Petri-Net Models for Risk Analysis of Hazardous Liquid Loading Operations

N. Balasubramanian,† Chuei-Tin Chang,* and Yi-Feng Wang

Department of Chemical Engineering, National Cheng Kung University, Tainan, Taiwan 70101, ROC

A vigorous hazard assessment is almost mandatory for the safety and risk-free operation of any chemical plant. A systematic approach has been developed in this study to construct a generic Petri-net (PN) model for analyzing the liquid ammonia loading process. A set of sub-PNs were first built for all components in the system. Failure mechanisms were then developed and incorporated into these component models. On the basis of predefined hazardous conditions, the critical fault propagation scenarios were identified accordingly with simulation studies. It is observed from the simulation results that the proposed model can be effectively used for hazard identification in the sequential operations.

Introduction

To satisfy the needs of various industrial activities, many hazardous chemicals, e.g., ammonia, chlorine, ethylene oxide, and liquefied petroleum gas, are shipped almost daily on public highways and loaded into large storage facilities. Accidental release of such materials can cause deaths, serious injuries, lasting health effects, and damages to the environment. To comply with government regulations and enhance process safety, a vigorous risk analysis of the loading operations of hazardous chemicals becomes necessary.

Numerous methodologies have been established for analyzing complex chemical processes. These include fault-tree analysis, event-tree analysis, hazard and operability study (HAZOP), failure mode and effect analysis, etc. However, if implemented manually on an ad hoc basis, these methodologies are often ineffective and error-prone in practical applications. Several tools were thus proposed in the literature to develop computer aids for improving the quality of analysis.[1−5] Lapp and Powers[6] proposed the first digraph-based computer-aided fault-tree synthesis methods. Vaidyanathan and Venkatsubramanian[1,2] developed a systematic approach to automatically perform HAZOP analysis for continuous processes. Chang et al.[7,8] improved the Lapp−Powers algorithm with qualitative simulation techniques. Khan and Abbasi[9] built an expert system OPTHAZOP for hazard identification and verified it with the chloroalkali process. Srinivasan and Venkatsubramanian[10,11] extended the work of Vaidyanathan and Venkatsubramanian[1,2] for batch operations according to the hybrid Petri-net (PN)−digraph models.

From a critical review of the above works on hazard analysis, one can observe the following:

1. Digraph is mostly applicable to continuous processes, while PN can be used to represent both continuous and batch operations.

2. The PN−digraph hybrid models are not suitable for describing some of the important features in realistic sequential operations, e.g., concurrent activities, cyclic operations, continuous transients, and multipurpose productions.[12]

3. One common deficiency of the existing computer aids is the lack of transparency on the stepwise path leading to hazardous outcomes.

4. Most of the approaches to implement automatic hazard analysis were demonstrated on small-scale processes or with academic examples.

Loading of hazardous chemicals is a typical sequential operation for which safety analysis is mostly done manually. As mentioned in the previous discussions, the existing techniques may not be suitable for analyzing such operations. It is thus the objective of the present study to develop a generic approach to construct improved PN models, which either can be used on a stand-alone basis or incorporated in automatic HAZOP/fault-tree analysis/failure mode and effect analysis systems.

The rest of the paper is organized as follows. First of all, the detailed operating procedure of the liquid ammonia loading process is described. Second, a number of PN models have been developed for all process units in the loading operation. These component models are then assembled according to the process flow sheet and operating procedure toward the development of a system model. Next different failure mechanisms of each individual component are introduced into this system model. On the basis of the resulting PN model and a set of predefined system hazards, simulation studies are carried out to identify critical fault propagation scenarios. Finally, the results of several interesting case studies are presented at the end of this paper.

Loading Operation of Liquid Ammonia

To illustrate the proposed modeling approach, a typical sequential operation is considered in this paper. Specifically, let us consider the simplified P&ID of the liquid ammonia loading facility presented in Figure 1.[13] This facility contains four major equipments: ammonia storage tank, compressor, truck, and waste ammonia dilution drum.

The ammonia storage tank is fitted with a safety valve, a pressure gauge, a refrigeration system, and a liquid level indicator. Because of its high affinity toward water, liquid ammonia is transported from truck to

* Corresponding author. Tel: 886-6-275-7575 ext. 62663. Fax: 886-6-234-4496. E-mail: ctchang@mail.ncku.edu.tw.

† Permanent address: Department of Pollution Control, Central Electrochemical, Research Institute, Karaikudi, 630 006 Tamilnadu, India.

10.1021/ie010639r CCC: $22.00
Published on Web 00/00/0000 **PAGE EST: 13.7**

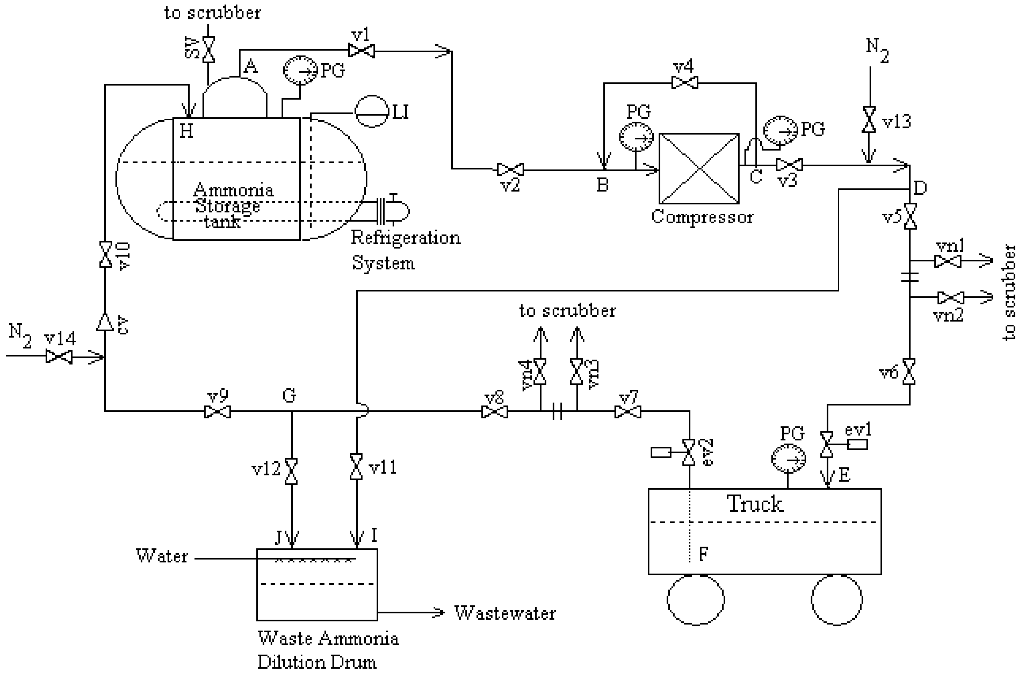

Figure 1. Simplified P&ID of the liquid ammonia loading facility.

storage tank by compressing gaseous ammonia. The compressor inlet is connected to the storage tank. The vapor pressure in the storage tank is maintained at approximately 3 kg/cm^2 gauge by controlling the liquid temperature with a refrigeration system. The truck pressure is increased with the compressor to a level higher than that of the storage tank. The pressure difference between truck and tank causes flow in the liquid transport line.

The loading procedure consists of a number of specific tasks. For the sake of brevity, it is assumed that this operation starts when both liquid and gas transport lines are properly connected. In other words, only the operation steps executed after line connection are considered here. A brief outline of these tasks are given below:

Task 1: Preparation of the gas transport line.

Step 1.1: Open valves v1−v3, v5, and v6.

Step 1.2: Open the emergency isolation valve ev1.

Task 2: Preparation of the liquid transport line

Step 2.1: Open the emergency isolation valve ev2.

Step 2.2: Open the valves v7−v10.

Task 3: Compressor start-up.

Step 3.1: Close the inlet and outlet valves v2 and v3.

Step 3.2: Open the recycle valve v4.

Step 3.3: Switch on the compressor.

Step 3.4: Open the inlet and outlet valves v2 and v3 and close the recycle valve v4 after the compressor outlet pressure is increased to 0.2−0.5 kg/cm^2 above its inlet pressure.

Task 4: Monitoring the loading operation.

Check and record the readings of the pressure gauges and liquid level sensor at regular intervals. Terminate the loading operation when the reading of the level sensor reaches a predetermined value.

Task 5: Compressor shutdown.

Step 5.1: Close the inlet and outlet valves v2 and v3.

Step 5.2: Open the recycle valve v4.

Step 5.3: Switch off the compressor.

Step 5.4: Close the recycle valve v4.

Task 6: Purging the gas transport line with N_2.

Table 1. Hierarchy in the PN Model for Liquid Ammonia Loading Operation

level	components
1	operator
2	valves, compressor
3	tanks, truck, dilution drum, pipelines
4	ammonia
5	level sensors, pressure gauges, safety valve

Step 6.1: Close the valves v1 and ev1.

Step 6.2: Open valve v13 on the nitrogen supply line.

Step 6.3: Purge the remaining ammonia gas in the gas transport line to the dilution drum by opening valve v11.

Step 6.4: Close valves v5, v6, v11, and v13.

Task 7: Purging the liquid transport line with N_2.

Step 7.1: Close valves v10 and ev2.

Step 7.2: Open valve v14 on the nitrogen supply line.

Step 7.3: Purge the remaining liquid ammonia in the liquid transport line to the dilution drum by opening valve v12.

Step 7.4: Close valves v7−v9, v12, and v14.

After completion of task 7, the vent valves vn1 to vn4 should be opened before disconnecting the flanges and then the same should be closed afterward.

Development of Component Models

After a careful review of the P&ID and operating procedure, all components in the ammonia loading facility have been identified and classified according to Table 1. A hierarchical approach is followed in the present investigation to construct the PN-based models. In the loading process, the first-level component, i.e., the operator, executes the operating steps specified in a recipe. His or her actions alter the states of valves and also the compressor in the second level. The states of these components, in turn, determine the process configuration and/or the operation mode of each process unit in the third level. The changes in the states of process materials in the fourth level are governed by

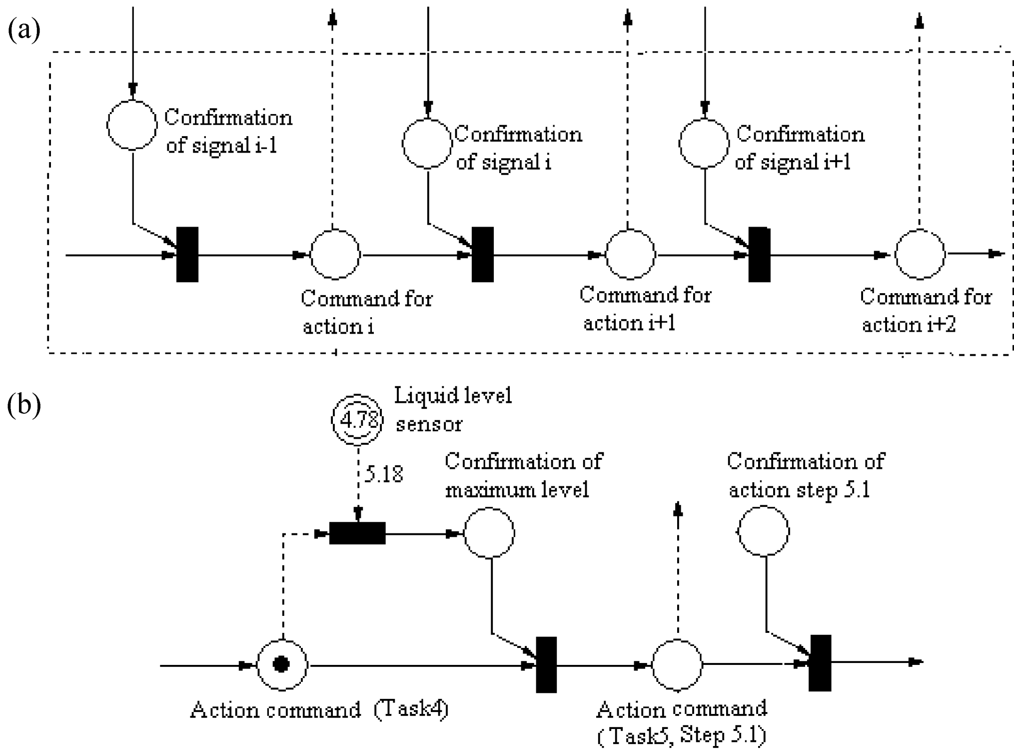

Figure 2. (a) General PN model of a plant operator. (b) PN model for an operator during task 4.

the operating mode, and these process states can be monitored via sensors in the last level.

The PN models for all components in each level of the hierarchy are developed in this section. For the sake of brevity, the description of the symbols used in standard PNs are omitted. Only special extensions will be explained later in this paper. The readers may refer to a review paper, e.g., David and Alla,[14] for further details.

Level 1. It is assumed in this study that the operator always faithfully executes the actions specified in the recipe. From the operating procedure described in the previous section, each operator action should be carried out after completion of a previous action and/or confirmation of an external signal. The PN model can be constructed according to the general structure presented in Figure 2a. Notice that the dotted arrows represent test arcs.[14] Notice also that the external signals can be sensor readings or equipment states that are identifiable to the operator. On the other hand, the action commands are always concerned with alteration of the states of second-level components or checking and recording of the sensor outputs in the fifth level. Say, for example in task 4, the operator regularly monitors the liquid level sensor during the loading process (Figure 2b). The confirmation place will get a token when the liquid level in the tank reaches the predetermined value. Upon obtaining this information, the operator moves to the next course of action, i.e., step 5.1.

Level 2. As mentioned before, the second level of hierarchy in this model consists of 20 valves and a compressor. The states of any valve can be characterized with its positions, i.e., open or close. The corresponding PN model is presented within the dashed line in Figure 3. Notice that the places representing action commands to open and close valves should be included in the operator model.

The other component in this level is a compressor. A compressor can be described with two states: on and off. The transition to alter the compressor state is also enabled by action commands. The PN model for a compressor is given in Figure 4.

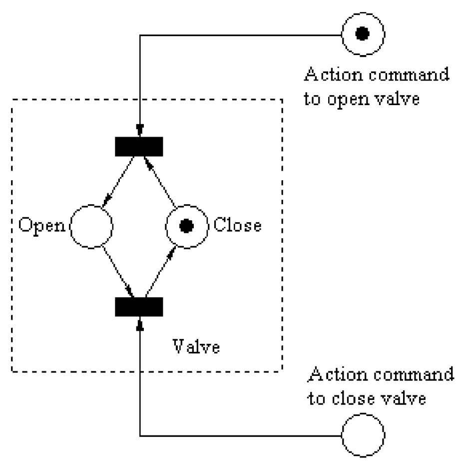

Figure 3. PN model of a valve.

Level 3. The components in this level are the truck, the storage tank, the dilution drum, and the pipelines. A careful review of the P&ID shows that there are eight pipelines in the ammonia loading facility: Pipeline 1 connects the liquid ammonia storage tank and compressor, i.e., from point A to point B. Pipeline 2 connects the compressor outlet and the joint of the gas purge line, i.e., from point C to point D. Pipeline 3 connects the joint of the gas purge line and the truck inlet, i.e., from point D to point E. Pipeline 4 connects the truck outlet and the joint of the liquid ammonia purge line, i.e., from point F to point G. Pipeline 5 connects the joint of the liquid purge line and the inlet of the storage tank, i.e., from point G to point H. Pipeline 6 is the compressor recycle line, i.e., from point C to point B. Pipeline 7 is the gaseous ammonia purge line, i.e., from point D to

Table 2. States of the Compressor and Pipelines during the Loading Process

task no.	pipeline states line 1	line 2	line 3	line 4	line 5	line 6	line 7	line 8	compressor state
1	+1	+1	+1	0	0	0	0	0	0
2	+1	+1	+1	+1	+1	0	0	0	0
3	+1 (0)	+1 (0)	+1	+1	+1	0 (+1)	0	0	+1
4	+1	+1	+1	+1	+1	0	0	0	+1
5	0	0	+1	+1	+1	0 (+1)	0	0	0
6	0	0	0	+1	+1	0	0 (+1)	0	0
7	0	0	0	0	0	0	0	0 (+1)	0

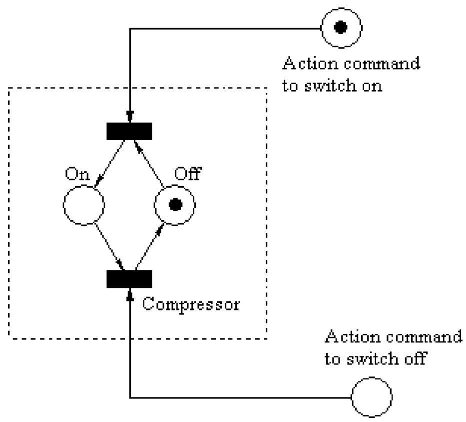

Figure 4. PN model of a compressor.

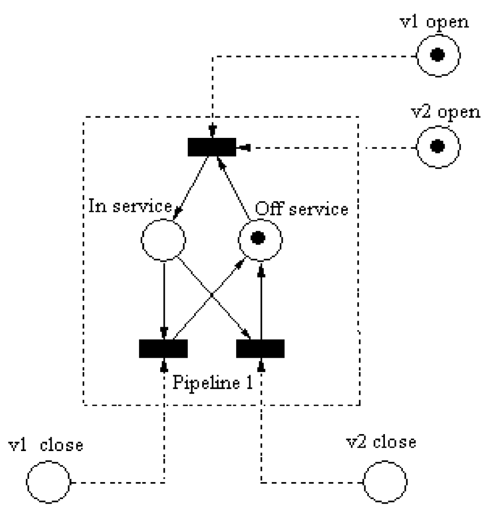

Figure 5. PN model of pipeline 1.

point I. Pipeline 8 is the liquid purge line, i.e., from point G to point J.

In principle, a pipeline is installed to connect two process units to facilitate material flow. All of the valves on this pipeline must be opened to ensure that it is “in service”, and it becomes “off service” if otherwise. Let us consider pipeline 1 as an example; the corresponding PN model is shown in Figure 5. It is clear from this model that, to move from “off service” to “in service”, both valves v1 and v2 must be opened. On the other hand, it is only necessary to close one of them to take the pipeline “off service”.

The operation status of the system is clearly reflected in the states of the compressor and also these pipelines. For example, after completion of task 1, pipelines 1 and 2 are “in service” while other pipelines are “off service”. The states of the compressor and all pipelines at the end of each task are listed in Table 2. In this table, the state of a compressor or pipeline is marked by “+1” if it is “on” or “in service” and “0” if otherwise. Notice that, in several entries (tasks 3 and 5−7), an extra “+1” or “0” is placed in parentheses. These notations are used to denote the temporary changes in pipeline states during the particular task. Say, for example, pipelines 1 and 2 become “off service” temporarily in task 3 and then become “in service” at the end of task 3. Notice also that the initial states of all pipelines and the compressor should be “0” and all of them return to the initial states at end of task 7.

Finally, notice that the operation modes of all other connected level 3 components, i.e., truck, storage tank, and dilution drum, can be determined according to the states of the pipelines. Because the process topology at different stages can be identified implicitly, the corresponding PN models are omitted for the sake of brevity.

Level 4. The fourth-level models are used to represent the variations of process conditions at different locations. In particular, a set of PNs can be constructed to compute the pressures at different locations (from A to H), the liquid levels in the truck and storage tank, and also the flow rates in pipelines 4 and 5. Notice that the changes in the states of process materials are governed by the operating modes and component states covered in the second and third levels. As mentioned previously, the pressure at point A is maintained at 3 kg/cm^2 gauge with the help of a refrigeration system. Thus, the normal pressure at point A may be assumed to be constant in the present work, i.e.

$$P_A = C_A \tag{1}$$

where the value of constant C_A is 3 kg/cm^2 gauge. As long as pipeline 1 is “in service”, the pressure at point B may be estimated according to the following relation:

$$P_B \cong P_A \tag{2}$$

Here, the pressure at point B is considered to be approximately the same as P_A. In other words, the pressure drop due to friction is neglected in the present model even when there is a flow in this pipeline. Similarly, the pressure at point C is assumed to have the pressure at points D and E when the pipelines 2 and 3 are “in service”, i.e.

$$P_C \cong P_D \cong P_E \tag{3}$$

When the compressor is switched on, the pressure ratio of inlet to outlet follows a characteristic curve if the rotation speed is constant. It is assumed in this study that the compressor is operated in a region where the characteristic curve is flat. In other words,

$$P_C \cong C_B P_B \tag{4}$$

The value of constant C_B is chosen to be 1.2 in the

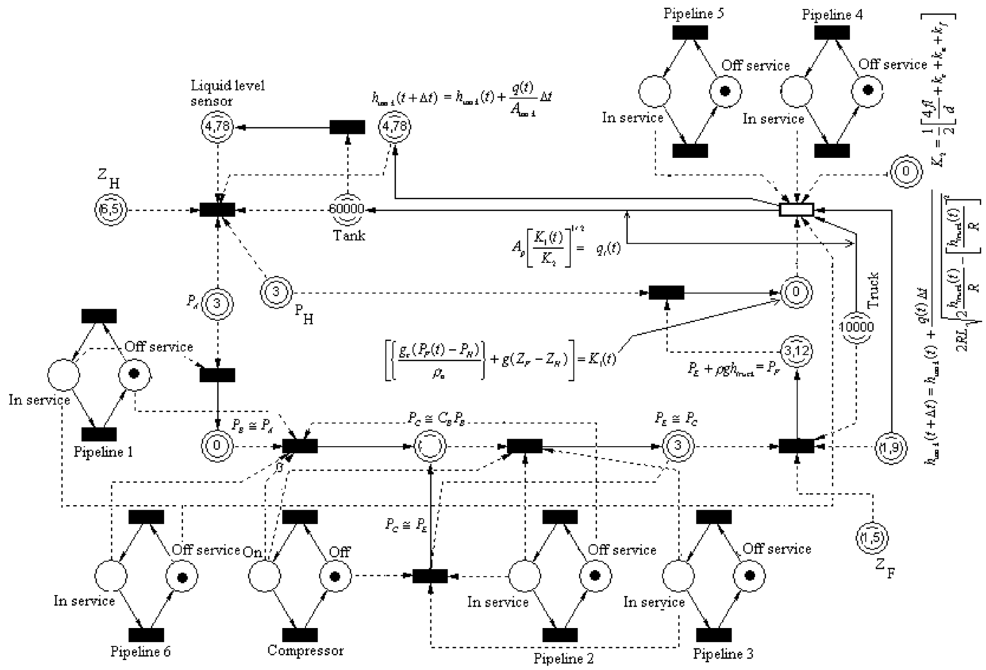

Figure 6. PN models for estimating process conditions at different locations.

present work. The pressure at point E represents the pressure at the exit of the gas transport line, i.e., the vapor pressure in the truck. A change in pressure at point E affects the pressure at point F, i.e., the inlet pressure of pipeline 4. The pressure at point F can be estimated by the following equation:

$$P_{\mathrm{F}} = P_{\mathrm{E}} + \rho g h_{\mathrm{truck}} \tag{5}$$

The second term on the right-hand side of the above equation represents the pressure due to the static liquid head in the truck. Finally, the pressure at point H is assumed to be the same as P_{A}, i.e.

$$P_{\mathrm{H}} = P_{\mathrm{A}} \tag{6}$$

The volumetric flow rates in pipelines 4 and 5 can be related to the rates of change in liquid volumes in the truck and tank according to the following equations:

$$A_{\mathrm{truck}}(t)\,\frac{\mathrm{d}h_{\mathrm{truck}}}{\mathrm{d}t} = -q(t) \tag{7}$$

and

$$A_{\mathrm{tank}}\,\frac{\mathrm{d}h_{\mathrm{tank}}}{\mathrm{d}t} = q(t) \tag{8}$$

where A_{truck}, A_{tank} and h_{truck}, h_{tank} are the cross-sectional areas and liquid heights in the truck and tank, respectively. The initial conditions for the liquid heights can be written as

$$h_{\mathrm{truck}}(0) = C_{\mathrm{truck}} \tag{9}$$

$$h_{\mathrm{tank}}(0) = C_{\mathrm{tank}} \tag{10}$$

In this work, the storage tank is assumed to be cylindrical with a constant cross-sectional area of 12.56 m^2. On the other hand, the vessel on the truck is assumed to be a horizontal cylinder with a radius of 1 m. The cross-sectional area of the truck can be determined using the following equation:

$$A_{\mathrm{truck}}(t) = 2RL\sqrt{2\frac{h_{\mathrm{truck}}(t)}{R} - \left[\frac{h_{\mathrm{truck}}(t)}{R}\right]^2} \tag{11}$$

where R and L represent respectively the radius and horizontal length of the vessel on the truck and $L = 4$ m. It is assumed that the standard 4 in. pipes are used throughout the loading facility. The volumetric flow rate of liquid ammonia in pipelines 4 or 5 can be estimated with Bernoulli's equation, i.e.

$$q(t) = A_{\mathrm{p}}\left[\frac{K_1(t)}{K_2}\right]^{1/2} \tag{12}$$

$$K_1(t) = \frac{g_{\mathrm{c}}[P_{\mathrm{F}}(t) - P_{\mathrm{H}}]}{\rho_{\mathrm{a}}} + g(Z_{\mathrm{F}} - Z_{\mathrm{H}}) \tag{13}$$

and

$$K_2 = \frac{1}{2}\left[\frac{4fl}{d} + k_{\mathrm{c}} + k_{\mathrm{e}} + k_{\mathrm{f}}\right] \tag{14}$$

The PN models for estimating pressures at various points, the heights of liquid levels in the truck and tank, and the volumetric flow rates in the liquid transport pipeline are shown in Figure 6. In this PN, the shaded transitions are nontimed and the hollow ones denote transitions with time delays. The delay times are all set to be 1 s in the present study. On the other hand, the places with double circles contain continuous token numbers while the single circles denote regular discrete places.[14] Notice that liquid levels in the truck and tank vary during loading operation (task 4), and they can be estimated using the following equations:

$$h_{\mathrm{truck}}(t+\Delta t) = h_{\mathrm{truck}}(t) - \frac{q(t)}{A_{\mathrm{truck}}(t)}\Delta t \tag{15}$$

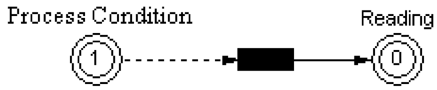

Figure 7. PN model of a sensor.

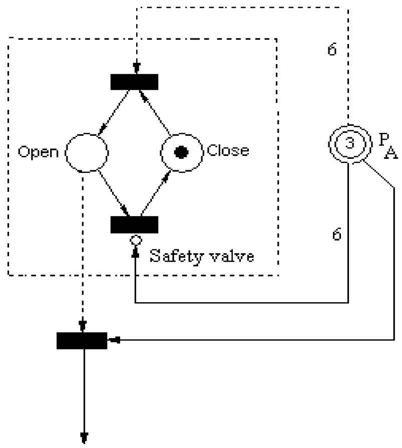

Figure 8. PN model of a safety valve.

and

$$h_{\mathrm{tank}}(t+\Delta t) = h_{\mathrm{tank}}(t) + \frac{q(t)}{A_{\mathrm{tank}}}\Delta t \qquad (16)$$

Level 5. The readings of measuring instruments are directly affected by the process conditions. Their component models can be constructed according to Figure 7. The other important component in this level of hierarchy is the safety valve. The safety valve can also be modeled with two states: open and close (Figure 8). The state of the safety valve is “close” as long as the system pressure is lower than the design value and becomes “open” if otherwise. It can be noted that the limiting pressure is set to be 6 kg/cm^2 gauge in this case.

The System Model

The PN model developed for the individual components can be connected as per the simplified P&ID given in Figure 1 and also the corresponding recipe. A detailed construction procedure is presented in the sequel: The operation procedure should be first described with the PN model for operator/controller. In essence, this practice implies that the information in the recipe is stored in the memory or “hard disk” of the operator/controller. More specifically, the submodel of each operation step is built by connecting the places representing the action commands and the initiation/termination signal according to the standard configuration given in Figure 2a, and the overall first-level component model can then be constructed by assembling these submodels in the correct order given in the recipe. Because the states of the second-level components, i.e., compressor and valves, can be regulated only by an operator/controller, their models should be connected to the first-level component model according to Figures 3 and 4. Next, notice that the states of third-level components are affected only by those of second-level components. In particular, the state of a pipeline is governed by the states of valves on the same pipeline. Consequently, its component model should be attached to the corresponding valve models in level 2 (see Figure 5). As mentioned before, the operation modes of all other third-level components, i.e., truck, storage tank, and dilution drum, can be identified implicitly according to the states of the compressor and pipelines. The corresponding PN models are thus omitted for the sake of brevity. Finally, the fourth- and fifth-level component models can be connected according to P&ID. In simulation, the component models of the process conditions are adopted on the basis of the states of the corresponding third-level components (see Figure 6), and the sensor output in Figure 7 is used as the basis for issuing initiation/termination signal to the operator/controller.

The complete system model is shown in Figure 9. For better visualization of the PN model, token movement during task 2 is shown in Figure 10 separately as an example. By the time task 1 is completed, pipelines 1−3 are “in service”. The operator then opens emergency isolation valve ev2 and valves v7−v10 in sequence. At the end of task 2, pipelines 4 and 5 also become “in service”.

To carry out the simulation studies, a number of initial conditions should be chosen in this study. Let us assume that initially the tank contains 60 000 L of liquid ammonia and the truck contains 10 000 L, in which only 5000 L can be transferred to the tank. In other words, the liquid height in the tank is 4.78 m before the loading operation, and the maximum allowable height is 5.18 m. The initial height of the liquid level in the truck is 1.9 m, and the level is lowered to 1.12 m at the end of loading operation. The initial pressures of the tank and truck are chosen as 3 kg/cm^2 gauge,[13] i.e., $P_A = P_E = P_H = 3$ kg/cm^2 gauge. The pressure at point F can be estimated with eq 5, and the pressures at the other locations [i.e., P_B, P_C, P_D, and P_G] are assumed to be slightly above the atmospheric pressure.

The simulation can be initiated by placing a token in the starting place. During simulation, the token numbers at various places are recorded. The simulation results of the complete operating sequence are given in Table 3. The columns are associated with operation steps, while the rows correspond to the places in PN. The entries in this table are the token numbers obtained after executing each step.

Let us consider task 1 as an example. The operator opens valves v1−v3, v5, and v6 in step 1.1 and emergency isolation valve ev1 in step 1.2. Pipelines 1 and 2 become “in service” when the operator completes step 1.1 (column 2 in Table 3), and pipeline 3 becomes “in service” after step 1.2 (column 3 in Table 3). It may be noted that, after the operator opens the emergency isolation valve, the pressure at point C is increased to a value equal to the pressure at point E (column 3 in Table 3).

As another example, let us consider task 3. By the time operator comes to task 3, pipelines 1−5 become “in service” and the pressures at points A to E are the same (3 kg/cm^2 gauge). The inlet and outlet valves of the compressor (i.e., v2 and v3) should then be closed, and the recycle valve v4 opened before the compressor is switched on (steps 3.1 and 3.2). In other words, the states of pipelines 1 and 2 should be changed to “off service” and that of pipeline 6 to “in service” (columns 6 and 7). The compressor outlet pressure (P_C) is increased to 3.6 kg/cm^2 gauge once the compressor is switched on. Upon reading this value on the pressure gauge, the operator opens the inlet and outlet valves

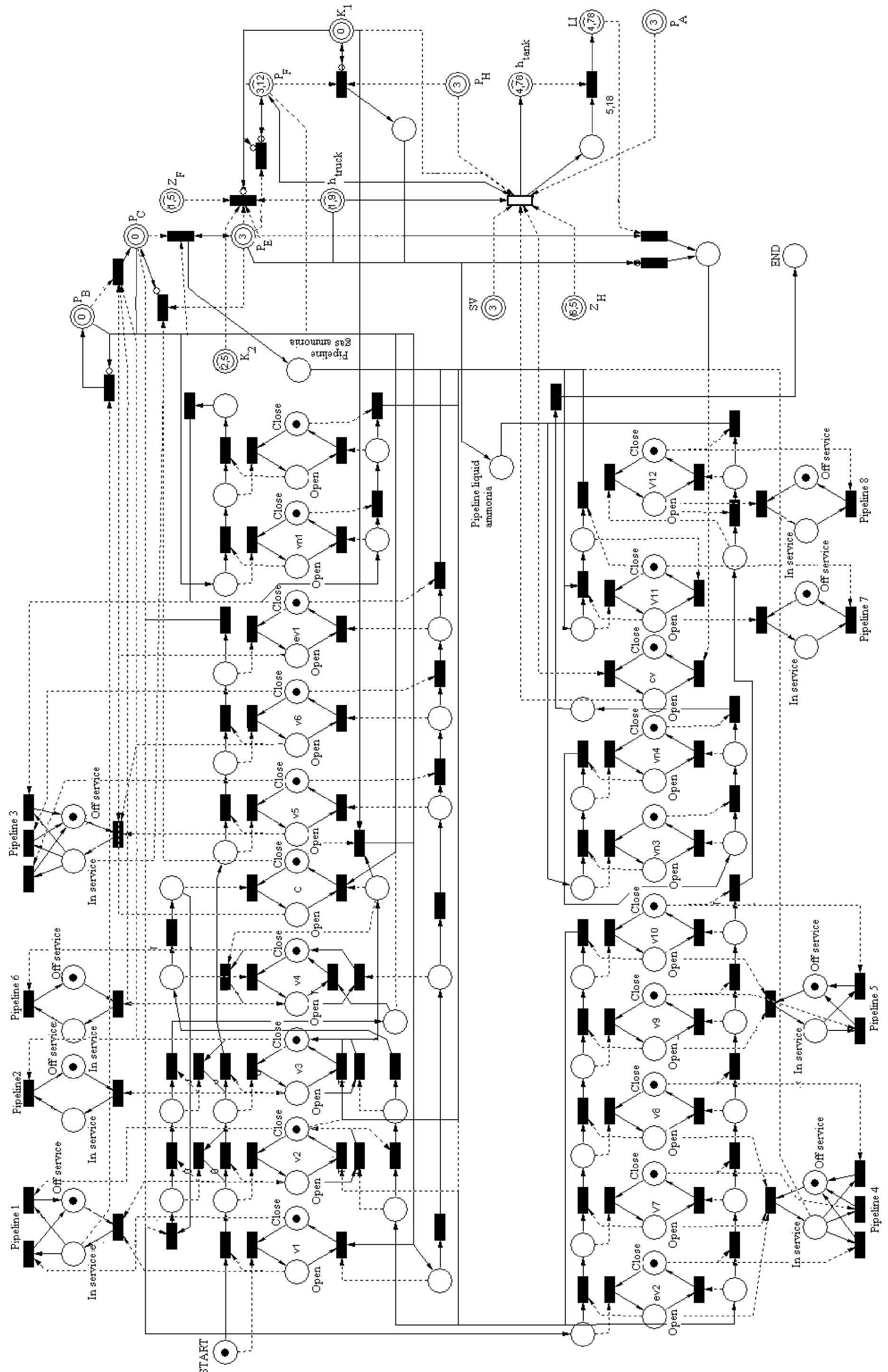

Figure 9. System model of the liquid ammonia loading process.

and closes the recycle valve of the compressor. These actions bring once again pipelines 1 and 2 to “in service” and pipeline 6 to “off service” (column 9).

The liquid ammonia is transferred from truck to tank during task 4. In this task, the operator monitors the sensor readings of pressures at various locations and that of the liquid level in the tank. The liquid heights in the tank and truck are recorded during simulation (Figure 11a,b). It can be seen that h_{tank} increases from the initial value of 4.78 m to the desired value of 5.18 m. On the other hand, h_{truck} is reduced to 1.12 m from the initial value of 1.9 m.

Failure Mechanisms

In the earlier sections, a set of PN models have been developed for the individual components and then assembled to form a system model. The correctness of the system model has also been verified with simulation under normal operating conditions. However, in an industrial environment, equipment may fail for various reasons. Thus, proper failure mechanisms should also be built into the PN model in order to access their impacts. A list of component failure models is presented in the sequel. It should be noted that this list is by no

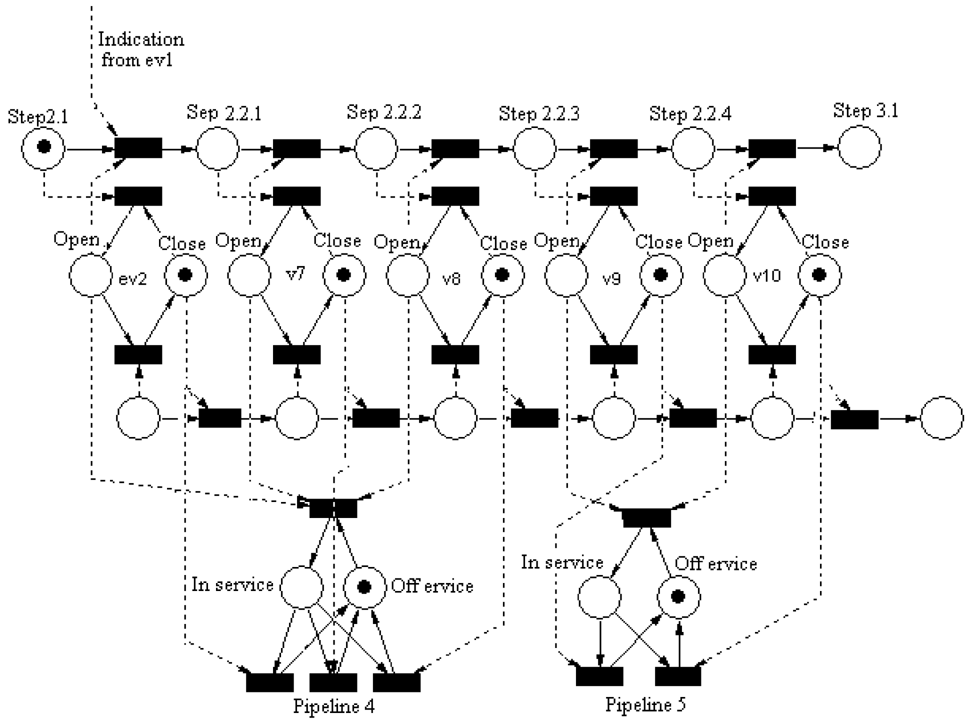

Figure 10. PN model of the operation steps in task 2.

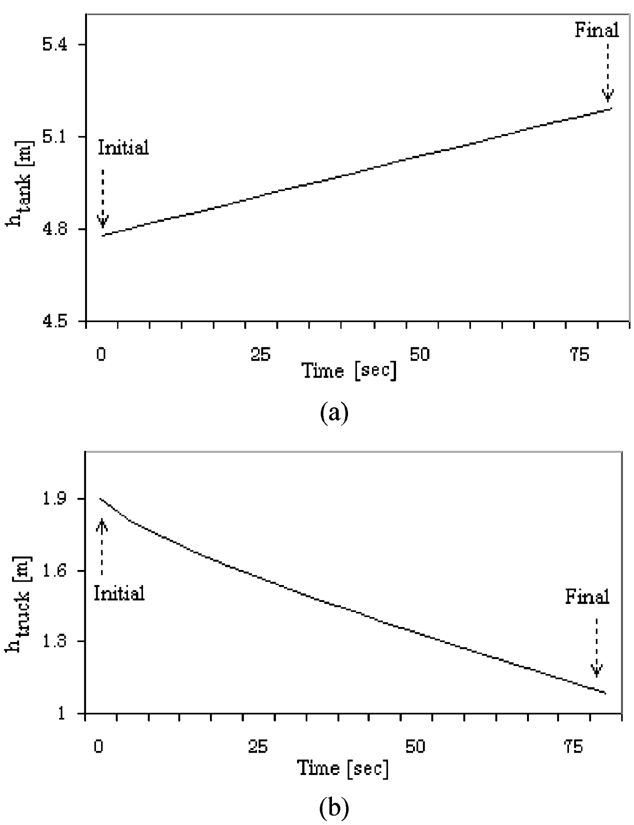

Figure 11. Simulation results under normal operating conditions: (a) liquid level in the tank; (b) liquid level in the truck.

means comprehensive. These models are used in this paper as examples for illustrating the PN construction procedure.

Operator. As mentioned before, the operator sequentially executes action commands given in the operating procedure according to external signals. There may be several human errors in this situation:

(a) The operator may bypass one of the actions.

(b) The operator may carry out one or more extra action.

(c) The operator may implement a different action.

(d) The operator may fail to confirm the signal.

The PN models for failure modes a and d are shown in parts a and b of Figure 12, respectively. Notice that, in these PNs, an arrow with a small circle attached to its end denotes an inhibitor arc.[14] The other failure models are omitted for the sake of brevity.

Valve. As already stated, a valve has two states: open and close. Three failure mechanisms are considered in this work: "fails open", "fails close", and "stuck". The PN models for these valve failures are shown in Figure 13.

Compressor. The compressor has two states: on and off. Only one compressor failure is considered here, i.e., loss of power. The corresponding PN is presented in Figure 14.

Pipeline. In addition to the malfunctions caused by valve failures or operator errors, the pipeline itself may fail because of blockage in the fluid flow pathway. The PN model for pipeline blockage is shown in Figure 15.

Tank/Truck. The tank and truck are maintained at 3 kg/cm^2 gauge by the refrigeration system. The possible failures considered here are loss of refrigeration and/or thermal insulation. The resulting increase in liquid temperature in turn increases vapor pressure in the tank/truck gradually. The PN model for the refrigeration insulation failure is shown in Figure 16.

Dilution Drum. At the end of each loading process, the liquid/gaseous ammonia left in the respective transport lines must be purged into the dilution drum using nitrogen gas. In this study, loss of the water supply is the only failure associated with the dilution drum. This failure mode is represented in PN simply with a single place. Its effects are determined according to the states of pipelines 7 and 8.

Table 3. Simulation Results of the Complete Operation Sequence in the Liquid Ammonia Loading Process

	initial	task 1		task 2		task 3				task4	task 5				task 6				task 7			
	state	1.1	1.2	2.1	2.2	3.1	3.2	3.3	3.4	4	5.1	5.2	5.3	5.4	6.1	6.2	6.3	6.4	7.1	7.2	7.3	7.4
V1	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0	0	0	0	0	0	0	0
V2	0	+1	+1	+1	+1	0	0	0	+1	+1	0	0	0	0	0	0	0	0	0	0	0	0
V3	0	+1	+1	+1	+1	0	0	0	+1	+1	0	0	0	0	0	0	0	0	0	0	0	0
V4	0	0	0	0	0	0	+1	+1	0	0	0	+1	+1	0	0	0	0	0	0	0	0	0
V5	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0	0	0	0	0
V6	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0	0	0	0	0
ev1	0	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0	0	0	0	0	0	0	0
ev2	0	0	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0	0	0	0
V7	0	0	0	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0
V8	0	0	0	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0
V9	0	0	0	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0
V10	0	0	0	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0	0	0	0
C	0	0	0	0	0	0	0	+1	+1	+1	+1	+1	0	0	0	0	0	0	0	0	0	0
V11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	+1	0	0	0	0	0
V12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	+1	0
V13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	+1	+1	0	0	0	0	0
V14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	+1	+1	0
PL1	0	+1	+1	+1	+1	0	0	0	+1	+1	0	0	0	0	0	0	0	0	0	0	0	0
PL2	0	+1	+1	+1	+1	0	0	0	+1	+1	0	0	0	0	0	0	0	0	0	0	0	0
PL3	0	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0	0	0	0	0	0	0	0
PL4	0	0	0	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0	0	0	0
PL5	0	0	0	0	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	0	0	0	0
PL6	0	0	0	0	0	0	+1	+1	0	0	0	+1	+1	0	0	0	0	0	0	0	0	0
PL7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	+1	0	0	0	0	0
PL8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	+1	0
P_A	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
P_B	0.5	3	3	3	3	3	3	3	3	3	3	3	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
P_C	0.5	0.5	3	3	3	3	3	3	3.6	3.6	3.6	3.6	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
P_E	3	3	3	3	3	3	3	3	3.6	3.6	3.6	3.6	3	3	3	3	3	3	3	3	3	3
P_F	3.12	3.12	3.12	3.12	3.12	3.12	3.12	3.12	3.72	3.67	3.67	3.67	3.07	3.07	3.07	3.07	3.07	3.07	3.07	3.07	3.07	3.07
P_H	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
h_{tank}	4.78	4.78	4.78	4.78	4.78	4.78	4.78	4.78	4.78	5.18	5.18	5.18	5.18	5.18	5.18	5.18	5.18	5.18	5.18	5.18	5.18	5.18
h_{truck}	1.9	1.9	1.9	1.9	1.9	1.9	1.9	1.9	1.9	1.12	1.12	1.12	1.12	1.12	1.12	1.12	1.12	1.12	1.12	1.12	1.12	1.12

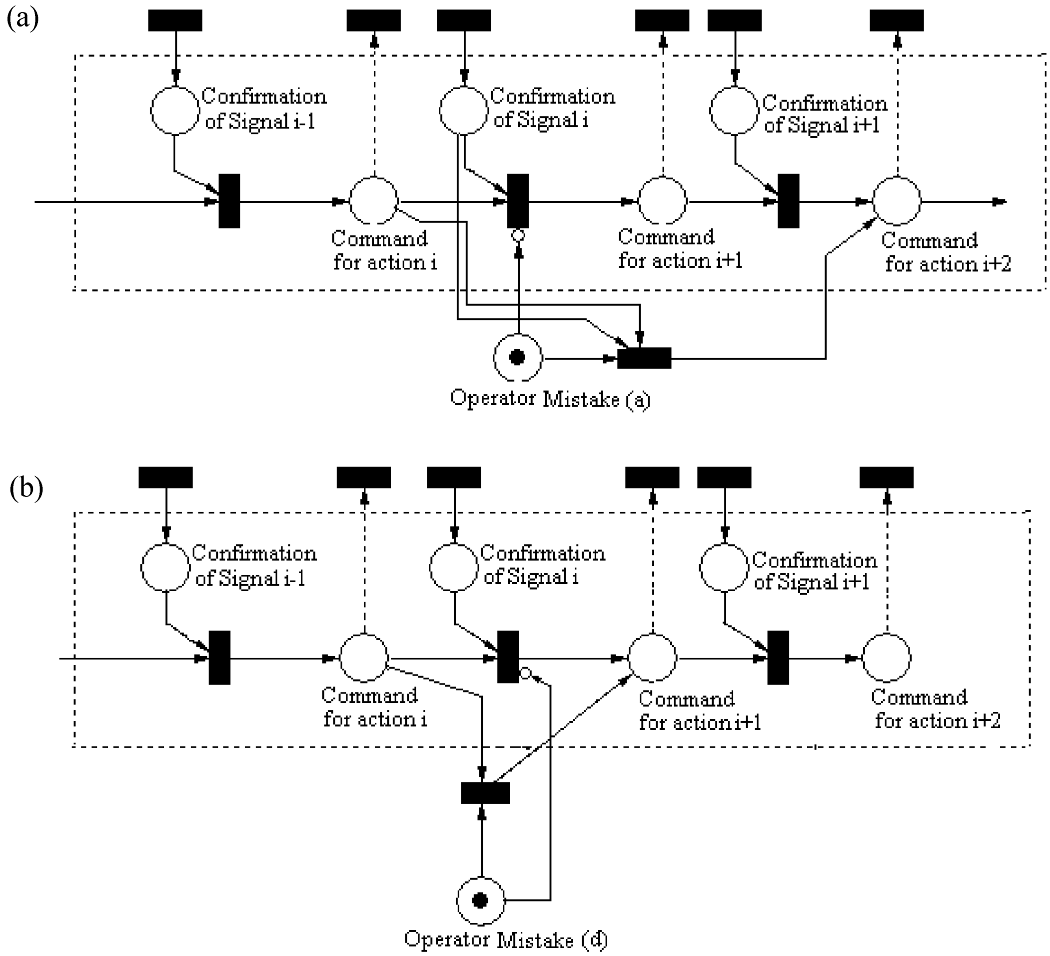

Figure 12. PN models for operator errors: (a) The operator bypasses an operation step. (b) The operator fails to confirm the signal.

Sensor. In the present process, two types of measuring instruments are used: level indicator and pressure gauge. Three failure mechanisms are considered in this study for all measuring devices in general: (a) stuck, (b) bias low, and (c) bias high. The corresponding PN failure models are shown in Figure 17.

Safety Valve. There are two failure mechanisms that can be considered for a safety valve: "fails open" and "stuck". The corresponding PN models are given in Figure 18.

Hazardous System Conditions

The system PN is suitable for hazard identification if it is properly combined with the above component failure models. In particular, the fault propagation behavior can be simulated to determine the consequences of one or more failures. To identify critical scenarios which cause hazardous consequences, a list of hazardous system conditions must be specified in advance. Generally speaking, the hazardous system conditions can be characterized on the basis of process configuration or process condition. The following is a detailed description of these conditions:

Hazardous Process Configuration. The process configuration of the ammonia loading system is reflected in the states of pipelines and the compressor. The normal system configuration associated with each operation step can be found in Table 2 and/or 3. The most serious concerns in the loading operation are (a) the release of ammonia into the environment and (b) equipment damage. Examples of the abnormal process configurations leading to undesirable consequences are listed in Table 4. Notice that a hyphen is used to indicate that the corresponding state is irrelevant in characterizing the given hazardous condition and each consequence is explained in detail in the table legend.

Hazardous Process Condition. The process conditions can be computed with fourth-level component models. Toward unambiguous identification of hazards, operation limitations are imposed upon critical process conditions (Table 5). Violation of these limits may also lead to undesirable consequences.

Identification of Critical Scenarios

Having presented the approach to incorporate the failure mechanisms and to specify the hazardous operation conditions, let us now try to identify critical fault propagation scenarios. Notice that one of the main objectives of a hazard analysis is to determine if any of the hazardous system conditions could be caused by a given set of component failures. This question can be answered with simulation studies. It should also be noted that the fourth-level component models used in this study are only approximations of the true behaviors of the process conditions. The range of applicability of each model is limited. However, it can be argued that these models are still useful in identifying a sufficiently comprehensive list of valid fault propagation scenarios.

In principle, the fault propagation scenarios of every failure listed in this paper can be simulated with the

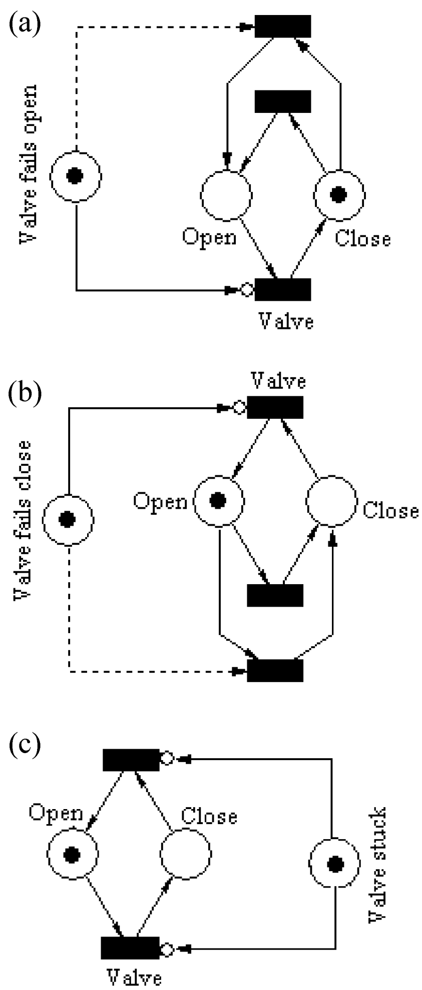

Figure 13. PN models for valve failures: (a) The valve fails open. (b) The valve fails close. (c) The valve is stuck.

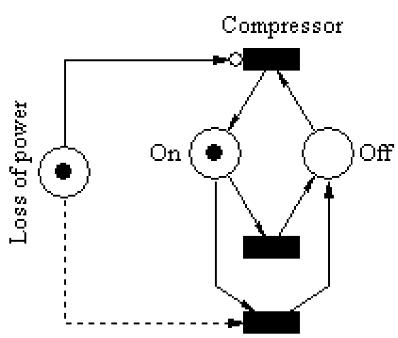

Figure 14. PN model for compressor failure (loss of power).

PN model. Notice that the effects of a failure are dependent upon its occurrence time during operation. Thus, a series of separate simulation runs should be carried out to determine the scenarios corresponding to a single failure and, in each of these runs, the failure is introduced when a distinct operation step is implemented. A very large number of scenarios were thus generated. However, not all of them are "interesting". Some of them lead to insignificant consequences, while some of the other fault propagation mechanisms appear to be quite trivial. For the sake of brevity, only six cases are selected for presentation from the exhaustive simulation results:

Case 1. First, let us consider the failure "valve v11 fails open" before executing task 4. As a result of this

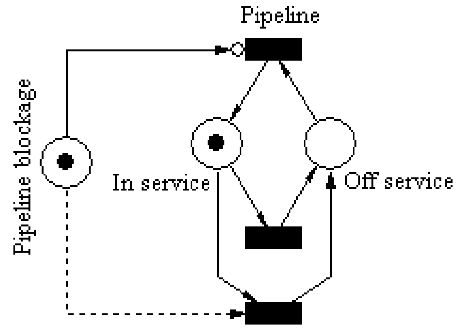

Figure 15. PN model for pipeline blockage.

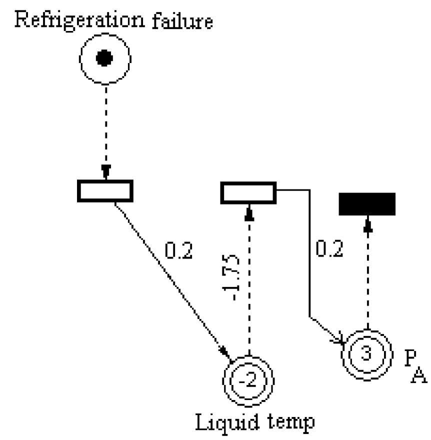

Figure 16. PN model for refrigeration insulation failure.

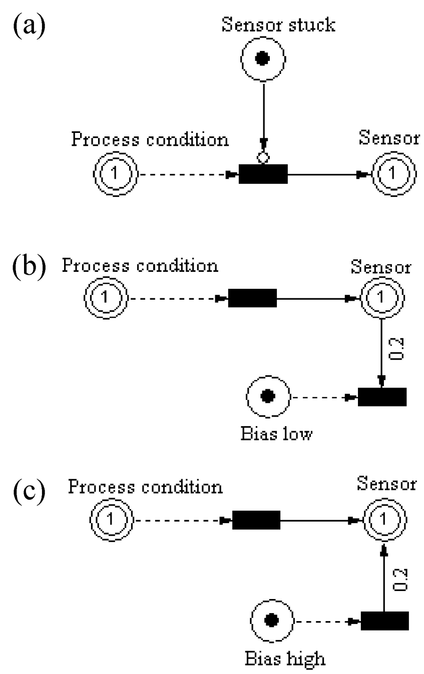

Figure 17. PN models for sensor failures: (a) The sensor is stuck. (b) The sensor is biased low. (c) The sensor is biased high.

failure, pipeline 7 becomes "in service" and the process configuration satisfies the condition given in row 6 of Table 4 after the operator completes task 3. Consequently, a large amount of gaseous ammonia may be discharged into the dilution drum during task 4.

Case 2. Let us next consider an operator's error; i.e., the operator mistakenly opens v12 during task 2. This error makes the pipeline 8 "in service" and allows liquid ammonia flow from the truck to the dilution drum via

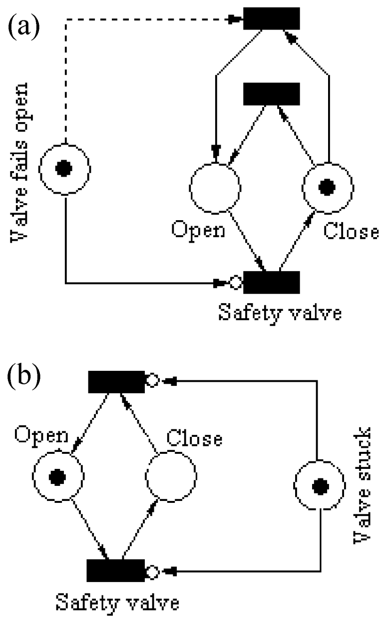

Figure 18. PN model for safety valve failures: (a) The safety valve fails open. (b) The safety valve is stuck.

Table 4. Abnormal Process Configurations and Their Consequences: (C_1) Compressor Mechanical Failure; (C_2) Pressure Increases at Points C−F; (C_3) Pressure Increases at Points C−G; (C_4) Liquid Ammonia Flows from Tank to Dilution Drum; (C_5) Liquid Ammonia Flows from Truck to Dilution Drum; (C_6) Gaseous Ammonia Flows from Tank to Dilution Drum; (C_7) Gaseous Ammonia Flows from Tank to Dilution Drum

states of components									
pipeline									
1	2	3	4	5	6	7	8	comp	consequences
	0				0			+1	C_1
+1	+1	+1	0		0	0	0	+1	C_2
+1	+1	+1	+1	0	0	0	0	+1	C_3
				+1			+1		C_4
			+1				+1		C_5
+1	+1					+1		+1	C_6
		+1				+1			C_7

Table 5. Operation Limits

process conditions	upper/lower limits	process conditions	upper/lower limits
point A	4.5 kg/cm^2 (U)	point F	5 kg/cm^2 (U)
point B	4.5 kg/cm^2 (U)	point H	4.5 kg/cm^2 (U)
point C	6 kg/cm^2 (U)	h_{tank}	5.18 m (U)
point E	4.5 kg/cm^2 (U)	h_{truck}	0 m (L)

pipelines 4 and 8. In other words, the condition given in row 5 of Table 4 is satisfied after opening valves v7, v8, and v12.

Case 3. The failure of the liquid level sensor is considered here. The corresponding PN is shown in Figure 19a. The moment a token is introduced in the place representing sensor failure, the transition from h_{tank} to the place denoting sensor reading becomes disabled and the reading remains unchanged. On the other hand, the liquid level in the tank keeps increasing and finally exceeds the upper limit of 5.18 m. The simulation results are plotted in Figure 19b. The solid line represents the indicator's reading, while the actual liquid height is shown as the dotted line. It is clear that the failure occurs at the time when there is an abrupt change in the slope of the solid line, and the reading of the level indicator remains the same value afterward.

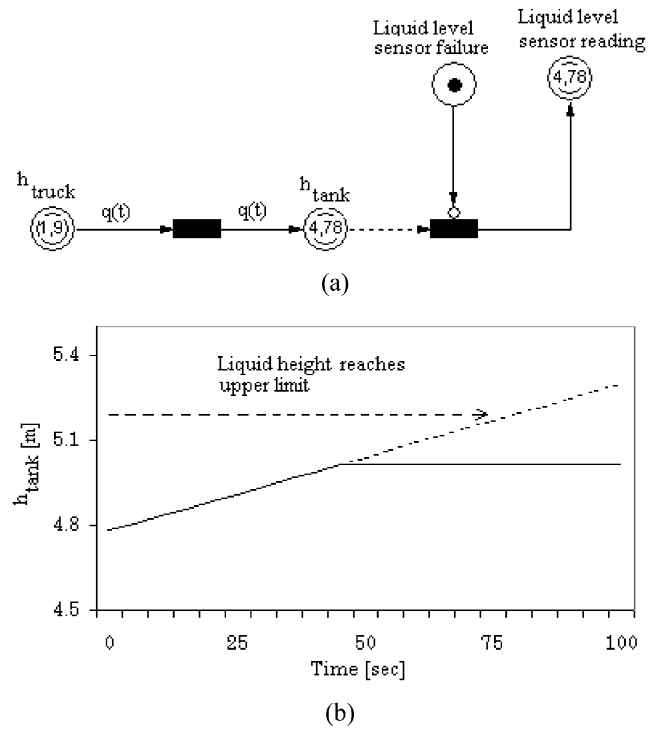

Figure 19. (a) PN model of liquid level sensor failure in case 3. (b) Simulation results of case 3.

On the other hand, the liquid height in the tank increases continuously as the loading process continues.

Case 4. Let us consider another operator's error in this case. As explained earlier, the compressor should be switched on after the inlet and outlet valves v2 and v3 are closed and recycle valve v4 is opened during task 3. The valves v2 and v3 should then be opened and valve v4 closed after the compressor outlet pressure reaches 3.6 kg/cm^2 gauge (step 3.4). Let us assume that the operator bypasses the action opening of valve v3 (Figure 20a), which makes the resulting process configuration (Figure 20b) satisfy the condition given in row 1 of Table 4. As a result, compressor surge occurs because of the abnormal increase in the pressure at the outlet.

Case 5. The failure of pipeline 4 (i.e., blockage) during task 4 is considered here. During task 4 the transfer of liquid occurs only when the pipelines 1−5 are "in service" and the compressor is "on". The PN model for pipeline blockage is shown in Figure 21a. A token in the place representing blockage changes the state of pipeline 4 from "in service" to "off service". The resulting process configuration (Figure 21b) satisfies the condition listed in row 2 of Table 4, which increases the pressure at point C and subsequently the pressure at other locations (i.e., points D−F). The increases in pressures at these locations are recorded during simulation. It was found that the pressure at point E first exceeds the upper limit given in Table 5. The increase in pressure at point E due to the above failure is shown in Figure 21c.

Case 6. The failure of the refrigeration system is considered in this case. A token in the place representing refrigeration system failure enables the transition for increasing the liquid temperature and then the ammonia vapor pressure in the storage tank (see Figure 16). Let us introduce this failure in task 4. The immediate effect should be an increase in the pressure at point A. This pressure increase should propagate to the other

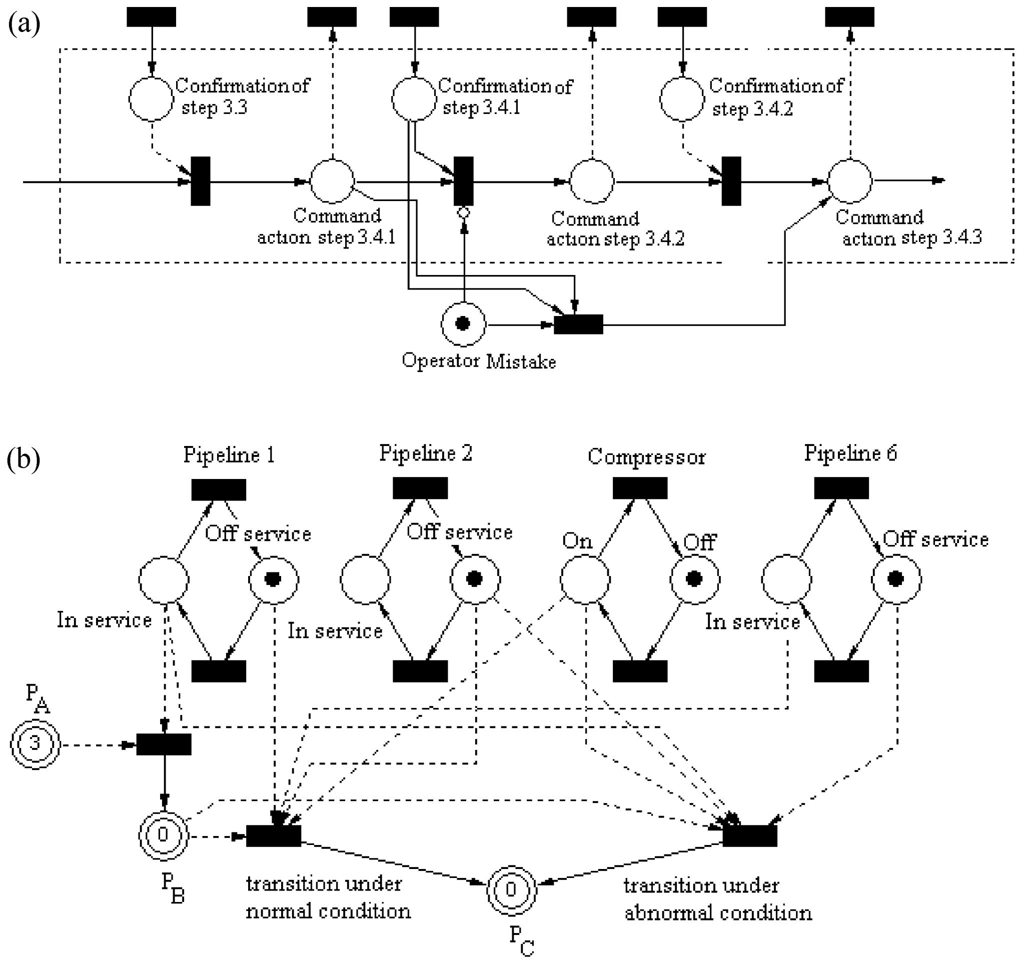

Figure 20. (a) PN model of the operator error in case 4. (b) Abnormal process configuration in case 4.

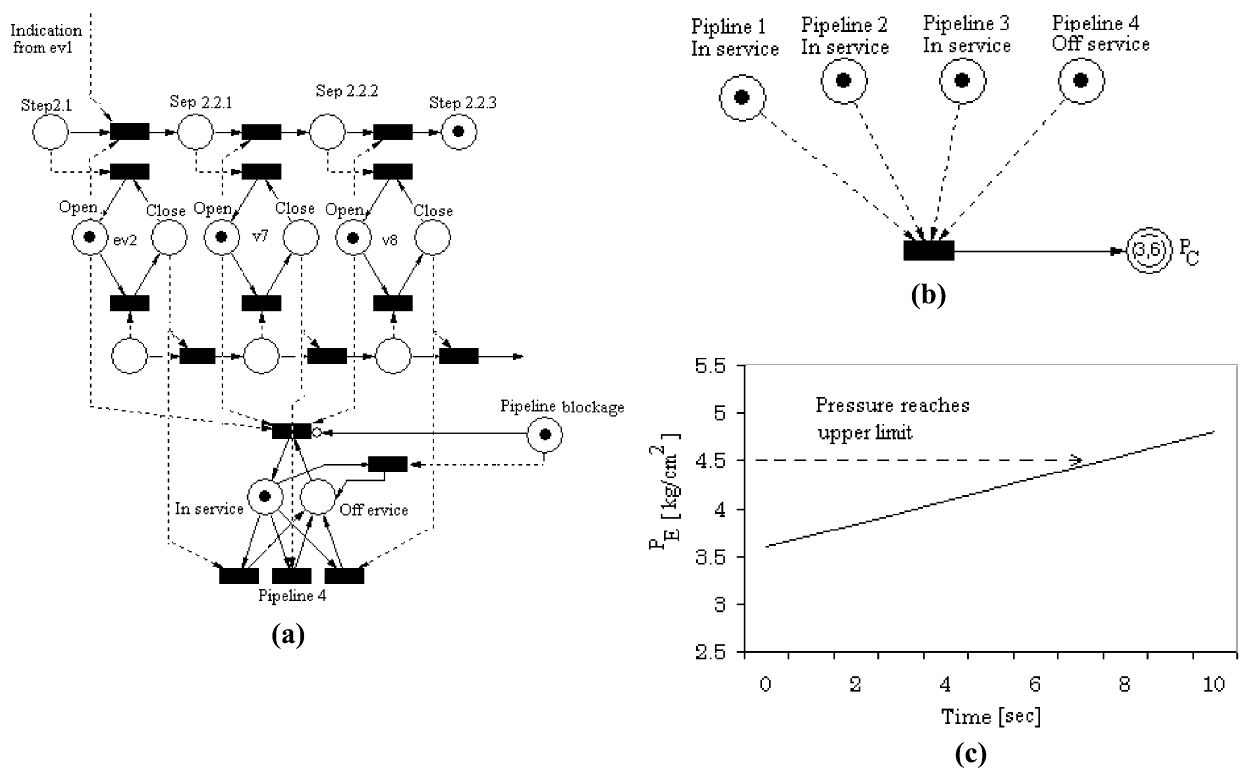

Figure 21. (a) PN model of a blockage in pipeline 4 in case 5. (b) Abnormal process configuration in case 5. (c) Simulation results of case 5.

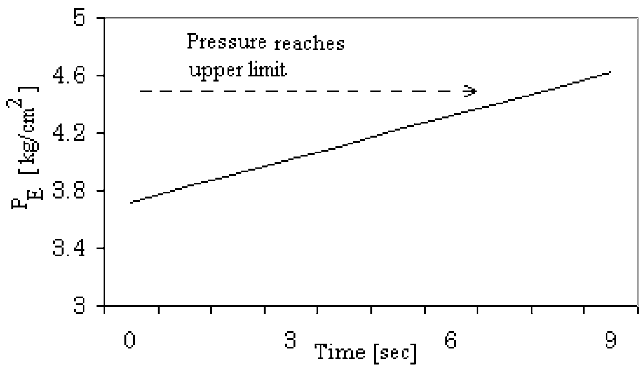

Figure 22. Simulation results of case 6.

locations, i.e., from points B to F, because pipelines 1−5 are “in service”. It is observed from the simulation results that the pressure at point E approaches the upper limit first. The simulated result of a pressure increase at point E is shown in Figure 22.

Conclusions

A hierarchical approach to construct a PN model has been developed for describing the liquid ammonia loading operation. Different failure models have also been developed and included in the system model toward identification of critical fault propagation scenarios. It can be observed from the simulation results that the proposed PN model is quite useful for vigorous hazard analysis of the sequential operations.

Acknowledgment

This work is supported by the National Science Council of ROC under Grant NSC89-2214-E006-027.

Notation

A_{truck} = cross-sectional area of the truck, m^2
A_{tank} = cross-sectional area of the tank, m^2
A_p = cross-sectional area of the transporting pipe, m^2
C_A, C_B = constants in eqs 1 and 4
C_{truck}, C_{tank} = constants in eqs 9 and 10
C_1-C_7 = consequences given in Table 4
d = pipe diameter, m
f = fanning friction factor
g = gravitational constant
h_{tank} = liquid height in the tank, m
h_{truck} = liquid height in the truck, m
L = truck length, m
l = pipe length, m
K_1, K_2 = constants in eq 12
k_c, k_e, k_f = coefficients for contraction, expansion, and other fittings
P_A-P_H = pressure at points A−H, kg/cm^2
ρ_a = density of liquid ammonia, kg /m^3
q = volumetric flow rate, m^3/s
R = radius of the truck, m
T = process time, s
Δt = incremental time, s
Z_F, Z_H = elevations of points F and H, m

Literature Cited

(1) Vaidyanathan, R.; Venkatsubramanian, V. Digraph-Based Models for Automated HAZOP Analysis. *Reliab. Eng. Syst. Saf.* **1995**, *50*, 33.

(2) Vaidyanathan, R.; Venkatsubramanian, V. A Semiquantitative Reasoning Methodology for Filtering and Ranking HAZOP Results in HAZOPExpert. *Reliab. Eng. Syst. Saf.* **1996**, *53*, 185.

(3) Srinivasan, R.; Venkatasubramanian, V. Petri Net-Digraph Models for Automating HAZOP Analysis of Batch Process Plants. *Comput. Chem. Eng. (Suppl. A)* **1996**, *20*, S719.

(4) Kumamoto, H.; Henley, E. Safety and Reliability Synthesis of Systems with Control Loops. *AIChE J.* **1979**, *20*, 376.

(5) Kuo, D. H.; Hsu, D. S.; Chang, C. T.; Chen, D. H. Prototype for Integrated Hazard Analysis. *AIChE J.* **1997**, *43*, 1494.

(6) Lapp, S. A.; Powers, G. J. Computer-Aided Synthesis of Fault-Trees. *IEEE Trans. Reliab.* **1977**, *2*, R-26.

(7) Chang, C. T.; Hsu, D. S.; Hwang, H. Studies on the Digraph-Based Approach for Fault Tree Synthesis, I: The Ratio-Control Systems. *Ind. Eng. Chem. Res.* **1994**, *33*, 1520.

(8) Chang, C. T.; Hsu, D. S.; Hwang, H. Studies on the Digraph-Based Approach for Fault-Tree Synthesis, II: The Trip Systems. *Ind. Eng. Chem. Res.* **1994**, *33*, 1700.

(9) Khan, F. I.; Abbasi, S. A. OptHAZOP—An Effective and Optimum Approach for HAZOP Study. *J. Loss Prev. Pro. Ind.* **1997**, *10*, 191.

(10) Srinivasan, R.; Venkatsubramanian, V. Automating HAZOP Analysis of Batch Chemical Plants: Part 1. The Knowledge Representation Framework. *Comput. Chem. Eng.* **1998**, *22*, 1345.

(11) Srinivasan, R.; Venkatsubramanian, V. Automating HAZOP Analysis of Batch Chemical Plants: Part II. Algorithm and Application. *Comput. Chem. Eng.* **1998**, *22*, 1357.

(12) Wang, Y. F.; Wu, J. Y.; Chang, C. T. Automatic Hazard Analysis of Batch Operations with Petri Nets. *Reliab. Eng. Syst. Saf.* **2002**, *76*, 91.

(13) Society of Industrial Safety and Hygiene. *Standard Operating Procedure for Loading/Unloading of Liquid Ammonia*; Labor Council: Taipei, Taiwan, 1991.

(14) David, R.; Alla, H. Petri Net for Modeling of Dynamic Systems—A Survey. *Automatica* **1994**, *30* (2), 175.

Received for review July 27, 2001
Accepted June 27, 2002

IE010639R