Katz, 1970). A prime illustration is the increased public resistance to the siting of nuclear power stations near population centers where operation is most economically attractive (Kendall, 1972). Not only is there a moral prerogative to ensure public and worker safety, but enactment of legislation (witness the Occupational Safety and Health Act) makes safe practices mandatory.

Concern over the loss potentials associated with large, single-train plants has caused insurance costs to increase rapidly and was a factor in the withdrawal of London underwriters from the U.S. chemical market (Kuist, 1970). The result has been a demand for plant design and operation that will minimize business interruptions and losses.

APPROACHES TO FAILURE PREVENTION

Within the context of the above discussion, what are the approaches that may be taken to prevent the occurrence of process failures? Although on the detailed level there may be as many different techniques as there are organizations pursuing active failure prevention programs, on a conceptual basis only two categories are necessary: the protective systems approach; and the systems safety approach.

Protective Systems Approach (Powers, 1973b)

The orientation of the approach is basically that of disaster limitation. It is an external, after-the-fact point of view which assumes the existence of process failure and attempts to reduce consequences of the failure. Obvious examples of protective systems are sprinkler systems, fire walls, emergency cooling systems, explosion limiting devices, etc. Protective devices are an integral part of any processing system where the consequences of failure are serious (involving potential injury or large economic losses) even though the probability of occurrence may be low.

Systems Safety Approach

In contrast to the protective systems approach, the systems safety approach involves an internal, preventative viewpoint. The objective is to determine the possible failure pathways within the processing system and its environment and, through redesign or changes in operating procedure, to reduce the probabilities of occurrence of the failure pathways to acceptable levels. In practice, of course, both approaches will invariably be applied together for any processing operation of consequence. The focus of this investigation is along the lines outlined for the systems safety approach.

Economic Considerations

No process exists with zero probability of failure, and cannot in principle exist, except under zero production capability conditions as long as components of the system have finite failure probabilities. However, expenditures

may be made to reduce the probability of failure to very low values. Just how much the expenditure should be depends on the costs and benefits for the system. The cost-effectiveness approach is most often utilized to decide upon the failure prevention measures that will be taken (Recht, 1966). Under this approach, the gain in overall system performance is weighed against the cost of implementing the failure prevention measures, and only those measures will be taken whose benefits outweigh the cost involved. From the point of view of economic theory, investment in increased reliability and protective systems will be undertaken until the marginal utility of the investment equals the marginal cost involved (Rudd, 1968). In order to make the most intelligent decisions as to how to invest in process reliability, one must have a quantitative framework consisting of the possible failure pathways, the associated probabilities, and the possible consequences of failure. An objective of this paper is to assist in providing this framework.

FAILURE ANALYSIS

Traditional CPI Approach

Although it should now be apparent that failure prevention is becoming increasingly important, the continuing incidence of process failures ranging from disasters to near misses (Buehler, 1970; Carpenter, 1964) indicates substantial room for improvement in current procedures. A commonality among many failures, particularly those of the more disastrous nature, is the occurrence of an unforeseen failure mode (Browning, 1969; Katz, 1970) which was proven significant after the event. A brief examination of the traditional approach towards safety and reliability with the CPI will help to identify the inherent weaknesses which allow the existence of unspecified failure pathways and provide a basis upon which improvements may be suggested.

Until recently, a quantitative framework within which to perform safety and reliability analysis had not existed. The approach to identification of failure pathways and consequences has been largely intuitive (Powers, 1973a): a design or safety engineer will examine a process flowsheet and, based upon experience, ask "what if" a particular component fails in a specified manner (Williams, 1970) and attempt to determine the relevant failure pathways. This approach, unfortunately, is not guaranteed to consider all failure modes, and the result is that the correct failure prevention measures are often taken only after a failure has occurred.

Failure Analysis Requirements

The foundation upon which effective failure prevention is based is that of complete, rigorous failure analysis. If it is known that an undesirable event can occur with a finite probability, and the event sequences leading from initial failures are identified, steps may be taken such as redesign or changes in operating procedure to lower the probability of occurrence to acceptable levels. The general requirements for a rigorous analysis are the following (IEEE, 1972; Ostrander, 1970; Powers, 1973a):

1. All failure pathways must be identified.
2. Probabilities must be calculated for each pathway.
3. The consequences of each final failure event must be identified.
4. The critical failure modes must be determined through the joint consideration of probabilities and consequences.

There are two major implications inherent in the above requirements. First, the analysis must take a systems orientation; that is, all interactions among individual components, subsystems, the entire system, and its environment must be taken into account. Second, a systematic, formalized methodology must be developed which will provide the analysis framework for consideration of a general processing system. Performance of such an analysis requires the following information:

1. A detailed process flowsheet or equivalent description
2. The normal mode of operation
3. The current state of the process
4. The properties (chemical and physical) of all materials within and around the system
5. A description of the system behavior (steady state and dynamic)
6. Event probabilities

Two safety analysis procedures which have found extensive use in the aerospace and nuclear field are discussed in the following section.

FORMALIZED METHODS

Experience in Other Industries

The formal development of the systems safety approach was initiated in the aerospace industry (Crosetti, 1971; Recht, 1965). It developed as a natural outgrowth of the consideration of possible failure consequences: malfunction of a complex missile or aircraft system could result in widespread loss of life and the cost of millions of dollars. It was imperative that potential failures be identified apriori. Both the nuclear power and electronic industries were quick to implement the aerospace developments: the former because of the disaster potential associated with major nuclear reactor failures and the latter due to the complexity of many electronic devices (for example, digital computers). To date, however, the CPI has been slow to take advantage of the substantial body of experience available in other industries. Although many different names are applied to the techniques developed for systems safety analysis, all appear to have been developed from the basic concepts of only two: Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis.

Failure Mode and Effects Analysis (IEEE, 1972; Garner, 1970; Recht, 1966)

In its barest essentials, FMEA is simply a formalization of the traditional "what if" approach alluded to earlier. The key word is formalization, implying a standard methodology which can be applied to complex systems. The technique involves the following steps:

1. Identification of all individual system components
2. Determination of all failure modes for each component
3. For each failure mode, determination of the effects on other system components
4. Identification of the overall effects on performance of the system
5. Estimation of the seriousness of the specific failure.

One or more simultaneous component failures are handled in the same fashion. The key feature is that the logical information flow begins with component failure and works toward the final hazard event(s), considering the system as an entity.

Fault Tree Analysis

The development of fault tree analysis in 1962 (Recht, 1965) provided an increased dimension to the systems safety approach to failure prevention. As implied by the terminology above, the basis for the technique is the fault

tree. Briefly, the fault tree consists of a logic diagram which identifies all event sequences which can lead to a specified failure event (explosion, fire, etc.). The methodology involved in the analysis is the following:

1. A failure event of interest is specified.
2. The seriousness of this failure event is estimated.
3. Within the context of the processing system and its environs, the immediate precursor events are identified.
4. The generation of precursor events is continued until primal (initiating) failures are encountered.
5. Probabilities are assigned to primal events and through use of the algebra of logic, the probability of the final failure event is calculated.

As contrasted with FMEA, fault tree analysis establishes the logical information flow from the final event to the initiating event(s), again within the framework of the total system.

FMEA vs Fault Tree Analysis (Crosetti, 1970; IEEE, 1972; Powers, 1973b)

The critical difference between these methods is the direction in which the analysis is performed: FMEA involves generation of event sequences from initiating events to final events, while fault tree analysis begins with the final event and works backwards to initiating events. Fault tree analysis has a distinct advantage in that only event sequences leading to failures of interest are considered. FMEA, on the other hand, does not guarantee that the propagation of a specific component failure will result in a final event of interest. In fact, to guarantee that all interesting final failures are considered, all combinations of initiating (primal) events must be investigated. For a complex system, the time requirements to generate all such event sequences would be prohibitive, even given the use of high speed computers.

Through consideration of the smaller number of events leading to a specific failure, fault tree analysis can be quantified where data are available on failure probabilities of primal events. Unless an exhaustive FMEA has been carried out, quantification of event probabilities loses meaning, for there is no guarantee that all failure pathways leading to a particular event have been considered.

Given the above comparisons, fault tree analysis has been chosen to provide the conceptual framework for chemical process safety analysis. In actual practice a hybrid method is used. The fault tree guides the overall search for failure pathways and failure modes and effects is used to fill in parts of the path.

FAULT TREE-QUALITATIVE ASPECTS

As the term is generally used in the aerospace industry, fault tree refers to event sequences leading to a significant failure such as loss of mission where there exists potential for injury of personnel and/or large economic losses. For chemical processing systems a broader implication is desirable to include less significant (but still interesting) failures (for example, off-specification product). Henceforth, the term fault tree will both be used to signify the more general class of failure.

Logical Properties of Fault Trees

The fault tree is a graphical representation of the logic which describes information flow (in this case failure propagation) in the processing network. The basic building blocks of the fault tree consist of the logical interconnections among event sequences, known as logical gates. A logical gate defines the input conditions which must be met in order for a failure sequence to propagate up the fault tree toward the final failure event at the top node. There are two basic logical gates, (although more may be defined under certain circumstances (Hill, 1968)): the "and" gate; and the "or" gate. The "and" gate provides an output event if, and only if, *all* the input events are simultaneously present. The "or" gate transmits an output event if *one* or *more* of the input events are present. Figure 1 gives the symbolic representation of each logical gate with accompanying truth tables. Fussell (1973a) presents a more detailed discussion of the properties of fault trees.

Figure 2 presents the instrumentation and flow schematic of a hypothetical process due to Browning (1972). The explicit assumption is that flow regulation of the feed is used to control the reaction temperature of a highly exothermic reaction. At X + 20°, it is assumed that the reaction will run away with catastrophic results. Protective instrumentation is designed to shut off all flow of feed at X + 10°. Figure 3 illustrates the fault tree for the final event temperature hazard-reactor. On the diagram, primal events (basic initiating events) are represented by circles and resultant events (primal event combinations using "or" and "and" logic) are represented by rectangles.

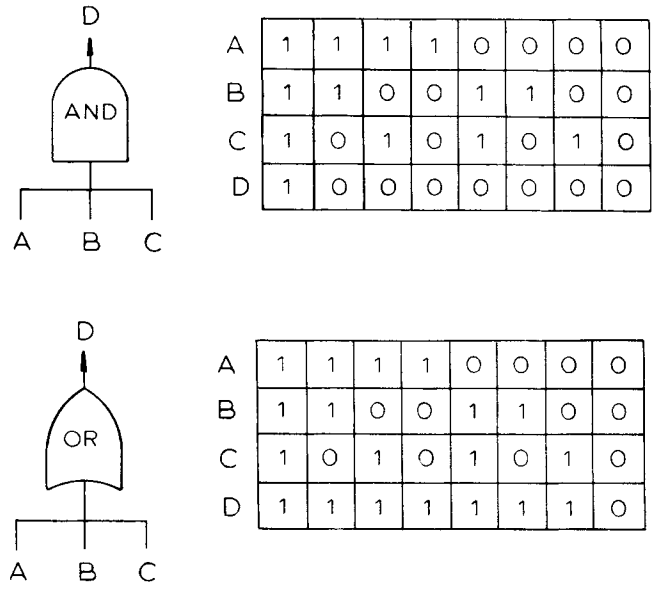


Fig. 1. Symbols and truth tables for AND and OR gates.

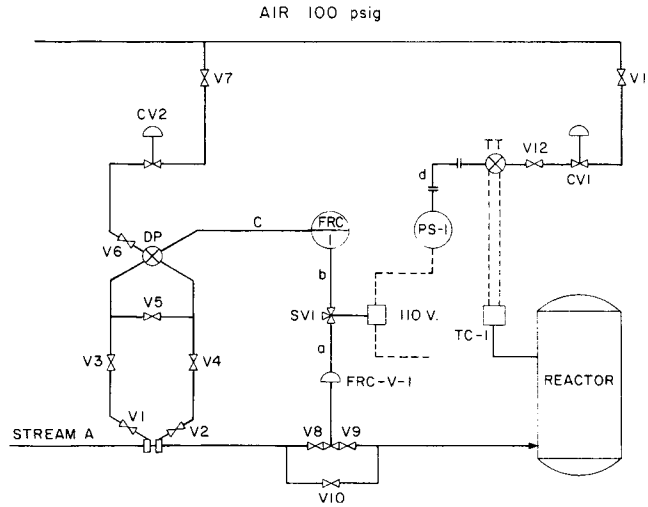


Fig. 2. A reactor and control system for a potentially dangerous reaction. (Browning, 1972).

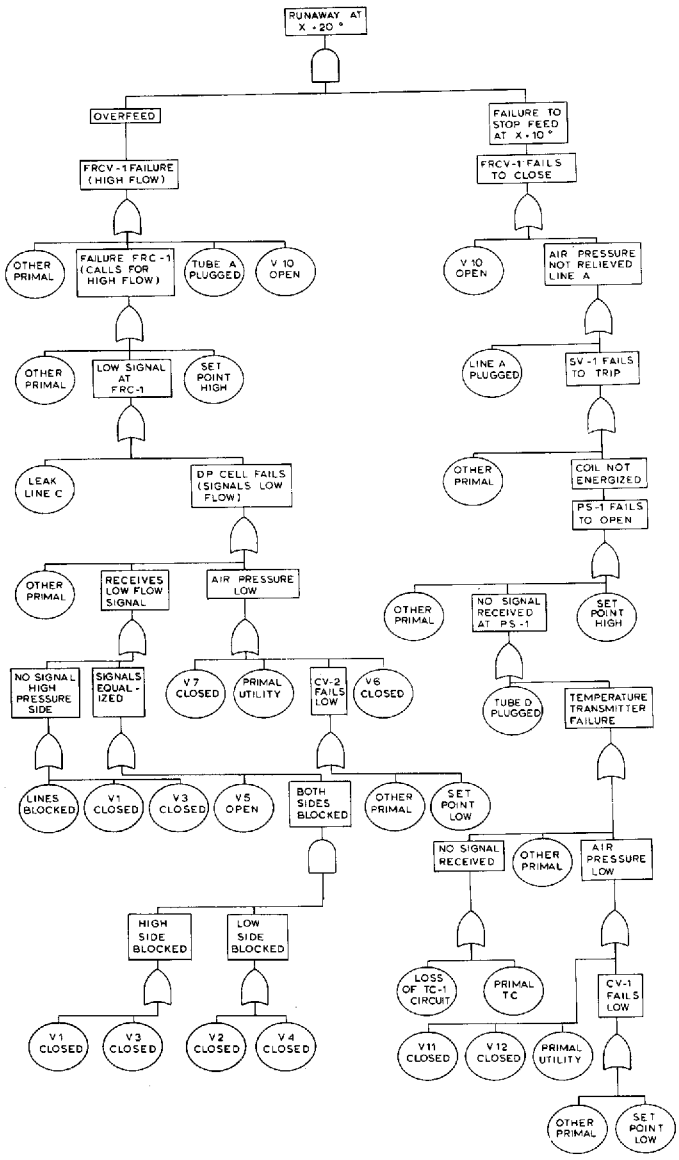


Fig. 3. A fault tree for the system shown in Figure 2. The hazardous event is explosion of the reactor.

Fault Tree Generation: State of the Art (IEEE, 1972; Kay, 1966; Powers, 1973b; Patterson, 1968)

Given the apparent power of fault tree analysis, it may appear strange that the technique has not been adopted wholeheartedly by the CPI. A brief consideration of the current state of the art indicates the reason: there exists no automated, systematic methodology for fault tree generation in the chemical process industry. Fussell (1973) has developed a method for generating fault trees for electrical circuits. Fault trees are currently generated by hand, an arduous task when one considers the combinatorial aspects of large scale, integrated, complex systems. With hand generation, the likelihood of missing critical pathways is increased and a large investment in time and manpower may be required. Experience in the nuclear power industry illustrates the importance of the latter consideration. Fault trees are used as an on-line aid for the diagnosis of faults at some nuclear power generating stations. The complete set of trees for one installation (Patterson, 1968) required an interdisciplinary committee of five two years to generate! A fault tree recently constructed by the United States Atomic Energy Commission for part of a nuclear plant required over 25 man years to complete (N. Rasmussen, 1973). Note also that any design changes may require considerable additional effort to modify the previous event tree structures.

With the above considerations, it is not surprising that fault tree analysis has not seen widespread use within the CPI. Some of the basic groundwork has been carried out, however. The approach has been advocated by Recht (1968) and a simplified technique based upon fault tree analysis has been implemented by Browning (1970). Again, the very real limitations imposed by hand generation neutralize the inherent utility of the technique. It is apparent that a means to quickly and systematically generate fault trees will be required for the application of fault tree analysis to continuous processing systems.

INFORMATION FOR FAULT TREE GENERATION

Figure 4 illustrates the various kinds of information required for fault tree generation. These diverse kinds of information cause part of the problem with hand generation of fault trees. It is difficult to assemble and manipulate by hand, the quantity and quality (detail) of information required for fault tree generation.

System Description

In order to perform a meaningful fault tree analysis, one important source of information is a detailed system description, equivalent at least to a piping and instrument diagram and a process flow sheet. The information required may be broken down into four general headings: equipment, streams, controls, and sensors. Table 1 contains a sample of the type of information which will be required to describe a chemical process system for safety analysis.

Several features of the system description require additional discussion. First, nearly all the information in Table 1 is readily available in the form of flowsheets, piping and instrument diagrams, specification forms, and operating instructions. Unfortunately, when the information is in this graphic form, it is not easily manipulated by computer. Hence it will be necessary to put the information in a form more readily usable by machine. Fortunately modern information processing technology offers several means for rapidly transforming graphic and tabular data into data structures useful for machine manipulation (Powers,

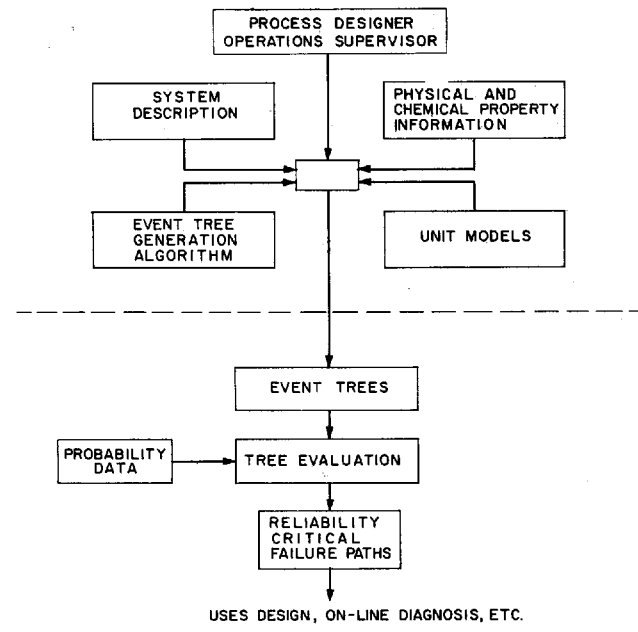


Fig. 4. Information requirements for fault tree generation.

Table 1. Information Required to Describe a Chemical Processing System for Safety Analysis

1. Equipment
   a. Name
   b. Function (gas/liquid separation, reaction, etc.)
   c. Normal Operating Conditions
      (1) temperature
      (2) pressure
      (3) phase
      (4) level
   d. Characteristics
      (1) maximum rated temperature
      (2) maximum rated pressure
      (3) materials of construction
      (4) volume
      (5) age
      (6) location (x, y, z)
      (7) manufacturer and batch number
      (8) explosion proof, etc.
      (9) rotating shafts
   e. Output Streams
   f. Input Streams
   g. Chemical Species
      (1) name
      (2) concentration
   h. Sensors
2. Streams
   a. Equipment at Origin
   b. Equipment at Destination
   c. Normal Operating Conditions
      (1) direction
      (2) phase
      (3) temperature
      (4) pressure
      (5) rate
   d. Characteristics
      (1) maximum rated temperature
      (2) maximum rated pressure
      (3) materials of construction
      (4) age
      (5) length
      (6) diameter
      (7) location (x, y, z)
      (8) manufacturer and batch number
      (9) explosion proof, etc.
3. Controllers
   a. Name
   b. Function (temperature, pressure, pH, etc.)
   c. Input Sensors
   d. Equipment controlled
   e. Mode (feedforward, feedback, proportional, etc.)
   f. Characteristics
      (1) maximum rated temperature
      (2) maximum rated pressure
      (3) materials of construction
      (4) age
      (5) high set point
      (6) low set point
      (7) location (x, y, z)
      (8) manufacturer and batch number
      (9) manual/automatic capability
      (10) explosion proof
   g. Type (electric, pneumatic, etc.)
4. Sensors
   a. Name
   b. Function (pressure, temperature, pH, etc.)
   c. Input Signal Origins (equipment or stream)
   d. Output Signal Destination (controller, display, etc.)
   e. Characteristics
      (1) maximum rated temperature
      (2) maximum rated pressure
      (3) materials of construction
      (4) age
      (5) alarm
      (6) location (x, y, z)
      (7) manufacturer and batch number
      (8) explosion proof
   f. Type (electric, pneumatic)

1973a). The data structures which describe the process interconnections are also directly available from various process synthesis programs, such as AIDES (Siirola, 1970). Another important feature of the process description is the amount of detail included. It is necessary to include enough detail in the process description to reflect the true process environment. The level of detail will depend on the scope of the processing system and the amount of information available. If the safety of three adjoining chemical plants is being investigated, less detail will be considered than for an analysis of a specific distillation column. The information on the location (x,y,z coordinates) of components in the system is required so that external propagation of failures by explosion or fire can be considered. The maintenance of the process description is a difficult problem. If changes are made in the process without modification of the description, it is possible to introduce failure modes which will not be detected in the fault tree analysis.

CHEMICAL AND PHYSICAL PROPERTY INFORMATION

In order to generate fault trees it is necessary to define hazardous events. Hazardous events can be grouped into two classes:

1. Hazards associated with species in and around the process.
2. Hazards associated with equipment in the process. Species dependent hazards are related to the intrinsic properties of the materials in and around the process. These properties include the flammability, corrosivity, reactivity, and toxicity of the species in the process system.

Process dependent failures are related to the structure of and components in the processing system. Failures such as release of toxic material from a valve that was mistakenly opened, or the rupture of a pressure vessel due to failure of a positive displacement pump controller are examples of process dependent failures.

In order to systematically generate hazard states, it is necessary to have information on species and process properties. The process properties are primarily associated with the system description (pressure and temperature ratings, materials of construction, and age), while species properties are characteristic of the molecules within the system.

Species related properties may be divided into two categories: physical and chemical. Table 2 presents a summary of properties which preliminary considerations indicate will be useful for fault tree analysis.

Two approaches to obtaining the species properties have been advocated. The first method is to gather and store data on a wide range of hazardous compounds. (For example, NFPA Hazardous Chemicals Handbooks.) this method has the advantage of answering certain specific species hazard questions with data gathered for that specific situation. Unfortunately, the number of potentially hazardous compounds is much larger than those for which quality data exists and the conditions under which these compounds are used is very diverse. These disadvantages have given rise to a number of approaches in which the properties of species are predicted from their molecular characteristics. The CHETAH program being developed by the ASTM Committee E27 is one example of attempts to predict hazardous properties (Seaton, 1972). This program is used to predict the spontaneous explosive decomposition of a wide range of chemical species.

We are currently developing a prototype information system which uses both direct (rote) storage of hazardous properties and general prediction algorithms.

TABLE 2. PROPERTY DATA USEFUL IN EVENT TREE GENERATION

I Physical
1. Freezing point
2. Boiling point
3. Specific gravity
4. Vapor pressure
5. Water solubility
6. Phase
7. Flash point
8. Vapor density

II Chemical
1. Toxicity
2. Flammable concentration limits (upper and lower)
3. Corrosivity to standard materials of construction
4. Molecular weight
5. Auto ignition temperature
6. Reactivity with other chemical species
7. Reaction rate
8. Heat of reaction
9. Reaction products
10. Catalyst requirements
11. Radioactivity

The hazards for each species have also been ranked on a scale from zero to ten. These rankings are similar to those used by insurance companies to categorize species hazards for insurance rate determination.

UNIT MODELING

Basic Considerations

A prerequisite for performing fault tree analysis is the existence of an adequate description of system behavior. A general process flowsheet may be considered to be a network consisting of units (equipment, streams, controllers, and sensors) interconnected in a specified fashion. This suggests a modular approach to modeling behavior: decompose the flowsheet into its basic units; develop a behavior model for each module; and finally, link the unit models together in a network representation. This section is concerned with the development of the unit models; the linking process is described in the next section.

For each unit it is necessary to define the mass, energy, and momentum relationships which describe the unit's behavior. There are several ways of defining these relationships. At one extreme, the unit may be modeled by writing the general unsteady state differential equations for the mass, energy, and momentum transport in the unit.

This level of description has the advantage that, if properly done, the movement of the process from a safe operating state to a hazardous state can be accurately predicted. An example of this type of model is the recent work on emergency cooling systems for nuclear reactors (IEEE, 1972).

The disadvantages of this level of modeling are:

1. The models are complex and require a great deal of information on the properties of the species and the equipment in the system,
2. The models are often difficult to solve, and
3. These types of models are usually constrained to a specific operating region and a specific mode of failure.

Of these disadvantages, the third one is probably the most important. If a hazard has been identified to the point where a detailed dynamic model has been prepared, then that failure mode is well on the way to being understood. What these kinds of models cannot usually predict, however, is the mode of failure which was not foreseen. It has been well documented that it is these oversight failure modes which are potentially the most hazardous (Katz, 1970).

A different type of model is required to reveal failure modes which may have escaped detection. Information flow models would appear to be ideally suited to this problem (Rudd, 1968). First of all, the information flow representation is simply a way of indicating how the variables which characterize each unit in the process are coupled when the units are connected in a process network. Information is passed from component to component within a processing system by variables common to several components, the output from one component being an input to others. This transfer of information traces out an information flow structure of the system, which provides a skeleton upon which we can organize an orderly search for safety problems.

One simple information flow representation for a heat exchanger is given in Figure 5. The variables and equations which describe the information flow are shown on Figure 5 in the form of a bipartite graph.

A simple information flow model only indicates that a particular output variable, say the temperature of a stream leaving a heat exchanger, depends on several input variables, flow rates, entering temperatures, area, heat transfer coefficient, etc. The quantification of the dependency depends on the solution of the set of equations describing the unit in question: in this case a heat exchanger. The solution to the equations gives the direction of variable change and its magnitude. Several approximations to the solution of the exact equations are possible. For example, it is often sufficient in safety analysis to merely know that an output variable depends on a certain input variable even though the exact nature of the dependency is not known. This type of information will allow the safety analyst to consider nearly all possible failure modes which depend on variable interactions. This can be an important step in avoiding overlooked failure modes. Hence, just knowing that simple theory predicts a cause and effect

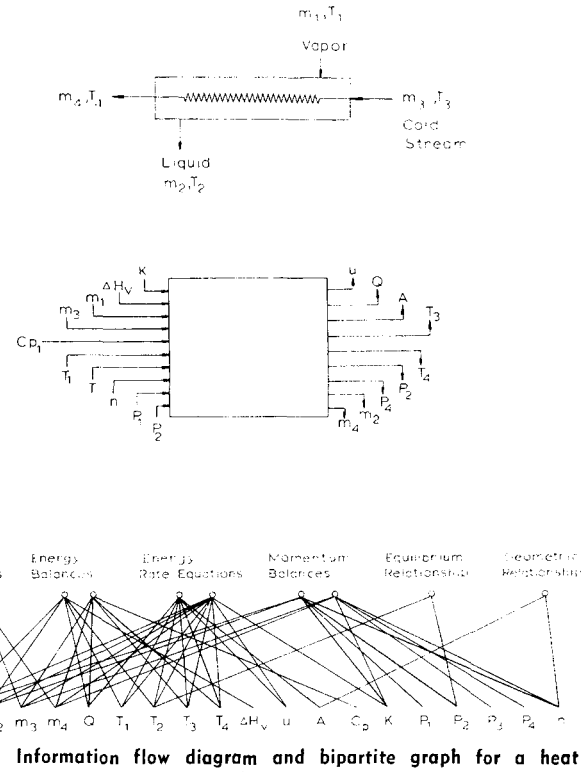


Fig. 5. Information flow diagram and bipartite graph for a heat exchanger.

relationship between variables which describe a unit's behavior can contribute to a formal safety analysis procedure. This is especially true when the safety analyst might not be aware of even the simple theory for the particular part of the plant under analysis.

A second level of approximation to the solution of the equations which describes the system is to give both the variable couplings (that is, which variables depends on other variables) and the sign of the dependency (+, −). With this information it is possible to investigate the direction (+, −) of variable changes which could lead to a hazardous event. Finally, if the variable coupling, sign, and magnitude are known it would be possible to quantify further how the system behaves.

A further degree of sophistication would involve the description of the dynamics associated with variable interaction.

An abbreviated matrix of coupled variables for a liquid/liquid countercurrent heat exchanger is shown in Figure 6.

For preliminary safety analysis it appears that simple information flow models based on steady state mass, momentum, and energy balances will be sufficient. With these models it is possible to reveal a great deal about the safety behavior of a chemical processing system. The variable interactions and signs have been sufficient for preliminary analysis (Tompkins, 1973). The sign and magnitude of the interaction is required for more detailed studies.

A method for including the control system in the information flow structure has also been developed (Powers, 1973c).

Table 3. General Failure Modes for Chemical Processing Equipment

I. Material balance failures (species related)
- A. Routing—(wrong flow path)
- B. Flow
  1. Low
  2. High
  3. Wrong direction
- C. Leakage
  1. Internal
  2. External
- D. Species (not normally present in system or environs)
- E. Reaction
  1. Undesired side products
  2. Incorrect conversion
  3. Wrong location
  4. Wrong reaction

II. Momentum balance failures (pressure related)
- A. Reaction
  1. Gas release
  2. Gas consumption
- B. Pressure sources
- C. Species (Vapor pressure)
- D. Pressure sinks
- E. Leakage
  1. Internal
  2. External
- F. Phase changes

III. Energy balance failures (temperature related)
- A. Reaction
  1. Endothermic
  2. Exothermic
- B. Internal heat sources
- C. Phase changes
- D. External heat sources
- E. Frictional heat sources (rotating equipment)
- F. Leakage
  1. Internal
  2. External
- G. Fouling of transfer surfaces

UNIT FAILURE MODELS

In order to perform the fault tree analysis, not only must models be generated for system performance as designed, but models must also be developed for describing failure modes. In line with the modular approach described above, a failure model will be associated with each unit performance model. In terms of the descriptive framework for the unit models (steady state material, momentum, and energy balances), the failure modes may conveniently be classified for each unit as material, momentum, and energy balance failures. This is not to imply that the balances do not hold when written for a particular failure state, but that the conditions represented are undesirable in some sense [for example, the generation of a potentially explosive mixture in a processing unit due to an air leak, (mass balance failure)].

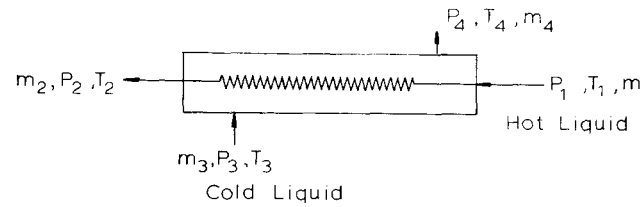
Associated with each balance is a variable which is a primary descriptor of the system state:

1. Material balance → chemical species (concentration and flow rate)
2. Energy balance → temperature
3. Momentum balance → pressure

A failure state is assumed to exist when one or more of the species, temperatures, or pressures are not within specified limits. General failure modes for each category are presented in Table 3. Note that the entries in Table 3 represent immediate causative factors, not necessarily primal failures. For instance, an energy balance failure category may be the result of a material balance failure which may in turn depend upon a momentum balance failure, etc.

The general failure modes provide the framework within which specific failure models for a particular unit (reactor, separator, pump, etc.) may be formulated. For instance, for the heat exchanger of Figure 6 the condition "energy balance failure—T_2 too high" could have the following failure modes (assuming no temperature control, and no reaction in the exchanger):

1. Exogenous increases in T_1, T_3, P_1, or P_4
2. Exogenous decreases in P_2, or P_3
3. Decreases in U or A due to fouling
4. External leak in stream 3



Dependent Variables

Independent Variables	m_1	m_3	T_2	T_4	u
T_1	O	O	+	+	O
T_3	O	O	+	+	O
u	O	O	-	+	X
A	O	O	-	+	O
P_1	+	O	+	+	+
P_2	-	O	-	-	-
P_3	O	+	-	-	+
P_4	O	-	+	+	-

Fig. 6. Variable coupling matrix for a liquid/liquid heat exchanger. The sign indicates the change in the dependent variable for a positive change in the independent variable.

5. External heating of the unit due to fire or weather conditions
6. Change of phase (liquid to gas) in stream 3
7. Exogenous change in composition of stream 3 resulting in lower heat capacity

Conditions 1, 2, and 7 represent exogenous factors in that each is determined by conditions either upstream or downstream of the exchanger (that is, these predecessor failure states are associated with the failure models of other units in the processing network). Conditions 4 and 5 are obtained from the failure model for this type of heat exchanger.

FAULT TREE GENERATION

In fault tree generation the basic question to be answered is: "Given a hazard event of interest (explosion, fire, temperature hazard, etc.), what sequences of events may possibly take place to result in the hazard state?"

Central to answering this question is the establishment of the information flow structure for the system and the determination of the logic required for event tree generation.

The general methodology for the generation of fault trees is the successive identification of predecessor events from the top node of the tree (the final hazard event) to the outermost nodes (the sequence-initiating or primal events). Fault tree generation starts with the definition of final hazard states. The final hazard states are defined by mini-fault trees which correspond to species or process properties. The output from the tree is the top hazard event and the inputs are process variables and conditions. An example of a simplified mini-fault tree for an explosion is given in Figure 7. The specific form and location for the final hazard event is dependent on the properties of the materials in the system and the characteristics of the equipment in the system. The hazardous properties information described earlier, together with the process description, will provide the information necessary to synthesize the failure state description which in turn serves as the starting point for generation of the event tree. The failure state descriptors decompose the problem of generating the fault tree into several small subproblems. Each process variable (pressure, temperature, species, concentration) which is a descriptor of a failure state may be considered to be the top node of a subtree of events. The final fault tree is then composed of the appropriate subtrees linked together through the logical relationships implied by the failure state description. After a final hazard state definition the problem is to identify all the ways the system could achieve the states associated with each descriptor of the final hazard state. This, in general, involves tracing through the information flow structure for the processing system. The logic which guides this search is the essence of fault tree generation. Figure 8 illustrates the overall strategy. The major task in generating the subtrees is searching for paths in the information flow structure which allow mass, momentum, or energy related variables to achieve certain states. The information flow structure contains information on both unit model behavior and unit failure modes. As an example consider a material balance related failure for Figure 7. In Figure 7 one descriptor for the explosion requires that a particular species be present at the location in question within certain concentration limits. The presence of a species and its concentration are material balance variables. In generating the fault tree leading to these descriptors it is necessary to identify all the possible ways that the species might arrive at the location. A check of the system description will indicate whether it is normally present at the location. If the species is not present, an exhaustive listing of the flow paths from sources of the species in or around the system to the location can be constructed. The information flow unit model for equipment along the flow path is used to indicate how these units must fail in order that the required species flow result. Similar search procedures for pressure and temperature descriptors have been developed. In this manner it is possible to generate the complete fault tree for each specified final failure event (Powers, 1973 c).

This method is illustrated for the heat exchanger system shown in Figure 9. Partial event trees for the events T2 High and T2 Low were generated by searching the information flow structure for the system and are illustrated in Figures 10 and 11.

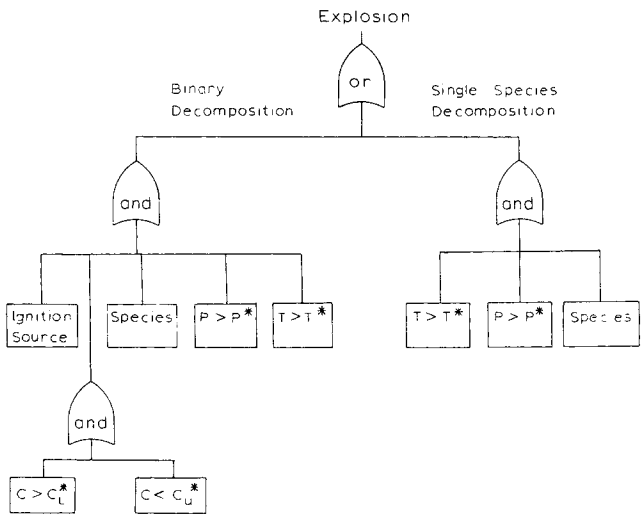


Fig. 7. A mini fault tree for explosion. The right branch of the tree is for the explosive decomposition of a single species. The left branch is for explosions which require two species (for example, oxygen and hydrocarbon).

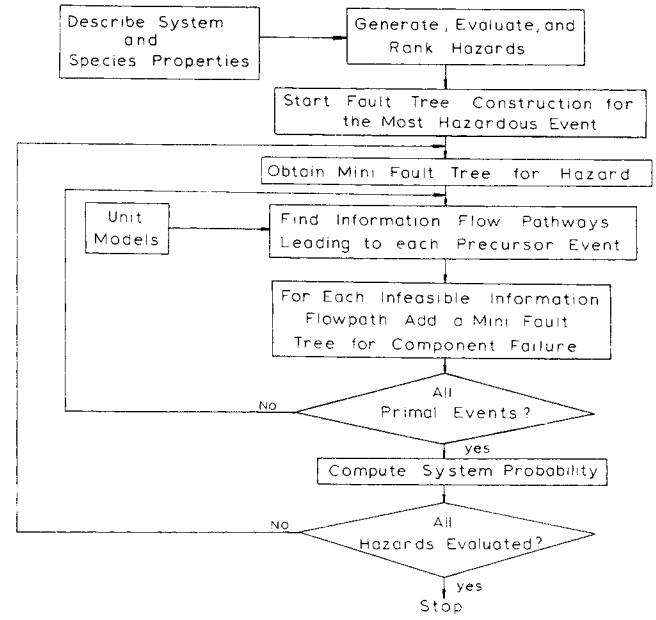


Fig. 8. The overall strategy for generating event trees. After definition of system hazards, a mini fault tree for the hazard is defined (see Figure 7). For precursor variables in the hazard, information flow paths for normal and failed states of the system are searched out. Mini fault trees which represent specific failure modes of equipment are used to bridge gaps in the information flow paths.

FAULT TREE EVALUATION

Event Probabilities

Given a fault tree that describes the failure possibilities for a processing system, it is desirable to determine which path through the tree is most likely to occur. In order to find these critical paths we need data on the probability that primal events—events at the bottom nodes in the tree—will occur. The logical structure dictated by the form of the fault tree prescribes the manner in which the probabilities must be combined to yield both the probability of the top node (final hazard event) and the probabilities of individual event sequences. The overall accuracy of event sequence prediction, therefore, depends directly upon both the availability and quality of the basic probability data. Failure rate data are needed in three basic categories: equipment failure; human error; and abnormal environmental stresses (so-called "acts of God"—sudden freezes, high winds, earthquakes, etc.).

Considerable data on failure probabilities have been gathered by the Defense Department and by the various agencies associated with nuclear power stations (IEEE, 1972). Table 4 illustrates data gathered by Anykora, et al. (1971) on the failure of instruments used in chemical processing systems. The data bank developed by the United Kingdom Atomic Energy Authority (UKAEA) and used by the Systems Reliability Service of the UKAEA is quite extensive and has been used with considerable success in the chemical industry (Ablitt, 1973).

The study of human errors, their causes, and prevention has been carried out systematically for the past twenty years. Many studies have been made to determine error rates for a wide range of human activities. One system for predicting failure rate data for human activities has been developed by the Sandia Corporation. The approach called THERP (Technique for Human Error Rate Prediction [Swain, 1973]) has been used in several industries where human errors could lead to hazardous events. Table 5 gives a representative collection of human error rate data. However, there is a lack of data on the higher-level human reasoning activities which are required in the operation of chemical plants (J. Rasmussen, 1973).

Data on abnormal environmental events such as earthquakes or storms have been compiled by several governmental agencies (IEEE, 1972). Currently no formal predictive method exists for earthquakes or storms and data on past events are used. New techniques for monitoring earth movements to predict earthquakes is undergoing rapid development (IEEE, 1972).

In general, the amount of probability data that exists for chemical processing systems is surprisingly large. Several governmental agencies have been gathering data for many years on units commonly used in the chemical industry. Unfortunately, the environments under which the units were operated are often different. Several means for assessing environmental stress effects on failure rates has been developed to overcome part of the difficulty. (Green, 1973)

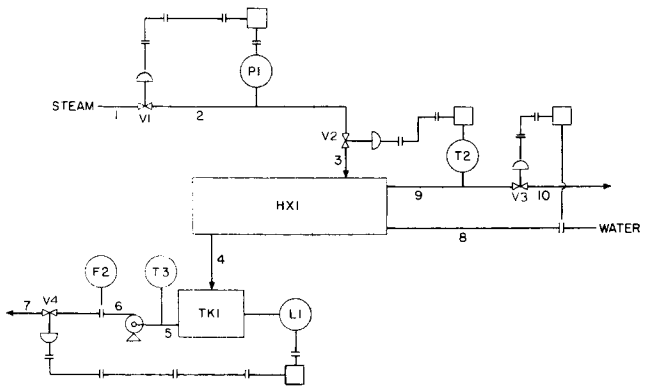


Fig. 9. A model heat exchanger system.

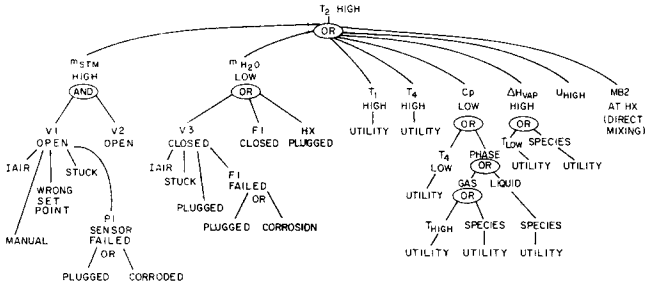


Fig. 10. A partial fault tree for the system shown in Figure 9 for the event T_2 too high.

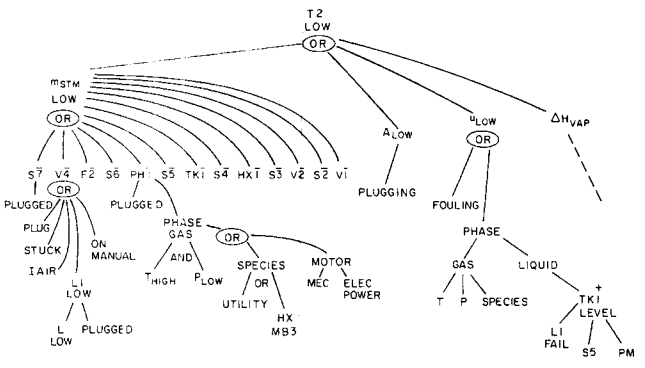


Fig. 11. A fault tree for the system shown in Figure 9 for the event T_2 too low.

Computation of Critical Paths

In principle, the calculation of final hazard event probabilities, given the primal failure probabilities, is a simple procedure of combining and carrying forward the primal event probabilities in a manner dictated by the logical structure of the fault tree. In practice, however, considerable difficulty may be introduced for large trees by the requirement that the final Boolean probability expression be in a mutually exclusive form. Mutual exclusivity serves to eliminate event redundancies (the appearance of an event at more than one place in the same tree, indicating that certain combinations of events are not mutally independent), resulting from properties of the union ("or") operation. In other words, the same event might occur in several parts of one fault tree. This situation indicates that the potential for a common mode failure exists. That is, a failure which increases the probability of all or nearly all of the branches of the fault tree. These events are of major importance because they can greatly alter the probability that the hazard event will occur. The computational techniques associated with fault tree evaluation are well advanced (Vesely, 1969, 1970). Vesely and others have developed Monte Carlo techniques for evaluating final event probabilities and for determining critical failure paths. A technique for determining the sensitivity of the final event probability to variation in primal event probabilities has also been developed (Vesely, 1970). A powerful method for determining the minimal cut sets for logic trees has been developed by Fussell (1973b).

Hazard Evaluation

The consequences of a failure must also be determined to assess realistically the safety of a processing system. Given a potentially large number of individual fault trees

TABLE 4. INSTRUMENT RELIABILITY DATA (FROM ANYKORA, 1971)

Instrument†	No. at risk	Environmental factor	No. of faults	Failure Rate (faults/yr.)
Control valve	1,330	2	359(327)	0.57(0.51)
Globe(p)	1,195			
Butterfly(p)	105			
Diaphragm(p)	30			
Valve positioner(p)	320‡	1	62	0.41
Solenoid valve	168	1	24	0.30
Current/pressure transducer	89	1	23	0.54
Pressure measurement:	193	3	89(82)	0.97(0.89)
Absolute pressure transducer(p)	124			
Differential pressure transducer(p & e)	69			
Flow measurement(fluids)	1,733	3	902(890)	1.09(1.08)
Differential pressure transducer(p & e)	473	3	419	1.86
Transmitting variable area flowmeter(p)	100	3	48	1.01
Indicating variable area flowmeter	857	3	137	0.34
Mercury manometer flowmeter	137			
Turbine steam flowmeter	60			
Piston flowmeter	61			
Turbine flowmeter	45			
Level measurements(liquids)	316	4	233(206)	1.55(1.37)
Differential pressure transducer(p & e)	130	4	106	1.71
Float-type level transducer	158	4	124	1.64
Capacitance-type level transducer	28	4	3	0.22
Temperature measurement	2,391	3	326(320)	0.29(0.28)
Thermocouple	663	3	127	0.40
Resistance thermometer	441	3	68	0.32
Mercury in steel thermometer	996	2	13	0.027
Temperature transducer	291	3	118	0.85
Controller	1,083	1	133(120)	0.26(0.23)
General purpose(p)	767			
General purpose(e)	81			
Temperature	235			
Pressure switch	519	2	75	0.30
Flame failure detector	43	3	28	1.37
Analyser	48		141	6.17
*p*H meter	29		59	4.27
Gas-liquid chromatograph	3		30	20.9
O_2 analyser	9		30	7.0
CO_2 analyser	4		20	10.5
Infra-red liquid analyser	3		2	1.40
Impulse lines	842	3	364(341)	0.91(0.85)
Pressure transducer	124			
Differential pressure transducer	672			
Pressure switch	25			
Analyser	21			
Purge systems	100	4	48	1.00
Control loop	1,083		120	0.23)
Controller setting	1,083		66	0.13

† p: pneumatic
e: electronic
‡ estimated number

for a process, a basis must be established upon which to take corrective action (design changes, respecification of operating procedures, etc.). This basis logically consists of a joint consideration of event probabilities and consequences. For example, an event with a relatively high probability of occurrence but minimal process interruption and personnel injury potential may be tolerated relative to another event low probability, but significant disaster potential.

Consequences of process failure may be classified into three areas: equipment damage, business interruption, and product losses. The figures could then be combined with the probability of each hazard event to form a basis for corrective action (Starr, 1970).

Current Status

Fault trees for several more complicated systems are currently under development. A liquified natural gas unloading, storage, and distribution plant is being studied to test these methods for generating fault trees.

This work is in its preliminary phases. There are many problems to be solved. How to define the scope of the system? Can we maintain an accurate description of the process as it is repaired and redesigned? Are the models accurate? Are the physical and chemical property data realistic? Is the procedure used to generate the fault trees correct? Can we predict the behavior of the human operator in a process environment? All of these questions are serious ones. Each of them needs additional research work. In this paper we have shown how these various problems relate to the overall systems safety analysis procedure. A formal methodology has been developed in increase the accuracy and speed of fault tree generation.

TABLE 5. REPRESENTATIVE HUMAN ERROR RATES
(After Recht, 1966)

Task element			
Action	Object	Error	BER*
Observe	Chart	Inappropriate switch actuation	1,128
Read	Gauge	Incorrectly read	5,000
Read	Instructions	Procedural error	64,500
Connect	Hose	Improperly connected	4,700
Torque	Fluid lines	Incorrectly torqued	104
Tighten	Nuts, bolts	Not tightened	4,800
Install	Nuts, bolts	Not installed	600
Install	O-ring	Improperly installed	66,700
Solder	Connectors	Improper solder joint	6,460
Assemble	Connectors	Bent pins	1,500
Assemble	Connectors	Omitted parts	1,000
Close	Valve	Not closed properly	1,800
Adjust	Mechanical linkage	Improper adjustment	16,700
Install	Line orifice	Wrong size installed	5,000
Machine	Valve port	Wrong size drilled and tapped	2,083

* Basic error rate (errors per million operations).

LITERATURE CITED

Anykora, S. N., G. F. M. Engel, F. P. Lees, "Some Data on the Reliability of Instruments in the Chemical Plant Environment," *The Chem. Engineer* (Nov., 1971).

Browning, R. L., "Analyzing Industrial Risks," *Chem. Eng.*, (Oct. 20, 1969).

———., "Calculating Loss Exposures," *ibid.*, (Nov. 17, 1969).

———., "Estimating Loss Probabilities," *ibid.*, (Dec. 15, 1969).

———., "Finding the Critical Path to Loss," *ibid.*, (Jan. 26, 1970).

———., "Using Systems Analysis to Improve Protective Instrumentation in the Process Industries," *I.S.A., C.P.D.*, 72107 (1972).

Buehler, J. H., et al. "Report on Explosion at Union Carbide's Texas City Butadiene Refining Unit," *Chem. Eng.*, (Sept. 7, 1970).

Carpenter, K. G. "Anticipating Hazards, the Key to Safe Operation," *Chem. Eng. Progr.*, **60**, (4) (1964).

Cornett, C. L., and J. L. Jones, "Reliability Revisited," *AIChE Symp. Reliability of Operation in the Process Industries*, San Juan, (May, 1970).

Crosetti, Paul A. "Fault Tree Analysis with Probability Evaluation," Douglas United Nuclear, Inc., Richland, Wash. (1971).

Fussell, J. B., "Synthetic Tree Model—A Formal Methodology for Fault Tree Construction," Aerojet-Nuclear Report ANCR 01098, March (1973a).

———., "Fault Tree Analysis—Concepts and Techniques," NATO Adv. Study Inst. on Generic Techniques in Systems Reliability Assessment, England (1973.) In press (Nordhoff).

Garner, Norman R., and John A. Huetinck, "Equipment Aging Analysis: An Extension to Reliability," *AIChE Symp. Reliability of Operation in the Process Industries*, San Juan, (May, 1970).

Green, A. E., and J. Bourne, *Reliability Technology*, Wiley, New York (1973).

Hill, F. J., and G. R. Peterson, *Introduction to Switching Theory and Logical Design*, Wiley, New York (1968).

IEEE Standards Committee, *IEEE Trial-Use Guide: General Principles for Reliabiltiy Analysis of Nuclear Power Generating Station Protection Systems.* IEEE Std. 352, (1972).

Katz, Donald L., "A View of Safety in the Petroleum Industry," *National Academy of Eng. Symp.: Public Safety: A Growing Factor in Modern Design*, Wash., D. C. (1970).

Kay, P. C. M., and P. W. Heywood, "Alarm Analysis and Indication at Oldbury Nuclear Power Station," *IEEE Conf. Publ. No. 16, part 1* (March, 1966).

Kendall, Henry W., "Nuclear Reactor Safety," Mech. Seminar, Mass. Inst. Technol., Cambridge (Dec. 1972).

King, Carl F., and Dale F. Rudd, "Design and Maintenance of Economically Failure-Tolerant Processes," *AIChE J.*, **18**, 257 (1972).

Kuist, Blaine B., "What Price for Continuity for Polymer Plants?" *AIChE Symp.: Reliability of Operation in the Process Industries*, San Juan (May, 1970).

National Fire Protection Assoc., *Fire Hazard Properties of Properties of Flammable Liquids, Gases, Volatile Solids*, Boston (1969).

———., *Manual of Hazardous Chemical Reactions*, Boston, Mass. (1971).

———., *National Fire Codes*, Vols. 1 to 3, Boston (1971).

Ostrander, V. Pierce, "Spare Vehicle Reliability Techniques for Industrial Plants," *AIChE Symp. Reliability of Operation in the Process Industries*, San Juan (May, 1970).

Patterson, D., "Application of a Computerized Alarm-Analysis System to a Nuclear Power Station," *Proc. IEE*, **115** (12) (Dec., 1968).

Powers, Gary J., Foxboro Research Paper, No. 73-P7 (Jan., 1973).

———., and F. C. Tompkins, "Fault Tree Synthesis," *NATO Conf. on Reliability*, Liverpool, England (1973).

———., "Safety and Reliability Analysis," Course Notes in Advanced Process Synthesis, Mass. Inst. Technol., Cambridge (1973).

Rasmussen, Norman, Dept. of Nuclear Eng., Mass. Inst. Technol., personal communication (1973).

Rassmussen, J., "The Role of the Man-Machine Interface in Systems Reliability," NATO Conf. on Generic Techniques in Systems Reliability Assessment, Liverpool, England (July, 1973). To be published by Nordhoff.

Rudd, Dale F., and Charles C. Watson, *Strategy of Process Engineering*, Wiley, New York (1968).

Recht, J. L., "Systems Safety Analysis: An Introduction," *National Safety News*, (Dec., 1965).

———., "Systems Safety Analysis: Failure Mode and Effect," *ibid.*, (Feb., 1966).

———., "Systems Safety Analysis: The Fault Tree," *ibid.*, (April, 1966).

———., "Systems Safety Analysis: Error Rates and Costs," *ibid.*, (June, 1966).

Rucker, William, and William E. Cline, "Plant Reliability and its Impact on Large Plant Design and Economics," *AIChE Symp.: Reliability of Operation in the Process Industries*, San Juan (May 1970).

Seaton, W. H., and E. Freedman, "Computer Implementation of a Second Order Additivity Method for the Estimation of Chemical Thermodynamic Data, paper presented at the 65th meeting of Am. Inst. Chem. Engrs., New York (1972).

Siirola, J. J., G. J. Powers, and D. F. Rudd, "System Synthesis Part III: Toward a System Concept Generator," *AIChE J.*, **17**, 677 (1971).

Starr, Chauncey, "An Overview of the Problems of Public Safety," *National Academy of Eng. Symp.: Public Safety: A Growing Factor in Modern Design*, Wash., D. C. (1970).

Semanderes, Stavros N., "ELRAFT: A Computer Program for the Efficient Logic Reduction Analysis of Fault Trees," IEEE Trans. on Reliability, 126 (Nov., 1970).

Swain, A. "Human Factors Assessment," *NATO Conf. on Reliability*, Liverpool, England (1973).

Vesely, W. E., "Analysis of Fault Trees by Kinetic Tree Theory," IN-1330 (Oct., 1969).

———., and R. E. Narum, "PREP AND KITT: Computer Codes for the Automatic Evaluation of a Fault Tree," IN-1349 (Aug., 1970).

———.,"Reliability and Fault Tree Applications at the NRTS," Idaho Nuclear Corp., Idaho Falls, Idaho (1970).

Welbourne, D., "Alarm Analysis and Display at Wylfa Nuclear Station," paper presented before IEE Control and Automation, London (Nov., 1968).

Williams, Henry L., and Bentley H. Russell, "The Application of N.A.S.A. Reliability Techniques to the Chemical Industry," *AIChE Symp.: Reliability of Operation in the Process Industries*, San Juan (May, 1970).

Manuscript received October 23, 1973; revision received December 19 and accepted December 20, 1973.