Critical pairs based diagnosability analysis of timed fault in Time Petri Nets

Camille Coquand, Audine Subias, Yannick Pencolé, Éric Lubat

Critical pairs based diagnosability analysis of timed fault in Time Petri Nets

Camille Coquand * **Audine Subias** * **Yannick Pencolé** ** **Éric Lubat** *

* *CNRS, LAAS, Univ de Toulouse, INSA, LAAS, F-31400 Toulouse, France (e-mail: firstname.lastname@laas.fr).*
** *CNRS, LAAS, Univ de Toulouse, LAAS, F-31400 Toulouse, France (e-mail: yannick.pencole@laas.fr)*

Abstract: Time Petri Nets are a suitable tool for the modeling of timed Discrete Event Systems. This paper is about the diagnosability of single timed fault in Time Petri Nets. To check the existence of critical pairs, an abstraction of the systems infinite behaviours, called path, is presented as a set of observable constraints associated with a particular sequence of transitions. Properties on the set of solutions of a partition of this abstraction are then provided to check the diagnosability of the timed fault.

Keywords: Discrete event system, Time Petri nets, State class graph, diagnosability, critical pair.

1. INTRODUCTION

Diagnosability of a fault is the property of a partially observable system to provide the necessary information to notice with certainty the occurrence of a fault. It has been studied in the formalism of Discrete Event Systems (DES) since Sampath et al. (1995). The authors build a diagnoser on which the property can be checked. Time extension has been proposed for diagnosis of DES, first on timed automata (Tripakis (2002)) and then later on Time Petri Nets (TPN) (Basile et al. (2015), Wang et al. (2015)). Based on this extension diagnosability has been studied first using similar methods as before (Liu et al. (2014)), then after using Integer Linear Programing techniques (Basile et al. (2016)). Recent work develop diagnosability analysis on more complex faults called timed patterns (Pencolé and Subias (2021)) using the twin plant method. This method is based on products between the system and the fault pattern. Another recent extension also based on a twin plant has been proposed (Lubat et al. (2020)) using a new product of TPN. Twin plant methods check for diagnosability by looking for the existence of critical pairs in the twin plant. Critical pairs are pairs of infinite behaviours, one faulty and the other not sharing the same observable informations, introduced in Pecheur et al. (2002).

The aim of this paper is to provide tools for the analysis of single timed fault in systems modeled as safe Labeled Time Petri Nets. Contrary to the works previously cited, the fault considered here is temporally constrained. The main idea is to abstract runs of the system that share the same sequence of transitions as a pair composed of the sequence and a set of time constraints that covers the possible dates of firing of each transition of the sequence. Based on these abstractions an analysis of the existence of critical pairs in the system is proposed. Two conditions are then provided for the diagnosability of this type of fault in such systems, one necessary, and the other necessary and sufficient.

The paper is articulated as follows. Section 2 recalls some elements about safe Labeled Time Petri Nets. Section 3.2 presents the diagnosis problem, the notion of diagnosability and its relation to critical pairs. Section 4 introduces the abstraction of the system runs called path. Then before concluding, Section 5 presents the analysis of critical pairs on the paths and presents a necessary and sufficient condition for diagnosability of single timed fault.

2. BACKGROUND ON TIME PETRI NETS

2.1 Safe Labeled Time Petri Net

Definition 1. A safe Labeled Time Petri Net (LTPN) is a 6-uple $N = \langle P, T, A, \Sigma, \ell, I_s \rangle$ where:

- P is a finite set of places
- T is a finite set of transitions ($P \cap T = \emptyset$)
- $A \subseteq (P \times T) \cup (T \times P)$ is a binary relation modeling the arcs between the transitions and the places
- Σ is a finite alphabet of transition labels
- $\ell : T \to \Sigma$ is the transition labeling function
- $I_s : T \to I_{\mathbb{Q}_+}$ is a static interval function $I_s(t)$, for which the lower bound, also called the date of earlier firing is denoted $\downarrow(I_s(t)) \in \mathbb{Q}_+$, and its upper bound, also called the date of later firing, is denoted $\uparrow(I_s(t)) \in \mathbb{Q}_+ \cup \{+\infty\}$

M is the marking of the net (M: $P \to \{0, 1\}$).

The *preset* of a transition t is the set of input places $pre(t) = \{p \in P |\ (p, t) \in A\}$, and similarly the *postset* of t is the set of output places $post(t) = \{p \in P |\ (t, p) \in A\}$. For a *safe* LTPN, a state is a couple $S = \langle M, I \rangle$ where I is the partial firing interval application (I: $T \to I_{\mathbb{Q}_+}$) that

associates to any transition a time interval of $\mathbb{Q}_+$ in which t can be fired as soon as it is enabled. $S_0 = \langle M_0, I_0 \rangle$ is the initial state of the net where M_0 is the initial marking of the net and I_0 is defined as follows: for any transition t enabled by M_0, $I_0(t) = I_s(t)$, else $I_0(t) = \varnothing$. For a marking M, a transition t is firable at the date θ if and only if:

- t is enabled (*i.e.* $\forall p \in pre(t)$, $M(p) > 0$)
- $\theta \in I(t)$ and for all t' enabled by M, $\theta \leq \uparrow (I(t')$

The firing of a transition t at a date θ is denoted: $\langle M, I \rangle \xrightarrow{\theta t} \langle M', I' \rangle$ and defined such that

- M' is such that $\forall p \in pre(t) \setminus post(t), M'(p) = 0$, $\forall p \in post(t) \setminus pre(t)$, $M'(p) = 1$ else $M'(p) = M(p)$
- for any transition $t' \in T$ $(t' \neq t)$ enabled by M and still enabled by M', $I(t') = [a, b] \Rightarrow I'(t') = [max(0, a - \theta), b - \theta]$
- for every transition t' enabled by M', not by M, and each transition disabled by the firing of t and newly enabled by it (loops), $I'(t') = I_s(t')$

A state S is reachable in a marked LTPN if there exists a run $r = \theta_1 t_1 \dots \theta_n t_n, n \in \mathbb{N}^*$ *such that* $S_0 \xrightarrow{\theta_1 t_1} S_1 \xrightarrow{\theta_2 t_2} S_2 \dots \xrightarrow{\theta_n t_n} S$. The set of reachable states of a LTPN N is denoted $R(N, S_0)$.

A run $r = \theta_1 t_1 \dots \theta_n t_n$ of a LTPN is said to be admissible if there exists $S_1, \dots S_n$ reachable states of N such that $S_0 \xrightarrow{\theta_1 t_1} S_1 \xrightarrow{\theta_2 t_2} S_2 \dots \xrightarrow{\theta_n t_n} S_n$.

A *timed sequence* over an alphabet Σ is a sequence of pairs $(d, e) \in \mathbb{R}_+ \times \Sigma$ where d corresponds to the date of firing of symbol e. A run produces a unique timed sequence.

Definition 2. The language $\mathcal{L}(N)$ of a LTPN N is the set composed of every timed sequence ρ such that there exists $r = \theta_1 t_1 \dots \theta_n t_n$ an admissible run for N with $\rho = \theta_1 \ell(t_1) \dots \theta_n \ell(t_n)$.

Berthomieu and Menasche (1983) defines a State Class Graph (SCG) which is an abstraction of the LTPN as an automaton. Each state is a covering class between the states of the LTPN that share their marking and their firing domain i.e the time constraints on the firable transitions from the marking. The initial firing domain is defined by $I_0(t)$ for each t enabled by M_0.

Definition 3. A State Class Graph (SCG) of a LTPN $N = \langle P, T, A, \Sigma, \ell, I_s \rangle$ is a triple (C,$\mathcal{C}_0, \rightarrow$) *such that*:

- $\mathcal{C}_0 = (M_0, F_0)$ where M_0 is the initial marking of N and $F_0 \in (I_{\mathbb{Q}_+})^T$ is the initial firing domain of N
- C $\in \{0,1\}^P \times (I_{\mathbb{Q}_+})^T$ is the set of all classes corresponding to states reachable in N
- $\rightarrow \in C \times T \times C$ is the transition function defined as follows : $(M, F) \xrightarrow{t} (M', F')$ iff
  - t is firable from (M, F)
  - $M' = M - pre(t) + post(t)$
  - $F' = next(F, t)$

where $next : (I_{\mathbb{Q}_+})^T \times T \rightarrow (I_{\mathbb{Q}_+})^T$ is the procedure to build the firing domain F' associated with a reachable marking M' reached from M by the firing of t that is defined as follows:

(1) for each transition t' enabled in M, compute the firing of t by adding the two constraints $\theta \leq \theta'$ and $\theta' = \theta + \theta'_{upd}$ (θ'_{upd} is a substitution variable)
(2) eliminate variables relative to transitions enabled in M and not in M'
(3) add the constraints relative to the newly enabled transitions (in M')
(4) determine the canonical form of each constraint in F'

2.2 Preliminary result

In this section a result about the dates of firing of a transition in a cycle of a SCG is presented. The main idea is to show that the earlier and later dates of firing of a transition relatively to the preceding transition in the cycle do not depend on the number of times the cycle has been fired previously. Let C be a class in a SCG. The earlier and later dates of firing of a transition t in a sequence relatively to the transition previously fired t' are denoted α_t and β_t respectively. Let $\sigma = t_i \dots t_k$ be a cycle in the SCG firable from C. Let us consider $\Pi = \{\alpha_{t_i} \leq d_i \leq \beta_{t_i}, \dots \alpha_{t_k} \leq d_k \leq \beta_{t_k}\}$, where $d_{i,i\in[0,n]}$ is the firing date of t_i. Π is a set of constraints that represents the earlier and later dates of firing of the transitions of σ according to the cycle σ. The repeated firing k times of σ is denoted σ^k.

Lemma 1. Let us consider $k \in \mathbb{N}^*$. Considering the k^{th} firing of a transition t_j in σ^k, the time constraints on its date of firing is the same as its constraint for σ, *i.e.* $\alpha_{t_j} \leq d_j \leq \beta_{t_j}$.

Sketch proof: *As α_t represents for a transition t in σ the earlier date of firing relatively to the previous transition fired in σ, for each value of k, t will be fired from the same class in the SCG.*

Remark: The earlier and later dates of firing of a transition in a sequence do not depend only on the firing domains of this transition in its firign class but also of the order of the transitions fired before and after it.

Example 1. Let us consider the cycle $C_5 = \{0 \leq t_3 \leq 1\}$, $C_7 = \{1 \leq t_4 \leq 2\}$, $C_9 = \{1 \leq t_5 \leq 4\}$, $C_{11} = \{3 \leq t_6 \leq 4\}$, $C_{13} = \{2 \leq t_7 \leq 4\}$ in the extract of SCG presented in Figure 2, and the loop $(t_3.t_4.t_5.t_6.t_7)^3$ (3 repeated firing of the sequence $t_3.t_4.t_5.t_6.t_7$). If the third firing of the loop is considered, the firing of t_4 is relative to the one of t_3, $[1, 2]$ (here given by C_7), which is the same as its firing in the first loop.

3. DIAGNOSABILITY: PROBLEM STATEMENT

This section presents the modeling of the diagnosis problem as a fault matching and recalls the notion of critical pair and its relation to diagnosability checking.

3.1 Modeling

In this work the system is modeled as a partially observable safe LTPN $\Theta = \langle P_\Theta, T_\Theta, A_\Theta, \Sigma_\Theta, \ell_\Theta, I_{s,\Theta} \rangle$. Each firing interval is closed with its bounds belonging to $\mathbb{Q}_+$. The alphabet is partitioned into two sets: $\Sigma_{o\Theta} = \{o_1, \dots, o_n\}$ the set of observable events on Θ, and $\Sigma_{u\Theta} = \{uo_1, \dots, uo_p\}$ the set of unobservable events. Similarly T_Θ is partitioned

into $T_{o\Theta}$ the set of transitions labeled by an observable event, and $T_{u\Theta}$ the set of transitions labeled by an unobservable event. Some other assumptions are formulated about Θ:

- **A0** the SCG of the system is finite
- **A1** there is no cycle of unobservable transitions in the system
- **A2** the system has no zeno run (a zeno run is an infinite sequence of transitions that can occur in a finite amount of time).

Condition **A0** ensures that for each transition $t \in T_\Theta$, there is a finite number of arcs in the SCG of Θ labeled by t. Condition **A1** ensures that the system is ultimately observable, meaning that an observable transition will always be fired in a finite amount of time after another one. Condition **A2** prevents an infinite number of events from occurring in a finite amount of time, which is unrealistic in real systems.

Definition 4. A timed fault Ω over a system Θ is an unobservable event $f \in \Sigma_{u\Theta}$ associated to a closed rational interval $[a_\Omega, b_\Omega] \in \mathbb{Q}_+^2$. The language associated to Ω is $\mathcal{L}(\Omega) = \{d_i f | d_i \in [a_\Omega, b_\Omega]\}$.

The occurrence of a timed fault in a run of the system is considered as a matching problem:

Definition 5. A timed sequence $\rho \in \mathcal{L}(\Theta)$ matches a timed fault Ω (denoted $\rho \Rrbracket \Omega$) if there exists a sub-word ρ' of ρ (i.e ρ' is an ordered set of events extracted from ρ) such that $\rho' \in \mathcal{L}(\Omega)$.

Without ambiguity, it is said that a run r matches a timed fault Ω ($r \Rrbracket \Omega$) if the timed sequence ρ produced by r matches Ω. For a timed sequence for which there exists more than one solution to match a fault Ω, the faulty event is the first to be faulty, *i.e.* if there exists two faulty events only the first is considered faulty as the fault has already occurred when the second occurs.

3.2 Critical pair: diagnosability checking

Diagnosability of a fault is the property for a system to know with certainty that a fault has occurred a certain amount of time after its occurrence. In other words, a system is Ω-diagnosable if for an observable timed sequence ρ_o associated to a run r for which the fault has occurred ($r \Rrbracket \Omega$), there exists ρ'_o a continuation of ρ_o for which one is sure that the fault has occurred. This implies that each run producing ρ'_o as its observable time sequence necessarily matches the fault.

The projection of a timed sequence onto the observable alphabet of the system (also called observable timed trace) is defined as follows:

• $\mathbf{P}_{\Sigma_\Theta \to \Sigma_{o\Theta}}(\theta_1 e_1.\theta_2 e_2 \dots \theta_n e_n) = \theta_1 e_1.\mathbf{P}_{\Sigma_\Theta \to \Sigma_{o\Theta}}(\theta_2 e_2 \dots \theta_n e_n)$ if $e_1 \in \Sigma_{o\Theta}$
• $\mathbf{P}_{\Sigma_\Theta \to \Sigma_{o\Theta}}(\theta_1 e_1.\theta_2 e_2 \dots \theta_n e_n) = \mathbf{P}_{\Sigma_\Theta \to \Sigma_{o\Theta}}((\theta_1 + \theta_2) e_2 \dots \theta_n e_n)$ otherwise

Based on the definition introduced in Pencolé and Subias (2021), the notion of diagnosability for timed system can be defined as:

Definition 6. Θ is said to be Ω-diagnosable iff $\exists \tau \in \mathbb{R}_+$ *s.t.* $\forall (\rho_1, \rho_2) \in \mathcal{L}(\Theta)^2$, $\rho_1 = \rho'_1.\rho''_1, time(\rho''_1) \geq \tau$, $\rho'_1 \Rrbracket \Omega \wedge \mathbf{P}_{\Sigma \to \Sigma_{o\Theta}}(\rho_2) = \mathbf{P}_{\Sigma \to \Sigma_{o\Theta}}(\rho_1) \Rightarrow \rho_2 \Rrbracket \Omega$.

where *time* is the function that associates to each timed sequence its duration.

Then from definition 6, checking whether a system Θ is Ω-diagnosable consists in determining that there are no infinite timed sequence ρ_1 and ρ_2 in $\mathcal{L}(\Theta)$ with $\rho_1 \Rrbracket \Omega$ and $\rho_2 \not\Rrbracket \Omega$, such that $\mathbf{P}_{\Sigma \to \Sigma_{o\Theta}}(\rho_2) = \mathbf{P}_{\Sigma \to \Sigma_{o\Theta}}(\rho_1)$.

To check diagnosability one can search for the existence of *critical pairs* (Pecheur et al. (2002)).

Definition 7. A critical pair is a couple of infinite runs (r_1, r_2) of a system Θ such that:

- $r_1 \Rrbracket \Omega$
- $r_2 \not\Rrbracket \Omega$
- $\mathbf{P}_{\Sigma \to \Sigma_{o\Theta}}(\rho_1) = \mathbf{P}_{\Sigma \to \Sigma_{o\Theta}}(\rho_2)$

where ρ_1 and ρ_2 are the timed sequences associated to r_1 and r_2.

A *critical pair* is basically the revelation of an ambiguity for an observable timed sequence, the proof that it is not possible to decide whether the fault has occurred or not for these observations. Based on Jiang et al. (2001) and Pecheur et al. (2002) is recalled a general result on diagnosability:

Proposition 1. Θ is Ω-diagnosable iff there is no critical pair.

The aim of this proposal is to provide analytic properties to check the existence of critical pairs in a system for a timed fault. As critical pairs are infinite runs, for a given timed fault, an abstraction of infinite runs of the system sharing the same transition sequence as its support, called path, is proposed in the next section.

4. ABSTRACTION OF SYSTEM RUNS: PATHS OF THE SCG

To extract the system behaviours from the *SCG* it is first necessary to be sure that the behaviours captured in the *SCG* are the ones that the Petri model of the system can execute. But the behaviours modeled in the *SCG* do not take into account potential parallelism in the system. For a sequence of transition $\sigma = t_0 \dots t_n$ firable in a *SCG* it is then possible in case of parallelism that some combinations of dates of firing of the sequence are not admissible for the system. The admissible combinations of dates have to respect constraints of the form $\alpha' \leq \sum_i d_i \leq \beta'$.

Example 2. Considering the LTPN of Figure 1, its SCG has 4 classes: C_0 ($P_0P_2, 1 \leq t_0 \leq 3, 1 \leq t_1 \leq 3$), C_1 ($P_1P_2, 0 \leq t_1 \leq 2$), C_2 ($P_0P_3, 1 \leq t_0 \leq 2$) and C_3 (P_1P_3). For a sequence of transitions $t_0.t_1$, the run $r = 3t_0.2t_1$ respects the firing domains of the SCG of the LTPN in Figure 1, but this is not an admissible run for the system. Every behaviour based on the firing sequence $t_0.t_1$ must also satisfy the constraint $1 \leq d_0 + d_1 \leq 3$ where d_0 and d_1 are the dates of firing of t_0 relatively to the starting of the system and t_1 relatively to the firing of t_0.

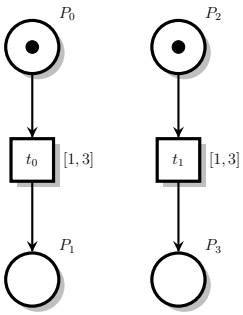

Fig. 1. LTPN illustrating the constraints imposed by parallelism in a system

Once the admissible constraints have been integrated, the set of observable constraints relative to a sequence σ denoted Π, can be obtained by a method of variable elimination (Fourier-Motzkin as an example) applied to the linear inequality system derived from the time constraints on the firing dates of the transitions of σ. This set of constraints can be written as $\{\{C(t_{o,i})\}, \{AC\}\}_{t_{o,i} \in \sigma}$ where $C(t_{o,i})$ and AC are two types of observable constraints (constraints on the dates of the observable transitions of the associated sequence) defined as:

- $C(t_{o,i}) = \alpha_{o,t_i} \leq d_{o,i} \leq \beta_{o,t_i}$ where α_{o,t_i} (resp. β_{o,t_i} is the earlier (resp. later) date of firing of $t_{o,i}$ relatively to the previous observable transition fired in σ (the start of the system for the first observable transition of σ)
- $AC = \alpha_I \leq \sum_{i \in I} d_{o,i} \leq \beta_I$ where α_I and β_I are the bounds of the admissibility constraint of $t_{o,i}$ and I a set of indices of observable transitions

In the case of infinite executions of the system as those of a critical pair, the observable constraints set Π is not finite. Indeed, the transitions sequences each member of the critical pair is using as a support contains an infinite looping of transitions that are going to be fired indefinitely. Nevertheless, it is possible for such infinite behaviours of a critical pair to define a finite abstraction called *path*. As each critical pair is relative to a specific timed fault Ω, the finite abstraction *path* built must be also linked to the considered timed fault Ω. Then, considering all the infinite executions of the system (i.e infinite runs) supported by the same transitions sequence σ_π, and a given timed fault Ω, a *path* is defined as follows:

Definition 8. A path $\pi = (\sigma_\pi, \Pi)$ in $SCG(\Theta)$ (the SCG of a system Θ) is a couple where:

(1) $\sigma_\pi = t_0 \dots t_n$ is such that:
- t_0 is enabled by M_0
- $\sigma_\pi \in \rightarrow^*$
- there exists $i \in [2, (n-1)]$ such that t_i is an observable transition whose absolute date of firing (*i.e.* date of firing relatively to the starting of the system) is greater than b_Ω the time interval upper bound of the timed fault Ω
- after t_i the rest of the sequence leads to a loop in the SCG
- t_n is observable (it is always possible to build such sequences as Θ is ultimately observable)

(2) Π is the set of inequations on the firing dates of the observable transitions of σ_π

The set of paths of a system is denoted $\mathcal{P}_\Theta$.

Using the fact that t_o and t_n are observable and Lemma 1, the firing date of any transition in the loop part of σ_π is subject to the constraints of Π. Thus any continuation of the sequence σ_π is also subject to the constraints of Π, meaning every run using any continuation of σ_π can be characterized by Π, *i.e.* by π.

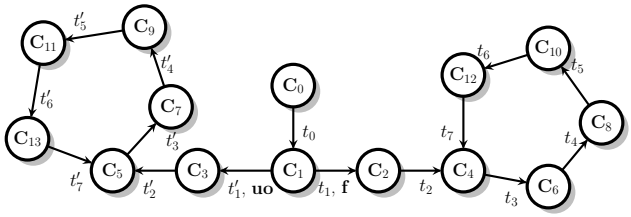

Fig. 2. Part of a SCG exhibit the transition sequences of two paths and the visited classes associated

Example 3. Figure 2 gives a partial view of the *SCG* of a system Θ. The fault considered on this example is $[a_\Omega, b_\Omega]f$, where f is the faulty event. It appears, two types of infinite behaviours due to the two strong connected components of the graph $\{C_5, C_7, C_9, C_{11}, C_{13}\}$ and $\{C_4, C_6, C_7, C_{10}, C_{12}\}$. From Figure 2 considering the fault, a path π_1 can be abstracted, admitting $\sigma_{\pi_1} = t_0.t_1.t_2.t_3.t_4.t_5.t_6.t_7$ as its transition sequence. Each transition sharing the same indices $i \in [2, 7]$ is sharing the same label $e_i \in \Sigma_{o\Theta}$. In this SCG t_1 is labeled by a faulty event f (its firing domain is $\alpha_1 \leq t_1 \leq \beta_1$) and t'_1 is labeled by a non-faulty unobservable event u_o. Except t_1 and t'_1 every transition is observable. By considering π_1, the observable transition following the fault t_1 is in this case t_2 and the looping part is $t_3.t_4.t_5.t_6.t_7$. For this example let us suppose that the firing domain of class C_4 is $\{2 \leq t_3 \leq 5, 1 \leq t_9 \leq 3\}$ meaning there is a transition t_9 (not in the Figure) that is in structural conflict with t_3. Considering the sequence σ_{π_1}, from C_4 the transition t_3 must be fired before t_9, that induces $C(t_{o,3}) = \{2 \leq d_{o,3} \leq 3\}$ (t_3 must be fired before 3 time units after its enabling (t_2 is observable)) where $d_{o,3}$ is the observable date of t_3.

5. DIAGNOSABILITY: CRITICAL PAIR ANALYSIS

When a closer look is taken on the set of observable constraints Π of a sequence σ_π of a path π, for a particular solution there are three cases: either the solution corresponds to faulty runs exclusively, or it corresponds to non-faulty runs exclusively, or it can correspond to both faulty and non-faulty runs. On the basis of this remark, the set can therefore be partitioned as follows:

(1) Π_s the set of observable constraints for which it is sure that the fault has not occurred. For each observable run r_o which results in the projection of a run r onto its observable transition, each run r admitting r_o as its observable projection is such that $r \not\Vdash \Omega$.
(2) Π_c the set of observable constraints for which the occurrence of the fault is certain. For each observable run r_o each run r admitting r_o as its observable projection is such that $r \Vdash \Omega$.
(3) Π_a the set of observable constraints for which there is an ambiguity. For each observable run r_o there exists (r_1, r_2) admitting r_o as their observable projection is such that $r_1 \Vdash \Omega \wedge r_2 \not\Vdash \Omega$.

In this section some conditions for the inexistence of ambiguity are presented based on the study of Π_a first (Section 5.1), and then on Π_s and Π_c (Section 5.2). If there is no ambiguity, then the system does not admit any critical pair.

5.1 Critical pair extracted from one path

Let us consider a path π. The set of solutions of a set of constraints Π is denoted $\mathcal{S}(\Pi)$.

Considering π, if $\mathcal{S}(\Pi_a)$ is not empty this means that there exists at least two runs, one faulty and the other not, sharing the same observable timed trace belonging to π.

Lemma 2. If there exists a path π for which $\mathcal{S}(\Pi_a) \neq \emptyset$, then there exists two runs of π that form a critical pair. Consequently Θ is not Ω-diagnosable.

Sketch proof: *Direct consequence of the existence of an ambiguity.*

In the following, the work presented focuses on the study of the conditions of emptiness of $\mathcal{S}(\Pi_a)$. The notion of "faulty candidate transition" is introduced as a transition labeled by the faulty event that may occur at a date that complies with the time interval of the fault. Considering a faulty candidate transition t_Ω, knowing if it will be a source of ambiguity is equivalent to determine the observable date covering its firing, *i.e.* the observable date of the first observable transition $t_{o,\Omega}$ fired after t_Ω. If there is a faulty candidate transition for which the knowledge of the firing observable date of $t_{o,\Omega}$ is not sufficient to conclude whether the fault occured or not, then there is at least one solution in Π_a. The time interval of firing of t_Ω relatively to the start of the system is denoted $[\alpha_\Omega, \beta_\Omega]$.

Proposition 2. Let us consider π a path. The following statement holds: if there exists t_Ω in σ_π such that $a_\Omega \leq \alpha_\Omega \leq \beta_\Omega \leq b_\Omega$, then for every run r of Θ admissible for the system using a support σ' such that $\sigma_\pi \in prefix(\sigma')$, r matches Ω ($r \Subset \Omega$). In other words, for such a π, $\mathcal{S}(\Pi_a) = \emptyset$.

Sketch proof: *Considering a run r of π, if this run matches Ω before t_Ω, meaning there exists a faulty transition preceeding t_Ω, then $r \Subset \Omega$. If there exists no faulty transition before the firing of t_Ω in r, then as $a_\Omega \leq \alpha_\Omega \leq \beta_\Omega \leq b_\Omega$ t_Ω will necessarily be faulty.*

Example 4. Let us go back to the example of Figure 2. Considering the path π_1 admitting as its sequece $\sigma_{\pi_1} = t_0.t_1.t_2.t_3.t_4.t_5.t_6.t_7$, the faulty transition t_1, with $\alpha_1 \leq t_1 \leq \beta_1$ and $a_\Omega \leq d_\Omega \leq b_\Omega$, let us assume that $a_\Omega \leq \alpha_1 \leq \beta_1 \leq b_\Omega$, then for every continuation σ' of σ_{π_1} the firing of t_1 will always be faulty. Then from Proposition 2, $\mathcal{S}(\Pi_{a,\pi_1} = \emptyset)$.

Proposition 2 states that if a faulty candidate transition t_Ω satisfies the condition, any run of this path will necessarily be faulty. This is not the only condition that may predispose a system to diagnosability. The other condition is the case of one-off intervals associated with each transition from the faulty candidate transition to the next observable transition (this observable transition included).

Lemma 3. If there is $(t_\Omega, t_{o,\Omega})$ such that $\alpha_{o,\Omega} = \beta_{o,\Omega}$, then there is no ambiguity on t_Ω. In other words, the possible observable dates of firing of $t_{o,\Omega}$ can be split into two sets without intersection: the dates for which t_Ω is faulty and the ones for which t_Ω is not faulty.

Sketch proof: *If $\alpha_{o,\Omega} = \beta_{o,\Omega}$, then the observable date of firing relatively to the previous observable transition can be decomposed as $d_{obs,\Omega} = d_{obs-1,\Omega} + \alpha_{o,\Omega}$ which can be provided by sensors. There is only one unknown value in this equation, then it is possible to know if it fits Ω or not.*

Example 5. For the example of Figure 2 , let us consider that $\alpha_1 < a_\Omega \leq \beta_1 \leq b_\Omega$, and that for the transition t_2, $\alpha_2 = \beta_2 = 3$. Let us denote d_1 the date of firing of t_1. The observable date of t_2 is then given by $d_{o,2} = d_1 + d_2 = d_1 + 3$. If $d_1 \in [\alpha_1, a_\Omega[$, then $d_{o,2} < a_\Omega + 3$. If $d_1 \in [a_\Omega, \beta_1]$, then $d_{o,2} \geq a_\Omega + 3$. Thus it is possible with the knowledge of $d_{o,2}$ to decide whether the run matches the fault or not. In other words $\mathcal{S}(\Pi_{a,\pi_1}) = \emptyset$.

Corollary 1. If for a path:

(1) there exists a faulty candidate transition that satisfies Proposition 2 or
(2) every faulty candidate transition satisfies Lemma 3

then for this path $\mathcal{S}(\Pi_a) = \emptyset$.

5.2 Critical pair extracted from two different paths

This section provides a necessary and sufficient condition for the diagnosability of a timed fault.

In the previous section the condition of emptiness of $\mathcal{S}(\Pi_a)$ as a necessary condition has been presented. This condition can be seen as a verification of the inexistence of critical pair inside a path. In the following proposition the inexistence of critical pairs is verified for pairs of runs extracted from two different paths.

For a better reading the sets $\mathcal{P}_{safe}$ and $\mathcal{P}_{certain}$ are defined as follows:

- $\mathcal{P}_{safe} = \{(\sigma_\pi, \Pi_s) \mid \pi = (\sigma_\pi, \Pi) \in \mathcal{P}_\Theta\}$
- $\mathcal{P}_{certain} = \{(\sigma_\pi, \Pi_c)\} \mid \pi = (\sigma_\pi, \Pi) \in \mathcal{P}_\Theta\}$

If for every path $\mathcal{S}(\Pi_a) = \emptyset$, then $\mathcal{P}_{safe}$ and $\mathcal{P}_{certain}$ cover all the runs of the system.

Proposition 3. If $\forall((\sigma_{\pi_1}, \Pi_{c,\pi_1}), (\sigma_{\pi_2}, \Pi_{s,\pi_2})) \in \mathcal{P}_{certain} \times \mathcal{P}_{safe}$ s.t. $\sigma_{\pi_1,o} = \sigma_{\pi_2,o}$, $\mathcal{S}(\Pi_{c,\pi_1}) \cap \mathcal{S}(\Pi_{s,\pi_2}) = \emptyset$ where $\sigma_{\pi_1,o}$ and $\sigma_{\pi_2,o}$ are the projections of σ_{π_1} and σ_{π_2} on their observable transitions, then no critical pairs can be extracted from two different paths.

Sketch proof: *If there exists a common solution, then there exists two different runs, one faulty and the other not, that share the same observable trace. This is a critical pair.*

Corollary 2. Θ is Ω-diagnosable $\Leftrightarrow$:

- $\forall\pi$, $\mathcal{S}(\Pi_a) = \emptyset$ and
- $\forall((\sigma_{\pi_1}, \Pi_{c,\pi_1}), (\sigma_{\pi_2}, \Pi_{s,\pi_2})) \in \mathcal{P}_{certain} \times \mathcal{P}_{safe}$ s.t. $\sigma_{\pi_1,o} = \sigma_{\pi_2,o}$, $\mathcal{S}(\Pi_{c,\pi_1}) \cap \mathcal{S}(\Pi_{s,\pi_2}) = \emptyset$

Example 6. Let us consider the two paths π_1 and π_2 that can be extacted from Figure 2 for which the two sequences of transitions are $\sigma_{\pi_1} = t_0.t_1.t_2.t_3.t_4.t_5.t_6.t_7$ and $\sigma_{\pi_2} = t_0.t'_1.t'_2.t'_3.t'_4.t'_5.t'_6.t'_7$. In this example the diagnosability result of Corollary 2 is illustrated, which means

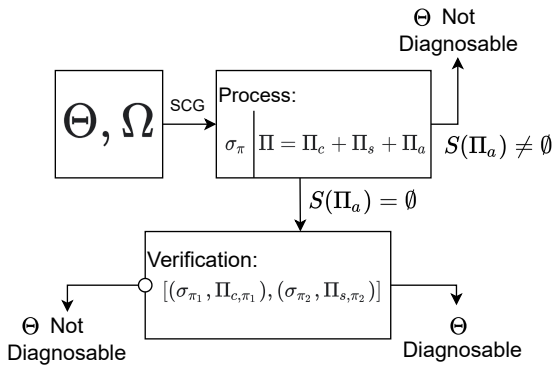

Fig. 3. Synthetic diagram for checking diagnosability of a timed fault Ω on a system Θ

that the involved faulty candidate transition t_1 satisfies Proposition 2 or Lemma 3, and then $\mathcal{S}(\Pi_a)$. Let us suppose that the time constraints relative to t_5 and t'_5 are respectively $\{2 \leq d_5 \leq 5\} \in \Pi_{c,\pi_1}$ and $\{4 \leq d'_5 \leq 6\} \in \Pi_{s,\pi_2}$. Let us suppose that $d_5 = d'_5 = 4$ satisfying the previous constraints. Let us also suppose that for every other $i \in [2,7] \setminus \{5\}$ there exists a common solution for each transition (t_i, t'_i), and let us denote d_i such a date. The observable sequence $1e_0.d_2e_2.d_3e_3.d_4e_4.4e_5.d_6e_6.d_7e_7$ can be produced by $1t_0.d_2t_2.d_3t_3.d_4t_4.4t_5.d_6t_6.d_7t_7$ (a run of σ_{π_1}) or $1t_0.d_2t'_2.d_3t'_3.d_4t'_4.4t'_5.d_6t'_6.d_7t'_7$ (a run of σ_{π_2}). Using Lemma 1, the observable sequence $\rho = 1e_0.d_2e_2.d_3e_3.d_4e_4.4e_5.d_6e_6.d_7e_7.d_3e_3.d_4e_4.4e_5.d_6e_6.d_7e_7.d_3e_3.d_4e_4.\ 4e_5.d_6e_6.d_7e_7 \ldots$ that is a continuation of the previous observable sequence can be produced by a run of each branch too. For ρ, it is possible to extract two sequences from $(\sigma_{\pi_1}, \Pi_{c,\pi_1})$ (which is faulty) and $(\sigma_{\pi_2}, \Pi_{s,\pi_2})$ (which is not faulty). That will lead to a critical pair. Let us now consider a new case where the time constraints relatives to t_5 and t'_5 are now respectively $2 \leq d_5 \leq 3$ (for Π_{c,π_1}) and $4 \leq d'_5 \leq 6$ (for Π_{s,π_2}), then it is not possible to build such a sequence, then there is no critical pair that can be extracted from $(\sigma_{\pi_1}, \Pi_{c,\pi_1})$ and $(\sigma_{\pi_2}, \Pi_{s,\pi_2})$.

Figure 3 gives an overview of the proposed method to check the diagnosability of a timed fault on a system. First the SCG of the system is calculated. Using Definition 8, the different paths of the system are extracted (there is a finite number of paths). Then a first verification is made on the sets of constraints of each path, verifying the set of solutions of each Π_a. If for every path, Π_a has no solution, then the second verification is processed with the pairs of paths admitting the same event sequence (using Π_s and Π_c).

6. CONCLUSION

This work proposes a new approach to verify the diagnosability of single timed fault in Discrete Event Systems modeled as safe Labeled Time Petri Nets. The diagnosability analysis is performed on an abstraction using the time characteristics of the fault as time constraints. To tackle the infinite run problem, the cycles are characterized with these constraints. Then properties on the solution sets of a partition of these constraints are provided.

Future works include the extension of this analysis to timed patterns, that are complex faults one can model as safe labeled timed Petri nets. Another issue is to propose an explanation of the non diagnosability of a system for a certain fault, and to develop a method to repair the system in order to make it diagnosable. Finally an extension to unsafe bounded Petri net is an interesting issue but demand a discussion about multi-sensibilisation.

REFERENCES

Basile, F., Cabasino, M.P., and Seatzu, C. (2015). State Estimation and Fault Diagnosis of Labeled Time Petri Net Systems With Unobservable Transitions. *IEEE Transactions on Automatic Control*, 60(4), 997–1009. doi:10.1109/TAC.2014.2363916.

Basile, F., Cabasino, M.P., and Seatzu, C. (2016). Diagnosability analysis of labeled time Petri net systems. *IEEE Transactions on Automatic Control*, 62(3), 1384–1396.

Berthomieu, B. and Menasche, M. (1983). An enumerative approach for analyzing time Petri nets. In *Proceedings IFIP*, 41–46. Elsevier Science Publishers.

Jiang, S., Huang, Z., ch, V., and Kumar, R. (2001). A polynomial algorithm for testing diagnosability of discrete event systems. *IEEE Transactions on Automatic Control*, 46. doi:10.1109/9.940942.

Liu, B., Ghazel, M., and Toguyéni, A. (2014). Diagnosis of labeled time Petri nets using time interval splitting. *IFAC Proceedings Volumes*, 47(3), 1784–1789.

Lubat, É., Dal Zilio, S., Le Botlan, D., Pencolé, Y., and Subias, A. (2020). A new product construction for the diagnosability of patterns in time Petri net. In *2020 59th IEEE Conference on Decision and Control (CDC)*, 104–109. IEEE.

Pecheur, C., Cimatti, A., and Cimatti, R. (2002). Formal verification of diagnosability via symbolic model checking. In *Workshop on Model Checking and Atificial intelligence (MoChArt-2002), Lyon, France.*

Pencolé, Y. and Subias, A. (2021). Diagnosability of event patterns in safe labeled time Petri nets: A model-checking approach. *IEEE Transactions on Automation Science and Engineering*, 1–12. doi: 10.1109/TASE.2020.3045565.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., and Teneketzis, D. (1995). Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 40(9), 1555–1575. doi:10.1109/9.412626.

Tripakis, S. (2002). Fault diagnosis for timed automata. In W. Damm and E.R. Olderog (eds.), *Formal Techniques in Real-Time and Fault-Tolerant Systems*, 205–221. Springer Berlin Heidelberg, Berlin, Heidelberg.

Wang, X., Mahulea, C., and Silva, M. (2015). Diagnosis of time Petri nets using fault diagnosis graph. *IEEE Transactions on Automatic Control*, 60(9), 2321–2335. doi:10.1109/TAC.2015.2405293.