IMMEDIATE DIAGNOSIS OF FAULTY BEHAVIOURS WITH PETRI NET MODELS

Dimitri Lefebvre

GREAH - Université Le Havre -76063 - Le Havre - France
dimitri.lefebvre@univ-lehavre.fr

Abstract: This paper is about fault detection and isolation for discrete event systems modeled with Petri nets. Faults are represented with failure transitions and a faulty behaviour occurs when a sequence of transitions is fired that contains at least one failure transition. The main contribution is to provide necessary and sufficient conditions to be satisfied by a given set of observable places for immediate detection and isolation of faulty behaviours. The diagnosis is immediate in the sense that the unsuitable behaviours are detected and isolated immediately after the occurrence of the faults and before the occurrence of any other event.

Keywords: faults detection and isolation, Petri nets, state observers, estimation.

1. INTRODUCTION

Fault detection and isolation are important issues for discrete event systems (DES) (Cassandras, 1993). Some applications of the supervisory control in fault detection have been developed that consider faults as forbidden states (Ramadge and Wonham, 1989). The observation of the marking was further investigated in order to design controllers with forbidden marking specifications (Giua and Seatzy, 2002). Another approach to study DES with faulty behaviours concerns PN models with failure transitions (Ushio *et al.*, 1998). In that case, the problem consists to detect and isolate the firing of failure transitions in a firing sequence. Both approaches are concerned with estimation algorithms: with the first approach, firing sequences are observed and marking is estimated and, in the second one, marking is measured and firing sequences are estimated.

This article focus on the second approach. Our aim is to provide some contributions useful to decide which sets of places are necessary and sufficient to be observed to detect and isolate a fault in a given unobservable firing sequences. Faults are represented with failure transitions and faulty behaviours result from the occurrence of firing sequences that include some failure transitions (Alcaraz-Mejia *et al.*, 2003; Chung *et al.*, 2003; Sampath *et al.*, 1995; Ushio *et al.*, 1998). Admissible sets of observable places (AOSP) and minimal AOSP (MAOSP) are characterized. An algorithm is also proposed that provides the list of all transitions subsets, for which a set of place is a MAOSP. At last, another algorithm is detailed that works out all MAOSP to estimate a given list of transitions subsets.As a consequence, “immediate diagnosers” are introduced. An “immediate diagnoser” detects and isolates a faulty behaviour immediately after the occurrence of the faults and before the occurrence of any other event. On the contrary, a “delayed diagnoser” may require the occurrence of intermediate events: it detects and

isolates the firing of failure transitions according to the observable traces generated by the system. Another article is proposed by the author to IFAC 05 that concerns "delayed" diagnosers based on the investigation of directed paths and causality relationships in PN models (Lefebvre *et al.,* 2004).

The paper is divided into 6 sections. The section 2 is about Petri nets. The section 3 gives an overview of the relevant literature. The section 4 concerns the characterization of AOSP and MAOSP for Petri nets models. In section 5, an example is discussed.

2. PETRI NETS

A Petri net (PN) with n places and p transitions is defined as $< P, T,$ Pre, Post, $M_I >$ where $P=\{P_i\}_{i=1,...,n}$ is a not empty finite set of places, $T=\{T_j\}_{j=1,...,p}$ is a not empty finite set of transitions, such that $P \cap T = \varnothing$. IN is defined as the set of integer numbers and IR^+ as the set of non negative real numbers. Pre: $P \times T \rightarrow IN$ is the pre-incidence application: Pre (P_i, T_j) is the weight of the arc from place P_i to transition T_j and $W_{PR} = (w^{PR}_{ij})_{i=1,...,n,\ j=1,...,p} \in IN^{n \times p}$ with w^{PR}_{ij} = Pre (P_i, T_j) is the pre-incidence matrix. Post: $P \times T \rightarrow IN$ is the post-incidence application: Post (P_i, T_j) is the weight of the arc from transition T_j to place P_i and $W_{PO} = (w^{PO}_{ij})_{i=1,...,n,\ j=1,...,p} \in IN^{n \times p}$ with w^{PO}_{ij} = Post (P_i, T_j) is the post-incidence matrix (Askin and Standridge, 1993; Brams, 1983; David and Alla, 1992; Diaz *et al*., 2001). The PN incidence matrix W is defined as $W = W_{PO} - W_{PR} \in IN^{n \times p}$. Let us also define $M = (m_i)_{i=1,...,n} \in IN^n$ as the marking vector and $M_I \in IN^n$ as the initial marking vector. ${}^\circ T_j$ (resp. $T_j{}^\circ$) stands for the preset (resp. post-set) places of T_j. Similarly, ${}^\circ P_i$ (resp. $P_i{}^\circ$) stands for the preset (resp. post-set) transitions of P_i. A firing sequence is defined as an ordered series of transitions that are successively fired from marking M to marking M'. Such a sequence is represented by its characteristic vector $X = (x_j)_{j=1,...,p} \in IN^p$ where x_j stands for the enabling degree of T_j. The marking M' resulting from the marking M after firing the sequence X is given by (1) (Murata, 1989; Vidal-Naquet and Choquet-Geniet, 1992):

$$\Delta M = M' - M = W.X. \qquad (1)$$

A subnet PN' of PN with n' places and p' transitions is defined as $< P', T',$ Pre', Post', $M'_I >$ with $P' \subset P$ and $T' \subset T$. Pre': $P' \times T' \rightarrow IN$ and Post': $P' \times T' \rightarrow IN$ are respectively the restrictions of the pre and post-incidence applications limited to the subsets P' and T'. $M'_I \in IN^{n'}$ is the initial marking vector of PN'. In that sense, a subnet PN' is defined for any subsets of places $P' = \{P'_i\}_{i=1,...,n'}$ and transitions $T' = \{T'_j\}_{j=1,...,p'}$. The marking vector $M' = (m'_i)_{i=1,...,n'} \in IN^{n'}$ of PN' is defined as the projection $M' = Q.M$ of the vector M over the set P' with $Q \in \{0, 1\}^{n' \times n}$. The same holds for the firing sequences vector $X' = (x'_j)_{j=1,...,p'} \in IN^{p'}$ of PN' that is defined as the projection $X' = D.X$ of the vector X over the set T' with $D \in \{0, 1\}^{p' \times p}$. The incidence matrix W' of PN' is defined in the same way as W. When two transitions T_j and $T_{j'}$ have one or several common places P_i in the preset (i.e. $\{T_j, T_{j'}\} \in P_i{}^\circ$), the PN has a structural conflict. Such a conflict can be considered as a subnet PN' with $P' = \{P_i\}$ and $T' = \{P_i{}^\circ\}$. The conflict becomes an effective one if there are not enough tokens in the common place(s) to fire both transitions.

The PN considered in this paper are autonomous PN. But all the proposed results are also available for other extensions of PN as timed PN or continuous PN (David and Alla, 1992; Diaz *et al*., 2001), because they are based on the study of the underlying digraph structure.

3. RELEVANT LITERATURE

Faults diagnosis in the context of DES was first formulated with automata (Sampath *et al.*, 1995) and then extended to PN (Chung *et al.*, 2003; Ushio *et al.*, 1998) with unobservable places. The considered PN are live, safe and have no unobservable cycle. A label $L \in \Delta = \{N\} \cup \Delta_F$ is associated to each transition. $L = N$ is interpreted as a "normal" behaviour; $L = F_k$ means that a failure of type k has occurred. $\Delta_F = \{F_k\}_{k = 1,...K}$ is the set of failure labels. Normal transitions and failure transitions appear usually in structural conflicts. Starting from an initial normal state, the system may evolve according to a "normal" behaviour by firing a "normal" transition or according to a faulty behaviour by firing a "failure" transition. The state of a PN model-based diagnoser consists of pairs of marking and label.

On the one hand, the diagnosability of the system is usually based on the study of undetermined cycles included in the marking tree of the associated diagnoser (Chung *et al.*, 2003; Ushio *et al.*, 1998). A cycle is called "determined" if it contains at least one state that results with no ambiguity from a normal firing sequence, or from a F_k - failure firing sequence (a firing sequence that contains a F_k - failure transition). Characterisation of the cycles is obtained according to label propagation and range functions. On the one hand, label propagation functions decide how to assign the failure labels from a diagnoser state to another over an observed sequence. On the other hand, range functions tell us how to estimate all the next possibly diagnoser states from an initial state and after an observable event. Starting from an observable initial marking, the diagnoser detects and isolates a failure transition in a given firing sequence from measurement of the successive observable markings generated by the system. The resulting diagnosers are "delayed" diagnosers in the sense that the occurrence of intermediate events may be necessary to detect and isolate the faults. On the

other hand, the problem of sensor selection for discrete event systems was investigated as an optimisation problem (Debouk *et al.,* 1999) It was also proved that deciding if a sensor selection satisfies diagnosability is an NP – problem (Yoo *et al.,* 2002).

Our contribution in the following section is to provide structural tools (i.e. not depending on the marking) to work out necessary and sufficient conditions to characterize admissible sets of observable places (AOSP) and minimal AOSP (MAOSP) for immediate diagnosis. A faulty behaviour is "immediately" detected if no intermediate event occurs between the occurrence of fault and the detection. Several differences between the undetermined cycles based approach and our approach must be noticed. The determination of undetermined cycles requires the construction of the observable marking tree. This approach is behavioural in the sense that it is based on the analysis of the state evolution. On the contrary, our approach takes into consideration the digraph structure of PN to provide structural information not depending on the state evolution. To work out the marking tree is not necessary. Another difference is that the undetermined cycles based approach provides delayed diagnosers whereas our approach provides immediate diagnosers. Thus, both results are complementary. Conditions for delayed diagnosis are less restrictive but the occurrence of intermediate events must be tolerated, whereas conditions for immediate diagnosis are stronger but no intermediate event occurs before the alarm. At last one can notice that the systematic determination of the set of AOSP and MAOSP is useful to decide the number and location of sensors that are required according to a given finite set of faults to be detected and isolated. The proposed algorithms provide immediate diagnosis whatever the initial marking is. No assumption are required concerning the safety and liveness of the PN models.

4. SETS OF OBSERVABLE PLACES FOR IMMEDIATE FIRING ESTIMATION

In the context of faults diagnosis, the determination of admissible sets of observable places (AOSP) and minimal AOSP (MAOSP) is concerned with the estimation of firing sequences that may include some failure transitions.

Let us divide the set P of PN places into the set P_O of m observable places and the set P_U of n-m unobservable ones: $P = P_O \cup P_U$. Only the marking M_O of the observable places is assumed to be measured. According to this partition, let us define the permutation matrix $Q \in IN^{n\,x\,n}$ such that $Q.M = (M^T_O, M^T_U)^T$ with $M_O \in IN^{+\,m}$, and $M_U \in IN^{+\,n-m}$. Let us also define a list $\theta \subset T^{p'}$ of p' subsets $\theta_k \subset T$ of transitions (eventually a list of p' transitions) and consider $X(\theta)$ the firing vector to be estimated: $X(\theta) = D(\theta).X$, where $D(\theta) \in \{0, 1\}^{p'x\,p}$ is a projector in the space of the firing sequences and $X(\theta) \in IN^{+\,p'}$. In other words, the k^{th} row of the matrix $D(\theta)$ characterizes θ_k, and the number of firings in the k^{th} subset of transitions (i.e. the k^{th} entry of $X(\theta)$) has to be estimated from the measurement of the observable marking M_O. Equation (1) results in (2):

$$Q\Delta M = Q.W.D(\theta)^{-1}.D(\theta).X$$
$$\begin{pmatrix}\Delta M_O\\ \Delta M_U\end{pmatrix} = \begin{pmatrix}W_O\\ W_U\end{pmatrix}.X(\theta) \qquad (2)$$

Linear algebra properties provide an exact estimation $\hat{X}(\theta)$ of the vector $X(\theta)$ if the matrix $D(\theta)$ is square and regular and W_O is of full column rank (Lefebvre and El Moudni, 2001). But, in many cases these conditions are not satisfied and the PN model must be completed with additive observable places (Lefebvre and El Moudni, 2001).

Another solution is to use not only linear relations but also information about the sign of the marking variation. Let us define for this purpose AOSP and MAOSP to estimate $X(\theta)$ and consider the following assumptions:

Hypothesis 1*: The considered PN has no selfloop (i.e. $\{P_i, T_j\}$ is a selfloop if $Pre(P_i, T_j) = Post(P_i, T_j)$).*

Hypothesis 2*: There is no simultaneous firing and there exists always an observation between two consecutive firings in a given firing sequence.*

The reason for hypothesis 1 is that the firing of a transition in a selfloop is always undetectable because it does not have any influence on the marking variation (figure 1, $\{P_4, T_3\}$ is a selfloop). The reason for hypothesis 2 is similar. For example the marking of a cycle with 2 places and 2 transitions is not modified if there is no observation between the firing of the first transition and the firing of the second one (figure 1, $\{P_2, T_3, P_3, T_4\}$ is a cycle). Moreover the marking of a given place is not modified if a transition in the preset and another one in the post – set are simultaneously fired (figure 1, the marking of the place P_1 is not changed if transitions T_1 and T_2 are simultaneously fired). According to hypothesis 2, $X(\theta) \in \{0, 1\}^{p'}$ and $||X(\theta)|| \leq 1$ (i.e. the p' entries of $X(\theta)$ are either 0 or 1 and $X(\theta)$ has at more one non zero entry).

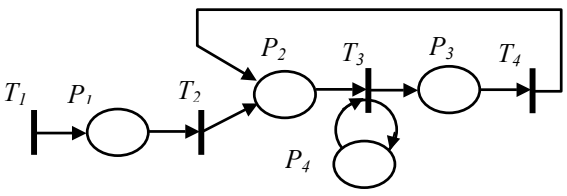

Figure 1: Example of PN with selfloops and cycles

Definition 1: *The subset of places $P_O \subset P$ is called an admissible observation set of places (AOSP) to estimate the firings of θ if hypothesis 1 and 2 are satisfied and if $X(\theta)$ can be estimated from the measurement of the marking vector variation ΔM_O*

P_O is an AOSP to estimate the firings of θ means that one can detect a firing in θ before the occurrence of any other event, by observing each place $P_i \in P_O$ before and after the transitions firing. Moreover one can isolate which subset $\theta_k \subset T$ is concerned.

Definition 2: *The subset of places $P_O \subset P$ is called a minimal admissible observation set of places (MAOSP) to estimate $X(\theta)$ if P_O is an AOSP to estimate $X(\theta)$ and if there is no subset of places $P' \subset P_O$, $P' \neq P_O$ that is an AOSP to estimate $X(\theta)$.*

P_O is an MAOSP to estimate the firings of θ means that P_O is a minimal AOSP for inclusion.

The problem that is solved in this section is to give necessary and sufficient conditions in order to decide if the set P_O of observable places is an AOSP or an MAOSP to estimate $X(\theta)$.The propositions 1 to 3 take advantage of the sign of the marking variation to estimate $X(\theta)$. Constructive algorithms are also provided to answer the following questions. Given a subset P_O of places, what is the list θ of transitions subsets, for which P_O is a MAOSP ? Given a list $\theta \subset T^{p'}$ of transitions subsets, what are all MAOSP to estimate the vector $X(\theta)$?

Proposition 1*: Let us consider the case of a unique observable place $P_O = \{P_i\}$. The following necessary and sufficient conditions hold:*

a) $\Delta M_i > 0$ if and only if there exists a unique $T_j \in {}^\circ P_i$ such that $X(T_j) = +1$.

b) $\Delta M_i < 0$ if and only if there exists a unique $T_j \in P_i^\circ$ such that $X(T_j) = +1$.

c) $\Delta M_i = 0$ if and only if $\forall T_j \in {}^\circ P_i \cup P_i^\circ$, $X(T_j) = 0$.

Proof: if $\Delta M_i > 0$, then according to hypothesis 2, there exists a unique $T_j \in {}^\circ P_i$ such that $X(T_j) = +1$. Reciprocally, if there exists a unique $T_j \in {}^\circ P_i$ such that $X(T_j) = +1$, then hypothesis 1 and 2 lead to $\Delta M_i > 0$. Thus condition a) holds. Condition b) is similarly obtained. Concerning condition c), one can state: if for all $T_j \in {}^\circ P_i \cup P_i^\circ$, $X(T_j) = 0$, then $\Delta M_i = 0$. Reciprocally, if $\Delta M_i = 0$, then the hypothesis 1 and 2 lead to $X(T_j) = 0$, for all $T_j \in {}^\circ P_i \cup P_i^\circ$. Thus condition c) holds.

Proposition 2*: Let us consider the case of a set of observable places $P_O \subset P$. The following necessary and sufficient conditions hold:*

a) For all $P_i \in P_O$, $\Delta M_i > 0$ if and only if there exists a unique $T_j \in \bigcap_{P_i \in P_O} {}^\circ P_i$ such that $X(T_j) = +1$.

b) For all $P_i \in P_O$, $\Delta M_i < 0$ if and only if there exists a unique $T_j \in \bigcap_{P_i \in P_O} P_i^\circ$ such that $X(T_j) = +1$.

c) For all $P_i \in P_O$, $\Delta M_i = 0$ if and only if $\forall T_j \in \bigcup_{P_i \in P_O} {}^\circ P_i \cup P_i^\circ$, $X(T_j) = 0$.

Proof: from proposition 1a, we can state that for all $P_i \in P_O$, $\Delta M_i > 0$ if and only if there exists a unique $T_{ji} \in {}^\circ P_i$ such that $X(T_{ji}) = +1$. According to hypothesis 2, $T_j = T_{ji}$ for all $P_i \in P_O$. Thus condition a) holds. Condition b) is similarly obtained. From proposition 1c we can state that for all $P_i \in P_O$, $\Delta M_i = 0$ if and only if for all $T_{ji} \in {}^\circ P_i \cup P_i^\circ$, $X(T_{ji}) = 0$. Thus for all $T_j \in \bigcup_{P_i \in P_O} {}^\circ P_i \cup P_i^\circ$, $X(T_j) = 0$, and condition c) holds.

Let us consider $P_O = P^+{}_O \cup P^-{}_O \cup P^0{}_O \subset P$ such that $P^+{}_O \cup P^-{}_O \neq \varnothing$ and $\Delta M_i > 0$ for all $P_i \in P^+{}_O$, $\Delta M_i < 0$ for all $P_i \in P^-{}_O$, $\Delta M_i = 0$ for all $P_i \in P^0{}_O$. Let us also consider the set of transitions $E(P^+{}_O, P^-{}_O, P^0{}_O) \subset T$ defined as:

$$E(P_O^+, P_O^-, P_O^0) = \left(\bigcap_{P_i \in P_O^+} {}^\circ P_i \right) \cap \left(\bigcap_{P_i \in P_O^-} P_i^\circ \right) \cap \left(\overline{\bigcup_{P_i \in P_O^0} {}^\circ P_i \cup P_i^\circ} \right) \quad (3)$$

where $\overline{(.)}$ stands for the complementary part of (.) in the set of places P. If $\mathrm{card}(P_O) = n'$ then $3^{n'}$-1 partitions exist for P_O according to the subsets $P^+{}_O$, $P^-{}_O$ and $P^0{}_O$.

Proposition 3: *The subset $P_O \subset P$ of cardinality n' is an AOSP to estimate $X(\theta)$ if and only if there exist p' among $3^{n'}$-1, partitions $(P^+{}_O(k), P^-{}_O(k), P^0{}_O(k))$ of the set of places P_O such that $E(P^+{}_O(k), P^-{}_O(k), P^0{}_O(k)) = \theta_k$, $k = 1,...,p'$. Moreover, P_O is MAOSP to estimate $X(\theta)$ if there exists no subset of places $P' \subset P_O$, $P' \neq P_O$ that verifies the previous property.*

Proof: let us consider a subset of transitions θ_k, $k = 1,...,p'$ such that $X(\theta_k) = +1$ (i.e. a unique transition of θ_k is fired between two consecutive marking measurements). If there exists a partition $(P^+{}_O(k), P^-{}_O(k), P^0{}_O(k))$ of the set of places P_O such that $E(P^+{}_O(k), P^-{}_O(k), P^0{}_O(k)) = \theta_k$ then according to proposition 2, we have: $\Delta M_i > 0$ for all $P_i \in P^+{}_O(k)$, $\Delta M_i < 0$ for all $P_i \in P^-{}_O(k)$ and $\Delta M_i = 0$ for all $P_i \in P^0{}_O(k)$. Thus $P_O \subset P$ is an AOSP to estimate the firing of θ_k.

Given a subset P_O of n' places and let $G(P_0)$ defined by equation (4):

$$G(P_O) = \{E(P_O^+, P_O^-, P_O^0), P_O = P_O^+ \cup P_O^- \cup P_O^0, P_O^+ \cup P_O^- \neq \emptyset\} \quad (4)$$

The algorithm 1 provides the list θ of all transitions subsets, for which P_O is a MAOSP.

Algorithm 1:
1. Let $P_O = \{P_{\alpha(1)}, \ldots, P_{\alpha(n')}\}$.
2. Let $k = 1$.
3. $P^+{}_O = P^-{}_O = P^0{}_O = \emptyset$.
4. For every $P_{\alpha(i)} \in P_O$ repeat 5 to 7:
5. $k = 3.q + r$, $q \in IN$, $r \in IN$, $r < 3$.
6. If $r = 2$, then $P^+{}_O = P^+{}_O \cup P_{\alpha(i)}$.
   If $r = 1$, then $P^-{}_O = P^-{}_O \cup P_{\alpha(i)}$.
   If $r = 0$, then $P^0{}_O = P^0{}_O \cup P_{\alpha(i)}$.
7. $\theta = \{\theta \mid E(P^+{}_O, P^-{}_O, P^0{}_O)\}$.
8. $k = k + 1$.
9. Goto 3 until $k = 3^{n'} - 1$.

Given a list $\theta \subset T^{p'}$ of p' transitions subsets $\theta_k \subset T$ and let $G(\theta_k)$ defined by equation (5):

$$G(\theta_k) = \{(P_O^+ \cup P_O^- \cup P_O^0), P_O^+ \subset P_O, P_O^- \subset P_O, P_O^0 \subset P_O, P_O^+ \cup P_O^- \neq \emptyset, \quad E(P_O^+, P_O^-, P_O^0) = \theta_k\} \quad (5)$$

The recursive algorithm 2 based on a combinatory exploration of the PN subsets of places works out all MAOSP to estimate $X(\theta_k)$.

Algorithm 2:
1. If $P_O = \{P_{\alpha(1)}, \ldots, P_{\alpha(n')}\}$ is an AOSP to estimate the firings of θ_k then $r = 1$ else $r = 0$.
2. If $r = 1$ goto 3 else goto 9.
3. Let $rm = 0$.
4. For every $P_{\alpha(i)} \in P_O$ repeat 5 to 7:
5. Let $P'_O = \{P_{\alpha(1)}, \ldots, P_{\alpha(i-1)}, P_{\alpha(i+1)}, P_{\alpha(n')}\}$.
6. Determine all MAOSP (G', r') in P'_O to estimate the firing of θ_k.
7. $rm = rm + r'$.
8. If $rm = 0$ and $P_0 \notin G(\theta_k)$ then $G(\theta_k) = \{ G(\theta_k) \mid P_0\}$, end if.
9. End.

Both algorithms are illustrated in section 5.

5. EXAMPLE

Let us consider the PN in figure 2 as an example (Ushio *et al.*1998). All transitions are assumed to be unobservable. The transitions T_4 and T_5 represent two failure events F_4 and F_5. The set of observable places is $P_O = \{P_1, P_2, P_3\}$ the set of unobservable places is given by $P_U = \{P_4, P_5\}$.
With the help of proposition 3 it is easy to state that the set of observable places $P_O = \{P_1, P_2, P_3\}$ is an AOSP to estimate immediately the firing of $\theta_1 = \{T_4\}$ (detection and isolation of fault F_4) It is also an AOSP to estimate immediately the firing of $\theta_2 = \{T_5\}$ (detection and isolation of fault F_5). At last it is an AOSP to estimate immediately the firing of the subset of transitions $\theta_3 = \{ T_4, T_5 \}$ (detection of faults F_4 and F_5).

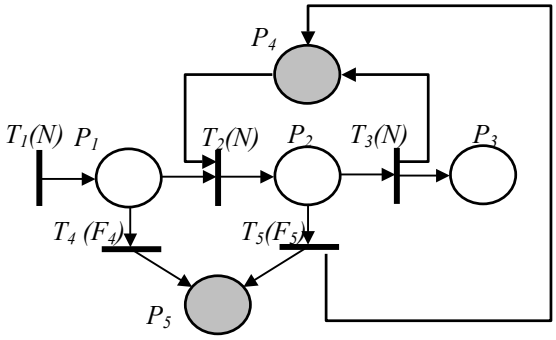

Figure 2: Example of a PN model based diagnoser

The same proposition is helpful to state that $P_O = \{P_1, P_2, P_3\}$ is not a MAOSP to estimate immediately the firing of the failure transition T_4 ($\{P_1, P_2\} \subset \{P_1, P_2, P_3\}$ is a AOSP for $\{T_4\}$) neither a MAOSP to estimate immediately the firing of the failure transition T_5 ($\{P_2, P_3\} \subset \{P_1, P_2, P_3\}$ is a AOSP for $\{T_5\}$). But $P_O = \{P_1, P_2, P_3\}$ is a MAOSP to estimate immediately the firing of the subset of transitions $\theta_3 = \{T_4, T_5\}$.

Table 1 : MAOSP for θ_1, θ_2, θ_3 and θ

Subsets of transitions to be estimated	Corresponding MAOSP
$\theta_1 = \{T_4\}$	$\{P_4, P_5\}$, $\{P_2, P_5\}$, $\{P_1, P_5\}$, $\{P_1, P_4\}$, $\underline{\{P_1, P_2\}}$
$\theta_2 = \{T_5\}$	$\{P_4, P_5\}$, $\{P_2, P_5\}$, $\{P_1, P_5\}$, $\{P_3, P_4\}$, $\underline{\{P_2, P_3\}}$
$\theta_3 = \{T_4, T_5\}$	$\{P_5\}$, $\underline{\{P_1, P_2, P_3\}}$, $\{P_1, P_3, P_4\}$
$\theta = \{\{T_4\}, \{T_5\}\}$	$\{P_4, P_5\}$, $\{P_2, P_5\}$, $\{P_1, P_5\}$, $\underline{\{P_1, P_2, P_3\}}$, $\{P_1, P_3, P_4\}$

The use of algorithm 2 provides all MAOSP for the estimation of $\{T_4\}$, $\{T_5\}$, or $\{T_4, T_5\}$ in a systematic way (the observable set of places are underlined, the common MAOSP for $\{T_4\}$ and $\{T_5\}$ are in bold). The MAOSP to estimate immediately the firings of $\theta = \{\theta_1, \theta_2\} = \{\{T_4\}, \{T_5\}\}$ are obtained as combination of the MAOSP to estimate the firings of θ_1 and θ_2. Let us mention that each MAOSP to estimate the firing of $\theta_3 = \{T_4, T_5\}$ is included in one MAOSP, at least, required to estimate the firings of $\theta = \{\{T_4\}, \{T_5\}\}$.

The use of algorithm 1 provides the list of all subsets of transitions for which the considered subset of places is a MAOSP.

As a conclusion one can state hat the sets of observable places $P_O = \{P_1, P_2, P_3\}$ is sufficient to detect and isolate the faults F_4 and F_5. But the observation of the complete set is not necessary if only one fault is considered F_4 or F_5. Finally, if the location of the sensors can be modified, the analysis points out that the subsets $\{P_4, P_5\}$, $\{P_2, P_5\}$, or $\{P_1, P_5\}$ are necessary and sufficient for detection and isolation of the faults F_4 and F_5. Moreover a single sensor in $\{P_5\}$ is also sufficient for detection (but not for isolation) of the faults F_4 and F_5.

Table 2 : List of transitions subsets whose firing can be estimated thanks to the observation of the marking of the MAOSP of $\{T_4\}$ and $\{T_5\}$.

Subset of places to be observed	List of transitions subsets
$\{P_4, P_5\}$	$\{\{T_1\}, \{T_3\}, \{T_4\}, \{T_5\}\}$
$\{P_2, P_5\}$	$\{\{T_1\}, \{T_3\}, \{T_4\}, \{T_5\}\}$
$\{P_1, P_5\}$	$\{\{T_1\}, \{T_2\}, \{T_4\}, \{T_5\}\}$
$\{P_1, P_4\}$	$\{\{T_1\}, \{T_2\}, \{T_4\}, \{T_3, T_5\}\}$
$\{P_1, P_2\}$	$\{\{T_1\}, \{T_2\}, \{T_4\}, \{T_3, T_5\}\}$
$\{P_3, P_4\}$	$\{\{T_2\}, \{T_3\}, \{T_5\}\}$
$\{P_2, P_3\}$	$\{\{T_2\}, \{T_3\}, \{T_5\}\}$

Table 3 : List of transitions subsets whose firing can be estimated thanks to the observation of the marking of the MAOSP of $\{T_4, T_5\}$.

Subset of places to be observed	List of transitions subsets
$\{P_5\}$	$\{T_4, T_5\}$
$\{P_1, P_2, P_3\}$	$\{\{T_1\}, \{T_2\}, \{T_3\}, \{T_4\}, \{T_5\}\}$
$\{P_1, P_3, P_4\}$	$\{\{T_1\}, \{T_2\}, \{T_3\}, \{T_4\}, \{T_5\}\}$

6. CONCLUSIONS

Fault detection and isolation for discrete event systems modeled with PN has been investigated from a structural point of view. For this purpose necessary and sufficient conditions have been established to be satisfied by a given set of observable places for immediate detection and isolation of faulty behaviours resulting from the occurrence of firing sequences including some failure transitions. The proposed results are easy to apply in the sense that they result in two complementary algorithms. The first algorithm starts from a set of observable places and computes the list of transitions subsets whose firing is detected and isolated. The second algorithm starts from a list of transitions subsets and computes the list of places subsets to be observed.

The perspectives of this work concern the design of delayed diagnosers. In this context, directed paths and causality relationships in PN will be further investigated (Lefebvre and Delherm, 2003; 2004) to analyse the observable traces generated by the system when a fault occurs.

REFERENCES

Alcaraz-Mejia M., Lopez-Mellado E., Ramirez-Trevino A., Rivera-Rangel I., (2003), Petri net based fault diagnosis of DES, *Proc IEEE Conf. SMC03*, pp. 4730-4735, Washington, USA.

Askin R.G., Standridge C. R., (1993), *Modelling and analysis of Petri nets*, John Wiley and sons Inc.

Brams G.W., (1983), *Réseaux de Petri*, Masson, Paris.

Cassandras C.G., (1993), *Discrete event systems: modeling and performances analysis,* Irwin, Boston, MA.

Chung S.L, Wu C.C., Jeng M., (2003), Failure diagnosis: a case study on modeling and analysis by Petri nets, *Proc IEEE Conf. SMC03*, pp. 2727-2732, Washington, USA.

David R., Alla H., (1992), *Petri nets and grafcet – tools for modelling discrete events systems*, Prentice Hall, London.

Debouk R., Lafortune S., Teneketzis D., (1999), On An Optimization Problem In Sensor Selection, *Proc. IEEE Conf. CDC99*, Phoenix , AZ.

Diaz M., (éditor), (2001), *Les réseaux de Petri*, Hermes, Paris.

Giua A., Seatzy C., (2002), Observability of place / transition nets, *IEEE – TAC*, vol. 47, no. 9, pp. 1424 – 1437.

Lefebvre D., El Moudni A., (2001), Firing and enabling sequences estimation for timed Petri nets, *IEEE-SMC, part A*, vol. 31, no.3, pp 153-62.

Lefebvre D, Delherm C., (2003), Structural sensitivity for the conflicts analysis in Petri nets, *Proc IEEE SMC03*, pp. 1051 – 1058, Washington, USA.

Lefebvre D, Delherm C., (2005), Causality relationships and directed paths in Petri net models for the diagnosis of DES, *Proc. IFAC 05.*

Murata T., (1989), Petri nets: properties, analysis and applications, *Proc. IEEE*, vol.77, n°. 4, pp 541-580.

Ramadge P.J., Wonham W.M., (1989), The control of discrete event systems, *Proc. IEEE*, vol. 77, no.1, pp. 81 – 91.

Sampath M., Sengupta R., Lafortune S., Sinnamohideen K., Teneketzis D., (1995), Diagnosibility of discrete event systems, *IEEE-TAC*, vol. 40, no.9, pp. 1555- 1575.

Ushio T., Onishi I., Okuda K., (1998), Fault detection based on Petri net models with faulty behaviours, *Proc. IEEE Conf. SMC98*, pp 113-118, San Diego, CA.

Vidal-Naquet G., Choquet-Geniet A., (1992) *Réseaux de Petri et systèmes parallèles*, A. Colin, Paris.

Yoo T., Lafortune S. (2002), NP-Completeness of Sensor Selection Problems Arising In Partially-observed Discrete-Event Systems *IEEE-TAC*, vol. 47, no. 9, pp. 1495-1499.