FROM RESEARCH TO INDUSTRY

cea tech

Towards Correct Transformation: From High-Level Models to Time-Triggered Implementations

H. GUESMI[3], B. BEN HEDIA[1], S. BLIUDZE[2], M. JAN[1] and S. BENSALEM[3]

[1]CEA, LIST, Embedded Real Time Systems Laboratory, **91191 Gif-sur-Yvette, France**
[2] EPFL IC IINFCOM RiSD, Station 14, **1015 Lausanne, Switzerland**
[3] Verimag, Université Joseph Fourrier, **38610 Gieres, France**

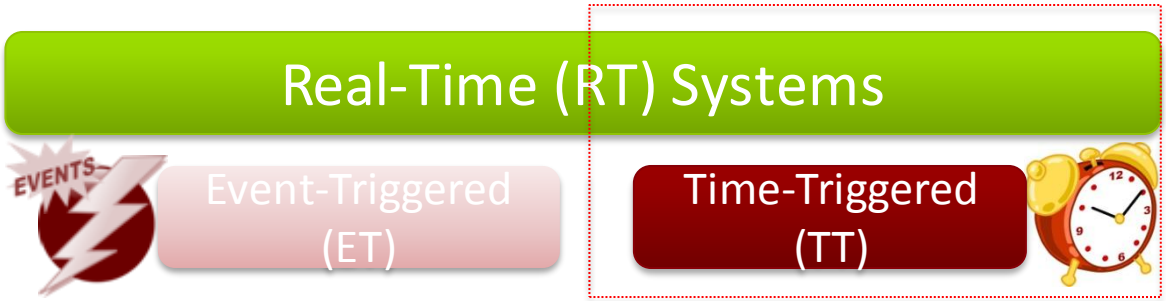
Verimag

Université Joseph Fourier GRENOBLE

www.cea.fr

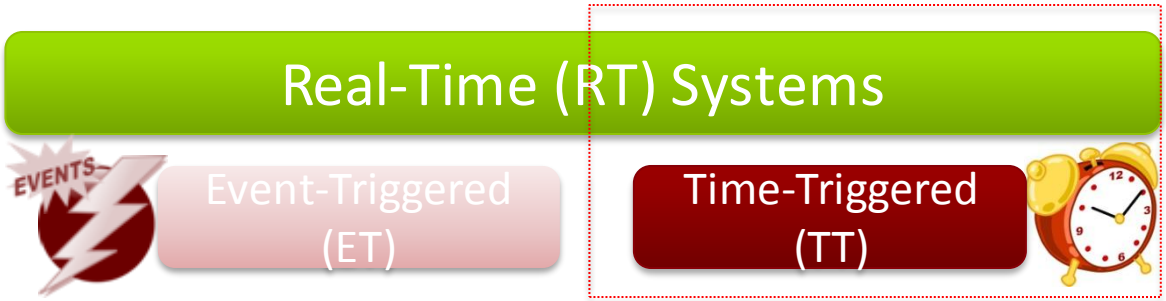
leti & list

Introduction



How to build Embedded RT systems of guaranteed quality, in a cost-effective manner??

Introduction

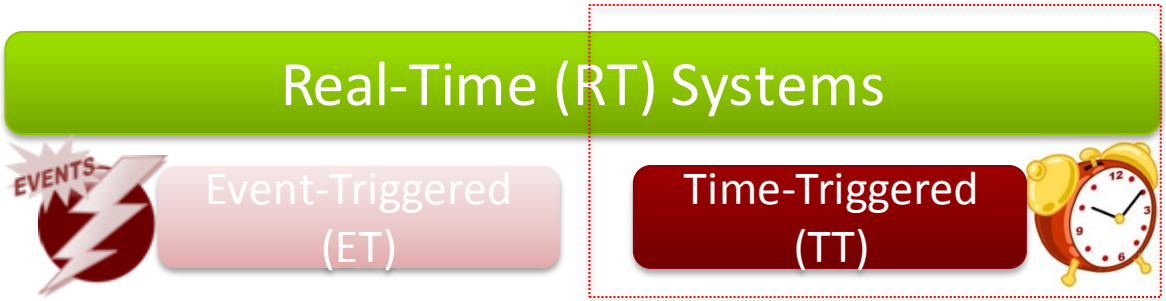


How to build Embedded RT systems of guaranteed quality, in a cost-effective manner??

Component-based design framework

- ✔ Abstracts away implementation details
- ✔ Validates the model through different techniques such as formal verification, simulation, and testing
- ✖ Targets generic execution model

Introduction



How to build Embedded RT systems of guaranteed quality, in a cost-effective manner??

Component-based design framework

- ✓ Abstracts away implementation details
- ✓ Validates the model through different techniques such as formal verification, simulation, and testing
- ✗ Targets generic execution model

RTOS-based implementation + TT approach

- ✗ No high-level programming models to tackle complexity
- ✓ Implement TT execution model

Introduction

Real-Time (RT) Systems

Event-Triggered (ET)

Time-Triggered (TT)

How to build Embedded RT systems of guaranteed quality, in a cost-effective manner??

Component-based design framework

RTOS-based implementation + TT approach

- ✔ Abstracts away implementation details
- ✔ Validates the model through different techniques such as formal verification, simulation, and testing
- ✖ Targets generic execution model

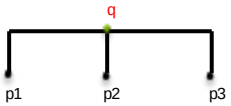
- ✖ No high-level programming models to tackle complexity
- ✔ Implement TT execution model

Background Concepts

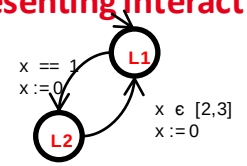
- RT-BIP Framework [1]:
  - Structure of a real-time BIP model:

→ **Mechanism for Conflict resolution between interactions**

→ **Connectors representing interactions**

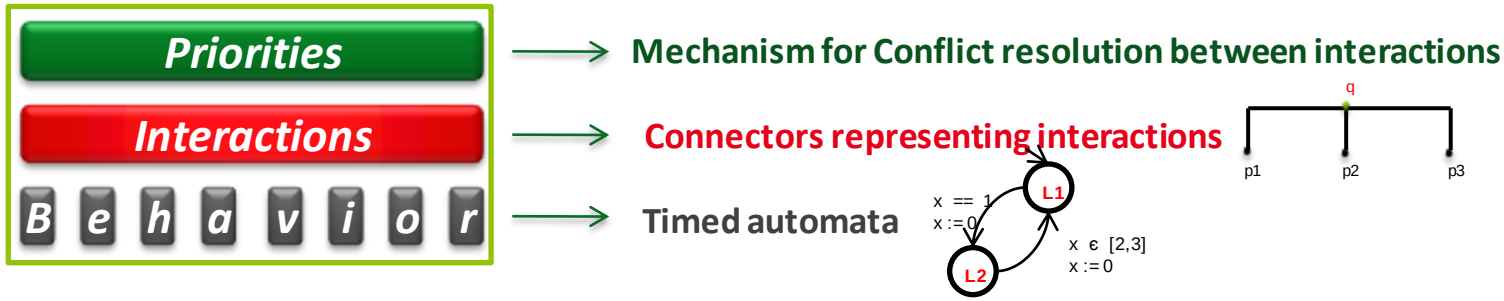


→ **Timed automata**

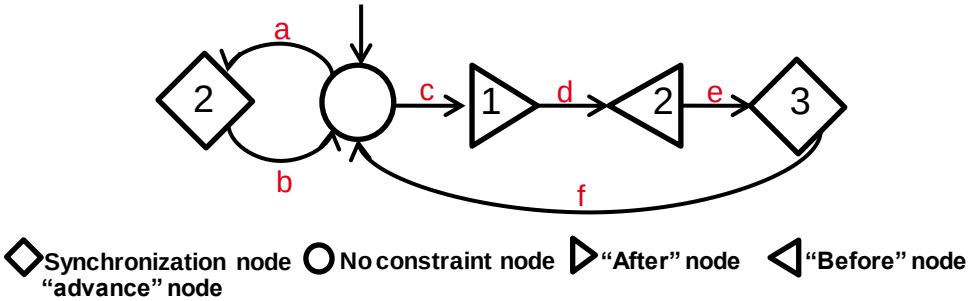


Background Concepts

- RT-BIP Framework [1]:
  - Structure of a real-time BIP model:

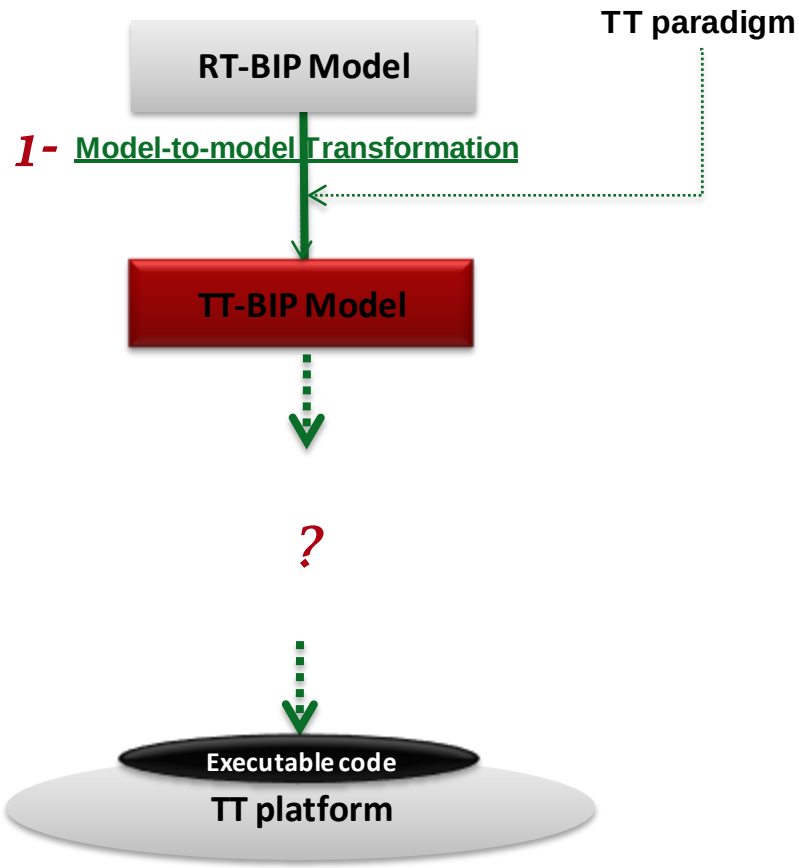


- TCA: Computation model of TT tasks in PharOS [2][5]:
  - The temporal behavior of a task is specified using a directed graph



Approach

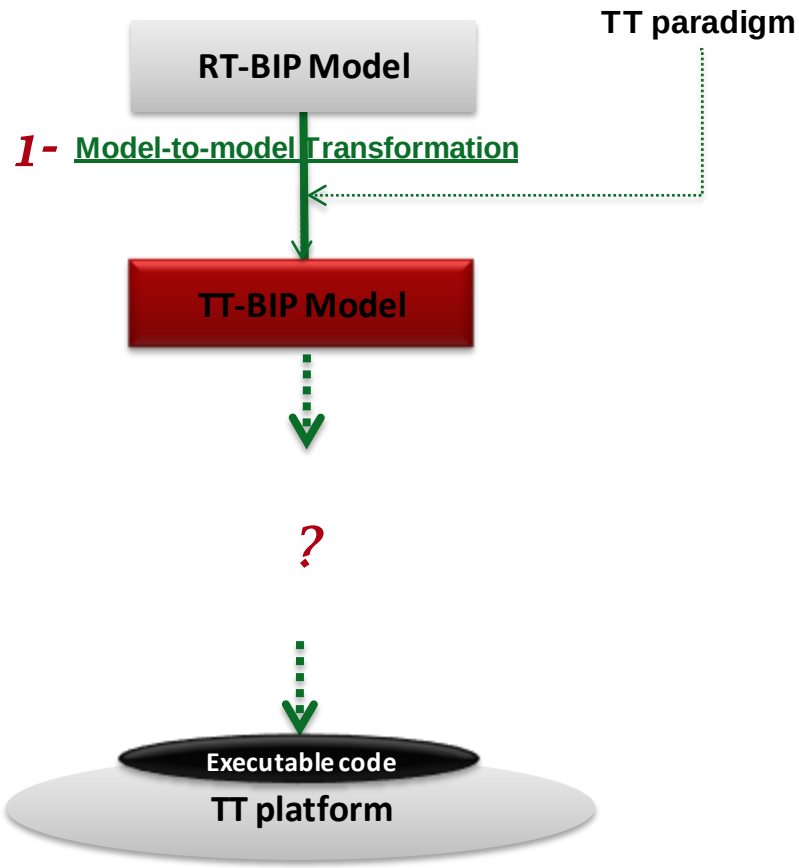
- 1/ Step1 [3]
  - TT-BIP = tasks components + communication components + unidirectional interactions.



Approach

- 1/ Step1 [3]
  - TT-BIP = tasks components + communication components + unidirectional interactions.

TT-BIP is not easily translated to an executable

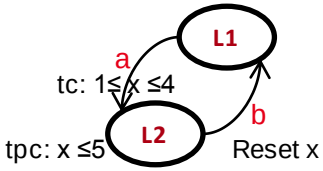


Approach

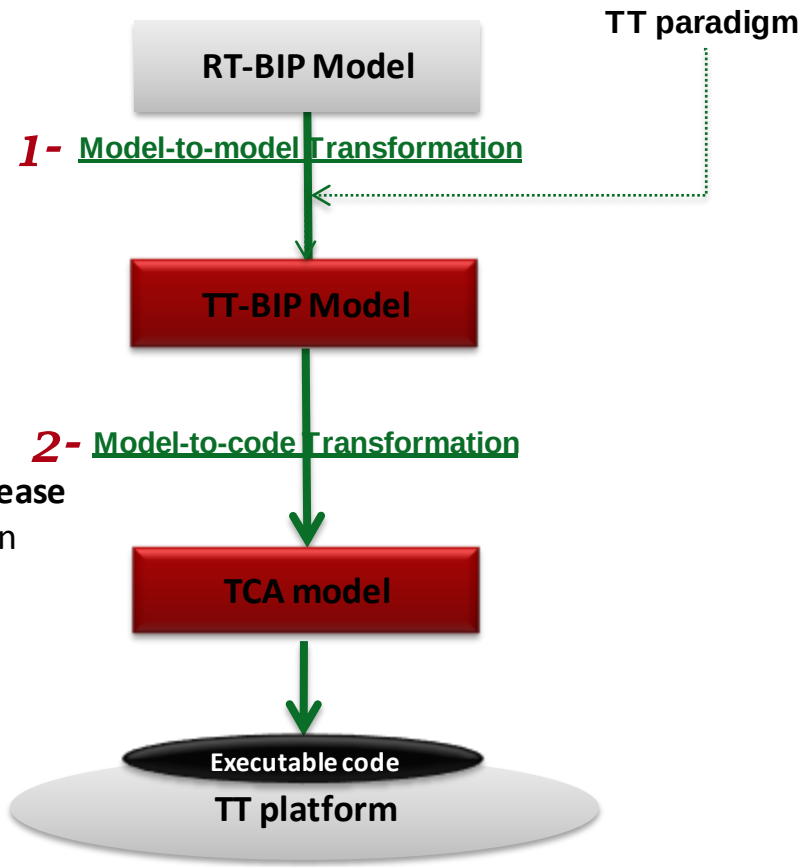
- 1/ Step1 [3]
  - TT-BIP = tasks components + communication components + unidirectional interactions.

- 2/ Step2:
  - Challenges:

1 Constraints only on the **start** instant of an action



Can be constrained both the **release** and **deadline** instants of an action

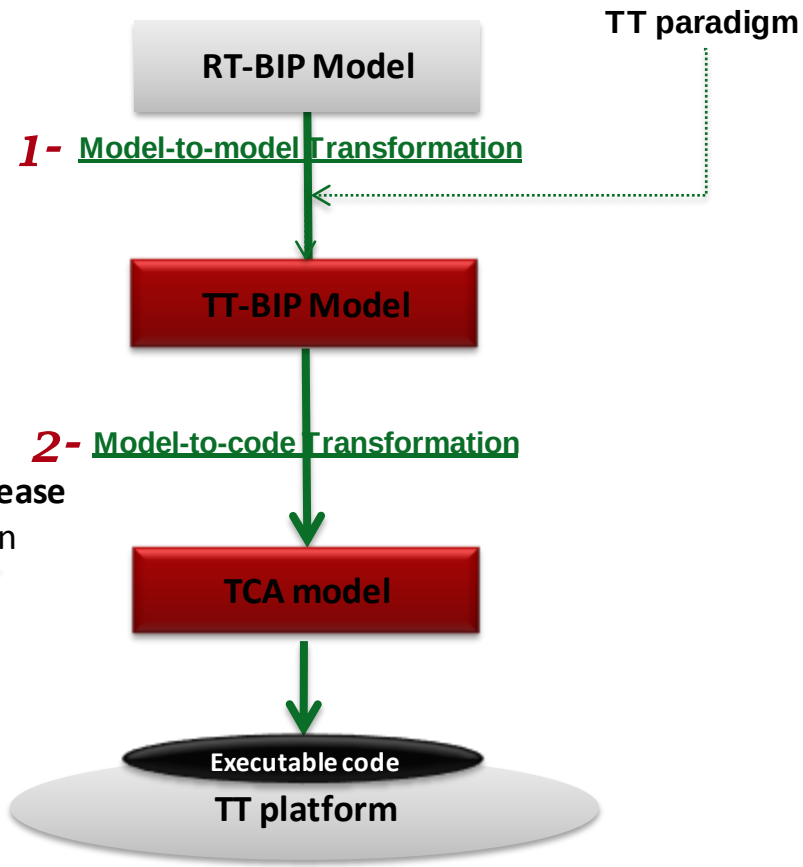


Approach

- 1/ Step1 [3]
  - TT-BIP = tasks components + communication components + unidirectional interactions.

- 2/ Step2:
  - Challenges:

1	Constraints only on the **start** instant of an action	Can be constrained both the **release** and **deadline** instants of an action
2	**Absolute** labeling of constraints	**Relative** labeling of constraints

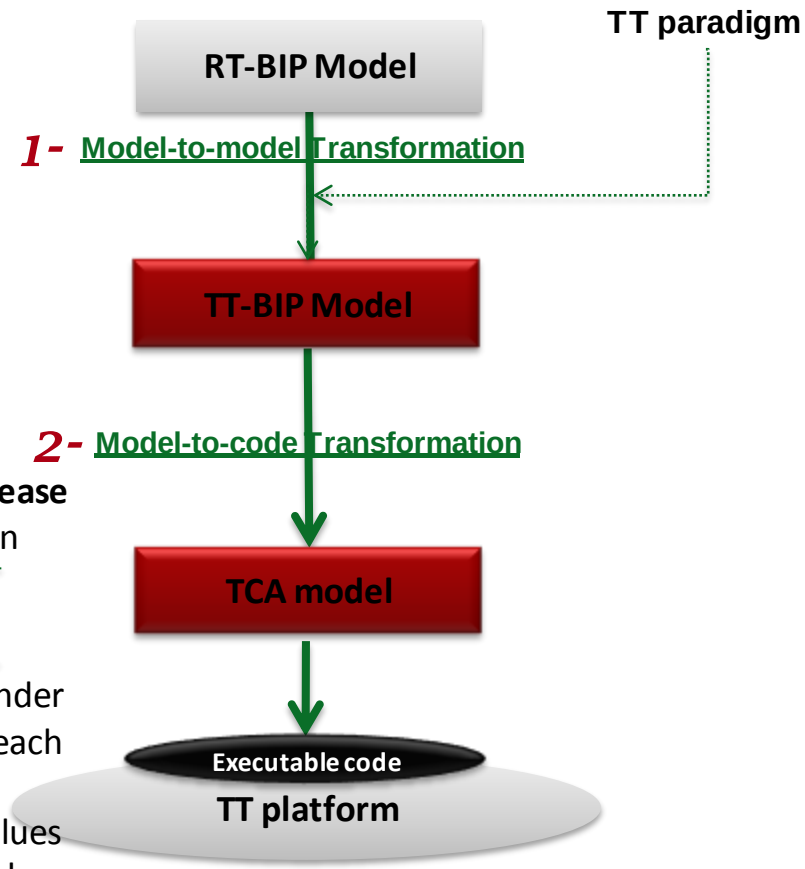


Approach

- 1/ Step1 [3]
  - TT-BIP = tasks components + communication components + unidirectional interactions.

- 2/ Step2:
  - Challenges:

1 Constraints only on the **start** instant of an action	Can be constrained both the **release** and **deadline** instants of an action
2 **Absolute** labeling of constraints	**Relative** labeling of constraints
3 Interactions = data transfer + **synchronization** between sending and receiving actions	**Desynchronized** interaction= sender provides new values at each synchronization point + Receivers can consult these values when their current time is equal or higher to the defined visibility dates.



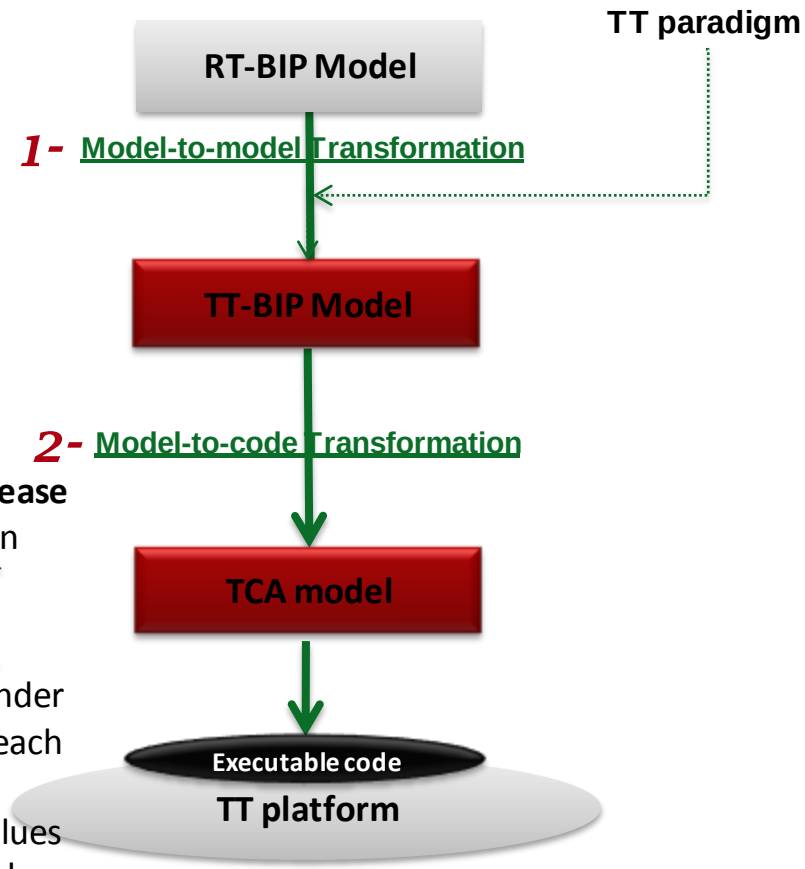
Approach

- 1/ Step1 [3]
  - TT-BIP = tasks components + communication components + unidirectional interactions.

- 2/ Step2:
  - Challenges:

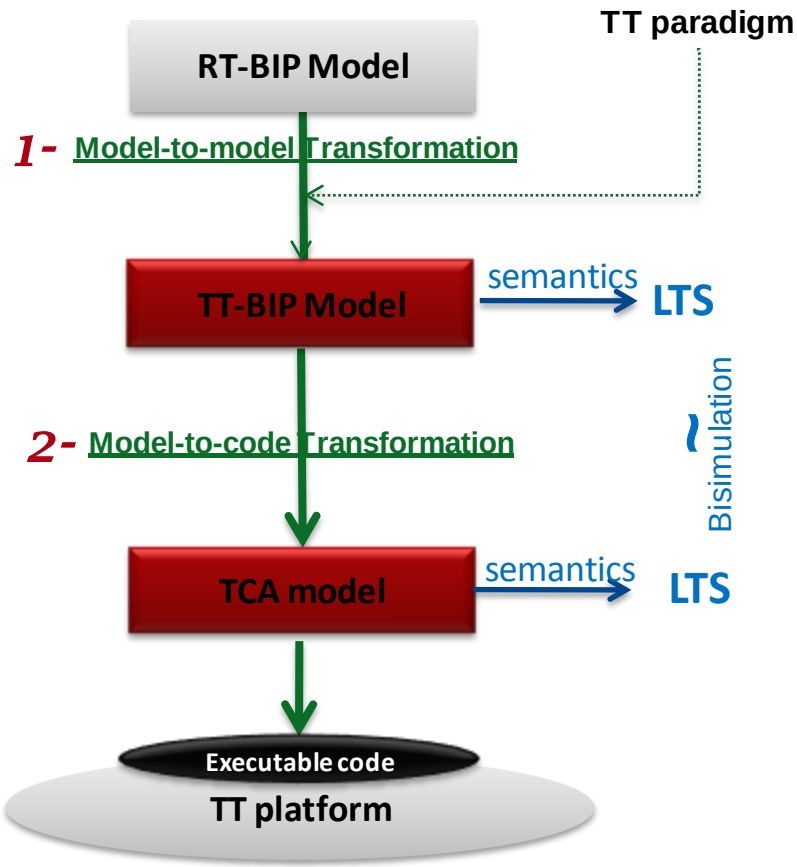
1. Constraints only on the **start** instant of an action — Can be constrained both the **release** and **deadlin**[illegible]ants of an action
2. **Absolute** labeling of constraints — **Re**[illegible] f constraints
3. Interactions = data[illegible] **synchronizati**[illegible] sending and re[illegible]ons — [illegible]**hronized** interaction= sender provides new values at each synchronization point + Receivers can consult these values when their current time is equal or higher to the defined visibility dates.

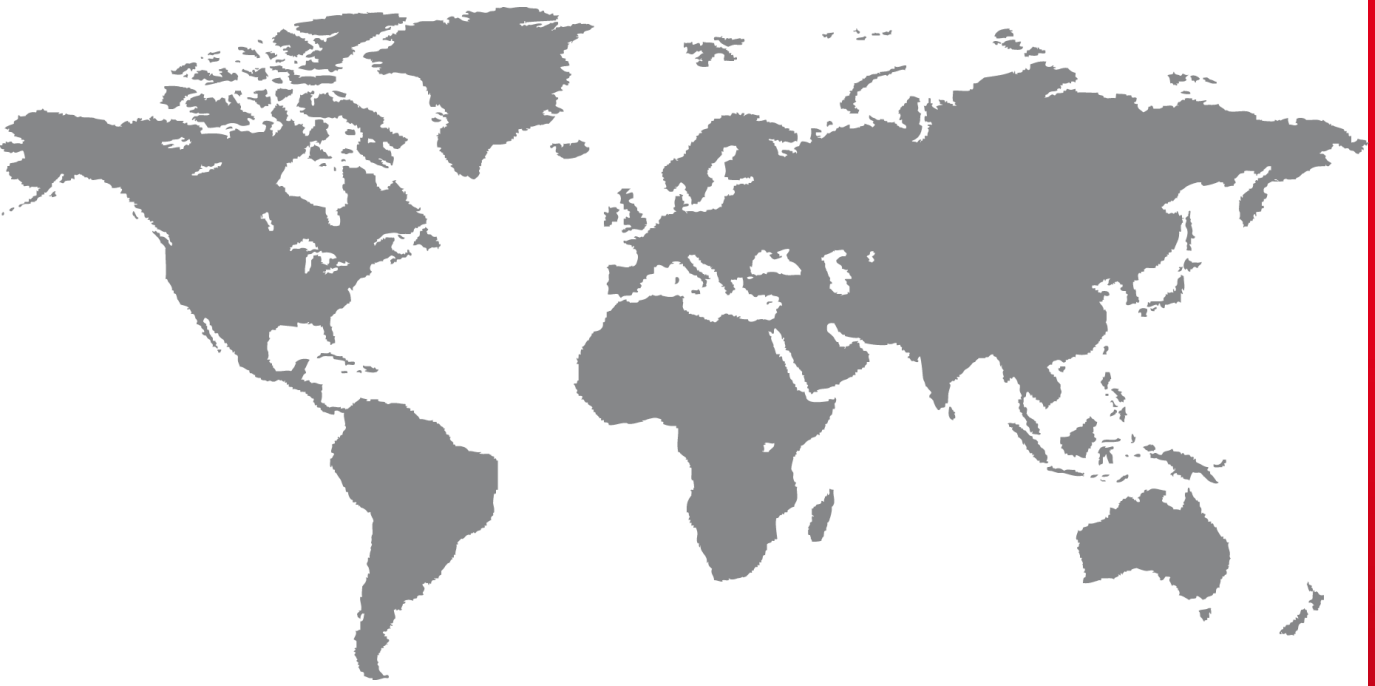
Algorithm details are given in the poster



Approach

- 1/ Step1 [3]
  - TT-BIP = tasks components + communication components + unidirectional interactions.
- 2/ Step2:
  - Challenges:
  - Correctness proof:
    - Expressing semantics of each model in terms of Labelled Transition system (LTS).
    - Proving equivalence between two LTSs by using bisimulation technique.
      → trace equivalence





Thank you!

[1] Tesnim Abdellatif. Rigourous Implementation of Real-Time Systems. PhD thesis, UJF, 2012.

[2] C Aussagues, D Chabrol, V David, D Roux, N Willey, A Tournadre, and M Graniou. PharOS, a multicore OS ready for safety-related automotive systems: results and future prospects. Proc. of The Embedded Real-Time Software and Systems (ERTS2), 2010.

[3] Hela Guesmi, Belgacem Ben Hedia, Simon Bliudze, Saddek Bensalem, and Jacques Combaz. Towards time-triggered component-based system models. In ICSEA15, pages 157–169, Barcelone, Spain, November 2015. ThinkMind.

[4] Robert Kaiser and Stephan Wagner. Evolution of the PikeOS microkernel. In Proceedings of the 1st International Workshop on Microkernels for Embedded Systems, pages 50–57, 2007.

[5] Matthieu Lemerre, Vincent David, Christophe Aussagu`es, and Guy Vidal-Naquet. An introduction to time-constrained automata. In Proc. Of the 3 rd Interaction and Concurrency Experience (ICE 2010), volume 38 of EPTCS, pages 83–98, 2010.

leti
Centre de Grenoble
17 rue des Martyrs
38054 Grenoble Cedex

list
Centre de Saclay
Nano-Innov PC 172
91191 Gif sur Yvette Cedex