DESIGN OF LOW INTERACTION DISTRIBUTED DIAGNOSERS FOR DISCRETE EVENT SYSTEMS

J. Arámburo-Lizárraga, E. López-Mellado and A. Ramírez-Treviño
CINVESTAV Unidad Guadalajara; Av. Científica 1145, Col. El Bajío; 45010 Zapopan, Jal, México

Keywords: Discrete Event Systems, Petri Nets, Distributed Diagnosis.

Abstract: This paper deals with distributed fault diagnosis of discrete event systems (*DES*). The approach held is model based: an interpreted Petri net (*IPN*) describes both the normal and faulty behaviour of *DES* in which both places and transitions may be non measurable. The diagnoser monitors the evolution of the *DES* outputs according to a model that describes the normal behaviour of the *DES*. A method for designing a set of distributed diagnosers is proposed; it is based on the decomposition of the *DES* model into reduced sub-models which require low interaction among them; the diagnosability property is studied for the set of resulting sub-models.

1 INTRODUCTION

Most of works study the diagnosability property and fault detection schemes based on a centralised approach using the global model of the *DES*. Recently, fault diagnosis of *DES* has been addressed through a distributed approach allowing breaking down the complexity when dealing with large and complex systems (Benveniste, et al., 2003; O. Contant, et al., 2004; Debouk, et al., 2000; Genc and Lafortune, 2003; Jiroveanu and Boel, 2003; Pencolé, 2004; Arámburo-Lizárraga, et al., 2005).

In (Debouk, et al., 2000) it is proposed a decentralised and modular approach to perform failure diagnosis based on Sampath's results (Sampath, et al., 1995). In (Contant, et al., 2004) and (Pencolé, 2004) the authors presented incremental algorithms to perform diagnosability analysis based on (Sampath, et al., 1995) in a distributed way; they consider systems whose components evolve by the occurrence of events; the parallel composition leads to a complete system model intractable. In (Genc and Lafortune, 2003) it is proposed a method that handles the reachability graph of the *PN* model in order to perform the analysis similarly to (Sampath, et al., 1995); based on design considerations the model is partitioned into two labelled *PN* and it is proven that the distributed diagnosis is equivalent to the centralised diagnosis; later, (Genc and Lafortune, 2005) extend the results to systems modelled by several labelled *PN* that share places, and present an algorithm to determine distributed diagnosis.

Our approach considers the system modelled as an interpreted *PN* (*IPN*) allowing describing the system with partially observable states and events; the model includes the possible faults it may occur. A structural characterisation and a diagnoser scheme was presented in (Ramírez-Treviño, et al., 2004); then in (Arámburo-Lizárraga, et al., 2005) we proposed a methodology for designing reduced diagnosers and presented an algorithm to split a global model into a set of communicating sub-models.

In this paper we present the formalisation of the distributed system model. The proposed distributed diagnoser scheme consists of communicating diagnoser modules, where each diagnoser can handle two kind of reduced models; the choice of the reduced models depends on some considerations of the system behaviour. In some cases the communication between modules is not necessary.

This paper is organised as follows. In section 2 basic definitions of *PN* and *IPN* are included. Section 3 summarises the concepts and results for centralised diagnosis. Section 4 presents the results related to distributed diagnosis analysis. Section V presents the method to get reduced sub-models that have low interaction among them.

Arámburo-Lizárraga J., López-Mellado E. and Ramírez-Treviño A. (2007).
DESIGN OF LOW INTERACTION DISTRIBUTED DIAGNOSERS FOR DISCRETE EVENT SYSTEMS.
In *Proceedings of the Fourth International Conference on Informatics in Control, Automation and Robotics*, pages 189-194
DOI: 10.5220/0001630501890194

2 BACKGROUND

We consider systems modelled by Petri Nets and Interpreted Petri Nets. A Petri Net is a structure $G = (P, T, I, O)$ where: $P = \{p_1, p_2, ..., p_n\}$ and $T = \{t_1, t_2, ..., t_m\}$ are finite sets of nodes called respectively places and transitions, I (O): $P \times T \rightarrow \mathbb{Z}^+$ is a function representing the weighted arcs going from places to transitions (transitions to places), where $\mathbb{Z}^+$ is the set of nonnegative integers.

The symbol $^\bullet t_j$ ($t_j^\bullet$) denotes the set of all places p_i such that $I(p_i,t_j)\neq 0$ ($O(p_i,t_j)\neq 0$). Analogously, $^\bullet p_i$ ($p_i^\bullet$) denotes the set of all transitions t_j such that $O(p_i,t_j)\neq 0$ ($I(p_i,t_j)\neq 0$) and the incidence matrix of G is $C=[c_{ij}]$, where $c_{ij}=O(p_i,t_j)-I(p_i,t_j)$.

A marking function M: $P\rightarrow\mathbb{Z}^+$ represents the number of tokens (depicted as dots) residing inside each place. The marking of a *PN* is usually expressed as an n-entry vector.

A Petri Net system or Petri Net (*PN*) is the pair $N=(G,M_0)$, where G is a *PN* structure and M_0 is an initial token distribution. $R(G,M_0)$ is the set of all possible reachable markings from M_0 firing only enabled transitions.

In a *PN* system, a transition t_j is enabled at marking M_k if $\forall p_i \in P$, $M_k(p_i) \geq I(p_i,t_j)$; an enabled transition t_j can be fired reaching a new marking M_{k+1} which can be computed as $M_{k+1} = M_k + Cv_k$, where $v_k(i)=0$, $i\neq j$, $v_k(j)=1$.

This work uses Interpreted Petri Nets (*IPN*) (Ramírez-Treviño, et al., 2003) an extension to *PN* that allow to associate input and output signals to *PN* models. An *IPN* (Q, M_0) is an Interpreted Petri Net structure $Q = (G, \Sigma, \lambda, \varphi)$ with an initial marking M_0, where G is a *PN* structure, $\Sigma = \{\alpha_1, \alpha_2, ..., \alpha_r\}$ is the input alphabet of the net, where α_i is an input symbol, λ: $T\rightarrow\Sigma \cup\{\varepsilon\}$ is a labelling function of transitions with the following constraint: $\forall t_j,t_k \in T$, $j \neq k$, if $\forall p_i$ $I(p_i,t_j) = I(p_i,t_k) \neq 0$ and both $\lambda(t_j) \neq \varepsilon$, $\lambda(t_k) \neq \varepsilon$, then $\lambda(t_j) \neq \lambda(t_k)$, in this case ε represents an internal system event, and $\varphi: R(Q,M_0)\rightarrow(\mathbb{Z}^+)^q$ is an output function that associates to each marking an output vector. Here q is the number of outputs. In this work φ is a $q\times n$ matrix. If the output symbol i is present (turned on) every time that $M(p_j)\geq 1$, then $\varphi(i,j)=1$, otherwise $\varphi(i,j)=0$.

A transition $t_j \in T$ of an *IPN* is enabled at marking M_k if $\forall p_i \in P$, $M_k(p_i) \geq I(p_i,t_j)$. When t_j is fired in a marking M_k, then M_{k+1} is reached, i.e., $M_k \xrightarrow{t_j} M_{k+1}$; M_{k+1} can be computed using the state equation:

$$\begin{aligned} M_{k+1} &= M_k + Cv_k \\ y_k &= \varphi(M_k) \end{aligned} \tag{1}$$

where C and v_k are defined as in *PN* and $y_k \in (\mathbb{Z}^+)^q$ is the k-th output vector of the *IPN*.

Let $\sigma = t_i t_j ... t_k ...$ be a firing transition sequence of an $IPN(Q,M_0)$ s.t. $M_0 \xrightarrow{t_i} M_1 \xrightarrow{t_j} ... M_x \xrightarrow{t_k} ...$ The set $£(Q,M_0)$ of all firing transition sequences is called the firing language $£(Q,M_0)=\{\sigma = t_i t_j ... t_k ... \wedge M_0 \xrightarrow{t_i} M_1 \xrightarrow{t_j} ... M_x \xrightarrow{t_k} ...\}$.

According to functions λ and φ, transitions and places of an *IPN* (Q,M_0) if $\lambda(t_i) \neq \varepsilon$ the transition t_i is said to be manipulated. Otherwise it is non-manipulated. A place $p_i\in P$ is said to be measurable if the i-th column vector of φ is not null, i.e. $\varphi(\bullet,i) \neq 0$. Otherwise it is non-measurable.

The following concepts are useful in the study of the diagnosability property. A sequence of input-output symbols of (Q,M_0) is a sequence $\omega = (\alpha_0,y_0)(\alpha_1,y_1)...(\alpha_n,y_n)$, where $\alpha_j \in \Sigma \cup\{\varepsilon\}$ and α_{i+1} is the current input of the *IPN* when the output changes from y_i to y_{i+1}. It is assumed that $\alpha_0 = \varepsilon$, $y_0 = \varphi(M_0)$. The firing transition sequence $\sigma \in £(Q,M_0)$ whose firing actually generates ω is denoted by σ_ω. The set of all possible firing transition sequences that could generate the word ω is defined as $\Omega(\omega) = \{\sigma \mid \sigma \in £(Q,M_0) \wedge$ the firing of σ produces $\omega\}$.

The set $\Lambda(Q,M_0) = \{\omega \mid \omega$ is a sequence of input-output symbols$\}$ denotes the set of all sequences of input-output symbols of (Q,M_0) and the set of all input-output sequences of length greater or equal than k will be denoted by $\Lambda^k(Q,M_0)$, i.e. $\Lambda^k(Q,M_0) = \{\omega \in \Lambda(Q,M_0) \mid |\omega| \geq k\}$ where $k \in \mathbb{N}$.

The set $\Lambda_B(Q,M_0)$, i.e., $\Lambda_B(Q,M_0) = \{\omega \in \Lambda(Q,M_0) \mid \sigma\in\Omega(\omega)$ such that $M_0 \xrightarrow{\sigma} M_j$ and M_j enables no transition, or when $M_j \xrightarrow{t_i}$ then $C(\bullet,t_i)=0\}$ denotes all input-output sequences leading to an ending marking in the *IPN* (markings enabling no transition or only self-loop transitions).

The following lemma (Ramírez-Treviño, et al., 2004) gives a polynomial characterisation of event-detectable *IPN*.

Lemma 1: A live *IPN* given by (Q,M_0) is event-detectable if and only if:

1. $\forall t_i, t_j \in T$ such that $\lambda(t_i) = \lambda(t_j)$ or $\lambda(t_i) = \varepsilon$ it holds that $\varphi C(\bullet,t_i) \neq \varphi C(\bullet,t_j)$ and
2. $\forall t_k \in T$ it holds that $\varphi C(\bullet,t_k) \neq 0$.

3 CENTRALISED DIAGNOSIS

The main results on diagnosability and diagnoser design in a centralised approach presented in (Ramírez-Treviño, et al., 2007) are outlined below.

3.1 System Modelling

The sets of nodes are partitioned into faulty (P^F and T^F) and normal functioning nodes (P^N and T^N); so $P = P^F \cup P^N$ and $T = T^F\cup T^N$. p_i^N denotes a place in P^N of the normal behaviour $\left(Q^N, M_0^N\right)$. Since $P^N \subseteq$

P then p_i^N also belongs to (Q,M_0). The set of risky places of (Q,M_0) is $P^R = {}^\bullet T^F$. The post-risk transition set of (Q,M_0) is $T^R = P^{R\bullet} \cap T^N$.

Example. Figure 1 presents an *IPN* model of a system. The model has three faulty states, represented by places p_{16}, p_{17}, p_{18}. Function λ is defined as $\lambda(t_1)$=a, $\lambda(t_3)$=b, $\lambda(t_4)$=x, $\lambda(t_7)$=y, $\lambda(t_9)$=c, $\lambda(t_{10})$=z, for others transitions $\lambda(t_i)=\varepsilon$. Measurable places are p_3, p_5, p_8, p_{12}, p_{15}, $P^R = \{p_4, p_7, p_{12}\}$, $T^R = \{t_4, t_7, t_{10}\}$, $T^F = \{t_{13}, t_{14}, t_{15}\}$ and $P^F = \{p_{16}, p_{17}, p_{18}\}$.

3.2 Reduced Models

In a previous work (Arámburo-Lizárraga, et al., 2005) we stated that the condition of event-detectability is needed only on $t_j \in {}^\bullet P^R$ and $t_j \in P^{R\bullet}$. This fact can be exploited in order to obtain a reduced model containing the pertinent parts of (Q^N, M_0^N) regarding the modelled faults in (Q,M_0).

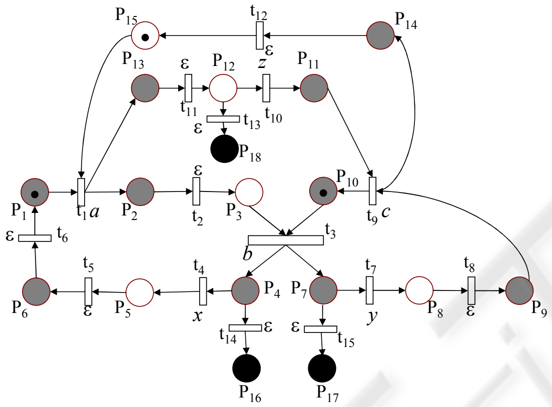

Figure 1: Global model.

Definition 1. Let (Q^N, M_0^N) be the embedded normal behaviour included in (Q,M_0). The reduced model (Q^{RM}, M_0^{RM}) of (Q^N, M_0^N) is the subnet induced by:

- $P^{RM} = P_a \cup P_b \cup P_c$, where $P_a = \{p_i \mid p_i \in P^R\}$, $P_b = \{p_j \mid p_j \in P^{R\bullet\bullet}\}$, and $P_c = \{p_k \mid p_k \in {}^{\bullet\bullet}P^R$, p_k is a measurable place$\}$. The sets P_b and P_c are necessary only when $\exists p_i \in P^R$, such that p_i is non-measurable.
- $T^{RM} = T_{in} \cup T_{out}$, where $T_{in} = \{{}^\bullet p_i \mid p_i \in P^{RM}\}$, $T_{out} = \{p_i{}^\bullet \mid p_i \in P^{RM}\}$.
- λ^{RM}: $T^{RM} \rightarrow \Sigma \cup \{\varepsilon\}, \forall t_i' \in T^{RM}, \lambda(t_i') = \lambda(t_i), t_i \in T^N$, $t_i' = t_i$.
- $\varphi^{RM} = \varphi|_{R(Q^{RM}, M_0^{RM})}$
- $M_0^{RM} = M_0|_{P^{RM}}$.

The firing rules of (Q^{RM}, M_0^{RM}) are defined:

- If $t_j \in T^{RM}$ is fired in (Q,M_0) then it must be fired in (Q^{RM}, M_0^{RM}).
- If the input symbol $\lambda(t_k)$, $t_k \in P^{R\bullet}$ is activated in the system then it must be activated in (Q^{RM}, M_0^{RM}).
- If $\exists t_j \in T^{RM}$, s.t., t_j is not event detectable then t_j is fired automatically when ${}^\bullet t_j$ was marked.

The reduced model nodes (places and transitions) are a copy of the original ones, and they have associated the same input-output symbols.

Figure 2 presents the reduced model of the global system model depicted in figure 1. Notice that in this example the number of places is reduced and T^{RM} are only event-detectable transitions.

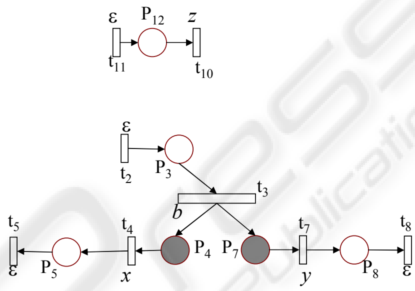

Figure 2: Diagnoser reduced model.

3.3 Characterisation of Diagnosability

The characterisation of input-output diagnosable *IPN* is based on the partition of $R(Q,M_0)$ into normal and faulty markings; all the faulty markings must be distinguishable from other reachable markings.

Definition 2: An *IPN* given by (Q,M_0) is said to be input - output diagnosable in $k < \infty$ steps if any marking $M_f \in F$ is distinguishable from any other $M_k \in R(Q,M_0)$ using any word $\omega \in \Lambda^k(Q,M_f) \cup \Lambda_B(Q,M_f)$, where $F = \{M \mid \exists p_k \in P^F$ such that $M(p_k)>0, M \in R(Q,M_0)\}$.

The following result extends that presented in (Ramírez-Treviño, et al., 2007).

Theorem 1: Let (Q,M_0) be a binary *IPN*, such that (Q^N, M_0^N) is live, strongly connected and event detectable on $t_j \in {}^\bullet P^R$ and $t_j \in P^{R\bullet}$. Let $\{X_1,...,X_\tau\}$ be the set of all T-semiflows of (Q,M_0). If $\forall p_i^N \in P^N$, $(p_i^N)^\bullet \cap T^F \neq \theta$ the following conditions hold:

1. $\forall r, \exists j\ X_r(j) \geq 1$, where $t_j \in (p_i^N)^\bullet - T^F$,
2. $\forall t_k \in (p_i^N)^\bullet - T^F, {}^\bullet(t_k) = \{p_i^N\}$ and $\lambda(t_k) \neq \varepsilon$.

then the *IPN* (Q,M_0) is input-output diagnosable.

Proof: It is similar to that included in (Ramírez-Treviño, et al., 2007).

4 DISTRIBUTED DIAGNOSIS

4.1 Model Partition

In order to build a distributed diagnoser, the *IPN* model (Q, M_0) can be conveniently decomposed into m interacting subsystems where different modules share common nodes.

Definition 3. Let (Q,M_0) be an *IPN*. The distributed Interpreted Petri Net model *DN* of (Q,M_0) is a finite set of modules $\mathcal{M}=\{\mu_1, \mu_2,\ldots,\mu_m\}$ such that:

each $\mu_k \in \mathcal{M}$ is an *IPN* subnet: $\mu_k = (N_k, \Sigma_k, \lambda_k, \varphi_k)$, $k \in \{1,2,\ldots,m\}$ modules.

- $N_k = (P_k, T_k, I_k, O_k, M_{0k})$ where $P_k \subseteq P$, $T_k \subseteq T$, $I_k(O_k) : P_k \times T_k \rightarrow Z^+$, s.t., $I_k(p_i,t_j) = I(p_i,t_j)$ $(O_k(p_i,t_j) = O(p_i,t_j))$, $\forall\ p_i \in P_k$ and $\forall t_j \in T_k$ and $M_{0k} = M_0\ |_{Pk}$
- $\Sigma_k = \{\alpha\in\Sigma \mid \exists t_i,\ t_i \in T_k,\ \lambda(t_i) = \alpha\}$
- $\lambda_k : T_k \rightarrow \Sigma_k \cup \{\varepsilon\}$, s.t. $\lambda_k(t_i) = \lambda(t_i)$ and $t_i \in T_k$
- $\varphi_k : R(m_k, M_{0k}) \rightarrow (Z^+)^q$, q is restricted to the outputs associated to P_k. $\varphi_k = \varphi|_{Pk}$

For each μ_k the following conditions hold:

a) $\exists\mu_l \in\mathcal{M}$, s.t. $T_k \cap T_l \neq\varnothing$, $P_k\cap P_l = \{{}^\bullet t_i \cup t_i^\bullet \mid t_i \in \{T_k \cap T_l\}\}$, $P_k\cap P_l$ are measurable places.

b) $\forall p_i \in \{P_k - (P_k\cap P_l)\}$ if $p_i \in P^R$ then $p_i{}^{\bullet\bullet} \subset P_k$.

c) $ICom(OCom)$: $P_k \times T_l \rightarrow Z^+$, s.t. $I_k(p_i,t_j) = I_l(p_i,t_j)$ $(O_k(p_i,t_j) = O_l(p_i,t_j))$, $\forall p_i \in P_k$ and $\forall t_j \in T_l$. *ICom* and *OCom* represent the communication between modules. The arcs are depicted as a dashed line.

The obtained *DN* captures the firing language $\pounds(Q,M_0)$ in a distributed way, $\forall t_x \in \sigma = t_i t_j \ldots t_k \ldots$ and for every (α_x,y_x) in $\omega = (\alpha_0,y_0)(\alpha_1,y_1)\ldots(\alpha_n,y_n)$ $\exists\mu_k \in\mathcal{M}$ where t_x is fired and (α_x,y_x) is also generated in *DN*.

Consider the *IPN* system model depicted in the Figure 1 (for the sake of simplicity, we use in the examples the same names for duplicated nodes (places or transitions) belonging to different modules). Figure 3 presents the distributed *IPN*, m = 3 modules, *ICom* and *OCom* are represented by the dashed arcs. For example we can get the sets $T_1 \cap T_2 = \{t_3\}$ and $T_1 \cap T_3 = \{t_1\}$, $P_1 \cap P_2 = \{p_3\}$ and $P_1 \cap P_3 = \{p_{15}\}$.

We are preserving the property of event detectability using duplicated measurable places, which they establish the outputs that each module needs from others modules.

4.2 Local Reduced Models

The local models can be reduced following the steps of sub-section 3.2 and obtaining a simpler distributed model considering the local nodes.

Definition 4. Let $\mu_i \in\mathcal{M}$ be an *IPN* module. The local reduced model $\left(Q^{RM}, M_0^{RM}\right)_i$ is the subnet induced as in definition 1.

Consider the *DN* distributed model depicted in figure 3, the figure 4 presents the local reduced models where the place p_3 is duplicated in module 2 for detecting the firing of t_3. The communication between modules is represented by the dashed arcs.

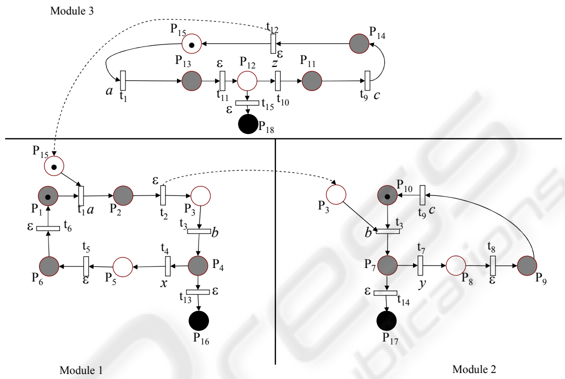

Figure 3: Distributed Interpreted Petri Net.

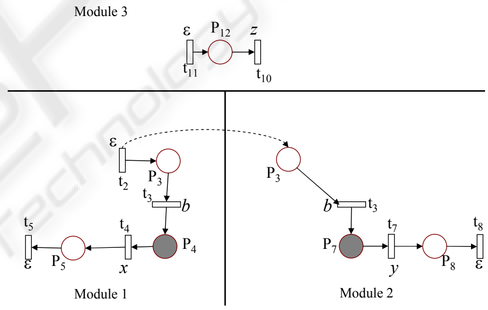

Figure 4: Local reduced models.

It is possible to obtain local reduced models where the communication is eliminated, since $T^{RM}{}_n$ can be event-detectable only by the local outputs.

4.3 Modular Fault Detection

The error between the system output and the local diagnoser model output is $E_{kn}=\varphi(M_k)-\varphi_n(M_k^{RM})$. The following algorithm, devoted to detect which local faulty marking was reached in *DN*, is executed when $E_{kn} \neq 0$ in $\mu_n \in\mathcal{M}$.

Algorithm 1. Detecting Local Faulty Markings

Inputs: $\varphi_n(M_k^{RM})$, M_n^{RM}, $\lambda(t_i)$, $t_i \in T^{RM}{}_n$, E_{kn}

Outputs: p_n^F

1.Constants: φC_n^{RM} -- local reduced normal behaviour

2.Repeat

2.a. Read $\varphi_n\left(M_k^{RM}\right)$ and $\lambda(t_i)$
2.b. If $\lambda(t_j) \in \lambda(P^{R\bullet})$ then computes
$\delta = \varphi_n\left(M_k^{RM}\right) - \varphi_n\left(M_{k-1}^{RM}\right)$ (a column of φC_n^{RM})
2.c. i = index of the column of φC_n^{RM}, s.t., φC_n^{RM} $(\bullet, i) = \delta$, i.e. t_i was fired;
2.d. If $E_{kn} \neq 0$ then
- $\forall p_n \in ({}^\bullet t_i)^{\bullet\bullet} \cap P^F{}_n$, $M_{fn}(p_n)=1$
- Return $(p_n{}^F)$
- Sends to all modules the message "A fault occurred in module μ_n in place $(p_n{}^F)$".

Since $\left(Q^{RM}, M_0^{RM}\right)_n$ is event detectable in ${}^\bullet P^R$ and $P^{R\bullet}$, then step 2.b. will compute just one column index; moreover, since $\left(Q^N, M_0^N\right)_n$ fulfils the conditions of theorem 1, then step 2.c. will compute just one place.

4.4 Distributed Input-output Diagnosability

The results of centralised diagnosability are applied to the modules issued from the partition.

The nodes of every $\mu_k \in \mathcal{M}$ are partitioned into local faulty nodes and normal nodes, i.e., $P_k = P^F{}_k \cup P^N{}_k$ and $T_k = T^F{}_k \cup T^N{}_k$.

$R(\mu_k, M_{0k})$ denotes the reachability set of a module μ_k and $LF = \{M_k \mid \exists p_j \in P^F{}_k$, such that $M_k(p_j)>0$, $M_k \in R(\mu_k, M_{0k})\}$ denotes the set of the local faulty markings.

$\Lambda^{int}{}_k(\mu_k, M_{0k})$ denotes the set of all input-output sequences that lead to a marking which puts a token into a duplicated place in other module μ_n, $\Lambda^{int}{}_k(\mu_k, M_{0k}) = \{\omega \mid \exists\sigma_m$, such that σ_m generates ω, and $M_{0m} \xrightarrow{\sigma_m} M_{jm}$ then M_{jm} marks a p_j s.t. $p_j \in P^{RM}{}_m$ in some module $\mu_m\}$.

Now, we introduce two notions for describing degrees of diagnosability in the modules of a distributed model.

A module is locally diagnosable if, for every local fault we can detect it only through local information, else it is conditionally diagnosable.

Definition 5. (Local Diagnosability) A module $\mu_n \in \mathcal{M}$ given by DN is said to be locally input-output diagnosable in $k < \infty$ steps if any marking $M_{fn} \in LF$ is distinguishable from any other $M_{kn} \in R(\mu_n, M_{0n})$ using any local word $\omega_n \in \Lambda^k{}_n(\mu_n, M_{0n}) \cup \Lambda_{Bn}(\mu_n, M_{0n})$.

Definition 6. (Conditional Diagnosability) A module $\mu_n \in \mathcal{M}$ given by DN is said to be conditional input-output diagnosable in $k < \infty$ steps if any marking $M_{fn} \in LF$ is distinguishable from any other $M_{kn} \in R(\mu_n, M_{0n})$ using any local word $\omega_m \in \Lambda^k{}_n(\mu_n, M_{0n}) \cup \Lambda_{Bn}(\mu_n, M_{0n})$ and any word $\omega_m \in \Lambda^{int}{}_n(\mu_n, M_{0n})$.

Proposition 1. Let (Q,M_0) be an *IPN* and *DN* its corresponding distributed *IPN* as stated in definition 3. If (Q,M_0) is input-output diagnosable as in theorem 1 then *DN* is distributed input-output diagnosable.

Proof. Assume that (Q,M_0) is input-output diagnosable. There exists a finite sequence of input-output symbols ω, s.t., $\omega \in \Lambda^k(Q,M_f) \cup \Lambda_B(Q,M_f)$, and $\sigma = t_i t_j t_k \ldots t_m$ is the firing transition sequence whose firing generates ω s.t. $M_0 \xrightarrow{\sigma_\omega} M_k$, $M_k \in F$. By theorem 1 M_k is distinguishable from any other $M_k \in R(Q,M_0)$ and (Q,M_0) is input-output diagnosable.

Since *DN* is the distributed behaviour of (Q,M_0), we suppose that the sequence σ can be fired in some modules $\mu_k \ldots \mu_l, \mu_m \in \mathcal{M}$ of *DN*, and the sequence generates the following local markings $M_{ik} \cup \ldots \cup M_{il} \cup M_{im}$, then $M_k = M_{ik} \cup \ldots \cup M_{il} \cup M_{im}$, s.t. $M_{ik} \ldots M_{il} \in LN$ and $M_{im} \in LF$. Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ sequences s.t. $\sigma = \sigma_1\sigma_2 \ldots \sigma_m$, suppose that σ_1 is fired in a module $\mu_k \in \mathcal{M}$ s.t. $M_{0k} \xrightarrow{\sigma_1} M_{ik}$, σ_2 is fired in $\mu_l \in \mathcal{M}$, s.t. $M_{0l} \xrightarrow{\sigma_2} M_{il} \ldots$, and σ_m is fired in $\mu_m \in \mathcal{M}$, s.t. $M_{0m} \xrightarrow{\sigma_m} M_{im}$, and σ occurs if the sequence σ_1 followed by a sequence $\sigma_2, \ldots$ followed by a sequence σ_m occur in the corresponding modules. Then by definition 5 and 6 μ_m can distinguish any $M_{im} \in LF$ from any other $M_{km} \in R(\mu_m, M_{0m})$. Hence there exists a module $\mu_m \in \mathcal{M}$ that can distinguish the corresponding faulty marking M_{im}; as μ_m can be any module and μ_m can be local or conditional input-output diagnosable, therefore *DN* is distributed input-output diagnosable. □

Proposition 1 considers both cases (local and conditional diagnosable modules) for establishing the distributed input-output diagnosability of *DN*.

5 REDUCING INTERACTIONS

In Section 3.2 we explained how to build reduced models. Now, let us consider the following assumption:

- The manipulated input symbols $\lambda(t_k) \neq \varepsilon$ are not activated arbitrarily, only when they are enabled at the marking $M_k(p_k)>0$, s.t. $p_k \in {}^\bullet t_k$.

This assumption regards for building smaller reduced models.

Definition 7. Let $\left(Q^N, M_0^N\right)$ be the embedded normal behaviour included in (Q,M_0). When the following condition holds: $\forall\lambda(t_k) \neq \varepsilon$, $t_k \in P^{R\bullet}$ are fired only when it is necessary, then the reduced model $\left(Q^{RM}, M_0^{RM}\right)$ of $\left(Q^N, M_0^N\right)$ of definition 1 is modified considering the following sets:

- $P^{RM} = P_a \cup P_b$, where $P_a = \{p_i \mid p_i \in P^R\}$ and $P_b = \{p_j \mid p_j \in P^{R\bullet\bullet}\}$;

- $T^{RM} = T_{in} \cup T_{out} \cup T_{af}$, where $T_{in} = \{{}^\bullet p_i \mid p_i \in P^{RM}\}$, $T_{out} = \{p_i{}^\bullet \mid p_i \in P^{RM}\}$ and $T_{af} = \{t_{edx} \mid t_{edx} \in {}^\bullet p_i$ and/or $t_{edx} \in p_i{}^\bullet$, t_{edx} is a new transition, $x = 1, 2, \ldots, z$ transitions non event-detectable$\}$, T_{af} is necessary only when $p_i \in P^{RM}$, such that p_i is non-measurable.
- $\lambda^{RM}: T^{RM} \rightarrow \Sigma \cup \{\varepsilon\}, \forall t_i' \in \{T_{in} \cup T_{out}\}$, $\lambda(t_i') = \lambda(t_i)$, $t_i \in T^N$, $t_i' = t_i$. If $t_i' \in T_{af}$, t_i' has no input symbols.
- $\varphi^{RM} = \varphi|_{R(Q^{RM}, M_0^{RM})}$
- $M_0^{RM} = M_0|_{P^{RM}}$. If $\exists p_k \in P^{RM}$, s.t., $M_k(p_k) = 0$, but, $p_k \in t_{ed}{}^\bullet$ then $M_k(p_k) > 0$.

The firing rules of $\left(Q^{RM}, M_0^{RM}\right)$ are defined as in definition 1 besides the following new firing rule:

- The transitions that belongs to T_{af} are fired automatically, i.e, $M({}^\bullet t_{ed}) > 0$ or $M(t_{ed}{}^\bullet) = 0$.

Figure 5 presents the distributed reduced model when we consider that the input symbols are not activated of an arbitrary way. We can see that the transition t_3 is not part of the reduced model of module 2, it is replaced by a transition t_{ed1}, $\lambda(t_{ed1}) = \varepsilon$. The goal for building smaller reduced models is to guarantee the observation of the system in critical situations.

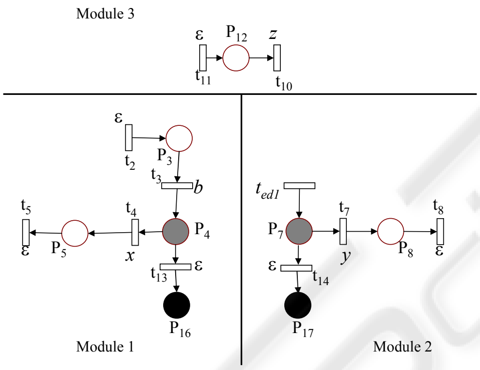

Figure 5: Reduced models for the centralised diagnoser.

6 CONCLUSIONS

A method for designing distributed diagnosers has been presented. The proposed model decomposition technique preserves the diagnosability of the global model into the distributed one and reduces the communication among the diagnosers. Current research addresses reliability of distributed diagnosers.

REFERENCES

Arámburo-Lizárraga J., E. López-Mellado, and A. Ramírez-Treviño (2005). "Distributed Fault Diagnosis using Petri Net Reduced Models". *Proc. of the IEEE International Conference on Systems, Man and Cybernetics*. pp. 702-707, October 2005.

Benveniste A., S. Haar, E. Fabre and C. Jara (2003). "Distributed and Asynchronous Discrete Event Systems Diagnosis". *42nd IEEE Conference on Decision and Control*. 2003.

Contant O, S. Lafortune and D. Teneketzis (2004). "Diagnosis of modular discrete event systems". *7th Int. Workshop on Discrete Event Systems* Reims, France. September, 2004.

Debouk R, S. Lafortune and D. Teneketzis (2000). "Coordinated Decentralized Protocols for Failure Diagnosis of Discrete Event Systems", Kluwer Academic Publishers, Discrete Event Systems: Theory and Applications, vol. 10, pp. 33-79, 2000.

Genc S. and S. Lafortune (2003). "Distributed Diagnosis of Discrete-Event Systems Using Petri Nets" *Proc. of the 24th. ATPN* pp. 316 - 336, June, 2003.

Genc S. and S. Lafortune (2005). "A Distributed Algorithm for On-Line Diagnosis of Place-Bordered Nets". 16th IFAC World Congress, Praha, Czech Republic, July 04-08, 2005.

Jalote P. (1994). *Fault Tolerance in distributed systems*. Prentice Hall. 1994

Jiroveanu G. and R. K. Boel (2003). "A Distributed Approach for Fault Detection and Diagnosis based on Time Petri Nets". *Proc. of CESA*. Lille, France, July 2003.

Pencolé Y. "Diagnosability analysis of distributed discrete event systems". *Proc. of the 15th International Workshop on Principles of Diagnosis*. Carcassonne, France. June 2004.

Ramírez-Treviño A., I. Rivera-Rangel and E. López-Mellado (2003). "Observability of Discrete Event Systems Modeled by Interpreted Petri Nets". *IEEE Transactions on Robotics and Automation*, vol. 19, no. 4, pp. 557-565, August 2003.

Ramírez-Treviño, E. Ruiz Beltrán, I. Rivera-Rangel, and E. López-Mellado (2004). A. Ramírez-Treviño, E. Ruiz Beltrán, I. Rivera-Rangel, E. López-Mellado. "Diagnosability of Discrete Event Systems. A Petri Net Based Approach". Proc. of the IEEE International Conference on Robotic and Automation. pp. 541-546, April 2004.

Ramírez-Treviño A, E. Ruiz Beltrán, I. Rivera-Rangel, E. López-Mellado (2007). "On-line Fault Diagnosis of Discrete Event Systems. A Petri Net Based Approach". *IEEE Transactions on Automation Science and Engineering*. Vo1. 4-1, pp. 31-39. January 2007.