# Localization of time shift failures in (max,+)-linear systems

Euriell Le Corronc, Alexandre Sahuguède, Yannick Pencolé, Claire Paya

# Localization of time shift failures in (max,+)-linear systems

**Euriell Le Corronc** [*] **Alexandre Sahuguède** [*]
**Yannick Pencolé** [*] **Claire Paya** [*]

[*] *LAAS-CNRS, Université de Toulouse, CNRS, UPS, Toulouse, France*

**Abstract:** The goal of this paper is to propose a localization method of time shift failures in timed discrete event systems (TDES) called $(max, +)$-linear systems and graphically represented by Timed Event Graph (TEG). First, a detection process produces indicators that determine whether such failures have happened by the observation of incoming and outcoming timed flows. Then, thanks to the knowledge of the behavior of the system through its corresponding TEG, set of failures that could explain the detected timed shift are obtained. It comes from matrices of signatures for each indicator built on each observable output of the system.

*Keywords:* Fault localization, Fault diagnosis, $(max, +)$-Linear Systems, Timed Event Graphs, Toolbox.

## 1. INTRODUCTION

Health monitoring of a system such as manufacturing systems, transportation systems or supply chains, often modelled by Discrete Event System (DES), is fundamental to guarantee its maximal use. If dysfunctions happen, this monitoring can help to do online re-scheduling of tasks or to do offline maintenance (replacement of faulty pieces). Among the possible dysfunctions, manifest breakdowns, that lead to complete stop of the system, have to be distinguished from performance problems of one or several equipments that lead to a decrease of the general performance of the system. This last context requires automatic techniques of failure diagnosis to localize the source of these general performance losses. In particular, timed shift failures, such as increasing of transmission delays, late arrival of deliveries, decreasing of production over time, have to be taken into account. It is important to know how to quickly diagnose them in order to maximize the productive and operational time of the system.

Nowadays, some methods deal with timed problem. Contributions of Dousson and Duong (1999); Pencolé and Subias (2009); Saddem and Philippot (2014) based on chronicles or temporal causal signatures can model partially ordered sets of observable events with temporal constraints. Then, failure diagnosis is about to provide sequences of observed timed event into a chronicle recognition system to obtain the recognized chronicle in these sequences that correspond to a faulty behavior. In Tripakis (2002) and Bouyer et al. (2005), the definition of a failure diagnosis uses timed automaton whereas other contributions use Petri nets (Ghazel et al. (2009); Jiroveanu et al. (2013); Liu et al. (2014)). These methods are based on the description of the nominal behavior of the system and the prediction of its behavior in the presence of failures.

In this paper, we propose a method using the $(max, +)$-linear system formalism based on the idempotent semiring theory (Baccelli et al. (1992); Cohen et al. (1989); MaxPlus (1991)). It is well-suited to represent DES that model synchronization between equipments, process durations and transmission times, typical phenomena of the systems studied here. Mathematical models of these systems bring efficient tools to detect dysfunctions causing time shifts. In particular, idempotent semiring $\mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]$ is used. Then, Timed Event Graphs (TEG), sub-class of Timed Petri Nets, bring the graphical model used to localize the source of such shifts among the components of the system.

A first step of time shift failure detection was proposed in Sahuguède et al. (2017). It uses the residuation operation of $(max, +)$-algebra to compute bounds on timed shifts between observed and expected timed output flows. It requires the observation of the timed input flow and the knowledge of the nominal behavior of the system through its transfer function. Indicators are then obtained for all the outputs of the system. This paper deals with the next step of the diagnosis, that is the localization process of the failures in the system. This method provides sets of candidate failures that could explain the detected timed shifts. They are gathered in matrices of signatures thanks to the knowledge of the corresponding TEG of the system. Indeed, all the paths by which the incoming flows can go to the outputs are needed to build these matrices that associate potential failures to indicators.

Section 2 introduces the $\mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]$ idempotent semiring and TEG. Section 3 defines the localization method of time shift failures in $(max, +)$-linear systems. Section 4 proposes an example of application with the use of a C++ toolbox. Section 5 concludes and gives the perspectives.

## 2. BACKGROUND ON $(MAX, +)$-LINEAR SYSTEMS

### 2.1 Dioid theory and residuation theory

*Definition 1.* (Idempotent semiring). An idempotent semiring $\mathcal{D}$ is a set endowed with two inner operations denoted

$\oplus$ and $\otimes$. The sum $\oplus$ is associative, commutative, idempotent (*i.e.* $\forall a \in \mathcal{D}, a \oplus a = a$) and admits a neutral element denoted $\varepsilon$. The product [1] $\otimes$ is associative, distributes over the sum and accepts $e$ as neutral element.

An idempotent semiring is said to be complete if it is closed for infinite sums and if the product distributes over infinite sums too. Due to the sum idempotency, an order relation can be associated with $\mathcal{D}$ by the following equivalences: $\forall a, b \in \mathcal{D},\ a \succeq b \iff (a = a \oplus b \text{ and } b = a \wedge b)$. Because of the lattice properties of a complete idempotent semiring, $a \oplus b$ is the least upper bound of $\mathcal{D}$ whereas $a \wedge b$ is its greatest lower bound. Finally, the *Kleene star* operator is defined as follows: $a^* = \bigoplus_{i \geq 0} a^i$ with $a^{i+1} = a \otimes a^i$ and $a^0 = e$.

*Theorem 2.* (MaxPlus (1991)). Implicit equation $x = ax \oplus b$, defined over a complete dioid $\mathcal{D}$, admits $x = a^*b$ as least solution.

*Example.* The set $\overline{\mathbb{Z}}_{max} = \mathbb{Z} \cup \{-\infty, +\infty\}$, endowed with the max operator as sum $\oplus$ and the classical sum as product $\otimes$, is a complete idempotent semiring where $\varepsilon = -\infty$, $e = 0$ and $T = +\infty$. On $\overline{\mathbb{Z}}_{max}$, the greatest lower bound $\wedge$ takes the sense of the min operator.

*Example.* The set of formal series with two commutative variables $\gamma$ and $\delta$, Boolean coefficients in $\{\varepsilon, e\}$ and exponents in $\mathbb{Z}$, is a complete idempotent semiring denoted $\mathbb{B}[\![\gamma, \delta]\!]$ where $\varepsilon = \bigoplus_{n,t \in \mathbb{Z}} \varepsilon \gamma^n \delta^t$ (null series) and $e = \gamma^0 \delta^0$. A series $s \in \mathbb{B}[\![\gamma, \delta]\!]$ is written in a single way by $s = \bigoplus_{n,t \in \mathbb{Z}} s(n,t) \gamma^n \delta^t$ where $s(n,t) = e$ or $\varepsilon$.

*Example.* The quotient set of $\mathbb{B}[\![\gamma, \delta]\!]$ by the modulo $\gamma^*(\delta^{-1})^*$ equivalence relation provides the complete idempotent semiring $\mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]$. This means that an element of $\mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]$ is an equivalence class denoted [2] $[a]_{\gamma^*(\delta^{-1})^*}$ gathering all the elements of $\mathbb{B}[\![\gamma, \delta]\!]$ equivalent modulo $\gamma^*(\delta^{-1})^*$. Neutral elements $\varepsilon$ and $e$ are identical to those of $\mathbb{B}[\![\gamma, \delta]\!]$.

*Definition 3.* (Dater functions). Let $s \in \mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]$ be a series, the *dater function* of $s$ is the non-decreasing function $\mathcal{D}_s(n)$ from $\mathbb{Z}$ to $\overline{\mathbb{Z}}$ such that $s = \bigoplus_{n \in \mathbb{Z}} \gamma^n \delta^{\mathcal{D}_s(n)}$.

Residuation is a general notion in lattice theory which allows for the definition of "pseudo-inverse" of some isotone maps.

*Definition 4.* (Residuated and residual mapping). Let $f : \mathcal{D} \to \mathcal{C}$ be an isotone mapping, where $\mathcal{D}$ and $\mathcal{C}$ are complete idempotent semirings. Mapping $f$ is said to be *residuated* if $\forall b \in \mathcal{C}$, the greatest element of subset $\{x \in \mathcal{D} | f(x) \preceq b\}$, denoted $f^\sharp(b)$, exists and belongs to this subset. Mapping $f^\sharp$ is called the *residual* of $f$.

When $f$ is residuated, $f^\sharp$ is the unique isotone mapping such that $f \circ f^\sharp \preceq \mathsf{Id}_\mathcal{C}$ and $f^\sharp \circ f \succeq \mathsf{Id}_\mathcal{D}$, where $\mathsf{Id}_\mathcal{C}$ and $\mathsf{Id}_\mathcal{D}$ are respectively the identity mappings on $\mathcal{C}$ and $\mathcal{D}$.

*Example.* Mapping $R_a : x \mapsto x \otimes a$ defined over a complete idempotent semiring $\mathcal{D}$ is residuated. Its residual is usually denoted $R_a^\sharp : x \mapsto x \phi a$ and called *right quotient.* Therefore, $b \phi a$ is the greatest solution to inequality $x \otimes a \preceq b$, *i.e.* $b \phi a = \hat{x} = \bigoplus \{x \mid x \otimes a \preceq b\}$. This example can be applied for the product of matrices such as $X \mapsto X \otimes A \in \mathcal{D}^{p \times m}$ with $A \in \mathcal{D}^{n \times m}$ and $X \in \mathcal{D}^{p \times n}$, that is:

$$R_A = X \otimes A \ : \ (X \otimes A)_{ij} = \bigoplus_{k=1}^{n} X_{ik} \otimes A_{kj}.$$

and the computation of $B \phi A \in \mathcal{D}^{p \times n}$ with $B \in \mathcal{D}^{p \times m}$ is given by:

$$R_A^\sharp(B) = B \phi A \ : \ (B \phi A)_{ij} = \bigwedge_{k=1}^{m} B_{ik} \phi A_{jk}. \qquad (1)$$

*Theorem 5.* (MaxPlus (1991)). Let $\mathcal{D}$ be a complete dioid and $A \in \mathcal{D}^{n \times n}$ be a square matrix. Then, $A \phi A \in \mathcal{D}^{n \times n}$ is a matrix which verifies

$$A \phi A = (A \phi A)^*. \qquad (2)$$

### *2.2 Models of (max,+)-linear systems*

The complete idempotent semiring $\mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]$ aims at modeling TDES as flows of events over time while keeping the history of their occurrences. Indeed, thanks to equivalence $\gamma^*(\delta^{-1})^*$, series of $\mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]$ are non-decreasing and represent the accumulation of event occurrences over time. Typical systems that can be modeled within this formal framework are automated assembly lines or box conveyors. Given a flow $u$ of input timed events (the presence of a new element to be processed in the assembly line, a new box in the conveyor...), the system's response is a flow $y$ of output timed events (delivery of a final product at the end of the assembly line, delivery of a box to its destination...). The relationship between the inputs $u$ and the outputs $y$ of the system is given by the following equation:

$$y = h \otimes u \qquad (3)$$

where $h$ is its transfer function. To be more specific, obtaining this input/output relation comes from the following state representation:

$$\begin{cases} x = Ax \oplus Bu \\ y = Cx \end{cases} \qquad (4)$$

where $A \in \mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]^{n \times n}$, $B \in \mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]^{n \times p}$ and $C \in \mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]^{q \times n}$ while $n$, $p$ and $q$ refer respectively to the state vector size of the system ($x$), the input vector size ($u$) and the output vector size ($y$). Then, by applying Theorem 2 the input/output relation is obtained $y = CA^*Bu = hu$. So $h = CA^*B$. Systems that are fully characterized by Equation (3) or Equation (4) are commonly called $(max, +)$-linear systems. A C++ library called `minmaxgd` enables series of $\mathcal{M}_{in}^{ax}[\![\gamma, \delta]\!]$ to be handled (see Cottenceau et al. (2000)).

Such systems can be graphically represented by Timed Event Graphs (TEG), subclass of Timed Petri Net in which each place has exactly one upstream and one downstream transition and for which arcs have weight one. The earliest firing rule is applied and corresponds to the use of the least solution in the transfer function. Entries of matrices $A$, $B$ and $C$ represent places of the TEG by the mean of a monomial $\gamma^n \delta^t$ where $n$ is the backward event shift between two transitions and $t$ is their backward time shift. When there is no connection between transitions, the entry is equals to $\varepsilon$. Then, for each transition, that

[1] As in usual algebra, $\otimes$ will be omitted when no confusion is possible.

[2] Notation $a$ without the bracket will be adopted in the sequel.

is for each element of vectors $x$, $u$ and $y$, one can write the flow, also called trajectory, of its event occurrences over time (meaning its firings) by a series of $\mathcal{M}_{in}^{ax}[\![\gamma,\delta]\!]$. A monomial $\gamma^m\delta^u$ of any of these series is interpreted as follows: *its* $(m+1)^{th}$ *event occurrence happens at earliest at time* $u$ (the $(m+1)$ is because of the numbering of event occurrences that starts at 0). When trajectories describe a finite number of production orders or a finite number of treated boxes, they contain a finite number of monomials in which the last monomial is written $\gamma^m\delta^{+\infty}$ (the $(m+1)^{th}$ event occurrence never happens).

*Definition 6.* (Observer). In a TEG, an observer is a downstream pair of place and transition attached to an internal transition, where the added place contains no tokens and has holding time 0, (so with $\gamma^0\delta^0$ as monomial in $C$). The transition of an observer is a new output observable transition.

Since there is no shift in the place of an observer, the firing of its transition will be identical to the firing of the transition to which we attached the observer. This represents the add of sensors in the system.

*Example.* Let us consider the TEG of a MIMO (Multiple Inputs - Multiple Outputs) $(max,+)$-linear system represented Figure 1. Its state representation is (point '.' is for $\varepsilon$):

$$\begin{cases} x = \begin{pmatrix} . & . & . & . \\ \gamma^0\delta^2 & . & . & \gamma^0\delta^1 \\ \gamma^0\delta^2 & . & \gamma^1\delta^1 & . \\ . & . & \gamma^0\delta^1 & . \end{pmatrix} x \oplus \begin{pmatrix} \gamma^0\delta^1 & . \\ . & . \\ . & \gamma^0\delta^3 \\ . & . \end{pmatrix} u, \\ y = \begin{pmatrix} . & \gamma^0\delta^3 & . & . \\ . & . & . & \gamma^0\delta^1 \\ \gamma^0\delta^0 & . & . & . \\ . & . & \gamma^0\delta^0 & . \end{pmatrix} x. \end{cases}$$

The transfer function (which is actually a matrix $h \in \mathcal{M}_{in}^{ax}[\![\gamma,\delta]\!]^{q\times p}$ with $q=4$ and $p=2$) of the system is computed:

$$h = CA^*B = \begin{pmatrix} \gamma^0\delta^8(\gamma^1\delta^1)^* & \gamma^0\delta^8(\gamma^1\delta^1)^* \\ \gamma^0\delta^5(\gamma^1\delta^1)^* & \gamma^0\delta^5(\gamma^1\delta^1)^* \\ \gamma^0\delta^1(\gamma^1\delta^1)^* & . \\ \gamma^0\delta^3(\gamma^1\delta^1)^* & \gamma^0\delta^3(\gamma^1\delta^1)^* \end{pmatrix}.$$

Let [3] $u_1 = \gamma^0\delta^2 \oplus \gamma^1\delta^4 \oplus \gamma^3\delta^{+\infty}$ and $u_2 = \gamma^0\delta^3 \oplus \gamma^1\delta^5 \oplus \gamma^3\delta^{+\infty}$ be the inputs. The corresponding outputs are:

$$y = \begin{pmatrix} \gamma^0\delta^{11} \oplus \gamma^1\delta^{13} \oplus \gamma^2\delta^{14} \oplus \gamma^3\delta^{+\infty} \\ \gamma^0\delta^8 \oplus \gamma^1\delta^{10} \oplus \gamma^2\delta^{11} \oplus \gamma^3\delta^{+\infty} \\ \gamma^0\delta^3 \oplus \gamma^1\delta^5 \oplus \gamma^3\delta^{+\infty} \\ \gamma^0\delta^6 \oplus \gamma^1\delta^8 \oplus \gamma^2\delta^9 \oplus \gamma^3\delta^{+\infty} \end{pmatrix}.$$

Outputs $y_3$ and $y_4$ are the observers of transitions $x_1$ and $x_3$.

## 3. LOCALIZATION OF TIME SHIFT FAILURES IN $(MAX,+)$-LINEAR SYSTEMS

In the formalism of $(max,+)$-linear systems, time shift failures can be detected. This detection step, introduced in Sahuguède et al. (2017) and recalled here, uses the residuation operation to compute bounds on timed shifts between observed outputs $y$ and expected outputs $\tilde{y} = h \otimes u$. This needs the observation of the inputs $u$ and the knowledge of the transfer function $h$. Indicators are then computed for all the observable outputs thanks to these bounds.

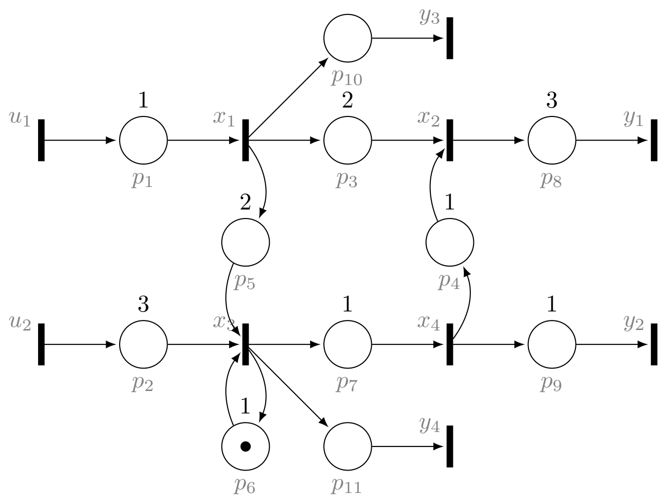

Fig. 1. A TEG of a MIMO $(max,+)$-linear system.

Next, if a time shift failure is detected, its source has to be found among the components of the system. This is the localization step: given indicator values and knowing the TEG of the system with all the paths the tokens can take from the inputs to the outputs, which potential failure can explain indicator that returns true? To answer that question, we produce matrices of signatures associating candidate failures to indicators, a failure being itself associated to a place of the TEG. Thus, we are able to propose a set of candidate failures that can be the source of the detected time shift.

### 3.1 *Time shift failure detection*

For the detection step, we first need a way to compare the expected output $\tilde{y}$ with the real observed output $y$, that is to compare series of $\mathcal{M}_{in}^{ax}[\![\gamma,\delta]\!]$.

*Definition 7.* (Time shift function). Let $a, b \in \mathcal{M}_{in}^{ax}[\![\gamma,\delta]\!]$ and their respective dater functions $\mathcal{D}_a(n)$ and $\mathcal{D}_b(n)$. The *time shift function* representing the time shifts between $a$ and $b$ for each $n \in \mathbb{Z}$ is defined by $\mathcal{T}_{a,b}(n) = \mathcal{D}_b(n) - \mathcal{D}_a(n)$.

Intuitively speaking, the time shift function associates the time difference between the $n^{th}$ event occurrence of series $a$ and the $n^{th}$ event occurrence of series $b$. Obviously, $\mathcal{T}_{a,a}(n) = 0, \forall n \in \mathbb{Z}$.

*Theorem 8.* (MaxPlus (1991)). Let $a, b \in \mathcal{M}_{in}^{ax}[\![\gamma,\delta]\!]$, the time shift function can be bounded as follows:

$$\forall n \in \mathbb{Z}, \quad \mathcal{D}_{b \not{a}}(0) \leq \mathcal{T}_{a,b}(n) \leq -\mathcal{D}_{a \not{b}}(0).$$

So, the comparison between series $a$ and $b$ can be reduced to determine the bounds $\mathcal{D}_{b \not{a}}(0)$ and $-\mathcal{D}_{a \not{b}}(0)$ of their time function $\mathcal{T}_{a,b}$ where $\mathcal{D}_{b \not{a}}(0)$ comes from $\gamma^0\delta^{\mathcal{D}_{b \not{a}}(0)} \in b \not{a}$ and $-\mathcal{D}_{a \not{b}}(0)$ comes from $\gamma^0\delta^{\mathcal{D}_{a \not{b}}(0)} \in a \not{b}$.

[3] Dater functions of $u_1$ and $u_2$ are $\forall n \in \mathbb{Z}, \mathcal{D}_{u_1}(n) = \{2, 4, 4, +\infty\}$ and $\mathcal{D}_{u_2}(n) = \{3, 5, 5, +\infty\}$.

*Example* Let $a, b \in \mathcal{M}_{in}^{ax}[\![\gamma,\delta]\!]$ such that $a = \gamma^0\delta^{12} \oplus \gamma^1\delta^{15} \oplus \gamma^2\delta^{18} \oplus \gamma^3\delta^{21} \oplus \gamma^4\delta^{+\infty}$, $b = \gamma^0\delta^{12} \oplus \gamma^1\delta^{15} \oplus \gamma^2\delta^{19} \oplus \gamma^3\delta^{23} \oplus \gamma^4\delta^{+\infty}$. The minimal time shift between $a$ and $b$ is $\mathcal{D}_{b \circ\!\!\!/ a}(0) = 0$ and is found in $b \circ\!\!\!/ a = \gamma^0\delta^{\mathbf{0}} \oplus \gamma^1\delta^3 \oplus \gamma^2\delta^7 \oplus \gamma^3\delta^{11} \oplus \gamma^4\delta^{+\infty}$. The maximal time shift is $-\mathcal{D}_{a \circ\!\!\!/ b}(0) = 2$ and is found in the monomial where the degree of $\gamma$ is 0 of $a \circ\!\!\!/ b = \gamma^0\delta^{-\mathbf{2}} \oplus \gamma^1\delta^2 \oplus \gamma^2\delta^6 \oplus \gamma^3\delta^9 \oplus \gamma^4\delta^{+\infty}$.

Thus, a time shift failure indicator is obtained to detect deviations $y$ and $\tilde{y}$.

*Definition 9.* (Indicator of time shift failure). Let $h \in \mathcal{M}_{in}^{ax}[\![\gamma,\delta]\!]^{q\times p}$ be the transfer function of a $(\max,+)$-linear system, let $u \in \mathcal{M}_{in}^{ax}[\![\gamma,\delta]\!]^{p}$ be the observable input trajectories of the system and $y \in \mathcal{M}_{in}^{ax}[\![\gamma,\delta]\!]^{q}$ be its output. If $y_i$ is observable, indicator $I_h(u, y_i)$ is the function:

$$I_h(u, y_i) = \begin{cases} \mathit{false} \text{ if for } \tilde{y}_i = hu, \ \Sigma_\tau(y_i, \tilde{y}_i) = [0;0], \\ \mathit{true} \text{ otherwise,} \end{cases}$$

with

$$\Sigma_\tau(y_i, \tilde{y}_i) = [\mathcal{D}_{y_i \circ\!\!\!/ \tilde{y}_i}(0); -\mathcal{D}_{\tilde{y}_i \circ\!\!\!/ y_i}(0)].$$

$\mathcal{I}$ is the set of the $k$ failure indicators of the system.

*Remark* If all the outputs of the system are observed, $k = q$ with $q$ the number of outputs. If not, indicators are available only for observable outputs (an observer can be attached to any internal transition). Anyway, all the inputs have to be observable.

To obtain these indicators, expected output $\tilde{y}$ is first computed with the knowledge of $h$ and of the observable input $u$. Then, thanks to the right quotient operation between observed output $y$ and expected output $\tilde{y}$, time shifts between them are obtained. The indicator is raised when at least one bound of the interval $\Sigma_\tau(y_i, \tilde{y}_i)$ is different from 0; it returns false when the two bounds are equal to 0. It is a correct indicator since it returns true only when a time shift failure is detected.

*Example* Let us consider the MIMO $(\max,+)$-linear system illustrated Figure 1 with $u_1 = \gamma^0\delta^2 \oplus \gamma^1\delta^4 \oplus \gamma^3\delta^{+\infty}$ and $u_2 = \gamma^0\delta^3 \oplus \gamma^1\delta^5 \oplus \gamma^3\delta^{+\infty}$ as inputs. All the outputs are observable. If a failure produces a delay of 4 time units between transitions $x_1$ and $x_2$ (place $p_3$ is labelled by 6 time units instead of 2), the observed output of $y_1$ becomes $y_1 = \gamma^0\delta^{12} \oplus \gamma^1\delta^{14} \oplus \gamma^3\delta^{+\infty}$ but the other observed outputs do not change. Computations of $\tilde{y} \circ\!\!\!/ y$ and $y \circ\!\!\!/ \tilde{y}$ give for $y_1$:

$$(\tilde{y} \circ\!\!\!/ y)_{11} = \tilde{y}_1 \circ\!\!\!/ y_1 = \gamma^0\delta^{-\mathbf{1}} \oplus \gamma^1\delta^0 \oplus \gamma^2\delta^2 \oplus \gamma^3\delta^{+\infty},$$
$$(y \circ\!\!\!/ \tilde{y})_{11} = y_1 \circ\!\!\!/ \tilde{y}_1 = \gamma^0\delta^{\mathbf{0}} \oplus \gamma^1\delta^1 \oplus \gamma^2\delta^3 \oplus \gamma^3\delta^{+\infty}.$$

Thus $I_h(u, y_1) = \mathit{true}$ because $\Sigma_\tau(y_1, \tilde{y}_1) = [0;1]$. A time shift failure is detected for this output. The indicators of the other outputs return false so there is no other detection of time shift failure.

### *3.2 Time shift failure localization*

A time shift failure in a $(max,+)$-linear system actually causes a modification of the holding times of places of the corresponding TEG. Thus, there are as many possible failures as places. Then, the effect of such a failure can be observed on several outputs and so several indicators can be involved. From the knowledge of the system TEG, it is possible to obtain links between the output designated by the indicator and the failure that causes the time shift. For instance, with the TEG illustrated Figure 1, output $y_4$ may be affected by places called $p_1, p_2, p_5, p_6, p_{11}$. In other words, the presence of a failure on one of these places can produce a time shift detected by indicator $I_h(u, y_4)$. So, indicator $I_h(u, y_4)$ is part of the *signature* of all these failures.

*Definition 10.* (Failure signature). Let $G$ be the TEG of a $(max,+)$-linear system and $\mathcal{I}$ the set of all its $k$ failure indicators. $\mathcal{I}_{f_i} \subseteq \mathcal{I}$ is the set of indicators that can return true when a time shift failure occurs. This failure is denoted $f_i$ with $i = 0, \ldots, l$ and $l$ the number of the TEG places (meaning that there is one possible time shift failure for each place). $\mathcal{I}_{f_i}$ is called the signature of $f_i$.

Each time shift failure has a signature containing all the indicators that can be raised if it occurs. They are all gathered in the *matrix of signatures* of the system.

*Definition 11.* (Matrix of signatures). Let $G$ be the TEG of a $(max,+)$-linear system, $\mathcal{I}$ the set of its $k$ failure indicators and $\mathcal{F}$ the set of the $l$ time shift failures. The matrix of signatures of the system is the relation $\mathcal{I} \times \mathcal{F}$ denoted $M \in \mathbb{B}^{k\times l}$ for which each element is defined by:

$$M_{ij} = \begin{cases} 1 \text{ if } I_h(u, y_i) \in \mathcal{I}_{f_j}, \\ 0 \text{ otherwise.} \end{cases}$$

*Example* The matrix of signatures of the TEG of Figure 1 is the following:

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Lines are indicators on the observed outputs: $\mathcal{I} = \{I_h(u, y_1), I_h(u, y_2), I_h(u, y_3), I_h(u, y_4)\}$. Columns are the time shift failures that can happen in this system: $\mathcal{F} = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}\}$.

Thanks to this matrix of signatures and with the state of indicators, a set of candidate failures is proposed.

*Definition 12.* (Candidate failure). A failure $f_j$ is a candidate failure if it exists an indicator $I_h(u, y_i)$ returning true and such that $M_{ij} = 1$.

*Example* In Figure 1, if indicators $I_h(u, y_1)$ and $I_h(u, y_3)$ return true whereas the other indicators return false, then $f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_{10}$ are the candidate failures. By construction, no failure among $f_9$ and $f_{11}$ can explain the value of indicators.

### *3.3 Refinement of the localization*

The matrix of signatures points out different failures that can explain the raise of indicators. However, it is about a set of possibilities, not a strict implication. Indeed, in a $(max,+)$-linear system, when a time shift failure occurs in a path upstream a synchronization, it is possible that its effect is totally hidden by the synchronization if the time shift is counterbalanced by a higher process duration in another path. For instance, in the TEG of Figure 1, several synchronizations are present between several paths that arrive on output $y_1$. The time shift failure $f_1$ *can* raise the indicator $I_h(u, y_1)$ but *not necessarily* because of downstream synchronizations. But, if one (and only one) failure happens in a place of the TEG necessarily involved in a path leading from one input to one output of the system but without synchronization, the indicator of this output will be necessarily raised. For instance, in TEG of Figure 1, if $f_8$ occurs, it will necessarily have an effect on the output $y_1$. Similarly, if $f_1$ or $f_{10}$ occur, a time shift will necessarily appear on $y_3$ without the possibility to be couterbalanced by any synchronization. Thus, the definition of a characteristic signature illustrating this statement is possible.

*Definition 13.* (Characteristic signature). Let $G$ be the TEG of a $(max, +)$-linear system and $\mathcal{I}$ the set of its $k$ failure indicators. $\mathcal{I}^c_{f_i} \subseteq \mathcal{I}$ is the set of indicators returning *necessarily* true when a time shift failure $f_i$ occurs. $\mathcal{I}^c_{f_i}$ is called the characteristic signature of $f_i$.

*Definition 14.* (Characteristic signature matrix). The matrix of characteristic signatures of the system is the relation $\mathcal{I} \times \mathcal{F}$ denoted $M^c \in \mathbb{B}^{k\times l}$ for which each element is defined by:

$$M^c_{ij} = \begin{cases} 1 \text{ if } I_h(u, y_i) \in \mathcal{I}^c_{f_j}, \\ 0 \text{ otherwise.} \end{cases}$$

*Example* The characteristic signature matrix of the TEG of Figure 1 is the following:

$$M^c = \begin{pmatrix} 0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&1&0&1&0&0 \\ 1&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&1 \end{pmatrix}.$$

As in the matrix of signatures, lines are the indicators over the observed outputs: $\mathcal{I} = \{I_h(u, y_1), I_h(u, y_2), I_h(u, y_3), I_h(u, y_4)\}$. Columns are the time shift failures that can happen in this system: $\mathcal{F} = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}\}$.

Such characteristic signature matrix can be used to refine the localization made in Subsection 3.2. Indeed, under the *single failure assumption* (only one failure has happened in the system), if an indicator of the characteristic signature of a failure $f_i$ has not raised, then $f_i$ surely has not happened and can be removed from the set of candidates.

*Definition 15.* (Minimal set of candidate failures). Under the *single failure assumption*, the minimal set of candidate failures contains failures $f_i$ for which *at least one* indicator of $\mathcal{I}_{f_i}$ return true and *all* indicators of $\mathcal{I}^c_{f_i}$ return true.

*Example* On Figure 1, if indicators $I_h(u, y_1)$ and $I_h(u, y_3)$ return true, the set of candidate failures found in $M$ is $\{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_{10}\}$. But, the analysis of the characteristic signature matrix $M^c$ tells us that there is no observation of time shift on $y_2$ that excludes failure $f_7$. So, the minimal set of candidate failures is $\{f_1, f_2, f_3, f_4, f_5, f_6, f_8, f_{10}\}$.

## 4. APPLICATION AND IMPLEMENTATION

This section illustrates the use of indicators and signature matrices for localizing the possible source of time shift failures in a TEG.

The proposed example is inspired from Baccelli et al. (1992). In this original example presented in Figure 2, some parts of different types (type 1 and 2) wait in separate buffers (buffers $A$ and $E$) before being heated individually by a furnace. The furnace heats parts from buffers alternatively (modeled by places $I$ and $K$), parts of type 1 must wait $\alpha_1$ time units in the furnace and parts of type 2 must wait $\alpha_3$. Then, they are sent to a stove (places $CN$ and $GP$) and assembled by pairs of different types (place $DHQ$) before leaving the workshop ($x_6$). Assembling two parts takes $\alpha_2$ time units.

To illustrate our method, we firstly propose to extend this example by adding observers (bold places and transitions in Figure 2) for transitions $x_3$, $x_4$ and $x_6$ that lead to the observations of the transitions $y_3$, $y_4$ and $y_6$. Basically, with help of $y_3$ and $y_4$ we observe the parts getting out of the furnaces and with help of $y_6$ we observe the assembled part moving out of the workshop. Secondly, we propose to derive from this initial example a more complex one that is composed of three TEGs, that are three workshops (namely $W_{00}, W_{01}, W_{11}$), where an assembled part of $W_{00}$ (resp. $W_{01}$) is a part of type 1 (resp. 2) for $W_{11}$. This system, as a set of three connected workshops, is then modeled by 36 places, 22 transitions and 9 observers (add one more place and one more transition per observer).

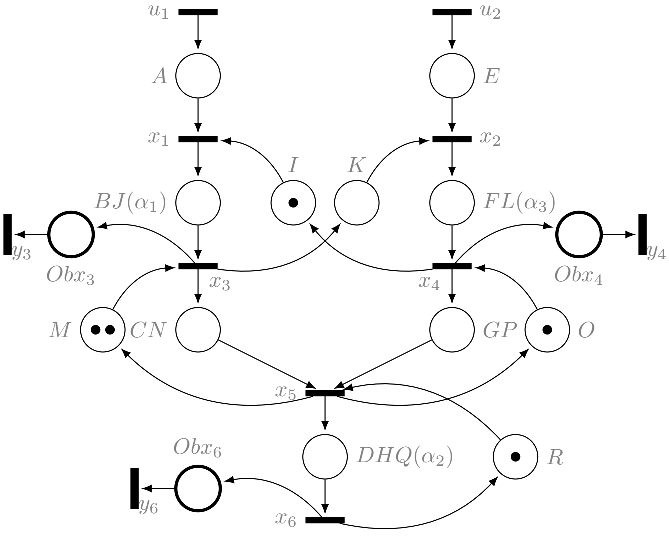

Fig. 2. Furnace model $FM(\alpha_1, \alpha_2, \alpha_3)$ of Baccelli et al. (1992) enriched with three observers $y_3$, $y_4$ and $y_6$.

By construction of this system, all the failures $f$ involving a place of workshop $W_{11}$ have the signature

$$\mathcal{I}_f = \{I_h(y_3^{11}, u), I_h(y_4^{11}, u), I_h(y_6^{11}, u)\}.$$

Any time shift failure $f$ involving $W_{11}$ cannot set any indicator of $W_{00}$ and $W_{01}$ to true. Similarly, all the failures $f$ involving a place of workshop $W_{0i}, i = \{0, 1\}$ has the following signature $\mathcal{I}_f = \{I_h(y_3^{0i}, u)$, $I_h(y_4^{0i}, u)$, $I_h(y_6^{0i}, u)$, $I_h(y_3^{11}, u)$, $I_h(y_4^{11}, u)$, $I_h(y_6^{11}, u)\}$. A failure of $W_{00}$ has no influence on $W_{01}$ and reciprocally. Only failures on places $DHQ_{00}, DHQ_{01}, DHQ_{10}$ can be associated with characteristic signatures: indicator $y_6^{00}$ is part of the characteristic signature of $DHQ_{00}$, indicator $y_6^{01}$ is part of the characteristic signature of $DHQ_{01}$ and so. This is due to the presence of transition cycles in each workshop.

To show the effect of possible failures in the given system, we present here 3 scenarios where we consider in any

| Scenarios | Outputs of the indicators set to true |
|---|---|
| $FL_{00}+6$ | $y_4^{00}, y_6^{00}, y_3^{11}, y_4^{11}, y_6^{11}$ |
| $DHQ_{01}-2$ | $y_6^{01}, y_4^{11}, y_6^{11}$ |
| $BJ_{11}+18$ | $y_3^{11}, y_4^{11}, y_6^{11}$ |

Fig. 3. The outputs involved in the indicators that are true for the three scenarios.

workshop that $\alpha_1 = 2$, $\alpha_2 = 3$, $\alpha_3 = 3$. For each independent scenario, we injected one type of failure in the system.

- Scenario 1 is a time shift of 6 in $FL_{00}$ (i.e. $\alpha_3 + 6$).
- Scenario 2 is a time shift of -2 in $DHQ_{01}$ (i.e. $\alpha_2 - 2$)
- Scenario 3 is a time shift of 18 in $BJ_{11}$ (i.e. $\alpha_1 + 18$).

For each scenario, we first simulate the system injected with the failure for a given $u$ to get the observed outputs $y$ and then we apply the proposed method by computing $\tilde{y}$ based on $u$ and then evaluate the set of indicators. For this experiment, $u$ is such that $u_1^{00} = \gamma^0\delta^1 \oplus \gamma^1\delta^{+\infty}$, $u_2^{00} = \gamma^0\delta^2 \oplus \gamma^1\delta^{+\infty}$, $u_1^{01} = \gamma^0\delta^4 \oplus \gamma^1\delta^{+\infty}$, $u_2^{00} = \gamma^0\delta^{10} \oplus \gamma^1\delta^{+\infty}$. Results are presented on Figure 3.

Under the single failure assumption, this figure shows that for Scenario 1, the problem can indeed be localized in $W_{00}$ as no indicators from $W_{01}$ are set to true. Similarly for Scenario 2, the problem can be localized in $W_{01}$. Moreover, as $y_6^{01}$ is the only output involved in $W_{01}$, as it is part of the characteristic signature of $DHQ_{01}$, $DHQ_{01}$ can be considered as a preferred candidate (part of the set of minimal candidates). Finally, Scenario 3 indicates that it cannot be a failure from $DHQ_{00}$ and $DHQ_{01}$ as the indicators from the characteristic signatures are not involved. Due to the structure of the system, candidates from $W_{11}$ are preferred but there is a lack of observers to ensure that it comes from $W_{11}$ (diagnosability issue).

These experiments are fully implemented within the MaxPlusDiag tool that is developped in LAAS-CNRS. This tool aims at providing a set of methods and algorithms for monitoring and diagnosing TEG relying on $(max, +)$-linear system formalism. This tool is implemented in C++ and is based on the C++ library `minmaxgd` (Cottenceau et al. (2000)).

## 5. CONCLUSION

This paper proposes a method to localize time shift failures in systems modeled by Timed Event Graphs and represented by $\mathcal{M}_{in}^{ax}[\![\gamma,\delta]\!]$ equations. The method defines a set of failure indicators by applying residuation operations to formally compare the expected and observed outputs of the system. Based on a structural analysis of the TEGs and the set of available indicators, we introduce the notion of failure signatures for TEG based on which it is then possible to determine the possible sources of the time shift in the system. This method is fully implemented in a new C++ toolbox, called MaxPlusDiag, that relies on the `minmaxgd` library.

There are many perspectives. A first way of investigation is to extend the TEG model to handle bounded holding time uncertainties in places thanks to the dioids of intervals. Moreover, the diagnosability question as well as the sensor placement problem is an interesting lead. Indeed, faults can be compensated by synchronization phenomena so that they might totally be silent from a global point of view, and adding local sensors is then necesssary. Finally, all this study could also be transposed to event shift failures corresponding to loss of ressources in the system. In that case, counter functions that deal with number of occurences of events should be used.

## REFERENCES

Baccelli, F., Cohen, G., Olsder, G.J., and Quadrat, J.-P. (1992). *Synchronization and linearity: an algebra for discrete event systems.* Wiley and sons.

Bouyer, P., Chevalier, F., and D'Souza, D. (2005). Fault diagnosis using timed automata. In *Proceedings of the 8th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS).*

Cohen, G., Moller, P., Quadrat, J.-P.., and Viot, M. (1989). Algebraic tools for the performance evaluation of discrete event systems. *Proceedings of the IEEE*, 77(1), 39–85.

Cottenceau, B., Lhommeau, M., Hardouin, L., and Boimond, J.-L. (2000). Data processing tool for calculation in dioid. In *5th International Workshop on Discrete Event Systems.* `http://www.istia.univ-angers.fr/ hardouin/outils.html.`

Dousson, C. and Duong, T.V. (1999). Discovering chronicles with numerical time constraints from alarm logs for monitoring dynamic systems. In *Proceedings of the Sixteenth International Joint Conference on Artificial Intelligence.*

Ghazel, M., Toguyéni, A., and Yim, P. (2009). State observer for des under partial observation with time petri nets. *Discrete Event Dynamic Systems*, 19(2), 137–165.

Jiroveanu, G., Schutter, B., and Boel, R. (2013). *Taming Heterogeneity and Complexity of Embedded Control*, chapter The On-line Diagnosis of Time Petri Nets Based on Partial Orders, 21. John Wiley & Sons.

Liu, B., Ghazel, M., and Toguyéni, A. (2014). Diagnosis of labeled time petri nets using time interval splitting. In *19th World Congress of the International Federation of Automatic Control.*

MaxPlus (1991). Second order theory of min-linear systems and its application to discrete event systems. In *Proceedings of the 30th IEEE Conference on Decision and Control (CDC).*

Pencolé, Y. and Subias, A. (2009). A chronicle-based diagnosability approach for discrete timed-event systems: Application to web-services. *Journal of Universal Computer Science*, 15(17), 3246–3272.

Saddem, R. and Philippot, A. (2014). Causal temporal signature from diagnoser model for online diagnosis of discrete event systems. In *International Conference on Control, Decision and Information Technologies.*

Sahuguède, A., Le Corronc, E., and Pencolé, Y. (2017). Design of indicators for the detection of time shift failures in (max, +)-linear systems. In *20th World Congress of the International Federation of Automatic Control.*

Tripakis, S. (2002). Fault diagnosis for timed automata. In *7th International Symposium of Formal Techniques in Real-Time and Fault-Tolerant Systems.*