DIAGNOSIS WITH CAUSALITY RELATIONSHIPS AND DIRECTED PATHS IN PN MODELS

Dimitri Lefebvre, Catherine Delherm

Université Le Havre – GREAH, 25 rue P. Lebon, 76063 Le Havre, France
{dimitri.lefebvre;catherine.delherm}@univ-lehavre.fr

Abstract: Petri nets are a suitable tool for the diagnosis of discrete event systems. For this purpose, faulty behaviours are modelled by the firing of failure transitions. This paper is about structural sensitivity in Petri net with respect to the firing of the failure transitions. Algebraic results are provided to characterise the influence and dependence areas of the failure transitions and diagnosability of the systems is obtained as a consequence. The main advantage of our approach is to investigate the diagnosability without working out the marking tree of the diagnoser. *Copyright ©2005 IFAC*

Keywords: Petri nets, structural properties, sensitivity analysis, estimation, diagnosis.

1. INTRODUCTION

Fault detection and isolation are important issues for discrete event systems (DES) (Cassandras, 1993). Pioneer applications of the Petri nets (PN) supervisory control in fault detection have been developed that consider faults as forbidden states (Krogh, *et al.*,1991). The observation of the state was further investigated in order to design controllers with forbidden marking specifications (Giua, *et al,.* 2002). Another approach to study DES with faulty behaviours concerns PN models with "failure" transitions (Ushio, *et al.,* 1998). In that case, faults are represented with "failure" transitions and faulty behaviours are modelled as firing sequences including some "failure" transitions. The problem consists to detect and isolate the firing of the "failure" transitions that cannot be directly measured. This article focuses on the second approach. The main contribution is to provide some tools useful to decide if a set of observable places and transitions is necessary or sufficient to detect and isolate the firing of "failure" transitions in unobservable firing sequences. For that purpose, influence and dependence areas of the "failure" transitions are investigated according to the directed paths and causality relationships in PN models. Our study is based on the structural sensitivity analysis and result from the algebraic properties of the incidence matrices (Lefebvre, 2003, Lefebvre, *et al.,* 2003). As a consequence, the resulting diagnosers provide delayed alarms, in the sense that they may require the occurrence of intermediate events in order to detect and isolate the firing of "failure" transitions. Another article is proposed by the authors to IFAC 05 that concerns "immediate" diagnosers that detect and isolate the firing of "failure" transitions immediately after the occurrence of the faults (Lefebvre, 2004).

The paper is divided into 5 sections. The section 2 gives an overview of the relevant literature. The section 3 concerns the use of PN models for diagnosability of DES. The section 4 is about the structural sensitivity. The section 5 is devoted to the diagnosability characterisation.

2. RELEVANT LITERATURE

The objective of the diagnosis problem is to identify the occurrence and type of faults based on the observable traces generated by the system. Faults diagnosis in the context of DES was first formulated with automata (Sampath, *et al.,* 1995). The diagnosability of the system is based on the study of the undetermined cycles of the associated diagnoser. The previous results have been extended to PN (Ushio, *et al.,*1998). For the PN under consideration, it is assumed that some places are observable, other places are not, whereas all the transitions are not observable in the sense that their occurrences are not known. Moreover the PN are live and safe, and there does not exist any unobservable cycle. The firing of the transitions is estimated by the changes of marking at observable places. In (Chung, *et al.* 2003) some transitions are assumed to be observable in the sense that their firings can be measured. Asynchronous diagnosis by means of hidden state history reconstruction obtained from alarm observations was also investigated (Benveniste, *et al.,* 2003). This approach relies on PN unfoldings and event structures that are related via some causality relationships. As a consequence, diagnosis is performed by a distributed architecture of supervisors. At last, let us mention that the problem of diagnosis is related to the problem of sensor selection that was investigated for discrete event systems as an optimisation problem (Debouk, *et al.,* 1999) with NP complexity (*Yoo, et al.,* 2002).

Our approach is based neither on marking trees nor on PN unfolding. In fact, marking is not concerned and we focus on causality relationships and directed paths provided by the digraph structure of PN.

3. PN MODELS FOR THE DIAGNOSIS OF DES

3.1. Background notions on Petri nets

A Petri net (PN) with n places and p transitions is defined as $<P, T,$ Pre, Post, $M_0>$ where $P=\{P_i\}_{i=1,\ldots,n}$ is a not empty finite set of places, $T=\{T_j\}_{j=1,\ldots,p}$ is a not empty finite set of transitions, such that $P \cap T = \emptyset$ (David, *et al*., 1992, Murata, 1989). IN is defined as the set of integer 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 $W_{PR}=(w^{PR}_{ij})_{i=1,\ldots,n,\ j=1,\ldots,p} \in IN^{n \times p}$ 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 $W_{PO}=(w^{PO}_{ij})_{i=1,\ldots,n,\ j=1,\ldots,p} \in IN^{n \times p}$ with w^{PO}_{ij} = Post (P_i, T_j) is the post-incidence matrix. The PN incidence matrix W is defined as $W = W_{PO} - W_{PR} \in IN^{n \times p}$. Let us also define $M=(m_i)_{i=1,\ldots,n} \in IN^n$ as the marking vector and $M_0 \in IN^n$ as the initial marking vector. ${}^{\circ}T_j$ (resp $T_j{}^{\circ}$) stands for the pre-set (resp. post-set) places of T_j. A firing sequence is defined as an ordered serie of transitions that are successively fired from marking M to marking M'. Such a sequence is represented by its characteristic vector $X = (x_j)_{j=1,\ldots,p} \in IN^p$ where x_j stands for the number of T_j firings. The marking M' is related to the marking M and to the firing sequence X according to (1):

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

3.2 Subnets and conflicts

A subnet PN' of PN with n' places and p' transitions is defined as $<P', T',$ Pre', Post', $M'_0>$ where $P' \subset P$ is a subset of P and $T' \subset T$ is a subset of 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 sets P' and T'. $M'_0 \in IN^{n'}$ is the initial marking vector of PN'. In that sense, a subnet is defined for any subset of places $P'=\{P'_i\}_{i=1,\ldots,n'}$ and transitions $T'=\{T'_j\}_{j=1,\ldots,p'}$. The marking vector $M'=(m'_i)_{i=1,\ldots,n'} \in IN^{n'}$ of PN' is defined as the projection $M'=D'.M$ of the vector M over the set P' with $D' \in \{0, 1\}^{n' \times n}$. The same holds for the firing sequences vector $X'= (x'_j)_{j=1,\ldots,p'} \in IN^{p'}$ of PN' that is defined as the projection $X' = Q'.X$ of the vector X over the set T' with $Q' \in \{0, 1\}^{p' \times p}$. The incidence matrix W' of PN' is defined in the same way as W. When two transitions T_j and $T_{j'}$ have a common place P_i in the pre-set, the PN has a structural conflict. Such a conflict can be considered as a subnet PN' with $P'=\{P_i\}$ and $T'=\{P_i{}^{\circ}\}$.

3.3 Diagnosability with PN

In order to decide the diagnosability of a given system as well as to perform on line diagnosis with PN models, some additional notations are introduced. A label $L \in \Delta = \{N\} \cup \Delta_F$ is associated to each transition. $L = N$ is interpreted as a normal behaviour and $\Delta_F = \{F_k\},\ _{k = 1,\ldots m}$ is the set of failure labels (i.e. $L = F_k$ means that a failure of type k occurs). The set T of PN transitions is divided into two parts : "normal" transitions and "failure" transitions: $T = T_N \cup T_F$, where $T_F = T_{F1} \cup \ldots \cup T_{Fm}$ is the set of different types of failures. "Normal" transitions and "failure" transitions appear usually in structural conflicts: considering a given 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. At the same time, T is also divided into observable transitions and unobservable ones $T=T_O \cup T_U$, and failures transitions are assumed to be unobservable: $T_F \cap T_O = \emptyset$. At last, the set P of PN places is also divided into observable places and unobservable ones $P=P_O \cup P_U$. The state of a PN model-based diagnoser (Ushio, *et al.,*1998, Chung, *et* *al.,* 2003) consists of pairs of marking and label. When some places and some transitions are unobservable, undetermined cycles may occur. The determination of these 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. One can also notice that CR and DP investigation is not depending on the initial marking. No assumption is required concerning the safety and liveness of the PN models.

Figure1 shows the PN example we will use throughout this paper with $P = \{P_1, P_2, P_3, P_4, P_5\}$ and $T = \{T_1, T_2, T_3, T_4, T_5, T_6, T_7\}$ (Chung *et al.* 2003). The transitions T_1 and T_5 represent failure events F_1 and F_5. The set of observable places is $P_O = \{P_1, P_4, P_5\}$ the set of unobservable places is given by $P_U = \{P_2, P_3\}$ (grey circles in figure 1). The set of observable transitions is $T_O = \{T_2, T_3, T_4\}$, the set of unobservable ones is given by $T_U = \{T_1, T_5, T_6, T_7\}$.

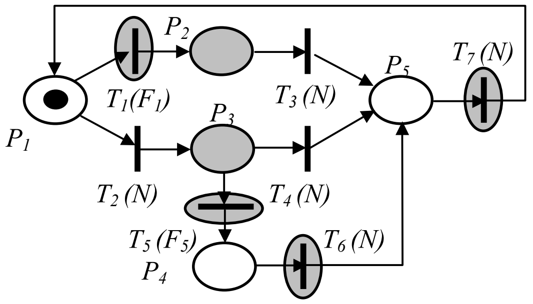

Fig. 1: PN example

4. STRUCTURAL SENSITIVITY IN PN MODELS

The structural sensitivity investigates the causality relationships (CR) and directed paths (DP) expressed by the pre and post incidence matrices (Lefebvre, 2003, Lefebvre, *et al,.* 2003). The CR is helpful to decide if the marking of a given node (place or transition) depends or not on the firing of a F_k - transition (i.e. the occurrence of a failure of type *k*). The DP gives an additive information to decide if such a dependence is direct or not.

Considering again the PN example given in figure 1, DP and CR can be intuitively introduced. A token in P_1 can fire the transition T_2 to move to place P_3, and then fire the transition T_4 or T_5 to move respectively to place P_5 or P_4. Thus, there exists two DP of length 1 place from T_2 to P_5 and from T_2 to P_4. There also exists two DP of length 1 place from T_2 to T_3 and from T_2 to T_4. In the same time, a token that fires T_2, cannot move directly to P_2, but can fire consecutively T_3, T_7 and T_1 to move to P_2. Thus, there exists a DP of length 3 places from T_2 to P_2. But the firing of T_2 will influence directly the marking of P_1 and then the firing of T_1. Thus two CR of length 1 place exists respectively from T_2 to T_1 and from T_2 to P_2.

4.1 Causality relationships

A CR exists from transition T_k to place P_i (resp. transition T_j) if the firing of T_k could yield a deviation of the P_i marking (resp. T_j firing) from its expected value. The minimal CR-rank from T_k to P_i, refereed as $CR(P_i, T_k)$, and from T_k to T_j, refereed as $CR(T_j, T_k)$, are obtained according to the pre and post incidence matrices (Lefebvre 2003):

$$CR(P_i,T_k) = \min_{r \in \{\mathbb{N} \cup \infty\}} \left(C_i^T ((W_{PR}+W_{PO}).(W_{PR})^T)^r.(W_{PR}+W_{PO}).B_k \neq 0\right) \tag{2}$$

$$CR(T_j,T_k) = \min_{r \in \{\mathbb{N} \cup \infty\}} \left(B_j^T ((W_{PR})^T.(W_{PR}+W_{PO}))^r.B_k \neq 0\right)$$

with $B_k = (b^k{}_j) \in \{0, 1\}^p$ such that $b^k{}_j = 0$ if $k \neq j$ and $b^k{}_k = 1$ and $C_i = (c^i{}_j) \in \{0, 1\}^n$ such that $c^i{}_j = 0$ if $i \neq j$ and $c^i{}_i = 1$. The CR - rank can be understood as the minimal number of places in the causality relationship from T_k to P_i or T_j. When no causality relationship exists, the CR-rank equals infinity.

Let us define $CR_{PT} = (CR(P_i, T_k))_{i = 1,\dots,n,\ k = 1,\dots,p} \in \{IN \cup \infty\}^{nxp}$ as the *CR* matrix of the places $P_i \in P$ with respect to the transitions $T_k \in T$ and $CR_{TT} = (CR(T_j, T_k))_{j = 1,\dots,p,\ k = 1,\dots,n} \in \{IN \cup \infty\}^{p \times n}$ as the *CR* matrix of the transitions $T_j \in T$ with respect to the transitions $T_k \in T$. Let us notice that the CR can not be obtained using the usual incidence matrix $W = W_{P0} - W_{PR}$ instead of $W_{P0} + W_{PR}$ because selfloops are ignored with the incidence matrix in the CR calculation.

$$\mathrm{CR}_{PT} = \begin{array}{c} \begin{matrix} T_1 & T_2 & T_3 & T_4 & T_5 & T_6 & T_7 \end{matrix} \\ \begin{pmatrix} 0 & 0 & 1 & 1 & 2 & 1 & 0 \\ 0 & 1 & 0 & 2 & 3 & 2 & 1 \\ 1 & 0 & 2 & 0 & 0 & 2 & 1 \\ 2 & 1 & 3 & 1 & 0 & 0 & 2 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \end{array} \begin{array}{c} \\ P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \end{array} \tag{3}$$

As an example, the *CR* matrix of the places for the PN in figure 1 is given by (3). Any place is sensitive with respect to all transitions. For example $CR_{PT}(P_2,T_2)=1$ (the labelled CR is given by $T_2P_1T_1P_2$) and $CR_{PT}(P_2,T_5) = 3$ (the labelled CR is given by $T_5P_4T_6P_5T_7P_1T_1P_2$).

4.2 Directed paths

A DP exists from transition T_k to place P_i (resp. transition T_j) if a token is able to move from T_k to P_i (resp. T_j). A DP between two nodes is also a CR but a CR between two nodes is not necessary a DP. The minimal DP-rank from T_k to P_i is refereed as $DP(P_i,$

T_k) and the minimal DP-rank from T_k to transition T_j is refereed as $DP(T_j, T_k)$. The following results hold (Lefebvre, 2003):

$$DP(P_i,T_k) = \min_{r \in \{IN \cup \infty\}} (C_i^T (W_{PO}.(W_{PR})^T)^r.W_{PO}.B_k \neq 0)$$

$$DP(T_j,T_k) = \min_{r \in \{IN \cup \infty\}} (B_j^T ((W_{PR})^T.W_{PO})^r.B_k \neq 0) \qquad (4)$$

As previously, let us define $DP_{PT}=(DP(P_i, T_k))_{i=1,\dots,n, k=1,\dots,p} \in \{IN \cup \infty\}^{nxp}$ as the DP matrix of the places $P_i \in T$ with respect to the transitions $T_k \in T$ and $DP_{TT} = (DP(T_j, T_k))_{j=1,\dots,p, k=1,\dots,n} \in \{IN \cup \infty\}^{pxn}$ as the DP matrix of the transitions $T_j \in T$ with respect to the transitions $T_k \in T$. Let us notice that the CR and DP matrices can be considered as an extension of the transitive matrix (Liu, *et al.*, 1999).

For the PN example in figure 1, $DP_{PT}(P_2,T_2)=3$ (the labelled DP is given by $T_2P_3T_3P_5T_7P_1T_1P_2$), $DP_{PT}(P_2,T_5)=3$ (the labelled DP is given by $T_5P_4T_6P_5T_7P_1T_1P_2$).

$$DP_{PT} = \begin{array}{c} \begin{array}{ccccccc} T_1 & T_2 & T_3 & T_4 & T_5 & T_6 & T_7 \end{array} \\ \begin{pmatrix} 2 & 2 & 1 & 1 & 2 & 1 & 0 \\ 0 & 3 & 2 & 2 & 3 & 2 & 1 \\ 3 & 0 & 2 & 2 & 3 & 2 & 1 \\ 4 & 1 & 3 & 3 & 0 & 3 & 2 \\ 1 & 1 & 0 & 0 & 1 & 0 & 2 \end{pmatrix} \end{array} \begin{array}{c} \\ P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \end{array} \qquad (5)$$

4.3 *Subnets sensitivity*

The structural sensitivity analysis can be extended to subnets. For this purpose, let us consider *PN'* as a subnet of *PN*. There exists a CR (resp. DP) from transition T_k to *PN'* if there exists a node $N' \in PN'$ with a CR (resp. DP) from T_k to *N'*. The causality relationships for *PN'* is characterised by the projection of the matrices CR_{PT} and CR_{TT} (resp. DP_{PT} and DP_{TT}) over the subnet *PN'*:

$$CR(PN') = \begin{pmatrix} D' & 0 \\ 0 & Q' \end{pmatrix} \cdot \begin{pmatrix} CR_{PT} \\ CR_{TT} \end{pmatrix} \in \{IN \cup \infty\}^{(n'+p')xp}$$

$$\qquad (6)$$

$$DP(PN') = \begin{pmatrix} D' & 0 \\ 0 & Q' \end{pmatrix} \cdot \begin{pmatrix} DP_{PT} \\ DP_{TT} \end{pmatrix} \in \{IN \cup \infty\}^{(n'+p')xp}$$

5. DIAGNOSABILITY OF PN MODELS

The structural sensitivity is helpful to decide the diagnosability of a system modeled by PN, in the sense that it provides in a systematic way the CR and DP between a "failure" transition and another node of PN. In the following, the influence and dependence areas of "failure" transitions are studied in order to evaluate the information provided by the set of observable places and transitions.

5.1 *Influence and dependence areas*

The set $I_{CR}(T_k)$ of nodes that are CR-sensitive with respect to the transition T_k is called the CR - influence area of T_k. This area is a subnet of *PN* defined as $I_{CR}(T_k) = <P_{ICR}(T_k), T_{ICR}(T_k), \text{Pre}_{ICR}(T_k), \text{Post}_{ICR}(T_k)>$ where $P_{ICR}(T_k) \subset P$ is the set of places P_i such that a CR exists from T_k to P_i (i.e. $CR(P_i, T_k) < \infty$), $T_{ICR}(T_k) \subset T$ is the set of transitions T_j such that a CR exists from T_k to T_j (i.e. $CR(T_j, T_k) < \infty$), $\text{Pre}_{ICR}(T_k)$ and $\text{Post}_{ICR}(T_k)$ are the restrictions of the pre - incidence and post – incidence applications limited to the sets $P_{ICR}(T_k)$ and $T_{ICR}(T_k)$. The DP - influence area $I_{DP}(T_k)$ is defined in a similar way.

We can also define the CR - dependence area of the node *N*. The set $T_{DCR}(N)$ of transitions that are likely to influence the node *N* through a causality relationship is called the CR - dependence area of *N*. The DP - dependence area $T_{DDP}(N)$ is defined in a similar way. The characterisation of the sets $I_{CR}(T_k)$, $I_{DP}(T_k)$, $T_{DCR}(N)$ and $T_{DDP}(N)$, results from the CR and DP matrices according to table 1 (Lefebvre *et al.*, 2003).

Table 1 : Influence and dependence areas

	CR	***DP***
$P_{I..}(T_k)$	position of the finite entries of the k^{th} column of CR_{PT}	position of the finite entries of the k^{th} column of DP_{PT}
$T_{I..}(T_k)$	position of the finite entries of the k^{th} column of CR_{TT}	position of the finite entries of the k^{th} column of DP_{TT}
$T_{D..}(P_i)$	position of the finite entries of the i^{th} row of CR_{PT}	position of the finite entries of the i^{th} row of DP_{PT}
$T_{D..}(T_j)$	position of the finite entries of the j^{th} row of CR_{TT}	position of the finite entries of the j^{th} row of DP_{TT}

Let us consider again the PN in figure 1. From the matrices CR_{PT} and DP_{PT} given by (3) and (5) one can first notice that $CR_{PT}(P,T_1)= (0\ 0\ 1\ 2\ 1)^T$ and $DP_{PT}(P,T_1)= (2\ 0\ 3\ 4\ 1)^T$. Similarly, $CR_{PT}(P_2,T)= (0\ 1\ 0\ 2\ 3\ 2\ 1)^T$ and $DP_{PT}(P_2,T)= (0\ 3\ 2\ 2\ 3\ 2\ 1)^T$. Thus $P_{ICR}(T_1) = P_{IDP}(T_1) = \{P_1, P_2, P_3, P_4, P_5\}$ and $T_{DCR}(P_2) = P_{DDP}(P_2) = \{T_1, T_2, T_3, T_4, T_5, T_6, T_7\}$.

5.2 *Diagnosability based on DP and CR*

According to the PN models described in section 3, faults are represented by specific transitions in structural conflicts. In order to study the potential influence of the failure F_k, let us consider the subnet PN' = $\{°T_k, (°T_k)°\}$ that contains all T_k upstream places and all transitions in conflict with T_k, The following propositions hold:

Proposition 1 : Let $N \in P_O \cup T_O$. A necessary condition such that the observation of node N contributes to the diagnosis of F_k is $N \in I_{CR}(T_k)$.

Proof : If $N \notin I_{CR}(T_k)$, then the firing of T_k does not influence the variable attached to the node N, and the measurement of this variable is not of interest for detection and isolation of failure F_k..

More results are obtained with the investigation of the sensitivity in the subnet PN/T_k where the transition T_k has been removed.

Proposition 2: Let $N \in P_O \cup T_O$. A sufficient condition to detect and isolate the firing of the failure transition T_k with the observation of node N is $N \in I_{DP}(T_k)$ and $T_{DDPk}(N) = \varnothing$ if N is a place or $T_{DDPk}(N) = \{N\}$ if N is a transition in PN/T_k..

Proof : If $N \in I_{CR}(T_k)$, then the firing of the failure transition T_k influences the variable attached to the node N *(*marking variable if N is a place or firing variable if N is a transition*)*. Moreover, if N is a place and $T_{DDPk}(N) = \varnothing$, then the variable attached to the node N depends only on the firing of T_k. Then the measurement of this variable is sufficient for detection and isolation of failure F_k. Similarly, if N is a transition and $T_{DDPk}(N) = \{N\}$, then the variable attached to the node N depends only on the firings of itself and T_k. Then the measurement of this variable is also sufficient for detection and isolation of F_k.

In cases where propositions 1 and 2 cannot be applied, (i.e. if $N \in I_{DP}(T_k)$ and $T_{DDPk}(N) \neq \varnothing$ or $T_{DDPk}(N) \neq \{N\}$ in PN/T_k) then the observation of N contributes but is not sufficient for the diagnosis of F_k. In this case the nodes that have to be observed at first correspond to the nodes with the smaller dependence areas. This study must be further investigated in order to combine the information obtained with the investigation of several dependence areas in order to provide minimal admissible sets of observable places as the ones resulting from immediate diagnosis.

Let us consider again the PN in figure 1, where transitions T_2, T_3, T_7 are characterised with deterministic delays $d_{min\ 2} = 10$, $d_{min\ 3} = 20$, $d_{min\ 7} = 30$ and T_1, T_4, T_5, T_6 are characterised with stochastic delays given by exponential distributions $\mu_1 = 0.1$, $\mu_4 = 0.1$, $\mu_5 = 0.2$, $\mu_6 = 0.2$.

All reachable markings belong to the set $\{s_1 = (1\ 0\ 0\ 0\ 0)^T$, $s_2 = (0\ 1\ 0\ 0\ 0)^T$, $s_3 = (0\ 0\ 1\ 0\ 0)^T$, $s_4 = (0\ 0\ 0\ 1\ 0)^T$, $s_5 = (0\ 0\ 0\ 0\ 1)^T\}$ and all observable markings belong to $\{s_{0O} = (0\ 0\ 0)^T$, $s_{1O} = (1\ 0\ 0)^T$, $s_{4O} = (0\ 1\ 0)^T$, $s_{5O} = (0\ 0\ 1)^T\}$. The figure 2a shows a possible trajectory in the marking space according to the given firing sequence $X = T_2\, T_4\, T_7\, \underline{T_1}\, T_3\, T_7\, \underline{T_1}\, T_3\, T_7\, \underline{T_1}\, T_3\, T_7\, \underline{T_1}\, T_3\, T_7\, \underline{T_1}\, T_3\, T_7\, T_2\, \underline{T_5}\, T_6$ where 5 F_1 - failures and 1 F_5 – failure occur consecutively (faults are underlined). The figure 2b shows the observable part of this marking trajectory according to the same firing sequence X. Let us notice that the observable part of the marking trajectory can result not only from the actual firing sequence X but also from another corrupted sequence: for instance, $X' = T_2\, T_4\, T_7\, T_2\, T_3\, T_7\, T_2\, T_3\, T_7\, T_2\, T_3\, T_7\, T_2\, T_3\, T_7\, T_2\, T_3\, T_7\, T_2\, \underline{T_5}\, T_6$ where only 1 F_5 – failure occurs. As a consequence, the observation of the observable part of the marking trajectory does not provide enough information to detect and isolate directly the faults F_1 and F_5 and the diagnosis problem must be solved.

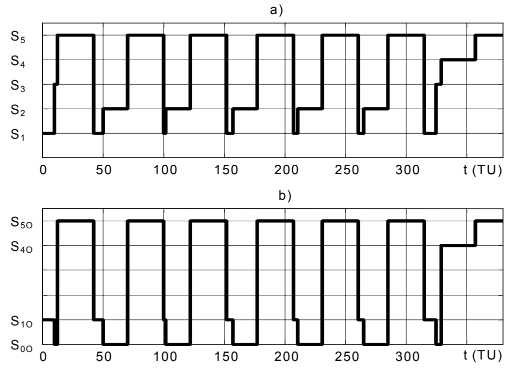

Fig. 2: a) Marking trajectory b) Observable part of the marking trajectory

The sensitivity analysis is useful to provide efficient diagnosers without building the marking tree. By working out the matrix CR_{PT} (equation 3) one can first notice that $P_{ICR}(T_1) = \{P_1, P_2, P_3, P_4, P_5\}$ and $T_{ICR}(T_1) = \{T_1, T_2, T_3, T_4, T_5, T_6, T_7\}$. The observation of each place and each transition contributes to the diagnosability of the system.

By working out the matrices DP_{PT} and DP_{TT} in PN/T_1 (equation 7) and PN/T_5 one can also notice that $T_{DDP1}(P_2) = T_{DDP5}(P_4) = \varnothing$, $T_{DDP1}(T_3) = \{T_3\}$ and $T_{DDP5}(T_6) = \{T_6\}$. A diagnoser of F_1 and F_5 can be obtained with the observation of the couples of nodes $\{T_3, T_6\}$, or $\{P_2, P_4\}$ or $\{T_3, P_4\}$ or $\{P_2, T_6\}$. According to the sets of unobservable nodes T_U and P_U, the unique admissible diagnoser is based on the observation of the nodes $\{T_3, P_4\}$. Such a diagnoser detects and isolates the faults according to the measurement and analysis of the observable firing sequences and observable markings. The delay between the occurrence of the failures F_1 and the fault detection correspond to the duration $d_{min\ 1} = 10$ TU (figure 3a). The detection of the F_5 fault is immediate (figure 3b).

The proposed diagnoser has better performances (detection and isolation of faults F_1 and F_5) and require less information (observation of only 2 nodes) in comparison with the one proposed by Chung *et al.* who suggest to use $P_O = \{P_1, P_4, P_5\}$ and $T_O = \{T_3\}$ in order to detect F_1. Moreover, our approach does not require the construction of the marking tree.

$$\mathrm{DP}(PN\ /\ T_1) = \begin{array}{c} \\ \left(\begin{array}{cccccc} T_2 & T_3 & T_4 & T_5 & T_6 & T_7 \\ 2 & 1 & 1 & 2 & 1 & 0 \\ \infty & \infty & \infty & \infty & \infty & \infty \\ 0 & 2 & 2 & 3 & 2 & 1 \\ 1 & 3 & 3 & 0 & 3 & 2 \\ 1 & 0 & 0 & 1 & 0 & 2 \\ 0 & 2 & 2 & 3 & 2 & 1 \\ \infty & 0 & \infty & \infty & \infty & \infty \\ 1 & 3 & 0 & 4 & 3 & 2 \\ 1 & 3 & 3 & 0 & 3 & 2 \\ 2 & 4 & 4 & 1 & 0 & 3 \\ 2 & 1 & 1 & 2 & 1 & 0 \end{array}\right) \end{array} \begin{array}{c} \\ P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \\ T_2 \\ T_3 \\ T_4 \\ T_5 \\ T_6 \\ T_7 \end{array} \tag{7}$$

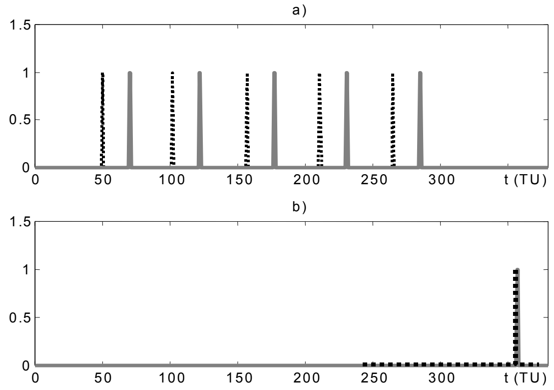

Fig.3. a) Detection of fault F_1 b) Detection of fault F_2 (measurements of the T_6 or T_3 firings in full line, faults occurrence in dotted line)

6. CONCLUSIONS

This paper has proposed some structural results concerning the sensitivity analysis of PN. CR and DP have been investigated in a systematic way. Influence and dependence areas of failure transitions were obtained for PN models of DES with faulty behaviours. The diagnosability of the considered systems has been obtained as a consequence. The main advantage of our approach is to decide in many cases the diagnosability without working out the observable marking tree. In some cases the diagnosability is not decidable, but in all cases our approach is helpful to build the minimal set of nodes to be observed.

Our perspectives are to investigate further the CR and DP for diagnosis issues and to provide a structural solution when the observation of several nodes is required. Moreover this work takes part in our study about monitoring and safe control of DES and hybrid dynamical systems (Zaytoon, *et al.* 1998) modelled with PN. The use of CR and DP will also be developed for observability and controllability issues.

REFERENCES

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

Benveniste A., Fabre F., Jard C., Haar S. (2003). Diagnosis of asynchronous discrete event systems, a net unfolding approach. *IEEE-TAC*, vol.48, no.5.

Cassandras C.G. (1993). *Discrete event systems: modeling and performances analysis,* Aksen Ass. Inc. Pub.

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

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

Debouk R., Lafortune S., Teneketzis D. (1999). On An Optimization Problem In Sensor Selection, *IEEE Conf. on Decision and Control*, Phoenix , Arizona , December, 7-10.

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

Krogh, B.H.; Holloway, L.E. (1991). Synthesis of Feedback Control Logic for Discrete Manufacturing Systems, *Automatica*, vol. 27, no. 4, pp. 641-651.

Lefebvre D. (2003). Sensibilité paramétrique des réseaux de Petri continus à vitesse variable, *JESA*, vol. 37, no 1, pp. 83 - 108.

Lefebvre D, Delherm C. (2003). Structural sensitivity for the conflicts analysis in Petri nets, *IEEE - SMC03*, 7-10 october, Washington, USA,.

Lefebvre D. (2004). Admissible sets of observables places for immediate diagnosis of faulty behaviours with PN models, *submit. to IFAC 05.*

Liu J., Itoh Y., Miyazawa I., Sekiguchi K. (1999). A research on Petri net properties using transitive matrix, *IEEE-SMC99*, vol. 1, pp 888-893, Tokyo, Japan.

Murata T. (1989). Petri nets: properties, analysis and applications, *Proc. IEEE*, vol.77, no. 4, pp541-580.

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, *IEEE – SMC*, pp 113-118.

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.

Zaytoon J., (editor) (1998). Hybrid dynamical systems, *APII - JESA*, vol 32, n° 9-10.