CISTER
Research Center in
Real-Time & Embedded
Computing Systems

# Technical Report

## Towards Specification and Verification Frameworks for Concurrent Real-Time Systems

**David Pereira**
**André Pedro**
**Luis Miguel Pinho**
**Jorge Sousa Pinto**

CISTER-TR-130109
Version:
Date: 1/28/2013

# Towards Specification and Verification Frameworks for Concurrent Real-Time Systems

David Pereira, André Pedro, Luis Miguel Pinho, Jorge Sousa Pinto

CISTER Research Unit

Polytechnic Institute of Porto (ISEP-IPP)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8340509

E-mail: dmrpe@isep.ipp.pt, anmap@isep.ipp.pt, lmp@isep.ipp.pt,

http://www.cister.isep.ipp.pt

## Abstract

In this work we propose an hybrid verification framework for hard real-time systems. The approach is to use both static and dynamic verification techniques in the sense that dynamic verification is used to address the parts on which static verification fails or is very hard to obtain success.

# Towards the Specification and Verification Frameworks for Concurrent Real-Time Systems

CISTER Research Center in Real-Time & Embedded Computing Systems

HASLab HIGH-ASSURANCE SOFTWARE LABORATORY INESCTEC

David Pereira, André Pedro,
Luís Miguel Pinho, Jorge Sousa Pinto
{dmrpe,anmap,lmp}@isep.ipp.pt, jsp@di.uminho.pt

## The Problem

- Concurrent real-time systems are growing dramatically, both in size and complexity
- Verification, already challenging, is highly impacted from this growth
- Integrated frameworks are fundamental to tackle all the intricacies of these systems
- Formal languages that specify both timed and functional properties (at the source-level)

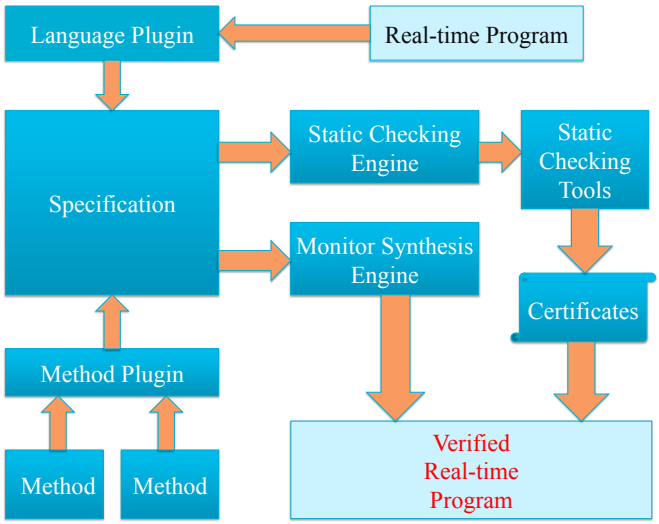
## Proposed Approach

- Support the use of several techniques in cooperation
- Hybrid frameworks: both static and run-time verification
- Address mainly the temporal correctness of source-level, real-time programs
- Programming language independency
- Fostering the use of tools that have been proved valuable (theorem provers, model checkers, deductive verification frameworks)

## Preliminary Ideas

- Regular expressions as formally verified models for lightweight and expressive runtime monitoring systems
- Timed and hybrid logics as a high-level specification for monitoring synthesization
- Integration of both methods (and possibly others in the future) in a single formal specification language
- Focus on real-time design patterns

## The Approach in a Picture




## Example Specification

- Example using temporal logic as underlying method:

```
mon Monitor_A
  head <...>
    gen model l.mtl of X as lmtl; -- Construct Model
  spec
    smemory is lmtl.sat[sread implies true until<=10
        mwrite];
  oper
    set sampled 5 to smemory;
    change smemory period to 5 in checkpoint_1;
```

## Final Remarks

- First prototype of the specification language
- Model of runtime monitor system based on timed regular expressions extended with Boolean assertions
- currently defining a formal logic to express and reason about lazy linear hybrid automata

AVIACC, project FCOMP-01-0124-FEDER-020486. Co-financed by:

COMPETE FCT isep Instituto Superior de Engenharia do Porto INESCTEC