Control of Cyber-Physical Systems with Logic Specifications

Piazza Duomo, L'Aquila, Italy

Giordano Pola
DISIM - DEWS
University of L'Aquila (Italy)
giordano.pola@univaq.it

Cyber-Physical Systems

Cyber-Physical Systems (CPS) are physical, biological and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core

Critical aspects of CPS

- Heterogeneity: plants, controllers and specifications described in different mathematical frameworks
- Non-ideal communication infrastructure: control action delivered with delay on the basis of delayed and corrupted measure of the states of the plants, lack of information (packet drops), etc.
- Complexity: large number of possibly distributed sub-systems
- Logic specifications
- …

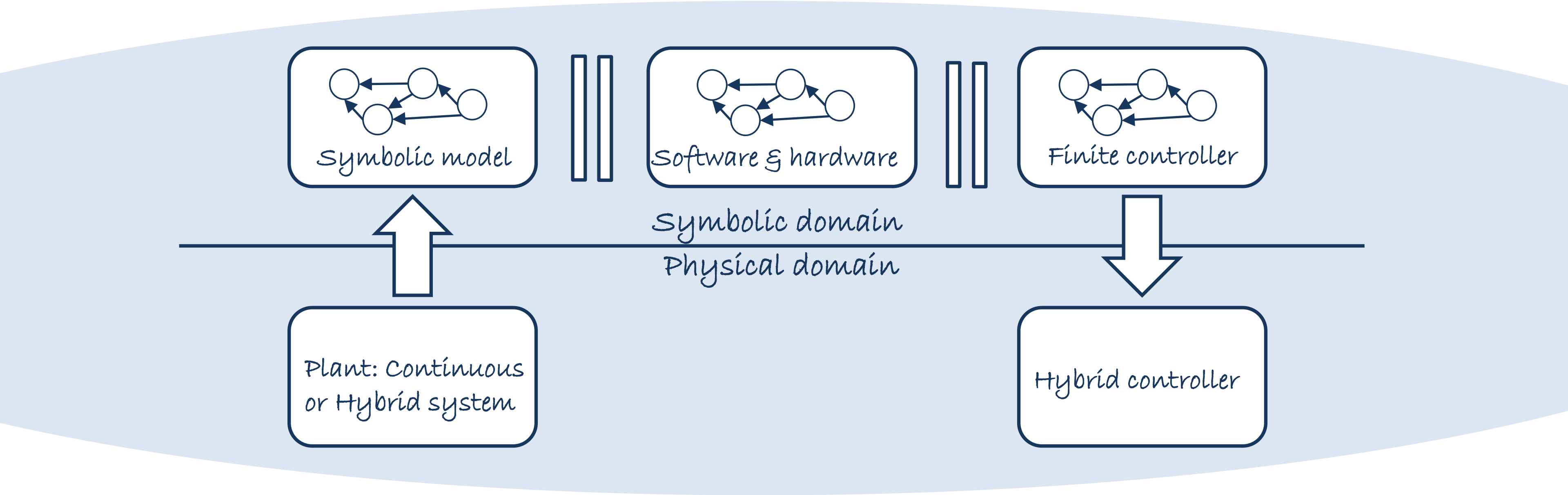
Formal methods: a tool to homogenize heterogeneity …

<u>A three phases process :</u>

#1. Construct the finite/symbolic model T approximating the plant system P

#2. Design a finite/symbolic controller C that solves the specification S for T

#3. Refine the controller C to the controller C' to be applied to P



Advantages :

- Integration of software and hardware constraints in the control design of purely continuous or hybrid processes
- Relevant logic specifications can be addressed

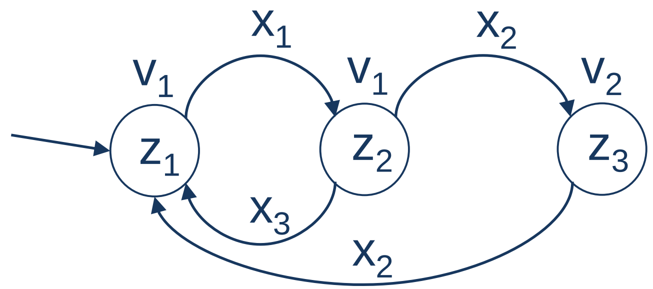
Plant and controller

- Plant:

$$P: \begin{cases} \dot{x}(t) = f\big(x(t), u(t)\big) \\ x(t) \in \mathbb{R}^n, u(t) \in \mathrm{U} \subset \mathbb{R}^m \end{cases}$$

U finite set
$\boldsymbol{x}(t, x_0, u)$ state reached at time t with initial state x_0 and control input u

- Controller C: Finite State Machine



inputs of C: quantized measurements of the state of P

outputs of C: control signal v(k) to be inferred to the plant P

- Controlled plant P^C obtained by coupling dynamics of P and C with

ZoH: $\{u(t) = v(k), \forall t \in [k\tau, (k+1)\tau[, k \in \mathbb{N}$

$\tau > 0$ sampling time

Logic specifications: Regular languages

Recall

- Let Υ be a finite set representing an alphabet
- A word over Υ is a finite sequence with symbols in Υ
- A language L over Υ is a collection of words in Υ

Definition

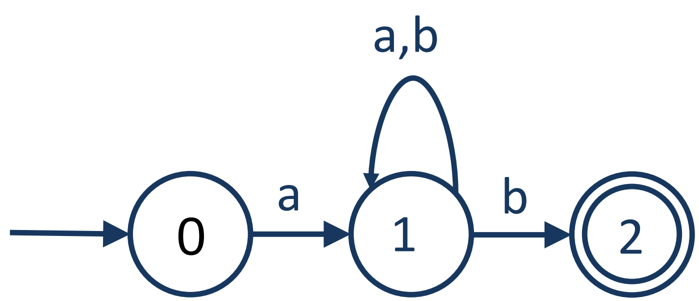
A language is regular if it can be represented by a Finite State Automaton (FSA)

Example

$\Upsilon = \{ \mathrm{a}, \mathrm{b} \}$

$L=$ all words over Υ $\mathrm{starting\ with\ symbol\ a\ and\ ending\ with\ symbol\ b}$

L is regular because of existence of FSA:



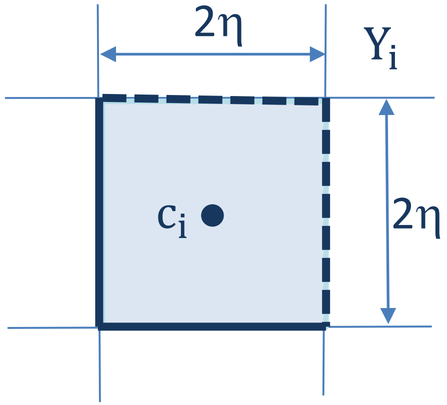
Logic specifications: Regular languages

Alphabet: collection Y of
left-closed right-open hyper-cubes $\mathrm{Y_i}$ of $\mathbb{R}^n$

$\mathrm{Y_i} = \mathrm{c_i} + \Pi_{i=1}^{n} [-\eta, \eta[$

$\mathrm{c_i} \in 2\eta\, \mathbb{Z}^n$

Y is a partition of $\mathbb{R}^n$



We consider a specification expressed as a regular language $\mathrm{L_Q}$ over Y

Specifications for CPS handled via regular language formalism :

- Reachability
- Controlled invariance in finite time horizon
- Obstacle avoidance in finite time horizon
- Motion planning
- Enforcing periodic orbits
- State-based switching specifications
- …

Control Problem Formulation

Given

- the plant P
- a sampling time $\tau > 0$
- a regular language specification $\mathrm{L_Q}$
- a desired accuracy $\theta > 0$

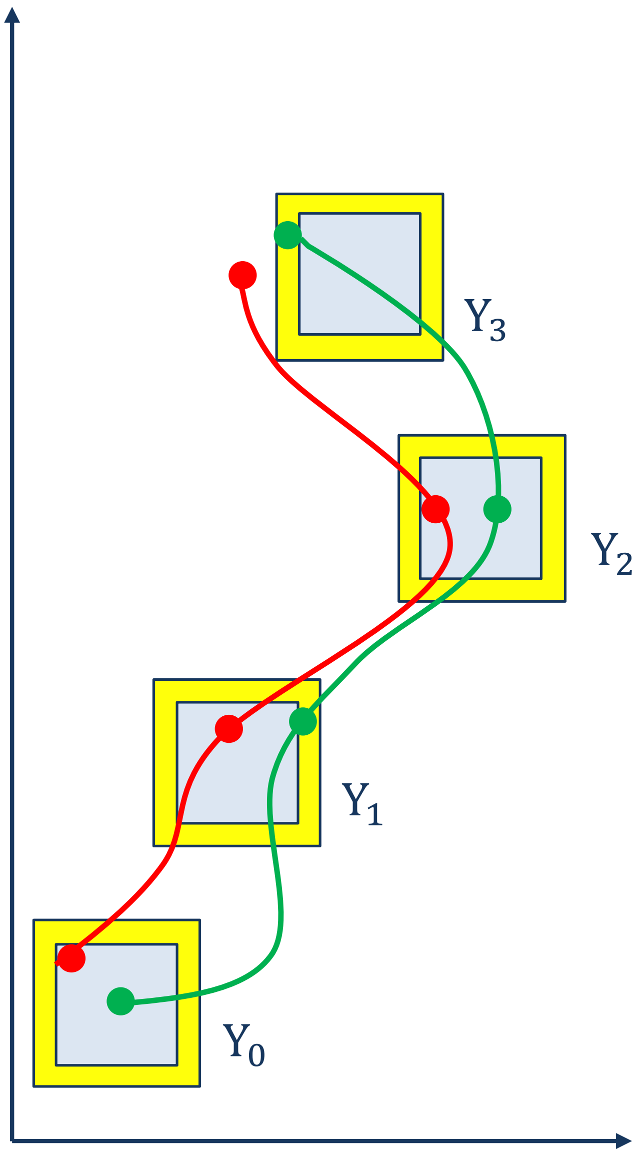
Find

- a controller C with set of initial states $X_{c,0}$
- a relation of initial states $R_0 \subseteq \mathbb{R}^n \times X_{c,0}$ of P^C

such that the controlled plant P^C satisfies the specification $\mathrm{L_Q}$ up to the accuracy θ, i.e.

for any trajectory $\mathrm{x}(.)$ of P^C with $(\mathrm{x}(0), x_c(0)) \in R_0$, there exists a word $\mathrm{q}_0\mathrm{q}_1 \ldots \mathrm{q}_{k_\mathrm{f}}$ of $\mathrm{L_Q}$ such that

$$\|\mathrm{x}(\mathrm{k}\tau) - \mathrm{q_k}\| \leq \theta, \forall \mathrm{k} \in [0; \mathrm{k_f}]$$

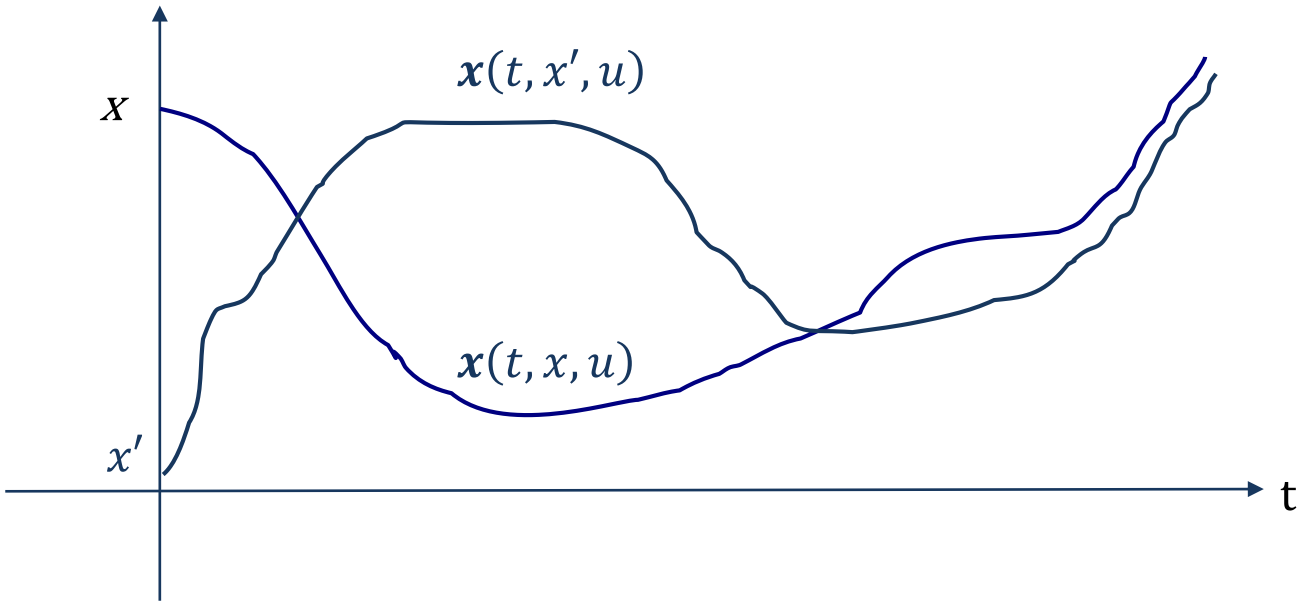


Key assumptions on the plant P

Definition *[Angeli, TAC-2002]*

Plant P is incrementally globally asymptotically stable (δ-GAS) if there exists a $\mathcal{KL}$ function $\beta: \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}^+$ such that for any $t \geq 0$, any initial conditions x, x' and any input u

$$\|\boldsymbol{x}(t,x,u) - \boldsymbol{x}(t,x',u)\| \leq \beta(\|x - x'\|, t)$$



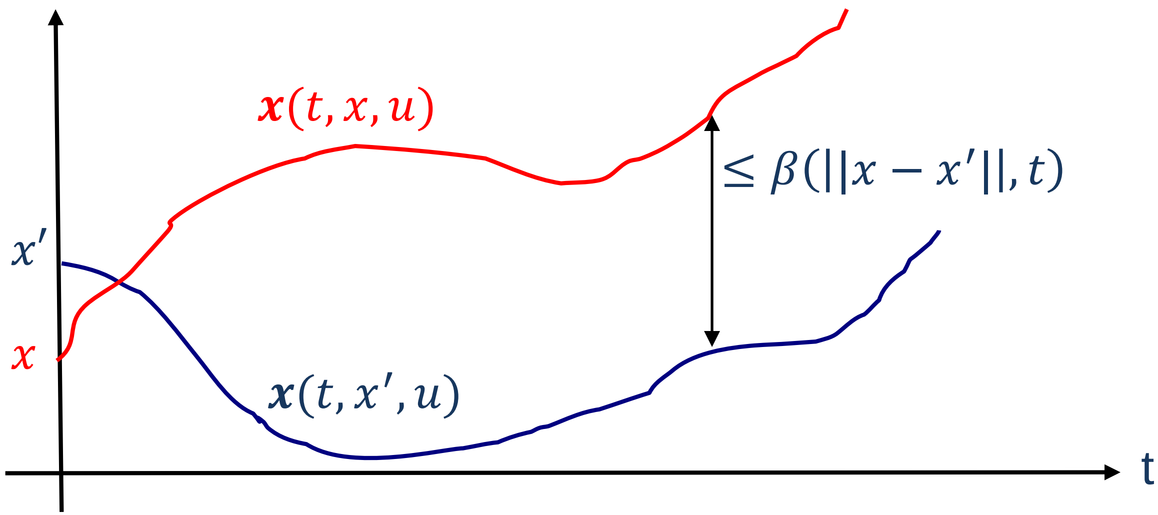
Remark δ-GAS can be checked by using Lyapunov-like inequalities

Key assumptions on the plant P

Definition *[Zamani et al., TAC-2012]*

Plant P is incrementally forward complete (δ-FC) if there exists a continuous function $\beta: \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}^+$ such that for every $s \in \mathbb{R}^+$, function $\beta(.,s)$ belongs to class $\mathcal{K}_\infty$ and for any $x, x' \in \mathbb{R}^n$ and any u

$$||\boldsymbol{x}(t,x,u) - \boldsymbol{x}(t,x',u)|| \leq \beta(||x - x'||, t)$$



Remarks

- Any (possibly unstable) linear system is δ-FC
- δ-FC can be checked by using Lyapunov-like inequalities
- δ-GAS implies δ-FC while the converse is not true

Solution

Contribution

For δ-FC (and hence δ-GAS) plants, we designed algorithms solving the control problem for any desired sampling time $\tau > 0$ and accuracy $\theta > 0$

Remarks

- Symbolic model T of P obtained by time and state space discretization of P
- If P is δ-GAS then T is an approximate bisimulation [5] of time discretization of P
- If P is δ-FC then T is an alternating approximate simulation [4] by time discretization of P
- Design of controllers inspired by supervisory control algorithms
- *The «completeness property»: If* P is δ-GAS then a control strategy enforces a given specification on P if and only if it can be found on T (guaranteed by approximate bisimulation)

Based on:

[1] Pola, G., Girard A., Tabuada, P., Approximately bisimilar symbolic models for nonlinear control systems, Automatica, 44(10):2508-2516, 2008

[2] Zamani, M., Pola, G., Mazo, M., Tabuada, P., Symbolic models for nonlinear control systems without stability assumptions, IEEE Transactions on Automatic Control, 57(7):1804-1809, July 2012

[3] Pola, G., Di Benedetto, M.D., Control of Cyber–Physical–Systems with Logic Specifications: A Formal Methods Approach, Annual Reviews in Control, 47(2019):178-192

[4] Pola, G., Tabuada, P., Symbolic models for nonlinear control systems: Alternating approximate bisimulations, SIAM Journal on Control and Optimization, 48(2):719-733, 2009

[5] Girard, A., Pappas, G.J., Approximation metrics for discrete and continuous systems. IEEE Transactions on Automatic Control, 52(5), 782–798, 2007

Including more features of CPS

- Stable nonlinear switched systems

  TOOLS: δ-UGAS and its check through common and multiple Lyapunov functions

  with Antoine Girard and Paulo Tabuada

- Stable nonlinear control systems with disturbance inputs

  TOOLS: δ-ISS, alternating approximate bisimulation and spline analysis

  with Paulo Tabuada, Alessandro Borri and Maria Domenica Di Benedetto

- Stable nonlinear time-delay systems

  TOOLS: δ-ISS, δ-IDSS, alternating approximate bisimulation and spline analysis

  with Pierdomenico Pepe and Maria Domenica Di Benedetto

- Networked control systems

  TOOLS: strong alternating approximate simulation and bisimulation

  with Alessandro Borri and Maria Domenica Di Benedetto

- Decentralized supervisory control

  TOOLS: extensions of supervisory control to concurrent settings

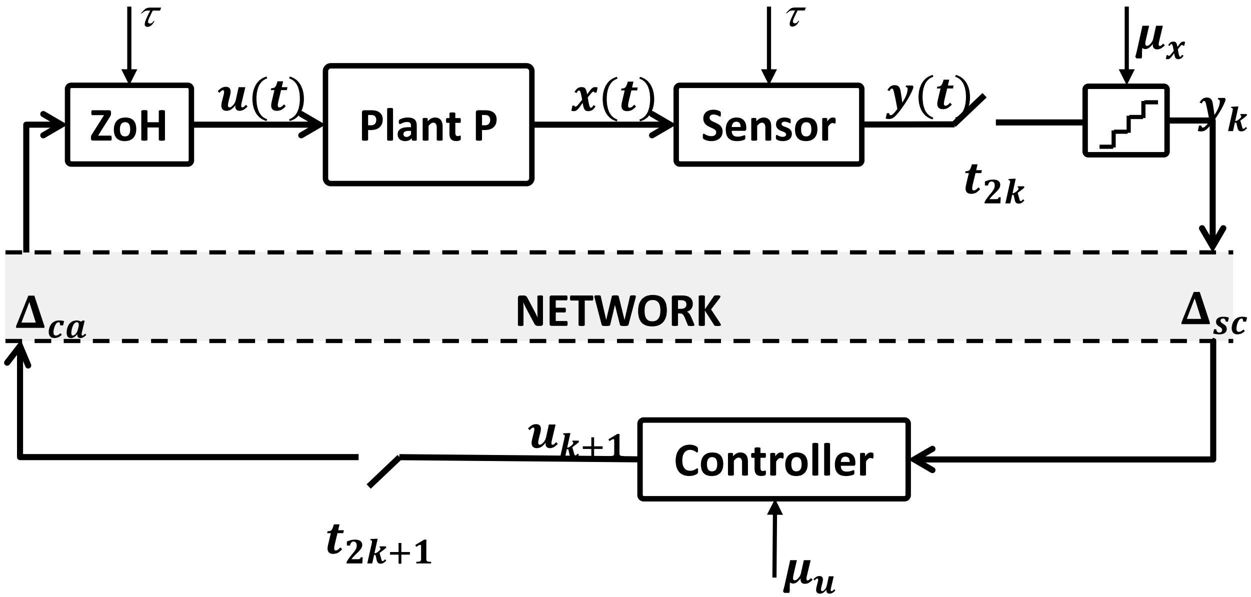
  with Pierdomenico Pepe and Maria Domenica Di Benedetto

- Control design of stable nonlinear systems with outputs

  TOOLS: δ-GAS, approximate bisimulation

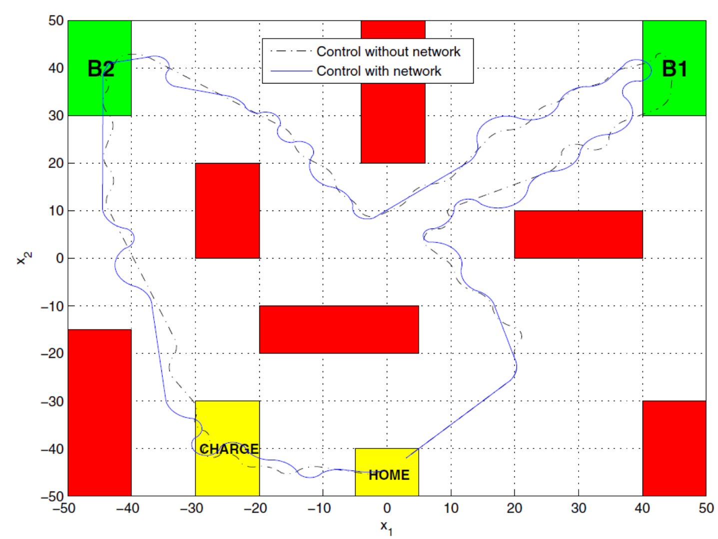
  with Maria Domenica Di Benedetto and Alessandro Borri

Networked control systems



Nonidealities considered:

- Quantization errors
- Bounded time-varying network access times
- Bounded time-varying communication delays induced by the network
- Limited bandwidth
- Bounded packet losses
- Bounded time-varying computation time of computing units



Conclusions

We proposed an approach based on formal methods for the control of CPS with logic specifications

Future work: Design of efficient control algorithms and their software implementation

Thanks!

References on formal methods for the control of CPS

1. [Pola et al., AUT19] Pola, G., Di Benedetto, M.D., Borri, A., Symbolic Control Design of Nonlinear Systems with Outputs, Automatica, November, 2019
2. [Fakhroleslam et al. IPC19] Fakhroleslam, M., Pola, G., De Santis, E., Di Benedetto, M.D., Time-optimal symbolic control of a changeover process based on an approximately bisimilar symbolic model, Journal of Process Control, 81(2019):126–135
3. [Pola et al., ARC19] Pola, G., Di Benedetto, M.D., Control of Cyber–Physical–Systems with Logic Specifications: A Formal Methods Approach, Annual Reviews in Control, 47(2019):178-192
4. [Borri et al. TAC19] Borri, A., Pola, G., Di Benedetto, M.D., Design of Symbolic Controllers for Networked Control Systems, IEEE Transactions on Automatic Control, 63(3):1034-1046, March 2019
5. [Pola et al., TAC18] Pola, G., Pepe, P, Di Benedetto, M.D., Decentralized Approximate Supervisory Control of Networks of Nonlinear Control Systems, IEEE Transactions on Automatic Control, 63(9):2803-2817, September 2018
6. [Pola et al., TAC16] Pola, G., Pepe, P. Di Benedetto, M.D., Symbolic Models for Networks of Control Systems, IEEE Transactions on Automatic Control, 61(11):3663-3668, November 2016
7. [Pola et al., IJRNC15] Pola, G., Pepe, P. Di Benedetto, M.D., Symbolic Models for Time–Varying Time–Delay Systems via Alternating Approximate Bisimulation, International Journal of Robust and Nonlinear Control, 25:2328–2347, September 2015
8. [Pola et al., TAC14] Pola, G., Di Benedetto, M.D., Symbolic Models and Control of Discrete-Time Piecewise Affine Systems: An Approximate Simulation Approach, IEEE Transactions on Automatic Control, 59(1):175-180, January 2014
9. [Borri et al., IJC12] Borri, A., Pola, G., Di Benedetto, M.D., Symbolic models for nonlinear control systems affected by disturbances, International Journal of Control, 85(10):1422-1432, September 2012
10. [Zamani et al., TAC12] Zamani, M., Pola, G., Mazo, M., Tabuada, P., Symbolic models for nonlinear control systems without stability assumptions, IEEE Transactions on Automatic Control, 57(7):1804-1809, July 2012
11. [Pola et al., TAC12] Pola, G., Borri, A., Di Benedetto, M.D., Integrated design of symbolic controllers for nonlinear systems, IEEE Transactions on Automatic Control, 57(2):534-539, February 2012
12. [Pola et al., SCL10] Pola, G., Pepe, P., Di Benedetto, M.D., Tabuada, P., Symbolic models for nonlinear time-delay systems using approximate bisimulation, Systems & Control Letters 59(6): 365-373, June 2010
13. [Girard et al., TAC10] Girard, A., Pola, G., Tabuada, P., Approximately bisimilar symbolic models for incrementally stable switched systems, IEEE Transactions on Automatic Control, 55(1):116-126, January 2010
14. [Pola et al., SIAM09] Pola, G., Tabuada, P., Symbolic models for nonlinear control systems: Alternating approximate bisimulations, SIAM Journal on Control and Optimization, 48(2):719-733, 2009
15. [Pola et al., AUT08] Pola, G., Girard A., Tabuada, P., Approximately bisimilar symbolic models for nonlinear control systems, Automatica, 44(10):2508-2516, October 2008
16. [Di Benedetto et al., EPTCS13] Di Benedetto, M.D., Pola, G., Networked Embedded Control Systems: from Modelling to Implementation, Electronic Proceedings in Theoretical Computer Science (EPTCS) 124, pp. 9-13, Bortolussi L., Bujorianu M.L., Pola G. (Eds.): HAS 2013, doi:10.4204/EPTCS
17. [Borri et al., ERCIM14] Borri, A., Di Benedetto, M.D., Pola, G., Towards a Unified Theory for the Control of CPS: A Symbolic Approach, ERCIM News No. 97, April 2014, Special theme: Cyber-Physical Systems, Guest editors M. D. Di Benedetto, F. L. Lagarrigue, E. Schoitsch
18. [Borri et al., NECSYS13] Borri, A., Dimarogonas, D.V., Johansson, K.H., Di Benedetto, M.D., Pola, G., Decentralized symbolic control of interconnected systems with application to vehicle platooning, 4th IFAC Workshop on Distributed Estimation and Control in Networked Systems, Koblenz, Germany, September 2013, pp. 285-292