Resilience to Failures and Reconfigurations in the Supervision Based on Place Invariants

Marian V. Iordache and **Panos J. Antsaklis**
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556
iordache.1@nd.edu

July 2, 2004

The Terms

We show that the SBPI has remarkable qualities for designs tolerant to failures and reconfigurations that may lead to minor supervision updates.

Failures: Changes in the structure or state of the plant model due to the occurrence of faults.

Reconfigurations: Changes in the supervisory goals.

Failures $\longrightarrow$ modified plant structure or state.

Reconfigurations $\longrightarrow$ modified specification.

Response to failures/reconfigurations:

Update the supervisor structure and/or state to implement current specification on the current plant model for the current state.

Outline

We show that the SBPI has remarkable qualities for designs tolerant to failures and reconfigurations that may lead to minor supervision updates.

The talk is organized as follows:

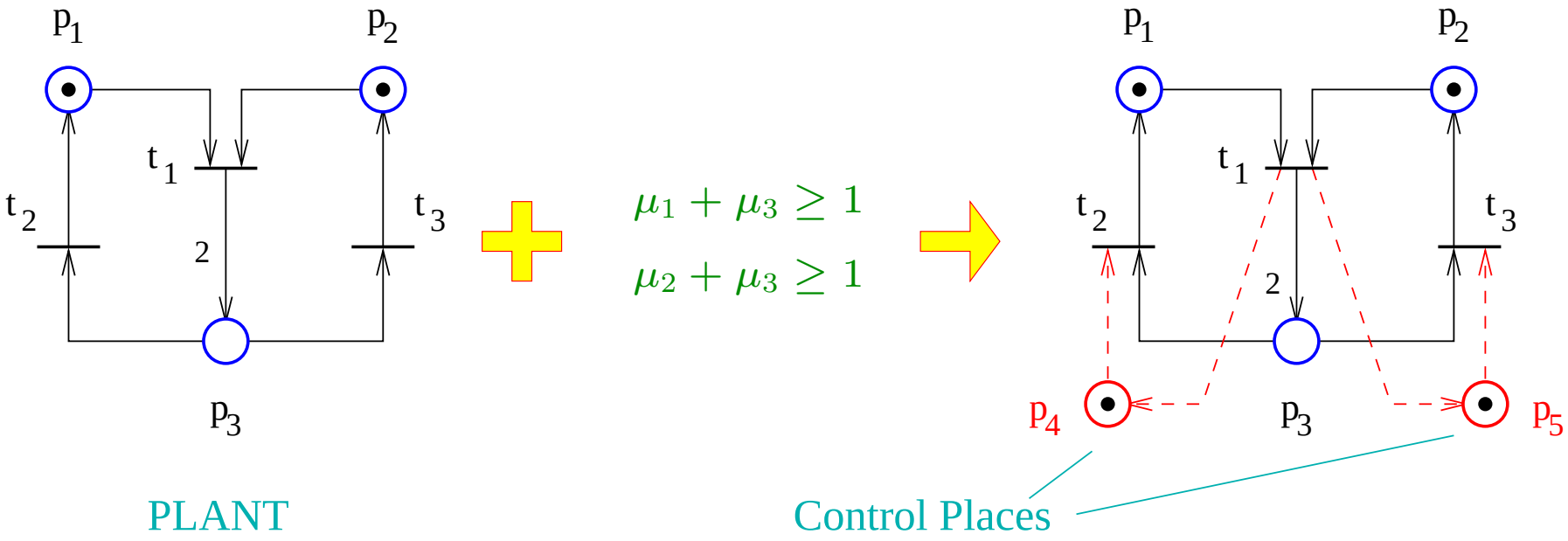
1. Overview of the SBPI
2. The structural approach for liveness enforcement
3. Properties of interest for fault-tolerance
4. Final Remarks

Overview of the SBPI

In the *supervision based on place invariants (SBPI)* we are given:

1. as plant, a PN
2. as specification, a set of constraints $L\mu \leq b$.

The supervisor is designed as a set of **control places**.



PLANT:

incidence matrix: D

initial marking: μ_0

SUPERVISOR:

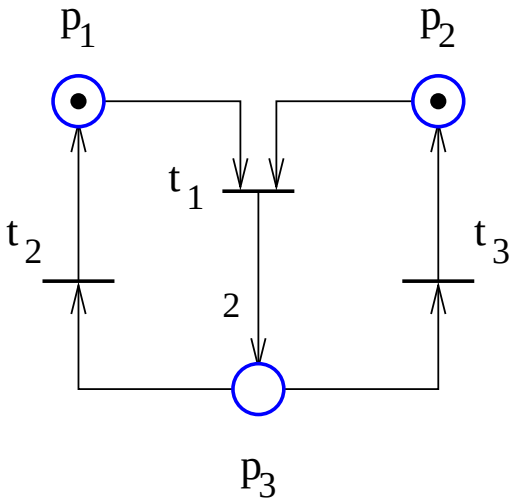
inc. matrix: $D_s = -LD$

ini. marking: $\mu_{s0} = b - L\mu_0$

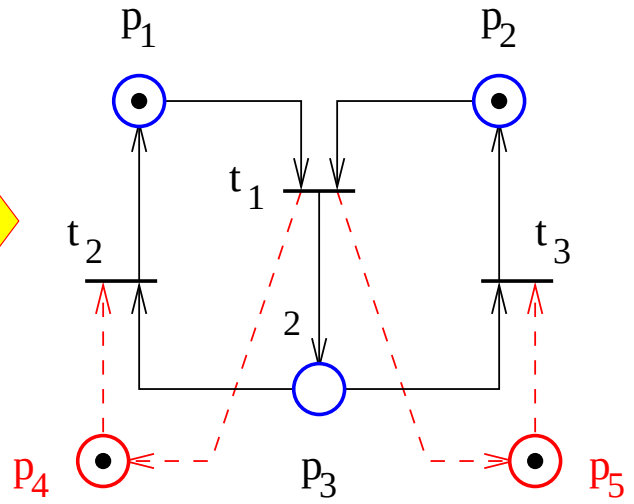
CLOSED LOOP:

inc. matrix: $D_c = \begin{bmatrix} D \\ D_s \end{bmatrix}$

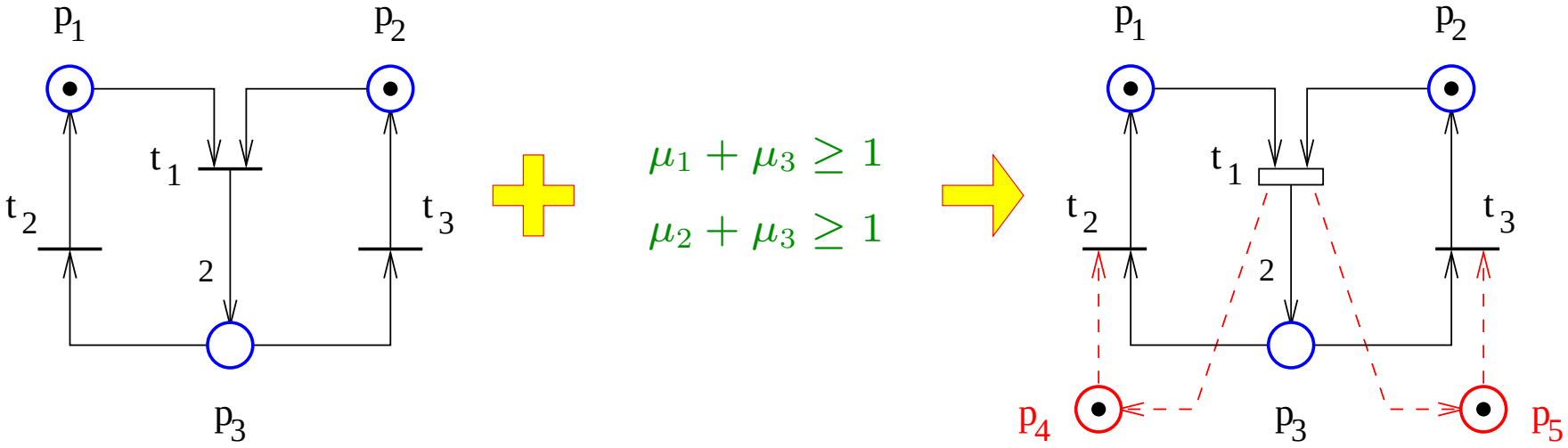
ini. marking: $\mu_c = \begin{bmatrix} \mu_0 \\ \mu_{s0} \end{bmatrix}$



$$\mu_1 + \mu_3 \geq 1$$
$$\mu_2 + \mu_3 \geq 1$$



$$D = \begin{bmatrix} -1 & 1 & 0 \\ -1 & 0 & 1 \\ 2 & -1 & -1 \end{bmatrix} \qquad D_s = -LD = \begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 0 \end{bmatrix}$$



Assume t_1 unobservable ...

Problem: the firing of t_1 varies the markings of the supervisor!

A supervisor design should not attempt inhibiting uncontrollable transitions or observing unobservable transitions.

A supervisor design should not attempt inhibiting uncontrollable transitions or observing unobservable transitions.

Structural Admissibility Conditions:

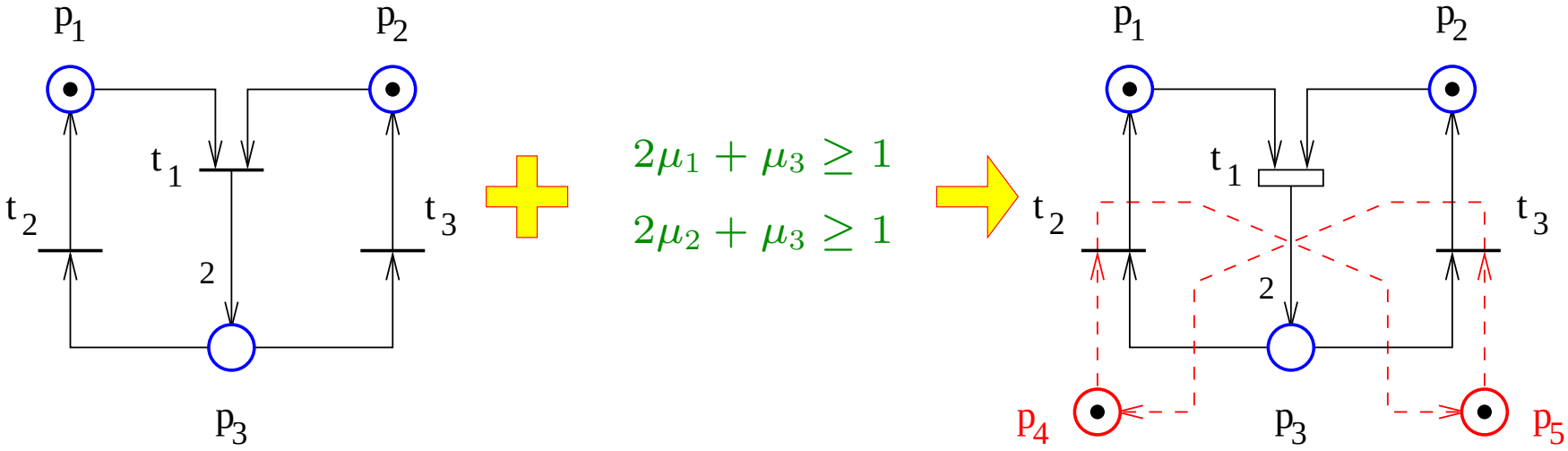
$$LD(\cdot, T_{uo}) = 0 \text{ and } LD(\cdot, T_{uc}) \leq 0 \quad (1)$$

T_{uc}/T_{uo}: the sets of uncontrollable/unobservable transitions.

Given $L\mu \leq b$ and a plant:

1. **If** L satisfies (1) **then**
   the supervisor has $D_s = -LD$ and $\mu_{s0} = b - L\mu_0$.
2. **Else** transform $L\mu \leq b$ to $L_a\mu \leq b_a$ such that:
   (a) $L_a\mu \leq b_a \Rightarrow L\mu \leq b$
   (b) L_a satisfies (1)
   the supervisor has $D_s = -L_aD$ and $\mu_{s0} = b_a - L_a\mu_0$.

$$\begin{cases} \mu_1 + \mu_3 \geq 1 \\ \mu_2 + \mu_3 \geq 1 \end{cases}$$ (inadmissible) ⇒ $$\begin{cases} 2\mu_1 + \mu_3 \geq 1 \\ 2\mu_2 + \mu_3 \geq 1 \end{cases}$$ (admissible)



This structural approach

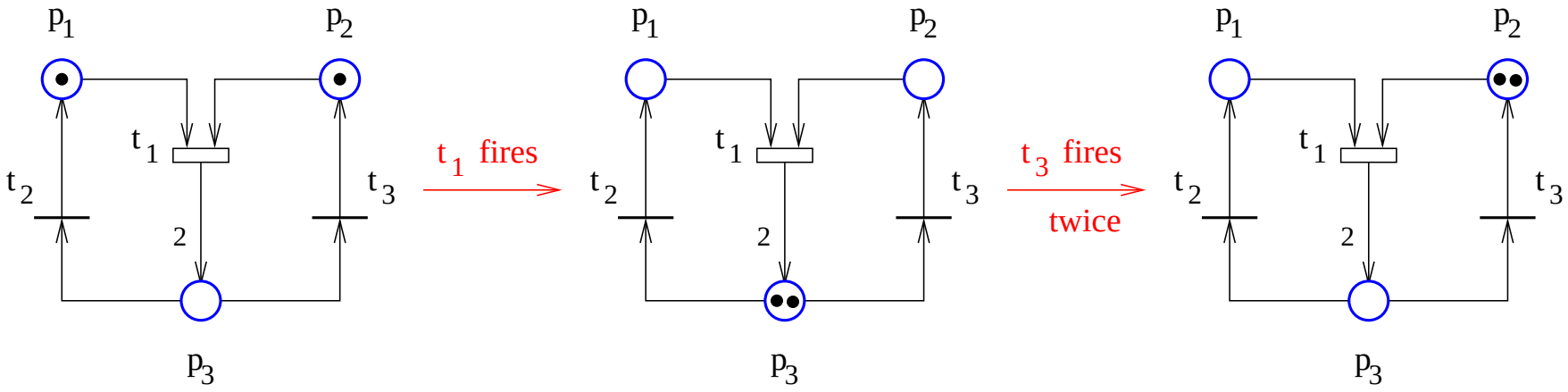
1. is computationally efficient
2. is modular
3. can approach more general PNs (e.g. labeled PNs)
4. but may result in suboptimal designs
5. ***has benefits for fault-tolerant designs***

Outline

We show that the SBPI has remarkable qualities for designs tolerant to failures and reconfigurations.

The talk is organized as follows:

1. Overview of the SBPI
2. *The structural approach for liveness enforcement*
3. Properties of interest for fault-tolerance
4. Final Remarks



Supervision constraints may also cause deadlocks.

A structural approach extending the SBPI for liveness enforcement is available.

Given a subset of transitions $\mathcal{T}$, the liveness enforcement procedure generates (if it terminates) two sets of constraints:

- $C\mu \leq d$: describes the supervisor enforcing $\mathcal{T}$-liveness;
- $C_0\mu \leq d_0$: additional constraints on μ_0.

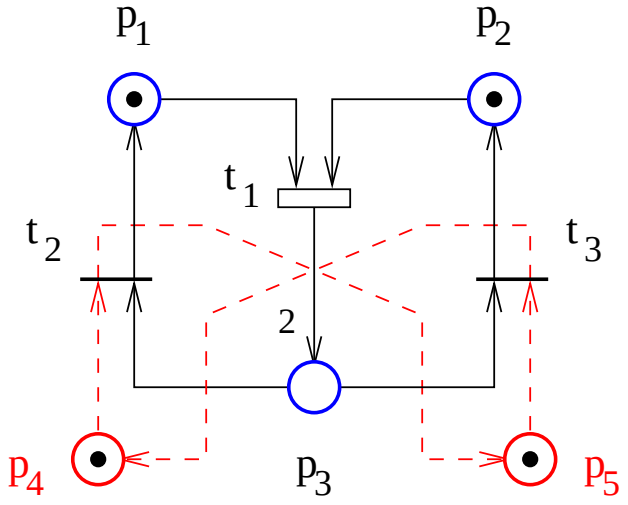
The procedure guarantees that

- the plant is $\mathcal{T}$-live for all μ_0 s.t. $C\mu_0 \leq d$ and $C_0\mu_0 \leq d_0$, whenever $C\mu \leq d$ is enforced;
- the constraints $C\mu \leq d$ are admissible.

Liveness enforcement:

$$C\mu \leq d: \quad \begin{cases} 2\mu_1 + \mu_3 \geq 1 \\ 2\mu_2 + \mu_3 \geq 1 \end{cases}$$

$$C_0\mu \leq d_0: \quad 2\mu_1 + 2\mu_2 + 2\mu_3 \geq 3$$

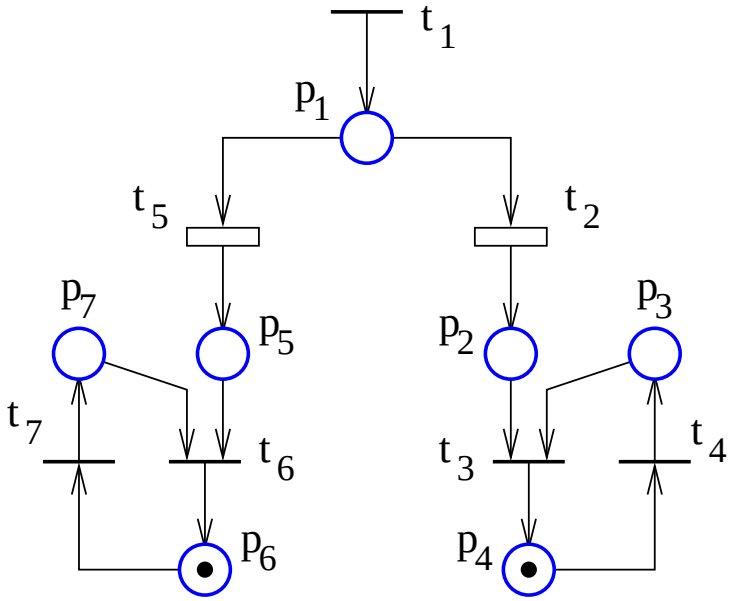


Outline

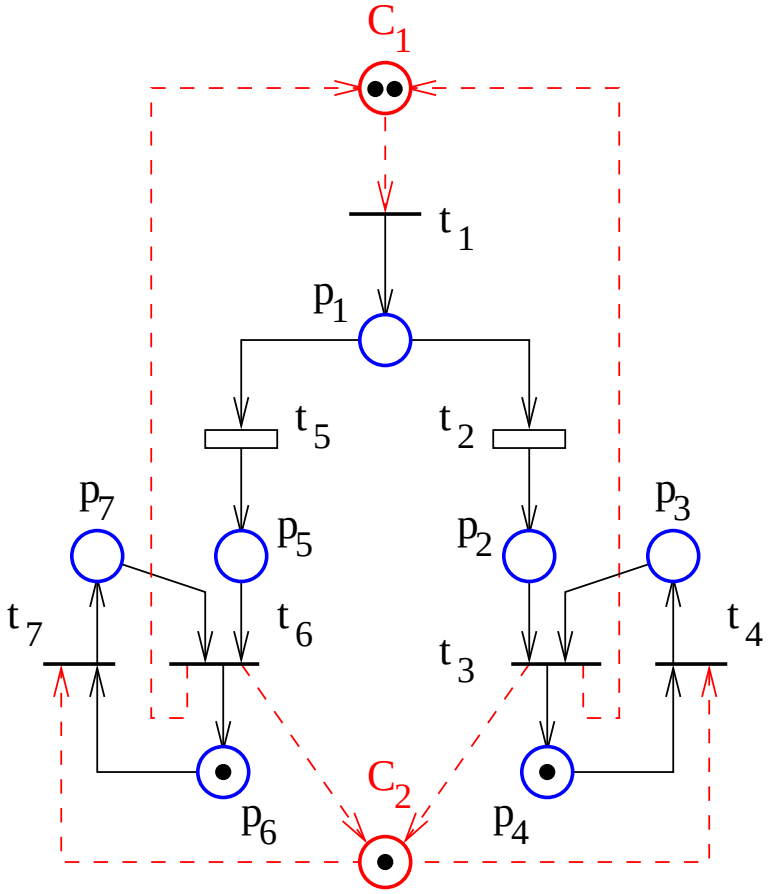
We show that the SBPI has remarkable qualities for designs tolerant to failures and reconfigurations.

The talk is organized as follows:

1. Overview of the SBPI
2. The structural approach for liveness enforcement
3. *Properties of interest for fault-tolerance*
   (a) *Changes in marking*
   (b) *Actuator/sensor failures*
   (c) *Changes in constraints*
   (d) *SBPI under modeling of failures/reconfigurations*
4. Final Remarks



Plant: simplified PN model of an unreliable machine.



Specification:

$$\mu_1 + \mu_2 + \mu_5 \leq 2 \quad (C_1)$$

$$\mu_3 + \mu_7 \leq 1 \quad (C_2)$$

Changes in Marking

When needs a marking change $\Delta\mu$ be detected?

How should the supervisor be updated when a marking change $\Delta\mu$ is detected?

Given the specification $L\mu \leq b$:

1. If $L\Delta\mu \not\leq 0$, the change should be detected, or else the specification may be violated.
2. If $L\Delta\mu \leq 0$ and $L\Delta\mu \neq 0$, the only effect of an undected change is a loss of permissiveness in supervision.
3. If $L\Delta\mu = 0$, the change of marking has no effect on the supervision.
4. If $\Delta\mu$ is detected, the marking of the control places should be updated according to $\mu_s = \mu_s - L\Delta\mu$. There are two cases
   (a) if $\mu_s \not\geq 0$, the supervisor needs redesign.
   (b) if $\mu_s \geq 0$, no redesign is required.

Changes in Marking

1. Changes with $L\Delta\mu \not\leq 0$

Assume this fault: $\mu_1 = 1 \longrightarrow \mu_1 = 2$.

$\mu_1 + \mu_2 + \mu_5 = 1 \longrightarrow \mu_1 + \mu_2 + \mu_5 = 2$

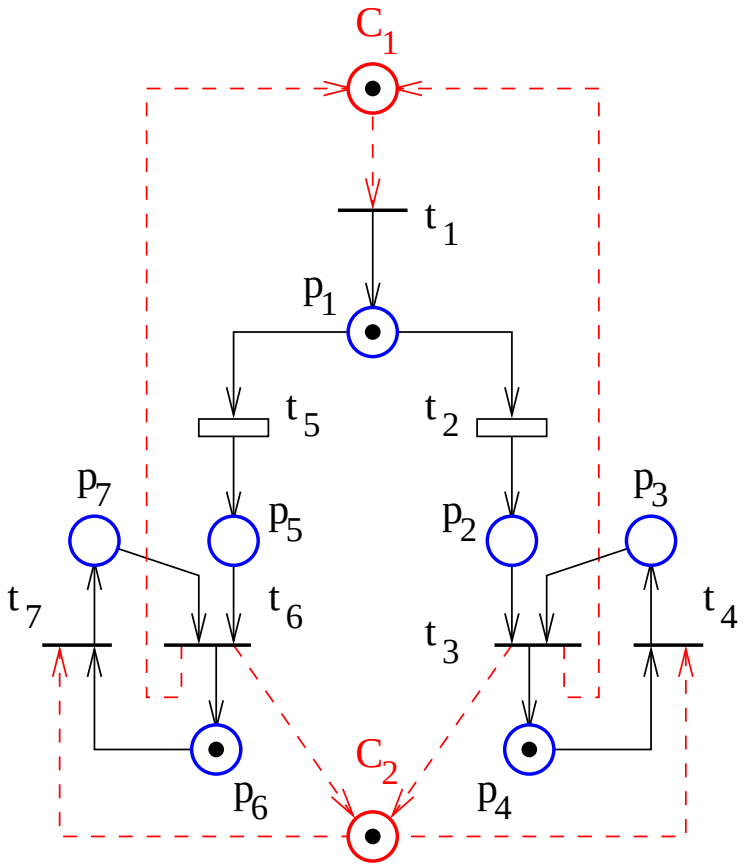
Unless $\Delta\mu_1$ *detected,* t_1 *allowed to fire*

$\longrightarrow \mu_1 + \mu_2 + \mu_5 = 3!$

2. Changes with $L\Delta\mu \leq 0$

Assume this fault: $\mu_1 = 1 \longrightarrow \mu_1 = 0$.

$\mu_1 + \mu_2 + \mu_5 = 1 \longrightarrow \mu_1 + \mu_2 + \mu_5 = 0$



$\Delta\mu_1$ not detected $\longrightarrow$ overrestrictive supervision, e.g. $t_1 t_1$ not enabled!

3. Changes with $L\Delta\mu = 0$

Assume this fault: $\mu_6 = 1 \longrightarrow \mu_6 = 3$. Detecting $\Delta\mu$ not necessary!

Changes in Marking

Similar observations for the liveness enforcement case ...

In addition to $L\mu \leq b$:

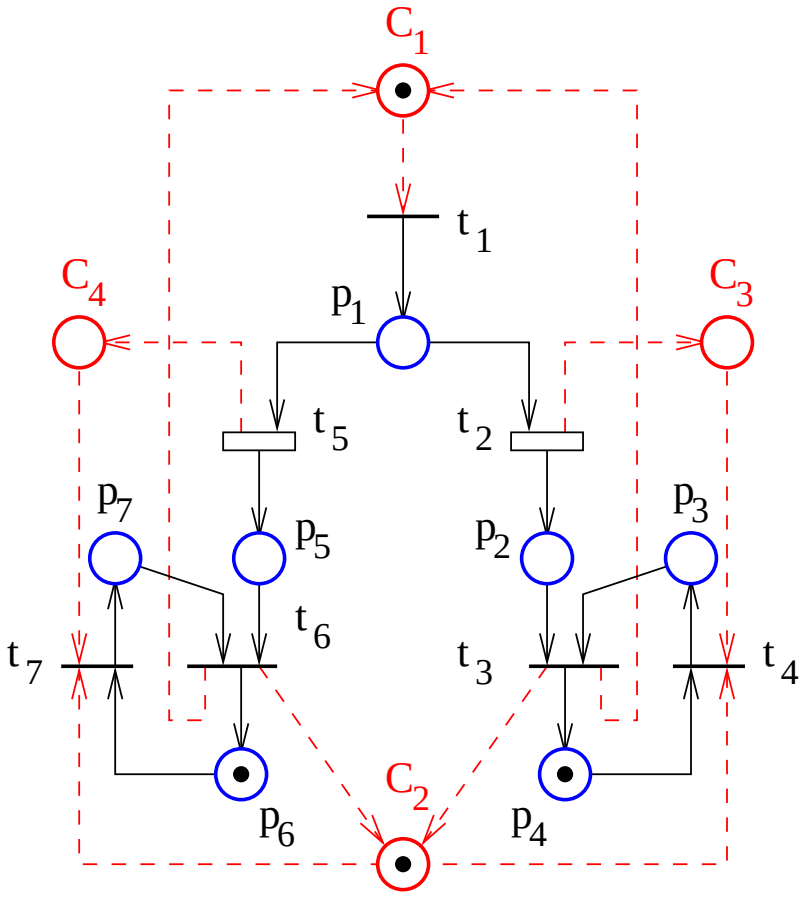
$$\mu_1 + \mu_2 + \mu_5 \leq 1 \quad (C_1)$$
$$\mu_3 + \mu_7 \leq 1 \quad (C_2)$$

we have $C\mu \leq d$:

$$\mu_2 - \mu_3 \geq 0 \quad (C_3)$$
$$\mu_5 - \mu_7 \geq 0 \quad (C_4)$$

and $C_0\mu \leq d_0$:

$$\mu_3 + \mu_4 \geq 1$$
$$\mu_6 + \mu_7 \geq 1$$



Actuator/Sensor failures

When should a change in controllability/observability be detected?

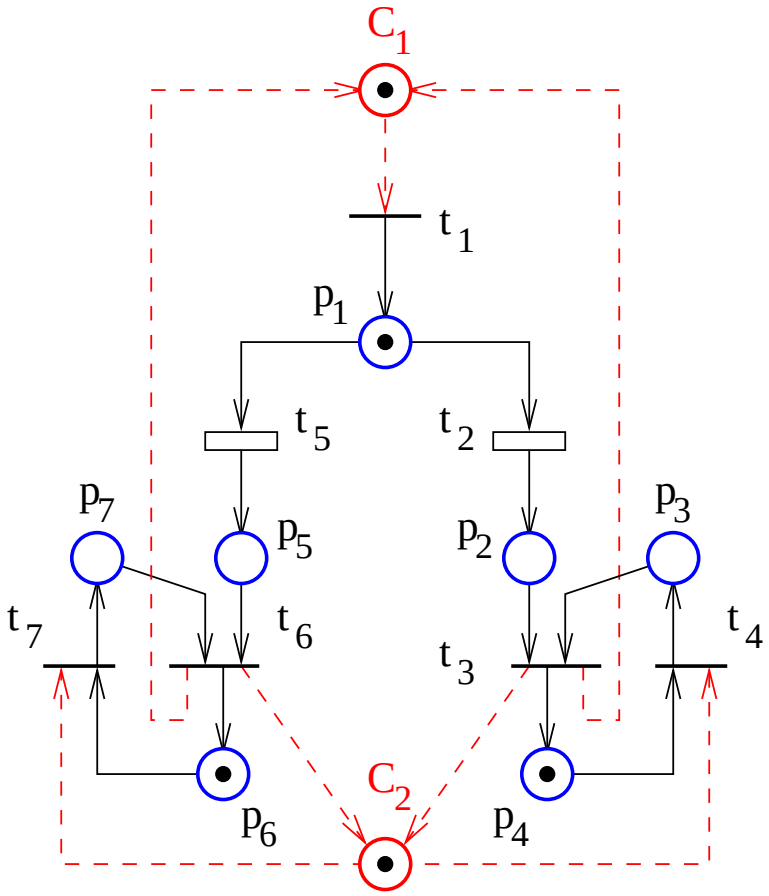
Fault types:

- t becomes uncontrollable
- t becomes unobservable
- t and t' can no longer be distinguished

Recall, $D_s = -LD$.

No changes required when ...

- t becomes *uncontrollable* and $D_s^-(\cdot, t) = 0$ (e.g. $t = t_6$)
- t becomes *unobservable* and $D_s^-(\cdot, t) = D_s^+(\cdot, t)$ (e.g. $t = t_2$)
- t and t' become *indistinguishable* and $D_s(\cdot, t) = D_s(\cdot, t')$ (e.g. $t = t_3$, $t' = t_6$).



Otherwise, changes are to be detected and redesign is required for affected constraints!

Changes in Desired Constraints

What is involved in changing the constraints?

SBPI is modular *(only the constraints that change need to be considered!)* Several cases:

1. $L\mu \leq b$ is replaced by $L'\mu \leq b'$
2. $L\mu \leq b$ is replaced by $L\mu \leq b'$ (only b changes)

Two more possibilities:

A. supervision for liveness required also

B. no additional supervision required

Case 1A: difficult

Case 1B: may be approachable online (depending on the real-time requirements)

Case 2A: may be approachable online, depending on how the liveness supervisor was obtained. See Case 2B.

Case 2B: simply replace μ_s by $\mu_s + b' - b$.

Failures/Reconfigurations that are modeled

Modeling failures/reconfigurations may result in PNs that are not repetitive.

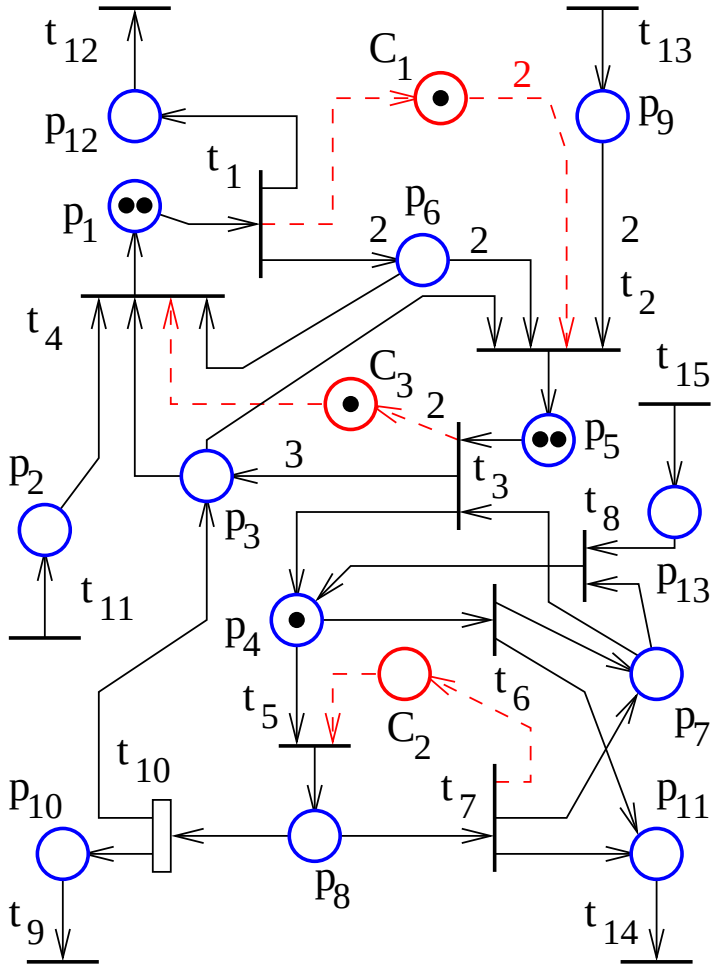
This does not raise a problem for the SBPI.

It may be a problem for liveness enforcement methods ...

... but not for the proposed approach, which handles $\mathcal{T}$-liveness enforcement.

In the fig.: t_{10} models failure.

Supervision for $\mathcal{T}$-liveness displayed.



Final Remarks

This paper examines the properties of SBPI for systems with faults and reconfigurations.

We show that the SBPI and its related liveness approach have qualities that may lead to designs requiring only minor updates in case of failure/reconfigurations.

These qualities rely on the facts that:

- the supervisor structure is independent of the initial marking;
- the supervisor structure is independent of the free term b of $L\mu \leq b$.

Moreover, this is made possible by a structural approach in which

- the structural admissibility conditions are independent of the initial marking;
- the structural admissibility conditions allow a modular design approach.