Research at the SW Technologies Lab
(Time Petri Nets nella verifica e valutazione di sistemi real-time)

Giacomo Bucci, Laura Carnevali, Luigi Sassoli, Enrico Vicario
Sw Technologies Lab, Dept.Sistemi e Informatica, University of Florence
vicario@dsi.unifi.it, www.dsi.unifi.it/~vicario
People

- G.Bucci, E.Vicario, A.Fantechi

Collaborations

- Galileo Avionica, Regione Toscana, GE Transportation Systems, Marelli
- I+, Rigel, Planet, Rinascimento Digitale, ITTIG.CNR, ISTI.CNR
- Polo biotecnologico di unifi, Azienda Ospedaliera Careggi, …
3 main areas of expertise

- **SW architectures and development practices (Bucci, Vicario)**
  - Enterprise architectures and application interoperability (eGovernment)
  - Ontological architectures and applications
  - Workflow management architectures
  - OO Testing
  - Focus on experimentation, development capability, technology transfer

- **Qualitative verification and quantitative evaluation (Bucci, Vicario)**
  - Nondeterministic/stochastic, timed, reactive systems
    - Time Petri Nets, preemptiveTPN, stochasticTPN, …
    - Symbolic state space analysis
  - Real time testing

- **Formal modelling of embedded safety critical systems (Fantechi)**
  - Specific focus on railway signaling systems
  - Model driven development
    - modeling, model checking, automatic code generation, code deployment on target, system testing
  - Experimentation with commercial modelling tools
    - IAR Visualstate, Ilogix Statemate, Matlab Stateflow, Esterel Tech.SCADE
Verification of reactive, timed, non deterministic systems

- Sequencing of events
- Min-max time between events
Reactive, dense timed, non-deterministic, non-preemptive systems
Symbolic state space analysis
  - State classes, Difference Bound Matrix, symbolic runs

IEEE TSE01: vicario
Preemptive Time Petri Nets (pTPN)

- Represents suspension
  - breaks DBM encoding
- Tight DBM approximation,
- Selection of critical paths and clean-up of false behaviors

IEEE TSE04: bucci, fedeli, sassoli, vicario
Communicating Time Petri Nets (cmTPN)

- Modular decomposition
  - TPN without preemption
- Separate state space enumeration, required/provided interface
- Projection and composition

IEEE TSE95: bucci, vicario
Exploit theory of pTPN to support design and testing
Integration in process standards
- RTCA 178B, V-model, …
- architecture design and validation,
- disciplined coding, execution time profiling
- test case selection, sensitization, oracle, coverage analysis
- Collaboration with Galileo Avionica

Experimentation on Linux-RTAI

ECRTS07, ETFA07: carnevali, sassoli, vicario
Quantitative evaluation of stochastic reactive timed systems

- Associate non-determinism with a stochastic characterization
  - Instantaneous choices
  - Temporal parameters
- Provide a measure of probability for alternative behaviors
  - Symbolic runs
  - Run timings
Time intervals associated with general distribution

Discrete time
  - Maximal step semantics, confusion and well definedness

Stochastic state transition system
  - Embeds a Discrete Time Markov Chain
  - Joint verification of possible behaviors and evaluation of their probability
  - E.g. overrun handling policies: correctness and efficiency

IEEE TSE05: bucci, sassoli, vicario
stochastic Time Petri Nets

- Dense time, no preemption
- Extend state classes with state density
  - symbolic calculus of density functions
  - Mathematica API, c++ implementation for exp-polynomial distributions

Stochastic extension of the class graph
- regeneration classes and boundedness
- Markov renewal theory, Continuous Time Markov Chain

QEST05, QEST06, QEST07: bucci, sassoli, vicario
- Main work under revision at IEEE TSE: sassoli, vicario
All results implemented in the ORIS tool

- Plug-in architecture
- C++/Java
- http://www.stlab.dsi.unifi.it/oris/index.html
Research at the SW Technologies Lab
(Time Petri Nets nella verifica e valutazione di sistemi real-time)

Giacomo Bucci, Laura Carnevali, Luigi Sassoli, Enrico Vicario
Sw Technologies Lab, Dept.Sistemi e Informatica, University of Florence
vicario@dsi.unifi.it, www.dsi.unifi.it/~vicario