COMPUTER-AIDED HAZARD IDENTIFICATION IN SEQUENTIAL OPERATIONS USING PETRI NETS

Yi-Feng Wang and Chuei-Tin Chang
Department of Chemical Engineering
National Cheng Kung University
Tainan, Taiwan 70101, Republic of China

Abstract

A systematic procedure is presented in this paper to construct Petri nets (PN) for modeling the fault propagation behaviors in sequential operations. A complete system model is basically organized according to a hierarchy of four levels, i.e. (1) the controller/operator, (2) the valves, (3) the process units, and (4) the sensors. Every component model is built with two distinct elements. One is used to characterize the equipment states and the other the input-output relations. For the purpose of reducing model construction effort, the general structure of object-oriented abbreviations is also developed to represent the PN in a user-friendly format. The effectiveness and correctness of the proposed methodology has been applied successfully to the air-drying process reported by Shaeiwitz *et al* (1977). The results show that it is more accurate and more comprehensive when compared with the conventional approaches.

Keywords

Fault tree analysis, Sequential operation, Petri net, Digraph, Hierarchical approach.

Introduction

In order to ensure operation safety, hazard analysis is one of the basic tasks that must be performed in designing or revamping any chemical process. A variety of techniques have been presented, namely, fault tree analysis (FTA), event tree analysis (ETA), and hazard and operability study (HAZOP), etc. In implementing these methods, there are always needs (1) to reason deductively for finding all combinations of basic events that could lead to an undesirable condition and/or (2) to predict all possible consequences of a given fault origin. However, if the task of identifying every fault propagation mechanism is to be done manually, a rigorous hazard analysis is bound to be labor- and time-consuming and its results often error-prone. Thus, there are real incentives to automate such a cause-finding process.

For *continuous* processes, due to the development of efficient modeling tools like the digraph (DG), techniques for automated fault tree analysis have been matured considerably. However, since the digraph cannot be used to describe the dynamic causal relationships among time, discrete events, equipment states and system configurations, it is unsuitable for modeling *batch* or *semi-batch* processes. On the other hand, the Petri net is well known for its capability in representing the discrete-event systems and/or sequential operations. Thus, the aim of this paper is to develop a systematic procedure to construct Petri nets for automatic hazard identification in batch processes.

The Elements in Petri-Net Models

In order to facilitate proper representation of sequential operations, several special extensions are chosen in this work. Specifically, both the discrete and continuous places are allowed in the proposed PN model and the transitions can be timed and non-timed. In addition, three different types of place-to-transition arcs are utilized, i.e. the weighted arcs, the inhibitor arcs and the static test arcs, and all transition-to-place arcs are weighted arcs. If an arc is directed toward or away from a continuous place, the independent variables of its weight function should be the token number in one or more user-selected place. For the sake of brevity, the definitions of these elements are omitted in this paper. A detailed description can be found in the literature (David and Alla, 1994; Wang *et al*., 2002).

The Hierarchy in a System Model

A hierarchical approach has been taken in this work to construct Petri nets for modeling the *normal* operation steps in batch processes. The components in a complete system model can be classified into the four different levels shown in Table 1. In general, every item in the P&ID is described with a component model here. Each component consists of two distinct parts. One is used to characterize the equipment state and the other the input-output conditions. In the latter case, several different versions are needed if a change in the equipment state alters the relations among process conditions.

Table 1. The Hierarchy in PN-Based System models for Sequential Operations.

Level	Component Models
1	timer, operator, PLC
2	valve, pump, compressor
3	process unit
4	sensor

Following is a general description of the component models in every level.

- *Level 1:* The operating steps specified in a recipe are executed sequentially by a 1st-level component. In general, each operation step can be characterized with two elementary actions: (1) confirmation of an initiation signal and (2) execution of an operation command. The input-output model of a controller/operator can be developed accordingly by following Figure 1. The input place *PS*(*i*) denotes the status of the *i*th initiation signal. The initiation signal can be obtained either from a sensor in the 4th level or from an internal clock. The non-timed transition *TS*(*i*) denotes the confirmation action of the *i*th initiation signal. The output place *PC*(*i*) is used to reflect the status of the *i*th operation command. Notice that it is not necessary to model its equipment state in this case since there is only one possibility during normal operation, i.e. the component is in service.

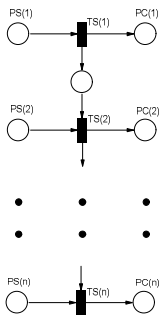

Figure 1. The PN Model Representing the Input-Output Relations of an Operator/Controller.

- *Level 2:* All 2nd-level components can be described with two alternative equipment states. The PN model of a 3-way valve is presented in Figure 2. In this Petri net, the places *PV*(+) and *PV*(-) denote two alternative valve positions connecting lines 1&2 and 1&3 respectively, and the transitions *TV*(1) and *TV*(2) represent the valve-switching actions from *PV*(+) to *PV*(-) and vice versa. Notice that the input places *PC*(1) and *PC*(2) of the two transitions *TV*(1) and *TV*(2) are associated with the corresponding operation commands issued by controller/operator. On the other hand, the causal relations between the input and output conditions of a level-2 component are described *qualitatively* in this work. Let us use the 3-way valve again as example. Its input and output flow rates can be related with the Petri net in Figure 3. Notice that the places called *deviation places* here represent qualitative deviation levels from their normal values. This type of deviation places is a new extension created mainly to facilitate simulation of the fault propagation behaviors in sequential operations. Each of them can be constructed with the elements described in the previous section. As shown in Figure 3, a deviation place is represented with two circles. The outer circle is drawn with a solid line and the inner one a dotted line.

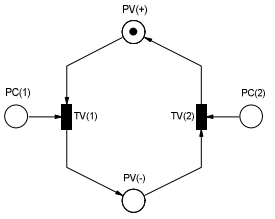

Figure 2. The PN Model Describing the Equipment States of a 3-Way Valve.

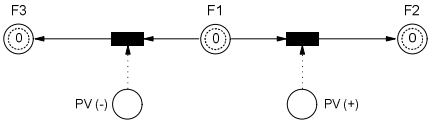

Figure 3. The PN Model Representing the Input-Output Relations of a 3-Way Valve.

- *Level 3:* Basically all process units in the P&ID can be considered as the 3rd-level components. The input-output models of a level-3 component can be constructed with deviation places. The model structure is essentially the same as that of any level-2 component. On the other hand, the equipment state of a process unit can usually be assumed to be unchanged under normal operating conditions. However, this assumption may not be

valid if (1) there is a continuous accumulation (or depletion) of mass and/or energy in the unit or (2) the performance of a unit deteriorates quickly during operation. Thus, it is necessary to describe the transients in these process units with continuous places. A generalized version is presented in Figure 4. Here, the *continuous* place *PES*(*j*) represents the *j*th equipment state used to characterize a level-3 component; the discrete place *POM*(*i*) denotes the *i*th operation mode defined by the equipment states of level-2 components; $TES_{in}(i)$ and $TES_{out}(i)$ are time-delayed transitions enabled after the *i*th mode is activated in operation; the weight function W_{in} and W_{out} denote respectively the amounts of increase and decrease in the continuous state variable during a very small time increment Δt. In other words, $W_{in}/\Delta t$ and $W_{out}/\Delta t$ can be considered as the approximate rates of increase and decrease of the state variable respectively.

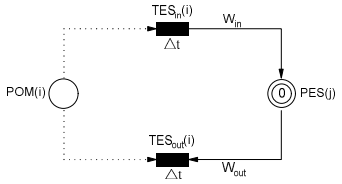

Figure 4. The PN Model Describing the Equipment State of a Process Unit in Level 3.

- *Level 4:* The input of a sensor is the equipment state or the output condition of a 3rd-level component. The sensor output is the measurement signal. The corresponding model structure can also be found in Figure 3. Since it can be assumed that a sensor is always in the working state during normal operation, there is no need to model its equipment state.

The Failure Mechanisms in Component Models

To facilitate hazard analysis, it is still necessary to incorporate additional sub-PNs in each component model to depict the fault propagation behaviours caused by various equipment failures. A generalized failure model can be found in Figure 5. In this model, the direct outcome of a failure is treated as a change in the equipment state of a component. The equipment state caused by the *i*th failure is represented by the place *PFS*(*i*). The effects of a failure can be readily modeled with a combination of the inhibitor arcs and static test arcs. The former arcs are used to disable the transitions corresponding to the routine events, i.e. *TN*(*j*), and the latter activate the alternative transitions representing the failure events, i.e. *TF*(*k*).

The Model Construction Procedure

In building a PN-based system model for hazard analysis, the component models should be constructed first and then connected in sequence from top to bottom level according to the P&ID. In principle, all component models should be included to ensure the comprehensiveness of analysis. However, some of them may be excluded for the sake of simplicity. Specifically, a component can be neglected if (1) its failure mechanisms are not of interest, (2) there is only one normal equipment state, and (3) it is a single-input-and-single-output component.

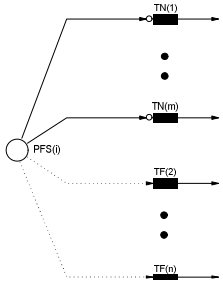

Figure 5. A Generalized Failure Model.

The Object-Oriented Abbreviations

Strictly speaking, the PN models constructed with the above procedure are only suitable for analyzing small systems with moderately complex recipes. This is mainly due to state-space explosion caused by the need to describe not only the process configurations but also the operation steps in an industrial-size system model. In order to handle this practical problem, the object-oriented abbreviations (Drath, 1998) have been utilized in this study to simplify model structure and to reduce the model-building effort.

As mentioned previously, a complete system model consists of a large number of interacting components. Each component can be treated as an object. Basically, every object can be fabricated according to a three-layer structure. In the upper layer, it is only necessary to build an object frame. This object frame is always labeled with a heading and equipped with multiple interface ports. There are two connected sub-frames in the underlying second layer. They are used to encapsulate the PNs in the bottom layer for describing equipment states and input-output conditions respectively. The structures of these two sub-frames are essentially identical to that of the object frame. Let us illustrate an example, the object frame for a 3-way valve and its two sub-frames can be found in Figure 6.

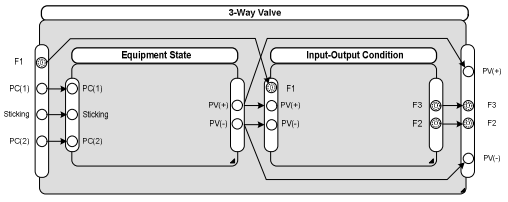

Figure 6. The Object Net of a 3-Way Valve.

Applications

Figure 7 is the flow diagram of a sequential process for drying air by using fixed alumina bed (Shaeiwitz *et al*., 1977). Ambient air which contains water vapor enters in stream 9. The air passes through a bed of alumina (Bed I) where the water vapor is adsorbed. 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 the inlet air, the other bed 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 form the alumina. The hot air leaving the regenerating bed is passed through a condenser where water is removed. The air is reheated 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.

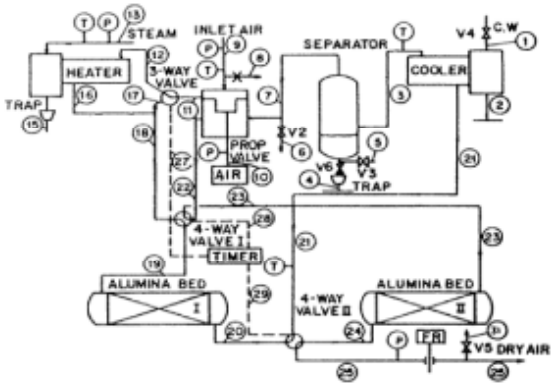

Figure 7. The Process Flow Diagram of a Utility Air Drying Process.

Let us assume that a reasonable condition for hazard analysis may be "H_2O concentration in stream 25 is too high." This is due to the fact that, if the outlet air from the air-drying process contains too much water, a large number of valuable instruments downstream may be damaged.

According to the process description, the above undesirable consequence should be caused by:

1. *temperature of served bed is too hot,*
2. *adsorbents in served bed are saturated, and*
3. *inlet air temperature in served bed is too hot.*

In this study, simulation runs have been carried out to confirm if a given set of failures and/or disturbances can be considered as the root cause of the designated event. To identify the corresponding root causes, all possible combinations of timer and valve failures were thus tested in a series of exhaustive case studies. A comprehensive list was generated in this fashion. Due to the limitation of space, let us consider only two of them as examples. One scenario is resulted from a single failure (valve 3W sticking) and the other a combination of two failures (valve 3W sticking and spurious controller command to 4W-II). If valve 3W sticks in period 1, the inlet air for regeneration should pass through the heater in period 2. 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 be occur in the next time period. On the other hand, if valve 3W sticks in period 1, the system should behave normally during the same period. If, in addition, valve 4W-II is abnormally reversed in period 2, the inlet air should be misdirected to Bed-I must be discharged to stream 25. Hence, the temperature and moisture content in stream 25 should be abnormally high in period 2.

Since the above scenarios are only concerned with level-1 and/or level-2 component failures, it is necessary to examine other possibilities, i.e. the external disturbances and the level-3 component failures. From the P&ID presented in Figure 7, it is clear that changes in the upstream conditions, i.e. flow rate, temperature or H_2O concentration, can be introduced into cooling water (stream 1), inlet air (stream 9) and steam (stream 13). Simulation runs can be observed that the undesirable consequence can be caused by any of the following seven external disturbances during the *same* operation period, i.e., *F1*(-1), *T1*(+1), *F9*(+1), *T9*(+1), *C9*(+1), *F13*(+1) and *T13*(+1). On the other hand, the effects of level-3 component failures can also be assessed by simulation. It was found that an increase in the concentration of stream 25 can be caused by any of the following five level-3 component failures during the *same* operation period, i.e., proportionating valve failing high, external fire near cooler, separator trap plugged, Bed-I channeling in period 3 and 4 and Bed-II channeling in period 1 and 2.

Conclusions

A hierarchical approach is proposed in this study to construct a comprehensive PN model for any batch process. By carrying out simulation studies, identification and enumeration of critical fault propagation scenarios become very efficient. It is clear from the application results that the proposed PN models can indeed be used as the basis for rigorous hazard analysis.

References

David, R. and Alla, H. (1994). Petri Nets for Modeling of Dynamic Systems – A Survey. *Automatica*, **30(2)**, 175.

Drath, R. (1998). Hybrid Object Nets: An Object Oriented Concept for Modeling Complext Hybrid Systems, Hybrid Dynamical Systems. 3rd International Conference on Automation of Mixed Processes, ADPM'98, Reims.

Shaeiwitz, J. A., Lapp, S. A., and Powers, G. J. (1977). Fault Tree Analysis of Sequential Systems. *Ind. Eng. Chem. Process Des. Dev.*, **16(4)**, 529.

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