Workflow Soundness Verification based on Structure Theory of Petri Nets
Kamel Barkaoui, Rahma Ben Ayed, and Zohra Sbaï
Pages 51 - 61

Workflow Soundness Verification based on Structure Theory of Petri Nets

Kamel Barkaoui [1], Rahma Ben Ayed [2], and Zohra Sbaï [2]
[1] CEDRIC-CNAM, Paris, France.
barkaoui@cnam.fr
[2] SysCom-ENIT, Tunis, Tunisia.
{rahma.benayed, zohra.sbai}@enit.rnu.tn

Abstract: *Modern workflow management systems have to support tasks with complex dependency constraints and to cope with resource allocation problem. Therefore the need for analysis method to verify the correctness of workflow specification is becoming crucial. This paper exploits recent advances of structure theory of Petri nets to find efficient structural characterization of the basic soundness property. The obtained results allow the identification and analysis of workflow net classes allowing the modelling of complex synchronization and routing workflow constructs of practical need in particular in the context of collaborative management systems.*

Keywords: *workflow nets, structure theory of Petri nets, soundness verification, resource constraints.*

Received: May 1, 2006 **|** ***Revised:*** June 30, 2006 **|** ***Accepted:*** September 30, 2006

1. Introduction

The main purpose of workflow management systems (WFMSs) [15] is to support the definition, execution and control of workflow processes. A workflow process defines a set of activities and the specific order they are to be executed to achieve a common goal. During the execution of a business process, an activity can be executed multiple times, once or never; decisions on alternative routings, (i.e. choices between the execution of alternative activities) have to be made; human (e.g. employee) and/or non-human (e.g., device, software, hardware) shared resources needed for the execution of activities have to be granted and some temporal constraints or performance parameters have to be met. Approving loans, processing insurance claims, billing, processing tax declaration, hospital process are some typical workflow often supported by WFMSs. Contemporary WFMSs provide only simulation tools for validating workflow models, in particular they do not allow to check the correctness of a workflow.

Dealing with control flow of workflow processes under temporal constraints and resource allocation leads to a more complex workflow models and make crucial the need of suitable techniques and tools for their verification and validation. In this paper, we tackle with the soundness property verification, i.e. that for any case, the process termination is ensured and no anomaly is occurred (no dangling references, no deadlocks and no livelocks). At least three good reasons for choosing and using Petri nets as a workflow language [3]: formal semantics despite the graphical nature, state-based instead of (just) event-based and variety of analysis techniques. This results in a model called workflow nets (WF-nets) introduced in [3].

In this paper, we deal with two key issues in workflow verification. The first concerns the soundness property while abstracting from resources needed for the execution of activities. The second deals with the influence of resources needed for the system to work, more precisely we have to make sure that resource sharing is going correctly and that soundness property is preserved. This leads us to the strengthening of analysis methods to be used in jPnet tool presented in [13]. This work extends and generalizes the results described in [1,7,10].

In [1], the authors exploit three basic Petri nets structural characterizations for the soundness verification of workflow: free-choice nets, well-structured nets and S-coverable nets. They suggest that S-coverability is a required property any workflow should satisfy. The results presented in [1] help designers to construct correct workflows. However, the WF-nets treated are simple compared to the workflow patterns encountered in practice.

In [7], the authors introduce first the notion of structural soundness by using the CS-property [8]. In the general case, the cs-property guarantees the absence of deadlock apart from the final marking, but the soundness is not ensured. The authors characterize some sub-classes of WF-nets, namely Circuit Free WF-nets, where they establish equivalence between the CS-property and the soundness property. They give an extension of WF-nets by taking into account shared resources needed for the execution of activities and show how soundness property can be proved structurally and efficiently.

To achieve our goals, we begin with mentioning some results on the soundness characterization of workflows and the influence of resources constraints. Then, we revisit and clarify the constructs which may endanger the correctness of a workflow and establish new and efficient structural and generalized soundness characterizations based on recent results [5]. Finally, we deal with the influence of resources constraints on workflow soundness and provide necessary and sufficient structural conditions preserving the soundness property and more operational compared to those described in [10].

2. Basics of Petri nets

This section gives basic definitions and notations of Petri nets and main results of their structure theory used in this work.

2.1 Place/Transition Nets

Place/Transition nets is the standard class of Petri nets.

Definition 1. A Petri net is a tuple $N = (P, T, F, W)$ where:

1. $P \neq \phi$ is a finite set of node places;
2. $T \neq \phi$ is a finite set of node transitions;
3. $F \subseteq P \times T \cup T \times P$ is the flow relation;
4. $W : F \rightarrow \mathbb{N} \wedge [W(x, y) = 0 \Leftrightarrow (x, y) \notin F]$ is the weight function.

If $W(u) = 1 \forall u \in F$ then N is said to be ordinary net and it is denoted by $N = (P, T, F)$.

Definition 2. A marking of a Petri net N is a function $M : P \rightarrow \mathrm{N}$. The initial marking of N is denoted by M_0.

Notation 1.

$$\forall x \in P \cup T, {}^{\bullet}x = \{ y \in P \cup T | (y, x) \in F \}$$
$$x^{\bullet} = \{ y \in P \cup T | (x, y) \in F \}$$
$$\forall (p, t) \in P \times T : C(p, t) = W(t, p) - W(p, t).$$

Definition 3. A transition $t \in T$ is enabled in a marking M (denoted by $M[t\rangle$ if and only if $\forall p \in {}^{\bullet}t : M(p) \geq W(p, t)$.

If transition t is enabled in marking M, it can be fired, leading to a new marking M' such that: $\forall p \in P : M'(p) = M(p) + C(p, t)$.

Where C is the matrix indexed by $P \times T$ and defined by $C(p, t) = W(t, p) - W(p, t)$. It is called the incidence matrix of the net.

The firing is denoted by $M[t\rangle M'$.

The set of all markings reachable from a marking M is denoted by $[M\rangle$.

Definition 4. Let N be a Petri net and M_0 its initial marking.

1. a marking M_h is a home state if and only if $\forall M \in [M_0\rangle, M_h \in [M\rangle$;
2. (N, M_0) is reversible $\Leftrightarrow$ M_0 is a home state;
3. (N, M_0) is bounded $\Leftrightarrow$ $\forall p \in P : [\exists k \in \mathbb{N}: \forall M \in [M_0\rangle, M(p) \leq k] \Leftrightarrow [M_0\rangle$ is finite;
4. (N, M_0) is quasi-live $\Leftrightarrow$ $\forall t \in T : \exists M \in [M_0\rangle, M[t\rangle$;
5. (N, M_0) is deadlock-free $\Leftrightarrow$ $\forall M \in [M_0\rangle : \exists t \in T, M[t\rangle$;
6. (N, M_0) is live $\Leftrightarrow$ $\forall t \in T : [\forall M \in [M_0\rangle : \exists M' \in [M\rangle, M'[t\rangle]$;
7. (N, M_0) is structurally live $\Leftrightarrow$ $[\exists M_0 | (N, M_0)$ is live].

Definition 5. Let N be a Petri net. An integer vector $f, f \neq 0$, indexed by $P (f \in Z^P)$ is a P-invariant iff it satisfies ${}^t f.C = 0$.

An integer vector $g, g \neq 0$, indexed by $T (g \in \mathbb{N}^T)$ is a T-invariant iff it satisfies $C.g = 0$.

$\| f \| = \{ p \in P | f(p) \neq 0 \}$ is called the support of f.

We denote by $\| f \|^+ = \{ p \in P | f(p) > 0 \}$ and by $\| f \|^- = \{ p \in P | f(p) < 0 \}$.

N is said to be conservative iff there exists a P-invariant f such that $\| f \| = \| f \|^+ = P$.

If N is conservative then N is structurally bounded (i.e. bounded for all M_0).

Definition 6. Let $N = (P, T, F, W)$ be a Petri net. N is S-coverable if and only if

$\forall p \in P, \exists P_S \subseteq P : p \in P_S$ and the net induced by $(P_S, P_S^{\bullet} \cup {}^{\bullet}P_S)$ is a strongly connected state machine.

2.2 Controlled Siphon property

Liveness is an important behavioral property of nets. It corresponds to the absence of global or local deadlock situations. The liveness of a Petri net is closely related to the satisfying of some predicates on siphons. A siphon is a subset of places once insufficiently marked will never again get new tokens. A siphon is said to be controlled if for each reachable marking the siphon remains sufficiently marked.
We highlight here some basic definitions and propositions related to siphons.

Let (N, M_0) be a P/T system.

Definition 7. A nonempty set $S \subseteq P$ is called a siphon if and only if ${}^{\bullet}S \subseteq S^{\bullet}$. S is said minimal if and only if it contains no other siphon as a proper subset.

We denote by

$$\max_{p^{\bullet}} = \max_{t \in p^{\bullet}} W(p,t)$$
$$\min_{{}^{\bullet}p} = \min_{t \in {}^{\bullet}p} W(t,p)$$

place p is said to be non-blocking if $\min_{{}^{\bullet}p} \geq \max_{p^{\bullet}}$.
In the following, we consider P/T nets with homogeneous valuation
$\forall p \in P, \forall t, t' \in p^{\bullet}, W(p,t) = W(p,t') = W(p)$

Definition 8. Let S be a siphon of (N, M_0), S is said to be *controlled* if and only if S is marked at any reachable marking i.e.
$\forall M \in [M_0\rangle, \exists p \in S | M(p) \geq W(p)$.

Definition 9. (N, M_0) is said to be satisfying the *controlled-siphon property (**CS-property**)* if and only if all minimal siphons of (N, M_0) are controlled.

In order to check the CS-property, two main structural conditions (sufficient but not necessary) permitting to determine whether a given siphon is controlled are developed in [8]. These conditions are recalled below.

Proposition 1. Let S be a siphon of (N, M_0). If one of the two following conditions holds, then S is controlled:

1. $\exists R \subseteq S$ such that $R^{\bullet} \subseteq {}^{\bullet}R$, R is marked at M_0 and all places of R are non-blocking (siphon S is said to be containing a marked trap R).
2. $\exists$ a P-invariant $f \in Z^P$ such that $S \subseteq \|f\|$ and $\forall p \in (\|f\|^- \cap S), W(p) = 1, \|f\|^+ \subseteq S$, and $\sum_p [f(p) M_0(p)] > \sum_{p \in S} [f(p).(W(p) - 1)]$.

A siphon controlled by the first (resp. second) mean is said to be trap controlled (resp. invariant controlled).

In the case where every minimal siphon is trap controlled, CS-property is called **commoner's property**.

Let N be a [Trial mode] net, if every siphon of [Trial mode] is either trap-controlled or invariant-controlled, N is said to be satisfying **IT-CS property**.

Finally, we recall two well-known basic relations between liveness and the CS-property [8]. The first states that the CS-property is a sufficient deadlock-freeness condition, the second states that the CS-property is a necessary liveness condition.

Proposition 2. Let (N, M_0) be a P/T System. The following property holds: (N, M_0) satisfies the CS-property $\Rightarrow (N, M_0)$ is weakly live (deadlock-free).

Proposition 3. Let (N, M_0) be a P/T System. The following property holds: (N, M_0) is live $\Rightarrow (N, M_0)$ satisfies the CS-property.

Hence, for P/T systems where the CS-property is a sufficient liveness condition, there is an equivalence between liveness and CS-property.

3. Workflow nets

A Place/Transition net which models the control-flow dimension of a workflow, is called a workflow net (WF-net). Clearly, a WF-net can be used to specify the routing of cases. Tasks are modelled by transitions and causal dependencies are modelled by places and arcs.

Originally, WF-nets introduced in [3] were intended to model the execution of a single case i.e. the initial marking of N consists of a single token on the source place. Here we consider WF-nets modelling the processing of k cases ($k \in \mathbb{N}$), i.e. initial marking of N consists of k tokens on the source place [7].

Definition 10. A Petri net $N = (P, T, F, W)$ is called a workflow net (WF-net) if and only if:

1. N has one source place i (i.e. ${}^{\bullet}i = \phi$) called initial place.

2. N has one sink place f (i.e. $f^{\bullet} = \phi$) called final place.
3. for every node $n \in P \cup T$, there exists a path from i to n and a path from n to f.

The so-called soundness property of workflow as first introduced in [3] is defined as follows: For any case, the procedure will terminate eventually and the moment the procedure terminates there is a token in place o and all the other places are empty. Moreover, there should be no dead tasks, i.e., it should be possible to execute an arbitrary task by following the appropriate route though the WF-net.

In our case, we focus on an important consistency property called k-soundness. It means the proper termination of the k-cases execution and the lack of tasks or conditions which do not contribute to the processing of cases.

We denote by initial and final markings respectively the markings $k.i$ and $k.f$ ($k \in \mathbb{N}$).

Definition 11. A WF-net $N = (P, T, F)$ is k-sound (or structurally sound) if and only if:

1. For every state *M* reachable from initial marking, there exists a firing sequence leading from state *M* to final marking.
   Formally: $\forall M \in [k.i\rangle, k.f \in [M\rangle$;
2. Final state is the only state reachable from initial state with at least *k* tokens in place *f*.
   Formally: $\forall M \in [k.i\rangle : M(f) \geq k \Rightarrow M = k.f$;
3. There are no dead transitions in $(N, k.i)$.
   Formally: $\forall t \in T, \exists M \in [k.i\rangle : M[t\rangle$.

k-soundness (or structural soundness) is a natural extension of 1-soundness [3] and was proved decidable in [7,14]. It gives rise to the concept of generalized soundness meaning k-soundness for all $k \geq 1$.

Definition 12. *N* is sound (or generalized sound) if and only if it is k-sound for all $k \in \mathbb{N}$, $k > 0$.

Generalized soundness is proved decidable in [11].

4. WF-nets Soundness verification

In this main section, using structural methods for the analysis of Petri nets, we deal first with the k-soundness property: "Given a WF-net $N = (P, T, F)$, we want to decide structurally whether *N* is k-sound" and investigate relationship between 1-soundness and soundness.

Let us recall some basic and important results related to k-soundness property and its verification.

Definition 13. Closure of WF-net. Let *N* be a WF-net, we denote by $N^* = (P^*, T^*, F^*, W)$ the *P/T* net obtained from *N* by adding transition $t*$ and defined as follows:

$P^* = P$,
$T^* = T \cup \{t^*\}$,
$F^* = F \cup \{(f, t^*), (t^*, i)\}$,
$W(u) = 1$ if $u \in F$,
$\mathrm{W}(\mathrm{f}, \mathrm{t}^*) = \mathrm{W}(\mathrm{t}^*, \mathrm{i}) = \mathrm{k}$.

N^* is called the closure of the WF-net *N* and t^* the closing transition. By (3) of definition 11, N^* is strongly connected. It is proved that k-soundness property can be reduced to liveness and boundedness of N^*.

Theorem 1. A WF-net *N* is k-sound if and only if $(N^*, k.i)$ is live and bounded (i.e. N^* is well-formed).

Proof: given in [3] for $k = 1$ and in [7] for all $k > 0$.

Proposition 4. Let *N* be a WF-net. If *N* is k-sound then $(N^*, k.i)$ is bounded and satisfies the CS-property.

Proof: Follows directly from proposition 3 and theorem 1.

To be useful in practice, we have to relate this general result to structural conditions ensuring equivalence between CS-property and liveness.

In this direction, a first result was established in [1], some subclasses of *P/T* nets for which commoner's property is a necessary and sufficient liveness condition: Free Choice (FC) nets [6] and Ensec nets [4]). For these two subclasses, well-formedness (liveness and boundedness) implies not only S-coverability but also conservativeness and each minimal siphon is a trap and its induced subnet is a strongly connected state machine.

An immediate consequence of theorem 1 is:

Corollary 1. Let *N* be a WF-net such that $N*$ is Free-Choice or an Ensec net. *N* is k-sound if and only if $(N^*, k.i)$ is conservative and satisfies commoner's property.

Example: Let us consider the WF-net N of Figure 1.

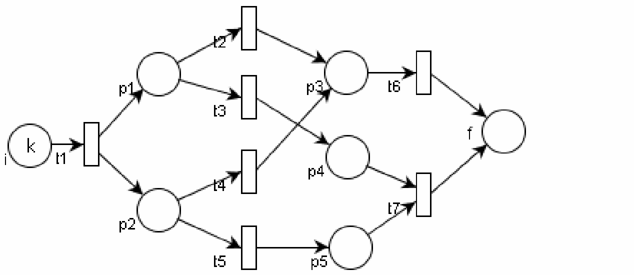

Figure 1. A not sound WF-net

N^* is a FC net satisfying the commoner's property (N^* is live) but it is not conservative (it contains a minimal siphon which is not a trap), therefore by corollary 1, N^* cannot be k-sound [11,14].

For these two subclasses efficient analysis techniques exist yielding to the following result:

Corollary 2. Let *N* be a WF-net such that N^* is a FC net or an Ensec net then k-soundness problem can be decided in polynomial time.

Proof: By corollary 1, k-soundness problem is reduced to the problem of deciding whether $(N^*, k.i)$ is conservative and satisfies commoner's property. This can be solved in polynomial time using structural and parameterized algorithms developed in [4,6,9,12].

The main interest of these two subclasses of WF-nets is that one can model the basic building blocks enacted by most WFMS's to specify workflow procedures.

In order to avoid the introduction of infinite loop, another subclass of Wf-nets namely circuit free WF-nets (CFWF-nets) was introduced in [7].

Definition 14. Let *N* be a WF-net. *N* is a Circuit Free WF-net (CFWF-net) if *N* has no circuit.

Using the concept of norm function, the following result is established in [7].

Corollary 3. Let *N* be a CFWF-net. *N* is k-sound if and only if $(N^*, k.i)$ is bounded, quasi-live and satisfies commoner's property.

Due to the particular initial marking of workflow nets where only source place is marked and due to the strong connectivity of N^*, we deduce the following basic structural soundness requirements.

Proposition 5. Let *N* be a k-sound WF-net, then the following holds:

1. all siphons of N^* contain source place *i* (and final place *f* since ${}^\bullet i = \{t^*\}$ and ${}^\bullet t^* = \{f\}$)
2. all traps of N^* contain final place *f* (and source place *i* since $f^\bullet = \{t^*\}$ and $t^{*\bullet} = \{i\}$)

Proof:

1. Otherwise, N^* contains initially an unmarked siphon *S*, CS-property is not satisfied, therefore, *N* cannot be k-sound.
2. Assume that N^* contains initially an unmarked trap *T*, since *N* is sound, property (3) of definition 11 ensures the existence of a reachable marking *M* on which *T* is marked, and therefore property (1) of same definition cannot be satisfied: contradiction with k-soundness hypothesis.

Proposition 6. Let N be a WF-net and *S* a siphon of N^*. If *S* satisfies one of the two following properties:

1. $\exists R \in S$ such that: $R^\bullet \subseteq {}^\bullet R$ (*S* contains a trap *R*).
2. $\exists$ a P-invariant *I* such that $S \subseteq \|I\|, \|I\|^+ \subseteq S$.

then *S* is controlled for all $k > 0$.

Proof:

1. Let *S* be siphon in N^* containing a trap. As source place *i* is included in *S*, *S* is trap controlled as soon as $k > 0$.
2. Let *S* be a siphon in N^* and let *I* be a P-invariant such that $S \subseteq \|I\|$, and $\|I\|^+ \subseteq S$. As source place *i* is included in *S*, the initial marking condition ((2) of proposition 1) is satisfied for all $k > 0$, therefore, *S* is invariant controlled for all $k > 0$.

It is interesting to note that these structural requirements imply soundness monotonicity with respect to initial marking of source place *i* and can ensure generalized soundness property for large class of workflow nets.

An immediate consequence of this last result is the following:

Corollary 4. Let *N* be a WF-net such that N^* is FC or Ensec net. If *N* is 1-sound then *N* is (generalized) sound.

Proof: Let *N* be a such WF-net.
By corollary 1, 1-soundness implies that every minimal siphon is a monomarked trap. By proposition 6 (1), *N* is k-sound for all $k \in \mathbb{N}$ and therefore N is sound.

Corollary 5. Let *N* be a WF-net: if *N* is an extended free choice net or an Ensec net then generalized soundness problem can be decided in polynomial time.

Proof: Same as corollary 2.

In practice, it is possible to meet sound WF-nets which are neither free-choice nor Ensec nets. In [1], it is suggested that S-coverabilty of N^* is one of the basic structural soundness requirement any workflow net should satisfy. In order to extend and generalize the previous structural characterizations of soundness, we focus here on the relationship between soundness and CS-property rather than on S-coverability, which cannot be considered as a basic requirement for siphon's control.

Our investigation based on recent advances of structure theory of Petri nets yields us to identify two new subclasses of WF-nets namely OWF-nets and KWF-nets allowing the modelling of complex synchronization and routing constructs of practical need and for which soundness can be structurally characterized and solved effectively.

4.1 Ordered Workflow nets

Definition 15. Let $N = (P,T,F,W)$ be a P/T net, $r \in P, t \in r^\bullet$. *r* is said to be a root place for *t* if and only if $r^\bullet \subseteq p^\bullet, \forall p \in {}^\bullet t$.

Definition 16. Let *N* be a P/T net and *t* be a transition of *T*. *t* is said to be an ordered transition if and only if $\forall p,q \in {}^\bullet t, p^\bullet \subseteq q^\bullet$ or $q^\bullet \subseteq p^\bullet$.

Definition 17. Let *N* be a P/T net. *N* is said to be an ordered P/T system if and only if all its transitions are ordered.

Theorem 2. Let (N, M_0) be an ordered P/T system. The two following statements are equivalent:
1. (N, M_0) satisfies the CS-property,
2. (N, M_0) is live.

This last result established in [8] highlights the structural and behavioral unity between subclasses of ordered P/T systems (not necessarily bounded) asymmetric choice systems (AC), Join Free (JF) systems, Equal Conflict (EC) systems, and Extended Free Choice (EFC) nets. Moreover, for all these subclasses, except AC nets, the CS-property is reduced to the Commoner's property and liveness monotonicity [8] holds.

Definition 18. Let *N* be a WF-net. N is called an Ordered WF-net (OWF-net) if and only if *N* is an ordered net (N^* is also an ordered net).

The class of OWF-nets contains strictly the FC-WF-nets. We extend the results related to FC and Ensec nets to OWF-nets.

Corollary 6. Let *N* be an OWF-net, *N* is k-sound if and only if N^* is bounded and satisfies CS-property.

Proof: As immediate consequence of theorem 2, and theorem 1.

Corollary 7. Let *N* be a WF-net such that N^* is a conservative OWF-net satisfying IT-CS property, then 1-soundness implies generalized soundness.

Proof: Conservativeness hypothesis ensures structural boundedness, and by proposition 6, CS-property is preserved for all $k > 0$.

Example: Consider the WF-net N of Figure 2. N^* is an ordered net (*N* is neither free choice WF-net nor an Ensec-net, it is an AC net) satisfying IT-CS property (each minimal siphon of N^* is also a trap) therefore *N* is (generalized) sound.

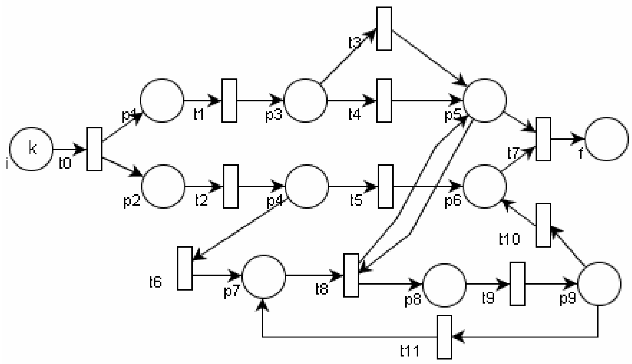

Figure 2. A sound OWF-net

4.2 K-Workflow nets

K-systems introduced in [5] can be viewed as the large class of nets for which the equivalence between CS-property, deadlock-freeness and liveness holds.

Definition 19. Let (N, M_0) be a P/T system. A reachable marking $M^* \in [M_0\rangle$ is said to be stable iff $\forall t \in T, t$ is either live or dead for M^*. Hence, T is partitioned into two subsets $T_D(M^*)$ and $T_L(M^*)$, where all transitions of $T_L(M^*)$ are live and all transitions of $T_D(M^*)$ are dead.

Definition 20. Let (N, M_0) be a P/T system. (N, M_0) is a K-system iff for all stable marking $M^*, T_D(M^*) = T$ or $T_L = T$.
The above property is called the *K-property*.

Definition 21. Let *N* be a WF-net such that N^* is a K-system, then *N* is called a K-Workflow-net (KWF-net).

Theorem 3. Let *N* be a KWF-net. *N* is sound if and only if N^* is bounded and satisfies the CS-property.

Proof: According to the equivalence between liveness and CS-property for K-systems [5] and theorem 1.

Corollary 8. For all a conservative KWF-net satisfying IT-CS property, 1-soundness implies generalized soundness.

Proof: Same as corollary 7.

The definition of KWF-nets is a behavioral one; we give two subclasses of KWF-nets namely Root WF-nets and Closure Consistent WF-nets for which the membership in the class of K-systems can be structurally and effectively done.

Definition 22. Let $N=(P,T,F,W)$ be a P/T net. *N* is a Root net if and only if $\forall t\in T,\exists$ a place $r\in P$ which is a root for *t*.

Definition 23. Let *N* be a Root net and $Root_N$ be the set of its root places. The Root Component of *N* is the net $N^*=(Root_N,T^*,F^*,W^*)$ defined as follows:

1. $T^*=Root_N^\bullet=T$,
2. $F^*\subseteq(F\cap((Root_N\times T^*)\cup(T^*\times Root_N)))$, s.t. $(p,t)\in F^*$ iff $(p,t)\in F$ and *p* is a root place for *t*, and $(t,p)\in F^*$ iff $(t,p)\in F$.
3. *W* is the restriction of *V* on F^*.

Definition 24. Let *N* be a WF-net. *N* is called a Root WF-net if and only if N^* is Root net and its Root component is bounded and strongly connected.

Definition 25. Let *N* be a WF-net. *N* is called a Closure Consistent WF-net (CCWF-net) if and only if
$\forall$ T-invariant *g* of $N^*,t^*\subseteq\|g\|$.

Theorem 4. Let *N* be a Root WF-net or a CCWF-net, *N* is k-sound if and only if N^* is bounded and satisfies the CS-property.

Proof: $(N^*,k.i)$ is a bounded K-system satisfying the CS-property, therefore N^* is bounded and live. By theorem 1, this corresponds to k-soundness.

The subclass of Root WF-nets contains strictly the FC-WF nets (Root component of N^* coincides with N^*). and the subclass of CCWF-nets contains strictly CF-WF-nets (circuit freeness in *N* is a sufficient but not necessary condition for membership in CCWF-nets).

There is no inclusion relation between Root WF-nets and CCWF-nets. For example, the Root net of Figure 3 is not a CCWF-net and the CCWF-net of Figure 4 is not a Root WF-net.

Corollary 9. For conservative Root WF-nets and CCWF-nets satisfying IT-CS property: 1-soundness implies generalized soundness

Proof: Can be proved analogously to corollary 7.

An example of Root WF-net is shown in Figure 3.

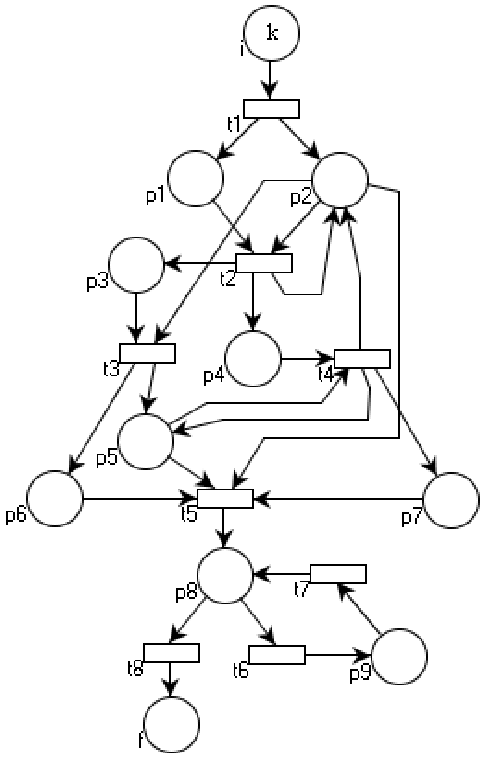

Figure 3. A sound root WF-net (not S-coverable)

The WF-net *N* of Figure 3 is a Root WF-net (not CCWF-net). N^* is Root net and its Root component $N^*-(p_2,p_5)$ is strongly connected. N^* is conservative but not S-coverable and satisfies the IT-CS property: therefore *N* is generalized sound (sound for all $k>0$).

N^* contains five minimal siphons controlled as soon as $k>0$:
$S_1=i,p_1,p_3,p_5,p_8,p_9,f$;
$S_2=i,p_1,p_3,p_6,p_8,p_9,f$;
$S_3=i,p_1,p_4,p_7,p_8,p_9,f$;
$S_4=i,p_2,p_5,p_8,p_9,f$ and
$S_5=i,p_2,p_4,p_8,p_9,f$.

The four siphons S_1,S_2,S_3,S_4 are also traps and S_5 which is not a trap is controlled by the invariant $i+p_2+p_4+f-p_3$.

One could remark that if we consider initial marking $i+p_3$ (forbidden in workflow context where only source place *i* can be initially marked) then siphon S_5 becomes non controlled and N^* is not live: the deadlock state $p_1 + p_5 + p_6$ is reachable.

Figure 4 shows an example of CCWF-net.

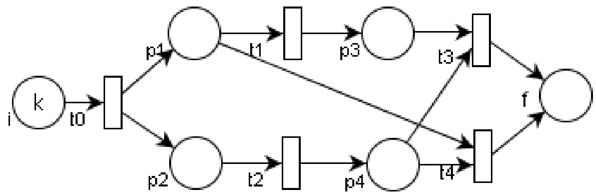

Figure 4. A sound CTWF-net

The CCWF-net *N* of Figure 4 is not Root WF-net. N^* is conservative and satisfies the IT-CS property (its two minimal siphons S_1 and S_2 are trap (or invariant) controlled as soon as $k > 0$, therefore *N* is generalized sound.

5. Soundness verification under resource allocation constraints

In previous section, we considered the soundness while abstracting from the allocation of (shared) resources needed for the execution of tasks. Here, we cope with the influence of these resources on soundness and precise necessary and/or sufficient structural conditions ensuring its preservation [7], [10].

To model properly the resource information in the initial model, only resource places (one place per type of resource) will be added. Indeed, it is assumed that WF-nets specify the handling of tasks (transitions).

Thus, it is important to note that the obtained extended model called WFR-net only limits the behavior of the initial WF-net.

Moreover the considered resources are durable. A requested resource will eventually be released and a resource released has previously been requested. Thus resources have to be preserved, along the execution process (neither creation nor destruction). Available Resources become part of case tokens when they are used. Once all cases are completed i.e. the final marking of the underlying WF-net is reached and all resources are released (become free). Hence, if we denote by $ki + R$ the initial marking of the WFR model (where *R* is the initial marking of resources places), its proper termination corresponds to final marking: $kf + R (k \in \mathbb{N})$.

According to the previous requirements, we define the WFR-net as follows:

Definition 26. A WFR-net is a tuple $N = (P \cup P_R, T, F \cup F_R, W \cup W_R)$ where:

1. $N_w = (P, T, F, W)$ is a bounded WF-net.
2. $P_R \neq \phi \wedge P \cap P_R = \phi$ (P_R is the set of resources)
3. $F_R \subseteq (P_R \times T) \cup (T \times P_R)$ (flow relation for resources)
4. $\forall u \in F_R, W_R(u) \geq 1$ (resource use)
5. $\forall r \in P_R, \exists I_r \geq 0: {}^tI_r.C = 0 \wedge \|I_r\| \cap P_R = \{r\}$ (resource preservation)

By associating a place invariant to each resource as specified in (5) of the above WFR-net definition, the resource preservation along execution process is ensured.

One can note that in WFR model, several resources can be requested/released at a same time and subnets induced by invariants are not necessarily state machines.

5.1 WFR-soundness

As a first step, we extend soundness to WFR-nets with respect to initially available resources (denoted by initial submarking *R*) [10].

Definition 27. (k,R)-soundness. Let *N* be a WFR-net. *N* is said to be (k,R)-sound if and only if

1. For every state *M* reachable from initial marking *ki+R*, there exists a firing sequence leading from state *M* to final marking *ki+R*.
   Formally: $\forall M \in [ki + R\rangle, kf + R \in [M\rangle$.
2. Final state is the only state reachable from initial state with at least *k* tokens in place *f*. Formally: $\forall M \in [ki + R\rangle : M(f) \geq k \Rightarrow M = kf + R$.
3. There are no dead transitions in *(N,ki+R)*.
   Formally: $\forall t \in T, \exists M \in [ki + R\rangle : M[t\rangle$.

Due to the invariant requirement (5) in the definition of WFR-nets, it is easy to verify that for every state *M* reachable from initial marking: $M_R \leq R$ (where the submarking M_R is the projection of *M* on resource places).

As additional resource places only limit the behavior of the underlying WF-net denoted by N_w, soundness of N_w is a necessary soundness condition of *N*.

Proposition 7. Let *N* be a WFR-net.
If *N* is (k,R)-sound then N_w is k-sound.

Proof: By definition of (k,R)-soundness, we can ensure that N_w^* is quasi-live and *k.i* is a home state, therefore, N_w^* is bounded and live which means that N_w is k-sound.

In the following, we denote by N^{**} the net obtained from WFR-net by substituting N_w by its closure N_w^*.

Theorem 5. (k,R)-soundness. Let *N* be a WFR-net. *N* is (k,R)-sound iff N^{**} is live and bounded.

Proof:
($\Rightarrow$) Let us assume that $(N, ki + R)$ is sound. We first prove that $(N^{**}, ki + R)$ is bounded.
Suppose that *N* is not bounded. Then
$\exists M_1 \in [ki + R\rangle : \exists M_2 \in [M_1\rangle, M_2 > M_1$.
As $(N, ki + R)$ is sound, we know by definition 27.(1) that there exists a sequence of transitions $\sigma \in T^* : M_1[\sigma\rangle kf + R$.
Thus $\exists M, M_2[\sigma\rangle M : M > kf + R$.
This contradicts the soundness hypothesis (definition 27.(2)).
Thus $(N, ki + R)$ is bounded and therefore $(N^{**}, ki + R)$ is bounded.

We prove now that $(N^{**}, ki + R)$ is live.
As $(N, ki + R)$ is sound, from definition 27.(1)
$\forall M \in [ki + R\rangle : kf + R \in [M\rangle$.
Then, by firing t^*, we obtain:
$\forall M \in [ki + R\rangle : ki + R \in [M\rangle$, i.e. $ki + R$ is a home state of $(N^{**}, ki + R)$. Using definition 27.(3), we conclude that all transitions are quasi-live and thus $(N^{**}, ki + R)$ is live.

($\Leftarrow$) Let us suppose that $(N^{**}, ki + R)$ is live and bounded.
Thus, $\forall M \in [ki + R\rangle : \exists M' \in [M\rangle, M'(f) \geq k$.
Let us suppose that $M' = kf + M''$,
If $M'' \neq R$, then $M'[t^*\rangle k.i + M''$, which contradicts the boundedness hypothesis of N_w^*. Therefore $M' = kf + R$ and conditions (1) and (2) of definition 27 are satisfied. Finally, the condition (3) is guaranteed by liveness.

Corollary 10. Let *N* be a WFR-net. If *N* is (k,R)-sound then $(N^{**}, ki + R)$ is bounded and satisfies the CS-property.

Definition 28. k-soundness. Let *N* be a WFR-net. *N* is said to be k-sound if and only if there exists R_0 such that *N* is (k,R)-sound for all $R \geq R_0$.

Theorem 6. Let $(N, ki + R)$ be a conservative WFR-net. If N_w is k-sound then there exists R_0 such that for all $R \geq R_0$, *N* satisfies the CS-property.

Proof: N_w is k-sound, so we only have to show that $\exists R_0$ such that any siphon in the WFR-net containing at least one resource place can be controlled as soon as $R \geq R_0$.
Let us consider such a siphon *S* which is not controlled. We denote by $I(r)$ the minimal P-invariant associated to resource *r*, and by *f(p)* the minimal P-invariant associated to $p \in N_w$ (*f(p)* exists since *N* is conservative).

Let
$$I_S = \sum_{r \in S} I(r)$$
$$Out(S) = \|I_S\| \backslash S$$
$$H_S = \sum_{p \in Out(S)} f(p)$$
$$\lambda_S = \max_{p \in Out(S) \cap \|H_S\|} (I_S(p))$$
$$Z_S = I_S - \lambda_S . H_S$$

One can always find R_0 such that the following condition is satisfied:
$${}^t Z_S . M_0 > \sum_{p \in S} (Z_S(p). \max_{p^\bullet} - 1))$$
Therefore $\forall R > R_0$: *S* is invariant controlled.

Definition 29. Soundness. Let *N* be a WFR-net. *N* is said to be sound if and only if there exists R_0 such that N is (k,R)-sound for all $k, R \geq R_0$.

Corollary 11. Let *N* be a conservative WFR-net. If *N* is sound then N_w is sound.

Now, using structural soundness characterizations established previously, we derive some classes of WFR-nets for which necessary and sufficient structural soundness condition can be obtained and decided effectively.

Definition 30. Let *N* be a WFR-net. *N* is called an OWFR-net if and only if N^{**} is an ordered net.

Definition 31. Let *N* be a WFR-net. *N* is called a Root WFR-net if and only if N^{**} is a Root net and its Root component is bounded and strongly connected.

Theorem 7. Let *N* be an OWFR-net or a Root WFR-net. *N* is k-sound if and only if N^{**} is bounded and satisfies the CS-property.

Proof: Follows directly from theorem 5 and the equivalence between CS-property and liveness for ordered systems and K-systems.

Corollary 12. For conservative OWFR-nets and Root WFR-nets satisfying IT-CS property, k-soundness implies soundness.

Proof: Same as in corollary 7.

Proposition 8. Let *N* be WFR-net. If N_w is a CCWF-net then *N* is also a CCWF-net. (*N* is called a CCWFR-net)

Proof: Note that $C.g = 0 \Rightarrow C_w.g = 0$.

So, we only have to show that $C_w.g = 0 \Rightarrow C.g = 0$.

This implication is ensured due to invariant associated to each resource place as defined in definition 26.(5).

Theorem 8. Let N be a CCWFR-net. *N* is k-sound if and only if N^{**} is bounded and satisfies the CS-property.

Proof: Similar to theorem 7.

Corollary 13. For conservative CCWFR-nets satisfying IT-CS property, k-soundness implies soundness.

Proof: Same as proof in corollary 7.

An example of conservative CCWFR-net is given in Figure 5.

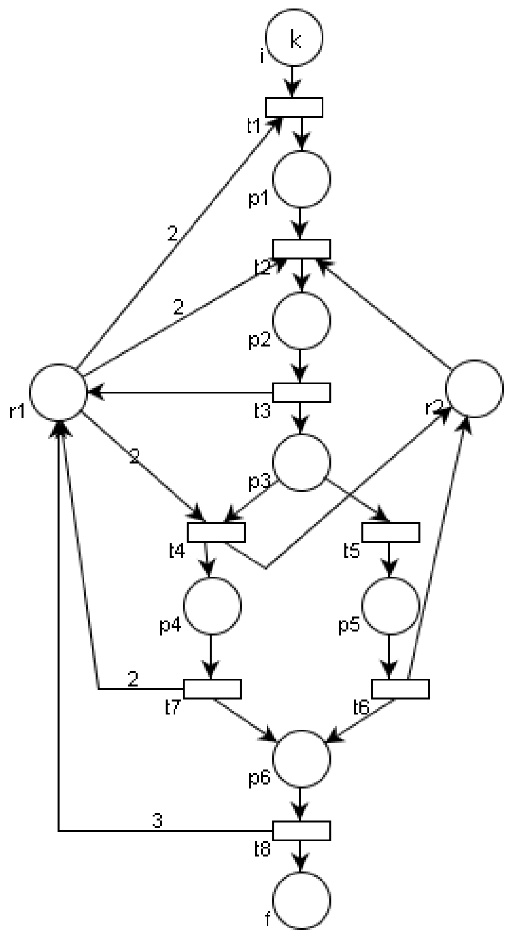

Figure 5. A CCWFR-net

In the CCWFR-net of Figure 5, the siphons are:

$S_1 = i, p_1, p_2, p_3, p_4, p_5, p_6, f$

$S_2 = r_2, p_2, p_3, p_5$

$S_3 = r_1, p_2, p_3, p_4, p_5, p_6$

Siphons S_1 and S_2 are the support of positive flows. S_1 is controlled as soon as $M_0(i) > 0$, S_2 is controlled for $M_0(r_2) > 0$.

S_3 is a strict minimal siphon (it is not a trap):

$I_{S_3} = I_{r_1} = r_1 + 2p_1 + 4p_2 + 3p_3 + 5p_4 + 3p_5 + 3p_6$

$Out(S_3) = \{p_1\}; \lambda_{S_3} = 2$

$H_{S_3} = 1 + p_1 + p_2 + p_3 + p_4 + p_5 + p_6 + f$

$Z_{S_3} = r_1 - 2i + 2p_2 + p_3 + 3p_4 + p_5 + p_6 - 2f$

Therefore S_3 is controlled for all *k* satisfying $r_1 > 2k$. So *N* is (k,R)-sound $\forall k$ and $\forall R \geq R_0$. $R_0 = (r_1, r_2) = (2k+1, 1)$; this means that *N* is (generalized) sound.

6. Conclusion and future work

In this paper we dealt with a basic property that any workflow process definition should satisfy: the soundness property. Using advanced results on structure theory of Petri nets, we have identified new subclasses of WF-nets: OWF-nets, Root WF-nets, CCWF-nets for which soundness can be structurally characterized and solved effectively. The main interest of these subclasses is that they allow to cope with resource allocation problem and to model complex synchronization and routing constructs of practical need in particular in the context of collaborative workflow management systems.

We are currently working on the development of a decision procedure for CS-property with a low complexity by exploiting the WF-nets structure.

References

[1] W.M.P. van der Aalst, "Workflow Verification: Finding Control-Flow Errors using Petri-net based Techniques", Business Process Management, LNCS N° 1806, pp. 161-183, Springer-Verlag, 2000.

[2] W.M.P. van der Aalst, "The Application of Petri Nets to Workflow Management", The Journal

of Circuits, Systems and Computers, 8(1):pp. 21–66, 1998.

[3] W.M.P. van der Aalst, "Verification of Workflow nets", ICATPN 97, LNCS N ° 1248, 1997.

[4] K. Barkaoui, J.M. Couvreur and C. Dutheillet, "On liveness in extended non self-controlling nets", ICATPN 1995, LNCS N ° 935, pp. 25-44, 1995.

[5] K. Barkaoui, J.M. Couvreur and Kais Klai, "On the Equivalence between Liveness and Deadlock-Freeness in Petri Nets", ICATPN 05, LNCS N ° 3536, Springer Ed, 2005

[6] K. Barkaoui and M. Minoux, "A polynomial-time graph algorithm to decide liveness of some basic classes of bounded Petri nets", ICATPN 92, LNCS N ° 616, pp. 62-75. Springer-Verlag Ed, June 1992.

[7] K. Barkaoui and L.Petrucci, "Structural Analysis of Workflow Nets with Shared Resources", Proc. Workflow Management: Net-based Concepts, Models, Techniques and Tools (WFM98), Lisbon, Portugal, June 1998, volume 98/7 of Computing Science Reports, pp. 82-95, Eidhoven University of Technology, 1998.

[8] K. Barkaoui and J.F. Peyre, "On liveness and controlled siphons in Petri nets", Proc. ICATPN 96, LNCS N ° 1091, Springer-Verlag Ed, 1996.

[9] J. Esparza and M. Silva, "A polynomial-time algorithm to decide liveness of bounded free choice nets", Theor. Comput. Sci., 102(1): pp. 185-205, 1992.

[10] K. van Hee, N. Sidorova and M. Voorhoeve, "Resource-Constrained Workflow nets", Fundamenta Informatica XX (2005) pp. 1-15, 2005.

[11] K. van Hee, N. Sidorova and M. Voorhoeve, "Generalized Soundness of Workflow Nets is Decidable", ICATPN 04, LNCS N ° 3099, 2004.

[12] K. Kemper and F. Bause, "An efficient polynomial-time algorithm to decide liveness and boundedness of free-choice nets", ICATPN 92, LNCS N ° 616, 1992.

[13] Z. Sbaï, R. Ben Ayed and K. Barkaoui, "Vers l'analyse des processus d'entreprise jPdl fondée sur les réseaux de Petri", In Nouvelles Tendances Technologiques en Génie Electrique et Informatique, GEI'06, pp. 171-181, Ed CPU, 2006.

[14] F.L. Tiplea and D.C. Marinescu, "Structural soundness of workflow nets is decidable", Information Processing Letters 96 (2005) pp. 54-58, 2005.

[15] WFMC, "Workflow management coalition terminology and glossary (WFMC-TC-1011)", Tech. Rep., Workflow Management Coalition, Brussals, February 1999.

Kamel Barkaoui received a Ph.D. degree in Computer Science in 1988 from the University Paris 6. He is currently a Professor at the Conservatoire National des Arts et Métiers (CNAM - Paris). His research interests include verification techniques and performance evaluation methods of concurrent and distributed systems and their applications to computer and communication systems. Dr Barkaoui has served on PCs and as PC chair for numerous international workshops and conferences. He was a guest editor of Journal of Systems and Software and has received the 1995 IEEE Int. Conf. on System Man and Cybernetics Outstanding Paper Award.

Rahma Ben Ayed received her Doctorat in Computer Science from the Faculty of Science of Tunis in 1990. She is currently a Professor at the Department of Information and Communication Technologies at the Ecole Nationale d'Ingénieurs de Tunis (ENIT) and a member of SysCom Research Laboratory. Her research interests include V&V of software systems, dependability and wireless sensor networks. She teaches several courses on programming languages, software engineering and protocol engineering.

Zohra SBAI received her Engineer Diploma in Computer Science from the Ecole Nationale d'Ingénieurs de Tunis (ENIT) in 2003 and her Master Diploma in ATS from ENIT in 2004. She is working towards his Ph.D. at the ENIT. Her research is focused on Workflow Systems, their Verification using Petri Nets and their adaptability.