REVERT: A Monitor Generation Tool for Real-Time Systems

CISTER – Research Centre in Real-Time & Embedded Computing Systems

Sangeeth Kochanthara, Geoffrey Nelissen, David Pereira, Rahul Purandare
sangeeth1455@iiitd.ac.in, {grrpn,dmrpe}@isep.ipp.pt, purandare@iiitd.ac.in

Runtime Verification of Real-Time Systems

Limitations of classic (static) approaches:

- Number of reachable states too large for testing
- Potential blow-up when automatically exploring the system's state-space (e.g., model-checking)
- Limited automation in machine assisted proof construction tools (e.g., SMT solvers, proof-assistants)
- Difficulties in capturing data expected to be available only at run-time (need for abstraction leads to lack of precision)

Limitations of existing Runtime Verification solutions:

- Vast majority of tools developed for non-real-time applications;
- In most cases, it is difficult to capture extra-functional properties:
  - either no support at all; or
  - via complex specifications that are not accessible for the non-expert or the typical industrial practitioner
- Lack of a specification language that is user friendly, and that allows to capture distinct classes of timing properties

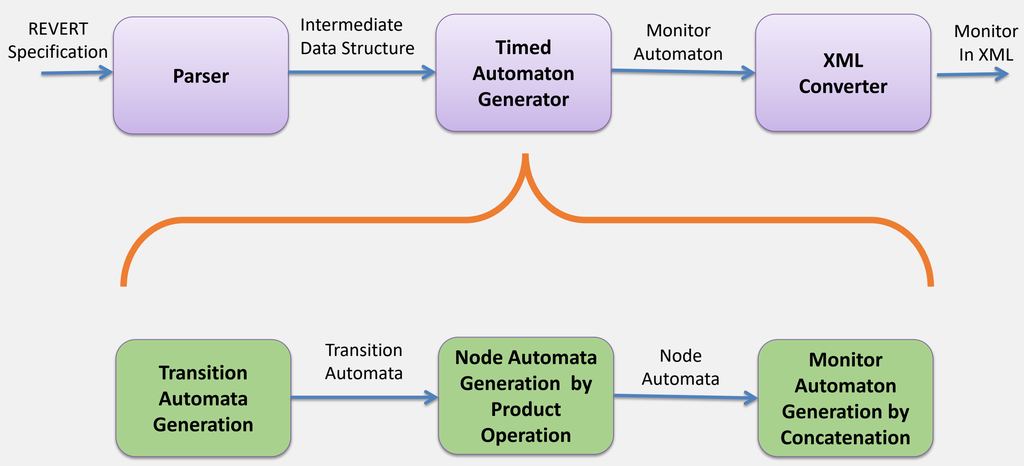
The REVERT Framework

1) A new specification language:

- Intuitive, easy to use domain specification language
- Capture changes in the system via guarded state-machine transitions between nodes (monitor states)
- Functional behavior as extended regular expressions
- Support for associating events with job specifications
- Three classes of timing constraints relevant for real-time systems: time, duration and jitter.
  - Timing constraint on sequences of events,
  - Execution time of a job,
  - Jitter on time and duration.
- Local variables and local code (e.g., for monitor initialization, calling counter-measure actions, etc)

2) A new monitor generation process:

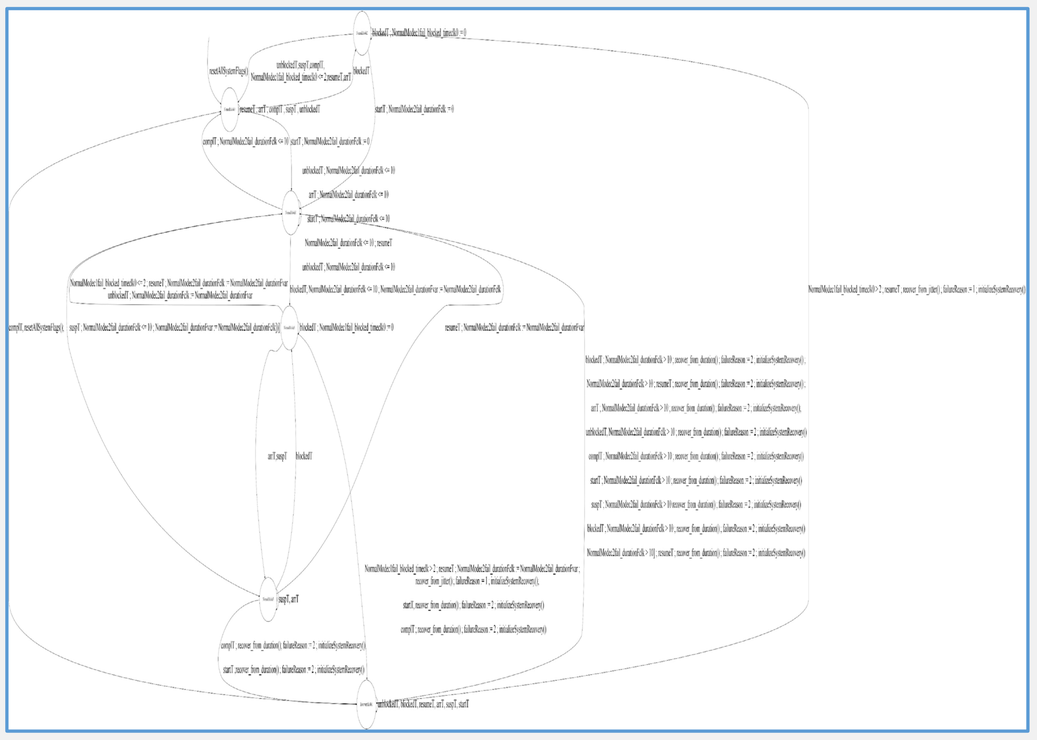
1. REVERT specifications are parsed into intermediate data-structure;
2. Generation of the corresponding automata (via combination of intermediate types of finite automata)
3. Translation of the generated timed state-machine into XML format



Example REVERT specification

```
use "T_Events.ev";
use "Ext_Procs.h";

monitor MyMon {

   observe { arrT, startT, suspT, blockedT,
             resumeT, unblockedT, complT }

variables { failureReason : integer; }

jobs {
   Job1 {
     start: {startT}
     suspend: {suspT, blockedT}
     resume: {resumeT, unblockedT}
     complete: {complT}
   }
}

nodes { NormalMode, RecoveryMode }
initial { NormalMode }

node NormalMode {
   init{
     resetAllSystemFlags();
   }
   constraints {
      c1: time(blockedT resumeT)) ≤ 2;
      c2: duration(Job1) ≤ 10;
   }
   transitions {
      fail_blocked_time: failure(c1) →
RecoveryMode {
         failureReason := 1;
         recover_from_blocking();
      }
      fail_duration: failure(c2) → RecoveryMode {
         failureReason := 2;
         recover_from_duration();
      }
   }
}
node RecoveryMode {
   init{
      initializeSystemRecovery();
   }
   constraints {
      c1[ERE]: _ complT;
   }
   transitions {
      job_completion: success(c1) →
NormalMode;
   }
}
}
```

Generated Monitor Diagram



Generated Monitor XML

- Generate the corresponding code from the XML in order to make the monitor execution online, together with the target monitored system;
- Use the monitor to verify traces offline and therefore detect unexpected/unkown behaviors
- Overall, improve the reliability and trust on the target system

Concluding Remarks

- New specification language for runtime verification of RTSs
- Novel method to generate timed finite state machines that avoids state blowup in run-time
- Implemented the framework as a tool-chain

CISTER Research Unit (CEC/04234), co-financed by:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundos Europeus Estruturais e de Investimento FCT Fundação para a Ciência e a Tecnologia

CISTER Research Centre/INESC-TEC
ISEP, Polytechnic Institute of Porto
Rua Dr. Antº Bernardino de Almeida, 431
4249-015 Porto, Portugal
+351 228 340 502
www.cister.isep.ipp.pt
cister-info@isep.ipp.pt
facebook.com/cisterrealtime