Modular fault diagnosis in discrete-event systems with a CPN diagnoser

Yannick Pencolé [*] **Romain Pichard** [**] **Pierre Fernbach** [***]

[*] *LAAS-CNRS, Univ. de Toulouse, (e-mail: yannick.pencole@laas.fr)*
[**] *LAAS-CNRS, Univ. de Toulouse, (e-mail: romain.pichard@laas.fr)*
[***] *LAAS-CNRS, Univ. de Toulouse, (e-mail: pierre.fernbach@laas.fr)*

Abstract: This paper addresses the problem of fault diagnosis in discrete-event system. The system under investigation is modelled as a labelled Petri net. We first propose an equivalent encoding of the classical diagnoser with the help of a CPN diagnoser. We then apply this encoding to define a modular CPN diagnoser.

Keywords: Diagnosis, Discrete-event System, Petri-nets, Supervision, Encoding.

1. INTRODUCTION

The problem we are dealing with is the supervision of fault events in a discrete event system as introduced in Sampath et al. (1995); as stated in the survey of Zaytoon and Lafortune (2013), this is a very active research area. As opposed to the classical and initial modelling approach, the system here is modelled as a labelled Petri net defined as an extension of the classical Petri net formalism. The use of Petri nets for solving diagnosis problems received much more attention these recent years like in Genc and Lafortune (2007), Dotoli et al. (2009), Cabasino et al. (2011) and several new diagnosis definitions relying on the Petri net formalism has been proposed and investigated. The first objective of this paper is to import the initial diagnosis problem introduced in Sampath et al. (1995) into the world of labelled Petri net and more specifically to define a diagnoser with Petri nets that solves exactly the same problem with the same time efficiency (constant time). The paper comes out with the original definition of an equivalent diagnoser as a coloured Petri net (CPN) that has the advantage to have a graphical representation that is drastically reduced and can be helpful for further anaylyses. This new representation is then used to implement a modular diagnoser that also benefit of this size reduction and that is more suitable for large distributed system.

2. PROBLEM STATEMENT

2.1 Background

Definition 1. A *Petri net* is a 3-uple $N = \langle P, T, A\rangle$ such that:

- P is a finite set of places;
- T is a finite set of transitions, with $P \cap T = \emptyset$;
- $A : (P \times T) \cup (T \times P) \to \mathbb{N}$ is the relation between places and transitions that represents the arcs and their weights.

A state of a Petri net is defined by a marking $M : P \to \mathbb{N}$ which maps any place of the net to the number of tokens that it contains. A marked Petri net is a couple $\langle N, M_0\rangle$ where N is a Petri net and M_0 is an initial marking. Let ${}^\bullet t = \{p \in P | A(p, t) > 0\}$ denote the preset of t and let $t^\bullet = \{p \in P | A(t, p) > 0\}$ the post set of t. A transition t is fireable if for any place p of ${}^\bullet t$, $M(p) \geq A(p, t)$. A transition that is fired from a marking M leads to the marking M' such that for any p $M'(p) = M(p) + A(t, p) - A(p, t)$. We say that M' is reachable from M by t and is denoted: $M \xrightarrow{t} M'$. From this immediatly follows the notion of firable transition sequences from marking M denoted: $M \xrightarrow{t_1} M_1 \ldots M_{n-1} \xrightarrow{t_n} M_n$, $n \in \mathbb{N}$.

With the help of this formalism, any event e that occurs in the system is modelled as a transition $t_e \in T$, in other words, any effective occurrence of the event e in the system is modelled by the fire of the transition t_e. For the sake of generality and flexibility, we propose to model the system with an extended version of Petri nets, called *labelled Petri net.*

Definition 2. A *labelled Petri net* is a 6-uple $S = \langle P, T, A, \ell, \Sigma, M_0\rangle$ such that:

- $\langle P, T, A, M_0\rangle$ is a marked Petri net;
- Σ is the set of transition labels;
- $\ell : T \to \Sigma$ is the label mapping.

An event of the system, here, is modelled as a label of Σ. Two net transitions may be associated to the same label (if ℓ is a bijection, the labelled Petri net is just a classical Petri net). Any effective occurrence of the event e in the system is modelled by the fire of one transition $t \in T$ such that $\ell(t) = e$. We can therefore model non-determininistic behaviours of the system.

2.2 Diagnosis problem

In the model-based diagnosis as introduced in Sampath et al. (1995), we assume that the system can be modelled as a discrete event system over a finite set of events Σ. Events are either observable ($\Sigma_o \subseteq \Sigma$) or non-observable ($\Sigma_{uo} \subseteq \Sigma$). Among the set of non-observable events, there are the fault events ($\Sigma_f \subseteq \Sigma_{uo}$).

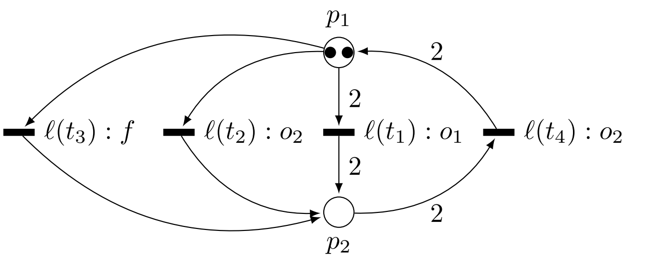

Fig. 1. System example

Definition 3. The *model* of the supervised system is a bounded labelled Petri net such that Σ is the set of events of the system composed of:

- Σ_o the set of observable events;
- Σ_{uo} the set of unobservable events, and among them the set of fault events Σ_f.

Figure 1 depicts a small example that will be used throughout this paper as a running example. This system has a fault event f and two observable events (namely o_1 and o_2). It is bounded and contains 3 reachable marking states ($M_1 : [p_1 = 2, p_2 = 0]$) denoted $2p_1$, $M_2 : [p_1 = 0, p_2 = 2]$ denoted $2p_2$ and $M_3 : [p_1 = 1, p_2 = 1]$ denoted p_1p_2).

Given the model of the system, now we are ready to recall the statement of a diagnosis problem on such a system. Let $\mathbb{P} : \Sigma^* \to \Sigma_o^*$ denote the natural observable projection recursively defined as follows: for any $\sigma.e, \sigma \in \Sigma^*, e \in \Sigma$, $\mathbb{P}(\sigma.e) = \mathbb{P}(\sigma).e$ if $e \in \Sigma_o$ otherwise $\mathbb{P}(\sigma.e) = \mathbb{P}(\sigma)$ and $\mathbb{P}(\varepsilon) = \varepsilon$.

Definition 4. Let S be a model of a discrete event system, let $\sigma = \sigma'.o, \sigma' \in \Sigma_o^*, o \in \Sigma_o$ be an observable sequence of the system, the diagnosis of σ in S, denoted $\Delta(S, \sigma)$ is the maximal set $\{(M_1, F_1), \ldots, (M_n, F_n)\}$ such that:

1. if σ is empty, $\Delta(S, \sigma) = \{(M_0, \varnothing)\}$;
2. if σ is not empty, then for any $i \in \{1, \ldots, n\}$ there exists at least a firable sequence $M_o \xrightarrow{t_{1i}} \ldots \xrightarrow{t_{ki}} M_i$ such that $\bigcup_{j=1}^{k} \ell(t_{ji}) \cap \Sigma_f = F_i$ and $\mathbb{P}(\ell(t_{1i}).\ell(t_{2i}) \ldots \ell(t_{ki})) = \sigma$ with $\ell(t_{ki}) = o$.

Going back to Example 1, here are different diagnosis problems and their solution: $\Delta(S, \varepsilon) = \{(2p_1, \varnothing)\}$, $\Delta(S, o_1) = \{(2p_2, \varnothing)\}$, $\Delta(S, o_2o_2) = \{(2p_2, \{f\}), (2p_2, \varnothing)$, $(2p_1, \{f\}), (p_1p_2, \{f\})\}$.

Proposition 5. Definition 4 is equivalent to the problem defined in Sampath et al. (1995).

Proof. As the model of the system is bounded, its reachable marking graph G is finite and gathers the set of firable sequences from the marking M_0. So G is exactly the finite state machine, called global model, that is defined in Sampath et al. (1995). On the other side, given a finite state machine G, as defined in Sampath et al. (1995), it is trivial to convert it into a bounded labelled Petri net (any state of G becomes a place, any transition of G becomes a net transition), hence the equivalence.

2.3 Problem statement with silent closure

$\Delta(S, \sigma)$ summarizes what could have possibly happened before the last observation of σ. Another problem that can also be considered to extend $\Delta(S, \sigma)$ with the *silent closure* (Lamperti and Zanella (2003)) by also taking into account what could happen after the last observation and that is non-observable. This problem, is important in a modular framework (see Section 4.2).

Definition 6. Let S be a model of a discrete event system, let $\sigma = \sigma'.o, \sigma' \in \Sigma^*.o, o \in \Sigma_o$ be an observable sequence of the system, the extended diagnosis of σ in S, denoted $\Delta^+(S, \sigma)$ is the maximal set $\{(M_1, F_1), \ldots, (M_n, F_n)\}$ such that for any $i \in \{1, \ldots, n\}$ there exists at least a firable sequence $M_o \xrightarrow{t_{1i}} \ldots \xrightarrow{t_{ki}} M_i$ such that $\bigcup_{j=1}^{k} \ell(t_{ji}) \cap \Sigma_f = F_i$ and $\mathbb{P}(\ell(t_{1i})\ell(t_{2i}) \ldots \ell(t_{ki})) = \sigma$.

Back to Example 1, here are different solutions of extended diagnosis problems: $\Delta^+(S, \varepsilon) = \{(2p_1, \varnothing), (p_1p_2, \{f\}), (2p_2, \{f\})\}$, $\Delta^+(S, o_1) = \{(2p_2, \varnothing)\}$, $\Delta^+(S, o_2o_2) = \{(2p_2, \{f\}), (2p_2, \varnothing), (2p_1, \{f\}), (p_1p_2, \{f\})\}$.

3. COLORED PETRI NET DIAGNOSERS

3.1 Classical diagnoser

To fully solve the diagnosis problem on-line, the classical solution is to compute a specific deterministic finite state machine that maps any possible observable sequence σ of the system to the diagnosis result, namely $\Delta(S, \sigma)$, this machine is called a diagnoser. We propose here its definition relying on the model of the system as a labelled Petri net. Let $\mathcal{M}$ denote the finite set of reachable markings of S (as S is supposed to be bounded).

Definition 7. The diagnoser of S is the finite state machine $D = (Q, E, \Sigma_o, q_o)$ such that:

1. Q is a finite set of states; a state is a non-empty subset of $2^{\mathcal{M} \times 2^{\Sigma_f}}$;
2. $E \subseteq Q \times \Sigma_o \times Q$ is a finite set of transitions;
3. Σ_o is the set of observable events;
4. $q_0 \in Q$ is the initial state.

Q and E are defined by induction as follows. Let $Q_0 = \{q_0\}$ with $q_0 = \{(M_0, \varnothing)\}$, and $E_0 = \{\}$. Given Q_i, $i \geq 0$, we compute Q_{i+1}. So, for any state q in Q, for any $o \in \Sigma_o$, let q'_obe the maximal set $\{(M'_1, F'_1), \ldots, (M'_k, F'_k)\}$ such that for any $(M', F') \in q'_o$, there exists $(M, F) \in q$ and $M \xrightarrow{t_1} \ldots \xrightarrow{t_m} M'$ in S with $\ell(t_m) = o$ and $\forall r \in \{1, \ldots, m-1\}$ $\ell(t_r) \notin \Sigma_o$ and $F' = F \cup (\{\ell(t_r)\}_{r \in \{1,\ldots,m-1\}} \cap \Sigma_f)$. If the state $q'_o \neq \varnothing$ and $q'_o \notin \bigcup_{j=0}^{i} Q_j$, then $q'_o \in Q_{i+1}$.

The transition $q \xrightarrow{o} q'_o$ is in E_{i+1}. By construction, as the set of reachable markings and the set of faults is finite, there exists n such that $Q_n = \varnothing$ and $E_n = \varnothing$. And finally, $Q = \bigcup_{i=0}^{n-1} Q_i$ and $E = \bigcup_{i=0}^{n-1} E_i$.

By definition, for any observable sequence σ of the system, the transition path of the diagnoser from the initial state q_0 that follows σ leads to the state $q = \Delta(S, \sigma)$.

Back to the system S of Figure 1, its classical diagnoser contains 11 states and 19 transitions. Its initial state is $q_0 = \Delta(S, \varepsilon) = \{(2p_1, \varnothing)\}$. There is a transition $q_0 \xrightarrow{o_1} q_1 = \Delta(S, o_1) = \{(2p_2, \varnothing)\}$, and so on.

Trivially, we can also define the extended diagnoser $D^+ = (Q^+, E^+, \Sigma_o, q_0^+)$ in the similar way as D. The only difference is in the construction of Q^+. First q_0^+ is the maximal set $\{(M_1,F_1),\dots,(M_k,F_k)\}$ such that there exists for any $i \in \{1,\dots,k\}$, a sequence $M_0 \xrightarrow{t_1} \dots \xrightarrow{t_m} M_k$ in S with $\forall r \in \{1,\dots,m\}, \ell(t_r) \notin \Sigma_o$ and $F_k = \{\ell(tr)\}_{r\in 1,\dots,m} \cap \Sigma_f$. The other difference is in the construction of Q^+_{i+1} from Q^+: in the selection of a transition sequence $M \xrightarrow{t_1} \dots \xrightarrow{t_m} M'$ in S, instead of imposing that $\ell(t_m) = o$ and $\forall r \in \{1,\dots,m-1\}, \ell(t_r) \notin \Sigma_o$, we just impose that there exists one and only one transition $t_i, i \in \{1,\dots,m\}$ such that $\ell(t_i)$ is observable and $\ell(t_i) = o$. Finally F' becomes $F \cup (\{\ell(t_r)\}_{r\in\{1,\dots,m\}} \cap \Sigma_f)$. The rest remains unchanged. Back to the system S of Figure 1, its extended diagnoser contains 8 states and 13 transitions. Its initial state is $q_0 = \Delta^+(S,\varepsilon) = \{(2p_1,\varnothing),(p_1p_2,\{f\}),(2p_2,\{f\})\}$. There is a transition $q_0 \xrightarrow{o_1} q_1 = \Delta^+(S,o_1) = \{(2p_2,\varnothing)\}$, and so on.

3.2 About coloured Petri nets

We present here a simplified version of the definition of coloured Petri nets that will be sufficient throughout this paper. The principle of coloured Petri net is to extend the notion of token with a type, also called a colour. Let C be a finite set of colours. For any place p, we associate a set of possible colours (denoted $C_{sec}(p) \subseteq C$). A colour marking M of p is then a function that associates to any possible colour $c \in C_{sec}(p)$ a number of tokens of this colour: if $M(p,c) = n$, it means that n tokens of colour c hold in the place p in the marking M. For any transition t, we also associate a set of possible colours (denoted $C_{sec}(t) \subseteq C$). For any colour c_t of $C_{sec}(t)$, we define an input arc relationship, denoted $A_-(p,t,c_t)$, as a function that maps any colour $c_p \in C_{sec}(p)$ to a pre-incidence weight: $A_-(p,t,c_t)(c_p) = n$ means that the transition t cannot be fired on the colour c if $M(p,c_p) < n$ and if the transition is effectively fired on colour c_t , n tokens of colour c_p are consumed in the place p. From this follows a notion of preset ${}^\bullet t(c_t) = \{p \in P | \exists c_p \in C_{sec} \wedge A_-(p,t,c_t)(c_p) > 0\}$. In a similar way, we define an output arc relationship, denoted $A_+(p,t,c)$, as a function that maps any colour $c_p \in C_{sec}(p)$ to a post-incidence weight: $A_+(p,t,c)(c_p) = n$ means that if the transition t is fired on the colour c then n tokens of colour c_p are produced in the place p. From this follows a notion of postset $t^\bullet(c_t) = \{p \in P | \exists c_p \in C_{sec} \wedge A_+(t,p,c_t)(c_p) > 0\}$. All this is finally summarised in the following definition.

Definition 8. A marked coloured Petri net is a 5-uple $(P,T,A_-,A_+,C,C_{sec},M_0)$ such that:

- P is a finite set of places;
- T is a finite set of transitions;
- C is a finite set $\{c_1,\dots,c_n\}$ of n colours;
- $C_{sec} : P \cup T \to 2^C$ is a colour mapping for places/transitions;
- $A_- : (P \times T \times C) \to (C \times \mathbb{N})$ is the function which maps any preset place $p \in P$ of a transition $t \in T$ for a colour $c \in C_{sec}(t)$ to a weight function which maps a colour of $C_{sec}(p)$ to a weight ($\in \mathbb{N}$).
- $A_+ : (T \times P \times C) \to (C \times \mathbb{N})$ is the function which maps any postset place $p \in P$ of a transition $t \in T$ for a colour $c \in C_{sec}(t)$ to a weight function which maps a colour of $C_{sec}(p)$ to a weight ($\in \mathbb{N}$).
- $M_0 : P \times C \to \mathbb{N}$ is the initial marking.

A transition $t \in T$ is c_t-firable given a marking M iff $c_t \in C_{sec}(t)$ and $\forall p \in P, \forall c_p \in C_{sec}(p), M(p,c_p) \geq A_-(p,t,c_t)(c_p)$. Firing t from a marking M on a colour $c_t \in C_{sec}(t)$ leads to the new marking $\forall p \in {}^\bullet t(c_t) t^\bullet(c_t)$, $\forall c_p \in C_{sec}(p)$, $M_0(p,c_p) = M(p,c_p) + A_+(t,p,c_t)(c_p)$ $-A_-(p,t,c_t)(c_p)$. Firing a transition is denoted $M \xrightarrow{t} M'$. Note that the proposed coloured Petri nets are supposed to be deterministic, for any reachable marking, if a transition is c-firable it cannot be c'-firable with $c' \neq c$, so the notation $M \xrightarrow{t} M'$ is not ambiguous.

3.3 Coloured diagnoser

We propose to define a coloured Petri net that is equivalent to the classical diagnoser, that is for any observable sequence σ of the system, the coloured version also returns $\Delta(S,\sigma)$. The principle of the encoding is the following.

(1) $\Delta(S,\sigma)$ is a set of couples (M,F) where M is a reachable marking of S and F is a subset of faults from Σ_f, such a couple is called a diagnosis hypothesis. A place of the coloured diagnoser will represent such a hypothesis.
(2) $\Delta(S,\sigma)$ as a whole is called a belief state (a set of diagnosis hypotheses). We propose to model any possible belief state of the classical diagnoser as a colour.
(3) Finally, the transitions of the classical diagnoser are labelled with observable events of Σ_o, in our encoding, any observable event o of the diagnoser will be represented by one transition and one transition only.

The formal definition of the diagnoser is as follows. Recalling the classical diagnoser $D = (Q,E,\Sigma_o,q_o)$. Let $H = \{h_1,\dots,h_m\}$ be the set of diagnosis hypotheses that can be found in D ($h \in H$ iff there $q \in Q$ such that $h \in q$).

Definition 9. The coloured diagnoser of S is the coloured Petri net $D_C = (P,T,A_-,A_+,C,C_{sec},M_{0C})$ such that:

- P is the finite set of places $\{p_i\}_{i|h_i \in H}$, one place per diagnosis hypothesis;
- T is the set of transitions $\{t_o\}, o \in \Sigma_o$;
- C is the set of colours $\{c_i\}_{i|q_i \in Q}$, one colour per diagnosis;
- C_{sec} is the colour mapping function, as defined belows;
- A_- and A_+ are the set of arcs as defined belows;
- M_{0C} is the initial state, such that $M_{0C}(p_0,c_0) = 1$ with p_o the place that is associated to the hypothesis $h_0 = (M_0,\varnothing)$ and c_0 the colour associated to $q_0 \in Q$ and for any other combinations of $p \in P$ and $c_p \in C_{sec}(p), M_{0C}(p,c_p) = 0$.

For any $p \in P$, $C_{sec}(p) = \{c_i \in C | h \in q_i \in Q\}$ where h is the hypothesis of H associated to p, in other words each colour associated to the place p represents a diagnoser state of D where the hypothesis h associated to p is present. For any $t_o \in T$, $C_{sec}(t_o) = \{c_i \in C | \exists q_i \xrightarrow{o} q_j \in E\}$. $A_-(p,t_o,c_i)$ is defined if and only if there exists a diagnoser transition $q_i \xrightarrow{o} q_j$ in E such that h, the hypothesis of H associated to p, is in q_i (to summarise, c_i is the colour of $q_i \in D$, t_o is the net transition associated

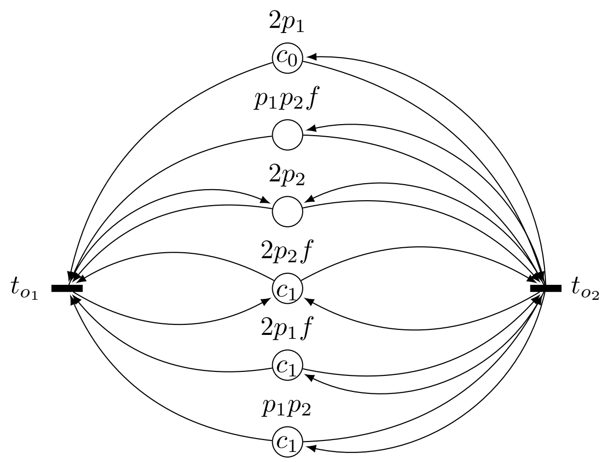

Fig. 2. Coloured diagnoser of system S.

with the observable o and p is associated to a hypothesis that is in q_i). For any $c \in C_{sec}(p)\backslash\{c_i\}, A_-(p,t_o,c_i)(c) = 0$ and $A_-(p,t_o,c_i)(c_i) = 1$. Finally, $A_+(t_o,p,c_i)$ is defined if and only if there exists a diagnoser transition $q_i \xrightarrow{o} q_j$ in E such that h, the hypothesis of H associated to p, is in q_j. For any $c \in C_{sec}(p) \setminus \{c_j\}, A_+(t_o,p,c_i)(c) = 0$ and $A_+(t_o,p,c_i)(c_j) = 1$.

Figure 2 presents the coloured diagnoser of the system S presented in Figure 1. It is composed of 6 places, 2 transitions and 20 arcs. This coloured diagnoser contains 11 colours $C = \{c_0,\dots,c_{10}\}$. On the figure, we present two reachable markings. The first one has the colour c_0, it is the initial marking, c_0 is associated to $\{(M_o = 2p_1, \varnothing)\} = \Delta(S,\varepsilon)$. The second marking is represented by the colour c_1, it is associated to the diagnosis $\{(2p_1,\{f\}),(p_1p_2,\{\}),(2p_2,\{f\})\} = \Delta(S,o_2)$. With help of the transition t_{o2}, these two markings encode the classical diagnoser transition $\{(2p_1,\varnothing)\} \xrightarrow{o_2} \{(2p_1,\{f\}),(p_1p_2,\varnothing),(2p_2,\{f\})\}$. The corresponding input arc relationship is defined by

$$A_-(2p_1,t_o,c_0) = (1,0,\dots,0) \text{ (1 only for } c_0)$$

and the corresponding output arc relationship is defined by

$$A_+(t_o,2p_2f,c_0) = (0,1,0,\dots,0) \text{ (1 only for } c_1)$$
$$A_+(t_o,2p_1f,c_0) = (0,1,0,\dots,0)$$
$$A+(to,p1p2,c0) = (0,1,0,...,0).$$

Proposition 10. Let $\sigma = o_1,\dots,o_k$ be an observable sequence of the system S, there exists in D_C one and only firing sequence $M_{0C} \xrightarrow{t_{o1}} \dots \xrightarrow{t_{ok}} M$ leading to a reachable marking M that encodes $\Delta(S,\sigma)$.

Proof. By construction.

Definition 11. The extended coloured diagnoser of S is the coloured Petri net D_C^+ defined as in Definition 9 by replacing D by D^+.

3.4 Comparative analysis

This subsection presents a comparative analysis between the classical diagnoser and the coloured one. First, as stated by Proposition 10, the coloured diagnoser solves the same problem as the classical diagnoser (see Definition 4). One main advantage of the classical diagnoser for solving a diagnosis problem on-line is the fact that updating a diagnosis after the reception of a new observation is in constant time. This advantage is obviously kept with the coloured diagnoser (from the current coloured marking, the update consists in triggering the unique transition associated to the new observation and the in-going colour). The main difference is from a graphical viewpoint. The classical diagnoser explicitly enumerates the set of possible diagnoses of the system (each diagnosis of the system is a state of the diagnoser). A diagnosis $\Delta(S,\sigma)$ is a subset of $\mathcal{M} \times 2^{\Sigma_f}$ where $\mathcal{M}$ is the set of reachable markings of the system S (see Definition 3) and Σ_f is the set of faults. In the worst case, $|\mathcal{M}|$ is in $o(2^{|P|})$ where P is the set of places of S so the number of possible diagnosis hypotheses is in $o(2^{|P|} \times 2^{|\Sigma_f|})$. As $\Delta(S,\sigma)$ can be any non-empty subset of $\mathcal{M} \times 2^{\Sigma_f}$, the number of possible diagnoser states is in the worst-case in $o(2^{2^{|P|}\times 2^{|\Sigma_f|}})$. Regarding the number of transitions, it obviously follows the same trend. In the worst-case, there are $|\Sigma_o|$ output transitions from any diagnoser state so the number of transitions is also in $o(2^{2^{|P|}\times 2^{|\Sigma_f|}})$. Now, looking back to the coloured diagnoser, the set of diagnoser information is presented in a more factorized way. The coloured diagnoser is not a finite state machine but is represented as a Petri net. Diagnosis information of any $\Delta(S,\sigma)$ is then dispatched over a set of places. One place is associated with one and only one diagnosis hypothesis (an element of $\mathcal{M} \times 2^{\Sigma_f}$) therefore the number of places of D_C is in the worst-case in $o(2^{|P|} \times 2^{|\Sigma_f|})$. As far as the number of transitions, it is by construction $|\Sigma_o|$ and the number of arcs is in the worst-case in $o(2^{|P|} \times 2^{\Sigma_f})$. The double exponentiality that is necessary to encode the complete diagnosis problem is in the number of colours (in $o(2^{2^{|P|}\times 2^{|\Sigma_f|}})$).

The last question to answer is: is the display of a coloured diagnoser always smaller than its classical counterpart? The answer is no. By construction, the number of transitions in the coloured version is smaller than in the classical version in any case. But it might happen that the number of places in D_C is greater than the number of states in D. It happens when the set of diagnosis hypotheses H that is involved in the set of diagnoses $\Delta(S,\sigma)$ is greater than the set of diagnoses itself. In this case the classical diagnoser contains few states with a lot of distinct diagnosis hypotheses in them.

4. MODULAR SUPERVISION OF A DISCRETE-EVENT SYSTEM

For large systems, it might not be possible (due to the double exponential number of belief states) or even interesting to compute the global diagnoser D. We propose here a modular coloured diagnoser. The principle here is to decompose the system S into a set of modules S_i and to compute a coloured diagnoser based on this decomposition. The challenge here is to define a net which can provide a set of module diagnoses $\Delta(S_i,\mathbb{P}_{Si}(\sigma))$ (set of local markings + local faults based on the observation of module S_i only) that is globally consistent, i.e. for any module hypothesis h (state + faults) there exists in $\Delta(S,\sigma)$ a global hypothesis that contains h and for any global hypothesis of $\Delta(S,\sigma)$, it must be composed of a module hypothesis h of $\Delta(S_i, \mathbb{P}_{S_i}(\sigma))$. Details can be found in Contant et al. (2006) for instance.

4.1 Module decompositions

Recalling that the model of the system S is a labelled Petri net $\langle P, T, A, \ell, \Sigma, M_o\rangle$ (see Definition 3), we define the notion of module as follows.

Definition 12. (Module). A module is a labelled Petri net which is a part of S. $S_k = \langle P_k, T_k, A_k, \ell_k, \Sigma_k, M_{0k}\rangle$ is a module of $S = \langle P, T, A, \ell, \Sigma, M_0\rangle$ such that:

- $P_k \subseteq P$;
- $T_k \subseteq T$ such that for any $t \in Tk$, ${}^\bullet t \cap P_k \neq \varnothing$ and $t^\bullet \cap P_k \neq \varnothing$;
- $A_k \subseteq A$ with $A_k = \{a | a \in A((P_k \times T_k) \cup (T_k \times P_k))\}$;
- $\Sigma_k = \{e | \exists t \in T_k \wedge \ell(t) = e\}$;
- ℓ_k is the labelling function $\forall t \in T_k, \ell_k(t) = \ell(t)$;
- M_{0k} is such that $\forall p \in P_k, M_{0k}(p) = M_0(p)$ and $\exists p \in P_k | M_{0k}(p) > 0$.

By construction a module contains its own set of faults Σ_k^f, its own set of non-observable events Σ_k^{uo} and its own set of observable events Σ_k^o . At any time, there is at least one token in a place of the module (a module is therefore an independent process). To perform modular diagnosis, it is required to have a decomposition that fully covers S. We also consider in this setting that two modules only communicate through synchronised events, which means that only transitions can belong to several modules.

Definition 13. A set of modules $S_1, \ldots, S_m$ is a sound decomposition if

(1) any place of P is in one and only one module S_i,
(2) any transition of T belongs to at least one module S_i,
(3) for any observation $o \in \Sigma_o$, if o belongs to several sets $\{\Sigma_{k1}^o, ..., \Sigma_{km}^o\}, m \geq 2$ then any transition t of T such that $\ell(t) = o$ is such that ${}^\bullet t \subseteq \bigcup_{j=1}^m P_{kj}$ and for any $j \in \{1, \ldots, m\}, {}^\bullet t \cap P_{kj} \neq \varnothing$.

Conditions 1 and 2 state that the set of modules covers the system, there is no place and transition that is not in a module. Condition 1 also states that the resources of the system are not shared (every module has its own resources, that is its own places). Condition 2 states that some transitions might be shared between modules. They represent synchronous communications between modules. Condition 3 asserts the localisation of any observation, in other words, an observation o contains enough information to know the source of this observation.

In the following, we will focus on specific sound decompositions where any shared transition t is observable. With this assumption, we ensure that the decomposition is accurate in the sense of Pencolé et al. (2006) so we get the modularity.

Figure 3 presents a modular system. It is composed of two modules: the module S_1 contains the places p_0, p_1 and p_2 and the transitions a, f_1, d_1, d_2 whereas the module S_2 contains the places p_3, p_4 and the transitions a, b_1, f_2. The events a, d_1, d_2 and b_1 are observable. The events f_1 and f_2 are non-observable and faulty events. The transition labelled with event a is a shared transition. This decomposition is sound and accurate.

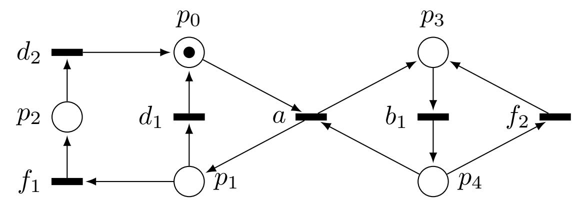

Fig. 3. Modular system S.

4.2 Modular coloured diagnoser

This section defines a coloured diagnoser that relies on a sound module decomposition and therefore improves its space complexity. The basic idea is to compute one diagnoser per module and compute transition synchronisations between each of them. In order to have a correct modular diagnoser in the end, it is necessary to start with the construction of an extended colour diagnoser per module.

For any module S_i, we can compute an extended modular diagnoser D_i^+. Let S_i' be the labelled Petri net that contains any place p of S_i and any non-shared transition t of S_i with their respective label. For any shared transition $t \in T_i$, add to S_i' the transition t' such that ${}^\bullet t' = {}^\bullet t \cap P_i$ and $t'^\bullet = t^\bullet \cap P_i$, the label of t' is the label of t.

Definition 14. The extended modular diagnoser D_i^+ of S_i is the extended diagnoser of the system S_i' (see below Definition 7).

At this stage, any module S_i is considered as a whole system (due to the transformation from S_i to S_i'). The coloured diagnoser that we propose for such a module S_i is simply defined as follows.

Definition 15. The coloured diagnoser of S_i is the extended coloured diagnoser $D_{Ci}^+ = (P_i^+, T_i^+, A_{i-}^+, A_{i+}^+, C_i^+, C_{seci}^+, M_{0i}^+)$ over S_i' obtained by Definition 11.

A coloured diagnoser for a given module is an independent net that is able to follow the flow of observations from that module, disregarding any other observations: given a global sequence of observation σ, the diagnoser observes $\mathbb{P}_{\Sigma_i^o}(\sigma)$ (the observation from S_i) and is able to provide a local diagnosis $\Delta^+(S_i', \mathbb{P}_{\Sigma_i^o}(\sigma))$, that is a subset of $\mathcal{M}_i' \times 2^{\Sigma_i^f}$ where $\mathcal{M}_i'$ is the set of reachable markings from the system S_i'. Until now, the set of local diagnosers are not synchronised so now we need to consider such synchronisations to complete the construction of the modular diagnoser. If a shared transition labelled with an event o between modules $\{S_{k1}, \ldots, S_{km}\}$ exists, it is observable and the diagnosers of $\{S_{k1}, \ldots, S_{km}\}$ can see it and should be synchronized on any occurrence of the event o.

Now we are ready to complete the construction of the extended modular coloured diagnoser. Let $S_1, \ldots, S_m$ be a sound module decomposition of a system S with their respective coloured diagnoser D_{Ci}^+. We assume that any D_{Ci}^+ has its own colours (no common colours). Let ${}^{\bullet i}t$, $t^{\bullet i}$ denote the respective preset and postset of any node t in the diagnsoser D_{Ci}^+. Let $\Sigma_{so} \subseteq \Sigma_o$ be the set of shared observations (at least two diagnoser modules can see such an event).

Definition 16. Let $S_1, \ldots, S_m$ be a sound module decomposition of a system S, the extended modular coloured

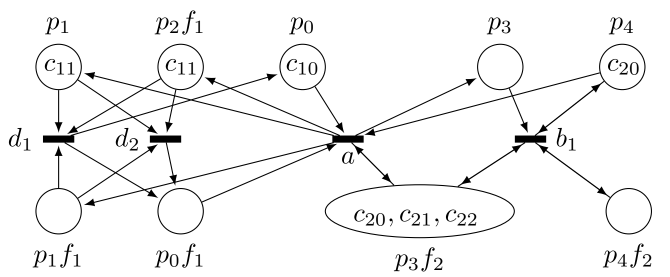

Fig. 4. Modular coloured diagnoser of system in Figure 3.

diagnoser $D^+_{MC} = (P^+, T^+, A^+_-, A^+_-, C^+, C^+_{sec}, M^+_0)$ is the coloured Petri net such that:

- $P^+ = \bigcup_{i=1}^m P_i^+$;
- $T^+ = \bigcup_{i=1}^m T_i^+ \setminus \{t_o^i \in T_i^+, o \in \Sigma_{so}\} \cup T_{so}$ where T_{so} is the observable shared transitions (see below);
- A^+_-, A^+_- (see below);
- $C^+ = \bigcup_{i=1}^m C_i^+ \cup C_{so}$ where C_{so} is the set of colours defined over T_{so} (see below);
- C^+_{sec} is such that $\forall p \in P^+ \cap P_i^+, C^+_{sec}(p) = C^+_{seci}(p), \forall t \in T^+ \cap T_i^+, C^+_{sec}(t) = C^+_{seci}(t)$ and $\forall t \in T_{so}, C^+_{sec}(t) = C^{so}_{sec}(t)$ where $C^{so}_{sec}(t)$ is the colour mapping associated to a shared transition t (see below);
- M_0^+ is such that $\forall i \in \{1, \ldots, m\}, \forall p \in P^+ \cap P_i^+, \forall c \in C_{sec}(p), M_0^+(p, c) = M_{0i}^+(p, c)$.

For any $o \in \Sigma_{so}$, T_{so} contains one unique transition t_o. Let n_o be the number of diagnoser modules that can see o, and assume, without loss of generality, that these diagnosers are $\{D_i^+\}_{i \in \{1,\ldots,n_o\}}$. So t_o replaces the transitions $\{t_{oi} \in T_i^+\}_{i \in \{1,\ldots,n_o\}}$ associated to o in the modular diagnoser. For any n_o-uple $(c_1, \ldots, c_{n_o})$ of the product $\prod_{i=1}^{n_o} C_{seci}(t_{oi})$, we generate a new colour $c(c_1, \ldots, c_{n_o})$ that we add to $C^{so}_{sec}(to)$ and to C_{so}. A^+_- is then defined as follows: $\forall t \in T^+ \cap T_i^+, c_t \in C^+_{seci}(t), \forall p \in {}^{\bullet i}t(c_t), \forall c_p \in C^+_{seci}(p), A^+_-(p, t, c_t)(c_p) = A^+_{i-}(p, t, c_t)(c_p)$ (intuitively any non shared transition is unchanged in the modular diagnoser), and for any $t_o \in T_{so}, \forall c(c_1, ..., c_{n_o}) \in C^{so}_{sec}(to), \forall i \in \{1, \ldots, n_o\} \forall p \in {}^{\bullet i}t(c_i), \forall c_p \in C^+_{seci}(p), A^+_-(p, t_o, c(c_1(p), \ldots, c_{n_o}))(c_p) = 1$, 0 otherwise. And finally A^+_+ is $\forall t \in T^+ \cap T_i^+, c_t \in C^+_{seci}(t), \forall p \in t^{\bullet i}(c_t), \forall c_p \in C^+_{seci}(p), A^+_+(t, p, c_t)(c_p) = A^+_{i+}(t, p, c_t)(c_p)$, and for any $t_o \in T_{so}, \forall c(c_1, \ldots, c_{n_o}) \in C^{so}_{sec}(t_o), \forall i \in \{1, \ldots, n_o\} \forall p \in t^{\bullet i}(c_i), \forall c_p \in C^+_{seci}(p)$, $A^+_+(t_o, p, c(c_1, ..., c_{n_o}))(c_p) = 1$, 0 otherwise.

Figure 4 presents the modular diagnoser of the system in Figure 3. It contains 4 transitions, 9 places and 25 arcs. Example 1 is $\Delta^+(S, \varepsilon) = \{(p_4, \varnothing), (p_3, \{f_2\})\}$ which is the initial marking of the diagnoser in Figure 4 (colour c_{10} for module 1, colour c_{20} for module 2). Example 2 is $\Delta^+(S, b_1) = \{(p_0p_3, \{f_2\}), (p_0p_4, \{f_2\})\}$. As ${}^{\bullet 2}b_1(c_{20}) = \{p_4, p_3f_2\}, A^+_-(p_4, b_1, c_{20})(c_{20}) = 1$ and $A^+_-(p_3f_2, b_1, c_{20})(c_{20}) = 1$, b_1 is c_{20}-firable. Moreover, $A^+_+(b_1, p_4f_2, c_{20})(c_{21}) = 1$ and $A^+_+(a, p_3f_2, c_{20})(c_{21}) = 1$. The next marking of module 2 is associated to $\{(p_3, \{f_2\}), (p_4, \{f_2\})\}$. Module 1 did not change the diagnosis of the modular diagnoser so it is consistent with $\Delta^+(S, b_1)$ (colour c_{10} and c_{21}). Last example is $\Delta^+(S, b_1a) = \{(p_2p_3, \{f_1, f_2\}), (p_1p_3, \{f_2\})\}$. By construction, the transition a is $c(c_{10}, c_{21})$-firable. The modular diagnoser reaches the marking of c_{11} (module 1) and c_{22} (module 2). The diagnosis of module 1 is $\{(p_2, \{f_1\}), (p_1, \varnothing)\}$ and the one of module 2 is $\{(p_3, \{f_2\})\}$, they are globally consistent with $\Delta^+(S, b_1a)$.

5. DISCUSSION

We propose to solve the fault diagnosis problem on DES by the use of a CPN diagnoser. We first present a CPN diagnoser that is fully equivalent to the diagnoser of Sampath et al. (1995) but its graphical representation is drastically reduced. This representation as a CPN diagnoser is then used to implement a modular diagnoser which also benefits of the size reduction. Correctness and accuracy of the modular diagnoser is based on a sound and accurate module decomposition. To our best of knowledge, the closest work to this one is the work of Moreira et al. (2012) that defines a Petri Net diagnoser relying on a automaton model and not a Petri net model. Perspectives are now to start from this new representation to exploit CPN and design extended diagnosers (intermittent faults, supervision patterns, unsound module decompositions) with an optimal size.

REFERENCES

Cabasino, M.P., Giua, A., Pocci, M., and Seatzu, C. (2011). Discrete event diagnosis using labeled petri nets. an application to manufacturing systems. *Control Engineering Practice*, 19(9), 989–1001.

Contant, O., Lafortune, S., and Teneketzis, D. (2006). Diagnosability of discrete event systems with modular structure. *Journal of Discrete Event Dynamic Systems: Theory and Applications*, 16, 9–37.

Dotoli, M., Fianti, M.P., Mangini, A.M., and Ukovich, W. (2009). On-line fault detection in discrete event systems by petri nets and integer linear programming. *Automatica*, 45(11), 2665–2672.

Genc, S. and Lafortune, S. (2007). Distributed diagnosis of place-bordered petri nets. *IEEE Transactions on Automation Science and Engineering*, 4(2), 206–219.

Lamperti, G. and Zanella, M. (2003). *Diagnosis of active systems*. Kluwer Academic Publishers.

Moreira, M.V., Cabral, F.G., and Diene, O. (2012). Petri net diagnoser for des modeled by finite state automata. In *51st IEEE Conference on Decision and Control*, 6742–6748. Maui, Hawai, United States.

Pencolé, Y., Schumann, A., and Kamenetsky, D. (2006). Towards low-cost fault diagnosis in large component-based systems. In *6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, 1473–1478. Beijing, China.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., and Teneketzis, D. (1995). Diagnosability of discrete-event systems. *Transactions on Automatic Control*, 40(9), 1555–1575.

Zaytoon, J. and Lafortune, S. (2013). Overview of fault diagnosis methods for discrete event systems. *Annual Reviews in Control*, 37, 308–320.