Combining Free choice and Time in Petri Nets

S. Akshay
IIT Bombay
Email: akshayss@cse.iitb.ac.in

Loïc Hélouët
INRIA Rennes
Email: loic.helouet@inria.fr

Ramchandra Phawade
IIT Bombay
Email: ramchandra@cse.iitb.ac.in

Abstract—Time Petri nets (TPNs) [13] are a classical extension of Petri nets with timing constraints attached to transitions, for which most verification problems are undecidable. We consider TPNs under a strong semantics with multiple enabling of transitions. We focus on a structural subclass of unbounded TPNs, where the underlying untimed net is free choice, and show that it enjoys nice properties in the timed setting under a multi-server semantics. In particular, we show that the questions of firability (whether a chosen transition can fire), and termination (whether the net has a non-terminating run) are decidable for this class. We then consider the problem of robustness under guard enlargement [14], i.e., whether a given property is preserved even if the system is implemented on an architecture with imprecise time measurement. This question was studied for TPNs in [3], and decidability of several problems was obtained for bounded classes of nets. We show that robustness of firability is decidable for unbounded free choice TPNs with a multi-server semantics.

I. INTRODUCTION

Modern systems are composed of several distributed components that work in real-time to satisfy a given specification. This makes them difficult to reason about manually and encourages the use of formal methods to analyze them automatically. This in turn requires the development of models that capture all the features of a system and still allow efficient algorithms for analysis. Further, to bring formal models closer to real world implementations, it is important to design robust models, i.e., models that preserve their behavior or at least some important properties under imprecise time measurement.

In this paper, we consider Petri nets extended with time constraints. These models have been used for modeling real-time distributed systems, but for timed variants of Petri nets, many basic problems are usually undecidable or algorithmically intractable. Our goal is to consider structural restrictions which allow to model features such as unbounded resources as well as time-deadlines while remaining within the realm of decidability and satisfying some robustness properties.

Time Petri nets (TPNs) [13] are a classical extension of Petri nets in which time intervals are attached to transitions and constrain the time that can elapse between the enabling of a transition and its firing date. In such models, the basic verification problems considered include: reachability, i.e., whether a particular marking (or a configuration) can be reached in the net, termination, i.e., whether there exists an infinite run in the net, boundedness, whether there is a bound on the number of tokens in the reachable markings, and firability, i.e., whether a given transition is fireable in some execution of the net. It turns out that all these basic problems are in general undecidable [11] for TPNs, though they are decidable for the untimed version of Petri nets. The main reason is that TPNs are usually equipped with an urgent semantics: when the time elapsed since enabling of a transition reaches the maximal value of its interval, a transition of the net has to fire. This semantics breaks monotony (the behaviors allowed from a marking, and from a larger marking can be completely different). Indeed, with a TPN, one can easily encode a two-counter machine, yielding undecidability of most of verification problems (see [16] for such an encoding). In order to obtain decidability, one has either to restrict to bounded classes [12], or weaken the semantics to ignore or restrict urgency, as in [2], [16].

Another important problem in this setting is the question of robustness. Robustness can be defined as a question regarding the preservation of properties of systems that are subject to imprecision of time measurement. The main motivation for considering these problems is that formal models usually have an idealized representation of time, and assume an unrealizable precision in time measurement, that cannot be guaranteed by real implementations. Robustness has been considered extensively for timed automata since [14], and more recently for TPNs [3], but decidability results are only obtained in a bounded-resource setting.

The definition of the semantics plays an important role both to define the expressive power of a model and to obtain decidability results. When considering unbounded nets, where multiple (and in fact unboundedly many) tokens may be present at every place, one has to fix a policy on whether and how multiply-enabled transitions are handled. And this becomes even more complicated when real-time constraints are considered. Indeed, several possible variants for the multiple enabling semantics have been considered, as discussed in [5]. In this paper, we fix one of the variants and consider TPNs equipped with a multi-enabling urgent semantics, which allows to start measuring elapsed time from every occurrence of a transition enabling. This feature is particularly interesting: combined with urgency, it allows for instance to model maximal latency in communication channels. We adopt a semantics where time is measured at each transition’s enabling, and with urgency, i.e. a discrete transition firing has to occur if a transition has been enabled for a duration that equals the upper bound in the time interval attached to it. Obviously, with this semantics, counter machines can still be encoded, and undecidability follows in general.

We focus on a structural restriction on TPNs, which restricts the underlying net of the given TPN to be free-choice, and
call such nets *Free-choice TPNs*. Free-choice Petri nets have been extensively studied in the untimed setting [9] and have several nice properties from a decidability and a complexity-theoretic point of view. In this class of nets, all occurrences of transitions that have a common place in their preset are enabled at the same instant. Such transitions are said to belong to a cluster of transitions. Thus, with this restriction, a transition can only prevent transitions from the same cluster to fire, and hence only constrain firing times of transitions in its cluster. Further, we disallow instantaneous occurrence of infinite behaviors, that we call 0-delay firing sequences in our nets. This can easily be ensured by another structural restriction forbidding transitions or even loops in TPNs labeled with \([0,0]\) constraints.

Our main results are the following: we show that for a free-choice TPN \(N\) under the multiple-enabling urgent semantics, and in the absence of 0-delay infinite firing sequences, the problem of fireability of a transition and of termination are both decidable. The main idea is to show that, after some pre-processing, we can reduce these problems to corresponding problems on the underlying untimed free-choice PN. More precisely, we are able to show that every partially-ordered constraints to arcs, and allow firing of a transition iff all constraints attached to transitions are satisfied by at least one token in each place of its preset. This variant, called Timed-arc Petri nets, enjoys decidability of coverability [1], but cannot be used to define equivalences among time Petri nets. Unfolding and processes were refined by [7] to obtain symbolic unfoldings for *safe* Petri nets. The closest work to ours is [8], where processes are defined to reason on the class of free-choice *safe* TPNs. However, this work does not consider unbounded nets, and focuses more on semantic variants wrt time-progress than on decidability or robustness issues.

The paper is organized as follows: section II introduces notations and defines a class of TPNs with multi-enabling semantics. Section III defines processes for these nets. Section IV introduces the subclass of Free-choice TPNs and, in Section VI, to address robustness of TPNUs, this is used to prove decidability of firability and termination for FC-TPNs and, in Section VI, to address robustness of firability. Section VII discusses our assumptions and deals with issues related to decidability of other problems in FC-nets.

**II. Multi-enabledness in TPNs**

Let \(\Sigma\) be a finite alphabet, \(\Sigma^*\) be the set of finite words over \(\Sigma\). For a pair of words \(w, w' \in \Sigma^*\), we will write \(w \leq w'\) iff \(w' = w.v\) for some \(v \in \Sigma^*\). Let \(\mathbb{N}, \mathbb{Q}, \mathbb{R}_{\geq 0}\), respectively, denote the sets of naturals, non-negative rationals, and real numbers. An interval \(I \subseteq \mathbb{R}_{\geq 0}\), if its left endpoint belongs to \(\mathbb{Q}_{\geq 0}\) and right endpoint belongs to \(\mathbb{Q}_{\geq 0} \cup \{\infty\}\). Let \(T\) denote the set of \(\mathbb{Q}_{\geq 0}\)-intervals of \(\mathbb{R}_{\geq 0}\). For a set \(X\) of (clock) variables, a valuation \(v\) for \(X\) is a mapping \(v : X \to \mathbb{R}_{\geq 0}\). Let \(v_0(X)\) be the valuation which assigns value 0 to each clock in \(X\). For any \(d \in \mathbb{R}_{\geq 0}\), the valuation \(v + d\) is \(: \forall x \in X, (v + d)(x) = v(x) + d\).

A Petri net (PN) \(U\) is a tuple \(U = (P,T,F)\), where \(P\) is a set of places, \(T = \{t_1,t_2,\ldots,t_K\}\) is a set of transitions, and \(F \subseteq (P \times T) \cup (T \times P)\) is a flow relation. A marking \(M\) is a function \(P \to \mathbb{N}\) that assigns a number of tokens to each place. We let \(M_0\) denote an initial marking for a net. For any \(x \in P \cup T\) (called a node) let \(\bullet x = \{y \in P \cup T \mid (y,x) \in F\}\) and \(x^* = \{y \in P \cup T \mid (x,y) \in F\}\). For a transition \(t\), we will call \(\bullet t\) the preset of \(t\), and \(t^*\) the *postset* of \(t\). The semantics of a Petri net is defined as usual: starting from a marking \(M\), a transition \(t\) can be fired if for every \(p \in \bullet t, M(p) > 0\). This firing results in new marking \(M'\) such that \(M'(p) = M(p) - \lvert \bullet t \cap \{p\} \rvert + \lvert t^* \cap \{p\} \rvert\). We denote a discrete move of a Petri net from \(M_0\) to \(M'\). \((U,M_0)\) denotes the set of reachable markings, that can be obtained via an arbitrary number of moves starting from \(M_0\). Let \(x\) be any node of a net. The *cluster* of \(x\) (denoted by \([x]\)) is a minimal set of nodes of \(N\) satisfying following conditions: (i) \(x \in [x]\), (ii) if a place \(p\) is in \([x]\), then \(p^* \subseteq [x]\), and (ii) if a transition \(t\) is in \([x]\), then \(\bullet t \subseteq [x]\).
Definition 1: A time Petri net (TPN) $N$ is a tuple $(\mathcal{U}, M_0, I)$ where $\mathcal{U} = (P, T, F)$ is the underlying net, $M_0$ is an initial marking, and $I: T \rightarrow \mathcal{I}(Q_{\geq 0})$ associates with each transition a firing interval.

We denote by $eft(t)$ and $lft(t)$ the lower and upper bound of interval $I(t)$. For a TPN $N = (\mathcal{U}, M_0, I)$ let $\text{Untime}(N) = (\mathcal{U}, M_0)$ denote the underlying net i.e., with no timing constraints for any transitions.

Let us now describe the semantics of Time Petri nets with multi-enabledness. In a multi-enabling semantics, when a marking associates to each place in the preset of a transition a number of tokens that is several times the number of tokens needed for the transition to fire, then this transition is considered as enabled several times, i.e. several occurrences of this transition are waiting to fire. Defining a multi-enabling semantics needs to address carefully which instances of enabled transitions can fire, what happens when an instance of a transition fires, in terms of disabling and creation of other enabled transitions can fire, what happens when an instance of a transition fires, in terms of disabling and creation of other instances. Several policies are possible as discussed in [5]. In the rest of the paper, we adopt a semantics where the oldest instances of transitions fire first, are subject to urgency requirements, and the oldest instances are also the disabled ones when a conflict occurs. We formalize this below.

Definition 2: Let $M$ be a marking of a TPN $N = (\mathcal{U}, M_0, I)$. A transition $t \in T$ is $k$-enabled at marking $M$, for $k > 0$, if for all $p \in *t$, $M(p) \geq k$ and there exists a place $p \in *t$ such that $M(p) = k$. In this case, $k$ is called the enabling degree of $t$ at marking $M$, denoted $\text{deg}(M, t)$.

Therefore, from a marking $M$, and for each transition $t$, there are exactly $\text{deg}(M, t)$ instances of transition $t$ which are enabled. A configuration of a time Petri net associates a clock with each instance of a transition that has been enabled.

This is called Threshold semantics in [5]. Time can elapse if no urgency is violated, and an occurrence of a transition is allowed to fire if it has been enabled for a duration that lays within the interval attached to $t$.

Formally, a configuration is a pair $C = (M, \text{enab})$, where $M$ is a marking, and $\text{enab}$ is a partial function $\text{enab}: T \rightarrow (\mathbb{R}_{\geq 0})^{|N|}$. We denote by $\text{enab}(t)_i$ the $i$th entry of $\text{enab}(t)$. For a marking $M$, $t \in T$, $\text{enab}(t)$ is defined iff there exists $k > 0$ such that $t$ is $k$-enabled at $M$. We further require that the length of vector $\text{enab}(t)$ is exactly $\text{deg}(M, t)$, and if $1 \leq i < j \leq \text{deg}(M, t)$, then $\text{enab}(t)_i \geq \text{enab}(t)_j$.

In a configuration $C = (M, \text{enab})$ each enabled transition $t$ is associated with a vector $\text{enab}(t)$ of decreasing real values, that record the time elapsed since each instance of $t$ was newly enabled. With this convention, the first enabled instance of a transition $t$ (that must have the maximal clock value) is the first entry $\text{enab}(t)_1$ of the vector. For a value $\delta \in \mathbb{R}$, we will denote by $\text{enab}(t) + \delta$ the function such that associates $\text{enab}(t)_i + \delta$ to the $i$th occurrence of $t$. The initial configuration of a TPN is $C_0 = (M_0, v_0(X_0))$, where $X_0$ is a set of vectors containing $\text{deg}(M_0, t)$ clocks per transition $t$. A timed move form a configuration $C = (M, \text{enab})$ consists in letting $\delta$ time units elapse, i.e. move to a new configuration $C' = (M, \text{enab} + \delta)$. Such move is allowed only if it does not violate urgency, i.e. $\text{enab}(t)_i + \delta \leq lft(t)$ for every instance $i$ of $t$.

A discrete move consists in firing an instance of a transition $t$ which clock lays in interval $I(t)$. When firing transitions, we will use the first enabled first fired (FEFF) policy, that is the instance of transition $t$ fired is the one with the highest value of time elapsed, i.e., $\text{enab}(t)_1$. Similarly, we disable transitions according to the first enabled first disabled (FEFD) policy. A standard way to address time in TPNs semantics is to start measuring time for a transition as soon as this transition is newly enabled. However, as highlighted in [16], there are several possible interpretations of new enabledness. A frequently used semantics is the intermediate semantics, which considers intermediate markings, i.e. when firing a transition $t$, we consider the marking $M''$ obtained after removing the tokens in $*t$ from $M$, and comparing the set of enabled transitions in $M''$ with those enabled after production of tokens in the places of $t^*$. Let transition $t$ be $k$-enabled at marking $M$ for $k > 0$, and $\text{enab}(t)_1 \in I(t)$. Then, an instance of $t$ can fire, and we obtain a new marking $M'$ via an intermediate marking $M''$ as follows:

$M''(p) = M(p) - 1$ if $p \in *t$ else $M''(p) = M(p)$.

Then we obtain marking $M'$ as:

$M'(p) = M''(p) + 1$ if $p \in *t$ else $M'(p) = M''(p)$.

Firing an instance of a transition $t$ changes the enabling degree several transitions (and not only of $t$). We will say that a transition is newly enabled by firing of $t$ from $M$ iff its enabling degree is larger in $M'$ than in $M''$. Then newly enabled transitions are attached an additional clock initially set to 0 in $\text{enab}$. For transitions which enabling degree decreases (i.e. that are in conflict with $t$), the first clock in $\text{enab}$ is discarded. We refer to the appendix for a more formal presentation of the semantics. We will write $C \xrightarrow{t} C'$ when there exists a move from $C$ to $C'$ allowed by net $N$.

A timed firing sequence of $N$ starting from configuration $q_1 = (M_1, \text{enab}_1)$ is a sequence of timed and discrete moves $\rho = q_1 \xrightarrow{\alpha_1} q_2 \xrightarrow{\alpha_2} \ldots \xrightarrow{\alpha_n} q_n$ where $\alpha_i$ is either a transition of $T$ or a value from $\mathbb{R}_{\geq 0}$. A configuration $C$ is reachable iff there exists a firing sequence from the initial configuration to $C$. Let $\text{Reach}(\mathcal{N}, C_0)$ denote the set of reachable configurations of a TPN $N$, starting from configuration $C_0$. For a configuration $C = (M, \text{enab})$ we denote by $\text{Untime}(C) = M$ the un timing of configuration $C$. Similarly, $\text{Untime}(\text{Reach}(\mathcal{N}))$ denotes the set of markings $M$ such that there exists a reachable configuration $(M, v)$ of $\mathcal{N}$. Note that Reach and Un time operations are not commutative and $\text{Reach}(\text{Untime}(\mathcal{N}))$ could be different from $\text{Untime}(\text{Reach}(\mathcal{N}))$ for a TPN $N$. A TPN $\mathcal{N}$ is bounded if $\text{Untime}(\text{Reach}(\mathcal{N}))$ is finite.

A timed word over $T$ is a word of $(T \times \mathbb{R}_{\geq 0})$. Let $\rho = q_1 \xrightarrow{\alpha_1} q_2 \xrightarrow{\alpha_2} \ldots \xrightarrow{\alpha_n} q_n$ be a firing sequence starting from $q_1$, and let $i_1, \ldots, i_k$ denote the indexes of discrete moves in $\rho$. The timed word associated with $\rho$ is the word $w = (t_1, d_1) \ldots (t_k, d_k)$, where each $t_j$ is transition $\alpha_i$, $d_1 = \sum_{j < i_1} \alpha_j$, and for every $m > 1$, $d_m = d_{m-1} + \sum_{i_{m-1} < j < i_m} \alpha_j$. A timed word $w$ is enabled at configuration $C$ if there exists a timed firing sequence $\rho$ starting from $C$,
and $w$ is the timed word associated with this sequence. The
untiming of a timed word $w = (t_1, d_1) \ldots (t_n, d_n)$ is the word
Untime($w$) = $t_1 \ldots t_n$.

For a TPN $\mathcal{N} = (\mathcal{U}, M_0, I)$, let $\text{Lang}(\mathcal{N})$ denote the set of
all timed words enabled at initial configuration $M_0$, and $ULang(\mathcal{N})$ be defined as
Untime($\text{Lang}(\mathcal{N})$), i.e., the set of words obtained by removing the timing component from
of $\text{Lang}(\mathcal{N})$. Observe that $ULang(\mathcal{N})$ can be different from $\text{Lang}(\text{Untime}(\mathcal{N}))$. In a similar way, we let $R(\mathcal{N}, C_0) = \text{Untime}(\text{Reach}([\mathcal{N}, C_0]))$ be the set of (untimed) reachable markings, i.e., $R(\mathcal{N}, C_0) = \{M | \exists (M, v) \text{ Reach}(\mathcal{N}, C_0)\}$.

A 0-delay timed firing sequence of $\mathcal{N}$ is a sequence from
$(Q \times T)^\infty$ such that $q_{i-1} \xrightarrow{a_i} q_i$, where $a_i$ is an transition for $T$ with $\text{eft}(a_i) = \text{lft}(a_i) = 0$. Hence transitions are enabled at each configuration and fired immediately without letting any other transition of the net fire.

III. PROCESSES OF UNTIMED AND TIMED NETS

We now define a partial-order semantics for timed nets with multi-enabledness using processes. These notions will be central to reason about TPNs and their properties. The notion of time causal process for TPNs have been introduced by [4], and later used by [7] to study a truly concurrent semantics for TPNs. First, we recall the definitions in the untimed setting.

Definition 3 (causal net): A causal net $ON = (B, E, G)$ is a finitary (each node has finite number of predecessors) acyclic net with $B$ as a set of conditions, $E$ as set of events, flow relation $G \subseteq B \times E \cup E \times B$, such that $E = \{e | (e, b) \in G\} \cup \{e | (b, e) \in G\}$, and for any condition $b$ of $B$ we have $\{e | (e, b) \in G\} \subset 1$ and $\{e | (b, e) \in G\} \subset 1$.

When causal nets are used to give a partial order semantics to Petri nets, events represent occurrences of transitions firings, and conditions occurrences of places getting filled with tokens.

The last condition in the definition states that a token in a place in produced by a single transition firing, and is consumed by a single transition. As conditions have a single successor, causal nets are conflict free. They are hence well suited to represent executions of nets. Let $\preceq = G^*$ and $\succeq = G^*$. We define $e \downarrow \ell$ as the downward closure $e \downarrow \ell = \{f \in E | f \preceq e\}$. A set $E' \subseteq E$ is downward closed iff $\downarrow E' = E'$.

We define $ON^* = \{b \in B | b^* = \emptyset\}$ and $\star ON = \{b \in\ B | b^* = \emptyset\}$; frontier$(ON) = \{e \in E | (e \star)^* = \emptyset\}$. Note that if we are looking at finite causal nets then $ON^*$ is always defined. For any downward-closed subset $E'$ of $E$ we define $\text{Cut}(E) = \{E' \cup \star ON\} \setminus E'$.

Definition 4 (causal process): Given a PN $\mathcal{U}$, a causal process of $\mathcal{U}$ is a pair $U = (ON, \pi)$ where, $\pi$ is mapping from $B \cup E \rightarrow P \cup T$, satisfying following conditions:

1) $\pi(B) \subseteq P$ and $\pi(E) \subseteq T$
2) $\pi \downarrow \ell_e$ is a bijection between sets $e^* \text{ and } \pi(e)^*$.
3) $\pi \downarrow \ell_e$ is a bijection between sets $e^* \text{ and } \star \pi(e)$.
4) For each $p$, $M_0(p) = \{b \in \star ON | \pi(b) = p\}$.

To relate transitions of a PN and events of a causal net, we will consider that events are of the form $e = (X, t)$, where $\pi(e) = t$ and $X = e^*$ i.e., event $e$ corresponds to firing of transition $t$ and $X$ is a set of conditions consumed when firing $t$. We will also let conditions be of the form $b = (e, p)$, where $e$ is the event that creates condition $b$, and $p = \pi(b)$ is the place that is represented by condition $b$. We will write $place(b)$ to denote such place in the original net. We let $posb(ON)$ denote the set of possible events which could be added to $ON$ and is defined as $posb(ON) = \{e = (X, t) | X \subseteq B \land \pi(X) = \bullet t \land \forall x \in X, x^* = \emptyset\}$. Following these definitions, one can inductively build processes to capture the semantics of (eventually unbounded) Petri nets.

Proposition 1: Let $\mathcal{U}$ be any untimed net. For any word $w \in \text{Lang}(\mathcal{U}, M_0)$, there exists a causal process $U$ of $\mathcal{U}$, such that $w \in \text{Lang}(U)$.


Definition 5 (time causal net): A time causal net is a tuple $ON = (B, E, G, \tau)$ where $(B, E, G)$ is a causal net, and $\tau : E \rightarrow \mathbb{R}_{\geq 0}$ is a timing function such that $e_{G^+} t_{\tau} e' \leq t_{\tau}(e')$.

For a time causal net $ON = (B, E, G, \tau)$, we define $\text{Untime}(ON)$ as the net $(B, E, G)$ i.e., $ON$ without its timing function. Now, given two untimed causal nets $ON = (B, E, G)$ and $ON' = (B', E', G')$, $ON'$ is said to be prefix of $ON$, denoted by $ON' \preceq ON$ if $B' \subseteq B, E' \subseteq G', G' = G \cap (B' \times E' \cup E' \times B')$, where $E'$ is finite and downward closed subset of $E$. If $ON$ and $ON'$ are timed causal nets, $E'$ is required to be timely sound, i.e., for all $e' \in E'$ we have $t_{\tau}(e') \leq t_{\tau}(e)$.

Definition 6 (time causal process): A time causal process a TPN $\mathcal{N}$ is a pair $N = (ON, \pi)$ where $ON$ is a timed causal net, and $\pi$ is mapping from $B \cup E \rightarrow P \cup T$, satisfying conditions 1-4 of a causal process, and:

5) For every event $e = (X, t)$, $\min_{e \subseteq X} t(\pi(e)) = t(\pi(e))$, i.e. the time elapsed between enabling of the occurrence of $t$ represented by $e$ and its firing belongs to $I(t)$.

6) if there exists $X \subseteq ON^*$ and a transition $t$ such that $\text{Place}(X) = \bullet t$ and $\pi(\tau)X < t_{\min}(t)$, then $\max(\pi(\tau)X) < \min(t_{\min}(t))$. This last condition means that if a transition was urgent before the date of the last event in $ON$, then it belongs to the time causal net, or was not appended due to a conflict.

For a time causal process $(ON, \pi)$ we define $\text{Untime}(ON, \pi)$ as $(\text{Untime}(ON), \pi)$. As for Petri Nets, for a timed causal net $ON = (B, E, G, \tau)$, we denote by $\text{posb}(ON)$ (and we define similarly) the set of events that can be appended to $ON$ (regardless of timing considerations).

Abusing our notation, for a condition $b = (e, p)$ we will define $\pi(b) = \tau(t)$.

As for Petri nets, we can show that time causal processes faithfully describe the semantics of Time Petri nets. Given a time causal process $N = (ON, \pi)$, where $ON = (B, E, G, \tau)$, a timed word of $N$ is a timed word $w = (e_1, d_1) \ldots (e_\ell, d_\ell)$ such that $e_1 \ldots e_\ell$ is a linearization of $\text{Untime}(ON)$, $d_i = \tau(e_i)$. Note that as $w$ is a timed word, this means in addition that for every $i < j$, we have $d_i < d_j$. We denote by $\text{Lang}(\mathcal{N})$
the set of timed words of time causal process \( N \). Note that there exist some words \( w \in \text{Lang}(\text{Untime}(N)) \) such that \( w \) is not the untiming of a word in \( \text{Lang}(N) \). We can now prove the following proposition:

**Proposition 2:** Let \( P \) be the set of time causal processes of a time Petri net \( N \). Then, \( \text{Lang}(N) = \bigcup_{N \in P} \text{Lang}(N) \)

**Example 1:** Consider the FC-TPN \((N, M_0)\) shown in Figure 6. Nets \( O_{N_1} \) and \( O_{N_2} \) in Figure 1 are causal nets of \( \text{Untime}(N, M_0) \). One can notice that \( O_{N_1} \leq O_{N_2} \).

![Fig. 1. Untimed causal nets \( O_{N_1} \) and \( O_{N_2} \)](image)

Figure 2 below illustrates timed causal nets. Nets \( O_{N_3} \) and \( O_{N_4} \) in Figure are timed causal nets of \((N, M_0)\). In this Figure, we have \( O_{N_3} \leq O_{N_4} \). Let us now compare \( O_{N_3} \) and \( O_{N_4} \) with (untimed) causal processes: we have \( O_{N_1} \leq \text{Untime}(O_{N_3}) \) and \( O_{N_2} \leq \text{Untime}(O_{N_4}) \).

![Fig. 2. Timed causal net \( O_{N_3} \) and \( O_{N_4} \)](image)

### IV. FREE CHOICE TIME PETRI NETS

Time Petri nets with urgent semantics [13] are very expressive. They can be used to model distributed timed systems with unbounded resources. Unsurprisingly, most problems, particularly those listed below are undecidable for this model:

- **Fireability:** Given a TPN \( N = (U, M_0, I) \) and a transition \( t \), is there a configuration \((M, \text{enab}) \in \text{Reach}(N, C_0)\) such that \( t \) is fireable at \((M, \text{enab})\)?
- **Termination:** Given a TPN \( N = (U, M_0, I) \), does it have a non-terminating run?
- **Coverability:** A TPN \( N = (U, M_0, I) \) and marking \( M \), is there a marking \( M' \in \text{Reach}(N, M_0) \) such that \( M' \geq M \)?
- **Reachability:** A TPN \( N = (U, M_0, I) \) and a marking \( M \), decide if \( M \in \text{Reach}(N, M_0) \).
- **Boundedness:** Given a PN \( N = (U, M_0, I) \) decide if \( \text{Reach}(N, M_0) \) is finite.

To obtain decidability, one often considers bounded TPNs, where the number of tokens in places cannot grow arbitrarily. In this case, TPNs can be translated into finite timed automata (see for instance [12]) and all properties decidable on timed automata become decidable. However, bounded TPNs cannot represent systems with unbounded resources. Furthermore, it is undecidable in general whether a TPN is bounded. One usually has to rely on a priori known bounds on place contents, or restrict to the class of nets such that \( \text{Untime}(N) \) is bounded.

In this paper, we consider a different structural restriction of TPNs, which is based on the untimed underlying PN, namely free-choice. This is a standard restriction in the untimed setting, that allows for efficient algorithms (see [9]). In this section, we show the interesting properties it engenders in TPNs and in the next section we will show how it affects their robustness under guard enlargement.

**Definition 7 (Free choice PN and Free choice TPN):** A Petri net \( U = (P, T, F) \) is called (extended) free choice, denoted FC-PN, if for any pair of transitions \( t \) and \( t' \) in \( T \): \( \{ t \} \cap \{ t' \} \neq \emptyset \iff t \neq t' \). A TPN \( N = (U, M_0, I) \) is called a free choice TPN (FC-TPN for short), if its underlying untimed net \( \text{Untime}(N) = U \) is free choice.

### A. Pruning a TPN while preserving reachability

As mentioned above, the firability and termination problems are undecidable for TPNs in general. In next section we show that they are decidable for FC-TPNs. As a first step, given an FC-TPN \( N \), whose underlying net is free choice, we construct another FC-TPN \( \text{Prune}(N) \) in which we remove transitions from a cluster if they can never be fired (due to the lower bound of their time constraint) and tighten timing constraints. Note that we do not delete all dead transitions from the net, but remove only transitions for which we can decide locally, by considering their clusters, that they will never fire. Let us illustrate this with an example.

**Example 2:** Consider the FC-TPN \( N \) in Figure 3. Consider transition \( b \), and its cluster \([\beta] \). One can notice from the definition of FC-TPNs that all transitions from the same cluster have a new instance created as soon as any transition from the same cluster has a new instance. Note also that in this example that it is clear that transition \( c \) will never be fired: in a configuration \((M, \text{enab})\), every instance of \( c \) is created at the same time as another instance of \( b \) and \( d \), and hence we have \( \text{enab}(c) = \text{enab}(b) = \text{enab}(d) \). Let \( \text{enab}(c) = \text{enab}(b) = r_1 \ldots r_k \). Transition \( b \) has to fire or be disabled at \( lft(b) - r_1, lft(b) - r_2, \ldots \). If \( b \) fires or is disabled, then the oldest instance of \( c \) is also disabled. As we have \( lft(c) > lft(b) \) every \( i \)th instance of \( b \) will fire or be disabled before the \( i \)th instance of \( c \). Hence one can safely remove transition \( c \) without changing the semantics of the net.

Similarly, in the cluster \([\epsilon] \), we cannot say for sure that some transition will be never fired, but only that the maximum amount of time any transition can elapse is 2 time units. Note that, in fact, neither transition \( f \) nor \( e \) is fireable in this net, but we cannot decide it just by looking at the clusters. Indeed in order to decide if \( e \) and \( f \) are fireable, we have to study the behaviour of the net. Hence our pruning operation does not modify this. Thus, after removing transition \( c \) from its cluster and modifying flow relation appropriately, and changing the upper bounds of remaining transitions, we obtain the free choice net in Figure 4. One can see that \( \text{Reach}(N, M_0) = \text{Reach}(\text{Prune}(N), M_0) \). Therefore, we also get that \( \text{Lang}(N, M_0) = \text{Lang}(\text{Prune}(N), M_0) \).

Formally, we can define pruning as follows:
Definition 8 (pruned cluster and pruned net): Given an FC-TPN $\mathcal{N} = (\mathcal{U} = (P, T, F), M_0, I)$, we define pruned cluster of a transition $t$ as $\text{Prune}(t) = \{t' \in \mathcal{T} | eft(t') \leq \text{min}_{t' \in \mathcal{T}}(eft(t'))\}$. The pruning of a FC-TPN $\mathcal{N}$ is the pruned net $\text{Prune}(\mathcal{N}) = (\mathcal{U}' = (P, T', F'), M_0, I')$, where:

- $T' = T \setminus \cup_{t \in T} \text{Prune}(t)$;
- $F' = F \setminus T' \subseteq (P \times T') \cup (T' \times P)$;
- For each transition $t$ in $T'$, we define $I'(t) = (eft(t), \text{min}_{t' \in T}(eft(t')))$. 

Lemma 1 below shows that pruning away unfirable transitions from clusters of a FC-TPN, does not modify its semantics. More precisely, the LTS obtained for a pruned FC-TPN is isomorphic to the LTS for the original net. This is not surprising and has already been considered in [8], where pruning is called ‘normalization’ and is used to reason about free-choice (but not to remove transitions nor places).

Lemma 1 (Pruning Lemma): Given an FC-TPN $\mathcal{N}$, the net $\text{Prune}(\mathcal{N})$ is such that $(C_N, \rightarrow_N)$ is isomorphic to $(C_{\text{Prune}(\mathcal{N})}, \rightarrow_{\text{Prune}(\mathcal{N})})$.

Proof (Sketch) Let $\mathcal{N}$ be a FC-TPN, and let $\mathcal{N}' = \text{Prune}(\mathcal{N})$. We will design a relation $R$ from configurations of $\mathcal{N}$ to configurations of $\mathcal{N}'$, and show that this relation is an isomorphism. This relation simply erases clock values attached to pruned transitions. Showing that $R$ is an isomorphism is performed by induction on the length of runs, and showing that discrete and timed moves preserve isomorphism. A more detailed proof can be found in the appendix. □

An immediate consequence of Lemma 1 is that $\text{Lang}(\mathcal{N}) = \text{Lang}(\text{Prune}(\mathcal{N}))$. Note that this lemma holds only under the free-choice assumption. Indeed, in a standard TPN, one can disable the most urgent transition from a cluster without disabling other instances of transitions in this cluster. In the example of Figure 5, for instance, transition $t_2$ and $t_3$ belong to the same cluster, and pruning would remove $t_3$. However, in the unpruned net, transition $t_2$ can be disabled by firing of $t_1$, which allows $t_3$ to fire later. Hence, for this non-FC-TPN, $\text{Lang}(\mathcal{N}) \neq \text{Lang}(\text{Prune}(\mathcal{N}))$.

B. Simulating runs in the timed and untimed FC-TPN

In this section, we prove our main theorem, which relates time causal processes of pruned FC-TPNs with untimed causal processes of their untimed nets. In the next section, we will use this theorem to show decidability.

Theorem 1 (Inclusion of untimed prefixes): Let $\mathcal{N} = (\mathcal{U}, M_0, I)$ be a pruned FC-TPN (without 0-delay time firing sequences) and let $\mathcal{U}' = \text{Untime}(\mathcal{N})$. Let $\mathcal{U}''$ be an (untimed) causal process of $\mathcal{U}'$. Then there exists a time causal process $\mathcal{N}'$ such that $\mathcal{U}'' \subseteq \text{Untime}(\mathcal{N})$.

Proof: We are given $\mathcal{U}'$ a causal process of $\mathcal{U}'$. We will iteratively construct a pair $\rho_i, \sigma_i$, where $\rho_i$ is a causal process of $\mathcal{U}'$, $\sigma_i$ a time causal process of $\mathcal{N}$, and such that $\rho_i$ is a prefix of $\text{Untime}(\sigma_i)$. The construction ends at some $n \in N$ such that $\rho_n = \mathcal{U}'$. At that stage of the algorithm, $\sigma_n$ is a time causal process such that $\mathcal{U}'' \subseteq \text{Untime}(\sigma_n)$ which is the desired result. For this, we maintain the following invariants at every intermediate step, i.e., for all $0 \leq i \leq n$:

1. $\rho_i$ is a prefix of $\mathcal{U}''$ and
2. $\rho_i$ is a prefix of $\text{Untime}(\sigma_i)$
3. either $|\rho_i| + 1 = |\rho_{i+1}|$ or $|\sigma_i| + 1 = |\sigma_{i+1}|$
4. $e \in \text{posb}(\rho_i)$ and $e \notin \sigma_i$ implies that $e \in \text{posb}(\sigma_i)$
5. $e_{G_i}^x \Rightarrow e' \Rightarrow (e') \leq (e')^x\text{, (with } G_i\text{ the flow relation of } \sigma_i)\text{.}$

The first two conditions have been explained above. Condition (I3) ensures that the algorithm progresses at every iteration, either in $\rho_i$ or $\sigma_i$. Condition (I4) says that if an event $e$ is enabled in the untimed causal process $\rho_i$ and has not yet been fired in $\sigma_i$, then it must be enabled at $\sigma_i$. Note that due to urgency, $e$ may still be not firable in $\sigma_i$. Finally, Condition (I5) ensures that the time stamps that we add in $\sigma_i$ are consistent with its causal order.

We start by defining, for a time causal process $\mathcal{O}N$, the maximal firing date for an event $e = (X, t) \in \text{posb}(\mathcal{O}N)$ as $\text{mfd}(\mathcal{O}N, e) = \max_{x \in X}(\tau(x)) + eft(t)$. This represents the maximal date that can be attached to event $e = (X, t)$ when it is appended to $\mathcal{O}N$. Further, we use $\text{td}(\mathcal{O}N, e)$ to denote the difference between $\text{mfd}(\mathcal{O}N, e)$ and the maximal date attached to an event in $\mathcal{O}N$. Note that this value can be negative if the maximal date in $\mathcal{O}N$ is above $\text{mfd}(\mathcal{O}N, e)$, i.e., $e$ has already been fired in $\mathcal{O}N$. This represents the time that has to elapse before (or has elapsed after) event $e$ corresponding to firing of a transition $t$ becomes urgent.
Finally, for a (time) process $ON$ and an event $e$, we use $ON \cup \{e\}$ to denote the (time) process obtained by appending event $e$ to $ON$, when it is possible to do so. Now we start from an untimed causal process and describe a time-stamping algorithm to obtain a timed causal process in Algorithm 1.

**Algorithm 1**: Causal-net-to-time-causal-net

- **Input**: $N = (U, M_0, I)$ a pruned FC-TPN without 0-delay firing sequences, $U' = (B', E', G')$ a (untimed) causal process of $U' = 	ext{Untime}(N)$
- **Output**: $N$ a timed causal process of $N$ such that $U' \leq 	ext{Untime}(N)$

1. **Initialization**: // $\rho_i$ (resp. $\sigma_i$) is a untimed (resp. time) causal process
   - $\text{CLK} := 0, \rho_0 := (B_0, \emptyset, \emptyset), \sigma_0 := (B_0, \emptyset, \emptyset)$
   - **while** $\rho_i \neq U'$ **do**
     - Choose an event $e = (X_e, t_e)$ from $\text{posb}(\rho_i) \cap U'$;
     - **if** $e \in \sigma_i$ **then**
       - $\rho_{i+1} \leftarrow \rho_i \cup \{e\}; \quad \sigma_{i+1} \leftarrow \sigma_i$
     - **else**
       - $\min = \min_{e' \in \text{posb}(\sigma_i)} \text{mfd}(\sigma_i, e')$
       - $S_i = \{e' \in \text{posb}(\sigma_i) | \text{mfd}(\sigma_i, e') = \min \}$
       - **if** $S' = S_i \cap E' \neq \emptyset$ **then**
         - Pick an event $e_t = (X, t)$ from $S'$;
       - **else**
         - **if** $S_i = \emptyset$ **then**
           - $\text{CLK}' = \text{CLK} + \max\{0, \text{td}(\sigma_i, e)\}$;
           - $\tau(e) = \text{CLK}'$;
           - $\sigma_{i+1} \leftarrow \sigma_i \cup \{e\}; \quad \rho_{i+1} \leftarrow \rho_i$; \texttt{GOTO Step-23};
         - **else**
           - Pick an event $e_t = (X, t)$ from $S_i$;
           - $\text{CLK}' = \text{CLK} + \text{left}(t) - \text{td}(\sigma_i, e_t)$;
           - $\tau(e_t) = \text{CLK}'$ // adding time stamp
           - $\sigma_{i+1} \leftarrow \sigma_i \cup \{e_t\}; \quad \rho_{i+1} \leftarrow \rho_i$;
           - $i \leftarrow i + 1$

Let us now explain the algorithm. At initialization, $B_0$ is the set of conditions corresponding to marked places in $M_0$, and $CLK$, a real valued variable which stores the time elapsed till now, is set to 0. $\rho_i$ and $\sigma_i$ are respectively, untimed and time causal processes at $i$-th iteration. $S_i$ is the set of events that are the most urgent instances of transitions in $\sigma_i$.

The idea is that, at each iteration, we pick (in line 4) an event $e$ enabled in the current $\rho_i$, which would grow $\rho_i$ to eventually reach the untimed causal process $U'$. If this event has already been fired in $\sigma_i$, then we just add it to $\rho_i$ and go to the next iteration.

Else, we try to fire it in $\sigma_i$. However, to do so, we first compute $S_i$ the set of all urgent transitions in $\sigma_i$ (line 8–9). If there is an urgent transition instance $e_t$ whose corresponding event is also in $U'$, then we pick it (in line 11) and fire it, i.e., add it to $\sigma_i$ and update time information correctly (line 20–23). This makes sure $\sigma_i$ has grown at this iteration so we go to the next iteration. On the other hand, if there is no urgent transition in $S_i$ which is also in $U'$, we check if there is no urgent transition at all, i.e., $S_i$ is empty. In this case, we elapse time till $e$ can fire and fire it as soon as possible (line 14), updating clocks appropriately.

Finally, if there is some urgent transition in $S_i$ but this is not in $U'$, then we fire it as late as possible (line 20–23). The fact that this does not change the enabling of $e$ (due to conflicts) is proved by our invariant I4.

If invariants I1, I2, I3, I4 and I5 are satisfied for all iterations then Algorithm 1 is correct. Due to lack of space we only sketch some arguments here. A formal proof of the preservation of all invariants is provided in appendix (Lemma 3).

First, it is easy to see that invariants I1, I2 are preserved. They hold at the beginning and if we assume that they hold at the end of $i$-th iteration of while loop, then in the $(i+1)$-th iteration, we have: if we exit the iteration in step 22 then it means that $\rho_{i+1} = \rho_i$ and $\sigma_{i+1} = \sigma_i \cup \{e\}$ and by induction hypothesis, we have $\rho_i \leq U'$, and $\rho_i \leq \sigma_i$. Hence $\rho_{i+1} \leq U'$ and $\rho_i \leq \sigma_{i+1}$. Otherwise we have exited the iteration in step 6 and it means that $\sigma_{i+1} = \sigma_i$ and $\rho_{i+1} = \rho_i \cup \{e\}$. So we have $e \in \text{posb}(\rho_i)$ and $e \in U' \setminus \rho_i$ and $\sigma_i = \sigma_{i-1} \cup \{e\}$. Hence $\rho_{i+1} \leq U'$ and $\rho_i \cup \{e\} \leq \sigma_i \leq \sigma_{i+1}$. Similarly, assuming I4 holds at the previous iteration, it is easy to see that I3 will hold at each iteration as either $\rho_i$ or $\sigma_i$ grows. And we can also check that our time-stamps are indeed consistent with the causality imposed by the flow relation. We leave proof of I4 to the appendix.

The last thing left is to prove that the Algorithm 1 terminates for any input.

**Lemma 2**: Algorithm 1 terminates in finitely many steps.

**Proof**: (sketch) A complete proof is given in appendix. It shows that $\sigma$ cannot grow unboundedly. Each step of the algorithm adds either an event to $\rho_i$, or to $\sigma_i$. While the number of steps that add events to $\rho_i$ is finite, the algorithm may still not terminate if $\sigma$ can grow unboundedly, i.e., the while loop is exited at line 22 unboundedly without progress in $\rho$. Now, the crux of the proof is that at every step, a set of events from $U'$ are listed as possible events. At every step, since we do not have 0-delay firing sequences, time has to progress, so these events can not remain ignored forever.$\blacksquare$

The correctness proof and termination lemma allow to conclude the proof of Theorem 1.$\square$

We can now extend Theorem 1 from causal nets to words. Let $U = (P, T, F)$ be an untimed Petri net. Given a causal process $U = (ON = (B, E, G), \pi)$ of $U$, consider the partial order $\preceq = G^*$. We denote by $\text{lin}(U)$, the set of words over alphabet of transitions obtained by considering linearizations of the partial order of $G^*$ and projecting onto the labeling alphabet (of transitions $T$), i.e., $\text{lin}(N) = \{\rho \in T^* | \exists \rho' \text{ a linearization of } G^* \text{ such that } \pi|_E(\rho') = \rho\}$.

Now, recall that given an untimed net $U$, its language $\text{Lang}(U, M_0)$ is a set of firing sequences, i.e., words over the
Corollary 1 (Words version): Let $\mathcal{N}$ be a pruned FC-TPN (without 0-delay time firing sequences) and let $\mathcal{U}' = \text{Untime}(\mathcal{N})$. Then, for each $w \in \text{Lang}(\mathcal{U}',M_0)$ there exists a time causal process $N$ of $\mathcal{N}$ such that $w \leq w'$.

Proof: Given a word $w \in \text{Lang}(\mathcal{U}',M_0)$, using Proposition 1, we get an untimed causal process $U'$ of net $\mathcal{U}'$, such that $w \in \text{lin}(U')$. By Theorem 1, we get a timed causal process $N$ of net $\mathcal{N}$ such that $U' \leq \text{Untime}(N)$. Now since $w \in \text{lin}(U')$, and $U' \leq \text{Untime}(N)$, we can extend $w$ to $w'$ in $\text{lin}(\text{Untime}(N))$. $\square$

V. DECIDABILITY RESULTS FOR FC-TPNS

In this section, we will show some consequences of the above characterization.

Theorem 2 (Firability): Given an FC-TPN $\mathcal{N} = (\mathcal{U}, M_0, I)$ (without 0-delay time firing sequences), and a particular transition $t \in T$, checking firability of transition $t$ in $\mathcal{N}$ is decidable.

Proof: Given a FC-TPN $\mathcal{N}$, one can compute an equivalent pruned version $\mathcal{N}_{\text{Pruned}}$, i.e. a Petri nets with the same timed language and the same set of processes, but which clusters have only firable transitions. One can compute a Petri net $\mathcal{U}' = \text{Untime}(\mathcal{N}_{\text{Pruned}})$. For every PN, it is well known that coverability of a marking is decidable [15]. A particular transition $t$ is firable in a Petri net $\mathcal{U}$ iff its preset $\bullet t$ is coverable. Coverability can be obtained by construction of a coverability tree, or using backward algorithms (see for instance [16] for recent algorithms). In both cases, one can exhibit a sequence of transitions witnessing coverability of a particular marking. If $w = t_0, \ldots, t_k$ is such a sequence witnessing coverability of $\bullet t$ from $M_0$ in $\text{Untime}(\mathcal{N}_{\text{Pruned}})$, then one can immediately infer that $w.t \in \text{Lang}(\mathcal{U}')$, and hence $t$ is firable in $\mathcal{U}'$. Using Corollary 1, there exists a timed word $v = (t_0, d_0) \ldots (t_k, d_k), (t, d_k + 1) \in \text{Lang}(\mathcal{N}_{\text{Pruned}})$, and hence $v \in \text{Lang}(\mathcal{N})$. Conversely, assume that $t$ is not firable in $\text{Untime}(\mathcal{N})$ and that it is firable in $\mathcal{N}$. Then there exists a run $\rho$ of $\mathcal{N}$ firing $t$. Then, $\text{Untime}(\rho)$ is a run of $\text{Untime}(\mathcal{N})$ which fires $t$ (contradiction). $\square$

Theorem 3 (Termination): Given an FC-TPN $\mathcal{N}$ (without 0-delay time firing sequences), it is decidable if $\mathcal{N}$ terminates.

Proof: Let $\mathcal{N}$ be a FC-TPN and let $\mathcal{N}_p$ be its pruned version. Since the reachability graphs of $\mathcal{N}$ and $\mathcal{N}_p$ are isomorphic by pruning Lemma 1, it is sufficient to decide if $\mathcal{N}_p$ has only terminating runs. Let $\mathcal{N}' = \text{Untime}(\mathcal{N}_p)$. If $\mathcal{N}'$ does not terminate, then it allows sequences of transitions that are unboundedly long. As we know from Corollary 1 that for every word $w'$ of $\text{Lang}(\mathcal{N}')$, there exists a timed word $w$ of $\text{Lang}(\mathcal{N}_p)$ of length $|w| \geq |w'|$, then $\mathcal{N}_p$ (and hence $\mathcal{N}$) allows sequences of transitions of unbounded lengths, i.e., it does not terminate either. In the other direction, if $\mathcal{N}_p$ has an infinite run, as time constraints in free choice TPNs can only prevent occurrence of a transition, then the untimed net clearly has an infinite run too. Thus, we have reduced the problem to termination of an untimed Petri net, which is decidable by the classical coverability tree construction. $\square$

VI. ROBUSTNESS OF FC-TPNS TO GUARD ENLARGEMENT

As mentioned in the introduction, robustness problems address the question of preservation of properties of systems that are subject to imprecision of time measurement. In this section, we show decidability of robustness of firability for the class of FC-TPNs. Note that this class contains unbounded nets. To the best of our knowledge, this is the first decidability result of robustness for an unbounded class of TPNs allowing urgency. The main idea to obtain this result is to use the reduction of firability checking in FC-TPNs to the problem of firability in the untimed underlying net shown in section V.

Let us now formally define the notion of robustness and the problems considered in this paper. Let $\text{int} = [a, b]$ be a time interval. The enlargement of $\text{int}$ by $\Delta$ is the interval $\text{int}_\Delta = [\max(0, a - \Delta), b + \Delta]$. Let $\mathcal{N} = (\mathcal{U}, M_0, I)$ be a FC-TPN. The enlargement of $\mathcal{N}$ by a real value $\Delta$ is the net $\mathcal{N}_\Delta = (\mathcal{U}, M_0, I_\Delta)$, obtained from $(\mathcal{U}, M_0, I)$ by replacing every interval $I(t)$ by its enlarged version $I(t)_\Delta$. Robustness for an chosen enlargement $\Delta$ consists in deciding whether, properties of a net (reachability, boundedness, coverability) or its (untimed) language are preserved in $\mathcal{N}_\Delta$. A more general robustness question consists in deciding whether there exists a value for $\Delta$ such that $\mathcal{N}_\Delta$ preserves reachability, coverability, or the (untimed) language of $\mathcal{N}$. A positive answer to this question means that slightly changing guards preserves the considered property, i.e. that this property of the system is robust to a small time imprecision.

In general, robustness problems are undecidable for TPNs, as shown in [3], and become decidable when the considered nets are bounded. An interesting question is whether robustness of some of the above mentioned problems is decidable for TPNs with multiple enabling outside bounded classes of nets. Answering this question would provide useful tools to check properties of systems made of bounded timed processes communicating through bag channels.

Let us now consider robustness of firability: let $\text{Firable}(\mathcal{N})$ denote the set of transitions which are firable in $\mathcal{N}$. We will say
that a net $\mathcal{N}$ is robust w.r.t firability of transition iff there exists a real value $\Delta > 0$ such that $Firable(\mathcal{N}) = Firable(\mathcal{N}_\Delta)$.

Intuitively, this property says that in an imperfect time measurement setting, there exists some precision of clocks that allows to preserve firability of transitions of $\mathcal{N}$ during an implementation. It is easy to observe (see Appendix for details) that all FC-TPNs are not robust.

**Proposition 3**: The class of FC-TPNs is not robust wrt firability of transitions.

As firability of every transition in a FC-TPN is decidable, for a fixed enlargement $\Delta$, one can decide whether the firability set of $\mathcal{N}$ differs from that of $\mathcal{N}_\Delta$. So the next question is to decide whether there exists a $\Delta > 0$ such that net $\mathcal{N}$ is robust with respect to firability.

**Definition 9 (Firability robustness problem)**: Given a TPN $\mathcal{N}$, does there exist a $\Delta$ in $\mathbb{Q}_{>0}$ such that $Firable(\mathcal{N}) = Firable(\mathcal{N}_\Delta)$?

**Theorem 4**: Let $\mathcal{N}$ be a FC-TPN without 0-delay sequence. Then robustness of firability is decidable. If $\mathcal{N}$ has robust firability, then one can effectively compute a value $\Delta$ such that $Firable(\mathcal{N}) = Firable(\mathcal{N}_\Delta)$.

**Proof**: We first observe that in a pruned FC-TPN $\mathcal{N}$, a transition $t$ is firable if all transitions in $t$’s cluster are firable. Next, all timed words of $\mathcal{N}$ are also timed words of $\mathcal{N}_\Delta$. So, enlarging a net can only result in new behaviors. As a consequence, if a transition $t$ is firable in $\mathcal{N}$, it is necessarily firable in $\mathcal{N}_\Delta$. Further, note that as they have the same underlying untimed net, $\mathcal{N}$ and $\mathcal{N}_\Delta$ are both free-choice and they have the same clusters. Now the pruning operation applied to each of these nets results in removing transitions (it can never add transitions) and pruning lemma holds for both of them. If after the pruning, we still have the same clusters, then the set of firable transitions remains the same. The only way to have an extra transition that can fire in $Prune(\mathcal{N}_\Delta)$ is if this transition $t$ in cluster $C$ has been removed in $Prune(\mathcal{N})$ but remains in $Prune(\mathcal{N}_\Delta)$ due to enlargement. By our pruning construction this means that there must exist another firable transition in this cluster in $Prune(\mathcal{N})$ (else we would not remove $t$). That is,

**Claim**: For any $\Delta > 0$, $Firable(\mathcal{N}) \neq Firable(\mathcal{N}_\Delta)$ iff there exists a cluster $C_\Delta$ of $Prune(\mathcal{N}_\Delta)$ such that $C \subseteq C_\Delta$ for some cluster $C$ of $Prune(\mathcal{N})$, and at least one transition $t$ of $C$ is firable.

Thus, it suffices to look at each cluster of $Prune(\mathcal{N})$ and compute the smallest possible enlargement that does not give new behaviors. More formally, two intervals $I_1, I_2$ are neighbors if the smallest closed intervals containing them have a non-empty intersection. Given two intervals $I_1$ with end-points $a \leq b$ and $I_2$ with end-points $c \leq d$ that are not neighbors and such that $b < c$, then one can easily compute a value $\Delta_{I_1,I_2} = (c - b)/2$. One can for instance choose $\Delta_{t_1,t_2} = (c - b)/2$. For a cluster $C$ of $\mathcal{N}$ with transitions $t_1 \ldots t_k$ such that $t_1 \ldots t_i$ are not pruned, and $t_{i+1} \ldots t_k$ are pruned, we have $eft(t_j) > \min\{eft(t_q), q \in 1..i\}$ for every $j \in i + 1..k$. Similarly we can compute $\Delta_C = \min\{eft(t_j) - \min\{eft(t_q), q \in 1..i\}\}$. Then, enlarging $\mathcal{N}$ by $\Delta_C$ does not change the set of transitions preserved by pruning. Now, if any transition of $t_{i+1} \ldots t_k$ is a neighbor of $[0, \min\{eft(t_q), q \in 1..i\}]$, such a $\Delta_C$ does not exist.

Consequently to check robustness of firability, it suffices to check existence of a value $\Delta_C$ for each cluster $C$ of $\mathcal{N}$ that has a firable transition. If one such cluster does not allow computing a strictly positive enlargement, then the net is not robust. Otherwise, it suffices to choose as $\Delta$ the smallest value allowing enlargement encountered for a cluster of $\mathcal{N}$. Clearly, enlarging $\mathcal{N}$ by $\Delta$ does not change the firability set of $\mathcal{N}$. □

From the above proof we can characterize a class of unbounded FC-TPNs for which robustness of firability set is guaranteed by definition.

**Corollary 2**: Let $\mathcal{N}$ be a FC-TPN such that $Untime(Prune(\mathcal{N})) = Untime(\mathcal{N})$. Then the firability set of $\mathcal{N}$ is robust w.r.t guard enlargement.

VII. DISCUSSION

Our proof technique used to obtain decidability of firability and termination holds for free-choice Time Petri nets with a multiple server semantics, when we disallow 0-delay infinite runs. We now show that all these conditions are necessary for our proofs to hold.

Let us first address the free choice assumption. Without which the problems considered are undecidable. Indeed, the two counter machine encoding of [11] relies on urgency and uses non-free choice nets, in which transitions have at least one place with a single token. Hence, this encoding works even under a multiple server semantics. In particular, Theorem 1 does not hold without the free choice assumption. Consider the non-free choice net $\mathcal{N}_{nfc}$ in Figure 7 (left). A causal process for $Untime(\mathcal{N}_{nfc})$ is shown in Figure 7 (right, above). One can verify in this untimed net that transition $c$ is firable. However, there is no way to build a timed causal net that contains this causal net. Indeed, transition $c$ is not firable in $\mathcal{N}_{nfc}$ and one cannot add event $e_3$ in the only timed causal net defined by $\mathcal{N}_{nfc}$ depicted in Figure 7 (right, below). Note also that marking $\{p_1, p_3\}$ is reachable in $Untime(\mathcal{N}_{nfc})$ (and allows firing of $c$), but not in $\mathcal{N}_{nfc}$.

![Fig. 7. A non-free choice TPN $\mathcal{N}_{nfc}$ (left), and a causal process (right, up) and a timed causal process (right, below) for it.](image-url)
a cluster keep their clocks unchanged. Such a semantics is meaningful and arguably powerful enough, for instance, to address business processes with time that do not contain fork-join constructs, i.e. where case processing are sequences of choices up to completion. Unsurprisingly, with a single server semantics, where we keep only one clock per transition instead of one for every instance of a multi-enabled transition, even our Pruning Lemma 1 fails. This follows as we cannot remove useless transitions easily, as multi-enabling in a single-server may make the transitions urgent at a later date.

Finally, the 0-delay assumption forbids an arbitrary number of transitions to occur at the same time instant. If this condition is not met, then our algorithm used to build a timed process of \( N \) from an untimed process of \( \text{Untime}(\text{Prune}(N_P)) \) does not necessarily terminate (Lemma 2). Furthermore, eagerness of urgent transitions firing in zero time can prevent other transitions from firing, which may result in discrepancies between untiming of timed processes of a net and untimed processes of the untiming of this net. Consider the pruned and free choice net \( N_2 \) depicted in the Figure below. The only allowed executions of \( N_2 \) are \( \text{Lang}(N_2) = \{ (a, 0)^k | k \in \mathbb{N} \} \). Hence, \( N_2 \) has a 0-delay firing sequence \( a^\omega \), and transition \( b \) is not firable. However, \( \text{Untime}(N_2) \) allows sequences of the form \( a^k . b \), and hence transition \( b \) is firable. Note that this does not mean that there is no effective procedure to build a timed causal net from an untimed causal net, and our algorithm could be adapted to handle Zeno behaviors.

![Fig. 8. A Free choice TPN \( N_2 \) with Zeno behavior](image)

**Open issues:** While we have shown decidability of firability, termination, and robustness of firability for FC-TPNs with no 0-delay runs, closely-related problems such as coverability and boundedness are still left open. Indeed, it turns out that our proof above does not apply directly for these problems.

Consider the FC-TPN \( N_{cov} \), shown in Figure 9. Clearly, when removing time constraints from \( N_{cov} \), the obtained (untimed) Petri net allows sequence of transitions \( a . b \), which leaves the net in a marking \( M \) such that \( M(p_1) = M(p_3) = 1 \) and \( M(p_2) = 0 \). However, the timed language of \( N \) contains only \( w = (a, 1)(a, 2)(b, 8) \) and its prefixes. So, marking \( M \) is not reachable or even coverable by \( N \). Thus, unlike for firability and termination, one cannot immediately decide coverability (or reachability) of a marking in an FC-TPN just by looking at its untimed version. This does not contradict Corollary 1: once untimed, the causal process for \( w \) does indeed contain the causal process associated with \( a . b \).

Next, the question of boundedness also does not immediately follow on the same lines as the proofs of theorems 2 and 3. Consider, for instance, the net \( N_{bd} \) of figure 10. The untimed version of this net allows sequences of transitions of the form \( (t_1 . t_2)^k \), for arbitrary value \( k \in \mathbb{N} \). At each iteration of this sequence, place \( p_3 \) receives a new token. This net is free choice, and following the result of theorem 1, for every untimed process \( N_k \) associated with a sequence \( (t_1 . t_2)^k \), there exists a timed process \( N_{k,b} \) which is filled, the only sequences of moves allowed by \( N_{k,b} \) are of the form \( (t_1 . t_2 . t_3)^k \), and hence \( N_{bd} \) is bounded, even if \( \text{Untime}(N_{bd}) \) is unbounded.

Despite these remarks, we conjecture that we can indeed modify the techniques in this paper to get decidability for coverability and boundedness problems for FC-TPNs. It is unclear whether reachability for FC-TPNs would similarly be decidable. Finally, several questions for robustness are still open, and we hope the result in this paper serves as a proof-of-concept for future work.

**REFERENCES**


APPENDIX

FORMAL DEFINITION OF SEMANTICS WITH MULTI-ENABLEDNESS

The set of conflicting transitions and the set of newly enabled transitions are computed as follows:

Let $t$ and $t'$ be two transitions enabled in $M$ and let $k = deg(M, t)$ and $k' = deg(M', t')$ be their enabling degrees at marking $M$. Transition $t$ is in conflict with transition $t'$ in $M$ iff in the intermediate marking $M''$ computed when firing $t$, the enabling degree of $t'$ is decreased w.r.t. $M$, i.e. if firing $t$ consumes one token from at least a place $p$ with marking $M(p) = deg(M, t')$ in the preset of $t'$. So if the enabling degree of $t'$ at $M$ is $k'$ and its enabling degree at $M'' = M - t$ is $k' - 1$ then one enabled instances of $t'$ is disabled when moving from $M$ to $M''$ i.e. when firing $t$. We disable transitions according to the first enabled first disabled (FEED) policy: disabling the oldest instance of a transition simply consists in removing $\text{enab}(t)_1$ from $\text{enab}$. We will denote by $\text{cnfl}(M, t)$ the set of enabled transitions that are in conflict with $t$ at marking $M$.

Let $\text{newenab}(M, t)$ denote the set of newly enabled instances in the marking reached from $M$ after firing oldest instance of transition $t$. If a transition $t'$ has $k'$ enabled instances at $M''$ and $k' + 1$ enabled instances $M'$ as defined in the above paragraph, then firing $t$ create one new enabled instance of $t'$. Note that as we consider intermediate markings, firing $t$ can disable the oldest instance of some transition $t'$, and at the same time create a new enabled instance of $t'$.

Let $C = (M, \text{enab})$ and $C' = (M', \text{enab}')$ be configurations. A move from $C$ to $C'$ can be either a timed move (that simply lets time elapse), or a discrete move, that represents a transition firing. A transition $t$ is urgent in a configuration $C = (M, \text{enab})$ iff $\text{enab}(t)_1 = \text{lft}(t)$. An initial configuration in a configuration $C_0 = (M_0, \text{enab}_0)$ such that for every $t \in T$ we have $\text{enab}(t) = O_{deg(M, t)}$.

A timed move of $\delta$ time units from a configuration $(M, \text{enab})$ to a transition $(M', \text{enab}')$ is denoted by $(M, \text{enab}) \xrightarrow{\delta} (M', \text{enab}')$, and is allowed iff

- $M' = M$,
- for every $t \in \text{dom}(\text{enab})$, $\text{enab}(t)_1 + \delta \leq \text{lft}(t)$

Note that urgency disallows time elapsing: as soon as a transition is urgent, i.e. $\text{enab}(t)_1 = \text{lft}(t)$, one can not increase its clock value, and has to fire $t$ or a conflicting transition that discards its first enabled instance before elapsing time.

A discrete move (firing an instance of transition $t$ from a configuration $(M, \text{enab})$ to a transition $(M', \text{enab}')$) is denoted by $(M, \text{enab}) \xrightarrow{t} (M', \text{enab}')$, and is allowed iff

- $t \in \text{dom}(\text{enab})$, and $\text{enab}(t)_1 \in \text{lft}(t)$
- for every $p \in P$, $M'(p) = M(p) - t\cdot(p) + t\cdot(p)$,
- $\text{enab}'$ is computed as follows. Let $\text{enab}(t) = (v_1, \ldots, v_k)$, and let $\text{enab}(t') = (v'_1, \ldots, v'_k)$ for every $t' \in \text{dom}(\text{enab}(M'))$.

We first define $\text{enab}''$ as $\text{enab}''(t) = (v_2, \ldots, v_k)$ or is undefined if $\text{deg}(M, t) = 1$. Then for every $t' \in T \setminus \{t\}$,

- $\text{enab}''(t') = (v_2, \ldots, v_k)$ if $t' \in \text{dom}(\text{enab}) \cap \text{cnfl}(M, t)$,
- $\text{enab}''(t') = \text{enab}(t')$ otherwise.

Then, for every $t_i \in T$, we have:

- $\text{enab}(t_i) = \text{enab}''(t_i), 0$ if $\text{deg}(M', t) = \text{deg}(M'', t) + 1$
- and $t_i \in \text{dom}(\text{enab}'')$,
- $\text{enab}(t_i) = \text{enab}''(t_i)$ if $\text{deg}(M', t_i) = \text{deg}(M'', t_i)$
- and $t_i \in \text{dom}(\text{enab}'')$,
- $\text{enab}(t_i) = (0)$ if $t_i \notin \text{enab}''$, and $\text{deg}(M', t) = 1$ is undefined otherwise.

So when an instance of transition $t$ is fired at configuration $(M, \text{enab})$, all the transition instances which are in conflict with $t_i$ are removed from the $\text{enab}$ list, i.e. we remove from $\text{enab}$ the value representing their associated clock to obtain $\text{enab}''$. The clock attached to each newly enabled transition instance is set to 0 and these instances are inserted at the end of the $\text{enab}''$ vector to obtain $\text{enab}'$. See that the timing information attached to a transition instance is not reset in the time period starting from the moment it is inserted into the $\text{enab}$ list to the moment it is removed from the list (either after being fired or disabled).

PRUNING OF FC-TPNs

**Lemma 1:** Given an FC-TPN $N$, the net $\text{Prune}(N)$ is such that $(C_N, \rightarrow_N)$ is isomorphic to $(C_{\text{Prune}(N)}, \rightarrow_{\text{Prune}(N)})$.

**Proof:** Let $N$ be a FC-TPN, and let $N' = \text{Prune}(N)$. We will design a a relation $\mathcal{R}$ from configurations of $N$ to configurations of $N'$, and show that this relation is an isomorphism. A configuration is a pair $C = (M, \text{enab})$ where $M$ is a marking, and $\text{enab}$ assign a finite sequence of real values $\text{enab}(t)$ (clock values) to every transition of the net. For every configuration $C'$ of $N'$, $\text{enab}(t)$ is a map that attaches to every transition $t$ a set of real values $r^1_1, r^1_2, \ldots, r^1_{\text{deg}(t)}$. One can notice that in configurations of free choice nets, all transitions from a cluster are newly enabled at the same date, and hence are attached the same valuations.

Let us now consider a transition $t'$ that was pruned out. This transition comes from a cluster $T(t') = t_2, T(t'), \ldots, t_k, T(t'), t'$, of size greater than 1. Let $\mathcal{R}()$ be the relation that associates to every configuration $C = (M, \text{enab}')$ from $N'$ the configuration $\mathcal{R}(C') = (M', \text{enav})$, i.e. with identical marking $M'$, and such that $\text{enab}(t) = \text{enab}(t)$ if $t$ is not a pruned transition, and $\text{enab}(t) = \text{enab}(t_1, T(t'))$ otherwise. This relation $\mathcal{R}$ is reversible, and $\mathcal{R}^{-1}(C)$ is simply obtained using a restriction of $\text{enab}$ to unpruned transitions. Roughly speaking, $\mathcal{R}$ copies values of a particular transition in the cluster to obtain a configuration of $N$. For a particular set of clocks $\text{enab}(t) = \{r^1_1, r^1_2, \ldots, r^1_{\text{deg}(t)}\}$ and a real value $\delta \in \mathbb{R}$, we will denote by $\text{enab}(t, \delta)$ the set $\{r^1_1 + \delta, r^1_2 + \delta, \ldots, r^1_{\text{deg}(t)} + \delta\}$.

We can now prove that $\mathcal{R}$ is an isomorphism. First of all, let $C_0'$ be the initial configuration of $N'$ and $C_0$ be the initial configuration of $N$. We obviously have $\mathcal{R}(C_0') = C_0$. Now, we have to prove that for every timed or discrete transition
Suppose \( C' \rightarrow \text{prune}(\mathcal{N}) \) \( C_2 \) and every configuration \( C_1 \) such that \( \mathcal{R}(C') = C_1 \), we have \( C_1 \rightarrow \mathcal{N} \) \( C_2 \) and \( C_2 = \mathcal{R}(C_2') \).

- \( C_1' \xrightarrow{\delta} \text{prune}(\mathcal{N}) C_2' \). We have \( \text{enab}_2'(t) = \text{enab}_1'(t) + \delta \) for every transition \( t \), and \( \delta \) violates no urgency, i.e., for every transition \( t \), the maximal value \( r \) in \( \text{enab}_1'(t) \) is such that \( r + \delta \leq lft(t) \). Obviously, in \( C_1 = \mathcal{R}C_1' \), as values of clocks are unchanged for unpruned transitions, and as for pruned transitions the latest firing time is greater that the latest firing time of transition in the same cluster, then a timed move of \( \delta \) from \( C_1 \) violates no urgency, and is also allowed in \( C_1 \). Elapsing time from \( C_1 \) results in a new configuration \( C_2 = (M_1', \text{enab}_1 + \delta) \). One can also easily show that \( (C_2', C_2) \in \mathcal{R} \).

- \( C_1' \xrightarrow{t} \text{prune}(\mathcal{N}) C_2' \). This transition \( t \) can fire from \( C_1' \) if \( \text{enab}_2'(t) \in [\varepsilon \ell ft(t), \ell ft(t)] \), and the marking \( M_1 \) associated with \( C_1' \) is greater than \( \text{pre}(t) \). This transition can also fire from \( C_1 \) as \( \mathcal{R} \) does not change markings nor clocks of unpruned transitions (and \( t \) is necessarily an unpruned transition), and as time constraints of \( \mathcal{N}' \) are larger than those of \( \mathcal{N} \). The effect of firing \( t \) on markings is the same from \( C_1' \) and \( C_2' \), i.e. markings \( M_2' \) and \( M_2 \) are identical in \( C_2' \) and \( C_2 \). Let us now consider the clock part. Firing \( t \) removes the first clock value from \( \text{enab}_2'(t_i) \) (resp from \( \text{enab}_1(t_i) \)) for every transition \( t_i \) such that \( \text{pre}(t_i) = \text{pre}(t) \), i.e., transition from the same cluster as \( t \), and adds a clock with value 0 to every transition which degree is modified w.r.t the intermediate marking. In \( C_2' \) and \( C_2 \) modified clock values are identically updated for unpruned transitions in \( \text{enab}_2 \) and \( \text{enab}_2 \), and clock values in \( \text{enab} \) for pruned transitions remains copies of clock values for transitions in their cluster. Hence, we still have \( C_2 = \mathcal{R}(C_2') \).

Let us now prove that \( \mathcal{N} \) does not allow additional transitions.

- Suppose \( C_1' \xrightarrow{\delta} \text{prune}(\mathcal{N}) C_2' \) and not \( C_1' \xrightarrow{\delta} \text{prune}(\mathcal{N}) C_2' \) or \( (C_2', C_2) \notin \mathcal{R} \). Note that for a chosen \( \delta \) allowed in a configuration, the next configuration reached after elapsing \( \delta \) time units is deterministically chosen. If \( \delta \) can fire, then obviously \( (C_2', C_2) \in \mathcal{R} \). So the remaining possibility is that elapsing \( \delta \) time units is not allowed from \( C_1' \). However, this is impossible, as \( C_1 \) has more transitions than \( C_1' \) for each cluster, identical clocks attached to unpruned transitions and hence can only impose more constraints on possible values of \( \delta \).

- Suppose \( C_1' \xrightarrow{t} \text{prune}(\mathcal{N}) C_2' \) and not \( C_1' \xrightarrow{t} \text{prune}(\mathcal{N}) C_2' \) or \( (C_2', C_2) \notin \mathcal{R} \). Transition \( t \) is allowed in configuration \( C_1' = (M_1, \text{enab}_1) \) iff \( M_1 \geq \text{pre}(t) \), and \( \max(\text{enab}_1(t))(\varepsilon) = \ell ft(t) \). As we have \( C_1' = (M_1, \psi_1) \), the first condition is met, and as \( t \) can only be an unpruned transition, \( \psi(t) = v_1(t) \), so firing \( t \) is also enabled in \( C_1' \). It hence remains to show that the (unique) pair of configurations obtained after firing \( t \) from \( C_1 \) and \( C_1' \) is still in \( \mathcal{R} \). As the marking part is the same in \( C_1 \) and \( C_1' \), it remains to compare the clock part. The clocks attached to transitions by \( \text{enab}_2(t) \) (resp. \( \text{enab}_2(t) \)) are updated iff the degree of \( t \) is modified either from \( M_1 \) (resp. \( M_1' \)) to the intermediate marking \( M_1 \setminus \text{pre}(t) \) (resp. \( M_1' \setminus \text{pre}(t) \)) or from the intermediate marking to the target marking \( M_2 \) (resp. \( M_2' \)). For transitions with decreased degree in the intermediate marking, we have \( \text{enab}_1(t) = \text{enab}_1(t) \setminus \max(\text{enab}_1(t)) \), and for other transitions \( \text{enab}_1(t) = \text{enab}_1(t) \) (ans similarly for \( \text{enab}_1(t) \)). For transitions which degree increases w.r.t temporary marking, we have \( \text{enab}_1(t) = \text{enab}_1(t) \cup \{0\} \), and for remaining ones, \( \text{enab}_1(t) = \text{enab}_1(t) \). This applies similarly for \( \text{enab}_2(t) \) w.r.t \( \text{enab}_1(t) \). In \( \text{enab}_2(t) \), the value of clocks is identical for all transitions from the same cluster, and hence in particular for pruned transitions. Hence, after firing a transition \( t \), \( \text{enab}_2(t) \) is still a restriction of \( \text{enab}_2(t) \) to unpruned transitions, and \((C_2', C_2) \in \mathcal{R} \).

Hence, \( \mathcal{R} \) is a bijective relation from \( \text{Reach}(\mathcal{N}') \) to \( \text{Reach}(\mathcal{N}) \) that preserves moves, i.e. an isomorphism. □

**Processes for TPNs**

**Proposition 1:** Let \( U \) be any untimed net. For any word \( w \in \text{Lang}(U, M_0) \), there exists a causal process \( U \) of \( U \), such that \( w \in \text{lin}(U) \).

**Proof:** We will proceed by induction on the length of words in \( \text{Lang}(U, M_0) \). Recall that words in the language of a net are sequences of transitions \( w = t_1 \ldots t_k \), allowed from the initial marking \( M_0 \). We can then establish a relation between markings obtained after execution a word \( w = t_1 \ldots t_k \), and the sets of maximal conditions that appear in a causal net obtained by appending successively \( t_1 \ldots t_k \). Let \((\mathcal{O}, \pi)\) be a causal process and \( \mathcal{O}^\bullet \) denote its maximal conditions. We denote by \( M_{\mathcal{O}N} \) the marking that associates \( |\mathcal{O}^\bullet \cap \pi^{-1}(p)| \) tokens to every place \( p \in \mathcal{P} \). Similarly, considering a word \( w = t_1 \ldots t_k \in \text{Lang}(U) \), we define \( M_w \) as the marking obtained by successively applying transitions \( t_1 \ldots t_k \) to marking \( M_0 \).

A causal process for a net can be built inductively. One starts from a causal process \( O_{N_0} \) containing only a set of conditions \( X_0 = x_1 \ldots x_n \) and a map \( \pi_0 \) such that \( M_{\mathcal{O}N_0} = M_0 \). Then one can inductively build a process \( O_{N_{n+1}} \) from \( O_{N_n} \) by appending to the set of event \( E_n \) and event \( e_{n+1} = (X, t) \) such that \( X \subseteq \mathcal{O}N_n \), and to the set of conditions \( B_n \) a set of conditions \( \{(e_{n+1}, p) | p \in \mathcal{T} \} \).

Clearly, for a given word \( w \), there exist several causal nets containing in their sets of linearizations. Now we have the following claims: Let \( w = t_1 \ldots t_n \in \text{Lang}(U) \) and let \( U \) be a causal net obtained by appending successively transitions \( t_1 \ldots t_k \) then we have \( M_w = M_0 \) by every transition \( t \) such that \( w.t \in \text{Lang}(U) \) can be appended to \( U \). This property is true for a word of length 0. Now, if the property holds up to a word of length \( n \) we can show that it also holds for a word of length \( n + 1 \). As \( t \) can be appended to \( w \), we have \( M_w(p) = M_{U}(p) \geq \pi \cap \{p\} \). So there there exists \( M_{w}(p) \) conditions in \( \mathcal{U}^\bullet \) which image by \( \pi \) is \( p \). Hence, as \( M_w(p) \) allows firing of \( t \), conditions in \( \mathcal{U}^\bullet \) also allow appending...
t. Now \( M_{w,t}(p) = M_w(p) - |t \cap \{ p \}| + |t^* \cap \{ p \}|. \) As appending transition \( t \) to \( ON \) results in a causal net \( ON' \) such that \( ON'^* = ON'^* \setminus X \cup X' \), where \( X \) contains as many occurrences of \( p \) as \( t^* \) and \( X' \) as many occurrences of each \( p \) as \( p^* \) we have \( M_{w,t} = M_{ON'} \). \( \square \)

Proposition 2: Let \( N \) be a time Petri net, and let \( P \) be the set of all its time causal processes. Then, \( \text{Lang}(N) = \bigcup_{N \in P} \text{Lang}(N) \)

Proof: We will proceed by induction on the length of words and processes. Let us define the property \( P(i) \): for every word of length \( i \), we have \( \{ w \in \text{Lang}(N) : |w| = i \} = \bigcup_{N \in P, |N|=i} \text{Lang}(N) \). Obviously, this property holds for \( i = 0 \), as the empty word \( \epsilon \) of length 0 is a word of any process starting from initial conditions. Let us assume that \( P \) holds up to \( n \). For a given timed word, there exists a unique firing sequence \( C_0, \ldots, C_n \), where \( C_i \) is the configuration reached immediately after execution of event \( e_n \). Let \( ON \) be a time causal net of size \( n \) such that \( w \in \text{Lang}(ON) \). At least one such net exists, as \( P(i) \) holds up to \( n \). Now suppose that \( w \) can be extended to a word of size \( n+1 \), i.e., that \( C_n \) allows execution of an additional event \( e_{n+1} \) at date \( d_{n+1} \), that is an occurrence of some transition \( t \). There is a connection between clocks in configurations and dates in timed causal nets: every occurrence of a clock \( x_i \) attached to the \( i \)-th occurrence of a transition \( t \) is created when a new complete occurrence of \( t^* \) is created. For event \( e_{n+1} \), the date of creation of such clock is a date \( d_k \leq d_{n+1} \) of occurrence of some event \( e_k \), that appended enough new tokens in \( t^* \) to increase the degree of \( t \). When \( e_{n+1} \) fires, it consumes tokens from a marking, that are maximal conditions in \( ON \).

So, there is a correspondence between clocks instances and conditions in time causal nets: \( ON^* \) is an union of conditions that contains occurrences of \( p_1, \ldots, p_j \in t^* \), and such that \( \max_{\{ p_1, \ldots, p_j \}} \) exists. Note that \( d_k \) is not necessarily the maximal date attached to a condition in \( ON \), but is maximal in \( e_{n+1} \cap \text{ON}^* \). Now if \( e_{n+1} \), representing an occurrence of \( t \) can occur at date \( d_{n+1} \) starting from \( C_n = (ON^*, \text{enab}) \) then there exists a clock \( x_1^* \in \text{enab} \) and a delay \( \delta \) such that \( x_1^* \) is the oldest remaining clock created for an instance of \( t \) in \( C_n \) and \( x_1^* + \delta = d_{n+1} \in I(t) \). Recall that \( x^*_1 \) was initialized at date \( d_k \). Hence, there exists a set of conditions \( X \) in \( ON^* \) such that the places appearing in \( X \) are exactly \( t^* \), \( \max(t(X)) + \delta \in I(t) \), and hence \( ON \cup \{ e_{n+1} = (X,t) \} \) with \( \tau(e_{n+1}) = d_{n+1} \) is a process of \( N \), as \( d_{n+1} - d_k \in I(t) \), we have \( \tau(e_{n+1}) - \tau(e_k) = \min_{\exists \omega \in \mathbb{X}} (\tau\omega(e_{n+1}) - \tau\omega(x_1^*)) \in I(t) \). One can prove similarly that if a new event \( e_{n+1} \) can be appended to \( ON \), then this event is allowed from \( C_n \) after elapsing \( \tau(e_{n+1}) - \max(\tau(E_n)) \) time units, and hence \( w.(e_{n+1},\tau(e_{n+1})) \) is a word of \( N \) of size \( n+1 \). \( \square \)

**Proof of correctness of main theorem**

**Lemma 3:** In Algorithm 1, each of the invariants are preserved at end of each iteration of while loop.

**Proof:** Proof is given by induction on number of iterations. We note that each iteration must end either in 6, 17 or 22 (before incrementing \( i \) and going to the next iteration).

(11) \( \rho_i \) is a prefix of \( U' \) It is true at the beginning of loop i.e., base step of \( i = 0 \). Assume that it is true at the end of \( i \)-th iteration of while loop. Now we have to prove that this holds at the end of \( (i+1) \)-th iteration. If we exit the iteration in step 17 or step 22, then it means that \( \rho_{i+1} = \rho_i \) and by induction hypothesis, we have \( \rho_i \leq U' \) hence \( \rho_{i+1} \leq U' \). Otherwise we have exited the iteration in step 6 and it means that \( \sigma_{i+1} = \sigma_i \) and \( \rho_{i+1} = \rho_i \cup \{ e \} \). So we have \( e \in \text{posb}(\rho_i) \) and \( e \in U' \backslash \rho_i \). Hence \( \rho_{i+1} \leq U' \).

(12) \( \rho_i \) is a prefix of \( \text{Utime}(\sigma_i) \) It is true at the beginning of loop i.e., base step of \( i = 0 \), since \( \rho_0 = \sigma_0 \). Assume that it is true at the end of \( i \)-th iteration of while loop. Now we have to prove that this holds at the end of \( (i+1) \)-th iteration. If we exit the iteration in step 17 or step 22 then it means that \( \rho_{i+1} = \rho_i \) and \( \sigma_{i+1} = \sigma_i \cup \{ e \} \) for \( e_i = e \) or \( e_i = e_r \). By induction hypothesis we have that \( \rho_i \leq \sigma_i \). Hence we have \( \rho_{i+1} = \rho_{i+1} \leq \sigma_{i+1} \). Otherwise we have exited the iteration in step 6 and it means that \( \sigma_{i+1} = \sigma_i \) and \( \rho_{i+1} = \rho_i \cup \{ e \} \). So we had \( \sigma_i = \sigma_{i-1} \cup \{ e \} \) in the previous (i.e., \( i \)-th) iteration (or even before that!) and therefore \( \rho_i \cup \{ e \} \leq \sigma_i \leq \sigma_{i-1} \).

(13) \( |\rho_i| + 1 = |\rho_{i+1}| \) or \( |\sigma_i| + 1 = |\sigma_{i+1}| \) At the beginning of loop i.e., at \( i = 0 \), we have \( \rho_0 = \sigma_0 \), and \( |\rho_0| = |\sigma_0| = 0 \). At the first iteration, we necessarily begin the loop discovering that any event in \( \text{posb}(\rho_0) \notin \sigma_0 \). Hence, an event is appended to \( \sigma_0 \) to obtain \( \sigma_1 \) and \( \rho_1 = \rho_0 \). So invariant I3 holds for \( i = 0 \). Assume that I3 holds up to \( i \)-th iteration of while loop. Now we have to prove that it holds at the end of \( (i+1) \)-th iteration. If we exit the iteration in step 17 or step 22 then it means that \( \rho_{i+1} = \rho_i \) and \( \sigma_{i+1} = \sigma_i \cup \{ e \} \) for \( e_i = e \) or \( e_i = e_r \). To perform this step of growing \( \sigma_{i+1} \) we need to add the event \( e \) corresponding to an instance of transition in the net \( N \). This transition must be enabled at \( \sigma_i \), which is guaranteed by Claim A given in I4 (proof given below). Hence, we have that \( |\sigma_i| + 1 = |\sigma_{i+1}| \). Otherwise we have exited the iteration in step 6 and this means that \( \sigma_{i+1} = \sigma_i \) and \( \rho_{i+1} = \rho_i \cup \{ e \} \). Therefore we have that \( |\rho_{i+1}| + 1 = |\rho_{i+1}| \).

(14) For all events \( e \in \text{posb}(\rho_i) \) and \( e \notin \sigma_i \), implies \( e \in \text{posb}(\sigma_i) \). Again, recall that for ease of writing, we slightly abuse notation here; when we say that an event of an untimed causal process belongs (or does not) to a time causal process, we implicitly mean that it belongs to the untiming of the time causal process and so on.

The invariant holds at the beginning of loop i.e., at base step \( i = 0 \). Indeed, all enabled transitions in marking \( M_0 \) correspond to transitions enabled in the initial configuration of \( N \), and all of them can fire if a sufficiently large delay is elapsed. Assume that it is true at the end of \( i \)-th iteration of while loop. Now we have to prove that this holds at the end of \( (i+1) \)-th the iteration. So we enter
the $i + 1$-th iteration with $i$, $\rho_i$, $\sigma_i$ and exit with values $i + 1$, $\rho_{i+1}$, $\sigma_{i+1}$. Let $I^4$ denote the invariant $I^4$ at the $i + 1$-th iteration and $I^4$ denote the invariant $I^4$ at the $i$-th iteration, which are explicitly stated below:

$I^4: f \in posb(\rho_{i+1})$ and $f \notin \sigma_{i+1} \implies f \in posb(\sigma_{i+1})$

$I^4: f \in posb(\rho_i)$ and $f \notin \sigma_i \implies f \in posb(\sigma_i)$.

Let $f$ be some event of $posb(\rho_{i+1})$ (we use $f$ as a generic event to not confuse with $e$, the event picked in step 4).

We have two cases:

1. **Case (exit by step 6).** This means that $\sigma_{i+1} = \sigma_i$ and $\rho_{i+1} = \rho_i \cup \{e_i\}$ for some event $e_i$. To execute this step, $e_i \in posb(\rho_i)$ is a pre-requisite, and $e_i \notin posb(\rho_{i+1})$.

   If $f \neq e_i$. Then either $f$ was newly enabled after adding $e_i$ or $f$ was already enabled before adding $e_i$.

   - **First consider the case in which $f$ was newly enabled after adding $e_i$ to $\rho_i$.** Assume that it satisfies premise of $I^4$-1. Now we have to prove that $f \in posb(\sigma_{i+1})$ to prove that invariant $I^4$ is preserved. Since $f$ was enabled at $\rho_{i+1}$ and not at $\rho_i$, event $f \notin posb(\rho_i)$. Therefore, it trivially satisfies property $I^4$. Hence, we get that $f \in posb(\sigma_i)$. Now as $i$-th iteration of the while loop exited at step 6, we have $\sigma_{i+1} = \sigma_i$ and hence $posb(\sigma_{i+1}) = posb(\sigma_i)$. Therefore we obtain $f \in posb(\sigma_{i+1})$.

   - **Now consider the case in which $f$ was already enabled before adding $e_i$ to $\rho_i$.** Assume that it satisfies premise of $I^4$-1, i.e. $f \notin \sigma_{i+1}$. Now we have to prove that $f \in posb(\sigma_{i+1})$. Since it satisfies premise of $I^4$-1 we have $f \notin \sigma_{i+1}$, implying $f \notin \sigma_i$. Now, as $I^4$ holds up to step 6, $I^4$ holds, and as we know that $f \in posb(\rho_i)$ we get that $f \in posb(\sigma_i)$. Now when we exit at step 6, we have that $\sigma_{i+1} = \sigma_i$ and hence $posb(\sigma_{i+1}) = posb(\sigma_i)$. Therefore we get that $f \in posb(\sigma_{i+1})$.

   - **Case (exit by step 22 or step 17):** If we exit the iteration in either step, then it means that $\rho_{i+1} = \rho_i$ and $\sigma_{i+1} = \sigma_i \cup \{e_i\}$ for some event $e_i$ (in case of exit by step 17, $e_i = e$ of that iteration). In both cases, there are two cases to consider: $f = e_i$ or $f \neq e_i$, i.e., whether $f$ is the event which is used to grow $\sigma_i$ to get $\sigma_{i+1}$ or not.

   - **First, we prove this invariant for $f \neq e_i$ satisfying premise of $I^4$-1.** After adding $e_i$ to $\sigma_i$, we cannot have event $f$ newly enabled i.e., $f \in posb(\rho_{i+1})$ and $f \notin posb(\rho_i)$ because $\rho_i = \rho_{i+1}$. So we consider the case when $f$ was already enabled i.e., $f \in posb(\rho_{i+1})$ and $f \in posb(\rho_i)$ also. Since $f$ satisfies premise of $I^4$ we have that $f \notin \sigma_{i+1}$, implying $f \notin \sigma_i$ as $\sigma_i \leq \sigma_{i+1}$. So we have both clauses of $I^4$ satisfied for event $f$. Therefore we have that $f \in posb(\sigma_i)$. Let $t$ be the transition corresponding to event $e_i$ and let $s$ be the transition corresponding to event $f$. Let $t_u$ and $s_u$ be the most urgent transition instances of $t$ and $s$ respectively at $M(\sigma_i)$.

     Both these transition instances were firable at marking $M(\sigma_i)$. So when $\sigma_{i+1}$ was obtained by adding event $e_i$ to $\sigma_i$, correspondingly we have $M(\sigma_i) \xrightarrow{t} M(\sigma_{i+1})$. Now if $s$ and $t$ were independent i.e., not sharing a pre-place in the net (and it does not matter if $s_u$ and $t_u$ were equally urgent) transition $t_u$ is still enabled at marking $M(\sigma_{i+1})$ and firable, implying that its event $f \in posb(\sigma_{i+1})$ which was what we wanted to prove. Otherwise $s$ and $t$ are in conflict i.e., sharing a pre-place in the net, and both $s_u$ and $t_u$ were enabled at marking $M(\sigma_i)$, which means that both the corresponding events $e_i$ and $f$ were in conflict too. But $\rho_i \leq N'$, and we had $e_i$ and $f$ from $N'$ and in posb($\rho_i$), so we have $\rho_i \cup \{f, e_i\} \leq N'$, but $N'$ being a causal net, we could have only one of these events in it. So this case never arises.

   - **Now, on the other hand, if $f = e_i$, event $e_i$ is added to $\sigma_i$, then we have $e \in \sigma_{i+1}$ which falsifies a clause in the premise of $I^4$-1 hence trivially satisfying it. But for this, we need to crucially show that we can indeed add $e_i$, i.e., we can fire $t$ the transition corresponding to event $e_i$ in the net $N$ (it has not got disabled by firing of any other urgent transitions). We show this below which completes the proof.

   In the untimed net, at a marking, multiple enabled instances of a transition are indistinguishable from each other. One such instance of transition $t$ gave rise to event $e_i$ in the untimed causal net. To get the matching event in the timed causal net, it is sufficient to fire some instance of $t$ in the timed net. Since transition instances of same transition are not in conflict with each other, and by FEFD policy, all we need to prove is that the first enabled transition instance of $t$ is firable at $M(\sigma_i)$. Let $t_u$ be this transition instance.

**Claim A. Transition $t_u$ it is firable at marking $M(\sigma_i)$.** Proof: Assume the contrary, i.e., transition instance $t_u$ is not firable at $M(\sigma_i)$. Inductively, let us assume that this is the first time that such transition which was not firable, while building time causal net $N$, from the beginning where initial conditions were same and set of enabled events same for both causal nets $N'$ and $N$. Let $e_i \not\in\{e_i\}$ denote the set of predecessors for $e_i$ in causal net $N'$; it contains all events and conditions needed for event $e_i$ to occur. As we are in $i + 1$-th iteration, $e_i \in posb(\rho_i)$ and since we are exiting this iteration by step 22 or 17, it means $e_i \notin \sigma_i$. By induction we have invariant $I2$ true at $i$-th iteration so $\rho_i \leq \sigma_i$, implying $e_i \notin \rho_i$, so $e_i \not\in\{e_i\}$. Therefore all the pre-places $\bullet t$ are marked at the configuration with marking component $M(\sigma_i)$. Now the only possible reason that transition instance $t_u$ is not firable in the timed net at this configuration, is that there exists some instance $t_u'$ of another transition $t'$ which shares a pre-place with $t$ (and hence by FEFD policy, transition instance $t_u'$ is in conflict...
Lemma 2: Algorithm 1 terminates in finitely many steps. If we exit this step then also means that \( \tau_i = t \) and therefore, transition \( t \) is enabled at marking \( M(\sigma_i) \), and since net is pruned we have cluster \([t]_t\) pruned, and so \( lft(t) = lft(t') \), which is a contradiction even in the case when \( lft(t) = \infty \). So it must be the case that \( \sigma_i \in posb(\sigma_i) \) in time causal net \( N \). Note that this step of the proof uses free-choice, pruning as well as our choice of semantics critically.

\[
(I5) \quad \epsilon G^t_\tau e' \implies \tau(e) \leq \tau(e').
\]

In the base case of \( i = 0 \), timed causal net \( \sigma_0 \) has no events and so the invariant is trivially satisfied. Assume that induction holds up to the \((i-1)\)-th iteration. That is when we enter with \( \sigma_{i-1} \) and \( \rho_{i-1} \) in the loop and come out with \( \sigma_i \) and \( \rho_i \). So we have that:

\[
(I5)^1: \quad \epsilon G^t_\tau e' \implies \tau(e) \leq \tau(e').
\]

Now for the inductive step, assume that we are in \( i \)-th iteration and \( \epsilon G^t_\tau e' \). If events \( e \) and \( e' \) both are in \( \sigma_i \) then by \((I5)^1\) we have that \( \tau(e) \leq \tau(e') \). Let us now consider cases where \( e \) and \( e' \) are not both in \( \sigma_i \). Adding an event \( e = (X,t) \) to an existing causal net means creating causal dependencies from predecessors of conditions in \( X \) to \( e \). Since we add at most one event to \( \sigma \) at each iteration of the loop, and since we have \( \epsilon G^t_\tau e' \) it cannot be the case that \( e \in \sigma_{i+1} \setminus \sigma_i \) and \( e' \in \sigma_{i+1} \setminus \sigma_i \). Therefore, \( e, e' \in \sigma_i \setminus \sigma_{i+1} \). But \( \epsilon G^t_\tau e' \) also implies that \( e \in e' \setminus lft(e) \) which means event \( e \) was added at some iteration \( k \) where \( k \leq i \). When an event \( e = (X,t) \) is appended to a timed causal net \( \sigma_k \), it gets a time stamp \( \tau(e) = CLK + lft(t(e)) - td(\sigma_i,e) \) or \( t(e) = CLK + max\{0,td(\sigma_i,e)\} \). Now, it is easy to see that during the execution of the algorithm, the value of \( CLK \) is non-decreasing. Hence, we have \( \tau(e') \geq \tau(e) \).

Lemma 2: Algorithm 1 terminates in finitely many steps.

**Proof:** We prove that eventually \( \rho_i = N' \) for some \( i \). For that it is sufficient to prove that we do not exit by step 22 or by step 17 infinitely often in the while loop. If we could execute finite number of times then it means that \( \rho_i \) can be grown to include all the events \( N' \) which itself is finite.

Let \( CLK = 0 \), and let \( e \) be the event chosen in step 4 at the beginning of while loop in the \( i + 1 \)-th iteration and let \( t \) be the transition corresponding to it. Suppose not, that is we exit by step 22 infinitely often. Let us assume that last time we exited from step 6 was at the end of \( i \)-th iteration. If we exit by this step then also means that \( S_i \neq \emptyset \) which means \( lft(t) \neq \infty \). So it implies that we have an infinite run \( q_1 \xrightarrow{\epsilon} q_1 \xrightarrow{\epsilon} q_2 \xrightarrow{\epsilon} \ldots \) starting at \( q_1 \), adding events to \( \sigma_i \). Since net is finite, set of transitions occurring in this run is finite, so there exist at least one transition which occurs infinitely often in this run, let \( s \) be this transition. Now if \( lft(s) > 0 \) then there exist a minimal constant \( K \) such that \( \sum_{k=0}^{K} lft(s) > lft(t) \).

Therefore, before \( K \)-th occurrence of \( s \) in this infinite sequence transition \( t \) would have become urgent and we would have fired it, contradicting that there is no transition in the sequence which contributes an event to \( \rho \). So it must be the case that \( lft(s) = 0 \), and this is true of any transition occurring infinitely often in this infinite sequence. Now there exist \( m \geq 1 \) such that each transition after \( q_m \) occurs infinitely often. It means that we have a 0-delay timed firing sequence starting \( q_m \), which is a contradiction.

Now to complete the proof by contradiction, we suppose that, we exit by Step 17 infinitely often, which is not possible because events like \( e \) are taken from untimed causal net \( N' \) which is finite.

**ROBUSTNESS**

**Proposition 3** The class of FC-TPNS is not robust wrt firablity of transitions.

**Proof:** To prove this we exhibit a net FC-TPN \( N' \) and a perturbation \( \Delta \) such that \( \text{Firable}(N') = \text{Firable}(N' \Delta) \). Consider FC-TPN \( N' = (\mathcal{U}, M_0 = \{p_1\}, I) \) given in Figure 11. Its reachable markings are \( \text{Untime}(\text{Reach}(N', M_0)) = \{1, 2\} \).

Under guard enlargement \( G > 0 \), FC-TPN \( N' \Delta \) has set of reachable markings \( \text{Untime}(\text{Reach}(N' \Delta, M_0)) = \{1, 2, 3\} \).

![Fig. 11. A non-robust FC-TPN](image-url)
process contains a (possibly empty) prefix $N'$ that is a process of $\text{Uptime}(N)$. The configuration reached after $N'$ allows at least one firable transition of $N_\Delta$ that is not firable in $N$. Hence, this both contradicts the fact that all clusters that have firable transitions remains unchanged or are never fired.