RISK REDUCTION OF OPERATING PROCEDURES AND PROCESS FLOWSHEETS

Vital Aelion, Gary J. Powers

EDRC 06-126-92

Risk Reduction of Operating Procedures and Process Flowsheets

by
Vital Aelion and Gary J. Powers
Department of Chemical Engineering
Carnegie Mellon University
Pittsburgh, PA

Abstract

A unified risk reduction strategy, that uses *Fault Tree Analysis,* proposes modifications in chemical operations that include the process flowsheet, control system, and operating procedures. The modifications commonly involve the establishment of *stationary states.* These states allow for longer process time constants and support intermediate state verification. *Relative importance* is used to identify quantitatively the dominant causes of risk, which are modified to produce safer and more reliable processes. The strategy is tested on the design of a pump system startup, and risk reduction of several orders of magnitude is achieved.

1. Introduction

Tighter constraints in safety, reliability, quality control, and environmental protection constraints require new process designs, which involve sophisticated control systems and high integrity operating procedures. This paper presents a risk reduction strategy for designing these operations.

The need for safer operations has been recognized both by the government and the private sector. Recently new legislation established standards for process safety management of chemicals and air pollution control (Department of Labor, 1990; The Bureau of National Affairs, 1991). The American Institute of Chemical Engineers (AIChE) established the Center for Chemical Process Safety (CCPS) in 1985. CCPS has developed and disseminated technical information for use in the prevention of major chemical accidents, and published a series of guideline books on process safety.

Operating procedures are crucial in process safety. High integrity operating procedure synthesis involves identifying and evaluating the important process aspects that collectively characterize successful operations. Such aspects include operator training, stability and verifiability of intermediate operating states, and flowsheets capable of supporting high integrity operating procedures. Relevant flowsheet characteristics may be plant layout, equipment redundancy, auxiliary equipment, and bypass/purge lines whose function is to allow safe and reliable transitions during operation.

Chemical process safety and reliability can be improved by considering four aspects (Englund, *et al.*, 1992): *equipment design, steady state* and *sequential operation, fault detection,* and *corrective action.* Our work presents a common framework, based on the use of *Fault Tree Analysis,* which evaluates these four process aspects, and suggests ways to improve the chemical operation.

2. Prior Work

Research in a multitude of fields is relevant to this work, ranging from operating procedure synthesis, overall process evaluation, risk analysis and assessment, discrete and continuous process simulation, planning and scheduling, flowsheeting, and others. The first three fields are briefly reviewed.

2.1 Operating Procedure Synthesis

Recent work in operating procedure synthesis has been based on artificial intelligence planning (Fusillo and Powers, 1987,1988a, 1988b; Lakshmanan and Stephanopoulos, 1988a, 1988b, 1990; Aelion and Powers, 1991), and on a combination of artificial intelligence and mathematical planning and scheduling (Crooks and Macchietto, 1992).

In our 1991 paper we present a methodology for the retrofit synthesis of flowsheets for

improving operating procedures, based on supporting stationary states. Stationary states exhibit the following characteristics (Fusillo and Powers, 1987):

1. The system is at steady state or changing very slowly.
2. The values of (most of) the variables lie between their initial and goal-state values.
3. Connections between a subsystem and its neighbors are closed, so the subsystems do not interact.
4. If the stationary state is capacitance related, it must be *effectively* isolated from its neighboring subsystems.

Stationary states often arise because of the presence of simultaneous inverse operations and/or large capacitance for a physical quantity, such as thermal energy, pressure or mass. A distillation column operating under total reflux, for example, exhibits a stationary state. Evaporation at the bottom of the column and condensation at the top is an example of simultaneous inverse operations. A stirred tank reactor may exhibit a stationary state when filled with one reagent and/or solvent and the contents are heated until the rest of the reagents are ready to be fed. This stationary state results from the capacitance of the reactor for material and thermal energy.

Stationary states have been used as *planning islands* in the synthesis of feasible operating procedures. They are capable of absorbing process transients, providing longer time constants, and improving verification of intermediate states. This work investigates the risk reduction of chemical operations which involve stationary states.

2.2 Overall Process Evaluation

The present work combines the risk assessment and retrofit design of the process flowsheet, control system, and operating procedures in one risk reduction design/analysis framework, and supports the design of inherently safer and more reliable processes. Similar approaches of combining traditionally separate design issues, include the work of Umeda (1982), who presents a hierarchical/iterative approach to design, and proposes objectives for each step of the design hierarchy. Other examples are the simultaneous synthesis and control of chemical processes (Grossmann and Morari, 1983), the synthesis of flexible processes (Pistikopoulos and Grossmann, 1988), the design of inherently controllable chemical processes (Huang and Fan, 1989), and others.

2.3 Risk Analysis and Assessment

Managing risk in chemical processing systems involves: (a) learning from past accidents, (b) developing methodologies to predict the likelihood and consequences of future accidents, and (c) inventing ways to reduce this risk. Quantifying risk requires the definition of the.

hazardous events, an estimate of their magnitude (consequences), and the likelihood (frequency) of each event

Responding to these needs, CCPS published two guidelines books, which review relevant methodologies currently in practice. (AIChE/CCPS, 1985) presents various structured qualitative techniques for identifying possible hazards in chemical facilities* (AIChE/CCPS, 1989a) is a comprehensive review of quantitative methods for analyzing acute risk hazards. This book presents methodologies for quantitative risk analysis, consequence analysis, event probability and failure frequency analysis, measurement calculation and presentation of risk estimates. Also, (AIChE/CCPS, 1989b) presents process equipment failure data, to be used in quantitative risk estimates.

Risk assessment, i.e. deciding what level of risk is acceptable, is frequently based on specific information and previous practices of each individual company. Analysis tools are helpful in this process by providing qualitative and quantitative information, and by helping to allocate resources in parts of the process which can be improved substantially.

3. Fault Tree Analysis (FTA)

Fault Tree Analysis, FTA, is a method for evaluating acute hazards in processes. FTA evaluates a set of undesirable events, specified by a designer. These are called *top events.* For each top event we develop a *digraph,* which models interactions among process variables. From each digraph *&fault tree* is built using the *Lapp-Powers Fault Tree Algorithm* (Lapp and Powers, 1977). Fault trees are composed of AND and OR logical gates, which trace the top and intermediate events to their causes. Events which are not traced to further causes are called *primal events.* These events can *have failure rates, mean time to detection and repair,* and *demand probabilities,* defined in section 5.1.

In addition to the failure rate of the top event, *minimal cut set* and *relative importance* analyses can be employed for qualitative and quantitative assessment A minimal cut set is a set of primal events which alone can cause the top event (Powers and Lapp, 1989). Qualitatively, the fewer the minimal cut sets and the larger the number of members in each minimal cut set, the safer the process. Quantitatively, minimal cut sets with higher failure rate contribute the most to the top event failure rate. Relative importance measures the fraction of the top event that is caused by an event (Delboy, *et ai,* 1991). Minimal cut set and relative importance information can be used in identifying ways to improve chemical processes. FTA is applicable to both steady state and sequential processes. An application to sequential systems appears in (Shaeiwitz, *et al.,* 1977).

In the next section, we use FTA for reducing the risk in chemical systems that include events which range from the failure of operator actions to that of valves. The analysis identifies the major causes of risk and provides guidance in improving the process.

4. Risk Reduction of Chemical Operations

A unified strategy for reducing the risk of a chemical operation is shown in Figure 1. The terms *chemical operation, design,* and *process* are used interchangeably to indicate a new or an existing process, including the flowsheet, control system, and operating procedures.

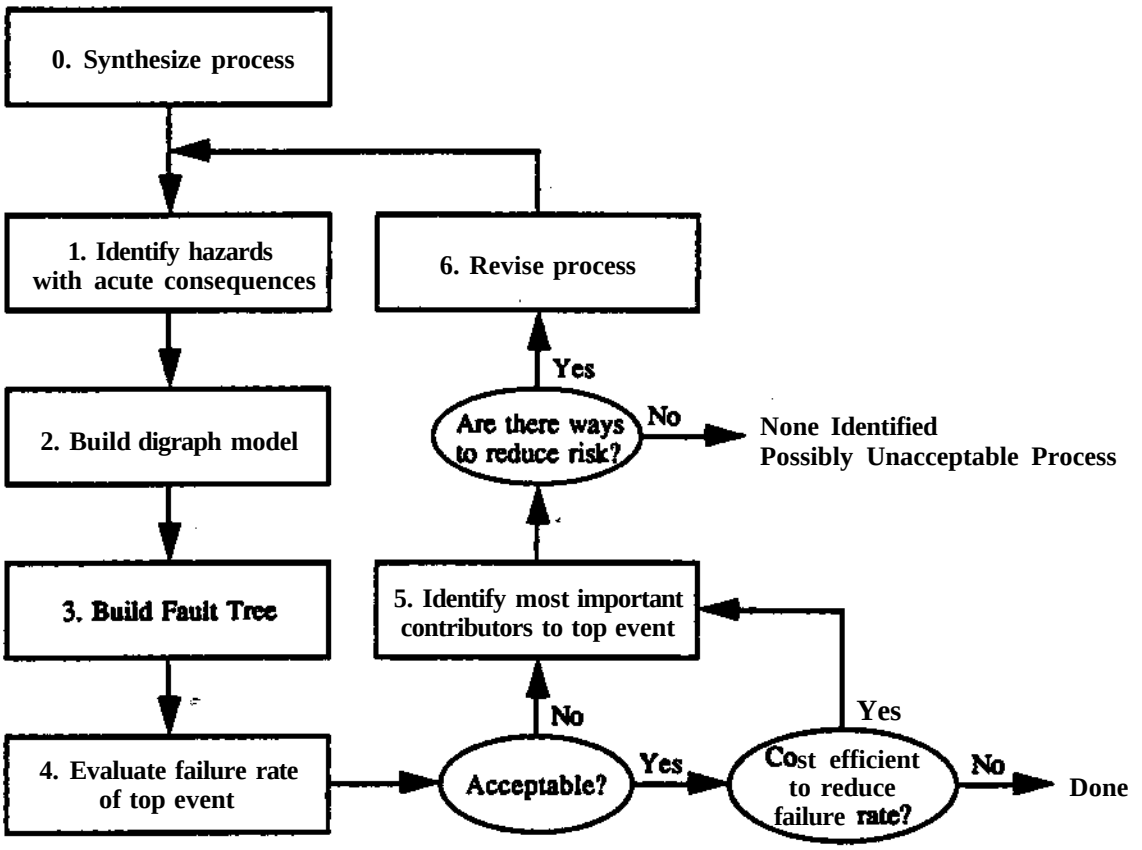

Figure 1. Unified Risk Reduction Strategy

In step 1, the designer identifies hazards in the process. This can be done by employing a number of methodologies, including hazards and operability studies (HAZOP), checklists, and others. (AIChE/CCPS, 1985) presents alternative techniques for hazards identification. Among the identified hazards, some are of small consequences and/or easily corrected. After correction, these require no further analysis. The remaining acute hazards are subjected to further analysis.

For each acute hazard, called a top event, a digraph model is built (step 2). This model is a causal network of interactions among process variables. Such variables may be flow, temperature, pressure, alarm warning, operator action, control response, and others. Each digraph is algorithmically turned into a fault tree (step 3). Primal event failure rates, demand probabilities and unavailabilities are used to compute the failure rates of the hazards (step 4).

Realizing that zero failure rates are practically impossible, we check if the failure rates of the hazardous events are acceptable. If so, we ask whether it is cost efficient to further reduce the likelihood of the top events. If not, the process in question is considered acceptable and the risk reduction is terminated. If either the failure rates are not acceptable, or the risk can be reduced efficiently, we proceed to identify the most important contributing scenarios to the top event failure rates (step 5). As explained in section 3, this analysis can be done by performing a minimal cut set analysis, or by computing the relative importance of the events in each fault tree.

Identifying the major contributors to the top event failure rates can provide targets for improving the operation. For example, if the analysis indicates that errors in specific procedural steps can be very dangerous, then we can emphasize operator training, require redundant checks of these steps, or replace some operator duties with more reliable automated alternatives, if such exist If certain subsystems have high failure rates during startup or shutdown, we can incorporate stationary states, which can improve verification, absorb process transients, and alleviate the burden of very short time constants. Based on such considerations, we propose modifications to the current design (step 6).

Most process modifications aim to improve specific aspects of the operation, but they may compromise others. Frequently, desirable process qualities such as safety, reliability, and controllability, are in conflict. In principle, every process revision requires a new risk assessment, as indicated by the algorithm of Figure 1. An application of the unified risk reduction strategy is demonstrated in the next section.

5. Pump Design. An Example

This example is motivated by (Englund, *et* a/., 1992), who present designs and operating procedures of *centrifugal* and *positive displacement* pump startups for preventing backflow. In this example we design a pump system and investigate the risk of fatality during startup. We consider systems which involve a centrifugal or a positive displacement pump.

The analysis in this example follows the steps of the unified risk reduction strategy, shown in Figure 1. Step 1 is the identification of hazards capable of causing fatalities. In this process, a large explosion/flash fire, which occurs either from an unwanted reaction inside the pump, or from a chemical release and subsequent ignition outside the pump, can cause fatalities.

Step 2 specifies that digraphs for each pump system and each event be built These digraphs model the causal relations among events in a process. Digraph models are omitted in this analysis. Based on these digraphs, we build fault trees for each event and each process alternative (step 3). The risk of fatality can be analyzed by the fault tree shown in Figure 2. In this tree the top event is *fatality*.

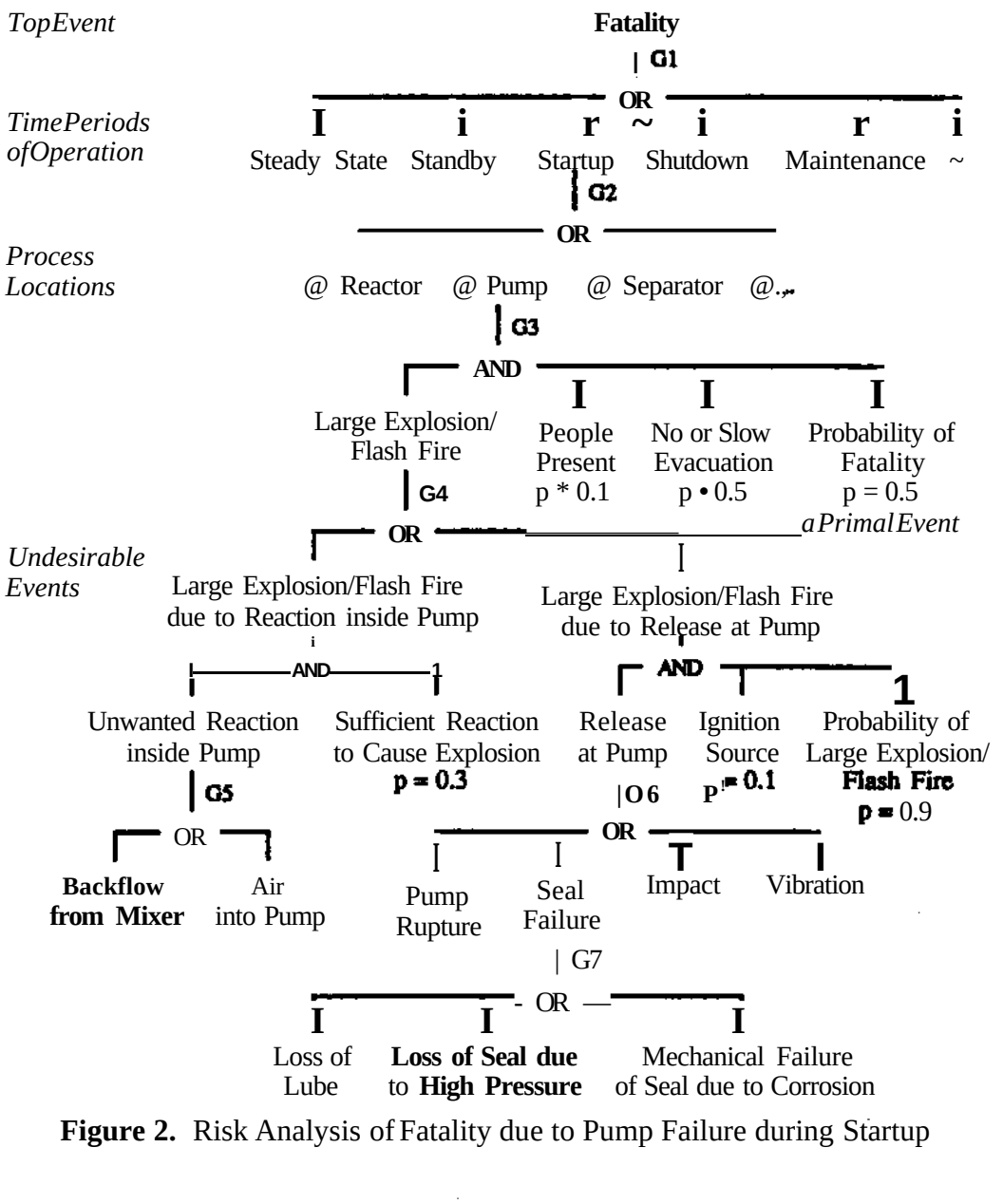

Figure 2. Risk Analysis of Fatality due to Pump Failure during Startup

As indicated in gate G1, fatalities can occur in any period of operation, each of which carries its own risk scenarios. In each time period, the hazardous events can happen in a number of locations in the chemical plant, including the pump system (G2). In gate G3 it is assumed that an explosion/flash fire can cause fatalities only if people are present, do not evacuate quickly enough, and the injuries they sustain are serious enough to cause fatalities. Gate G4 specifies that large explosions/flash fires in the pump can be caused by two events: an unwanted reaction inside the pump of sufficient magnitude, or a chemical release which ignites. Unwanted reactions can occur through backflow from the downstream mixer during starting up the pump, or air entering the pump casing (G5). Gate G6 indicates that releases can

happen in a number of ways, including seal failure which can be caused by over-pressure (G7). For simplicity we only investigate the following events:

- ***loss of seal due to high pressure,*** **and**
- ***backflow to the feed.***

5.1 The Design of a Centrifugal Pump System

The design of a centrifugal pump system is shown in Figure 3. The system includes a centrifugal pump, a pressure gauge, a block discharge valve, and a control valve which receives signals from a flowmeter during steady state operation. During startup the flow control loop is on manual. A set of startup operating procedures for this system is given in (Englund, *et* a/., 1992):

- with discharge valve initially closed, start pump;
- observe pressure buildup;
- open discharge valve;
- do flow control starting with control valve in closed position; and
- be sure not to leave pump on dead-headed for too long, to avoid overheating.

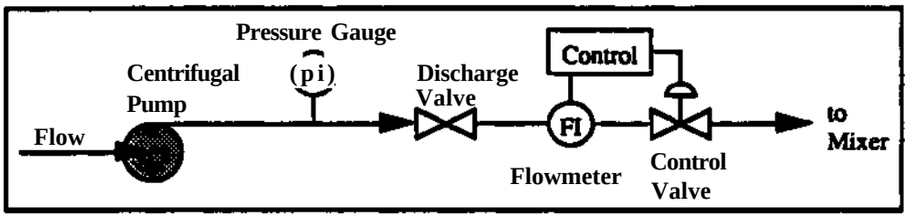

Figure 3. Design of a Centrifugal Pump System

Digraphs of this process are built for backflow and for loss of seal due to high pressure. These digraphs capture the behavior of both the hardware and the human operator. They are used to produce fault trees for analyzing the risk of each event The corresponding preliminary trees are shown in Figure 4. Before we describe these trees, we provide the following definitions (Powers and Lapp, 1989):

Primal Event **- An event which cannot be further decomposed into other causal events. Primal events are assumed to be independent**

Failure Rate, **FR - The frequency of failure of an event [1/yr]. Failure rates are assumed constant**

Mean time to detection and repair, **x - The time needed to either repair the fault or move the system to a safe state [yr]. We assume that x « (Testing Interval)/2.**

Unavailability, **q - The probability that a component is not available at time t Unavailability is time dependent For repairable components, q =** $\frac{FR \cdot \tau}{vl\backslash, X + 1}$ **(1 - e" <ra + 1/T> *). If t» x, then**

$q = \frac{FRt}{FR\tau + 1}$, and if FR x « 0.1, then q - FR x.

Demand Probability, p - The probability that an event is *true** given that an appropriate cause occurs.

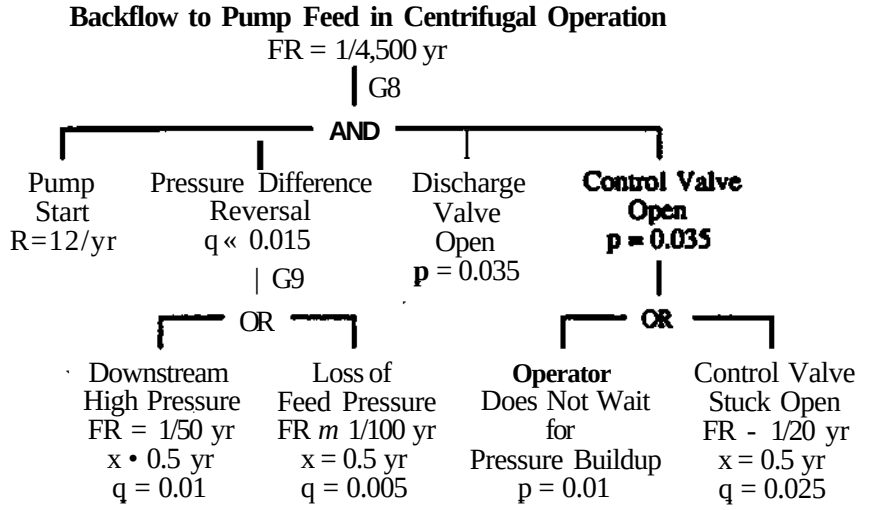

Figure 4a. FT A for Backflow in a Centrifugal Pump System

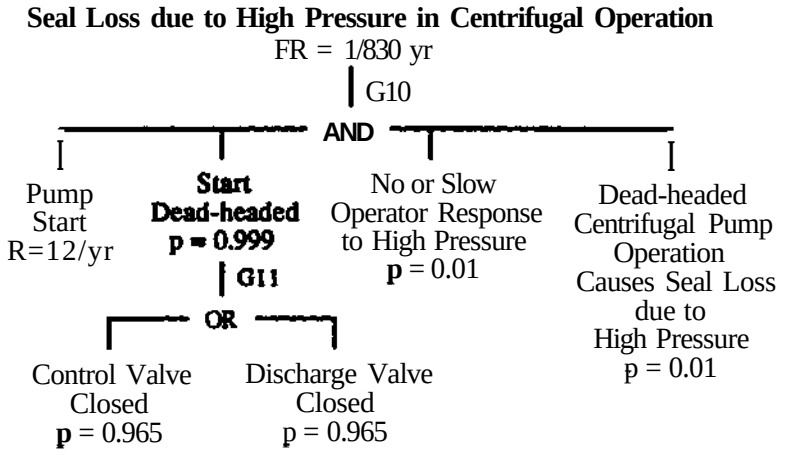

Figure 4b. FTA for Seal Loss in a Centrifugal Pump System

In Figure 4a, gate G8 indicates that backflow during startup can occur when all of the following are true: the pump starts, there is a reversal of the proper pressure gradient, and the connecting valves are open. In this case, the *initiation event* is the action of the pump and the remaining events *enable* the backflow. The initiation event contributes a failure rate and the enabling events contribute demand probabilities, or unavailabilities. This tree includes both structural and procedural variables. An example of how structure determines the fault tree logic is the location and number of valves. The action of an operator, *opening the control valve without waiting for pressure buildup,* is a procedural consideration which also determines the fault tree logic. The values of failure rates, mean times to detection and repair, unavailabilities,

and demand probabilities have been adapted from (AIChE/CCPS, 1989b).

Probabilities across logical OR gates (u) are combined according to the following formula:

$$P(A) \text{ u } P(B) = P(A) + P(B) - P(A) \text{ n } P(B). \quad (1)$$

If P(A) and P(B) « 0.1, then

$$P(A) \text{ u } P(B) - P(A) + P(B). \quad (1a)$$

Probabilities across logical AND gates (n) are given in Equation 2:

$$P(A) \text{ n } P(B) = P(A)*P(B). \quad (2)$$

These calculations are applicable when the probabilities and unavailabilities represent independent events.

Under gate G9 of Figure 4a, the unavailability of the *downstream high pressure,* q ≈ 0.5 * (1/50) = 0.01. Similarly, the *unwail&İnlity of the bss of feed pressure* is 0.005. Then, according to Equation la, the unavailability of the *pressure difference upset* is approximately equal to 0.015 (G9). The failure rate of the backflow is the product of the demand probabilities and unavailabilities of the enabling events, 0.035 * 0.035 * 0.015, times the failure rate of the initiation event, 12/yr. The resulting failure rate in G8 is 1/4,500 yr.

Step 4 of the unified risk reduction strategy is the evaluation of the top event Table 1 presents the fatality rates which result from backflow or seal loss in the pump (G1 of Figure 2). The total risk of fatality, either from an unwanted reaction due to backflow or from a release in the pump during startup, is 1/230,000 yr. If these two events were the only contributors to the top event rate, this failure rate might be acceptable. The risk reduction strategy proposes that we investigate if ether cost effective means for reducing the risk of fatality are readily available.

Step 5 is the identification of the most important contributors to the risk of fatality. This step is motivated by the assumption that modifying the contributors with the largest relative importance will give the largest improvement *Relative importance* is the fraction of the top event which results by a specific event As seen in Table 1, the risk of fatality due to a chemical release from seal loss in this case has the highest relative importance (0.62).

Table 1. Results of Risk Analysis for the Centrifugal Pump System

Fatality	Failure Rate	Relative Importance
due to Reaction from Backflow	1/600,000 yr	0.38
due to Release from Seal Loss	1/370,000 yr	**0.62**
Combined Risk (G1)	1/230,000 yr	1.00

The fault tree of Figure 4b indicates that there are two alternative sets of events capable of causing seal loss. Each of these *minimal cut sets* is comprised of the three primal events of gate G10 and one of the two primal events of gate GIL Each set of events alone is able to cause seal loss due to over-pressure. One way to improve safety is by requiring that additional events be necessary to cause the undesirable top event. This might be accomplished by making procedural, structural, or alarm/control system modifications. In this example, most procedural and structural modifications are based on establishing stationary states in the original design. Stationary states will allow *waiting longer* during startup without causing seal loss.

We revise the original design in step 6, by proposing specific design alternatives which incorporate stationary states. Figure 5 shows a series of structural modifications to the basic centrifugal pump design. A recirculation line around the centrifugal pump (Figure 5a) creates a stationary state because of the presence of a set of inverse operations, namely the creation of momentum from the pump and the dissipation of momentum from the friction in the new line. Both the large holding tank and the purge line (Figures 5b and 5c, respectively) establish stationary states, which are based on large capacitance of the new designs for material flow. The two designs differ in that the holding tank provides extra material capacitance locally, and the line to the purge provides capacitance in a remote location. The startups of the new designs also incorporate modifications in the operating procedures, which take advantage of the new structural features. The impact of these new procedures appears in the fault trees of Figures 6 and 7.

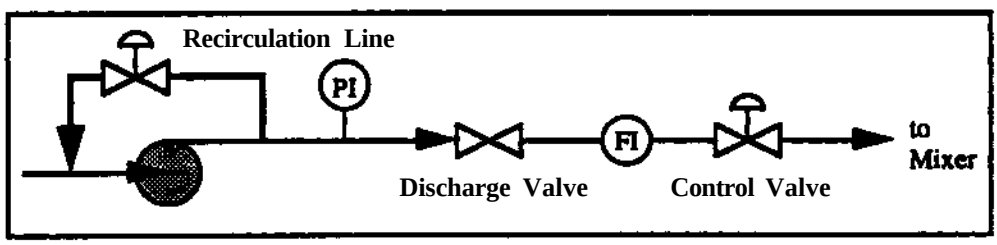

Figure 5a. Centrifugal Operation with Recirculation Line

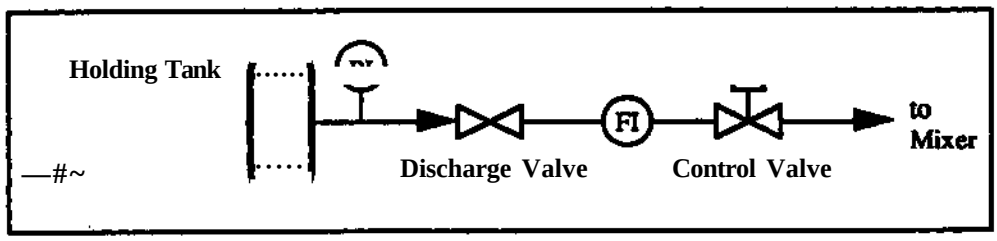

Figure 5b. Centrifugal Operation with Holding Tank

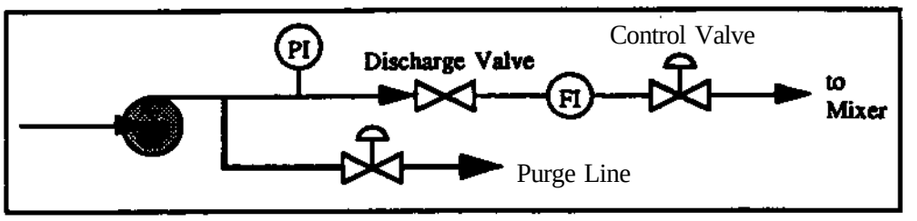

Figure 5c Centrifugal Operation with Purge Line

For each of the designs shown in Figure 5, fault trees for the risk of seal loss due to over-pressure are shown in Figure 6. Comparing these trees to that of the original design (Figure 4b), we can see that additional events must happen to cause seal loss, and the failure rate of seal loss has been reduced. However, the designs which involve the recirculation and purge lines have higher risk for backflow than the original design, because these lines present alternative routes for backflow. The design with the holding tank has the same risk for backflow as the original design (Figure 4a). The risk of backflow in the new designs is modeled in the fault trees of Figure 7. These results are summarized in Table 2.

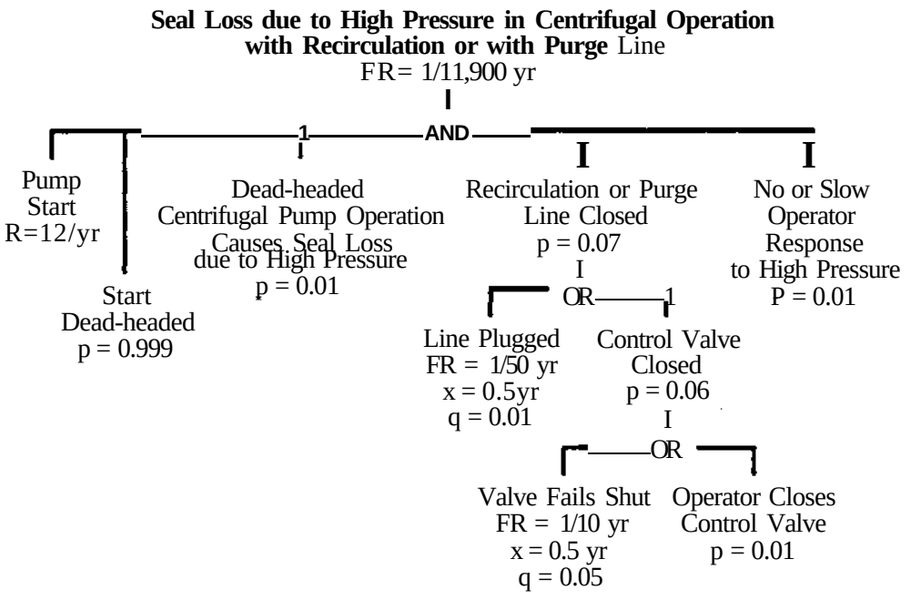

Figure 6a. FTA for Seal Loss in a Centrifugal Operation with either a Recirculation or a Purge Line

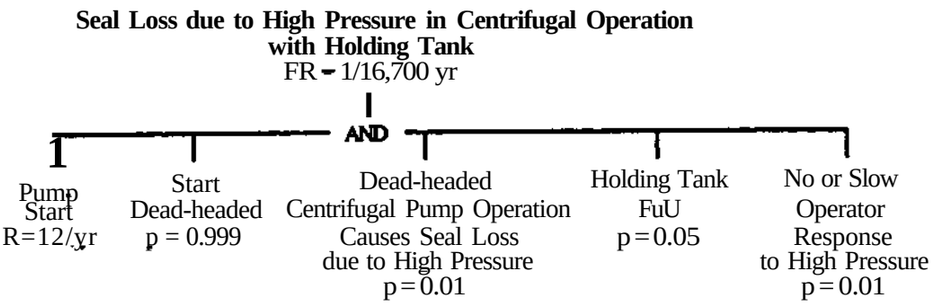

Figure 6b. FTA for Seal Loss in a Centrifugal Operation with a Holding Tank

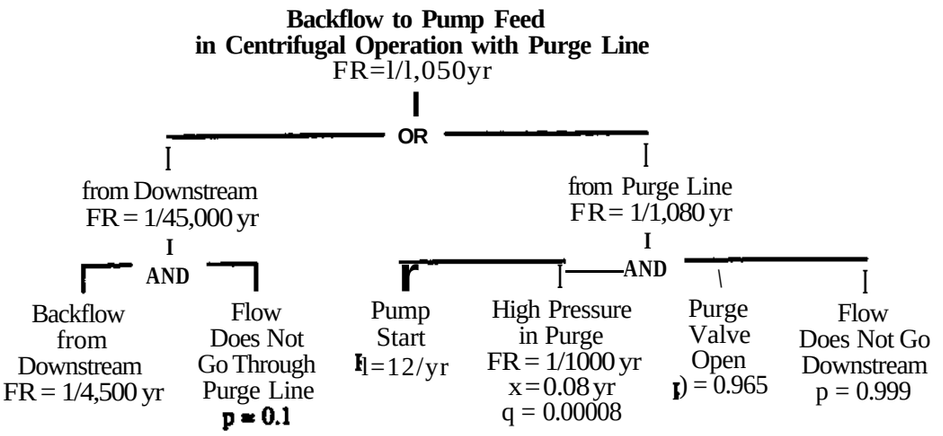

Figure 7a. FTA for Backflow in Centrifugal Operation with Purge Line

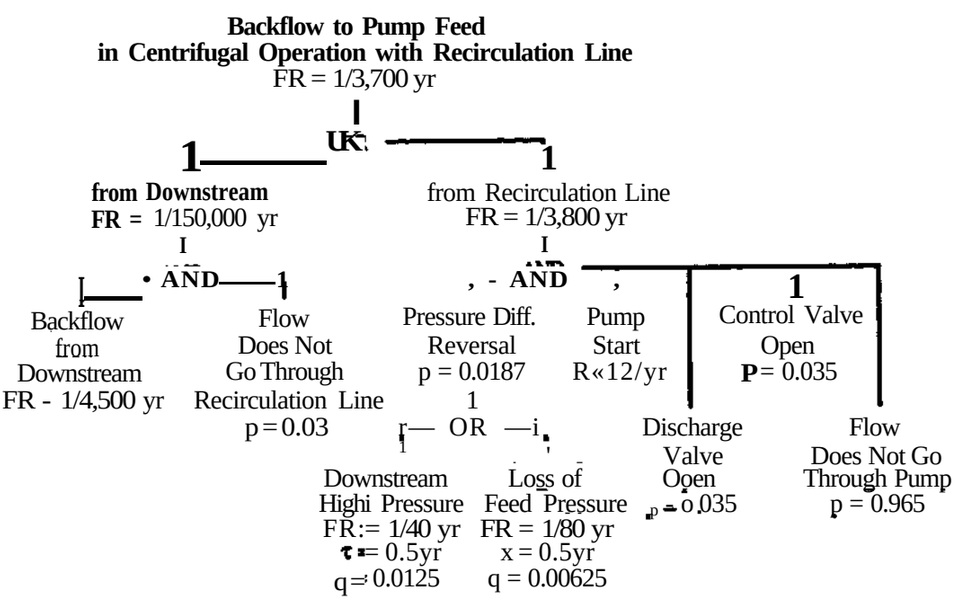

Figure 7b. FTA for Backflow in Centrifugal Operation with Recirculation Line

Table 2. Results of Risk Analysis for Alternative Centrifugal Pump Systems

Fatality	Basic Centrifug. Operation	Operation with RecircuL Line	Operation with Holding Tank	Operation with Purge Line
due to Reaction from Backflow	1/600,000 yr	1/490,000 yr	1/(004)00 yr	1/140,000 yr
due to Release from Seal Loss	1/370,000 yr	1/5300,000 yr	1/7,400,000 yr	1/5,300,000 yr
Combined Risk (Gl)	1/230,000 yr	1/450,000 yr	175504)00 yr	1/140,000 yr

Among the presented alternatives, the design with the lowest overall risk is the centrifugal pump system with the holding tank (Table 2). In this design, most of the risk is contributed by the branch of the tree which accounts for the unwanted reaction from backflow (relative importance = 0.92). Going through the risk analysis strategy once more we conclude that if further improvement is desirable, it should focus on reducing the risk of backflow.

One way to achieve this is by installing a pressure gauge downstream. This gauge can prevent backflow by providing an additional check that the pressure downstream is lower than upstream, before the operator opens the discharge and control valves during startup. This modification combines a change in the alarm system and the operating procedures. The new structure is shown in Figure 8 and the corresponding fault tree for backflow is shown in Figure 9. It is assumed that the new pressure gauge has no failure modes.

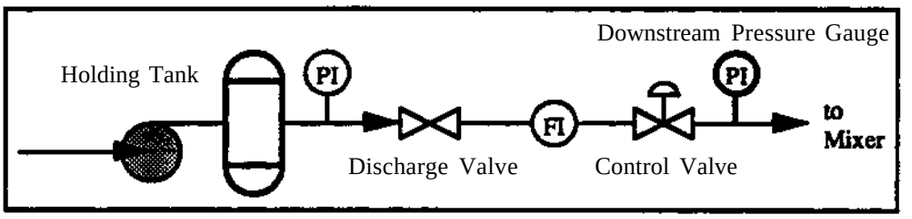

Figure 8. Centrifugal Pump System with Downstream Pressure Gauge

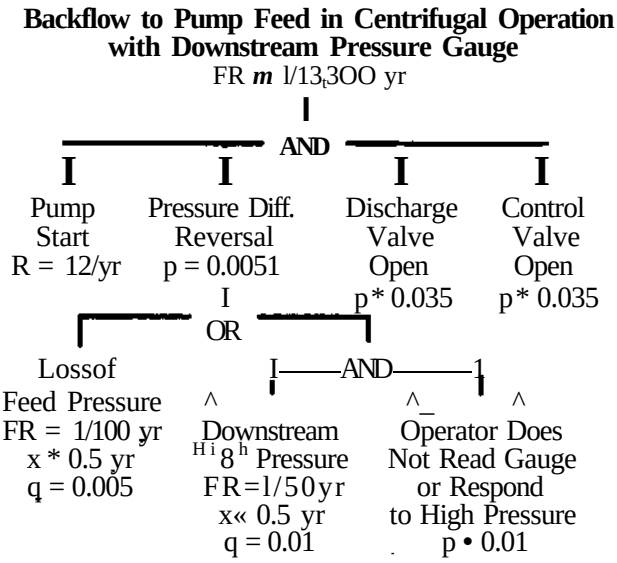

Figure 9. FTA for Backflow in Centrifugal Pump with Downstream Pressure Gauge

This modification reduces the risk of fatality from an unwanted reaction from **17600,000 yr** to **1/1^00,000 yr,** and the combined risk of fatality from **1/550,000 yr** to **1/1,400,000 yr.** This improvement is also applicable to the other design alternatives. This analysis indicates that, based on the given failure rate information, among the presented alternatives the best **system uses a *holding tank and a downstream pressure gauge.* More detailed FTA could** reveal other important features of this system. Also, other design modifications, such as the addition of check valves, could give further risk reductions.

5.2 The Design of a Positive Displacement Pump System

A similar analysis is carried out for a system which uses a positive displacement pump. The choice between a centrifugal and a positive displacement pump frequently depends on the desired pressure level, because the latter type is usually capable of higher pressures. For pumps capable of similar pressure levels, there may exist a choice between them based on risk. This analysis compares the two systems.

The design of a positive displacement pump system is shown in Figure 10. A set of possible startup operating procedures is given below:

- with discharge and control valves initially open, start pump;
- stabilize pressure using control valve;
- do flow control; and
- shut down if feed loss is detected.

  A pressure switch detects loss and turns pump off automatically.

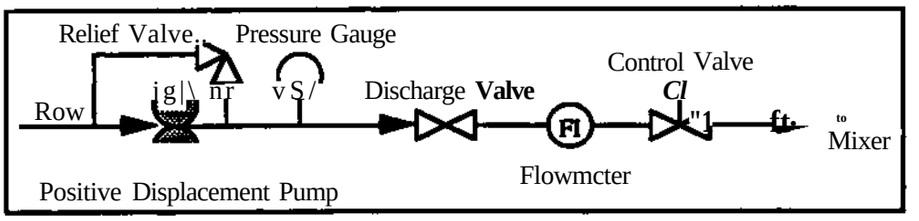

Figure 10. Design of a Positive Displacement Pump System

The fault trees for this system are given in Figure 11. The positive displacement pump system uses a pressure switch, which turns the pump off in case of feed loss. This new feature appears in the tree which evaluates the risk for backflow (G12 in Figure 1 la). The presence of the relief valve in this design is reflected in the tree for seal loss (G13 in Rgure lib).

Note that similar events can have different probabilities when they occur in the centrifugal or the positive displacement operation. The *slow operator response,* for example, has demand probability 0.1 (G13 of Figure 1 lb), as opposed to the same event in the centrifugal operation which has demand probability 0.01 (G10 of Figure 4b). The probabilities differ because the operator has less time to take corrective action in operating dead-headed a typical positive displacement pump, than a centrifugal pump. Again, a dead-headed operation can *cause seal loss* much easier in a positive displacement pump than in a centrifugal pump, which is reflected by the difference in probabilities in Figures 4b and lib.

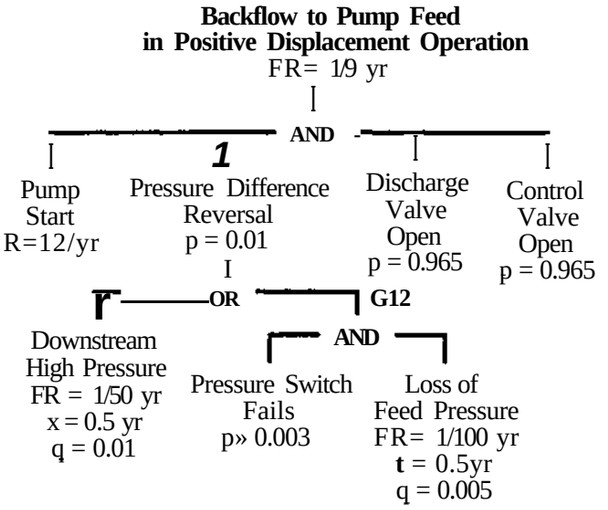

Figure lla. FTA for Backflow in Positive Displacement Pump

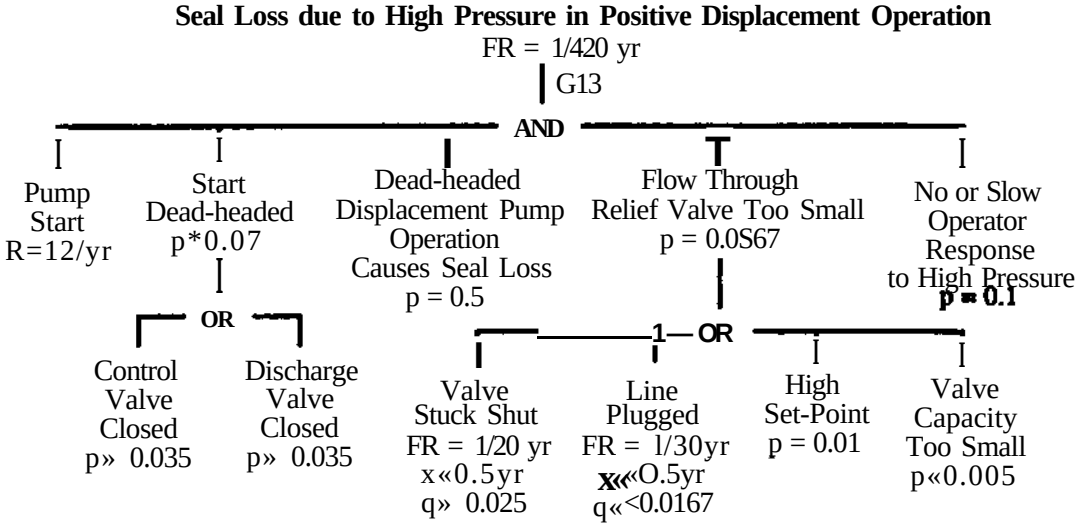

Figure lib. FTA for Seal Loss in Positive Displacement Pump

The results of this analysis are presented in Table 3. Comparing these results with those of Table 1, we conclude that the proposed positive displacement pump system has a higher risk of fatality than the corresponding centrifugal pump system. In this case, however, it is the risk of backflow which dominates the combined risk of fatality (relative importance = 0.99). The high risk of backflow reflects that initially the system is not operated dead-headed (high demand probability of the valves being open). This suggests an opportunity for risk reduction by modifying the operating procedures.

Table 3. Results of Risk Analysis for the Positive Displacement Pump System

Fatality	**Failure Rate**	Relative Importance
due to Reaction from Backflow	1/1,200 yr	**0.99**
due to Release from Seal Loss	1/190,000 yr	0.01
Combined Risk (Gl)	1/1,200 yr	1.00

An alternative set of startup operating procedures, aimed at preventing backflow, is based on (Englund, *et al.*[9]1992):

- with discharge valve initially closed and control valve initially open, start pump;
- observe pressure buildup;
- open discharge valve, modulate control valve to give desired pressure;
- do flow control; and
- shut down if loss of feed is detected.

To avoid backflow, these operating procedures specify that the discharge valve be initially

closed. The new trees for this revised system are shown in Figure 12 and the results of modifying the operating procedures are summarized in Table 4. The combined risk of fatality has been reduced, but the risk of a chemical release has been increased. We can further reduce the risk for seal loss by making structural modifications to create stationary states. The presence of stationary states is expected to reduce the risk of seal loss for the same reasons that it did in the improved designs of the centrifugal pump system. Figure 13 shows these alternative process configurations.

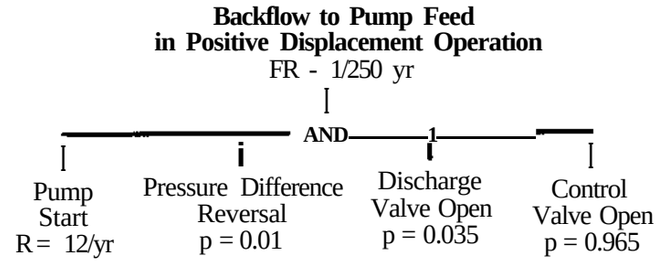

Figure 12a. FTA for Backflow in Positive Displacement Pump with Modified Operating Procedures

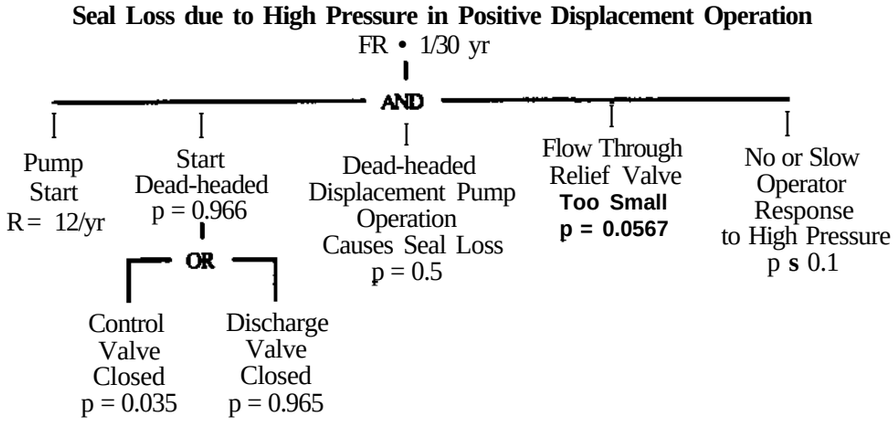

Figure 12b. FTA for Seal Loss in Positive Displacement Pump with Modified Operating Procedures

Table 4. Results of Risk for Modified Positive Displacement Pump Operating Procedures

Fatality	Original Procedures	Modified Procedures
due to Reaction from Backflow	1/1,200 yr	**1/33,000 yr**
due to Release from Seal Loss	**1/190,000 yr**	1/13,000 yr
Combined Risk (Gl)	1/1,200 yr	**1/930 yr**

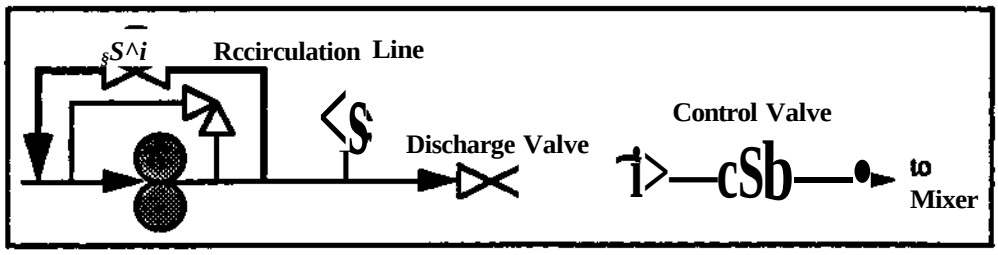

Figure 13a. Positive Displacement Operation with Recirculation Line

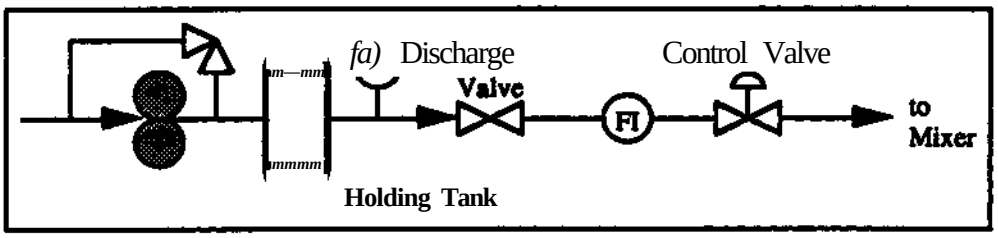

Figure 13b. Positive Displacement Operation with Holding Tank

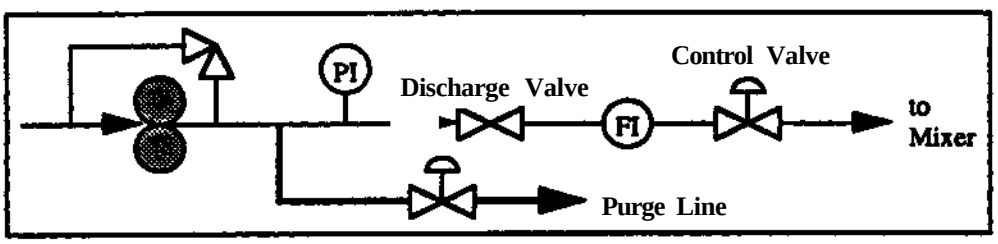

Figure 13c Positive Displacement Operation with Purge Line

The fault trees for the new designs are presented in Figures 14 and 15. In these designs, the modified operating procedures are adopted, i.e. the alternative systems start with the discharge valve closed. The fault tree for backflow in the system with the holding tank (Hgure 13b) is the same as the corresponding tree of the original design (shown in Figure 12a).

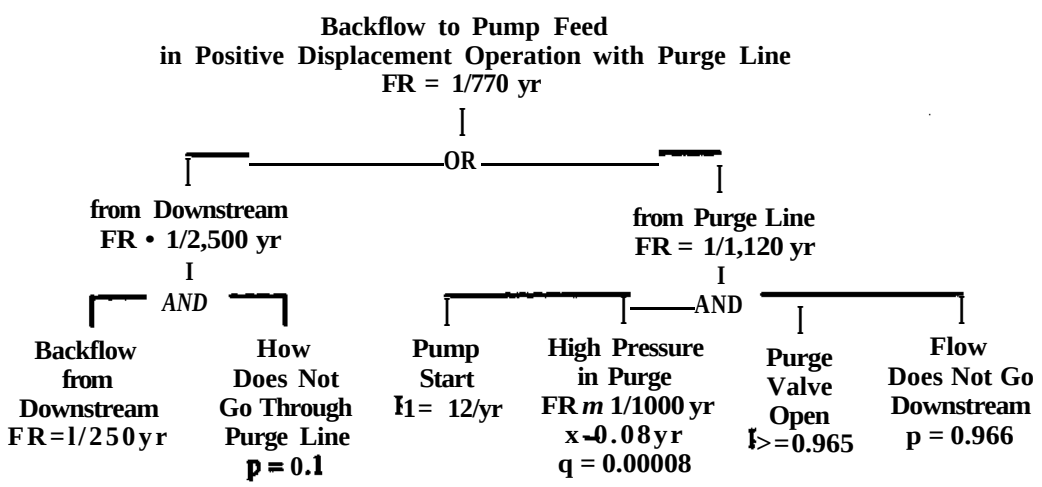

Figure 14a. FTA for Backflow in Positive Displacement Pump with Purge Line

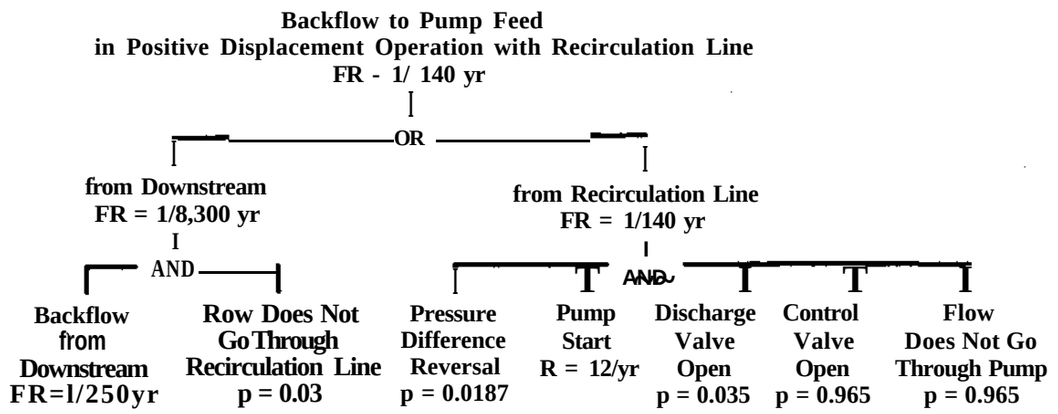

Figure 14b. FTA for Backflow in Positive Displacement Pump with Recirculation Line

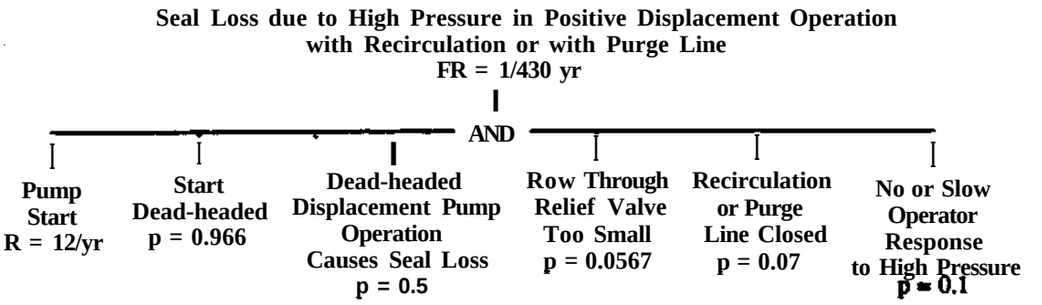

Figure 15a. FTA for Seal Loss in Positive Displacement Pump with Recirculation or Purge Line

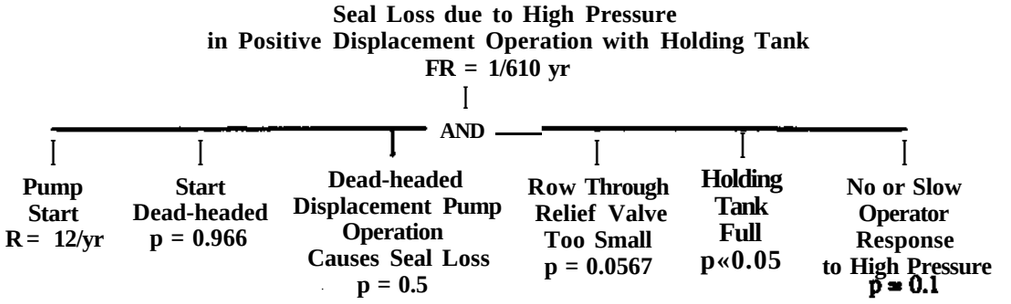

Figure 15b. FTA for Seal Loss in Positive Displacement Pump with Holding Tank

The results of the risk analysis are summarized in Table 5. The lowest risk of fatality due to backflow is exhibited by the design which involves the purge line (Figure 13c) and the lowest risk of seal loss is exhibited by the design with the holding tank (Figure 13b). The design with the purge line has the lowest combined risk.

Table 5. Results of Risk Analysis for Alternative Displacement Pump Systems

Fatality	Basic Displac. Operation	Operation with Recircul. Line	Operation with Holding Tank	Operation with Purge Line
due to Reaction from Backflow	1/33,000 yr	1/19,000 yr	1/33,000 yr	**1/100,000 yr**
due to Release from Seal Loss	1/13,000 yr	1/190,000 yr	**1/270^)00 yr**	1/190,000 yr
Combined Risk (Gl)	1/9,300 yr	1/17,000 yr	1/29,000 yr	**1/66,000 yr**

Similarly with the design of Figure 8, further reduction of the risk of backflow can be achieved by adding a pressure gauge downstream. This modification is applied to the design with the holding tank, because this design already has the lowest risk of seal loss. The resulting system and the new tree for backflow are shown in Figures 16 and 17 respectively.

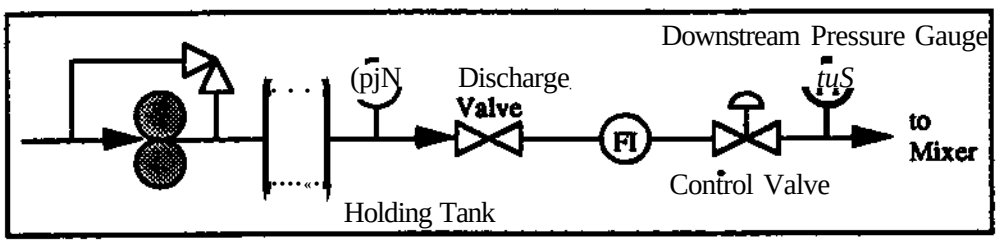

Figure 16. Positive Displacement Pump System with Downstream Pressure Gauge

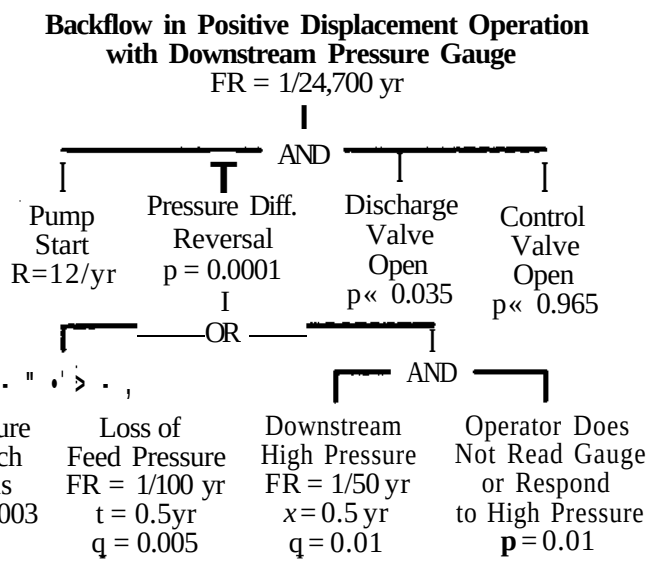

Figure 17. FTA for Backflow in Positive Displacement Pump with Downstream Pressure Gauge

The addition of the pressure gauge and the corresponding modification of the operating procedures reduces the risk of fatality due to an unwanted reaction from **1/33,000 yr** to

1/3^00,000 yr, and the combined risk of fatality from **1/29,000 yr** to **1/250,000 yr.** Among the presented designs, the safer system uses a *holding tank and a downstream pressure gauge.* Also, for these assumptions, the centrifugal pumps have lower risk than the corresponding positive displacement pumps.

The accuracy of the risk analysis depends the depth of FTA and on the availability of reliable statistics on primal events. We can undertake sensitivity studies of specific events by performing the risk assessment for a range of statistical failure values. An example of sensitivity analysis appears in (Delboy, *et al.,* 1991). This analysis can answer questions of the sort*

what if the operator errs 10 times as often as the typical operator error rate?

The unified risk reduction strategy can determine whether this high failure rate has a strong impact on the overall risk and, if so, propose better operator training, or possible replacement of certain operator tasks with potentially more reliable automated alternatives.

6. Conclusion

A unified risk reduction strategy has been presented. The approach has assessed the risk of chemical operations that included the process flowsheet, control system, and operating procedures simultaneously. It has also provided guidance in improving these operations. The main features of this strategy are: (a) the qualitative and quantitative risk evaluation using *Fault Tree Analysis,* and (b) the modification of the dominant causes of risk using *relative* ***importance.***

The proposed strategy has been applied to the design of a pump system startup and, in some cases, reduced the risk by several orders of magnitude. Alternative pump systems have been developed by modifying the structural, procedural, and control characteristics of the original design. Most of the modifications have focused on establishing *stationary states.* The presence of these states can alter the process time constants and support intermediate state verification.

This risk reduction strategy can also be applied to environmental impact studies, where the undesirable event might be the release of a toxic chemical. As we apply this hazard reduction strategy to more complex designs, we will better assess the design effort and the failure rate data required to develop safer designs.

7. Acknowledgment

This work has been supported by NSF Grants DDM-8616889 and CTS-9114050.

8. References

Aelion, V. and G. J. Powers. A Unified Strategy for the Retrofit Synthesis of Flowsheet Structures for Attaining or Improving Operating Procedures. Computers & Chemical Engineering, 15, 5, 349-360, May 1991.

AIChE/CCPS. *Guidelines for Chemical Process Equipment Reliability Data.* Center for Chemical Process Safety, AIChE, New York, 1989b.

AIChE/CCPS. *Guidelines for Chemical Process Quantitative Risk Analysis.* Center for Chemical Process Safety, AIChE, New York, 1989a.

AIChE/CCPS. *Guidelines for Hazard Evaluation Procedures.* Center for Chemical Process Safety, AIChE, New York, 1985.

Crooks, C. A. and S. Macchietto. A Combined MILP and Logic-Based Approach to the Synthesis of Operating Procedures for Batch Plants. To be published in *Chemical Engineering Communications,* 1992.

Delboy, W. J., R. F. Dubnansky, and S. A. Lapp. Sensitivity of Process Risk to Human Error in an Ammonia Plant *Plant! Operations Progress,* 10,4,207-211, October 1991.

Department of Labor, Occupational Safety and Health Administration. Process Safety Management of Highly Hazardous Chemicals; Notice of Proposed Rulemaking. Federal Register, 29150 - 29173, July 17,1990.

Englund, S. M., J. L. Mallory, and D. J. Grinwis. Prevent Backflow. *Chemical Engineering Progress,* 88, 2,47-53, February 1992.

Fusillo, R. H. and G. J. Powers. A Synthesis Method for Chemical Plant Operating Procedures. *Computers & Chemical Engineering,* 11,369-382 ,1987.

Fusillo, R. H. and G. J. Powers. Computer-Aided Planning of Purge Operations. *AIChE Journal,* 34,558-566,1988a.

Fusillo, R. H. and G. J. Powers. Operating Procedure Synthesis using Local Models and Distributed Goals. *Computers & Chemical Engineering,* 12,1023-1034,1988b.

Grossmann, I. E. and M. Morari. Operability, Resiliency and Flexibility - Process Design Objectives for a Changing World. In the *Proceedings of the Second International Conference on Foundations of Computer-Aided Design,* Snowmass, Colorado, June 19-24,1983.

Huang, Y. L. and L. T. Fan. A Distributed Strategy for Integration of Process Design and Control: An Artificial Intelligence Approach for Incorporation of Controllability into Process Design. *Presented at the Annual AIChE Meeting,* San Francisco, CA, Paper 27e, November, 1989.

Lakshmanan, R. and G. Stephanopoulos. Synthesis of Operating Procedures for Complete Chemical Plants. Part I: Hierarchical, Structured Modeling for Nonlinear Planning. *Computers & Chemical Engineering,* 12,985-1002,1988a.

Lakshmanan, R. and G. Stephanopoulos. Synthesis of Operating Procedures for Complete Chemical Plants. Part II: A Nonlinear Planning Methodology. *Computers & Chemical Engineering,* 12,1003-1021,1988b.

Lakshmanan, R. and G. Stephanopoulos. Synthesis of Operating Procedures for Complete Chemical Plants. Part in: Planning in the Presence of Qualitative Mixing Constraints. *Computers & Chemical Engineering,* 14,301-317,1990.

Lapp, S. A. and G. J. Powers. Computer-Aided Synthesis of Fault-Trees. ***IEEE Transactions on Reliability,*** **2,13, April 1977.**

Powers, G. J. and S. A. Lapp. ***A Short Course on Risk and Reliability Assessment by Fault Tree Analysis.*** **Manuscript in preparation, 1989.**

Pistikopoulos, E. N. and I. E. Grossmann. Optimal Retrofit Design for Improving Process Flexibility in Linear Systems. ***Computers & Chemical Engineering,*** **12, 7, 719-731, July 1988.**

Shaeiwitz, J. A., S. A. Lapp and G. J. Powers. Fault Tree Analysis of Sequential Systems. ***Industrial & Engineering Chemistry, Process Design & Development,*** **16,4, 529-549,1977.**

The Bureau of National Affairs. ***The Clean Air Act Amendments: BNA's Comprehensive Analysis of the New Law.*** **Washington, DC, 1991.**

Umeda, T. Computer Aided Process Synthesis. In ***PSE'82 Proceedings,*** **Kyoto, Japan, 79-109, August 23-27,1982.**