Positive Non–Interference in Elementary and Trace Nets

Nadia Busi and Roberto Gorrieri

Dipartimento di Scienze dell'Informazione, Università di Bologna
Mura A. Zamboni, 7, 40127 Bologna, Italy

Abstract. Several notions of non-interference have been proposed in the literature to study the problem of confidentiality in concurrent systems. The common feature of these non-interference properties is that they are all defined as extensional properties based on some notion of behavioural equivalence on systems. Here we also address the problem of defining non-interference by looking at the structure of the net systems under investigation. We define *structural* non-interference properties based on the absence of particular places in the net. We characterize a structural property, called *PBNI+*, that is equivalent to the well-known behavioural property *SBNDC*. We start providing a characterization of *PBNI+*on contact-free Elementary Net Systems, then we extend the definition to cope with the richer class of Trace nets.

1 Introduction

Non-interference has been defined in the literature as an extensional property based on some observational semantics: the high part of a system does not interfere with the low part if whatever is done at the high level produces no visible effect on the low part of the system. The original notion of non-interference in [9] was defined, using trace semantics, for system programs that are deterministic. Generalized notions of non-interference were then designed to include (nondeterministic) labeled transition systems and finer notions of observational semantics such as bisimulation (see, e.g., [13, 7, 12, 14, 8]). Relevant properties in this class are the trace-based properties *SNNI* and *NDC*, as well as the bisimulation-based properties *BSNNI*, *BNDC* and *SBNDC* proposed by Focardi and Gorrieri some years ago [7, 8] on a CCS-like process algebra. In particular, *SNNI* states that a system R is secure if the two systems $R \setminus H$ (all the high level actions are prevented) and R/H (all the high level actions are permitted but are unobservable) are trace equivalent. *BNDC* intuitively states that a system R is secure if it is bisimilar to R in parallel with any high level process Π w.r.t. the low actions the two systems can perform. And *SBNDC* tells that a system R is secure if, whenever a high action h is performed, the two instances of the system before and after performing h are bisimilar from a low level point of view.

In the first part of the paper we show that these non–interference properties can be naturally defined also on Petri Nets; in particular – to keep the presentation as simple as possible – we use Elementary Nets [6]. The advantage of this proposal is the import in the Petri Net theory of security notions that makes possible the study of security problems. Technically, what we do is to introduce two operations on nets, namely parallel composition (with synchronization in TCSP-like style) and restriction, and suitable notions of observational equivalences on the low part of the system (low trace equivalence and low bisimulation); then, five security properties are defined and compared in a rather direct way. In particular, the two properties based on low trace semantics, namely *SNNI* and *NDC*, are equivalent. On the contrary, in the bisimulation case, *BSNNI* is weaker than *BNDC*, which turns out to be equivalent to *SBNDC*.

In this approach, the security property is based on the dynamics of systems; they are all defined by means of one (or more) equivalence check(s); hence, non-interference checking is as difficult as equivalence checking, a well-studied hard problem in concurrency theory.

In the second part of the paper we address the problem of defining statically non-interference for Elementary nets, by looking at the structure of the net systems under investigation:

- in order to better understand the causality and conflict among different system activites, hence grounding more firmly the intuition about what is an interference, and
- in order to find more efficiently checkable non-interference properties that are sufficient conditions for those that have already received some support in the literature.

We define structural non-interference properties based on the absence of particular places in the net. We identify two special classes of places: *causal places*, i.e., places for which there are an incoming high transition and an outgoing low transition; and, *conflict places*, i.e. places for which there are both low and high outgoing transitions. Intuitively, causal places represent potential source of interference (*hilo* flow for *high input – low output*), because the occurrence of the high transition is a prerequisite for the execution of the low transition. Similarly, conflict places represent potential source of interference (*holo* flow for *high output – low output*), because the occurrence of a low event tells us that a certain high transition will not occur.

We show that when causal and conflict places are absent, we get a property, called *Positive Place–Based Non–Interference* (*PBNI+* for short), which turns out to be equivalent to *SBNDC*. More precisely, the net N has no causal and no conflict places if and only if it satisfies *SBNDC*.

In the third part of the paper we extend the definition of *PBNI+* to cope with the richer class of Trace nets[1]. We provide an example showing how our property can be used to capture the information flows arising in a shared variable that can be accessed and modified by both high and low users.

The paper is organised as follows. In Section 2 we recall the basic definitions about transition systems and Elementary Nets. In Section 3 we recast the behavioural approach to non-interference properties, originally defined in a process algebraic setting, on Elementary Nets. The original structural property *PBNI+* for Elementary Nets is introduced in Section 4. In Section 5, after recalling the basic definitions about Trace Nets, we extend the definition of *PBNI+* to Trace Nets. Finally, some conclusive remarks are drawn.

2 Basic definitions

Here we recall the basic definition about transition systems and elementary net systems we will use in the following.

2.1 Transition systems

Definition 1. *A transition system is a triple $TS = (St, E, \rightarrow)$ where*

- *St is the set of states*
- *E is the set of events*
- *$\rightarrow \subseteq St \times E \times St$ is the transition relation.*

In the following we use $s \xrightarrow{e} s'$ to denote $(s, e, s') \in \rightarrow$.

Given a transition $s \xrightarrow{e} s'$, s is called the source*, s' the* target *and e the* label *of the transition.*

A rooted *transition system is a pair (TS, s_0) where $TS = (St, E, \rightarrow)$ is a transition system and $s_0 \in St$ is the* initial state*.*

2.2 Elementary net systems

Definition 2. *An* elementary net *is a tuple $N = (S, T, F)$, where*

- *S and T are the (finite) sets of* places *and* transitions*, such that $S \cap T = \emptyset$*
- *$F \subseteq (S \times T) \cup (T \times S)$ is the flow relation*

A set over the set S of places is called a *marking*. Given a marking m and a place s, if $s \in m$ then we say that the place s contains a token, otherwise we say that s is empty.

Let $x \in S \cup T$. The *preset* of x is the set ${}^\bullet x = \{y \mid F(y, x)\}$. The *postset* of x is the set $x^\bullet = \{y \mid F(x, y)\}$. The preset and postset functions are generalized in the obvious way to set of elements: if $X \subseteq S \cup T$ then ${}^\bullet X = \bigcup_{x \in X} {}^\bullet x$ and $X^\bullet = \bigcup_{x \in X} x^\bullet$. A transition t is enabled at marking m if ${}^\bullet t \subseteq m$ and $t^\bullet \cap m = \emptyset$. The firing (execution) of a transition t enabled at m produces the marking $m' = (m \setminus {}^\bullet t) \cup t^\bullet$. This is usually written as $m[t\rangle m'$. With the notation $m[t\rangle$ we mean that there exists m' such that $m[t\rangle m'$.

An *elementary net system* is a pair (N, m_0), where N is a net and m_0 is a marking of N, called *initial marking*. With abuse of notation, we use (S, T, F, m_0) to denote the net system $((S, T, F), m_0)$.

The set of *markings reachable from* m, denoted by $[m\rangle$, is defined as the least set of markings such that

- $m \in [m\rangle$
- if $m' \in [m\rangle$ and there exists a transition t such that $m'[t\rangle m''$ then $m'' \in [m\rangle$.

The set of *firing sequences* is defined inductively as follows:

- m_0 is a firing sequence;
- if $m_0[t_1\rangle m_1 \ldots [t_n\rangle m_n$ is a firing sequence and $m_n[t_{n+1}\rangle m_{n+1}$ then $m_0[t_1\rangle m_1 \ldots [t_n\rangle m_n[t_{n+1}\rangle m_{n+1}$ is a firing sequence.

Given a firing sequence $m_0[t_1\rangle m_1 \ldots [t_n\rangle m_n$, we call $t_1 \ldots t_n$ a *transition sequence.* The set of transition sequences of a net N is denoted by $TS(N)$. We use σ to range over $TS(N)$. Let $\sigma = t_1 \ldots t_n$; we use $m[\sigma\rangle m_n$ as an abbreviation for $m[t_1\rangle m_1 \ldots [t_n\rangle m_n$.

The *marking graph* of a net N is

$$MG(N) = ([m_0\rangle, T, \{(m, t, m') \mid m \in [m_0\rangle \wedge t \in T \wedge m[t\rangle m'\})$$

A net is *simple* if the following condition holds for all $x, y \in S \cup T$: if ${}^\bullet x = {}^\bullet y$ and $x^\bullet = y^\bullet$ then $x = y$.

A marking m contains a *contact* if there exists a transition $t \in T$ such that ${}^\bullet t \subseteq m$ and $not(m[t\rangle)$. A net system is *contact–free* if no marking in $[m_0\rangle$ contains a contact. A net system is *reduced* if each transition can occur at least one time: for all $t \in T$ there exists $m \in [m_0\rangle$ such that $m[t\rangle$.

In the following we consider contact-free net systems that are simple and reduced.

3 A Behavioural Approach to Non-interference for Elementary Nets

In this section we recall from [5] some basic properties, initially proposed in a process algebraic setting by Focardi and Gorrieri [7, 8]. Our aim is to analyse systems that can perform two kinds of actions: high level actions, representing the interaction of the system with high level users, and low level actions, representing the interaction with low level users. We want to verify if the interplay between the high user and the high part of the system can affect the view of the system as observed by a low user. We assume that the low user knows the structure of the system, and we check if, in spite of this, he is not able to infer the behavior of the high user by observing the low view of the execution of the system.

Hence, we consider nets whose set of transitions is partitioned into two subsets: the set H of high level transitions and the set L of low level transitions. To emphasize this partition we use the following notation. Let L and H be two disjoint sets: with (S, L, H, F, m_0) we denote the net system $(S, L \cup H, F, m_0)$.

The non-interference properties we are going to introduce are based on some notion of *low* observability of a system, i.e., what can be observed of a system from the point of view of low users. The low view of a transition sequence is nothing but the subsequence where high level transitions are discarded.

Definition 3. *Let $N = (S, L, H, F, m_0)$ be a net system. The* low view *of a transition sequence of N is defined as follows:*

$\Lambda_N(\varepsilon) = \varepsilon$

$\Lambda_N(\sigma t) = \begin{cases} \Lambda_N(\sigma)t & \textit{if } t \in L \\ \Lambda_N(\sigma) & \textit{otherwise} \end{cases}$

The definition of Λ_N *is extended in the obvious way to sets of transitions sequences:* $\Lambda_N(\Sigma) = \{\Lambda_N(\sigma) \mid \sigma \in \Sigma\}$ *for* $\Sigma \subseteq (L \cup H)^*$.

Definition 4. *Let* N_1 *and* N_2 *be two net systems. We say that* N_1 *is* low-view trace equivalent *to* N_2*, denoted by* $N_1 \overset{\Lambda}{\approx}_{tr} N_2$*, iff* $\Lambda_{N_1}(TS(N_1)) = \Lambda_{N_2}(TS(N_2))$.

We define the operations of parallel composition (in TCSP-like style) and restriction on nets, that will be useful for defining some non-interference properties.

Definition 5. *Let* $N_1 = (S_1, L_1, H_1, F_1, m_{0,1})$ *and* $N_2 = (S_2, L_2, H_2, F_2, m_{0,2})$ *be two net systems such that* $S_1 \cap S_2 = \emptyset$ *and* $(L_1 \cup L_2) \cap (H_1 \cup H_2) = \emptyset$*. The parallel composition of* N_1 *and* N_2 *is the net system*

$N_1 \mid N_2 = (S_1 \cup S_2, L_1 \cup L_2, H_1 \cup H_2, F_1 \cup F_2, m_{0,1} \cup m_{0,2})$

Definition 6. *Let* $N = (S, L, H, F, m_0)$ *be a safe net system and let* U *be a set of transitions. The restriction on* U *is defined as* $N \backslash U = (S, L', H', F', m_0)$*, where*

$L' = L \setminus U$

$H' = H \setminus U$

$F' = F \setminus (S \times U \cup U \times S)$

Strong Nondeterministic Non-Interference (*SNNI* for short) is a trace-based property, that intuitively says that a system is secure if what the low-level part can see does not depend on what the high-level part can do.

Definition 7. *Let* $N = (S, L, H, F, m_0)$ *be a net system. We say that* N *is SNNI iff* $N \overset{\Lambda}{\approx}_{tr} N \backslash H$.

The intuition is that, from the low point of view, the system where the high level transitions are prevented should offer the same traces as the system where the high level transitions can be freely performed. In essence, a low-level user cannot infer, by observing the low view of the system, that some high-level activity has occurred.

As a matter of fact, this non-interference property captures the information flows from high to low, while admits flows from low to high. For instance, the net N' of Figure 1 is *SNNI* while the net N'' is not *SNNI*.

An alternative notion of non-interference, called *Nondeducibility on Composition* (*NDC* for short), says that the low view of a system N in isolation is not to be altered when considering each potential interaction of N with the high users of the external environment.

Definition 8. *Let* $N = (S, L, H, F, m_0)$ *be a net system. We say that* N *is a high-level net if* $L = \emptyset$.

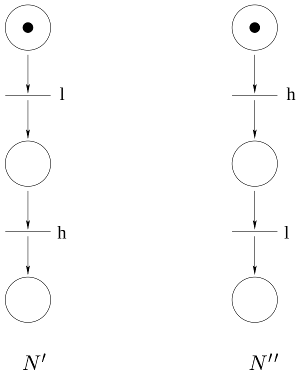

Fig. 1. The net system N' is *SNNI* while N'' is not *SNNI*.

Definition 9. *Let $N = (S, L, H, F, m_0)$ be a net system. N is NDC iff for all high-level nets $K = (S_K, \emptyset, H_K, F_K, m_{0,K})$: $N \backslash H \overset{\Lambda}{\approx}_{tr} (N \mid K) \backslash (H \setminus H_K)$.*

The left-hand term represents the low view of the system N in isolation, while the right-hand term expresses the low view of N interacting with the high environment K (note that the activities resulting from such interactions are invisible by the definition of low view equivalence). *NDC* is a very intutive property: whatever high level system K is interacting with N, the low effect is unobservable. However, it is difficult to check this property because of the universal quantification over high systems. Luckily enough, we will then prove that *SNNI* and *NDC* are actually the same non-interference property.

Theorem 1. *Let $N = (S, L, H, F, m_0)$ be a net system. N is SNNI if and only if N is NDC.*

The two properties above are based on (low) trace semantics. It is well-known [8] that bisimulation semantics is more appropriate than trace semantics because it captures also some indirect information flows due to, e.g., deadlocks. For this reason, we now consider non-interference properties based on bisimulation. To this aim, we first need to introduce a notion of low–view bisimulation.

Definition 10. *Let $N_1 = (S_1, L_1, H_1, F_1, m_{0,1})$ and $N_2 = (S_2, L_2, H_2, F_2, m_{0,2})$ be two net systems. A* low–view bisimulation *from N_1 to N_2 is a relation on $\mathcal{M}(S_1) \times \mathcal{M}(S_2)$ such that if $(m_1, m_2) \in R$ then for all $t \in \bigcup_{i=1,2} L_i \cup H_i$:*

- *if $m_1[t\rangle m'_1$ then there exist σ, m'_2 such that $m_2[\sigma\rangle m'_2$, $\Lambda_{N_1}(t) = \Lambda_{N_2}(\sigma)$ and $(m'_1, m'_2) \in R$*
- *if $m_2[t\rangle m'_2$ then there exist σ, m'_1 such that $m_1[\sigma\rangle m'_1$, $\Lambda_{N_2}(t) = \Lambda_{N_1}(\sigma)$ and $(m'_1, m'_2) \in R$*

If $N_1 = N_2$ we say that R is a low–view bisimulation on N_1.

We say that N_1 *is* low–view bisimilar *to* N_2*, denoted by* $N_1 \overset{\Lambda}{\approx}_{bis} N_2$*, if there exists a low–view bisimulation* R *from* N_1 *to* N_2 *such that* $(m_{0,1}, m_{0,2}) \in R$*.*

The first obvious variation on the theme is to define the bisimulation based version of *SNNI*, yielding *BSNNI*.

Definition 11. *Let* $N = (S, L, H, F, m_0)$ *be a net system. We say that* N *is BSNNI iff* $N \overset{\Lambda}{\approx}_{bis} N \backslash H$*.*

Obviously, *BSNNI* $\subseteq$ *SNNI*. The converse is not true: the net N in Figure 2 is *SNNI* but not *BSNNI*. Note that *SNNI* misses to capture the indirect information flow present in this net: if the low transition l cannot be performed, the low user can infer that the high transition h has been performed, hence deducing one piece of high knowledge.

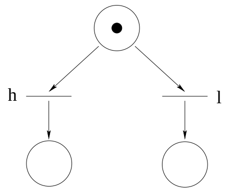

Fig. 2. A net system that is *SNNI* but not *BSNNI*.

Similarly, *BNDC* can be defined from *NDC*, yielding a rather appealing security property, which is finer than *BSNNI*.

Definition 12. *Let* $N = (S, L, H, F, m_0)$ *be a net system.* N *is BNDC iff for all high-level nets* $K = (S_K, \emptyset, H_K, F_K, m_{0,K})$*:* $N \backslash H \overset{\Lambda}{\approx}_{bis} (N \mid K) \backslash (H \setminus H_K)$*.*

Theorem 2. *Let* $N = (S, L, H, F, m_0)$ *be a net system. If* N *is BNDC then* N *is BSNNI.*

Unfortunately, the converse is not true: Figure 3 reports a net that is *BSNNI* but not *BNDC*; the reason why can be easily grasped by looking at their respective marking graphs in Figure 4.

BNDC is quite appealing but, because of the universal quantification on all possible high level systems, it is difficult to check. The next property, called *Strong Bisimulation Non Deducibility on Composition* (*SBNDC* for short), is actually an alternative characterization of *BNDC* which is easily checkable.

Definition 13. *Let* $N = (S, L, H, F, m_0)$ *be a net system.* N *is SBNDC iff for all markings* $m \in [m_0\rangle$ *and for all* $h \in H$ *the following holds:*

if $m[h\rangle m'$ *then there exists a low–view bisimulation* R *on* $N \backslash H$ *such that* $(m, m') \in R$*.*

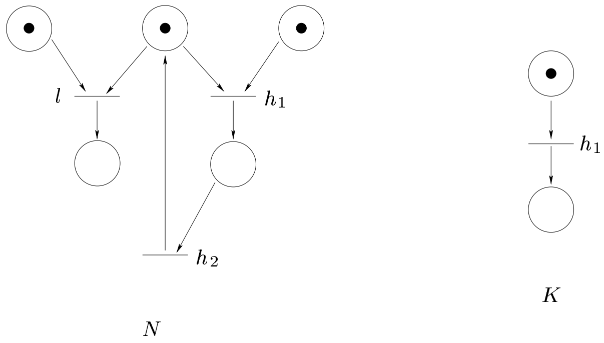

Fig. 3. A net system that is *BSNNI* but not *BNDC*.

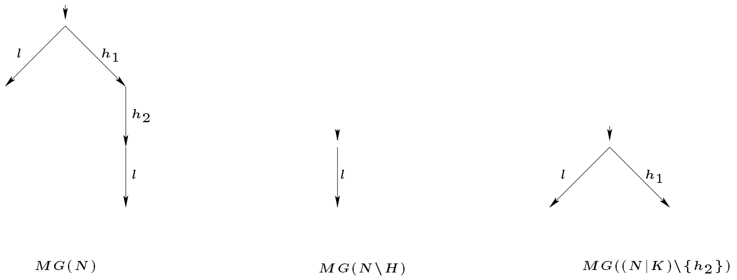

Fig. 4. The marking graphs of the net systems N, $N\backslash H$ and $(N \mid K)\backslash\{h_2\}$.

Theorem 3. *Let $N = (S, L, H, F, m_0)$ be a net system. N is BNDC if and only if N is SBNDC.*

The theorem above holds because we are in an unlabeled setting: transitions are not labeled. In [7, 8] it is proved that – for the Security Process Algebra – *SBNDC* is strictly finer than *BNDC*.

4 Positive Place-Based Non-Interference in Elementary Nets

In [4, 5] we defined two notions of non-interference, namely, *PBNI* and *RBNI*, aiming at capturing any kind of information flow from high users to low users. Those notions capture both positive and negative informations on the high behaviour of the system. More precisely, a positive information flow arises when the occurrence of a high level transition can be deduced from the low level behaviour of the system, whereas a negative information is concerned with the fact that a high level transition has not occurred.

In this paper we provide a characterisation of positive information flows, i.e., we consider a system secure if it is not possible to deduce that some high level action has been performed by observing the low level behaviour.

To this aim, we define the *PBNI+* property based on the absence of some kinds of places in a net system. Consider a net system $N = (S, L, H, F, m_0)$.

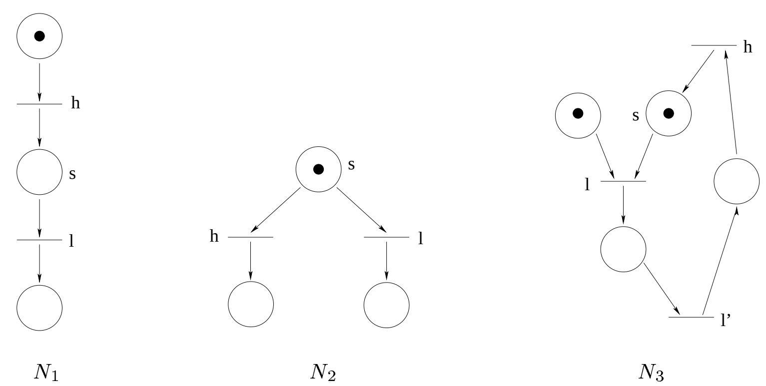

Fig. 5. Examples of net systems containing conflict and (potentially) causal places.

Consider a low level transition l of the net: if l can fire, then we know that the places in the preset of l are marked before the firing of l; moreover, we know that such places become unmarked after the firing of l. If there exists a high level action h that produces a token in a place s in the preset of l (see the system N_1 in Figure 5), then the low level user can infer that h has occurred if he can perform the low level action l. We note that there exists a causal dependency between the transitions h and l, because the firing of h produces a token that is consumed by l. Consider now the situation illustrated in the system N_2 of Figure 5: in this case, place s is in the preset of both l and h, i.e., l and h are competing for the use of the resource represented by the token in s. Aware of the existence of such a place, a low user knows that the high-level action h has been performed, if he is not able to perform the low-level action l. Place s represents a conflict between transitions l and h, because the firing of h prevents l from firing.

Our idea is to consider a net system secure if it does not contain places of the kinds illustrated above.

In order to avoid the definition of a security notion that is too strong, and that prevents systems that do not reveal information on the high-level actions that have been performed, we need to refine the concepts illustrated above. Consider the net system N_3 reported in Figure 5. Although s is a potentially causal place, the net system has to be considered secure, as the (unique) possible firing of l is at the initial marking, hence it is not caused by h. For s to be a source of information on the occurrence of h, there must exists a firing sequence where l consumes a token produced by h. In other words, s is an active causal place if there exists a path in $MG(N_3)$ connecting (an occurrence of) h to (an occurrence of) l, such that the transitions occurring after h and before l do not produce tokens in s.

Regarding conflicts, consider the net system N_4 reported in Figure 6. At first sight, the net N_4 could appear not secure because of the presence of the conflict place s. However, we note that the occurrence of h has no effect on the low behaviour of the system, as the possibility to fire l has already been ruled out by the firing of transition l'. Hence, for s to be a source of information on the occurrence of h, there must exist a reachable marking where the firing of h rules out the possibility to fire (immediately or after some other transitions) l. In other words, s is an active conflict place if there exists a path in $MG(N_4)$ connecting the source of (an occurrence of) h to (an occurrence of) l, such that the transitions occurring in the path do not produce tokens in s.

Definition 14. *Let $N = (S, L, H, F, m_0)$ be an elementary net system. Let s be a place of N such that $s^\bullet \cap L \neq \emptyset$.*

The place $s \in S$ is a potentially causal place *if ${}^\bullet s \cap H \neq \emptyset$.*

A potentially causal place s is an active causal place *if the following condition holds: there exist $l \in s^\bullet \cap L$, $h \in {}^\bullet s \cap H$, $m \in [m_0\rangle$ and a transition sequence σ such that $m[h\sigma l\rangle$ and $s \notin t^\bullet$ for all $t \in \sigma$.*

The place $s \in S$ is a potentially conflict place *if $s^\bullet \cap H \neq \emptyset$.*

A potentially conflict place is a active conflict place *if the following condition holds: there exist $l \in s^\bullet \cap L$, $h \in s^\bullet \cap H$, $m \in [m_0\rangle$ and a transition sequence σ such that $m[h\rangle$, $m[\sigma l\rangle$ and $s \notin t^\bullet$ for all $t \in \sigma$.*

Definition 15. *Let $N = (S, L, H, F, m_0)$ be an elementary net system. We say that N is PBNI+ (*positive Place Based Non-Interference*) if, for all $s \in S$, s is neither an active causal place nor an active conflict place.*

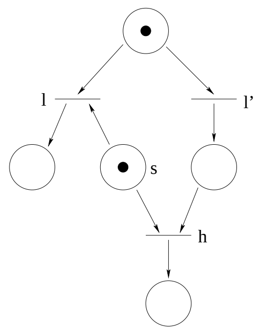

Fig. 6. A net system containing a potentially conflict place but no active conflict places.

We have that the absence of both causal and conflict places is a necessary and sufficient condition for *SBNDC*.

Theorem 4. *Let $N = (S, L, H, F, m_0)$ be an elementary net system. If N is PBNI+ then N is SBNDC.*

Theorem 5. *Let $N = (S, L, H, F, m_0)$ be an elementary net system. If N is SBNDC then N is PBNI+.*

Corollary 1. *Let $N = (S, L, H, F, m_0)$ be an elementary net system. Then N is PBNI+ iff N is BNDC.*

5 Non-Interference in trace nets

In this section we extend the definition of *PBNI+* to cope with the richer class of Trace nets [1] and we show that the results presented in the previous section for elementary nets continue to hold also in this setting. Finally, we provide an example to show how our property can be used to capture the information flows arising in a shared variable that can be accessed and modified by both high and low users.

5.1 Trace nets

Trace nets [1] are an extension of elementary nets: besides the classical flow arcs, also arcs permitting to test for presence/absence of tokens in a place, as well as arcs permitting to fill/empty a place regardless of its previous contents, are added.

Definition 16. *A* trace net *is a tuple $N = (S, T, W)$, where*

- *S and T are the (finite) sets of* places *and* transitions*, such that $S \cap T = \emptyset$*

– $W : (S \times T) \rightarrow \{in, out, nop, read, inhib, set, reset\}$ *is the flow function, such that* $\forall t \in T \exists s \in S : W(s,t) \neq nop$.

The arcs of kind in and out correspond to the flow arcs of elementary nets: more precisely, a flow arc from a place s to a transition t is represented in trace nets by setting $W(s,t) = in$, whereas a flow arc from t to s is represented by setting $W(s,t) = out$. The arcs of kind $read$ and $inhib$ permit to test a condition on a place, without altering its contents. A read (resp. inhibitor) arc from s to t requires that s contains a token (resp. no tokens) for t to fire. The arcs of kind set and $reset$ permit to set the contents of the place to a given value, independently of the previous contents of the place. A set (resp. reset) arc from s to t sets the number of tokens in place s to 1 (resp. 0) when t fires. Finally, an arc of kind nop denotes the absence of any kind of relation among the contents of s and the firing of t.

We adopt the graphical convention proposed in [2], and depicted in Figure 7 to draw trace nets: input (resp. output) arcs are represented as directed segments with an arrow on the transition (resp. place) side; read (resp. inhibitor) arcs are represented as segments with a small black (resp. white) circle on the transition side; set (resp. reset) arcs are represented as segment with a small black (resp. white) circle on the place side.

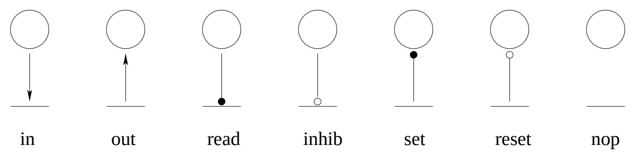

Fig. 7. Graphic conventions for drawing trace nets.

To lighten the definitions of enabling of a transition and of the firing rule, we introduce the following auxiliary relations. Intuitively, $t\ test1\ s$ (resp. $t\ test0\ s$) holds if it is necessary that s contains one (resp. zero) tokens for t to fire. On the other hand, $t\ set1\ s$ (resp. $t\ set0\ s$) holds if, after the firing of t, s contains one (resp. zero) tokens.

Givens $s \in S$ and $t \in T$, we define the following relations:

$t\ test1\ s$ iff $W(s,t) \in \{in, read\}$

$t\ test0\ s$ iff $W(s,t) \in \{out, inhib\}$

$t\ set1\ s$ iff $W(s,t) \in \{out, set\}$

$t\ set0\ s$ iff $W(s,t) \in \{in, reset\}$

A transition t is enabled at marking m if $\{s \mid t\ test1\ s\} \subseteq m$ and $\{s \mid t\ test0\ s\} \cap m = \emptyset$.

The firing (execution) of a transition t enabled at m produces the marking $m' = \{s \in S \mid t\ set1\ s\} \cup \{s \in m \mid W(s,t) = nop\}$. This is usually written as $m[t\rangle m'$.

A *trace net system* is a pair (N, m_0), where N is a trace net and m_0 is a marking of N, called *initial marking*. With abuse of notation, we use (S, T, W, m_0) to denote the trace net system $((S, T, W), m_0)$.

The definitions of reachable markings, firing sequences, marking graph and reduced system given in Section 2 for elementary nets apply also for trace nets.

In the following we consider trace net systems that are reduced.

5.2 Positive Place Based Non-Interference for trace nets

As already done for elementary nets, we consider trace nets whose set of transitions is partitioned into two subsets: the set H of high level transitions and the set L of low level transitions. Also for trace nets, given two disjoint sets L and H, with (S, L, H, W, m_0) we denote the trace net system $(S, L \cup H, W, m_0)$.

We extend the definitions of causal an conflict places for Elementary nets of Section 4 to Trace nets.

An extension of the definition of potentially causal place for contact free elementary nets to trace nets leads to the following: a place s is a potentially causal place if there exist a high transition h that puts a token in s (either through an output or a set arc) and a low transition l that needs place s to be full to fire (because s and l are connected by a read or an input arc). However, as contact freeness no longer holds for trace nets, we have to take into account also causal dependencies arising from the fact that a high transition h removes a token contained in a place s (either through an input or a reset arc) that is required to be empty for a low transition l to fire (because s and l are connected by an output or an inhibitor arc).

Also for potentially conflict places, two kinds of conflicts can arise. Similarly to elementary nets, s is a potentially conflict place if there exists a high transition h that removes a token from s and a low transition l that needs place s to be full to fire. Morevoer, s has to be considered a potentially conflict place also if there exists a high transition h that produces a token in S and a low transition l that needs place s empty to fire.

Definition 17. *Let $N = (S, L, H, W, m_0)$ be a trace net system.*

The place $s \in S$ is a potentially causal place *if there exist $h \in H$, $l \in L$ and $X \in \{0, 1\}$ such that h setX s and l testX s.*

A potentially causal place s is an active causal place *if the following condition holds: there exist $h \in H$, $l \in L$ and $X \in \{0, 1\}$ such that:*

- *h setX s*
- *l testX s*
- *there exists a marking $m \in [m_0\rangle$ and a transition sequence σ such that*
  - *$m[h\sigma l\rangle$*
  - *$s \in m$ iff $X = 0$*
  - *for all $t \in \sigma$: $\neg(t \; set1 \; s)$ and $\neg(t \; set0 \; s)$*

The place $s \in S$ is a potentially conflict place *if there exist $h \in H$, $l \in L$ and $X \in \{0,1\}$ such that h setX s and l test$(1-X)$ s.*

A potentially conflict place is a active conflict place *if the following condition holds: there exist $h \in H$, $l \in L$ and $X \in \{0,1\}$ such that:*

- *h setX s*
- *l test$(1-X)$ s*
- *there exists a marking $m \in [m_0\rangle$ and a transition sequence σ such that*
  - *$m[h\rangle$ and $m[\sigma l\rangle$*
  - *$s \in m$ iff $X = 0$*
  - *for all $t \in \sigma$: $\neg(t$ set1 $s)$ and $\neg(t$ set0 $s)$*

Definition 18. *Let $N = (S, L, H, F, m_0)$ be a trace net system. We say that N is PBNI+ (*positive Place Based Non-Interference*) if, for all $s \in S$, s is neither an active causal place nor an active conflict place.*

The definitions of parallel composition and restriction presented in Section 3 are extended to trace nets in the obvious way:

Definition 19. *Let $N_1 = (S_1, L_1, H_1, W_1, m_{0,1})$ and $N_2 = (S_2, L_2, H_2, W_2, m_{0,2})$ be two trace net systems such that $S_1 \cap S_2 = \emptyset$ and $(L_1 \cup L_2) \cap (H_1 \cup H_2) = \emptyset$. The parallel composition of N_1 and N_2 is the trace net system*
$N_1 \mid N_2 = (S_1 \cup S_2, L_1 \cup L_2, H_1 \cup H_2, W_1 \cup W_2, m_{0,1} \oplus m_{0,2})$

Definition 20. *Let $N = (S, L, H, W, m_0)$ be a trace net system and let U be a set of transitions. The restriction on U is defined as $N \backslash U = (S, L', H', W', m_0)$, where*
$L' = L \setminus U$
$H' = H \setminus U$
$W' = W \setminus (S \times U)$

The results presented in Section 3 continue to hold also for trace nets:

Theorem 6. *Let $N = (S, L, H, W, m_0)$ be a trace net system. N is BNDC if and only if N is SBNDC.*

Theorem 7. *Let $N = (S, L, H, W, m_0)$ be a trace net system. N is PBNI+ if and only if N is SBNDC.*

5.3 Example: binary memory cell

In this section we recast the example of a binary memory cell proposed in [3] in our framework.

A binary memory cell can contain a binary value, i.e., either 0 or 1. The memory cell is accessible to both high and low users, that can read and write a value in the cell. The trace net representing the binary cell is reported in Figure 8.

A token in place c_0 (resp. c_1) represents the fact that the current value contained in the cell is 0 (resp. 1). Each operation is modeled by two transitions,

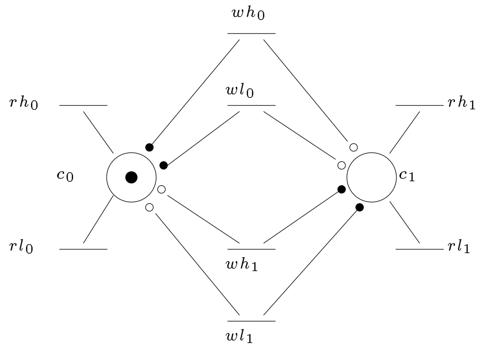

Fig. 8. The trace net modeling a binary memory cell.

one for each binary value that can be contained in the cell. For example, transition wh_0 (resp. wh_1) is performed by a high level user that writes the value 0 (resp. 1) in the cell. A write operation of e.g. value 0 in the cell is represented by a transition that sets the contents of place c_0 (i.e., puts one token in place c_0 regardless of its previous contents), and resets the contents of place c_1 (i.e., removes the possible token present in place c_1). A read operation of e.g. value 0 is represented by a transition with a read arc on place c_0, i.e., a transition that can happen only if place c_0 contains a tokens.

As already pointed out in [3], the binary memory cell depicted in Figure 8 is completely insecure, as a high level user can send confidential information to a low level user through the binary cell. In fact, the binary cell is not *PBNI+* because of the existence of (at least) the active causal place c_1. Note that c_1 is a potentially causal place, because the high transition wh_1 has a set arc on c_1, and the low transition rl_1 has a read arc on c_1. Moreover, if we consider the firing sequence $\{c_0\}[wh_1\rangle\{c_1\}[rl_1\rangle\{c_1\}$ also the conditions for the potentially causal place c_1 to be an active causal place are fulfilled.

In order to avoid the flow of information from the high user to the low user, we can either forbid all the read operations performed by a low user or forbid all the write operations performed by a high user, thus obtaining the trace nets depicted in Figures 9 and 10.

The trace nets obtained in this way do not contain any (potential) causal or conflict place.

6 Conclusion

A structural non-interference property *PBNI+* is proposed to firm more strongly the intuition about the nature of interferences and to obtain more efficiently checkable property. We start defining *PBNI+* for the simpler class of contact free elementary net systems, then the definition is extended to the richer class of trace net systems. We showed that *PBNI+* turns out to be equivalent to the

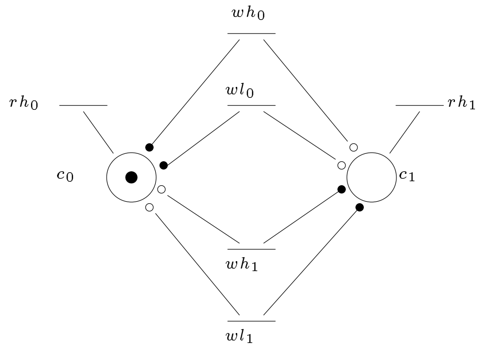

Fig. 9. The trace net obtained by removing the low level read operations.

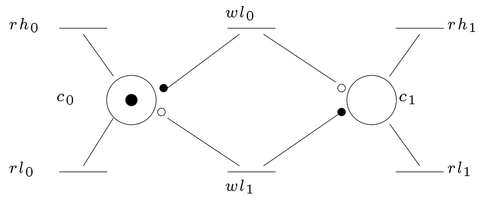

Fig. 10. The trace net obtained by removing the high level write operationsl.

behavioural property *SBNDC*, initially proposed in a process algebraic setting [7, 8].

The property *PBNI+* is structural because no notion of observational equivalence is considered in its definition; however, to be precise, the definition of *PBNI+* requires a limited exploration of the state space (marking graph), hence it is in some sense a *behavioural* property.

The main difference of *PBNI+* w.r.t. the non-interference properties *PBNI* and *RBNI*, introduced in [4, 5], is that *PBNI+* captures only flows of positive information from high users to low users, whereas *RBNI* (and in some cases also *PBNI*) capture both positive and negative flows. Consider for example the net system N_4 in Figure 6: the net N_4 does not satisfy *PBNI* and *RBNI*, because of the presence of the conflict place s. Indeed, there exists a negative information flow from high users to low users: if the low action l is performed, the low user knows that the high action h has not been performed (and will never be performed). On the other hand, N_4 is *PBNI+*, because s is not an active conflict place. Indeed, no positive information can flow from high users to low users.

The current investigation was conducted for two classes of "safe" net systems, i.e., for nets whose places can contain at most one token. A natural extension of this approach is to consider Place/Transition systems, where each place can contain more than one token.

References

1. E. Badouel and Ph. Darondeau. Trace nets and process automata. *Acta Informatica*, 32, 647–679, 1995.
2. E. Badouel and Ph. Darondeau. Theory of regions. *Lectures on Petri Nets I: Basic Models*, Springer LNCS 1491:529:586, 1998.
3. A. Bossi, R. Focardi, D. Macedonio, C. Piazza and S. Rossi. Unwinding in Information Flow Security. ENTCS, to appear.
4. N. Busi and R. Gorrieri. Structural Non-Interference with Petri Nets. Workshop on Issues in the Theory of Security (WITS'04), 2004.
5. N. Busi and R. Gorrieri. A Survey on Non-Interference with Petri Nets. Advanced Course on Petri Nets 2003, Springer LNCS, to appear.
6. J.Engelfriet and G. Rozenberg. Elementary Net Systems *Lectures on Petri Nets I: Basic Models*, Springer LNCS 1491, 1998.
7. R. Focardi, R. Gorrieri, *"A Classification of Security Properties"*, Journal of Computer Security 3(1):5-33, 1995
8. R. Focardi, R. Gorrieri, *"Classification of Security Properties (Part I: Information Flow)"*, Foundations of Security Analysis and Design - Tutorial Lectures (R. Focardi and R. Gorrieri, Eds.), Springer LNCS 2171:331-396, 2001
9. J.A. Goguen, J. Meseguer, *"Security Policy and Security Models"*, Proc. of Symposium on Security and Privacy, IEEE CS Press, pp. 11-20, 1982
10. C. A. Petri, *Kommunikation mit Automaten*, PhD Thesis, Institut für Instrumentelle Mathematik, Bonn, Germany, 1962.
11. W. Reisig, "Petri Nets: An Introduction", EATCS Monographs in Computer Science, Springer, 1985.
12. A.W. Roscoe, *"CSP and Determinism in Security Modelling"*, Proc. of IEEE Symposium on Security and Privacy, IEEE CS Press, pp. 114-127, 1995
13. P.Y.A. Ryan, *"Mathematical Models of Computer Security"*, Foundations of Security Analysis and Design - Tutorial Lectures (R. Focardi and R. Gorrieri, Eds.), Springer LNCS 2171:1-62, 2001
14. P.Y.A. Ryan, S. Schneider, *"Process Algebra and Noninterference"*, Proc. of 12th Computer Security Foundations Workshop, IEEE CS Press, pp. 214-227, 1999