Safety Verification Using a Hybrid Knowledge-Based Mathematical Programming Framework

R. Srinivasan, V. D. Dimitriadis, N. Shah, and V. Venkatasubramanian
Laboratory for Intelligent Process Systems, School of Chemical Engineering, Purdue University, W. Lafayette, IN 47907

Hazard and operability analysis (HAZOP) is widely used to perform hazards analysis of chemical plants. It is labor- and knowledge-intensive and could benefit from automation. Toward that goal, a knowledge-based framework for automating HAZOP analysis (HAZOPExpert) was proposed. Recently, Dimitriadis et al. proposed a quantitative model-based approach that uses a dynamic model of the plant and a description of process disturbances and parameters for hazard evaluation. These two different approaches have their own merits and demerits. The qualitative analysis performed by HAZOPExpert is thorough and computationally efficient, but can lead to ambiguous conclusions. The quantitative approach can perform an exact analysis without ambiguities, but a complete analysis can be computationally prohibitive. Thus, these two frameworks appear to complement each other. This article presents an integrated approach for hazard identification and evaluation, which overcomes the shortcomings of purely qualitative and quantitative methods. In the integrated framework, the overall features of a particular hazardous scenario are extracted by inexpensive qualitative analyses. If necessary, a detailed quantitative analysis is then performed, and that too only on those parts of the plant identified by the qualitative analysis as hazardous. The results of this framework are compared to those of purely qualitative reasoning using an industrial case study.

Introduction

Process hazards analysis (PHA) is the systematic identification and mitigation of potential process hazards that could endanger the health and safety of humans and cause serious economic losses. This is an important activity that requires a significant amount of time, effort, and specialized expertise. The importance of this activity is underscored by the Occupational Safety and Health Administration's (OSHA) Process Safety Management Standard Title 29 CFR 1910.119, which requires initial PHAs of all the processes covered by the standard to be completed no later than May 26, 1997. A wide range of methods such as Checklist, What-If Analysis, Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis, and Hazard and Operability (HAZOP) Analysis are available for performing PHA (CCPS, 1985).

HAZOP analysis is widely used and recognized as a preferred PHA approach by the chemical process industry. The basic principle of HAZOP analysis is that hazards arise in a plant due to deviations from acceptable normal behavior. HAZOP analysis is performed by a multidisciplinary team of experts who have extensive knowledge of the design, operation, and maintenance of the plant. The team of experts systematically examines the process P&IDs to determine the abnormal causes and adverse consequences for every conceivable deviation from normal behavior of the process plant. In order to cover all the possible malfunctions in the plant, the process deviations are generated by systematically applying a set of guide words such as MORE OF, LESS OF, NONE, REVERSE, PART OF, AS WELL AS, and OTHER THAN to the process variables or parameters of the process. Detailed descriptions of the analysis procedure with illustrative examples have been given by Lawley (1974, 1976), CCPS (1985), Kletz (1986), and Knowlton (1989).

HAZOP analysis is a difficult, labor-, and knowledge-intensive activity that can benefit from automation in several

Correspondence concerning this article should be addressed to N. Shah or V. Venkatasubramanian.

V. D. Dimitriadis and N. Shah are affiliated with Centre for Process Systems Engineering, Imperial College of Science, Technology and Medicine, London SW7 2BY, UK.

ways. An automated HAZOP analysis system would reduce the time and effort involved in a HAZOP review, make the review more thorough and detailed, minimize or eliminate human errors, facilitate documentation for regulatory compliance, and make the study results available on-line. Despite the importance of automating HAZOP, there has only been limited work in this area (Karvonen et al., 1990; Rushton, 1995; Venkatasubramanian and Preston, 1996). Recently, a digraph model-based expert system called HAZOPExpert was reported (Vaidhyanathan and Venkatasubramanian, 1995).

HAZOPExpert was reported to emulate successfully the human experts' reasoning and identify all hazards on several industrial case studies. (Venkatasubramanian and Vaidhyanathan, 1994; Vaidhyanathan and Venkatasubramanian, 1995; Vaidhyanathan and Venkatasubramanian, 1996a). However, in several cases HAZOPExpert generated more consequences compared to the HAZOP team. Many of the additional consequences were deemed as minor or unrealistic by human experts. This drawback of generating "spurious" consequences is mainly due to the strict qualitative reasoning approach implemented using the digraph models together with the requirement that the system must perform a conservative analysis. To improve this situation, Vaidhyanathan and Venkatasubramanian (1996b) proposed a semiquantitative reasoning methodology to filter and rank the consequences generated by HAZOPExpert. This filtering approach combined the design and operating specification of the process units and process material property values to eliminate some of the unrealizable consequences. Although this approach eliminates a significant number of spurious consequences, it cannot resolve ambiguities stemming from physical limits on the process. A more formal and rigorous framework for evaluating hazards under ambiguous conditions is therefore required. Though HAZOP analysis is a qualitative approach, the human experts performing the analysis filter their initial, qualitative results by using additional quantitative knowledge in the form of quantitative operating conditions, bounds on process parameters, inputs, and disturbances, and the presence of control and automatic protection systems. In order to automate such human reasoning, a quantitative safety analysis becomes necessary.

A quantitative, model-based approach to the safety-verification problem was recently proposed by Dimitriadis et al. (1995). In their framework, a state-transition representation of the system was used. Associated with each state is a set of differential and algebraic variables and equations describing the system in that state. Transitions between states are triggered when certain logical conditions are satisfied. For safety verification, the process is deemed unsafe if it reaches an undesirable state (where process variables take values in undesirable ranges) under the influence of external inputs and equipment failures. The safety-verification problem is formulated as a mixed integer-optimization problem (MI(N)LP), where the objective is to minimize the amount of time during which the process is safe. The general framework is designed for hybrid process systems that exhibit both continuous and discrete characteristics. However, it is equally applicable to the special cases of purely continuous or purely discrete systems. Dimitriadis et al. (1995, 1996, 1997) illustrated this framework on several systems. However, one disadvantage of this framework is that the size of the resulting optimization problem can be very large for industrial-scale processes. For plants described by linear models with process discontinuities the corresponding mixed-integer linear program (MILP) can be expensive to solve. In the general case of plants where nonlinearities are present in the process model, the NLP or MINLP suffer from local optima problems. Thus, the safety of the process for such cases cannot always be guaranteed based on the results of this approach.

It is apparent that the qualitative digraph-based and the quantitative model-based approaches have complementary strengths. Automated hazard analysis using the qualitative approach is fast even for industrial-scale processes. Also, the results produced by this approach are comprehensive. Hazard evaluation using the quantitative model-based approach can determine whether a given hazard is physically realizable, given the dynamic model of the process and ranges on process inputs and disturbances. In this article, we propose an integrated framework for process safety verification that combines the strengths of both the approaches. In our framework, hazard analysis and evaluation is performed in two phases. First, HAZOPExpert is used to identify all probable hazards in the worst-case sense. From these hazards, ambiguous scenarios and serious hazards that need to be evaluated thoroughly are identified. In the second phase, these hazards are evaluated in detail to determine if they are realizable, using the quantitative process model. If a hazard is found to be realizable, its severity can be calculated, as can the precise sequence of events leading up to it. This two-phase hazard identification and evaluation framework can hence resolve qualitative ambiguities while reducing the size of the optimization problem to be solved during evaluation. Another use of this approach is in helping the human expert determine whether any process modifications would be necessary to safeguard against a process hazard, since the quantitative analysis incorporates all the existing safety mechanisms in the design.

The organization of this article is as follows: in the next section, the qualitative and the quantitative hazard-identification frameworks are reviewed and the motivation for the integrated framework is established. In the third section, the integrated qualitative–quantitative hazard-identification and evaluation framework is proposed. In the fourth section, the performance of the integrated approach on an industrial-scale sour-water stripper case study is presented along with comparisons with HAZOPExpert results.

Knowledge-Based and Mathematical Programming Approaches: Overview

A qualitative model-based approach for automating HAZOP analysis, called HAZOPExpert, has been proposed by Vaidhyanathan and Venkatasubramanian (1995). HAZOPExpert uses digraph models of process units to represent the causal relationships between the process variables. The HAZOP digraph (HDG) is a variation of the standard digraph commonly used in the literature. In a standard digraph, each node represents a process variable and a directed arc connecting two nodes indicates the influence of any deviation in the first process variable on the second process variable. The digraph nodes can take the values high, normal, and low and the directed arcs can have gains '+' or '−'. The HDG model

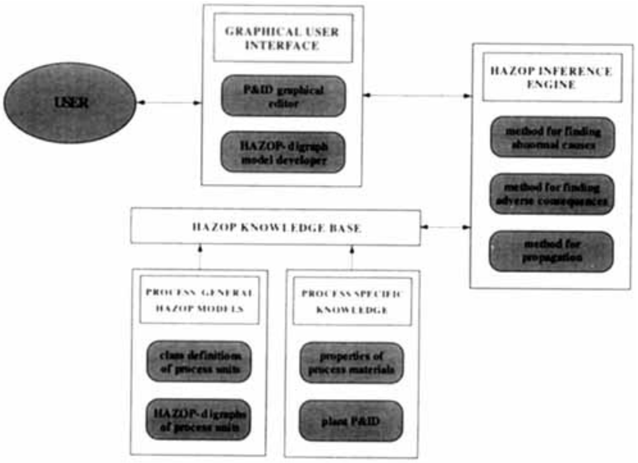
USER
GRAPHICAL USER INTERFACE
P&ID graphical editor
HAZOP-digraph model developer
HAZOP INFERENCE ENGINE
method for finding abnormal causes
method for finding adverse consequences
method for propagation
HAZOP KNOWLEDGE BASE
PROCESS GENERAL HAZOP MODELS
class definitions of process units
HAZOP-digraphs of process units
PROCESS SPECIFIC KNOWLEDGE
properties of process materials
plant P&ID

Figure 1. Architecture of HAZOPExpert.

has two additional types of nodes—abnormal cause nodes and adverse consequence nodes—that contain the hazard-identification knowledge required for HAZOP analysis. Also, the process-variable nodes in the HDG are allowed to have the value zero that corresponds to the guideword NONE in HAZOP analysis. The reader is referred to Vaidhyanathan and Venkatasubramanian (1995) for a detailed discussion of HDG models.

HAZOPExpert was implemented in an object-oriented framework. Figure 1 shows the architecture of HAZOPExpert. Each process unit class in HAZOPExpert has an HDG model associated with it to represent the causal and hazard-identification knowledge. This is the process-generic part of the knowledge in HAZOPExpert. The process-specific knowledge comprises the plant P&ID and the properties of the process materials. The HAZOP inference engine of HAZOPExpert comprises methods for finding abnormal causes and adverse consequences and the method for propagation of process-variable deviations. These methods use the HDG models of process units to perform HAZOP analysis.

Qualitative causal reasoning used by HAZOPExpert can lead to ambiguous values for some process-variable deviations. For example, in the case of a tank with two inlets, if one of the inlet flows has the qualitative value "high" and the other inlet flow has a qualitative value "low," the qualitative value of the level in the tank can have values "high," "low," or "normal," depending on the actual values of the two inlet flow deviations. In the absence of quantitative information, the worst-case scenario is assumed by HAZOPExpert and consequences for both the possible deviations "high level" and "low level" are flagged in order to be conservative.

The human team also faces these problems during conventional HAZOP analysis. This is because they also use qualitative guide words for generating process-variable deviations. In addition, the mental models used by them are essentially qualitative in nature. However, the team bring in (either explicitly or implicitly) additional quantitative information about the plant such as operating conditions, design specifications and ranges on process disturbances and parameters to sort out the ambiguities.

A quantitative, model-based approach for process safety verification of hybrid systems was proposed by Dimitriadis et al. (1995, 1997). In their approach, a state-transition network was used to represent hybrid behavior. Purely discrete or purely continuous processes are special cases in this representation. Each state in the state-transition network was characterized by a set of continuous describing variables, a set of equations that determine the dynamic behavior of system when in that state, and a (possibly empty) set of transitions to other states. Each transition comprised of initial state (s), a final state (s'), a logical condition that must be satisfied for the transition to occur, and a set of relationships that allows the value of the describing variables in state s' to be determined from the values of those in state s. Using the state-transition representation, a mathematical model of the system in the discrete time domain was constructed that expressed the system behavior in terms of equality and inequality constraints.

A key feature of the modeling approach is the broad concept of system inputs that drive the behavior of the system. In this case, these inputs may indeed correspond to typical process inputs, for example, feed streams, but may additionally be used to represent possible disturbances entering the system or possible failure modes of equipment.

The *initial* state of the system in the state-transition network can be identified from the values of the process variables. The process can thus be in any one of a set of states, and the values of the describing variables can lie within a known range. A process is deemed *unsafe* when under the effect of the inputs, it reaches any *undesirable state* and the describing variables in that state take values within undesirable regions. The safety verification problem in this framework can then be formulated as shown in Figure 2. In other words, given the mathematical description of the process, does there exist a sequence of disturbances that can lead the system from any of the initial conditions to any unsafe condition? The mathematical formulation results in a mixed-integer optimization problem.

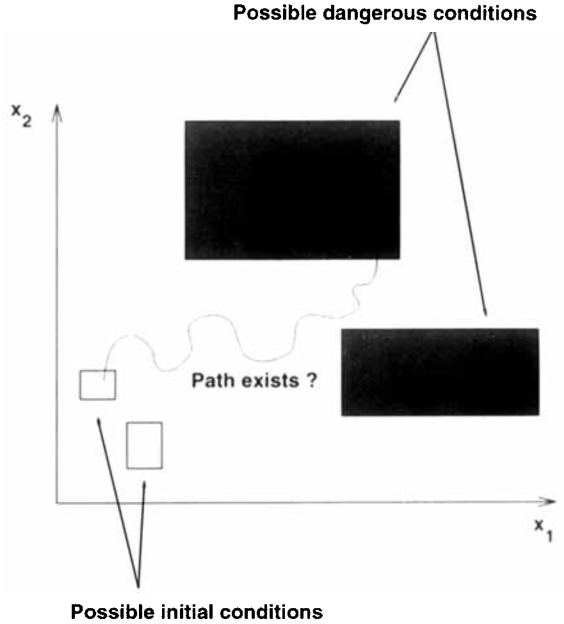

Figure 2. Quantitative hazard evaluation problem.

Dimitriadis et al. (1995, 1996, 1997) have shown the application of the framework to several examples where the system was able to identify disturbance profiles that could lead to hazards. Based on these examples, the following shortcomings of this approach can be identified. For most processes the entire plant model—the continuous differential and algebraic equations that describe the system in the continuous time domain—has to be discretized over the time horizon of interest. Therefore, the size of the mathematical program that has to be solved can be very large, depending on the number of variables needed to model the system, and the number of time steps considered. For the special case of continuous processes where the state-transition representation of the plant contains exactly one state (and there is only one initial state for the plant), time discretization can be circumvented if only one unsafe condition has to be investigated. In general, though, for industrial-scale problems, the resulting optimization problems may be difficult to solve, particularly if significant nonlinearities are present in the system model. The latter can lead to difficulties when used with local optimization techniques. In particular, even when the solution of the mathematical program indicates that the system is "safe" for the time horizon considered, in the presence of local optima, there is no guarantee that none of the hazards considered in the analysis can occur.

It is clear from the preceding discussion that the qualitative model-based approach of HAZOPExpert and the quantitative model-based approach have complementary strengths. Hazard analysis using the qualitative model-based approach is fast and comprehensive. Hazard evaluation using the quantitative model-based approach can determine whether a given hazard is physically realizable. Integrating these two approaches can help in performing detailed evaluation of the hazard identified by HAZOPExpert but generate focused, small mathematical programs that can be more easily solved. The hierarchical problem-solving strategy that can be implemented by integrating the two approaches obviates the need to perform extensive evaluation of simple, "routine" hazards, but has the ability to perform detailed evaluation for cases where process chemistry and operating conditions have to be accounted for, and the quantitative analysis does not suffice.

Integrated Qualitative–Quantitative Framework

In this section, the proposed integrated framework for hazard identification and evaluation is presented. The hazard analysis proceeds in two phases. In the first phase, a qualitative analysis of the entire process is performed using HAZOPExpert. From the results of this qualitative analysis, scenarios that require further detailed analysis can be identified. In the second phase, a quantitative safety-verification problem is formulated for each of these short-listed cases. The quantitative analysis of a scenario indicates whether the hazard is realizable, and if so its severity and possible causes.

The first phase of analysis can be performed for all process-variable deviations that can occur in the plant because the qualitative analysis of HAZOPExpert is computationally efficient. This analysis generates a list of causes and consequences for each deviation. The power of this phase of causal reasoning comes from the fact that it is complete. Most of the hazards identified at this stage are valid and do not need further analysis. As discussed earlier, however, some of the hazards flagged by HAZOPExpert could be unlikely. This conclusion can only be arrived at by a more detailed analysis. For example, a HIGH inlet flow into a tank would lead to high level and high pressure, and the adverse consequences due to high pressure (e.g., vessel rupture) are generally possible. However, to determine whether pressure would exceed the maximum allowed pressure for the particular system under consideration would require account to be taken of ranges of the input and output flow rates.

Some hazards are therefore short-listed to be analyzed further using quantitative safety verification. Since only a small number of the total set of hazards identified are ambiguous, detailed analyses need not be extensively used. Even when ambiguities arise, their source is identified by HAZOPExpert at a shallow level, as explained below. Thus, the computational expense needed to evaluate the ambiguous situations is small compared to that which would be necessitated by a detailed analysis of the entire process.

In the second phase of analysis, quantitative safety verification is performed. For each hazard that has been classified as requiring further quantitative analysis, a mathematical programming problem is generated to identify the worst possible case according to the dynamic process model and its inputs. The dynamic model used at this stage needs focus only on the section of the process under consideration and identified by HAZOPExpert and not on the entire plant. This is because the quantitative safety verification is used to investigate whether a particular hazard (for example, pressure greater than design pressure) can occur and if so its severity (maximum possible pressure). In addition, since the quantitative investigation focuses on one hazard at a time, the mathematical program for purely continuous systems (or subsystems) may not involve discrete variables and is hence easier to solve.

Figure 3 illustrates this two-phase nature of the integrated approach. The first phase consists of HDG-based qualitative reasoning considering only the HIGH, NORMAL, LOW, or ZERO nature of the deviations of a sample process variable. Based on this, process variables for which the deviation magnitude is important are identified. The upper part of Figure 3 thus corresponds to the qualitative value HIGH of the process variable obtained during the first phase. In the second phase, the quantitative verification procedure is used to focus on the identified process variable to determine the envelope within which it can vary. It should be noted here that the mathematical model generated at this stage focuses only on the HIGH and NORMAL ranges of this variable. The lower part of Figure 3 corresponds to the quantitative safety-verification phase. In the example shown, the process variable can never violate its safety limit. The hazard that would have occurred due to this variable crossing the safety limit is thus deemed to be impossible by detailed analysis.

A conventional HAZOP as practiced considers only single-fault scenarios, that is, when a process variable deviation is analyzed, only single faults that can lead to that deviation are considered to determine if that deviation is possible. This approach has the disadvantage that some scenarios that can be extremely hazardous could occur due to two (or more) faults occurring simultaneously. The difficulty in analyzing multiple hazards is due to the combinatorial number of such situations that would have to be considered. Though the likeli-

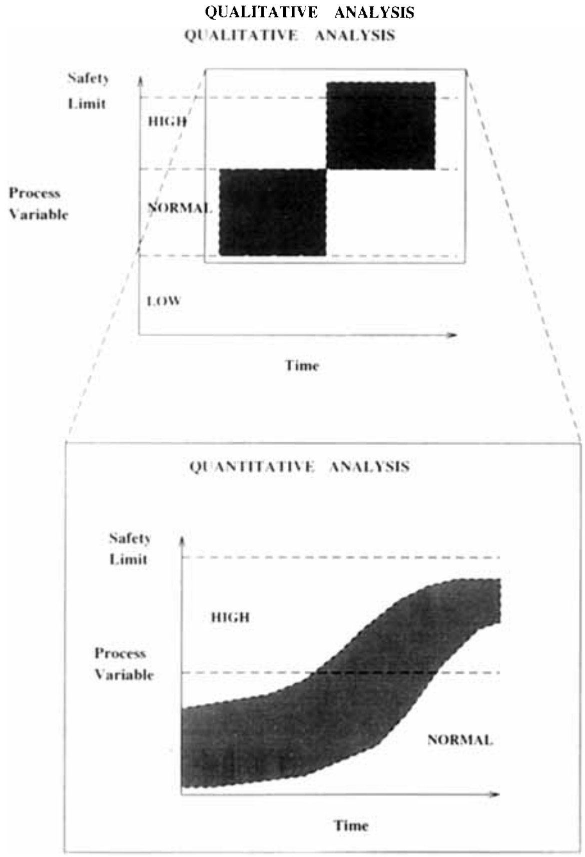

Figure 3. Integrated qualitative–quantitative safety analysis.

hood of multiple hazards occurring simultaneously may appear to be small, many serious industrial accidents reported in the literature have been caused by such seemingly unlikely events. A thorough PHA should therefore consider the occurrence of multiple faults also, but without being computationally prohibitive.

The integrated approach proposed here provides a framework for considering multiple-fault scenarios. The quantitative approach considers *all* possible combinations of inputs that can lead the process to an unsafe state. Thus, multiple faults leading to hazards can be automatically detected.

The operation of many process units in continuous plants exhibits both continuous and discrete characteristics, the latter arising due to discontinuities in physical phenomena, equipment geometry, or discrete process control. The digraph-based HAZOPExpert cannot explicitly account for the discrete nature of such units. Srinivasan and Venkatasubramanian (1995, 1998a,b) proposed integrating Petri nets with digraphs to perform HAZOP analysis for processes that exhibit such hybrid behavior. Such a framework can be applied to account for hybrid characteristics in continuous process units explicitly in the first phase. However, the approach followed in this article is to account implicitly for the hybrid behavior using the HDG as implemented in HAZOPExpert. When a hazard to be evaluated in detail involves a process with hybrid characteristics, the resulting quantitative model *does* account explicitly for the hybrid nature.

Safety Analysis Case Study

In this section, the application of the integrated framework to a real-life industrial case study is presented. This case study was first reported by Vaidhyanathan and Venkatasubramanian (1995). A conventional HAZOP analysis of this process was performed earlier by a team of experts and their results are available to us for comparison. The industrial case study involves the HAZOP analysis of a sour-water stripping plant shown in Figure 4. This process contains a refinery sour-water stream that is separated in a surge drum to remove slop oil from the sour water. The sour water is pumped to a storage tank where any carried-over slop oil can be skimmed off. From the storage tank the sour water is pumped through a heat exchanger to a steam stripper where ammonia and hydrogen sulfide are stripped from the water.

Vaidhyanathan and Venkatasubramanian (1995) reported the results of a HAZOP analysis as performed by the purely qualitative HAZOPExpert and compared these results with the conventional HAZOP study results. They reported that in general HAZOPExpert found about twice the number of causes and consequences than were recorded by the HAZOP team. Some of these extra consequences were due to HAZOPExpert's capability to perform a thorough analysis including propagations through the P&ID. However, several of these extra consequences were spurious in the sense discussed earlier. In this section, we show how the integrated framework can be applied to prune improbable hazards and to estimate the severity of a hazard reported by HAZOPExpert.

The important safety concerns in this plant are:

- Hydrocarbon oil is flammable
- Hydrogen sulfide and ammonia are toxic.

The release of any of these materials is a severe hazard. Also, if there is poor separation of hydrocarbon oil from the sour water, the oil will escape into the stripper, which can gum-up the stripper, thus leading to operational problems. HAZOPExpert identified that these hazards could occur for several process-variable deviations. Table 1 shows HAZOPExpert's results for ZERO flow into surge drum. One of the identified hazards—ZERO interface level—could be potentially dangerous since the organic layer would then drain to the storage tank. Although zero inlet flow would eventually lead to zero interface level, as predicted by HAZOPExpert, it is more useful for safety purposes to calculate the elapsed time after which such a deviation becomes safety critical. This provides an estimate of the time available to rectify the cause of the deviation (example, pump failure) or shut down the plant or take other corrective actions. Hence a quantitative safety verification of the surge drum operation was performed.

Surge drum

Figure 5 shows the portion of the plant around the surge drum in detail. Since HAZOPExpert has already identified that the potential hazard is in the surge drum, only this section of the plant has to be considered during detailed analysis. The sour water with the hydrocarbon oil enters the main reservoir where the lighter oil separates from the aqueous phase. The top oil layer flows over the weir and collects in the side oil reservoir. The PI controller controls the liquid

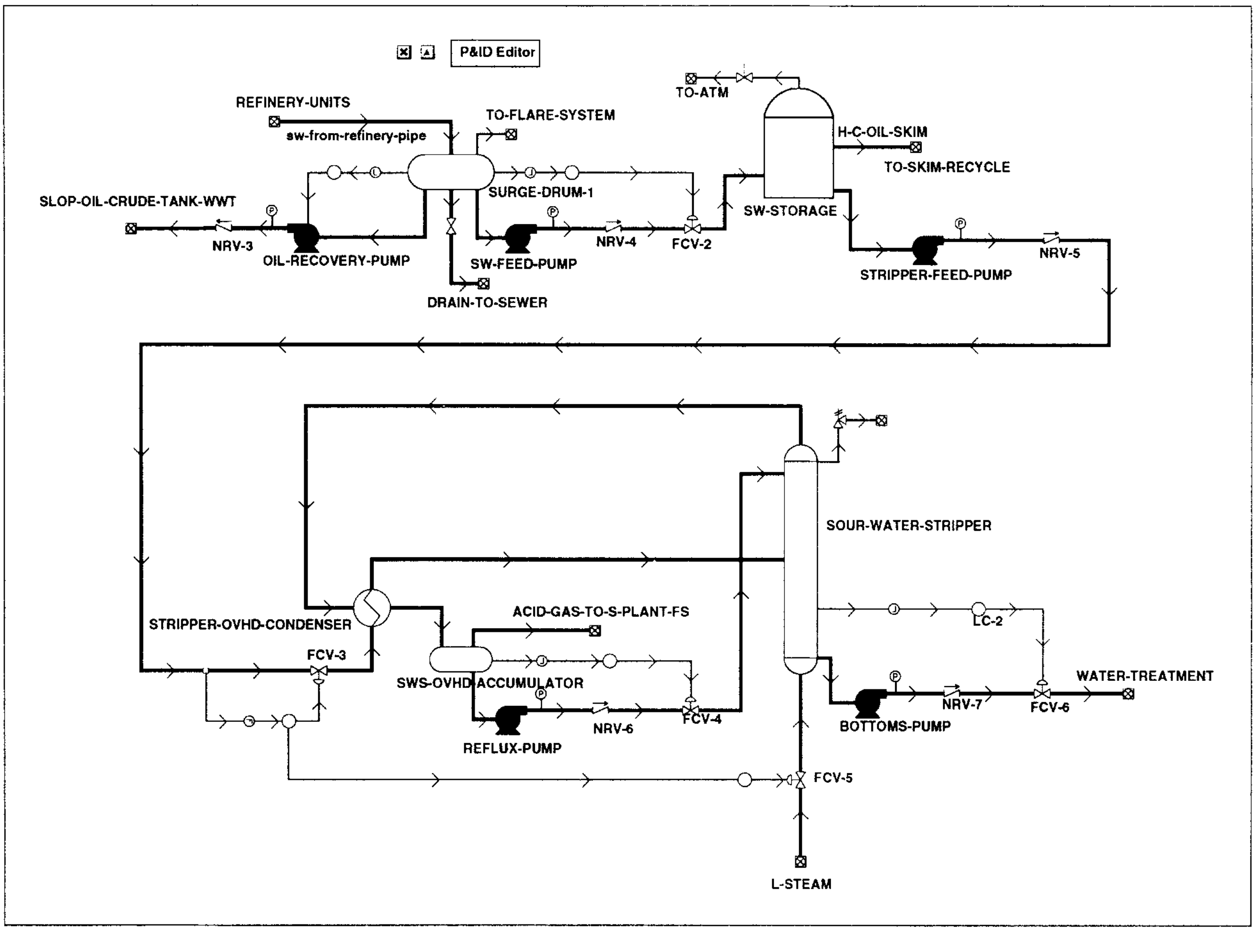

Figure 4. Sour-water stripper plant P&ID.

level in the main reservoir and the On–Off controller the level in the oil reservoir.

For quantitative safety verification of the surge drum, the hybrid behavior of the surge drum has to be explicitly represented. The state-transition model consists of four discrete states as shown in Figure 6. The states are described in Table 2, and the conditions for the transitions between the states to occur are indicated in Figure 6. Since the hazards to be focused on relate only to the amounts of the two phases, the mathematical model comprises only the mass balances for the main and side reservoirs. Also, the relative amounts of ammonia, hydrogen sulfide, and water in the aqueous phase need not be explicitly considered. The balance equations for the aqueous and the organic phases and the side outlet flow equations are the same in all the states. The F_{side} and $F_{\text{out,main}}$ equations, however, are different in each state.

Table 1. Conventional HAZOP Study and HAZOPExpert's Results

Process Variable Deviation: Zero Flow in sw-from-Refinery-Pipe
Conventional HAZOP Study Causes: Valve at battery limits is closed
HAZOPExpert's causes: Complete blockage of or major pipe fracture in sw-from-refinery-pipe
Conventional HAZOP study consequences: Upstream units cannot purge sour water
HAZOPExpert's consequences: Release of flammable hydrocarbon oil into plant area due to leak, causing fire hazard Zero interface level in surge drum 1 Zero level in surge drum 1 Zero heavy outlet flow in surge drum 1 Zero light outlet flow in surge drum 1

The model of the surge drum used for safety verification is shown in Appendix A. Binary variables are used to represent the surge drum state $[X_d(S_i,t)]$, logical conditions for transitions to occur $[L_d(S_i,\ S_j,\ t)]$, and transition occurrence $[\tilde{L}_d(S_i,\ S_j,\ t)]$.

$$X_d(S_i,t)=\begin{cases}1 & \text{if surge drum is in state } S_i \text{ at time } t\\ 0 & \text{otherwise}\end{cases}$$

$$L_d(S_i,S_j,t)=\begin{cases}1 & \text{if the logical conditions for the transition from state } S_i \text{ to state } S_j \text{ are satisfied at time } t\\ 0 & \text{otherwise}\end{cases}$$

$$\tilde{L}_d(S_i,S_j,t)=\begin{cases}1 & \text{if the transition from state } S_i \text{ to state } S_j \text{ occurs at time } t\\ 0 & \text{otherwise.}\end{cases}$$

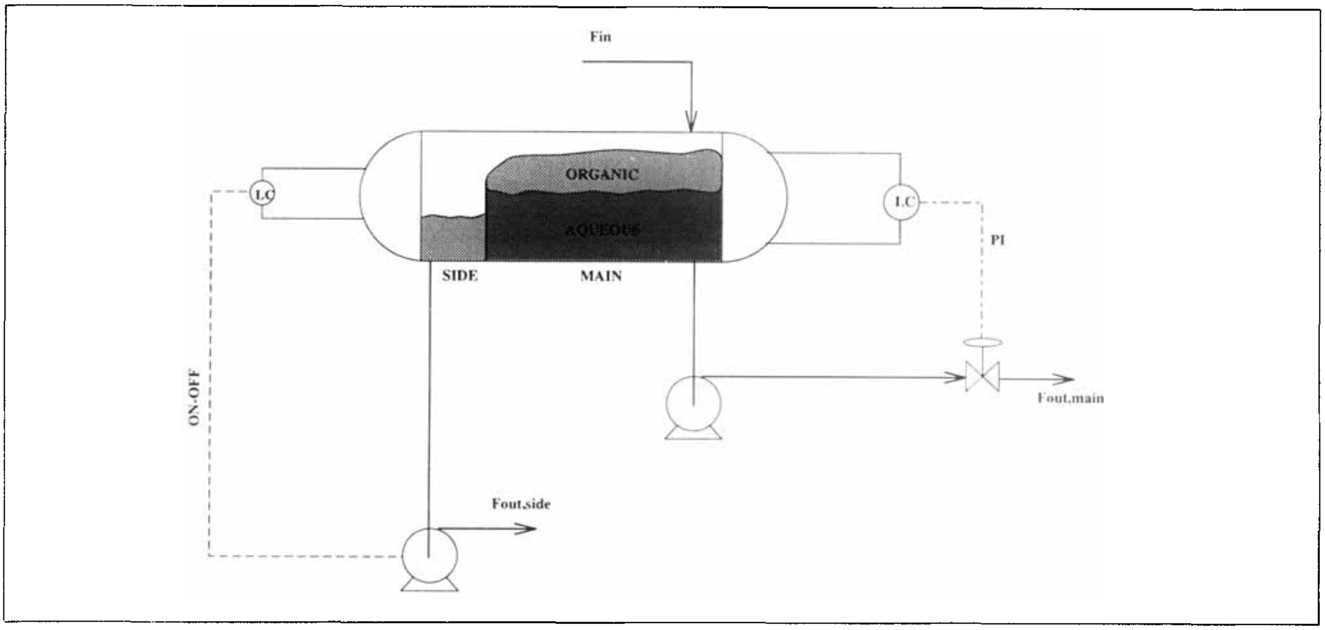

Figure 5. P&ID of the surge drum.

The objective is to maximize the time for which the system is in the HIGH or EMPTY states.

$$\max \sum_t X_d(\text{HIGH}, t) + \sum_t X_d(\text{EMPTY}, t).$$

Low or zero flow into the drum can cause the interface level to fall. When H_{main} falls below H_{low}, the slop-oil content in the main outflow increases sharply. This can eventually lead to buildup of the oil in the stripper, leading to gumming up of the trays. The quantitative verification phase was applied to determine the safe bounds on the input flow rates to the surge drum. Due to the hybrid nature of the surge drum operation, the safety formulation for this scenario results in a MILP formulation. For the low/no-flow deviation, based on HAZOPExpert results, only the states NORMAL, LOW, and EMPTY have to be considered along with the appropriate transitions between them. The disturbances considered are the inlet flow rates of the organic and aqueous phases—$F_{\text{in}}^{(o)}$ and $F_{\text{in}}^{(a)}$.

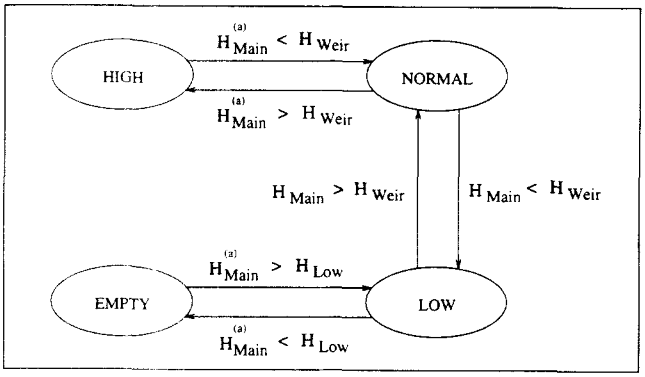
HIGH
NORMAL
EMPTY
LOW
$H_{\text{Main}}^{(a)} < H_{\text{Weir}}$
$H_{\text{Main}}^{(a)} > H_{\text{Weir}}$
$H_{\text{Main}} > H_{\text{Weir}}$
$H_{\text{Main}} < H_{\text{Weir}}$
$H_{\text{Main}}^{(a)} > H_{\text{Low}}$
$H_{\text{Main}}^{(a)} < H_{\text{Low}}$

Figure 6. State-transition representation for surge drum.

Engineering simplifications can be used in the dynamic process model required for safety analysis. For example, detailed modeling of the separation of the organic layer from the aqueous layer in the surge drum is not essential. Instead, the minimum time for organic flow through the main outlet to occur (a hazardous situation) was evaluated for different values of H_{low} – this gives an indication of the time available for corrective measures. Also, the miscibility of the organic and the aqueous phases can be ignored. The height of liquid in the organic reservoir ("side") was assumed to be below the weir.

An open-loop safety analysis was first performed for this system. The results for the low-flow scenario are summarized in Table 3. The system was specified to be initially in the NORMAL state. This constrains the initial values of $H_{\text{main}}^{(a)}$ and $H_{\text{main}}^{(o)}$. For all values of H_{low} the system reached the EMPTY state, and the time before this occurred was higher for smaller values of H_{low}. The optimal disturbance profiles calculated in all these cases were found to correspond to the maximum allowed organic flow (0.18 mol/s) and minimum allowed aqueous flow (0 mol/s).

With the controllers present in this system, the setpoint of the controller becomes an additional "disturbance" that has to be considered. Table 4 summarizes the results for the closed-loop low/no-flow analysis, with H_{low} as 0.1 m. It can be seen from these that even for zero inlet flows, if the setpoint ($H_{\text{main},SP}$) is above 1.25, drainage of the drum is not a potential problem for 2000 s. It is very unlikely that the setpoint would ever be set below H_{weir} ($= 1.55$ *m*). This com-

Table 2. Description of States of the Surge Drum

State	Description
HIGH	Interface above H_{weir}
NORMAL	Interface below H_{weir}, total height above H_{weir}
LOW	Total height below H_{weir}, aqueous phase above H_{low}
EMPTY	Aqueous phase below H_{low}

Table 3. Surge Drum Open-Loop Low/No-Flow Results

$\mathcal{K}$	H_{Low} m	Time to Reach Unsafe State s
10	0.5	1,200
10	0.3	1,600
15	0.1	2,200

pares well with the experts' results where the consequences for this deviation do not include slop oil entering the sour-water storage tank.

HAZOPExpert's consequences for HIGH flow into surge drum are listed below.

- Pipe subjected to surge pressure, flange leak, possible pipe rupture, and loss of containment
- High interface level in surge drum
- High heavy outlets flow rate
- High light outlets flow rate
- High level in surge drum
- Filling up of surge drum, possibility of liquid entering vent
- Release of flammable hydrocarbon oil into plant area due to filling up and overflow of surge drum, causing fire hazard.

One of the identified hazards—release of flammable hydrocarbon oil—is another serious hazard that needs to be evaluated further. An analysis similar to the one just made was performed for HIGH inlet flow-rate deviation. In the interest of space, only a summary is reported. The analysis indicated that the system would remain safe even for a 50% increase from the steady-state flow rate for both the open-loop and closed-loop cases for over 30 min.

Stripper

Safe operation of the stripper is obviously important. The direct application of the quantitative safety formulation to such a system would lead to an extremely large mathematical optimization problem. In this section, the safety analysis of the stripper in the integrated framework is reported. This part of the flow sheet consists of the stripper, with an overhead condenser and accumulator. Sour water, fed to the top of the column, is stripped with steam fed directly to the column bottom. Most of the ammonia and hydrogen sulfide is concentrated in the distillate with the bottoms containing mostly water and small quantities of ammonia. One of the potential hazards identified by HAZOPExpert in the stripper is due to high feed flow rate. This can lead to high bottoms level causing column flooding, potential tray damage, buildup of high pressure, and release of flammable hydrocarbon oil and toxic ammonia and hydrogen sulfide. A detailed analysis of the stripper to estimate when column flooding can occur was performed.

Table 4. Surge Drum Closed-Loop Low/No-Flow Results

Bounds on $H_{\text{main},SP}$ m	Time to Reach Unsafe State s
≤ 0.92	1,000
(0.92, 1.04)	1,200
(1.04, 1.13)	1,400
(1.13, 1.19)	1,600
(1.19, 1.25)	1,800
≥ 1.25	> 2,000

A dynamic model for this section of the flow sheet was created using the dynamic simulator gPROMS (Barton and Pantelides, 1994). Simplifications of the dynamic model of the stripper were made based on HAZOPExpert results. None of the hazards in this plant are related to the actual concentrations of the trace ammonia or hydrogen sulfide. Hence from a safety perspective, their presence can be ignored in the vapor-liquid equilibria, enthalpy, and density calculations. Also, theoretical trays were assumed. An additional simplification of fast energy dynamics (resulting in an algebraic energy balance) was made. This was primarily for numerical simplicity to overcome stiff systems of differential algebraic equations. The gPROMS model of the stripper section used for safety verification is shown in Appendix B.

A safety analysis of the stripper for the HIGH bottoms level was performed using gOPT. gOPT is a dynamic optimization package that can directly use gPROMS models as constraints (gPROMS Project, 1995). The continuous nature of the stripper operation obviates the need for discretization, but otherwise the concepts behind the safety-verification problem are the same as for the surge drum. Safety verification was considered for a total time horizon of 2,500 s. This time horizon was divided into three time intervals—the first was of fixed duration (1,500 s), during which the system reached steady state, the division of the remaining 1,000 s between the second and third intervals was determined by the optimization. The system was noted to be returning to steady state at the end of the third interval. The optimization variables in this analysis are the feed flow rate to the stripper, the controller parameters (K_c and K_I) on the bottoms level controller, and the duration of the second and third time intervals. Of these, K_c and K_I are time-invariant parameters, while the feed flow rate is time-dependent-piecewise-constant in each interval. The objective of the optimization was to make the system "unsafe" for the maximum possible time. The system was considered unsafe if the bottoms level exceeded 1.5 m. Though this was arbitrarily fixed, it is based on experience with similar systems. The nature of the analysis itself is independent of the exact value of the limit.

Table 5 shows the maximum bottoms level that occurred for the open-loop case, and Table 6 for the closed-loop case. It can be seen from the open-loop results that a flow rate of over 543 mol/s is required for the bottoms level to rise over 1.5 m, if no controller is present. However, when a PI controller is added to maintain the bottoms level, for a wide range of values on the controller parameters, the bottoms of the stripper can flood even at lower flow rates. Figure 7 shows an example of such a scenario where column flooding occurs. Here, when the feed flow decreases from its steady-state value to 210.44 mol/s, the integral error in the PI controller grows and the outlet flow rate drops. Then, when the feed flow rate increases to 491.02 mol/s, due to the large integral error the

Table 5. Open-Loop Safety Analysis of Stripper

Feed Flow mol/s	Max. Bottoms Level m	Flooding Possible? Yes/No
[210.44, 491.02]	1.37	No
543.63	1.50	Yes

Table 6. Closed-Loop Safety Analysis of Stripper

Conditions Feed in mol/s	Max. Bottoms Level m
Feed = 491.02 $K_c \in [0.0, 1.0]$ $k_i = 1.0$	1.25
Feed = 491.02 $K_c < 0.688$ $K_i \in [0.0, 1.0]$	≥ 1.5
Feed $\in [210.44, 491.02]$ $K_c = 1.0$ $K_i = 1.0$	1.63
Feed $\in [210.44, 491.02]$ $K_c \in [0.7, 3.0]$ $K_i \in [1.25, 3.0]$	1.62
Feed $\in [210.44, 491.02]$ $K_c \in [2.0, 4.0]$ $K_i \in [2.75, 5.0]$	1.55
Feed $\in$ [210.44, 491.02 $K_c \in [2.0, 4.0]$ $K_i \in [3.75, 5.0]$	< 1.5

outlet flow rate increases slowly, thus causing flooding. It can be seen from the closed-loop results that flooding of the column can be prevented by proper controller tuning.

Conclusions and Discussion

Process hazards analysis is an important and difficult problem that would benefit from automation. Previous attempts at automating HAZOP analysis were successful but suffered from qualitative ambiguity. On the other hand, the quantitative safety-verification approach often leads to large mathematical programs that are difficult to solve. In this article, we have proposed a framework for integrating qualitative and quantitative safety analyses. This approach has the capability of performing exact analysis when required and thus overcomes qualitative ambiguity, but results in focused mathematical programs that are smaller and easier to solve. Typical performance results are reported for an industrial HAZOP case study of a sour-water stripper plant.

The integrated framework requires some detailed information about the process units, such as the dimensions of the process units, safe temperature, and pressure. However, such information is usually available at the stage of design when detailed safety analysis is carried out. For existing plants, such information can be easily obtained from the plant P&IDs. Also, exact values for process parameters are not needed and approximate bounds on these parameters are sufficient. This approach presumes the availability of dynamic models for the process units in the process. Currently, models exist for several common units like tanks, surge drum, and stripper. We are developing models for some more units. Using these unit models, the process model to be used in the quantitative analysis phase for each hazard can be generated. At present, this process model has to be generated manually. We are currently working on automating the generation of the process model based on the unit models and the hazards identified during the qualitative analysis so that once hazards have been identified using qualitative analysis, the second phase of quantitative analysis can be performed automatically without any manual intervention.

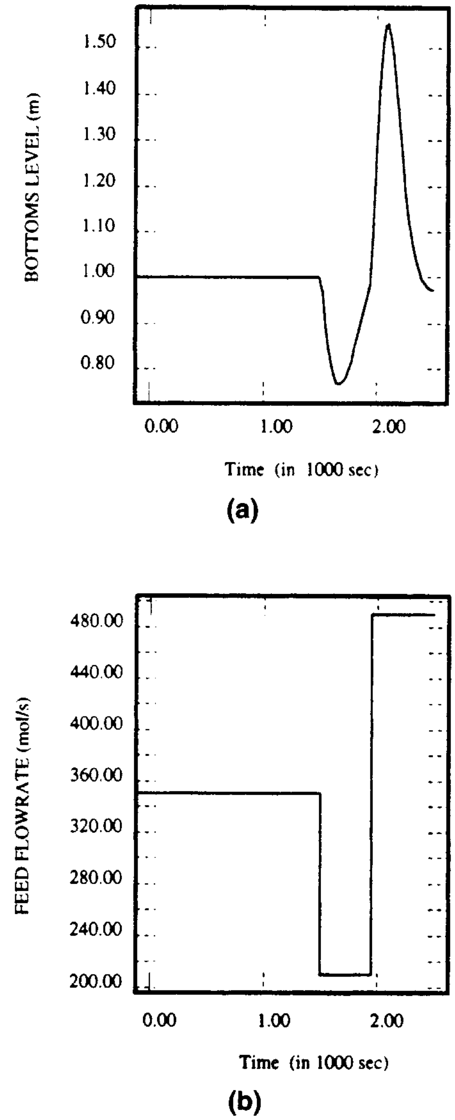

Figure 7. (a) Bottom level in stripper for the optimal flow profile in (b).

Notation

A_{main} = area of main reservoir
A_{side} = area of side reservoir
F_{in} = total flow rate into the surge drum
$F_{\mathrm{in}}^{(a)}$ = aqueous flow rate into the surge drum
$F_{\mathrm{in}}^{(o)}$ = organic flow rate into the surge drum
F_{side} = total flow rate from the main reservoir to the side reservoir
$F_{\mathrm{side}}^{(a)}$ = aqueous flow rate from the main reservoir to the side reservoir
$F_{\mathrm{side}}^{(o)}$ = organic flow rate from the main reservoir to the side reservoir
$F\mathrm{out}_{\mathrm{main}}$ = total outlet flow rate from the main reservoir
$F\mathrm{out}_{\mathrm{main}}^{(a)}$ = aqueous outlet flow rate from the main reservoir
$F\mathrm{out}_{\mathrm{main}}^{(o)}$ = organic outlet flow rate from the main reservoir
$F\mathrm{out}_{\mathrm{side}}$ = total outlet flow rate from the side reservoir
$F\mathrm{out}_{\mathrm{side}}^{(a)}$ = aqueous outlet flow rate from the side reservoir
$F\mathrm{out}_{\mathrm{side}}^{(o)}$ = organic outlet flow rate from the side reservoir
H_{main} = height of liquid in the main reservoir of the surge drum
$H_{\mathrm{main}}^{(a)}$ = height of aqueous phase in the main reservoir of the surge drum

$H^{(a)}_{\text{main}}$ = height of aqueous phase in the main reservoir of the surge drum
$H^{(o)}_{\text{main}}$ = height of organic phase in the main reservoir of the surge drum
H_{side} = height of liquid in the side reservoir of the surge drum
$H^{(a)}_{\text{side}}$ = height of aqueous phase in the side reservoir of the surge drum
$H^{(o)}_{\text{side}}$ = height of organic phase in the side reservoir of the surge drum
H_{weir} = height of the weir in the surge drum
H_{low} = height of the aqueous phase when the organic drainage through the main outlet begins
K_{main} = flow resistance constant for main reservoir
K_{side} = flow resistance constant for side reservoir
K_{weir} = weir constant

Literature Cited

Barton, P. I., and C. C. Pantelides, "Modeling of Combined Discrete/Continuous Processes," *AIChE J.*, **40**(6), 966 (1994).

CCPS, *Guidelines for Hazard Evaluation Procedures*, New York (1985).

Dimitriadis, V., J. Hackenberg, N. Shah, and C. Pantelides, "A Case Study in Hybrid Process Safety Verification," *Comput. Chem. Eng.*, **20**(Suppl), S503 (1996).

Dimitriadis, V., N. Shah, and C. Pantelides, "Model-Based Safety Verification of Discrete/Continuous Chemical Processes," AIChE Meeting, San Francisco (1995).

Dimitriadis, V., N. Shah, and C. Pantelides, "Modelling and Safety Verification of Discrete/Continuous Processing Systems," *AIChE J.*, **43**(4), 1041 (1997).

gPROMS Project, "Solving Dynamic Optimisation Problems in gPROMS," Tech. Rep., Centre for Process Systems Engineering, Imperial College, London (1995).

Karvonen, I., P. Heino, and J. Suokas, *Knowledge Based Approach to Support HAZOP-Studies*, Res. Rep., Technical Research Center of Finland, Helsinki, (1990).

Kletz, T. A., *HAZOP & HAZAN Notes on the Identification and Assessment of Hazards*, The Institution of Chemical Engineers, Rugby, England (1986).

Knowlton, R. E., *Hazard and Operability Studies: The Guide Word Approach*, Chematics International Company, Vancouver, WA (1989).

Lawley, H. G., "Operability Studies and Hazard Analysis," *Chem. Eng. Prog.*, **70**, 105 (1974).

Lawley, H. G., "Size Up Plant Hazards this Way," *Hydroc. Process.*, **55**, 247 (1976).

Rushton, A. G., "Approaches and Methods in Computer Emulation of HAZOP," *Loss Prevention and Safety Promotion in the Process Industries*, J. J. Mewis, H. J. Pasman, and E. E. D. Rademaeker, eds., Vol. II, Elsevier, New York, p. 741 (1995).

Srinivasan, R., and V. Venkatasubramanian, "Integrating Petri Nets and Digraphs to Represent the HAZOP Knowledge of Batch Processes," AIChE Meeting, Miami Beach, FL (1995).

Srinivasan, R., and V. Venkatasubramanian, "Automating HAZOP Analysis of Batch Chemical Plants: I. Knowledge Representation Framework," *Comput. Chem. Eng.*, (1998a).

Srinivasan, R., and V. Venkatasubramanian, "Automating HAZOP Analysis of Batch Chemical Plants: II. Algorithms and Application," *Comput. Chem. Eng.*, (1998b).

Vaidhyanathan, R., and V. Venkatasubramanian, "Digraph-Based Models for Automated HAZOP Analysis," *Reliab. Eng. Syst. Saf.*, **50**, 33–49 (1995).

Vaidhyanathan, R., and V. Venkatasubramanian, "HAZOPExpert: An Expert System for Automating HAZOP Analysis," *Process Saf. Prog.*, **15**(2), 80 (1996a).

Vaidhyanthan, R., and V. Venkatasubramanian, "A Semi-Quantitative Reasoning Methodology for Filtering and Ranking HAZOP Results in HAZOP Expert," *Reliab. Eng. Syst. Saf.*, **53**, 185 (1996b).

Venkatasubramanian, V., and M. Preston, "A Perspective on Intelligent Systems for Process Hazards Analysis," *Proc. Intelligent Conf. on Intelligent Systems in Process Engineering*, J. F. Davis, G. Stephanopoulos, and V. Venkatasubramanian, eds., CACHE, New York, NY, p. 160 (1996).

Venkatasubramanian, V., and R. Vaidhyanathan, "A Knowledge-Based Framework for Automating HAZOP Analysis," *AIChE J.*, **40**, 496 (1994).

Appendix A: Model of Surge Drum

Figure 5 shows the portion of the plant around the surge drum in detail. The model of this section used in the quantitative verification phase is presented below.

The mass-balance equations in the main and side section equations are the same in all the four states:

$$A_{\text{main}} H^{(o)}_{\text{main}}(t+1) = A_{\text{main}} H^{(o)}_{\text{main}}(t) + \Delta t[Fin^{(o)}(t) - Fside^{(o)}(t) - Fout^{(o)}_{\text{main}}(t)] \quad \text{(A1)}$$

$$A_{\text{main}} H^{(a)}_{\text{main}}(t+1) = A_{\text{main}} H^{(a)}_{\text{main}}(t) + \Delta t[Fin^{(a)}(t) - Fside^{(a)}(t) - Fout^{(a)}_{\text{main}}(t)] \quad \text{(A2)}$$

$$A_{\text{side}} H^{(o)}_{\text{side}}(t+1) = A_{\text{side}} H^{(o)}_{\text{side}}(t) + \Delta t[Fside^{(o)}(t) - Fout^{(o)}_{\text{side}}(t)] \quad \text{(A3)}$$

$$A_{\text{side}} H^{(a)}_{\text{side}}(t+1) = A_{\text{side}} H^{(a)}_{\text{side}}(t) + \Delta t[Fside^{(a)}(t) - Fout^{(a)}_{\text{side}}(t)]. \quad \text{(A4)}$$

It can be assumed that the side section of the surge drum never runs dry. Therefore, the equations for $Fout_{\text{side}}$ would also be the same for all states:

$$Fout^{(o)}_{\text{side}}(t) = K_{\text{side}} H^{(o)}_{\text{side}}(t) \quad \text{(A5)}$$

$$Fout^{(a)}_{\text{side}}(t) = K_{\text{side}} H^{(a)}_{\text{side}}(t). \quad \text{(A6)}$$

The equations for $Fside$ and $Fout_{\text{main}}$, however, are different for each state.

The equations for the HIGH state are

$$Fside^{(o)}(t) = K_{\text{weir}} H^{(o)}_{\text{main}}(t) \quad \text{(A7)}$$

$$Fside^{(a)}(t) = K_{\text{weir}}[H^{(a)}_{\text{main}}(t) - H_{\text{weir}}] \quad \text{(A8)}$$

$$Fout^{(o)}_{\text{main}}(t) = 0 \quad \text{(A9)}$$

$$Fout^{(a)}_{\text{main}}(t) = K_{\text{main}}[H^{(o)}_{\text{main}}(t) + H^{(a)}_{\text{main}}(t)]. \quad \text{(A10)}$$

The equations for NORMAL state are

$$Fside^{(o)}(t) = K_{\text{weir}}[H^{(o)}_{\text{main}}(t) + H^{(a)}_{\text{main}}(t) - H_{\text{weir}}] \quad \text{(A11)}$$

$$Fside^{(a)}(t) = 0 \quad \text{(A12)}$$

$$Fout^{(o)}_{\text{main}}(t) = 0 \quad \text{(A13)}$$

$$Fout^{(a)}_{\text{main}}(t) = K_{\text{main}}[H^{(o)}_{\text{main}}(t) + H^{(a)}_{\text{main}}(t)]. \quad \text{(A14)}$$

The equations for LOW state are

$$Fside^{(o)}(t) = 0 \quad \text{(A15)}$$

$$Fside^{(a)}(t) = 0 \quad \text{(A16)}$$

$$Fout^{(o)}_{\text{main}}(t) = 0 \quad \text{(A17)}$$

$$Fout^{(a)}_{\text{main}}(t) = K_{\text{main}}[H^{(o)}_{\text{main}}(t) + H^{(a)}_{\text{main}}(t)]. \quad \text{(A18)}$$

The equations for EMPTY state are

$$F\text{side}^{(o)}(t)=0 \tag{A19}$$

$$F\text{side}^{(a)}(t)=0 \tag{A20}$$

$$F\text{out}^{(o)}_{\text{main}}(t)=K_{\text{main}}H^{(o)}_{\text{main}}(t) \tag{A21}$$

$$F\text{out}^{(a)}_{\text{main}}(t)=0. \tag{A22}$$

Appendix B: Model of the Stripper Section

The stripper section of the case study consists of a tray column, an overhead condensor, and an accumulator. For the qualitative verification phase, a model of the stripper section was created using gPROMS (Barton and Pantelides, 1994). A part of the model is shown below:

```
MODEL Tray
 PARAMETER
  NC             as INTEGER     # No of components
  MW             as REAL        # Molecular weights
 # Tray Parameters
  AREA           as REAL
  HOLEAREA       as REAL
  KWeir          asREAL
  HWEIR          as REAL

  ALPHA          as REAL
  BETA           as REAL
  G              as REAL
 UNIT
  ThermoVLE     as ThermoMyVLE
  THERMoHL      as ThermoLEnthalpy
  THermoHV      as ThermoVEnthalpy
VARIABLE
  press,pressBot,pressTop           as Pressure
  temp                              as Temperature
  MHoldup                           as MolarHoldup
  v, 1, vBot, 1Top                  as MolarFlowrate
  vel                               as vapVelocity
  liqDens,vapDens                   as LiquidDensity
  liqLevel                          as LiqHeight
  H1,H1Top                          as LiqEnthalpy
  Hv,HvBot                          as VapEnthalpy
  q                                 as Power
STREAM
# Physical Streams
  vaporBot:pressBot,vBot,HvBot      as IOVapor Stream
  liquidTop:pressTop,1Top,H1Top     as IOLiquidStream
  vapor    :press, v, Hv            as IOVaporStream
  liquid   :press, 1, H1            as IOLiquidStream

# Thermodynamics Virtual Streams
  VLESt         :press,temp         as IOThermoVLEStream
  LEnthalpySt   :press,temp,H1      as IOThermoHLStream
  VEnthalpySt   :press,temp,Hv      as IOThermoHVStream

SET
  AREA       : = 0.65669 ; #m2
  HOLEAREA   : =  .1 ; #m2
  KWeir      : = 1.41;
  HWEIR      : = 0.3 ;

  ALPHA      : = 1.0;
  BETA       : = 3E-4 ;
  G          : = 10;

EQUATION
# Mass Balances
  $MHoldup = vBot  + 1Top  − v  − 1;
# Energy Balances
  0 = vBot * HvBot  + 1Top * H1Top  − v * Hv − 1 * H1 + q;
# Flow rates
  liqDens = 1E6; #Water Density
  vapDens = 1E3; #Steam Density

  liqLevel = MHOLDUP * MW/(liqDens  *  AREA);
  1 = KWeir * 0.1 * liqDens
       * max((liqLevel-HWEIR) ^ 1.5,0); # Francis Weir Law

  v =  vapDens * HOLEAREA * vel;
  pressBot - press  =  ALPHA * (vel ^ 2) * vapDens
                                 + BETA * liqDens * G * (liqLevel);

# Thermo properties connections
   ThermoVLE.input   IS VLESt;
   ThermoHL.input    IS LEnthalpySt ;
   ThermoHV.input    IS VEnthalpySt ;

END # Tray Model
```

Manuscript received Apr. 11, 1997, and revision received Nov. 18, 1997.