UNIVERSITY
OF TRENTO - Italy

Parametric Real-Time System Feasibility Analysis Using Parametric Timed Automata

PhD Dissertation

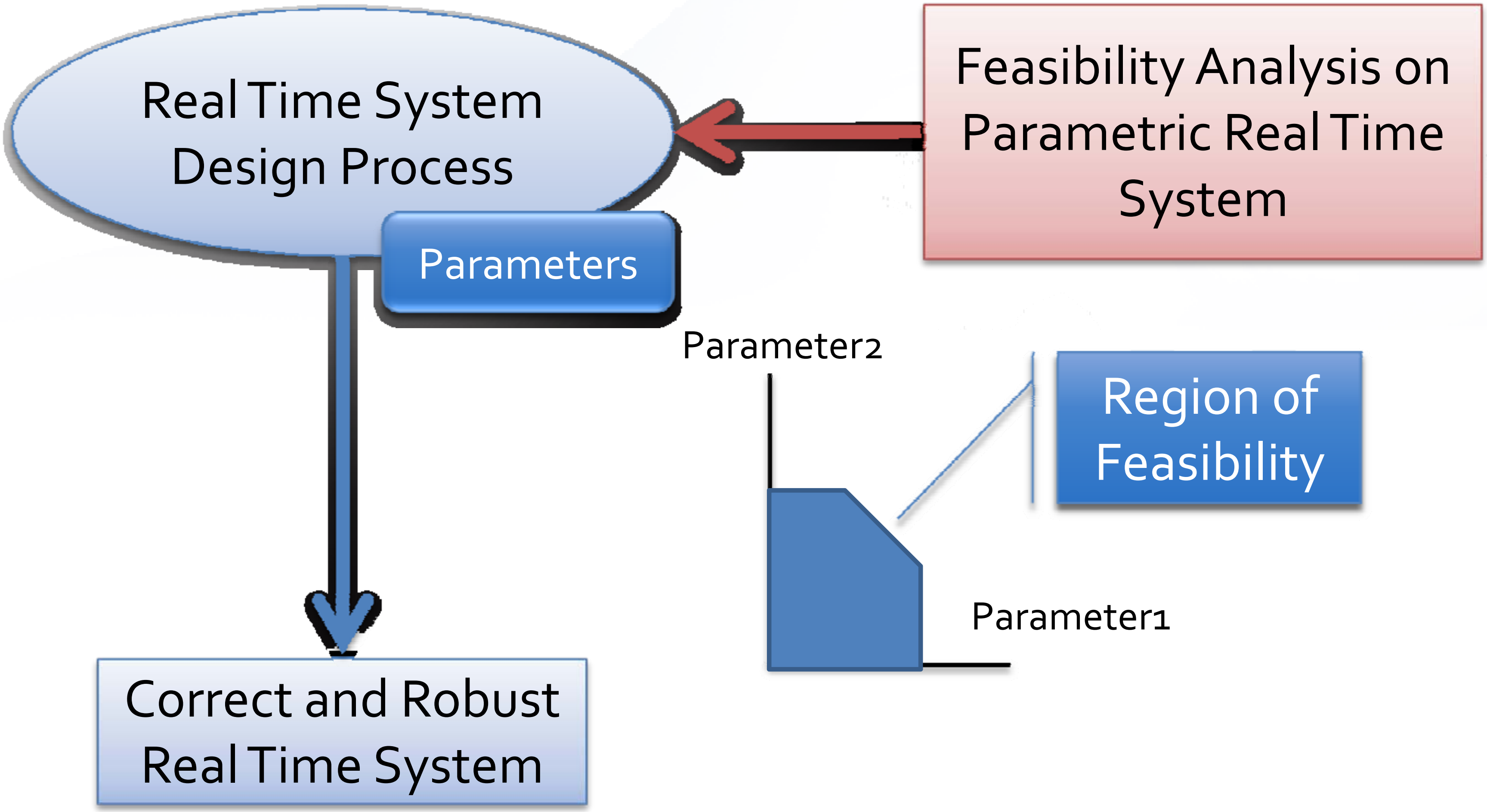
Yusi Ramadian

Advisor : Luigi Palopoli
Co-advisor : Alessandro Cimatti

Real-Time System Applications

- A computer based system, which produces results to inputs complying with some temporal constraints

Main Research Idea



Contribution of PhD research

UNIVERSITY OF TRENTO - Italy

- Parametric Timed Automata (PTA) definition and representation of Real Time System
- Parametric Verification of Temporal Properties (PVTP) method
- Implementation in tool Quinq
- Application in case problems :
  - periodic task system [RTSS08],
  - heterogeneous system [ETFA10],
  - collaboration with Modular Performance Analysis Toolbox (MPA) [CASES11].

Presentation Outline

UNIVERSITY OF TRENTO - Italy

- Motivation
  - Real time system design
  - Example scenario
  - Problem Statement
- Solution
  - Parametric Timed Automata
  - Parametric Verification of Temporal Property Method
- Implementation in Quinq
  - Architecture
  - Demo
- State of the art
- Conclusion

The Importance of CORRECT & ROBUST Real Time System

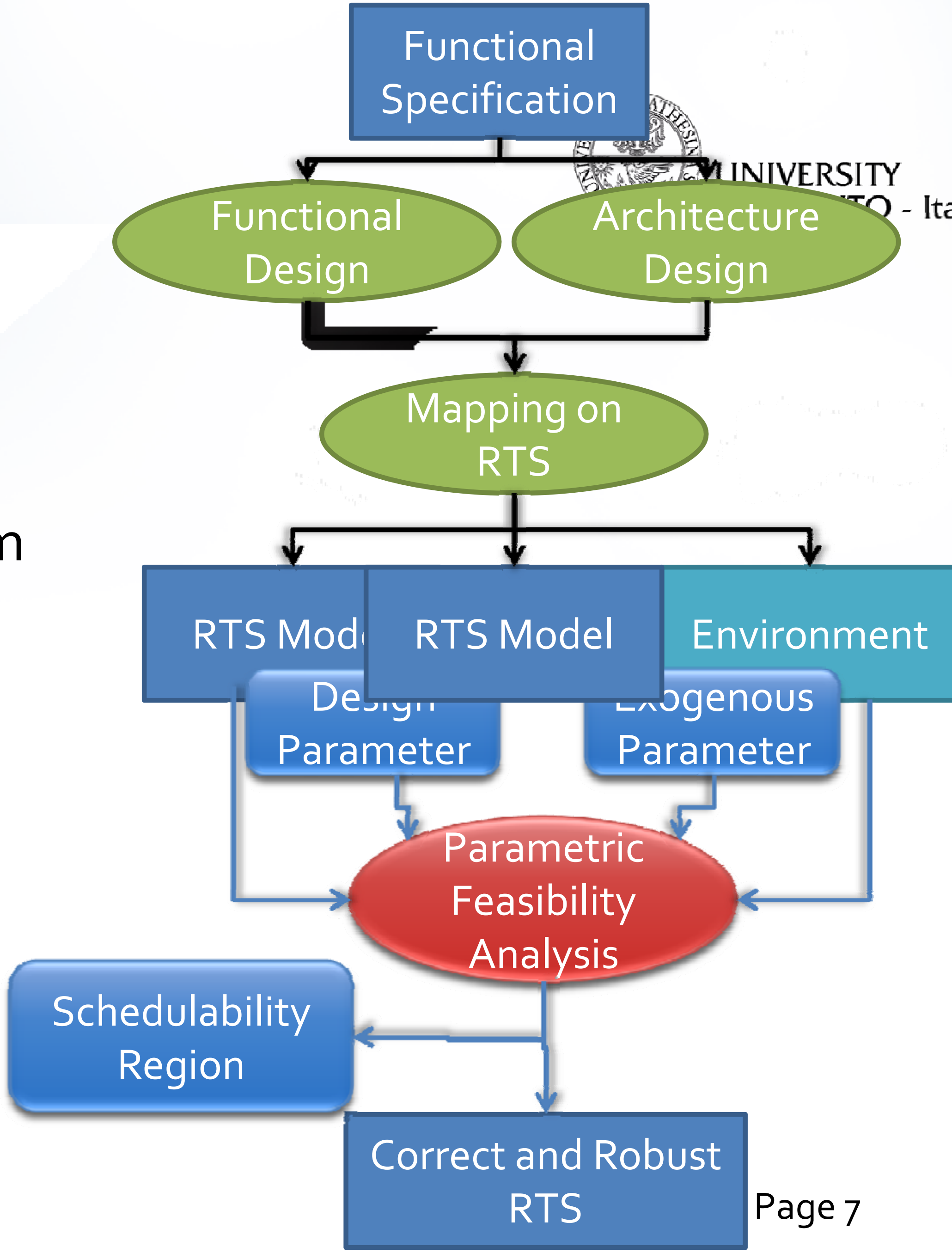
UNIVERSITY OF TRENTO - Italy

- Safety consideration
- Manufacturing consideration
- Variability in environment and run-time

→Need for formalization of design process

Design Process

- Design & Modelling
  - Activation pattern
  - Timing properties
  - Scheduling Algorithm
- Robustness & Parameter Tuning
  - Assign values
  - Evaluate system robustness w.r.t to parameters



Presentation Outline

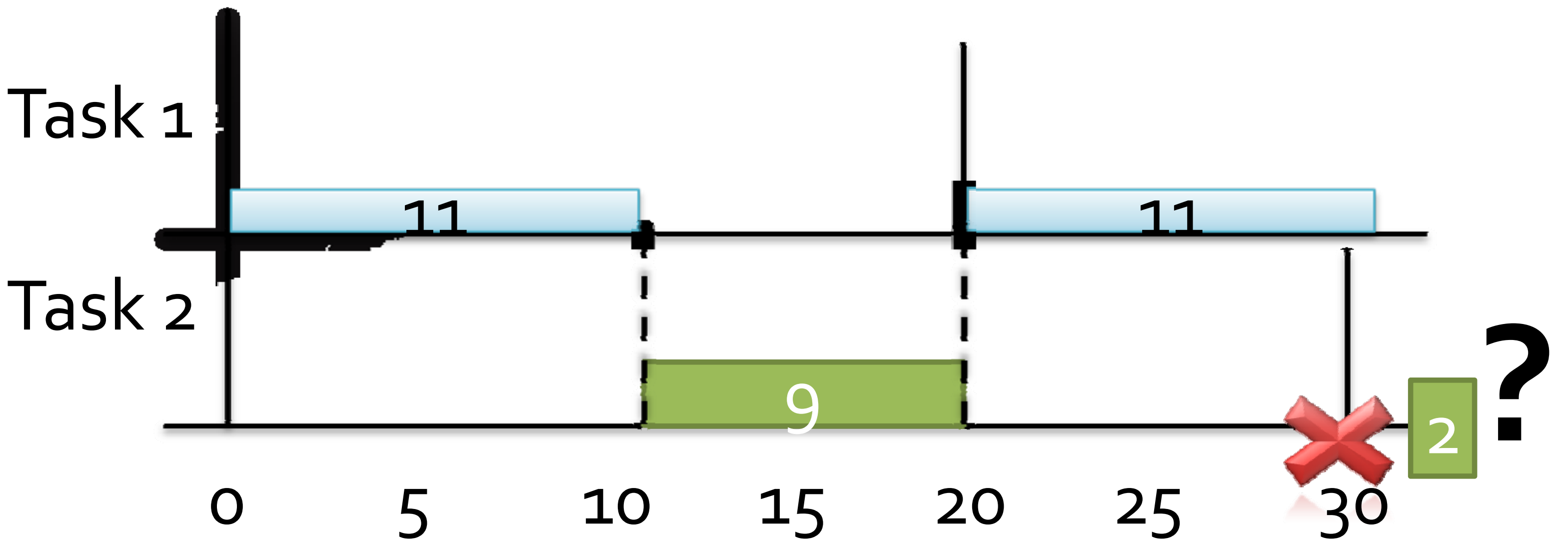
UNIVERSITY
OF TRENTO - Italy

- Motivation
  - Real time system design
  - Example scenario
  - Problem Statement
- Solution
  - Parametric Timed Automata
  - Parametric Verification of Temporal Property Method
- Implementation in Quinq
  - Architecture
  - Demo
- State of the art
- Conclusion

Sensitivity Analysis : Example Scenario

UNIVERSITY OF TRENTO - Italy

Parameters	Task 1	Task 2
Period	20	30
Deadline	20	30
Computation Time	11	12
Offset	0	0



Sensitivity Analysis : Example Scenario Discussion #1

UNIVERSITY OF TRENTO - Italy

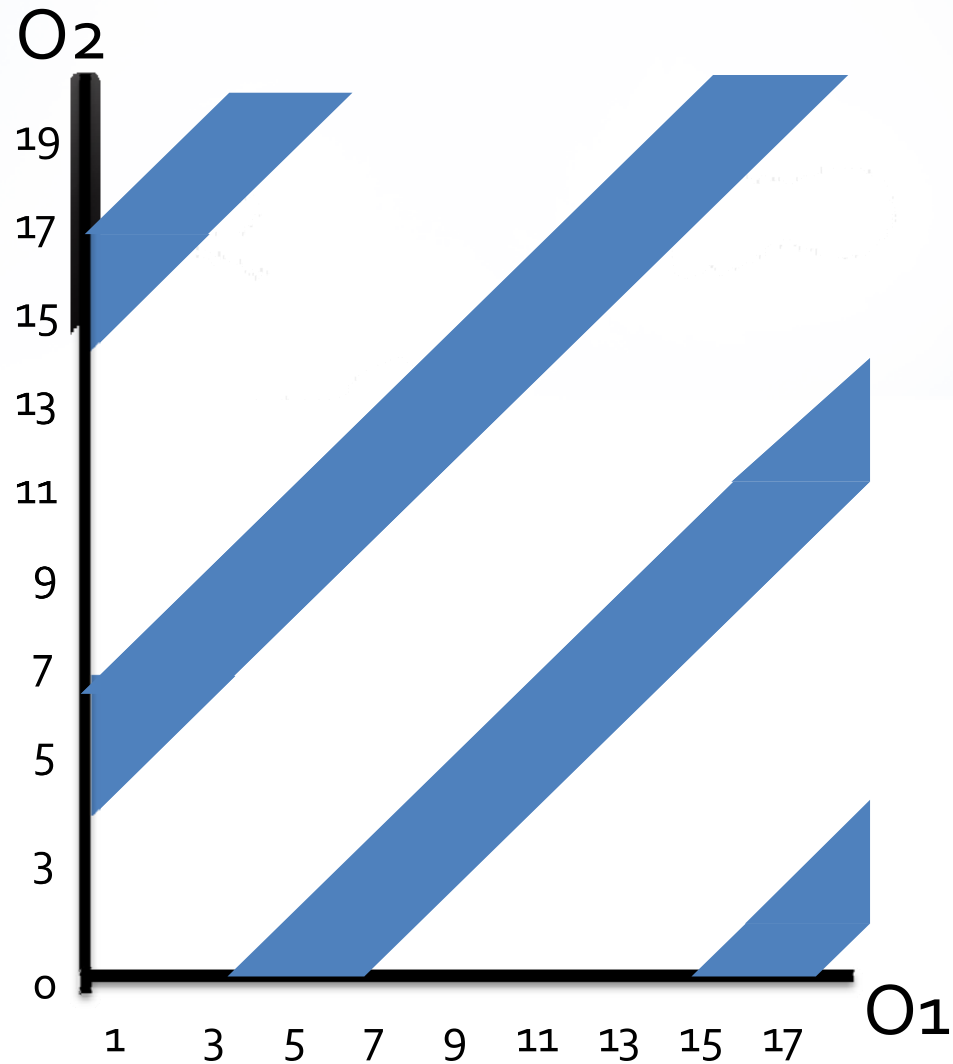
- Classical scheduling theory → system failure
  Task system is not schedulable

- Solution
  - Stronger machine (Hardware solution)
  - Tweaking offset..

Sensitivity Analysis : Region of Schedulability on Offsets

UNIVERSITY OF TRENTO - Italy

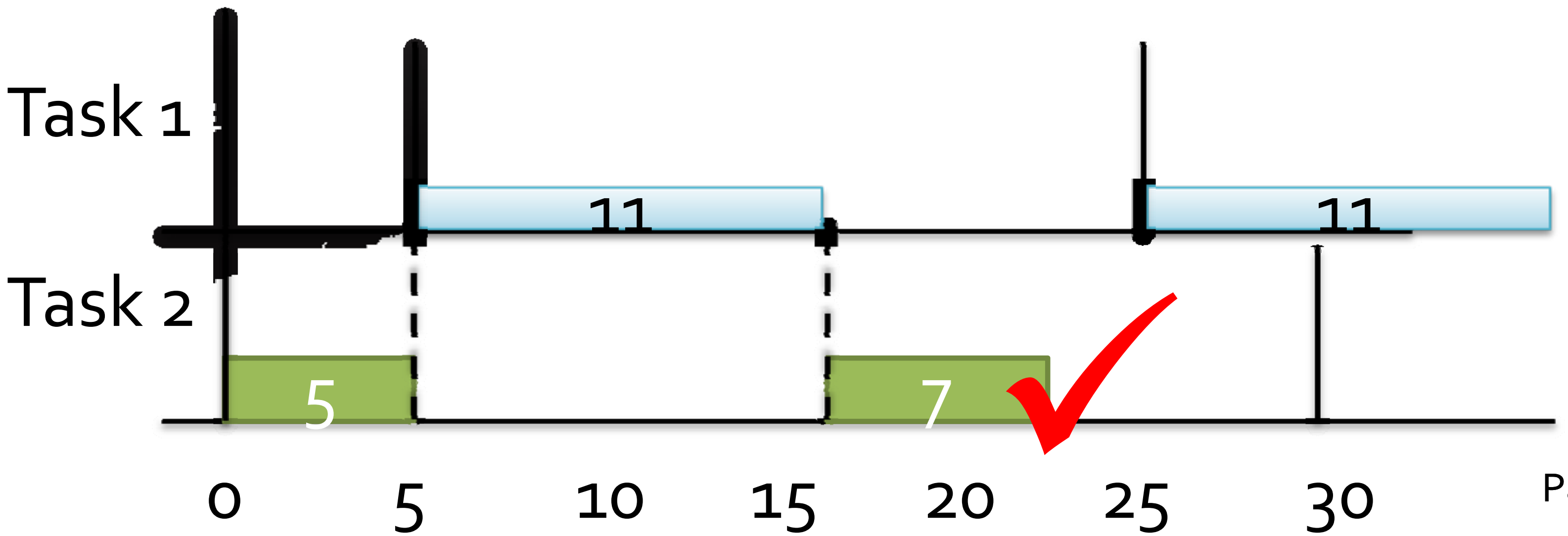
Parameters	Task 1	Task 2
Period	20	30
Deadline	20	30
Computation Time	11	12
Offset	**?**	**?**



Sensitivity Analysis: Corrected Scenario

UNIVERSITY OF TRENTO - Italy

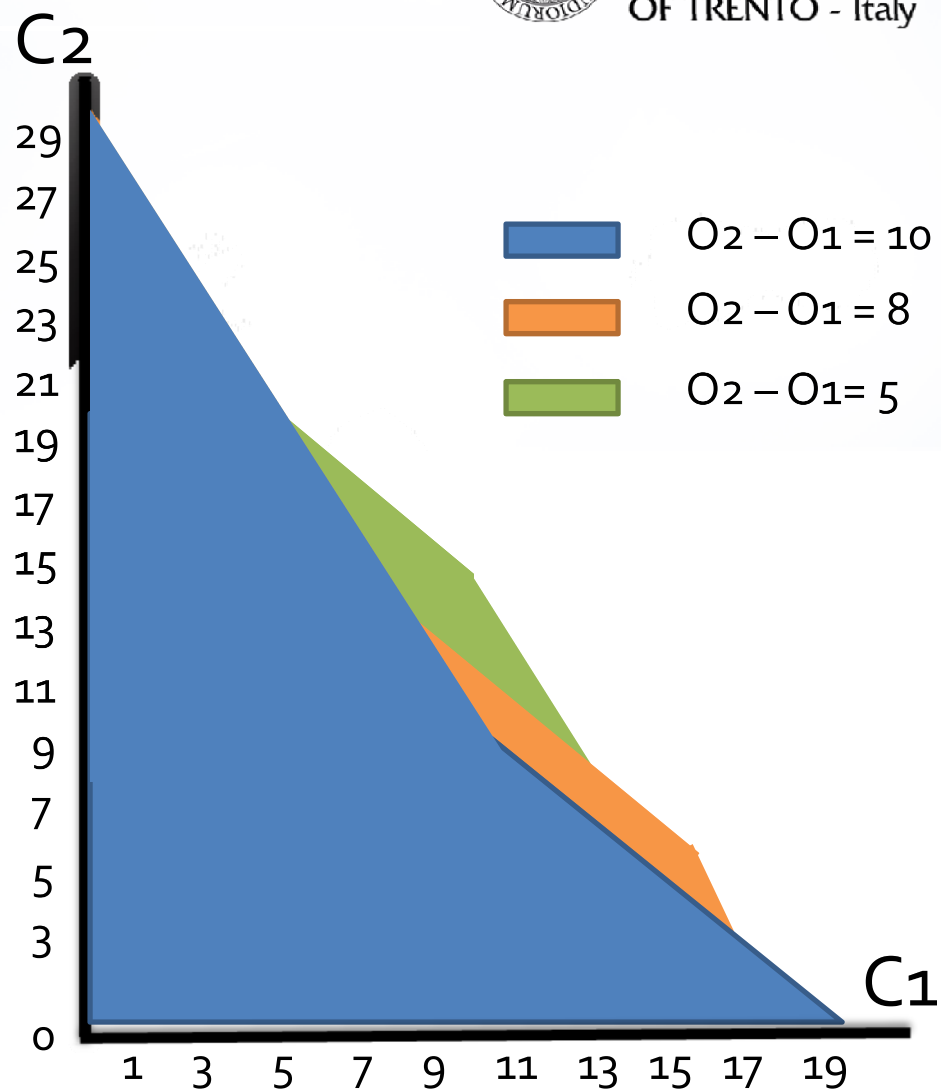
Parameters	Task 1	Task 2
Period	20	30
Deadline	20	30
Computation Time	11	12
Offset	**5**	**0**



Sensitivity Analysis: Example Scenario Discussion #2: Robustness

Parameters	Task 1	Task 2
Period	20	30
Deadline	20	30
Computation Time	**?**	**?**
Offset	**5**	**?**

System robustness = ?



Sensitivity Analysis

UNIVERSITY OF TRENTO - Italy

Requirement conclusion #1:

We want to find out :

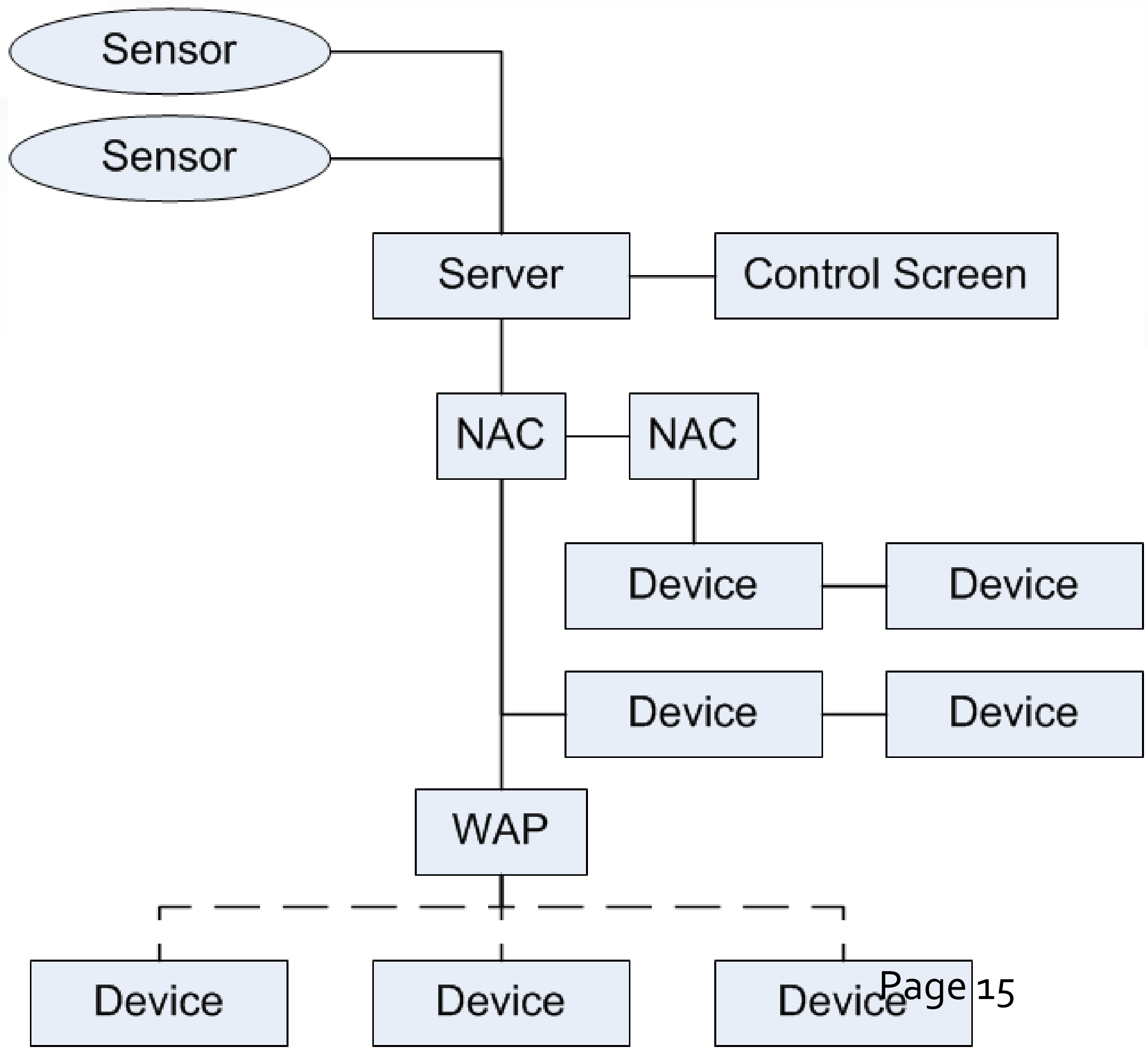
the schedulability regions in the space of parameters

→ most robust design for our real-time systems

Sensitivity Analysis:
Example Scenario Discussion #3:

UNIVERSITY OF TRENTO - Italy

- System model not in classical RTS
- Examples:
  - System with buffers
  - Complex activation pattern
  - Heterogeneous, distributed system
  - Flexible deadline (e.g. Firm Deadline)



Sensitivity Analysis

- Requirement conclusion #2

  Sensitivity analysis for **general** real-time system

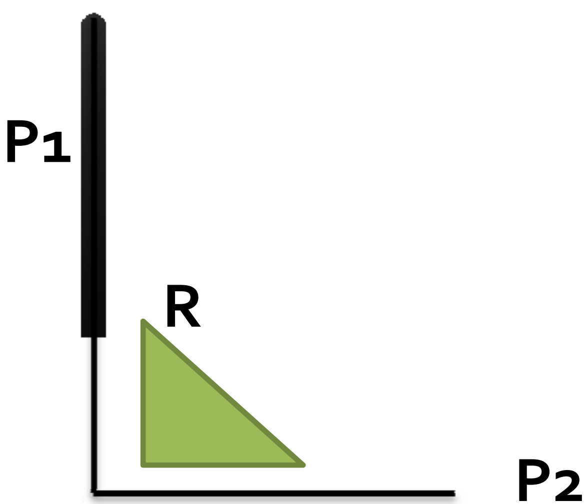
Presentation Outline

UNIVERSITY OF TRENTO - Italy

- Motivation
  - Real time system design
  - Example scenario
  - Problem Statement
- Solution
  - Parametric Timed Automata
  - Parametric Verification of Temporal Property Method
- Implementation in Quinq
  - Architecture
  - Demo
- State of the art
- Conclusion

Sensitivity Analysis: Formal problem definition

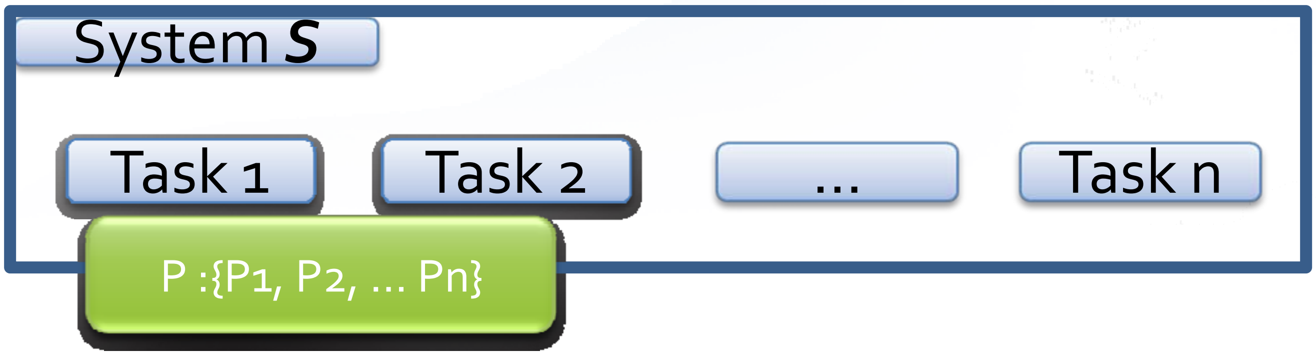
- **Problem 1**:

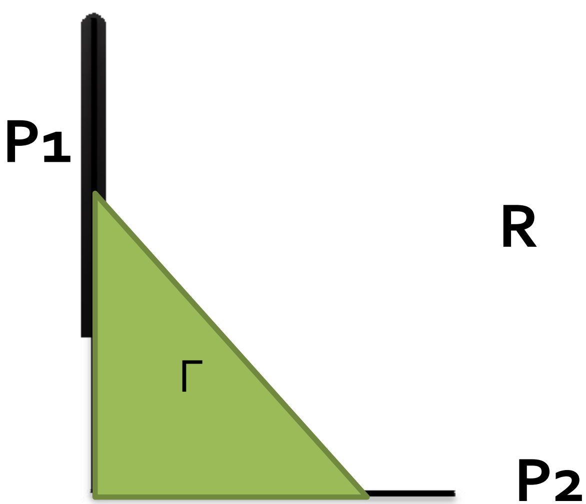


Sensitivity Analysis: Formal problem definition

UNIVERSITY OF TRENTO - Italy

- **Problem 2**:





Presentation Outline

UNIVERSITY OF TRENTO - Italy

- Motivation
  - Real time system design
  - Example scenario
  - Problem Statement
- Solution
  - Parametric Timed Automata
  - Parametric Verification of Temporal Property Method
- Implementation in Quinq
  - Architecture
  - Demo
- State of the art
- Conclusion

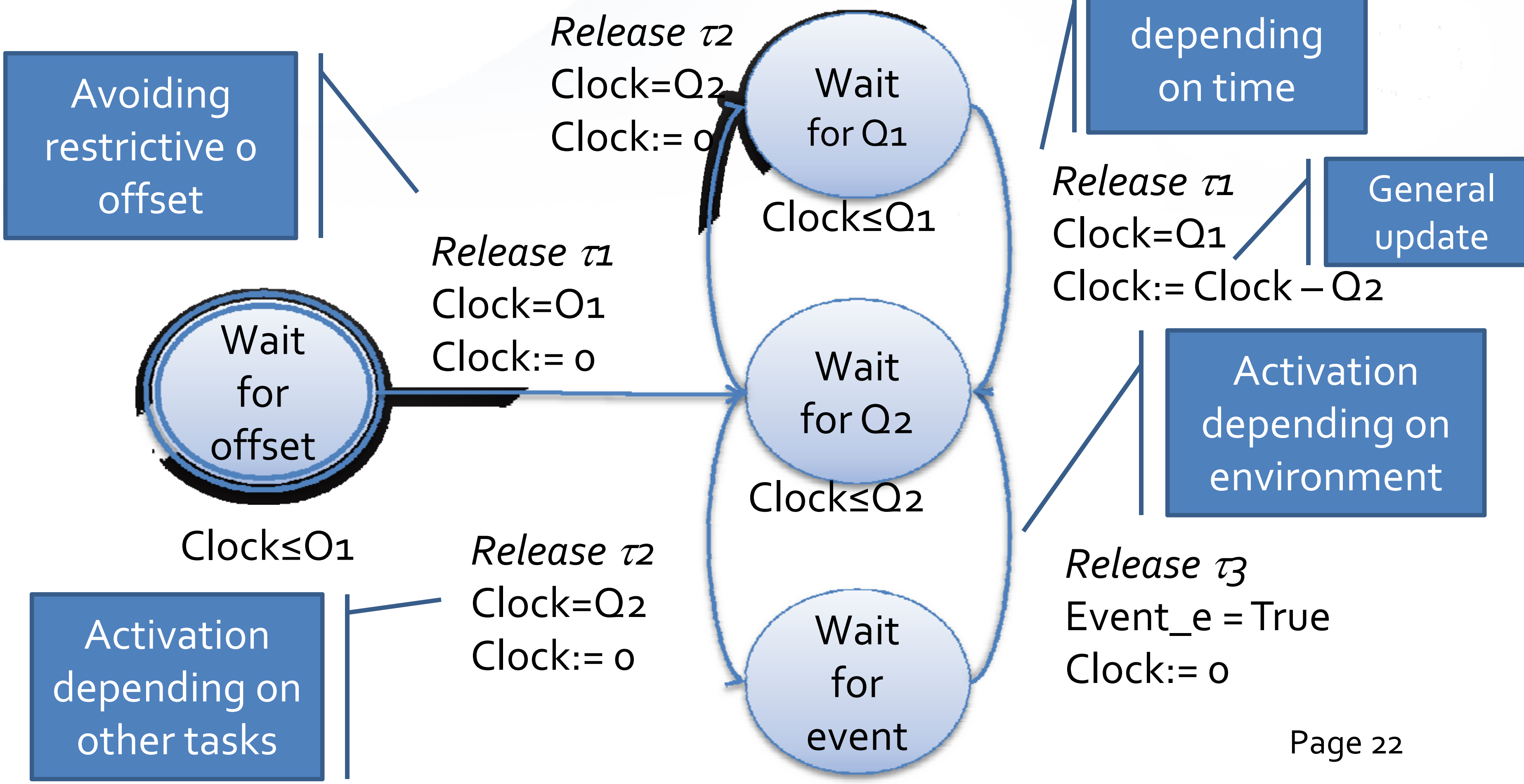
Parametric Timed Automata

UNIVERSITY OF TRENTO - Italy

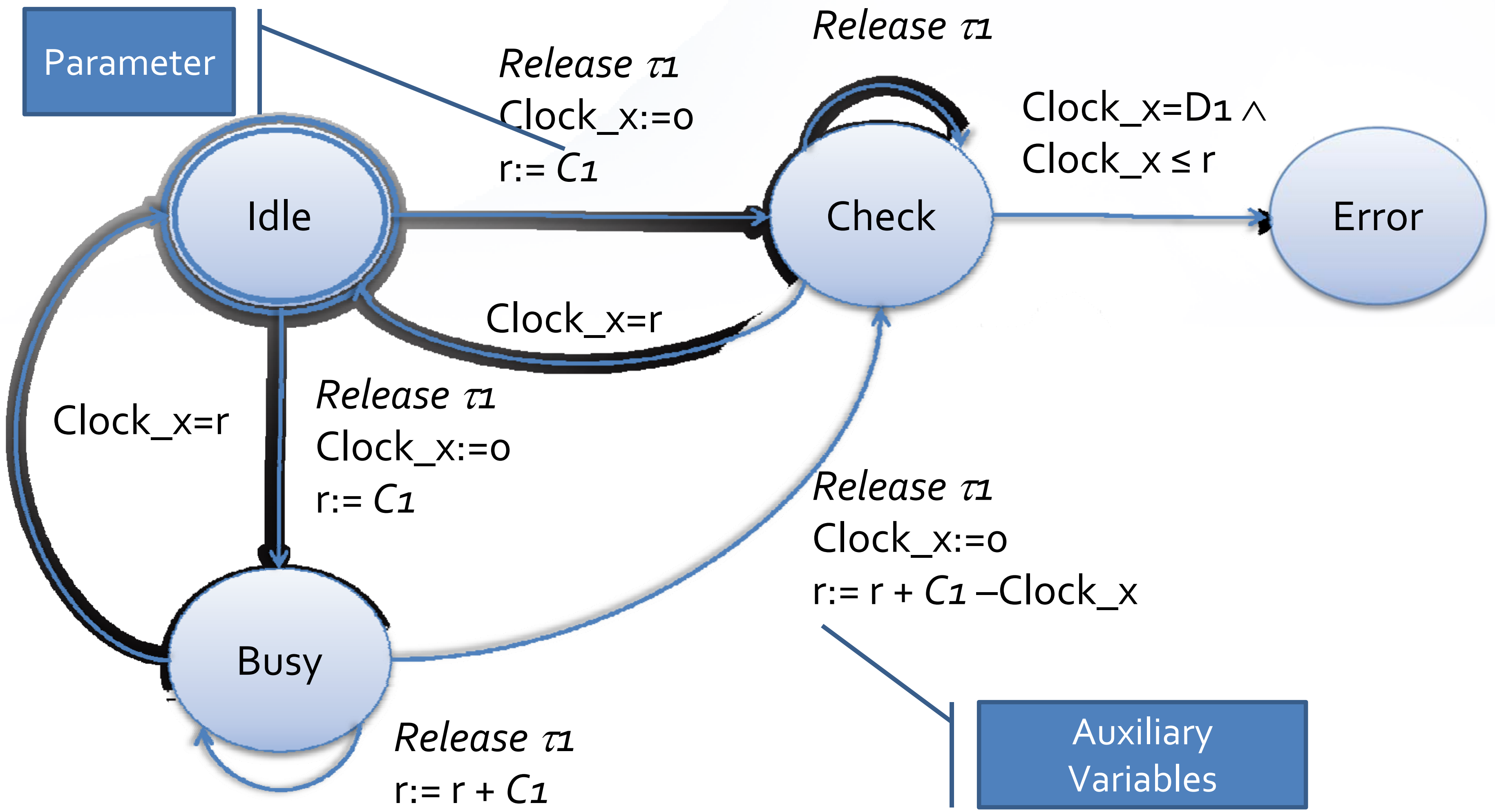
- Timed automata with parameters extension
- Main differences:
  - Parameters
  - Auxiliary variables
  - General update statement

Real Time System in PTA: Activation Pattern

- Allow complex activation pattern

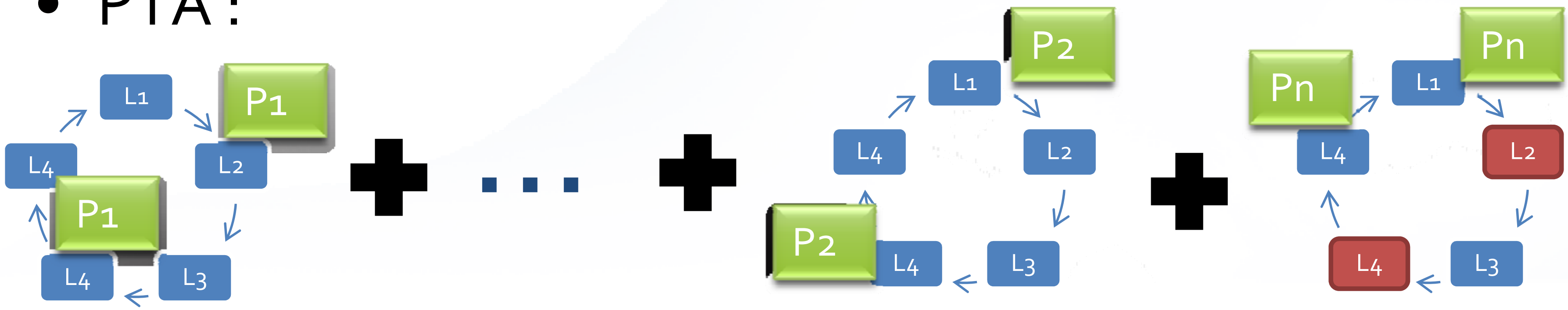


Real Time System in PTA: Feasibility Checker



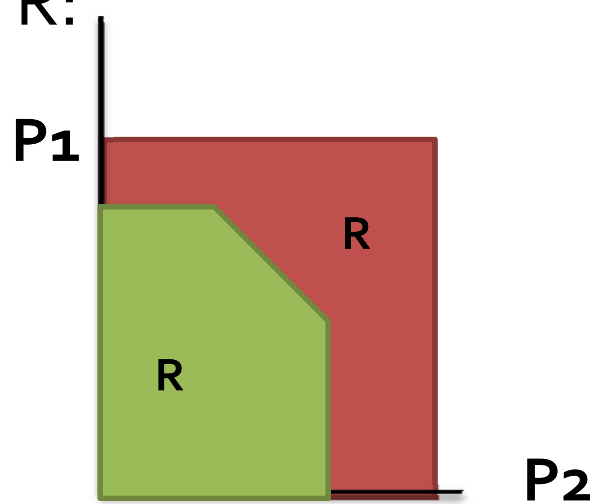
Sensitivity Analysis via PTA

- PTA :



Activation Automata | Activation Automata | Activation Automata | Feasibility Checker Automata

- Feasibility region R:



Symbolic representation of PTA

UNIVERSITY OF TRENTO - Italy

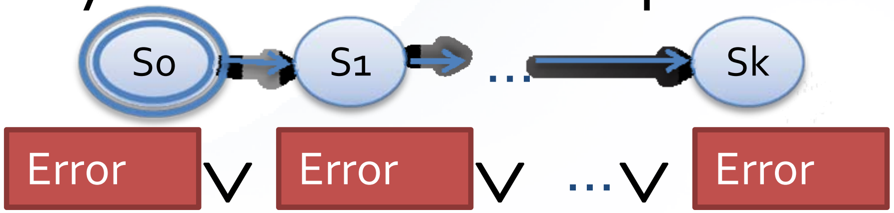
- Current state variables V:
  Discrete vars D: Location, transitions as *boolean*
  Continuous vars X: Clocks and other variables as *real*

- Symbolic model of PTA : set of constraints on boolean and real variables

- Examples:
  $Loc_i \rightarrow x\text{-}y \leq O1$
  $Trans_i \rightarrow (x \geq C1) \wedge (x' = C1+x) \wedge (y' = y)$

Bounded Model Checking (BMC)

- Look only for counterexample made of *k*-states



- BMC(*k*):
- $I(V^0) \wedge R(V^0,V^1) \wedge \ldots \wedge R(V^{k-1},V^k) \wedge Error(V^k)$

- Completeness of the solution is not guaranteed

- Complementing method : inductive reasoning

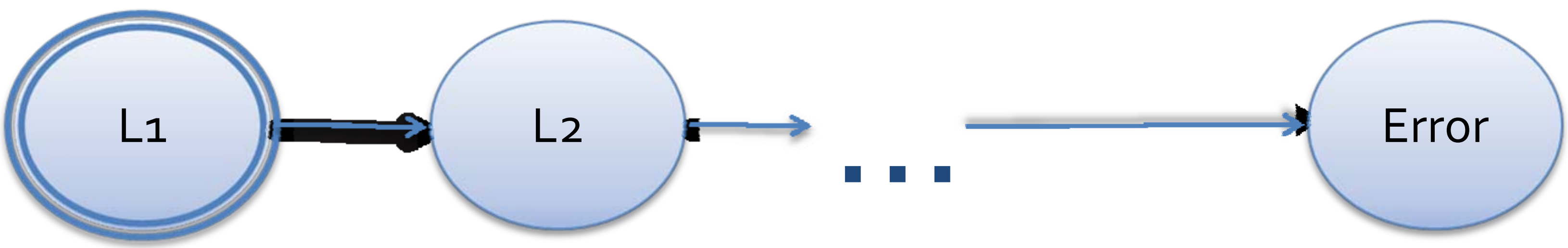
Presentation Outline

UNIVERSITY OF TRENTO - Italy

- Motivation
  - Real time system design
  - Example scenario
  - Problem Statement
- Solution
  - Parametric Timed Automata
  - Parametric Verification of Temporal Property Method
- Implementation in Quinq
  - Architecture
  - Demo
- State of the art
- Conclusion

PTVP algorithm intuition: Search for an error trace

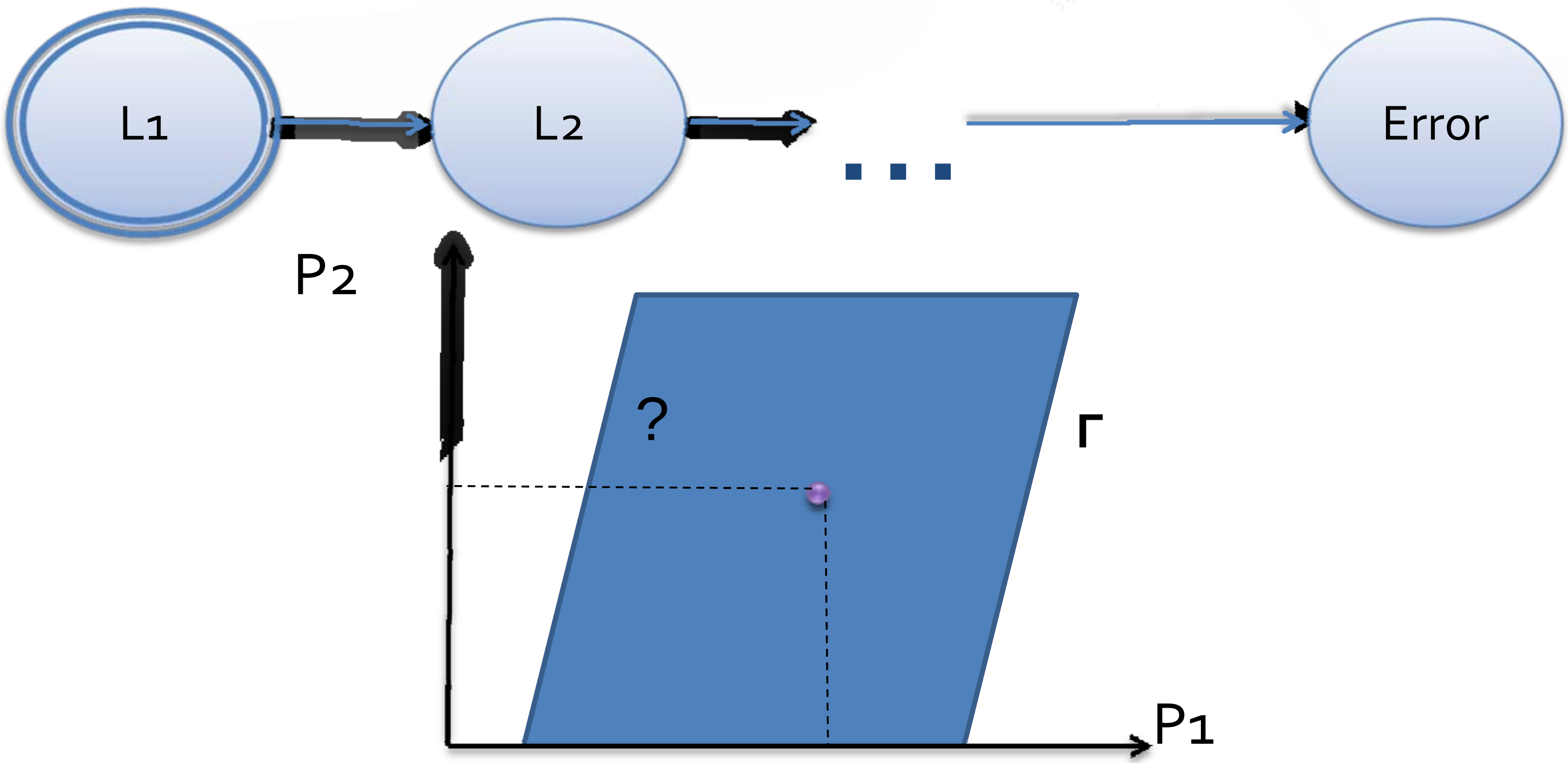
- Verification on reachability problem using BMC:
  An error trace for every found counterexample
- Alternatively, error trace can be searched via non-parametric model checker
- An error trace π :



PTVP algorithm intuition: An error trace π

UNIVERSITY OF TRENTO - Italy

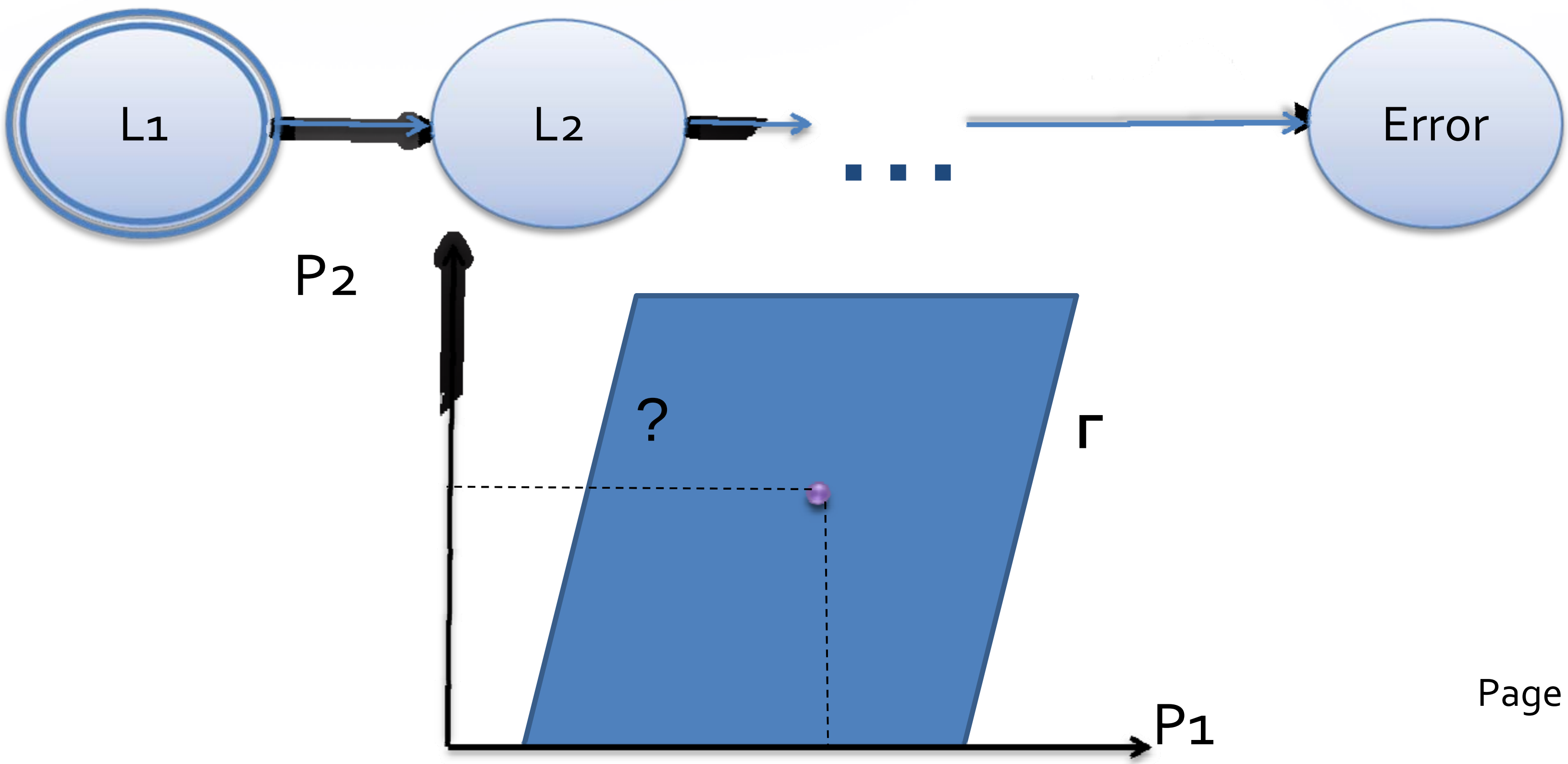
- Along with the trace, an assignment for the parameters that validate the trace is produced



PTVP algorithm intuition:
Sensitivity analysis to an error trace

UNIVERSITY OF TRENTO - Italy

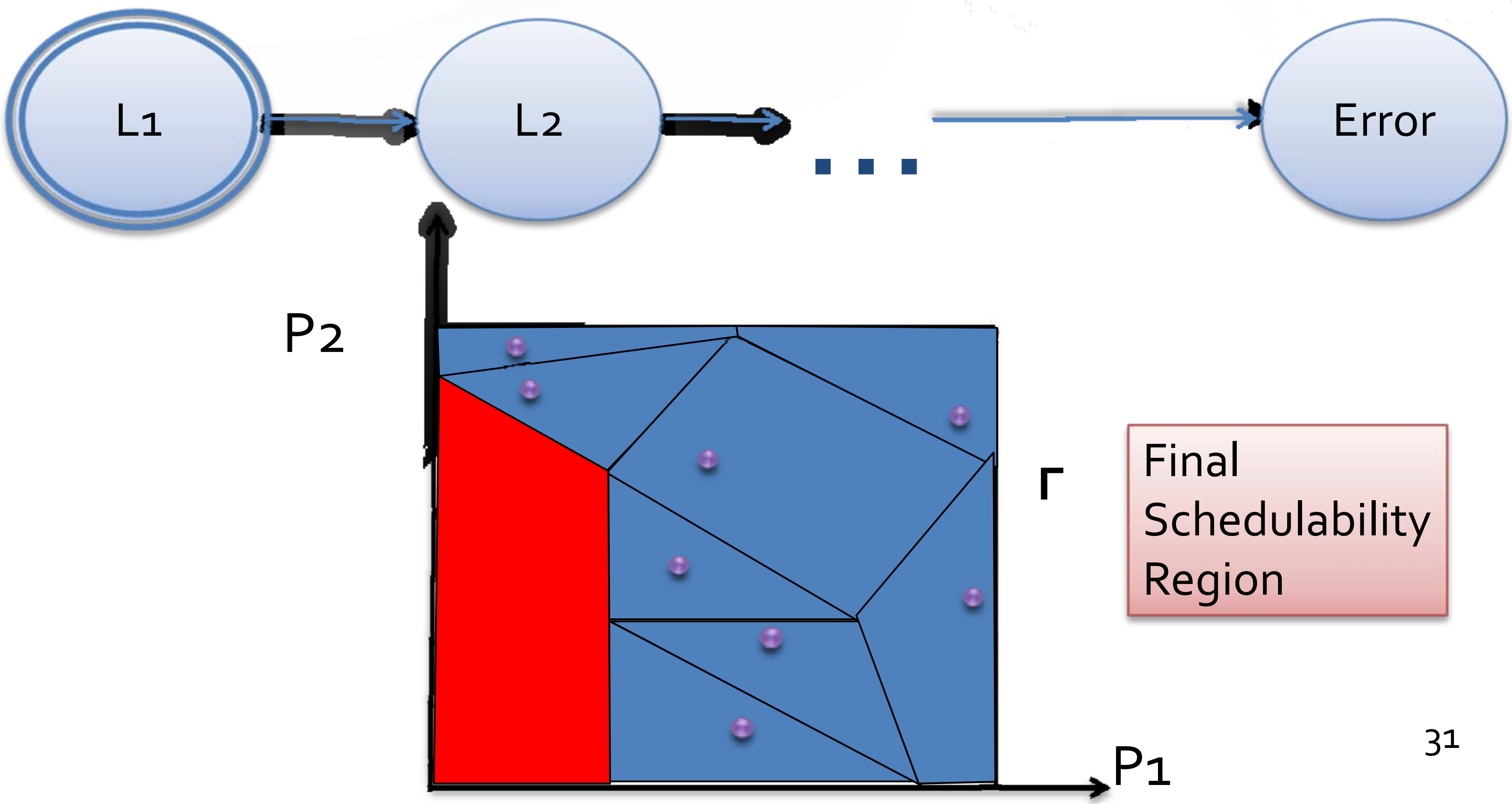
- By processing the trace, the surrounding region of parameters that make the trace true is identified
- ...And we rule this region out from the next search



PTVP algorithm intuition: Schedulability region

UNIVERSITY OF TRENTO - Italy

- Feasibility region : found by iteratively bounding the parameter space from the unschedulability regions



Final Schedulability Region

Parametric Verification of Temporal Properties (PVTP) Algorithm


```
Require: PTA describing activations and scheduling of n tasks
Ensure: Schedulability Region
for i = 1 to n do
    PTA.init(ParamSchedProblemForTask(i))
    j = 0
    while PTA.reachable(Error) do
        trace = PTA.get_trace()
        Unfeasible[j] = PTA.get_parameter(trace)
        PTA.add_constraints( negate( Unfeasible[j]))
        j++
    Feasible[i] = not(big_or(0, j, Unfeasible))
Return big_and(0, n, Feasible)
```

Error Trace Search

Sensitivity Analysis

Region Exclusion

Collection of regions

Sensitivity Analysis

- Given Polyhedron in the space of clocks and parameters Poly{P, X}
- Obtain Poly{P} <-> ∃ X, Poly {P, X}

→ Existential Quantifier Elimination

Presentation Outline

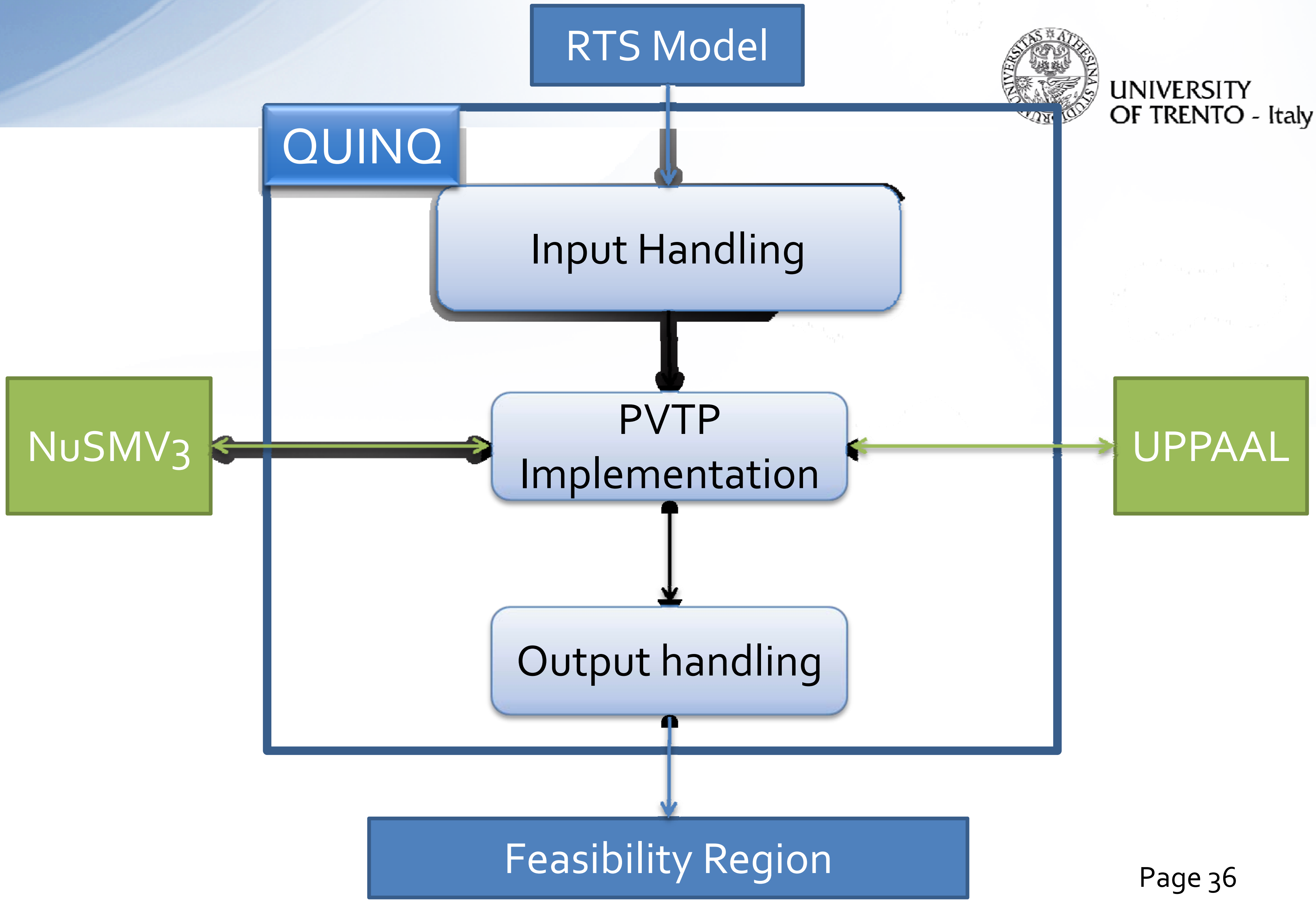
- Motivation
  - Real time system design
  - Example scenario
  - Problem Statement
- Solution
  - Parametric Timed Automata
  - Parametric Verification of Temporal Property Method
- Implementation in Quinq
  - Architecture
  - Demo
- State of the art
- Conclusion

Implementation in Quinq

UNIVERSITY OF TRENTO - Italy

- Based on NuSMV3 symbolic model checker with underlying MathSAT SMT solver
- Main functionalities :
  - Input handling
  - PVTP algorithm implementation
  - Completion check
  - Output handling
- Components
  - Sensitivity add-on
  - High level periodic system analysis
  - Search optimization
  - Model checker drivers
  - Graph generator
- Blackbox components : UPPAAL, JUNT, existelim

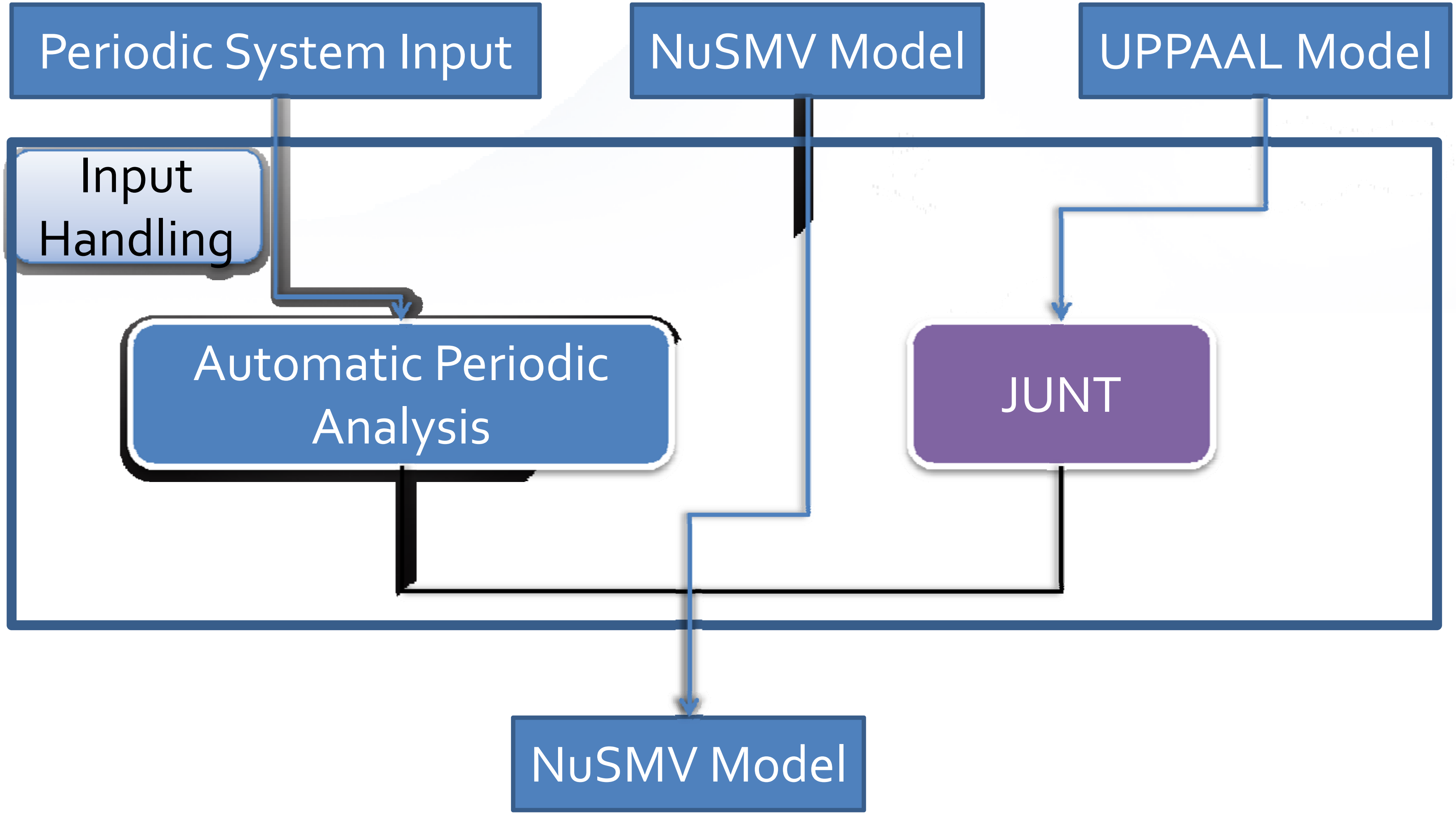
Architecture



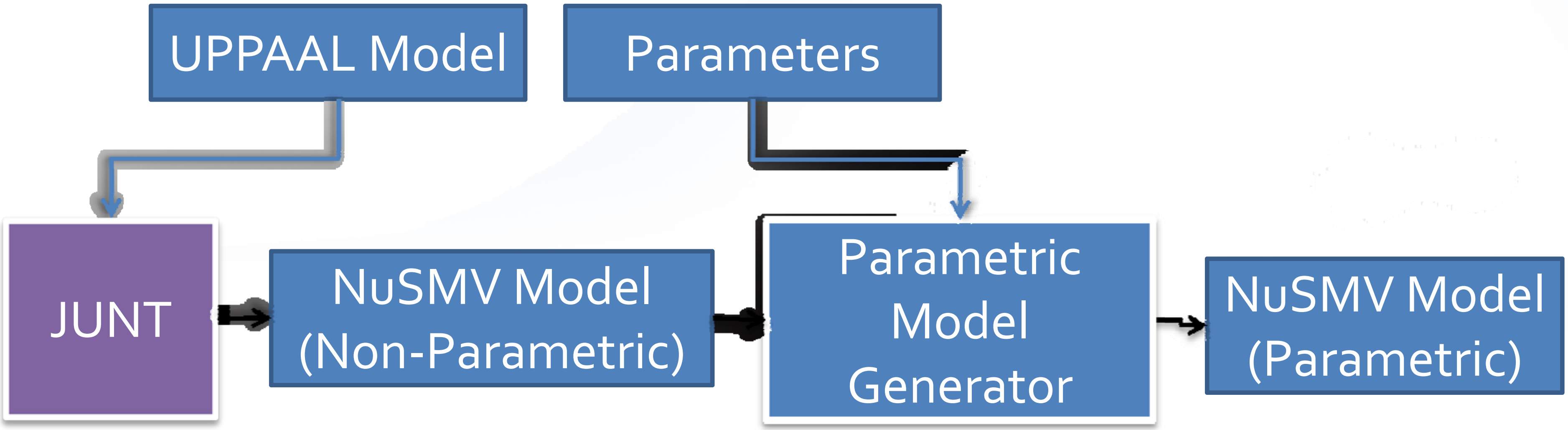
UNIVERSITY OF TRENTO - Italy

Input Handling

UNIVERSITY OF TRENTO - Italy

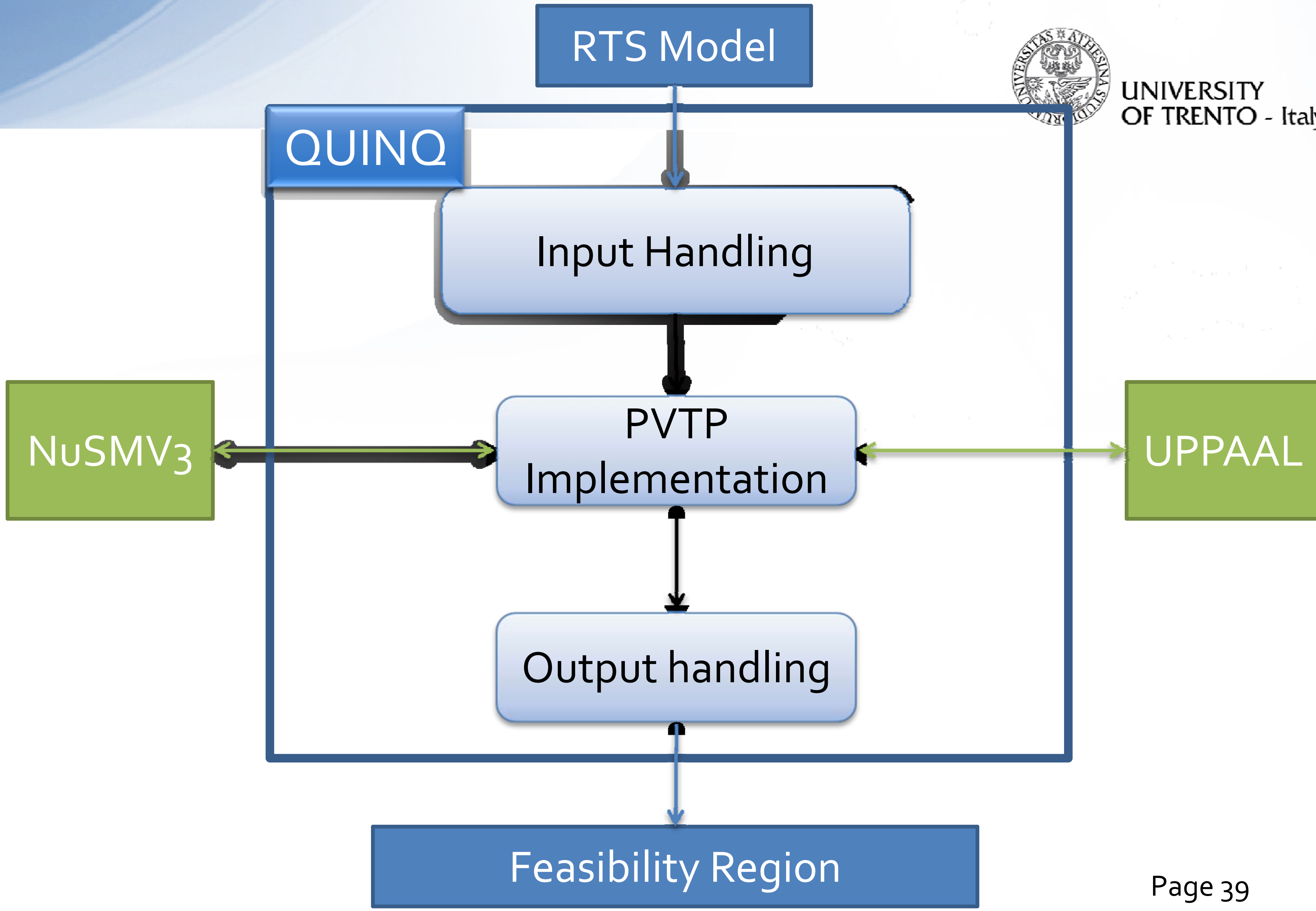


Input via UPPAAL Model



- Point of Considerations:
  - Integer vs Real domain
  - Array data structure
  - Clocks
  - Transition synchronization

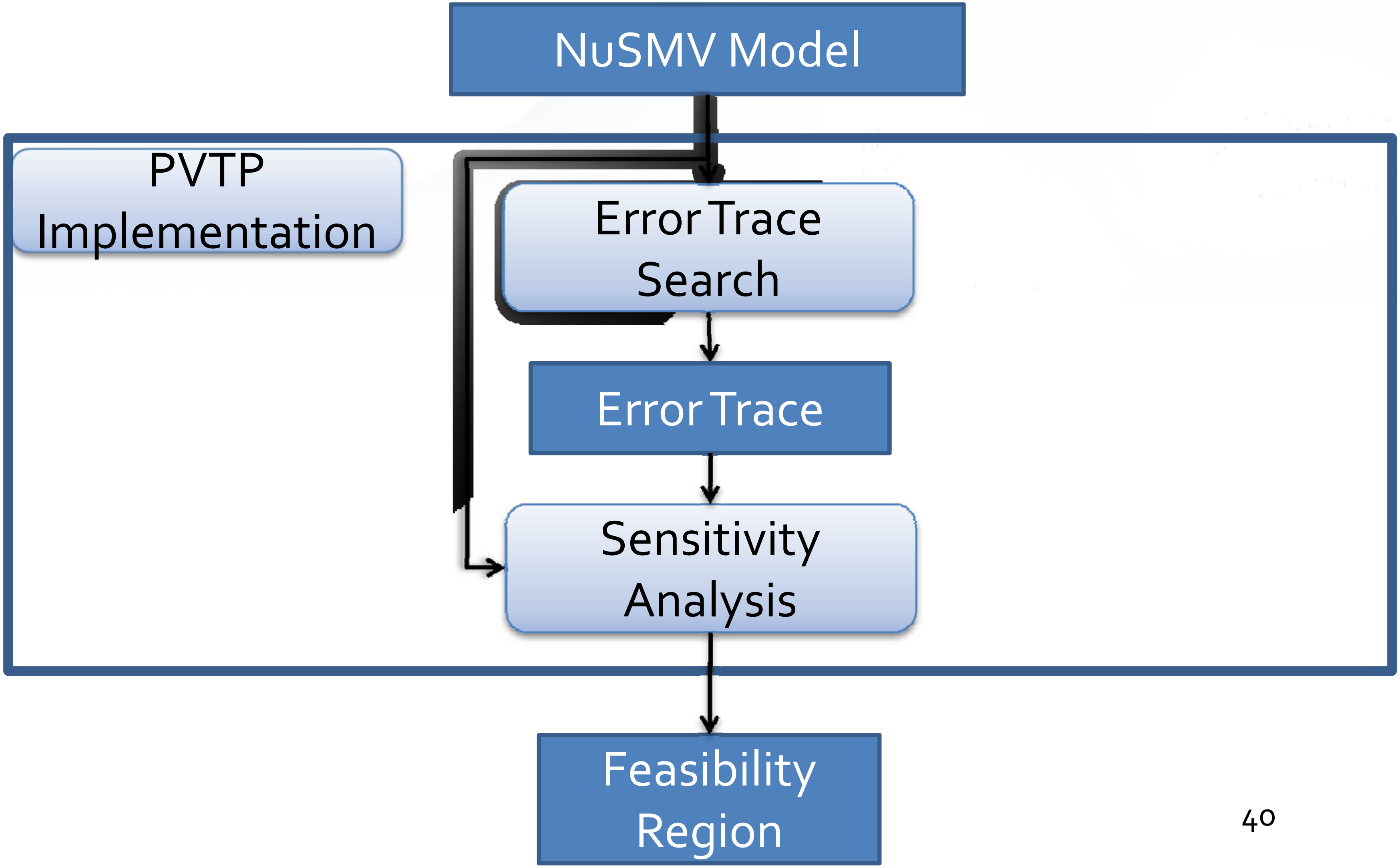
Architecture



UNIVERSITY OF TRENTO - Italy

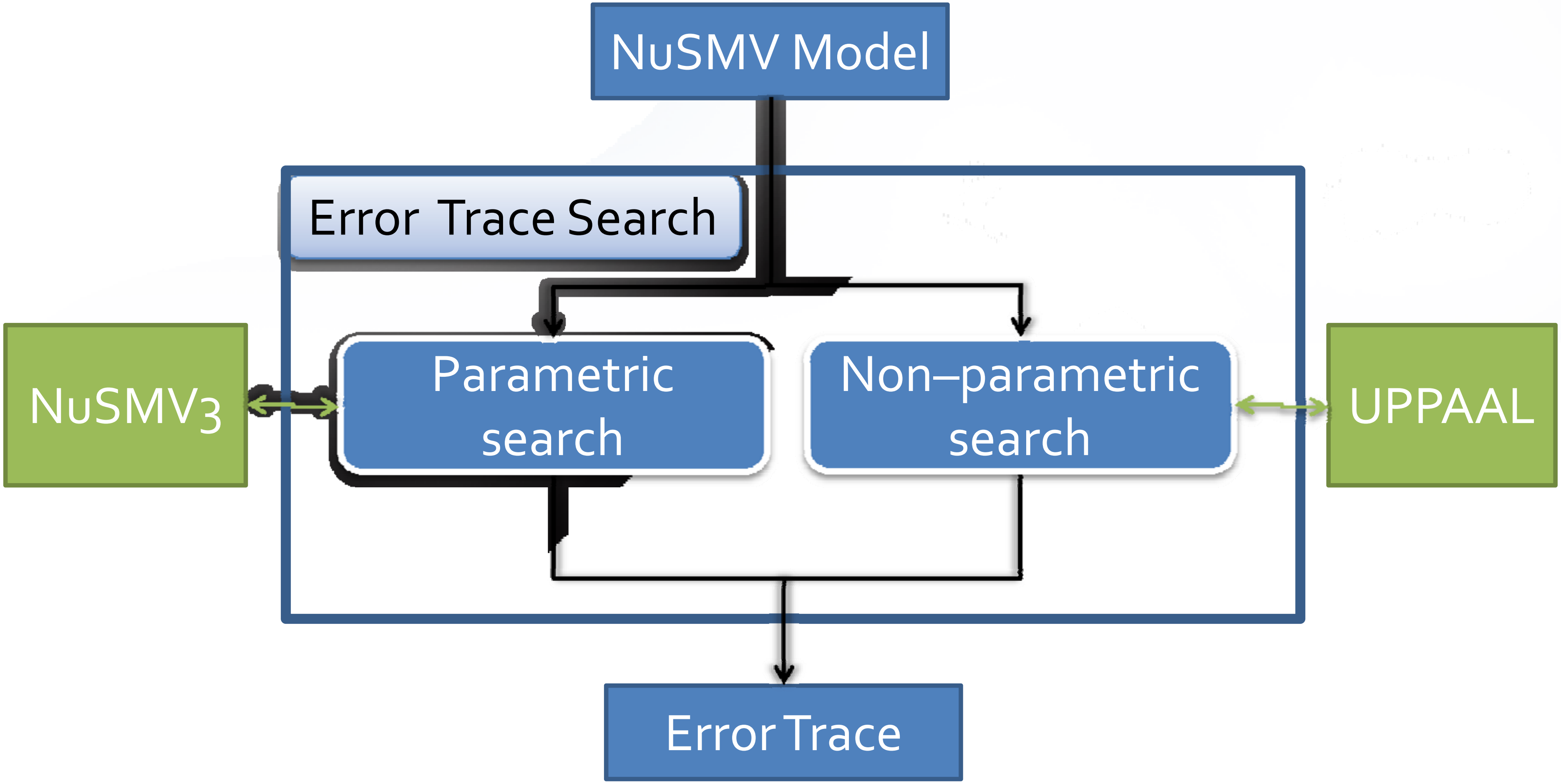
Parametric Verification of Temporal Property Implementation

UNIVERSITY OF TRENTO - Italy

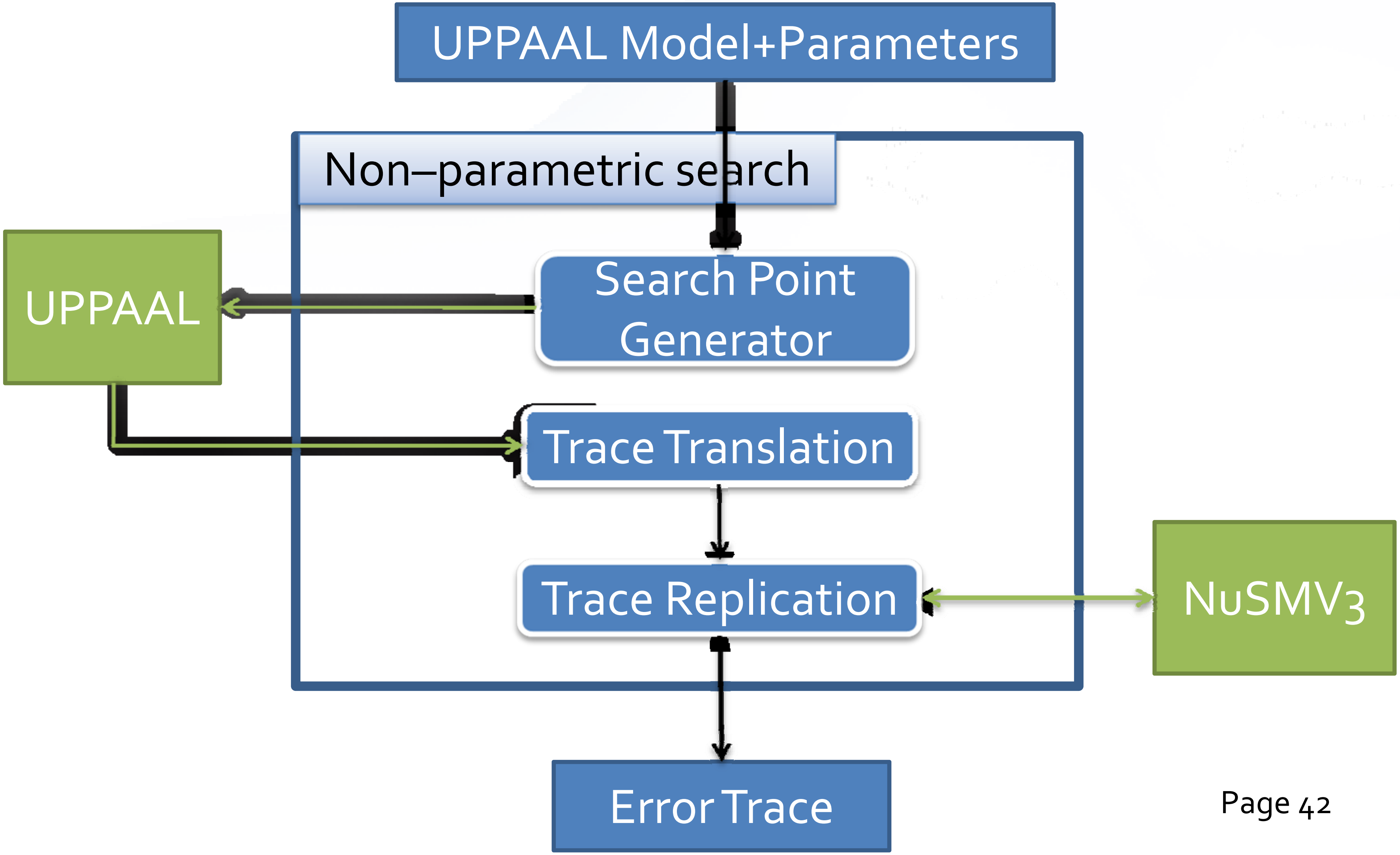


PTVP Algorithm Implementation

UNIVERSITY OF TRENTO - Italy

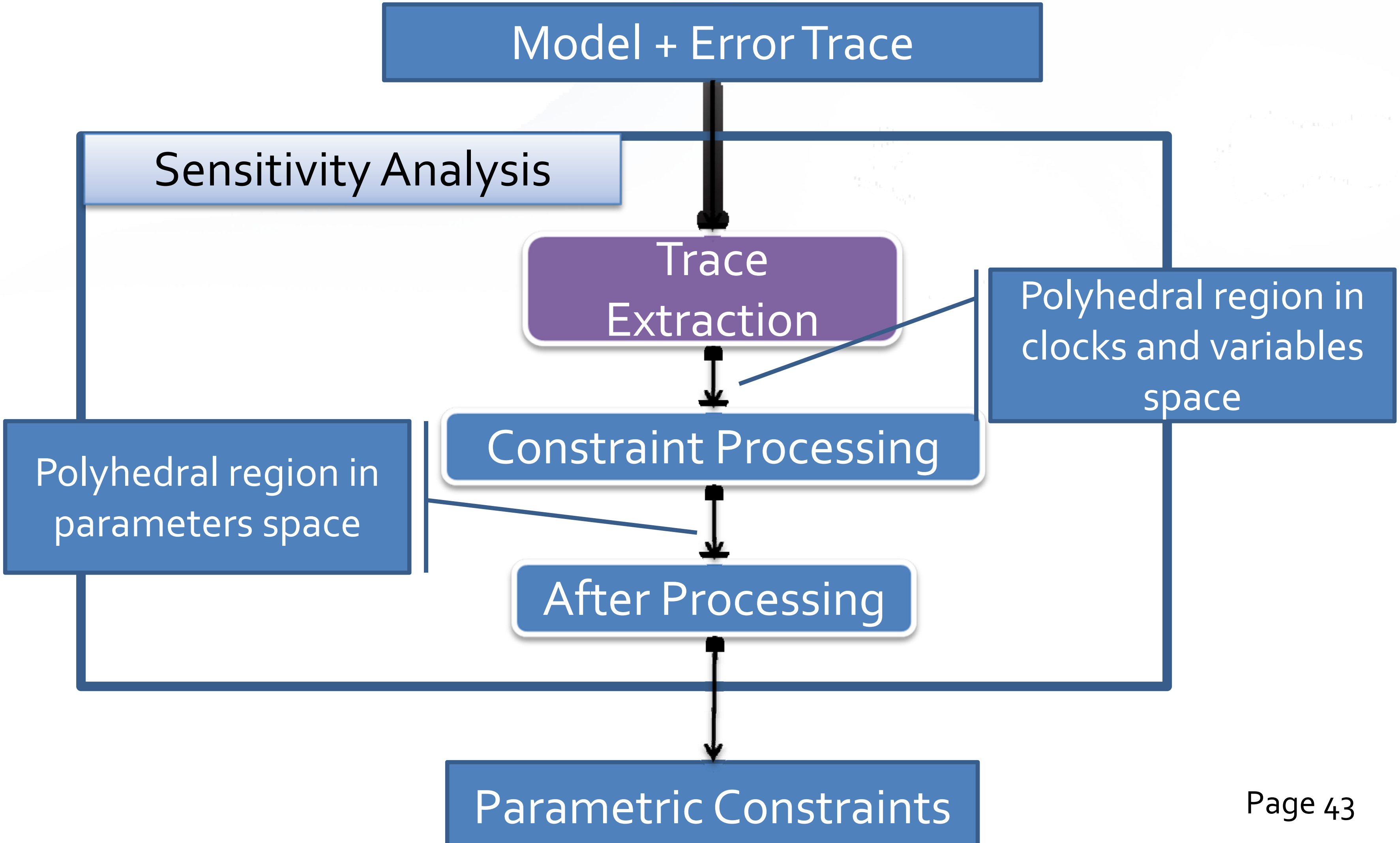


Non-Parametric Search



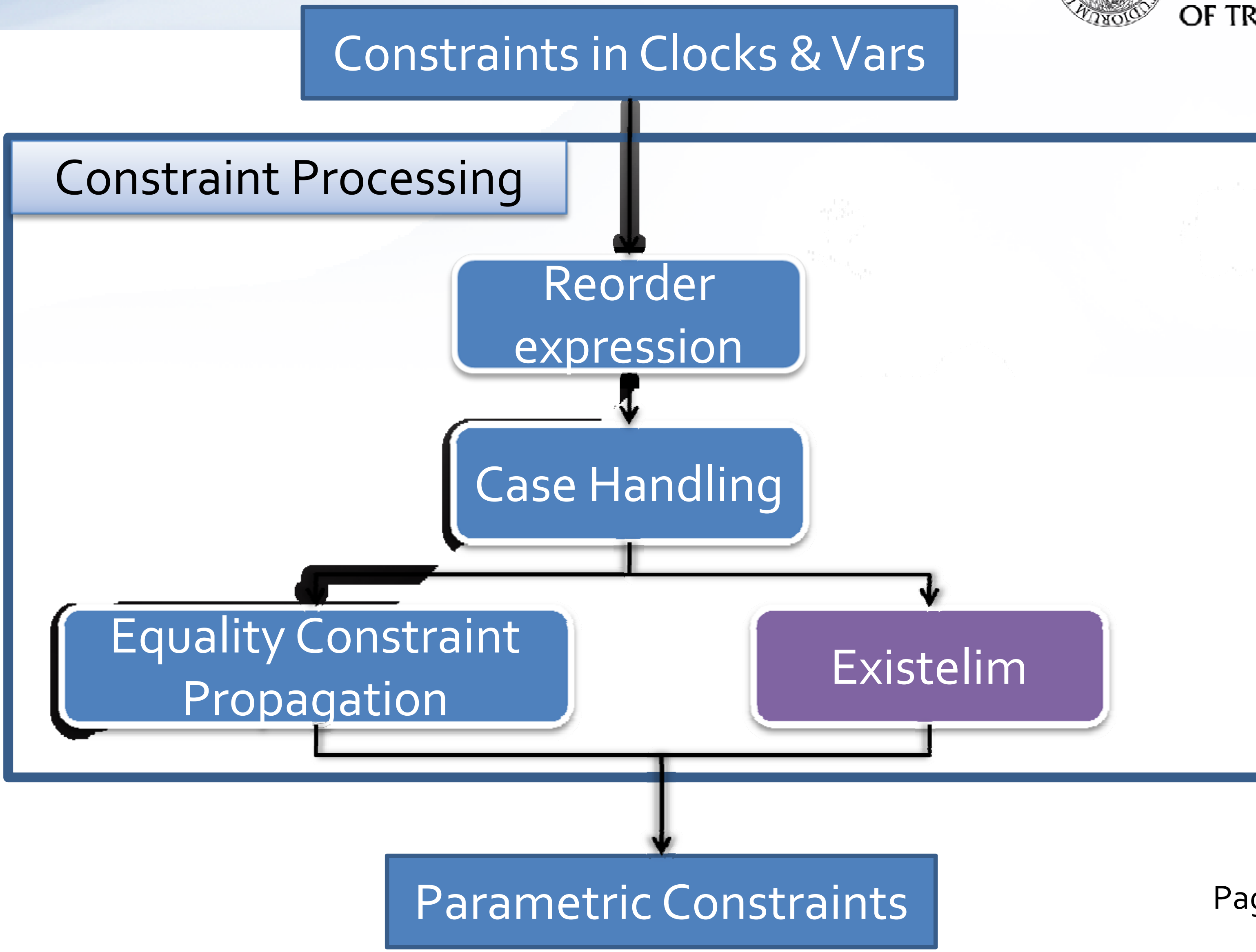
Sensitivity Analysis : Implementation

UNIVERSITY OF TRENTO - Italy



Constraint Processing

UNIVERSITY OF TRENTO - Italy



Presentation Outline

UNIVERSITY OF TRENTO - Italy

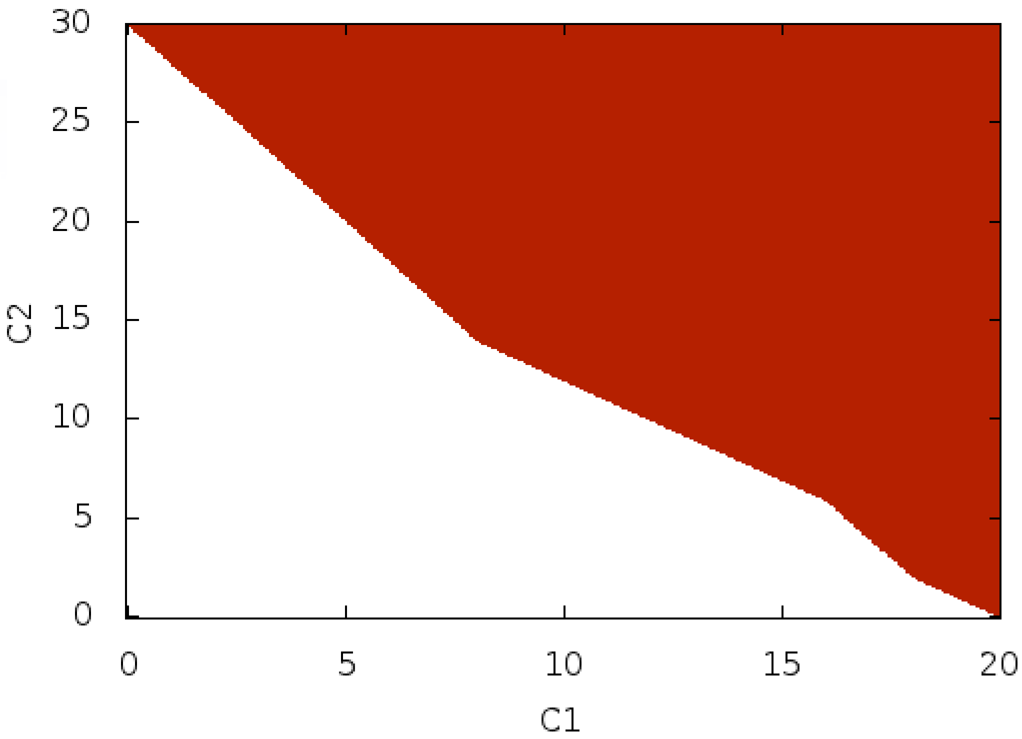
- Motivation
  - Real time system design
  - Example scenario
  - Problem Statement
- Solution
  - Parametric Timed Automata
  - Parametric Verification of Temporal Property Method
- Implementation in Quinq
  - Architecture
  - Demo
- State of the art
- Conclusion

DEMO

- Previously Illustrated example:
  2 periodic tasks system with 3 parameters
- S = {task1, task2}
- Periodic tasks : $T_1=D_1=20$, $T_2=D_2=30$
- Offset : $O_1 = 0$
- Parameters :
  - Computation time: C_1 , C_2
  - Offset : O_2

Demo:result

- Offseta = 8



Presentation Outline

UNIVERSITY OF TRENTO - Italy

- Motivation
  - Real time system design
  - Example scenario
  - Problem Statement
- Solution
  - Parametric Timed Automata
  - Parametric Verification of Temporal Property Method
- Implementation in Quinq
  - Architecture
  - Demo
- State of the art
- Conclusion

Sensitivity Analysis Tools

UNIVERSITY OF TRENTO - Italy

Tool	Flexible RTS	Expression	System known apriori	Inference Point	Number of Parameters	Feasibility Region
Bini	-	-	-	-	No limit	✓
MAST	-	-	-	✓	-	-
SMART	✓	*	✓	-	No limit*	✓
IMITATOR	✓	*	-	✓	2	✓
QUINQ	✓	✓	-	-	No limit*	✓

Presentation Outline

UNIVERSITY OF TRENTO - Italy

- Motivation
  - Real time system design
  - Example scenario
  - Problem Statement
- Solution
  - Parametric Timed Automata
  - Parametric Verification of Temporal Property Method
- Implementation in Quinq
  - Architecture
  - Demo
- State of the art
- Conclusion

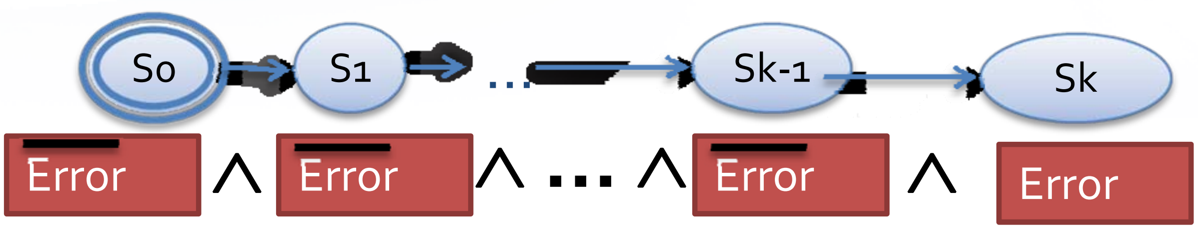
Conclusion

UNIVERSITY OF TRENTO - Italy

- PTA representation → flexible activation pattern , general RTS presentation
- PVTP algorithm → General method to obtain feasibility region
- Implemented in Quinq with applications on some example cases
- Edge on comparison with other tools:
  - Flexible RTS representation
  - No reference point input needed
  - Whole region of schedulability result

K-Induction

- Does there exist k such that the following formula is unsatisfiable



- if *unsatisfiable* and BMC(*k*) *unsatisfiable* then error state unreachable