Resilience and Home-Space for WSTS ⋆

Alain Finkel[1,2] and Mathieu Hilaire[1]

[1] Université Paris-Saclay, CNRS, ENS Paris-Saclay, LMF, Gif-sur-Yvette, France
[2] Institut Universitaire de France

Abstract. Resilience of unperfect systems is a key property for improving safety by insuring that if a system could go into a bad state then it can also leave this bad state and reach a safe state. We consider six types of resilience (one of them is the home-space property) defined by an upward closed set Safe (Safe $=\uparrow$ Safe) or a downward-closed set (Safe $=\downarrow$ Safe), and by the existence of a bound k on the length of minimal runs starting from Bad and reaching Safe, where Bad is generally the complementary of Safe. We study the decidability of each type of resilience for two kinds of models: WSTS and VASS. We first show that most of all resilience problems are undecidable for WSTS with strong compatibility (and with effective pred-basis). Then we prove the decidability of resilience for completion-post-effective ω^2-WSTS with strong compatibility (almost all known WSTS are in this class) and Safe $=\uparrow$ Safe. Moreover, some resilience properties are decidable for three other classes of WSTS : (1) WSTS with effective $\uparrow$ post* basis and Safe $=\uparrow$ Safe ; (2) ideal-effective WSTS with downward and upward compatibilities ; and (3) ideal-effective downward-compatible WSTS with Safe $=\downarrow$ Safe. Finally, we study the resilience for VASS with semi-linear subsets Bad and Safe and for variations of VASS (lossy counter machines, integer VASS and continuous VASS); most of the resilience properties are shown decidable.

Keywords: Verification, Resilience, Home-Space, Well-structured transition systems, Vector addition system with states

1 Introduction

Context. Resilience is a key notion for improving safety of unperfect systems and resilience engineering is a paradigm for safety management that focuses on systems coping with complexity and balancing productivity with safety [19]. Some systems are subjects at frequent intervals to accidents, attacks or changes. Think for instance of a supply chain, or an airport's air trafic control. In such cases, a question that arises is that of whether the system can return to its normal (safe) behavior after an accident or attack pushed it towards some kind of 'error state' and, if it can, whether it can perform the return in a satisfactory timeframe.

⋆ This work was partly done while the authors were supported by the Agence Nationale de la Recherche grant BraVAS (ANR-17-CE40-0028).

Home-spaces. In 1986, Memmi and Vautherin introduced the notion of home-space [14] for a system $\mathscr{S} = (S, \to)$ with an initial state s_0 : a subset $H \subseteq S$ is an *home-space* if $\mathsf{post}^*(s_0) \subseteq \mathsf{pred}^*(H)$. If the home-space contains a single element, this element is an *home-state*. It could be easily generalized for two subsets X, H and we say that H is an *home-space for* X if $\mathsf{post}^*(X) \subseteq \mathsf{pred}^*(H)$. In 1989, de Frutos Escrig and Johnen proved that the home-space problem (for X a singleton and H a finite union of linear sets with the same period) was decidable for VASS (only published as an internal report). In 2023, Jancar and Leroux proved the decidability of the (complete) semilinear home-space problem (X and H are both semilinear) in VASS [13].

Resiliences. The (general) resilience property for a transition system $\mathscr{S} = (S, \to)$ and a subset of states $\mathsf{Safe} \subseteq S$ consists of the following: $\mathscr{S}$ is *Safe-resilient* if $S \subseteq \mathsf{pred}^*(\mathsf{Safe})$. It can be stated as an home-space problem : $\mathscr{S}$ is Safe-resilient if $\mathsf{post}^*(S) \subseteq \mathsf{pred}^*(\mathsf{Safe})$. Similarly, $\mathscr{S}$ is Safe-state-resilient for an initial state s_0 if $\mathsf{post}^*(s_0) \subseteq \mathsf{pred}^*(\mathsf{Safe})$. We will study three decidability questions for each type of set Safe. The resilience problem is to decide whether a transition system $\mathscr{S} = (S, \to)$ is Safe-resilient (for a given subset of states $\mathsf{Safe} \subseteq S$). The resilience problem could be easily generalized for two subsets Bad and Safe by asking whether $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$. The k-resilience problem is to decide whether $S \subseteq \mathsf{pred}^{\leq k}(\mathsf{Safe})$ (for a given k) and the bounded resilience problem is to decide whether there exists an k such that $\mathscr{S}$ is Safe-k-resilient. We adapt these three definitions to state-resilience.

State of the art. In 2016, Prasad and Zuck introduced in [21] interesting definitions and results (without detailed proofs) about resilience in the framework of process algebra. They built the composition of the process and its adversary as a transition system and they gave conditions that insure that the composed transition system is an effective WSTS with both upward and reflexive downward compatibilities (and some other technical conditions). In this framework and under these hypotheses, resilience reduces to coverability which is decidable on WSTS.

In 2021, Özkan and Würdemann [18] and Özkan [17], in 2022, proved the decidability of the bounded state-resilience problem and the k-state-resilience problem for WSTS with strong compatibility and with the supplementary (strong) hypothesis that there exists an algorithm that computes a finite basis of $\uparrow \mathsf{post}^*(s)$ for all state s (called effective $\uparrow \mathsf{post}^*$ basis) in the case $\mathsf{Safe} = \uparrow \mathsf{Safe}$ and $\mathsf{Bad} = \downarrow \mathsf{Bad}$.

Remark that the reflexive downward compatibility (of an effective WSTS) hypothesis in [21] implies the existence of an algorithm that computes a finite basis of $\uparrow \mathsf{post}^*(s)$ for all state s; this provides a way to use [18] for proving the announced result by Prasad and Zuck. However, neither Prasad & Zuck nor Özkan & Würdemann established the strong relation between resilience and the home-space property.

Our contributions

– Surprinsingly, the general undecidability statements about resilience were not known neither proved. We show that resilience and state-resilience prob-

lems are both undecidable for WSTS with strong compatibility. Moreover, state-resilience, bounded-state-resilience and k-state-resilience are undecidable for strongly upward-compatible WSTS with effective pred-basis when $\mathsf{Safe} = \uparrow \mathsf{Safe}$. We made a reduction of zero-reachability in reset-VASS to state-resilience in reset-VASS.

- The three resilience problems are decidable for completion-post-effective ω^2-WSTS with strong compatibility and $\mathsf{Safe} = \uparrow \mathsf{Safe}$.
- The resilience problem is decidable for ideal-effective WSTS with $\mathsf{Safe} = \downarrow \mathsf{Safe}$ and the additional hypothesis that for all downward-closed set $D \subseteq S$, the set $\mathsf{pred}^*(D)$ is downward-closed.
- We generalize the main theorem of [18, 17] by relaxing the strong compatibility hypothesis. We also show that removing the effective $\uparrow \mathsf{post}^*$ basis hypothesis leads to undecidability. We extend and prove the main result in [21] : the three state-resilience problems are decidable for ideal-effective WSTS with downward and upward compatibilities (k-state-resilience and bounded-state-resilience are decidable for ideal-effective WSTS with strong downward compatibility).
- We study the resilience problems for VASS and variations of VASS where most of the resilience problems are shown decidable.

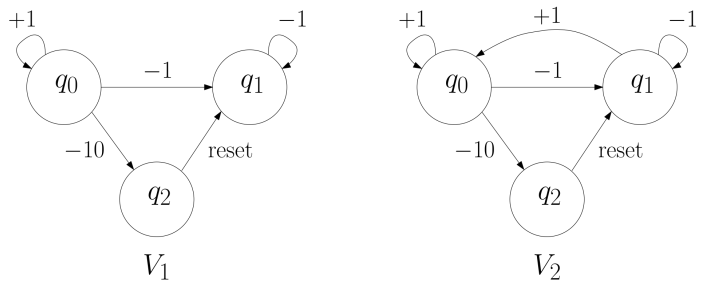

Fig. 1: Two reset-VASS with three control-states and one counter.

Example 1. (**Reset-VASS example).** Consider the reset-VASS V_1 from Figure 1. Consider first $\mathsf{Safe} = \{q_0(n) \mid n \in \mathbb{N}\}$; In this case, resilience, k-resilience and bounded resilience are not satisfied: there is no way back from q_2 or q_1 to q_0. Consider now $\mathsf{Safe} = \{q_1(0)\}$; then resilience hold: it is possible to reach $q_1(0)$ from any state of V_1. However, bounded resilience does not hold, since, for all $n \in \mathbb{N}$, from $q_1(n)$, there is no path of length less than n towards $q_1(0)$. Consider now the reset-VASS V_2, which is V_1 plus an $+1$ transition from q_1 back to q_0. In V_2, bounded resilience hold, since 6-resilience hold. Indeed, from any state with value of the counter bigger than 9, it is possible to reach q_2 in two steps or less, then use the (unique) reset transition. From $q_1(n)$ or $q_0(n)$ with

$n \in \{1,2,3,4,5,6\}$ it is possible to reach $q_1(0)$ in 6 steps or less. From $q_1(n)$ or $q_0(n)$ with $n \in \{7,8\}$ it is possible to reach $q_0(10)$ in 3 steps or less, from which $q_1(0)$ is reachable in 2 steps.

Hence we can see how adding transitions can turn a system that is not bounded resilient into one that is.

2 Well-structured transition systems and VASS

A *transition system* is a pair $\mathscr{S} = (S, \to)$ where S is a set of *states* and $\to \subseteq S \times S$ is a binary relation on the set of states, denoted as the set of *transitions*. We write $s \to s'$ to denote $(s, s') \in \to$. We write $\to^k$, $\to^+$, $\to^=$, $\to^*$ for the k-step iteration of $\to$, its transitive closure, its reflexive closure, its reflexive and transitive closure. Let $X, Y \subseteq S$ and $k \in \mathbb{N}$; we denote $X \longrightarrow^* Y$ (resp. $X \longrightarrow^{\leq k} Y$) if from all states $x \in X$ there exists a path (resp. of length smaller than k) that reaches a state $y \in Y$. The set of *(immediate) successors* of a state $s \in S$ is defined as $\mathsf{post}(s) = \{s' \in S \mid \ s \to s'\}$. The set of *(immediate) predecessors* of a state $s \in S$ is defined as $\mathsf{pred}(s) = \{s' \in S \mid \ s' \to s\}$. By iterating pred and post we obtain $\mathsf{post}^n(s) = \{s' \in S \mid \ s \to^n s'\}$ and $\mathsf{pred}^n(s) = \{s' \in S \mid \ s' \to^n s\}$. However, we are generally more interested in $\mathsf{post}^{\leq n}(s) = \bigcup_{1 \leq i \leq n} \mathsf{post}^i(s)$, $\mathsf{post}^*(s) = \bigcup_{1 \leq i} \mathsf{post}^i(s)$ and $\mathsf{pred}^{\leq n}(s) = \bigcup_{1 \leq i \leq n} \mathsf{pred}^i(s)$ and $\mathsf{pred}^*(s) = \bigcup_{1 \leq i} \mathsf{pred}^i(s)$. The *reachability problem* asks, given a transition system $\mathscr{S} = (S, \to)$, two states $s, t \in S$, whether $s \to^* t$.

A *quasi-ordering* (a qo) is any reflexive and transitive relation $\leq$ over some set X and we often write $(X, \leq)$. Given $(X, \leq)$ a quasi-ordering, an *upward-closed set* is any set $U \subseteq X$ such that if $y \geq x$ and $x \in U$ then $y \in U$. A *downward-closed set* is any set $D \subseteq X$ such that if $y \leq x$ and $x \in D$ then $y \in D$. It is an *ideal* if it is also *directed*, i.e. it is nonempty and for every $a, b \in D$, there exists $c \in D$ such that $a \leq c$ and $b \leq c$. To any subset $A \subseteq X$, we may associate its *upward-closure*, $\uparrow A = \{x \in X \mid \exists a \in A \ y \geq a\}$ and its *downward-closure*, $\downarrow A = \{x \in X \mid \exists a \in A \ y \leq a\}$. We abbreviate $\uparrow \{x\}$ (resp. $\downarrow \{x\}$) as $\uparrow x$ (resp. $\downarrow x$). A *basis* of an upward-closed set I is a set I_b such that $I = \uparrow I_b$.

A *well-quasi-ordering* (wqo) is any quasi-ordering $(X, \leq)$ such that, for any infinite sequence $x_0, x_1, x_2, \ldots$ in X, there exist indexes $i \leq j$ with $x_i \leq x_j$. Wqo admits many other equivalent formulations. As an example, $(\mathbb{N}^d, \leq)$, the set of vectors of d natural numbers (where d is finite) with component-wise order is a wqo. Quasi-orderings that have no infinite subset of mutually incomparable elements (antichains) enjoy a similar *finite decomposition* property than wqo: every downward-closed subset $D \subseteq X$ can be decomposed into a *finite* set of ideals $J_1, J_2, \ldots, J_n$ such that $D = \downarrow (J_1 \cup J_2 \cup \ldots \cup J_n)$. In what follows, a downward-closed set D is represented by its finite set of ideals (or by the minimal elements of its upward-closed complement), and an upward-closed set U is represented by its finite set of minimal elements.

Let us now recall the (most general) definition of well-structured transition systems.

Definition 1. *[7, 10] A* well-structured transition system *(WSTS)* $\mathscr{S} = (S, \to, \leq)$ *is a transition system* $(S, \to)$ *equipped with a wqo* $\leq \subseteq S \times S$ *such that the transition relation* $\to$ *is (upward) compatible with* $\leq$*, i.e., for all* $s_1, t_1, s_2 \in S$ *with* $s_1 \leq s_2$ *and* $s_1 \to t_1$*, there exists* $t_2 \in S$ *with* $t_1 \leq t_2$ *and* $s_2 \to^* t_2$*.*

We say that a WSTS $\mathscr{S}$ has *strong (upward) compatibility* when moreover for all $s_1, t_1, s_2 \in S$ with $s_1 \leq s_2$ and $s_1 \to t_1$, there exists $t_2 \in S$ with $t_1 \leq t_2$ and $s_2 \to t_2$.

Several families of formal models of processes give rise to WSTSs in a natural way with disfferent compatibilities, e.g. Petri nets when inclusion between markings is used as the well-ordering (WSTS with strong compatibility) and lossy channel systems with the subword ordering (WSTS, compatibility is not strong).

Let us recall a result of Jancar [12] that we will use as a simple definition of an ω^2-wqo: a wqo $(X, \leq)$ is an ω^2-wqo iff $(Ideals(X), \subseteq)$ is a wqo. There exists wqo that are not ω^2-wqo (see the use of the Rado ordering in [12]).

Definition 2. *[8] A WSTS* $\mathscr{S} = (S, \to, \leq)$ *is an* ω^2*-WSTS if* $(S, \leq)$ *is an* ω^2*-wqo.*

All naturally occurring WSTS are in fact ω^2-WSTS: for example, Petri nets, VASS, reset/transfer VASS, affine VASS with d counters and Q a finite set of control-states are ω^2-WSTS for the usual ordering $(= \times \leq^d)$ on $S = Q \times \mathbb{N}^d$. Similarly, lossy channel systems with d channels and Q a finite set of control-states are ω^2-WSTS for the ordering $= \times \sqsubseteq^d$ (where $\sqsubseteq$ is the subword ordering on Σ^*) on $S = Q \times (\Sigma^*)^d$.

On effectivity. Let $\mathscr{S} = (S, \to, \leq)$ be a WSTS. We say that $\mathscr{S}$ is *effective* if there exists a pair of algorithms $(M_\to, M_\leq)$ operating on $\mathbb{N} \times \mathbb{N}$ such that $M_\to$ computes the transition relation "$\to$" and $M_\leq$ the ordering relation "$\leq$". We say that $\mathscr{S}$ is *post-effective* if it is effective, and if there exists an algorithm that computes $|\mathsf{post}(x)| \in \mathbb{N} \cup \{\infty\}$ on input $x \in X$. We say that $\mathscr{S}$ has *effective pred-basis* [10, 1] if there exists an algorithm accepting any state $s \in S$ and returning $pb(s)$, a finite basis of $\uparrow \mathsf{pred}(\uparrow s)$. We say that $\mathscr{S}$ is *ideal-effective* [5] if (1) the function mapping the encoding of a state s to the encoding of the ideal $\downarrow s$ is computable; (2) inclusion of ideals is decidable; (3) the downward closure $\downarrow \mathsf{post}(I)$ expressed as a finite union of ideals is computable from the ideal I.

Now, we may recall a simple condition that insures that a finite basis of $\mathsf{pred}^*(\uparrow s)$ is computable for every $s \in S$. We will use the following property: if $\mathscr{S}$ is a WSTS with strong compatibility and $U \subseteq S$ is upward-closed, then $\mathsf{pred}(U)$, $\mathsf{pred}^k(U)$ with $k \geq 0$, and $\mathsf{pred}^*(U)$ are all upward-closed [10]. For a WSTS $\mathscr{S} = (S, \to, \leq)$ and an upward-closed set $U \subseteq S$, let us study the convergence of the sequence defined by $U_0 = U$ and $U_k = U_{k-1} \cup \mathsf{pred}(U_{k-1})$ for $k \geq 1$. When $\mathscr{S}$ has strong compatibility, the sets U_k are upward-closed and $U_k \subseteq U_{k+1}$ so we know that the sequence $(U_k)_k$ converges. Let us define the *index* of convergence of the sequence U_k as the smallest k_0 s.t. $U_k = U_{k_0}$ for all $k \geq k_0$. We may compute k_0 and we then have: $\mathsf{pred}^*(U) = U_{k_0}$. When $\mathscr{S}$ have upward-compatibility but

not strong compatibility, we can similarly compute $\mathsf{pred}^*(U)$ by studying the sequence $(\uparrow U_k)_k$ instead. With the effective pred-basis hypothesis, we obtain:

Theorem 1. *[10, 1] A finite basis of $\mathsf{pred}^*(U)$ is computable for any effective WSTS $\mathscr{S} = (S, \to, \leq)$ with effective pred-basis and any upward-closed set $U \subseteq S$ given with its finite basis B_U. Hence coverability is decidable.*

With the ideal-effective hypothesis, we obtain the decidability of coverability for a class of ordered transition systems larger than WSTS.

Theorem 2. *[5] Coverability is decidable for any ideal-effective ordered upward-compatible transition system $\mathscr{S} = (S, \to, \leq)$ where $\leq$ is without infinite antichains.*

Let us recall the definition of vector addition system with (control-)states.

Definition 3. *A* vector addition system with (control-)states (VASS) *in dimension d (d-VASS for short) is a finite $\mathbb{Z}^d$-labeled directed graph $V = (Q, T)$, where Q is the set of* control-states*, and $T \subseteq Q \times \mathbb{Z}^d \times Q$ is the set of* control-transitions*.*

Subsetquently, $Q \times \mathbb{N}^d$ is the set of states of the transition system associated with a d-VASS V. For all states $p(\mathbf{u}), q(\mathbf{v}) \in Q \times \mathbb{N}^d$ and for every control-transition $t = (p, \mathbf{z}, q)$, we write $p(\mathbf{u}) \xrightarrow{t} q(\mathbf{v})$ whenever $\mathbf{v} = \mathbf{u} + \mathbf{z} \geq \mathbf{0}$ When in the context of a d-VASS, we denote 0^d by $\mathbf{0}$.

A *vector addition system (VAS)* in dimension d (d-VAS for short) is a d-VASS where the set of control-states is a singleton; hence it can be only defined by T.

3 Resilience for WSTS

In a transition system $\mathscr{S} = (S, \to)$, we consider a subset of states $\mathsf{Safe} \subseteq S$, and its complement, Bad. The *resilience problem* (resp. the *k-resilience problem*) for $(\mathscr{S}, \mathsf{Safe})$ is to decide whether from *any* state in S, *there exists* a path (resp. a path of length smaller than or equal to k) that reaches a state in Safe. Resilience is then akin to the Home-Space problem (defined in the introduction) for the set Safe. We use the notation $S \longrightarrow^* \mathsf{Safe}$ (resp. $S \longrightarrow^{\leq k} \mathsf{Safe}$) for $\forall x \in S, \exists y \in \mathsf{Safe}$ such that $x \longrightarrow^* y$ (resp. $\forall x \in S, \exists y \in \mathsf{Safe}$ such that $x \longrightarrow^{\leq k} y$). In our framework, $\mathsf{Safe} \subseteq S$ is possibly infinite but must admit a computable finite representation : for example, downward-closed sets and upward-closed sets in wqo and semilinear sets in $\mathbb{N}^d$ have finite representations.

Let us formalize three resilience problems.

RESILIENCE (RP)
INPUT: A transition system $\mathscr{S} = (S, \to)$ and a set $\mathsf{Safe} \subseteq S$.
QUESTION: $S \longrightarrow^* \mathsf{Safe}$?

k-RESILIENCE (KRP)
INPUT: A transition system $\mathscr{S} = (S, \to), k \in \mathbb{N}$ and a set $\mathsf{Safe} \subseteq S$.

QUESTION: $S \longrightarrow^{\leq k} \mathsf{Safe}$?

Bounded resilience (BRP)
INPUT: A transition system $\mathscr{S} = (S, \rightarrow)$ and a set $\mathsf{Safe} \subseteq S$.
QUESTION: $\exists k \geq 0$ such that $S \longrightarrow^{\leq k} \mathsf{Safe}$?

These three resilience problems are decidable for finite transition systems but undecidable for (general) infinite-state transition systems. So we restrict our framework to the class of infinite-state WSTS. Since most of decidable properties in WSTS rely on the computation of upward or downward-closed sets [1, 10], we consider upward-closed or downward-closed sets Safe. Since $\mathsf{Safe} \subseteq \mathsf{pred}^*(\mathsf{Safe})$, one only need to decide whether the complement of Safe is in $\mathsf{pred}^*(\mathsf{Safe})$. From now on, we use Bad to denote the complement of Safe. In [18], the authors considered that Safe is upward-closed.

Related problems. Resilience and the home-space problem are also linked to the model-checking of basic reachability and safety formulae. In particular [23] shows that the "from-all" formula $\forall s \in X\ \exists t \in Y\ s \rightarrow^* t$ is decidable for Lossy Counter Machine (LCM) when X and Y are semi-linear sets. Other decidable formulae include "one-to-one" ($\exists s \in X\ \exists t \in Y\ s \rightarrow^* t$), and "all-to-same" ($\exists t \in Y\ \forall s \in X\ s \rightarrow^* t$), whereas "one-to-all" ($\exists s \in X\ \forall t \in Y\ s \rightarrow^* t$), "all-to-all" ($\forall s \in X\ \forall t \in Y\ s \rightarrow^* t$) and "to-all" ($\forall t \in Y\ \exists s \in X\ s \rightarrow^* t$) are undecidable (again, for LCM).

3.1 Case: Safe $=\uparrow$ Safe.

We start with the case $\mathsf{Safe} =\uparrow \mathsf{Safe}$, hence $\mathsf{Bad} =\downarrow \mathsf{Bad}$. Resilience can be viewed as a generalizeation of coverability, as it asks whether for *every* element of Bad it is possible to cover an element of the basis of Safe.

Let us recall that the *completion* [5] of a WSTS $\mathscr{S} = (S, \rightarrow, \leq)$ is the associated ordered transition system $\hat{\mathscr{S}} = (Ideals(S), \rightarrow, \subseteq)$ where $Ideals(S)$ is the set of ideals of S and $I \rightarrow J$ if J belongs to the finite ideal decomposition of $\downarrow \mathsf{post}_{\mathscr{S}}(I)$. The completion is always finitely branching but it is not necessarily a WSTS since $\subseteq$ is not necessarily a wqo. $\hat{\mathscr{S}}$ is WSTS iff $\mathscr{S} = (S, \rightarrow, \leq)$ is ω^2-WSTS (intuitively speaking, $(S, \leq)$ must not contain the Rado set). A WSTS $\mathscr{S} = (S, \rightarrow, \leq)$ is *completion-post-effective* if it is post-effective, and there exists an algorithm $M_{\downarrow}$ that computes $\downarrow s$, on input $s \in S$, and some algorithm $M_{\uparrow^c}$ that computes the ideal decomposition of $S \setminus \uparrow \{s_1, s_2, \ldots, s_m\}$, on input $s_1, s_2, \ldots, s_m \in S$. Coverability is shown decidable [Theorem 44] in [5] for completion-post-effective ω^2-WSTS (we don't need the pred-basis hypothesis).

Let us recall two other results in [5]. Proposition 30 establishes a strong relation between the runs of a WSTS $\mathscr{S} = (S, \rightarrow, \leq)$ and the runs of its completion $\hat{\mathscr{S}}$. It states that if $x \xrightarrow{k} y$ in $\mathscr{S}$ then for every ideal $I \supseteq \downarrow x$, there exists an ideal $J \supseteq \downarrow y$ such that $I \xrightarrow{k} J$ in $\hat{\mathscr{S}}$. Proposition 29 establishes that if $I \xrightarrow{k} J$ in $\hat{\mathscr{S}}$ then for every $y \in J$, there exists $x \in I$ and $y' \geq y$ such that $x \xrightarrow{k'} y'$ in

$\mathscr{S}$. Moreover, if $\mathscr{S}$ has transitive compatibility then $k' \geq k$; if $\mathscr{S}$ has strong compatibility then $k' = k$.

Theorem 3. *Let $\mathscr{S} = (S, \rightarrow, \leq)$ be a completion-post-effective ω^2-WSTS with strong compatibility and a set $\mathsf{Safe} = \uparrow \mathsf{Safe}$.* RESILIENCE, BOUNDED RESILIENCE *and k-*RESILIENCE *are decidable.*

Proof. Let $\{b_1, b_2, ..., b_m\}$ be the (unique) minimal basis of Safe and $\{J_1, J_2, ..., J_n\}$ be the ideal decomposition of Bad. The resilience problem can be reduced to the following infinite number of instances of the coverability problem in $\mathscr{S}$: for all $x \in \mathsf{Bad}$ does there exist an j such that b_j is coverable from x. Let us show how this infinite set of coverability questions can be reduced to a *finite* set of coverability questions in the completion $\hat{\mathscr{S}} = (Ideals(S), \rightarrow, \subseteq)$ of $\mathscr{S} = (S, \rightarrow, \leq)$.

Let us prove that b_j is coverable from x in $\mathscr{S}$ if and only if $\downarrow b_j$ is coverable (for inclusion) from $\downarrow x$ in $\hat{\mathscr{S}}$. Suppose that b_j is coverable from x then there exists a run $x \xrightarrow{k} y \geq b_j$. From Proposition 30, there exist an ideal J and a run $\downarrow x \xrightarrow{k} J$ where $J \supseteq \downarrow y \supseteq \downarrow b_j$ in $\hat{\mathscr{S}}$, hence $\downarrow b_j$ is covered from $\downarrow x$. Conversely, if $I \xrightarrow{k} J$ in $\hat{\mathscr{S}}$ with $\downarrow b_j \subseteq J$ then there exists $x \in I$ and $y' \geq b_j$ such that $x \xrightarrow{k} y' \geq b_j$ in $\mathscr{S}$ and then b_j is coverable from x in $\mathscr{S}$.

Hence we obtain: $\mathscr{S}$ is resilient iff for all $i = 1, .., n$ and $j = 1, ..m$, $\downarrow b_j$ is coverable from ideal J_i in $\hat{\mathscr{S}}$. Let us denote by $k_{i,j}$ the length of a covering sequence that covers $\downarrow b_j$ from J_i in $\hat{\mathscr{S}}$ and let $k_{i,j} \stackrel{\text{def}}{=} \infty$ if $\downarrow b_j$ is not coverable from J_i. Let us now define $K_{\mathscr{S}}(\mathsf{Safe}) = \max(k_{i,j} \mid i = 1, .., n \text{ and } j = 1, ..m)$.

We now have $\mathscr{S}$ is resilient iff $K_{\mathscr{S}}(\mathsf{Safe})$ is finite iff $\mathscr{S}$ is $K_{\mathscr{S}}(\mathsf{Safe})$-resilient with $K_{\mathscr{S}}(\mathsf{Safe})$ finite.

This implies that resilience and bounded resilience are equivalent to coverability. Since coverability is decidable for completion-post-effective ω^2-WSTS, we deduce that both the resilience problem and the bounded resilience problem are decidable.

Let us now show that the k-resilience problem, with $k \in \mathbb{N}$, is also decidable. Let us denote by $k'_{i,j}$ the *minimal* length of a covering sequence that covers $\downarrow b_j$ from J_i in $\hat{\mathscr{S}}$ if it exists and let $k'_{i,j} \stackrel{\text{def}}{=} \infty$ if $\downarrow b_j$ is not coverable from J_i. If $\downarrow b_j$ is coverable from J_i, we first compute an $k_{i,j}$, and then we compute $k'_{i,j}$ by iteratively checking whether there exists a sequence of length $0, 1, ..., k_{i,j} - 1$ that covers $\downarrow b_j$ from J_i until we find the minimal one which is necessarly smaller (or equal to) than $k_{i,j}$.

Let us now define $K'_{\mathscr{S}}(\mathsf{Safe}) = \max(k'_{i,j} \mid i = 1, .., n \text{ and } j = 1, ..m)$ and we deduce that $\mathscr{S}$ is k-resilient iff $k \geq K'_{\mathscr{S}}(\mathsf{Safe})$. □

Remark that the above proof doesn't make use of the property that Bad is the complement of Safe, simply using $\mathsf{Bad} = \downarrow \mathsf{Bad}$ and $\mathsf{Safe} = \uparrow \mathsf{Safe}$, thus the above results still hold in the more general case where Bad and Safe are not complements of each others.

The completion-post-effective hypothesis is needed to decide Resilience. Indeed, consider the family $\{f_j : \mathbb{N}^2 \to \mathbb{N}^2\}$ of increasing recursive functions from [9] defined as

$$f_j(n,k) = \begin{cases} (n,0) & \text{if k=0 and } \mathrm{TM}_j \text{ runs for more than n steps} \\ (n,n+k) & \text{otherwise,} \end{cases}$$

where TM_j is the j-th Turing machine (in a classical enumeration) which moreover begins by writing the integer j on its tape, and consider additionnally the function $g : \mathbb{N}^2 \to \mathbb{N}^2$ defined by $g(n,k) = (n+1,k)$. The transition system $S_j = (\mathbb{N}^2, \{f_j, g\}, \leq)$ is a WSTS and has the property that it is $\uparrow(1,1)$-resilient iff TM_j halts on input j, since $(1,1)$ is coverable from $(0,0)$ iff TM_j halts on input j. Hence there is no Turing machine which correctly determines resilience and halts whenever its input is a WSTS. Hence resilience for WSTS in general is undecidable.

3.2 Case: Safe $=\downarrow$ Safe.

Let us now consider the case $\mathsf{Safe} =\downarrow \mathsf{Safe}$ hence $\mathsf{Bad} =\uparrow \mathsf{Bad}$. It is of interest to note this case can be linked to the problem of mutual exclusion. Indeed the well-known mutual exclusion property can be modelized, in a d-VASS with d counters, by the property that a special counter c_{mutex} must be bounded by $k \geq 1$ which counts the (maximal) number of processes that are allowed to be simultaneously in the critical section. Then, the set $\mathsf{Safe} = \{c_{mutex} \leq k\} \times \mathbb{N}^{d-1}$ is downward-closed and $\mathsf{Bad} = \{c_{mutex} \geq k+1\} \times \mathbb{N}^{d-1}$ is the upward-closed complementary of Safe.

Theorem 4. Resilience *is decidable for ideal-effective WSTS with* $\mathsf{Safe} =\downarrow \mathsf{Safe}$ *and the additional hypothesis that for all downward-closed set* $D \subseteq S$*, the set* $\mathsf{pred}^*(D)$ *is downward-closed.*

Proof. By hypothesis $\mathsf{pred}^*(\mathsf{Safe})$ is downward-closed, since Safe is downward-closed. The resilience problem can be reformulated as $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$. Since $\mathscr{S} = (S, \to, \leq)$ is ideally effective, we can compute intersections of upward- or downward-closed subsets. Hence we can compute the intersection of Bad and $S \setminus \mathsf{pred}^*(\mathsf{Safe})$, which are both upward-closed. Since $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$ can be reformulated as $\mathsf{Bad} \cap (S \setminus \mathsf{pred}^*(\mathsf{Safe})) = \emptyset$ the resilience problem is decidable. □

Let us recall that a system $\mathscr{S} = (S, \to, \leq)$ is *downward compatible* [10] if for all $s_1, s_2, t_1 \in S$ with $s_2 \leq s_1$ and $s_1 \to t_1$ there exists $t_2 \in S$ with $t_2 \leq t_1$ and $s_2 \to^* t_2$.

Corollary 1. Resilience *is decidable for ideal-effective downward-compatible WSTS with* $\mathsf{Safe} =\downarrow \mathsf{Safe}$*.*

Proof. Let D be a downward-closed subset of S and let $x \in \downarrow \mathsf{pred}^*(D)$. By downward closure, there exists $y \in \mathsf{pred}^*(D)$ such that $x \leq y$. By definition of $\mathsf{pred}^*(D)$ then there exists $d \in D$, $m \geq 0$ and $(a_i)_{0 \leq i \leq m+1} \in S^{m+2}$ such that $y = a_0 \to a_1 \to a_2 \to \cdots \to a_m \to a_{m+1} = d$.

By downward compatibility $a_0 \to a_1$ implies that there exists $a'_1 \in S$ such that $a'_1 \leq a_1$ and $x \to^* a'_1$. More generally $a_i \to a_{i+1}$ and $a'_i \leq a_i$ implies the existence of $a'_{i+1} \in S$ with $a'_{i+1} \leq a_{i+1}$ and $a'_i \to^* a'_{i+1}$, and, by induction, $x \to^* a'_1 \to^* \cdots \to^* a'_m \to^* a'_{m+1} = d'$ with $d' \leq d$. Since d' belongs to D by downward closure of D, $x \in \mathsf{pred}^*(D)$. □

In the case of a ideal-effective WSTS where the additional hypothesis that for all downward-closed set $D \subseteq S$, the set $\mathsf{pred}^*(D)$ is downward-closed is not met, the above construction can provide a proof of non-resilience i.e. when $\mathsf{Bad} \cap (S \setminus \downarrow \mathsf{pred}^*(\mathsf{Safe})) \neq \emptyset$ then $\mathsf{Bad} \not\subseteq \downarrow \mathsf{pred}^*(\mathsf{Safe})$ and hence $\mathsf{Bad} \not\subseteq \mathsf{pred}^*(\mathsf{Safe})$. When $\mathsf{Bad} \cap (S \setminus \downarrow \mathsf{pred}^*(\mathsf{Safe})) = \emptyset$ however it is not enough to conclude.

In the case of a ideal-effective WSTS where the hypothesis that for all downward-closed set $D \subseteq S$, the set $\mathsf{pred}^*(D)$ is downward-closed is not met, Resilience is undecidable. This stems from the fact that it is undecidable for Minsky machines with more than one counter, which can be simulated by WSTS.

Indeed, Resilience is undecidable for Minsky machine with at least 3 counters. This is due to the undecidability of 2-counter Minsky machine termination [16, 15]. From a 2-counter Minsky machine M, one can construct a 3-counter Minsky machine M' such that machine M terminates for all inputs iff machine M' can reach $(0, 0, 0)$ from any input with at least 1 on its third counter. We build M' to simulate M until it reaches a control-state indicative of termination, then lower the first two counters until they reach 0, then, and only then, finally lower the third counter until it reaches 0. Remark that in the construction, from any input with at least 1 on its third counter, it is not possible to reach $(1, 0, 0)$, $(0, 1, 0)$ or $(1, 1, 0)$. Based on this construction, the problem of deciding whether the downward closed set $\downarrow (1, 1, 0)$ is reachable in a 3-counter Minsky machine from any input with at least 1 on its third counter is undecidable. Hence Resilience is undecidable for Minsky machines.

Executions of Minsky machines can be simulated by reset-VASS [2]. Reset-VASS extend the basic VASS model with special "reset transitions" that set to 0 some coordinates in the vector. Let us recall their definition here.

Definition 4. *A* reset-VASS *in dimension d is a finite labeled directed graph $V = (Q, T)$, where Q is the set of* control-states*, $T \subseteq Q \times Op \times Q$ is the set of* control-transitions*, and $Op = \{add(\boldsymbol{z}) \mid \boldsymbol{z} \in \mathbb{Z}^d\} \cup \{reset(i) \mid i \in \{1, \ldots, d\}\}$.*

Again $Q \times \mathbb{N}^d$ denotes the set of states of V. For every states $p(\mathbf{u}), q(\mathbf{v}) \in Q \times \mathbb{N}^d$ and every control-transition t we write $p(\mathbf{u}) \xrightarrow{t} q(\mathbf{v})$ when

- $t = (q, add(\mathbf{z}), q') \in T$ and $\mathbf{u} + \mathbf{z} = \mathbf{v} \geq 0$,
- $t = (q, reset(\gamma), q') \in T$ and $\mathbf{v}[\gamma] = 0$, and $\mathbf{v}[\gamma'] = \mathbf{u}[\gamma']$ for all $\gamma' \in \{1, \ldots, d\} \setminus \gamma$.

It is well known that reset-VASS are WSTS [6]. Since reset-VASS can simulate executions of a Minsky machine, Resilience is undecidable for reset-VASS and hence for WSTS in general as well.

Remark we did not make use of the property Bad complement of Safe, simply $\mathsf{Bad} = \uparrow \mathsf{Bad}$ and $\mathsf{Safe} = \downarrow \mathsf{Safe}$, thus the above results still hold in the more general case where Bad and Safe are not complements of each others.

Synthesis of the main decidability results

	$\mathsf{Safe} = \uparrow \mathsf{Safe}$	$\mathsf{Safe} = \downarrow \mathsf{Safe}$
RP	Decidable (Thm 3)	Decidable (Thm 4)
BRP	Decidable (Thm 3)	?
kRP	Decidable (Thm 3)	?

4 State-resilience

Resilience is a strong property that implies that from every element there must exist a path to Safe. However, when one considers a system with an initial state s_0, it could be sufficient to only ask that from $\mathsf{post}^*(s_0)$, there must exist a path to Safe. The three previous problems become:

STATE-RESILIENCE (SRP)
INPUT: A transition system $\mathscr{S} = (S, \to)$, $s \in S$ and $\mathsf{Safe} \subseteq S$.
QUESTION: $\mathsf{post}^*(s) \to^* \mathsf{Safe}$?

k-STATE-RESILIENCE (KSRP)
INPUT: A transition system $\mathscr{S} = (S, \to)$, $s \in S$, $k \geq 0$ and $\mathsf{Safe} \subseteq S$.
QUESTION: $\mathsf{post}^*(s) \longrightarrow^{\leq k} \mathsf{Safe}$?

BOUNDED-STATE-RESILIENCE (BSRP)
INPUT: A transition system $\mathscr{S} = (S, \to)$, $s \in S$ and $\mathsf{Safe} \subseteq S$.
QUESTION: $\exists k \geq 0$ such that $\mathsf{post}^*(s) \longrightarrow^{\leq k} \mathsf{Safe}$?

Remark that STATE-RESILIENCE is HOME-SPACE with input set Safe. Since these problems are undecidable for general infinite-state transition systems, we restrict our study to WSTS. As in the Section 3, we study decidability results for Safe downward-closed and upward-closed.

4.1 Case: Safe $=\uparrow$ Safe

We start with the case $\mathsf{Safe} = \uparrow \mathsf{Safe}$. Unfortunately, in this case STATE-RESILIENCE is undecidable for (general) WSTS even with strong upward-compatibility. This stems from the fact that it is undecidable in the particular case of reset-VASS, where t-liveness is both undecidable and reducible to STATE-RESILIENCE. This undecidability result furthermore implies the undecidability of the other two state resilience problems by straightforward reductions.

We now recall the undecidable [2] decision problem of *zero-reachability* in reset-VASS of dimension d, which consists in, given a reset-VASS $V = (Q, T)$, and $p(\mathbf{u}) \in Q \times \mathbb{N}^d$, deciding whether $\exists q \in Q\ p(\mathbf{u}) \to^* q(\mathbf{0})$. We reduce the zero-reachability problem to the problem of deciding whether a control-transition is live, which we then reduce to STATE-RESILIENCE. A control-transition t of a reset-VASS is *live* in a state $r(\mathbf{w})$ if for each $q(\mathbf{v}) \in \mathsf{post}^*(r(\mathbf{w}))$ there exists a state $p(\mathbf{u})$ such that $q(\mathbf{v}) \to^* p(\mathbf{u}) \xrightarrow{t}$ (t is enabled in $p(\mathbf{u})$). We say that the

whole reset-VASS is live if all its control-transitions are live. This leads to the following problem.

t-LIVENESS

INPUT: A reset-VASS $V = (Q, T)$ of dimension d, a transition $t \in T$, an initial state $s_0 \in Q \times \mathbb{N}^d$

QUESTION: Is t live in s_0 ?

Let us define the set of states such that t is enabled: $pre(t) = \{p(\mathbf{u}) \in Q \times \mathbb{N}^d \mid \exists q(\mathbf{v})$ such that $p(\mathbf{u}) \xrightarrow{t} q(\mathbf{v})\}$. Remark that $pre(t)$ is upward-closed.

Proposition 1. *t-LIVENESS is reducible to STATE-RESILIENCE in reset-VASS.*

Proof. We reformulate t-liveness in a reset-VASS (Q, T) with initial state s_0 as the following formula

$$\forall p(\mathbf{u}) \in Q \times \mathbb{N}^d,\ s_0 \to^* p(\mathbf{u}) \implies \exists q(\mathbf{v}) \in pre(t),\ p(\mathbf{u}) \to^* q(\mathbf{v})$$

The previous formula reduces itself to STATE-RESILIENCE where $\mathsf{Safe} = pre(t)$.

The following Proposition is a variation to reset-VASS of Theorem 5.5 in [20] originally stated for Petri nets, whose proof can be seen in Appendix A.

Proposition 2. *The zero reachability problem can be reduced to t-LIVENESS.*

Since the zero-reachability problem for reset-VASS is undecidable, the reduction implies t-LIVENESS is undecidable.

Since t-LIVENESS is undecidable, from Proposition 1, we deduce that STATE-RESILIENCE is undecidable for reset-VASS, which are WSTS with strong upward-compatibility. Hence STATE-RESILIENCE is undecidable for WSTS with strong upward-compatibility.

Theorem 5. STATE-RESILIENCE, BOUNDED-STATE-RESILIENCE *and* k-STATE-RESILIENCE *are undecidable for strongly compatible WSTS with effective pred-basis when* $\mathsf{Safe} = \uparrow \mathsf{Safe}$.

Proof. STATE-RESILIENCE itself is undecidable since t-LIVENESS is undecidable in reset-VASS and reducible to STATE-RESILIENCE. Additionally, in WSTS with strong compatibility and effective pred-basis, BOUNDED-STATE-RESILIENCE is reducible to k-STATE-RESILIENCE: since $\mathsf{Safe} = \uparrow \mathsf{Safe}$ and $\mathscr{S} = (S, \to, \leq)$ is a WSTS with strong compatibility, then $\mathsf{pred}^{\leq n}(\mathsf{Safe}) = \uparrow\ \mathsf{pred}^{\leq n}(\mathsf{Safe})$ for all $n \in \mathbb{N}$, and there exists $n_0 \in \mathbb{N}$ such that $\mathsf{pred}^{\leq n_0}(\mathsf{Safe}) = \uparrow \mathsf{pred}^{\leq n_0}(\mathsf{Safe}) = \uparrow \mathsf{pred}^*(\mathsf{Safe}) = \mathsf{pred}^*(\mathsf{Safe})$. We compute n_0, then iteratively check whether k-state-resilience hold for k from 0 to n_0. Furthermore, in WSTS with strong compatibility and effective pred-basis, $\mathsf{Safe} = \uparrow \mathsf{Safe}$, BOUNDED-STATE-RESILIENCE is equivalent to STATE-RESILIENCE, since $\mathsf{pred}^{\leq n_0}(\mathsf{Safe}) = \uparrow \mathsf{pred}^{\leq n_0}(\mathsf{Safe}) = \uparrow \mathsf{pred}^*(\mathsf{Safe}) = \mathsf{pred}^*(\mathsf{Safe})$. Hence the undecidability of BOUNDED-STATE-RESILIENCE and k-STATE-RESILIENCE. □

On the positive side, let us recall a result about Bounded-state-resilience (called resilience in [17, 18]).

Theorem 6. *[17, 18]* Bounded-state-resilience *and* k-state-resilience *are decidable for WSTS S with strong compatibility and such that $\uparrow \mathsf{post}^*(s)$ is computable for $s \in S$ when $\mathsf{Safe} = \uparrow \mathsf{Safe}$.*

We may immediately generalize this last result by strengthening to *unbounded* State-resilience. The proof is essentially the same than the previous one.

Corollary 2. State-resilience *is decidable for WSTS with strong compatibility and such that $\uparrow \mathsf{post}^*(s)$ is computable for $s \in S$ when $\mathsf{Safe} = \uparrow \mathsf{Safe}$.*

Proof. Since $\mathscr{S}$ is a WSTS there exists an $n_0 \in \mathbb{N}$ such that $\mathsf{pred}^*(\mathsf{Safe}) = \mathsf{pred}^{\leq n_0}(\mathsf{Safe})$. We can compute the least n_0 by iteratively computing $\mathsf{pred}^{\leq n+1}(\mathsf{Safe})$ from $\mathsf{pred}^{\leq n}(\mathsf{Safe})$, checking $\mathsf{pred}^{\leq n+1}(\mathsf{Safe}) = \mathsf{pred}^{\leq n}(\mathsf{Safe})$, returning n if that is the case. Then, because n_0-state-resilience is decidable, checking $\uparrow \mathsf{post}^*(s) \subseteq \mathsf{pred}^{\leq n}(\mathsf{Safe}) = \mathsf{pred}^*(\mathsf{Safe})$ is, and State-resilience is decidable. □

The proof of Theorem 6 rely on the computability of $\uparrow \mathsf{post}^*(s)$ and on the following lemma.

Lemma 1. *Let $A \subseteq S$, $D \subseteq S$ be a downward-closed set and $U \subseteq S$ be an upward-closed set. Then $A \cap D \subseteq U$ iff $(\uparrow A) \cap D \subseteq U$.*

Proof. Let us suppose that $A \cap D \subseteq U$. Then $\uparrow (A \cap D) \subseteq \uparrow U = U$. Let us show that $(\uparrow A) \cap D \subseteq \uparrow (A \cap D)$. Let $x \in (\uparrow A) \cap D$, then there exists $a \in A$ such that $x \geq a$. Since $x \in D$ and D is downward-closed, we also have $a \in D$. Hence $a \in A \cap D$ and then $x \in \uparrow (A \cap D)$. In the other direction, since $A \subseteq \uparrow A$, the inclusion $(\uparrow A) \cap D \subseteq U$ implies $A \cap D \subseteq (\uparrow A) \cap D \subseteq U$. □

The computability of $\uparrow \mathsf{post}^*(s)$ however seems a strong hypothesis. What are the WSTS for which $\uparrow \mathsf{post}^*(s)$ is computable for $s \in S$? Özkan [17] argues that it is precisely the WSTS for which the following problem is decidable.

Downward-reachability problem

INPUT: A transition system $\mathscr{S} = (S, \to)$, $s \in S$ and a downward-closed set $D \subseteq S$.

QUESTION: $s \to^* D$?

Proposition 3 (Proposition 1 in [17]). *For finite-branching WSTS, a basis of $\uparrow \mathsf{post}^*(s)$ is computable for every state s iff the downward-reachability problem is decidable.*

The idea behind the proof is the following. For deciding whether a downward-closed set D is reachable from s, one checks whether $B_{\uparrow \mathsf{post}^*(s)} \cap D = \emptyset$, where $B_{\uparrow \mathsf{post}^*(s)}$ is a basis of $\uparrow \mathsf{post}^*(s)$, that is equivalent to $\mathsf{post}^*(s) \cap D = \emptyset$ by Lemma 1. For the converse direction, one computes the sequence of upward-closed

sets $U_n = \uparrow \mathsf{post}^{\leq n}(s)$ until it becomes stationnary. Decidability of downward-reachability leads to the decidability of the following stop condition: asking whether $S \setminus U_n$ is reachable from s.

More concretely, VASS for instance are $\uparrow \mathsf{post}^*$-effective WSTS [18]. It is well-known that VASS are WSTS with strong compatibility and since there is an algorithm that computes a finite basis of $\uparrow \mathsf{post}^*(s)$, [17] deduced that Bounded-state-resilience is decidable for VASS. Hence State-resilience is decidable for VASS. However, the hypothesis that $\uparrow \mathsf{post}^*$ is computable cannot be tested in the general WSTS framework. Moreover there exist classes of WSTSs with strong compatibility for which there doesn't exist an algorithm computing a basis of $\uparrow \mathsf{post}^*$, such as reset-VASS.

Keeping the $\uparrow \mathsf{post}^*$ effectiveness hypothesis but loosening the strong compatibility one still yields some decidability result for the general State-resilience. Using the same proof structure as Theorem 1 from [18] we obtain:

Theorem 7. State-resilience *is decidable for WSTS with effective* $\uparrow \mathsf{post}^*$ *basis when* $\mathsf{Safe} = \uparrow \mathsf{Safe}$.

Proof. Let $B_{\uparrow \mathsf{post}^*(s)}$ be a basis of $\uparrow \mathsf{post}^*(s)$, and B_{Safe} a basis of Safe. By applying Lemma 1 twice, we obtain

$$\mathsf{post}^*(s) \subseteq \mathsf{pred}^*(\mathsf{Safe}) \text{ iff } B_{\uparrow \mathsf{post}^*(s)} \subseteq \mathsf{pred}^*(\mathsf{Safe})$$

Since $B_{\uparrow \mathsf{post}^*(s)}$ is finite and we can compute a basis of $\mathsf{pred}^*(\mathsf{Safe})$ from B_{Safe}, we can check that $B_{\uparrow \mathsf{post}^*(s)} \setminus \mathsf{pred}^*(\mathsf{Safe}) = \emptyset$. □

However when removing strong compatibility, some precision is lost. Since $\mathsf{pred}(\uparrow \mathsf{Safe})$ is not necessarily upward-closed, it is possible to have $\uparrow \mathsf{post}^*(s) \cap S \not\subseteq \mathsf{pred}(\mathsf{Safe})$, despite having $\mathsf{post}^*(s) \cap S \subseteq \mathsf{pred}(\mathsf{Safe})$. In such a case, the algorithm in [17] would deduce that 1-state-resilience does not hold, which is incorrect.

Thus in case of a WSTS with an effective basis of $\uparrow \mathsf{post}^*$ and (not strong) compatibility, we don't know the decidability status of k-state-resilience and Bounded-state-resilience.

Results synthesis in the case $\mathsf{Safe} = \uparrow \mathsf{Safe}$

Hypothesis	strong compatibility	$\uparrow \mathsf{post}^*$ effective	strong compatibility + $\uparrow \mathsf{post}^*$ effective
SRP	Undecidable (Thm 5)	Decidable (Thm 7)	Decidable (Thm 2)
BSRP	Undecidable (Thm 5)	?	Decidable (Thm 6)
kSRP	Undecidable (Thm 5)	?	Decidable (Thm 6)

4.2 Case: $\mathsf{Safe} = \downarrow \mathsf{Safe}$

We now consider the case $\mathsf{Safe} = \downarrow \mathsf{Safe}$. Unfortunately State-resilience is undecidable in this case. As for Resilience in WSTS when $\mathsf{Safe} = \downarrow \mathsf{Safe}$, this stems from undeciability of the corresponding problem in Minsky machines, the executions of which can be simulated by reset-VASS, as seen in Section 3.2.

Theorem 8. STATE-RESILIENCE *is undecidable for effective WSTS with strong compatibility when* $\mathsf{Safe} =\downarrow \mathsf{Safe}$.

Despite this, it is possible to yield positive results. Indeed, in many ways the case where $\mathsf{Safe} =\downarrow \mathsf{Safe}$ is symmetrical to the case $\mathsf{Safe} =\uparrow \mathsf{Safe}$. For instance one can write the following lemma:

Lemma 2. *(Symmetrical from Lemma 1) Let $A \subseteq S$, $D \subseteq S$ be a downward-closed set and $U \subseteq S$ be an upward-closed set. Then $A \cap U \subseteq D$ iff $(\downarrow A) \cap U \subseteq D$.*

Proof. Let us suppose that $A \cap U \subseteq D$. Then $\downarrow (A \cap U) \subseteq \downarrow D = D$. Let us show that $(\downarrow A) \cap U \subseteq \downarrow (A \cap U)$. Let $x \in (\downarrow A) \cap U$, then there exists $a \in A$ such that $x \leq a$. Since $x \in U$ and U is upward-closed, we also have $a \in U$. Hence $a \in A \cap U$ and then $x \in \downarrow (A \cap U)$. In the other direction, since $A \subseteq \downarrow A$, the inclusion $(\downarrow A) \cap U \subseteq D$ implies $A \cap U \subseteq (\uparrow A) \cap U \subseteq D$. □

In the case of a WSTS with *downward* compatibility, not necessarily strong, then Safe downward-closed implies $\mathsf{pred}^*(\mathsf{Safe})$ downward-closed and Lemma 2 can be used to show that if $\mathsf{Safe} =\downarrow \mathsf{Safe}$, then $\mathsf{post}^*(s) \subseteq \mathsf{pred}^*(\mathsf{Safe})$ iff $(\downarrow \mathsf{post}^*(s)) \subseteq \mathsf{pred}^*(\mathsf{Safe})$.

Theorem 9. STATE-RESILIENCE *is decidable for ideal-effective WSTS with downward and upward compatibilities,* $\mathsf{Safe} =\downarrow \mathsf{Safe}$.

Proof. In order to decide whether $\mathsf{post}^{\leq n}(s) \subseteq \mathsf{pred}^*(\mathsf{Safe})$, we execute two procedures in parallel, one looking for a resilience certificate and one looking for a non-resilience certificate. Procedure 1 enumerates inductive invariants in some fixed order D_1 , D_2 , . . . , i.e. downward-closed subsets $D_i \subseteq S$ such that $\downarrow \mathsf{post}(D_i) \subseteq D_i$. Every inductive invariant D_i is an "over-approximation" of $\downarrow \mathsf{post}^*(s)$ if it contains s. Notice that, by upward compatibility, $\downarrow \mathsf{post}^*(s)$ is such an inductive invariant and may eventually be found.

Procedure 1 stops when it finds an invariant D such that $D \subseteq \mathsf{pred}^*(\mathsf{Safe})$. Indeed $D \subseteq \mathsf{pred}^*(\mathsf{Safe})$ implies $\downarrow \mathsf{post}^*(s) \subseteq \mathsf{pred}^*(\mathsf{Safe})$ since $\downarrow \mathsf{post}^*(s) \subseteq D$.

The second procedure iteratively computes $\mathsf{post}^{\leq n}(s)$ until it finds an element not in $\mathsf{pred}^*(\mathsf{Safe})$. □

Strong downward compatibility implies furthermore the decidability of k-STATE-RESILIENCE and BOUNDED-STATE-RESILIENCE.

Corollary 3. k-STATE-RESILIENCE *and* BOUNDED-STATE-RESILIENCE *are decidable for ideal-effective WSTS with strong downward compatibility and upward compatibility when* $\mathsf{Safe} =\downarrow \mathsf{Safe}$.

5 Resilience for VASS and variations

In this section we study VASS. Since they are completion-post-effective WSTS, they inherit the decidability results for WSTS in the case $\mathsf{Safe} =\uparrow \mathsf{Safe}$. Lacking

downward compatibility or a more relaxed hypothesis that for all downward-closed set D, the set $\mathsf{pred}^*(D)$ is downward-closed, VASS do not inherit the decidability results for WSTS in the case $\mathsf{Safe} =\downarrow \mathsf{Safe}$. In this section, we work to re-establish decidability results for VASS when Safe is downward-closed. We also extend decidability to resilience for semilinear sets rather than simply upward and downward-closed ones.

Theorem 10. RESILIENCE *is decidable for VASS when* Safe *is a semilinear set.*

Proof. We consider the case when Safe is semilinear and $\mathsf{Bad} = S \setminus \mathsf{Safe}$ is semilinear too. RESILIENCE asks whether $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$. We have $\mathsf{post}^*(\mathsf{Bad}) \setminus \mathsf{Safe} = \mathsf{Bad}$ by extension of $S \setminus \mathsf{Safe} = \mathsf{Bad}$. Thus $\mathsf{post}^*(\mathsf{Bad}) = \mathsf{Bad} \cup (\mathsf{Safe} \cap \mathsf{post}^*(\mathsf{Bad}))$. Since $(\mathsf{Safe} \cap \mathsf{post}^*(\mathsf{Bad})) \subseteq \mathsf{pred}^*(\mathsf{Safe})$, we have

$$\mathsf{post}^*(\mathsf{Bad}) \subseteq \mathsf{pred}^*(\mathsf{Safe}) \quad iff \quad \mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe}).$$

Since it is decidable whether $\mathsf{post}^*(\mathsf{Bad}) \subseteq \mathsf{pred}^*(\mathsf{Safe})$ when Bad and Safe are both semilinear [13], RESILIENCE is decidable. □

RESILIENCE is also decidable for other classes of counter machines for which the reachability relation can be expressed in a decidable logic. Recall that lossy counter machines [23] are counter machines that may loose tokens in each control-state.

Theorem 11. RESILIENCE *is decidable for lossy counter machines when* Safe *is a semilinear set.*

Proof. We deduce from Theorem 3.6 in [23] that $\mathsf{pred}^*(\mathsf{Safe})$ is a computable semilinear set if Safe is semilinear. Hence since the inclusion between two semilinear sets is decidable, we deduce that $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$ is decidable if Bad is semilinear. □

Integer VASS or $\mathbb{Z}-$VASS [11] are VASS that are allowed to take values from the integers.

Theorem 12. RESILIENCE *is decidable for integer VASS when* Safe *is a semilinear set.*

Proof. The reachability relation of integer d-VASS is definable by a sentence in Presburger in $\mathbb{Z}^{2d}$ hence $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$ is decidable when Safe and Bad are semilinear sets.

Continuous VASS [4] are a relaxation of classical discrete VASS in which transitions can be fired a fractional number of times, and consequently counters may contain a fractional number of tokens.

Theorem 13. RESILIENCE *is decidable for continuous VASS when* Safe *is definable in the existential theory of the rationals with addition and order.*

Proof. The reachability relation of continuous VASS is definable by a sentence of linear size in the existential theory of the rationals with addition and order whose complexity is EXPSPACE [4]. Hence, $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$ is decidable (and also in EXPSPACE). □

Remark that Theorem 11 and Theorem 12 (resp. Theorem 13) did not make use of the hypothesis that Bad is the complement of Safe, simply relying on the semilinearity of the set (resp. its definability in the existential theory of the rationals with addition and order). Thus the mentionned theorems still hold in the more general case where Bad and Safe are not complements of each others.

The above results concern only unbounded resilience. We consider now Bounded resilience and k-resilience, and focus on the length of the path from Bad to Safe when Safe is downward-closed. Unfortunately, we have the following:

Proposition 4. Bounded resilience *and* k-resilience *never hold for VAS when* $\mathsf{Safe} = \downarrow \mathsf{Safe}$.

Proof. Consider a given $k \in \mathbb{N}$, $\mathsf{Bad} \subseteq \mathbb{N}^d$ upward-closed and $\mathsf{Safe} \subseteq \mathbb{N}^d$ downward-closed, and consider a given VAS V. Let us call $c_{\max}$ the maximal absolute value of a constant appearing in a coordinate of a transition of V. The set Bad admits a finite basis B_{Bad}. Consider the vector $\mathbf{v}_{\mathsf{Bad}}$ obtained by summing all members of the basis of Bad and then consider the vector $\mathbf{u}_k = \mathbf{v}_{\mathsf{Bad}} + (k+1) \cdot (c_{\max}, c_{\max}, \ldots, c_{\max})$.

All states reachable from $\mathbf{u}_k$ in k or less steps are above $\mathbf{v}_{\mathsf{Bad}}$ and thus, are in Bad, by upward-closedness. Hence Safe is not reachable from $\mathbf{u}_k$ in k or less steps and k-resilience does not hold. Since the reasoning hold for all $k \in \mathbb{N}$, Bounded-resilience does not hold either. □

This all changes when one considers VASS (having control-states). For a VASS $V = (Q, T)$, a set $\mathsf{Bad} = \uparrow \mathsf{Bad}$, for all $q \in Q$, either there is an element of the basis of Bad with state q — then $q(\mathbf{v})$ with $\mathbf{v} > \mathbf{v}_{\mathsf{Bad}}$ is necessarily in Bad by upward closure; if this hold for all $q \in Q$, then k-resilience does not hold — either there is none. If there is none, then $\uparrow q(\mathbf{0})$ is in the complement of Bad, i.e. Safe. One can then exhibit upward-closed subsets of Safe and compute basis for the sets of elements from which they are reachable in at most k steps. Substracting these predecessor from Bad yields either a finite number of elements from which one has to check Safe is reachable in at most k steps, either an infinite number of elements of which there is one which cannot reach Safe in at most k steps - for much the same reasons Bounded resilience and k-resilience never hold for VAS when $\mathsf{Safe} = \downarrow \mathsf{Safe}$ and $\mathsf{Bad} = \uparrow \mathsf{Bad}$. This lead to a decision procedure which lead to the following decidability result:

Theorem 14. k-resilience *and* Bounded resilience *are decidable for VASS when* $\mathsf{Safe} = \downarrow \mathsf{Safe}$.

Proof. Let V be a given d-VASS and consider a given $k \in \mathbb{N}$. Consider $\mathsf{Bad} \subseteq Q \times \mathbb{N}^d$ upward-closed and $\mathsf{Safe} = S \setminus \mathsf{Bad}$ downward-closed. Let us call $c_{\max}$ the maximal absolute value of a constant appearing in a coordinate of a transition.

The set Bad admits a finite basis $B_{\mathsf{Bad}} = \{q_{i_1}(\mathbf{v}_{i_1}), q_{i_2}(\mathbf{v}_{i_2}), \ldots, q_{i_m}(\mathbf{v}_{i_m})\}$. Consider the vector $\mathbf{v}_{\mathsf{Bad}} = \Sigma_{1 \leq j \leq m} \mathbf{v}_{i_j}$, and then consider the vector $\mathbf{u}_k = \mathbf{v}_{\mathsf{Bad}} + (k+1) \cdot (c_{\max}, c_{\max}, \ldots, c_{\max})$. For all $p \in Q$, all states reachable from $p(\mathbf{u}_k)$ in k or less steps are of the form $q(\mathbf{v})$ with $\mathbf{v} > \mathbf{v}_{\mathsf{Bad}}$.

For all $q \in Q$, either there is an element of the basis of Bad with state q — then $q(\mathbf{v})$ with $\mathbf{v} > \mathbf{v}_{\mathsf{Bad}}$ is necessarily in Bad by upward closure; if this hold for all $q \in Q$, then k-resilience does not hold — either there is none. If there is none, then $\uparrow q(\mathbf{0})$ is in the complement of Bad, i.e. Safe.

Let us assume from now on $\uparrow q_{j_1}(\mathbf{0}), \uparrow q_{j_2}(\mathbf{0}), \ldots \uparrow q_{j_\ell}(\mathbf{0})$ are all subsets of Safe and that their union contain all upward-closed subsets of Safe. Because these subsets are upward-closed, we can compute a basis of $\mathsf{pred}^{\leq k}(\uparrow q_{j_1}(\mathbf{0}))$, $\mathsf{pred}^{\leq k}(\uparrow q_{j_2}(\mathbf{0}))$, $\ldots$ $\mathsf{pred}^{\leq k}(\uparrow q_{j_\ell}(\mathbf{0}))$.

We now consider the set $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k}(\uparrow q_{j_\ell}(\mathbf{0})))$. We inductively check for any element in the set whether or not it is possible to reach from it the set Safe in k or less steps. If the set is finite then we stop the procedure once we have checked found a witness that k-resilience does not hold or once we have checked for every element, whichever comes first. If it is infinite then k-resilience does not hold and we eventually find a witness that k-resilience does not hold. Indeed, if $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k}(\uparrow q_{j_\ell}(\mathbf{0})))$ is infinite then there exists an element of the form $q(\mathbf{u})$ with $\mathbf{u} > \mathbf{v}_{\mathsf{Bad}} + (k+1) \cdot (c_{\max}, \ldots, c_{\max})$ that is in Bad but not in any of the $\mathsf{pred}^{\leq k}(\uparrow q_{j_i}(\mathbf{0}))$, and hence from which it is not possible at all to reach Safe in k or less steps. This also means that, even in the case where $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k}(\uparrow q_{j_\ell}(\mathbf{0})))$ is finite, we only need to check reachability of Safe in k or less steps for the elements with vectorial component at most $\mathbf{v}_{\mathsf{Bad}} + (k+1) \cdot (c_{\max}, \ldots, c_{\max})$. Binding the search space thus leads to an $\mathsf{EXPSPACE}$ upper bound for k-RESILIENCE.

In order to deal with BOUNDED RESILIENCE now, remark that there exists some $k_0 \in \mathbb{N}$ for which and hence $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k_0}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k_0}(\uparrow q_{j_\ell}(\mathbf{0})) = \mathsf{Bad} \setminus (\mathsf{pred}^*(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \mathsf{pred}^*(\uparrow q_{j_\ell}(\mathbf{0})))$. We start the decision procedure by checking k-RESILIENCE from 0 until k_0.

From k_0 onwards, $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k}(\uparrow q_{j_\ell}(\mathbf{0})) = \mathsf{Bad} \setminus (\mathsf{pred}^*(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \mathsf{pred}^*(\uparrow q_{j_\ell}(\mathbf{0})))$ is stationnary. If the set is finite then we stop the procedure once we have checked for every element whether it is possible to reach Safe from it. If it is possible to reach Safe from every element then k_m-RESILIENCE hold for $k_m = \max(k_0, k_\pi)$ with k_π the maximum of the length of the paths from $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k_0}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k_0}(\uparrow q_{j_\ell}(\mathbf{0}))$ to Safe. If it is infinite then for every $k \in \mathbb{N}$, k-resilience does not hold, and we eventually find a witness that k-resilience does not hold. Indeed, if $\mathsf{Bad} \setminus (\mathsf{pred}^*(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^*(\uparrow q_{j_\ell}(\mathbf{0})))$ is infinite then there exists an element of the form $q(\mathbf{u})$ with $\mathbf{u} > \mathbf{v}_{\mathsf{Bad}} + (k+1) \cdot (c_{\max}, \ldots, c_{\max})$ that is in Bad but not in any of the $\mathsf{pred}^{\leq k}(\uparrow q_{j_i}(\mathbf{0}))$, and hence from which it is not possible at all to reach Safe in k or less steps. □

6 Conclusion and perspectives

We have extended the state-resilience problem introduced in [21, 18, 17]. We complemented previous results by providing some undecidability proofs for resilience and state-resilience in general. We also exhibited classes of WSTS with decidable resilience, namely, completion-post-effective ω^2-WSTS with strong compatibility (in the case $\mathsf{Safe} =\uparrow \mathsf{Safe}$) and downward-compatible ideal-effective WSTS (in the case $\mathsf{Safe} =\downarrow \mathsf{Safe}$).

Several questions still remain. For instance, we have been concerned with decidability only, and a detailed complexity analysis of the different resilience problems still remains to be done for concrete models. One other angle of attack not studied here is the synthesis of sets Safe for resilience, for instance, finding the maximal upward-closed (resp. downward-closed) subset Safe so that a system is Safe-resilient. Another question could be to analyse the resilience in the framework of a controller and its environment. One could also extend upon the classes of set Safe considered. As with semilinear sets for VASS, one could study resilience for sets defined in a boolean logic on upward and downward-closed subsets [3]. Finally, while we mention VASS, a more detailed analysis of the resilience problems could be also done for other computational models such as pushdown automata, one-counter automata or timed automata.

A Reset-VASS and state-resilience

Let us recall the *zero-reachability* problem in (reset-)VASS.

ZERO-REACHABILITY
INPUT: A d-reset-VASS $V = (Q, T)$, and $p(\mathbf{u}) \in Q \times \mathbb{N}^d$.
QUESTION: $\exists q \in Q,\ p(\mathbf{u}) \to^* q(\mathbf{0})$?

The zero-reachability problem is decidable in VASS and it is undecidable in reset-VASS [2]. For a better representation, we will use reset Petri nets [6] rather than reset-VASS. A *reset Petri net* $N = (P, T, E, R, \mu)$ consists of a finite set of *places* $P = \{p_1, p_2, ...p_{|P|}\}$, a finite set of *transitions* $T = \{t_1, t_2, ..., t_{|T|}\}$, a finite set of *arcs* $E \subseteq (P \times T) \cup (T \times P)$, a finite set of *reset-arcs* $R \subseteq T \times P$, and an *initial marking* $\mu : P \to \mathbb{N}$. It is well-known that Petri nets and VASS are equivalents models with regards of the decidability of reachability problems: an d-VASS can be encoded into a Petri net with $d + 2$ places and conversely, a Petri net with p places can be encoded into a p-VASS [22]. The same equivalence hold between reset-VASS and reset Petri nets.

We will show that the *zero-reachability* problem can be reduced to t-LIVENESS in reset Petri nets; this is done by "adjusting" a similar result for Petri nets (Theorem 5.5 in [20]).

Proposition 2 *In reset Petri nets, the zero reachability problem can be reduced to* t-LIVENESS.

We may then deduce that:

Corollary *In reset-VASS, the zero reachability problem can be reduced to t-*LIVENESS.

Proof. If we wish to determine if a marking in which every place is empty is reachable for a reset Petri net $N_1 = (P_1, T_1, E_1, R_1, \mu_1)$ we construct a reset Petri net $N_2 = (P_2, T_2, E_2, R_2, \mu_2)$ which is live in N_2 if and only if the *zero marking*, which assigns 0 to every place of P_1, is not reachable from μ_1 in N_1.

Construction of N_2

The reset Petri net N_2 is constructed from N_1 by the addition of two places p_a and p_b and $|P_1| + 2$ transitions t_{p_a}, $\{t_p \mid p \in P_1\}$ and t_{p_b}. We first modify all transitions of N_1 to include p_a as both an input and an output. The initial marking μ_2 will include a token in p_a and no token in p_b. This new place p_a serve to mark that the run is ongoing. As long as it contains a token, the adjusted transitions of N_1 are live and can be used normally. Thus any marking which is reachable in the places of N_1 is also reachable in the corresponding places of N_2. We add an additional transition t_{p_a} which has p_a as an input and a null output. This allows to disable the transitions of N_1 and to "freeze" the marking of the places of P_1 in N_2. The place p_a and transition t_{p_a} allow the net N_2 to reach any reachable marking in N_1 and then for t_{p_a} to fire and freeze the net at that marking. We introduce a new place p_b and new transitions t_p, for all $p \in P_1$, which have p as input and p_b as output. Lastly, we add a transition t_{p_b} with p_b as its output and every place of P_2 as output, which "floods" the net with tokens, assuring that every transition is live in N_2 if a token is ever put in p_2.

Let us now prove that t_{p_2} is live in N_2 if and only if the zero marking is not reachable from μ_1 in N_1.

Suppose that the zero marking is reachable from μ_1 in N_1, then t_{p_2} is not live in N_2.

Indeed the marking with zero in every place of P_1 and in p_b is reachable in N_2, by executing the same sequence of transition firings. Then t_{p_a} can fire, leading to the marking which assigns zero to every place of P_2. From this marking the transitions t_p are not live and neither are the transitions inherited from N_1 nor t_{p_a}, and, finally, nor is t_{p_2}. Thus t_{p_2} is not live in N_2.

Suppose that t_{p_2} is not live in N_2, then the zero marking is reachable from μ_1 in N_1

Indeed, if t_{p_2} is not live in N_2, then a marking μ must be reachable in which $\mu(p_2) = 0$ and there is no reachable state in which p_2 has a token (in particular, since we do not allow token removal from p_2, the marking μ must be reached in a sequence of transitions that do not place any token in p_2). This means that no transition t_p is live in N_2 in μ since any transition t_p can place a token in p_2.

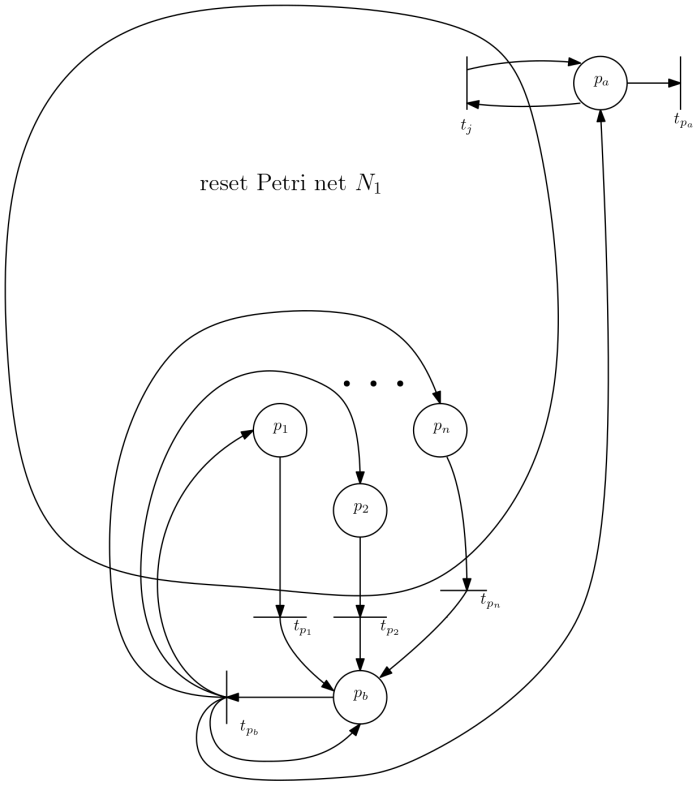

Fig. 2: Construction of N_2 from N_1.

Thus, every place of P_2 inherited from N_1 must be devoid of token. Moreover, since the marking μ must be reached in a sequence of transitions that do not place any token in p_2, it can be reached without using the transitions t_p or t_{p_2}. Since t_{p_a} do not modify the places inherited from P_1 nor does it enable new transitions, the reachability of μ implies the reachability of a marking where every place of P_2 inherited from P_1 is devoid of token using only the transitions inherited from N_1. Thus the zero marking is reachable from μ_1 in N_1.