From Verification to Implementation: A Model Translation Tool and a Pacemaker Case Study

Miroslav Pajic, Zhihao Jiang, Insup Lee, Oleg Sokolsky, Rahul Mangharam

1 Model-Driven Development

Goal is to integrate:
- system modeling
- verification
- model-based WCET analysis
- simulation
- code generation
- testing

UPPAAL model → UPP2SF
→ Stateflow model
→ Verification
→ Platform Testing
→ C/C++ Code
→ VHDL/Verilog Code

2 UPP2SF: UPPAAL → Stateflow

Network of UPPAAL automata P₀, P₁, ..., Pₙ

 clk

PO P₁ ... Pn

Eng

Send events

Legend:
- Parallel states
- Exclusive states
- Synchronization over binary and broadcast channels
- Guards and clock invariants
- Committed and urgent states

Translation procedure maps:
- add variable tr_cnt
- resets tr_cnt = tr_cnt + 1
- A[ ]tr_cnt ≤ N

WCET Analysis
- add variable tr_cnt
- resets tr_cnt = tr_cnt + 1
- A[ ]tr_cnt ≤ N

3 Pacemaker Case Study

Pacemaker timing cycles

VP - ventricular pace, VS - ventricular sense, AP - atrial pace, AS - atrial sense.

4 Pacemaker Modeling in UPPAAL

Interaction between the pacemaker and heart

Heart
Ain
Vin
v_p
P0
P1
Pn

Parallel states
Exclusive states

Eng

Verified

UPP2SF
Stateflow model
Simulation

5 Pacemaker Stateflow Design

Legend:
- Parallel states
- Exclusive states
- Guards and clock invariants
- Synchronization over binary and broadcast channels
- Committed and urgent states

Translation procedure maps:
- add variable tr_cnt
- resets tr_cnt = tr_cnt + 1
- A[ ]tr_cnt ≤ N

WCET Analysis
- add variable tr_cnt
- resets tr_cnt = tr_cnt + 1
- A[ ]tr_cnt ≤ N

6 Code Synthesis

Listing 1. bitsForTID0 definition

struct {
  uint_T is_AVI:3;
  uint_T is_LRI:2;
  // ... other variables
}

Listing 2. c1_ChartName procedure

Listing 3. sf_previousEvent

Listing 4. processState

Listing 5. broadcast_tt()

Listing 6. procedure

7 Testing of the Physical Implementation

Real-Time requirements - e.g., Pacing in the atrium:
1. AP cannot occur during the interval 0 ≤ t ≤ LRI₁ - AVI₂
2. If AS does not occur within the interval, AP should occur at t = LRI₁ - LRI₄
3. If AS occurs at t (0 ≤ t ≤ LRI₂ - AVI₁), AP should not be applied in the atrium within the interval 0 ≤ t ≤ LRI₂ - AVI₄

Implementation – on top of the nanoRK RTOS

Test Scenarios