Resource-Constrained Workflow nets (extended abstract)

Kees van Hee, Natalia Sidorova, and Marc Voorhoeve

Department of Mathematics and Computer Science
Eindhoven University of Technology
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
k.m.v.hee@tue.nl, n.sidorova@tue.nl, m.voorhoeve@tue.nl

Abstract. We study concurrent processes modelled as workflow Petri nets extended with resource constrains. We define structural criteria for the correctness of such models based on traps and siphons. We also define a behavioural correctness criterion called *soundness*: given a sufficient initial number of resources, all cases in the net are guaranteed to terminate successfully, no matter which schedule is used. We prove some properties of sound nets.
Keywords: Petri nets; concurrency; workflow; resources; verification.

1 Introduction

In systems engineering, coordination plays an important role on various levels. Workflow management systems coordinate the activities of human workers; the principles underlying it can also be applied to other software systems, like middleware and web services. Petri nets are well suited for modelling and verification of concurrent systems; for that reason they have proven to be a successful formalism for Workflow systems (see e.g. [2]).

Workflow systems are modelled by so-called *Workflow Nets (WF-nets)*, i.e. Petri nets with one initial and one final place and every place or transition being on a directed path from the initial to the final place. The execution of a *case* is represented as a firing sequence that starts from the initial marking consisting of a single token on the initial place. The token on the final place with no garbage (tokens) left on the other places indicates the *proper termination* of the case execution. A model is called *sound* iff every reachable marking can terminate properly.

Originally, WF-nets were intended to model the execution of a single case. In [8] and [9] we considered WF-nets modelling the execution of batches of cases in WF-nets and defined the notion of generalised soundness: "States reachable after starting with k tokens on the initial place will be able to reach the state with only k tokens on the final place, for any natural number k".

WF-nets are models emphasising the partial ordering of activities in the process and abstracting from *resources*, e.g. machines or personnel, which may further restrict the occurrence of activities. In this paper we consider the influence

of *resources* on the processing of cases in Workflow Nets. Resources are claimed and released during the execution, and the task of the designer is often seen as producing a model that uses resources in the most efficient way. We concentrate here however on fundamental correctness requirements for Resource-Constrained Workflow nets (RCWF-nets): no redundancy in the system design, resource conservation laws (every claimed resource is freed before the case terminates and no resource is created) and no deadlocks or livelocks that occur due to the lack of resources. We introduce some *structural* correctness criteria for RCWF-nets, extend the notions of soundness to RCWF-nets and give necessary conditions for soundness expressed in terms of net invariants.

The rest of the paper is organised as follows. In Section 2, we sketch the basic definitions related to Petri nets and Workflow nets. In Section 3 we introduce the notion of Resource-Constrained Workflow Nets and consider some structural correctness criteria for them. In Section 4 we define and investigate the notion of soundness for RCWF-nets. We conclude in Section 5 with discussion of the obtained results, related work and directions for future work.

2 Preliminaries

$\mathbb{N}$ denotes the set of natural numbers, $\mathbb{Z}$ the set of integers and $\mathbb{Q}$ the set of rational numbers.

Let P be a set. A *bag (multiset)* m over P is a mapping $m : P \to \mathbb{N}$. The set of all bags over P is $\mathbb{N}^P$. We use $+$ and $-$ for the sum and the difference of two bags and $=, <, >, \leq, \geq$ for comparisons of bags, which are defined in a standard way. We overload the set notation, writing $\emptyset$ for the empty bag and $\in$ for the element inclusion. We write $m = 2[p] + [q]$ for a bag m with $m(p) = 2$, $m(q) = 1$, and $m(x) = 0$ for all $x \notin \{p, q\}$.

For (finite) *sequences* of elements over a set T we use the following notation: The empty sequence is denoted with ϵ; a non-empty sequence can be given by listing its elements between angle brackets. The *Parikh vector* $\overrightarrow{\sigma}$ of a sequence σ maps every element $t \in T$ to the number of occurrences of t in σ, denoted by $\overrightarrow{\sigma}(t)$.

Transition Systems A *transition system* is a tuple $E = \langle S, Act, T \rangle$ where S is a set of *states*, Act is a finite set of *action names* and $T \subseteq S \times Act \times S$ is a *transition relation*. A *process* is a pair $\langle E, s_0 \rangle$ where E is a transition system and $s_0 \in S$ an initial state. We denote (s_1, a, s_2) from T as $s_1 \xrightarrow{a} s_2$, and we say that a leads from s_1 to s_2. For a sequence of transitions $\sigma = \langle t_1, \ldots, t_n \rangle$ we write $s_1 \xrightarrow{\sigma} s_2$ when $s_1 = s^0 \xrightarrow{t_1} s^1 \xrightarrow{t_2} \ldots \xrightarrow{t_n} s^n = s_2$, and $s_1 \xrightarrow{\sigma}$ when $s_1 \xrightarrow{\sigma} s_2$ for some s_2. In this case we say that σ is a trace of E. Finally, $s_1 \xrightarrow{*} s_2$ means that there exists a sequence $\sigma \in T^*$ such that $s_1 \xrightarrow{\sigma} s_2$. To indicate that the step a is taken in the transition system E we write $s \xrightarrow{a}_E s'$.

Given two transition systems $N_1 = \langle S_1, Act, T_1 \rangle$ and $N_2 = \langle S_2, Act, T_2 \rangle$. A relation $R \subseteq S_1 \times S_2$ is a *simulation* iff for all $s_1 \in S_1, s_2 \in S_2$, $s_1 R s_2$ and $s_1 \xrightarrow{a} s_1'$ implies that there exists a transition $s_2 \xrightarrow{a} s_2'$ such that $s_1' \mathcal{R} s_2'$.

Petri nets A *Petri net* is a tuple $N = \langle P, T, F^+, F^- \rangle$, where:

- P and T are two disjoint non-empty finite sets of *places* and *transitions* respectively, the set $P \cup T$ are the *nodes* of N;
- F^+ and F^- are mappings $(P \times T) \to \mathbb{N}$ that are *flow functions* from transitions to places and from places to transitions respectively.

$F = F^+ - F^-$ is the *incidence matrix* of net N.

We present nets with the usual graphical notation.

Markings are states (configurations) of a net. We denote the set of all markings reachable in net N from marking m as $\mathcal{R}(m)$. The set of markings from which marking m is reachable is denoted as $\mathcal{S}(m)$.

Given a transition $t \in T$, the *preset* ${}^\bullet t$ and the *postset* $t^\bullet$ of t are the *bags* of places where every $p \in P$ occurs $F^-(p,t)$ times in ${}^\bullet t$ and $F^+(p,t)$ times in $t^\bullet$. Analogously we write ${}^\bullet p, p^\bullet$ for pre- and postsets of places. We overload this notation further and apply preset and postset operations to a set B of places: ${}^\bullet B = \{t \mid \exists\, p \in B : t \in {}^\bullet p\}$ and $B^\bullet = \{t \mid \exists\, p \in B : t \in p^\bullet\}$. Note that ${}^\bullet B$ and $B^\bullet$ are not bags but sets. We will say that node n is a *source* node iff ${}^\bullet n = \emptyset$ and n is a *sink* node iff $n^\bullet = \emptyset$. A *path* of a net is a sequence $\langle x_0, \ldots, x_n \rangle$ of nodes such that $\forall\, i : 1 \leq i \leq n : x_{i-1} \in {}^\bullet x_i$.

A transition $t \in T$ is *enabled* in marking m iff ${}^\bullet t \leq m$. An enabled transition t may *fire*. This results in a new marking m' defined by $m' \stackrel{\text{def}}{=} m - {}^\bullet t + t^\bullet$. We interpret a Petri net N as a transition system/process where markings play the role of states and firings of the enabled transitions define the transition relation, namely $m + {}^\bullet t \xrightarrow{t} m + t^\bullet$. The notion of reachability for Petri nets is inherited from the transition systems. For a firing sequence σ in a net N, we define ${}^\bullet\sigma$ and $\sigma^\bullet$ respectively as $\sum_{t \in \sigma} {}^\bullet t$ and $\sum_{t \in \sigma} t^\bullet$, which are the sums of all tokens consumed/produced during the firings of σ. So $m \xrightarrow{\sigma} (m + \sigma^\bullet - {}^\bullet\sigma)$. We will use the well-known *Marking Equation Lemma*:

Lemma 1 (Marking Equation). *Given a finite firing sequence σ of a net N: $m \xrightarrow{\sigma} m'$, the following equation holds: $m' = m + F^+ \cdot \overrightarrow{\sigma} - F^- \cdot \overrightarrow{\sigma}$, or in other words, $m' = m + F \cdot \overrightarrow{\sigma}$.*

Note that the reverse is not true: not every marking m' that is representable as a sum $m + F \cdot v$ for some $v \in \mathbb{N}^T$ is reachable from the marking m.

We will write $F.X$ for the set of vectors $\{F \cdot x \mid x \in X\}$.

Traps and Siphons (see [5]) A set R of places is a *trap* if $R^\bullet \subseteq {}^\bullet R$. The trap is a *proper trap* iff it is not empty. A set R of places is a *siphon* if ${}^\bullet R \subseteq R^\bullet$. The siphon is a *proper siphon* iff it is not empty. Important properties of traps and siphons are that *marked traps remain marked* and *unmarked siphons remain unmarked* whatever transition firings would happen. As follows from the definition, traps and siphons are dual by their nature.

Invariants (see [10]) A *place invariant* is a row vector $I : P \to \mathbb{Q}$ such that $I \cdot F = 0$. When talking about invariants, we consider markings as *vectors*. The main property of place invariants is that for any two markings m_1, m_2 such that $m_1 \xrightarrow{*} m_2$ and any place invariant I holds: $I \cdot m_1 = I \cdot m_2$.

A *transition invariant* is a column vector $J : P \to \mathbb{Q}$ such that $F \cdot J = 0$. For any markings m, m' and firing sequences σ, γ, if $m \xrightarrow{\sigma} m'$ and $m \xrightarrow{\gamma} m'$, then $\overrightarrow{\sigma} - \overrightarrow{\gamma}$ is a transition invariant. This also means that for any firing sequence σ such that $m \xrightarrow{\sigma} m$, $\overrightarrow{\sigma}$ is a transition invariant.

Workflow Petri nets In this paper we primarily focus upon the *Workflow Petri nets (WF-nets)* [1]. As the name suggests, WF-nets are used to model the processing of tasks in workflow processes. The initial and final nodes indicate respectively the initial and final states of processed cases.

Definition 2. *A Petri net N is a* Workflow net (WF-net) *iff:*

1. *N has two special places: i and f. The initial place i is a source place, i.e. ${}^\bullet i = \emptyset$, and the final place f is a sink place, i.e. $f^\bullet = \emptyset$.*
2. *For any node $n \in (P \cup T)$ there exists a path from i to n and a path from n to f. (We call this property the* path property *of WF-nets.)*

We consider the processing of batches of tasks in Workflow nets, meaning that the initial place of a Workflow net may contain an arbitrary number of tokens. Our goal is to provide correctness criteria for the design of these nets. One natural correctness requirement is *proper termination*, which is called *soundness* in the WF-net theory. We will use the generalised notion of soundness for WF-nets introduced in [8]:

Definition 3. *We say that a marking $m \in \mathcal{R}(k[i])$ in a WF-net N* terminates properly *iff $m \xrightarrow{*} k[f]$.*
N is k-sound *for some $k \in \mathbb{N}$ iff for all $m \in \mathcal{R}(k[i])$, m terminates properly.*
N is sound *iff it is k-sound for all $k \in \mathbb{N}$.*

We will use terms *initial* and *final* markings for markings $k[i]$ and $k[f]$ respectively ($k \in \mathbb{N}$).

3 Resource-Constrained Workflow Nets

Workflow nets specify the handling of tasks within the organisation, factory, etc. without taking into account resources available there for the execution. We extend here the notion of WF-nets to include the information about the use of resources into the model.

A resource belongs to a type; we have one place per type in the net, where the resources are located when they are free. The resources become part of case tokens when they are occupied. We assume that resources are durable, i.e. they can be neither created nor destroyed, i.e. they are claimed during the handling procedure and then released again. By abstracting from the resource places we obtain the WF-net that we call *production net*.

Definition 4. *We will say that a WF-net* $N = \langle P_p \cup P_r, T, F_p^+ \cup F_r^+, F_p^- \cup F_r^- \rangle$ *with initial and final places* $i, f \in P_p$ *is a* Resource-Constrained Workflow net (RCWF-net) *with the set* P_p *of production places and the set* P_r *of resource places iff*

- $P_r \neq \emptyset$,
- $P_p \cap P_r = \emptyset$,
- F_p^+ *and* F_p^- *are mappings* $(P_p \times T) \to \mathbb{N}$,
- F_r^+ *and* F_r^- *are mappings* $(P_r \times T) \to \mathbb{N}$, *and*
- $N_p = \langle P_p, T, F_p^+, F_p^- \rangle$ *is a WF-net, which we call a* production *net of* N.

Note that introducing resource places will only limit the behaviour of the production net:

Lemma 5. *Let* $N = \langle (P_p \cup P_r), T, F^+, F^- \rangle$ *be an RCWF-net with* N_p *as its production net. Then* $R = \{(m_p + m_r, m_p) \mid m_p \in \mathbb{N}^{P_r} \wedge m_r \in \mathbb{N}^{P_p})\}$ *is a simulation relation.*

We start with discussing structural correctness criteria for WF-nets based on traps and siphons and then show how these criteria can be adapted to the RCWF-nets.

3.1 Redundant and Persistent Places

In [9] we introduced notions of redundant and persistent places in WF-nets and showed how to find them with the use of siphons and traps. Here we give a brief summary of the results from [9] we need here and use the notions of redundancy and persistency to analyse structural correctness of RCWF-nets.

A logical requirement for the correct design of an RCWF-net is *non-redundancy*, namely: every transition of the net can potentially fire and every place of the *production net* can potentially obtain tokens, provided that there are enough tokens on the initial place i and resource tokens. Production net N_1 in Fig. 1 does not satisfy this requirement because transition d can never fire and place s can never get tokens. So d and s are *redundant*. The *resource places* are, contrary to the production places, *redundant* by their nature, since the resource tokens cannot be created by the production net.

On the other hand, it should be possible for all places of the *production net* (except for f) to become unmarked again—otherwise the net is guaranteed to be not sound, as e.g. net N_2 in Fig. 1—place s can obtain tokens but it can never become unmarked after that, i.e. this place is *persistent*. Similarly, there should be no persistent transition in the production net, i.e. a transition producing a token to a non-final place of the production net which cannot be "moved" to a final place later on. The *resource* places, on the other hand, are *persistent*, since every claimed resource should have been released before the production process is completed. In formal terms:

Definition 6. *Let* $N = \langle P, T, F \rangle$ *be a WF-net.*
A place $p \in P$ *is* non-redundant *iff there exist* $k \in \mathbb{N}$ *and* $m \in \mathbb{N}^P$ *such that*

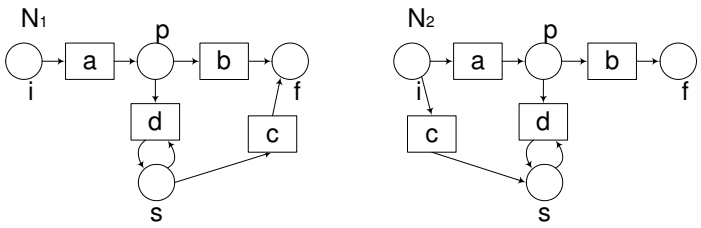

Fig. 1. Redundant and persistent places

$k[i] \xrightarrow{*} m \wedge p \in m$.
A place $p \in P$ *is* non-persistent *iff there exist* $k \in \mathbb{N}$ *and* $m \in \mathbb{N}^P$ *such that* $p \in m \wedge m \xrightarrow{*} k[f]$.
A transition t *is* non-redundant *iff there exist* $k \in \mathbb{N}$ *and* $m \in \mathbb{N}^P$ *such that* $k[i] \xrightarrow{*} m \xrightarrow{t}$.
A transition t *is* non-persistent *iff there exist* $k \in \mathbb{N}$ *and* $m, m' \in \mathbb{N}^P$ *such that* $m \xrightarrow{t} m' \xrightarrow{*} k[f]$.

It is easy to prove that the following correlation for places and transitions takes place [9]:

Lemma 7. *(1) A WF-net* N *has no redundant places iff it has no redundant transitions. (2) A WF-net* N *has no persistent places iff it has no persistent transitions.*

3.2 Structural Correctness Requirements for RCWF-Nets

Non-redundancy and non-persistency are behavioural properties. They imply though the following restrictions on the structure of the net: all proper siphons of the net should contain i and all proper traps should contain f. If N contained a proper siphon without i, the transitions consuming tokens from places of that siphon would be dead, no matter how many tokens are inserted into i. Similarly, if N contained a trap without f, the net could not terminate properly. It is not surprising that the absence of traps and siphons is a necessary condition for the correctness of the design. What is more interesting is that the absence of such siphons and traps is a *sufficient* condition for the absence of redundant and persistent places respectively: if a net has a redundant place, there exists a proper siphon without i, and if a net has a persistent place, there exists a proper trap without f, i.e. these behavioural and structural characteristics are equivalent for WF-nets [9]:

Theorem 8. *Let* $N = \langle P, T, F \rangle$ *be a WF-net. Then the following holds:*
(1) $p \in P \setminus \{i\}$ *is a redundant place iff it belongs to a siphon* $X \subseteq (P \setminus \{i\})$.
(2) p *is a persistent place iff it belongs to a trap* $X \subseteq (P \setminus \{f\})$.

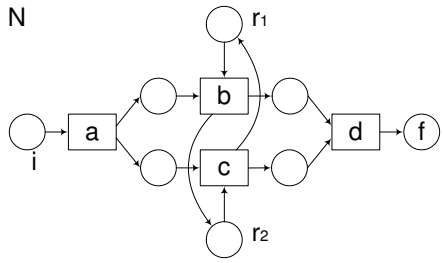

Fig. 2. An RCWF-net with dependent resource places

One can compute the largest siphon X in $P \setminus \{i\}$ in a standard manner [12]: initialize X with $P \setminus \{i\}$ and remove places that belong to $t^\bullet$ for some t such that $t \notin X^\bullet$ until the fixed point is reached. The largest trap not containing f can be computed with a similar algorithm.

Thus, let an RCWF-net N with an underlying production net N_p be given. To check the structural correctness requirements on N, we first check that the production net N_p has no redundant and persistent places, i.e. there is no any siphon in $(P_p \setminus \{i\})$ and there is no any trap in $(P_p \setminus \{f\})$. If redundant or persistent places are found, the error is reported to a designer. The production net without redundant and persistent places does not have redundant or persistent transitions either. We will call the production net that has neither redundant nor persistent places *structurally correct*.

Next, we check that all the resource places are redundant *and* persistent in net N. If this is not the case, there is an error in the design: resources can be created or destroyed during the processing. If the design is correct w.r.t. this criterion, we can proceed further with using different interpretations of "design correctness", depending on whether the resources are supposed to be *independent* or not. From the modelling point of view, resource dependence means that resource items may render to resource items of another type during the processing. We illustrate the notion of resource dependence with net N in Figure 2. A firing of transition b moves a resource from the resource place r_1 to the resource place r_2 while firing of transition c moves a resource from the resource place r_2 to the resource place r_1. Thus, during the processing of a task in the net $(N, [i]+[r_1]+[r_2])$ the resources r_1 and r_2 trade places. We call such resources *dependent*. Note that r_1 (r_2) is redundant and persistent in net N, but it is neither redundant nor persistent in the net obtained from N by projecting out place r_2 (r_1 respectively).

We will say that a resource r is *independent* of other resources in an RCWF-net $N = \langle P_p \cup P_r, T, F_p^+ \cup F_r^+, F_p^- \cup F_r^- \rangle$ with a structurally correct production net N_p iff projecting out all resource places except for r leads to an RCWF-net where place r is a resource place again, i.e. it is both redundant and persistent. We expect the designer to indicate which resource places in the net are supposed

to model independent resources; then the check whether they are independent indeed can be easily done by calculating traps and siphons.

4 Soundness of Resource-Constrained Workflow Nets

Soundness in WF-nets is the property that says that every marking reachable from an initial marking with k tokens on the initial place terminates properly, i.e. it can reach a marking with k tokens on the final place, for an arbitrary natural number k. In the RCWF-net, the initial marking of the net is a marking with some token on the initial place and a number of tokens on the resource places. Proper termination assumes then that the resource tokens are back to their resource places and all tasks are processed correctly, i.e. all the places of N_p except for f are empty. Moreover, we want the net to work properly not only with some fixed amount of resources but also with any greater amount. The extended definition of soundness reads thus as follows:

Definition 9. *Let N be an RCWF-net with marking $m \in \mathcal{R}(k[i] + m_r)$ where $m_r \in \mathbb{N}^{P_r}$. We say that (N, m)* terminates properly *iff $m \xrightarrow{*} (k[f] + m_r)$.*
*N is (k, m_r)-*sound *for some $k \in \mathbb{N}, m_r \in \mathbb{N}^{P_r}$ iff for all $m \in \mathcal{R}(k[i] + m_r)$, (N, m) terminates properly.*
*N is k-*sound *iff there exists $m_r \in \mathbb{N}^{P_r}$ such that it is (k, m')-sound for all $m' \geq m_r$.*
N is sound *iff there exists $m_r \in \mathbb{N}^{P_r}$ such that it is (k, m')-sound for all $k \in \mathbb{N}, m' \geq m_r$.*

Any (finite) firing sequence of the production net is possible in the RCWF-net if we take a sufficiently large resource marking. Since we require a sound RCWF-net to work properly for *all* "large" resource markings, the production net has to be sound as well:

Theorem 10. *Let N be an RCWF-net. (1) If N is k-sound, the underlying production WF-net N_p is k-sound as well. (2) If N is sound, N_p is sound, too.*

Proof. (1) Assume N is k-sound (i.e. it is (k, m'_r)-sound for all markings $m'_r \in \mathbb{N}^{P_r}$ such that $m'_r \geq m_r$, for some marking $m_r \in \mathbb{N}^{P_r}$) while N_p is not k-sound. Then there exists a marking m such that $k[i] \xrightarrow{\sigma}_{N_p} m$ for some firing sequence σ and m does not terminate properly, i.e. $m \not\xrightarrow{*}_{N_p} k[f]$. Now consider a marking $m'_r = m_r + m_\sigma$ where m_σ is the projection of the marking ${}^\bullet\sigma$ in N on the places P_r. Then $k[i] + m'_r \xrightarrow{\sigma}_N m + m''_r$, where $m''_r \in \mathbb{N}^{P_r}$. Since N is k-sound, $m + m''_r \xrightarrow{*}_N k[i] + m'_r$. By Lemma 5, $m \xrightarrow{*}_{N_p} k[i]$, which contradicts to our assumption. Thus k-soundness of N implies k-soundness of N_p.
(2) can be proven analogously. □

Thus the soundness of the underlying production net is the necessary condition of soundness of the RCWF-net. We do not discuss the decision procedure for soundness of WF-nets here but refer the interested reader to [9].

Another consequence of the requirement to work correctly for all "large" markings is that any transition invariant of the closure of the production net is a transition invariant of the the closure of the RCWF-net N, where the closure is the net obtained by adding a closing transition t_c such that ${}^\bullet t_c = [f]$ and $t_c^\bullet = [i]$ RCWF-net.

Theorem 11. *Let N be a* sound *RCWF-net such that its production net N_p has no redundant transitions, and N' and N'_p be their respective closures. Then for any vector $x \in \mathbb{Z}^T$ holds:*

$$F'_p \cdot x = 0 \Leftrightarrow F' \cdot x = 0. \tag{1}$$

Proof. ($\Rightarrow$): Let $F'_p \cdot x = 0$ for some $x \in \mathbb{Z}^T$. First we prove that there exist nonempty *firing sequences* σ_1, σ_2 in N'_p such that $\vec{\sigma_1} - \vec{\sigma_2} = x$. Indeed, since N_p has no redundant transitions, for every transition t there exist a firing sequence σ_t and $k \in \mathbb{N}$ such that $k[i] \xrightarrow{\sigma_t}_{N'_p} m_t \xrightarrow{t}_{N'_p} m'_t$. Then we can choose σ_1 as the concatenation of the sequences $(\sigma_t t)^{x(t)}$ for t such that $x(t) > 0$ and $(\sigma_t)^{x(t)}$ for t such that $x(t) < 0$. For σ_2 we choose the concatenation of the sequences $(\sigma_t)^{x(t)}$ for t such that $x(t) > 0$ and $(\sigma_t t)^{x(t)}$ for t such that $x(t) < 0$. Thus $\vec{\sigma_1} - \vec{\sigma_2} = x$ and σ_1, σ_2 are firable from the marking $k = \sum_{t \in T} k_t x(t)$.

Consider markings m_1, m_2 such that $k[i] \xrightarrow{\sigma_1}_{N'_p} m_1$ and $k[i] \xrightarrow{\sigma_2}_{N'_p} m_2$. Since $F'_p \cdot x = 0$ and $\vec{\sigma_1} - \vec{\sigma_2} = x$, we have $F'_p \cdot \vec{\sigma}_1 = F'_p \cdot \vec{\sigma}_2$. By the Marking Equation Lemma, $m_1 = k[i] + F'_p \cdot \vec{\sigma}_1 = k[i] + F'_p \cdot \vec{\sigma}_2 = m_2$. We set $m = m_1 = m_2$.

Since N is sound, N_p is sound as well (Theorem 10), and thus there exists γ such that $m \xrightarrow{\gamma}_{N'_p} k[f]$. We can take a resource marking m_r large enough so that $\sigma_1\gamma, \sigma_2\gamma$ are firable in $(N', k[i] + m_r)$. Thus $k[i] + m_r \xrightarrow{\sigma_1}{}'_N m + m'_r$ and $k[i] + m_r \xrightarrow{\sigma_2}{}'_N m + m''_r$. Since N is sound and we assume m_r to be large enough, $(N, m + m'_r)$ and $(N, m + m''_r)$ terminate properly, i.e. $k[i] + m_r \xrightarrow{\sigma_1}{}'_N m + m'_r \xrightarrow{\gamma}{}'_N k[f] + m_r$ and $k[i] + m_r \xrightarrow{\sigma_2}{}'_N m + m''_r \xrightarrow{\gamma}{}'_N k[f] + m_r$. By the Marking Equation Lemma, we have then $F' \cdot (\overrightarrow{\sigma_1\gamma}) = F' \cdot (\overrightarrow{\sigma_2\gamma})$. Then $F'(\vec{\sigma}_1 - \vec{\sigma}_2) = 0$, i.e. $F' \cdot x = 0$

($\Leftarrow$): trivial, since F'_p is a submatrix of F'. □

Thus, for any sound RCWF-net, the solution space of the equation $F'_p \cdot x = 0$ is a subset of the solution space of the equation $F'_r \cdot x = 0$. On the other hand, for any RCWF-net, if $F'_p \cdot x = 0 \Leftrightarrow F' \cdot x = 0$ holds we can conclude that if no deadlock or livelock caused by the lack of resources occurs then the net terminates properly:

Theorem 12. *Let N be an RCWF-net such that its production net N_p has no redundant transitions, and for the closure nets N' and N'_p holds that for any vector $x \in \mathbb{Z}^T$, $F'_p \cdot x = 0 \Leftrightarrow F' \cdot x = 0$. Then for any $k \in \mathbb{N}, m_r \in \mathbb{N}^{P_r}, m' \in \mathbb{N}^P$, $k[i] + m_r \xrightarrow{*} k[f] + m'$ implies $m_r = m'$.*

Proof. Follows directly from Theorem 11 and Theorem 10. □

Now we will investigate properties of sound RCWF-nets w.r.t. *place invariants*. First, we define an "extended reachability" relation and show that this relation has a simple algebraic characterization for sound RCWF-nets.

Definition 13. *The* extended reachability relation $\rightsquigarrow \subseteq \mathbb{N}^P \times \mathbb{N}^P$ *between markings of an RCWF-net N is defined by*
$m \rightsquigarrow m' \Leftrightarrow \exists\, k \in \mathbb{N}, m_r \in \mathbb{N}^{P_r} : m + k[i] + m_r \xrightarrow{*} m' + k[f] + m_r$.

Note that $\xrightarrow{*} \subseteq \rightsquigarrow$ (take $k = 0$ and $m_r = \emptyset$).

For sound RCWF-nets, $\rightsquigarrow$ turns out to be equality modulo the F-lattice:

Theorem 14. *Let N be a sound RCWF-net without redundant places and let $m, m' \in \mathbb{N}^P$. Then $m \rightsquigarrow m' \Leftrightarrow m - m' \in F.\mathbb{Z}^T$.*

Proof. ($\Rightarrow$): Since N is sound, $k[f] = k[i] + F \cdot x$ for some $x \in \mathbb{N}^T$ (Lemma 1). By Definition 13 and Lemma 1, $m + m_r + k[i] = m' + m_r + k[f] + F \cdot y$ for some $y \in \mathbb{N}^T$. Hence, $m = m' + F \cdot (x + y)$.
($\Leftarrow$): Suppose $m - m' \in F.\mathbb{Z}^T$, so there exist $x, y \in \mathbb{N}^T$ such that $m - m' = (F^+ - F^-) \cdot (y - x)$. Thus, $m + F^+ \cdot x + F^- \cdot y = m' + F^- \cdot x + F^+ \cdot y$.

Since N_p has no redundant places, we can find $k > 0, m_r \in \mathbb{N}^{P_r}, m_1 \in \mathbb{N}^P$ such that $k[i] + m_r \xrightarrow{*} F^- \cdot (x + y) + m_1$. Note that every firing sequence σ with Parikh vector y is enabled in $F^- \cdot (x + y) + m_1$, and $F^- \cdot (x + y) + m_1 \xrightarrow{\sigma} F^- \cdot x + F^+ \cdot y + m_1$. Since N is sound and $k[i] + m_r \xrightarrow{*} F^- \cdot x + F^+ \cdot y + m_1$, we deduce $F^- \cdot x + F^+ \cdot y + m_1 \xrightarrow{*} k[f] + m_r$.

On the other hand, $m + k[i] + m_r \xrightarrow{*} m + F^- \cdot (x + y) + m_1 \xrightarrow{*} m + F^+ \cdot x + F^- \cdot y + m_1 = m' + F^- \cdot x + F^+ \cdot y + m_1$. Since $F^- \cdot x + F^+ \cdot y + m_1 \xrightarrow{*} k[f] + m_r$, $m + k[i] + m_r \xrightarrow{*} m' + k[f] + m_r$, i.e. $m \rightsquigarrow m'$. □

Now we can prove that for every resource place r there is a place invariant where r has a non-zero weight while i and f do have zero-weights. Let $\mathcal{I}$ be the set of all place invariants of a net N.

Theorem 15. *Let N be a sound RCWF-net and $r \in P_r$. Then there exists a place invariant $I \in \mathcal{I}$ such that $I(i) = I(f) = 0$ and $I(r) \neq 0$.*

Proof. Since $[i] + m_r \xrightarrow{*} [f] + m_r$ for some $m_r \in \mathbb{N}^{P_r}$, $I(i) = I(f)$ for any $I \in \mathcal{I}$. Suppose that for any $I \in \mathcal{I} : I(i) = 0 \Rightarrow I(r) = 0$. Since $\mathcal{I}$ is a linear space over $\mathbb{Q}$, there exists $k/\ell \in \mathbb{Q}$ such that for any place invariant $I \in \mathcal{I} : I(r) = (k/\ell)I(i)$. Since $F.\mathbb{Q}^T$ is the subspace orthogonal to $\mathcal{I}$, $k[i] - \ell[r] \in F.\mathbb{Q}^T$. By multiplying out the denominator, we deduce the existence of $k, \ell \in \mathbb{N}$ such that $k[i] - \ell[r] \in F.\mathbb{Z}^T$. By Theorem 14, we have $k[i] \rightsquigarrow \ell[r]$, so there exist $K > 0, M_r \in \mathbb{N}^{P_r}$ such that $(k + K)[i] + M_r \xrightarrow{*} \ell[r] + K[f] + M_r$. By the soundness of N, there exists a marking $M'_r \in \mathbb{N}^{P_r}$ such that any marking reached from $(k + K)[i] + M_r + M'_r$ can reach $(k + K)[f] + M_r + M'_r$. Hence, $\ell[r] + K[f] + M_r + M'_r$ can reach $(k + K)[f] + M_r + M'_r$. But $\ell[r] + K[f] + M_r + M'_r$ contains only resource places and the sink place f, so it is a deadlock. This contradicts our initial assumption, thus proving the theorem. □

In Section 3 we formulated a criterion of place independence based on a check of traps and siphons. Theorem 15 allows a different characterization of independence as well as additional correctness criteria. The place invariants of a net N constitute a linear space $\mathcal{I}$. If N is a sound RCWF-net, the invariants satisfy $I(i) = I(f)$ and we can decompose $\mathcal{I}$ into the subspaces $\mathcal{I}_P$, the production invariants, and $\mathcal{I}_R$, the resource invariants satisfying $I(i) = I(f) = 0$. If the resources are independent, we can further decompose $\mathcal{I}_R$ into subspaces $\mathcal{I}_r$ for $r \in P_r$ such that $\forall\, I \in \mathcal{I}_r, q \in P_r : I(q) \neq 0 \Leftrightarrow q = r$. A desirable property for RCWF-nets with independent resources is the existence of bases for the $\mathcal{I}_r$ having nonnegative coefficients. This property indicates that resources can only become available when released after being claimed earlier. RCWF-nets with this property are connected to the S^4PR nets of [4].

5 Conclusion

We have introduced an extension of Workflow nets: *Resource-Constrained Workflow nets (RCWF-nets)* and given a number of necessary conditions of design correctness for these nets. One condition is a structural correctness criterion that guarantees the absence of redundant and persistent places and transitions and it can be checked by using traps and siphons. The second criterion postulates that the transition invariants of the closure of a sound RCWF-net and of its underlying production net are the same. This criterion guarantees resource conservation. We showed that soundness implies the existence of a resource place invariant for all resource places, which relates sound RCWF-nets to S^4PR nets. We also defined resource dependencies and discussed how to discover them in a model.

Related work Modelling the use of resources by Petri nets and analyzing these models is an active research field. We mention research on flexible manufacturing systems (FMS) (see [7, 4, 6, 11]), where the construction of appropriate *schedules* for such models is the key issue. Our approach emphasises the construction of robust nets that are free of deadlock irrespective of the number of resources available beyond a certain minimum.

In [3] the authors consider structural analysis of Workflow nets with shared resources. Their definition of structural soundness corresponds approximately to the existence of k, m_r such that the net is (k, m_r) sound. Since we consider systems where the number of cases going through the net and the number of resources can vary, and the system should work correctly for any number of cases and resources, the results of [3] are not applicable to our case.

Future work The RCWF-nets satisfying the correctness criteria defined in this paper are not sound only if they contain a deadlock or a livelock due to a lack of resources during the production process. Soundness is decidable for RCWF-nets with a fixed number of resources by using techniques from [9] but

it is still a question whether soundness is decidable for general RCWF-nets. Another research question is finding structural patterns for building sound-by-construction RCWF-nets.

References

1. W. van der Aalst. Verification of workflow nets. In P. Azéma and G. Balbo, editors, *Application and Theory of Petri Nets 1997, ICATPN'1997*, volume 1248 of *Lecture Notes in Computer Science*. Springer-Verlag, 1997.
2. W. van der Aalst and K. van Hee. *Workflow Management: Models, Methods, and Systems*. MIT Press, 2002.
3. K. Barkaoui and L. Petrucci. Structural analysis of workflow nets with shared resources. In *Workflow management: Net-based Concepts, Models, Techniques and Tools (WFM'98)*, volume 98/7 of *Computing science reports*, pages 82–95. Eindhoven University of Technology, 1998.
4. J. Colom. The resource allocation problem in flexible manufacturing systems. In W. van der Aalst and E. Best, editors, *Application and Theory of Petri Nets 2003, ICATPN'2003*, volume 2679 of *Lecture Notes in Computer Science*, pages 23–35. Springer-Verlag, 2003.
5. F. Commoner. *Deadlocks in Petri Nets*. Applied Data Research, Inc., Wakefield, Massachusetts, Report CA-7206-2311, 1972.
6. J. Ezpeleta. Flexible manufacturing systems. In C. Girault and R. Valk, editors, *Petri nets for systems engineering*. Springer-Verlag, 2003.
7. J. Ezpeleta, J. M. Colom, and J. Martínez. A Petri net based deadlock prevention policy for flexible manufacturing systems. *IEEE Transactions on Robotics and Automation*, 11(2):173–184, 1995.
8. K. van Hee, N. Sidorova, and M. Voorhoeve. Soundness and separability of workflow nets in the stepwise refinement approach. In W. van der Aalst and E. Best, editors, *Application and Theory of Petri Nets 2003, ICATPN'2003*, volume 2679 of *Lecture Notes in Computer Science*, pages 337–356. Springer-Verlag, 2003.
9. K. van Hee, N. Sidorova, and M. Voorhoeve. Generalised soundness of workflow nets is decidable. In J. Cortadella and W. Reisig, editors, *Application and Theory of Petri Nets 2004, ICATPN'2004*, volume 3099 of *Lecture Notes in Computer Science*, pages 197–216. Springer-Verlag, 2004.
10. K. Lautenbach. *Liveness in Petri Nets*. Internal Report of the Gesellschaft für Mathematik und Datenverarbeitung, Bonn, Germany, ISF/75-02-1, 1975.
11. M. Silva and E. Turuel. Petri nets for the design and operation of manufacturing systems. *European Journal of Control*, 3(3):182–199, 1997.
12. P. Starke. *Analyse von Petri-Netz-Modellen*. Teubner, 1990.