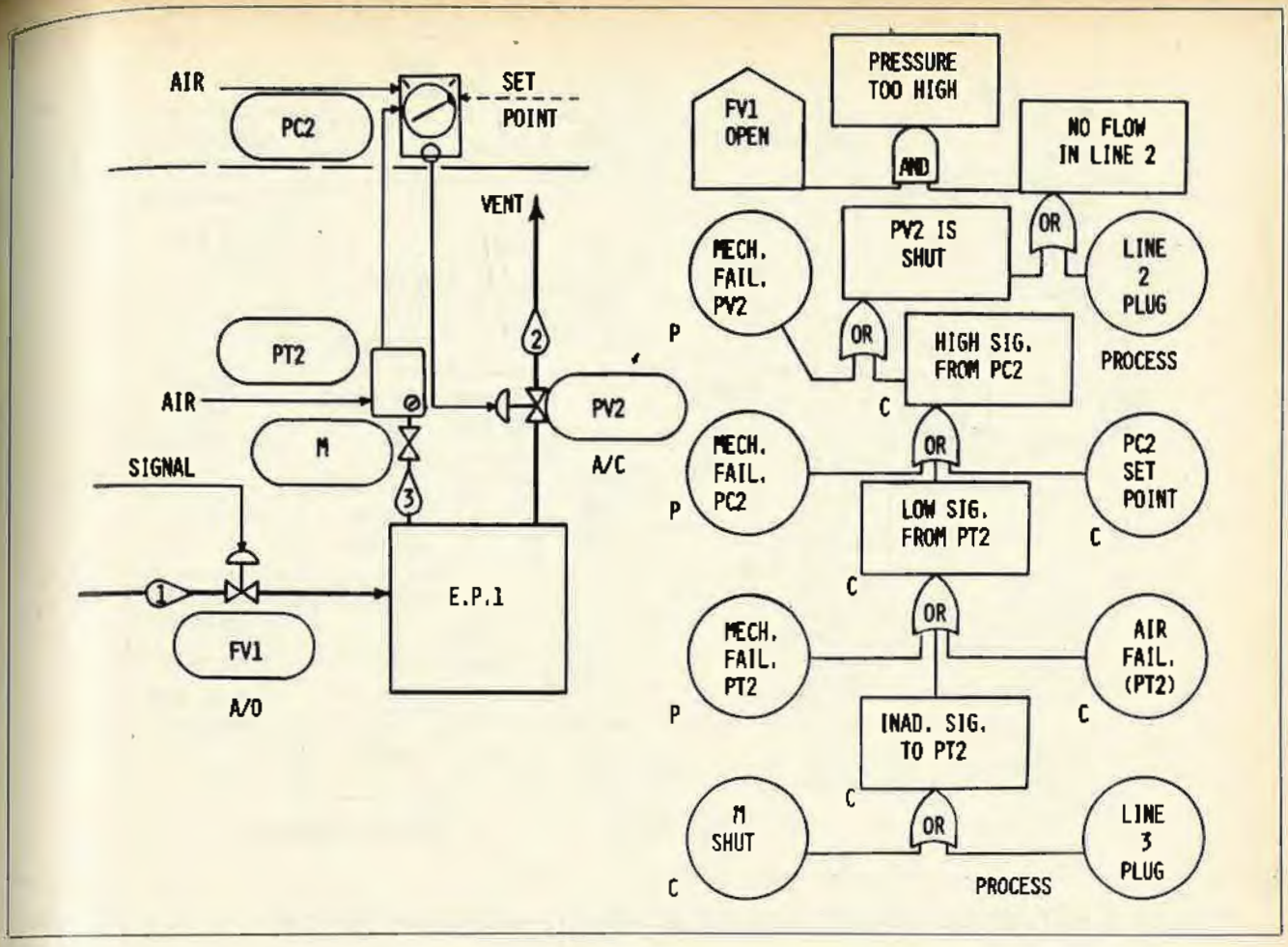


Figure 1. Effect-to-cause control system: primary/command/secondary procedure.

Application of Fault Tree Analysis

One of the advantages of Fault Tree Analysis is that process safety can be improved to any extent desired by restructuring the Tree and recalculating the top event frequency.

R. W. Prugh, Du Port Co., Wilmington, Del.

Recently, there have been considerable discussions on the basic concepts of Fault Tree Analysis and associated computational problems (*1–7*). However, the construction of Fault Trees has been addressed only in a limited manner (*8*). This article presents several standard and novel approaches to Tree construction.

Fault Tree Analysis was first used in the Du Pont Co. in 1966, about five years after its development at Bell Laboratories. This technique could not be immediately applied to chemical process safety analysis because the mathematical evaluation methods had been developed for batch, non-repairable systems. The appropriate equations for continuous processes were devised in the early 1970s, and the use of Fault Tree Analysis has progressed rapidly in the last few years.

It was recognized early on that considerable technical effort would be required to construct and evaluate Fault Trees. Du Pont's Engineering Service Division started to

0360-7275/80/3824-0059 $01.00 © 1980 AIChE

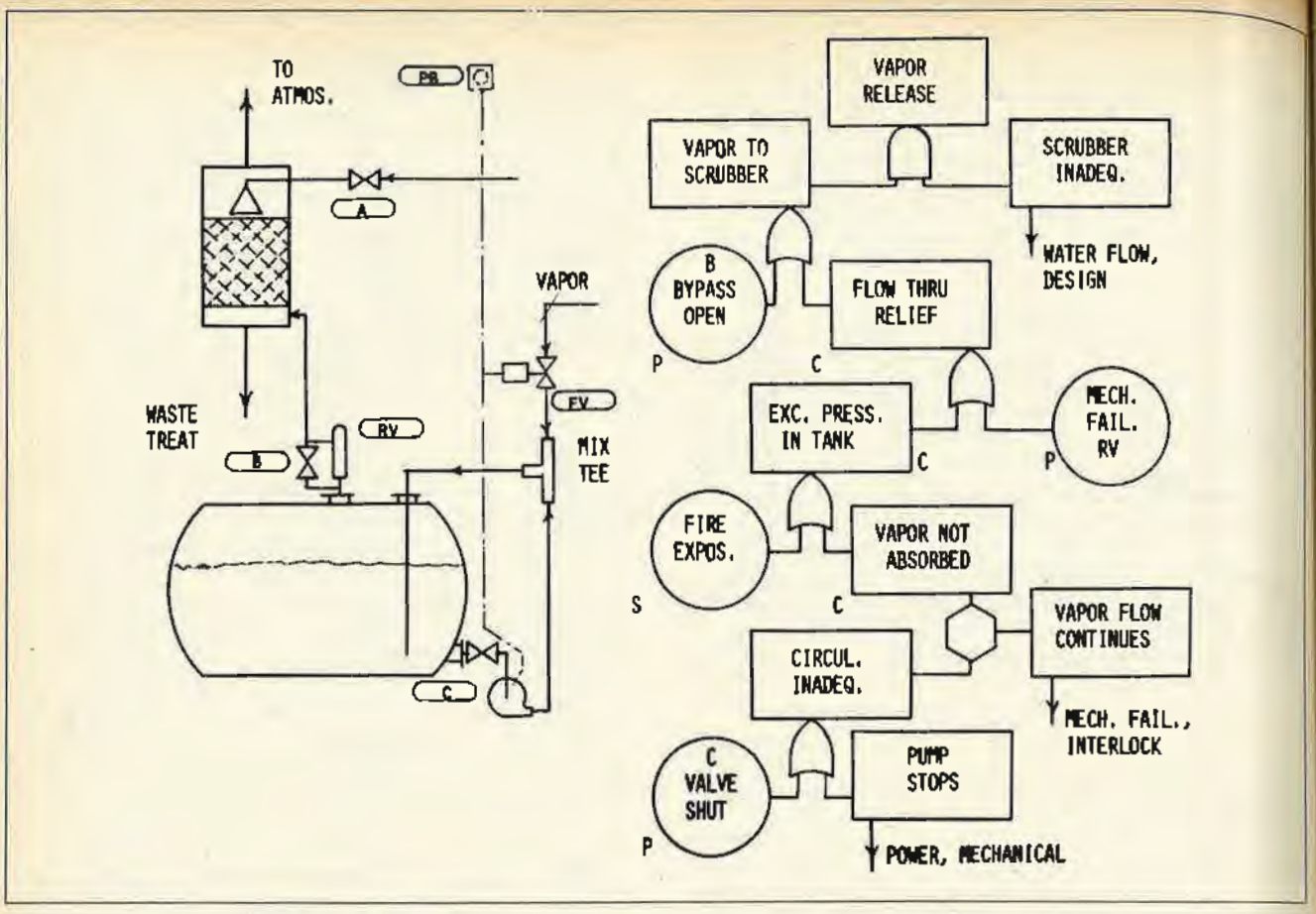


Figure 2. Effect-to-cause process: primary/command/secondary procedure.

develop construction and evaluation procedures which would minimize the effort without reducing the benefits of intensive investigation. Thus, a few guiding principles have been assembled, devised, and disseminated to assist analysts in constructing Trees. The following are several examples.

Effect-to-cause procedure

Figure 1 shows the standard symbols: rectangles, for failure events, including the Top Event at the top of the Tree or branch; circles, for basic causes; *house* symbols for high-probability normal events; and symbols for the AND and OR gates.

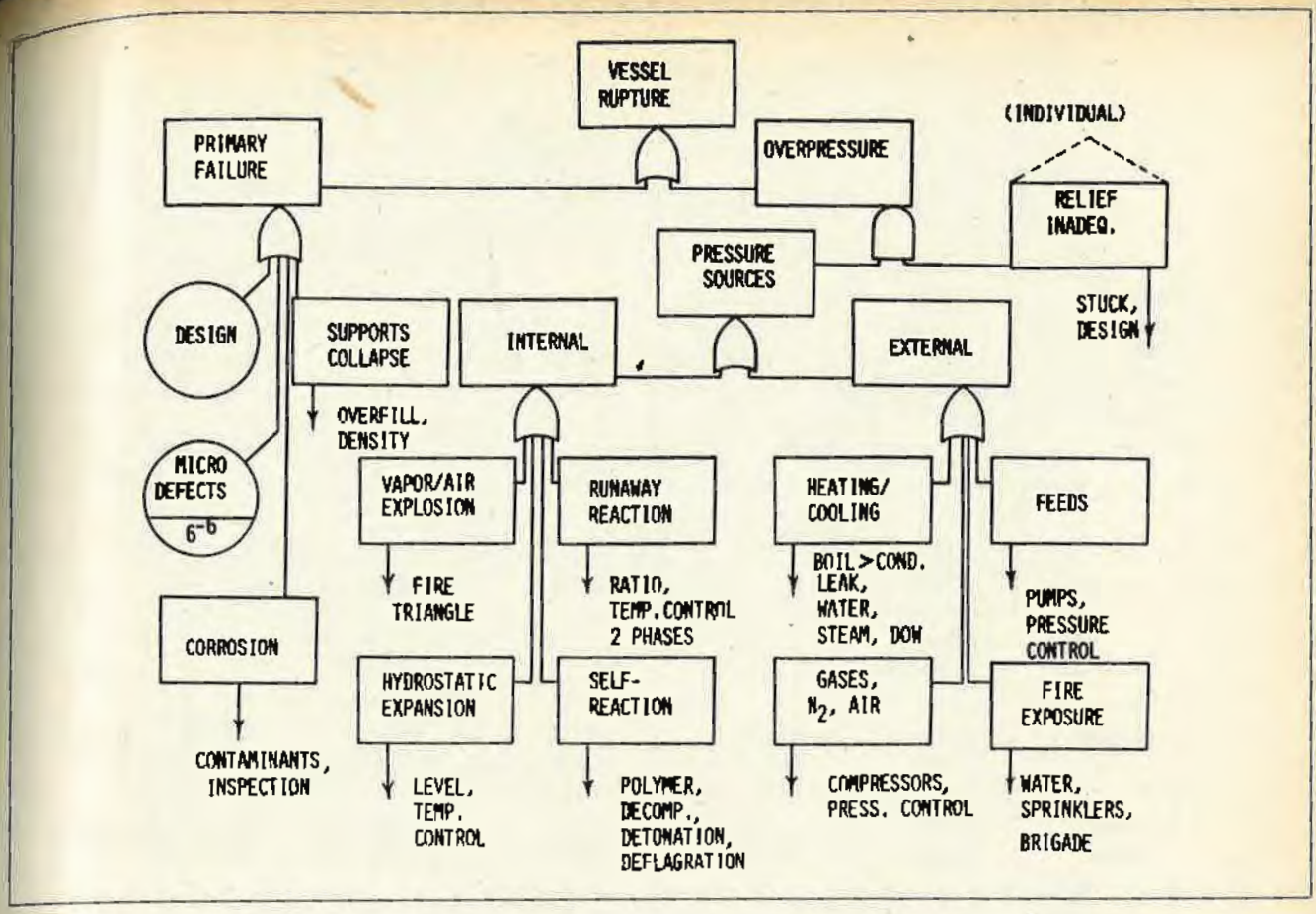
Construction of a Fault Tree is a deductive process, and the analyst works backward from effects toward causes. A good example of this method is found in the procedure for constructing branches for control systems. One starts at the component which acts on the process (usually a control valve) and works backward along the signal path toward the source (usually a sensor). Each component along the path has a primary (mechanical or internal) failure mode, and many components also can be commanded to fail by applying an undesirable control signal. For example, the pressure-control valve (PV2) can be *commanded* to close by applying a high-pressure air signal to this air-to-close valve. Similarly, the controller can be commanded to produce an unsafe, high output signal by reducing the signal from the pressure transmitter (PT2). Secondary (external) causes are those which can cause simultaneous failures of several components, as the result of an earthquake, nearby explosion, etc.

Note that the branch below *PV2-is-shut* consists of only OR gates, and this branch would be qualitatively and quantitatively the same with the one OR gate and seven inputs. The reason for proceeding stepwise backward along the signal path is to assure that all of the important causes are included.

The method on backward progression to develop branches can be occasionally applied to processes. This is particularly true if the Top Event is at the end of the process. In Figure 2, the analyst is concerned with venting a toxic material to the atmosphere. He starts backward into the process to develop causes for scrubber failure if the material enters the scrubber and also determines why the material would enter the scrubber. The path leads backward through valves, the storage vessel, the mixing circuit, and into the control systems, to develop the required branches of the Tree.

Vessel rupture is a major concern for safety analysts, because personnel may be injured and property loss may be severe. Figure 3 illustrates many of the common causes of vessel rupture, including mechanical (primary) failure and rupture from excessive internal pressure. At each of the precursor subevents, branches would extend downward to show how the subevent could occur. For example, at *heating/cooling* for a distillation column, there would be a branch showing excessive boil-up without compensating increased condensing capability OR failure of condensing capability without shutoff of boil-up.

It is likely that a relief device provided on the vessel of interest would perform differently for each cause of overpressure. For example, a relief valve may safely vent only 1% of vapor/air explosions, but may safely vent 95% of runaway reactions and 99% of excessive nitrogen-purge rates. Therefore, it may be necessary to construct a Tree which shows the effectiveness of relief for each cause; thus, the Tree would be considerably more complicated than the



▲ **Figure 3. Source analysis.**

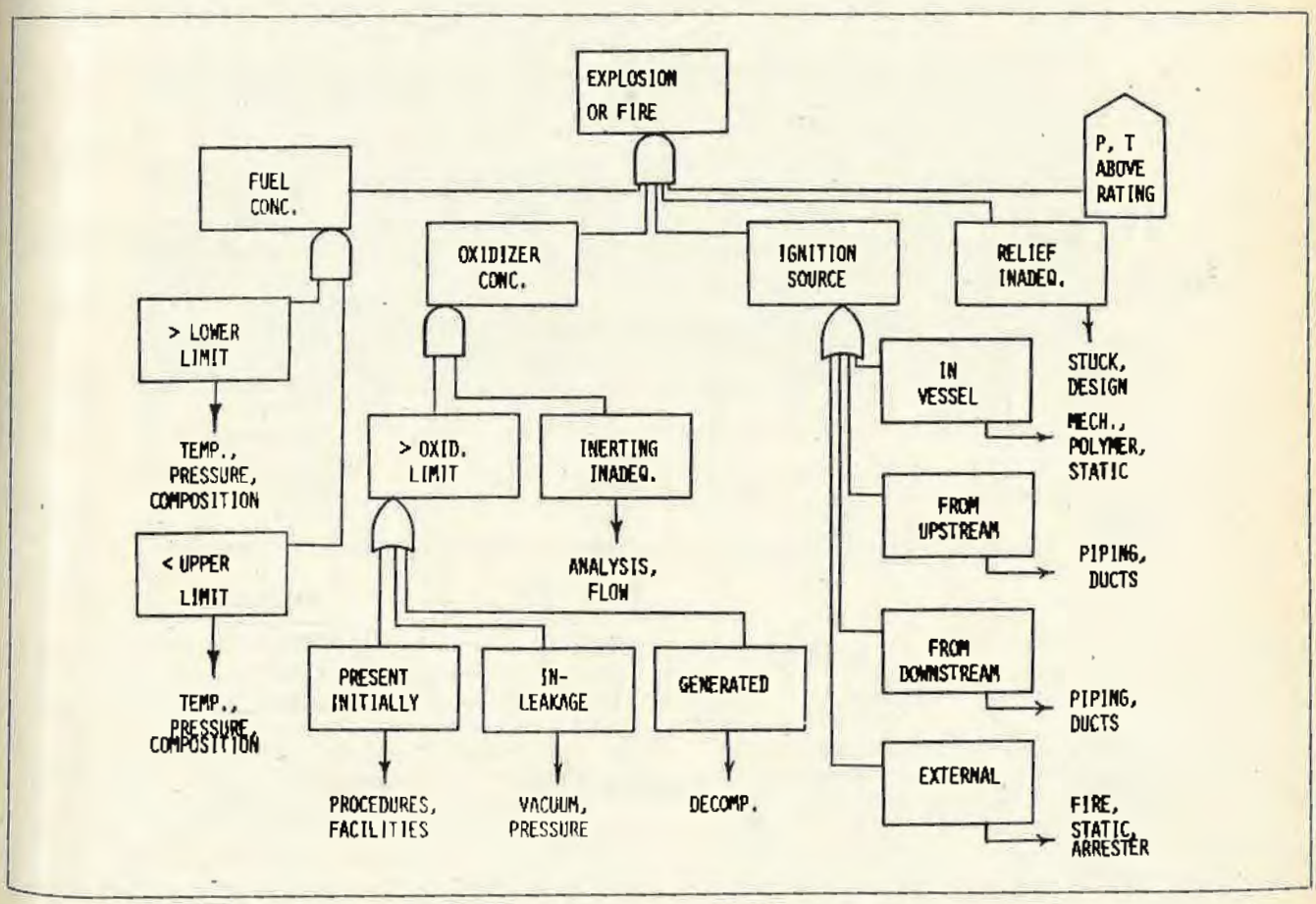
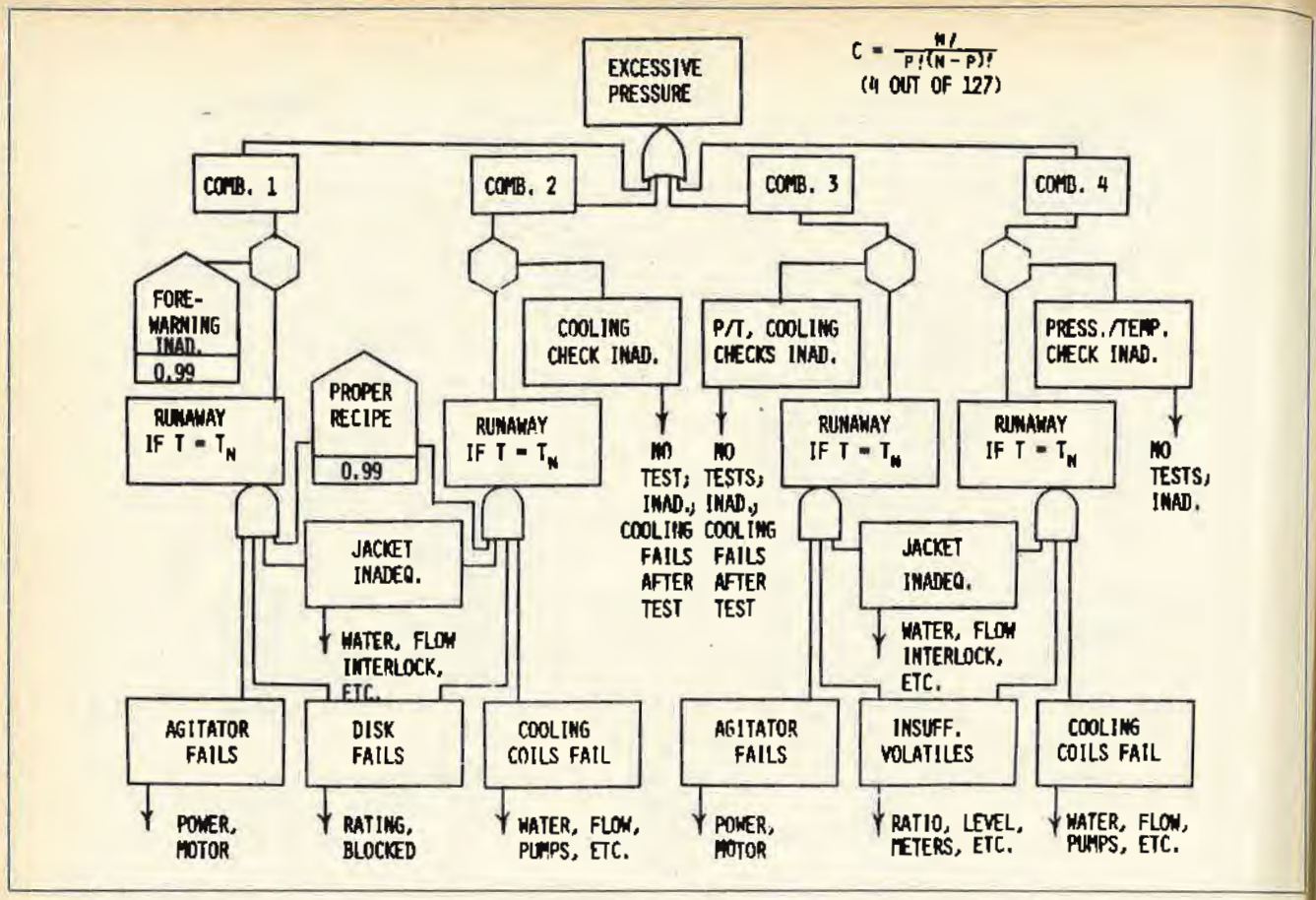


Figure 4. Fire triangle.



▲ Figure 5. Batch combinations.

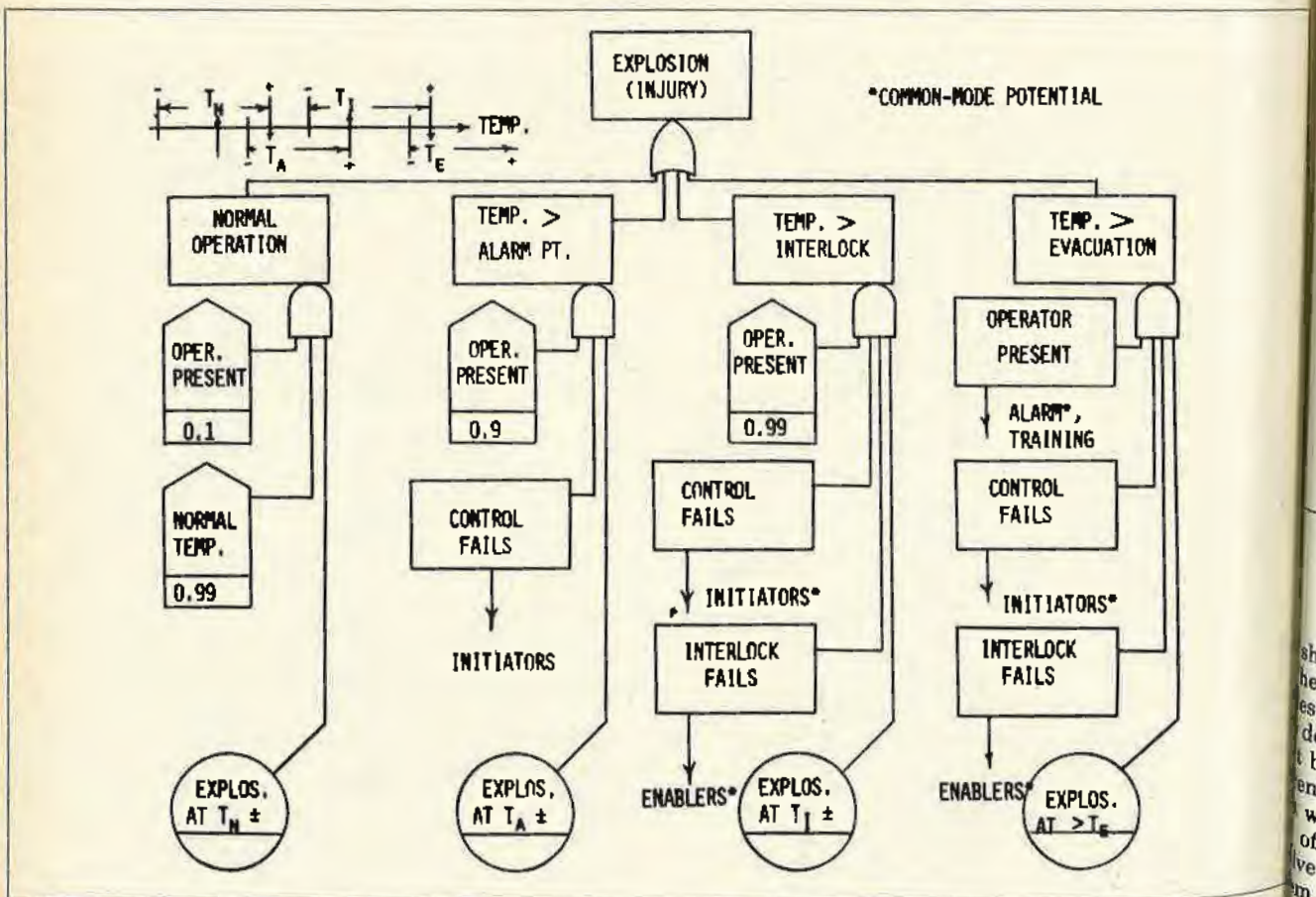


Figure 6. Action points.

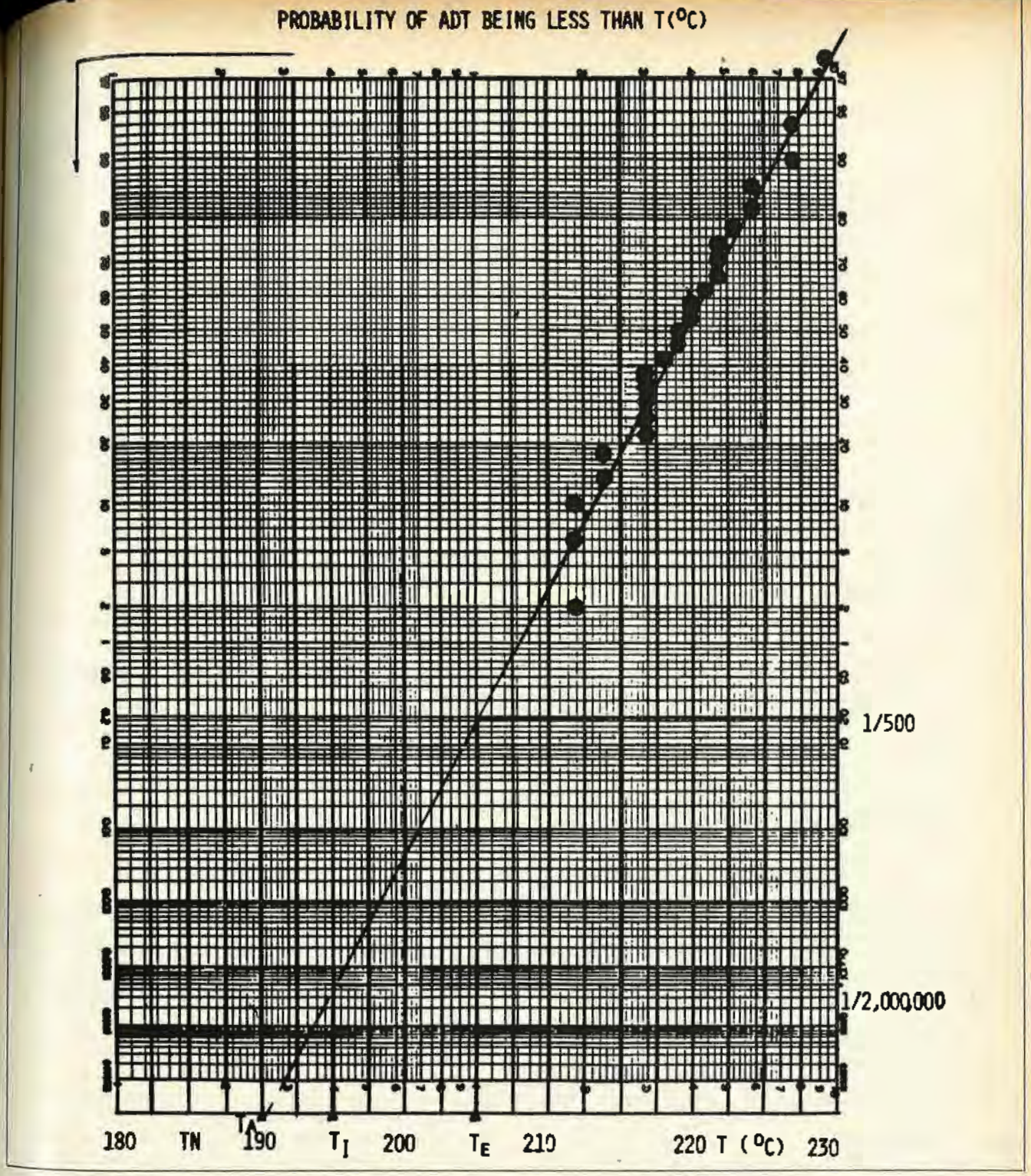


Figure 7. Distribution of auto-decomposition temperatures.

one shown here.

The causes of hazardous fire or explosion, Figure 4, can be described in a Fault Tree similar to the fire triangle. Not only does fuel have to be present, but the fuel concentration must be within the flammable range. Whether or not the concentration is above the lower limit and below the upper limit will depend on temperature, pressure, and composition of the vapor source. Presence of an oxidizer may involve in-leakage of oxidizer and failure of an inerting system. Several types of ignition sources may occur in a process, and the causes for each type should be determined and placed on the Tree. An explosion may not be hazardous, if it can be safely contained or relieved. Thus, the probability of the vessel withstanding an explosion (or fire) and the causes of overpressure-relief (or fire-protection) failure should be developed.

In many well-designed processes, there are several safeguards to prevent hazardoos loss of control, Figure 5. These include temperature, pressure, and ratio controls, alarms, overrides or excursion limits, interlocks, emergency-cooling facilities, automatic vent valves, relief valves, and rupture disks. Failure of all of them most probably would cause a serious incident, while failure of only one would be inconsequential. However, failure of three or four in various combi-

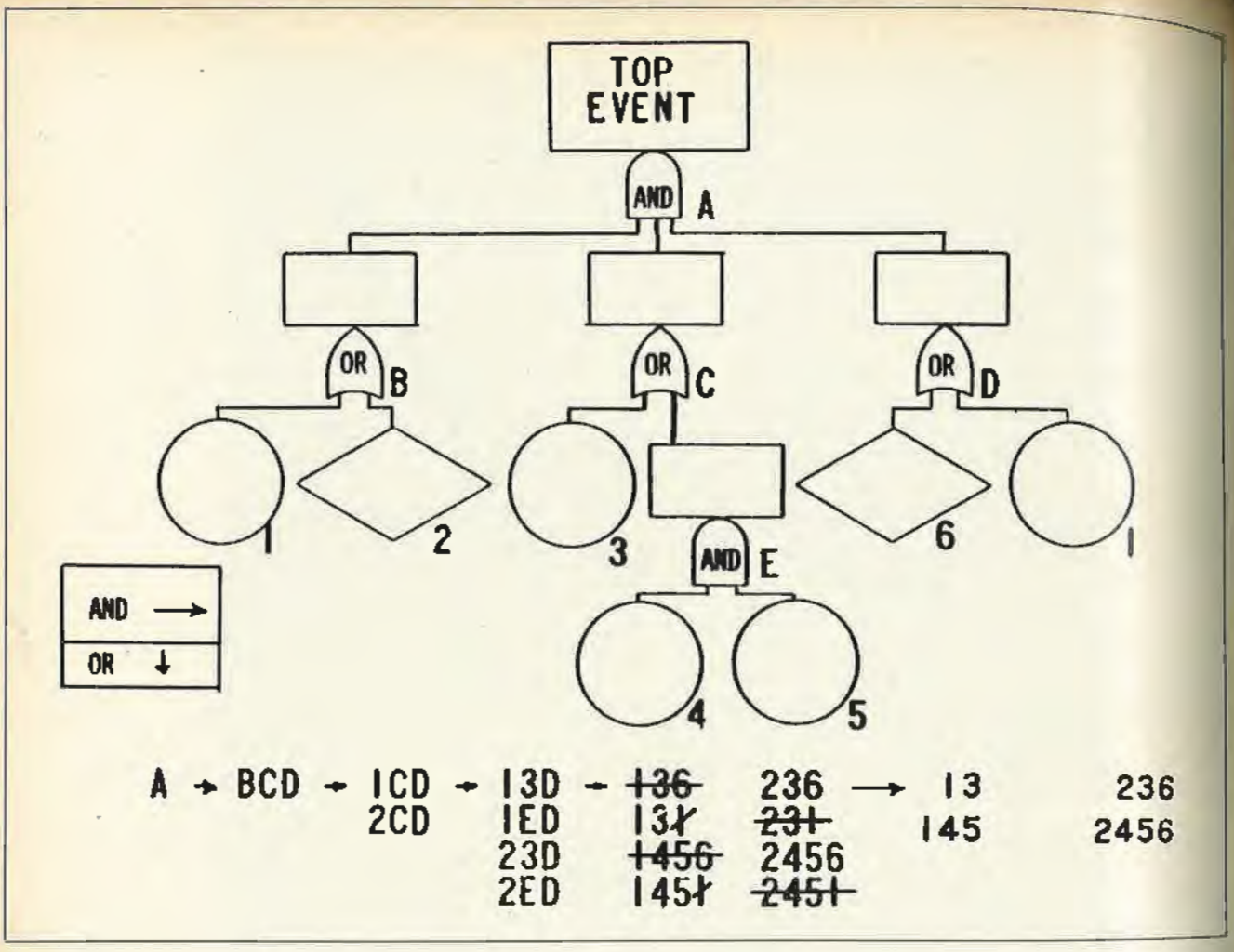


Figure 8. Failure and resolution.

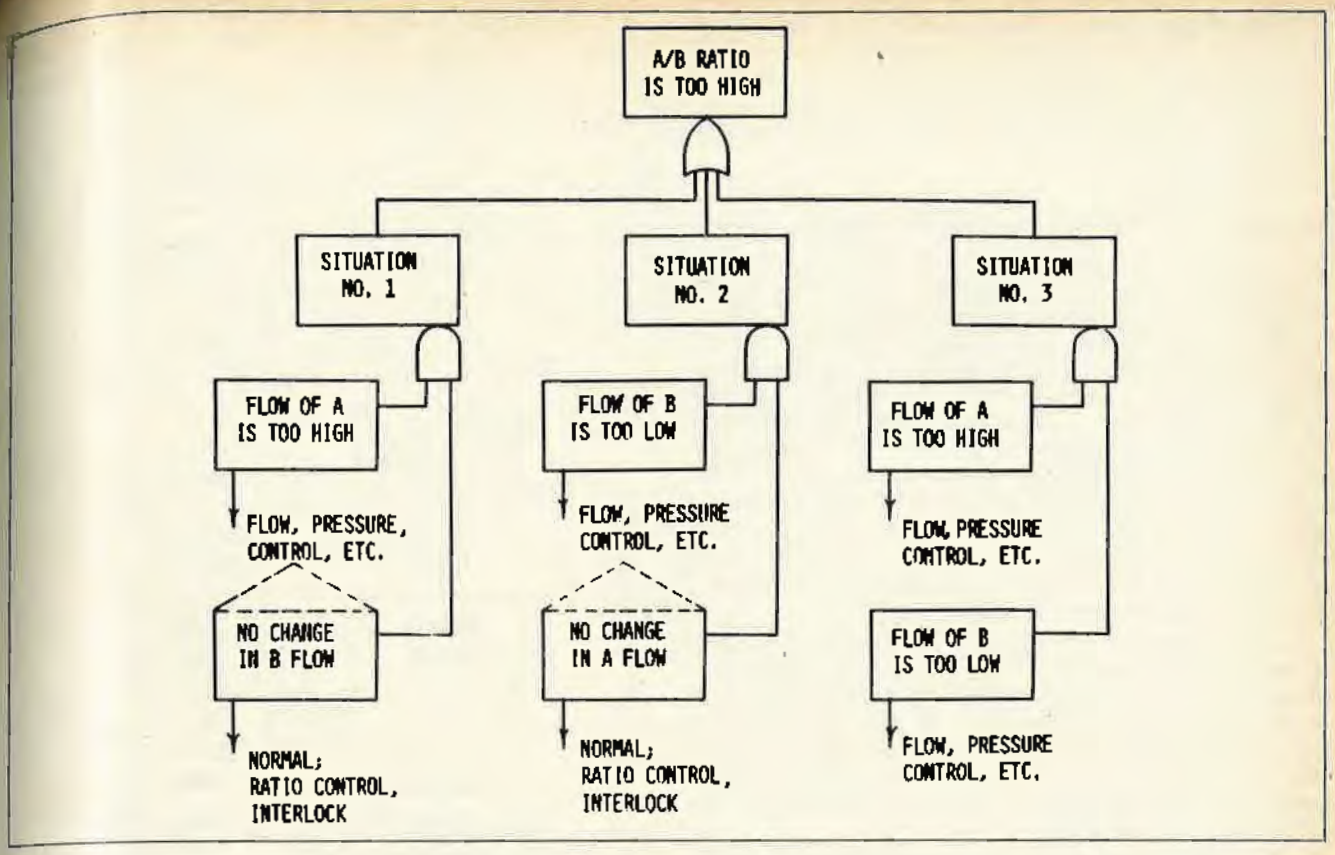
nations may also lead to an undesired incident. The Tree structure shown covers a batch process where one combination of three failures, two combinations of four failures, and one combination of five failures would cause the undesired excessive pressure. In this case, seven safety features were identified, and from the equation for combinations, there were 127 combinations which had to be evaluated to arrive at the four critical combinations shown in the Tree.

One approach to constructing a Fault Tree for a process is to determine the temperature or pressure levels at which automatic systems or the operator should act to control a process. In Figure 6, four important temperatures were identified: the normal operating temperature (185°C), the temperature alarm point (190°C), the temperature at which the interlock system should shut down the process (195°C), and the temperature at which a building-evacuation alarm sounds (205°C). To estimate the probability of explosion and injury, it would be necessary to evaluate the probability of the operator (or other persons) being present, the frequencies of control, interlock, and evacuation-alarm failures, and the probability of the unstable process material exploding at each temperature of interest.

To estimate the probability of explosion, it would be necessary to test the material and determine the temperature at which it would auto-decompose and explode. As is probably typical, there is not one auto-decomposition temperature but, instead, a range of temperatures. The data for tests on 25 batches of the starting ingredient plotted on a probability graph, Figure 7, indicate that there is a normal distribution of auto-decomposition temperatures. If this normal behavior can be assumed to extend to temperatures corresponding to normal operation, and the alarm, interlock, and evacuation temperatures, it is possible to estimate the probabilities needed for evaluation of the Fault Tree. For example, the graph indicates that one batch in each two million could be expected to explode after the high-temperature alarm sounds but before the interlock system could actuate to shut down the process.

This example also introduces the problem caused by common-mode failure. For example, the failure of a temperature sensor may cause the temperature control system to fail and also cause the interlock circuit and evacuation alarm to fail. Common-mode failures are identified when the same basic cause appears in two or more branches which meet at an AND gate. The Tree must be restructured to show the common-mode failure properly, or the subsequent qualitative and quantitative evaluations will be seriously incorrect and in an unsafe direction. A simple procedure for common-mode failure resolution, Figure 8, involves a stepwise replacement of events by inputs to their gates, following the rule: AND gates—inputs placed horizontally in the table; OR gates—inputs inserted vertically in the table.

An incorrect ratio of reactants can lead to runaway reactions or other incidents in many processes. The Tree structure in Figure 9 involves three situations which should be evaluated. Situation 1 is where the flow of one reactant (A) is too high and the flow of the other reactant (B) fails to increase proportionately to maintain the required safe ratio. Situation 2 is the reverse of the first, where the flow of one reactant (B) is too low and the flow of the other (A) fails to



▲ **Figure 9. Reactant ratios.**

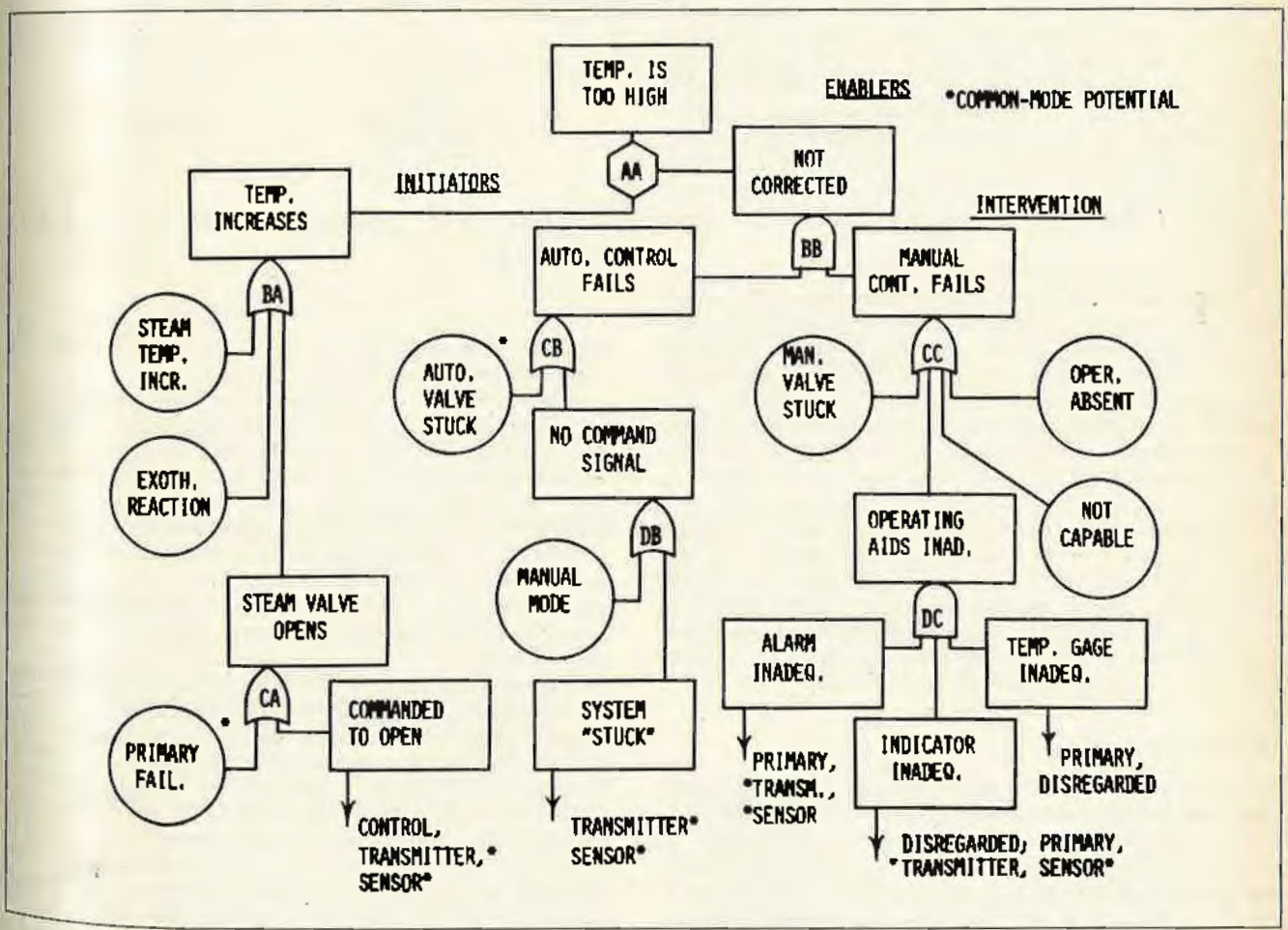


Figure 10. Initiators/enablers/intervention.

decrease proportionately—or stops altogether—to maintain a safe ratio. The third situation is where the reactant flows deviate unsafely in opposite directions at the same time; in most cases, the probability of this occurring is much less than either of the first two situations and does not need to be shown on the Tree.

Initiators, enablers, and intervention

The concept of initiating failure events and enabling failure events can aid in constructing a Fault Tree, Figure 10. Initiating events cause unsafe changes in a process; enabling events allow these initiating events to become more serious. These events allow opward progression of failure events in a Fault Tree. Enabling failures (such as stuck relief valves) are not usually detected when the failure occurs, but only during deliberate tests or as the result of a *demand* by the process. Thus, long failure durations (detection plus repair times) are associated with some enabling failures. On the other hand, the duration of an initiating event (such as failure of a steam pressure regulator or a lightning stroke) usually is short enough to be inconsequential in the fault tree calculations.

For most processes, the operator is an important element of process control. Indicators, alarms, and emergency-shutdown devices are provided by the process designer to enable the operator to intervene in case the automatic controls fail and then bring the process to a safe condition. The important aspects of human intervention (presence, capability, and operating aids) are shown on the Tree for later quantitative evaluation.

"Daisy Chain Manner." Some hazard incidents occur in a stepwise manner, Figure 11. Thus, there is a sequential relationship between the causes. This applies particularly to vehicle accidents and probably to many types of hatch processes. As shown in a Fault Tree for a ship accident, the analyst determines how frequently a collision course occurs (while entering a harhor, for example). He then estimates the probahility that the ship would fail to change course to avoid collision. In this combination of failures, a collision would occur unless the ship, which is about to be struck, does not move out of the way. Other aspects of accidents are evaluated similarly to estimate the frequency of cargo release.

In many processes, the hazards involved in starting up or shutting down a process are more serious than those which could occur during the continuous phase of operation. This situation might arise, if it is necessary to bypass interlock systems during start-up or to pass through a hazardous ratio of reactants during some types of shutdowns. To combine these different phases of operation in a Fault Tree, it is necessary to combine the batch type operations (the start-ups and shutdowns) with the continuous operation. This is accomplished by determining the per-year frequencies of occurrence and then adding them, as shown in Figure 12. The reciprocal of the sum is the average interval of Top Event occurrences or the probability of the Top Event occurring in terms of chances per year. This example also shows the mathematical method for combining frequencies and durations at AND, INHIBIT, and OR gates. These equations are presented in Tahle 1.

In summary

These Fault Tree structures do not cover all aspects of all processes, but may serve as models for Fault Tree construction. As Fault Tree Analysis continues to be applied to chemical processes, other useful models will be developed. For example, the Primary/Command/Secondary concept may be applicable to the chemistry of a process: primary (internal) failures may involve instability of ingredients or reactions, command failures may involve mixing, catalysis,

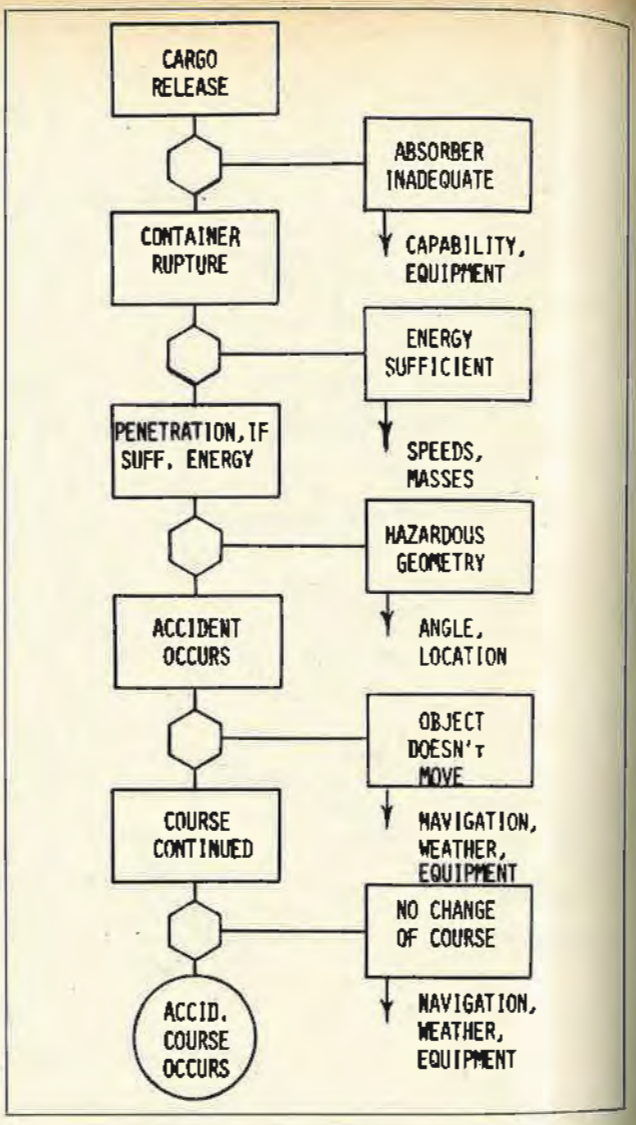


Figure 11. Daisy-chain (cause-to-effect).

etc., and secondary (external) failures would involve fire exposure, loss of utilities, etc.

One of the important results of Fault Tree Analysis is the calculated frequency of Top Event occurrence. For example, a Fault Tree may indicate that the process would explode at average intervals of 10 years. One of the advantages of Fault Tree Analysis is that the process can be improved by the analyst with subsequent restructuring of the Tree and recalculation of the Top Event frequency to any desired extent. The frequency of process explosion could be reduced to one chance in 1,000 per year (an average interval of 1,000 years) by adding an interlock system to the process controls.

Several questions arise. Would the original 10 years have been acceptable? If not, is the 1,000-year interval obtained with the interlock system acceptable? At what points (frequency or interval) would proposed process improvements be considered required or "gold-plating?" Other considerations include evaluating the exposure of operators, other personnel, and the public to process hazards (in relation to other day-to-day exposures to accidents and Act-of-God hazards), and the extent of property damage and business-interruption losses. Gibson (*9*) discusses some of the considerations and criteria recently taken by some companies for acceptability of process risks.

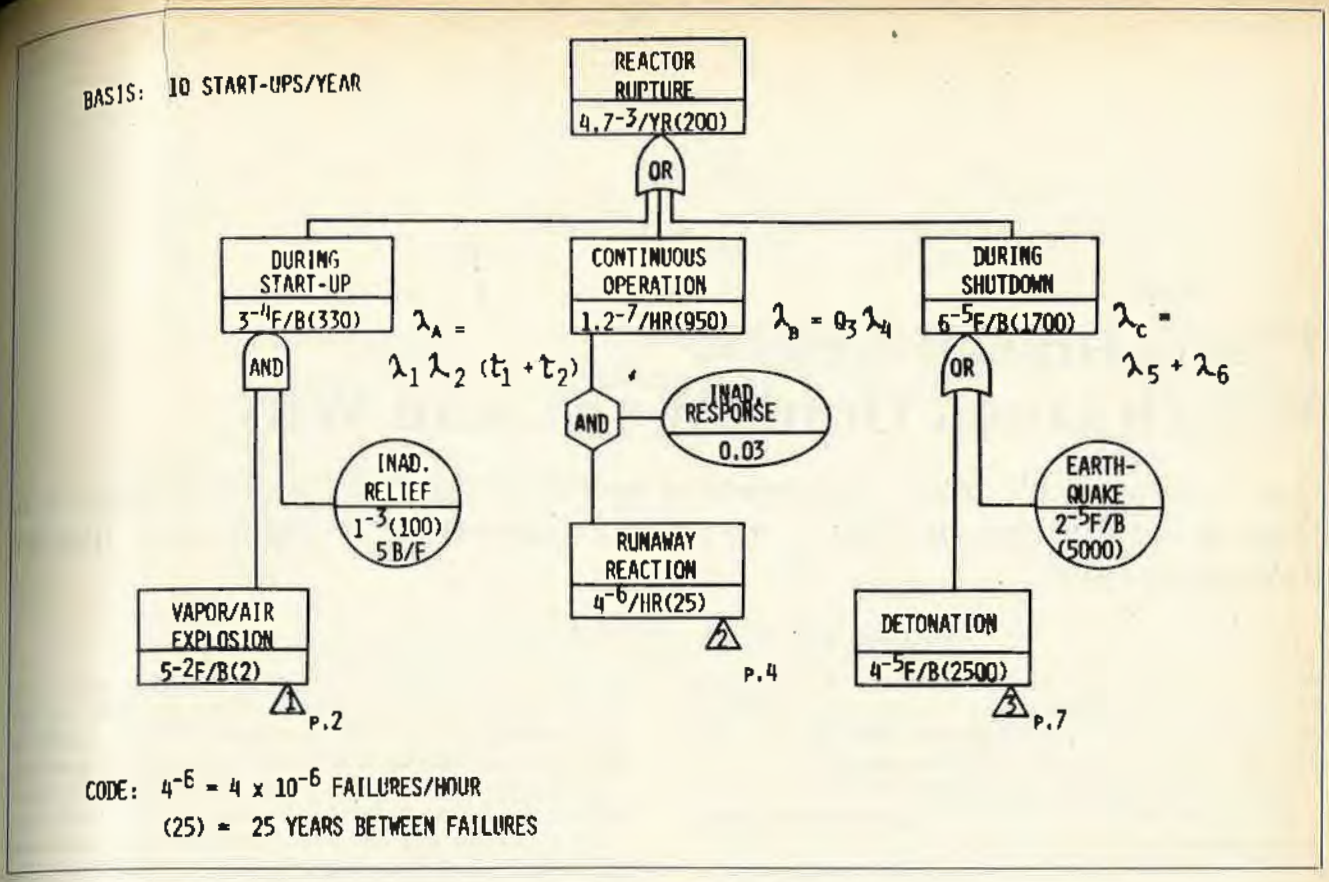


Figure 12. Combining batch and continuous operations.

Table 1. Fault tree equations.

		Logic Gate Formulas		
		2 Inputs	3 Inputs	i Inputs
AND	λ	$\lambda_1\lambda_2(\tau_1+\tau_2)$	$\lambda_1\lambda_2\lambda_3(\tau_2\tau_3+\tau_1\tau_3+\tau_1\tau_2)$	$\Sigma\,(1/\tau_i)\times\Pi\,Q_i$
	τ	$\frac{\tau_1\tau_2}{\tau_1+\tau_2}$	$\frac{\tau_1\tau_2\tau_3}{\tau_2\tau_3+\tau_1\tau_3+\tau_1\tau_2}$	$\frac{1}{\Sigma\,(1/\tau_i)}$
OR	λ	$\lambda_1+\lambda_2$	$\lambda_1+\lambda_2+\lambda_3$	$\Sigma\,\lambda_i$
	τ	$\frac{\lambda_1\tau_1+\lambda_2\tau_2}{\lambda_1+\lambda_2}$	$\frac{\lambda_1\tau_1+\lambda_2\tau_2+\lambda_3\tau_3}{\lambda_1+\lambda_2+\lambda_3}$	$\frac{\Sigma\,Q_i}{\Sigma\,\lambda_i}$
INHIBIT	λ	$\lambda_1 Q_2$	$\lambda_1 Q_2 Q_3$	—
	τ	τ_1	τ_1	—

The above relationships apply only where the product of λ and τ (which equals Q) is substantially less than 1.0.

Literature cited

1. Brown, D. B., "Systems Analysis and Design for Safety," Chapter 5, p. 152, Prentice-Hall (1976).
2. Fussell, J. B., "Fault Tree Analysis—Concepts and Techniques," p. 133, in "Generic Techniques in Systems Reliability Assessment," by E. J. Henley and J. W. Lynn, Noordhoff International Publishing (1976).
3. Gibson, S. B., "The Design of New Chemical Plants Using Hazard Analysis," p. 135, in "Process Industry Hazards," AIChE Symposium Series No. 47 (1976).
4. Malasky, S. W., "System Safety," Chapter 5, p. 142, Spartan Books (1974).
5. Rasmussen, N., *et al.*, "Reactor Safety Study," Appendix II, USAEC; WASH-1400 (August, 1974).
6. Yellman, T. W., "Comments on Fault Trees—A State of the Art Discussion," *IEEE Transactions on Reliability, R-24* (5), p. 344 (December, 1975).
7. Young, J., "Using the Fault Tree Analysis Technique," p. 827, in "Reliability and Fault Tree Analysis," by R. E. Barlow, *et al.*, Soc. for Ind. & Appl. Math. (1975).
8. Powers, G. J., and F. C. Tompkins, "Fault Tree Synthesis for Chemical Processes," *AIChE J.*, **20**, p. 376 (March, 1974).
9. Gibson, S. B., "Hazard Analysis and Numerical Risk Criteria," AIChE 14th Annual Loss Prevention Symposium (1980).

R. W. Prugh, who has had 20 years of experience in Du Pont's explosives, organic chemicals and safety and fire protection units, is now in the Hazards Engineering Dept. of the firm. He is a registered engineer in Delaware, Pennsylvania, and New Jersey.