Qualitative verification and quantitative evaluation of timed concurrent systems

Laura Carnevali

Dipartimento di Ingegneria dell'Informazione, Università di Firenze
laura.carnevali@unifi.it - http://stlab.dinfo.unifi.it/carnevali

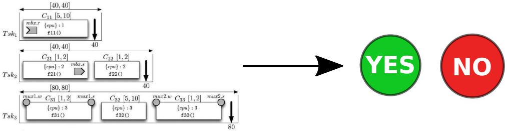
Firenze - April 16, 2019

Short bio

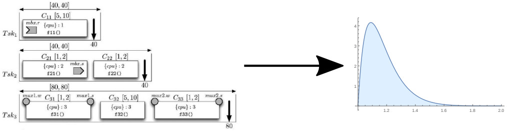
- Educazione
  - 2001–2004: Laurea in Ingegneria Informatica
  - 2004–2006: Laurea specialistica in Ingegneria Informatica
  - 2007–2010: Dottorato in Ingegneria Informatica, Multimedialità e Telecomunicazioni
- Posizioni accademiche
  - 2010–2013: Assegnista di ricerca
  - 2013–2016: Ricercatore a Tempo Determininato - Tipologia A
  - 2016–2019: Ricercatore a Tempo Determininato - Tipologia B
- Periodi di ricerca all'estero
  - 2014 (marzo–giugno): École normale supérieure de Cachan, Paris, France
- Abilitazioni
  - 2015: Abilitazione scientifica nazionale, seconda fascia, s.c. 09/H1 (s.s.d. ING-INF/05)
- Didattica
  - 2011–2013: Fondamenti di Informatica, Laurea in Ingegneria Meccanica (6 CFU)
  - 2013– . . . : Fondamenti di Informatica, Laurea in Ing. Elettronica e delle Telecom. (9 CFU)
  - Berretti, Carnevali, Vicario, "Fondamenti di programmazione", 2017.
- Partecipazione a progetti di ricerca e trasferimento tecnologico
  - Progetti europei: REMIND
  - Progetti regionali e nazionali: LINFA, INDIGO, GENIALE, ERNESTO, REICA, WISEDEMON, . . .
  - Progetto di ateneo NEW-ERTMS (in collaborazione con Enrico Meli - DIEF)
  - Collaborazioni con aziende: NEC Corporation (Japan), Visia Imaging s.r.l (Arezzo), . . .

Main research interests

1. **Qualitative** verification of timed concurrent systems
(*will a task miss its deadline or not?*)
    - Integration of formal methods in the life cycle of real-time software
    - Qualitative verification of hierarchical scheduling systems
    - Application to an industrial development process

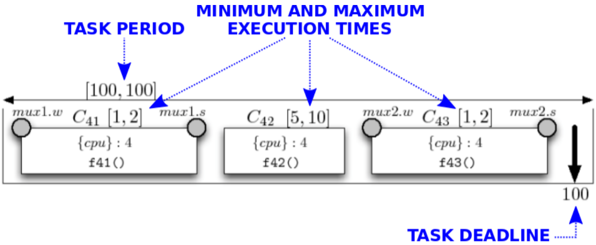


2. **Quantitative** evaluation of timed concurrent systems
(*which is the probability that a task misses its deadline?*)
    - Stochastic analysis of models with multiple concurrent non-Markovian timers
    - Input generation in testing of real-time stochastic systems
    - Application to performance and reliability analysis in various contexts
        - Performability evaluation of communication protocols in railway systems
        - Performability evaluation of cyber-physical systems during repair
        - Activity recognition in partially observable systems



1) Qualitative verification of timed concurrent systems: goal, motivation, challenges

- Integration of formal methods within the development cycle of real-time SW
  - Encouraged by certification standards, e.g., RTCA/DO-178B [1,2]
  - Provided that consolidated industrial practices are not disrupted
  - Addressed by Model Driven Development (MDD) approaches
- Faces different theoretical and practical challenges
  - Faces the effects of concurrency, timing, and suspension
  - Faces the gap between formal domains and industrial practices
- *An example referred to SW design: will a task miss its deadline or not?*



MINIMUM AND MAXIMUM EXECUTION TIMES

TASK PERIOD

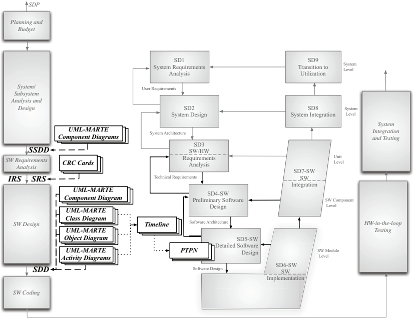
TASK DEADLINE

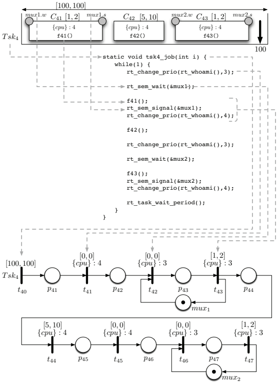
[1] RTC for Aeronautics, DO-178B, Software Considerations in Airborne Systems and Equipment Certification, 1992

[2] RTC for Aeronautics, DO-178C, Software Considerations in Airborne Systems and Equipment Certification, 2012

A methodology for integration of formal methods within the SW development cycle [3]

- V-Model tailored according to MIL-STD-498 [4]
  - Uses preemptive Time Petri Nets (pTPNs) [5] to support development (V-Model)
  - Uses UML-MARTE [6] to support documentation (MIL-STD-498)
- Application to an industrial development process at Selex ES - Firenze (now Leonardo) [7]





```
static void tsk4_job(int i) {
   while(1) {
      rt_change_prio(rt_whoami(),3);

      rt_sem_wait(&mux1);

      f41();
      rt_sem_signal(&mux1);
      rt_change_prio(rt_whoami(),4);

      f42();

      rt_change_prio(rt_whoami(),3);

      rt_sem_wait(&mux2);

      f43();
      rt_sem_signal(&mux2);
      rt_change_prio(rt_whoami(),4);

      rt_task_wait_period();
   }
}
```

[3] Carnevali, Ridi, Vicario, "Putting preemptive Time Petri Nets to work in a V-Model SW life cycle", IEEE Trans. on Software Engineering, 2011

[4] US Department of Defense," MIL-STD-498, Military standard for sw development and documentation", Tech. rep., USDoD, 1994

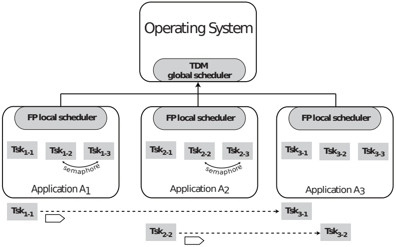
[5] Bucci, Fedeli, Sassoli, Vicario, "Timed state space analysis of real-time preemptive systems", IEEE Trans. on Software Engineering, 2004

[6] Object Managem. Group, "UML Profile for MARTE: Modeling and Analysis of Real-Time Embedded systems v1.0", 2009.

[7] Bicchierai, Bucci, Carnevali, Vicario, "Combining UML-MARTE and preemptive Time Petri Nets: An Industrial Case Study", IEEE Trans. Industrial Inform., 2013

Compositional verification of Hierarchical Scheduling (HS) systems [8]

- Addressing the ARINC-653 standard [9]
- Facing concurrency and timing in design and verification
  - Sequencing of events (e.g., mutual exclusion, deadlocks, inter-component interactions)
  - Timing of events (e.g., min-max execution times, deadlines)
- Leverages the theory of preemptive Time Petri Nets (pTPNs)
  - Exact verification of intra-application constraints
  - Approximate but safe verification of inter-application constraints
- Experimentation on avionic systems of real complexity (15 concurrent tasks) [10]



Appl.	Slot	Slot length	Task	Release	Offset	Jitter	Deadline	Chunk	Prio	Exec. Time	Sem	Mbx
A_1	T_1	3	Tsk_{11}	[10, 10]	0	[0, 0]	5	C_{111}	2	[**0.6**, **0.8**]	-	-
			Tsk_{12}	[40, 40]	0	[**0**, **1**]	40	C_{121}	3	[**1.0**, **1.2**]	-	-
								C_{122}	3	[**0.2**, **0.4**]	-	**mbx**$_{11}$(r)
			Tsk_{13}	[40, 40]	**10**	[**0**, **2**]	40	C_{131}	4	[**1.8**, **2.3**]	-	-
								C_{132}	4	[**0.6**, **0.9**]	-	**mbx**$_{11}$(s)
			Tsk_{14}	[**40**, ∞)	**20**	[0, 0]	40	C_{141}	5	[**1.1**, **1.4**]	-	-
								C_{142}	5	[**0.1**, **0.2**]	-	-
A_2	T_2	4	Tsk_{21}	[**40**, ∞)	0	[0, 0]	40	C_{211}	2	[**0.2**, **0.3**]	**mux**$_{21}$	-
								C_{212}	2	[**0.4**, **0.5**]	-	-
			Tsk_{22}	[50, 50]	0	[**0**, **1**]	50	C_{221}	3	[**4.6**, **6.1**]	-	-
								C_{222}	3	[**0.2**, **0.3**]	**mux**$_{21}$	-
			Tsk_{23}	[50, 50]	0	[**0**, **2**]	50	C_{231}	4	[**3.4**, **4.4**]	-	-
								C_{232}	4	[**0.2**, **0.4**]	**mux**$_{22}$	-
			Tsk_{24}	[50, 50]	**16**	[0, 0]	50	C_{241}	5	[**4.7**, **6.1**]	-	-
								C_{242}	5	[**0.1**, **0.3**]	**mux**$_{22}$	-
A_3	T_3	1	Tsk_{31}	[80, 80]	2	[0, 0]	80	C_{311}	2	[**3.6**, **4.8**]	-	-
			Tsk_{32}	[100, ∞)	**15**	[0, 0]	100	C_{321}	3	[**0.4**, **0.5**]	-	-
A_4	T_4	1	Tsk_{41}	[100, 100]	0	[**0**, **2.5**]	100	C_{411}	2	[**3.4**, **4.2**]	-	-
								C_{412}	2	[**0.8**, **1.4**]	**mux**$_{41}$	-
			Tsk_{42}	[**200**, ∞)	**10**	[0, 0]	200	C_{421}	3	[**0.4**, **0.5**]	-	-
								C_{422}	3	[**0.2**, **0.3**]	**mux**$_{41}$	-
A_5	T_5	1	Tsk_{51}	[200, 200]	**10**	[0, 0]	200	C_{511}	2	[**1.2**, **1.6**]	-	-
			Tsk_{52}	[**400**, ∞)	**3**	[0, 0]	400	C_{521}	3	[**3.6**, **4.8**]	-	-
			Tsk_{53}	[1000, 1000]	0	[**0**, **2**]	1000	C_{531}	4	[**3.0**, **4.0**]	-	-

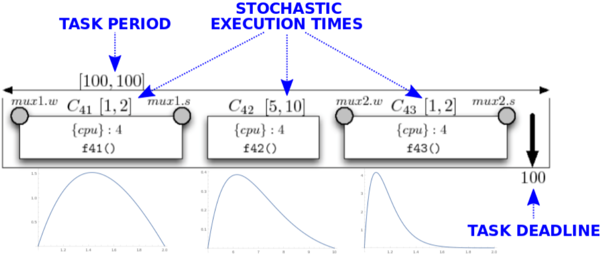
[8] Carnevali, Pinzuti, Vicario, "Compositional verification for Hierarchical Scheduling of Real-Time systems", IEEE Trans. on Software Engineering, 2013

[9] Avionics Electronic Engineering Committee (ARINC). "Avionics application software standard interface: Part 1 - required services". Technical report, 2006

[10] Locke, Vogel, Lucas, "Generic avionics software specification", Technical report, Software Engineering Institute, Carnegie Mellon University, 1990

2) Quantitative evaluation of timed concurrent systems: goal, motivation, challenges

- Quantitative evaluation of models with multiple concurrent non-Markovian timers
  - High variability in timed behavior is frequent (e.g., event-triggered systems)
  - Analysis based on Worst Case Execution Times (WCETs) yields too pessimistic results
  - RAMS requirements: not only Safety, but also Reliability, Availability, Maintainability
- Faces different theoretical and practical challenges
  - Non-Markovian temporal parameters keep *memory* of past history
  - Trade-off between the model expressivity and the analysis complexity
- *An example referred to SW design: which is the probability that a task misses its deadline?*

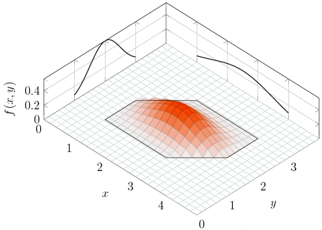

TASK PERIOD

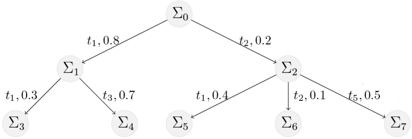
STOCHASTIC EXECUTION TIMES

TASK DEADLINE

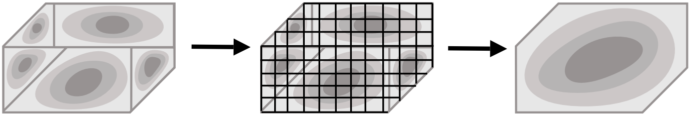
The method of stochastic state classes [11,12]

- Computes the joint Probability Density Function (PDF) of the active timers after each event
    - Timers may have a non-Markovian (i.e., non-Exponential) PDF possibly with bounded domain
    - Representation of bounded execution times, jitters, deadlines, periodic releases, timeouts, . . .





- Complexity can be reduced by approximating PDFs through Bernstein polynomials

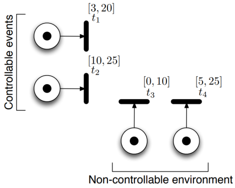


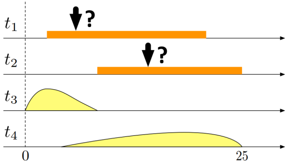
[11] Vicario, Sassoli, Carnevali, ”Using Stochastic State Classes in Quantitative Evaluation of Dense-Time Reactive Systems“, IEEE Trans. Software Eng., 2009

[12] Carnevali, Grassi, Vicario, ”State-Density Functions over DBM Domains in the Analysis of Non-Markovian Models“, IEEE Trans. Software Eng., 2009

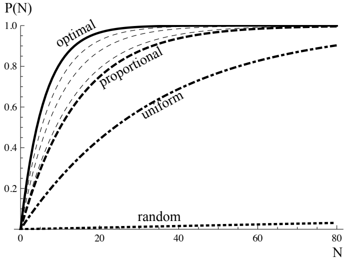
Testing of real-time stochastic systems: the problem of input generation [13]

- Temporal parameters of a real-time system can be *controllable* or *non-controllable*





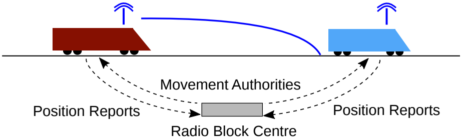
- Derives the probability of *conclusive* test execution as a function of controllable parameters
- Reduces the number of test repetitions with respect to random testing



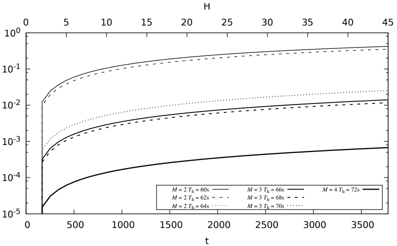
[13] Carnevali, Ridi, Vicario, "A Quantitative Approach to Input Generation in Real-Time Testing of Stochastic Systems", IEEE Trans. Software Engineering, 2013

Performability evaluation of the ERTMS/ETCS - Level 3 [14]

- ERTMS/ETCS - Level 3: an innovative standard for train signalling and traffic management
  - *Moving-block signalling*: trains check position and integrity autonomously
  - Continuous bidirectional (track ↔ train) mobile communication
  - Braking curve recomputed continuously ⇒ increased maximum speed, capacity gains



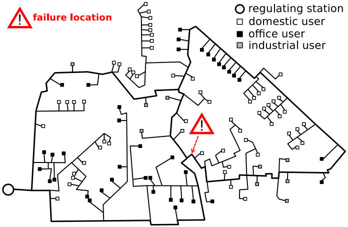
- Goal: evaluate the first-passage time distribution to a *spurious* emergency brake
  - Evaluation within 2 hyper-periods (periodic Position Reports + periodic handovers) is enough

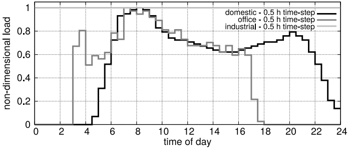


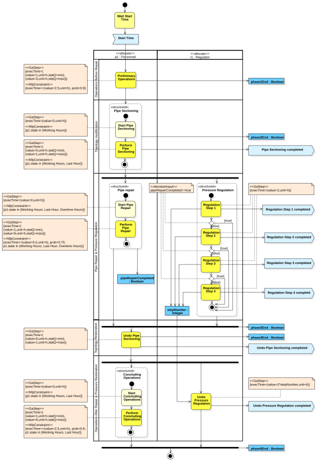
[14] Biagi, Carnevali, Paolieri, Vicario, "Performability evaluation of the ERTMS/ETCS - Level 3", Transportation Research Part C: Emerging Technologies, 2017

Performability evaluation of gas distribution networks during repair procedures [15]

- Gas networks couple *physical* fluid-dynamics with *cyber* management procedures
- Goal: evaluate the *low pressure risk* in the transient phase after a repair
  - Combine fluid-dynamic analysis of gas behavior and stochastic analysis of repair actions



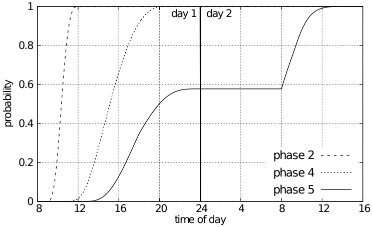


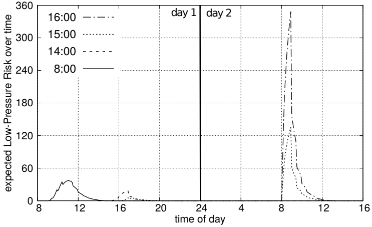

Wait Start Time
Start Time
<<allocate>> p1 : Personnel
<<allocate>> r1 : Regulator
Operations Before Repair
<<GaStep>> {execTime=({value=1,unit=h,statQ=min), {value=3,unit=h,statQ=max)}} <<NfpConstraint>> {execTime<=(value=2.5,unit=h), prob=0.9}
Preliminary Operations
phase1End : Boolean
Topology modification
«structured» Pipe Sectioning
<<GaStep>> {execTime=(value=0,unit=h)} <<NfpConstraint>> {p1.state in {Working Hours}}
Start Pipe Sectioning
<<GaStep>> {execTime=({value=0,unit=h,statQ=min), {value=1,unit=h,statQ=max)}} <<NfpConstraint>> {p1.state in {Working Hours, Last Hour}}
Perform Pipe Sectioning
phase2End : Boolean
Pipe Sectioning completed
Pipe Repair & Pressure Regulation
«structured» Pipe repair
<<GaStep>> {execTime=(value=0,unit=h)} <<NfpConstraint>> {p1.state in {Working Hours, Last Hour, Overtime Hours}}
Start Pipe Repair
<<GaStep>> {execTime=({value=1,unit=h,statQ=min), {value=9,unit=h,statQ=max)}} <<NfpConstraint>> {execTime<=(value=5.5,unit=h), prob=0.75; p1.state in {Working Hours, Last Hour, Overtime Hours}}
Perform Pipe Repair
pipeRepairCompleted : Boolean
<<decisionInput>> pipeRepairCompleted==true
«structured» Pressure Regulation
<<GaStep>> {execTime=(value=2,unit=h)}
Regulation Step 1
Regulation Step 1 completed
[true]
[false]
Regulation Step 2
Regulation Step 2 completed
[true]
[false]
Regulation Step 3
Regulation Step 3 completed
[true]
[false]
Regulation Step 4
Regulation Step 4 completd
stepNumber : Integer
phase3End : Boolean
Topology Restoration
<<GaStep>> {execTime=({value=0,unit=h,statQ=min), {value=1,unit=h,statQ=max)}
Undo Pipe Sectioning
phase4End : Boolean
Undo Pipe Sectioning completed
Operations After Repair & Pressure Restoration
«structured» Concluding Operations
<<GaStep>> {execTime=(value=0,unit=h)} <<NfpConstraint>> {p1.state in {Working Hours, Last Hour}}
Start Concluding Operations
<<GaStep>> {execTime=({value=1,unit=h,statQ=min), {value=6,unit=h,statQ=max)} <<NfpConstraint>> {execTime<=(value=2.5,unit=h), prob=0.6; p1.state in {Working Hours, Last Hour}}
Perform Concluding Operations
<<GaStep>> {execTime=(value=2*stepNumber,unit=h)}
Undo Pressure Regulation
Undo Pressure Regulation completed
phase5End : Boolean

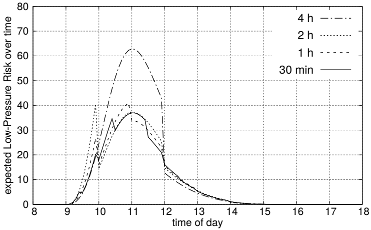
[15] Biagi, Carnevali, Tarani, Vicario, "Model-based quantitative evaluation of repair procedures in gas distribution networks", ACM Tran. Cyber-Phys. Sys., 2018

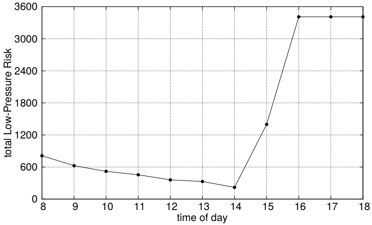
Performability evaluation of gas distribution networks during repair procedures [15]

- Gas networks couple *physical* fluid-dynamics with *cyber* management procedures
- Goal: evaluate the *low pressure risk* in the transient phase after a repair
  - Combine fluid-dynamic analysis of gas behavior and stochastic analysis of repair actions





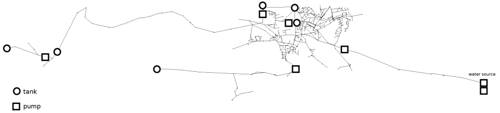


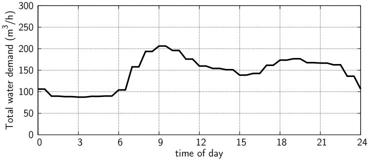


[15] Biagi, Carnevali, Tarani, Vicario, "Model-based quantitative evaluation of repair procedures in gas distribution networks", ACM Tran. Cyber-Phys. Sys., 2018

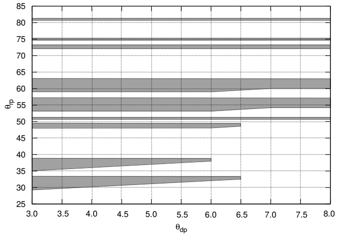
Performability evaluation of water distribution systems during repair procedures [16]

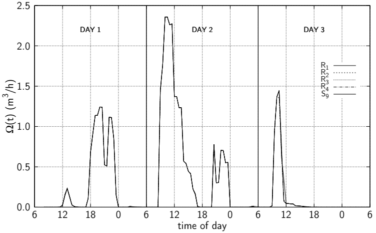
- A more complex problem referred to the class of *stochastic hybrid systems*
  - Water distribution systems feature a *continuous* and a *discrete* dynamics
  - Water level in tanks comprises a continuous element of *memory*
  - Topology and operation mode can be changed at *stochastic* time points





- Goal: evaluate the *expected demand not served* in the time after a repair
  - Combine fluid-dynamic analysis of gas behavior and stochastic analysis of repair actions

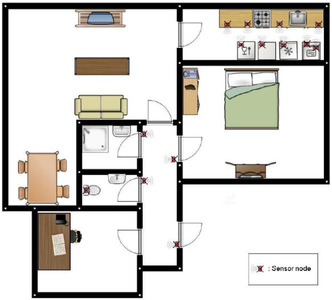


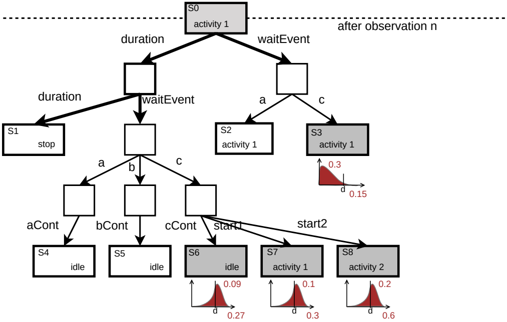


[16] Carnevali, Tarani, Vicario, "Performability evaluation of water distribution systems during maintenance procedures", IEEE Trans. Sys. Man Cyb., accepted

Activity Recognition (AR) in Ambient Assisted Living (AAL) [17]

- Monitoring of *high level* human activities through *low-level* observations by sensors
- A *continuous-time model-based* approach
  - A stochastic model is rejuvenated by *runtime* (typed and time-stamped) observations
  - Transient analysis of the model provides a likelihood for the possible current activities
- A kind of *continuous-time* extension of Hidden Markov Models (HMMs)





[17] **Biagi, Carnevali, Paolieri, Patara, Vicario, "A continuous-time model-based approach for activity recognition in pervasive environments", IEEE Transactions on Human-Machine Systems, accepted**

Some references

- Qualitative verification of real-time concurrent systems
  - I. Bicchierai, G. Bucci, L. Carnevali, and E. Vicario, "Combining UML-MARTE and preemptive Time Petri Nets: An Industrial Case Study", IEEE Transactions on Industrial Informatics, vol. 9, no. 4, pp. 1806-1818, November 2013.
  - L. Carnevali, L. Ridi, and E. Vicario, "Putting Preemptive Time Petri Nets to Work in a V-Model SW Life Cycle", IEEE Transactions on Software Engineering, vol. 37, no. 6, pp. 826-844, November/December 2011.
  - G.Bucci, L. Carnevali, L. Ridi, and E. Vicario, "Oris: a tool for modeling, verification and evaluation of real-time systems", International Journal of Software Tools for Technology Transfer, vol. 12, no. 5, pp. 391-403, 2010.
- Quantitative evaluation of real-time concurrent systems
  - M. Paolieri, M. Biagi, L. Carnevali, E. Vicario, "The ORIS Tool: Quantitative Evaluation of Non-Markovian Systems", IEEE Transactions on Software Engineering, submitted after minor revision.
  - M. Biagi, L. Carnevali, M. Paolieri, F. Patara, E. Vicario, "A continuous-time model-based approach for activity recognition in pervasive environments", IEEE Transactions on Human-Machine Systems, to appear.
  - L. Carnevali, F. Tarani, and E. Vicario, "Performability Evaluation of Water Distribution Systems During Maintenance Procedures", IEEE Transactions on Systems, Man, and Cybernetics: Systems, to appear.
  - M. Biagi, L. Carnevali, F. Tarani, and E. Vicario, "Model-based quantitative evaluation of repair procedures in gas distribution networks", ACM Transactions on Cyber-Physical Systems, vol. 3, no. 2, pp. 19:1–19:26, December 2018.
  - M. Biagi, L. Carnevali, M. Paolieri, and E. Vicario, "Performability evaluation of the ERTMS/ETCS - Level 3", Transportation Research Part C: Emerging Technologies, vol. 82, pp. 314-336, September 2017.
  - L. Carnevali, A. Pinzuti, and E. Vicario, "Compositional Verification for Hierarchical Scheduling of Real-Time Systems", IEEE Transactions on Software Engineering, vol. 39, no. 5, pp. 638-657, May 2013.
  - L. Carnevali, L. Ridi, and E. Vicario, "A Quantitative Approach to Input Generation in Real-Time Testing of Stochastic Systems", IEEE Transactions on Software Engineering, vol. 39, no. 3, pp. 292-304, March 2013.
  - E. Vicario, L. Sassoli, and L. Carnevali, "Using Stochastic State Classes in Quantitative Evaluation of Dense-Time Reactive Systems", IEEE Transactions on Software Engineering, vol. 35, no. 5, pp. 703-719, September/October 2009.
  - L. Carnevali, L. Grassi, and E. Vicario, "State-Density Functions over DBM Domains in the Analysis of Non-Markovian Models", IEEE Transactions on Software Engineering, vol. 35, no. 2, pp. 178-194, March/April 2009.