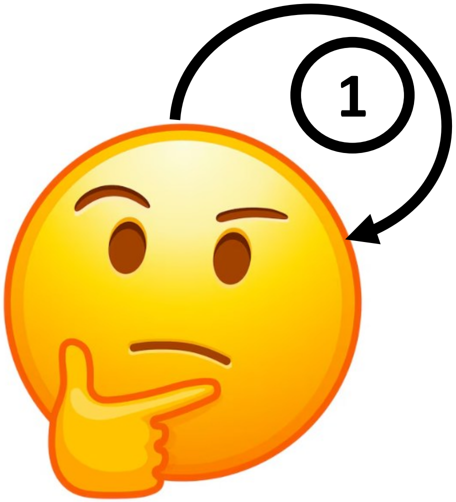
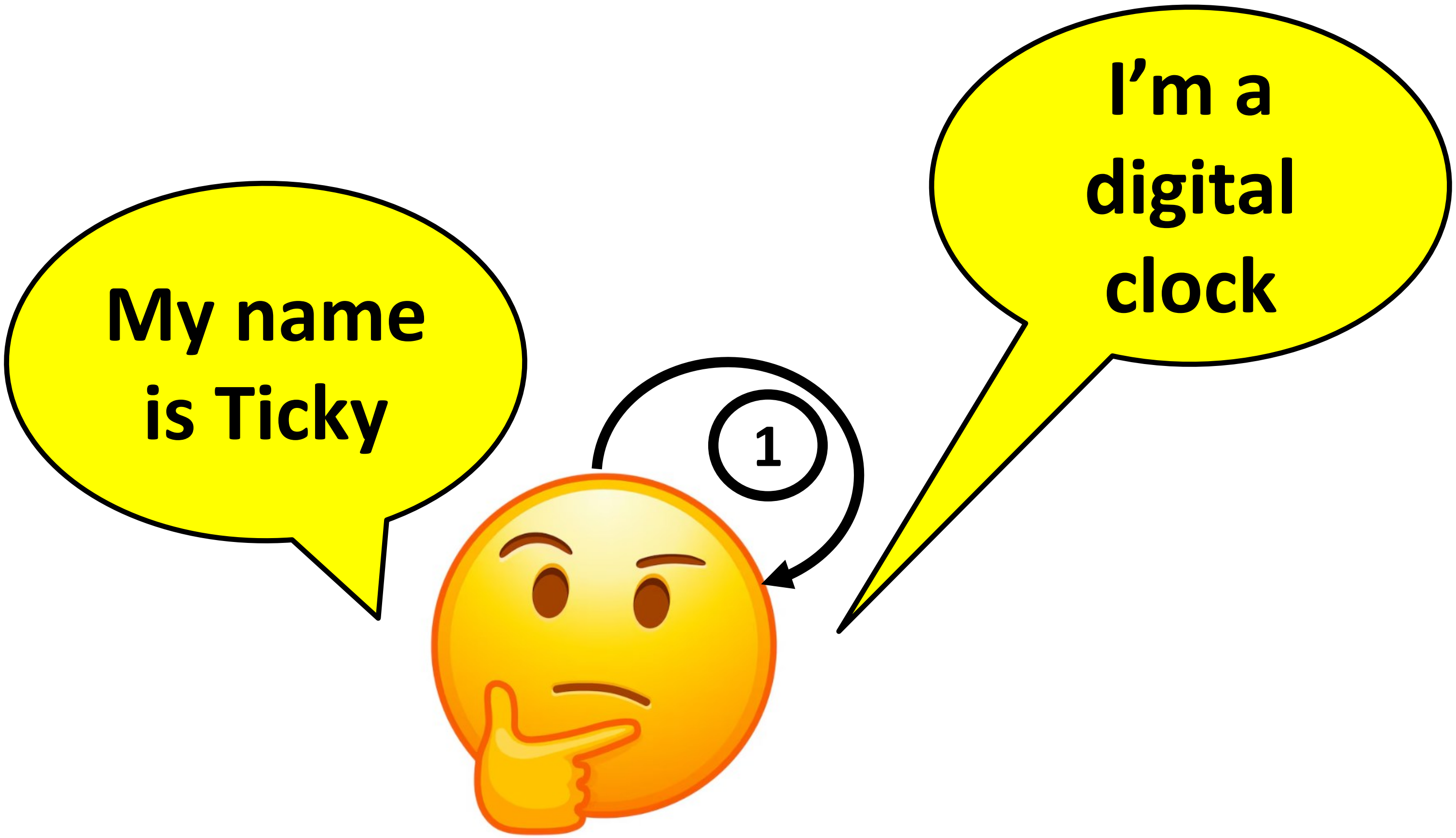
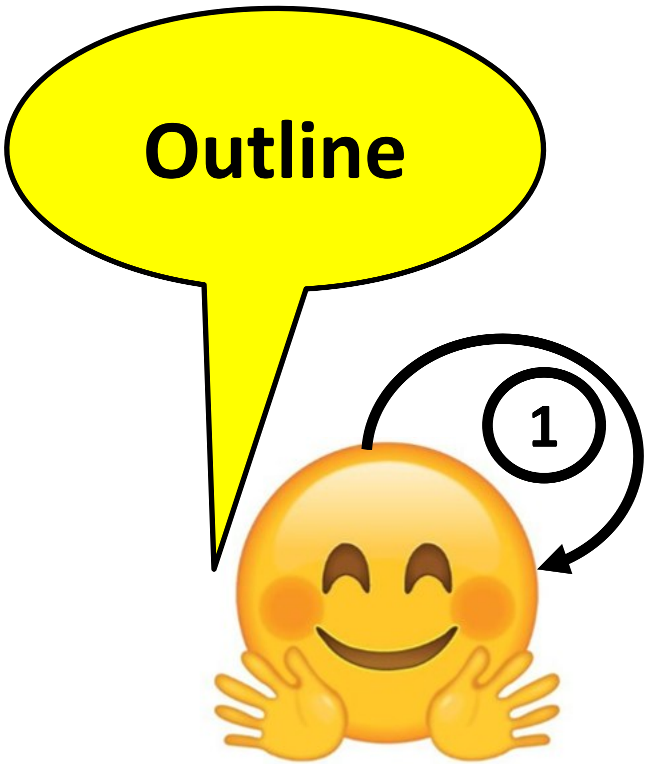
Clock Interval Automata for Timed DESs

Dimitri Lefebvre
Université Le Havre Normandie, France
GREAH



Supported by ANR MENACES 2022-CE10-0002
and RIN ASSAILLANT 2023 ref. 23E02599


My name is Ticky
I’m a digital clock
1



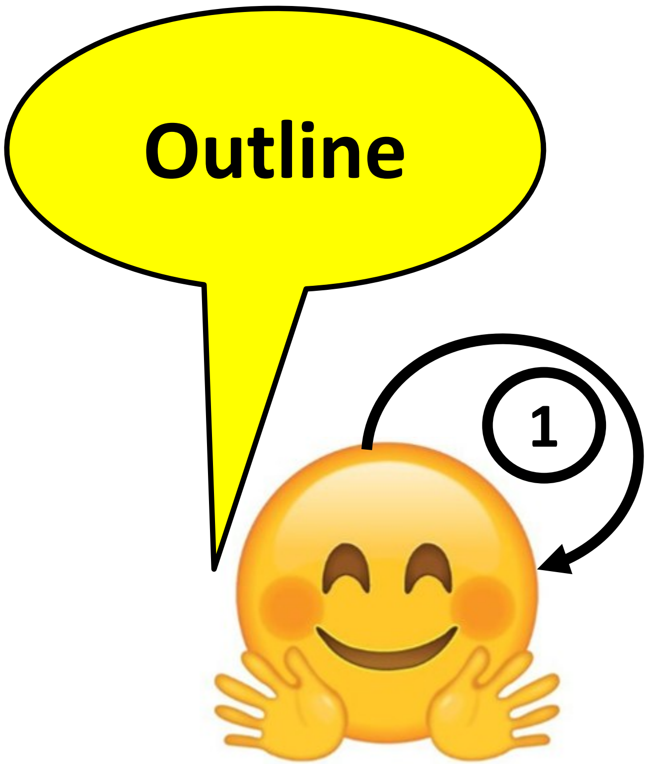
1. **Introduction and motivation**

2. **Modeling timed discrete event systems with automata**
   - Timed automata
   - Tick automata
   - Automata with time interval (ATI)
   - Clock Interval Automata (CIA)

3. **Observation mechanisms based on labeled CIA**
   - Static observation
   - Dynamic observation
   - Orwellian observation

4. **Application to cyber physical systems**
   - Fault diagnosis and diagnosability
   - Opacity analysis
   - Attack detection

5. **Conclusion and perspectives**



1. Introduction and motivation

2. Modeling timed discrete event systems with automata
- Timed automata
- Tick automata
- Automata with time interval (ATI)
- Clock Interval Automata (CIA)

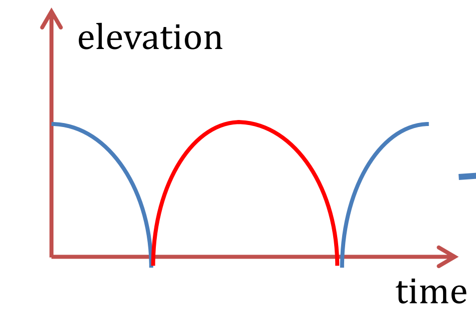
3. Observation mechanisms based on labeled CIA
- Static observation
- Dynamic observation
- Orwellian observation

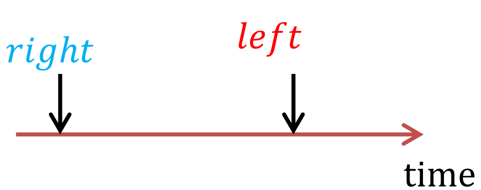
4. Application to cyber physical systems
- Fault diagnosis and diagnosability
- Opacity analysis
- Attack detection

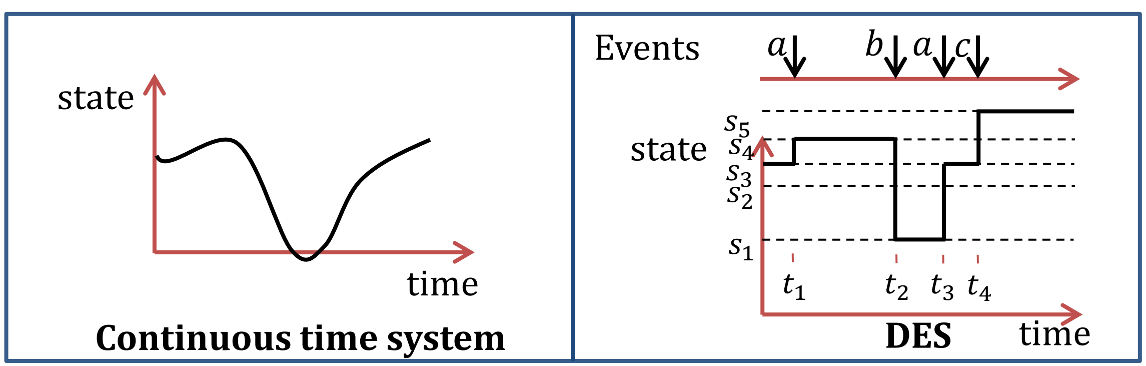
5. Conclusion and perspectives

Motivation for TIMED DISCRETE EVENT SYSTEMS

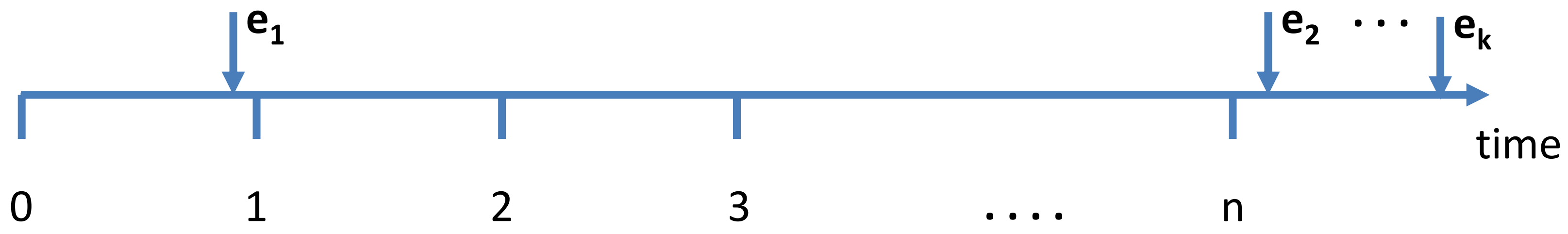
- ⇒ **An abstraction of the state**
- ⇒ **A possible abstraction of the time**







Motivation for TIMED DISCRETE EVENT SYSTEMS

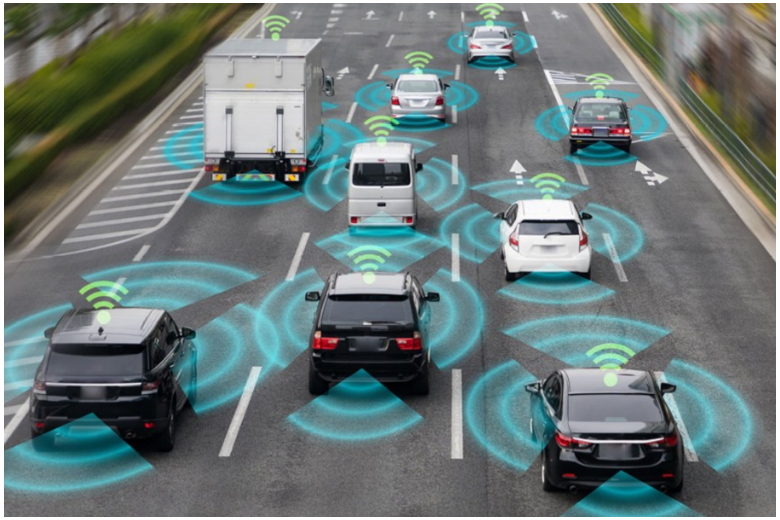


For some systems, successive events may be separated by long periods of time

As for other systems, successive events may occur more or less simultaneously

Time is critical in many domains: services, communication networks, manufacturing, robotics …

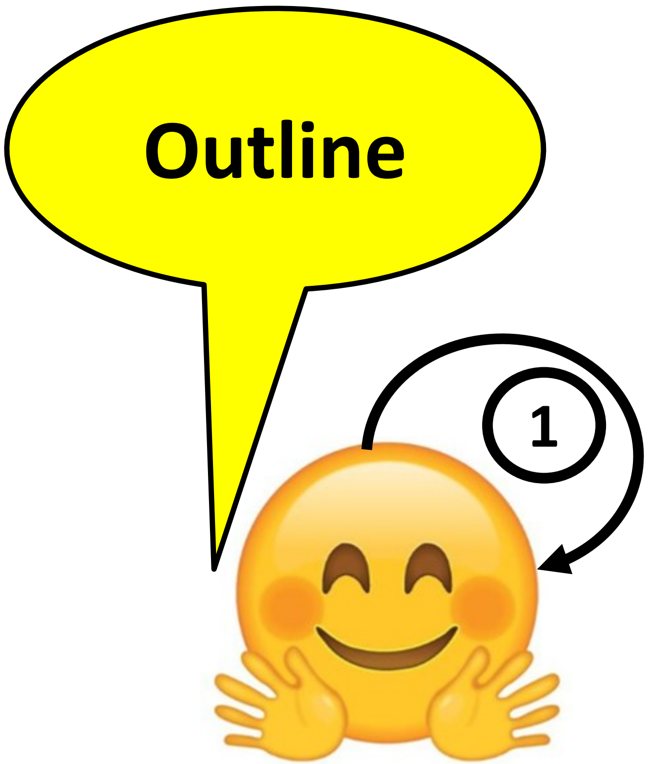
Time management in transport and logistics is required to satisfy costumers



Time management in automatic vehicules guidance is required for the security and confort of the users

Time management in medical and urgency scheduling can save life

Time analysis can save money in trading and financial operations



1. Introduction and motivation

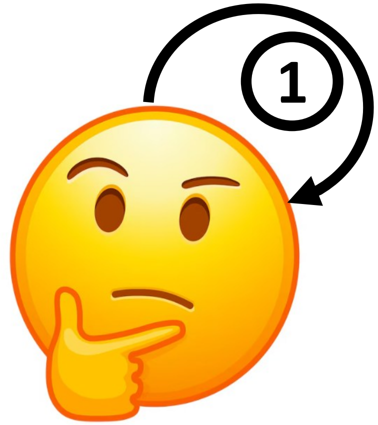
2. Modeling timed discrete event systems with automata
- Timed automata
- Tick automata
- Automata with time interval (ATI)
- Clock Interval Automata (CIA)

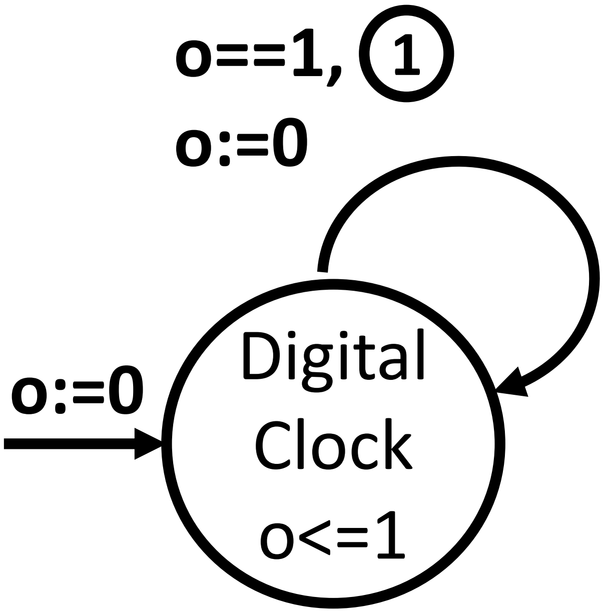
3. Observation mechanisms based on labeled CIA
- Static observation
- Dynamic observation
- Orwellian observation

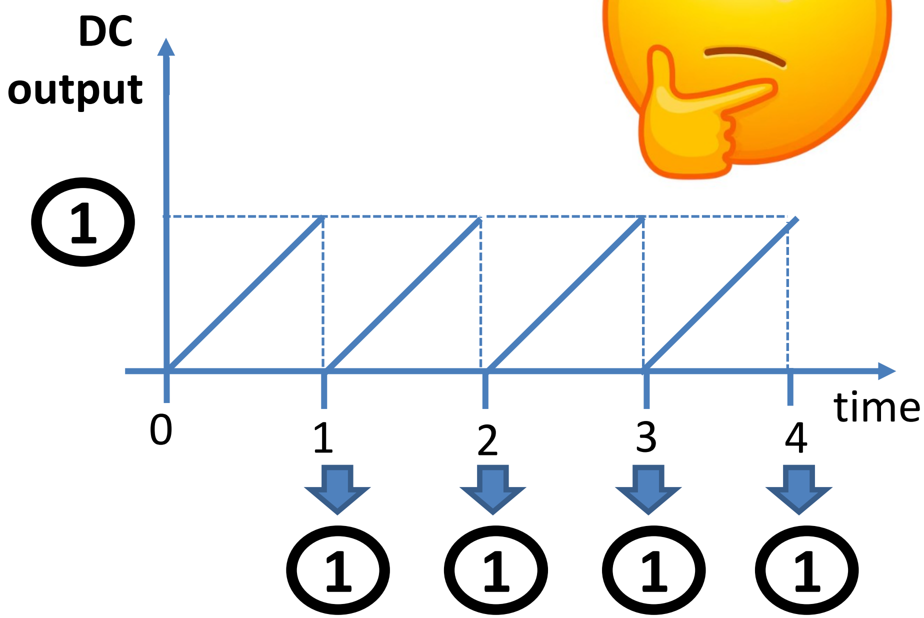
4. Application to cyber physical systems
- Fault diagnosis and diagnosability
- Opacity analysis
- Attack detection

5. Conclusion and perspectives

Digital clock without enforced reset



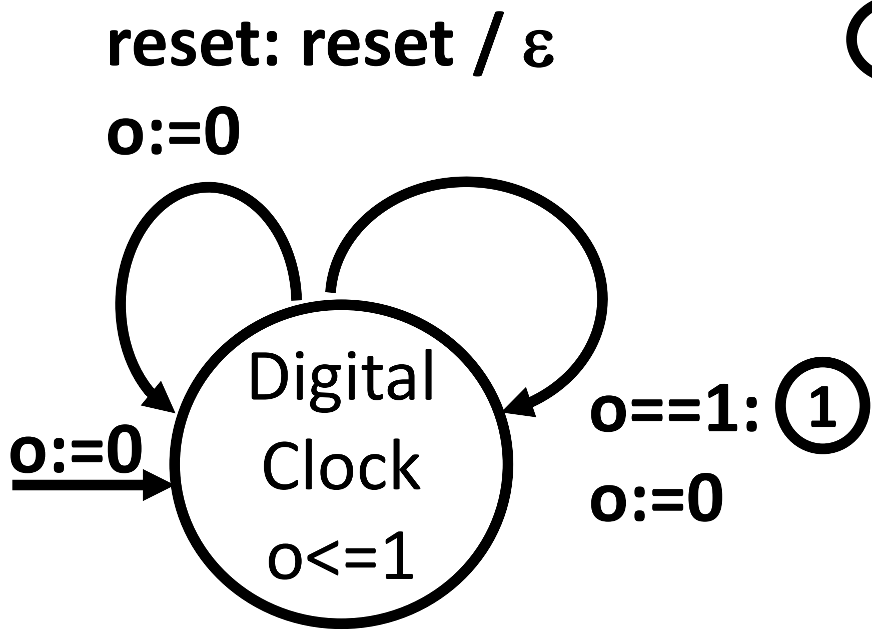


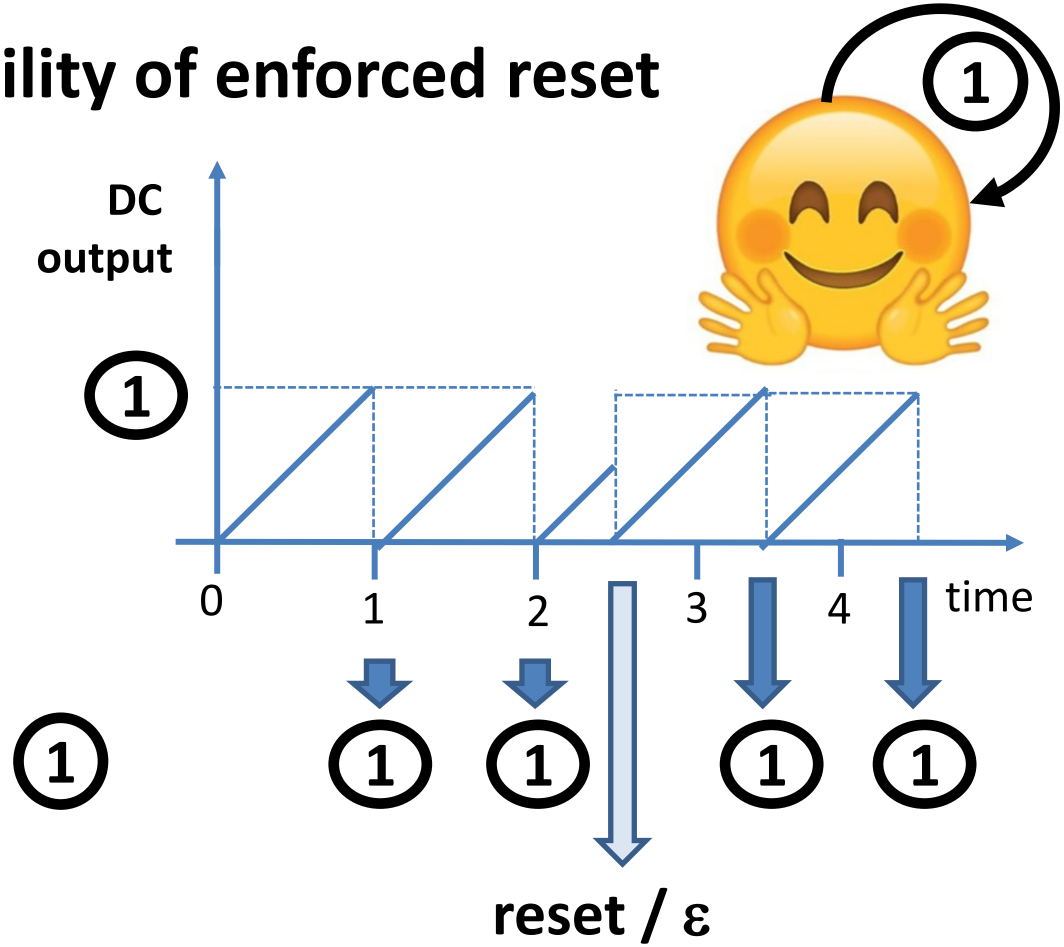


A DC without reset measures the « natural » time

Xu et al. 2010; Xu et al. 2011

Digital clock with possibility of enforced reset

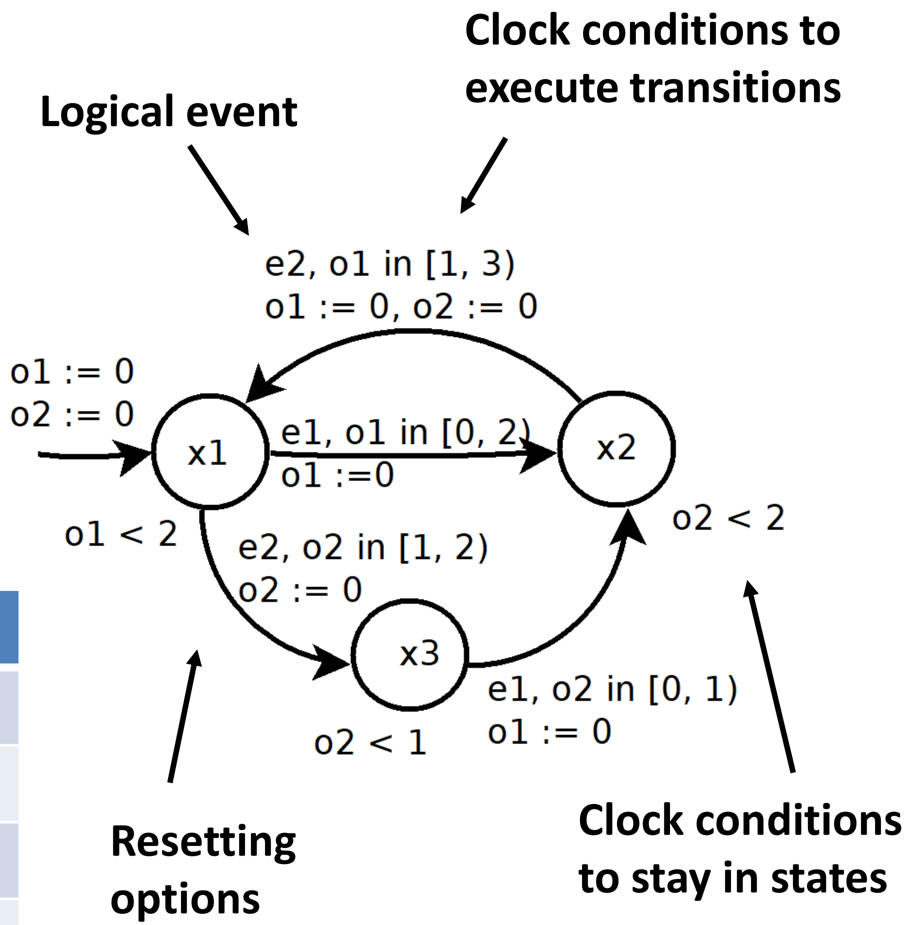




A DG with resets biases the « natural » time

2.1 Timed automata (TA)

- Time is continuous
- One or more clocks
- Various clock resetting options
- Events occur at any time that satisfy the clock constraints
- Time semantics is defined by the clock constraints



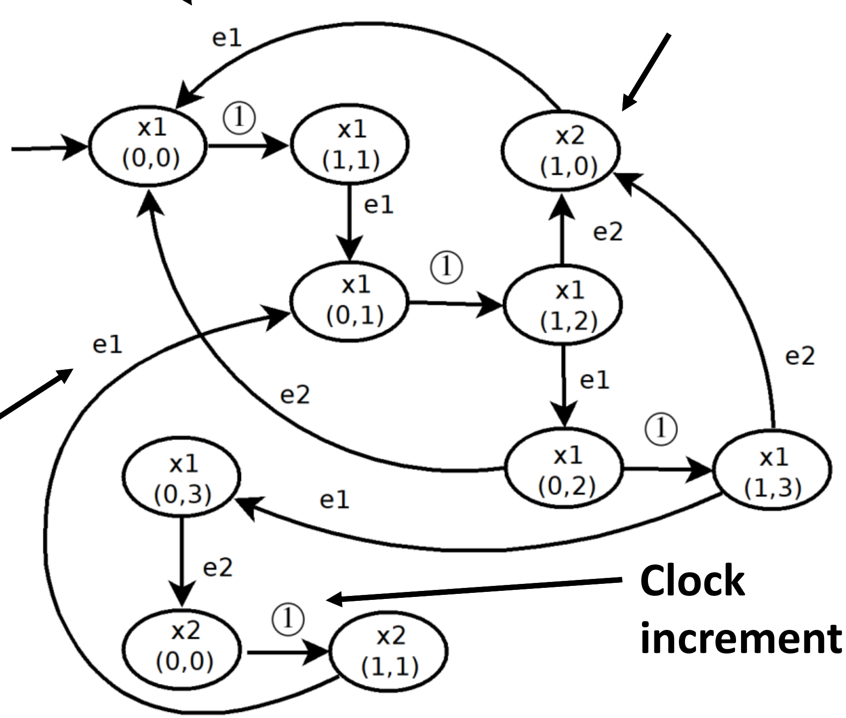
Transition	Event	Clock	Domain	Reset
(1,2)	e1	o1	[0, 2)	R1, H2
(1,3)	e2	o2	[1, 2)	H1, R2
(3,2)	e1	o2	[0, 1)	R1, H2
(2,1)	e2	o1	[1, 3)	R1, R2

Time specifications

Alur et al., 1994

2.2 Tick automata (Tick A)

- Time is discrete modeled by the tick events
- Events occur at specific time instants
- One clock is associated to each event
- Each event occurrence resets the corresponding clock
- Time semantics is strong



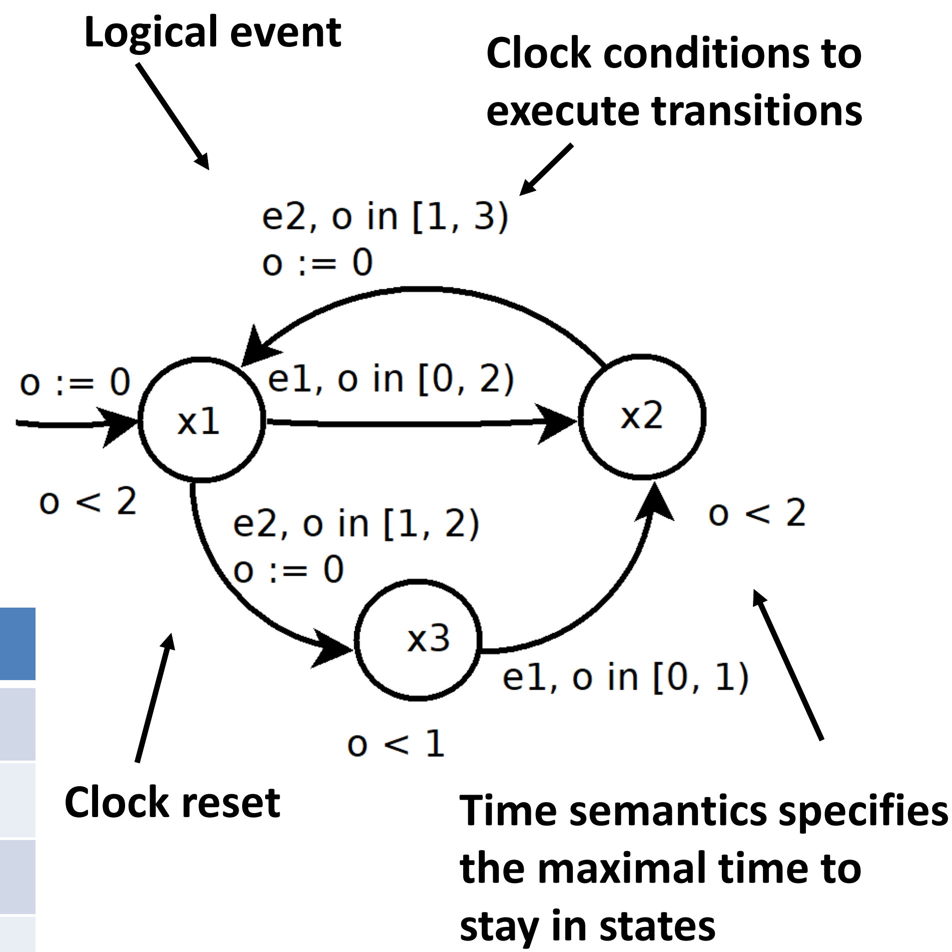
Event	Clock	Time domain	Reset
e1	o1	{1}	R1
e2	o2	{2, 3}	R2

Time specifications

Brandin et al., 1994

2.3 Automata with Time Intervals (ATI)

- Time is continuous
- Single clock
- Various clock resetting options
- Events occur within specific time intervals
- Time semantics is defined by the clock constraints

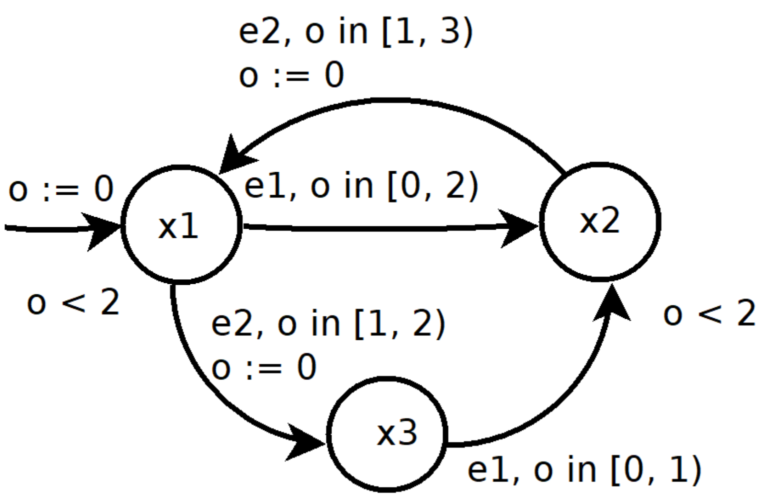


Transition	Event	Clock	Domain	Reset
(1,2)	e1	o	[0, 2)	H
(1,3)	e2	o	[1, 2)	R
(3,2)	e1	o	[0, 1)	H
(2,1)	e2	o	[1, 3)	R

Time specifications

Li et al., 2021; Gao et al., 2020; Lefebvre et al. 2023

Automata with Time Interval (ATI)



Definition : An **Automaton with Time Intervals** (ATI) is a 7-tuple A=(X, E, o, **I**, RC, Δ, TS, x_0) where

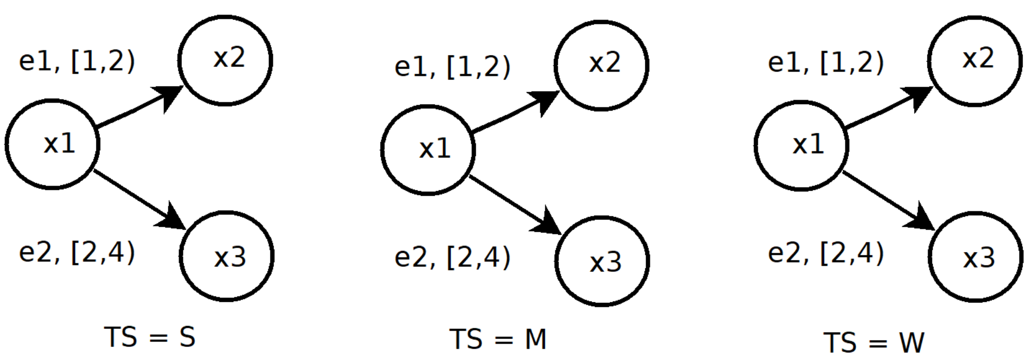
- X is a finite set of states
- E is a finite set of events
- o is a clock
- **I** is a set of time intervals of the form [a, b)
- **RC** = {R, H} is a set of resetting options
  - H = hold on
  - R = reset to 0
- $\Delta \subseteq X \times E \times$ **I** $\times$ **RC** $\times X$ is a timed transition relation
- TS is the time semantics defined by
  - W : weak
  - M : mixed or intermediate
  - S : strong
  - Additional clock constraints
- x_0 is the initial state

Comment 1 about the time semantics

In the **strong time semantics** (TS= S), when any of the activated transitions reaches the upper bound of its firing interval, then the transition must fire. Note that with strong TS some transitions may never fire and consequently some states may never be reached

In the **mixed (or intermediate) time semantics** (TS= M), one of the activated transitions at each state should fire within its time interval. This TS makes particular sense for timed fault patterns

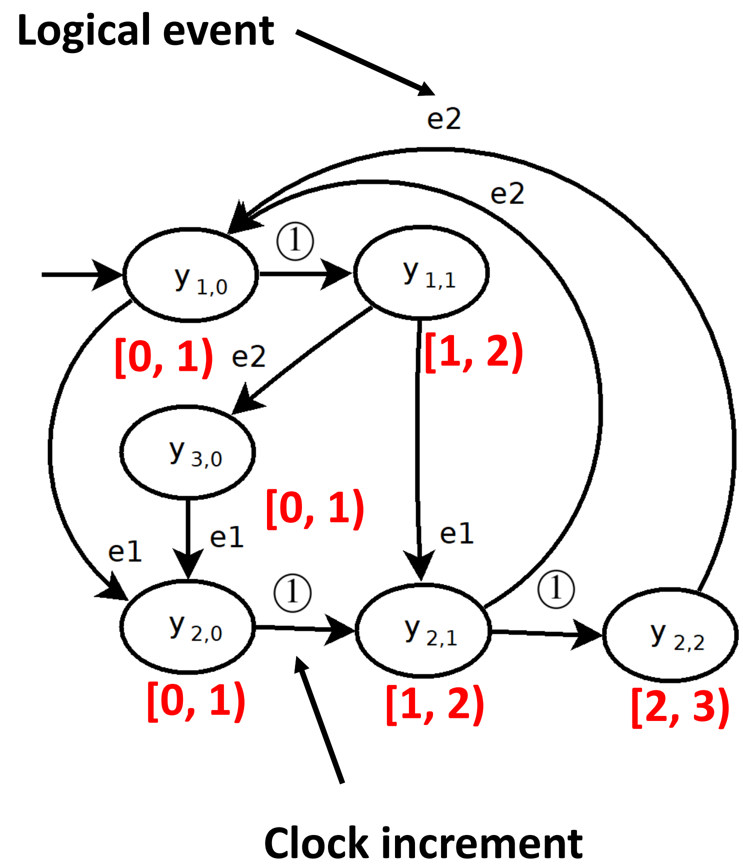
In the **weak time semantics** (TS= W), an activated transition can fire within its firing interval. If, in a given state, no activated transition fires within its time interval, then the system stays eternally at this state



maximal sojourn time in x1 : $\tau_{max}(x1) = 2$ TUs $\tau_{max}(x1) = 4$ TUs $\tau_{max}(x1) = +\infty$

2.4 Clock interval automata (CIA)

- Time is continuous
- Single clock
- Various clock resetting options
- Events occur within specific time intervals
- Time semantics is defined by the clock constraints



Transition	Event	Clock	Domain	Reset
(1,2)	e1	o	[0, 2)	H
(1,3)	e2	o	[1, 2)	R
(3,2)	e1	o	[0, 1)	H
(2,1)	e2	o	[1, 3)	R

Time specifications

Li et al., 2021; Gao et al., 2020; Basilio et al., 2023; Lefebvre et al. 2023

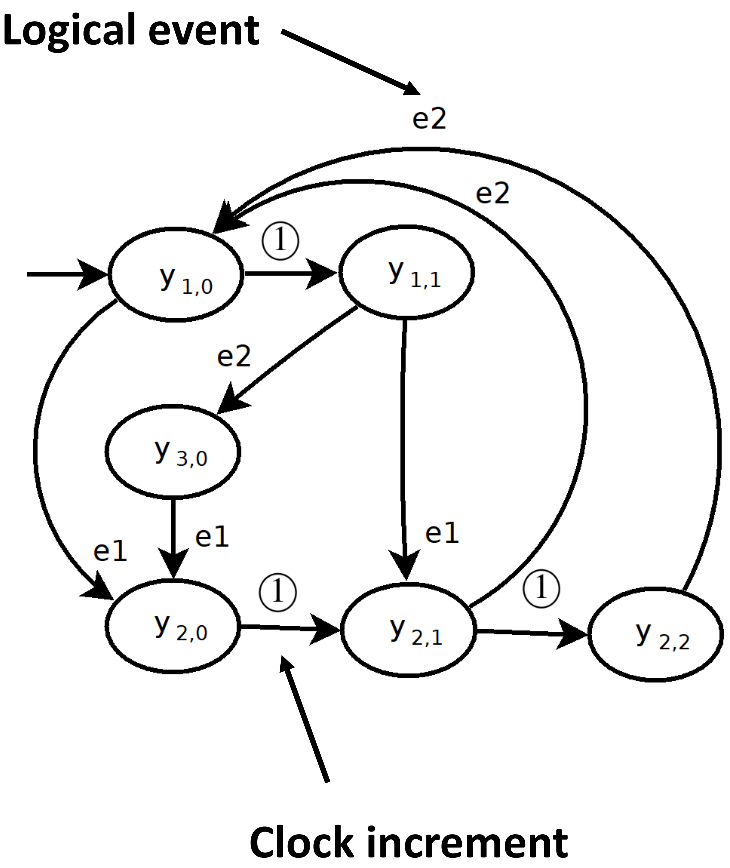
Transformation of an ATI into a CIA

Definition : A **clock interval automaton** (CIA) is a 5-tuple $Y_A=(Y, E_Y, o, \Delta_Y, y_0)$ where

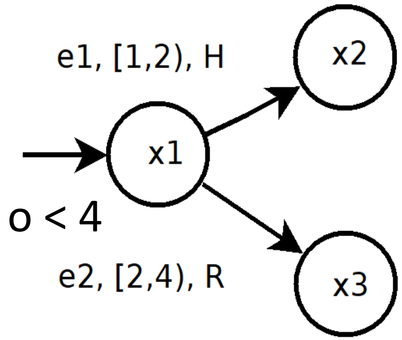
- Y is a finite set of extended states $y_{i,j}$
  - i refers to location x_i
  - j refers to clock domain [j , j+1)
- E_Y is a finite set of events
- o is a clock
- $\Delta_Y \subseteq X \times E_Y \times X$ is a transition relation
- y_0 is the initial state

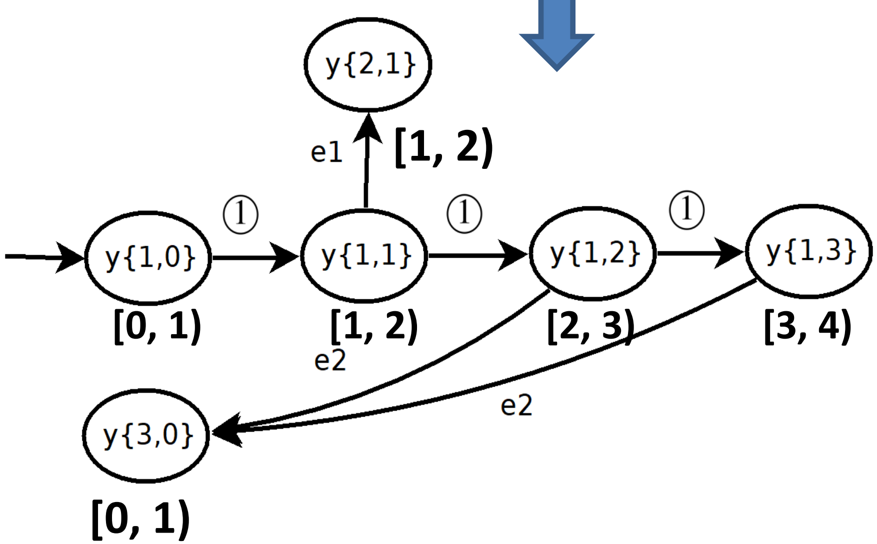
$E_Y = E \cup \{①\}$

① : tick event



Transformation of an ATI into a CIA





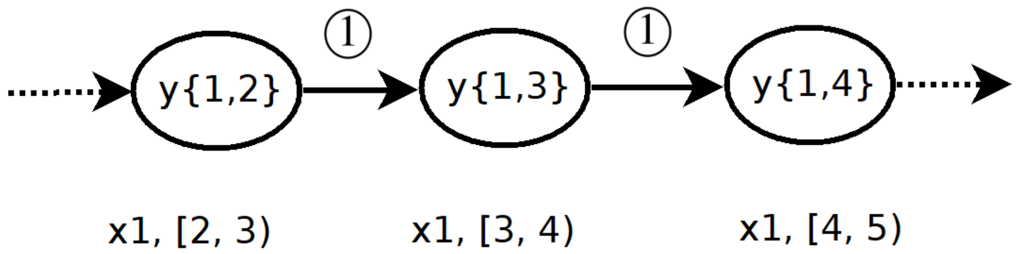
$\tau_{max}(x_i)$: the maximal sojourn time in x_i
$Y(x_i) = \{0, 1, \ldots, \tau_{max}(x_i)-1\}$
each $j \in Y(x_i)$ means that the system may stay at x_i within the time interval $[j , j + 1)$ of width 1

y{i,j} is an extended state that refers both to the state x_i and time domain $[j , j + 1)$

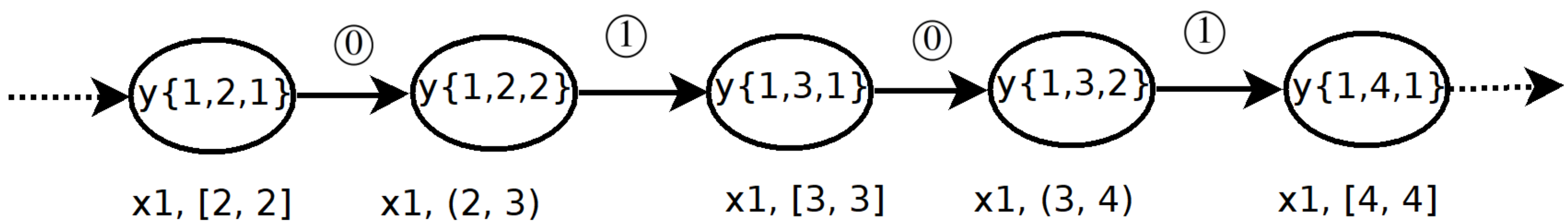
$\tau_{min}(x_i ,e , l, x_j)$: the minimal time at which transition (x_i ,e , l, x_j) may fire
$\tau_{max}(x_i ,e , l, x_j)$: the maximal time at which transition (x_i ,e , l, x_j) may fire
$Y(x_i ,e , l, x_j) = \{\tau_{min}(x_i ,e , l, x_j), \ldots, \tau_{max}(x_i ,e , l, x_j)-1\}$

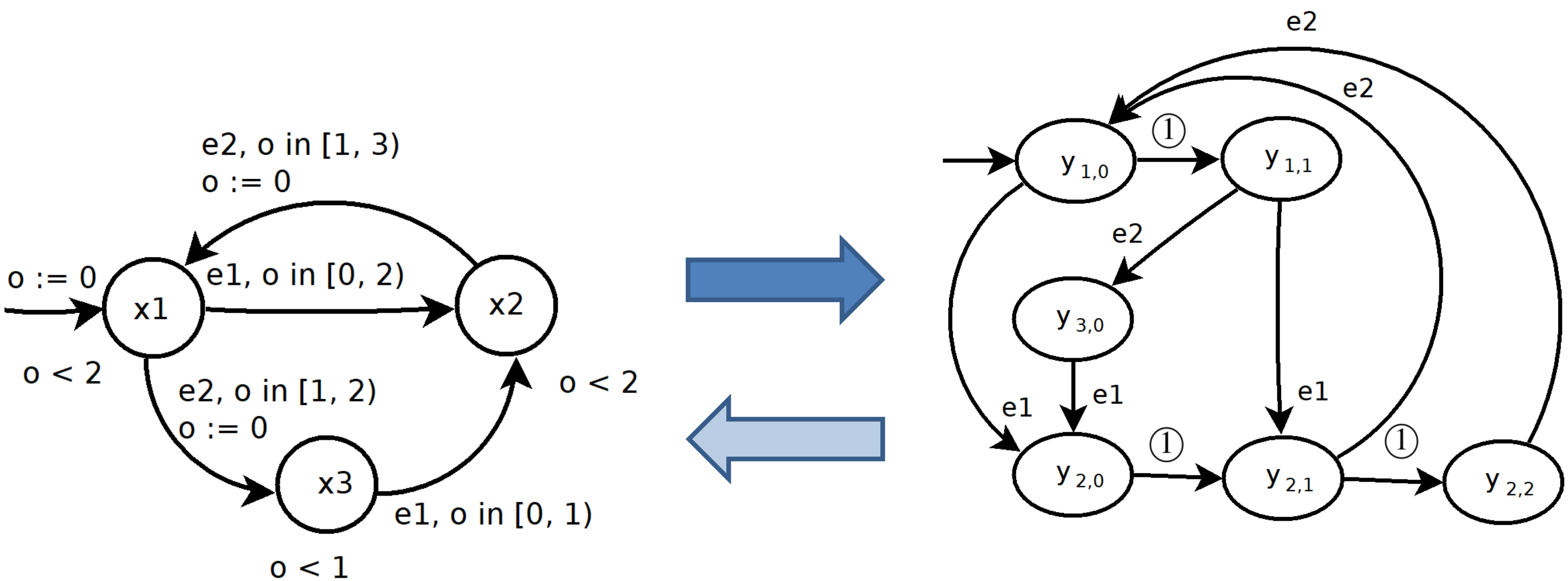
<u>Comment 2</u> about time intervals

$[2, 4) = [2, 3) \cup [3, 4)$



$[2, 4] = [2, 2] \cup (2, 3) \cup [3, 3] \cup (3, 4) \cup [4, 4]$





Automata with Time Intervals

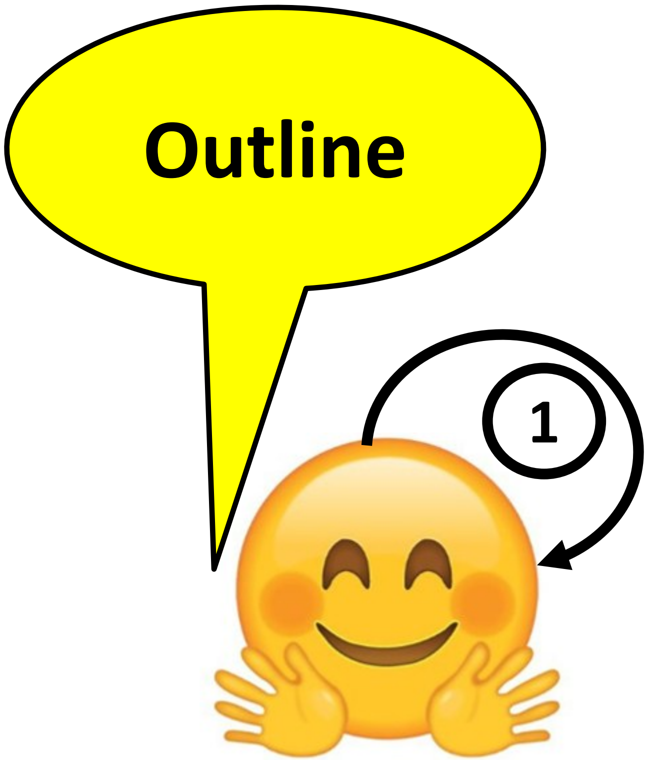
Clock Interval Automata

Intermediate conclusion

Advantages of CIA compared to other timed DES models
⇒ Use trivial extensions of standard compositions and operations

- Product
- Parallel composition
- Determinisation
- Silent closure

Limitations of CIA
⇒ Time precision / size
⇒ Multiple settings
- Time semantics
- Resetting options
- Interval bounds
- ....



1. Introduction and motivation

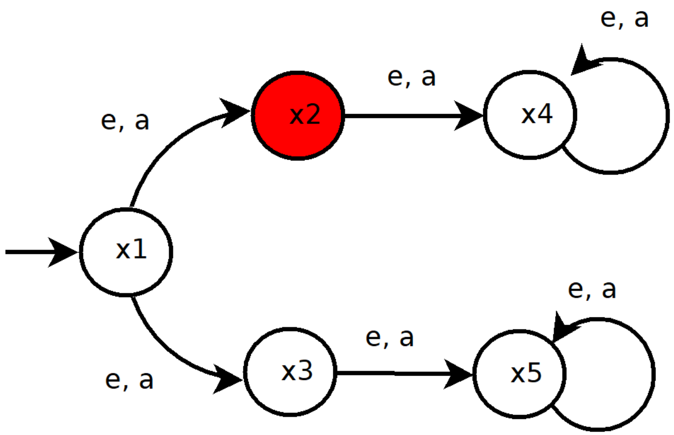
2. Modeling timed discrete event systems with automata
   - Timed automata
   - Tick automata
   - Automata with time intervals (ATI)
   - Clock Interval Automata (CIA)

3. Observation mechanisms based on labeled CIA
   - Static observation
   - Dynamic observation
   - Orwellian observation

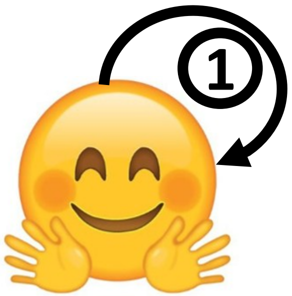
4. Application to cyber physical systems
   - Fault diagnosis and diagnosability
   - Opacity analysis
   - Attack detection

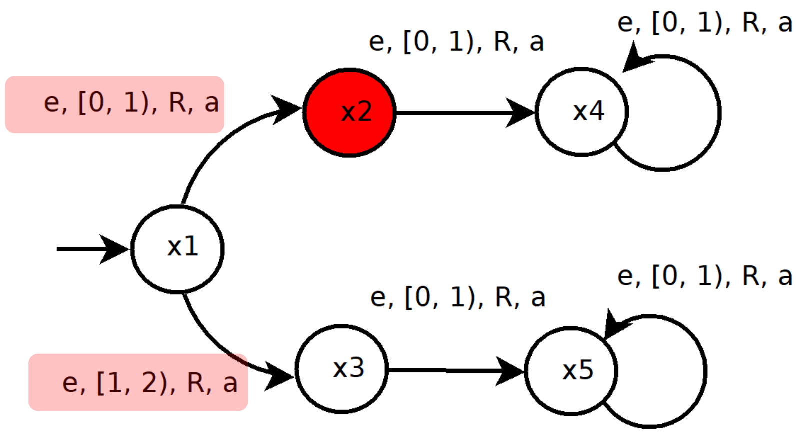
5. Conclusion and perspectives

Time in state estimation problems



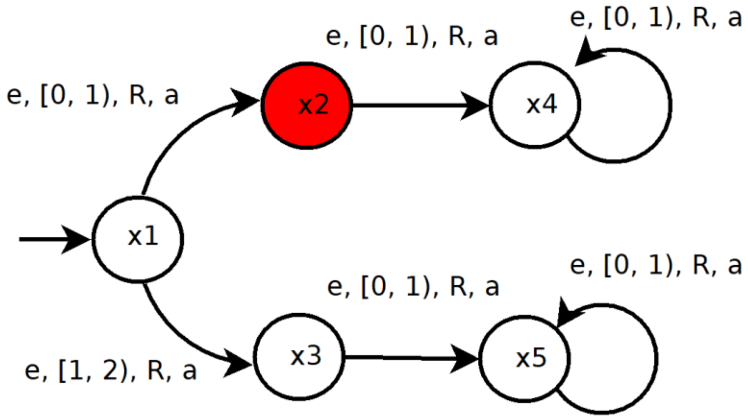
Logical setting : one cannot know if the system stays in x2





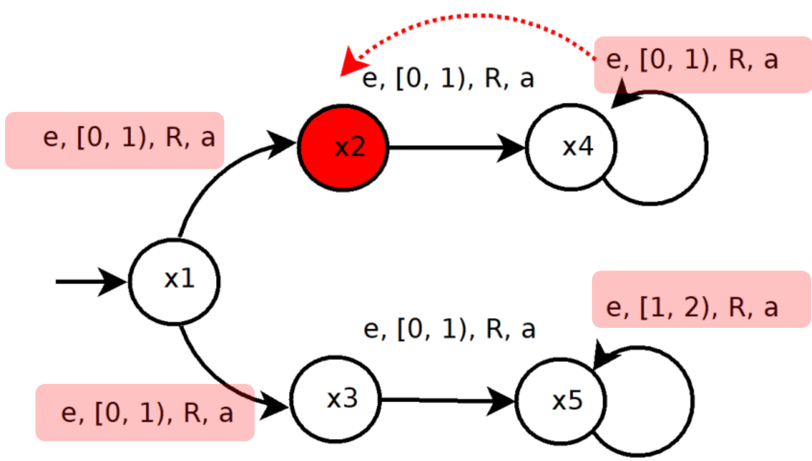
Time setting : one knows if the system stays in x2

Time in state estimation problems : state-trajectory opacity problem
One want to know if the system as visited x2



Static observation mechanism:
P : e -> a during [0, +∞)

Dynamic observation mechanism:
P : e -> a during [0, 1)



Orwellian observation mechanism:
P : e -> a during [0, 3)
Information is re-constructed a posteriori

3.1 Static observation mechanism

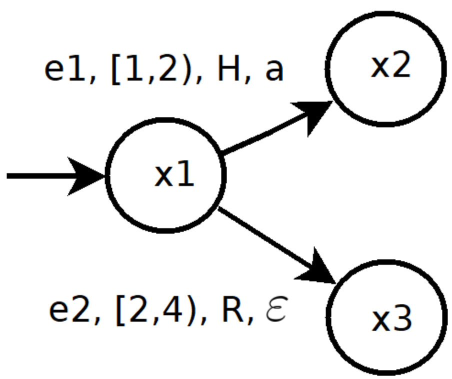
Definition : A labeled Automaton with Time Intervals (LATI) is a triplet (A, Q, P) where

- A is a CIA
- Q is a set of output labels
- P is a labeling function

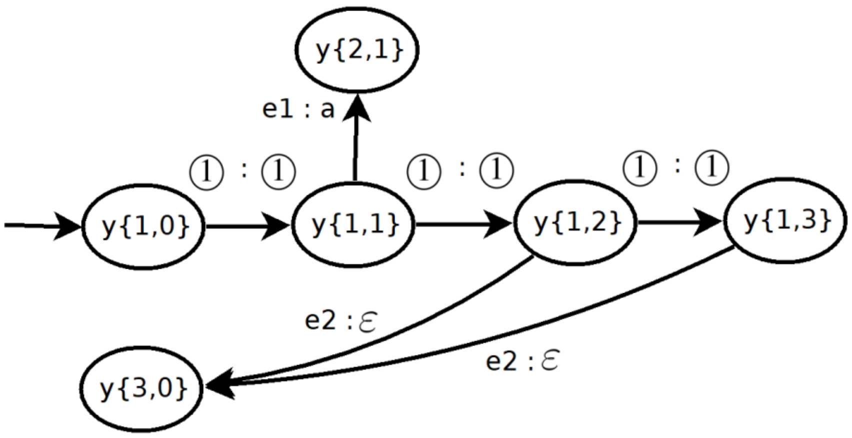
Definition : A labeled clock interval automaton (LCIA) is a triplet (Y_A, Q_Y, P_Y) where

- Y_A is a CIA
- Q_Y is a set of output labels
- P_Y is a labeling function

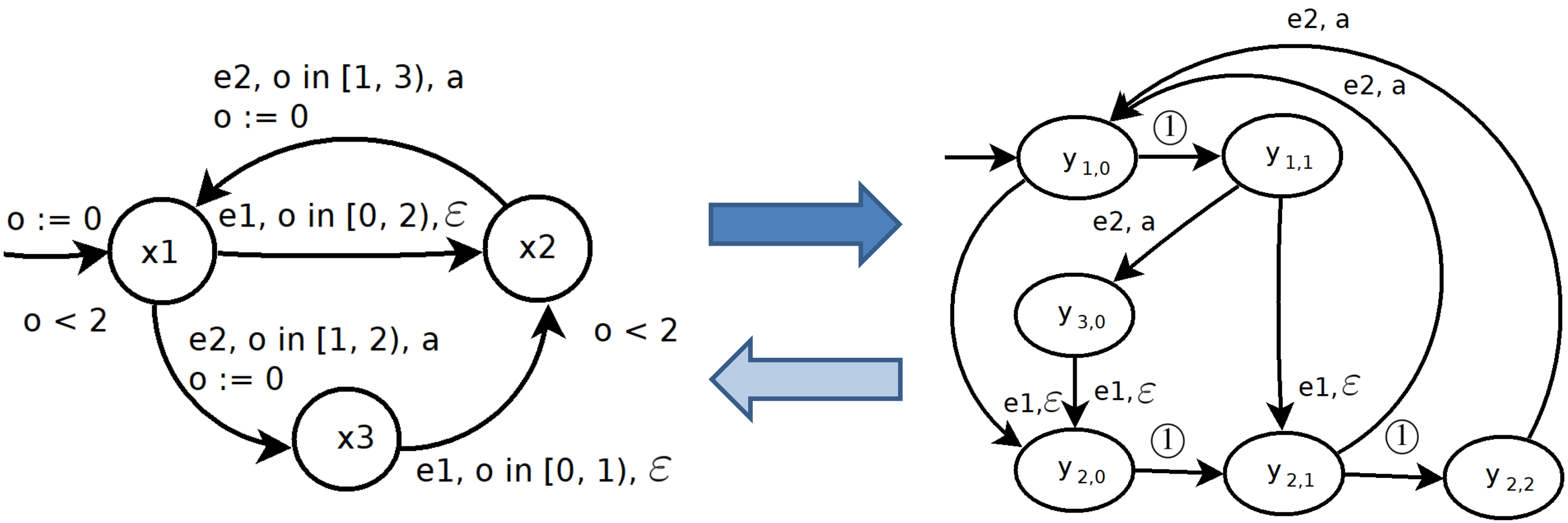
$Q_Y = Q \cup \{ ① \}$



Labeled ATI (LATI)



Labeled CIA (LCIA)



Labeled Automata with Time Intervals (LATI) **Labeled Clock Interval Automata (LCIA)**

Static observation mechanism
P : E -> Q

Transition	Event	P(e)
(1,2)	e1	ε
(1,3)	e2	a
(3,2)	e1	ε
(2,1)	e2	a

Static observation mechanism
P : E ∪ { ① } **->** Q ∪ { ① }

LATI level

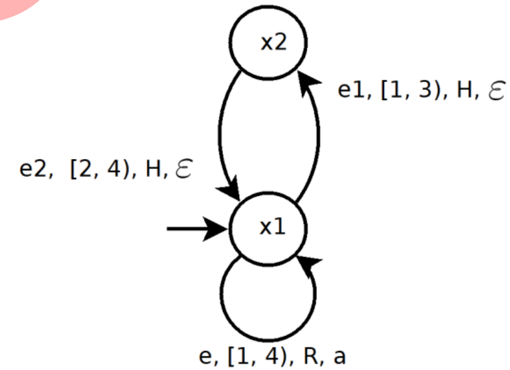
timed trajectory p: $(x_1, 0)$ - $(e_1, 1.5)$ -> $(x_2, 1.5)$ - $(e_2, 3)$ -> $(x_1, 3)$ - $(e, 3.5)$ -> $(x_1, 0)$

LATI

timed sequence of events : w = $(e_1, 1.5)$ $(e_2, 3)$ $(e, 3.5)$

Observation projection P

timed sequence of observations σ = (a, 3.5)



LCIA level

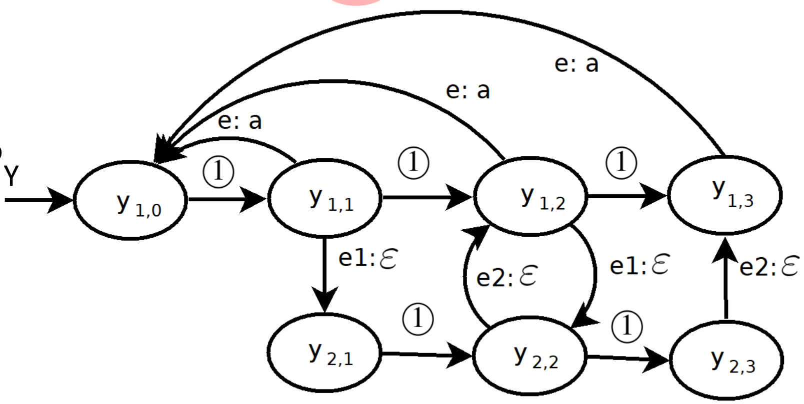
production p_Y : $y_{1,0}$ -①-> $y_{1,1}$ - e_1 -> $y_{2,1}$ -①-> $y_{2,2}$ -①-> $y_{2,3}$ - e_2 -> $y_{1,3}$ - e -> $y_{1,0}$

LCIA

sequence w_Y = ① e_1 ① ① e_2 e

Observation projection P_Y

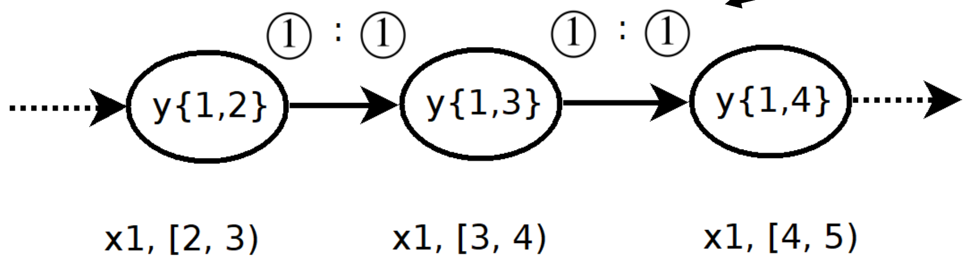
sequence of observations σ_Y = ① ① ① a



Comment 2 (follow up) about time intervals

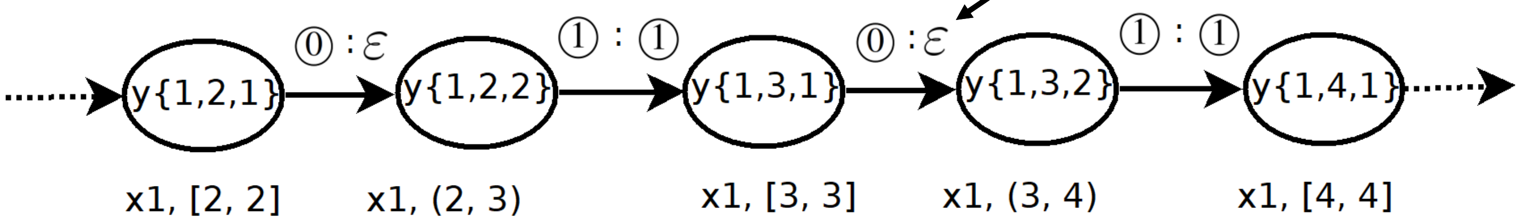
$[2, 4) = [2, 3) \cup [3, 4)$

Observable



Non observable

$[2, 4] = [2, 2] \cup (2, 3) \cup [3, 3] \cup (3, 4) \cup [4, 4]$



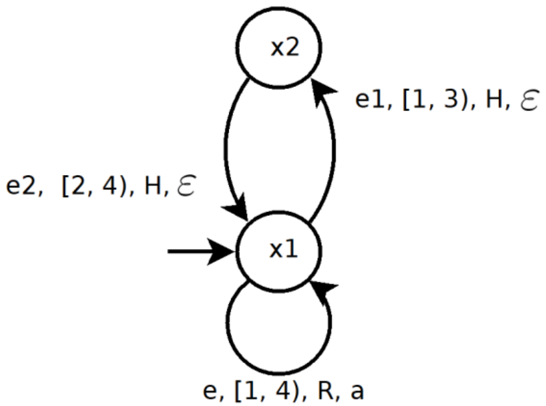
Observer design by determinisation

Definition : The **determinisation** (observer) of the LCIA $Y_A=(Y, E_Y, o, \Delta_Y, y_0, Q_Y, P_y)$ is defined as a deterministic CIA $O_A=(Z, Q_Y, o, \Delta_Z, z_0)$ where:

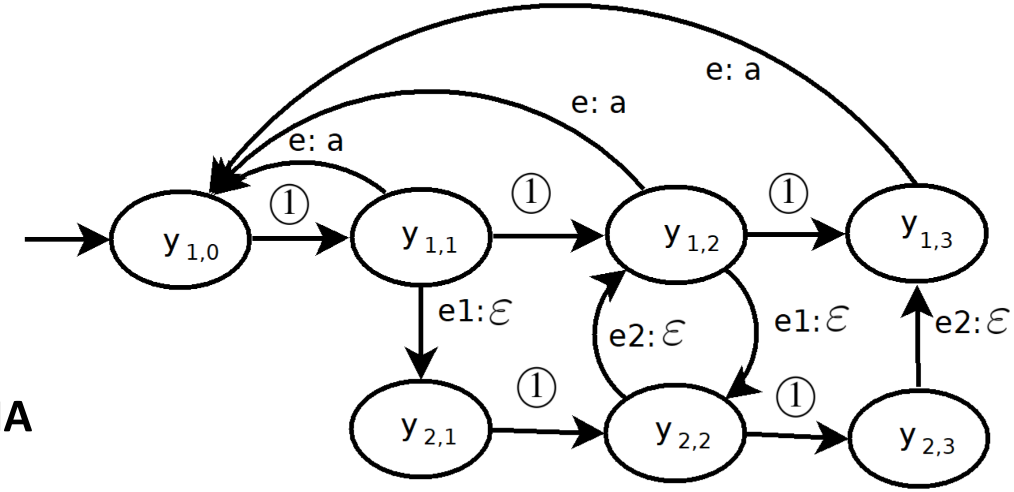
- $Z \subseteq 2^Y$: set of observer states
- Q_Y is the set of labels of Y_A
- o is the clock
- Δ_Z is the deterministic transition relation defined for all z and q by $(z,q, z') \in \Delta_Z$ with $z' = \cup \{S(y,q) : y \in z\}$ if $z' \neq \varnothing$
- $z_0 = S(y, \varepsilon)$ is the initial observer state

- $S(y, \varepsilon)$: set of extended states reachable Y by executing 0 or more unobservable transitions
- $S(y, q)$: set of extended states reachable from y by executing exactly 1 observable transition labeled by q followed by 0 or more unobservable transitions

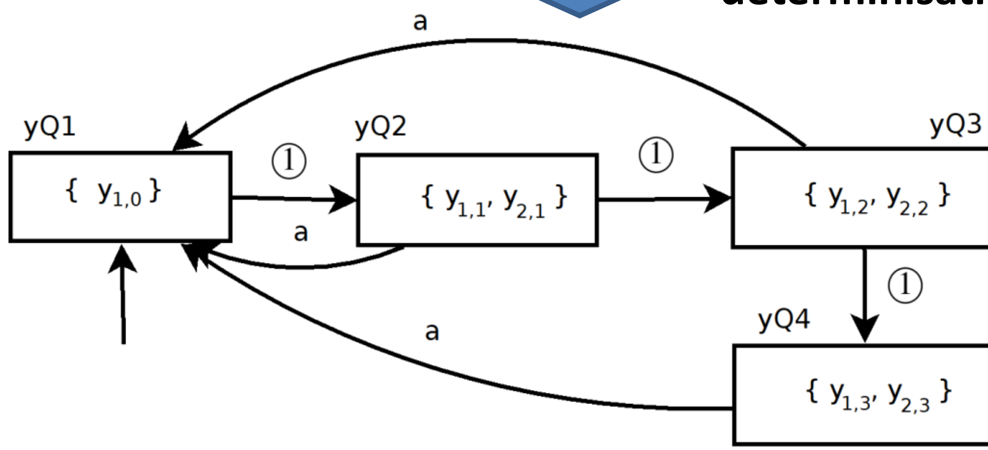
Observer design by determinisation



LATI to LCIA



determinisation



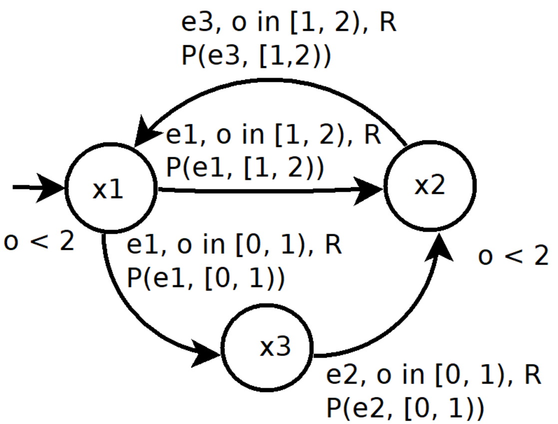
The determinisation provides
- **Set of locations**
- **Set of clock regions**

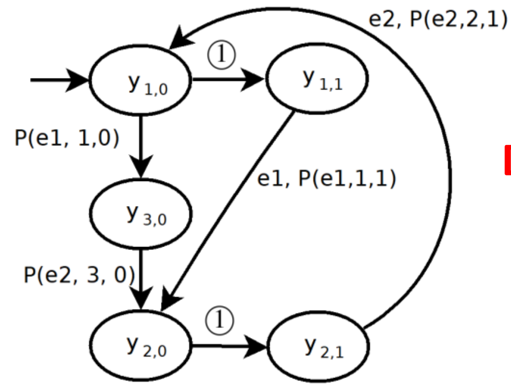
consistent with a given sequence of timed observations

The complexity is double EXP

Li et al. 2022; Gao et al., 2025;

3.2 Dynamic observation mechanism : energy saving, detectability or opacity enforcement





Sensor activation policy

Deterministic saves energy

Stochastic sensor failures

Transition	Event	Domain	$P_1(e)$
(1,2)	e1	[1, 2)	**a**
(1,3)	e1	[0, 1)	**a**
(3,2)	e2	[0, 1)	**b**
(2,1)	e3	[1, 2)	**c**

Transition	Event	Domain	$P_2(e,l)$	$P_3(e,l)$
(1,2)	e1	[1, 2)	**a**	**{ a, ε }**
(1,3)	e1	[0, 1)	**ε**	**{ a, ε }**
(3,2)	e2	[0, 1)	**b**	**b**
(2,1)	e3	[1, 2)	**c**	**c**

Static observation mechanism
P : E -> Q

Dynamic observation mechanism
P : E x IN x IN -> 2^Q

Shu et al., 2010; Wang et al. 2010; Yin et al 2019; Mao et al., 2024

3.3 Orwellian observation mechanism : declassification

$E = E_o \cup E_{do} \cup E_{uo}$ is a finite set of events:

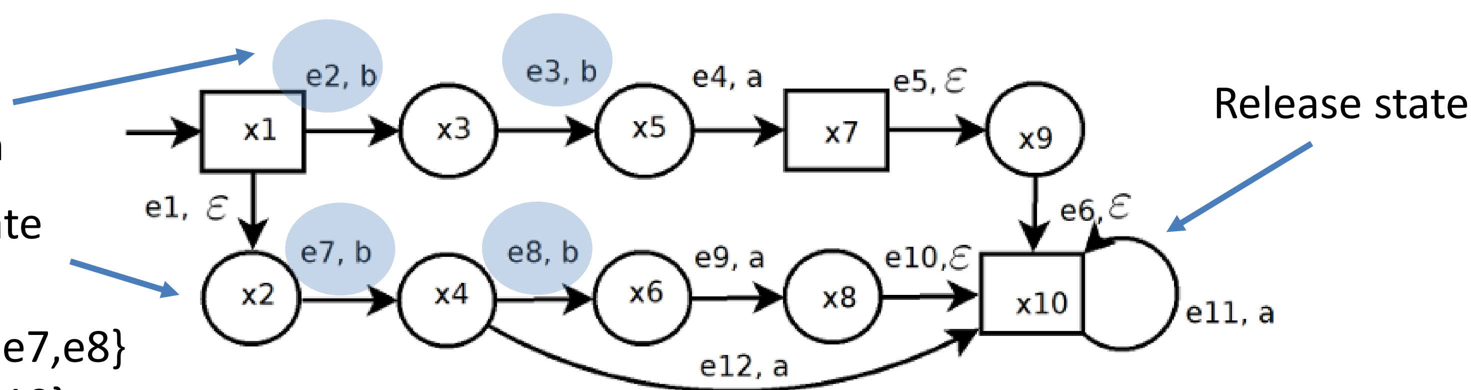
- E_o : subset of instantly observable events
- E_{do} : subset of events whose observation is delayed
- E_{uo} : subset of silent events

$X = X_R \cup X_H$ is a finite set of discrete locations:

- X_R subsets of states that release the delayed observations
- X_H subsets of states that hold on the delayed observations

Delayed observation

Hold on state

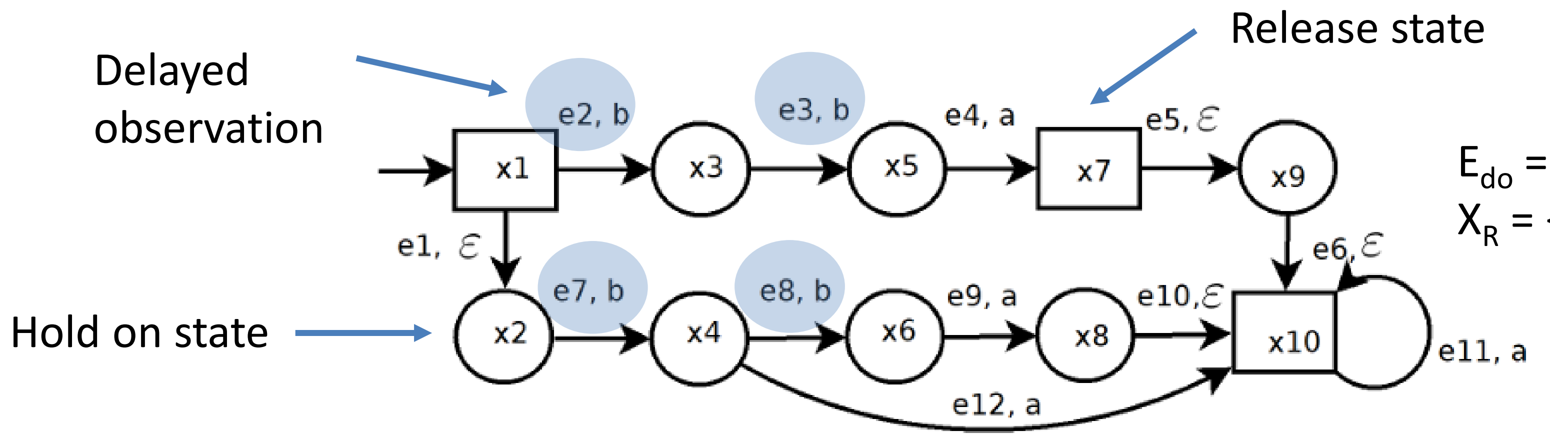


$E_{do} = \{e2, e3, e7, e8\}$

$X_R = \{x1, x7, x10\}$

All time intervals are assumed to be [0, 1), all events are assumed to reset the clock

Mullins et al., 2014 ;Hou et al., 2022



E_{do} = {e2,e3,e7,e8}
X_R = {x1,x7,x10}

timed trajectory p: $(x_1, 0)$ - $(e_2, 0.5)$ -> $(x_3, 0.5)$ - $(e_3, 1.2)$ -> $(x_5, 1.2)$ - $(e_4, 1.3)$ -> $(x_7, 1.3)$

LATI with release states

timed sequence of events : w = $(e_2, 0.5)$ $(e_3, 1.2)$ $(e_4, 1.3)$

Orwellian observation projection P

timed sequence of observations σ = (a, 1.3) (b, 1.3) (b, 1.3)

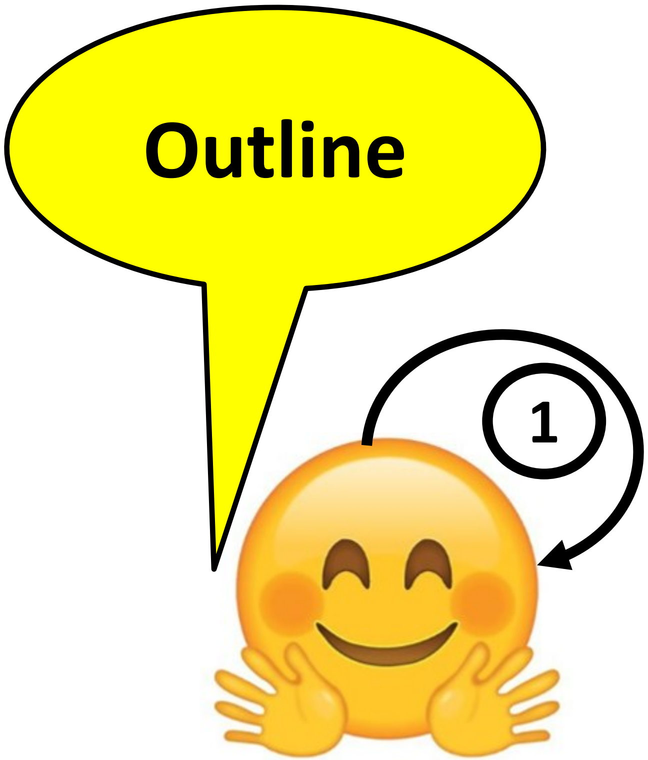
Intermediate conclusion

LCIA are ready to design various observation structures

$\Rightarrow$ **Delays**
$\Rightarrow$ **Losses**
$\Rightarrow$ **Release**
$\Rightarrow$ **…**

Current challenges include:

$\Rightarrow$ **Computational complexity : twin plants, … ??**
$\Rightarrow$ **Distributed setting :desynchronized multiple clocks, …. ??**



1. Introduction and motivation

2. Modeling timed discrete event systems with automata
   - Timed automata
   - Tick automata
   - Automata with time intervals (ATI)
   - Clock Interval Automata (CIA)

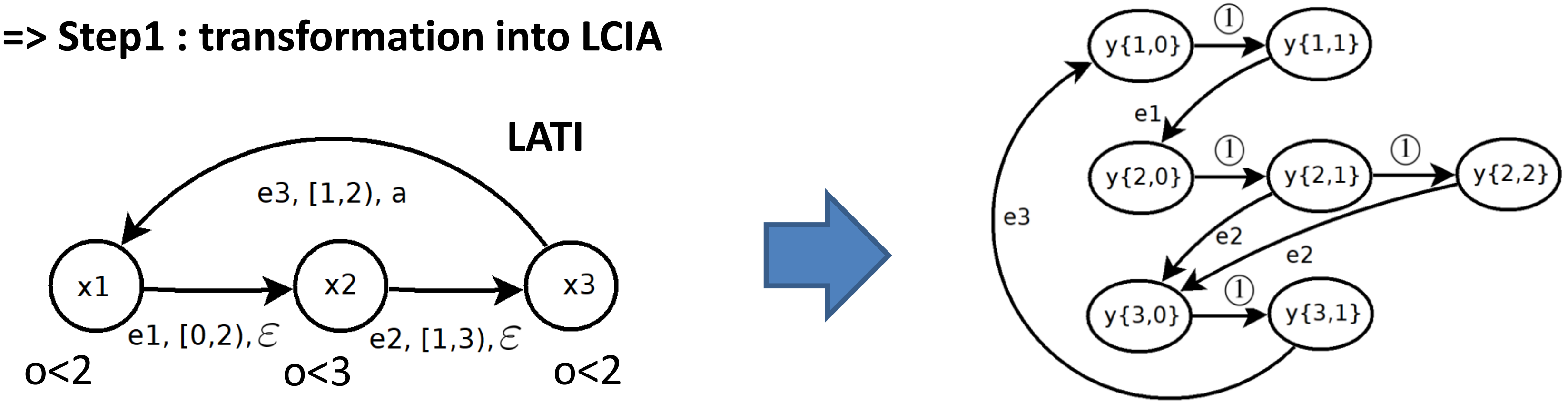
3. Observation mechanisms based on labeled CIA
   - Static observation
   - Dynamic observation
   - Orwellian observation

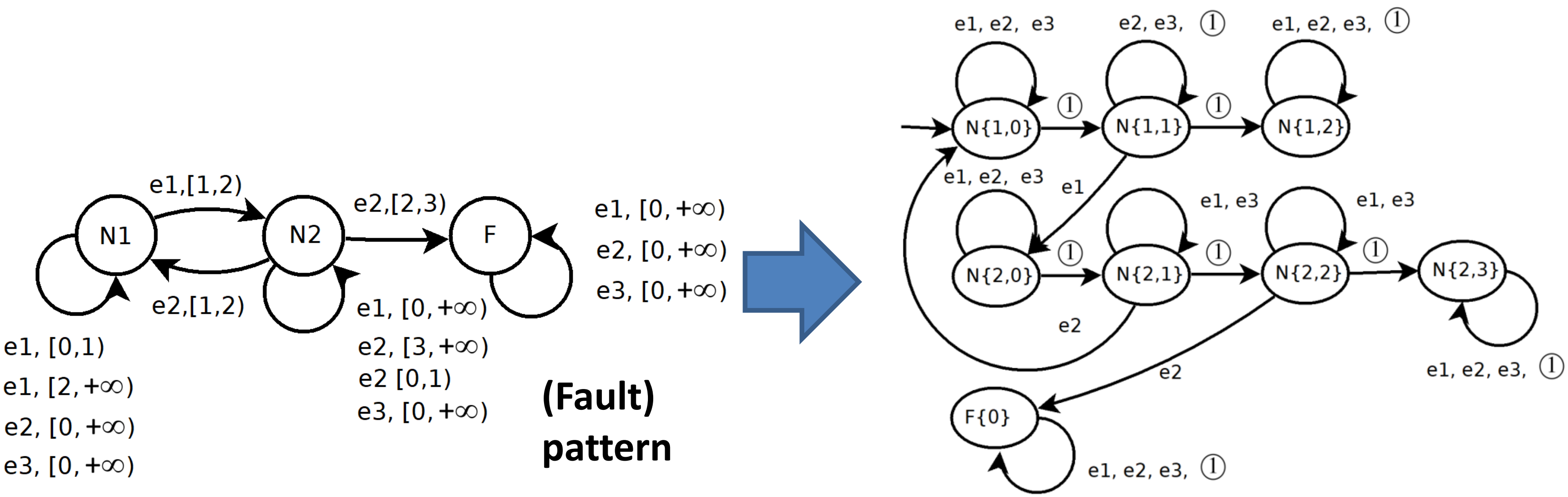
4. Application to cyber physical systems
   - Fault pattern diagnosis and diagnosability
   - Opacity verification
   - Attack detection

5. Conclusion and perspectives

4.1 Fault pattern diagnosis and diagnosability

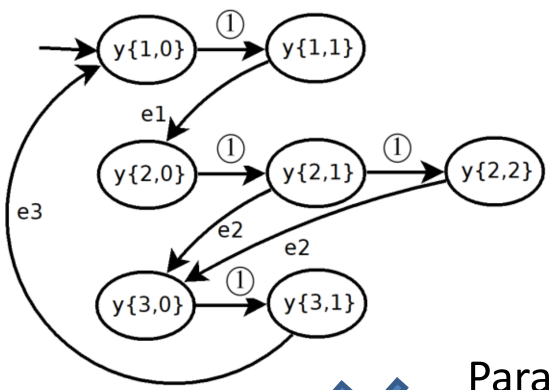
=> Step1 : transformation into LCIA



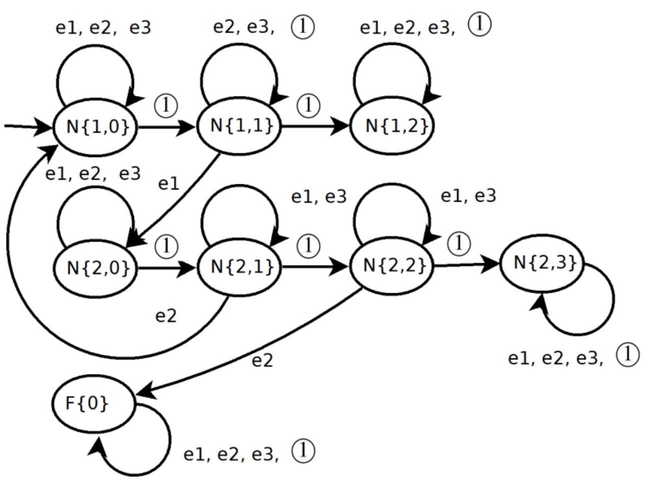


Lefebvre et al. 2023

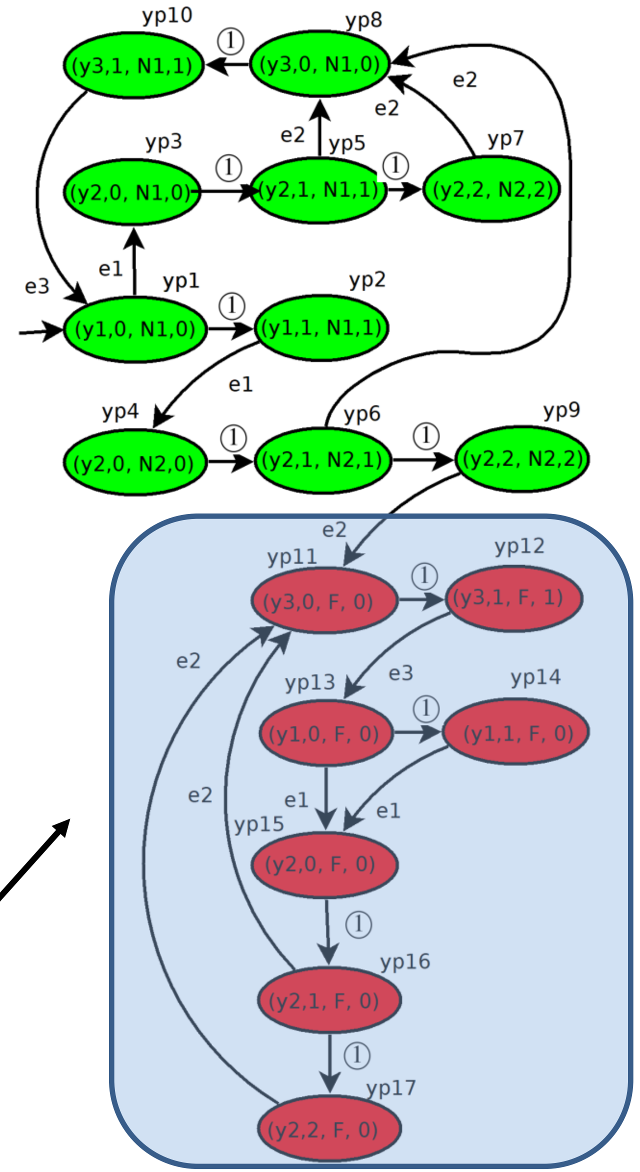
=> Step2 : Recognizer design



Parallel composition

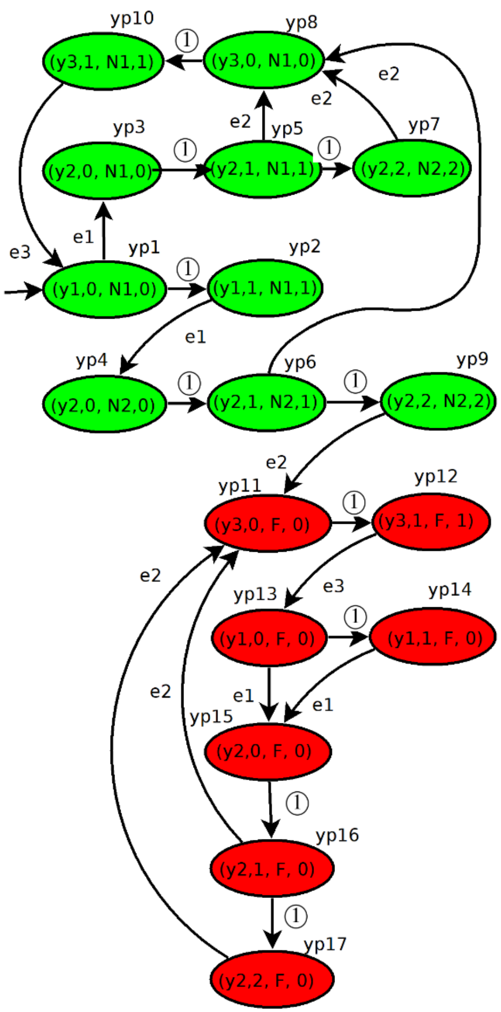


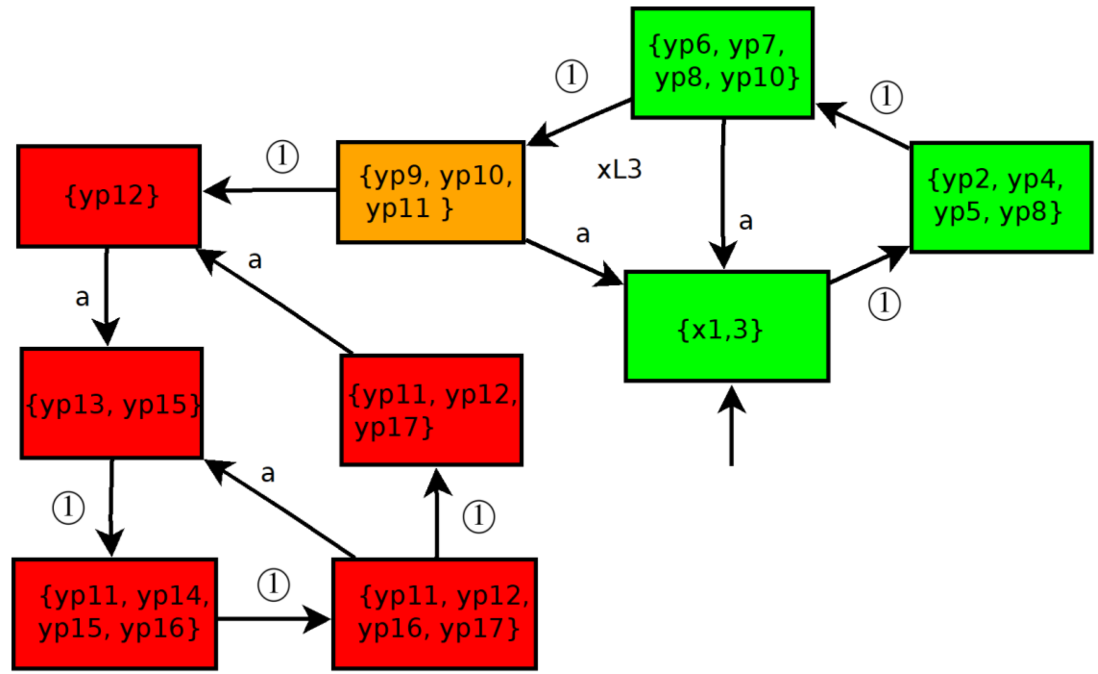
LCIA recognizer



F recognizes the first occurrence of the pattern

=> Step 3 : Observer design



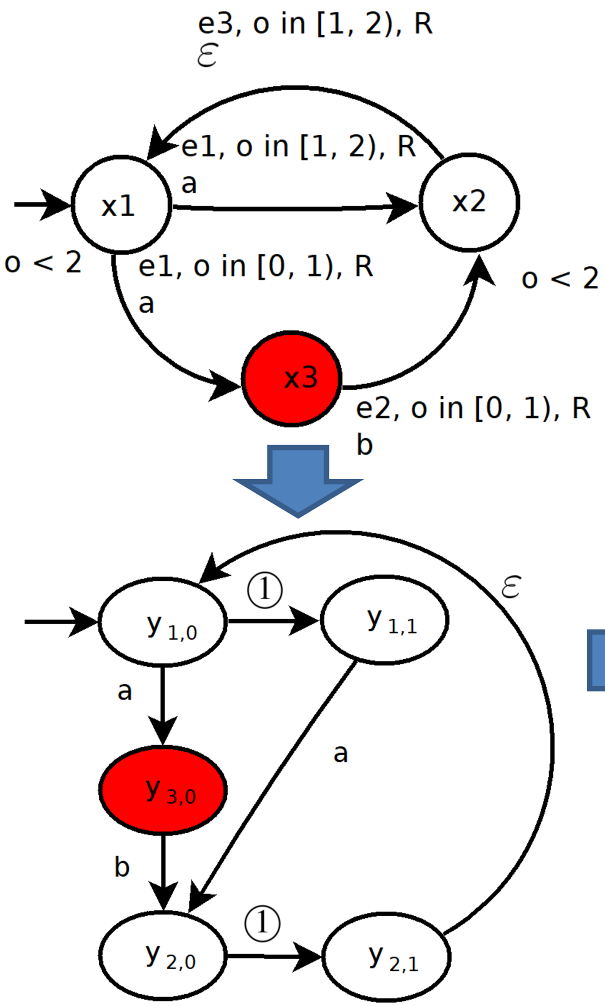


Observer

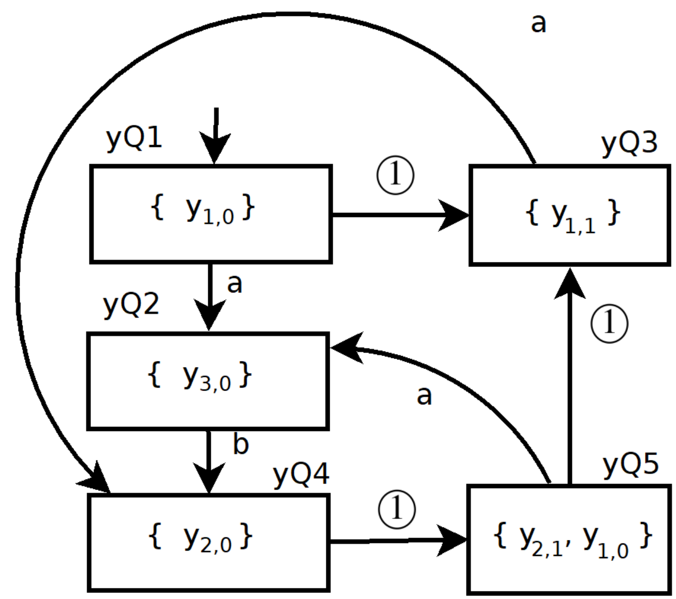
4.2 Opacity verification and enforcement

Transition	Event	Domain	P_4	P_5
(1,2)	e1	[1, 2)	a	a
(1,3)	e1	[0, 1)	a	ε
(3,2)	e2	[0, 1)	b	b
(2,1)	e3	[1, 2)	ε	ε

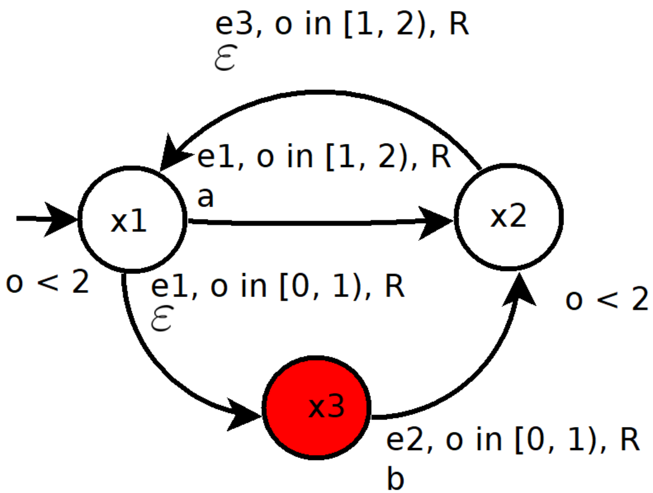
Secret = {x3}



P4 static labeling

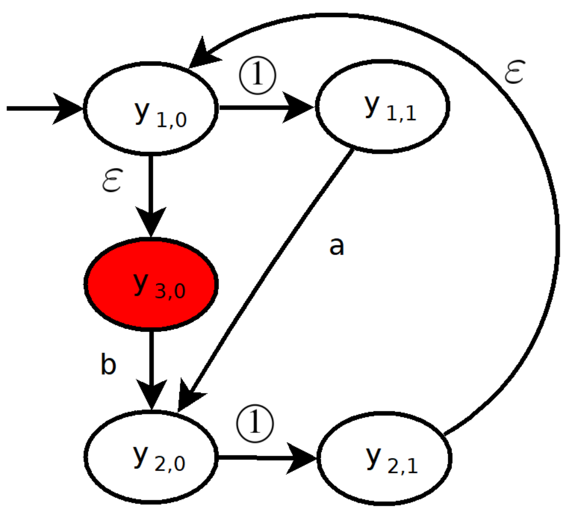


Zhang et al. 2021; Zhang et al. 2025; Hou et al. 2022

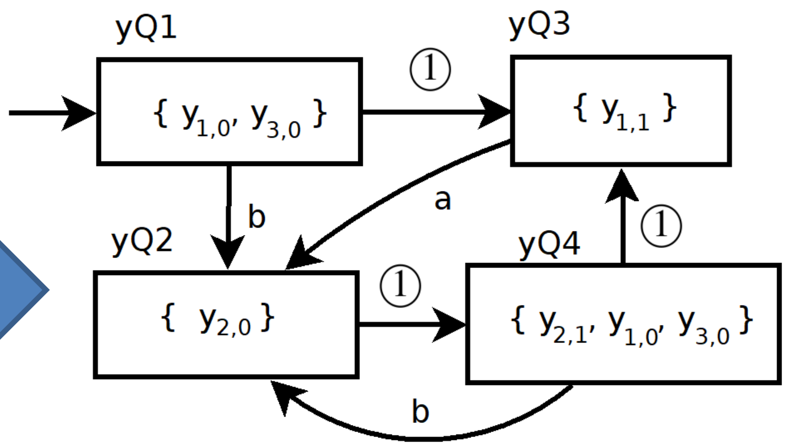


Transition	Event	Domain	P_4	P_5
(1,2)	e1	[1, 2)	a	a
(1,3)	e1	[0, 1)	a	ε
(3,2)	e2	[0, 1)	b	b
(2,1)	e3	[1, 2)	ε	ε

Secret = {x3}

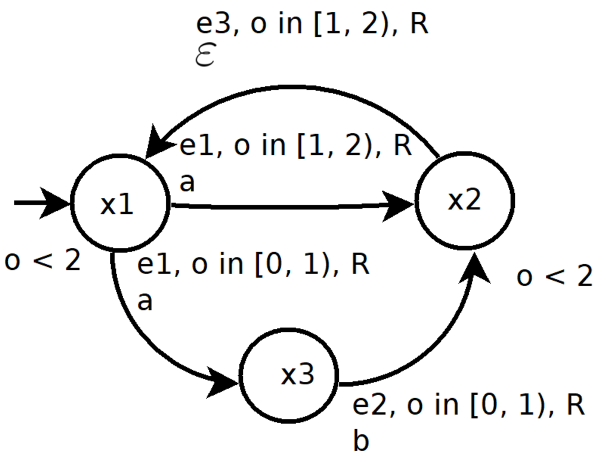


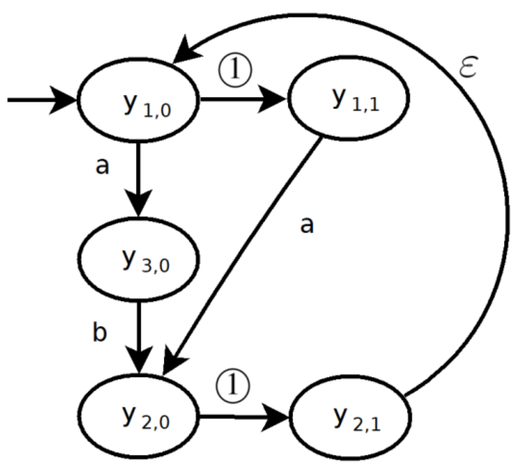
P5 dynamic deterministic labeling



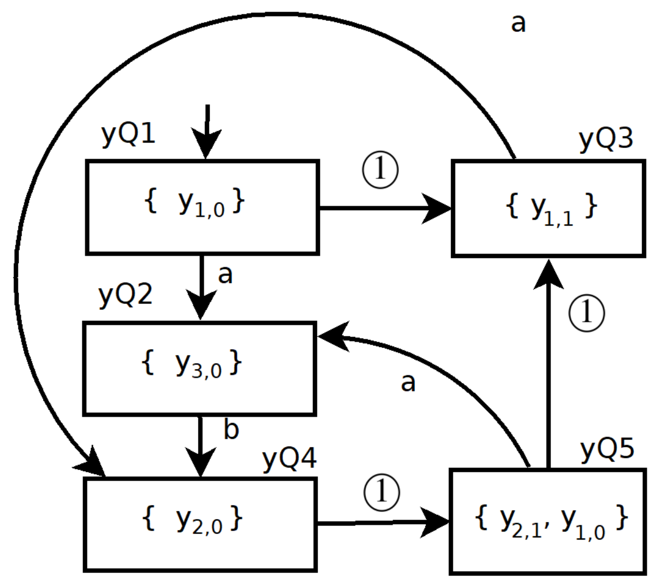
4.3 Detection of cyber attacks

sequence of observations	LATI	LCIA
Scenario 1	σ = (a, 1.2) (a, 3.5) σ’ = (a, 1.2) (a, 2.3)	σ_Y = ① a ① ① a
Scenario 2	σ = (a, 1.2) (a, 4.3) σ = (a, 1.2) (a, 3.1)	σ_Y = ① a ① ① ① a





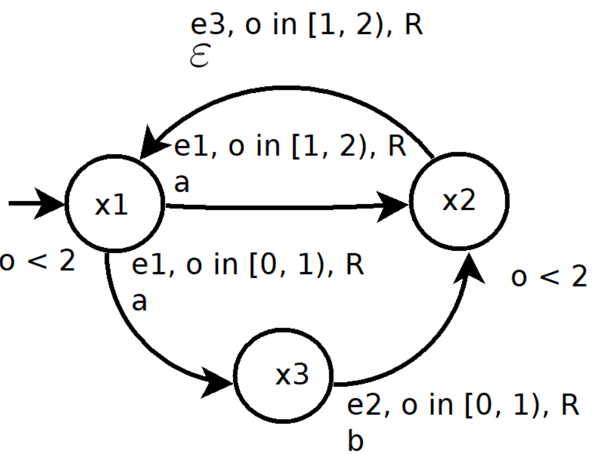
P4 static labeling



alarm

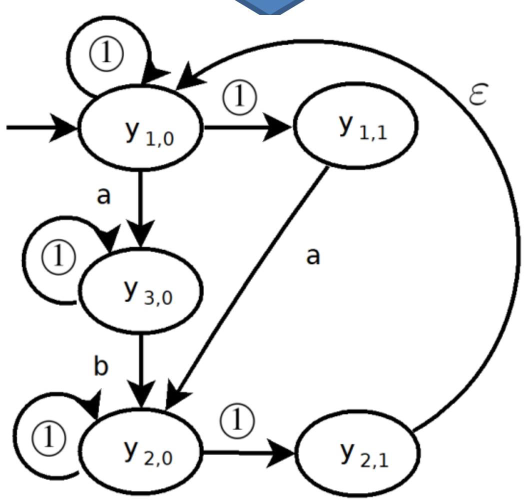
Gaouar, et al. 2025

4.3 Detection of cyber attacks : can we do better ?

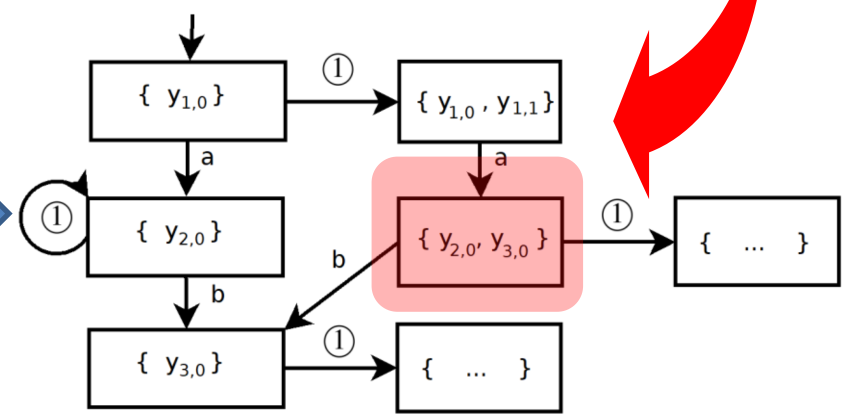


+ attacks that add delays

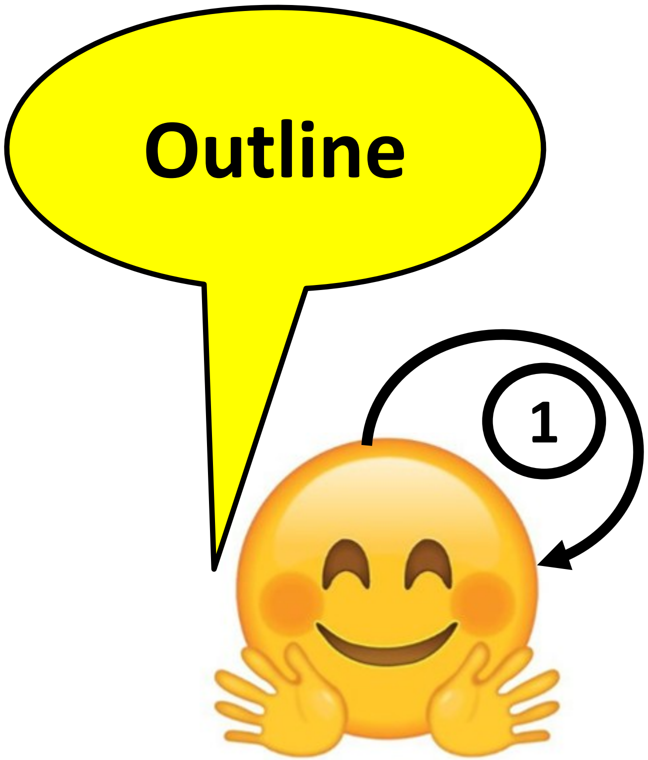
sequence of observations	LATI	LCIA
Scenario 3	σ = (a, 1.2) …	σ_Y = ① a



P4 labeling function



Gaouar, et al. 2025



1. **Introduction and motivation**

2. **Modeling timed discrete event systems with automata**
   - Timed automata
   - Tick automata
   - Automata with time intervals (ATI)
   - Clock Interval Automata (CIA)

3. **Observation mechanisms based on labeled CIA**
   - Static observation
   - Dynamic observation
   - Orwellian observation

4. **Application to cyber physical systems**
   - Fault diagnosis and diagnosability
   - Opacity verification
   - Attack detection

5. **Conclusion and perspectives**

What's next ?

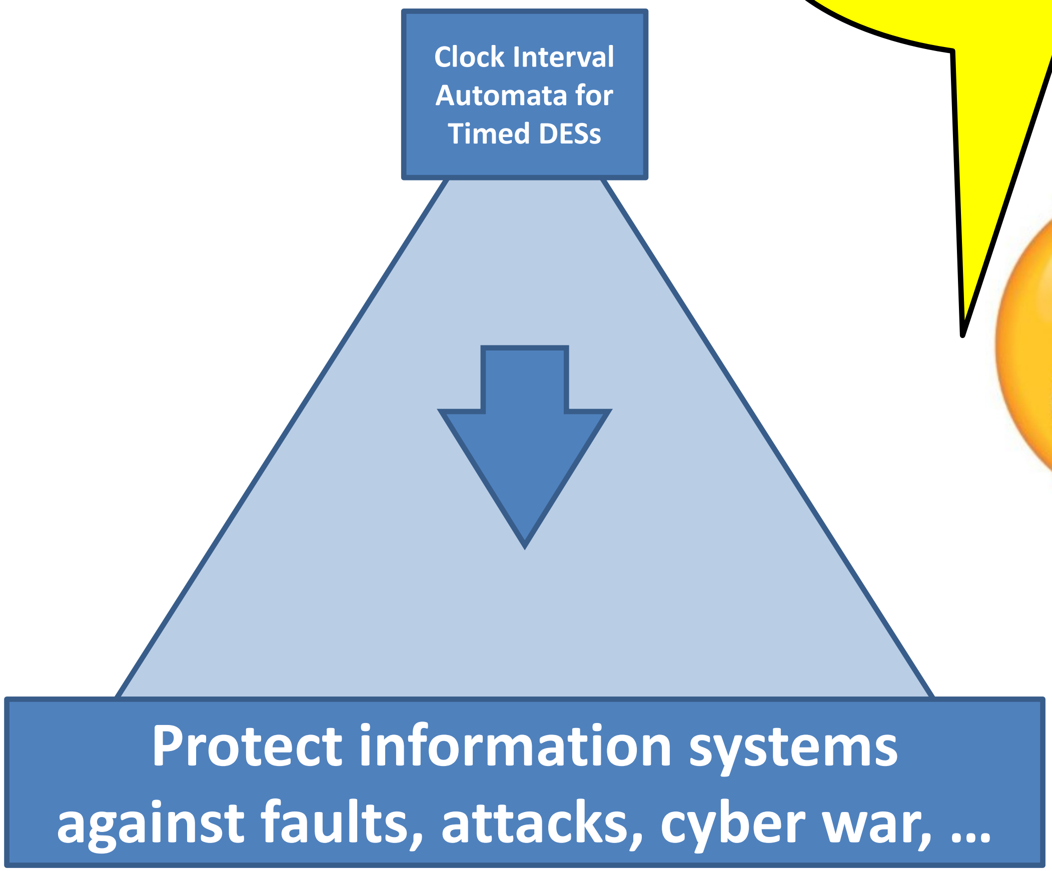
Clock unit defines the detection precision

…

and

the size

of the models



Thank you !!!

dimitri.lefebvre@univ-lehavre.fr

Special thanks to my colleagues :
Dr. Said Amari
Dr. Rabah Ammour
Dr. Omar Amri
Prof. Isabel Demongodin
Dr. Yifan Dong
Prof. Alessandro Giua
Dr. Chao Gao
Prof. Christoforos Hadjicostis
Prof. Jan Komanda
Dr. Edouard Leclercq
Dr. Jun Li
Prof. Zhiwu Li
Dr. Ye Liang
Prof. Gaiyun Liu
Prof. Olivier Roux
Prof. Carla Seatzu
Dr. Phong Tran
Dr. Ziliang Zhong
…. and many others…..

Alur et al., 1994 : https://www.sciencedirect.com/science/article/pii/0304397594900108
Brandin et al., 1994: https://ieeexplore.ieee.org/document/272327
Gao et al., 2025 : https://ieeexplore.ieee.org/document/10745754
Gaouar, et al. 2025 : https://ieeexplore.ieee.org/document/11018525
Hou et al. 2022 : https://www.sciencedirect.com/science/article/pii/S0005109822000838
Lefebvre et al. 2023: https://www.sciencedirect.com/science/article/pii/S0005109823002005
Li et al. 2022 : https://ieeexplore.ieee.org/document/9372781
Mao et al., 2024 : https://ieeexplore.ieee.org/document/10468632
Mullins et al., 2014: https://www.sciencedirect.com/science/article/pii/S1474667015374255
Shu et al., 2010 : https://www.sciencedirect.com/science/article/pii/S0167691109001340
Wang et al. 2010 : https://www.sciencedirect.com/science/article/pii/S0005109810001615
Xu et al. 2010 : https://ieeexplore.ieee.org/document/5491094
Xu et al. 2010 : https://ieeexplore.ieee.org/abstract/document/5411743
Yin et al 2019 : https://www.sciencedirect.com/science/article/pii/S000510981930161X
Zhang et al. 2021 : https://www.sciencedirect.com/science/article/pii/S0020025521004072
Zhang et al. 2025 : https://www.mdpi.com/2227-7390/13/10/1568

Y. Liang, D. Lefebvre, Z. Li, Silent closure-based pair verifier for fault pattern diagnosis of discrete event systems, IET Control Theory & Applications Journal, vol. 18, pp. 603–613, 2024.

J. Li, D. Lefebvre C. N. Hadjicostis, Z. Li, State estimation for constant-time labeled automata under dense time, Automatica, vol. 170, pp. 111874, 2024.

J. Zhou, D. Lefebvre, Z. Li, An extremum timed extended reachability graph for temporal analysis of time Petri nets. Discrete Event Dyn Syst, 2024.

J. Li, D. Lefebvre, C. N. Hadjicostis and Z. Li, Verification of state-based timed opacity for constant-time labeled automata, in IEEE Transactions on Automatic Control, vol. 70, no.1, pp. 503-509, 2025.

G. Gao, D. Lefebvre, C. Seatzu Z. Li, A. Giua, State estimation of timed automata under partial observation, IEEE Trans. Automatic Control, vol. 70, no. 3, pp. 1981-1987, March 2025.

Y. Liang, D. Lefebvre, Z. Li, Polynomial-Time Verification of Pattern Diagnosability for timed discrete event systems, Information Sciences 70, 121997, 2025.

M. Gaouar, R. Ammour, I. Demongodin, D. Lefebvre, Current state estimation of Timed Labeled Synchronized Petri Nets, IEEE LCSS, 2025.

J. Komenda, D. Lefebvre, O. Roux, On clock interval automata for a class of time PNs, accepted JDEDS, 2025.