FAILURE ANALYSIS FOR AN AIRBAG INFLATOR BY PETRI NETS

S. K. YANG
Department of Mechanical Engineering, National Chiao Tung University, Hsinchu 30010, Taiwan, R.O.C.

AND

T. S. LIU
Department of Mechanical Engineering, National Chiao Tung University, Hsinchu 30010, Taiwan, R.O.C.

SUMMARY

Petri nets are useful for modelling a variety of asynchronous and concurrent systems, such as automated manufacturing, computer fault tolerant systems, and communication networks. This study employs an airbag inflator system as an example to demonstrate a Petri net approach to failure analysis. This paper uses Petri nets to study minimum cut sets finding, marking transfer, and dynamic behaviour of system failure. For Petri net models incorporating sensors, fault detection and higher-level fault avoidance is dealt with. Compared with fault trees that present only static logic relations between events, Petri nets indeed offer more capabilities in the scope of failure analysis. © 1997 by John Wiley & Sons, Ltd.

KEY WORDS: Petri nets; failure analysis; reliability; airbag inflator

INTRODUCTION

A failure is defined as any change in the shape, size, or material properties of a structure, machine, or component that renders it unfit to carry out its specified function adequately.[1] For the purpose of reliability assurance, failures of a system need to be traced and analysed, especially for safety devices such as airbag systems in vehicles.

There have been many methods proposed for failure analysis,[2] among which fault tree analysis (FTA) is well known. It is a graphical method that presents relationships between basic events and the top event by logic gates and a tree construction.[3] Compared with fault trees, Petri net analysis is also a graphical approach that performs not only the static logic relations revealed in FTA, but also dynamic behaviour which greatly helps fault tracing and failure state analysis. Moreover, the system behaviour accounted for by Petri nets can improve the dialogue between analysts and designers of a system.[4]

Nowadays, deaths and injuries resulting from the use of motor vehicles are at a terribly high level worldwide. Available statistics report that over 154,000 deaths and 5,000,000 injuries occur each year all over the world.[5] As a result, airbag systems used for passengers' protection are fitted on modern vehicles in rapidly increasing numbers.[6–12] An airbag system is also called a supplemental inflatable restraint[8] or supplemental restraint system[9] and is composed of three major subsystems: inflator and bag assembly, diagnostic module, and crash sensors.[10] The inflator and bag assembly is used to inflate an airbag so that the head and chest injury severity of occupants can be reduced under airbag protection[8,11] when an automotive collision occurs. The fault tree analysis for detecting possible failures of an inflator has been presented.[12] In this study, the proposed fault tree will be transformed to a Petri net model in order to illustrate the present failure analysis method and to show the superiority of Petri nets over fault trees.

The correlations between fault trees and Petri nets will be presented first in this study. Two methods for obtaining minimum cut sets then follow. The third issue is the discussion of marking transfer by using a reorganized incidence matrix. Dynamic behaviour of Petri nets with failure rates formulation will be investigated. Finally, Petri nets endowed with sensors for fault detection are described.

TRANSFORMATION BETWEEN FAULT TREE AND PETRI NET

The basic symbols of Petri nets include:[13]

○	: *Place*, drawn as a circle, denotes event
━	: *Transition*, drawn as a bar, denotes event transfer
↑	: *Arc*, drawn as an arrow, between places and transitions
●	: *Token*, drawn as a dot, contained in places, denotes the data.

The transition is said to fire if input places satisfy an enabled condition. Transition firing will remove one token from all of its input places and put one token into all of its output places.[14] Figure 1 is a fault tree example in which events A, B, C, D, and E are basic causes of event 0. The logic relations between the events are described as well. The corre-

CCC 0748–8017/97/030139–13 $17.50

Received 30 December 1996
Revised 5 March 1997

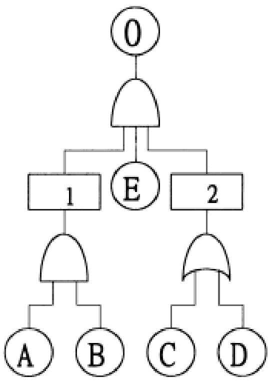


Figure 1. A fault tree

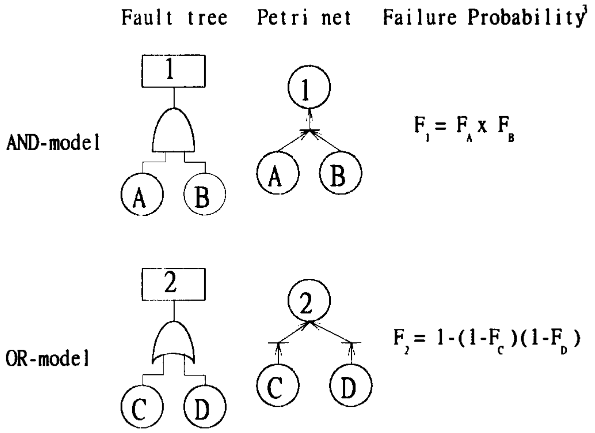


Figure 2. Correlations between fault tree and Petri net

lations between fault tree and Petri net are shown in Figure 2. Figure 3 is the Petri net transformed from Figure 1.

One potential problem in the deployment of an automobile airbag is an inadequate inflator system output that may be caused by delayed output, reduced output or no output, for which an inadequate inflator output in airbags has been investigated.[12] Figure 4 shows its proposed fault tree. As an illustrating example, based on the above statement, it can be tranformed into Petri net as shown in Figure 5. Its sequence numbers of places and transitions are prescribed, starting from basic events to the top event from the left side to the right side in the Petri net.

MINIMUM CUT SETS

There have been quite a few methods used to generate minimum cut sets for fault trees.[15–18] By contrast, a matrix method[2] for finding minimum cut sets based on Petri nets is carried out in the current study. The rules are stated as follows:

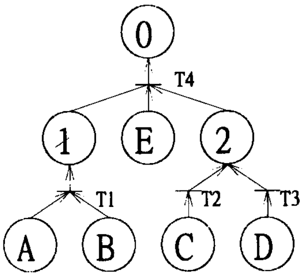


Figure 3. The Petri net of Figure 1

1. Put down the numbers of the input places in a row if the output place is connected by multi-arcs from transitions. This accounts for OR-models.
2. If the output place is connected by one arc from a transition then the numbers of the input places should be put down in a column. This accounts for AND-models.
3. The common entry located in rows is the entry shared by each row.
4. Starting from the top event down to the basic events until all places are replaced by basic events, a matrix is thus formed, called the basic event matrix. The column vectors of the matrix constitute cut sets.
5. Remove the supersets from the basic event matrix and the remaining column vectors become minimum cut sets.

This top-down fashion facilitates obtaining minimum cut sets logically. The differences between the present method and the MOCUS[19] algorithm include:

1. The present method is based on Petri net models, whereas the MOCUS algorithm is based on fault trees.
2. Events in fault trees correspond to places in Petri nets. Using Petri nets, logic gates do not appear in the matrix, in which only places are dealt with, whereas by MOCUS all logic gates in addition to events are processed in the generating steps.
3. The structure of the matrix looks like that of the Petri net itself such that it is amenable to constructing the matrix; however, tables composed of generating steps using MOCUS look unlike structures of fault trees.

Figure 6 illustrates minimum cut sets used to search the inadequate output for an inflator system, depicted in Figure 4, by the matrix method.

Minimum cut sets can be derived in an opposite direction, i.e. from basic places to the top place. Transitions with $T = 0$ are called immediate transitions.[14] If a Petri net has immediate transitions, i.e. the token transfer between places does not take time, then it can be abosrbed to a simplified form called the equivalent Petri net. Figure 7 shows the principle of absorption, by which Figure 8 is the equivalent Petri net resulting from Figure 5. After absorption, all the remaining places are basic events. The equivalent Petri net exactly constitutes the minimum cut sets, i.e. the input of each transition represents a minimum cut set. This method is in bottom-up fashion.

Therefore, both top-down and bottom-up methods have been proposed in this work to find minimum cut sets using the Petri net approach.

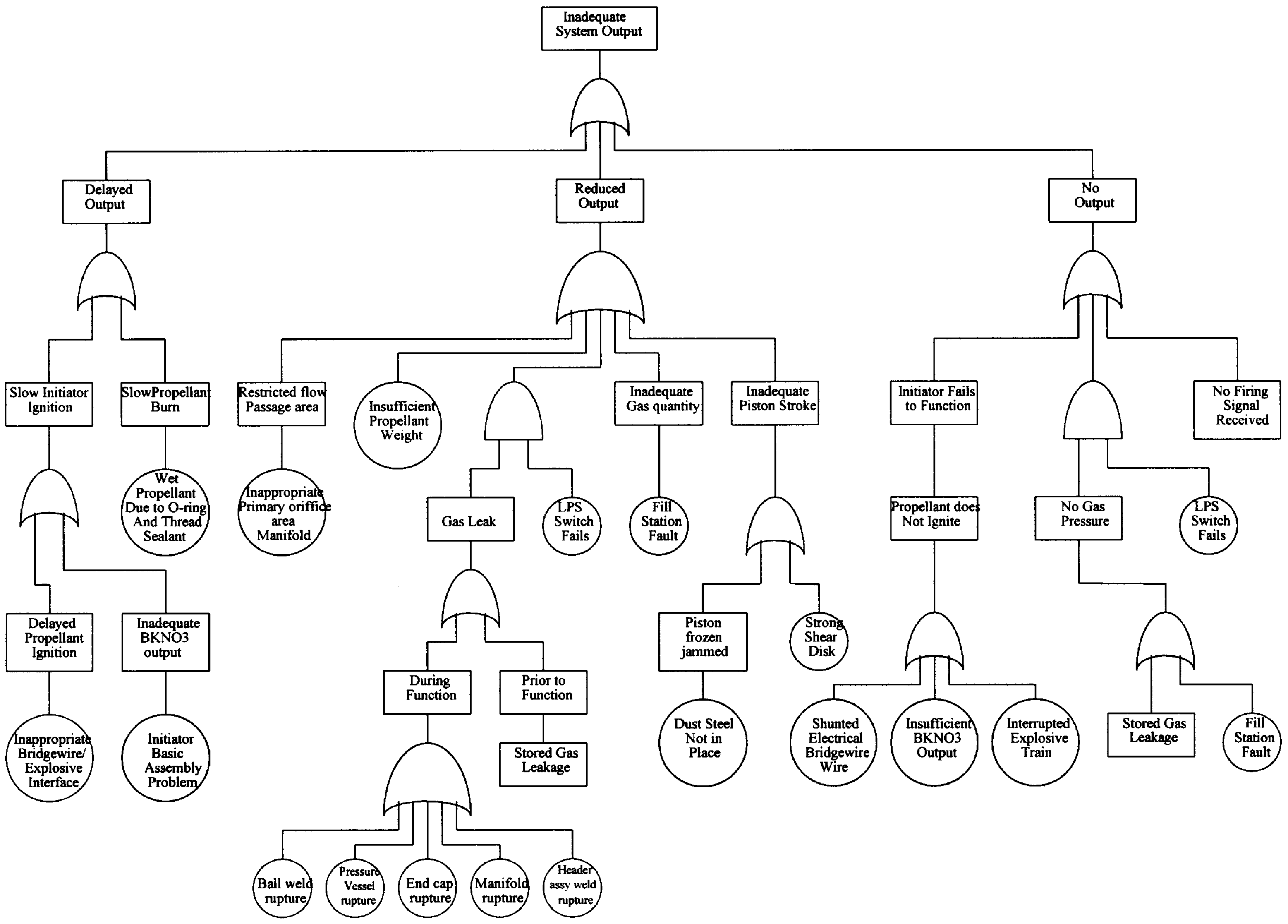


Figure 4. Fault tree analysis—inadequate system output

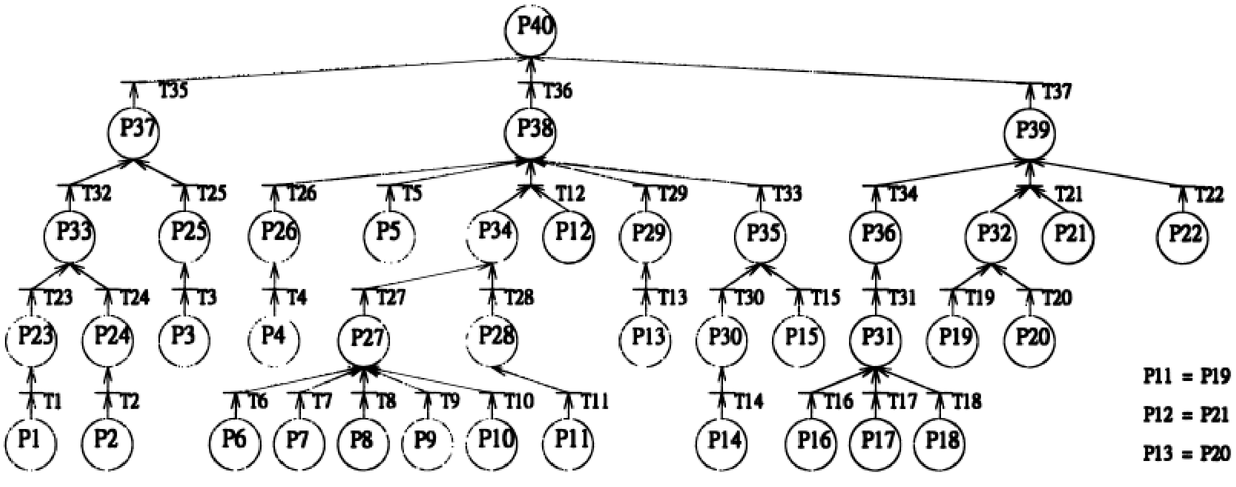
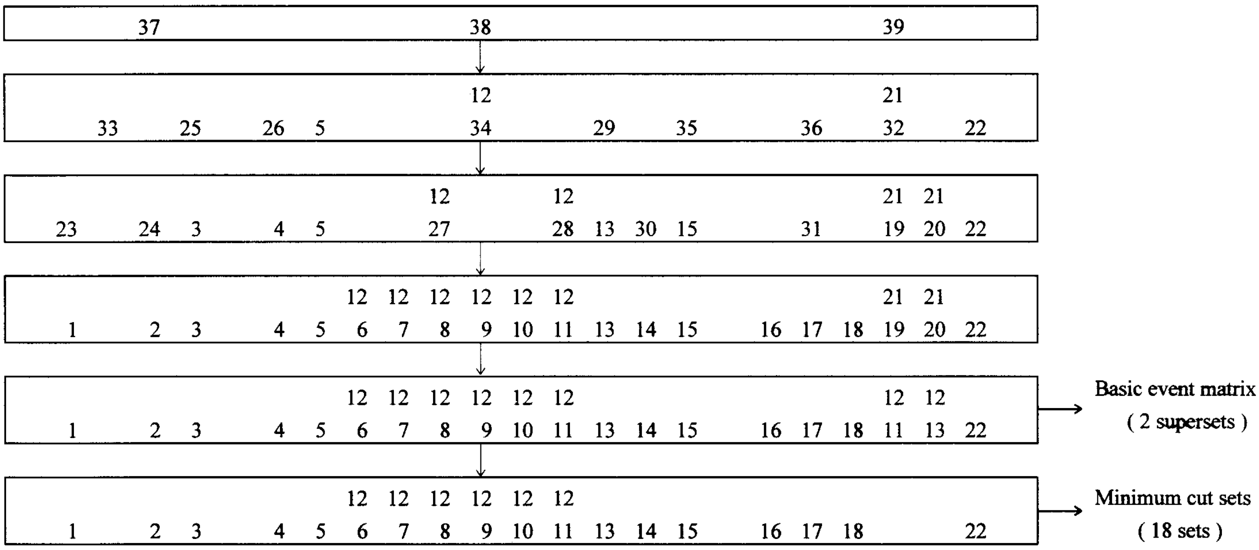


Figure 5. Petri net of an inadequate output inflator system


37 38 39

12 21
33 25 26 5 34 29 35 36 32 22

12 12 21 21
23 24 3 4 5 27 28 13 30 15 31 19 20 22

12 12 12 12 12 12 21 21
1 2 3 4 5 6 7 8 9 10 11 13 14 15 16 17 18 19 20 22

12 12 12 12 12 12 12 12
1 2 3 4 5 6 7 8 9 10 11 13 14 15 16 17 18 11 13 22

Basic event matrix
(2 supersets)

12 12 12 12 12 12
1 2 3 4 5 6 7 8 9 10 11 13 14 15 16 17 18 22

Minimum cut sets
(18 sets)

Figure 6. Minimum cut sets of an inadequate output inflator

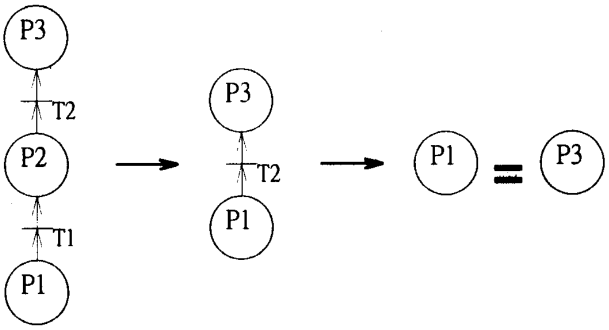


Figure 7. The absorption principle of equivalent Petri nets

MARKING TRANSFER

A marking of a Petri net is defined as the total number of tokens at each place,[20] denoted by a column vector $\mathbf{M}$. Thus the vector $\mathbf{M}_k = (n_1, n_2, \ldots, n_m)^T$ represents that token numbers of places $P_1, P_2, \ldots, P_m$ at state k are $n_1, n_2, \ldots, n_m$, respectively. Consequently, Petri nets can be expressed in state space form, which gives the next state $\mathbf{M}_{k+1}$ from its previous state $\mathbf{M}_k$:[13]

$$\mathbf{M}_{k+1} = \mathbf{A}\ \mathbf{M}_k + \mathbf{B}\ \mathbf{U}_k,\ k = 1,2,\ldots \tag{1}$$

where $\mathbf{M}_k$ is the marking at state k, an $m \times 1$ column vector, $\mathbf{U}_k$ is an input vector at state k, and $\mathbf{A}$ and $\mathbf{B}$ are coefficient matrices.

Combining all the marking transformation from an initial marking $\mathbf{M}_0$ to final marking $\mathbf{M}_n$, (1) can be rewritten as

$$\mathbf{M}_n = \mathbf{M}_0 + \mathbf{C}\ \boldsymbol{\Sigma} \tag{2}$$

or

$$\mathbf{M}_n - \mathbf{M}_0 = \mathbf{C}\ \boldsymbol{\Sigma} \tag{3}$$

where $\mathbf{C}$ is an $m \times n$ matrix called the incidence matrix, m and n being the total numbers of places and transitions, respectively. In addition, entries of $\mathbf{C}$ are

$c_{ij} = 1$, if transition j has an outgoing arc to place i
$c_{ij} = -1$, if transition j has an incoming arc from place i
$c_{ij} = 0$, if there is no arc between them

Moreover, $c_{ij} = 1$ (-1) means place i gains (loses) one token if transition j fired. In (3), $\boldsymbol{\Sigma}$ denotes a column vector, called the firing-count vector,[13] whose entry i denotes the number of times that

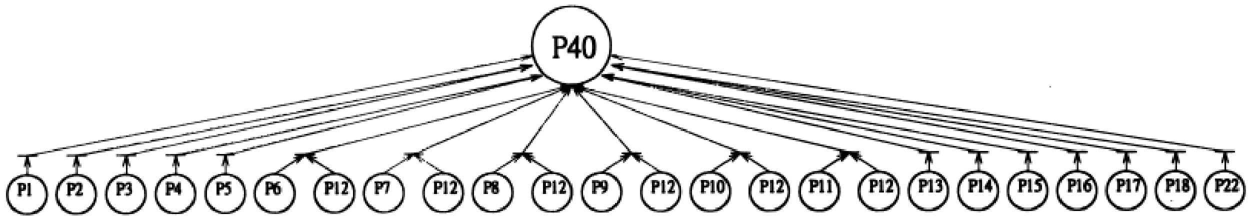


Figure 8. Equivalent Petri net of Figure 5

transition i fires in a firing sequence such that $\mathbf{M}_0$ is transformed into $\mathbf{M}_n$.

To renumber transitions, a method[2] is employed to establish a reorganized incidence matrix $\mathbf{C_R}$ that provides marking transfer steps from $\mathbf{M}_0$ up to $\mathbf{M}_n$. The rules for transition renumbering are:

1. Let the number assigned to each transition be the same number of the input place in this transition, no matter whether the input is multiple or not.
2. If the transition has multiple inputs, then the number of this transition includes every input number.

As a result, the renumbered Petri net for Figure 5 is shown in Figure 9.

The rules for constructing the reorganized incidence matrix are:

1. Assign each entry of the incidence matrix $\mathbf{C_R}$ in a manner similar to $\mathbf{C}$ as described previously, but append one column to $\mathbf{C_R}$. Accordingly, it becomes an $m \times m$ square matrix where m is the total number of places. Besides, let entry $\mathbf{C}_{\mathbf{R}m,m}$ be -1.
2. Underline all the entries that consititute multiple incoming transitions.

Once the reorganized incidence matrix is done, the upper-left $q \times q$ elements form a negative identity square matrix and there is a $q \times (m-q)$ null matrix at the upper-right, where q is the total number of basic places. The incidence matrix $\mathbf{C_R}$ resulting from Figure 9 is shown in Figure 10, where q is 22, m is 40 and $\mathbf{C}_{\mathbf{R}38,12}$, $\mathbf{C}_{\mathbf{R}38,34}$, $\mathbf{C}_{\mathbf{R}39,21}$ and $\mathbf{C}_{R39,32}$ are underlined.

Since the sequence numbers of places and transitions are the same, T_i may fire when P_i holds tokens. Suppose the initial marking for the inadequate output inflator (Figure 9) is

$$\mathbf{M}_0 = [0000010000010000000000000000000000000000]^{\mathrm{T}}$$

i.e. each of P_6 and P_{12} possesses a token, which from Figures 4 and 5 represent ball weld rupture and failure of the low pressure sensor (LPS) switch in the airbag inflator. Since P_6 holds a token, T_6 fires. Note that in the T_6 column in $\mathbf{C_R}$, only the entry $\mathbf{C}_{\mathbf{R}27,6} = 1$, which means that P_{27} gains a token when T_6 fires. Consequently, a token moves from P_6 to P_{27}. However, T_{12} will not fire, since the entry $\mathbf{C}_{\mathbf{R}38,12}$ is underlined, which means it cannot fire unless both P_{12} and P_{34} hold tokens at the same time. Thus, the marking becomes

$$\mathbf{M}_1 = [0000000000010000000000000010000000000000]^{\mathrm{T}}$$

In a similar manner, $\mathbf{C}_{\mathbf{R}34,27} = 1$, as shown in Figure 10, and T_{27} fires such that the token moves from P_{27} to P_{34}. Therefore,

$$\mathbf{M}_2 = [0000000000010000000000000000000001000000]^{\mathrm{T}}$$

Since $\mathbf{C}_{\mathbf{R}38,12} = \mathbf{C}_{\mathbf{R}38,34} = \underline{1}$ according to Figure 10 and both P_{12} and P_{34} hold a token, $T_{12}T_{34}$ fires so as to provide P_{38} a token. Accordingly,

$$\mathbf{M}_3 = [0000000000000000000000000000000000000100]^{\mathrm{T}}$$

Note that $\mathbf{C}_{\mathbf{R}40,38} = 1$ and T_{38} fires. A token hence moves to P_{40}, i.e. the top event of this airbag inflator system occurs, with marking

$$\mathbf{M}_4 = [0000000000000000000000000000000000000001]^{\mathrm{T}}$$

The associated reorganized incidence matrix $\mathbf{C_R}$ and

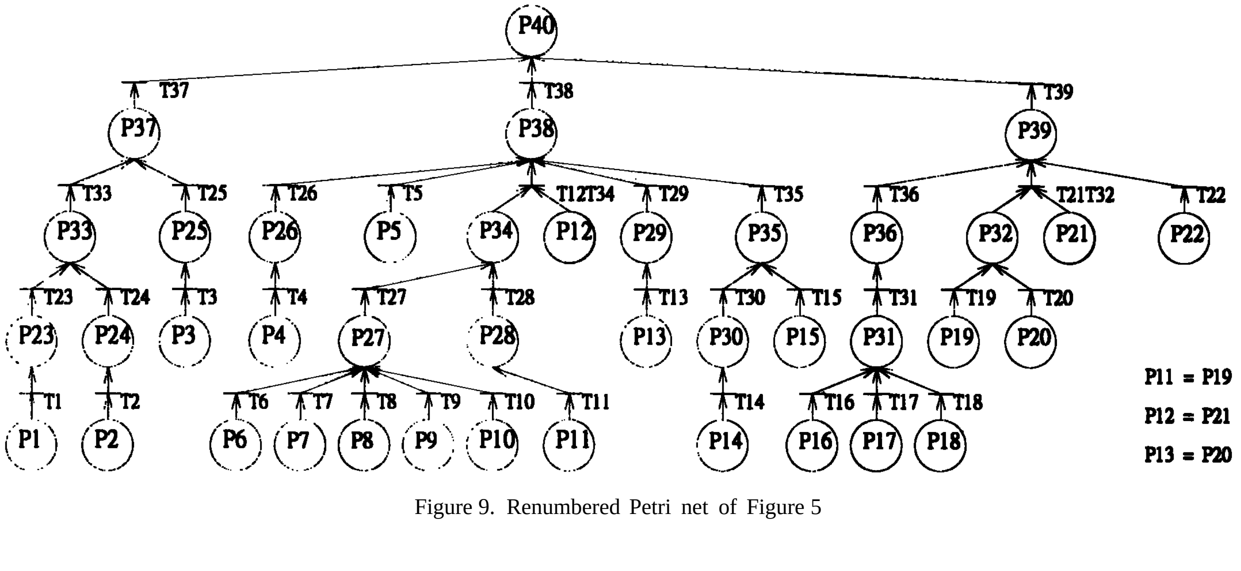


Figure 9. Renumbered Petri net of Figure 5

$$
\mathbf{C_R} = \begin{array}{c|cccccccccccccccccccccc|cccccccccccccccccc|}
T & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \\
\text{P1} \\
\vdots & \multicolumn{22}{c|}{-\mathbf{I}} & \multicolumn{18}{c|}{\mathbf{0}} \\
\text{P22} \\
\hline
\text{P23} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P24} & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P25} & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P26} & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P27} & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P28} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P29} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P30} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P31} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P32} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P33} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P34} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{P35} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
\text{P36} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
\text{P37} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
\text{P38} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \underline{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \underline{1} & 1 & 0 & 0 & -1 & 0 & 0 \\
\text{P39} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \underline{1} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \underline{1} & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\
\text{P40} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & -1
\end{array}
$$

$$\mathbf{M}_0 = [\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \mid 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ ]^T$$

$$\mathbf{M}_1 = [\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \mid 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ ]^T$$

$$\mathbf{M}_2 = [\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \mid 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ ]^T$$

$$\mathbf{M}_3 = [\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \mid 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ ]^T$$

$$\mathbf{M}_4 = [\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \mid 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ ]^T$$

Figure 10. Marking transfer steps $\mathbf{M}_0$ up to $\mathbf{M}_4$ observed from the reorganized incidence matrix $\mathbf{C_R}$

the marking transfer steps based on the reorganized incidence matrix are illustrated in Figure 10. This method enables deriving marking transfer by direct observation without calculation, which is different from (2) and (3) that were proposed by Hura and Atwood.[13] Failure state evolution can be observed, as illustrated in the inflator example. This is one of the advantages for failure analysis of using the Petri net approach.

DYNAMIC BEHAVIOUR

Since the vector $\mathbf{M}_k$ represents the marking in a Petri net at state k, the failure state of a system may vary with time. Hence, the markings of a Petri net depend on time dynamically. The dynamic behaviour of system failure is defined as the system failure state with time varied, and is determined by the movement of tokens in a Petri net model. A merit of the approach is that the dynamic behaviour of a system failure can be investigated by Petri nets,[20] whereas it cannot be done by fault trees. Define $m_i(t)$ as the marking of P_i, i.e. the token quantity at time t for place i, and assume that a basic place generates a token at every time period of T, i.e. the time between failures is T. Accordingly, the timed marking of P_i performs like a stair function. It is equal to zero during the first period, one during the second period, two during the third period, etc. Hence, a timed marking for a place can be written as[21]

$$m(t) = 0[u(t)-u(t-T)] + 1[u(t-T)-u(t-2T)]$$

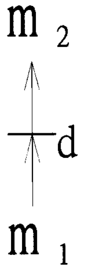


Figure 11. Single transition with single input

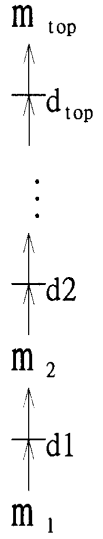


Figure 12. Hierarchial transition with single input

$$+\ 2[u(t–2T)–u(t–3T)] + \ldots = u(t–T)$$

$$+\ u(t–2T) + u(t–3T) + \ldots \qquad (4)$$

$$= \sum_{k=1}^{\infty} u(t–kT)$$

where $u(t)$ is a unit step function.

The timed marking transfer of places can be described as follows:

1. *Transition with single input*

In this case, the marking for an output place is the input marking with delay time d involved.

(*A*) *Single transition* (*Figure* 11). According to (4), let

$$m_1(t) = \sum_{k=1}^{\infty} u(t–kT) \qquad (5)$$

Hence,

$$m_2(t) = m_1(t)_d = \sum_{k=1}^{\infty} u(t–kT–d) \qquad (6)$$

where d denotes the delay time due to transition.

(*B*) *Hierarchial transition* (*Figure* 12). The marking of the top place in this construction is derived as

$$m_{\text{top}}(t) = m_1(t)_{d_1,d_2,\ldots,d_{\text{top}}}$$

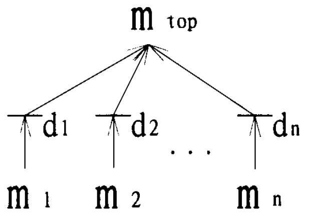


Figure 13. Single level transition with multi-inputs for the OR-model

$$= \sum_{k=1}^{\infty} u(t–kT–d_1–d_2–\ldots–d_{\text{top}})$$

$$= \sum_{k=1}^{\infty} u(t–kT–D) \qquad (7)$$

where $D = \sum_{s=1}^{\text{top}} d_s$ denotes the total delay time due to transitions.

2. *Transition with multi-inputs*

(*A*) *OR-model*. According to the property of Petri nets,[21] the output marking of an OR-model is the summation of input markings with delay times; i.e.

$$m_{\text{top}}(t) = [m_1(t)_{d_1} + m_2(t)_{d_2} + \ldots m_n(t)_{d_n}] \quad (8)$$

(a) Single level transition (Figure 13)

From (4), let basic place markings be

$$m_1(\text{t}) = \sum_{k=1}^{\infty} u(t–kr_1T)$$

$$m_2(\text{t}) = \sum_{k=1}^{\infty} u(t–kr_2T)$$

$$\ldots$$

$$m_n(\text{t}) = \sum_{k=1}^{\infty} u(t–kr_nT) \qquad (9)$$

where r_1 to r_n denote factors to account for different periods among events. Hence r_iT, $i = 1,2,3,\ldots,n$, represent the token generation period at place P_i. Substituting (9) into (8) yields the top place marking

$$m_{\text{top}}(t) = \sum_{k=1}^{\infty} u(t–kr_1T–d_1) + \sum_{k=1}^{\infty} u(t–kr_2T–d_2)$$

$$+ \ldots + \sum_{k=1}^{\infty} u(t–kr_nT–d_n) \qquad (10)$$

$$= \sum_{s=1}^{n} [\sum_{k=1}^{\infty} u(t–kr_sT–d_s)]$$

(b) Hierarchical transition (Figure 14)

From (8) and in accordance with Figure 14,

$$m_{\text{top}}(\text{t}) = [\ldots(\{[m_1(t)_{d_1} + m_2(t)_{d_2}]_{d_3} + m_4(t)_{d_4}\}_{d_5}$$

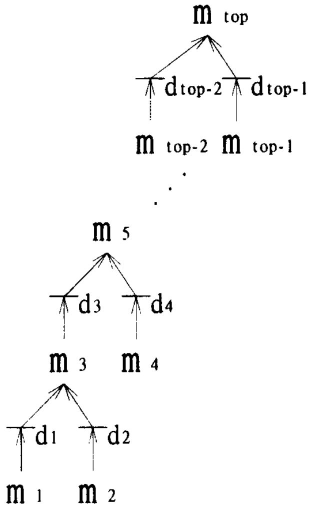


Figure 14. Hierarchical transition with multi-inputs for the OR-model

$$+ m_6(t)_{d_6})_{d_7} +\ldots+ m_{\text{top-3}}(t)_{d_{\text{top-3}}}]_{d_{\text{top-2}}} + m_{\text{top-1}}(t)_{d_{top\text{-}1}}$$

$$= [\ldots(\{[\sum_{k=1}^{\infty} u(t{-}kr_1T{-}d_1) + \sum_{k=1}^{\infty} u(t{-}kr_2T{-}d_2)]_{d_3}$$

$$+ \sum_{k=1}^{\infty} u(t{-}kr_4T{-}d_4)\}_{d_5} + \sum_{k=1}^{\infty} u(t{-}kr_6T{-}d_6))_{d_7}$$

$$+\ldots+ \sum_{k=1}^{\infty} u(t{-}kr_{\text{top-3}}T{-}d_{\text{top-3}})]_{d_{top\text{-}2}}$$

$$+ \sum_{k=1}^{\infty} u(t{-}kr_{top\text{-}1}T{-}d_{\text{top-1}})$$

$$= \sum_{k=1}^{\infty} u(t{-}kr_1T{-}d_1{-}d_3{-}d_5{-}\ldots{-}d_{\text{top-2}})$$

$$+ \sum_{k=1}^{\infty} u(t{-}kr_2T{-}d_2{-}d_3{-}d_5{-}\ldots{-}d_{\text{top-2}})$$

$$+ \sum_{k=1}^{\infty} u(t{-}kr_4T{-}d_4{-}d_5{-}d_7{-}\ldots{-}d_{\text{top-2}})$$

$$+ \sum_{k=1}^{\infty} u(t{-}kr_6T{-}d_6{-}d_7{-}d_9{-}\ldots d_{\text{top-2}})$$

$$+\ldots+ \sum_{k=1}^{\infty} u(t{-}kr_{\text{top-3}}T{-}d_{\text{top-3}}{-}d_{\text{top-2}})$$

$$+ \sum_{k=1}^{\infty} u(t{-}kr_{\text{top-1}}T{-}d_{\text{top-1}}) = \sum_{k=1}^{\infty} u(t{-}kr_1T{-}\sum_{s=1}^{R} d_{2s-1}) \quad (11)$$

$$+ \sum_{s=1}^{R-1} [\sum_{k=1}^{\infty} u(t{-}kr_{2s}T{-}d_{2s}{-}\sum_{u=s}^{R-1} d_{2u+1})]$$

$$+ \sum_{k=1}^{\infty} u(t{-}kr_{\text{top-1}}T{-}d_{\text{top-1}})$$

where $R = [(\text{top-2}) + 1]/2$

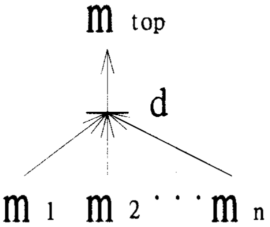


Figure 15. Single transition with multi-inputs for the AND-model

(*B*) *AND-model.* The output marking of an AND-model is the minimal number among input markings[21] with time delay; i.e.

$$m_{\text{top}}(t) = \min\,[m_1(t)_d,\ m_2(t)_d, \ldots\ .\ m_n(t)_d] \quad (12)$$

(a) Single transition (Figure 15)

From (9) and (12), the top place marking of Figure 15 is

$$m_{\text{top}}(t) = \min[\sum_{k=1}^{\infty} u(t{-}kr_1T{-}d),$$

$$\sum_{k=1}^{\infty} u(t{-}kr_2T{-}d), \ldots, \sum_{k=1}^{\infty} u(t{-}kr_nT{-}d)]$$

$$= \min\,[\sum_{k=1}^{\infty} u(t{-}kr_iT{-}d)],\ (\text{i} = 1,2,3,\ldots,n) \quad (13)$$

$$= \sum_{k=1}^{\infty} u(t{-}kr_{\text{b}}T{-}d)$$

where r_{b} is the largest number of all r_i. In other words, the token generation period of P_{b} is the longest one among all input places.

(b) Hierarchical transition (Figure 16)

From (12) and Figure 16, the top place marking of this construction is expressed by

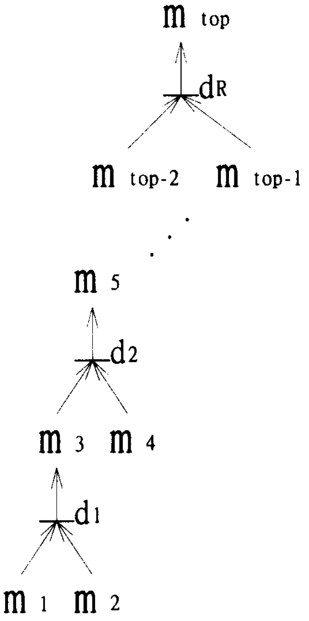


Figure 16. Hierarchical transition with multi-inputs for the AND-model

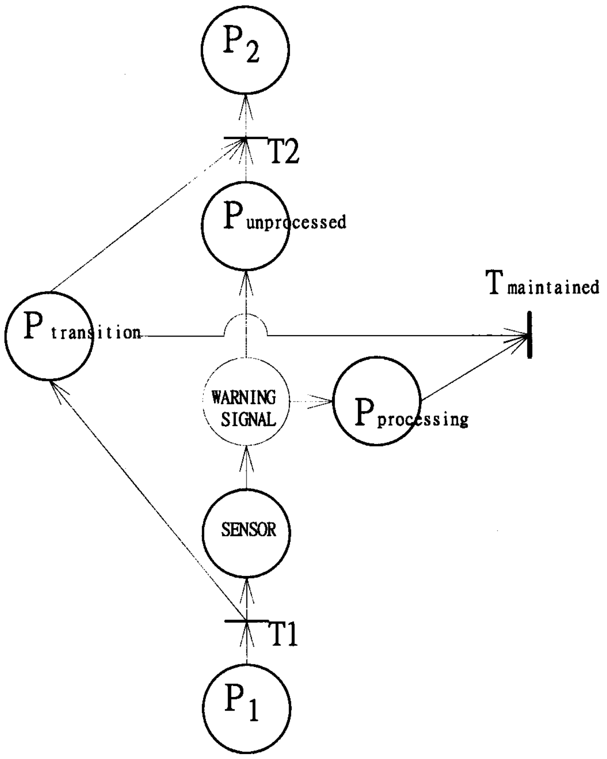


Figure 17. Fault detection arrangement

$$
\begin{aligned}
m_{\text{top}}(t) &= \min\,([\,.\,.\,.\min\,\{[\min\,(\{\min\\
&[m_1(t)_{d_1},\, m_2(t)_{d_1}]\}_{d_2},\, m_4(t)_{d_2})]_{d_3},\\
&m_6(t)_{d_3}\}_{d_4}\,.\,.\,.\,]_{d_R},\, m_{\text{top-1}}(t)_{d_R})\\
&= \min\,[\sum_{k=1}^{\infty} u(t-kr_1T-d_1-d_2-.\,.\,.-d_R),\\
&\sum_{k=1}^{\infty} u(t-kr_2T-d_1-d_2-.\,.\,.-d_R),\\
&\sum_{k=1}^{\infty} u(t-kr_4T-d_2-d_3-.\,.\,.-d_R),\\
&\sum_{k=1}^{\infty} u(t-kr_6T-d_3-d_4-.\,.\,.-d_R),\\
&\sum_{k=1}^{\infty} u(t-kr_8T-d_4-d_5-.\,.\,.-d_R),\,.\,.\,.,\\
&\sum_{k=1}^{\infty} u(t-kr_{\text{top-1}}T-d_R)] \qquad (14)\\
&= \min\,[\sum_{k=1}^{\infty} u(t-kr_1T-\sum_{s=1}^{R} d_s),\\
&\sum_{k=1}^{\infty} u(t-kr_2T-\sum_{s=1}^{R} d_s),\\
&\sum_{k=1}^{\infty} u(t-kr_{2v}T-\sum_{s=v}^{R} d_s)],\ (v = 2,3,4,.\,.\,.,R)
\end{aligned}
$$

Based on (4) to (14), the marking transfer for inadequate system output of the inflator, as depicted in Figure 9, can be derived as follows:

First from (8), one has marking for place 37 of the form

$$m_{37}(t) = m_{33}(t)_{d_{33}} + m_{25}(t)_{d_{25}}$$

From (8) and (6) this equation becomes

$$
\begin{aligned}
m_{37}(t) &= [m_{23}(t)_{d_{23}} + m_{24}(t)_{d_{24}}]_{d_{33}}\\
&+ m_3(t)_{d_3,d_{25}} = [m_1(t)_{d_1,d_{23}}\\
&+ m_2(t)_{d_2,d_{24}}]_{d_{33}} + m_3(t)_{d_3,d_{25}}
\end{aligned}
$$

Finally, employing (7) that deals with delay time at transitions leads to

$$m_{37}(t) = m_1(t)_{d_1,d_{23},d_{33}} + m_2(t)_{d_2,d_{24},d_{33}} + m_3(t)_{d_3,d_{25}} \qquad (15)$$

In a similar fashion,

$$
\begin{aligned}
m_{38}(t) &= m_{26}(t)_{d_{26}} + m_5(t)_{d_5} + \min\\
&[m_{34}(t)_{d_{34}},\, m_{12}(t)_{d_{12}}] + m_{29}(t)_{d_{29}} + m_{35}(t)_{d_{35}}\\
&= m_4(t)_{d_4,d_{26}} + m_5(t)_{d_5} + \min\ (\{[m_6(t)_{d_6,d_{27},d_{34}}\\
&+ m_7(t)_{d_7,d_{27},d_{34}} + m_8(t)_{d_8,d_{27},d_{34}}\\
&+ m_9(t)_{d_9,d_{27},d_{34}} + m_{10}(t)_{d_{10},d_{27},d_{34}}] \qquad (16)\\
&+ [m_{11}(t)_{d_{11},d_{28},d_{34}}]\},m_{12}(t)_{d_{12}})\\
&+ m_{13}(t)_{d_{13},d_{29}} + m_{14}(t)_{d_{14},d_{30},d_{35}} + m_{15}(t)_{d_{15},d_{35}}
\end{aligned}
$$

Besides,

$$
\begin{aligned}
m_{39}(t) &= m_{36}(t)_{d_{36}} + \min\,[m_{32}(t)_{d_{32}},\, m_{21}(t)_{d_{21}}]\\
&+ m_{22}(t)_{d_{22}} = m_{16}(t)_{d_{16},d_{31},d_{36}} + m_{17}(t)_{d_{17},d_{31},d_{36}}\\
&+ m_{18}(t)_{d_{18},d_{31},d_{36}} + \min\,\{[m_{19}(t)_{d_{19},d_{32}} \qquad (17)\\
&+ m_{20}(t)_{d_{20},d_{32}}],\, [m_{21}(t)_{d_{21}}]\} + m_{22}(t)_{d_{22}}
\end{aligned}
$$

As a consequence, the marking of the top place is written as

$$
\begin{aligned}
m_{40}(t) &= m_{37}(t)_{d_{37}} + m_{38}(t)_{d_{38}} + m_{39}(t)_{d_{39}}\\
&= \sum_{k=1}^{\infty} u(t-kr_1T-d_1-d_{23}-d_{33}-d_{37})\\
&+ \sum_{k=1}^{\infty} u(t-kr_2T-d_2-d_{24}-d_{33}-d_{37})\\
&+ \sum_{k=1}^{\infty} u(t-kr_3T-d_3-d_{25}-d_{37})\\
&+ \sum_{k=1}^{\infty} u(t-kr_4T-d_4-d_{26}-d_{38})\\
&+ \sum_{k=1}^{\infty} u(t-kr_5T-d_5-d_{38})\\
&+ \min\,(\{\sum_{s=6}^{10} [\sum_{k=1}^{\infty} u(t-kr_sT-d_s-d_{27}-d_{34}-d_{38})]\\
&+ \sum_{k=1}^{\infty} u(t-kr_{11}T-d_{11}-d_{28}-d_{34}-d_{38})\},\\
&\sum_{k=1}^{\infty} u(t-kr_{12}T-d_{12}d_{38}))
\end{aligned}
$$

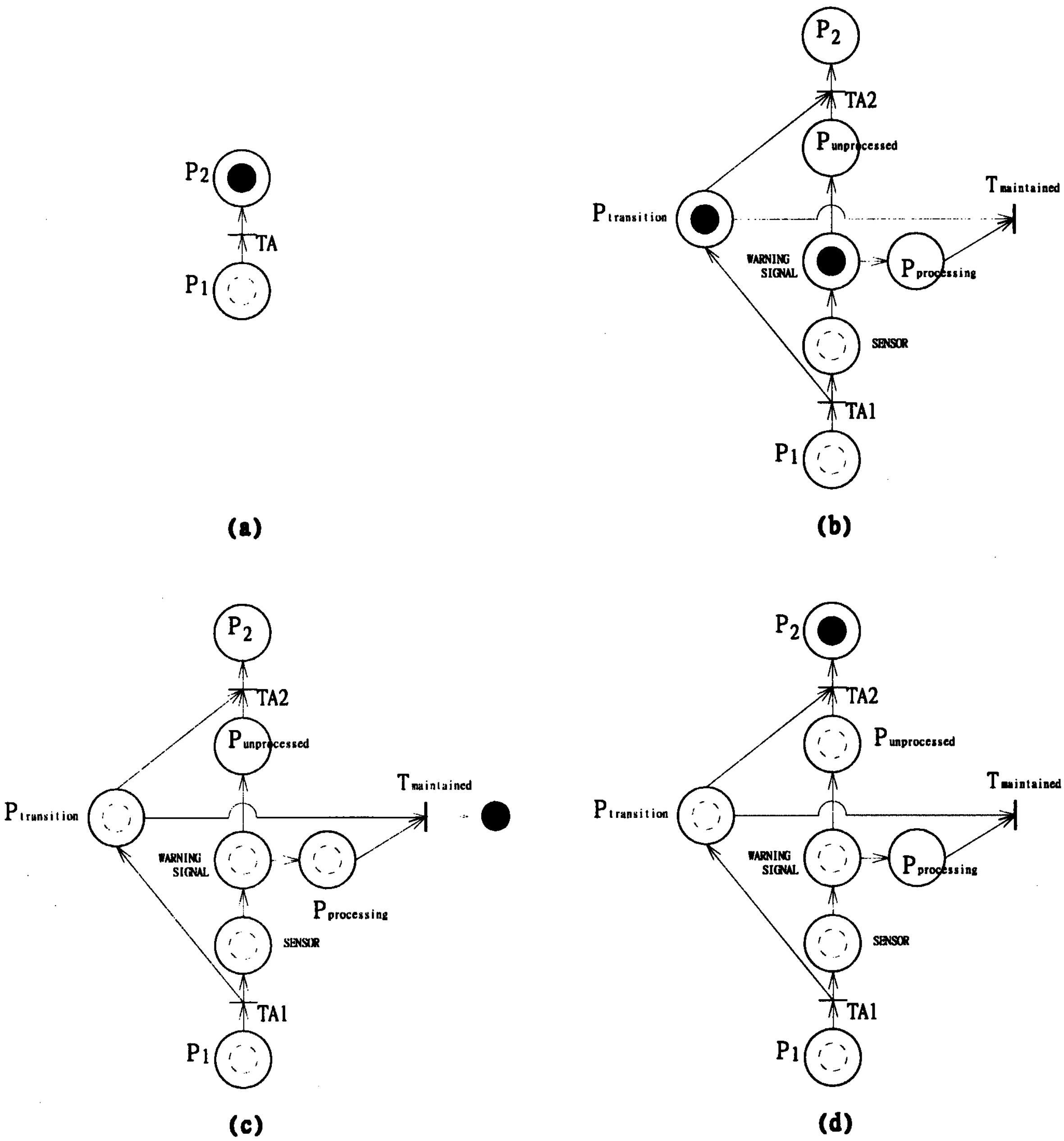


Figure 18. Token transfer in different situations

$$
\begin{aligned}
&+\sum_{k=1}^{\infty} u(t-kr_{13}T-d_{13}-d_{29}-d_{38})\\
&+\sum_{k=1}^{\infty} u(t-kr_{14}T-d_{14}-d_{30}-d_{35}-d_{38})\\
&+\sum_{k=1}^{\infty} u(t-kr_{15}T-d_{15}-d_{35}-d_{38}) \qquad (18)\\
&+\sum_{s=16}^{18} [\sum_{k=1}^{\infty} u(t-kr_{s}T-d_{s}-d_{31}-d_{36}-d_{39})]\\
&+\min\{\sum_{s=19}^{20} [\sum_{k=1}^{\infty} u(t-kr_{s}T-d_{s}-d_{32}-d_{39})],\\
&\sum_{k=1}^{\infty} u(t-kr_{21}T-d_{21}-d_{39})\}\\
&+\sum_{k=1}^{\infty} u(t-kr_{22}T-d_{22}-d_{39})
\end{aligned}
$$

Moreover, the failure rate[22] $F(t)$ of this system can be written as

$$F(t) = m_{40}(t)/t \qquad (19)$$

Failure rates derivation using the marking transfer calculation has been illustrated. Since the dynamic behaviour of a system failure can be investigated by Petri nets,[20] whereas it cannot be done by fault trees, it is also one of the advantages for failure analysis gained from the Petri net approach over FTA.

FAULT DETECTION AND REPAIR RATE

Once a token appears in a place of a Petri net, it represents that failure occurs in the system. If failure can be detected by sensors and properly processed in the early stage, the undesired and more serious faults of the system can be avoided. Therefore, sensors play an important role in fault detection. By suitable selection and proper installation, sensors

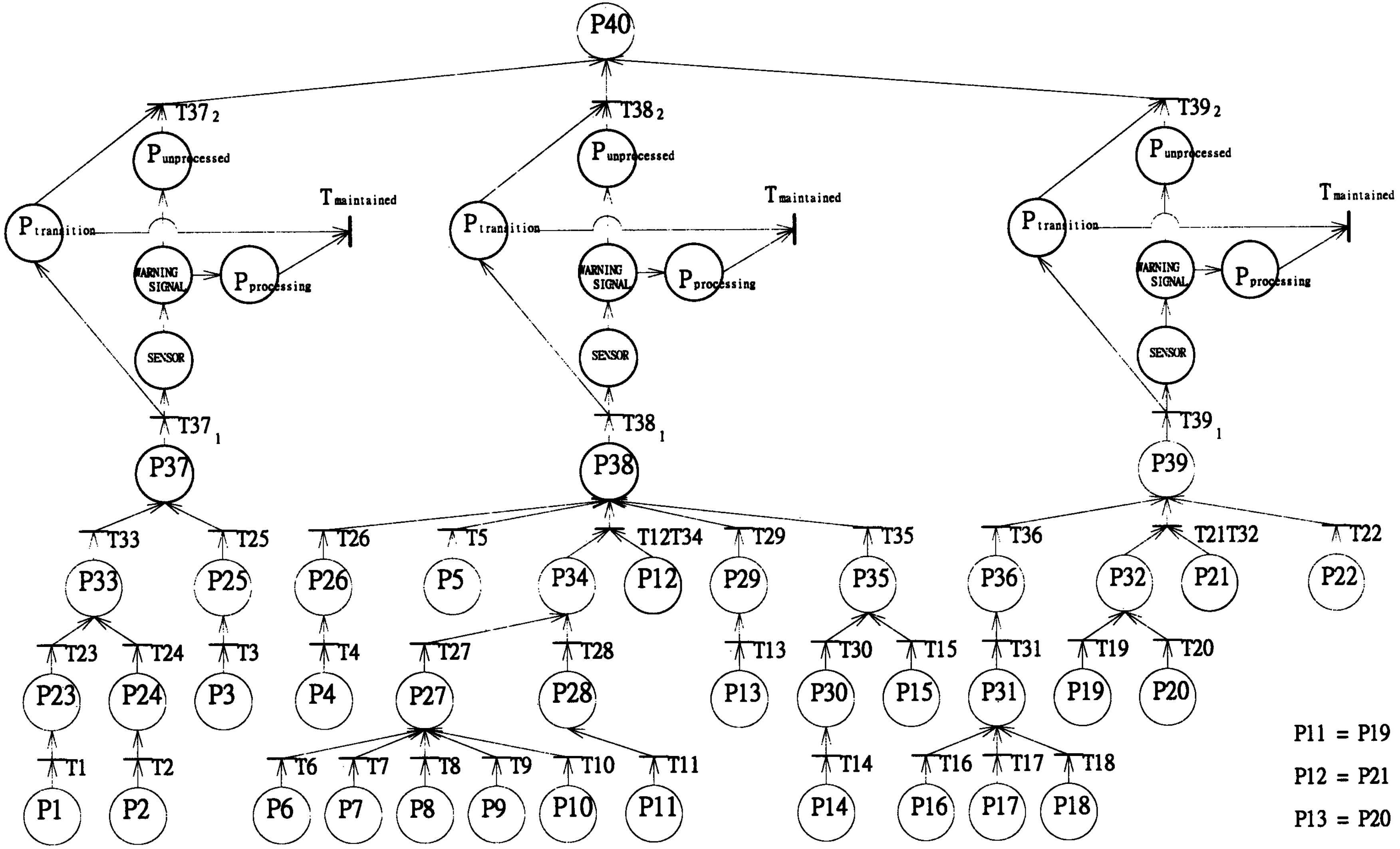


Figure 19. Fault detection arrangement for an inadequate output inflator system

offer a warning signal that may be a light indication,[8] a beep sound or some other form to remind that this situation be processed. The subsequent action may be either repair or replacement of faulty components. Since the dynamic characteristcs of a system failure can be observed by tracing token transfer,[20] the current study proposes an arrangement, with a concept of conditional transition as shown in Figure 17, which is endowed with sensors to achieve fault detection and higher-level fault avoidance. In this arrangement, $P_{\text{transition}}$ represents a transitional state inserted between P_1 and P_2, which is the original path from P_1 to P_2 without sensors installed, and its duration is T_1 plus T_2. Figure 18(a) shows a Petri net where if P_1 holds a token, i.e. P_1 failure occurs, P_2 will take place through the transition TA which represents the transitional time between P_1 and P_2 failures. However, in the fault detection arrangement depicted in Figure 18(b), P_1 failure fires TA1 to put a token into a transitional place that represents the transitional state. In addition, a token is put into the detection sensor that enables the warning signal, i.e. P_1 fault is detected. As soon as a processing action is taken, the token in the processing place that comes from the detection sensor together with the token in the transitional place will leave the Petri net through a transition that accounts for maintenance, such that a higher-level fault, i.e. P$_2$ failure, is avoided, as depicted in Figure 18(c). By contrast, if the warning signal is ignored, as shown in Figure 18(d), the token in the detection sensor, after moving to the unprocessed place, together with the token in the transitional place will enable transition TA2 to fire. Consequently, P_2 failure occurs.

Petri net models enable designers to determine where sensors should be installed in order to obtain warning signals from adequate places. Figure 19 shows the Petri net for an inadequate output in an inflator system with fault detection sensors. The fault detection arrangement can be installed at any, or all if necessary, locations between basic places and the top place. The failure rates of P_{37}, P_{38}, and P_{39} depend on $m_{37}(t)$, $m_{38}(t)$, and $m_{39}(t)$, depicted in (15), (16), and (17), respectively, i.e.

$$F_{37}(t) = m_{37}(t)/t$$
$$F_{38}(t) = m_{38}(t)/t$$
$$F_{39}(t) = m_{39}(t)/t \qquad (20)$$

If repair rates of P_{37}, P_{38}, and P_{39} are greater than $F_{37}(t)$, $F_{38}(t)$, and $F_{39}(t)$, respectively, the top place P_{40} will never happen.

CONCLUSIONS

This paper has presented failure analysis for an airbag inflator system by using Petri nets. Once the Petri net dealing with system failure is established, the associated minimum cut sets can be constructed either by the present matrix method or equivalent Petri nets. Renumbering transitions of a Petri net generates an incidence matrix which directly provides marking transfer without calculation. Dynamic behaviour of a timed Petri net has been investigated as well, from which the token transfer for various constructions of Petri nets and their failure rates can be derived. In addition, the scheme that avoids higher-level faults by incorporating sensors into a Petri net has been described in this study. All the above methods have been applied to an airbag inflator system, with inadequate output as the top event.

The transformation between fault trees and Petri nets is always achievable. However, in contrast to fault trees that only present static logic relations between events, the Petri net approach not only contains the capability of FTA, but also facilitates direct observation of marking transfer, analysing dynamic behaviour of system failure, fault detection arrangements, and repair rate calculations for failure analysis. It is worth constructing Petri net models rather than establishing fault trees at the outset of system failure analysis in order to gain the above-mentioned advantages.

REFERENCES

1. B. S. Dhillon, *Mechanical Reliability: Theory, Models and Applications*, AIAA Education Series, Washington DC, 1988.
2. S. B. Chiou, 'Failure analysis in reliability engineering using Petri nets', *MS Thesis*, National Chiao Tung University, Taiwan, Republic of China, 1995.
3. Patrick D. T. O'Connor, David Newton and Richard Bromley, *Practical Reliability Engineering*, Wiley, Chichester, England, 1995.
4. J.-F. Ereau and M. Saleman, 'Modeling and simulation of a satellite constellation based on Petri nets', *Proceedings of the Annual Reliability and Maintainability Symposium*, IEEE, 1996, pp. 66–72.
5. H. W. Mathews, Jr. 'Global outlook of safety and security systems in passenger cars and light trucks', *Proceedings of the International Congress on Transportation Electronics, Vehicle Electronics, Meeting Society's Needs: Energy, Environment, Safety*, Dearborn, 1992, pp. 71–93.
6. M. Ostertag, E. Nock and U. Kiencke, 'Optimization of airbag release algorithms using evolutionary strategies', *Proceedings of the 4th IEEE Conference on Control Applications*, 1995, pp. 275–280.
7. T. D. Hendrix, J. P. Kelley and W. L. Piper, 'Mechanical versus accelerometer based sensing for supplemental inflatable restraint systems', *Proceedings of the International Congress on Transportation Electronics, Vehicle Electronics, Meeting Society's Needs: Energy, Environment, Safety*, 1990, pp. 13–22.
8. D. Bergfried, W. Nitschke and M. Rutz. 'Airbag control modules—performance and reliability', *Proceedings of the International Congress on Transportation Electronics, Vehicle Electronics, Meeting Society's Needs: Energy, Environment, Safety*, Dearborn, 1992, pp. 155–162.
9. K. H. Yang, B. K. Latouf and A. I. King, 'Computer simulation of occupant neck response to airbag deployment in frontal impacts', *Journal of Biomechanical Engineering*, **114**, (3), 327–331 (1992).
10. S. Goch, T. Krause and A. Gillespie, 'Inflatable restraint system design considerations', *Proceedings of the International Congress on Transportation Electronics, Vehicle Electronics, Meeting Society's Needs: Energy, Environment, Safety*, 1990, p. 23–43.
11. S. M. Mahmud and A. I. Alrabady, 'A new decision making algorithm for airbag control', *IEEE Transactions on Vehicular Technology*, **44**, (3), 690–697 (1995).
12. Sheng-Hsien Teng and Shin-Yann Ho, 'Reliability analysis

for the design of an inflator', *Quality and Reliability Engineering International*, **11**, 203–214 (1995).

13. G. S. Hura and J. W. Atwood, 'The use of Petri nets to analyze coherent fault trees', *IEEE Transactions on Reliability*, **37**, (5), 469–474 (1988).
14. W. G. Schneeweiss, 'Mean time to first failure of repairable systems with one cold spare', *IEEE Transactions on Reliability*, **44**, (4), 567–574 (1995).
15. K. Dimitri, *Reliability Engineering Handbook, Vol. 2*, Prentice-Hall, Englewood Cliffs, New Jersey, 1991.
16. J. B. Fussell and W. E. Vesely, 'A new methodology for obtaining cut sets for fault trees', *Transactions of American Nuclear Society*, **15**, 262–263 (1972).
17. L. Rosenberg, 'Algorithm for finding minimal cut sets in a fault tree', *Reliability Engineering and System Safety*, **53**, 67–71 (1996).
18. J. D. Andrews and T. R. Moss, *Reliability and Risk Assessment*, Longmans, 1993.
19. J. B. Fussell, E. B. Henry and N. H. Marshall, 'Mocus—a computer program to obtain minimal cut sets from faulty tree', *ANCR*-1156, 1974.
20. M. Malhotra and K. S. Trivedi, 'Dependability modeling using Petri-nets', *IEEE Transactions on Reliability*, **44**, (3), 428–440 (1995).
21. J. L. Peterson, *Petri Net Theory and the Modeling of Systems*, Prentice-Hall, Englewood Cliffs, New Jersey, 1981.
22. K. C. Kapur and L. R. Lamberson, *Reliability in Engineering Design*, Wiley, New York, 1977.

Author's biographies:

S. K. Yang was born in Taiwan. He received his BS and MS in automatic control engineering from Feng Chia University, Taiwan in 1982 and 1985, respectively. From 1985 to 1991 he was an assistant researcher and system engineer of the Flight Test group, Aeronautic Research Laboratory, Chong Shan Institute of Science and Technology, Taiwan. Since 1991, he has been an instructor in the Department of Mechanical Engineering at Chin Yi Institute of Technology, Taiwan. Since 1994 he has been a Ph.D. student majoring in Mechanical Engineering at National Chiao Tung University, Taiwan. His research interests are in reliability, data acquisition and automatic control.

T. S. Liu received the BS from National Taiwan University in 1979 and the MS and Ph.D. from the University of Iowa, U.S.A. in 1982 and 1986, respectively, all in mechanical engineering. Since 1987, he has been with National Chiao Tung University, Taiwan where he is currently Professor. From 1991 to 1992 he was a visiting researcher in the Institute of Precision Engineering, Tokyo Institute of Technology, Japan. His current research interests include reliability, design, and motion control.