THALES

Applying parametric model-checking techniques for reusing real-time critical systems

B. Parquier[1], L. Rioux[1], R. Henia[1], R. Soulat[1]

O. H. Roux[2], D. Lime[2]

Étienne André[3]

[1] THALES Research & Technology

[2] IRCCyN

[3] Université Paris 13

Outline

1. Thales group
2. Objective
3. Case-study
4. Tools presentation:
    1. Romeo
    2. Imitator
5. Evaluation results
6. Conclusion

THALES group

Employees

62,000

(workforce under management at 31 Dec. 2015)

Global presence

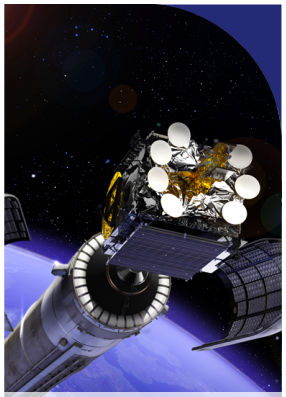
56 countries

Self-funded R&D* 2015

707 million euros

* Does not include therefore R&D undertaken with external funding.

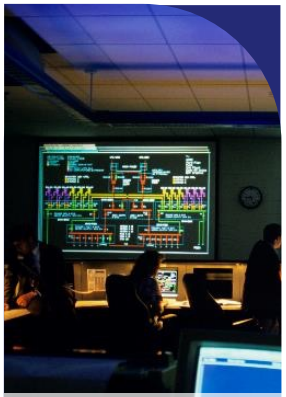
AEROSPACE



SPACE

GROUND TRANSPORTATION

DEFENCE



SECURITY

DUAL MARKETS

Military & Civil

THALES group

N°1 worldwide


Payloads
for telecom satellites


Air Traffic Management


Sonars


Security for interbank
transactions

N°2 worldwide

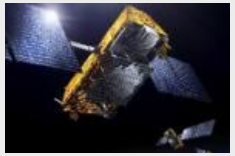

Rail signalling systems


In-flight entertainment
and connectivity


Military tactical
radiocommunications

N°3 worldwide


Commercial avionics


Civil satellites


Military surface radars

€14 billion
in revenues

Motivation & objective

Reuse is essential in industrial system engineering to save time and reduce development costs

- Requires adapting the existing product to meet the new performance requirements of the customers

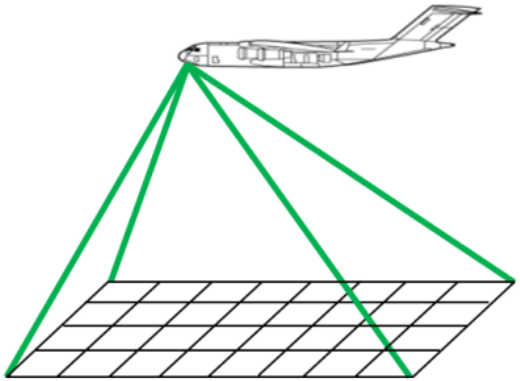
Current reuse process is poorly supported by methods & tools

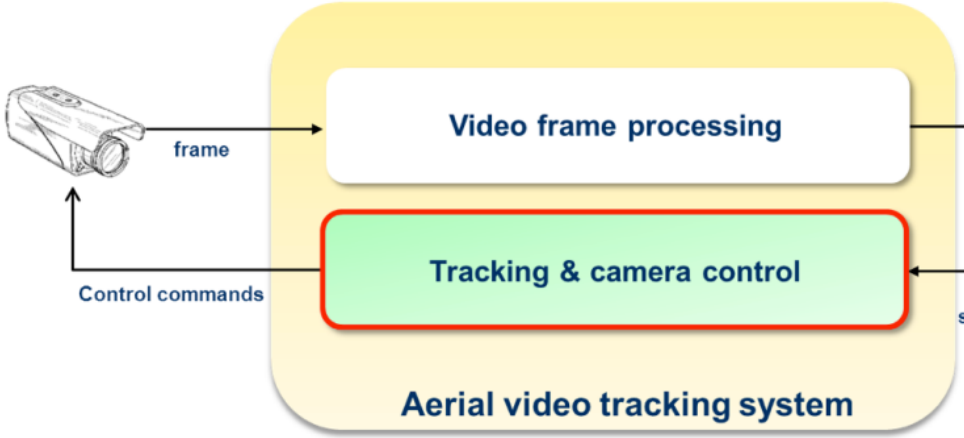
- experts verify manually if the existing product can be adapted to be reused

Objective:

Provide the architect with a reliable method/tool to calculate the performance parameters ranges for which the system behaves correctly

Thales case-study[1]: aerial video tracking system

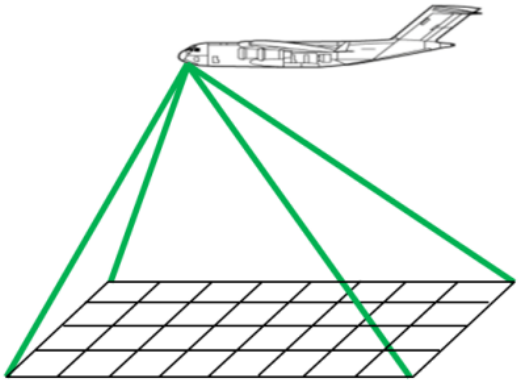


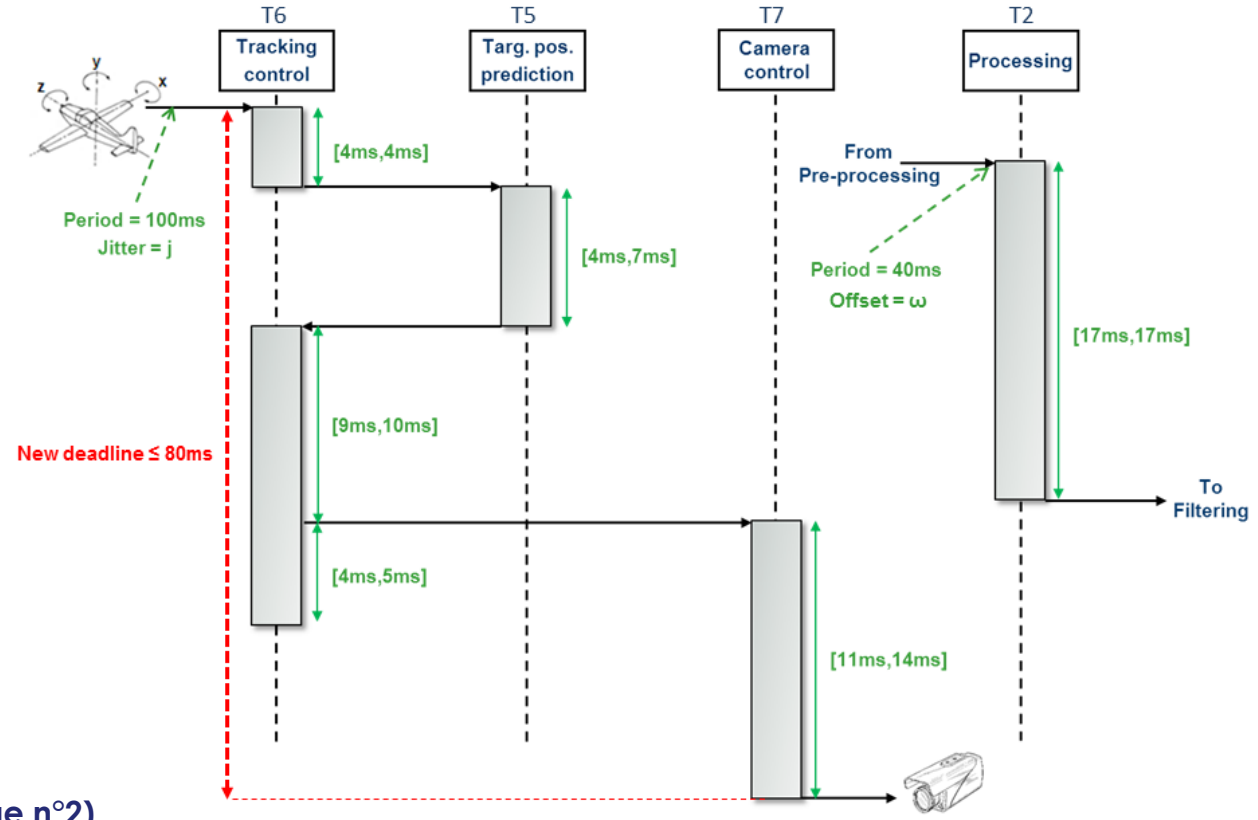


[1] Published in FMTV 2014 (challenge n°2)

Thales case-study[1]: aerial video tracking system

Uniprocessor system
Preemptive scheduling
Priorities : T2 > T6 > T5 > T7





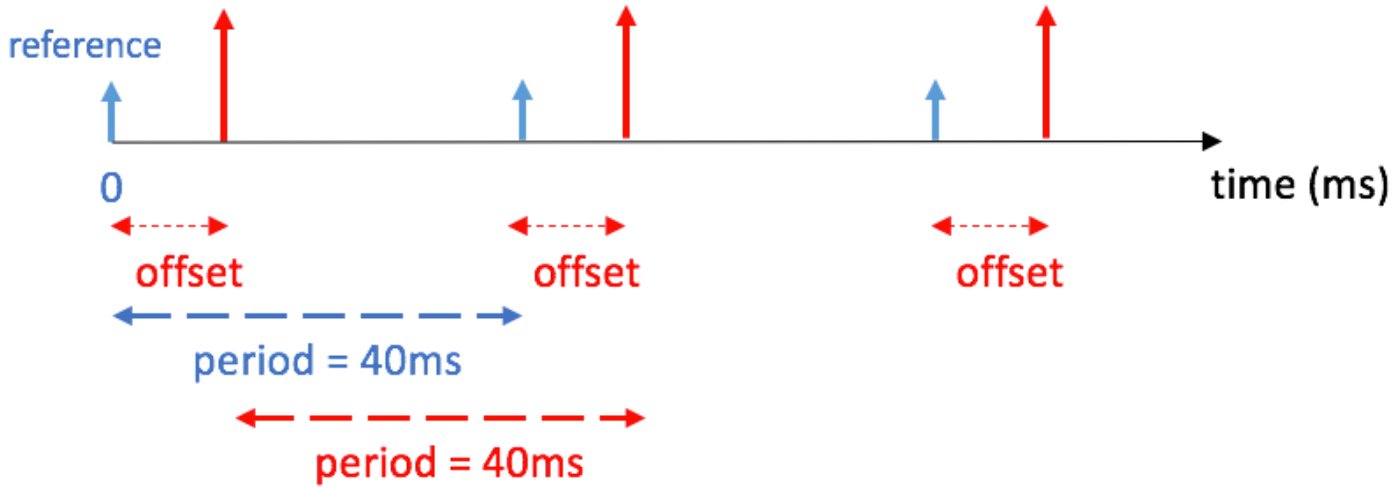
[1] **Published in FMTV 2014 (challenge n°2)**

THALES

Thales case-study

- Period
- Jitter
- Offset

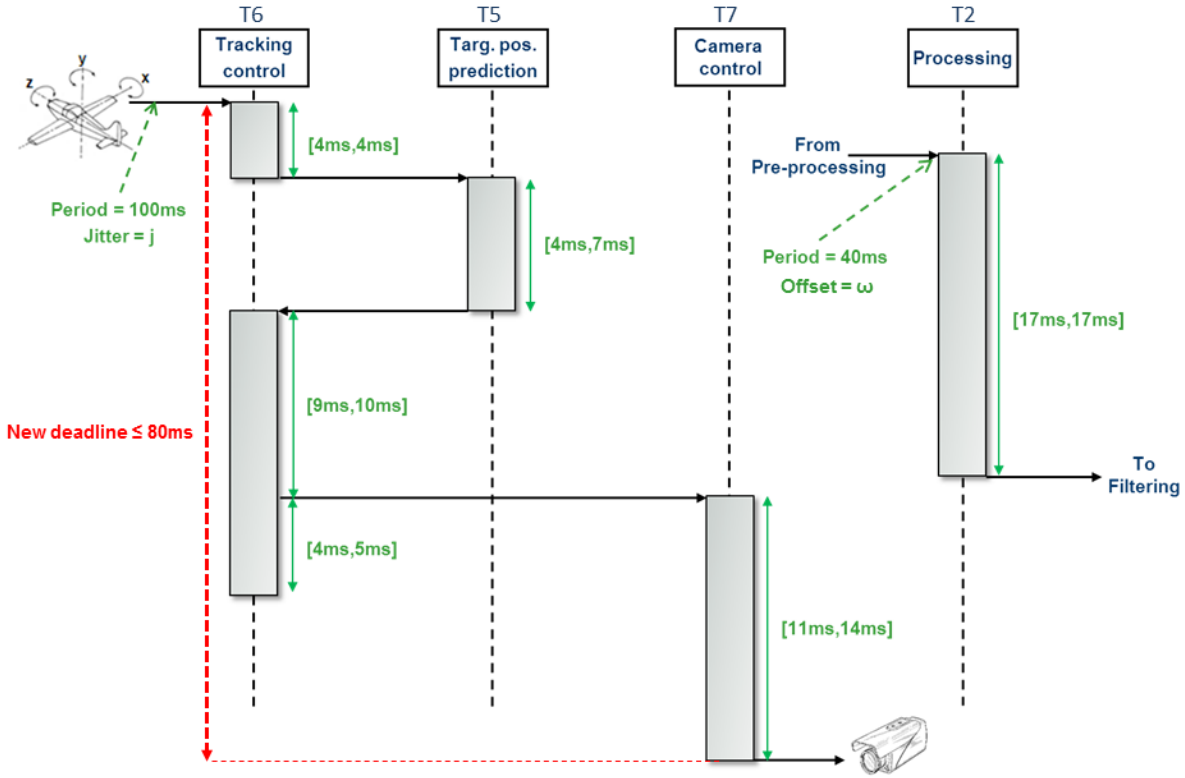
Stimulus



Thales case-study

- Period
- Jitter
- Offset

} Stimulus

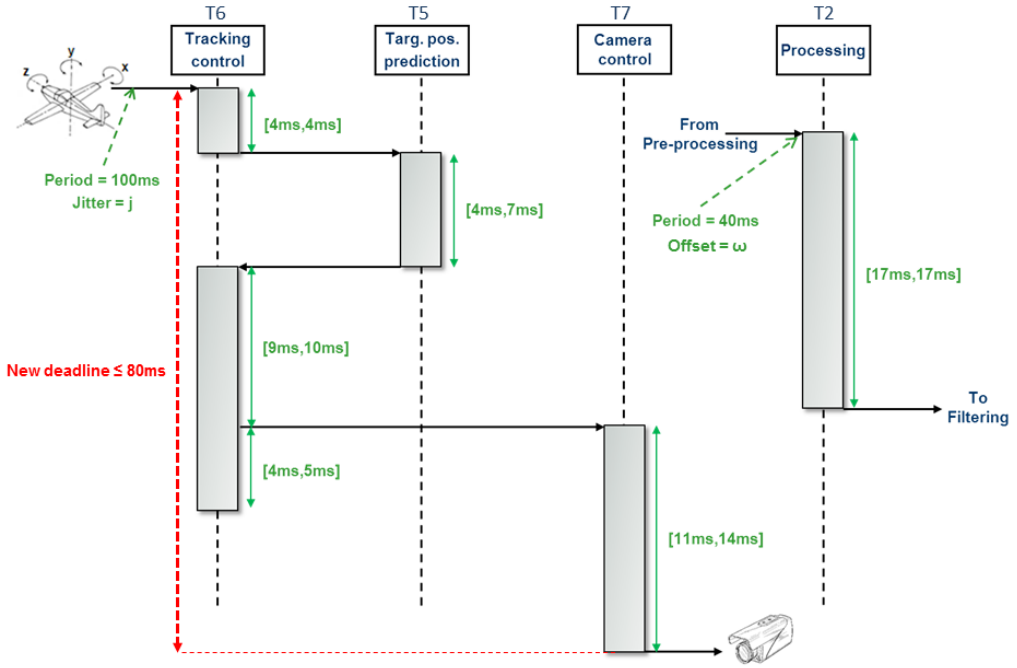


Thales case-study

« The latency between the activation of T6 and the termination of T7 must not exceed 80ms »

Jitter<=30ms, offset\in [0,40]ms

$$\begin{cases} jitter \leq 30ms \\ offset \in [0,40[ms \end{cases}$$



Identified verification tools

- Model-based verification tools (model checker)
- Parametric models

ROMEO

IMITATOR

ROMEO

Real-time modeling

- http://romeo.rts-software.org/
- Version 3.2.3

Parametric time Petri net

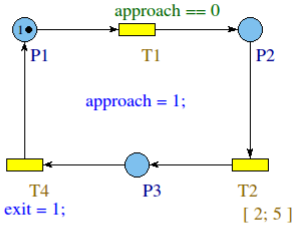
ROMEO

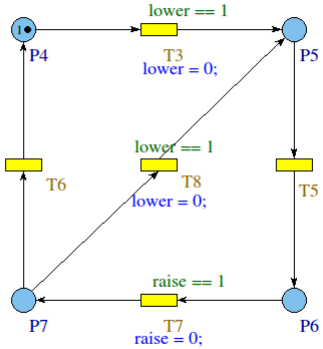
Real-time modeling

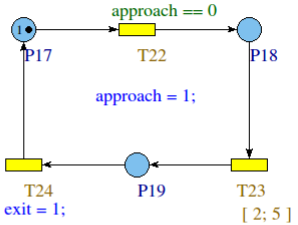
- http://romeo.rts-software.org/
- Version 3.2.3

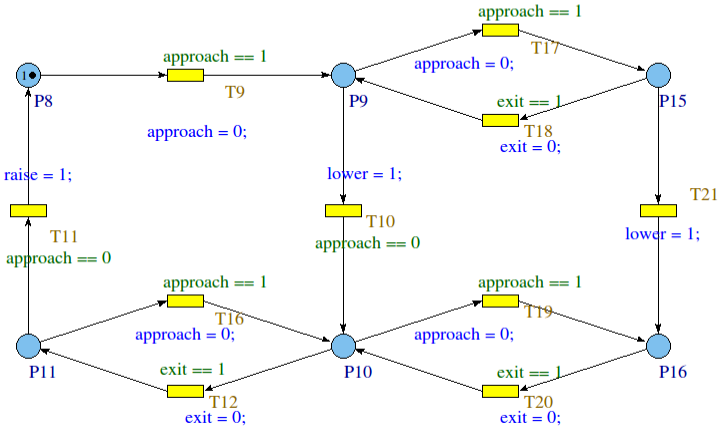
Parametric time Petri net

Institut de Recherche en Communications et Cybernétique de Nantes









IMITATOR

Real-time modeling

- http://www.imitator.fr/
- Version 2.7.3

Parametric timed automata

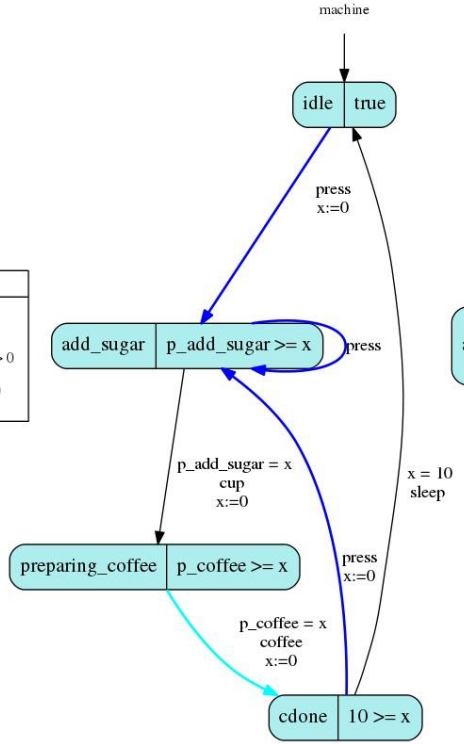
IMITATOR

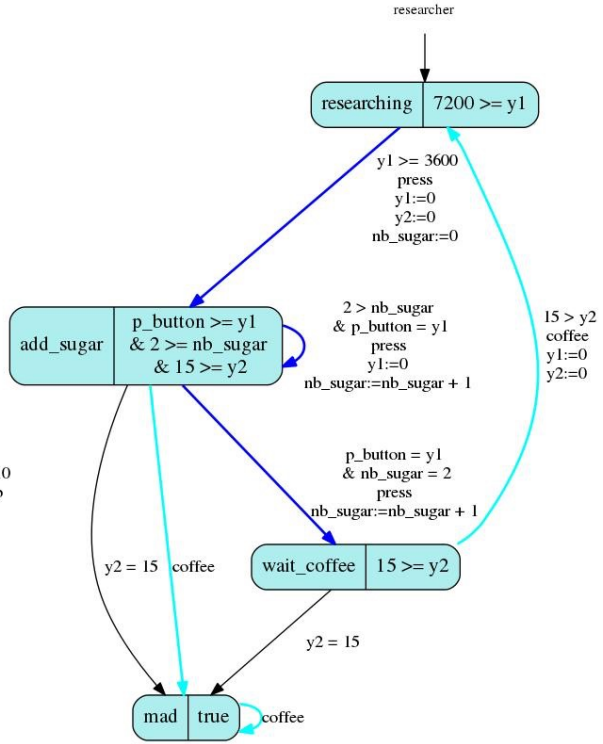
Real-time modeling

- http://www.imitator.fr/
- Version 2.7.3

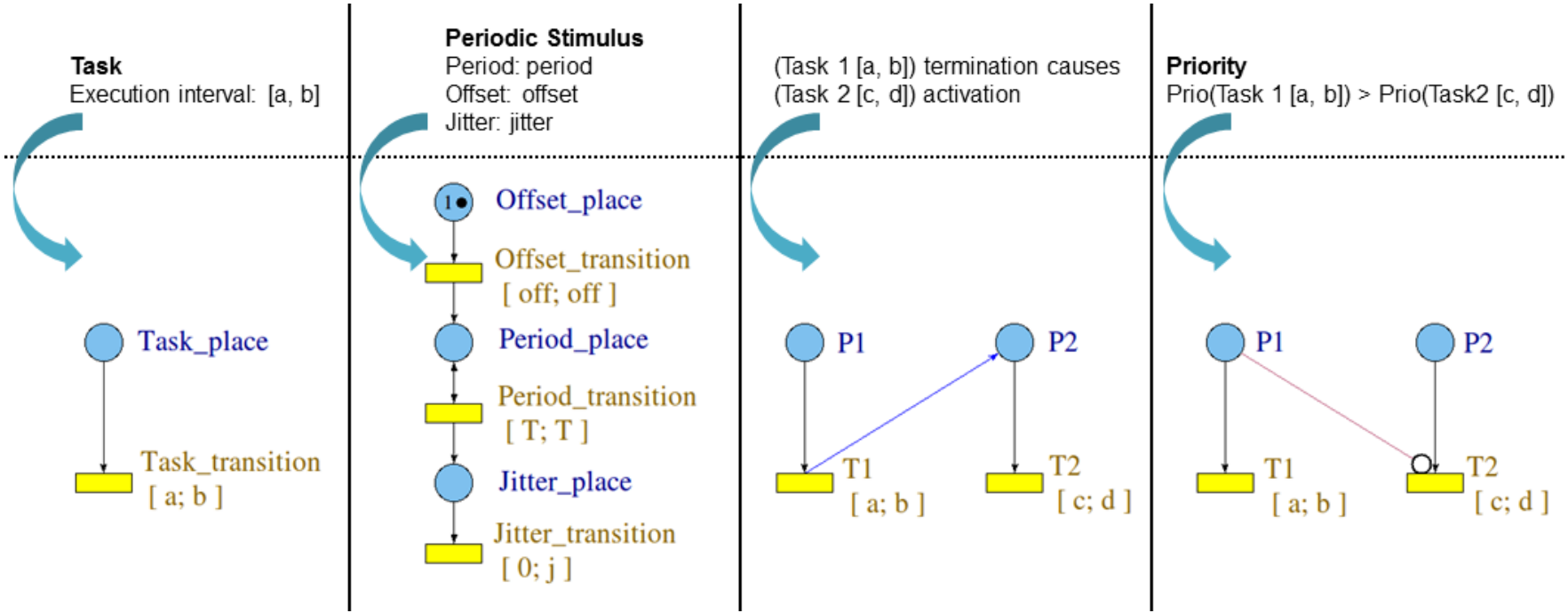
Parametric timed automata

Clocks	Parameters	Discrete	Initial
x y1 y2	p_add_sugar p_coffee p_button	nb_sugar	p_button > 0 & y1 >= 0 & y2 >= 0 & p_add_sugar > 0 & 7200 >= y1 & p_coffee > 0 & x = 0

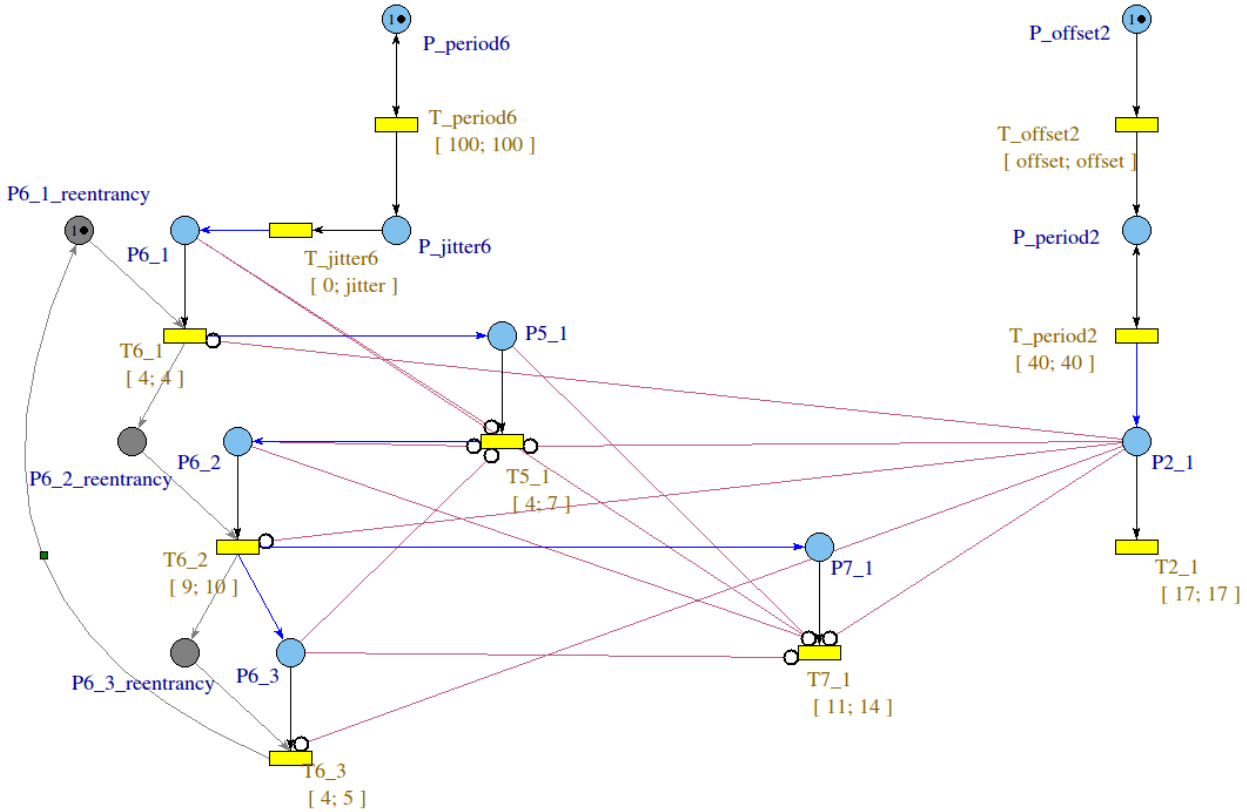




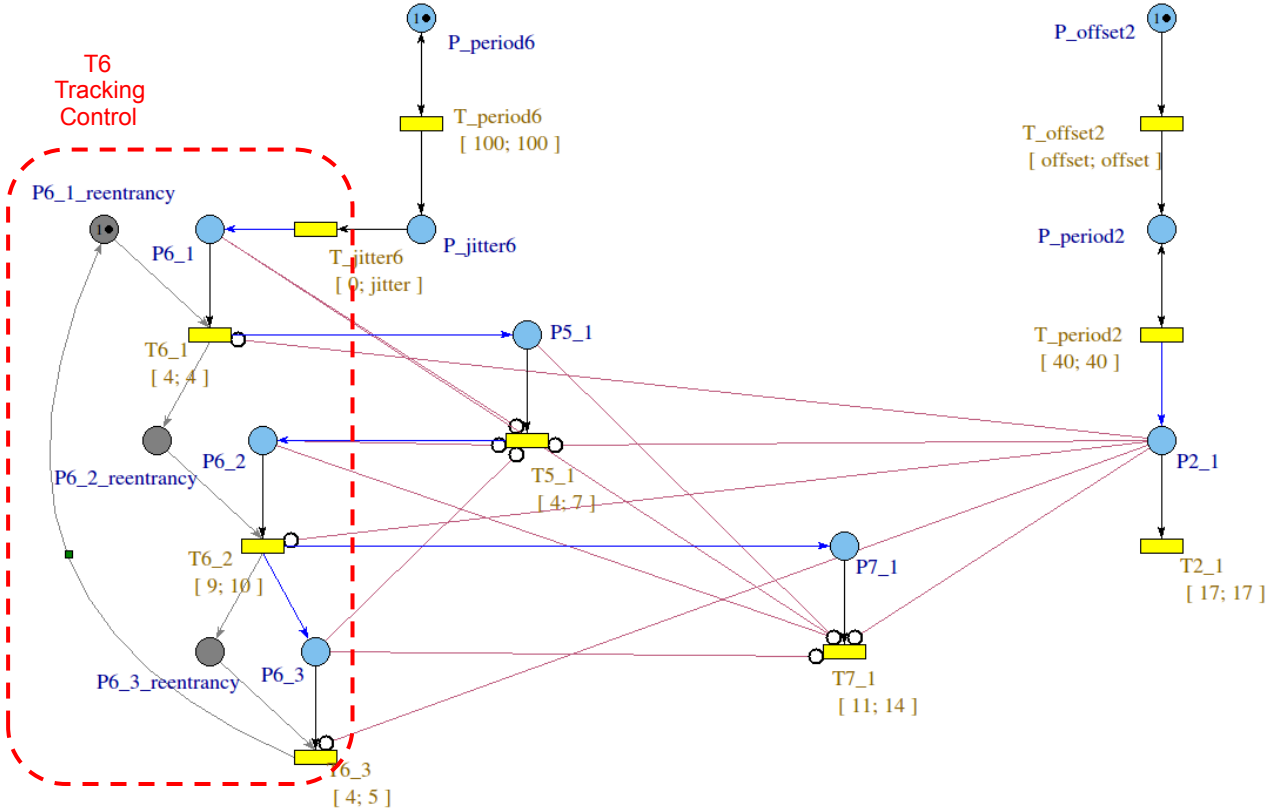
Thales case-study : modeling in ROMEO



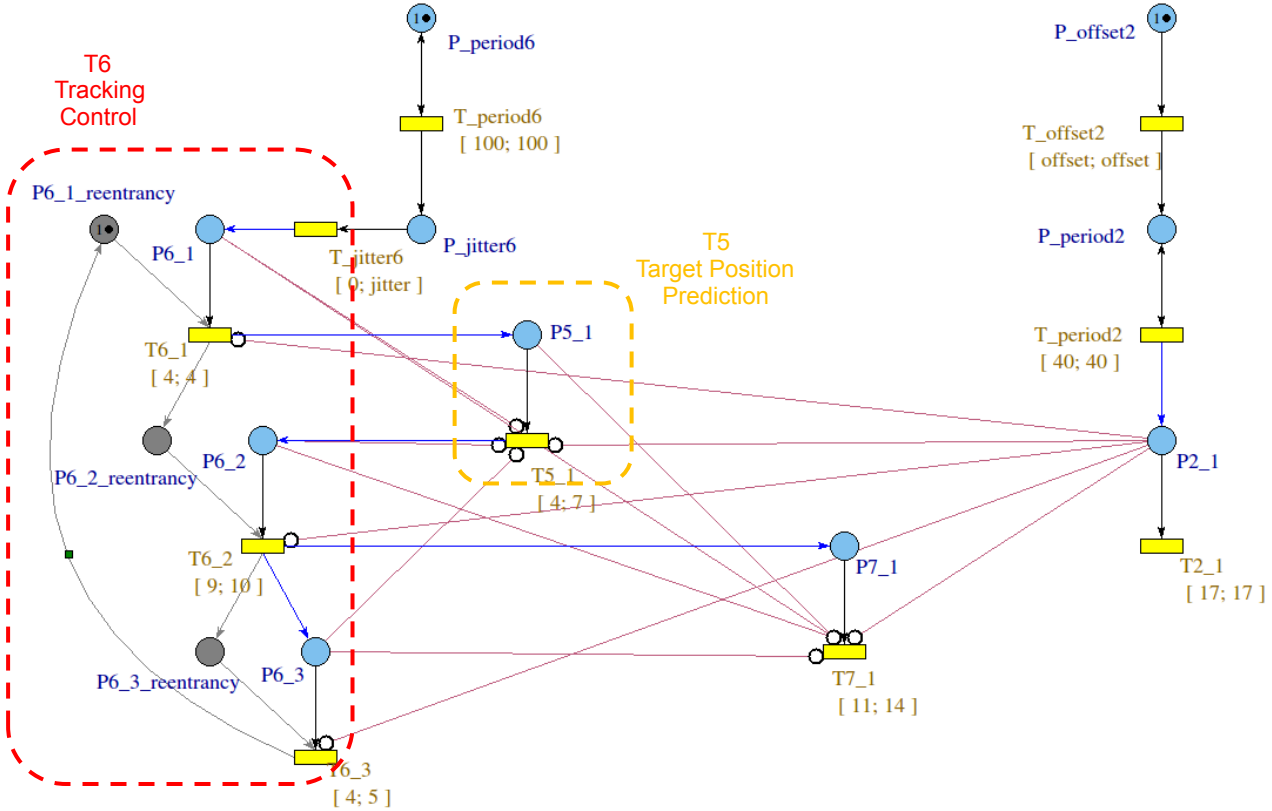
Thales case-study : modeling in ROMEO



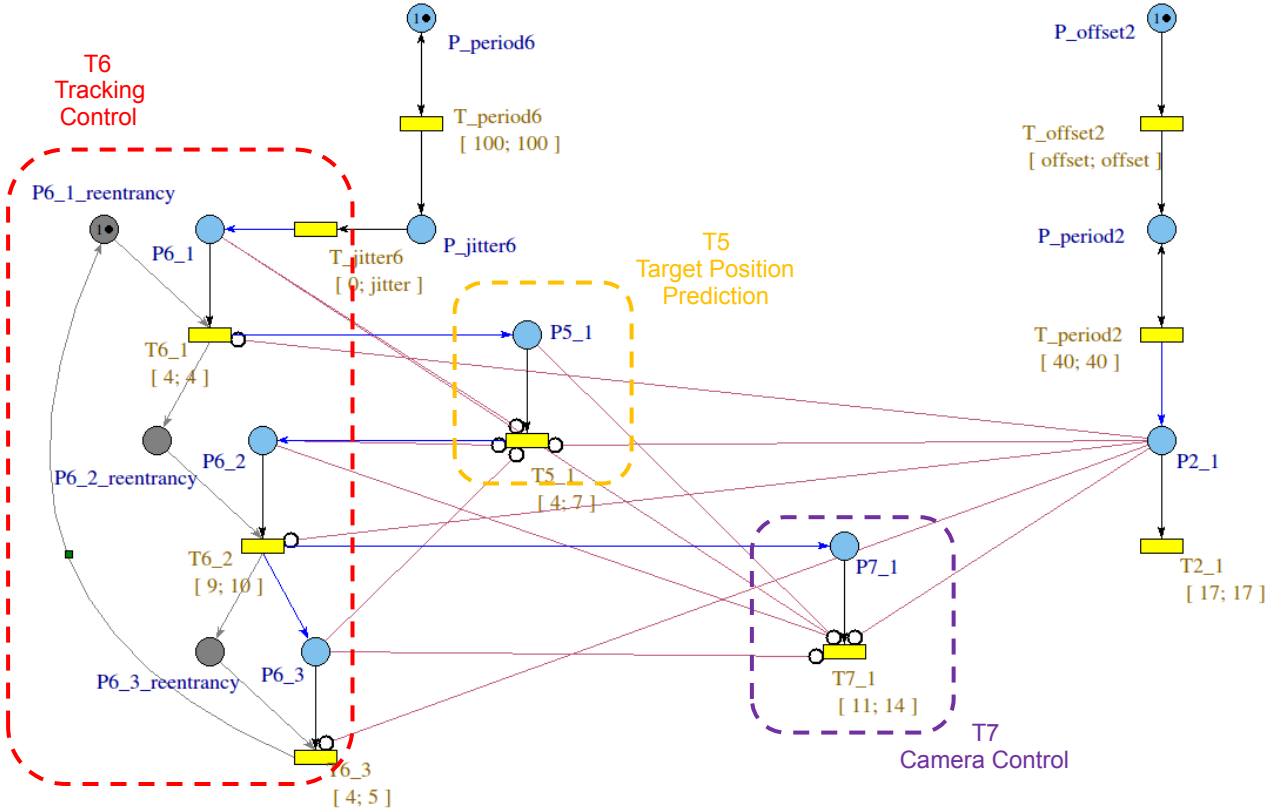
Thales case-study : modeling in ROMEO



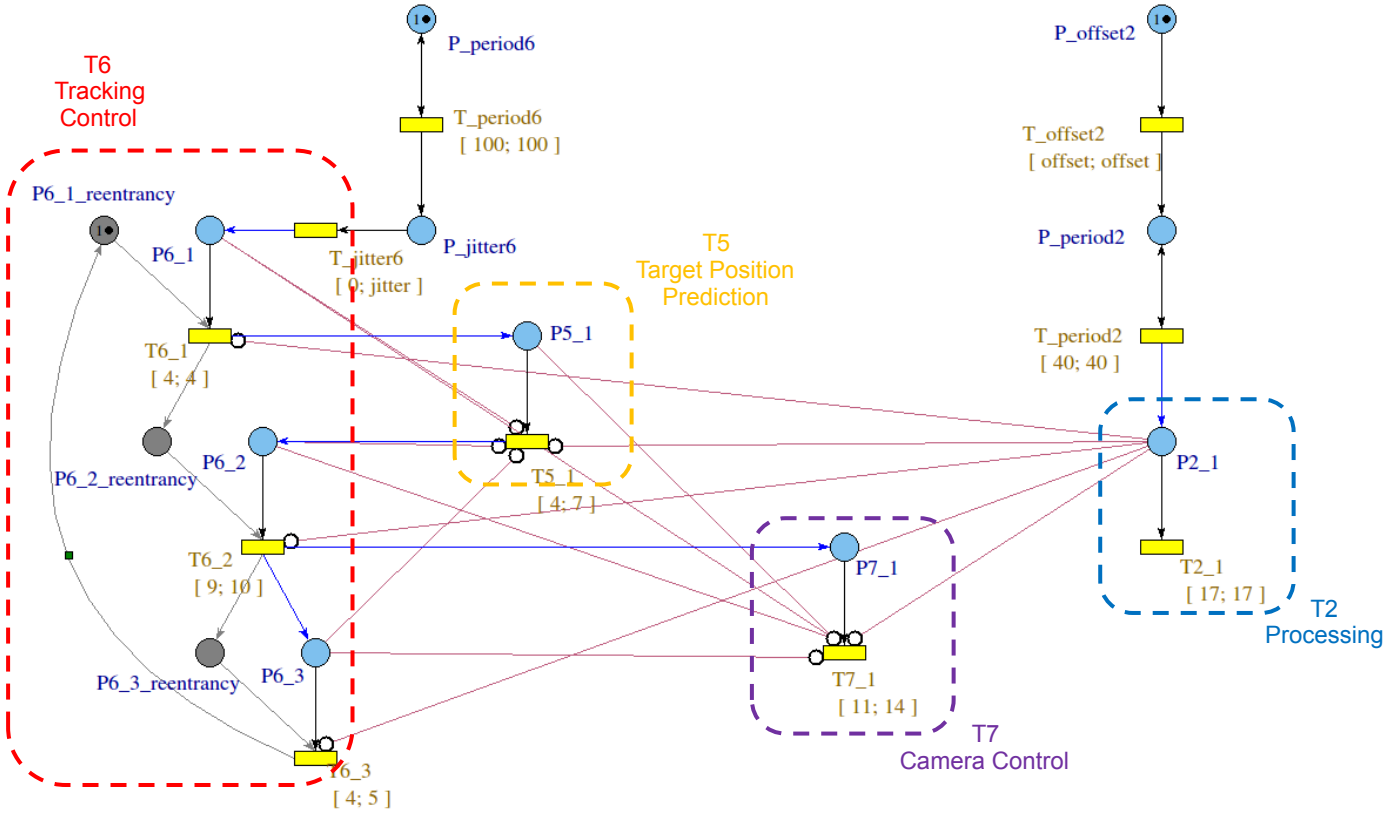
Thales case-study : modeling in ROMEO



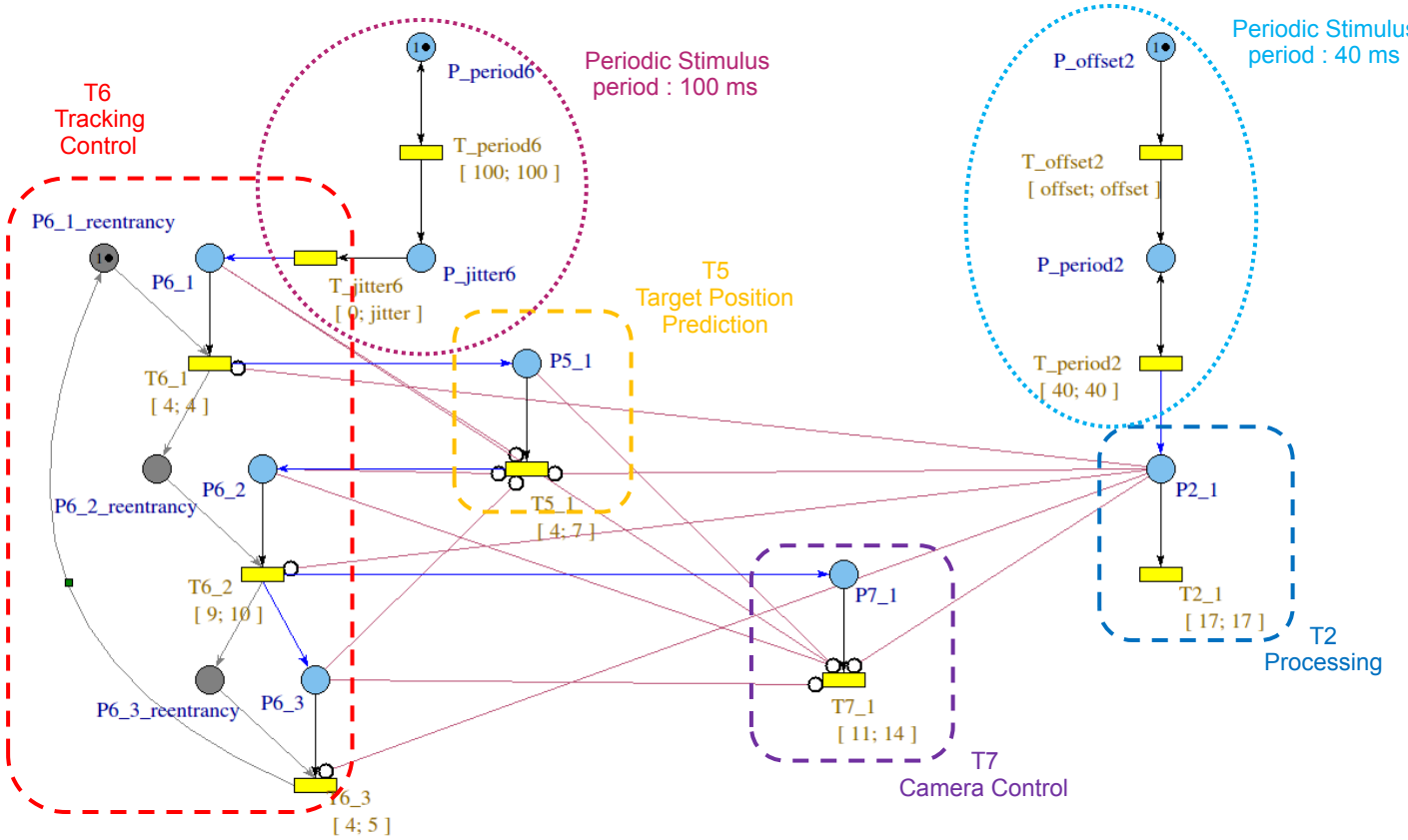
Thales case-study : modeling in ROMEO



Thales case-study : modeling in ROMEO

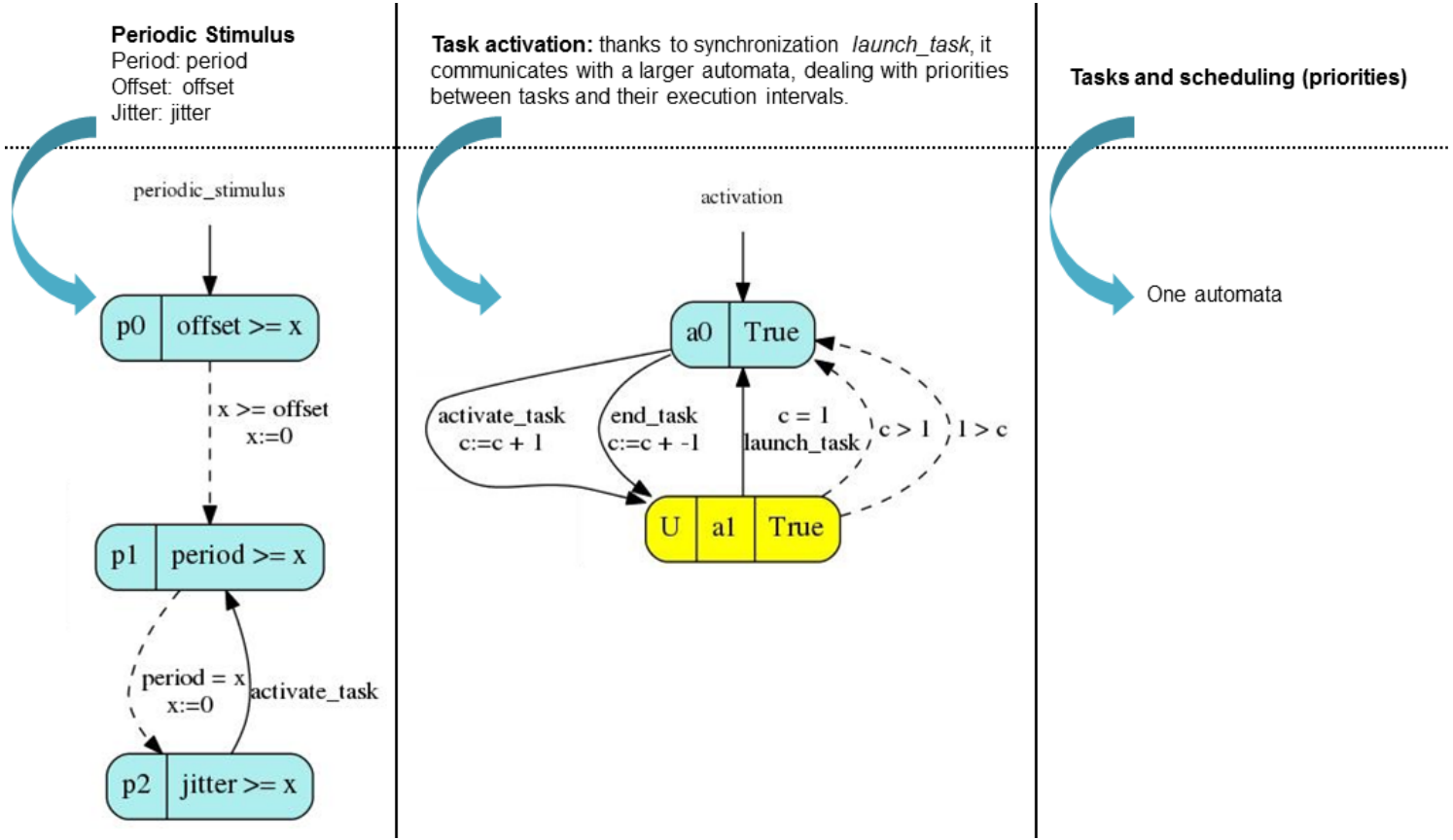


Thales case-study : modeling in ROMEO

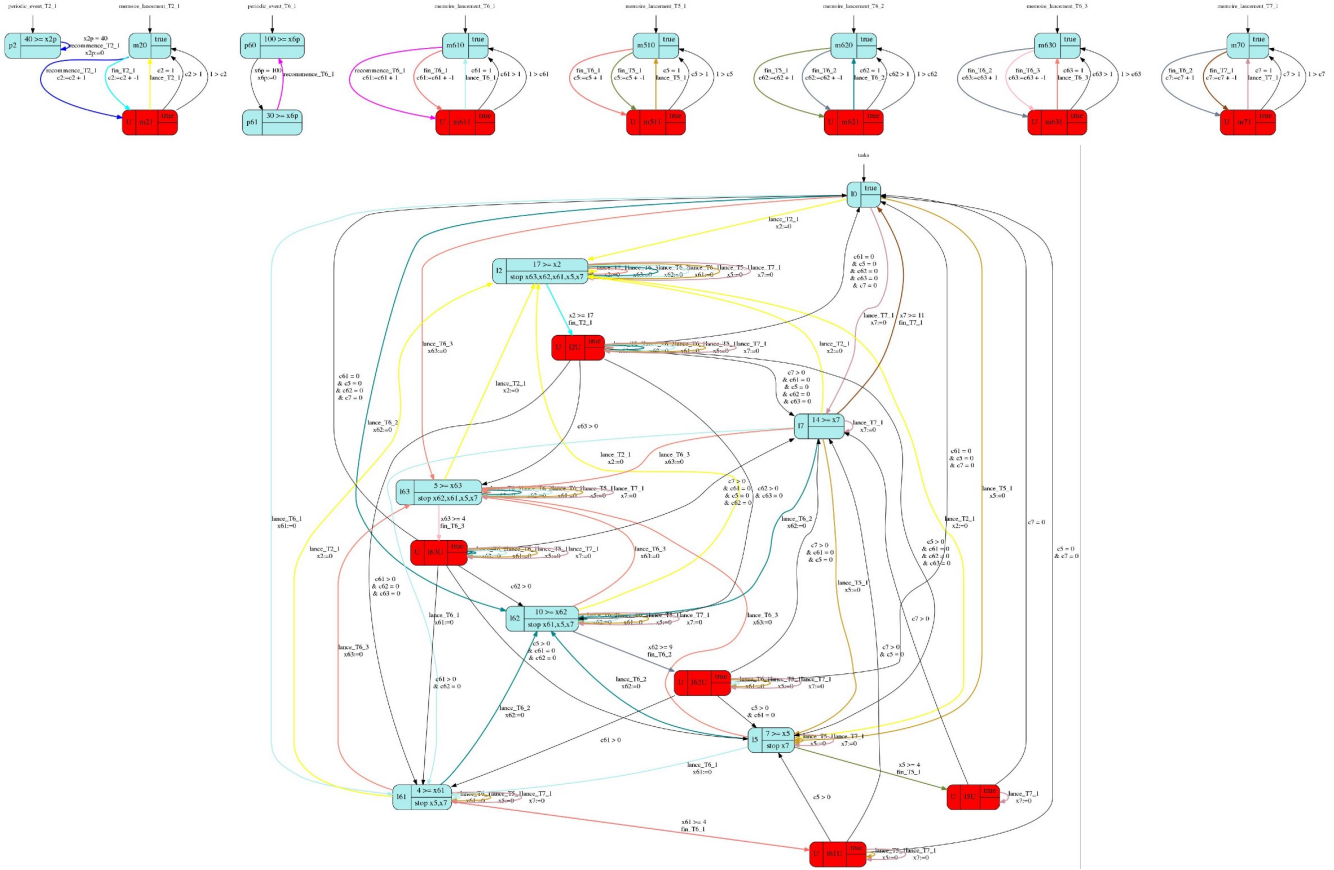


THALES

Thales case-study : modeling in IMITATOR

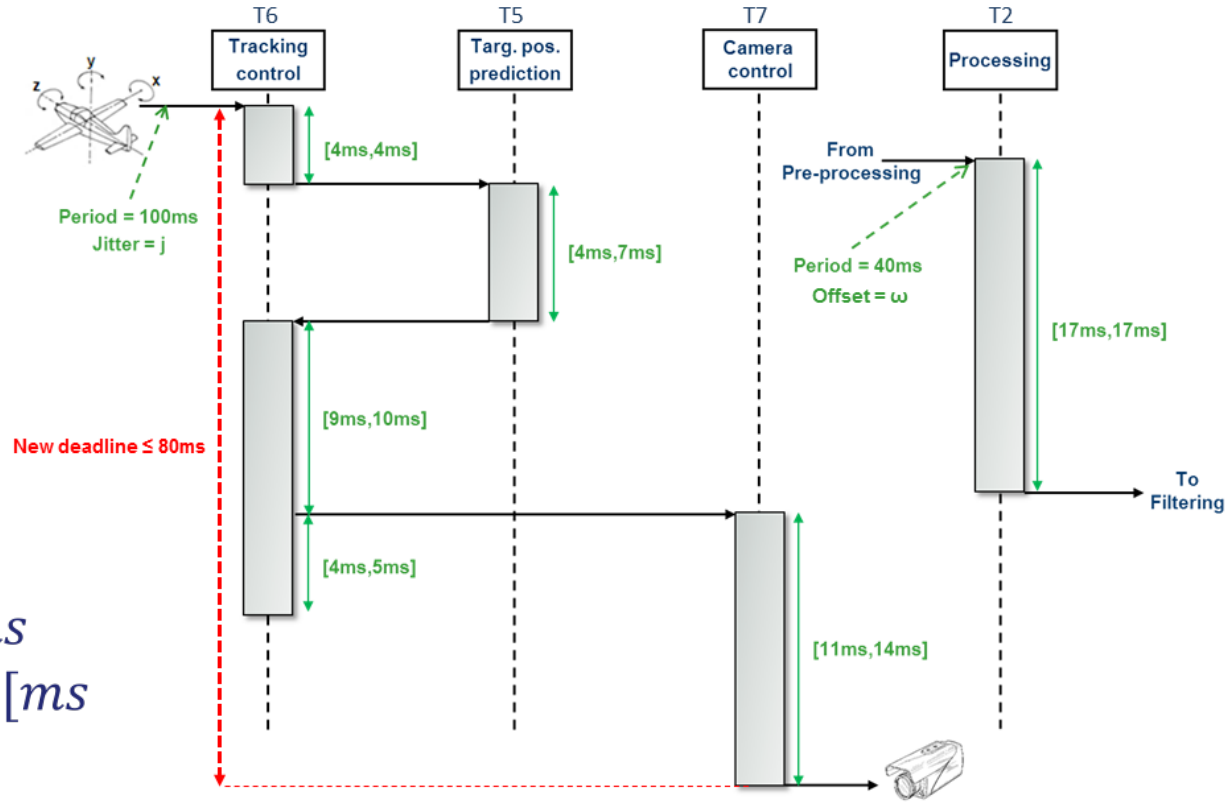


Thales case-study : modeling in IMITATOR



THALES

Thales case-study



$$\begin{cases} jitter \leq 30ms \\ offset \in [0, 40[ms \end{cases}$$

Thales case-study : results

Worst-case

$$\{ \blacksquare jitter = 30ms offset = 0ms$$

Thales case-study : results

Worst-case

$\{ \blacksquare jitter=30ms offset=0ms$

Worst-case response time		
Tool	ROMEO	IMITATOR
(worst time)	**117ms**	
Memory	16.2 Mo	342.3 Mo
Runtime	0.6 s	34.3 s
Performance	1	57

Thales case-study : results

Worst-case

$$\{ \blacksquare jitter=30ms offset=0ms$$

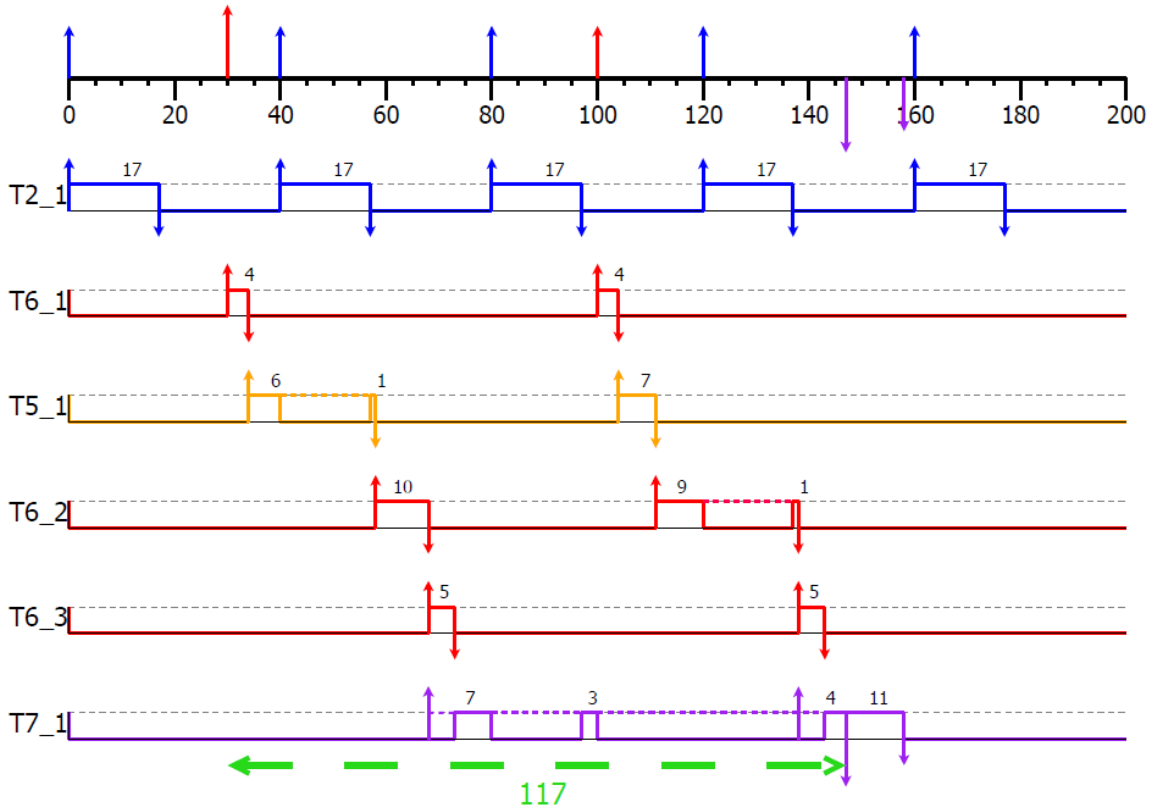
Worst-case response time		
Tool	ROMEO	IMITATOR
(worst time)	**117ms**	
Memory	16.2 Mo	342.3 Mo
Runtime	0.6 s	34.3 s
Performance	1	57

117ms > 80ms

Thales case-study : results

Worst-case

$\{\blacksquare jitter=30ms offset=0ms$



THALES

Thales case-study : results

Parametric offset

$$\{\blacksquare jitter = 30ms \; offset \in [0, 40[ms$$

Thales case-study : results

Parametric offset

$\{ \blacksquare jitter = 30ms offset \in [0, 40[ms$

Worst-case response time		
Tool	ROMEO	IMITATOR
	false	
Memory	64.0 Mo	1816 Mo
Runtime	3.3s	3m35s
Performance	1	65

Thales case-study : results

Parametric offset

$\{ \blacksquare jitter = 30ms offset \in [0, 40[ms$

Worst-case response time		
Tool	ROMEO	IMITATOR
	false	
Memory	64.0 Mo	1816 Mo
Runtime	3.3s	3m35s
Performance	1	65

No solution found

Thales case-study : results

Parametric jitter

$$\begin{cases} jitter \in [0, 30]ms \\ offset = 0ms \end{cases}$$

Thales case-study : results

Parametric jitter

$$\begin{cases} jitter \in [0, 30]ms \\ offset = 0ms \end{cases}$$

Worst-case response time		
Tool	ROMEO	IMITATOR
	true	
jitter (ms)	**[0, 26[**	
Memory	9.6 Mo	267.8 Mo
Runtime	0.5s	38.1s
Performance	1	76

Thales case-study : results

Parametric offset & jitter

$$\{\blacksquare jitter \in [0, 30] ms \; offset \in [0, 40[ms$$

Thales case-study : results

Parametric offset & jitter

$\{ \blacksquare jitter \in [0, 30] ms \; offset \in [0, 40[ms$

Worst-case response time			
	true	true	true
offset (ms)	[0, 6[	[0, 26[	[0, 40[
jitter (ms)	[0, 29[	[0, 29[	[0, 26[
Condition			
ROMEO	Memory : 117.3 Mo – Runtime : 7.5s		
IMITATOR	Memory : 2017 Mo – Runtime : 6m36s		

Selected tool after evaluation

Results validated based on additional examples

ROMEO
IMITATOR

Conclusions

- **Parametric model-checking is a very promising approach to adapt existing design architectures to match new requirements**
  - Garanteed upper bound calculation of response times
  - Reliable calculation of parameter ranges fo which the system behaves correctly
- **The applicability of the model-checking approach in the industrial context requires further investigations (higher system complexity, scalability, etc)**