# Assessment of Initial-State-Opacity in Live and Bounded Labeled Petri Net Systems via Optimization Techniques

Postprint version - Work published on Automatica (https://doi.org/10.1016/j.automatica.2023.110911)

Francesco Basile[a], Gianmaria De Tommasi[b], Carlo Motta[b]

[a]*DIEM, Università degli Studi di Salerno, 84084, Fisciano, Italy*
[b]*DIETI, Università degli Studi di Napoli Federico II, 80125 Napoli, Italy*

**Abstract**

Opacity is a property of discrete event systems (DES) that is related to the possibility of hiding a secret to external observers, the so called *intruders*. If the secret is the system initial state, then the related opacity problem is referred to as Initial State Opacity (ISO). This paper gives a necessary and sufficient condition to check ISO in DES modeled as bounded and live labeled Petri nets (PNs). The proposed approach relies on both the algebraic representation of labeled PNs dynamic, and on their structural representation in terms of minimal support T-invariants. The proposed necessary and sufficient condition enables ISO assessment by means of the solution of Integer Linear Programming problems, which can be efficiently solved nowadays by means of off-the-shelf optimization tools.

*Keywords:* opacity, labeled Petri nets, DES, integer linear programming

## 1. Introduction

Today's technological society is permeated by complex systems composed by multiple smart elements and devices interacting together by way of communication networks, often called distributed cyber-physical systems (CPSs). Examples of CPSs are autonomous automated highway systems, avionics, smart grids, and smart buildings. In CPSs, data are captured by physical objects or sensor devices and transferred through networks to the control system, which consequently becomes vulnerable to cyber-attacks. There is a great potential in this area for developing novel approaches using methodologies that pertain to discrete event systems (DESs [1]). Indeed, cyber-attacks act essentially at the higher levels of the control architecture, where the discrete event view is the most effective description of the system dynamics.

Various properties have been introduced to characterize privacy in the DES framework, the most common being non-interference [2, 3, 4] and opacity [5, 6, 7, 8]. This paper focuses on opacity, that is a property related to the possibility of hiding a secret to external observers (the so called *intruders*). In an opaque system, a user with full knowledge of the model, but with partial capabilities about the observation of the event occurrences cannot infer any secret, no matter for how long the system dynamic is partially observed.

When dealing with opacity, the secret is either a sublanguage of the language generated by the plant model (*language-based opacity*), or a system state, either initial, current or final (*state-based opacity*). When the latter type of opacity is considered, and the secret is the initial state the property is referred to as *Initial State Opacity* (ISO). A more general state-based notion of opacity is the so-called *infinite-step opacity* [9], which requires that any infinite sequence of events generates a sequence of observations that does not allow the intruder to infer that the state of the system, at any point in time (current, past, or initial), is revealed to belong in the given set of secret states

Opacity has been largely studied using finite state automata models [8], due to their dominant role in DES literature, and results in a relatively concise treatment of the topic, while also enabling extensions to richer automata models as well as other DES models. An effective alternative is to use Petri net (PN) models in view of their intuitive and compact graphical representation, and their convenient mathematical formulation. The main challenge in adopting an approach based on PNs is to avoid the construction of the corresponding Reachability Graph (RG, [10]), which in many ways will resemble a finite automaton, and therefore would imply no real advantages in using PN models.

In the existing literature, opacity problems in bounded PNs has been mainly solved resorting to graphs that try to represent in a compact way the RG. In [11], a graph called *basis reachability graph* (BRG), derived from the PN system and based on the notions of basis markings and explanations [12] is proposed. The approach proposed in [11] allows to avoid an exhaustive enumeration of the reachability space, since, depending on the net system, only a subset of reachable markings, i.e., the basis markings, should be enu-

merated, while other reachable markings are characterized by linear systems, one for each basis marking. Although in many cases the BRG is a compact representation of the RG, in the worst case the two graphs are the same. Such BRG-based approach has been also extended to the case of infinite-step (current-state) opacity in [13]. Authors of [14] proposed an approach that relies on a compact representation of the RG, the so called discernible reachability graph, and partially on mathematical programming, to deal with current state opacity, but under the assumption of partially (marking) observed nets. Along this line, recently results have been proposed in [15, 16] to verify also infinite step opacity.

Only few approaches have been proposed in literature that fully exploits the mathematical representation of PNs to avoid the explicit, although partial, state space estimation. In [17], the authors deal with current-state opacity, but a strong assumption on the secret is made, i.e., secret markings must be conjunction of a set of Generalized mutual Exclusion Constraints (GMECs). In [18], the same authors extended the approach also to ISO. However, compared to the one presented in this paper, the approach in [18] presents several limitations. Other than constraining the set of secret markings to be described by GMECs, both the subnets induced by observable and unobservable events need to be acyclic, while such an assumption is not made in this paper. Moreover, in our approach we consider an arbitrary set of uncertain initial markings, that includes both secret and non-secret ones. Such an assumption is made by the standard ISO definition given in [5], and is practically motivated by the fact that the intruder can know the system structure, but not the initial state. Finally, the approach proposed in [18] relies on the solution of optimization problems that depends on the sequence of observed events, therefore cannot be used to assess offline the ISO property.

The case of language-based opacity for systems modeled with PNs has been tackled in [19], although limited to secret languages with finite cardinality, while only a sufficient condition to assess non-ISO for unlabeled PNs is given in [20].

In this paper, we deal with labeled PNs, which are used to model the system under consideration. The observation function is assumed to be static and the states (i.e., the net markings) are not observable. Each event is naturally associated at least to one transition.

The main contribution of this work is a necessary and sufficient condition to verify if a live and bounded labeled net system is ISO. Liveness and boundedness are not strong assumptions, since they are basic properties usually required in practice. Moreover, generally privacy assessment is not a requirement tackled in the first step of system design. Therefore, it is reasonable that such additional requirement is applied to a system only after resource sharing and deadlock issues have been solved making it live and bounded.

The key problem addressed in this paper requires to check if, for any word that may occur from a secret initial marking, there exists at least another one with the same projection over the set of observable events, that is enabled from at least one of the non-secret initial markings. The main technique exploited in the paper to perform this assessment relies on the exact characterization of the reachability space of a given live and bounded PN through a finite set of linear inequalities. Moreover, for the considered class of systems, we exploit also the possibility to represent in a convenient way the sequences of enabled transitions by means of net structural components. Indeed, live and bounded systems are characterized by the existence of ergodic components in the RG, i.e. set of markings forming a subgraph of the RG, with no edges leading from a node that belongs to the considered component, to a node that does not belong to it. This behavior has also structural representation, being live and bounded systems also consistent. Consistency is a property that guarantees the existence of a T-invariant that *covers* all net transitions, i.e. with all positive components [21]. Such a specific invariant characterizes, in vector form, the sequences that may occur within each ergodic component, and those ones that bring the system from the initial marking to one that belongs to an ergodic component. This property of live and bounded nets helps to characterizes the system sequences in terms of linear inequalities, and to reduce the complexity when solving the considered opacity problem.

The remainder of the paper is organized as follows: the next section introduces the adopted PNs notation and some preliminary results. The main contribution of this paper, which is the necessary and sufficient condition to assess ISO, is given in Section 3. Section 4 shows the effectiveness of the proposed approach by means of some numerical examples. Finally some conclusions and future perspectives are drawn.

## 2. PRELIMINARIES

The adopted notation for labeled Petri net systems together with some basic definitions are introduced in this section. The concept of ISO is also recalled together with a preliminary result taken from [22]. The main assumptions exploited to derive the proposed necessary and sufficient condition are presented at the end of the section.

### *2.1. Notation*

In what follows different products will be considered. We will denote with " $\cdot$ " the standard matrix multiplication, while " $\circ$ " will denote the Hadamard product.

In this paper we deal with labeled Petri net systems. Let first briefly introduce the concept

of *Place/Transition* (P/T) net. A P/T net is a 4-tuple $N = (P, T, \mathbf{Pre}, \mathbf{Post})$, where $P$ is a set of $m$ places (represented by circles) and $T$ is a set of $n$ transitions (represented by boxes). $\mathbf{Pre} : P \times T \mapsto \mathbb{N}$ and $\mathbf{Post} : P \times T \mapsto \mathbb{N}$) are the *pre-* and *post-incidence* matrices, respectively. $\mathbf{Pre}(p,t) = w$ ($\mathbf{Post}(p,t) = w$) means that there is an arc with weight $w$ from $p$ to $t$ (from $t$ to $p$); $\boldsymbol{C} = \mathbf{Post} - \mathbf{Pre}$ is the incidence matrix.

A *marking* is a function $\overrightarrow{m} : P \mapsto \mathbb{N}$ that assigns to each place of a net a nonnegative integer number of tokens, drawn as black dots. The marking of a net is usually represented by a vector $\overrightarrow{m} \in \mathbb{N}^m$.

A *net system* $S = \langle N, \overrightarrow{m}_0 \rangle$ is a net $N$ with an initial marking $\overrightarrow{m}_0$. A transition $t$ is enabled at $\overrightarrow{m}$ if and only if $\overrightarrow{m} \geq \mathbf{Pre}(\cdot, t)$, and this is denoted as $\overrightarrow{m}[t\rangle$. An enabled transition $t$ may fire, bringing the system to the marking

$$\overrightarrow{m}' = \overrightarrow{m} + \boldsymbol{C}(\cdot, t)\,,$$

and this is denoted as $\overrightarrow{m}[t\rangle\overrightarrow{m}'$.

A *firing sequence* enabled from $\overrightarrow{m}$ is a sequence of transitions $\sigma = t_1 t_2 \ \ldots \ t_k$ such that $\overrightarrow{m}\big[t_1\rangle\overrightarrow{m}_1\big[t_2\rangle\overrightarrow{m}_2 \ \ldots \big[t_k\rangle\overrightarrow{m}_k$, and this is denoted as $\overrightarrow{m}[\sigma\rangle\overrightarrow{m}_k$. The notations $\overrightarrow{m}\big[\sigma\rangle$ denotes an enabled sequence under a marking $\overrightarrow{m}$. Furthermore, $t_i \in \sigma$ denotes that the transition $t_i$ belongs to the sequence $\sigma$, and the length of $\sigma$ is denoted with $|\sigma|$.

A marking $\overrightarrow{m}'$ is said to be *reachable* from $\overrightarrow{m}_0$ if and only if there exists a sequence $\sigma$ such that $\overrightarrow{m}_0[\sigma\rangle\overrightarrow{m}'$. The set $R(N, \overrightarrow{m}_0)$ contains all the reachable markings of the net system $\mathcal{S} = \langle N, \overrightarrow{m}_0 \rangle$. The language of a Petri net system $\mathcal{S}$ is defined as follows[1]

$$L(N\,, \overrightarrow{m}_0) = \left\{\sigma \in T^* \mid \overrightarrow{m}_0\big[\sigma\rangle\right\}\,. \tag{1}$$

The function $\overrightarrow{\sigma} : T \mapsto \mathbb{N}$, where $\overrightarrow{\sigma}(t)$ represents the number of occurrences of $t$ in $\sigma$, is called *firing count vector* of the firing sequence $\sigma$. As it has been done for the marking of a net, the firing count vector is usually represented by a vector $\overrightarrow{\sigma} \in \mathbb{N}^n$. The notation $\overrightarrow{\sigma} = \pi(\sigma)$ is used to denote that $\overrightarrow{\sigma}$ is the firing count vector corresponding to $\sigma$.

If $\overrightarrow{m}_0[\sigma\rangle\overrightarrow{m}$, then it is well known that the so-called *state equation* of the net system holds

$$\overrightarrow{m} = \overrightarrow{m}_0 + \boldsymbol{C} \cdot \overrightarrow{\sigma}\,. \tag{2}$$

We now introduce some basic definitions commonly given for P/T net and net systems. For more details, the interested readers can refer to [23] or [10, 21].

**Definition 1.** *(Reachability graph and live ergodic components [24, 25]) Given a net system* $\mathcal{S} = \langle N\,, \overrightarrow{m}_0 \rangle$ *and its reachability set* $R(N\,, \overrightarrow{m}_0)$*, the reachability graph is a labeled directed graph* $RG(N\,, \overrightarrow{m}_0) = (V\,, Edge\,, l)$ *with* $l : Edge \mapsto T$ *given by:*

- $V = R(N\,, \overrightarrow{m}_0)$*;*
- $((\overrightarrow{m}\,, \overrightarrow{m}') \in Edge \wedge l(\overrightarrow{m}\,, \overrightarrow{m}') = t) \Leftrightarrow \overrightarrow{m}\big[t\rangle\overrightarrow{m}'$*.*

*Given the reachability graph of a net system, let us denote with* $U$ *a subset of nodes* $U \subseteq R(N\,, \overrightarrow{m}_0)$*, and with* $U^\bullet = \left\{\overrightarrow{m}' \in R(N\,, \overrightarrow{m}_0) \mid (\overrightarrow{m}\,, \overrightarrow{m}') \in Edge\,, \overrightarrow{m} \in U\right\}$*.*
*The set* $\mathrm{succ}(U)$ *of successors of* $U$ *is the minimal set such that* $U^\bullet \subseteq \mathrm{succ}(U)$ *and* $\mathrm{succ}(U)^\bullet \subseteq \mathrm{succ}(U)$*. The subgraph of* $(V\,, Edge\,, l)$ *induced by* $U$ *is defined by*

$$G(U) = \left(U\,, (U \times U) \cap Edge\,, l|_{(U\times U)\cap Edge}\right)\,,$$

*where* $l|_{(U\times U)\cap Edge}$ *denotes the restriction of* $l$ *to the subset* $(U \times U) \cap Edge$*.*
*The set of labels of* $G(U)$ *is denoted with* $\Xi$*. The subset of nodes* $U$ *is said to be an* ergodic *component if and only if* $(U = \{v\} \wedge v^\bullet = \emptyset)$ *or* ($G(U)$ *is strongly connected and* $U = \mathrm{succ}(U)$*). Ergodic components of the first kind are also called deadlocks, while those of the second kind are called active ergodic components or, when* $\Xi = T$*, live ergodic components.* ◊

**Definition 2** (T-invariant)**.** *Given a net* $N$*, a vector* $\overrightarrow{y} \in \mathbb{N}^n$ *is called* T-invariant *if* $\boldsymbol{C} \cdot \overrightarrow{y} = \overrightarrow{0}$*.* ◊

**Remark 1.** *From Definition 2, it follows that the occurrence of any enabled sequence* $\sigma$ *such that* $\overrightarrow{m}\big[\sigma\rangle$ *with* $\overrightarrow{m} \in R(N\,, \overrightarrow{m}_0)$ *whose firing count vector coincides with a T-invariant, produces a null net marking variation. Therefore, the occurrence of such sequences, takes the PN system back to the starting marking (state)* $\overrightarrow{m}$*.* ▲

The set of transitions

$$||\overrightarrow{y}|| = \{t_j \in T \mid \overrightarrow{y}(t_j) > 0\}\,,$$

is called the support of the T-invariant. A T-invariant $\overrightarrow{y}$ has minimal support if there does not exist another T-invariant $\overrightarrow{y}'$ such that $||\overrightarrow{y}'|| \subset ||\overrightarrow{y}||$. A T-invariant $\overrightarrow{y}$ is minimal if there does not exist another T-invariant $\overrightarrow{y}$ such that $\overrightarrow{y}' \leq \overrightarrow{y}$. A *minimal support* (MS) T-invariant has minimal support and is minimal. The set of MS T-invariants $\mathcal{T}(N)$ is finite and constitutes a basis, i.e. any T-invariant can be obtained by linear combination of MS T-invariants. Algorithms to compute the set $\mathcal{T}(N)$ ([26]) have been implemented in off-the-shelf tools, such as TINA [27].

[1] The notation $T^*$ denotes the Kleene closure of $T$ (see [1, Ch. 2]).

**Definition 3** (Consistency). *A net $N$ is said to be* consistent *if and only if it is covered by T-invariants, i.e. if there exists a T-invariant $\overrightarrow{y} > \overrightarrow{0}$.* ◊

**Definition 4** (Boundedness). *A net system $\mathcal{S}$ is said to be* bounded *if the number of tokens in each place does not exceed a finite number $k$ for any marking $\overrightarrow{m} \in R(N, \overrightarrow{m}_0)$* ◊

**Definition 5** (Liveness). *A net system $\mathcal{S}$ is said to be* live *if all transitions $t \in T$ are live. A transition $t$ is said to be live if $\forall\ \overrightarrow{m} \in R(N, \overrightarrow{m}_0), \exists\ \overrightarrow{m}'$ such that $\overrightarrow{m}' \in R(N, \overrightarrow{m})$ and $\overrightarrow{m}'[t\rangle$.* ◊

When dealing with ISO, the information we are interested in hiding is the initial marking of the net, in what follows we will consider net systems with uncertain initial marking. To this aim we define $\mathcal{M}_0 \subseteq \mathbb{N}^m$ as the set of all the possible initial markings. Systems with uncertain initial marking are denoted as $\mathcal{S} = \langle N, \mathcal{M}_0 \rangle$.

Labeled P/T nets allow to map events to the transitions; in particular, the same event can be associated to more than one transitions.

**Definition 6** (Labeled P/T net system). *A labeled P/T net system is the triple $\mathcal{G} = \langle N, \mathcal{M}_0, \lambda \rangle$, where $N$ is a standard P/T net, $\mathcal{M}_0$ is the initial marking set, and*

$$\lambda : T \mapsto E \cup \{\varepsilon\} ,$$

*is the* labeling function *which assigns to each transition $t \in T$ an event from the set $E$, where $\varepsilon$ is the silent event.* ◊

In the following we will denote with

$$T^e = \{t \in T \mid \lambda(t) = e, \text{with } e \in E\} ,$$

the set of transitions associated with the same event $e$. We denote with $\text{card}(T^e)$ the cardinality of set $T^e$, and with $w$ the word of events associated to a sequence $\sigma$, i.e. $w = \lambda(\sigma)$, assuming the usual extension of the labeling function to sequences of transitions and events, that is by considering $\lambda : T^* \mapsto E^*$. As for sequences of transitions, given a word $w$ we will denote with $|w|$ its length, and $|\varepsilon| = 0$ by definition.

Given a labeled net system with uncertain initial marking, the concept of language (1) is extended as follows

$$\mathcal{L}(\mathcal{G}, \mathcal{M}_0) = \{w \in E^* \mid w = \lambda(\sigma) \text{ with } \overrightarrow{m}_0[\sigma\rangle \text{ and } \overrightarrow{m}_0 \in \mathcal{M}_0\} .$$

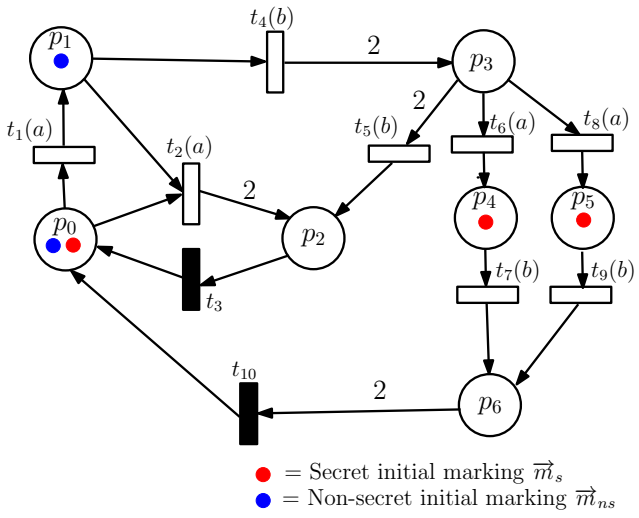


Figure 1: Example of labeled Petri net system with two unobserbable transitions ($t_3$ and $t_{10}$), a single secret marking (shown as red tokens), and a single non-secret ones (shown as blue tokens).

When dealing with opacity, $E$ is partitioned into the two disjoint sets of *observable* (whose correspondent transitions are represented by empty boxes) and *unobservable* events (whose correspondent transitions are represented by filled boxes), named respectively $E_o$ and $E_{uo}$.

Given a word $w \in E^*$, its observation is the output of the *natural projection function* $\text{Pr} : E^* \mapsto E_o^*$, which is recursively defined as

$$\text{Pr}(we) = \text{Pr}(w)\,\text{Pr}(e) ,$$

with $w \in E^*$ and $e \in E$; moreover, $\text{Pr}(e) = e$ if $e \in E_o$, while $\text{Pr}(e) = \varepsilon$ if $e \in E_{uo}$.

The partition between observable and unobservable events in a labeled P/T net induces a similar partition on the set of transitions $T$. Therefore $T = T_o \cup T_{uo}$, where

$$T_o = \{t \in T \mid \lambda(t) \in E_o\} ,$$
$$T_{uo} = \{t \in T \mid \lambda(t) \in E_{uo}\} ,$$

and obviously $T_o \cap T_{uo} = \emptyset$. Without lack of generality, in what follows it is assumed that for every $\bar{t} \in T_{uo}$ it is $\lambda(\bar{t}) = \varepsilon$.

Moreover, given $T = T_o \cup T_{uo}$ and $T_o \cap T_{uo} = \emptyset$, we denote with $\mathbf{Pre}_o$ ($\mathbf{Pre}_{uo}$) the restriction of the pre-incidence matrix to the set of observable (unobservable) transitions. The same applies for $\mathbf{Post}_o$ ($\mathbf{Post}_{uo}$) and $\boldsymbol{C}_o$ ($\boldsymbol{C}_{uo}$).

**Example 1.** *To illustrate some of the concepts introduced so far, consider the net shown in Fig. 1. The net has 7 places, $p_0, \ldots, p_6$ and 10 transitions, $t_1, \ldots, t_{10}$, while the corresponding set of events is $E = \{a, b\}$.*

*Given the choice of the labeling function $\lambda(\cdot)$ reported in Fig. 1, it is*

$$T^a = \{t_1\,, t_2\,, t_6\,, t_8\}\ ,$$
$$T^b = \{t_4\,, t_5\,, t_7\,, t_9\}\ ,$$

*where the two events $a$ and $b$ are assumed observable, while the two transitions $t_3$ and $t_{10}$ are assumed to be associated to unobservable events, being represented as filled boxes in Fig. 1. Therefore $t_3$ and $t_{10}$ are labeled with the silent event, i.e. $\lambda(t_3) = \lambda(t_{10}) = \varepsilon$.*

*The considered system has an uncertain initial marking, being*

$$\mathcal{M}_0 = \left\{(1\ 1\ 0\ 0\ 0\ 0\ 0)^T\,, (1\ 0\ 0\ 0\ 1\ 1\ 0)^T\right\}\ .$$

*Moreover, the rows of the following matrix $Y$ are the four MS T-invariant contained in $\mathcal{T}(N)$*

$$Y = \begin{pmatrix} \overrightarrow{y}_1^T \\ \overrightarrow{y}_2^T \\ \overrightarrow{y}_3^T \\ \overrightarrow{y}_4^T \end{pmatrix} = \begin{pmatrix} 1\ 1\ 2\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0 \\ 1\ 0\ 0\ 1\ 0\ 2\ 2\ 0\ 0\ 1 \\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 2\ 2\ 1 \end{pmatrix}\ . \tag{3}$$

▲

### 2.2. Initial State Opacity in Labeled Systems

When dealing with ISO, the $\mathcal{M}_0$ set is split into two disjoint subsets: the set of *secret* markings $\mathcal{M}_s$ and of *non-secret* markings $\mathcal{M}_{ns}$.

Given the system $\mathcal{G} = \langle N\,, \mathcal{M}_0\,, \lambda\rangle$ with $\mathcal{M}_0 = \mathcal{M}_s \cup \mathcal{M}_{ns}$ and $\mathcal{M}_s \cap \mathcal{M}_{ns} = \emptyset$, we give the following definition of ISO system (see also [5]).

**Definition 7.** *A labeled net system $\mathcal{G}$ with uncertain initial marking belonging to $\mathcal{M}_0$ is ISO* if and only if

$$\forall\ \overrightarrow{m}_s \in \mathcal{M}_s \text{ and } \forall\ w \in \mathcal{L}(\mathcal{G}\,, \overrightarrow{m}_s)\,, \exists\ \overrightarrow{m}_{ns} \in \mathcal{M}_{ns} \text{ and } \exists\ w' \in \mathcal{L}(\mathcal{G}\,, \overrightarrow{m}_{ns}) \text{ s.t. } \Pr(w) = \Pr(w')\,. \tag{4}$$

◊

**Example 2.** *Let us refer again to the labeled system shown in Fig. 1. In this case, it is easy to verify that if $\mathcal{M}_s = \{\overrightarrow{m}_s\} = \left\{(1\ 0\ 0\ 0\ 1\ 1\ 0)^T\right\}$ and $\mathcal{M}_{ns} = \{\overrightarrow{m}_{ns}\} = \left\{(1\ 1\ 0\ 0\ 0\ 0\ 0)^T\right\}$ the systems turns out to be ISO. Indeed, $\overrightarrow{m}_s(p_0) = \overrightarrow{m}_{ns}(p_0) = 1$, and for any sequence $\sigma_s$ enabled by $\overrightarrow{m}_s(p_4)$ and $\overrightarrow{m}_s(p_5)$, there is a sequence $\sigma_{ns}$ enabled by $\overrightarrow{m}_{ns}(p_1)$ such that*

$$\Pr\left(\lambda(\sigma_s)\right) = \Pr\left(\lambda(\sigma_{ns})\right)\ .$$

▲

### 2.3. Preliminary result

The next result is taken from [22] and will be extensively exploited in Section 3. It gives a necessary and sufficient condition that must be fulfilled by every sequence with finite length enabled under the marking $\overrightarrow{m}$.

**Lemma 1** ([22])**.** *There exists $\rho$ integer vectors $\overrightarrow{s}_1, \ldots, \overrightarrow{s}_\rho \in \mathbb{N}^n$ with $\rho \leq |\sigma|$ such that the following linear constraints are fulfilled*

$$\begin{aligned} &\overrightarrow{m}_0 \geq \mathbf{Pre}\cdot \overrightarrow{s}_1 \\ &\overrightarrow{m}_0 + \boldsymbol{C}\cdot \overrightarrow{s}_1 \geq \mathbf{Pre}\cdot \overrightarrow{s}_2 \\ &\ldots \\ &\overrightarrow{m}_0 + \boldsymbol{C}\cdot \sum_{i=1}^{\rho-1} \overrightarrow{s}_i \geq \mathbf{Pre}\cdot \overrightarrow{s}_\rho \end{aligned} \tag{5a}$$

$$\sum_{i=1}^{\rho} \overrightarrow{s}_i = \pi(\sigma) \tag{5b}$$

iff *there exists at least one sequence $\sigma$, which is enabled under the marking $\overrightarrow{m}_0$ such that $\pi(\sigma) = \overrightarrow{\sigma}$.*

### 2.4. Assumptions

We now introduce the assumptions that will be exploited in Section 3 to assess ISO in DES modeled as PN systems, together with the corresponding properties that can be derived once these assumptions hold.

**Assumption 1.** *The net system $\mathcal{S}$ is assumed to be bounded for any initial marking in the set $\mathcal{M}_0$.* ◊

**Remark 2.** *For bounded systems there exists an integer $\mathcal{J}_{\min}$ such that if $J \geq \mathcal{J}_{\min}$, then for each $\overrightarrow{m} \in R(N\,, \overrightarrow{m}_0)$ there exists at least one set of vectors $\overrightarrow{s}_1, \ldots, \overrightarrow{s}_J$ that fulfill the constraints* (5a) *and*

$$\overrightarrow{m} = \overrightarrow{m}_0 + \boldsymbol{C}\cdot \sum_{i=1}^{J} \overrightarrow{s}_i\,.$$

*In other words, for bounded systems $\mathcal{J}_{\min}$ firing count vectors are sufficient to describe the reachability set $R(N\,, \overrightarrow{m}_0)$ by means of the constraints* (5a)*. Although in the worst case $\mathcal{J}_{\min}$ may be equal to $\mathrm{card}\left(R\left(N\,, \overrightarrow{m}_0\right)\right) - 1$, in many cases $\mathcal{J}_{\min} \ll \mathrm{card}\left(R\left(N\,, \overrightarrow{m}_0\right)\right) - 1$. For a bounded but* non live *net system, an estimation of $\mathcal{J}_{\min}$ can be carried out by using the reachability graph of the system itself. For bounded and live systems and estimation of $\mathcal{J}_{\min}$ can be computed exploiting the concept of T-invariant; an upper bound to $\mathcal{J}_{\min}$ is given by*[2]*:*

$$\mathcal{J}_{\min} \leq 2\cdot \|\overrightarrow{m}_0\|_1 \cdot \left\| \sum_{y\in\mathcal{T}(N)} \overrightarrow{y} \right\|_1\ .$$

*For a more comprehensive discussion on this issue, the interested reader can refer to [28, Sec. 3].* ▲

[2] $\|\cdot\|_1$ denotes the 1-norm of a vector, that is the sum of the absolute values of the vector elements.

**Assumption 2.** *The net system $\mathcal{S}$ is assumed to be live for any initial marking in the set $\mathcal{M}_0$.* ◊

**Remark 3.** *Assumptions 1 and 2 imply that the net $N$ is consistent (see [29]).* ▲

**Example 3.** *The system reported in Fig. 1 is bounded and live for the two initial markings in $\mathcal{M}_0$ and is also covered by MS T-invariant, as can be easily verified by inspecting the entries of matrix* (3). ▲

It is worth to notice that Assumptions 1 and 2 do not imply structural boundedness and liveness, since this two properties must hold only for the markings in the set $\mathcal{M}_0$. Morever, if these two assumptions hold, the next lemma follows.

**Lemma 2.** *Given a net system $\mathcal{S}$, the fulfilment of Assumptions 1 and 2 imply that the firing count vector of any enabled sequence $\sigma \in L(N, \overrightarrow{m}_0)$ is* covered *by a weighted sum of MS T-invariants, i.e. $\forall\, \sigma \in L(N, \overrightarrow{m}_0)$ it is*

$$\overrightarrow{\sigma} \leq \sum_{\overrightarrow{y}_i \in \mathcal{T}(N)} k_i \overrightarrow{y}_i\,, \tag{6}$$

*with $k_i \in \mathbb{N}$.* ▲

*Proof.* First of all, let us recall that, due to Assumption 2, all the ergodic components of the reachability graph for the considered net system $\mathcal{S}$ are live.

Therefore, once the system *reaches* a marking in an ergodic component, being the system also bounded, inequality (6) readily follows from net consistency (see Remark 3).

As for the sequences that bring the system from the initial marking to a live ergodic component, also in this case the corresponding firing count vectors are such that inequality (6) holds. Indeed, if this would not be the case the system would be either non-live – if the sequences *consume* tokens – or unbounded – if the sequences *generate* tokens – (see also Remark 1), which contradicts our Assumptions 1 and 2. □

## 3. MAIN RESULT

The theorem presented in what follows represents the main contribution of this paper, that is a necessary and sufficient condition to assess ISO in labeled systems that meet the assumptions introduced in Section 2.4.

Given $J \geq \mathcal{J}_{\min}$ (see also Remark 2), the proposed approach requires the solution of the ILP (7)–(8) for each secret marking $\overrightarrow{m}_s \in \mathcal{M}_s$, and for each MS T-invariant $\overrightarrow{y} \in \mathcal{T}(N)$. In (7)–(8), $B \in \mathbb{N}$ denotes a sufficiently large positive integer, while $\overrightarrow{1}$ denotes the vector with all elements equal to 1.

$$\max \left\{ \sum_{j=1}^{J} \left[ (J-j+1) \cdot \sum_{\tau \in \| \overrightarrow{y} \|_o} \overrightarrow{s}_j(\tau) + B \cdot b_j \right] \right\} \tag{7}$$

subject to

$$\begin{cases} \overrightarrow{m}_s \geq \mathbf{Pre}_{uo} \cdot \overrightarrow{\epsilon}_{s_1} \\ \overrightarrow{m}_s + \boldsymbol{C}_{uo} \cdot \overrightarrow{\epsilon}_{s_1} \geq \mathbf{Pre}_o \cdot \overrightarrow{s}_1 \\ \overrightarrow{m}_s + \boldsymbol{C}_{uo} \cdot \overrightarrow{\epsilon}_{s_1} + \boldsymbol{C}_o \cdot \overrightarrow{s}_1 \geq \mathbf{Pre}_{uo} \cdot \overrightarrow{\epsilon}_{s_2} \\ \dots & \text{(8a)} \\ \overrightarrow{m}_s + \boldsymbol{C}_{uo} \cdot \sum_{j=1}^{J} \overrightarrow{\epsilon}_{s_j} + \boldsymbol{C}_o \cdot \sum_{j=1}^{J-1} \overrightarrow{s}_j \geq \mathbf{Pre}_o \cdot \overrightarrow{s}_J \\ \sum_{j=1}^{J} \overrightarrow{s}_j(\tau) \geq \overrightarrow{y}(\tau)\,, \quad \forall\, \tau \in T_o & \text{(8b)} \\ \overrightarrow{s}_j \leq B(1-b_j) \cdot \overrightarrow{1}\,, \quad j = 1, \dots, J & \text{(8c)} \\ \overrightarrow{\epsilon}_{s_j},\ \overrightarrow{s}_j \in \mathbb{N}^n\,, \qquad j = 1, \dots, J & \text{(8d)} \\ b_j \in \{0, 1\}\,, \qquad j = 1, \dots, J & \text{(8e)} \end{cases}$$

Due to constraint (8b), the vectors $\overrightarrow{s}_j$ that solve (7)–(8) correspond to a sequence of transitions enabled under the secret marking $\overrightarrow{m}_s$, and their sum $\sum_{j=1}^{J} \overrightarrow{s}_j$ *covers* the observable part of the given MS T-invariant $\overrightarrow{y}$.

Moreover, thanks to the presence of term $\sum_{j=1}^{J} B \cdot b_j$ in (7) and of the constraint (8c), the number of not null firing count vectors $\overrightarrow{s}_j$ is minimized. Finally, the decreasing weights in the term

$$\sum_{j=1}^{J} (J-j+1) \cdot \sum_{\tau \in \| \overrightarrow{y} \|_o} \overrightarrow{s}_j(\tau)\,,$$

of the objective function (7) allow to maximize the number of firings in each not null $\overrightarrow{s}_j$, as far as this is compatible with the enabling constraints (8a). As a result, the firing count vectors that solve (7)–(8) contain as much firings of observable transitions of $\overrightarrow{y}$ as possible.

**Remark 4.** *Let $\overrightarrow{s}^{\star}_k$ be the not null firing count vectors that solve problem* (7)–(8)*, with $k = 1, \dots, K \leq J$. In order to assess ISO, the proposed approach tries to find a sequence of transitions enabled from one of the non secret markings in $\mathcal{M}_{ns}$, whose corresponding words have the same projection on the observable events as the words that correspond to $\overrightarrow{s}^{\star}_k$. In order to do that, in what follows, the set of optimization vectors $\overrightarrow{q}_{k,1}, \dots, \overrightarrow{q}_{k,L_k} \in \mathbb{N}^n$, with*[3] *$L_k = \| \overrightarrow{s}^{\star}_k \|_1$, is used to justify each observable occurrence in $\overrightarrow{s}^{\star}_k$ with a sequence of unobservable transitions.* ▲

[3] $\| \cdot \|_1$ denotes the 1-norm of a vector, that is the sum of the absolute values of the vector elements.

**Theorem 1.** *Let $\mathcal{G} = \langle N, \mathcal{M}_0, \lambda \rangle$ be a labeled system bounded and live $\forall\ \vec{m}_0 \in \mathcal{M}_0$, and let $E = E_{uo} \cup E_o$, with $E_{uo} \cap E_o = \emptyset$, and $\mathcal{M}_0 = \mathcal{M}_s \cup \mathcal{M}_{ns}$, with $\mathcal{M}_s \cap \mathcal{M}_{ns} = \emptyset$; moreover, let $\mathcal{T}(N)$ be the set of MS T-invariants of $N$.*

*For a given secret marking $\vec{m}_s$ and MS T-invariant $\vec{y}$, let $\vec{s}^{\star}_1, \ldots, \vec{s}^{\star}_K$ be the not null vectors $\vec{s}_j$ that solve the ILP problem (7)–(8).*

*System $\mathcal{S}$ is ISO* if and only if *the feasibility problem (9) admits a solution $\forall\ \vec{m}_s \in \mathcal{M}_s$ and $\forall\ \vec{y} \in \mathcal{T}(N)$*[4].

$$
\begin{cases}
\vec{\mu} \geq \mathbf{Pre}_{uo} \cdot \vec{e}^{\,1}_{1,1} \\
\vec{\mu} + \boldsymbol{C}_{uo} \cdot \vec{e}^{\,1}_{1,1} \geq \mathbf{Pre}_{uo} \cdot \vec{e}^{\,2}_{1,1} \\
\cdots \\
\vec{\mu} + \boldsymbol{C}_{uo} \cdot \sum_{j=1}^{J} \vec{e}^{\,j}_{1,1} \geq \mathbf{Pre}_{o} \cdot \vec{q}_{1,1} & \text{(9a)} \\
\vec{\mu} + \boldsymbol{C}_{uo} \cdot \sum_{j=1}^{J} \vec{e}^{\,j}_{1,1} + \boldsymbol{C}_{o} \cdot \vec{q}_{1,1} \geq \mathbf{Pre}_{uo} \cdot \vec{e}^{\,1}_{1,2} \\
\cdots \\
\vec{\mu} + \boldsymbol{C}_{uo} \cdot \sum_{k=1}^{K} \sum_{i=1}^{L_k} \sum_{j=1}^{J} \vec{e}^{\,j}_{k,i} + \boldsymbol{C}_{o} \cdot \sum_{k=1}^{K-1} \sum_{i=1}^{L_{K-1}} \vec{q}_{k,i} \\
\quad + \boldsymbol{C}_{o} \cdot \sum_{i=1}^{L_K - 1} \vec{q}_{K,i} \geq \mathbf{Pre}_{o} \vec{q}_{K,L_K} \\
\sum_{i=1}^{L_k} \sum_{\tau \in T^e} \vec{q}_{k,i}(\tau) = \sum_{\tau \in T^e} \vec{s}^{\star}_{k}(\tau), \quad \forall\ e \in E_o, \quad k = 1, \ldots, K, \\
\qquad\qquad \text{and } i = 1, \ldots, L_k & \text{(9b)} \\
\vec{\mu} = \sum_{i=1}^{\mathrm{card}(\mathcal{M}_{ns})} \vec{m}_{ns_i} \circ (\mu_i \cdot \vec{1}) & \text{(9c)} \\
\sum_{i=1}^{\mathrm{card}(\mathcal{M}_{ns})} \mu_i = 1 & \text{(9d)} \\
\vec{e}^{\,j}_{k,i} \in \mathbb{N}^n, \quad j = 1, \ldots, J, k = 1, \ldots, K, i = 1, \ldots, L_k & \text{(9e)} \\
\vec{q}_{k,i} \in \mathbb{N}^n, \quad k = 1, \ldots, K, i = 1, \ldots, L_k & \text{(9f)} \\
\mu_i \in \{0, 1\}, \quad i = 1, \ldots, \mathrm{card}(\mathcal{M}_{ns}) & \text{(9g)}
\end{cases}
$$

*Proof.* Before proving the result, let us notice that, due to the constraints (9a), (9b), (9e) and (9f) the solution of problem (9) represents an *unobservable explanation* of the words whose observable projections are equal to the ones of the words that correspond to the solution $\vec{s}^{\star}_1, \ldots, \vec{s}^{\star}_K$ of (7)–(8). Moreover, constraints (9c)–(9d) and (9g) imply that that such unobservable explanation is enabled starting from one of the non-secret markings in $\mathcal{M}_{ns}$. Indeed, according to Lemma 1 (see also Remark 4), up to $J \geq \mathcal{J}_{\min}$ unobservable firing count vectors $\vec{e}^{\,j}_{k,i}$ are used in (9a) to explain each of the $L_k$ firings in $\vec{s}^{\star}_k$, with $k = 1, \ldots, K$.

*(if)*: in order to prove sufficiency, for a system $\mathcal{S}$ that meets Assumptions 1-2, let us assume that for each secret marking $\vec{m}_s \in \mathcal{M}_s$ and for each MS T-invariant $\vec{y} \in \mathcal{T}(N)$ the feasibility problem (9) admits a solution and, *ad absurdum*, that the system is not ISO. From Definition 7, if the system is not ISO then

$$
\exists\ \vec{m}'_s \in \mathcal{M}_s \text{ and } \exists\ w \in \mathcal{L}(\mathcal{G}, \vec{m}'_s), \forall\ \vec{m}_{ns} \in \mathcal{M}_{ns} \\
\text{and } \forall\ w' \in \mathcal{L}(\mathcal{G}, \vec{m}_{ns}) \text{ s.t. } \Pr(w) \neq \Pr(w'). \quad (10)
$$

Being $\mathcal{G}$ live and bounded for all markings in both $\mathcal{M}_s$ and $\mathcal{M}_{ns}$, Lemma 2 holds, implying that the firing count vector that corresponds to any sequence that in turns corresponds to an enabled word, either $w \in \mathcal{L}(\mathcal{G}, \vec{m}'_s)$ or $w' \in \mathcal{L}(\mathcal{G}, \vec{m}_{ns})$, is covered by a weighted sum of MS T-invariants (see Lemma 6). Therefore, given a secret marking such that (10) holds, there should be at least a MS T-invariant $\vec{y}'$ such that constraint (9b) is not fulfilled, which contradicts the initial assumption. Hence, if the feasibility problem (9) admit a solution for all $\vec{m}_s \in \mathcal{M}_s$ and for all $\vec{y} \in \mathcal{T}(N)$, then the system $\mathcal{G}$ is ISO.

*(only if).* Let us now assume, *ad absurdum*, that the system is ISO and there exists at least one secret marking $\vec{m}'_s \in \mathcal{M}_s$ and one MS T-invariant $\vec{y}' \in \mathcal{T}(N)$ such that the feasibility problem (9) does not admit a solution. It follows that it is not possible to find any non-secret marking able to *justify* the occurrence of the observable events to which the firings in the solution $\vec{s}^{\star}_1, \ldots, \vec{s}^{\star}_K$ maps to. Therefore there exists at least one word enabled from $\vec{m}'_s \in \mathcal{M}_s$ such that the property (4) does not hold, which contradicts the initial ISO assumption. It follows that if the system $\mathcal{G}$ is ISO, then problem (9) must admit a solution for all secret markings and all MS T-invariants. □

## 4. NUMERICAL EXAMPLES

In this section we show the effectiveness of the proposed condition to assess ISO in labeled systems by means of some examples.

Let us first consider the labeled system of Fig. 1. As already discussed in Example 2, with the given choice of secret and non-secret markings the system is ISO. Indeed, if we set $J = 6$ and we check the condition of Theorem 1, it turns out that the feasibility problem (9) is feasible for all the MS T-invariant in (3).

A different outcome can be drawn if we switch the secret and non-secret markings. If this is the case, it can be readily noticed that when $\vec{m}_s = (1\ 1\ 0\ 0\ 0\ 0\ 0)^T$ the word $w = aaa$ is such that $w \in \mathcal{L}(\mathcal{G}, \vec{m}_s)$, but $w \notin \mathcal{L}(\mathcal{G}, \vec{m}_{ns})$. Hence with this choice of secret and non-secret markings, the system is not ISO. Checking again the feasibility problem of Theorem 1 with $J = 6$, this turns to be unfeasible when the MS T-invariant $\vec{y}_1$ in (3) is considered.

The second example we consider in this section is based on the case study originally presented in [30]. Let us consider the campus map shown in Fig. 2. The campus is covered by four coarse regions, namely $A$, $B$, $C$

[4] In constraint (9c) "$\circ$" denotes the Hadamard product.

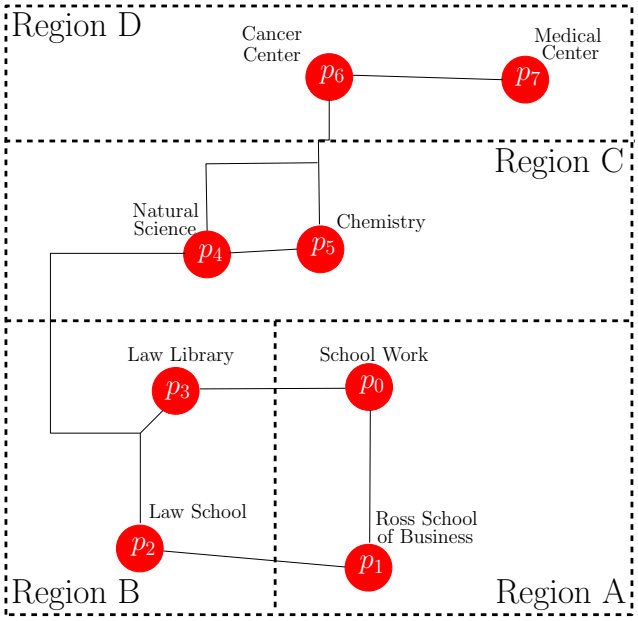


Figure 2: Campus map taken from the case study considered in [30], considered in Section 4.

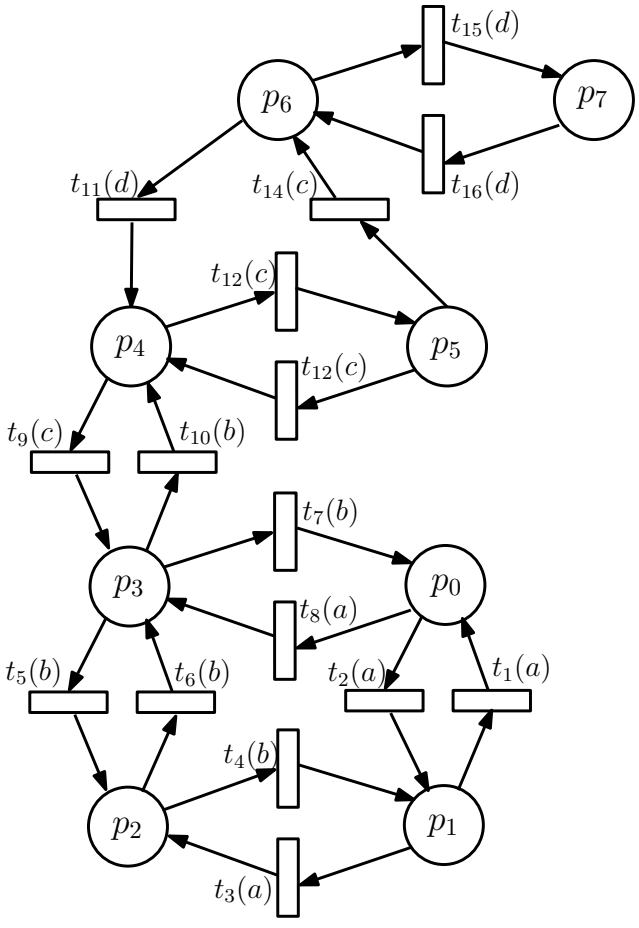


Figure 3: Labeled Petri net model of the walking paths of the campus whose map is shown in Fig. 2. It is assumed that this paths are monitored by a Location-Based Service that is able to detect the various events.

and $D$, in each of which two points of interest are selected. People moving in the campus are traced by a Location-Based Service (LBS) which provides networked services based on user location. In such a scenario, there is a privacy concern, since a malicious intruder may infer users' location by observing the events exchanged with the LBS.

The labeled net system of Fig. 3 models the events generated by a LBS user that moves in the campus. Each transition is labeled with the name of the coarse region a user is moving from, i.e. the source position. The events of the model in Fig. 3 are those monitored by the LBS, that can be also potentially intercepted by a malicious user.

The net in Fig. 3 is structurally bounded, being connected and belonging to a special class of Petri net, i.e. it is a so called *state machine* [23]. Moreover, being strongly connected, the considered net is also live for any possible initial marking [23]. Hence, according to Remark 3, the net is consistent and is covered by the ten MS T-invariants included as rows in the following matrix

$$Y' = \begin{pmatrix} \overrightarrow{y}_1^T \\ \overrightarrow{y}_2^T \\ \overrightarrow{y}_3^T \\ \overrightarrow{y}_4^T \\ \overrightarrow{y}_5^T \\ \overrightarrow{y}_6^T \\ \overrightarrow{y}_7^T \\ \overrightarrow{y}_8^T \\ \overrightarrow{y}_9^T \\ \overrightarrow{y}_{10}^T \end{pmatrix} = \begin{pmatrix} 1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0 \end{pmatrix} .$$

These invariants have been computed on a simple laptop by using the TINA tool, and the time needed for the computation is less than 1 $ms$. Our intent is to verify whether every possible initial position of an individual meet the privacy requirement. If this is not the case, we exploit Theorem 1 to find the minimum set of events by obscuring which to the intruder, the system is made ISO.

Let us consider a user starting from the region $D$, which, according to the scheme of the campus, has only two zones of interest which are the "Cancer Center" and the "Medical Center". Assuming that the user does not want the intruder to know that she/he has been in any of those two points of interest, we set up the first instance for this case study by selecting two secret initial markings corresponding to a token in $p_6$ or $p_7$, respectively, i.e.

$$\mathcal{M}_s = \{\overrightarrow{m}_{s_1}, \overrightarrow{m}_{s_2}\} = \{(0\,0\,0\,0\,0\,0\,1\,0)^T, \\ (0\,0\,0\,0\,0\,0\,0\,1)^T\} .$$

Similarly each of the six non-secret initial markings is obtained by positioning one token in the place that corresponds to one of the places in the set $\{p_0, \ldots, p_5\}$.

If we set $E_o = E = \{a, b, c, d\}$ and $J = 10$, the feasibility problem (9) fails at least for the MS T-invariant $\overrightarrow{y}_8$, implying that the system is not ISO. That outcome can be readily checked for both secret initial markings but, for sake of simplicity, let us consider the secret marking $\overrightarrow{m}_{s_1}$ from which the word $w = dc$ is enabled. This same word cannot be generate by starting from any of the non-secret markings.

For the same choice of the two sets $\mathcal{M}_s$ and $\mathcal{M}_{ns}$, and by letting $E_o = E\backslash\{c\}$, if we apply Theorem 1 the system in Fig. 3 turns out to be ISO.

Let now consider a second case study that deals again with the LBS model shown in Fig. 3. In particular, we run $N = 8$ tests, by recursively selecting the secret marking as follows

$$\overrightarrow{m}_{s_n}(p_i) = \begin{cases} 0, & i \neq n \\ 1, & i = n \end{cases}$$

with $n = 1, \ldots, N$. For each of those secret markings there are seven non-secret ones each of which is obtained by positioning one token in the place $p_j$ with $j \neq n$. Hence, when $\mathcal{M}_s$ is set equal to

$$\overrightarrow{m}_{s_1} = (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0)^T\ ,$$

then $\mathcal{M}_{ns}$ is set equal to

$$\Big\{(0\ 1\ 0\ 0\ 0\ 0\ 0\ 0)^T\ , (0\ 0\ 1\ 0\ 0\ 0\ 0\ 0)^T\ , \ldots, (0\ 0\ 0\ 0\ 0\ 0\ 0\ 1)^T\Big\}\ .$$

By setting again $J = 10$ and by applying Theorem 1, the system turns out to be not ISO when the set of observable events is set equal to $E_{o_1} = E\backslash\{c\}$.

That outcome can be readily checked by considering $\overrightarrow{m}_s = (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0)^T$, and the enable sequence:

$$\sigma_{p_0} = a\ b\ c\ c\ d\,,$$

obtained by considering the MS T-invariant $\overrightarrow{y}_6$, whose projection is equal to:

$$Pr(\sigma_{p_0}) = a\ b\ d\,.$$

Such a projection cannot be mimicked when starting from any of the non-secret markings. This is confirmed by our algorithm since the feasibility problem in (9) is unable to find a solution.

Therefore we need to shrink the observable subspace by letting $E_{o_2} = E\backslash\{a, c\}$, being $E_{o_3} = E\backslash\{b, c\}$ a valid solution as well. Indeed, for both choices, the eight instances of the feasibility problems (9) admit a solution, implying the system to be ISO.

Although it is well known that ILP problems have NP-hard complixity, in order to give some indication about the computational burden practically needed to apply the proposed method, in Table 1 we summarize some figures obtained when solving the various optimization problems in the Matlab environment by using the GLPK [31] solver on a PC with Intel® Core™ i7-1165G7 CPU 2.80 GHz and 16 GB of RAM. In particular, the data reported in Table 1 refers to the case when $J = 10$, and we consider the three observable sets discussed, namely $E_{o_1}$, $E_{o_2}$ and $E_{o_3}$. The table compares the total number of optimization variables and constraints to solve both the optimization problem (7)–(8) and the feasibility one (9).

As it can be readily seen, for a given net and a given $J$, both the number of constraints and optimization variables for the problem (7)–(8) do not depend on the chosen initial secret marking and MS T-invariant. On the other hand, the size of the feasibility problem (9) depends on the outcome retrieved from (7)–(8), which in turn depends on the choices made for the initial secret marking and on the the MS T-invariant. Out of clarity, for this case study, we report the outcome only for $\overrightarrow{m}_s = (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0)^T$ and the T-invariant $\overrightarrow{y} = \overrightarrow{y}_6$. It is worth to notice that each of the eight instances included in the second case study requires the solution of 10 optimization problems (7)–(8) as well as 10 feasibility problems (9); therefore 80 optimization and feasibility problems are to be solved. We reported the average time needed to find a solution to each one of them together with the standard deviation, and the total time needed to *construct*[5] and solve each of those.

Let us now consider a last case study applied on the LBS model shown in Fig. 3, chosen to highlight how the size of problem (9) grows as a function of the number of tokens in the initial marking, which is chosen as follows:

$$\overrightarrow{m}_{s_n}(p_i) = \begin{cases} 0, & i \neq n \\ \chi, & i = n \end{cases}$$

where $\chi$ is a variable that varies from 2 to 8. The problem so defined is indeed ISO regardless of $\chi$, both for $E_o = E\backslash\{a, c\}$ and $E_o = E\backslash\{b, c\}$. In Table 2 are reported some figures of the outcome retrieved by considering $E_o = E\backslash\{a, c\}$ and $J = 10$. The first column represents the total number of states in the reachability set and has been retrieved leveraging the TINA tool; in the second and third columns are reported the number of optimization variables and constraints, respectively, used for solving the feasibility problem (9) when $\overrightarrow{m}_s = (\chi\ 0\ 0\ 0\ 0\ 0\ 0\ 0)^T$ and the T-invariant $\overrightarrow{y} = \overrightarrow{y}_6$. The fourth column is the average time needed to solve a single feasibility problem;

[5]The total time needed to *construct* the problem includes the time needed by the script to generate the problem itself and the time needed by the YALMIP [32] parser to parse it before invoking the solver.

Table 1: Figures of computational strain to solve problems (7)–(8) and (9)

| **Observable events** | **Optimization Variables for** (7)–(8) \ (9) | **Constraints for** (7)–(8) \ (9) | **Average time to solve a single problem** (7)-(8) | **Average time to solve a single problem** (9) | **Total time to generate and solve the 80 problems** (7)–(8) | **Total time to generate and solve the 80 problems** (9) |
|---|---|---|---|---|---|---|
| $E_{o_1} = E\backslash\{c\}$ | 170 \ 163 | 446 \ 420 | $199 \pm 28\ ms$ | $1.9 \pm 0.7\ ms$ | $29.2\ s$ | $152\ ms$ |
| $E_{o_2} = E\backslash\{a, c\}$ | 170 \ 176 | 404 \ 357 | $74.4 \pm 19\ ms$ | $1.4 \pm 0.5\ ms$ | $16.2\ s$ | $112\ ms$ |
| $E_{o_3} = E\backslash\{b, c\}$ | 170 \ 194 | 393 \ 374 | $49.6 \pm 18\ ms$ | $1.3 \pm 0.4\ ms$ | $14\ s$ | $104\ ms$ |

Table 2: Figures of computational strain with increasing tokens in the secret marking when $E_o = E\backslash\{a, c\}$.

| **Number of tokens in** $\overrightarrow{m}_s$ | **States in Reachability set** $\mathbb{R}$ | **Optimization Variables for** (9) | **Constraints for** (9) | **Average time to solve a single problem** (9) | **Total time to generate and solve the 80 problems** (9) |
|---|---|---|---|---|---|
| $\chi = 2$ | 36 | 359 | 709 | $8\ ms$ | $640\ ms$ |
| $\chi = 3$ | 120 | 535 | 1061 | $18\ ms$ | $7.475\ s$ |
| $\chi = 4$ | 330 | 711 | 1413 | $43\ ms$ | $11.84\ s$ |
| $\chi = 5$ | 792 | 887 | 1773 | $69\ ms$ | $18.9\ s$ |
| $\chi = 6$ | 1716 | 1063 | 2125 | $108\ ms$ | $28.8\ s$ |
| $\chi = 7$ | 3432 | 1239 | 2477 | $143\ ms$ | $32.7\ s$ |
| $\chi = 8$ | 6435 | 1415 | 2821 | $197\ ms$ | $36.6\ s$ |

finally the total time needed to solve the 80 feasibility problems is reported in the last column.

As a final comment, note that the figures reported in Table 1 and Table 2 are acceptable for the off-line ISO assessment, which is the objective of the proposed result. Moreover, the performance can be further improved by considering ad-hoc hardware and software solutions rather than a standard PC and off-the-shelf software tools.

## 5. CONCLUSIONS

A necessary and sufficient condition to assess ISO in labeled live and bounded system has been given in this paper. The provided result relies on the solution of optimization problems in the form of ILP problems, which can be efficiently solved by using off-the-shelf tools (see also [33]). Possible future lines of research includes the extension of the approach to both *current* and *initial-and-final* opacity [5], and the exploitation of the proposed necessary and sufficient condition to dynamic enforce opacity by means of supervisory control, similarly to what has been proposed in the context of non-interference [34].

## References


[1] C. Cassandras, S. Lafortune, Introduction to Discrete Event Systems (3rd edition), Springer, 2021.

[2] N. Busi, R. Gorrieri, A Survey on Non-interference with Petri Nets, in: Lectures on Concurrency and Petri Nets, Springer, 2004, pp. 328–344.

[3] P. Baldan, A. Beggiato, Multilevel transitive and intransitive non-interference, causally, Theoretical Computer Science 706 (2018) 54–82.

[4] F. Basile, M. Boccia, G. De Tommasi, C. Motta, C. C. Sterle, An optimization-based approach to assess non-interference in labeled and bounded Petri net systems, Nonlinear Analysis: Hybrid Systems 44 (2022) 101153.

[5] Y. Wu, S. Lafortune, Comparative analysis of related notions of opacity in centralized and coordinated architectures, Discrete Event Dynamic Systems 23 (3) (2013) 307–339.

[6] R. Jacob, J. Lesage, J. Faure, Overview of discrete event systems opacity: Models, validation, and quantification, Annual Reviews in Control 41 (2016) 135–146.

[7] S. Lafortune, F. Lin, C. Hadjicostis, On the history of diagnosability and opacity in discrete event systems, Annual Reviews in Control 45 (2018) 257–266.

[8] C. Hadjicostis, Estimation and Inference in Discrete Event Systems, Springer, 2020.

[9] A. Saboori, C. Hadjicostis, Verification of infinite-step opacity and analysis of its complexity, in: 2nd IFAC Workshop on Dependable Control of Discrete Systems, 2009, pp. 46–51.

[10] M. Cabasino, A. Giua, C. Seatzu, Introduction to Petri Nets, in: Control of Discrete-Event Systems, Springer, 2013, pp. 191–211.

[11] Y. Tong, Z. Li, C. Seatzu, A. Giua, Verification of state-based opacity using Petri nets, IEEE Transactions on Automatic Control 62 (6) (2017) 2823–2837.

[12] M. Cabasino, A. Giua, C. Seatzu, Fault detection for discrete event systems using Petri nets with unobservable transitions, Automatica 46 (9) (2010) 1531–1539.

[13] H. Lan, Y. Tong, C. Seatzu, Verification of infinite-step opacity using labeled petri nets, IFAC-PapersOnLine 53 (2) (2020) 1729–1734.

[14] I. Saadaoui, Z. Li, N. Wu, Current-state opacity modelling and verification in partially observed Petri nets, Automatica 116 (2020) 108907.

[15] Y. Tong, H. Lan, C. Seatzu, Verification of K-step and infinite-step opacity of bounded labeled Petri nets, Automatica 140 (2022) 110221.

[16] Z. Ma, X. Yin, Z. Li, Verification and enforcement of strong infinite- and k-step opacity using state recognizers, Automatica 133 (2021) 109838.

[17] X. Cong, M. Fanti, A. Mangini, Z. Li, On-line verification of current-state opacity by Petri nets and integer linear programming, Automatica 94 (2018) 205–213.

[18] X. Cong, M. Fanti, A. Mangini, Z. Li, On-line verification of initial-state opacity by Petri nets and integer linear programming, ISA Transactions 93 (2019) 108–114.
[19] F. Basile, G. De Tommasi, An algebraic characterization of language-based opacity in labeled Petri nets, IFAC-PapersOnLine 51 (7) (2018) 329–336.
[20] G. De Tommasi, C. Motta, A. Petrillo, S. Santini, Optimization-Based Assessment of Initial-State Opacity in Petri Nets, in: Optimization and Data Science: Trends and Applications, 2021, pp. 127–138.
[21] M. Cabasino, A. Giua, C. Seatzu, Structural Analysis of Petri Nets, in: Control of Discrete-Event Systems, Springer, 2013, pp. 213–233.
[22] F. García Vallés, Contributions to the structural and symbolic analysis of place/transition nets with applications to flexible manufacturing systems and asynchronous circuits, Ph.D. thesis, Departamento de Informática e Ingeníeria de Sistemas, Centro Politecnico Superior, Universidad de Zaragoza (1999).
[23] T. Murata, Petri nets: Properties, analysis and applications, Proc. of IEEE 77 (4) (1989) 541–580.
[24] E. Teruel, M. Silva, Liveness and home states in equal conflict systems, in: Proceedings of the 14th International Conference on Application and Theory of Petri Nets, London, UK, 1993, pp. 415–432.
[25] P. Góra, Graph Theoretic Bound on Number of A.C.I.M. for Random Transformation, Proc. American Math. Soc. 116 (2) (1992) 401–410.
[26] A. Bourjij, M. Boutayeb, D. Koenig, T. Cecchin, On generating a basis of invariants in Petri nets, in: 1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation, Vol. 3, 1997, pp. 2228–2233.
[27] B. Berthomieu, F. V. P-.O. Ribet, The tool TINA–construction of abstract state spaces for Petri nets and time Petri nets, Int. J. Production Res. 42 (14) (2004) 2741–2756.
[28] F. Basile, P. Chiacchio, G. De Tommasi, On $\mathcal{K}$-diagnosability of Petri nets via integer linear programming, Automatica 48 (9) (2012) 2047–2058.
[29] M. Silva, E. Teruel, J. Colom, Linear Algebraic and Linear Programming Techniques for the Analysis of Place/Transition Net Systems, in: Lectures Notes in Computer Science, Vol. 616, Springer-Verlag, 1992, pp. 309–373.
[30] Y. Wu, K. Sankararaman, S. Lafortune, Ensuring privacy in location-based services: An approach based on opacity enforcement, IFAC-PapersOnLine 47 (2) (2014) 33–38.
[31] GLPK (GNU Linear Programming Kit), https://www.gnu.org/software/glpk/.
[32] J. Löfberg, YALMIP : A Toolbox for Modeling and Optimization in MATLAB, in: Proc. CACSD Conference, Taipei, Taiwan, 2004.
[33] F. Basile, A. Boussif, G. De Tommasi, M. Ghazel, C. Sterle, Efficient diagnosability assessment via ILP optimization: a railway benchmark, in: 23rd IEEE International Conference on Emerging Technologies and Factory Automation, Torino, Italy, 2018, pp. 441–448.
[34] F. Basile, G. De Tommasi, C. Sterle, Non-interference enforcement via supervisory control in bounded Petri nets, IEEE Transactions on Automatic Control 66 (2021) 3653–3666.

**Francesco Basile** Francesco Basile received the Laurea degree cum laude in electronic engineering and the Ph.D. degree in electronic and computer engineering from the University of Naples, Naples, in 1995 and 1999, respectively. In 1999, he was a Visiting Researcher with the Departamento de Ingenieria Informatica y Systemas, University of Zaragoza, Zaragoza, Spain, for six months. He is currently Full Professor of Automatic Control with the Dipartimento di Ingegneria dell'informazione ed elettrica e matematica applicata, Università di Salerno, Fisciano, Italy. He has published over 130 papers on international journals and conferences. His current research interests include modeling and control of discrete event systems, automated manufacturing, and robotics. Prof. Basile has been Associate Editor of the International Journal of Robotics and Automation, IEEE Transactions on Control Systems Technology and IEEE Transactions on Automation Science and Engineering. He has been member of IEEE Control System Society Conference Editorial Board. He is Associate Editor of IEEE Control Systems Letters. He has beeen General Chair of 14th International Workshop on Discrete Event Systems (WODES 2018).

**Gianmaria De Tommasi** was born in Milan, Italy, in 1975. He received the Laurea degree (summa cum laude) in electronic engineering and the Research Doctorate degree in computer and automatic engineering from the University of Naples Federico II, Naples, Italy, in 2001 and 2005, respectively. He is currently a Full Professor of Automatic Control with the Department of Electrical Engineering and Information Technology, University of Naples Federico II. He has been a Visiting Researcher with the Joint European Torus, Oxfordshire, U.K., the ITER Organization, Saint Paul-lez-Durance, France, the Experimental Advanced Superconducting Tokamak, Hefei, China, and the International Fusion Research Centre, Rokkasho, Japan, where he has participated in various projects connected to the plasma magnetic control systems. His current research interests include control of nuclear fusion devices, fault detection, and security of discrete-event systems modeled with Petri nets. He coauthored two monographs titled *Finite-Time Stability and Control* and *Finite-Time Stability: An Input-Output Approach.*

**Carlo Motta** Received his M.S. Degree in Automation Engineering (summa cum laude) from the University of Naples Federico II in 2020 with a thesis based on the development of methodologies to avoid collisions in trajectory planning for a bi-manual robotic system. He is now a PhD Student in Information Technology and Electrical Engineering. His research interests include but are not limited to assessment and enforcement of resilience and security properties in control systems.