Journal of Universal Computer Science, vol. 13, no. 2 (2007), 224-243
submitted: 31/7/06, accepted: 15/1/07, appeared: 28/2/07 © *J.UCS*

Using Place Invariants and Test Point Placement to Isolate Faults in Discrete Event Systems

Iwan Tabakow
(Wroclaw University of Technology, Poland
iwan.tabakow@pwr.wroc.pl)

Abstract: This paper describes a method of using Petri net P-invariants in system diagnosis. To model this process a net oriented fault classification is presented. Hence, the considered discrete event system is modelled by a live, bounded, and reversible place-transition Petri net. The notions of D-partition of the set of places P of a given place-transition net N and net k-distinguishability are first introduced. Next these two notions are extended to the set of all vertices, i.e. places and transitions of N. So the problem of fault identification of the vertices of N is transformed as a problem of fault identification of the places of a new net N´ called a net simulator of N . Any transition in N´ is assumed to be fault-free. Then the corresponding net place invariants are computed. The system k-distinguishability measure is obtained in a unique way from the place-invariant matrix. For a large value of k, the system model is extended by using some set of additional places called test points and at the same time preserving the original net properties. To obtain a 1-distinguishable net the notion of a marked graph component is used. It is shown a sufficient condition for 1-distinguishability of an arbitrary place-transition net and a corresponding algorithm is presented. Next two different diagnosis test strategies are discussed, i.e. combinational and sequential fault diagnosis. Corresponding (single) place and transition fault models are introduced. The complexity of the proposed method depends on the effectivity of the existing algorithms for computation of the P-cover, i.e. the set of P-invariants covering N. The proposed approach can be extended for higher level Petri nets, e.g. such as coloured nets or also to design self-diagnosable circuit realisations of Boolean interpreted Petri nets. Several examples are given.

Key Words: fault diagnosis, discrete event system, place-transition net, P-invariant, D-partition, k-distinguishability, test point
Categories: C.3, D.2.2, G.2.3, H.1.1, J.6, J.7

1 Introduction

Today's discrete event systems (e.g. such as computer or communication networks, automated manufacturing systems or other large-scale plants, computer operating systems, office information systems and so on.) are of increasing importance because they are growing in number, size, and sophistication. Any such system may be asynchronous and sequential, exhibiting many characteristics: concurrency, conflict, mutual exclusion, and non-determinism. These characteristics are very difficult to describe using traditional control theory. On the other hand, an inappropriate control of the occurrence of events may lead to a system deadlock, capacity overflows, or may otherwise degrade system performance [Zhou and DiCesare 1993]. Hence, the fault diagnosis becomes a more and more difficult process. The use of Petri net models in

diagnosis and reliable design of event-driven systems is a subject of interest to researchers since more than twenty years. In general, the most of the studies in this area focus attention on dynamical analysis concerning specification and implementation of some fault detection, fault diagnosis and/or fault recovery procedures, e.g. using partially stochastic Petri nets [Aghasaryan et al.1998], or also using trace analysis [Pietschker and Ulrich 2003], etc. The study of the system fault indistinguishability properties seems to be important because of the following two reasons. First, we have an additional possibility of describing the critical components of the considered system. Second, there exists a possibility of using some simple and at the same time exact tools for improving the system (self-) diagnosis capabilities in the early stages of its design [Immanuel and Rangarajan 2001], [Tabakow 2000] - [Tabakow 2005a].

The main purpose of this paper is a brief introduction to some rather deterministic fault diagnosis approach concerning the inherent place-transition net fault indistinguishability. This paper describes a method of using Petri net P-invariants in system diagnosis. To model this process a net oriented fault classification is presented. Hence, the considered discrete event system is modelled by a live, bounded, and reversible place-transition Petri net. The notions of D-partition of the set of places P of a given place-transition net N and net k-distinguishability are first introduced. Next these two notions are extended to the set of all vertices, i.e. places and transitions of N . So the problem of fault identification of the vertices of N is transformed as a problem of fault identification of the places of a new net N´ called a net simulator of N . Any transition in N´ is assumed to be fault-free. Then the corresponding net place invariants are computed. The system k-distinguishability measure is obtained in a unique way from the place-invariant matrix. For a large value of k , the system model is extended by using some set of additional places called test points and at the same time preserving the original net properties. This is in accordance with the introduced practical requirements. To obtain a 1-distinguishable net the notion of a marked graph component is used. It is shown a sufficient condition for 1-distinguishability of an arbitrary place-transition net and a corresponding algorithm is presented. Next two different diagnosis test strategies are discussed, i.e. combinational and sequential fault diagnosis (assuming $MTBF \to \infty$ and $MTTR \to 0$, respectively). Corresponding (single) place and transition fault models are introduced. The complexity of the proposed method depends on the effectivity of the existing algorithms for computation of the P-cover, i.e. the set of P-invariants covering N. The proposed approach can be extended for higher level Petri nets, e.g such as coloured nets or also to design self-diagnosable circuit realisations of Boolean interpreted Petri nets. Several examples are given.

2 Basic Notions

In general any place-transition net $N =_{df} (T,P,A,M_0,K,W)$, where (T,P,A) is a finite net containing sets of *transitions* , *places*, and *arcs* called also *edges*, $K : P \to (IN_\omega - \{0\})$ and $W : A \to \mathbb{N}$ are the corresponding *place capacity* and *edge multiplicity* (called also *weight*) functions, respectively. The *initial marking vector*

$M_0 : P \rightarrow IN_\omega$, where $\mathbb{N}$ denotes the set of all natural numbers, $IN =_{df} \mathbb{N} \cup \{0\}$, $IN_\omega =_{df} IN \cup \{\omega\}$, and ω is an infinite number such that: $\omega + k = \omega$ and $k < \omega$ (for any $k \in IN$) [Reisig 1985], [Reisig 1992]. The *forward marking class* of N, i.e. $[M_0> =_{df} \{ M \in IN_\omega^P / \exists \tau \in T^* (M_0[\tau>M) \}$.
In the next considerations we shall assume N is a pure (i.e. without any self-loops), live and bounded net. In the case of manufacturing systems the *net reversibility property* is also required, i.e. $\forall M \in [M_0> (M_0 \in [M>$) [Zhou and DiCesare 1993]. The notion of PN-connectivity matrix (also denoted by $\underline{N}$) is modified as follows. Let $\underline{t} : P \rightarrow \mathcal{Z}$ (the set of all integers) be a mapping such that $\underline{t}(p) =_{df}$ if $p \in {}^\bullet t$ ($p \in t^\bullet$) then $-$ w(p,t) (w(t,p)) else 0 fi. Then the *PN-connectivity matrix* $\underline{N} : T \times P \rightarrow \mathcal{Z}$, where $\underline{N}(t,p) =_{df} \underline{t}(p)$ (for any $t \in T$ and $p \in P$). The well-known transition enabling and firing rules are omitted here [Reisig 1985], [Reisig 1992]. Also the net interpretation will be omitted below, e.g. N may be considered as a PN model of a manufacturing, multiprocessor or distributed system. The net *P- (T-)invariants* are computed using $\underline{N} \cdot \underline{i} = \underline{0}$ ($\underline{N}^T \cdot \underline{i} = \underline{0}$, where $\underline{N}^T$ is the transposed matrix $\underline{N}$). By $s(N) =_{df} |T|+|P|+|A|$ we shall denote the *size* of N. Let N be a place-transition net. The *support* of any P-invariant $\underline{i}$ with respect to N (in short: wrt N) is defined as follows: $supp(\underline{i}) =_{df} \{p \in P / \underline{i}(p) \neq 0\} \subseteq P$. A P-invariant $\underline{i}$ of N is called *positive* iff $\forall p \in supp(\underline{i}) (\underline{i}(p) \geq 0) \wedge \exists p \in supp(\underline{i}) (\underline{i}(p) > 0)$. A positive P-invariant $\underline{i}$ is *minimal* iff $\forall \underline{i}' (\underline{N} \cdot \underline{i}' = \underline{0} \Rightarrow \underline{i}' \geq \underline{i})$. Let I be the set of all (positive) P-invariants of N and $\mathcal{J} \subseteq I$ is a subset. We shall say $\mathcal{J}$ is a *P-cover* of N iff $\forall p \in P \exists \underline{i} \in \mathcal{J} (\underline{i}(p) \neq 0)$. And so we have: $\bigcup_{\underline{i} \in \mathcal{J}} supp(\underline{i}) = P$. The P-*invariant matrix* of N wrt $\mathcal{J}$ is introduced as follows: $\underline{\mathcal{I}} : \mathcal{J} \times P \rightarrow IN$, where $\underline{\mathcal{I}}(\underline{i},p) =_{df} \underline{i}(p) \in IN$. It can be observed $\sum_{p \in supp(\underline{i})} M(p) \cdot \underline{i}(p) = const$ (for any $M \in [M_0>$ and $\underline{i} \in \mathcal{J}$). It is obvious that any linear combination of P- (T-)invariants is also a P- (T-) invariant, e.g. if $\mathcal{J}$ is a P-cover of N then $\underline{i}' =_{df} \sum_{\underline{i}_s \in \mathcal{J}} a_s \cdot \underline{i}_s$ is also a P-invariant, where a_s are some constants (at least one of them $\neq 0$). In fact, $\underline{N} \cdot \underline{i}' = \underline{0}$ is always satisfied.

For convenience only, we shall assume below that the P-cover $\mathcal{J}$ of N is a set of all positive and minimal P-invariants. Any such set can be considered as a set of *linearly independent P-invariants*. In fact any such positive and minimal P-invariants are preferable, but not necessary wrt the proposed method (e.g. any test point corresponds to some positive and minimal P-invariant). Also we shall use the notion of the *revised P-invariant matrix* of N, defined as: $\underline{\rho} : \mathcal{J} \times P \rightarrow \{0,1\}$, where $\underline{\rho}(\underline{i},p) =_{df} 1$ iff $\underline{i}(p) \neq 0$ [Immanuel and Rangarajan 2001]. For simplicity, it is assumed below N have a P-cover. Otherwise, this method is also applicable. In the last case some additional test points is necessary to be introduced.

3 Net k-Distinguishability and Test Points

Let $[M_0 >_\alpha =_{df} [M_0 > \cup \{ M_\alpha \}$, where M_0 is the initial marking and M_α be a marking of N such that $M_\alpha \notin [M_0 >$. We shall say M_α is a *faulty marking*. Since $M \cdot \underline{i} = M_0 \cdot \underline{i}$ (for any $M \in [M_0 >$ and $\underline{i} \in \mathcal{J}$) [Reisig 1985] then $\Delta M \cdot \underline{i} = 0$, where $\Delta M =_{df} M - M_0$. The last property is satisfied for any P-invariant $\underline{i} \in \mathcal{J}$. Hence we can obtain $\mathcal{J} \cdot \Delta M^T = \underline{0}$. Therefore for $M \in [M_0 >_\alpha$ the above equation may be violated. Thus we have: $\mathcal{J} \cdot \Delta M^T = \underline{a} \in \{0,1\}^{|\mathcal{J}|}$ (for any $M \in [M_0 >_\alpha$, obviously $\underline{a} = \underline{0}$ iff $M \in [M_0 >$).

Without losing any generality, below $(\underline{a})_s \neq 0$ are interpreted as $(\underline{a})_s = 1$ ($s \in \{1,..., |J|\}$). Hence, in accordance with [Murata 1983], any $(\underline{a})_s = 1$ will correspond to some subset of places $supp(\underline{i}_s) \subseteq P$ having a (potentially) faulty behaviour.

Let $\Omega(\underline{a}) =_{df} \bigcap_{(\underline{a})_s=1} supp(\underline{i}_s) \cap \bigcap_{(\underline{a})_s=0} supp(\underline{i}_s)' \subseteq P$, where $supp(\underline{i}_s)' =_{df} P - supp(\underline{i}_s)$ is the corresponding set complement operation (provided there is no ambiguity we shall use below the same designation " ´ " as an index, e.g. to denote M´, i.e. the marking M for N´, where N´ is the net simulator corresponding to N, in a similar manner Ω' is used for Ω of N´). And so, like [Mayeda 1972] the notion of D-partition can be introduced. Below are used some basic notions given in [Tabakow 2000].

Definition 1

By a *D-partition of the set of places* P of a given place-transition net N wrt the P-cover $\mathcal{J}$ of N, denoted by $\Omega(N,\mathcal{J})$, or Ω if N and $\mathcal{J}$ are understood, we shall mean the (multi) family $\Omega =_{df} \{ \Omega(\underline{a}) / \underline{a} \in \{0,1\}^{|\mathcal{J}|} \}$.

Proposition 1

(a) $\Omega(\underline{0}) = \varnothing$,
(b) $\forall \underline{a},\underline{b} \neq \underline{0} (\underline{a} \neq \underline{b} \Rightarrow \Omega(\underline{a}) \cap \Omega(\underline{b}) = \varnothing)$, and
(c) $\bigcup_{\underline{a} \in \{0,1\}^{|J|}} \Omega(\underline{a}) = P$.

Proof:

(a) $\Omega(\underline{0}) =_{df} \bigcap_{(\underline{a})_s=0} P_s' = \bigcap_{\underline{i}_s \in J} P_s' = (\bigcup_{\underline{i}_s \in J} P_s)' = P' = \varnothing$ (since $\mathcal{J}$ is a P-cover of N).

(b) Assume that $\Omega(\underline{a}), \Omega(\underline{b}) \neq \varnothing$. Let $K =_{df} \{ k / (\underline{a})_k \neq (\underline{b})_k \} \subset \mathbb{N}$. For $\underline{a} \neq \underline{b}$ we have: $\bigcap_{(\underline{b})_k = 1, k \in K} P_k = \bigcap_{(\underline{a})_k = 0, k \in K} P_k$ and $\bigcap_{(\underline{b})_k = 0, k \in K} P_k' = \bigcap_{(\underline{a})_k = 1, k \in K} P_k'$. Hence, we can obtain: $\Omega(\underline{a}) \cap \Omega(\underline{b}) =_{df} A(\underline{a}) \cap A(\underline{b}) \cap \bigcap_{(\underline{a})_k = 1, k \in K} P_k \cap \bigcap_{(\underline{a})_k = 0, k \in K} P_k' \cap \bigcap_{(\underline{a})_k = 0, k \in K} P_k \cap \bigcap_{(\underline{a})_k = 1, k \in K} P_k' = A(\underline{a}) \cap A(\underline{b}) \cap \varnothing \cap \varnothing = \varnothing$.

(c) Let $\mathcal{K} \subseteq \mathcal{J}$ is any subset such that $\bigcup_{\underline{a} \in \{0,1\}^{|\mathcal{K}|}} \Omega(\underline{a}) = P$ and $\underline{i}_s \in \mathcal{J} - \mathcal{K}$. By induction, assume that $\mathcal{L} =_{df} \mathcal{K} \cup \{ \underline{i}_s \} \subseteq \mathcal{J}$. We have: $\bigcup_{\underline{a} \in \{0,1\}^{|\mathcal{L}|}} \Omega(\underline{a}) =_{df} (P_s \cap (\bigcup_{\underline{a} \in \{0,1\}^{|\mathcal{K}|}} \Omega(\underline{a}))) \cup (P_s' \cap (\bigcup_{\underline{a} \in \{0,1\}^{|\mathcal{K}|}} \Omega(\underline{a}))) = (P_s \cap P) \cup (P_s' \cap P)$ $= (P_s \cup P_s') \cap P = P \cap P = P$. □

The notion of a k-distinguishable place-transition net under a D-partition of the set of places P of N is given in the next definition.

Definition 2

The Petri net N is a *k-distinguishable net under* Ω iff
(i) $\exists\, \Omega(\underline{a}) \in \Omega \; (|\Omega(\underline{a})| = k)$ and
(ii) $\forall\, \Omega(\underline{a}) \in \Omega \; (|\Omega(\underline{a})| \leq k)$.

The *support* of any D-partition is defined as follows: $supp(\Omega) =_{df} \{ \Omega(\underline{a}) \in \Omega \,/\, \Omega(\underline{a}) \neq \emptyset \}$. Let $\pi(P)$ be the partition generated by the set of subsets of places (i.e. classes), such that each class consists of places having identical columns in the revised P-invariant matrix $\underline{\rho}$ of N. The following proposition is satisfied [Immanuel and Rangarajan 2001] (a more formal proof is given below).

Proposition 2

$supp(\Omega) = \pi(P)$.

Proof:

Let $\underline{a} \in \{0,1\}^{|\mathcal{J}|} - \underline{0}$ be a vector such that $\Omega(\underline{a}) \neq \emptyset$. Assume that $p \in \Omega(\underline{a})$ and $\{S_0, S_1\}$ is a partition of the set of indexes $\{1, 2, \ldots, |\mathcal{J}|\}$, where $S_i =_{df} \{ s \,/\, (\underline{a})_s = i \}$ $(i = 0,1)$. In accordance with the definition of $\Omega(\underline{a})$ we can obtain:

$$
\begin{aligned}
p \in \Omega(\underline{a}) \;&\Leftrightarrow_{df}\; p \in \bigcap_{(\underline{a})_s=1} supp(\underline{i}_s) \cap \bigcap_{(\underline{a})_s=0} supp(\underline{i}_s)' \\
&\Leftrightarrow\; p \in \bigcap_{s \in S_1} supp(\underline{i}_s) \cap \bigcap_{s \in S_0} supp(\underline{i}_s)' \\
&\Leftrightarrow\; \forall\, s \in S_1 \, (p \in supp(\underline{i}_s)) \wedge \forall\, s \in S_0 \, (p \in supp(\underline{i}_s)') \\
&\Leftrightarrow\; \forall\, s \in S_1 \, (\underline{i}_s(p) \neq 0) \wedge \forall\, s \in S_0 \, (\underline{i}_s(p) = 0) \\
&\Leftrightarrow\; \forall\, s \in S_1 \, (\underline{\rho}(\underline{i}_s,p) = 1) \wedge \forall\, s \in S_0 \, (\underline{\rho}(\underline{i}_s,p) = 0). \\
&\Leftrightarrow\; \forall\, s \, (s \in S_1 \Rightarrow \underline{\rho}(\underline{i}_s,p) = 1) \wedge \forall\, s \, (s \in S_0 \Rightarrow \underline{\rho}(\underline{i}_s,p) = 0) \\
&\Leftrightarrow\; \forall\, s \, ((s \in S_1 \Rightarrow \underline{\rho}(\underline{i}_s,p) = 1) \wedge (s \in S_0 \Rightarrow \underline{\rho}(\underline{i}_s,p) = 0)) \\
&\Leftrightarrow\; \forall\, s \, (s \in S_1 \Leftrightarrow \underline{\rho}(\underline{i}_s,p) = 1). \qquad \{\text{contraposition of implication}\}
\end{aligned}
$$

And so, $\underline{a}$ corresponds to the p^{th} column of the P-invariant matrix $\underline{I}$. Moreover this is true for any $p \in \Omega(\underline{a})$. Hence a corresponding subset of $|\Omega(\underline{a})|$ identical columns is obtained. Since $\Omega(\underline{a}) \neq \varnothing$ then $supp(\Omega) = \pi(P)$. □

A generalisation of the fault identification process to the set of all vertices $x \in T \cup P$ of N is given below. With any P/T-net N it can be associated a new net, say N', such that any transition $t \in T$ of N is transformed to a subnet $(\{t^+,t^-\},\{p^t\},\{(t^+,p^t),(p^t,t^-)\})$ in N'. Any such transformation is closed in the class of P/T-nets. The size of N', i.e. $s(N') = s(N) + 4 \cdot |T|$. For simplicity, the additional places p^{ti} of N' will be denoted by $p_{|P|+i}$ ($i = 1,...,|T|$) [Tabakow 2000]. An example net N' is shown in Figure 3(b) below (see Example 3).

In accordance with the above given construction any marking M in N will correspond to exactly one marking M' in N'. Also different markings in N will correspond to different markings in N'. So there exists some injective mapping, e.g. ψ from $[M_0>$ in N to $[M_0'>$ in N'.

In general, the following definition can be introduced (very similar to the well-known classical notion).

Definition 3

We shall say that N' is a *net simulator* of N (or *simulates* N) iff for any marking sequence $M_0, M_1, ..., M_k, ...$ in N there exists a marking sequence $M_0', M_1', ..., M_r', ...$ in N' such that: (1) $M_0' = \psi(M_0)$, (2) If the above two sequences are finite having final markings M_k and M_r' then $M_r' = \psi(M_k)$ and (3) For any two neighbouring markings M_i, M_{i+1} in the first sequence there exist two markings M_u', M_v' in the second sequence such that $i \leq u < v$, $M_u' = \psi(M_i)$, and $M_v' = \psi(M_{i+1})$.

According to Definition 3, the net N' obtained under the above given transition transformation is a well-defined net simulator of N. Moreover, any such transformation will preserve the basic inherent properties of N (a more formal treatment is omitted).Let N' be a net simulator of N and $\underline{i}'$ be a P-invariant of N'. It was shown that $\underline{i}'$ can be directly obtained by means of the corresponding P-invariant $\underline{i}$ of N. Hence there exists a strongly defined relationship between the P-covers of N' and N. The above given Definition 2 is generalised as follows [Tabakow 2000].

Definition 4

Let N be a place-transition net. Then N is a *k-distinguishable net* iff $\exists N'$ (N' is a net simulator of N and N' is a k-distinguishable net under Ω').

Proposition 3

Let $\underline{i}' = (i_1,...,i_{|P|},i_{|P|+1},...,i_{|P|+|T|})$ be a P-invariant in N'. Then $\underline{i} =_{df} (i_1,...,i_{|P|})$ is a P-invariant in N.

Proof:

Since $\underline{N}' \cdot \underline{i}' = \underline{0}$ then for any $\underline{t}^o \in T'$: $\underline{t}^o \cdot \underline{i}' = 0$, where $\underline{t}^o \in \{\underline{t}^+, \underline{t}^-\}$. Hence $\underline{t}^+ \cdot \underline{i}' = 0$ and $\underline{t}^- \cdot \underline{i}' = 0$. Therefore $\underline{t}' \cdot \underline{i}' = 0$, where $\underline{t}' =_{df} \underline{t}^+ + \underline{t}^-$. Since $\underline{t}' = (\underline{t},\underline{0})$ then $(\underline{t},\underline{0}) \cdot \underline{i}' = 0$. Assume now that $\underline{i}' = (\underline{i},\underline{a})$ where: $\underline{i} =_{df}$

$(i_1,...,i_{|P|})$ and $\underline{a} =_{df} (i_{|P|+1},...,i_{|P|+|T|})$. Since $(\underline{t},\underline{0}) \cdot (\underline{i},\underline{a}) = 0$ then $\underline{t} \cdot \underline{i} + \underline{0} \cdot \underline{a} = 0$. Hence $\underline{t} \cdot \underline{i} = 0$ (for any $t \in T$). So we have $\underline{N} \cdot \underline{i} = \underline{0}$ and $\underline{i}$ is a P-invariant in N. □

It is obvious that the opposite implication is not always satisfied. Moreover, any P-cover of N' will implicate a corresponding P-cover for N (since $supp(\underline{i}') = supp((\underline{i},\underline{a})) = supp(\underline{i}) \cup supp(\underline{a})$).According to Proposition 2 the net k-distinguishability measure under Ω is uniquely defined by the maximal number of identical columns of the corresponding matrix $\underline{\rho}$ of N. A similar observation can be obtained considering $\underline{\rho}'$ of the net simulator N' and Ω'. So, a simple method of computation of the k-distinguishability measure can be obtained [Immanuel and Rangarajan 2001]. Without losing any generality, in the next considerations we shall concentrate our attention only to the k-distinguishability measure under Definition 2. Next the notion of test point is introduced as follows.

Definition 5

Let $p_{k_0} \in P$ be a given place of N such that the pre-set $\bullet p_{k_0} =_{df} \{t_1\}$ and the post-set $p_{k_0} \bullet =_{df} \{t_2\}$, where t_1 and t_2 are two different transitions of N. The additional place $p_{k_0'} \in \bullet t_1 \cap t_2 \bullet$ is said to be a *test point associated with* p_{k_0} iff the initial marking $\hat{M}_0$ of the obtained net $\hat{N}$ is specified as follows: $\hat{M}_0(p) =_{df}$ if $p = p_{k_0'}$ then $\max\{M(p_{k_0}) / M \in [M_0>\} - M_0(p_{k_0})$ else $M_0(p)$ fi (for any $p \in \hat{P} =_{df} P \cup \{p_{k_0'}\}$).

It can be observed that in some cases the considered Petri net may be *maximally indistinguishable*, e.g. a net which is a state-machine net and a marked graph at the same time. Then the corresponding P-cover will contain only one P-invariant having all components equal to one.

Proposition 4

Let N be a directed elementary cycle having m places ($m > 1$). Then N becomes $(2m - r)$-distinguishable if r additional test points are placed ($1 \le r \le 2m - 1$). □ {Df.4, Prop.2}

A generalisation of Definition 5 for *non-ordinary place-transition nets* (i.e. nets having some edges $a \in A$ with weights $w(a) \neq 1$) is omitted here. Any such generalisation of the last definition for place-transition nets, which are not ordinary, would require an isomorphism between the corresponding reachability graphs $RG(N)$ and $RG(\hat{N})$ (see Example 1 and Theorem 2 given below). Let $P_{\underline{a}} =_{df} \Omega(\underline{a})$ (for any $\underline{a} \in \{0,1\}^{|y|}$). Obviously $P_{\underline{a}} \in supp(\Omega)$ if $P_{\underline{a}} \neq \emptyset$.

Definition 6

Let $P_{\underline{a}} \neq \emptyset$, $T_{\underline{a}} =_{df} \bullet P_{\underline{a}} \cup P_{\underline{a}} \bullet$ and $A_{\underline{a}} =_{df} A \cap ((T_{\underline{a}} \times P_{\underline{a}}) \cup (P_{\underline{a}} \times T_{\underline{a}}))$. The corresponding subnet $N_{\underline{a}} =_{df} (T_{\underline{a}}, P_{\underline{a}}, A_{\underline{a}})$ of N is called a *graphical representation* of $P_{\underline{a}}$. We shall say $N_{\underline{a}}$ is a *marked graph component* (or *MG-*

component) iff $\forall p \in P_{\underline{a}}$ ($|{\bullet}p| = |p{\bullet}| = 1$). The subset of places $P_{\underline{a}}$ is said to be a *MG-component generator*.

The following theorem was shown [Tabakow 2003].

Theorem 1

Assume that N a live and bounded place-transition net having $|P| \geq 2$ and $supp(\Omega) =_{df} \{ P_{\underline{a}_1}, P_{\underline{a}_2}, ..., P_{\underline{a}_n} \}$, where $1 \leq n < |P|$. If any $P_{\underline{a}} \in supp(\Omega)$ is a MG-component generator then N can be transformed into a 1-distinguishable net by using $(|P| - n)$ test points.

Proof:

Let $supp(\Omega) =_{df} \{ P_{\underline{a}_1}, P_{\underline{a}_2}, ..., P_{\underline{a}_n} \}$ be the partition of P for N under Proposition 2 and $k_i =_{df} |P_{\underline{a}_i}|$ (i = 1, ... ,n). Consider the subfamily $\mathcal{A} =_{df} \{ P_{\underline{a}_i} \in supp(\Omega) / k_i \geq 2 \} \subseteq supp(\Omega)$, where $s =_{df} |\mathcal{A}|$. The elements of $\mathcal{A}$ are in pairs disjoint (i.e. $P_{\underline{a}_i} \cap P_{\underline{a}_j} = \emptyset$ for any different i and j). Hence we can obtain:

$$\sum_{P_{\underline{a}_i} \in \mathcal{A}} k_i + (n - s) = |P|$$

By Proposition 4 it follows that the MG-component $N_{\underline{a}i}$ generated by $P_{\underline{a}i} \in \mathcal{A}$ can be transformed into a 1- distinguishable net by using $(k_i - 1)$ test points. And so, the total number of test points used in $\mathcal{A}$ or equivalently the number of test points for N is given by:

$$\sum_{P_{\underline{a}_i} \in \mathcal{A}} (k_i - 1) = \sum_{P_{\underline{a}_i} \in \mathcal{A}} k_i - s = |P| - n. \square \qquad \{Df.6, Prop.4\}$$

According to the above given Theorem 1 the following *test point placement algorithm* can be specified:

Algorithm 1

Input: N, $\mathcal{J}$

Output: $\hat{N}$

To obtain the 1-distinguishable net $\hat{N}$ from the original place-transition net N and the given P-cover $\mathcal{J}$ of N:

(1) Define $\underline{\rho}$ from $\mathcal{J}$ of N;

(2) Complete supp(Ω) from $\underline{\rho}$;

(3) Let $\mathcal{A} =_{df} \{ P_{\underline{a}} \in \text{supp}(\Omega) / | P_{\underline{a}}| \geq 2\} \subseteq \text{supp}(\Omega)$. Specify the subfamily $\mathcal{A}$;

(4) Let $P_{\underline{a}} \in \mathcal{A}$ be a MG-component generator. Determine the corresponding net $N_{\underline{a}}$;

(5) Let $k_{\underline{a}} =_{df} | P_{\underline{a}}|$. Place $(k_{\underline{a}} - 1)$ test points in $N_{\underline{a}}$. The choice of the associated places corresponding to the subset $P_{\underline{a}} \subseteq P$ of N can be realised in an arbitrary way;

(6) Let the new subfamily $\mathcal{A} =_{df} \mathcal{A} - \{ P_{\underline{a}}\}$. If $\mathcal{A} \neq \emptyset$ then go to (4) else end. □

It is obvious that any P-invariant in N can be extended as a P-invariant in $\hat{N}$ by assuming 0's relating to the corresponding test point components, i.e. the following proposition is satisfied.

Proposition 5

If $\underline{i}$ is a P-invariant in N then $\hat{\underline{i}} =_{df} (\underline{i},\underline{0})$ is a P-invariant in $\hat{N}$, where the vector size of $\underline{0}$ is related to the number of used test points.

Proof:

Let $\hat{\underline{t}} =_{df} (\underline{t}, (\hat{t}(p_{|P|+1}), \ldots, \hat{t}(p_{|P|+s}))$ be an arbitrary row-vector in $\hat{\underline{N}}$ and $\underline{t}$ be the corresponding such vector in $\underline{N}$ ($s \geq 1$). Here, according to Definition 5, the original net N is extended to $\hat{N}$ assuming a finite set of test points, e.g. $\{p_{|P|+1}, \ldots, p_{|P|+s}\}$. Let $\hat{\underline{i}} =_{df} (\underline{i},\underline{0})$. Since $\underline{t} \cdot \underline{i} = 0$ then: $\hat{\underline{t}} \cdot \hat{\underline{i}} = (\underline{t}, (\hat{t}(p_{|P|+1}), \ldots, \hat{t}(p_{|P|+s})) \cdot (\underline{i}, (0, \ldots, 0)) = \underline{t} \cdot \underline{i} + 0 = 0$. □

Proposition 6

If $p_{k_0}{}'$ is a test point associated with $p_{k_0} \in P$ in N then $\hat{\underline{i}}_{k_0}$ is a P-invariant in $\hat{N}$, where $\text{supp}(\hat{\underline{i}}_{k_0}) = \{ p_{k_0}, p_{k_0}{}'\}$.

Proof:

Assume that $p_{k_0}{}'$ is a test point associated with $p_{k_0} \in P$ in N. According to Definition 5 $p_{k_0}{}'$ (p_{k_0}) is at the same time an input (output) place to t_1 and an output (input) place to t_2. By definition, a vector $\underline{x}$ is a P-invariant iff $\hat{\underline{N}} \cdot \underline{x} = \underline{0}$. Hence iff $\hat{\underline{t}} \cdot \underline{x} = \underline{0}$ (for any row-vector $\hat{\underline{t}}$ of $\hat{\underline{N}}$). And so, there exist exactly two equations related to t_1 (t_2) of the following form: $\ldots - x_{p_{k0}}{}' (+ x_{p_{k0}}{}') \ldots + x_{p_{k0}} (-$

$x_{p_{k0}}) ... = 0$. The P-invariant $\hat{\underline{i}}_{k_0}$ is obtained by assuming $x_{p_{k0}} = x_{p_{k0}}' = 1$ and $x_i = 0$ (for any $x_i \neq x_{p_{k0}}, x_{p_{k0}}'$). □

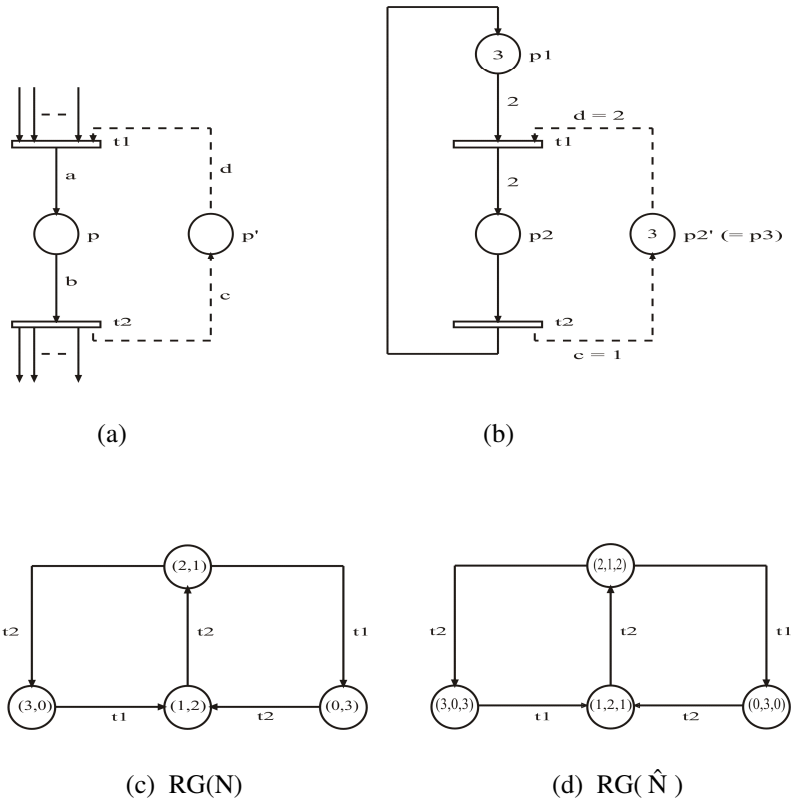


Figure 1: A hypothetical fragment of non-ordinary place-transition net (a) an example test point placement (b), and the corresponding reachability graphs RG(N) and RG($\hat{N}$) (c and d, respectively)

Proposition 7

If $\mathcal{J}$ is a P-cover of N then $\hat{\mathcal{J}} =_{df} \mathcal{J} \cup \{ \hat{\underline{i}}_{k_0} \}$ is a P-cover of $\hat{N}$. {Prop.6}

In a natural manner, the last two propositions can be extended for non-ordinary place-transition nets. This is illustrated in the next example.

Example 1

Consider the hypothetical fragment shown in Figure 1(a) above. Let p´ be a test point associated with $p \in P$ in N and $\hat{\underline{i}}$ be a P-invariant in $\hat{N}$ such that supp($\hat{\underline{i}}$)

$=_{df}$ {p, p´}. Using $\underline{\hat{N}} \cdot \underline{\hat{i}} = \underline{0}$ (assuming $\hat{i}(q) =_{df} 0$, for $q \in P - supp(\underline{\hat{i}})$) the following two equations can be obtained:

$$a \cdot \hat{i}(p) - d \cdot \hat{i}(p') = 0$$
$$-b \cdot \hat{i}(p) + c \cdot \hat{i}(p') = 0$$

Since the edge multiplicities a and b of N are a priori given then d and c can be defined in a unique way by assuming $\hat{i}(p) = \hat{i}(p') = 1$. Hence: $d =_{df} a$ and $c =_{df} b$. The obtained P-invariant $\underline{\hat{i}}$ is minimal and positive.

An example test point placement is shown in Figure 1(b) where an example live, bounded, and reversible place-transition net is presented. Assume that $T = \{t_1,t_2\}$ is a fault-free. According to Proposition 2 the considered net N is 2-distinguishable wrt the P-invariant $\underline{i} = (1,1)$ having two identical columns. Let $p_3 =_{df} p_2'$ be a test point such that $\hat{M}_0(p_3) =_{df} \max\{M(p_2) / M \in [M_0>\} - M_0(p_2) = 3 - 0 = 3$. According to Proposition 5 $\underline{\hat{i}} =_{df} (1,1,0)$ is a P-invariant in $\hat{N}$. Using $\underline{\hat{N}} \cdot \underline{x} = \underline{0}$ the following two equations can be obtained:

$$-2 \cdot x_1 + 2 \cdot x_2 - d \cdot x_3 = 0$$
$$x_1 - x_2 + c \cdot x_3 = 0$$

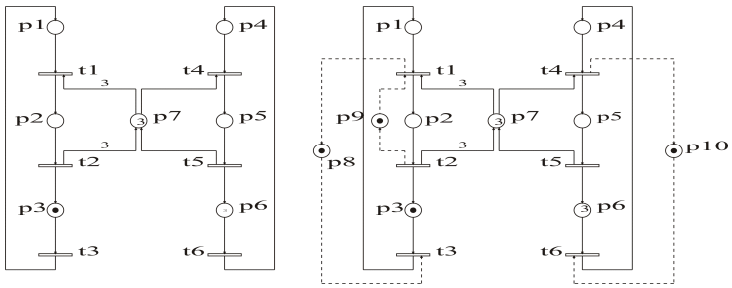
Let $x_1 = 0$, $x_2 = x_3 = 1$. Then $d = 2$ and $c = 1$. In accordance with Proposition 6 $\underline{\hat{i}}_2 =_{df} (0,1,1)$ is another P-invariant where $supp(\underline{\hat{i}}_2) = \{p_2, p_3\}$. In fact, we have $\hat{M}(p_2) + \hat{M}(p_3) = 3$ (for any $\hat{M} \in [\hat{M}_0>$ in $\hat{N}$). The obtained P-invariant matrix $\underline{\hat{J}} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ has all columns different and $\hat{N}$ is 1-distinguishable. The corresponding reachability graphs RG(N) and RG($\hat{N}$) are shown in the above Figure 1(c) and (d), respectively. It can be observed that any M of N is a prefix of the corresponding $\hat{M}$ of $\hat{N}$ and the last two reachability graphs are isomorphic. Hence, the original boundedness, liveness, and reversibility properties of N are preserved in $\hat{N}$. □

Example 2

Consider N of Figure 2(a) below describing the behaviour of a system consisting of one write- and three read-authorised processes [4,6,7]. The interpretation of the places and transitions is as follows: $p_1(p_4)$: process waiting for three keys (for one key), $p_2(p_5)$: writing process (reading process), $p_3(p_6)$: inactive process (inactive processes), p_7: keys, $t_1(t_4)$: take keys (take keys), $t_2(t_5)$: return keys (return keys), and $t_3(t_6)$: indication of need (indication of need).

The following P-cover can be obtained: $\mathcal{J} = \{\underline{i}_1,\underline{i}_2,\underline{i}_3\}$, where: $\underline{i}_1 = (1,1,1,0,0,0,0)$, $\underline{i}_2 = (0,0,0,1,1,1,0)$ and $\underline{i}_3 = (1,4,1,0,1,0,1)$.. According to Proposition 2, N is 3-distinguishable. The obtained test point improving is shown in

Figure 2(b). The net N becomes 2-distinguishable for $\mathcal{J} = \{\underline{i}_2,\underline{i}_3,\underline{i}_4\}$ or also $\mathcal{J} = \{\underline{i}_1,\underline{i}_2,\underline{i}_4\}$, where $\underline{i}_4 = (0,3,0,0,1,0,1)$. In the last case the number of test points can be reduced to 2 (e.g. by removing p_9). □ {Df.2, Prop.2, T1}



(a) N (b) $\hat{N}$

Figure 2: A system consisting of one write- and three read-authorised processes (a) and a net distinguishability improving using test points p_8,p_9 and p_{10} (b).

In general, the process of test point placement is related to the problem of finding minimal cost P-cover $\mathcal{J}$ such that the obtained diagnostic resolution is maximal (this is omitted). The following theorem is satisfied.

Theorem 2

Let N be live, bounded, and reversible place-transition net and p_{k_0}' be a test point associated with p_{k_0}.Then $\hat{N}$ is also live, bounded, and reversible.

Proof:

Without losing any generality, assume that $\mathcal{J}$ is a P-cover of N. Then $\hat{\mathcal{J}} =_{df} \mathcal{J} \cup \{\hat{\underline{i}}_{k_0}\}$ is a P-cover of $\hat{N}$.Otherwise, a P-cover of N can be obtained by assuming additional test points. According to Definition 5 $\hat{M}_0$ is bounded. Hence $\hat{N}$ is bounded.

Let $\overline{M} =_{df} \max\{M(p_{k_0}) / M \in [M_0>\}$ and $T(M) =_{df} \{t \in T / t$ is M-enabled in N$\}$. Assume that $t_1 \in T(M)$. Hence $t_1 \in T(\hat{M})$ iff $\hat{M}(p_{k_0}) + a \leq \overline{M}$ and $\hat{M}(p_{k_0}') \geq a$ (see the above Figure 1(a) assuming $p =_{df} p_{k_0}$ and $p' =_{df} p_{k_0}'$). However, in accordance with Definition 5 $\hat{M}(p_{k_0}) = M(p_{k_0})$ (for any $M \in [M_0>$). Hence $\hat{M}(p_{k_0}) + a = M(p_{k_0}) + a \leq \overline{M}$. Moreover, $\hat{\underline{i}}_{k_0}$ is a Boolean vector. Then $\hat{M}(p_{k_0}) + \hat{M}(p_{k_0}') = \overline{M}$ (for any $\hat{M} \in [\hat{M}_0>$ in $\hat{N}$).

Hence: $a + \hat{M}(p_{k_0}) + \hat{M}(p_{k_0}') = \overline{M} + a$. Since $a + \hat{M}(p_{k_0}) \leq \overline{M}$ then $\overline{M} + \hat{M}(p_{k_0}') \geq \overline{M} + a$. Hence $\hat{M}(p_{k_0}') \geq a$ and $t_1 \in T(\hat{M})$.

Assume now that $t_2 \in T(M)$. Hence $t_2 \in T(\hat{M})$ iff $\hat{M}(p_{k_0}) \geq b$ and $\hat{M}(p_{k_0}') + b \leq \overline{M}$ .Since $\hat{M}(p_{k_0}) = M(p_{k_0})$ the first condition $\hat{M}(p_{k_0}) \geq b$ is satisfied. Hence, using $\hat{M}(p_{k_0}) + \hat{M}(p_{k_0}') = \overline{M}$ we can obtain: $b + \hat{M}(p_{k_0}') \leq \overline{M}$.

Hence: $t \in T(M)$ iff $t \in T(\hat{M})$ (for $t \in \{t_1,t_2\}$).And so, the liveness and reversibility properties of N are preserved in $\hat{N}$. □ {Df.5, Prop.6, Prop.7}

Test points can be placed independently each other. Hence Theorem 2 can be generalised for any finite subset of such points.

4 The Fault Isolation Method

Testing of a system is an experiment in which the system is exercised and its resulting response is analysed to ascertain whether it behaved correctly. If incorrect behaviour is detected, a second goal of testing experiment may be to diagnose, or locate, the cause of the misbehaviour. *Diagnosis* assumes knowledge of the internal structure of the system under test. These concepts of testing and diagnosis have a broad applicability (consider, for example, medical tests and diagnoses, test-driving a car, diagnosability analysis of computer networks or large-scale plants, debugging a computer program, etc.).

Testing methods can be classified according to many criteria, e.g. *on-line* (*concurrent*) *testing* or also *off-line testing* (if it is important to know when is testing performed), etc. Two different diagnosis test strategies are discussed below, i.e. combinational and sequential fault diagnosis (assuming $MTBF \rightarrow \infty$ and $MTTR \rightarrow 0$, respectively). The *combinational fault diagnosis* approach can be classified as on-line fault diagnosis (any interruptions for testing purposes are not allowable during the work of the system). And so, in some cases this approach may be too expensive. The *sequential* (called also *adaptive*) *fault diagnosis* approach assumes some minimisation of the testing time. In sequential fault diagnosis the process of fault isolation is carried out step by step, where each step depends on the result of the diagnostic experiment at the previous step. Hence, any sequential diagnosis procedure can be graphically represented as *diagnostic tree* (in short: *D-tree*).

The concurrent systems we are considering here are those that can be represented by a live and bounded place-transition Petri net. Without losing any generality we shall also assume below any such net N is reversible. It can be observed boundedness, liveness, and reversibility are independent of each other. Hence, the main purpose of the proposed fault isolation method is to locate the physical fault(s) in the Petri net model of the considered system. The degree of accuracy to which faults can be located (i.e. the *diagnostic resolution*) is given in a unique way by the obtained k-distinguishability measure. Any place $p \in P$ of N having an incorrect

behaviour is said to be a *faulty place* (denoted also by p_α). The single faulty place model will be assumed below (called in short: *p-fault model*). Hence, it is assumed that any faulty marking M_α is a consequence of some p_α. This faulty place will implicate a violation of the firing rule. The violated firing rule will make the P-invariant assertion $\underline{J} \cdot \Delta M^T = \underline{0}$ false. Any validation of the last equation can be interpreted as a validation of the logical value $\in$ {'true','false'} of some two-argument predicate $R(M_k,\underline{i}_s)$, obtained for a given $M_k \in [M_0 >_\alpha$ and $\underline{i}_s \in \mathcal{J}$. Hence, the obtained proposition will be 'true' iff $\Delta M \cdot \underline{i}_s \equiv 0$. And so, this validation can be represented as an *elementary test* (or *measurement*) $\tau_s \in \Theta$ of the considered system, where Θ is the set of all such tests, i.e. $\Theta =_{df} \{ \tau_s / \underline{i}_s \in \mathcal{J} \}$.

We observe that for a given $M_k \in [M_0 >_\alpha$ there exists one-to-one correspondence between tests τ_s and the P-invariants $\underline{i}_s$ of N. Hence the P-invariant matrix $\underline{J}$ can be interpreted as a *diagnostic matrix*. Moreover, any such matrix can be considered as an *information system* $(P, \mathcal{J}, \{0,1\}, \varphi)$, where $\varphi : P \times \mathcal{J} \rightarrow \{0,1\}$ is the corresponding *information function* [Pawlak 1991]. Next we shall assume that the set of P-invariants $\mathcal{J}$ (i.e. 'attributes' of this information system) is a reduced set (or reduct wrt some superfluous P-invariants: the process of reduction is omitted here).

Let $\mathbb{R}^{\geq}$ be the set of all nonnegative reals and $c : \Theta \rightarrow \mathbb{R}^{\geq}$ be a *cost function* such that $c(\tau) \in \mathbb{R}^{\geq}$ be the cost of using the elementary test $\tau \in \Theta$. The *total cost* (in short: TC) in the case of the combinational fault diagnosis approach is given by $TC =_{df} \sum_{\tau \in \Theta} c(\tau)$. It can be observed TC is the cost of the P-cover of N, i.e. the cost of the family $\{P_1, P_2, \ldots, P_{|\mathcal{J}|}\}$, where $P_s =_{df} supp(\underline{i}_s) \subseteq P$ $(s = 1, 2, \ldots, |\mathcal{J}|)$.

The corresponding cost in the case of the sequential fault diagnosis approach will depend on the probability $Prob\{p\} \in [0,1]$ that $p \in P$ is a faulty place. Obviously $\sum_{p \in P} Prob\{p\} = 1$. Hence, the *cost of D-tree* (in short: CDT) is defined as follows: $CDT =_{df} \sum_{p \in P} Prob\{p\} \cdot c(p)$, where $c(p) =_{df} \sum_{\tau \in \Theta(p)} c(\tau)$. By $\Theta(p) \subseteq \Theta$ it is denoted the subset of tests isolating (or locating) fault in p.

The above considered costs TC and CDT correspond to the notions of P-cover and k-distinguishability, respectively. Moreover, it can be observed that $CDT \leq TC$. In fact, since $\Theta(p) \subseteq \Theta$ we can obtain:

$$
\begin{aligned}
CDT &=_{df} \sum_{p\in P} Prob\{p\}\cdot c(p)\\
&= \sum_{p\in P} Prob\{p\}\cdot \Big(\sum_{\tau\in\Theta(p)} c(\tau)\Big)\\
&\le \sum_{p\in P} Prob\{p\}\cdot \Big(\sum_{\tau\in\Theta} c(\tau)\Big)\\
&= \sum_{p\in P} Prob\{p\}\cdot TC\\
&= TC\cdot 1\\
&= TC.\ \square
\end{aligned}
$$

A particular case can be obtained by assuming that N is a directed elementary cycle having two places (e.g. p_1 and p_2) and only one test point (considered as a hardcore). Then we have: $CDT = Prob\{p_1\}\cdot c(\tau) + Prob\{p_2\}\cdot c(\tau) = (Prob\{p_1\} + Prob\{p_2\})\cdot c(\tau) = 1\cdot c(\tau) = TC$.

According to Definition 4 the above presented p-fault model can be generalised to the set of all vertices $x \in P \cup T$ of N. In particular, assuming that P is fault-free, the single faulty transition model can be obtained (called in short: *t-fault model*). Let $\underline{1}'$ and $\Delta M'$ be $\underline{1}$ and ΔM for N´ (the net simulator of N). Next by $\underline{1}'/X$ and $\Delta M'/X$ we shall denote $\underline{1}'$ and $\Delta M'$ restricted to the subset of columns corresponding to X, where $X \in \{P,T\}$ (obviously, we have: $\underline{1} = \underline{1}'/P$).

Proposition 8

If a t-fault model is assumed for N then: $\underline{1}'\cdot \Delta M'^{T} = \underline{1}'/T\cdot \Delta M'^{T}/T$.

Proof:

$$
\begin{aligned}
\underline{1}'\cdot \Delta M'^{T} &= [\underline{1}'/P, \underline{1}'/T]\cdot [\Delta M'/P, \Delta M'/T]^{T}\\
&= \underline{1}'/P\cdot \Delta M'^{T}/P + \underline{1}'/T\cdot \Delta M'^{T}/T\\
&= \underline{0} + \underline{1}'/T\cdot \Delta M'^{T}/T\\
&= \underline{1}'/T\cdot \Delta M'^{T}/T.\ \square
\end{aligned}
$$

Definition 7

The Petri net N is a *p-fault k-distinguishable net* (a *t-fault k-distinguishable net*) iff N is a k-distinguishable net under Ω assuming the p-fault model (t-fault model).

Example 3 (*combinational fault diagnosis: p-fault model*)

Let consider the place-transition net N of Figure 4(a) corresponding to the manufacturing system shown in Figure 3 below [Zhou and DiCesare 1993]. The places represent resource states or operations and the transitions represent start or completion of the corresponding discrete event. The interpretation of the places and transitions is as follows: p_1: represents pallets available, p_2: machine 1 loads, fixtures and processes a palleted raw part, p_3: robot unloads an intermediate part to the buffer, p_4: buffer stores an intermediate part, p_5: machine 2 loads and processes an intermediate part, p_6: robot unloads a final product from machine 2, defixtures and

returns pallet, p_7: represents the availability of machine 1, p_8: represents buffer available, p_9: represents the availability of machine 2, p_{10}: represents robot available, t_1: models the start of activity of p_2, t_2: the stop of activity in p_2 and the start of activity of p_3, t_3: the stop of p_3 and the start of the storage activity p_4, t_4: the stop of p_4 and the start of p_5 activity, t_5: the stop of activity p_2 and the start of p_6, and t_6: models the stop of p_6 activity.

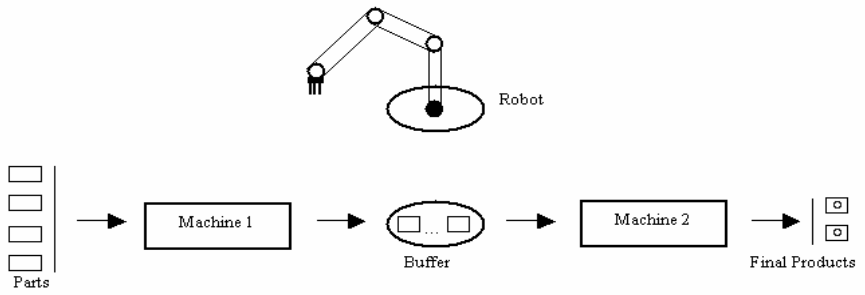
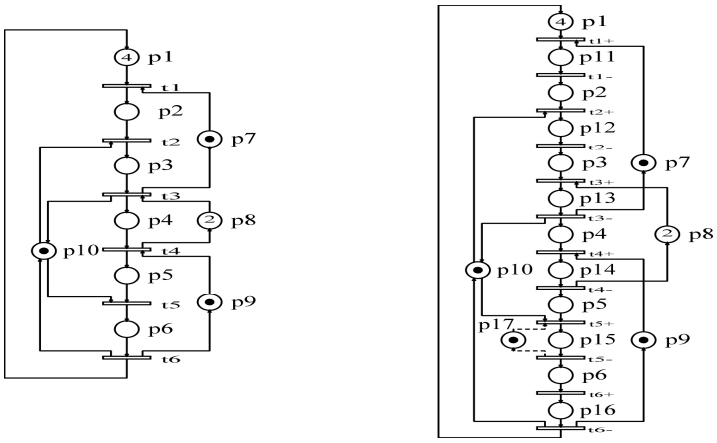


Figure 3: A simple manufacturing system

The system consists of two different machines, a robot, and a buffer. Every part from the input storage must be processed by Machine 1 first and then by Machine 2 to produce a final product. The robot is used for unloading both machines and the buffer is used to store intermediate parts.



(a) N (b) N´

Figure 4: The Petri net model (a) corresponding to the system of Figure 3 and the corresponding net simulator (b)

$$\text{Hence } \underline{\jmath}' = \left[\begin{array}{cccccccccc|cccccc} 1&1&1&1&1&1&0&0&0&0&1&1&1&1&1&1\\ 0&1&1&0&0&0&1&0&0&0&1&1&1&0&0&0\\ 0&0&1&0&0&1&0&0&0&1&0&1&1&0&1&1\\ 0&0&0&1&0&0&0&1&0&0&0&0&1&1&0&0\\ 0&0&0&0&1&1&0&0&1&0&0&0&0&1&1&1 \end{array}\right],$$

where $\underline{\jmath}' = [\underline{\jmath}'/P, \underline{\jmath}'/T]$ and the maximal number of identical columns in $\underline{\jmath}'/P$ (in $\underline{\jmath}'/T$) is 1 (is 2). According to Proposition 2, N is a p-fault 1-distinguishable net and a t-fault 2-distinguishable net. Here the revised P-invariant matrix $\underline{\rho}' = \underline{\jmath}'$.

Let now $p_\alpha =_{df} p_4$ be a single faulty place and $M_\alpha =_{df} (4,0,0,1,0,0,1,2,1,1)$. Hence $\Delta M = M_\alpha - M_0 = (0,0,0,1,0,0,0,0,0,0)$ and $\underline{\jmath}'/P \cdot \Delta M'^{T}/P = \underline{\jmath} \cdot \Delta M^T =$

$$\left[\begin{array}{cccccccccc} 1&1&1&1&1&1&0&0&0&0\\ 0&1&1&0&0&0&1&0&0&0\\ 0&0&1&0&0&1&0&0&0&1\\ 0&0&0&1&0&0&0&1&0&0\\ 0&0&0&0&1&1&0&0&1&0 \end{array}\right] \cdot \left[\begin{array}{c} 0\\0\\0\\1\\0\\0\\0\\0\\0\\0 \end{array}\right] = \left[\begin{array}{c} 1\\0\\0\\1\\0 \end{array}\right].$$

Hence, the fourth column of $\underline{\jmath}$ is obtained and this corresponds to fault in p_4. In fact, assuming $\underline{a} =_{df} (1,0,0,1,0)$ we can obtain: $\Omega(\underline{a}) = P_1 \cap P_2' \cap P_3' \cap P_4 \cap P_5' = \{p_4\}$, where $P_1 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$, $P_2' = \{p_1, p_4, p_5, p_6, p_8, p_9, p_{10}\}$, $P_3' = \{p_1, p_2, p_4, p_5, p_7, p_8, p_9\}$, $P_4 = \{p_4, p_8\}$, and $P_5' = \{p_1, p_2, p_3, p_4, p_7, p_8, p_{10}\}$.

The problem becomes worse in the case of multiple faults. The corresponding fault isolation process may not be correctly realised. For example, assuming the multiple fault $(p_2, p_3)_\alpha$, i.e. $M_\alpha =_{df} (4,1,1,0,0,0,1,2,1,1)$ we can obtain: $\underline{\jmath} \cdot \Delta M^T = (2,2,1,0,0)$. Hence $\underline{a} =_{df} (1,1,1,0,0)$, the third column of $\underline{\jmath}$ is obtained and this corresponds to single fault in p_3. Similarly, for $(p_5, p_6, p_7)_\alpha$ with $M_\alpha =_{df} (4,0,0,0,1,1,0,2,1,1)$ we have: $\underline{\jmath} \cdot \Delta M^T = (2,-1,1,0,2)$. Hence $\underline{a} =_{df} (1,1,1,0,1)$ and $\Omega(\underline{a}) = P_1 \cap P_2 \cap P_3 \cap P_4' \cap P_5 = \varnothing$. In fact, there is no any column in $\underline{\jmath}$ identical with $\underline{a}^T$. □

Example 4 (*combinational fault diagnosis: t-fault model*)

Consider the same net N as in the previous example. The net simulator N′ of N is shown in Figure 4(b). Here $t_i^{\pm}$ are assumed to be fault-free (i = 1, ... ,6) , where $s(N') = 38 + 4 \cdot 6 = 62$ [Tabakow 2000]. The net transitions $t \in T$ can be interpreted, e.g. as start or completion of the corresponding event [Zhou and DiCesare 1993]. Hence t^+ and t^- can be related to the initial and final time needed for realisation of any such event.

Since N is a t-fault 2-distinguishable, to distinguish between faults in t_5 and t_6, an additional test point p_{17} is placed (as it is shown in Figure 4(b), using dashed line). The extended P-invariant submatrix of N', i.e. the P-invariant matrix of $\hat{N}'$, $\underline{\hat{J}}'/T =$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

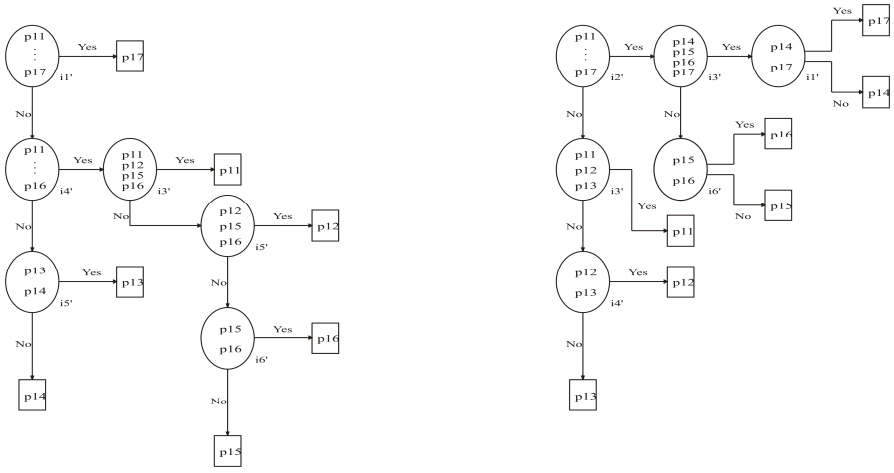
Since $\underline{\hat{J}}'/T$ has all columns different, any single faulty transition can be identified, e.g. assuming $\hat{M}_0' =_{df} (4,0,0,0,0,0,1,2,1,1,0,0,0,0,0,0,1)$ and $\hat{M}_\alpha' =_{df} (4,0,0,0,0,0,1,2,1,1,0,0,1,0,0,0,1)$ we can obtain: $\Delta\hat{M}' = (0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0)$. Hence $\Delta\hat{M}'/T = (0,0,1,0,0,0,0)$. In accordance with Proposition 8 we have: $\underline{\hat{J}}'/T \cdot \Delta\hat{M}'^{T}/T = (1,1,1,1,0,0)^T$. And so, the third column of $\underline{\hat{J}}'/T$ is obtained and this corresponds to fault in p_{13}, i.e. t_3. In fact, $p_\alpha \in \{p_{11}, p_{12}, p_{13}, p_{14}, p_{15}, p_{16}\} \cap \{p_{11}, p_{12}, p_{13}\} \cap \{p_{12}, p_{13}, p_{15}, p_{16}\} \cap \{p_{13}, p_{14}\} \cap \{p_{11}, p_{12}, p_{13}, p_{17}\} \cap \{p_{11}, p_{12}, p_{13}, p_{14}, p_{16}\} = \{p_{13}\}$. The total cost $TC = c(\tau_1) + c(\tau_2) + c(\tau_3) + c(\tau_4) + c(\tau_5) + c(\tau_6)$, where any τ_s corresponds to $\underline{i}_s'/T$. Hence, in the case of homogeneous costs, i.e. $c(\tau_s) = 1$ (for any s) we have: $TC = 6$. □

Example 5 (*sequential fault diagnosis: t-fault model*)

According to the previous example, the process of fault isolation can be carried out step by step, where each step depends on the result of the diagnostic experiment at the previous step. The graphical representation of this approach is is illustrated below, where two example D-trees are shown (see Figure 5(a,b) where any i_s' corresponds to $\Delta\hat{M}/T \cdot \hat{\underline{i}}_s'/T = 0?$, s = 1,2,...,6). Now, to distinguish between faults in p_{15} (i.e. t_5) and p_{16} (i.e. t_6), the additional place invariant $\underline{i}_6'/T$ is used (corresponding to the above introduced test point p_{17}). The obtained fault isolation improvement is shown using dashed line. The cost CDT / D-tree 1 $= \text{Prob}\{p_{17}\}\cdot c(\tau_1) + \text{Prob}\{p_{11}\}\cdot(c(\tau_1) + c(\tau_4) + c(\tau_3)) + \text{Prob}\{p_{13}\}\cdot(c(\tau_1) + c(\tau_4) + c(\tau_5)) + \text{Prob}\{p_{14}\}\cdot(c(\tau_1) + c(\tau_4) + c(\tau_5)) + \text{Prob}\{p_{12}\}\cdot(c(\tau_1) + c(\tau_4) + c(\tau_3) + c(\tau_5)) + \text{Prob}\{p_{16}\}\cdot(c(\tau_1) + c(\tau_4) + c(\tau_3) + c(\tau_5) + c(\tau_6)) + \text{Prob}\{p_{15}\}\cdot(c(\tau_1) + c(\tau_4) + c(\tau_3) + c(\tau_5) + c(\tau_6))$.

For example, by assuming an uniform distribution, i.e. a constant probability for any $p \in P$ we can obtain: CDT / D-tree 1 $= \frac{1}{7}\cdot c(\tau_1) + \frac{1}{7}\cdot(c(\tau_1) + c(\tau_4) + c(\tau_3)) + \frac{2}{7}\cdot(c(\tau_1) + c(\tau_4) + c(\tau_5)) + \frac{1}{7}\cdot(c(\tau_1) + c(\tau_4) + c(\tau_3) + c(\tau_5)) + \frac{2}{7}\cdot(c(\tau_1) + c(\tau_4) + c(\tau_3) + c(\tau_5) + c(\tau_6)) = c(\tau_1) + \frac{4}{7}\cdot c(\tau_3) + \frac{6}{7}\cdot c(\tau_4) + \frac{5}{7}\cdot c(\tau_5) + \frac{2}{7}\cdot c(\tau_6) < c(\tau_1) + c(\tau_2) + c(\tau_3) + c(\tau_4) + c(\tau_5) + c(\tau_6) = TC$. Hence, in the case of homogeneous costs:

CDT / D-tree 1 = $\frac{24}{7}$. In a similar manner, for D-tree 2 of Figure 5(b) we can obtain: CDT / D-tree 2 = $\frac{20}{7} < \frac{1}{2} \cdot \frac{42}{7}$ (= $\frac{1}{2} \cdot \mathrm{TC}$). □



(a) D-tree 1 (b) D-tree 2

Figure 5: Two example D-trees for N´ of Figure 4(b)

5 Conclusions

The above-considered approach gives a possibility of fault isolation in concurrent systems. This process is realised by using the Petri net model of the considered system. The degree of accuracy to which faults can be located, i.e. the diagnostic resolution is given in a unique way by the obtained k-distinguishability measure. The complexity of the proposed method depends on the effectivity of the existing algorithms for computation of the P-cover, i.e. the set of P-invariants covering N. The choice of diagnosis strategies, i.e. combinational or also sequential is depending on the used time requirements for testing. Moreover, an additional cost-minimisation can be obtained by assuming the considered test point set as a "hardcore". This approach can be extended for higher level Petri nets, e.g. such as coloured nets or also to design self-diagnosable circuit realisations of Boolean interpreted Petri nets.

References

[Aghasaryan et al.1998] Aghasaryan, A., Fabre, E., Benveniste, A., Boubour, R., Jard, C.: "Fault detection and diagnosis in distributed systems: an approach by partially stochastic Petri nets"; Discrete Event Dynamic Systems (Special issue on Hybrid Systems), *8*, 2 (Jun 1998), 203-231.

[Immanuel and Rangarajan 2001] Immanuel, B., Rangarajan K.: "System diagnosis and k-distinguishability in Petri nets"; Private communication, India (2001), 14pp.

[Mayeda 1972] Mayeda, W.: "Graph Theory"; John Wiley & Sons, Inc., New York (1972), 523 – 557.

[Murata 1983] Murata, T.: "Petri nets and their applications"; Journal Soc. Instrum. Control Eng. 22 (1983), 6572.

[Pawlak 1991] Pawlak, Z.: "Rough Sets, Theoretical Aspects of Reasoning about Data"; Kluwer Academic Publishers, Dordrecht, Boston, London (1991), 229pp.

[Pietschker and Ulrich 2003] Pietschker, A., Ulrich A.: "A light-weight method for trace analysis to support fault diagnosis in concurrent systems"; Journal of Systemics, Cybernetics and Informatics, 1, 6 (2003), 6pp.

[Reisig 1985] Reisig, W.: "Petri Nets. An Introduction"; Springer-Verlag (1985), 15,62 – 66.

[Reisig 1992] Reisig, W.: "A Primer in Petri Net Design"; Springer-Verlag (1992), 25 – 33.

[Tabakow 2000] Tabakow, I.G.: "Using Petri net invariants in system diagnosis"; Petri Net Newsletter 58 (2000), 21 – 31.

[Tabakow 2002] Tabakow, I.G.: "An introduction to the place-transition nets k-distinguishability"; Concurrency, Specification and Programming. Workshop.vol.2,Humboldt-Universität zu Berlin , Germany (2002), 355 – 369.

[Tabakow 2003] Tabakow, I.G.: "Using Test Points to Improve the Place –Transition Net k-Distinguishability"; Proc. of the 7th World Multiconference on Systemics, Cybernetics and Informatics SCI 2003, Orlando, Florida USA, IX: Computer Science and Engineering II (Jul 2003), 173 - 178.

[Tabakow 2005] Tabakow, I.G.: "Using place invariants to isolate faults in concurrent systems"; Petri Net Newsletter 68, Germany (2005),10 – 20.

[Tabakow 2005a] Tabakow, I.G.: "Fault Diagnosis of Discrete Event Systems Using Place Invariants"; Ninth International Conference on Knowledge-Based & Intelligent Information & Engineering Systems KES'2005, Invited Session on Communicative Intelligence, Melbourne, Australia, September 14 - 16 (2005) in: LNCS, Springer-Verlag vol. 3682 (2005), 541 - 547.

[Zhou and DiCesare 1993] Zhou M.C. and DiCesare F., "Petri net synthesis for discrete event control of manufacturing systems"; Kluwer AcademicPublishers, Dordrecht, Boston, London (1993), 233 pp.