Computer-Aided Fault Tree Synthesis

Procedures and computer programs now being developed should reduce the amount of time, now measured in man-years, for carrying out a fault tree analysis.

G. J. Powers and S. A. Lapp, Carnegie-Mellon Univ., Pittsburgh, Pa.

Fault tree analysis is one means for systematically identifying cause-and-effect chains of events which could lead to environmental hazards. Once a fault tree has been constructed it is possible to compute the time dependent probability of occurrence of the hazard, given the probability of occurrence of causing events.

The two major problems with this approach are in 1) generating the tree and 2) gathering the appropriate probability data. We have developed a computer program which aids in the generation of fault trees for chemical processes. It uses signed digraph models for equipment. The fault tree is deduced directly from this simple model of the system.

Environmental risk assessment is becoming a more important aspect of the design of chemical processing plants. Environmental impact statements, potential fines, and lawsuits make the potential environmental risks an important business issue. In the assessment of risks it is necessary to determine 1) the consequences of each potential risk, 2) the probability of occurrence of each event, 3) the chains of events which could cause the risk, and 4) the costs of potential changes to the process and its operation which might reduce the probability or consequences of the event.

A number of techniques advocated for determining the consequences of risks are commonly based on simulations of the transport and interaction of released chemicals with people and the environment. The results of the simulation are estimates of the potential damages that might result from releases of various sizes and types. The adequacy of these estimates often depends on the state of knowledge of the reactivity of the chemicals. At low concentration levels of exposure the prediction of consequences is very uncertain. In the following discussion only high concentration exposures, which usually occur over short time periods, are considered.

Prediction of the probabilities of exposure is a more difficult issue. Intuitive techniques are less suited for the prediction of probabilities than they are for consequence estimation.

"Safety First," a motto used by many chemical companies, illustrates the importance industry places on preventing personal, equipment, and business interruption hazards. The employee safety records of the major chemical companies have been good. The probability of being injured in a chemical processing plant is less than in many other industries and much less than staying at home. However, the process loss situation has not been as encouraging. A number of major losses have occurred due to fires, explosions, and releases of chemicals in chemical plants. In addition, more stringent laws are being promulgated to ensure worker safety and to prevent releases of toxic or otherwise hazardous materials into the environment.

How can the chemical industry improve the safety and reliability of their processes? How can they counteract well-meaning but sometimes misdirected governmental agencies? The key lies in careful attention to the design and operation of each part of the chemical processes.

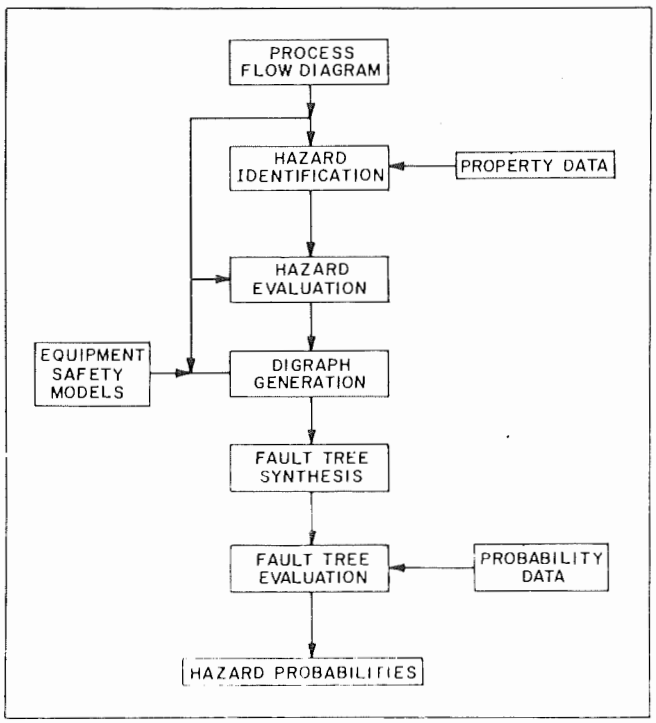


Figure 1. Steps in hazard assessment.

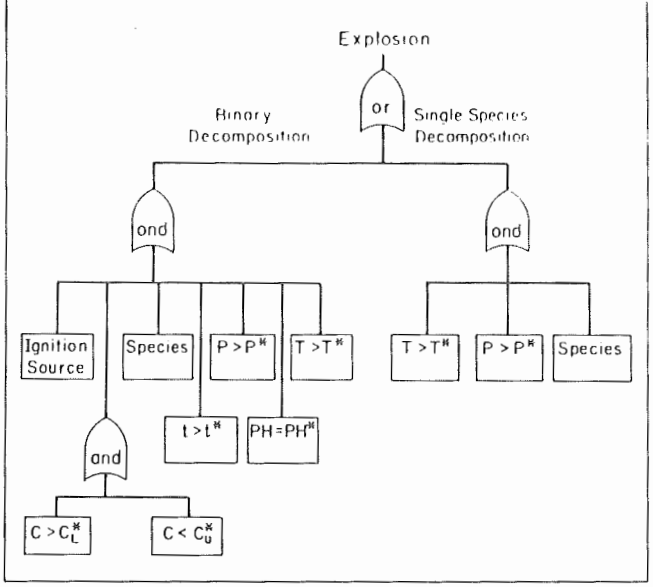


Figure 2.
The hazard equation for explosion.

Designers must be able to analyze processes to foresee potential failures. Operators of processes, as well as the automatic control systems, must be trained to respond rapidly to process failures.

In dealing with governmental agencies process designers must show that "all *reasonable* precautions have been taken to reduce the probability of events to *acceptable* levels." This last sentence contains the key features of the safety problem. The law is written so that the industry is responsible for 1) identifying the potential events, 2) deciding on *reasonable* precautions, and 3) reducing the probability of these events to *acceptable* levels. These three areas are where meaningful contributions to the safety analysis of chemical processes can be made. One needs to 1) identify events, 2) decide how to prevent these events from occurring, and 3) compute and determine what constitutes acceptable probabilities.

The following describes one approach to this analysis problem. The fundamental concepts for this approach have been described in previous papers. (*1,2*) This article will briefly describe the FTS (Fault Tree Synthesis) program and illustrate by a simple example how it might be used. The major points to be covered are 1) hazard identification, 2) hazard consequence estimation, 3) digraph models of individual equipment and complete chemical processes, 4) fault tree synthesis, 5) fault tree evaluation (probability calculations) and 6) use of the program for new designs and for the review of existing processes.

First need is to identify process flow

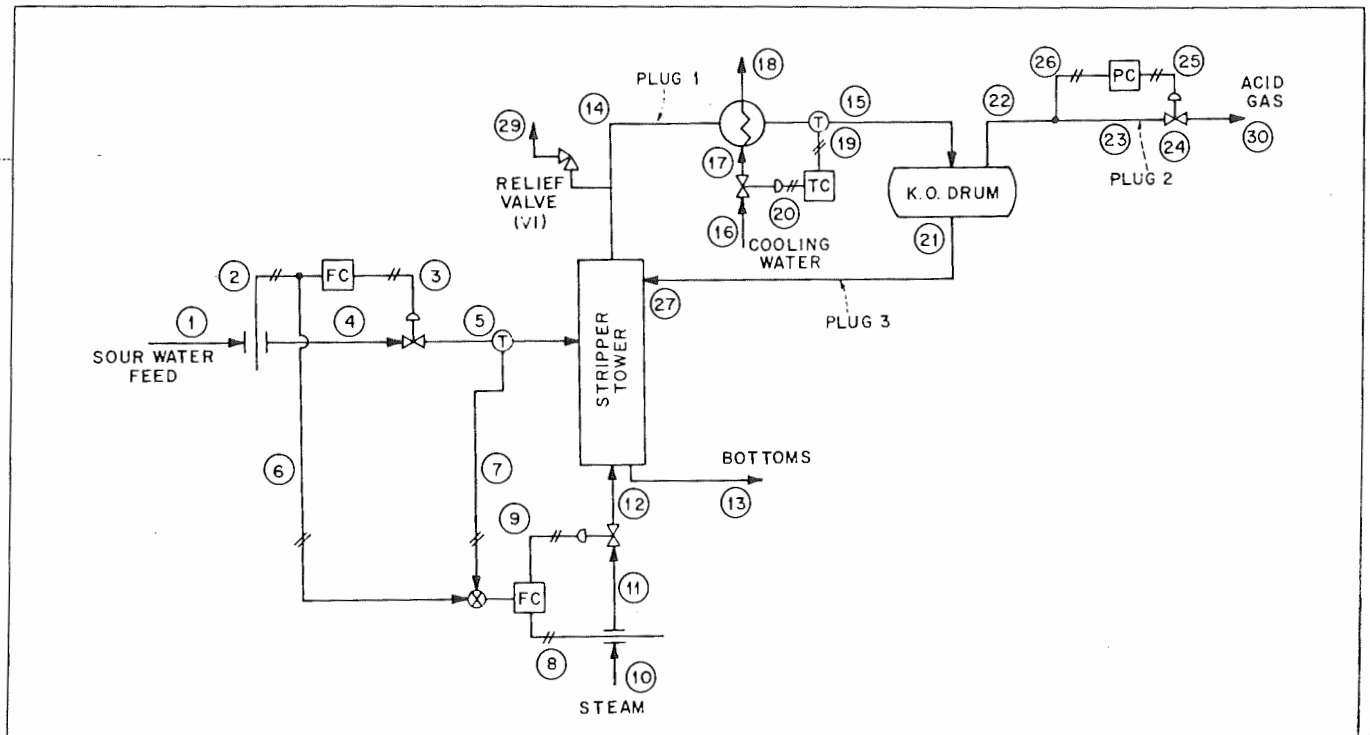
Figure 1 illustrates the major steps required to carry out the quantitative safety analysis of a chemical process. Initially the process flow diagram must be identified. Second, the hazardous events that might occur within or around the process must be discovered. Data are required on the physical and chemical properties of the species in the process and the mechanical and electrical properties of the process equipment. Each potentially hazardous event may then be evaluated to determine its possible costs (loss of life, loss of equipment and material, loss of business, and damage of the environment).

With the information derived from these steps a ranked list of potential hazards may be constructed. What is required is the probability of occurrence of each hazard.

Since most of these events will occur infrequently, it is not possible to take a direct statistical approach to the estimation of their rate of occurrence. What is needed is a means for estimating the probability of hazardous events from the probabilities of more common (and hence more accurately determined) events.

Fault tree analysis (FTA) is one means for carrying out this estimation. FTA is based on the assumption that the hazard is a logical consequence of other events. That is, if we knew the probability of occurrence of the set of events which contains the necessary precursors to a fire we could estimate the probability of the fire. In this manner, the causative events are reduced to smaller and smaller sets of events until a level is reached at which sufficient probability data are available.

Figure 3. A sour water stripping system.



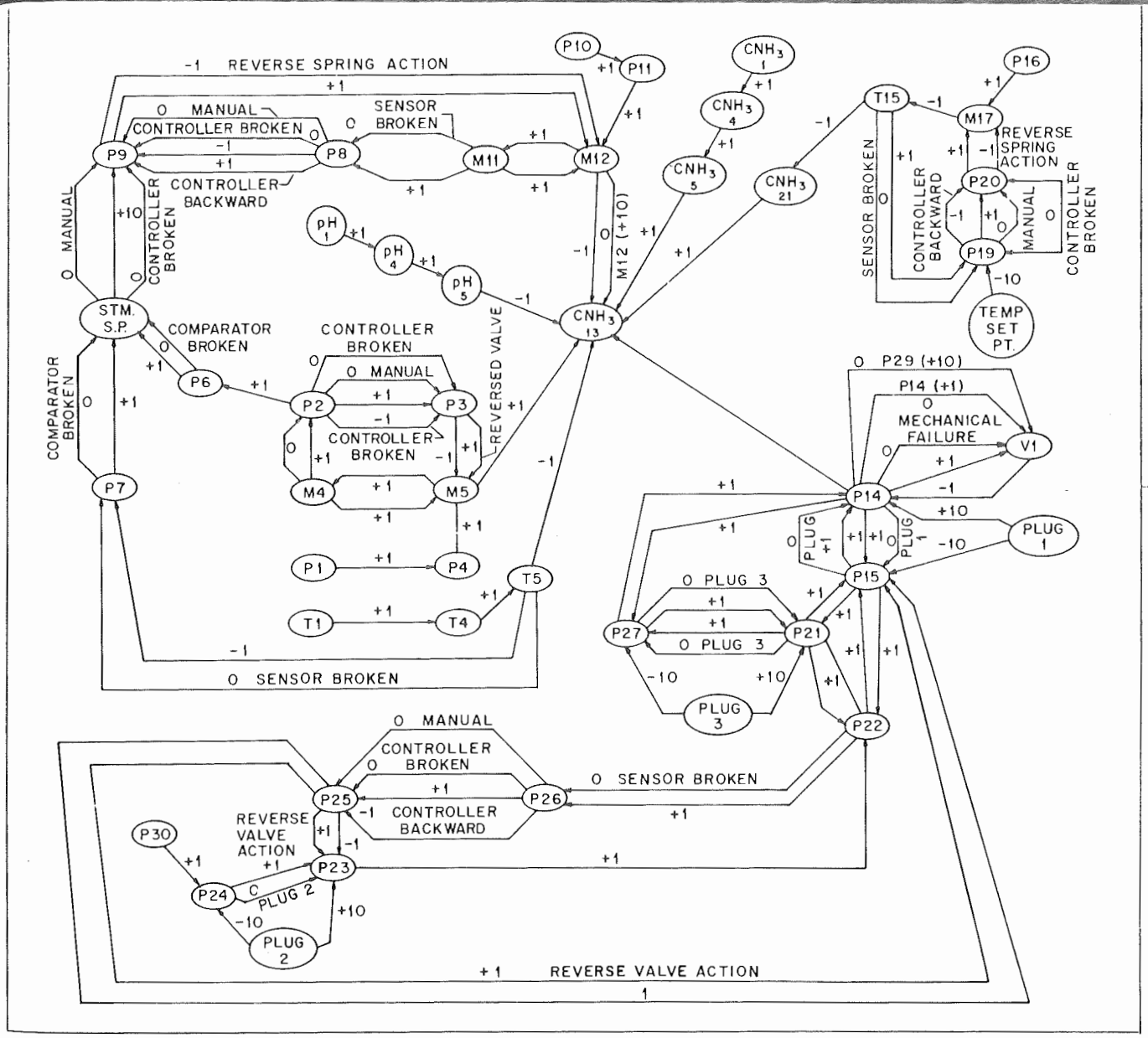


Figure 4. Digraph for sour water stripping system.

One major problem in this approach is the generation of the sets of precursor events. These sets must contain "all" the important events in the proper logical relationships. The generation of fault trees can be a very time consuming and error-prone procedure. For example, in an average chemical process there will commonly be over 50 hazardous events. This large number of incidents is because a single generic hazard, such as release of toxic material, could occur at a number of different locations within the process.

Each fault tree will often require two to three man-days to carry out the generation, documentation, and computation of probabilities of failure. Hence, several man-years of effort are commonly required to carry out a fault tree analysis. A recent study by the U.S. Atomic Energy Commission (WASH-1400) required over 25 man-years to generate the fault trees for one boiling water reactor and one pressurized water reactor. In addition, high quality people are required to carry out the analysis. The magnitude of the time required for analysis has retarded the growth of the fault tree method in the chemical process industry. We are currently developing procedures and computer programs (FTS) that we hope will greatly reduce the time required for quantitative safety analysis.

Symbolic process simulation

The FTS program is essentially a symbolic process simulation. Following identification and evaluation of process hazards, a symbolic model of the complete process is assembled from models of individual pieces of equipment within the process. Models that have been developed by experts represent the latest thinking on normal and failed behavior of processing equipment. The models are signed digraphs. We have developed an algorithm that deduces the fault tree directly from the properties of the digraph. Once the fault tree has been generated, it is placed in minimal cut-set form and the probability of the top event is computed.

The flow diagram is entered in a manner similar to other flow diagram simulators. The equipment and streams are numbered and the topology of the process network defined. The characteristics of each piece of equipment and each stream are also entered. The program constructs a multilinked data structure that contains the information on the process.

Potential hazards are identified by considering the physical and chemical properties of the species within the process and the strength of the equipment. The species

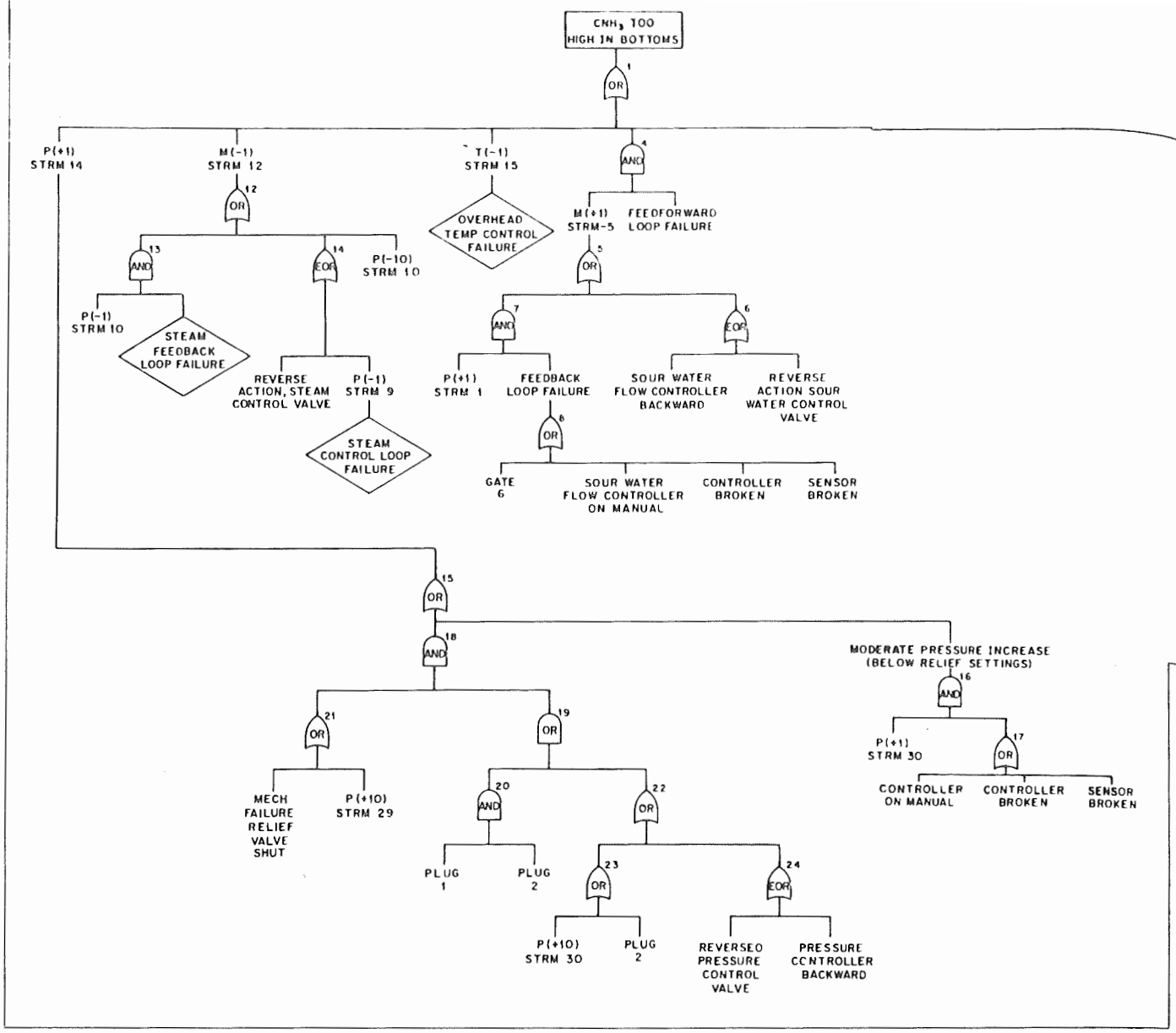


Figure 5. Fault tree for the event "concentration of NH_3 too high" for a sour water stripping system.

hazards are determined from 1) single species property data such as detonation tendencies, toxicity, flammability, explosivity, etc. and 2) binary species data.

Binary data are required to determine whether species within the process react with each other and if so under what conditions. A binary species reaction matrix is constructed from data in the program's library and from the program user. Equipment related hazards are identified by considering the pressure, temperature, and corrosion ratings of the equipment. The result of hazard identification is a list of hazards and the conditions required for their occurrence. Figure 2 gives the hazard "equation" for explosion.

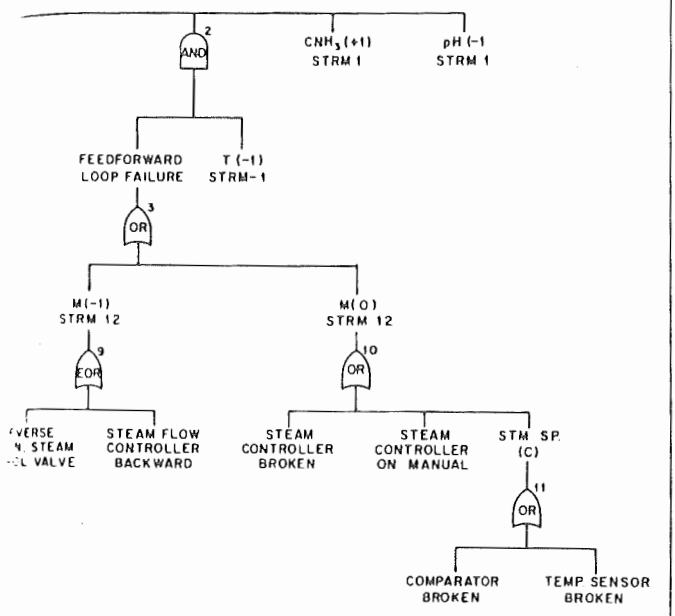
How costs are determined

The total cost of each potential hazard is determined in several ways. First, a detailed calculation of the blast wave radius and high radiation fire radius are computed. Equipment, people, and raw materials within these radii are used in the cost evaluation. Business interruption expenses are computed from product rates and values, and the current delivery times for major pieces of process equipment. The impact of the release of toxic material is based upon the magnitude of the release, plume spread calculations, and toxic nature of the chemical species. These features of the cost of a hazard are then combined to measure the total potential cost for each hazard. These estimates are used as a first approximation of the cost of a hazard. More detailed estimates of each hazard will commonly follow the generation of the fault trees.

The program also contains several rating schemes used by major insurance and chemical companies in the U.S. These schemes use a relative rating scale for species, equipment, etc. The ratings are based on past loss data and intuition. These methods give a very rapid means for screening potential total process hazards, but they are usually not discriminating enough to use on specific equipment faults within a process.

Following the evaluation of hazards within the process, a ranked list of hazards is constructed. What remains is to determine the probability of each hazard.

Signed digraphs are used as models for faults in the FTS program. Models have been prepared for pieces of equipment normally found in chemical processes (reactors, pumps, pipes, mixers, tees, valves, sensors, controllers,



etc.). Each module is an input/output matrix for the piece of equipment. The inputs are variables whose information could flow into the equipment.

In addition to the normal inputs, all known failure modes are considered as inputs. That is, if a failure occurs, how does it change an output variable? Finally, any changes in relationships between input and output variables due to failure modes are indicated. For example, plugging of a pipe changes the input/output relation for pressure in that pipe.

Given a particular hazard equation and process flow diagram, the FTS program assembles a digraph for the complete process. The assembly of the process digraph requires consideration of the gains and time constants for each input/output relationship and for loops within the digraph. The digraph is analyzed to determine the dominant loops with respect to gains and dynamics.

This reduced digraph is converted to a signed digraph where the gains are $+1, 0, -1, +10$, and -10. The gains of ± 10 indicate large changes which exceed the capacity of corrective actions such as occur with negative feedback loops. Modules also have been developed for the human operator's actions in the sensing of variables, computation of control action, and taking control action. External failure models that predict the propagation of failures outside of the process pipes are also being developed.

Synthesizing the fault tree

Lapp has developed an algorithm which deduces the correct system fault tree from a signed digraph for the process. The algorithm is based on a general classification of cut sets in signed digraphs. The key features of the algorithm follow:

1) The topology of the digraph is extremely important. Negative feedback and feedforward loops are detected and their elements determined. Cases of nested loops are also considered. 2) Conditional expansion of events is performed. That is, certain events may preclude others from occurring. The test for these conditions is performed at each expansion of an event. 3) The changes in relationships between variables due to failures are included. 4) Common cause failures are detected directly from the digraph. 5) Human operator actions are included. 6) Large deviations from normal conditions that alter relationships between variables are considered. 7) Events which have been previously developed are detected and copied. This results in a large computation time savings.

Fault tree synthesis by this algorithm is rapid. Trees containing 100 gates are generated in 10 cpu sec. on an IBM-360-67 computer. Following generation, the trees are "drawn" on a line printer.

The fault tree is passed to a subroutine which first places the tree in its minimal cut set form. An algorithm similar to that used by Fussell and Vesely (*3*) has been developed for this task. Once in cut set form, probability calculations are performed. At present, simple deterministic probability values are used. We are extending the algorithm to handle time dependent failure rates with repair.

Consider the flow diagram given in Figure 3. Ammonia and hydrogen sulfide are being steam stripped from a refinery stream. The bottoms from the column go to a biological waste treatment facility. The "bugs" used in this facility are very sensitive to the concentration of ammonia in the waste. Several "kills" of the bugs have occurred due to misoperation or failures of the stripper system. These losses of the waste disposal unit have caused fairly large releases of organics to the river into which the unit discharges.

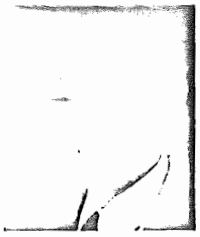
The stripper system contains several control loops for maintaining the constant operation of the unit. A reduced digraph for the concentration of ammonia in the bottoms, Figure 4, was constructed from unit models for the valves, sensors, controllers, stripper column, pressure relief valve, etc., that make up the stripper system. The fault tree for this digraph is given in Figure 5.

From the fault tree and probability data on the causing events it is possible to determine the important sets of events which might lead to high ammonia concentrations. Corrective designs could then be considered if the probability of occurrence proved to be too high. #

Literature cited

1. Powers, G. J., and F. C. Tompkins, Jr., "A Synthesis Strategy for Fault Trees in Chemical Processing Systems," Loss Prevention, **8**, *CEP* Technical Manual, AIChE, New York (1974).
2. Fussell, J. B., G. J. Powers, and R. G. Bennetts, "Fault Trees—A State of the Art Discussion," *IEEE Trans. on Reliability*, **R-23** (1) (April, 1974).
3. Fussell, J. B., and W. E. Vesely, "A New Methodology for Obtaining Cut Sets for Fault Trees," *Trans. Am. Nuclear Soc.*, **15** (1) (1972).

G. J. Powers is associate professor of chemical engineering and director, Design Research Center, at Carnegie-Mellon Univ. He has worked for the Ethyl Corp., Dow Chemical Co., and taught for several years at M.I.T. A consultant to numerous chemical companies in the area of process safety analysis, he has published several papers on the safety analysis of chemical processes and is the co-author of the text, "Process Synthesis." Powers earned his B.S.Ch.E. from the Univ. of Michigan and his Ph.D. from the Univ. of Wisconsin.



S. Lapp is research associate, Dept. of Chemical Engineering, Carnegie-Mellon Univ. Currently involved in the development of computer programs to aid in the generation and analysis of fault trees for chemical processes, Lapp has published several papers on fault tree analysis. He earned his B.S.Ch.E. at Carnegie-Mellon Univ.