Model Checking Process Algebra of Communicating Resources for Real-time Systems

Boudjadar, Jalil; Kim, Jin Hyun; Larsen, Kim Guldstrand; Nyman, Ulrik

Published in:
Proceedings of ECRTS 2014

DOI (link to publication from Publisher):
10.1109/ECRTS.2014.24

Publication date:
2014

Document Version
Accepted author manuscript, peer reviewed version

Link to publication from Aalborg University

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from vbn.aau.dk on: July 26, 2022
Model Checking Process Algebra of Communicating Resources for Real-time Systems

A.Jalil Boudjadar, Jin Hyun Kim, Kim G. Larsen, Ulrik Nyman
Institute of Computer Science, Aalborg University, Denmark
{jalil,jin,kgl,ulrik}@cs.aau.dk

Abstract—This paper presents a new process algebra, called PACoR, for real-time systems which deals with resource-constrained timed behavior as an improved version of the ACSR algebra. We define PACoR as a Process Algebra of Communicating Resources which allows to express preemptiveness, urgentness and resource usage over a dense-time model. The semantic interpretation of PACoR is defined in the form of a timed transition system expressing the timed behavior and dynamic creation of processes. We define a translation of PACoR systems to Parameterized Stopwatch Automata (PSA). The translation preserves the original semantics of PACoR and enables the verification of PACoR systems using symbolic model checking in UPPAAL and statistical model checking UPPAAL SMC. Finally we provide an example to illustrate system specification in PACoR, translation and verification.

I. INTRODUCTION

More and more complex systems are being used in a safety and mission critical setting. Such systems need to be specified in a rigorous and formal way and proved to be safe and correct in practice. As a complement to the many transition system based formal models, process algebras provide a means of compact and precise formal specification framework with a calculi for checking properties. This paper defines an improved dense time process algebra (PACoR) and provides a link to verification tools which makes it relevant for practical verification.

Algebra of Communicating Shared Resources (ACSR)[4], [14] is a process algebraic approach to specify resource-constrained real-time systems. It introduces the notion of prioritized transitions based on a preemption relation of concurrent real-time processes. Recently, ACSR has become more relevant as multi-core systems are increasingly being used for real-time systems. ACSR has inspired Process Algebra for Demand and Supply (PADS)[16] to specify hierarchical scheduling systems. ACSR has been defined over a dense real-time semantics, however the underlying verification tools, VERSA[7] and XVERSA[6], have only been able to deal with the discrete time version. Moreover, ACSR has some difficulties in describing real-time systems. In the continuous-time version of ACSR timed actions cannot be restored after they have been preempted [4], which is contrary to actual real-time system implementations. This notion of processes being restored can be described in the discrete time version of ACSR, but only with the granularity of one time unit.

Inspired by ACSR, this paper presents a new process algebra, called Process Algebra of Communicating Resources (PACoR), to address the above issues. PACoR supports more expressive descriptions for timed actions in terms of the urgentness and preemptiveness. Moreover, we present translation rules from PACoR to Parameterized Stopwatch Automata (PSA) models which can be analyzed using UPPAAL and UPPAAL SMC. The translation preserves the semantics of PACoR. The rest of this paper is organized as follows: Section II presents the related work. Section III presents the syntax and semantics of PACoR. Section IV provides the translation rules. Section V provides a train platform system example. Finally section VI concludes the paper.

II. RELATED WORK

Process algebras, like CCS [15] and CSP [12], have originally been introduced as a formal way to rigorously describe concurrent and communicating systems together with a calculi for the verification of their properties. Over the years, different algebras have been developed for the specification and analysis of domain-specific systems like ACSR [4], [14], mCRL2 [11] for resource sharing, Timed CSP [17] for time modeling, etc.

mCRL2 is a process algebra that includes data and time suitable for the specification and verification of real-time systems. It enables local communication, multi-actions and communication-independent parallelism that are key concepts of component-based and hierarchical systems. A toolset supporting the verification of mCRL2 models has been developed[8]. However the syntactic richness of mCRL2 makes the semantics and interaction between the different concepts hard to grasp, and leads to state space explosion that affects verification.

An alternative to algebra based formalisms are timed automata-based formalisms [2], [9], where systems are described as a set of concurrent automata modeling the concrete timed behavior of the systems. Such formalisms enable certain flexibility when describing systems but may suffer to deal with hierarchy. The PACoR language is relatively compact in terms of syntax comparing to other algebra, but provides sufficient expressiveness to model resource sharing in real-time systems in an elegant way, and also enables effective dense-time analysis thanks to its timed semantics and to the UPPAAL toolsuite.

The research presented in this paper has been partially supported by EU Artemis Projects CRAFTERS and MBAT.
III. PACoR: Process Algebra of Communicating Resources

Process Algebra of Communicating Resources (PACoR) is a revised and improved version of ACSR for requirement specification of real-time systems. It adopts the concept of timed actions and event actions of ACSR. The execution of a timed action requires a set of resources (potentially empty) that are requested with individual priorities. The execution time is given as an interval between best and worst cases. Event actions are instantaneous, and two events (e.g. e and e′) synchronize if they are compatible. An internal action, represented by the distinguished event τ, cannot synchronize with any other action. Unlike ACSR, we have chosen in PACoR not to associate priorities to the event actions. The reason for this being that event actions are not resource consuming, while our language framework is resource based. Moreover, PACoR changes the meaning of the ACSR operator "{}" so that timed actions can be non-urgent and preemptive. Instead of {}, we introduce ⟨⟩ as a urgent non-preemptive operator by which the execution of timed actions is never allowed to stop once it starts. The urgentness can be loosened or hardened when the operators ⟨⟩ and {} are composed with the scope operator Δ.

A resource requirement is specified as a pair (r, pri) representing a resource name r and an associated priority pri. An action is a (potentially empty) sequence of resource requirements. A timed action without any resource requirement is called empty-set timed action and denoted by ∅ or {}. An action a can be either preemptible (⟨a⟩) or non-preemptible (a) signifying whether it can be preempted by an action having a higher priority. Higher priorities have numbers greater than that of lower priorities. In PACoR, all priorities should be greater than 0, which is reserved for the empty-set timed actions. A timed action aδ is defined as an action a specified with a timed interval δ representing the best and worst case execution time. We use DR as a set of resources and DE a set of events. We also use x, y, z for clock variables; P, Q for processes; R for natural numbers; l, m, n, u for time values; and α and β for events and actions.

A. Syntax of PACoR

The syntax of PACoR is defined by the following grammar:

\[
P ::= \text{NIL} \mid \text{DONE} \mid A : P \mid E.P \mid P_1 + P_2 \mid P_1 || P_2 \mid [P] \mid P \sqcap F \mid \text{rec } X.P
\]

\[
A ::= \langle \alpha \rangle \delta \mid \langle S \rangle \mid \langle \rangle \delta
\]

\[
E ::= \varepsilon \nabla \langle n, P_1, P_2 \rangle \mid \varepsilon
\]

\[
\varepsilon ::= e \mid \bar{e} \mid \tau
\]

\[
S ::= \varepsilon \mid (r, \text{pri}), S
\]

\[
\delta ::= [l; u]
\]

NIL is a process that cannot progress, meaning that it is in deadlock. DONE is a regular termination statement. There are two prefix operators, corresponding to actions and events respectively. The timed action operator A : P executes a resource-consuming action A. A[\langle \rangle \delta] : P executes for a specific time bound δ = [l; u], and then proceeds to the process P. The event action operator E.P executes an event action instantaneously. Basically, the event actions are urgent, but they can be delayed by the scope operator. The Choice construct P_1 + P_2 represents a non-deterministic choice between two processes P_1 and P_2. The construct P_1 || P_2 represents the parallel composition of two processes P_1 and P_2 where they may progress synchronously or independently. PACoR includes also two scope constructors to bind timed and event actions to timing requirements. A[\langle \rangle \delta] \triangle \langle n, P_1, P_2 \rangle binds the timed action A to a temporal scope and incorporates time-out and exception handlers. A given time bound n ∈ R⁺ ∪ \{∞\}, the scope may be exited in 3 ways: 1) if A successfully terminates using resources for δ time units before the deadline n, then the system proceeds to the following process; 2) if A fails to execute and misses its deadline n, then the system proceeds to a time-out handler P_2; 3) the scoped timed action can be interrupted by an exception handler P_2 at any time. Urgent and non-preemptive timed actions associated with the scope operator Δ can be delayed unless resources are available, but they cannot cease using resources once they start the execution. In contrast, non-urgent and preemptive timed actions are enforced to execute as soon as they start by setting the deadline as same as the execution time. The Scope constructor E∇⟨n, P_1, P_2⟩ for event actions binds an event action E to a temporal scope, which requires an event to happen within the temporal scope n. The process P_2 executes when the event E does not happen within the temporal scope n. The waiting of event E can be interrupted by an exception process P_2. The Close operator [P] associates a special resource r_0 to all simultaneously enabled timed actions, so that all enabled timed actions including the empty-set timed action (∅ or {}) become comparable according to the priority relation. Moreover, it enables to choose a process among a set of processes using the same priorities for the same resources. The Restriction operator, P \sqcap F, limits the behavior of P in a way that no event with labels in F is permitted to execute. The construct rec X : P denotes a (finite) recursive process.

TABLE I

| System | \(\text{def} = \{[D_1 || D_2 || T_1 || T_2] \backslash \{s_1, s_2\}\}\) |
|--------|---------------------------------------------------------------|
| D_1    | \(\emptyset^5 : s_1, D_1\)                                 |
| D_2    | \(\emptyset^{10} : s_2, D_2\)                               |
|  T_1   | \(s_1 \nabla (\infty, \text{NIL, NIL, NIL}, C_1)\)         |
| T_2    | \(s_2 \nabla (\infty, \text{NIL, NIL, NIL}, C_2)\)         |
| C_1    | \(\{(\text{cpu}, 3)\}^2 \triangle (5, \text{NIL, NIL}) : T_1\) |
| C_2    | \(\{(\text{cpu}, 2)\}^3 \triangle (7, \text{NIL, NIL}) : T_2\) |

Example 3.1: Table I shows a PACoR example of two periodic tasks having the following attributes:

- \(T_1\): Period 5, Execution Time: 2, Deadline: 5
- \(T_2\): Period 10, Execution Time: 3, Deadline: 7
relation in order to consider event actions, making then all action types comparable. This priority relation also functions as a preemption relation between timed actions, and thus specifies in which cases a timed action can preempt another timed action.

**Definition 3.1: (Priority Relation)** Given two actions $\alpha$ and $\beta$, we say that $\beta$ has priority over $\alpha$, denoted by $(\alpha < \beta)$, if one of the following cases holds:

1. $\alpha \in D_R$ and $\beta \in D_E$
2. Both $\alpha$ and $\beta$ are actions in $D_R$, where
   \[
   \forall r \in p(\beta) \cap p(\alpha), (r, p) \in \alpha \land (r, p') \in \beta \Rightarrow p < p'
   \]
   According to the first condition, all instantaneous events have priority over timed actions. Besides, timed actions sharing a resource are arbitrated according to the second condition: if there exist resources shared by two timed actions $\alpha$ and $\beta$, then $\beta$ preempts $\alpha$ if and only if all the priorities of $\alpha$ over the shared resources are lower than the priorities of $\beta$ over the same resources. Our preemption relation is more strict than the ACSR preemption relation but helps to solve non-deterministic relations between tasks. Such a fact makes the system more deterministic.

**Example 3.2:** some relations between two timed actions can be as follows:

1. $\{(r_1, 2), (r_2, 5)\} \prec \{(r_1, 7), (r_2, 5)\}$
2. $\{(r_1, 2), (r_2, 5)\} \prec \{(r_2, 7), (r_3, 5)\}$
3. $\{(r_1, 2), (r_2, 5)\} \not\prec \{(r_1, 7), (r_2, 3)\}$
4. $\{(r_1, 2), (r_2, 0)\} \not\prec \{(r_1, 7)\}$
5. $\{(r_1, 2), (r_2, 1)\} \not\prec \{(r_1, 7)\}$
6. $\{(r_1, 3), (r_2, 3), (r_3, 1)\} \not\prec \{(r_1, 1), (r_2, 1), (r_3, 1)\}$

In ACSR, cases 2 and 4 are incomparable, no one has priority over the other, but in case 6 actions are comparable.

Let us first recall timed transition systems and their bisimulation relation. Timed Transition Systems (TTS) [13] represent an elegant model to define the semantics of real-time formalisms. Basically, a TTS is a labeled transition system where labels can be events or durations.

**Definition 3.2 (Timed transition System):** a timed transition system over an alphabet $\Sigma$ is a tuple $(\mathcal{S}, \mathcal{S}^0, \rightarrow)$ where $\mathcal{S}$ is a set of states, $\mathcal{S}^0 \subseteq \mathcal{S}$ is the set of initial states and $\rightarrow \subseteq \mathcal{S} \times \Sigma \cup \{(\tau)\} \cup \mathbb{R}_{\geq 0} \times \mathcal{S}$ is the transition relation.

Here and elsewhere, we write $s \xrightarrow{\lambda} s'$ for any transition $(s, \lambda, s) \in \rightarrow$. Moreover, a transition is continuous if it is labeled by a real value from $\mathbb{R}_{\geq 0}$, otherwise the transition is discrete. TTSs are comparable via simulation and bisimulation relations. The simulation relation of TTSs establishes a mapping between their timed traces [1] where, from a common state, we check whether for each outgoing transition of the simulating system, a corresponding transition can be triggered in the simulated system.

We introduce the transition relation $\rightarrow_{\pi\pi} = (\pi_2)\pi_1$ as a sequence of internal transitions such that for any event $\lambda$, $s \xrightarrow{\lambda}_{\pi\pi} s' = s \xrightarrow{\pi_2} s_1 \xrightarrow{\pi_1} s_j \xrightarrow{\pi_2} s_j'$. Such a transition relation enables to check the weak-bisimulation relation of TTS.

**Definition 3.3 (TTS simulation):** Given 2 TTSs $T_1 = (\mathcal{S}_1, \mathcal{S}_0^1, \rightarrow_1)$ and $T_2 = (\mathcal{S}_2, \mathcal{S}_0^2, \rightarrow_2)$ defined on the same alphabet $\Sigma$, $T_1$ simulates $T_2$ through a relation $\mathcal{R} \subseteq \mathcal{S}_1 \times \mathcal{S}_2$, denoted by $T_1 \subseteq_{\mathcal{R}} T_2$, if $\forall s \in \mathcal{S}_0^1 \exists s' \in \mathcal{S}_0^2[(s, s') \in \mathcal{R}$
We introduce \( ID \). According to the following theorem, the TTS restriction \( T \) of a TTS \( \langle S, Stem, \cdot \rangle \) by \( W \) over these events are deleted. Given a TTS \( T \) over a set of events is a TTS where transitions composable \( s \) \( \mapsto \) \( s' \) \( \land \) \( \langle s', s'' \rangle \in R \).

The restriction of a TTS \( \langle \cdot \rangle \) enables to ignore unmatched synchronizing transitions when composing different concurrent processes. Such a function implements the operator \( \setminus \) of \( \text{PACoR} \).

**Definition 3.4 (TTS restriction):** The restriction of a TTS over a set of events is a TTS where transitions composable over these events are deleted. Given a TTS \( T = \langle S, S^0, \cdot \rangle \) and a set of events \( W \), we define the restriction of \( T \) on \( W \), denoted \( T \setminus W \), to be the TTS \( \langle S, S^0, \cdot \rangle \setminus \{ s \mapsto s' \mid s \in W \} \).

According to the following theorem, the TTS restriction operation preserves the bisimulation relation.

**Theorem 3.1 (Bisimulation and restriction):** Let \( T_1 \) and \( T_2 \) be 2 TTS defined on the same alphabet \( \Sigma \) and \( \mathcal{R} \) be a simulation relation, then \( T_1 \sim \mathcal{R} T_2 \Rightarrow T_1 \setminus \Phi \sim \mathcal{R} T_2 \setminus \Phi \) for any \( \Phi \subseteq \Sigma \).

**Proof.** It is straightforward.

We introduce \( ID \) as a set of identifiers and \( \mathcal{P} \) as a set of processes.

- \( \text{Ident} : \mathcal{P} \rightarrow ID \) is a function associating an identifier to each process in order to distinguish between processes.
- \( \text{fresh}(ID) \) returns a free identifier from \( ID \).

**Definition 3.5 (Semantics of \( \text{PACoR} \)):** we define the semantics of \( \text{PACoR} \) in terms of a timed transition system \( TTS (\langle S, S^0, \cdot \rangle) \) where:

- \( S = \langle \text{Stem} \cup \text{Deadlock} \rangle \times \mathbb{R}_{\geq 0} \times ID \) is the set of states.
- \( \text{Stem} \) represents the \( \text{PACoR} \) statements derived from the non-terminal \( \mathcal{P} \) given in the grammar, \( \mathbb{R}_{\geq 0} \) represents the time instants, and \( ID \) is a set of process identifiers.
- \( S^0 \subseteq S \) is the set of initial states defined by \( \text{Stem}^0 \times \{ 0 \} \times \{ \text{Id}_0 \} \), where \( \text{Stem}^0 \) defines a set of statements representing the initial steps of the \( \text{PACoR} \) executions, and \( \text{Id}_0 \) is the identifier of the top level process \( \mathcal{P} \).
- \( \rightarrow \subseteq S \times \{ \{ \tau \} \cup E \cup A \cup \mathbb{R}_{\geq 0} \} \times S \).

The function \( \text{Stem}^0 \) is given in the following:

- \( \text{Stem}^0(NIL) = \emptyset \)
- \( \text{Stem}^0(E, P) = E \)
- \( \text{Stem}^0(P_{1} : P_{2}) = \text{Stem}^0(P_{1}) \cup \text{Stem}^0(P_{2}) \)
- \( \text{Stem}^0(P_{1} \parallel P_{2}) = \text{Stem}^0(P_{1}) \times \text{Stem}^0(P_{2}) \)
- \( \text{Stem}^0([P_{1}]) = \text{Stem}^0(P) \)
- \( \text{Stem}^0(P_{1} : F) = \{ s | s \in \text{Stem}^0(P) \land s \notin F \} \)
- \( \text{Stem}^0(\text{rec.X.P}) = \text{Stem}^0(P) \)

The transition relation \( \rightarrow \) is the smallest relation given by the rules of Table III.

In fact, we keep constructing the function \( \text{Ident} \) on the fly, so that when executing a statement we propagate the identifier of the statement process to the resulting process \( (\text{Ident}(P) := \text{Ident}(A : P)) \), respectively statement, in order to know at any instant the owner process of a statement. The first rule of \( \text{A-success} \) in Table III corresponds to a successful execution of an urgent timed action, whereas the second rule states the execution of a regular timed action with respect to its deadline. The urgent action \( A^{[t,u]} \) should be run immediately once the corresponding statement is reached, otherwise the system will be in a Deadlock according to the second rule of \( \text{A-failure} \). Moreover, an urgent action can be preempted by event actions only. \( \text{A-failure} \) rule corresponds to the execution of an action missing its deadline, the corresponding timeout handler process \( P_t \) is triggered once the deadline is met. The \( \text{Close} \) rule corresponds to the close operator where the action \( A \) is extended with a particular resource request \( (r_0, lp(A)) \) in order to make the action \( A \) comparable with other concurrent actions, and possibly leads to a priority decision in some non-deterministic cases. \( \text{A-delay} \) states a delay \( m \) of a non-urgent action when the corresponding deadline \( n \) allows \( (u < n - m) \). \( \text{Preemption} \) rule states a preemption of either an urgent or a non-urgent preemptive timed action. \( \text{E-success} \) rule is the same as \( \text{A-success} \), for urgent \( (E) \) and non-urgent \( (E \cup \{ n, P_t, P_r \}) \) events execution, where no time elapses because events execution is instantaneous. Rule \( \text{E-failure} \) corresponds to the triggering of a timeout handler process when the execution of an non-urgent event misses its deadline. Rule \( \text{Exception} \) corresponds to the triggering of an exception handler process \( P_e \) when a non-urgent event or timed action is waiting to be triggered. Rule \( \text{E-delay} \) expresses a delay of a non-urgent event while the corresponding deadline \( n \) is respected. Rules \( \text{E-Choice} \) and \( \text{A-Choice} \) specify a non-deterministic choice between 2 executions, where the left hand statement is taken. A synchronization of 2 compatible events is described by rule \( \text{E-sync} \). The resulting transition will be considered as an internal event \( \{ \tau \} \) of the composition. \( \text{E-Async} \) describes an asynchronous event of parallel composition. In rule \( \text{A-sync} \), 2 concurrent timed actions progress together if they do not require the same resources. The execution time of such a synchronization will be the maximum of the execution time of both actions. \( A_1 \cup A_2 \) is the union of resource requests of both actions \( A_1 \) and \( A_2 \). The priority relation is not considered because actions \( A_1 \) and \( A_2 \) do not compete the same resources, so they are incomparable. Rule \( \text{A-async} \) corresponds to the execution of a timed action \( A_1 \) having priority over the concurrent timed action \( A_2 \). Rule \( \text{Event-Action} \) states that event actions have priority over timed actions. Rule \( \text{NIL} \) states a system deadlock if one of the concurrent processes reaches a \( \text{NIL} \) statement. In the rules explained above, the set of activated process identifiers \( ID \) is not updated when executing any transition because no process is created or killed on the execution of these transitions. Rule \( \text{P-destroy} \) states an on-the-fly destruction of a process once it reaches a \( \text{DONE} \) statement. The identifier of the corresponding process \( (\text{Ident}(\text{DONE})) \) will be so removed from the set of active process identifiers \( ID \). For this reason, we propagated the process identifiers throughout transition rules in order to recognize the identifier of the owner process of each statement. Rule \( \text{P-create} \) expresses a dynamic creation of processes where the number of active processes in a system may differ from a state to another. The on-the-fly creation of a process \( [3] \) can be interpreted by the extension of the current system state by a new instance of such a process, where a fresh identifier is picked from the set of identifiers \( ID \) and assigned to such a process instance. Such a feature is recently integrated in the \( \text{UPPAAL toolsuite} \) [10].
A-success: \( m \in \mathbb{R}_{\geq 0}, 1 \leq m \leq u, \text{Ident}(P) := \text{Ident}(A^{[l,u]}; P) \) 
\( (A^{[l,u]}; P, x, ID) \xrightarrow{\rho(A_1)} (P, x + m, ID) \) 

A-failure: \( m \in \mathbb{R}_{\geq 0}, \text{Ident}(P) := \text{Ident}(A^{[l,u]}; P) \) 
\( (A^{[l,u]}; P; F, x, ID) \xrightarrow{\Delta} (P, x + m, ID) \) 

Close: \( m \in \mathbb{R}_{\geq 0}, \text{Ident}(P) := \text{Ident}(A^{[l,u]}; P) \) 
\( (A^{[l,u]}; F, x, ID) \xrightarrow{\Delta} (P, x + m, ID) \) 

Preemption: \( m \in \mathbb{R}_{\geq 0}, \text{Ident}(P) := \text{Ident}(A^{[l,u]}; P) \) 
\( (A^{[l,u]}; P, x, ID) \xrightarrow{\Delta} (P, x + m, ID) \) 

A-Delay: \( m \in \mathbb{R}_{\geq 0}, u \leq n - m, n' = n - m \) 
\( (A^{[l,u]}; A, P, x, ID) \xrightarrow{\Delta} (A^{[l,u]}; A, P, x + m, ID) \) 

E-success: \( \) 
\( (E.P, x, ID) \xrightarrow{\rho} (P, x, ID) \) 

E-succ: \( \) 
\( (E.P, x, ID) \xrightarrow{\rho} (P, x, ID) \) 

E-failure: \( \) 
\( (E.V, x, ID) \xrightarrow{\rho} (P, x, ID) \) 

E-Delay: \( m \in \mathbb{R}_{\geq 0}, m < n, n' = n - m \) 
\( (E.V, n, P, x, ID) \xrightarrow{\Delta} (P, x, ID) \) 

Event-Action: \( \) 
\( (A; [P, x, ID]) \xrightarrow{\Delta} (A; [P, x, ID]) \) 

A-ChoiceL: \( \) 
\( (A; P, x, ID) \xrightarrow{\rho(A_1 \cup A_2)} (P, ID) \) 

A-ChoiceL: \( \) 
\( (A; P, x, ID) \xrightarrow{\rho(A_1 \cup A_2)} (P, ID) \) 

A-async: \( \) 
\( \rho(A_1 \cap A_2) = \emptyset, m = \max(A_1, A_2) \) 
\( (A_1; P, x, ID) \xrightarrow{\Delta} (P, ID) \) 

A-async: \( \) 
\( \rho(A_1 \cap A_2) = \emptyset, m = \max(A_1, A_2) \) 
\( (A_1; P, x, ID) \xrightarrow{\Delta} (P, ID) \) 

P-destroy: \( \) 
\( (DONE; P, x, ID) \xrightarrow{\Delta} (P, x, ID) \) 

P-destroy: \( \) 
\( (DONE; P, x, ID) \xrightarrow{\Delta} (P, x, ID) \) 

P-create: \( \) 
\( P, x, ID) \xrightarrow{\Delta} (P, x, ID) \) 

P-create: \( \) 
\( P, x, ID) \xrightarrow{\Delta} (P, x, ID) \) 

IV. TRANSLATION OF PACOR TO PSA

In order to analyze PACOR models automatically, we define a translation rewriting any PACOR description in terms of UPPAAL time automata, while UPPAAL and UPPAAL SMC tools can be applied to simulate the system execution and check the underlying properties. To this end, we consider timed automata using stopwatches [5], often called Prioritized Stopwatch Automata (PSA). Roughly speaking, stopwatches are clocks that can be stopped and resumed at any time, without reinitialization, during the system execution.

A. Parametrized Stopwatch Automata

The stopwatch concept [5] provides a sophisticated clock mechanism to measure the execution time of preemptive tasks. Such a mechanism enables to accumulate time when the action is running, and once the action is preempted the stopwatch clock makes a pause and resumes when the corresponding action resumes its execution. Given a set variables \( \text{Var} \), by \( \mathcal{C}(\text{Var}) = \{x \in \mathbb{R} | x \in \text{Var}, v \in \mathbb{R}\} \) we define the set of variable constraints of \( \text{Var} \) where \( \preceq \in \{<, \leq, >, \geq, =\} \).

Definition 4.1 (Parameterized Stopwatch Automaton): A stopwatch automaton over a set of channels \( \Omega \) is given by a tuple \((Q, q^0, Com, C, V, V^0, \rightarrow, Act, Inv)\) where \( Q \) is a set of locations, \( q^0 \in Q \) is the initial location, function \( Com : Q \rightarrow \mathbb{B} \) states whether a location is committed or not, \( C \) is a set of stopwatch clocks, \( V \) is a set of discrete variables initialized according to the valuation \( V^0 \), \( \rightarrow \subseteq Q \times (C \cup V) \times \Omega! \cup \Omega? \cup \{\tau\} \times \Lambda \times Q \) is the transition relation where \( \Lambda : \{C \rightarrow \{0\}\} \cup \{V \rightarrow \mathbb{R}\} \) is a set of actions that reset some clocks and update some discrete variables, \( Act : Q \times C \rightarrow \mathbb{N} \) defines the set of actions that can be performed on stopwatch clocks at each location, and \( Inv : Q \rightarrow \mathbb{C}(C) \) associates to each location clock invariants.

We write \( q_1 \xrightarrow{g/\alpha} q_2 \) for a transition \((q_1, g, \alpha, q_2) \in \rightarrow\) outgoing from \( q_1 \) to \( q_2 \) guarded by \( g \), labeled with \( \alpha \) and performing the action \( \alpha \) on clocks and discrete variables. In fact, we have used a long right-arrow \((\rightarrow)\) in order to distinguish the transition relation of PSA from that of TTS \((\rightarrow)\). \( Act(q)(c) = v \) means that the first derivative of \( c \) at location \( q \) has value \( v \), which represents the rate of progress each one time unit. So, for any duration \( d \) the clock \( c \) progresses
with \( v \times d \).

Therefore, a network of PSA is a set of concurent PSA instances (processes) that can be created on the fly when it is needed. These processes are defined on the same set of channels where some clocks and variables can be shared. The dynamic creation of processes is the subject of a recent extension implemented in UPPAAL. Thus, the semantics is based on a dynamically evolving set of processes where at least one process (main) is immediately created when the system starts. For this reason, we associate to each process (template instance) an identifier \( Id \) enabling us to distinguish between the different instances of the same template. Moreover, we associate to each process a fresh variable \( loc \) of type \( Q \) stating the current location of the process. We also introduce \( f \triangleq g \) as the right overriding function where function \( g \) overrides function \( f \) for all elements in the intersection of their domains.

For all \( z \in \text{domain}(f \triangleq g) \),

\[
(f \triangleq g)(z) \triangleq \begin{cases} 
  g(z) & \text{if } z \in \text{domain}(g) \\
  f(z) & \text{if } z \in \text{domain}(f) \setminus \text{domain}(g)
\end{cases}
\]

**Definition 4.2 (Semantics of a network of PSA):** Given a network of PSA \( \langle T_0, \ldots, T_n \rangle \) defined on the same set of channels \( \Omega \) where some discrete variables and clocks can be shared (global). Assuming that \( T_0 \) is the main (root) template of our network. We associate the identifier \( Id_0 \) and variable \( loc \) to the first instance of \( T_0 \). The semantics of network \( \langle T_0, \ldots, T_n \rangle \) is given by the TTS \( \langle S, S^0, \rightarrow \rangle \) where \( S = \{ s \in \text{val}(W) | \forall i \vdash \text{Inv}_i(loc_i) \} \) is a set of valuations, each one satisfies the local invariants of the involved locations \( loc_i \), of the corresponding active processes. \( S^0 = \bigcup \{ V^0_1 \cup \{ C_i \mapsto \{0\} \} \} \cup \{ Id_0.loc \mapsto q^0 \} \). \( W = \bigcup \{ Id_0.C \} \cup \bigcup \{ Id_0.V \cup \{ loc \} \} \) is the set of discrete and continuous variables of the instances that can be created together with the newly introduced variables \( loc \). The transition relation is given by the rules of table. IV.

The TTS states of the semantics are partial functions where only variables of created objects are valued. The condition \( \text{comit}(s, Id) = \forall Id' \in s \text{ cont}_{Id}(s(Id'.loc)) \Rightarrow \text{comit}_{Id}(s(Id.loc)) \) states that if \( s \) contains a committed location, the current location of process \( Id \) should also be committed [3].

**Rule Action** of table. IV states that if there exists a process \( Id_i \) such that its current location \( Id_i.loc \) corresponds to the current reached location \( q \), and the current system state \( s \) satisfies the guard \( g \) of the PSA outgoing edge from \( q \) so the system moves to another state obtained by applying action \( a \) on state \( s \) where the current location of process \( Id \) is updated to \( q' \). Rule **Sync** describes a synchronization of 2 edges having compatible labels when the source locations match with the current system state \( s \), and both guards are satisfied. The resulting transition is labeled with internal event \( \tau \), where the receiver action \( a_j \) is applied after taking into account the update made by the sender action \( a_i \). Rule **Create** expresses the on-the-fly creation of processes. Such a feature is newly implemented in UPPAAL via statement \( \text{spawn} \). \( [T]_s \) defines an instance of template \( T \) where the template parameters are evaluated according to state \( s \). The rule associates to the newly created process a fresh identifier \( Id' \) := \text{fresh}(s) thanks to the function \( \text{Ident} \). The new instance will be immediately initialized through function \( f\text{Init} \) given by:

\[
f\text{Init}(Id', T) = \{ Id'.loc \mapsto T.q_0, \| v \in T.V \{ Id'.v \mapsto T.V^0(v) \} \| c \in T.C \{ Id'.c \mapsto 0 \} \}.
\]

Such a function consists of initializing variables and initial location according to the instantiated template declaration, whereas clocks are initialized to 0. Over the syntactic function \( \text{exit}() \) of rule **Destroy**, stating that the process execution is done, UPPAAL removes such a process from the system.

Rule **Delay** states that a delay \( d \) is allowed if the invariants of the current locations \( (s(Id'.loc)) \) of all processes \( (Id \in s) \) are still satisfied, and no one of the current locations is committed.

The time progress function \( s \oplus d \) updates the stopwatch clocks at state \( s \) by \( d \). In fact, \( d \) is the real amount of time units elapsed whereas the update of each clock depends on its rate, defined by function \( Act \). Formally, \( s \oplus d = \forall Id \in s, \forall c \in Id.C \ c := s(Id.c) + Act(Id.loc)(c) \times d \).

**B. Graphical Notations of PACoR**

The translation of PACoR to timed automata is carried out in two steps: translation of a PACoR system to a graphical PACoR model, and then translation of the gPACoR model into the corresponding timed automata model.

<table>
<thead>
<tr>
<th>Rule</th>
<th>PACoR</th>
<th>gPACoR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( p \overset{d\triangleq f}{\rightarrow} p' )</td>
<td>( p \overset{A}{\rightarrow} p' )</td>
</tr>
<tr>
<td>2</td>
<td>( p \overset{d\triangleq A{{l,u}}}{\rightarrow} p' )</td>
<td>( p \overset{A{{l,u}}}{\rightarrow} p' )</td>
</tr>
<tr>
<td>3</td>
<td>( p \overset{d\triangleq g}{\rightarrow} p' )</td>
<td>( p \overset{g}{\rightarrow} p' )</td>
</tr>
<tr>
<td>4</td>
<td>( p \overset{d\triangleq p_1 \parallel p_2}{\rightarrow} p' )</td>
<td>( p \overset{p_1 \parallel p_2}{\rightarrow} p' )</td>
</tr>
<tr>
<td>5</td>
<td>( p \overset{d\triangleq p_1 \parallel p_2}{\rightarrow} p' )</td>
<td>( p \overset{p_1 \parallel p_2}{\rightarrow} p' )</td>
</tr>
<tr>
<td>6</td>
<td>( p \overset{d\triangleq A{{l,u}} \triangle (n, p_r, p_u)}{\rightarrow} p' )</td>
<td>( p \overset{A{{l,u}} \triangle (n, p_r, p_u)}{\rightarrow} p' )</td>
</tr>
<tr>
<td>7</td>
<td>( p \overset{d\triangleq g \nabla (n, p_r, p_u)}{\rightarrow} p' )</td>
<td>( p \overset{g \nabla (n, p_r, p_u)}{\rightarrow} p' )</td>
</tr>
<tr>
<td>8</td>
<td>( \lbrack p \brack \overset{d\triangleq A{{l,u}}}{\rightarrow} p' )</td>
<td>( \lbrack p \brack \overset{A{{l,u}}}{\rightarrow} p' )</td>
</tr>
</tbody>
</table>

Table V shows PACoR syntax and the corresponding notations in gPACoR. As shown in Rule 1, a process is represented by a box with a name and a transition arrow to the definition of the process. Timed actions are depicted as a circle, called timed action node, with resource requirements \( A \), as shown in Rule 2. For timed action statements, a clock \( x \) is introduced to specify timing requirements. Using this clock, the upper bound of the execution time is represented by an invariant.
associated to the node (oval state in Rule 2) representing the timed action, and the lower bound is a guard on the outgoing transition from that node. Event actions are represented by edges from the box \( P \), as shown in Rule 3. Rule 4 and 5 show that gPACoR processes can be composed using Choice and Parallel operators. The Choice operator is represented by a choice connector + and arrows leading to possible processes, whereas the parallel composition is represented by a dashed box. The scoped timed action node, with resource requirements \( A \), is shown in Rule 6. It has 3 outgoing transitions leading to a normal process (\( P^2 \)), a time-out handler (\( P_1 \)), and an exception handler (\( P_e \)). A new clock \( y \) is introduced for the scoped timed action to measure the time elapsed (for deadline) since the scoped action is reached. Rule 7 shows the scoped event action node. It is almost the same as the scope timed action node. The event action node triggers an event \( E \) on the normal termination outgoing transition, and does not contain any resource-consuming requirements. Rule 8 shows a timed action node which is applied with the Close operator.

Table VI shows how each basic structure (transition) of gPACoR is implemented in PSA. The boxes in gPACoR represent process names and correspond to the circles in PSA. Such circles are the starting locations of the PSA model. The hexagons in both sides represent definition of actions. For a given \( P_{gPACoR} \), every PSA automaton, as shown Table VI, is given with a starting location \( P_{PSA} \). In later, all starting locations will be interpreted by the commit connector of \( UPPAAL \) because the outgoing transitions linked to the starting location of PSA should always be urgently taken. For gPACoR actions, the corresponding actions in PSA are defined according to translation rules given in this section. In fact, we only focus on the translation and implementation of gPACoR transition relation.

Rule 2-1 and 2-2 show how to translate a timed action node of gPACoR to a PSA automaton. Every single timed action node of gPACoR and its clocks is transformed to a PSA with a set of clocks. In principle, a PSA process requires a set of resources using the function \( \text{Request}(A) \) according to a resource requirement \( A \) before entering the timed action location. The PSA process should release resources, using the function \( \text{Release}(2R) \), when it exits from the timed action location. Inside a timed action node, the stopwatch \( x \) runs depending on the resource availability which is checked using \( \text{Available}(2R) \). If a process wants an exclusive (non-preemptive) use of resources, it sets itself to “non-preemptive” using \( \text{LockPreemp}(pid) \).
TABLE VI
TRANSLATION RULE 2-5

<table>
<thead>
<tr>
<th>Rule</th>
<th>gPAC</th>
<th>PSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$P_{\text{pre}}$</td>
<td>$P_{\text{psa}}$</td>
</tr>
<tr>
<td>2-1</td>
<td>$P$</td>
<td>$A$</td>
</tr>
<tr>
<td></td>
<td>$x = \text{Available}(A(t))$ &amp; $x \leq l$</td>
<td>Request($\rho(A)$)</td>
</tr>
<tr>
<td>2-2</td>
<td>$P$</td>
<td>$A$</td>
</tr>
<tr>
<td></td>
<td>$x = \text{Available}(A(t))$ &amp; $x \leq l$</td>
<td>Request($\rho(A)$)</td>
</tr>
<tr>
<td>3</td>
<td>$P$</td>
<td>$\varepsilon$</td>
</tr>
<tr>
<td>4-1</td>
<td>$P$</td>
<td>$P_1$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-2</td>
<td>$P$</td>
<td>$C$</td>
</tr>
<tr>
<td></td>
<td>$x = \text{Available}(A(t))$ &amp; $x \leq l$</td>
<td>Request($\rho(A)$)</td>
</tr>
<tr>
<td>4-3</td>
<td>$P$</td>
<td>$C$</td>
</tr>
<tr>
<td></td>
<td>$x = \text{Available}(A(t))$ &amp; $x \leq l$</td>
<td>Request($\rho(A)$)</td>
</tr>
<tr>
<td>5-1</td>
<td>$P$</td>
<td>$P_1$</td>
</tr>
<tr>
<td></td>
<td>$P_2$</td>
<td>$\text{spawn}[P_2]$</td>
</tr>
<tr>
<td>5-2</td>
<td>$P$</td>
<td>$\text{spawn}[P_1]$</td>
</tr>
</tbody>
</table>

Rule 3 shows how gPAC events are translated to a set of transitions into the corresponding PSA model. As shown in Rule 4, the Choice operator $+$ is replaced by the commit connector $\odot$ of UPPAAL. The Choice operator has alternatives of possible actions. In case of timed actions, the availability of resources should be known before the selection of an outgoing transition. Thus, as shown in Rule 4-1, all resources that the alternative timed actions require are requested, e.g. $\text{Request}(S(A_1))$, before making a choice and checked to be usable (transitions are enabled) when making the choice, e.g. $\text{Available}(\rho(A_1))$. The Parallel operator is realized by instantiating parallel composed processes, as shown in Rule 5.

In our translation, the processes instantiation can be static or on-the-fly. The static creation is implemented by a special event, $\text{Spawn}[pid]$, whereas the dynamic instantiation is supported by the UPPAAL statement $\text{Spawn}$ together with a template name. Rule 6 shows the translation of a scoped timed action of gPAC. According to whether the action is preemptive $\{S\}$ or not $\langle S \rangle$, the entering transition into the timed action location executes the function $\text{LockPreemp}(pid)$. Notice that the resource requirement $S(A_e)$ of the exception handler $P_e$ is required on the transition going to the timed action node,

TABLE VII
TRANSLATION RULE 6-10

<table>
<thead>
<tr>
<th>Rule</th>
<th>gPAC</th>
<th>PSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-1</td>
<td>$\langle S \rangle$, $\text{Stem}_0(P_e) = A_e$</td>
<td></td>
</tr>
<tr>
<td>6-2</td>
<td>$\langle S \rangle$, $\text{Stem}_0(P_e) = A_e$</td>
<td></td>
</tr>
<tr>
<td>6-3</td>
<td>$\langle S \rangle$, $\text{Stem}_0(P_e) = A_e$</td>
<td></td>
</tr>
<tr>
<td>7-1</td>
<td>$\langle S \rangle$, $\text{Stem}_0(P_e) = A_e$</td>
<td></td>
</tr>
<tr>
<td>7-2</td>
<td>$\langle S \rangle$, $\text{Stem}_0(P_e) = A_e$</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$\langle S \rangle$, $\text{Stem}_0(P_e) = A_e$</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>$\langle S \rangle$, $\text{Stem}_0(P_e) = A_e$</td>
<td></td>
</tr>
<tr>
<td>10-1</td>
<td>$\langle S \rangle$, $\text{Stem}_0(P_e) = A_e$</td>
<td></td>
</tr>
<tr>
<td>10-2</td>
<td>$\langle S \rangle$, $\text{Stem}_0(P_e) = A_e$</td>
<td></td>
</tr>
</tbody>
</table>
because the exception handler can have the same possibility to execute as the scoped timed action if it is enabled. Thus the resources requests for $P_e$ are performed before the execution of the scoped timed actions. Similarly, in case that $P_e$ is a composition of processes using the Choice operator, all alternative transitions are directly linked to the timed action location in order to make them possibly enabled when the timed action executes.

Rule 7-1 and 7-2 show the translation of the scoped event action. In Rule 7-1, the resources request of the exception handler $P_e$ is performed in the same way as in the scoped timed action. Rule 7-2 describes the case where the exception handler $P_e$ carries out an event action $e_e$. Rule 8 shows how to apply the Close operator to PSA. According to the semantics of PACoR, if a process extended with the Close operator, it adds a special resource requirement $(r, lp(A))$ to its resource requirements for the execution of its timed actions. Rule 9 and 10 show how to realize $NIL$ and DONE actions. The $NIL$ action is interpreted by a deadlock. For the DONE action, the final location can be one of two types: 1) Rule 10-1 shows the execution of DONE action, using the statement exit() of UPPAAL, in the case of dynamic process creation; 2) Rule 10-2 shows a final location for the static process creation, which has an ongoing transition labeled with the process instantiation event Spawn[pid]?

D. Composition and Instantiation of Process Models

Individual PSA automata are composed into a networked PSA system in the following way. First, every starting location for individual PSAs is replaced by a commit connector. Second, every edge leading to a final location is redirected to the starting location of the same name. PSA templates are instantiated either by static or dynamic process creation. If dynamic process creation is used, every PSA template has an initial location as shown in Fig. 3(a). Initially, only the top level process is instantiated, and other processes are instantly created when needed. If using static process creation, all processes are created at the same time and every PSA template has an initial location as shown in Fig. 3(b), except for the top level process which follows Fig. 3(a). The actual execution of a process, in case of static instantiation, begins by the instantiation event Spawn[pid] according to the Rule 5-1. Fig. 4 shows the PSA model of Example 3.1. Notice that it has the same structure as the gPACoR model of Fig 2. All boxes have been translated into initial and committed locations with names. The incoming transitions into C1 and C2 execute the function request() to request cpu, and the outgoing transitions from them call the function release() to release the resource.

**Theorem 4.1:** The TTS semantics restricted to $\tau$ and time-transitions of a PACoR system is bisimilar to the TTS associated to the PACoR translation into a network of PSA. **Proof concept.** The proof is direct and consists in checking that each TTS transition, except event transitions re-

![Fig. 4. PSA Model for Example 3.1](image-url)

Fig. 4. PSA Model for Example 3.1

Fig. 3. Initial locations of PSA
The formal semantics of PAC
This query generates the average of the maximum waiting time
timed transition system. We have provided translation rules
shows the probability distributions of the maximum waiting
time, which follow a Gaussian distribution.
Fig. 6 shows the probability distributions of the maximum waiting
time for trains according to different sets
of priorities of the tracks: if the same priority is given to all
the tracks, the average of the maximum waiting time for trains
are almost equal. However, for different priorities, the trains
running on tracks of higher priorities have shorter waiting time
than the ones running on tracks with lower priorities. Fig. 6
from PACOR to PSA which preserves the semantics. The
translation is not implemented yet, but it is designed to utilize
new features of UPPAAL, such as on-the-fly process creation.
Finally we have provided an example illustrating the complete
process from systems specification in PACOR, translation to
gPACOR, further translation to PSA and verification of system
properties using UPPAAL and UPPAAL SMC.


table VIII

| System | \[ T\text{r}n\text{R}eqP_{1,\text{pri}1} \parallel T\text{r}n\text{R}eqP_{2,\text{pri}1} \parallel ... \parallel T\text{r}n\text{R}eqP_{\text{seg},\text{pri}1} \]_{\text{seg}} \parallel \forall_{\text{seq}} \{ 1 \leq j \leq \text{seg} \} | \
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( T\text{r}n\text{R}eqP_{j,k} )</td>
<td>( \theta^{\infty}(wt, T\text{r}n\text{R}eqP_{1,k+1}{1 \leq j \leq (seg-1), \text{seq} })^{[0,\infty]} : \text{T}r\text{n}L\text{e}a\text{v}eP_{j,k} : \text{NI}L )</td>
</tr>
<tr>
<td>( T\text{r}n\text{Av}\text{r}l_{i} )</td>
<td>( \theta^{\infty} : \text{T}r\text{n}Av\text{r}l_{i} )</td>
</tr>
</tbody>
</table>

Table IX

<table>
<thead>
<tr>
<th>Case</th>
<th>(Seg = 2)</th>
<th>Case</th>
<th>(Seg = 2)</th>
<th>Case</th>
<th>(Seg = 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{pri}1 )</td>
<td>( \text{Wait Time} )</td>
<td>( \text{pri}1 )</td>
<td>( \text{Wait Time} )</td>
<td>( \text{pri}1 )</td>
<td>( \text{Wait Time} )</td>
</tr>
<tr>
<td>1</td>
<td>14.14±0.22</td>
<td>2</td>
<td>14.22±0.22</td>
<td>3</td>
<td>14.16±0.22</td>
</tr>
<tr>
<td>5</td>
<td>8.04±0.12</td>
<td>4</td>
<td>9.42±0.14</td>
<td>3</td>
<td>11.76±0.16</td>
</tr>
<tr>
<td>4</td>
<td>4.13±0.13</td>
<td>4</td>
<td>4.30±0.15</td>
<td>3</td>
<td>4.61±0.15</td>
</tr>
</tbody>
</table>

In order to check the safety of the system, first, we use the
following query:

\( A[ \text{not deadlock} ] \)

which inquires whether there is a deadlock in the system.

In addition to the analysis of the safety, UPPAAL SMC
enables us to analyze the response-time of the system. We
use the following query of UPPAAL SMC to inquire what is
the average of the maximum waiting time of the train for the
assignment of the segment:

\( E[\langle \text{simTime},\text{simCount}\rangle | \text{max:waitTime}[\text{i}]] \)

This query generates the average of the maximum waiting time
of the train for a given simulation time (\( \text{simTime} \)) and number of simulations (\( \text{simCount} \)). Table IX shows the variability of
the maximum waiting time of trains according to different sets
of priorities of the tracks; if the same priority is given to all
the tracks, the average of the maximum waiting time for trains
are almost equal. However, for different priorities, the trains
running on tracks of higher priorities have shorter waiting time
than the ones running on tracks with lower priorities. Fig. 6
shows the probability distributions of the maximum waiting
time, which follow a Gaussian distribution.

VI. CONCLUSION

In this paper we have defined PACOR which is an updated
and improved derivative of the classical process algebra ACSR.
The formal semantics of PACOR is given in the form of a
timed transition system. We have provided translation rules

REFERENCES

for timed automata composition. In *ATVA’11*, pages 105–119. LNCS
6996, 2011.

U. Nyman, and A. Skou. Hierarchical scheduling framework based on

uppaal for the modeling and verification of dynamic real-time systems.

shared resources with dense time and priorities. *Theoretical Computer


Xversa: An integrated graphical and textual toolset for the specification
and analysis of resource-bound real-time systems. In CAV, volume 1102

and analysis of resource-bound real-time systems. *Journal of Computer


of herschel-planck revisited using statistical model checking. In *Isola

model checking of dynamic networks of stochastic hybrid automata.


additivity axioms in timed transition systems. Technical report,

to the specification and analysis of resource-bound real-time systems.


resource demand and supply for the formal analysis of hierarchical