ELSEVIER

Reliability Engineering and System Safety 76 (2002) 91–104

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

Automatic hazard analysis of batch operations with Petri nets

Yi-Feng Wang, Jer-Yu Wu, Chuei-Tin Chang*

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

Received 1 February 2001; accepted 11 December 2001

Abstract

A systematic procedure has been proposed in this study to construct Petri nets for modeling the fault propagation behaviors in batch processes. An efficient algorithm has also been developed to enumerate all possible scenarios, which may lead to an undesirable consequence. This approach has been applied to a number of examples. The results show that it is more accurate and more comprehensive when compared with the conventional methods.

Keywords: Batch operation; Petri net; Digraph; HAZOP; Fault tree analysis; Minimal cut set

1. Introduction

Hazard analysis is an important step in designing or revamping any process plant. There are several techniques available for such a purpose in practice, e.g. fault tree analysis (FTA), failure modes and effects analysis (FMEA) and hazard and operability study (HAZOP), etc. In implementing any of these methods, there is always a need to reason deductively identify all combinations of basic events that could lead to an undesirable event or condition. Generally speaking the analysis performed with fault trees is believed to be most rigorous and comprehensive [1]. However, if the tasks of synthesizing fault trees and identifying the corresponding minimal cut sets (MCSs) are done manually, the demand for manpower and time tends to be overwhelming. Thus, there are real incentives to automate such a cause-finding process.

In the past two decades, the research on automatic fault-tree analysis has advanced significantly. Several efficient tools have been developed to synthesize fault trees, e.g. the digraph [2,3], the decision [4] and the minifault tree [5,6]. In essence, the approaches taken in these studies are the same, i.e. to build a qualitative system model for use in the fault-tree construction algorithm. It can be observed from the literature that the digraph is by far the most popular model [7–10]. Although this approach has been proven to be useful, it is effective mostly in applications concerning the continuous processes. This is due to the fact that the digraph is inherently unsuitable for describing the dynamic causal relationships among time, discrete events, equipment states and system configurations in the batch processes [11].

On the other hand, the Petri net (PN) is well known for its capability in modeling the discrete-event systems [12]. Several research projects that aimed to automate procedure HAZOP on the basis of Petri net-digraph hybrid models have already been reported in recent literature [13,14]. Although sufficient for automating simple HAZOP analysis, this modeling approach is not capable of representing a number of important features in more complex batch operations. Specifically

1. *Concurrent activities*. Concurrent activities can be easily expressed in terms of Petri nets. Most batch chemical processes are designed with a certain degree of parallelism to ensure flexibility and efficiency in operation. This type of operation has not been considered in the earlier studies.
2. *Cyclic operations*. In a sense, all batch operations are repetitive or cyclic. It is thus necessary to investigate the possibilities of a current failure causing undesirable consequences in the later cycles. Therefore, in certain cases, it is not enough to build a recipe-based PN model representing the operation steps only in a single batch.
3. *Continuous transients*. The batch operations are typically characterized by time-variant operating conditions and/or process variables. These quantities were discretized and expressed with digraphs in the previous studies. However, since they can be better represented with the continuous places, there is a strong incentive to model the batch systems in a unified format with PNs only.

* Corresponding author. Fax: +886-6234-4496.
E-mail address: ctchang@mail.ncku.edu.tw (C.-T. Chang).

0951-8320/02/$ - see front matter
PII: S0951-8320(02)00002-9

Nomenclature

I-H (II-H) the fresh air to Bed-I (Bed-II) is heated
I-C (II-C) the fresh air to Bed-I (Bed-II) is not heated
I-P (II-P) the recycled air is directed to Bed-I (Bed-II)
I-E (II-E) the outlet air from Bed-I (Bed-II) is discharged to stream 25
I-R (II-R) the outlet air from Bed-I (Bed-II) is recycled to the proportionating valve
I-T (II-T) the temperature of Bed-I (Bed-II)
I-M (II-M) the water content in Bed-I (Bed-II)

4. *Multi-purpose productions*. It is a common practice to manufacture more than one product with the same facilities in a batch plant. Due to the need to share resources, it may be necessary to run some units under different operation modes at different times. As a result, the process configuration, i.e. the connections among units, may be changed accordingly. Since the conventional recipe-based PN models are built individually for a single product, they cannot be easily integrated to represent the overall orchestrated production activities efficiently.

In addition, several other researchers have also developed PN-based techniques to identify the MCSs of a given fault tree [15,16]. These MCS identification methods are applicable only to systems that can be represented by the ordinary PNs. This is unacceptable for our purpose since a few special extensions of the ordinary PN are also needed to model batch operations properly. Thus, the objectives of this study are twofold: (1) to develop a systematic procedure to construct more appropriate PN models for the batch processes and (2) to establish an enumeration algorithm to determine all possible causes of any given hazardous event or abnormal condition.

The rest of this paper is organized as follows. First, the basic elements and the strategy for building a PN-based model are described in Section 2. In Section 3, a systematic procedure is presented to perform dynamic simulation according to a given initial marking. On the basis of this procedure, an enumeration algorithm is proposed in Section 4 to identify all possible causes of an undesirable event/condition. Finally, the proposed method is applied to a realistic example in Section 5 to demonstrate its effectiveness.

2. The PN-based models for batch processes

The Petri net is a graphical and also mathematical tool for describing relationships between the conditions and events. As a graphical tool, a PN model help visualize and represent the dynamic behavior of a given discrete-event system. Moreover, any PN can be translated into a mathematical model in the form of discrete state equations. The formal definitions of the elements in ordinary PN can be found in Refs. [17,18].

As mentioned previously, the applicability of ordinary PNs is very limited. In order to describe sequential operations properly, it is necessary to introduce additional special extensions in the PN model [18–20]. First of all, due to the dynamical nature of batch processes, the time-delayed as well as the nontimed transitions should be included to represent various events possibly taking place over a wide range of time span. In this work, the delay times are specified next to the corresponding transitions in PN. Without causing confusion, the nontimed transitions are not marked at all. Secondly, in addition to the standard places containing only integer number of tokens, the continuous places must also be adopted. The standard places can be used to represent discrete equipment conditions, e.g. the open/close position of a valve and the on/off state of a pump. On the other hand, since the token number in a continuous place is real, it is well suited for describing the variation of a process variable such as temperature, pressure or liquid level. In the Petri nets used in this study, the former places are represented with circles and the latter double circles. Finally, other than the standard arcs, two types of special place-to-transition arcs are adopted in this work, i.e. the inhibitor arcs and the static test arcs. An inhibitor arc is usually represented by a directed arc with a small circle at its end. It can be used in executing zero test or in modeling the failure mechanisms that inhibit the normal events in operation. The test arc is marked by a directed dash line. In general, it is often used for simplifying the self-looping structure in PN. Notice that the number of tokens in the input place of a test arc is not reduced by firing its output transition. This feature is often needed in building a PN model.

The transition enabling rules of all place-to-transition arcs in our study are listed in Table 1. In this table, M denotes the number of tokens in input places and W denotes the weight of corresponding input arc. Note that in general the standard transitions can be fired immediately after they are enabled. This implies that the input tokens are removed and output tokens are produced at the same time. However, when a time-delayed transition is enabled, although the input tokens can be removed immediately, the output tokens should not be created until the firing duration has elapsed.

A hierarchical approach is taken in this study to construct the PN-based models for batch processes. In general, a model in our application consists of the five different levels shown in Table 2. In any batch process, a first-level

Table 1
The transition enabling rules

Arc type	Enabling condition
Normal arc	$M \geq W$
Inhibitor arc	$M < W$
Test arc	$M \geq W$

Table 2
The hierarchy in PN-based models for batch processes

Level	Component models
1	PLC, timer, operator
2	Valve, pump, compressor
3	Process unit
4	Process material
5	Sensor

component is always used to execute the operating steps specified in a recipe on the basis of a given time schedule or a set of sensor measurements. Its actions alter the states of valves, pumps, compressors and switches in the second-level. The states of these components in turn determine the process configuration and, consequently, the operation mode and equipment condition of each process unit in the third-level. In the fourth-level, the changes in the states of process material within the process unit are governed by the operating mode and the equipment condition. Finally, these process states are monitored via sensors in the last level.

In building such a PN-based system model, the component models should be constructed and connected in sequence from top to bottom level according to the piping and instrumentation diagram (P&ID) and operation recipe of the process. Other than the normal behavior, the effects of failure events can also be described in the component models. Specifically, a failure can be represented with a nontimed primal transition, i.e. a transition without inputs, and its effects can be modeled with a sub-PN attaching to the directly affected places and transitions in the PN built for normal operation. In principle, all component models should be included to ensure the comprehensiveness of analysis. However, if the failure mechanisms associated with a component are not of interest and there is only one possible place associated with the normal condition, the corresponding component model may be ignored for the sake of conciseness.

Finally, it should be noted that only the normal operating steps are included in the proposed PN model. It is assumed in this study that the effects of failures cannot be detected until the undesirable final outcome occurs. This assumption is reasonable if the system under study does not include any fault monitoring device.

2.1. Example 1

Let us consider the simple mixing process given in Fig. 1. Here, tank 3 is being fed from the other two tanks. Initially, the amount of liquid A in tank 1 is 1 l and that of liquid B in tank 2 is 2 l. The mixing operation begins when valve V1 and valve V2 are opened by an operator. It is assumed that the flow rates of these two feed streams are the same: 1/60 l/s. The operator is instructed to close valve V2 whenever tank 1 is empty and vice versa.

This batch operation is modeled by the PN shown in Fig. 2. Notice that for simplicity, this model only contains components in the second and fourth levels of the hierarchy shown in Table 2. The first-level component in this example is the operator. By assuming that he (or she) always functions properly, the corresponding model is not included. The component models of the tanks and sensors in the third and fifth levels are also neglected due to the belief that they rarely fail.

There are two components in the second-level, i.e. valves V1 and V2. Their states can be described with two discrete places denoting ‘open’ and ‘closed’. Two types of valve failures are considered in this example, i.e. sticking and failing closed. The corresponding failure models are included in this PN. If the event ‘valve sticking’ occurs, it always disables a transition representing the action to change valve position. The corresponding token is therefore locked in its input place. On the other hand, if a valve is

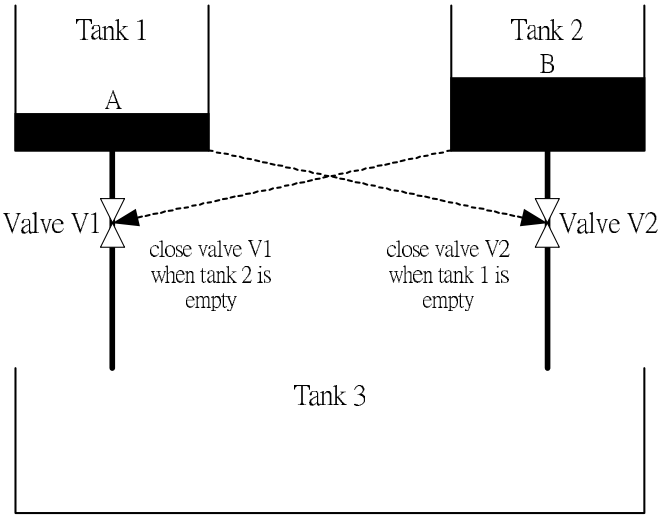

Fig. 1. A mixing operation.

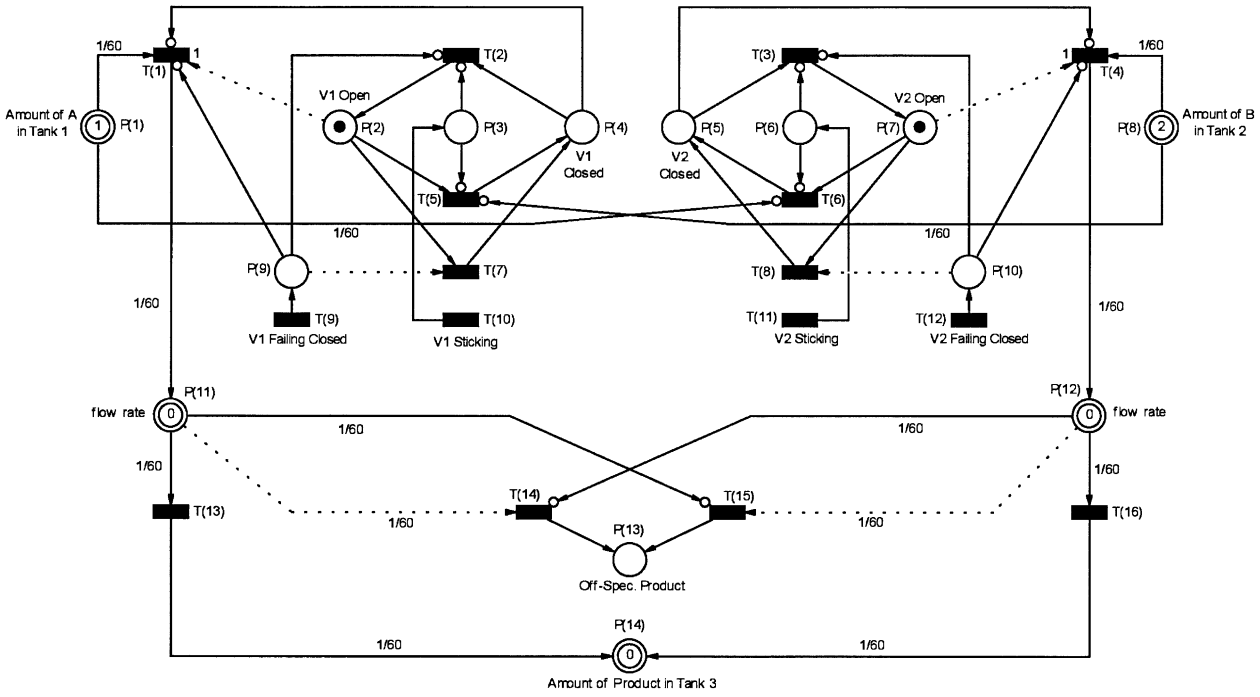

Fig. 2. The PN model of mixing operation.

originally open and the event 'valve failing closed' occurs during operation, such a failure always moves the token from the place representing the open position to the other place denoting the opposite valve state.

To characterize the states of process materials in this system, it is necessary to trace the variations of the liquid levels in all three tanks and also the liquid flow rates in the pipelines connecting the tanks. Five continuous places are thus adopted to represent these process variables. Notice that the dead times of all time-delayed transitions are set to 1 s. Consequently, the weights on their input and output arcs should be 1/60, which is the same as flow rate.

Finally, it is assumed that the desired ratio of A to B in product is 1. Thus, off-spec product may be produced if the flow rates of A and B are not equal. The corresponding failure mechanisms are also incorporated in the PN model presented in Fig. 2.

3. Dynamic simulation

As mentioned earlier, the dynamic behaviors of discrete-event systems can be described by the state equation [17], i.e.

$$\mathbf{M}_k = \mathbf{M}_{k-1} + \mathbf{A}^{\mathrm{T}}\mathbf{U}_k \qquad k = 1, 2, \ldots \tag{1}$$

where $\mathbf{U}_k$ is a column vector whose entries are binary numbers. A 1 at the ith position indicates that transition i should be fired at the kth firing. A 0 means otherwise. $\mathbf{M}_k$ is a column vector whose ith entry is the token number in place i after firing the transitions specified $\mathbf{U}_k$. $\mathbf{A}$ is a transition-to-place incidence matrix whose entries can be real or integer numbers. A positive value at the (i,j)th position in the matrix denotes the weight of the arc from the ith transition to the jth place. A negative value represents the weight of an arc in the opposite direction. Finally, there are three possibilities associated with a zero. The corresponding arc may be a static test arc, an inhibitor arc or it does not exist at all.

In a PN with only standard arcs, the firing vector $\mathbf{U}_k$ can be correctly determined on the basis of the prior marking $\mathbf{M}_{k-1}$ and incidence matrix $\mathbf{A}$. However, if the PN contains inhibitor or test arcs, this approach becomes infeasible since the corresponding entries in $\mathbf{A}$ are zeros. In order to overcome this problem, let us divide the incidence matrix into two parts, i.e.

$$\mathbf{A} = \mathbf{A}(-) + \mathbf{A}(+) \tag{2}$$

where $\mathbf{A}(-)$ and $\mathbf{A}(+)$ are constructed according to the following procedures:

1. Replace every negative entry in $\mathbf{A}$ by 0 to form $\mathbf{A}(+)$. Similarly, replace every positive entry in $\mathbf{A}$ by 0 to form $\mathbf{A}(-)$.
2. If the PN contains N_{T} test arcs with weights W_i^{T} $(i = 1, 2, \ldots, N_{\mathrm{T}})$, then change each corresponding 0 in $\mathbf{A}(+)$ to $+W_i^{\mathrm{T}}$ and each corresponding 0 in $\mathbf{A}(-)$ to $-W_i^{\mathrm{T}}$.
3. If the PN contains N_{I} inhibitor arcs with weights W_j^{I} $(j = 1, 2, \ldots, N_{\mathrm{I}})$, the change each corresponding 0 in $\mathbf{A}(+)$ to $-W_j^{\mathrm{I}}$ and each corresponding 0 in $\mathbf{A}(-)$ to $+W_j^{\mathrm{I}}$.

The firing vector $\mathbf{U}_k$ can thus be determined by comparing the prior marking $\mathbf{M}_{k-1}$ with the rows of $\mathbf{A}(-)$. In particular,

a simple algorithm (algorithm I) has been developed for this purpose:

1. Select the ith row vector $\mathbf{a}_i$ from $\mathbf{A}(-)$.
2. Perform the following calculations:
   (a) Subtract the positive entries in $\mathbf{a}_i$ from the corresponding entries in $\mathbf{M}_{k-1}$.
   (b) Add the negative entries in $\mathbf{a}_i$ to the corresponding entries in $\mathbf{M}_{k-1}$.
3. If all results in (a) are negative and all results in (b) are larger than or equal to zero, then the ith transition should be enabled. Otherwise, it is disabled.
4. Repeat Step 1 to Step 3 until all row vectors in $\mathbf{A}(-)$ are exhausted.

As discussed in Section 2, it is necessary to include time-delayed transitions in the PN-based models for batch processes. Consequently, the earlier algorithm can only identify the enabled transitions in PN. The nontimed transitions can be fired immediately after enabling. However, the firing of each time-delayed transition should be postponed until the specified time period elapses.

The simulation of a batch process can be performed according to the state equation at regular time intervals. The most appropriate time interval can be obtained by taking the common divisor of the dead times of all time-delayed transitions. The initial marking is assumed to be given and the initial firing vector at the starting time is a vector with only zeros. The first task that must be accomplished at any given time is to fire transitions according to a firing vector stored at a previous time. Next, algorithm I should be performed to determine the enabled and disabled transitions. The nontimed enabled transitions should be fired right away. If some of the transitions previously stored for future firing are found to be disabled, they should be removed from the corresponding firing vectors. The earlier tasks, i.e. implementing algorithm I, firing the enabled nontimed transitions and eliminating the disabled time-delayed transitions, should be repeated until only the time-delayed transitions are found to be enabled. These enabled transitions should then be stored for future firing according to their respective delay times.

The same simulation procedure should be carried out successively at every time interval. For our purpose, the computation is terminated when one of the following two conditions is satisfied:

1. One or more token is produced in a terminal place denoting the undesirable condition considered in hazard analysis.
2. All the future firing vectors contain only zeros.

3.1. Example 2

Let us consider the simple PN given in Fig. 3. The matrices $\mathbf{A}^{\mathrm{T}}$,$\mathbf{A}(-)^{\mathrm{T}}$ and $\mathbf{A}(+)^{\mathrm{T}}$ of this timed PN are:

$$\mathbf{A}^{\mathrm{T}} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ +1 & 0 & 0 & -1 \\ 0 & +1 & 0 & 0 \\ 0 & 0 & +1 & 0 \\ 0 & 0 & 0 & +1 \end{bmatrix},$$

$$\mathbf{A}(-)^{\mathrm{T}} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & +1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\mathbf{A}(+)^{\mathrm{T}} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ +1 & 0 & 0 & 0 \\ 0 & +1 & 0 & -1 \\ 0 & 0 & +1 & +1 \\ 0 & 0 & 0 & +1 \end{bmatrix}$$

Let us assume that the initial marking is $\mathbf{M}_0 = [1\ 1\ 1\ 1\ 0\ 0\ 0\ 0]^{\mathrm{T}}$, the terminal place is P(8) and the delay times of $T(1)$,$T(2)$ and $T(3)$ are 1, 2 and 3 min, respectively. The simulation time interval is chosen to be 1 min. The simulation procedure developed in this study has already been coded with MATLAB and the results for the present example can be found in Table 3. Following is a detailed description of the computation steps performed in this program at each time interval:

1. At $t = 0$ min, the transitions $T(1)$, $T(2)$ and $T(3)$ are found to be enabled on the basis of algorithm I. Since all transitions are associated with delay times, the actual firing vector $\mathbf{U}_1$ should be $[0\ 0\ 0\ 0]^{\mathrm{T}}$ and these enabled transitions should be stored in future firing vectors according to their respective delay times (see Fig. 4(a)).
2. At $t = 1$ min, the transition $T(1)$ should be fired first. This

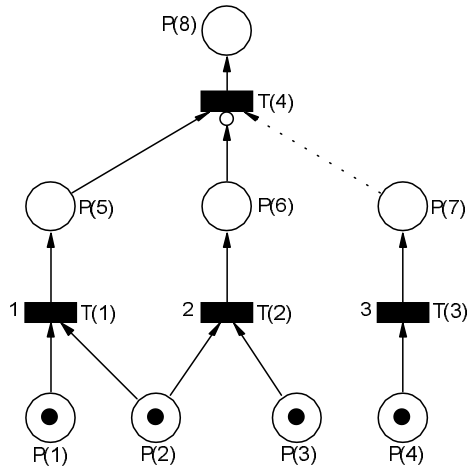

Fig. 3. A simple PN model.

yields the following marking: $\mathbf{M}_1 = [0\,0\,1\,1\,1\,0\,0\,0]^{\mathrm{T}}$. By applying algorithm I, we can find that the only enabled transition now is $T(3)$ and $T(2)$ is disabled. The result is depicted in Fig. 4(b).

3. At $t = 2$ min, no transition can be fired since the stored firing vector is empty.
4. After firing $T(3)$ at 3 min, the following marking can be obtained: $\mathbf{M}_2 = [0\,0\,1\,0\,1\,0\,1\,0]^{\mathrm{T}}$. According to this marking, we find the only enabled transition $T(4)$. After firing $T(4)$ immediately, the final marking is: $\mathbf{M}_3 = [0\,0\,1\,0\,0\,0\,0\,1]^{\mathrm{T}}$. Since the terminal place, i.e. the last entry in $\mathbf{M}_3$, contains one token, the simulation process should be terminated.

4. The MCS identification algorithm

Having presented our procedures for model construction and dynamic simulation, our algorithm to enumerate the causes of an undesirable event/condition can now be explained in detail. As mentioned previously, the failure events are represented with primal transitions in the PN model. In order to determine all possible fault propagating patterns, there is a need to fire these transitions at various time instances. Consequently, the PN model of an artificial failure-triggering device is augmented to each of the component models constructed with the hierarchical approach mentioned earlier. A general form of this PN is presented in Fig. 5. Here, the delay times associated with the transitions $T(j)$s are the occurrence times of the failure events. The place PF denotes the pre-condition of one of the failure events associated with the component under consideration. The primal places PM(i)s signify the existence or nonexistence of the respective failure modes. They are referred to in this work as the failure-mode places. On the other hand, the rest of primal places PT(j)s denote the failure occurrence times. They are referred to as the failure-time places. Notice that the structure of such a PN prevents a failure that occurs more than once at different times and, also, a component fails more than once due to different modes. Thus, the maximum number of scenarios that could be examined for the nth component (N_n^{sc}) should be:

$$N_{\mathrm{sc}}^n = N_{\mathrm{pt}}^n N_{\mathrm{pm}}^n + 1 \qquad n = 1, 2, \ldots, N_{\mathrm{comp}} \tag{3}$$

where, N_{pt}^n and N_{pm}^n denote the numbers of the failure-time and failure-mode places, respectively, and N_{comp} is the number of components in the PN model. Notice that the possibility of no failures is considered as one of the possible scenarios for component n. The maximum number of

Table 3
Detailed simulation results in Example 2

Time (min)	Firing vector	Marking
0.0	–	($\mathbf{M}_0$) $[1\,1\,1\,1\,0\,0\,0\,0]^{\mathrm{T}}$
1.0	($\mathbf{U}_1$) $[1\,0\,0\,0]^{\mathrm{T}}$	($\mathbf{M}_1$) $[0\,0\,1\,1\,1\,0\,0\,0]^{\mathrm{T}}$
2.0	–	($\mathbf{M}_1$) $[0\,0\,1\,1\,1\,0\,0\,0]^{\mathrm{T}}$
3.0	($\mathbf{U}_2$) $[0\,0\,1\,0]^{\mathrm{T}}$	($\mathbf{M}_2$) $[0\,0\,1\,0\,1\,0\,1\,0]^{\mathrm{T}}$
	($\mathbf{U}_3$) $[0\,0\,0\,1]^{\mathrm{T}}$	($\mathbf{M}_3$) $[0\,0\,1\,0\,0\,0\,0\,1]^{\mathrm{T}}$

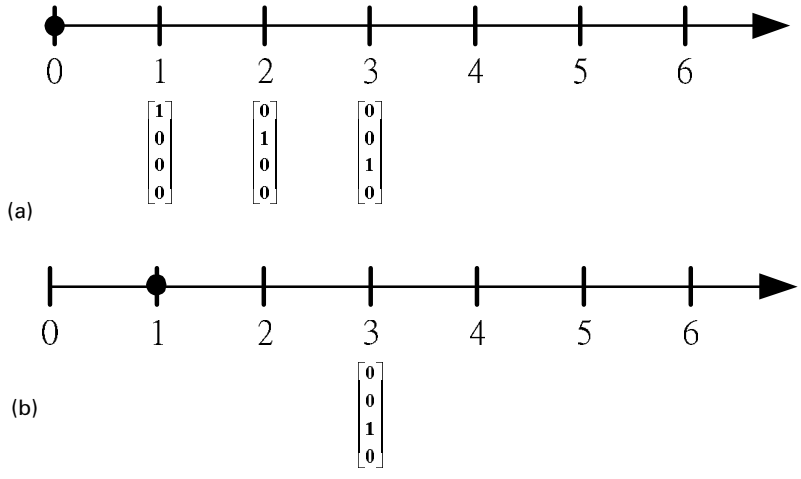

Fig. 4. (a) The future firing vectors at 0 min. (b) The future firing vectors at 1 min.

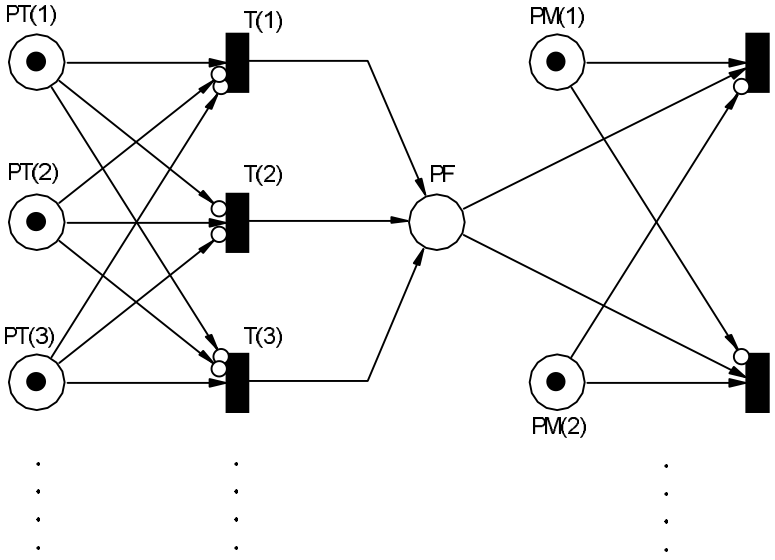

Fig. 5. The PN model of artificial failure-triggering device.

scenarios N_{sc}^{S} for the entire system can be determined on the basis of Eq. (3), i.e.

$$N_{sc}^{S} = \prod_{n=1}^{N_{comp}} N_{sc}^{n} - 1 \quad (4)$$

In this case, the normal operation, i.e. a failure-free system, is excluded from consideration.

After installing all the artificial failure-triggering devices, the following cause enumeration algorithm can then be applied to the resulting PN.

1. Produce the initial markings associated with all possible failure scenarios. This task can be done by implementing the following procedure repeatedly.
   (a) Place a token in each of the places corresponding to the initial conditions of normal operation. The rest of the places should be empty.
   (b) Select a combination of the failure-time and failure-mode places in each component model. Place a token in every chosen place. The marking of resulting PN is one of the initial markings for enumeration.
2. Select one of the initial markings and perform dynamic simulation. If the simulation process is terminated by the first criterion, then the set of failures in the initial marking represents a cause of the undesirable condition. Otherwise, the marking should be discarded.
3. Repeat Step 2 until all scenarios are exhausted.
4. Delete all supersets. The remaining sets should be the causes of the given undesirable condition.

The above procedure has been applied to Example 1. For the undesirable condition 'off-spec product', the simulation results can be found in Tables 4 and 5. It is clear from these results that the causes for the condition 'off-spec product' occurring between 0 and 1 min are {valve V1 failing close between 0 and 1 min} and {valve V2 failing close between 0 and 1 min} and the cause for the same condition occurring between 1 and 2 min is {valve V2 sticking between 0 and 1 min}.

5. Application

A practical example is used here to illustrate the implementation procedure of the proposed methodology and to demonstrate its effectiveness. A sequential process for drying air is adopted here for these purposes. Although a detailed process description is available in Ref. [21], let us still present a brief version in the sequel for the sake of completeness.

5.1. Process description

Fig. 6 is the flow diagram of a sequential process for drying air by using fixed alumina beds. Ambient air which contains water vapor enters in stream 9. The air passes through a bed of alumina where the water vapor is adsorbed.

Table 4
Simulation results of valve sticking in Example 1

Valve No.	Failure time (θ)	Occurrence time of 'off-spec product'	Final valve state
V1	$0 < \theta < 1$	–	V1: open, V2: closed
	$1 < \theta < 2$	–	V1: open, V2: closed
V2	$0 < \theta < 1$	> 1	V1: closed, V2: open
	$1 < \theta < 2$	–	V1: open, V2: closed

Table 5
Simulation results of valve failing closed in Example 1

Valve No.	Failure time (θ)	Occurrence time of 'off-spec product'	Final valve state
V1	$0 < \theta < 1$	$> \theta$	V1: closed, V2: open
	$1 < \theta < 2$	–	V1: closed, V2: closed
V2	$0 < \theta < 1$	$> \theta$	V1: open, V2: closed
	$1 < \theta < 2$	–	V1: open, V2: closed

The dried air passes out of the process in stream 25. In order to maintain a continuous supply of dry air, two beds are employed. When one bed is removing water from air, the other is being regenerated. Regeneration involves passing hot air through a bed which has been loaded to capacity with water. The hot air strips the water from the alumina. After leaving the regenerating bed, it is passed through a condenser where water is removed. Eventually, this air is recycled and passed through the operating dryer. The regenerated bed is then cooled with inlet air and switched back into service. The same procedure is followed for the other bed. Table 6 gives the sequence of operations for a complete cycle.

5.2. Model construction

The hierarchy presented in Table 2 is followed to build the PN for hazard analysis. Following is a description of the component models in each level.

5.2.1. Level 1

The first-level component in this system is the timer. It is assumed that this device is electrically powered and thus its states can be represented with two discrete places, i.e. power on and off. In addition, the component model should be able to reflect the fact that the timer is programmed to issue periodical signals marking the switching time of successive operating periods. This PN model and its initial marking are shown in Fig. 7(a). Notice that the normal condition of the timer is considered to be always 'power on' in this example. The delay times associated with transitions $T(i)$s ($i = 1, 2, 3, 4$) are the elapsed times of periods 1–4, respectively. Consequently, a token is introduced in place PS to mark the end of each of these four periods in correct order. If the timer fails, the resulting state should be 'power off' and consequently it should stop sending the periodical signals afterwards. The corresponding failure

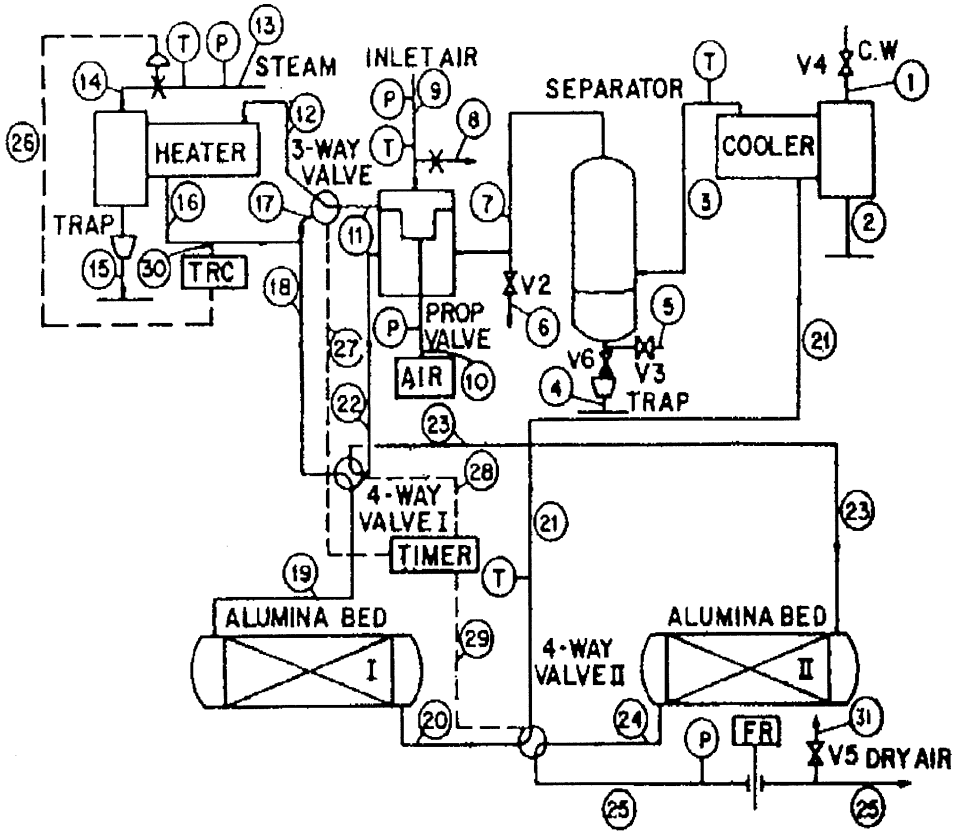

Fig. 6. Flow diagram of a utility air drying process [21].

Table 6
Operating procedure of the utility air drying system [21]

Time period	Valve position			Bed status	
	3W	4W-I	4W-II	Bed-I	Bed-II
1	11 → 12	18 → 19 22 → 23	20 → 21 24 → 25	Regeneration	In service
2	11 → 18	18 → 19 22 → 23	20 → 21 24 → 25	Cooling	In service
3	11 → 12	18 → 23 22 → 19	20 → 25 24 → 21	In service	Regeneration
4	11 → 18	18 → 23 22 → 19	20 → 25 24 → 21	In service	Cooling

model is attached to the place representing the normal condition of timer (see Fig. 7(b)).

5.2.2. Level 2

The second-level components are the three-way valve 3W and the two four-way valves 4W-I and 4W-II. As mentioned earlier, the system configuration is defined by the positions of these three valves. Valve 3W determines the route of inlet air flow. The fresh air can either be directed to the heater or simply bypass it. Valve 4W-I defines the connections between the alumina beds and their air sources. The air consumed in each bed can be taken either from system inlet (for regeneration or cooling) or from the lower port of proportionating valve (for dehumidification). Valve 4W-II governs the destinations of the exit airs from these two beds, i.e. the air can be either discharged or recycled. Thus, every valve in this system can only be switched to two alternative positions. They are labeled as +10 and −10, respectively. The relationships between the valve positions and the stream connections are shown in Table 7.

Let us consider the component model of valve 4W-I as an example (Fig. 8(a)). Notice that the initial marking, i.e. the marking associated with the position of 4W-I in period 1, is also given in this PN. Notice also that the place PS is the common place shared by the component model of timer and the present one. It is clear that the valve position can be changed from +10 to −10 (or vice versa) after two tokens are accumulated in the place representing a counter, i.e. PC. In other words, valve 4W-I should be switched repeatedly every two time periods at the end of period 2 and 4. Two failure events, valve sticking and valve reversed, are

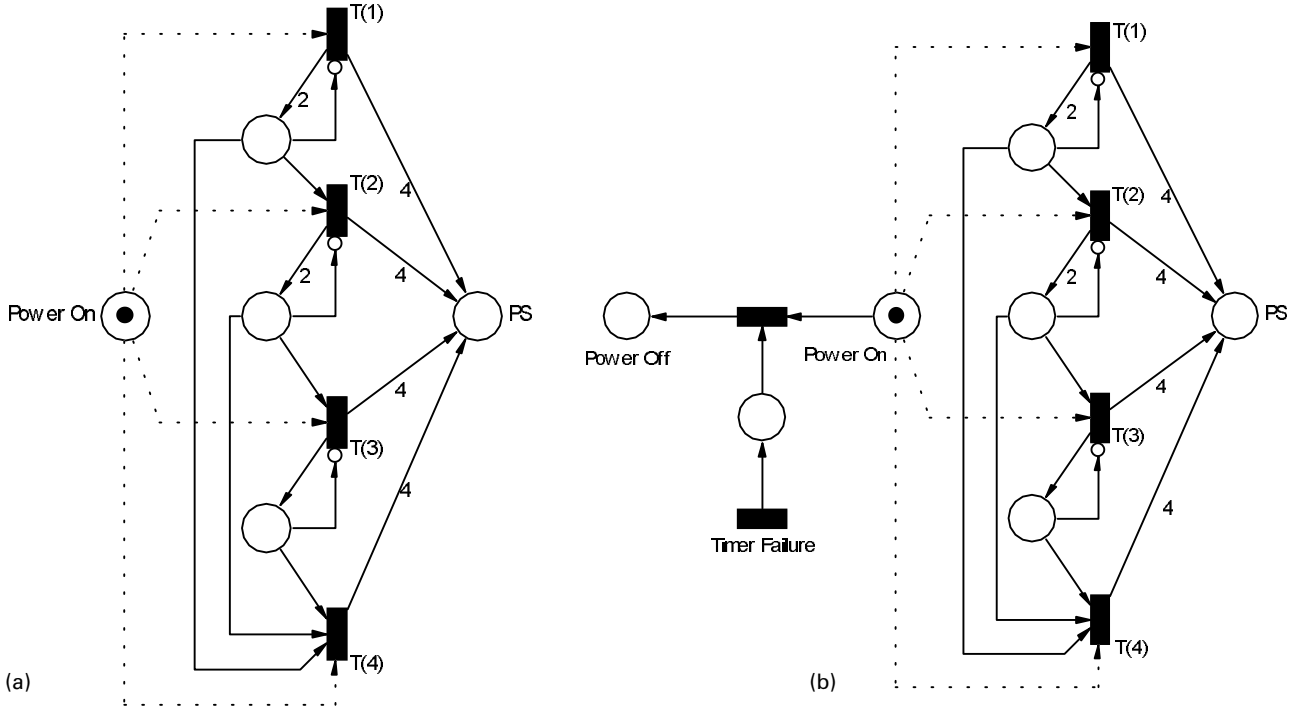

Fig. 7. (a) The component model of timer without failure. (b) The component model of timer with failure.

Table 7
The relationships between valve positions and stream connections

Valve	Valve position	Stream connection
3W	+10	11 → 12
	−10	11 → 18
4W-I	+10	18 → 19 and 22 → 23
	−10	18 → 23 and 22 → 19
4W-II	+10	20 → 21 and 24 → 25
	−10	20 → 25 and 24 → 21

considered in this model. The corresponding failure models can be attached to the normal PN as shown in Fig. 8(b).

The component models of 4W-II and 3W are very similar to that of 4W-I. Since the structure of 4W-II is essentially unchanged, it is only necessary to duplicate Fig. 8(b) and define a separate set of labels for the transitions and places in this PN. On the other hand, since the position of 3W is changed every period, the weights on the outward arcs of PC should all be assigned to be 1. Consequently, there can only be one possible failure-mode for 3W, i.e. valve sticking. For the sake of brevity, the models of 4W-II and 3W are not described in detail in this paper.

5.2.3. Level 3

The third-level components are the two alumina beds, the heater, the cooler, the separator and the proportionating valve. Other than the adsorption beds, the conditions of all process units should remain constant if none of them are affected by failures. Without loss of generality, let us limit the scope of hazard analysis performed in this example to the effects of component failures in Sections 5.2.1 and 5.2.2 only. Thus, all component models in the third-level (except the ones for alumina beds) can be excluded from the system PN.

Let us consider the behaviors of these adsorption beds. The condition of each unit can be described with two variables, i.e. the bed temperature and water content. The variations of these variables are continuous in nature. Consequently, the continuous places should be employed for their representation. The bed temperature is mainly affected by the temperature of input air. Within one time period, hot air should raise the bed temperature until reaching an upper bound and cool air should decrease it to a lower limit. The water content, on the other hand, is affected by the temperature of the inlet air and also the bed temperature. If both temperatures are low and the bed is unsaturated, the water content in alumina bed can be increased by passing either fresh air from environment or recycled air from the proportionating valve. The amount of water that can be captured in bed should eventually reach a saturation level in at most two time periods. A saturated bed cannot be used for dehumidification purpose. Hot air can strip water from the adsorption beds. It is assumed that the bed can be dried 'completely' in one time period.

Fig. 9 is a component model of Bed-I. It can be observed

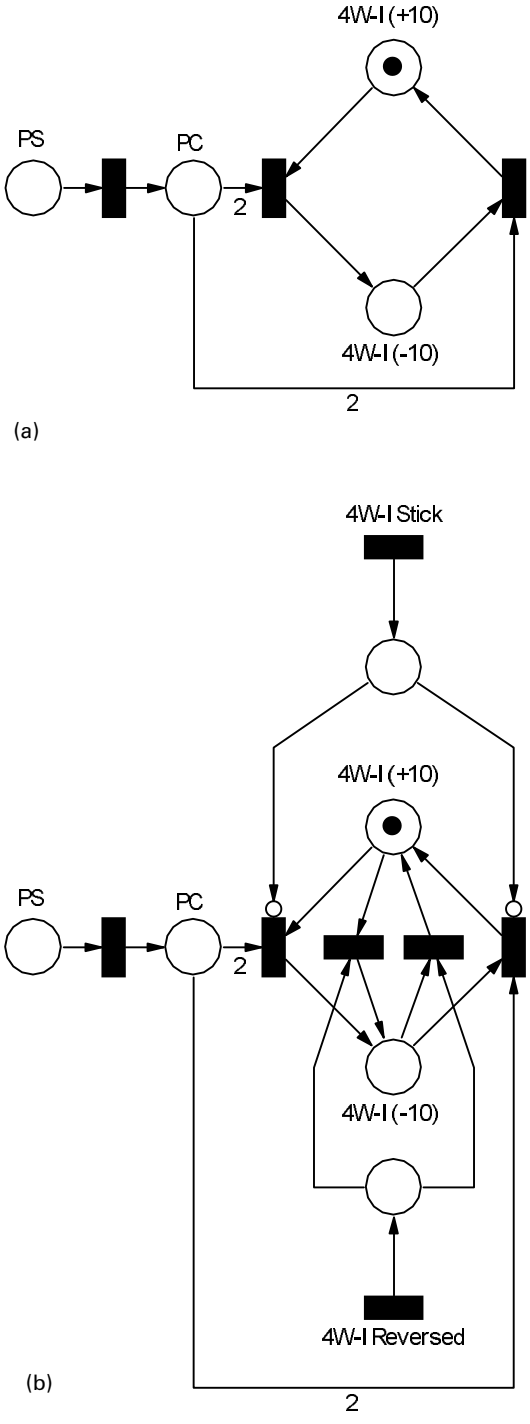

Fig. 8. (a) The component model of valve 4WI without failure. (b) The component model of valve 4WI with failure.

that two continuous places, I-T and I-M, are used to represent bed temperature and water content, respectively. Notice that their token numbers vary between 0 and 1 denoting the minimum and maximum values of the respective variables. As mentioned previously, these two variables are affected by the entering air. This implies that they can be controlled by manipulating the three-way valve 3W and four-way valve 4W-I. In order to make the resulting system model

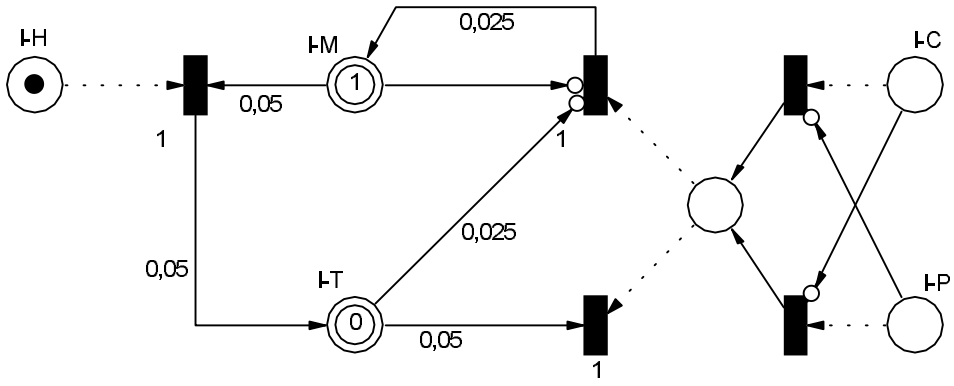

Fig. 9. The component model of Bed-I.

more transparent to the user, three additional discrete places, i.e. I-H, I-C and I-P, are introduced in this PN. They can be viewed as the operation modes of Bed-I. More specifically, I-H denotes the fact that the entering air is taken from environment and it is pre-heated; I-C indicates that cool fresh air is used in bed; I-P indicates that the entering air is obtained from the proportionating valve. It should be emphasized that these places are really not needed to construct a complete system model. This is due to the fact that the corresponding conditions are equivalent to three distinct combinations of the valve positions associated with 3W and 4W-I. Finally, a description of the component model for Bed-II is omitted in this paper for the sake of brevity.

5.2.4. Levels 4 and 5

The process material in the fourth level is air. Since only the first- and second-level failures are considered in this example, the possibilities of external disturbances in air temperature and moisture are excluded in this analysis. Thus, the corresponding models can be removed to simplify the resulting system PN. Finally, there is no need to discuss the component models in level 5 since none exist in the air drying process.

5.2.5. The complete system model

A complete system PN for the air drying process can be constructed by connecting all the component models mentioned earlier (Fig. 10). As indicated earlier, additional places have been introduced to enhance the readability of the system model. Their definitions can be found in nomenclature.

It should be noted that, although a total of eight possible process configurations can be generated with the three valves 3W, 4W-I and 4W-II, only one of them yields correct operation mode in a given time period. Obviously, the rest may result in undesirable consequences. It is thus to our interest to analyze the outcomes of timer failures and valve failures thoroughly with the complete system model.

Table 8
Outcome places associated with the sufficient conditions of undesirable consequence (Bed-I)

Outcome places	Sufficient conditions
I-H + I-E + I-T(1) + I-M(0)	(i) + (iii)
I-H + I-E + I-T(0) + I-M(0)	(iii)
I-H + I-E + I-T(0) + I-M(0.5)	(iii)
I-H + I-E + I-T(0) + I-M(1)	(ii) + (iii)
I-C + I-E + I-T(1) + I-M(0)	(i)
I-C + I-E + I-T(0) + I-M(1)	(ii)
I-P + I-E + I-T(1) + I-M(0)	(i)
I-P + I-E + I-T(0) + I-M(1)	(ii)

5.3. Hazard analysis

If the outlet air from the air-drying process contains too much water, a large number of valuable instruments downstream may be damaged. Thus, a reasonable condition for hazard analysis can be chosen as 'H_2O concentration in stream 25 is too high'. According to the process description, this undesirable consequence could be caused by:

(i) Temperature of served bed is too hot.
(ii) Adsorbents in served bed are saturated.
(iii) Inlet air temperature in served bed is too hot.

The combinations of places that cause one of the earlier three sufficient conditions in Bed-I are listed in Table 8. Notice that the required token numbers in I-T and I-M are specified in the adjacent parentheses in the first column. It should also be noted that the same combinations can be identified for Bed-II.

Numerous simulation studies have been performed to determine the causes of undesirable consequence. Let us first consider the propagation patterns of a single valve failure. The effects of valve 3W sticking in different time periods are listed in Table 9. Notice that the occurrence times of undesirable consequence is specified in the parentheses in the second column and the descriptions of the abnormal bed conditions are also provided in the same column. If

Table 9
The consequences of 3W sticking

Time period	Consequence
1	(3) The temperature of Bed-I is too high
2	(1) The adsorbents in Bed-II are saturated
3	(1) The temperature of Bed-II is too high
4	(3) The adsorbents in Bed-I are saturated

valve 3W sticks in period 1 (or period 3), the inlet air for regeneration should pass through the heater in period 2 (or period 4). Thus, the regenerated bed is not cooled in the same period. Because of the fact that condition (i) is satisfied, the designated undesirable condition should occur in the next time period. On the other hand, if valve 3W sticks in period 2 (or period 4), the inlet air for cooling should bypass the heater in period 3 (or period 1 in the next cycle) and thus Bed II (or Bed I) cannot be regenerated. When the alumina bed is in service during period 1 (or period 3) in the next cycle, it should still be saturated with water. Since condition (ii) is satisfied, the designated condition is bound to occur in this period.

Naturally, the undesirable consequence can be the result of timer failure and various combinations of valve failures. A more detailed listing of these scenarios concerning Bed-I can be found in Table 10. Let us consider the seventh row in Table 10 specifically in detail. If valve 3W sticks in period 3, the system should behave normally during the same period. If, in addition, valve 4W-I is reversed in period 4, the inlet air should be misdirected to Bed-I and it is still hot due to 3W sticking. Since valve 4W-II acts normally, the outlet air from Bed-I must be discharged to stream 25. Hence, the temperature and moisture content in stream 25 should be abnormally high in period 4. It should be noted that Table 10 represents only a condensed version of the most comprehensive list. A counterpart scenario corresponding to each combination of valve failures in this table has been neglected. The missing cases can be recreated by adding two periods to the occurrence times of undesirable outcomes and valve failures in the second and third column, respectively. Finally, notice also that the failure mechanisms associated with Bed-II can be produced by subtracting two periods from the occurrence times listed in the second and third columns of Table 10.

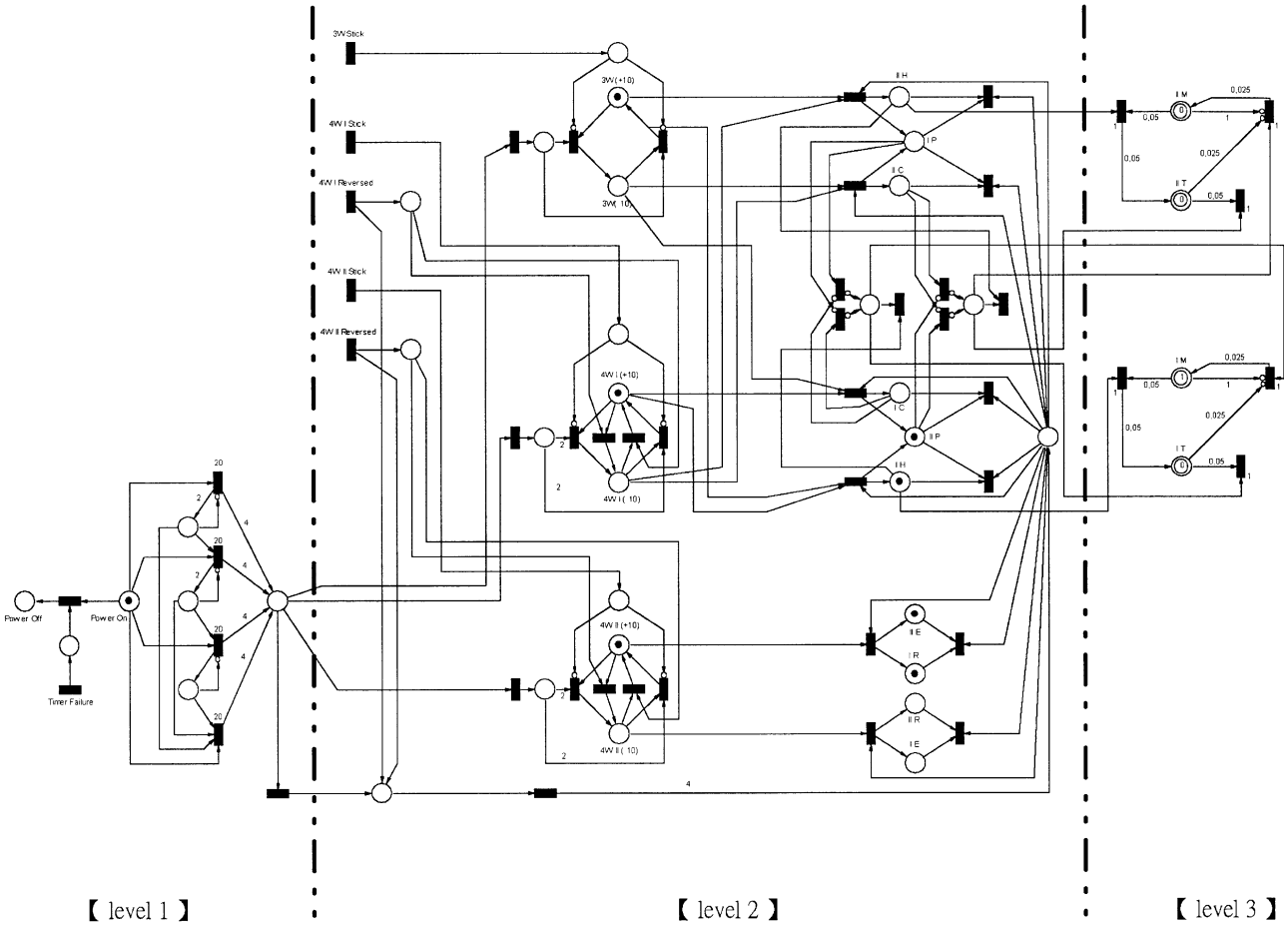

Fig. 10. The complete PN model of utility air drying process.

Table 10
Root causes of the undesirable consequence in the utility air drying process

Outcome places	Occurrence time	Root causes
I-H + I-E + I-T(1) + I-M(0)	(2)	3W sticking (1),4W-II reversed (2)
	(3)	3W sticking (1), 4W-I sticking
	(3)	3W sticking (1), 4W-I sticking (2)
I-H + I-E + I-T(0) + I-M(0)	(3)	4W-I reversed (2)
	(3)	4W-I sticking (1)
	(3)	3W-I sticking (2)
I-H + I-E + I-T(0) + I-M(0.5)	(4)	3W sticking (3), 4W-I reversed (4)
I-H + I-E + I-T(0) + I-M(1)	(1)	4W-II sticking (3)
	(1)	4W-II sticking (4)
I-C + I-E + I-T(1) + I-M(0)	(2)	4W-II reversed (2)
I-C + I-E + I-T(0) + I-M(1)	(1)	4W-II sticking (3), 3W sticking (4)
	(1)	3W sticking(2), 4W-II sticking (3)
	(1)	3W sticking (2), 4W-II sticking (4)
	(1)	3W sticking (4), 4W-II sticking (4)
	(3)	3W sticking(4), 4W-I reversed (4)
	(2)	3W sticking (4), 4W-II reversed (2)
	(3)	3W sticking(4), 4W-I reversed (2)
	(3)	3W sticking (4), 4W-I sticking
	(3)	3W sticking (4), 4W-I sticking (2)
I-P + I-E + I-T(1) + I-M(0)	(3)	3W sticking (1)
	(2)	4W-I reversed (2), 4W-II reversed (2)
I-P + I-E + I-T(0) + I-M(1)	(1)	4W-I sticking(3), 4W-II sticking (3)
	(1)	4W-I sticking (3), 4W-II sticking (4)
	(1)	4W-I sticking (4), 4W-II sticking (4)
	(1)	4W-I reversed (4), 4W-II sticking (4)
	(1)	4W-II sticking (3), 4W-I sticking (4)
	(1)	4W-II sticking (3), 4W-I reversed (4)
	(1)	4W-I reversed (2), 3W sticking (2), 4W-II sticking (3)
	(1)	4W-I reversed (2), 3W sticking (2), 4W-II sticking (4)
	(3)	3W sticking (4)
	(2)	3W sticking (4), 4W-I sticking (4), 4W-II reversed (2)
	(2)	3W sticking (4), 4W-I reversed (2), 4W-II reversed (2)
	(2)	4W-I sticking (3), 3W sticking (4), 4W-II reversed (2)
	(2)	4W-I reversed (4), 3W sticking (4), 4W-II reversed (2)
	(1)	Timer power off (3)
	(1)	Timer power off (4)

6. Conclusions

A hierarchical approach is proposed in this study to construct the PN models for batch operations. A systematic simulation procedure is also developed to properly describe the dynamic behaviors of batch operations. By using these techniques, enumeration of all possible causes of an undesirable consequence becomes very efficient. It is clear from the application results that the proposed PN models can indeed be used as the basis for comprehensive hazard analysis.

Acknowledgements

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

References

[1] Kuo DH, Hsu DS, Chang CT, Chen DH. Prototype for integrated hazard analysis. AIChE J 1997;43(6):1494.
[2] Lapp SA, Powers GJ. Computer-aided synthesis of fault-trees. IEEE Trans Reliab 1977;R-26:2.
[3] Chang CT, Hwang HC. New development of the digraph-based techniques for fault-tree synthesis. Ind Engng Chem Res 1992;31:1490.
[4] Kumamoto H, Henley EJ. Safety and reliability synthesis of systems with control loops. AIChE J 1979;20:376.
[5] Kelly BE, Lees FP. The propagation of faults in process plants: 1. Modelling of fault propagation. Reliab Engng 1986;16:3.
[6] Kelly BE, Lees FP. The propagation of fault in process plants: 2. Fault tree synthesis. Reliab Engng 1986;16:39.
[7] Allen DJ, Rao MSM. New algorithms for the synthesis and analysis of fault trees. Ind Engng Chem Fundam 1980;19:79.
[8] Andrews JD, Morgan JM. Application of digraph method of fault tree construction to process plant. Reliab Engng 1986;14:85.
[9] Chang CT, Hwang KS. Studies on the digraph-based approach for

fault-tree synthesis 1. The ratio-control systems. Ind Engng Chem Res 1994;33:1520.

[10] Chang CT, Hsu DS, Hwang DM. Studies on the digraph-based approach for fault tree synthesis 2. The trip systems. Ind Engng Chem Res 1994;33:1700.

[11] Srinivasan R, Venkatasubramaniyan V. Petri net-digraph models for automation analysis of batch process plants. Comput Chem Engng 1996;20(Suppl. A):S719.

[12] Cassangras CG. Discrete event systems: modeling and performance analysis. Boston: Aksen Associates, 1993.

[13] Srinivasan R, Venkatasubramaniyan V. Automationg hazop analysis of batch chemical plants: part i. The knowledge representation framework. Comput Chem Engng 1998;22(9):1357.

[14] Srinivasan R, Venkatasubramaniyan V. Automating hazop analysis of batch chemical plants: part ii. Algorithms and application. Comput Chem Engng 1998;22(9):1345.

[15] Hura GS, Atwood JW. The use of Petri nets to analyze coherent fault trees. IEEE Trans Reliab 1988;375:469.

[16] Liu TS, Chiou SB. The application of Petri nets to failure analysis. Reliab Engng Syst Safety 1997;57:129.

[17] Murata T. Petri nets: properties, analysis and applications. Proc IEEE 1989;77(4):541.

[18] Davis R, Alla H. Petri net for modeling of dynamics—a survey. Automatica 1994;30(2):175.

[19] Drath R, Engmann U, Schwuchow S. Hybrid aspects of modelling manufacturing systems using modified petri nets. IFAC, 1998.

[20] Bowden FDJ. A brief survey and synthesis of the role of time in Petri nets. Math Comput Modelling 2000;31:55.

[21] Shaeiwitz JA, Lapp SA, Powers GJ. Fault tree analysis of sequential systems. Ind Engng Chem Process Des Dev 1977;16(4):529.