Formal Methods for the Control of Large-scale Networked Nonlinear Systems with Logic Specifications

Basilica di Santa Maria di Collemaggio, L’Aquila (Italy), 1287

Lecture L1:

Introduction

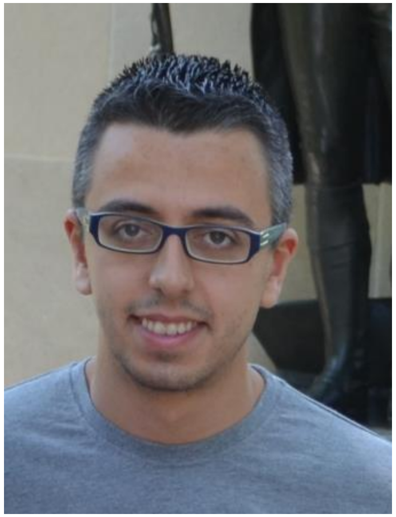
Speaker: Maria Domenica Di Benedetto

Organizers and Speakers

Maria Domenica Di Benedetto
Dipartimento di Ingegneria e Scienze dell'informazione e Matematica
Center of Excellence DEWS
University of L’Aquila, Italy
mariadomenica.dibenedetto@univaq.it

Giordano Pola
Dipartimento di Ingegneria e Scienze dell'informazione e Matematica
Center of Excellence DEWS
University of L’Aquila, Italy
giordano.pola@univaq.it

Pierdomenico Pepe
Dipartimento di Ingegneria e Scienze dell'informazione e Matematica
Center of Excellence DEWS
University of L’Aquila, Italy
pierdomenico.pepe@univaq.it



Alessandro Borri
Istituto di Analisi dei Sistemi ed Informatica "A. Ruberti" (IASI)
Consiglio Nazionale delle Ricerche (CNR), Rome, Italy
alessandro.borri@iasi.cnr.it

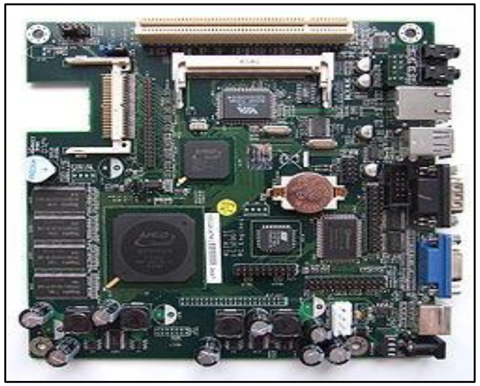
Cyber-Physical Systems of Systems

What is a Cyber-Physical System (CPS)?

- First generation CPS (Embedded Systems):

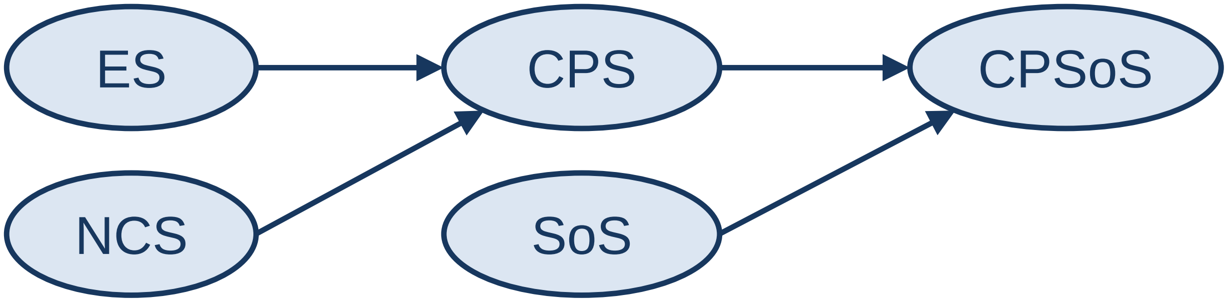
  Computational systems, but not stand alone computers, interfacing sensors and actuators, reactive to physical environment stimuli, designed to perform one or a few dedicated functions, often with real-time computing constraints

- Focus on the computation



Cyber-Physical Systems of Systems

- Second generation CPS: more importance to the link and communication between computational and physical elements
- CPSoS (*European working group CPSoS, www.cpsos.eu*) are large-scale, complex, heterogeneous, distributed and networked systems
- Tight combination of, and coordination between, physical process and computational and communication components



SoS: Autonomy of the subsystems, dynamic reconfiguration, emerging behaviors

Cyber-Physical Systems of Systems

Tight interaction of many distributed, real-time computing systems and physical systems

Examples

- Airplanes
- Cars
- Buildings with advanced HVAC controls
- Manufacturing plants
- Power plants
- ...

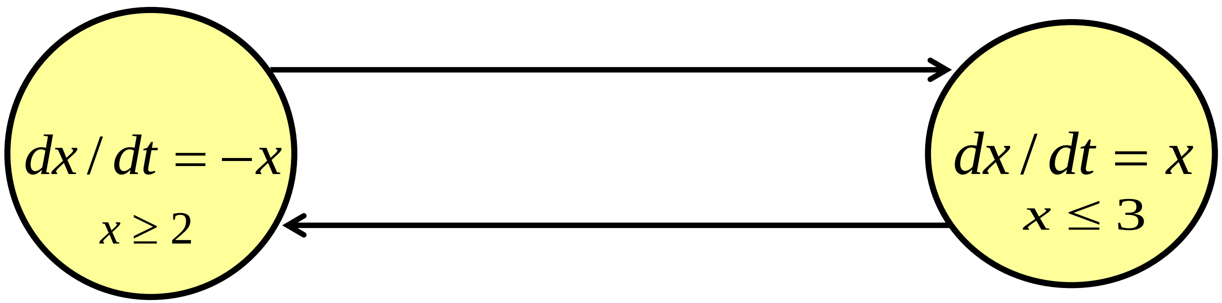
Cyber-Physical Systems of Systems

- “Are today’s resources and knowledge in control, communications and computing adequate to deal with such a kind of complex systems?”

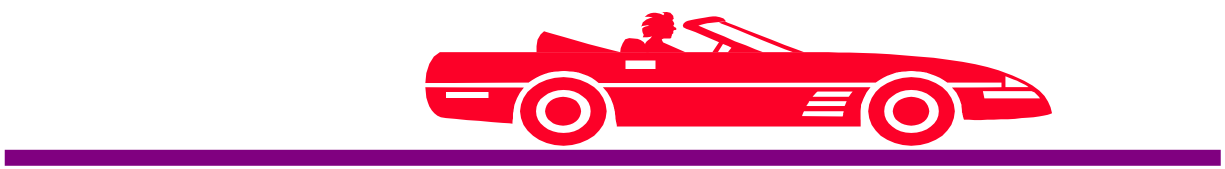
  (E. Lee, UC Berkeley)

Heterogeneous systems, the motivation for hybrid models

- Combination of discrete and continuous time with a prescribed hierarchy



- Models with “heterogeneous components”



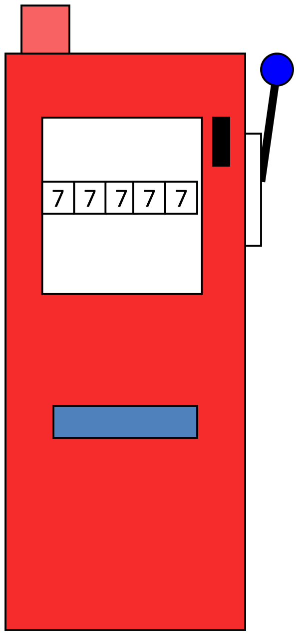
Heterogeneous systems, the motivation for hybrid models

- **Continuous systems with a phased operation:**
  - walking robots
  - biological cell growth and division

- **Continuous systems controlled by discrete logic:** need for design techniques that can guarantee safety and performance specifications of *embedded systems*, or systems that couple discrete logic with the analog physical environment.
  - thermostat
  - chemical plants with valves, pumps
  - control modes for complex systems, eg. intelligent cruise control in automobiles, aircraft autopilot modes

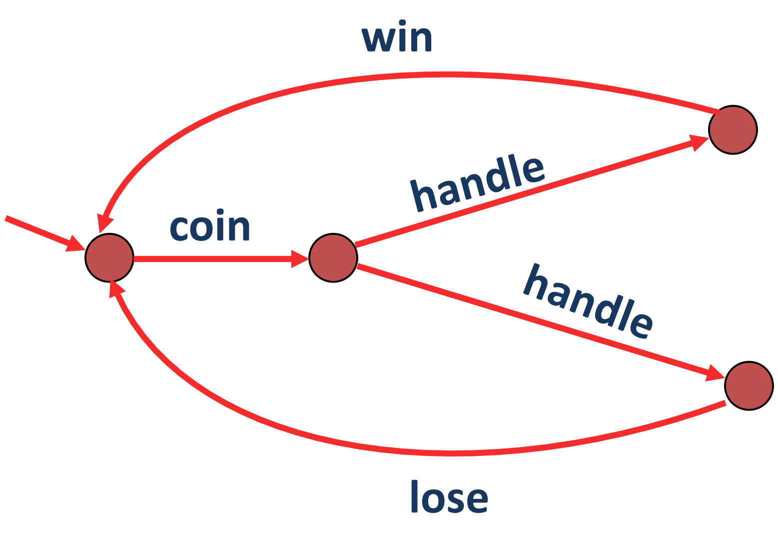
- **Coordinating processes:** many interacting subsystems (multi-agent systems) typically feature continuous controllers to optimize performance of individual agents, and coordination among agents to compete for scarce resources, resolve conflicts, etc.
  - air and ground transportation systems
  - swarms of micro-air vehicles

Finite state machines



Slot machine

1. Insert coin
2. Pull handle
3. Win if the combination is good, otherwise lose



Features of finite state machines

- Events are time-abstract
- Events are not necessarily equipped with any notion of ‘internal-external’ or ‘input-output’
- Compositionality is possible
- There can be non-determinism
- Just like modeling of continuous systems, the level of detail is ‘modeler dependent’

Physical System - Software Interaction

- Ariane V launched on 4th June 1996. It exploded 37s after launch
- The program had been running for 10 years, costing $7 billions
- Software worked perfectly on Ariane IV, the same was used in Ariane V

What had changed, was the physical system around the software …

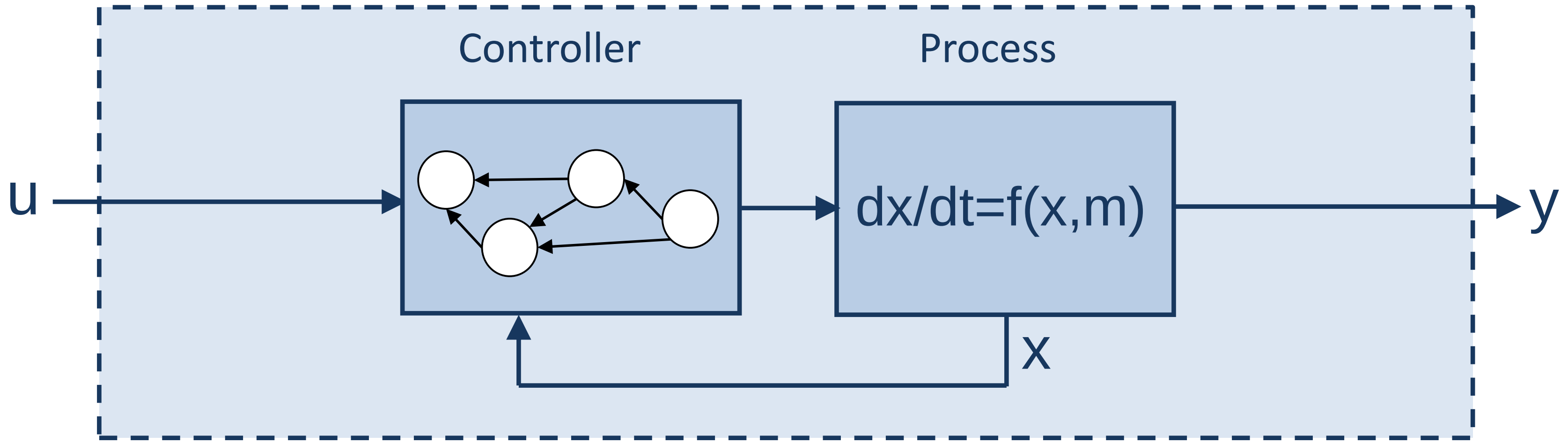
Networked systems

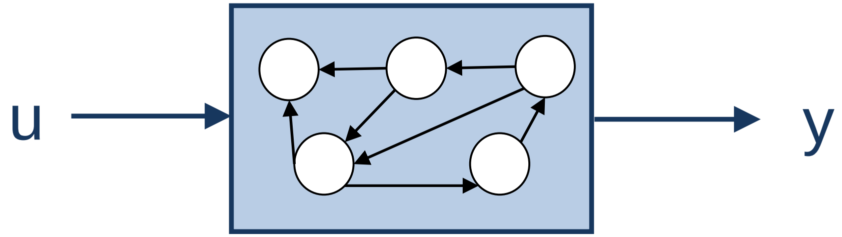
Nonidealities in communication infrastructures:

- Quantization errors
- Time-varying network access times
- Time-varying communication delays induced by the network
- Limited bandwidth
- Packet losses
- …

(e.g. [Andersson, IEEE-CDC-05], [Antsaklis, IEEE-TAC-04], [Heemels, IEEE-TAC-10], [Hespanha, Proc. IEEE-07], [Murray, SMTNS-06])

Logic specifications





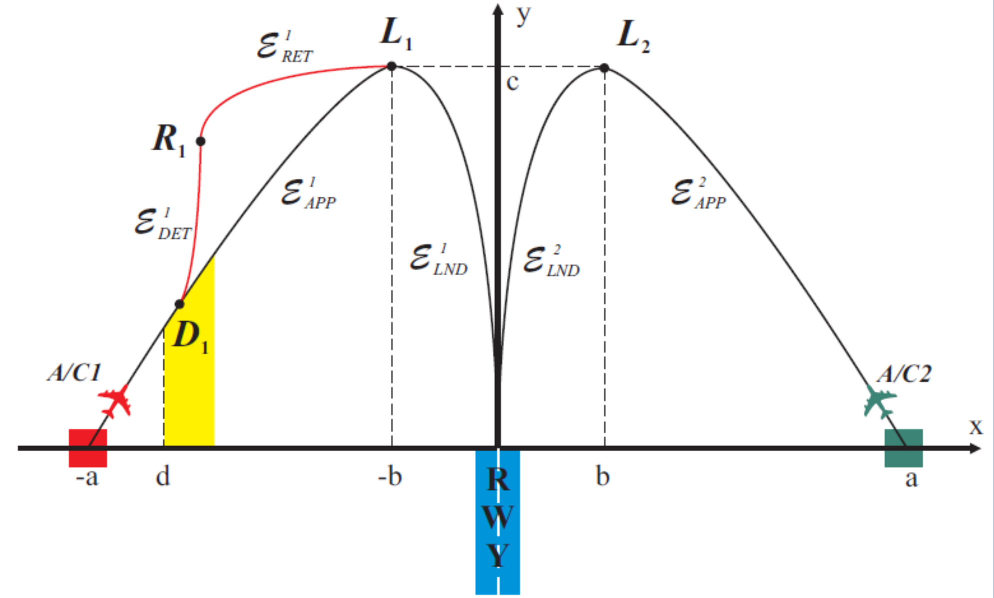
Logic specifications

Automata theory, Linear Temporal Logic, Computational Tree Logic, Metric Temporal Logic …

Examples:

- Language specifications
- Synchronization specifications
- Obstacle avoidance
- Switching specifications
- …

Landing Scheduling Problem



$$\varphi = \forall\left(\neg\phi_1 \wedge \neg\phi_2 U_{t\geq 0}(\neg\phi_1 \wedge \phi_2 U_{60\leq t\leq 180}\phi_1 \wedge \phi_2)\right)$$

[D'Innocenzo,Julius,Pappas,Di Benedetto,Di Gennaro;IEEE-CDC-2007]

Summarizing critical aspects of CPSoS …

- 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 systems composed of several, possibly distributed sub-systems
- Logic specifications

Triple C-convergence

Control Theory

Computer Science

Communication Systems

⇓

Heterogeneous, large-scale networked control systems

Todays' research approaches to CPSoS

- Resource aware control
- Distributed control
- Networked control systems

(see e.g. 7th PhD School on CPS, Lucca, June 12-15, 2017)

- Co-design of physical, computational and communication systems
- **Formal methods**

Formal Methods

Projects funded in the USA

- Correct-by-Design Control Software Synthesis for Highly Dynamic Systems (NSF 1239085)
- Towards robust cyber-physical systems (NSF 1035916)
- Closing the gap in controller synthesis (NSF 0953994)
- Automated Synthesis of Embedded Control Software (NSF 0717188)
- Formal Methods for Motion Planning and Control with Human-in-the-Loop (NSF NRI-1426907)
- A formal approach to control of hybrid systems (NSF CNS-0834260), etc.

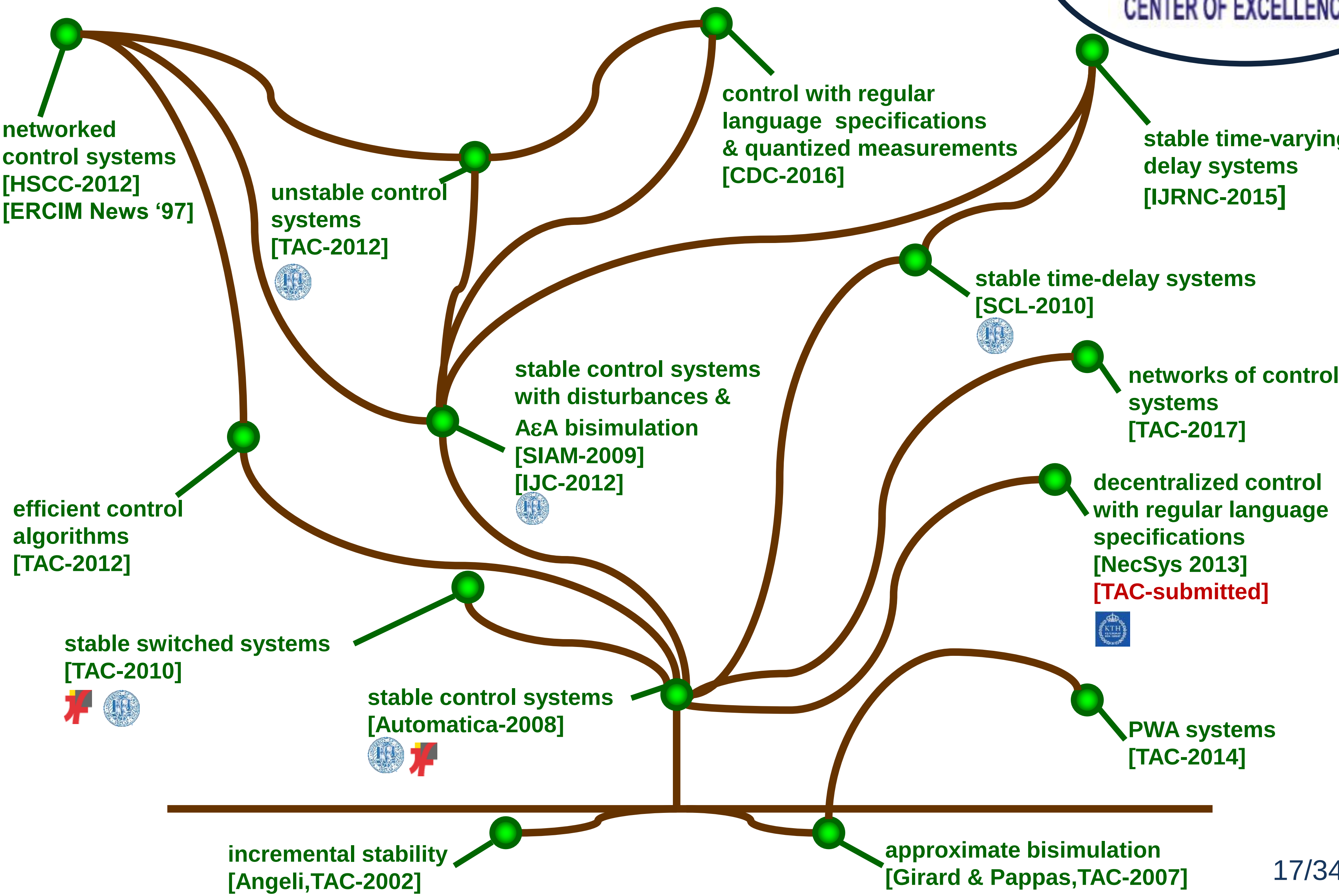
Special issues

- Symbolic Methods for Complex Control Systems (IEEE-TAC 2006)
- Formal Methods in Control (Journal of DEDS 2016), etc.

Plenary lectures

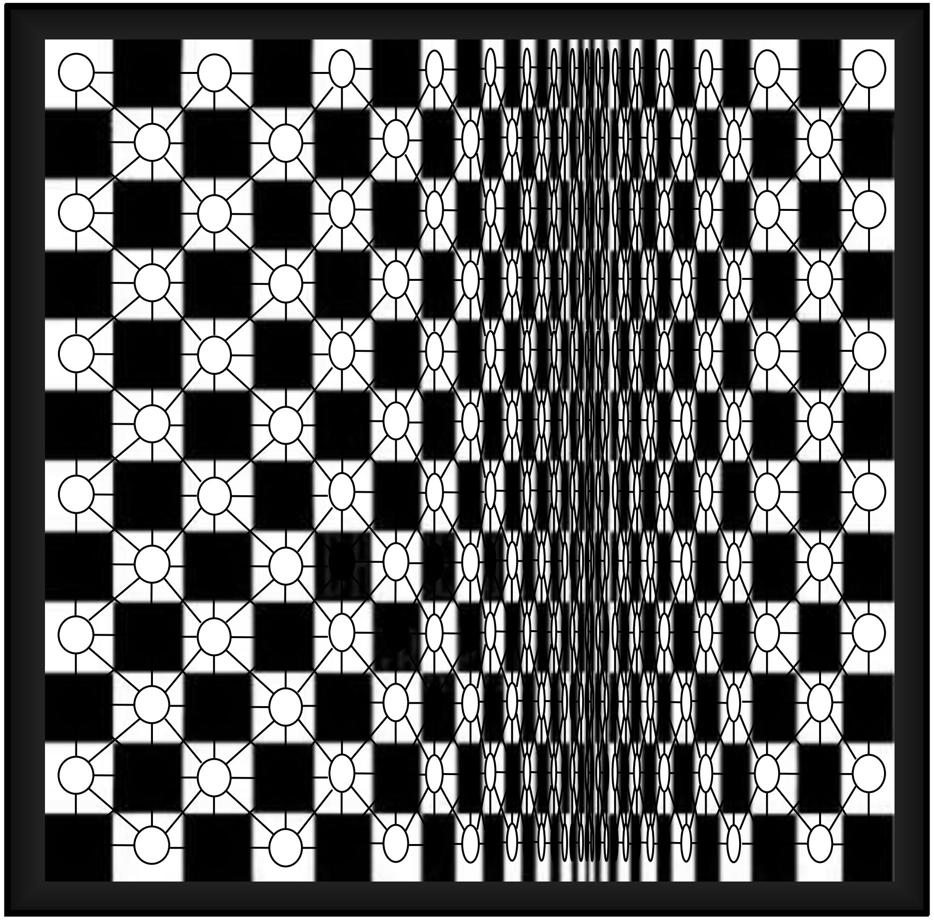
- Tabuada, Bisimulation: From Differential Equations to Finite-State Machines and Back (ACC 2010)
- Pappas, Approximate Bisimulation: A Bridge Between Computer Science and Control Theory (CDC 2011)
- Di Benedetto - Pola, Networked Embedded Control Systems: from Modelling to Implementation (ICSCS 2012), etc.

Research at DEWS



Formal methods: a tool to tame heterogeneity …

Key idea:
homogenizing
heterogeneities
in
the
formal
description
of
plants
controllers
and
specifications



Bridget Riley, *Movement in Squares, 1961*

… from continuous to discrete systems !

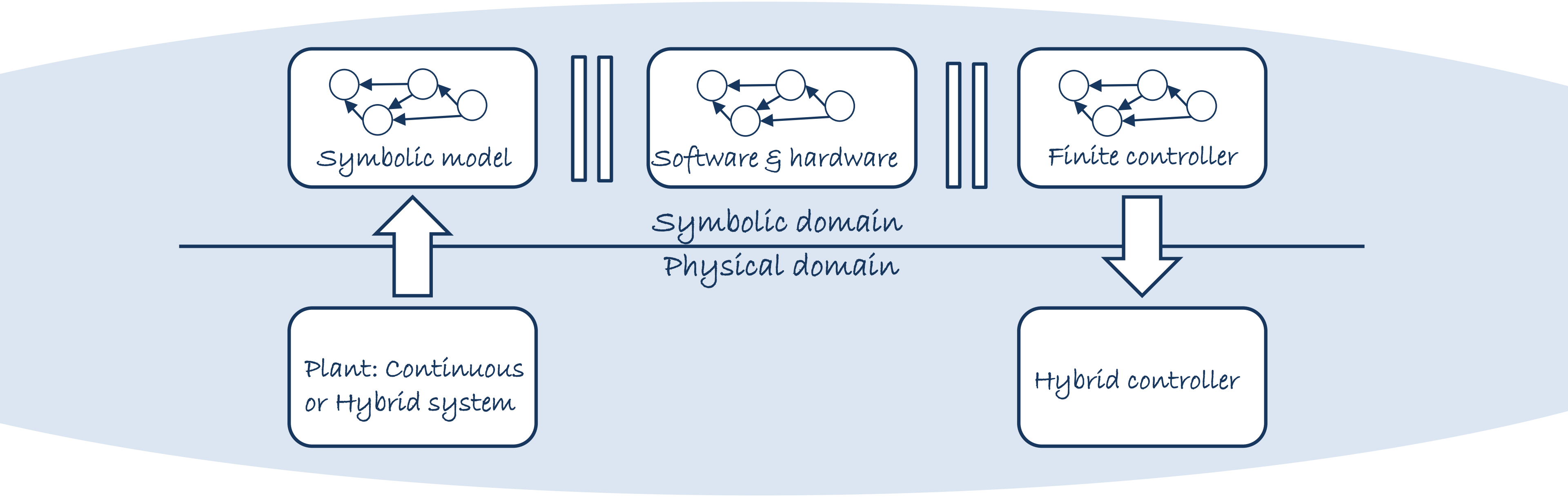
Solution based on Formal Methods

A three phases process :

#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



Correct-by-design embedded control software

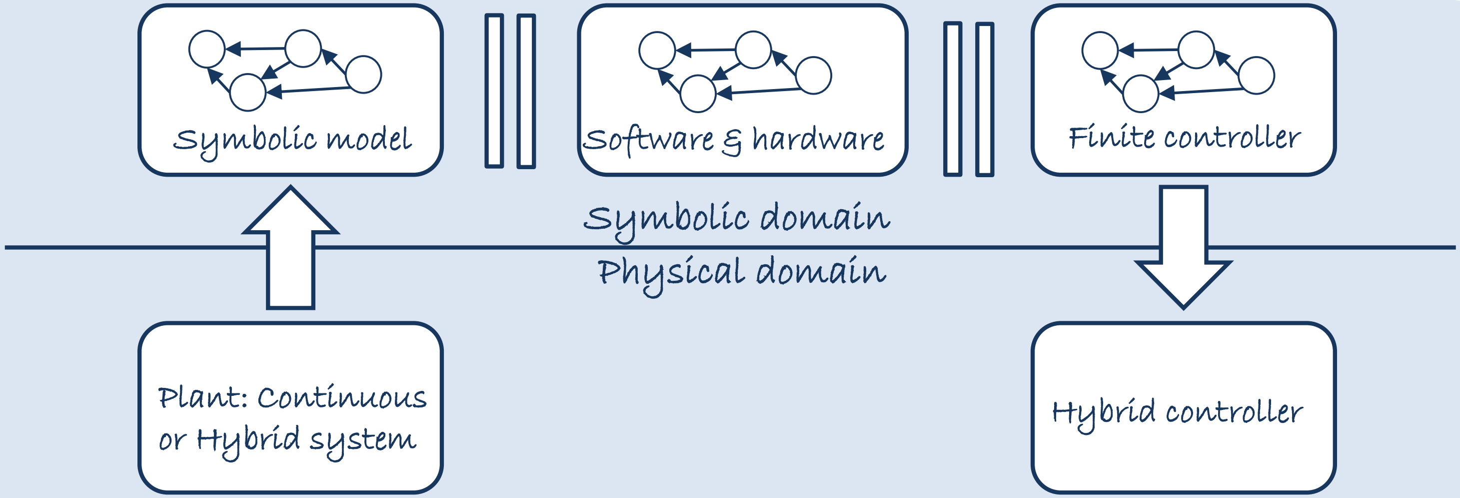
Solution based on Formal Methods

A three phases process :

#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 :

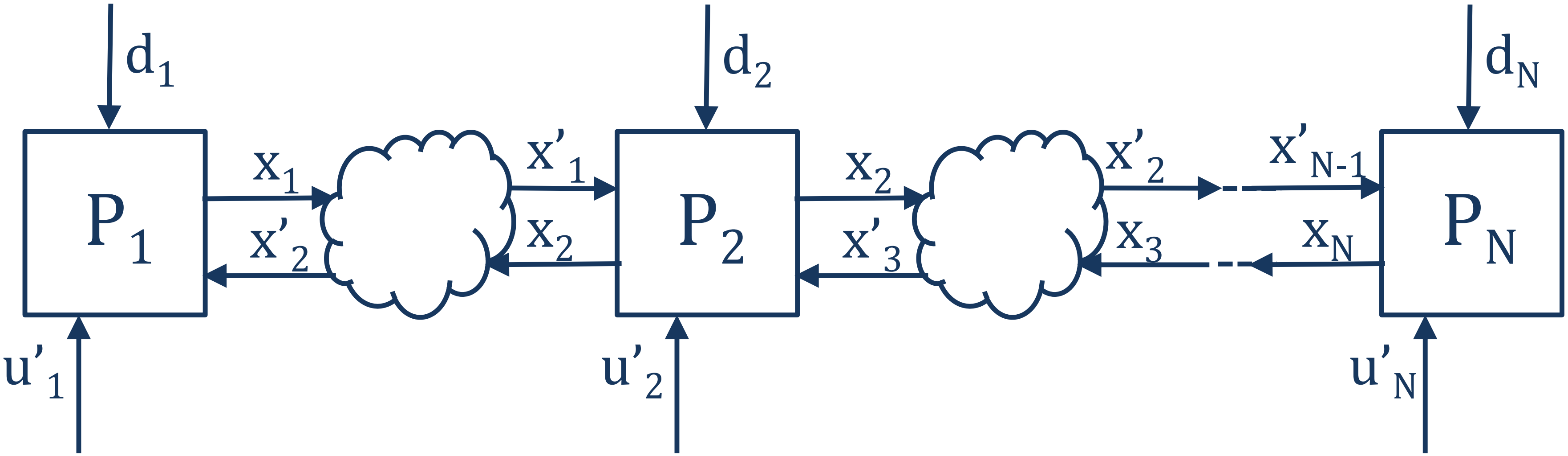
- Integration of software and hardware constraints in the control design of purely continuous processes
- Logic specifications can be addressed

… towards

Controlling

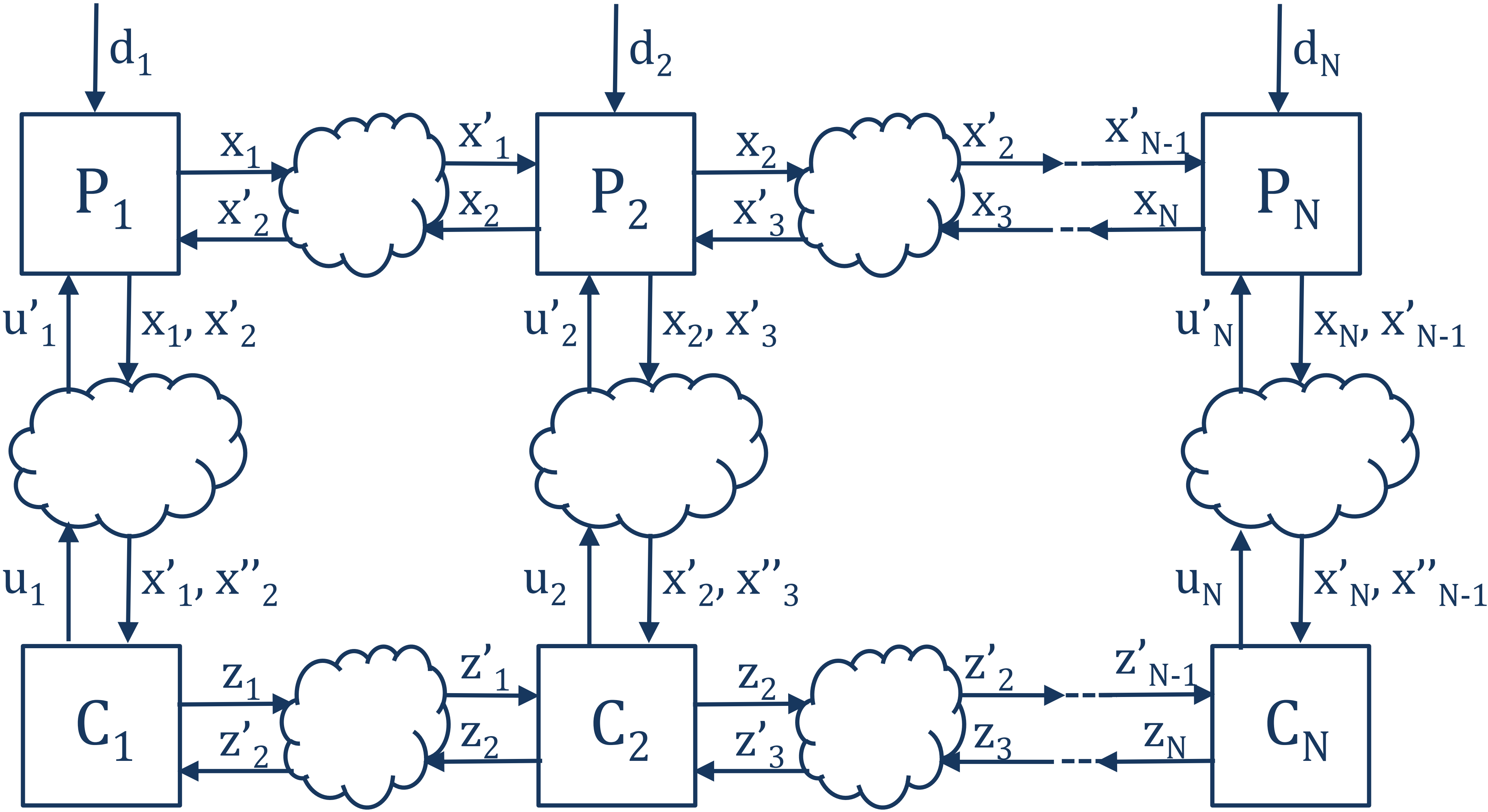
Large-scale networked nonlinear systems with logic specifications

Large-scale networked nonlinear systems



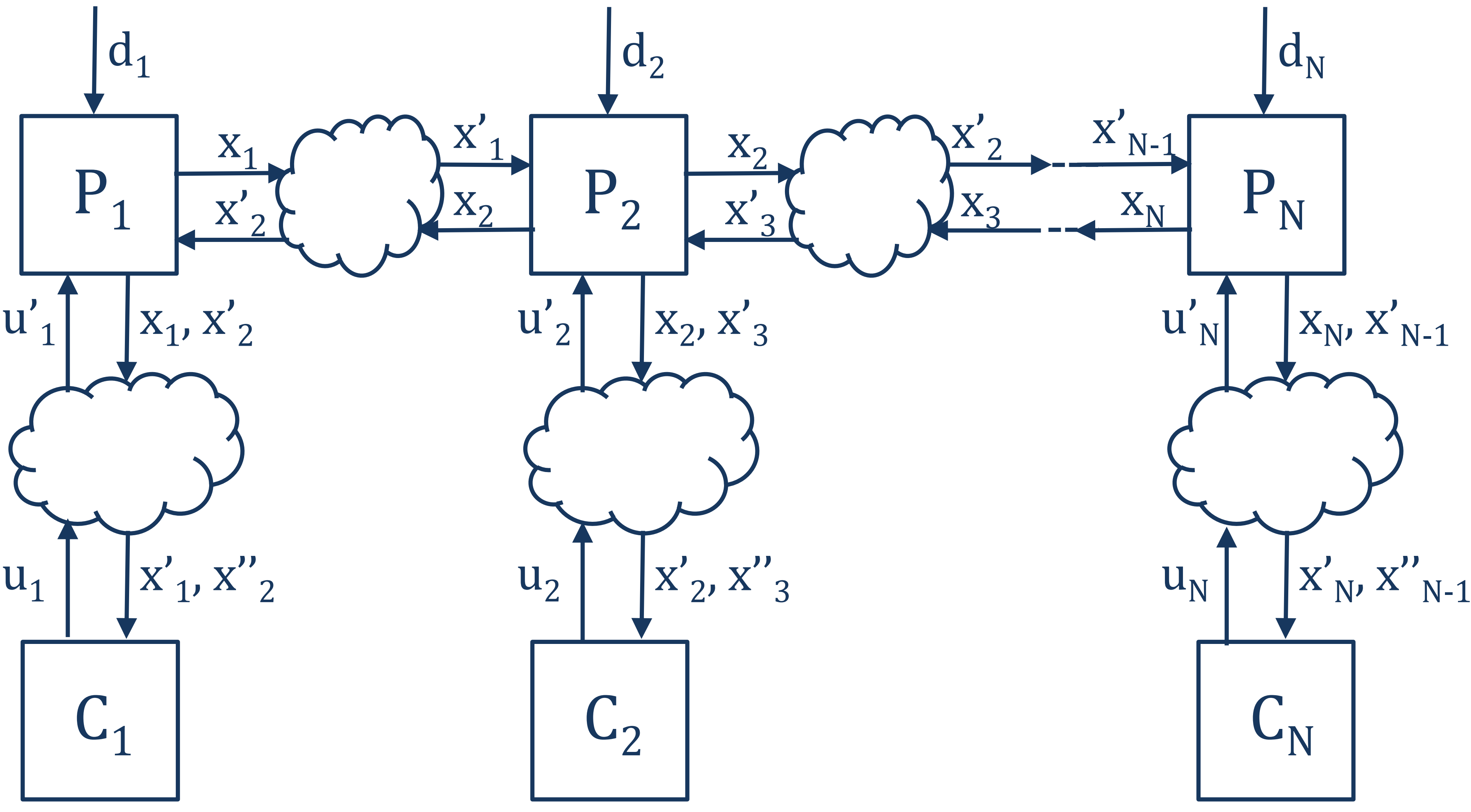
Large-scale networked nonlinear systems

Distributed Control Architecture

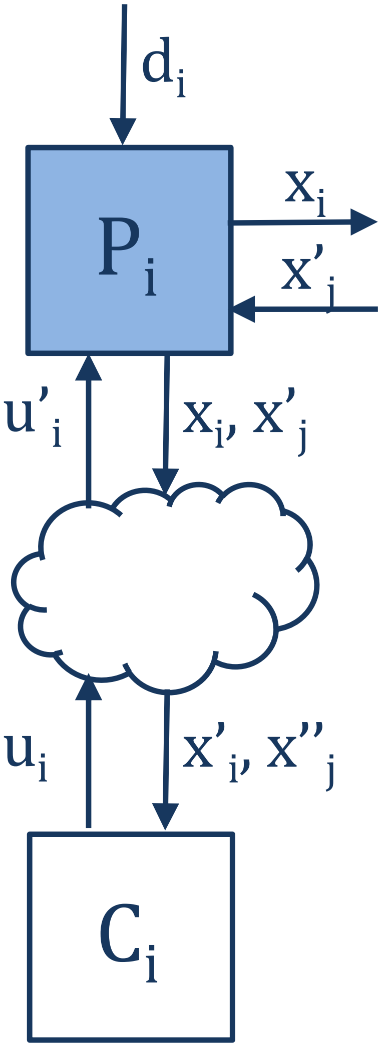


Large-scale networked nonlinear systems

Decentralized Control Architecture



Large-scale networked nonlinear systems



Plant P_i : nonlinear time-delay system

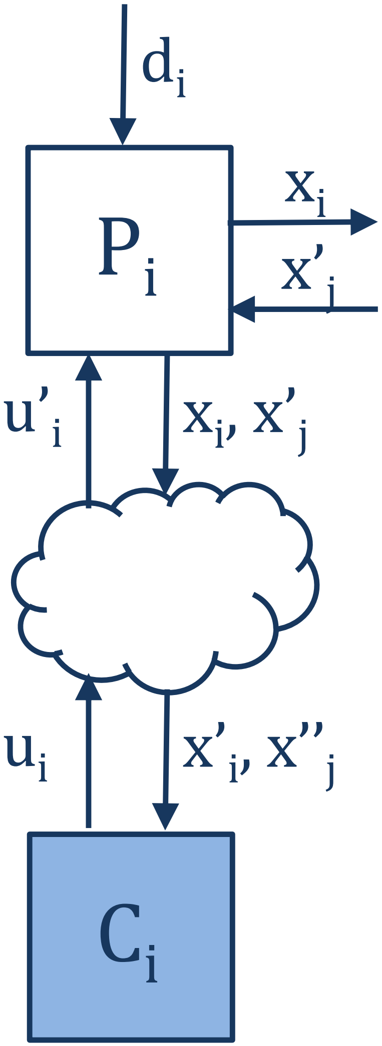
$$P_i: \begin{cases} \dot{x}_i(t) = f_i(x_i(t), x_i(t-\Delta_i(t)), x'_j(t), \dots, u_i(t), d_i(t)) \\ x_i(t) \in X_i \subseteq \mathbb{R}^{n_i}, x'_j(t) \in X_j \subseteq \mathbb{R}^{n_j}, u_i(t) \in U_i, d_i(t) \in D_i \subseteq \mathbb{R}^{l_i} \end{cases}$$

where:

- $x_i(t) \in X_i \subseteq \mathbb{R}^{n_i}$ internal state
- $x'_j(t) \in X_j \subseteq \mathbb{R}^{n_j}$ external measurable input (corresponding to the internal state of P_j corrupted by the network)
- $u_i(t) \in U_i$ control input, where set U_i is finite
- $d_i(t) \in D_i \subseteq \mathbb{R}^{l_i}$ external non-measurable disturbance
- $\Delta_i(t)$ time-varying delay

$\boldsymbol{P_i}$: infinite dimensional control system (because of delays)

Large-scale networked nonlinear systems



Controller C_i: automaton

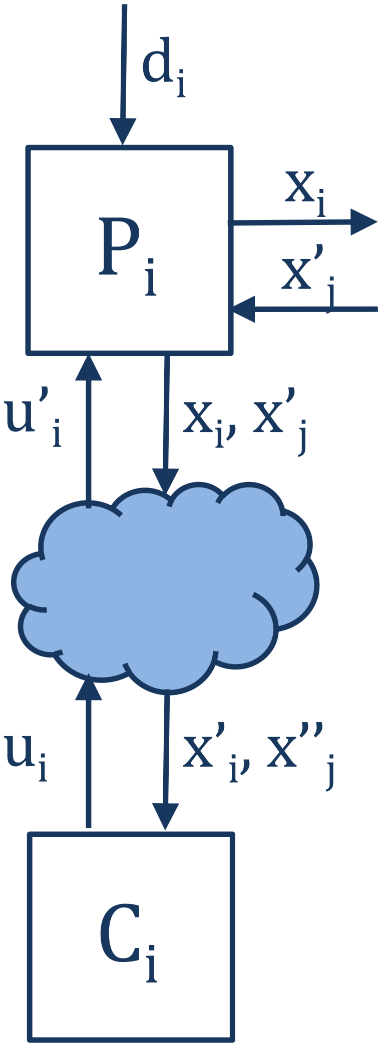
$$C_i: \begin{cases} z_i(k+1) \in g_i(z_i(k), x'_i(k), x'_{i'}(k), \dots) \\ u_i(k+1) \in h_i(z_i(k), x'_i(k), x'_{i'}(k), \dots) \\ z_i(k) \in Z_i, x'_i(k) \in X'_i, x'_{i'}(k) \in X'_{i'} \subseteq \mathbb{R}^{n_{i'}}, u_i(k) \in U_i \end{cases}$$

where:

- $z_i(k) \in Z_i$ internal state and Z_i finite set
- $x'_i(k) \in X_i$ external measurable input (corresponding to the internal state x_i(k) of P_i corrupted by the network)
- $x''_j(k) \in X_j$, external measurable input (corresponding to the internal state x_j(k) of P_j corrupted by the network
- $u_i(t) \in U_i$ is the output and U_i finite set

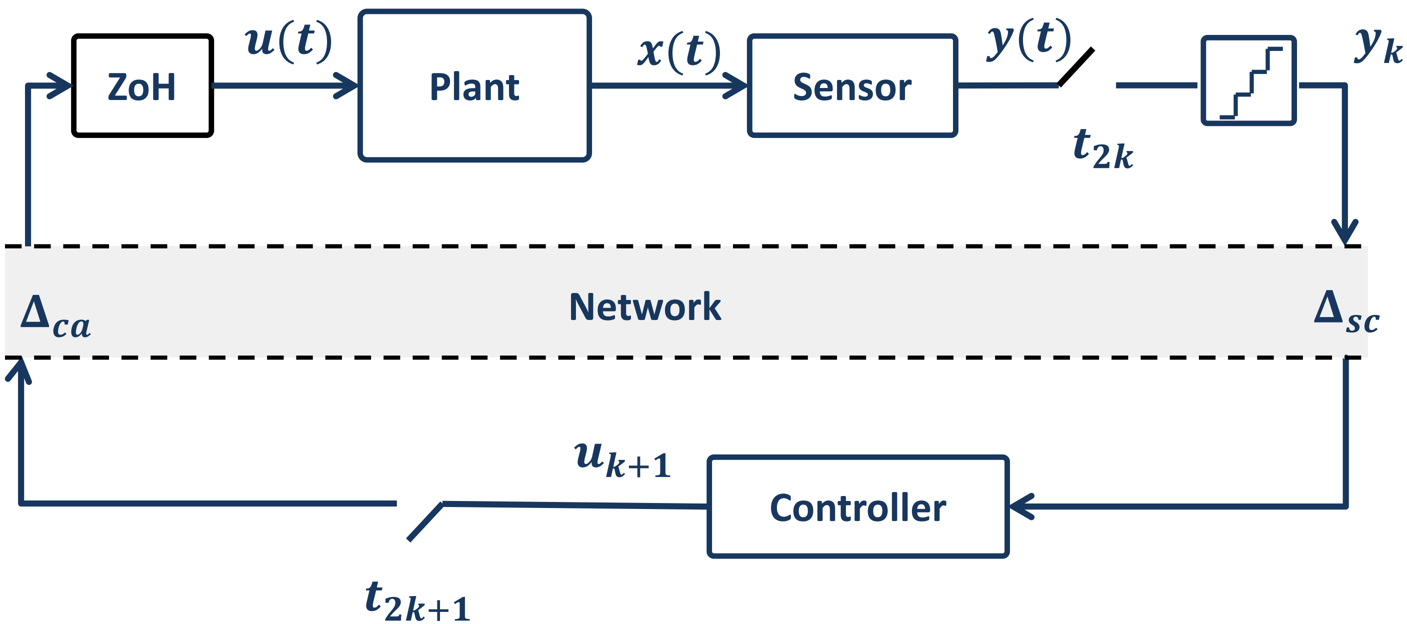
$\boldsymbol{C_i}$: finite, dynamic feedback and nondeterministic

Large-scale networked nonlinear systems



Nonideal communication infrastructure

Quantization errors, time-varying network access times, time-varying communication delays, limited bandwidth, packet losses, ...



Specifications: Regular languages

Recall

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

Example

$Y =$ the Latin alphabet

$L_1 =$ the Italian language $= \{ a, e, i, o, ad, al, ... \}$

$L_2 =$ all words over Y with symbol $a = \{ a, aa, aaa, aaaa, ... \}$

$L_3 =$ all words over Y of the form $a^n b^n$ with n integer $= \{ ab, aabb, aaabbb, ... \}$

L_1, L_2, L_3 are languages

Languages may be composed of a finite number or an infinite number of words

Example (continued)

L_1 is finite while L_2 and L_3 are not!

Specifications: Regular languages

Recall

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

Example

$Y =$ the Latin alphabet

$L_1 =$ the Italian language $= \{ a, e, i, o, ad, al, ... \}$

$L_2 =$ all words over Y with symbol $a = \{ a, aa, aaa, aaaa, ... \}$

$L_3 =$ all words over Y of the form $a^n b^n$ with n integer $= \{ ab, aabb, aaabbb, ... \}$

L_1, L_2, L_3 are languages

Definition

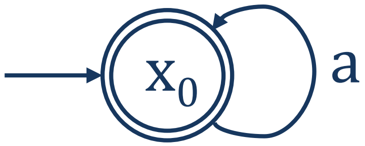
A language is regular if it can be represented by a finite state automaton

Example (continued)

L_1 is regular because it is finite

L_2 is regular because of existence of A_2

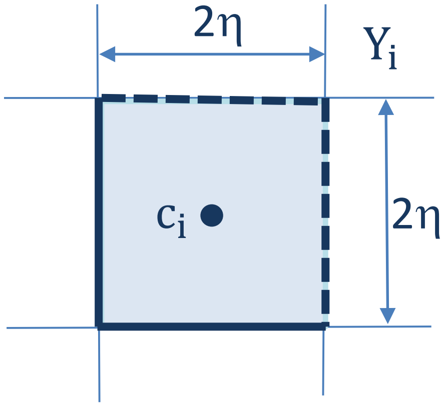
L_3 is not regular!



Automaton A_2 representing L_2

Specifications: Regular languages

Consider a collection Y of left-closed right-open hyper-cubes Y_i of $\mathbb{R}^n$



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

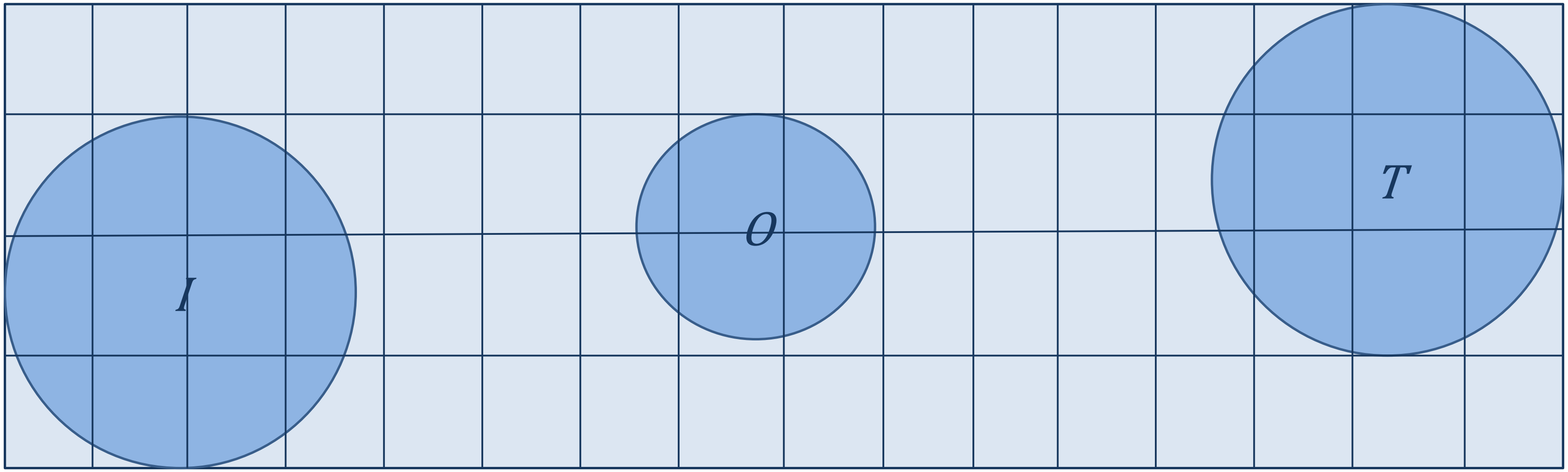
$c_i \in 2\eta\, \mathbb{Z}^n$

Y = Collection of Y_i

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

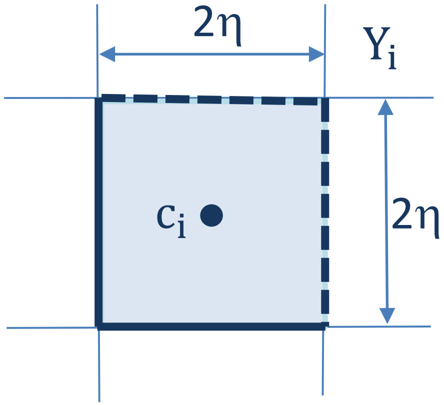
We consider a specification expressed as a regular language L_Q over Y

Example Starting from I reach T in finite time while avoiding O



Specifications: Regular languages

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



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

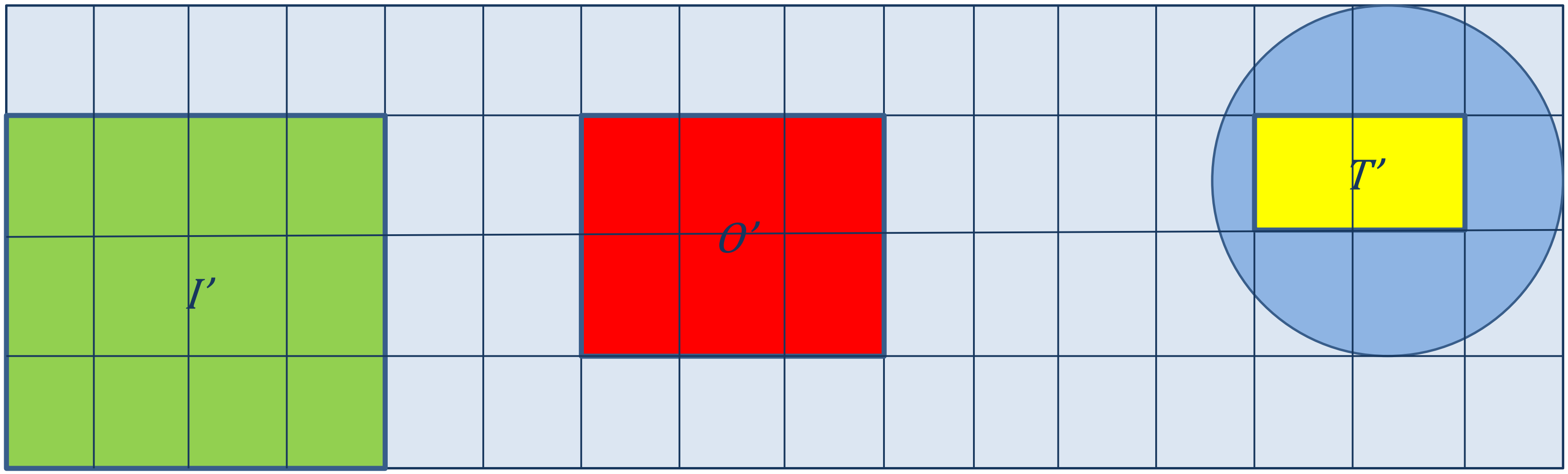
$\mathrm{c_i} \in 2\eta\, \mathbb{Z}^n$

Y = Collection of $\mathrm{Y_i}$

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

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

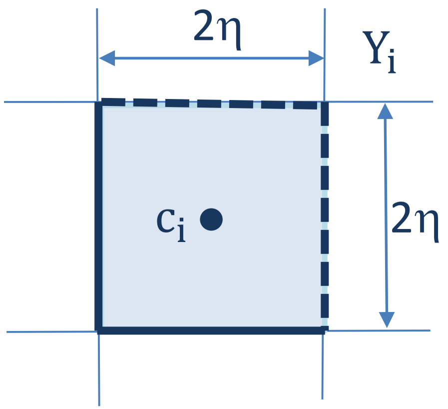
Example Starting from I reach T in finite time while avoiding O



L_Q = collection of words starting with [green], ending with [yellow] and with no [red]

Specifications: Regular languages

Consider a collection Y of left-closed right-open hyper-cubes Y_i of $\mathbb{R}^n$



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

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

Y = Collection of Y_i

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

We consider a specification expressed as a regular language L_Q over Y

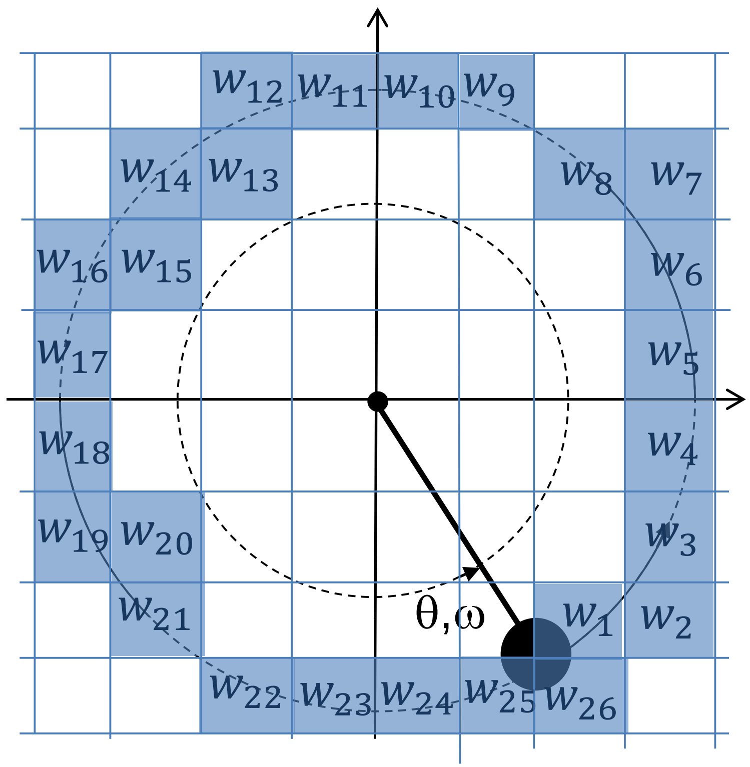
Specifications handled via regular language formalism :

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

Specifications: Regular languages

Example #1: Robotics

<u>Specification:</u> Enforcing periodic orbits



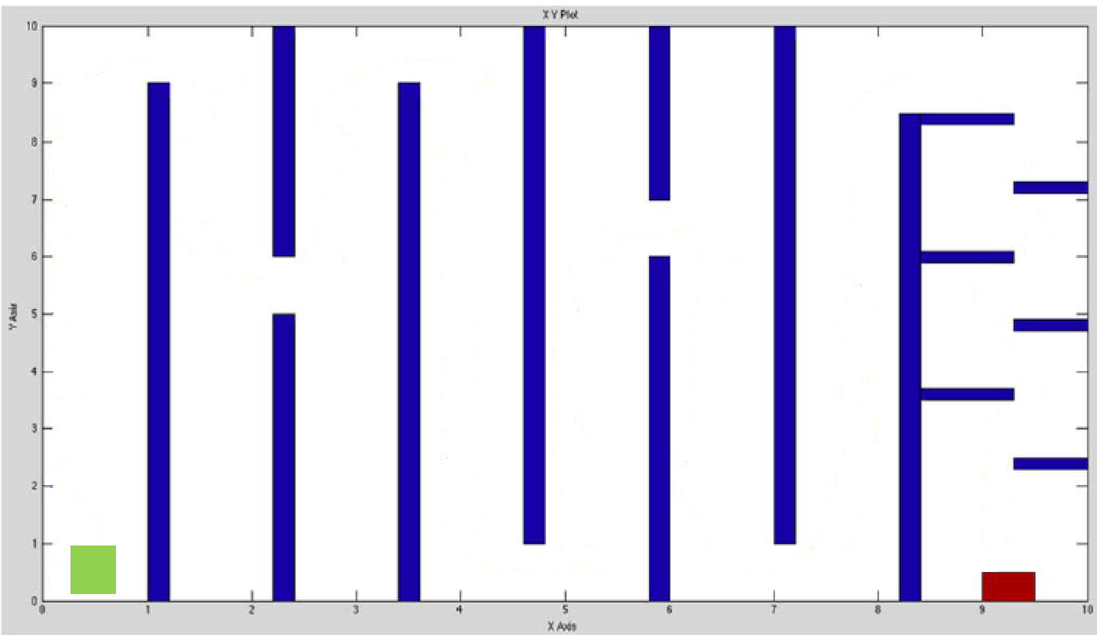
Robot KUKA IR363 @ LabAuRo in UNIVAQ

Regular language:
Word obtained by concatenating symbols $w_1 w_2 \dots w_{26}$

Specifications: Regular languages

Example #2: Robot motion planning

<u>Specification:</u> Starting from the green box, reach the red box while avoiding the blue obstacles



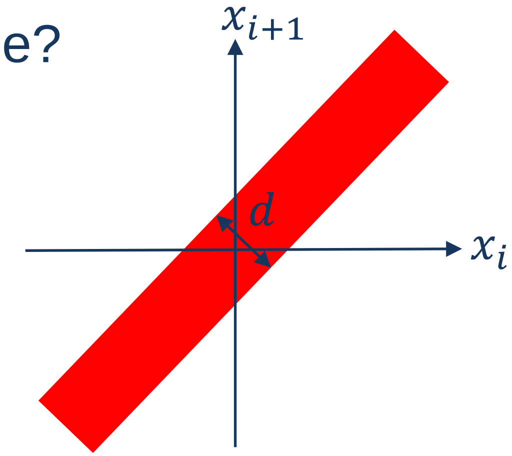
How to formalize this specification as a regular language?

Specifications: Regular languages

Example #3: Vehicle platooning

Specification: Maintain security distance from the vehicle in front of you

How to formalize this specification as a regular language?



Safety problem:
Define the set of good states as those for which $|x_i - x_{i+1}| \geq d$ and consider all words with symbols in the set of good states
(All words with no red symbols)

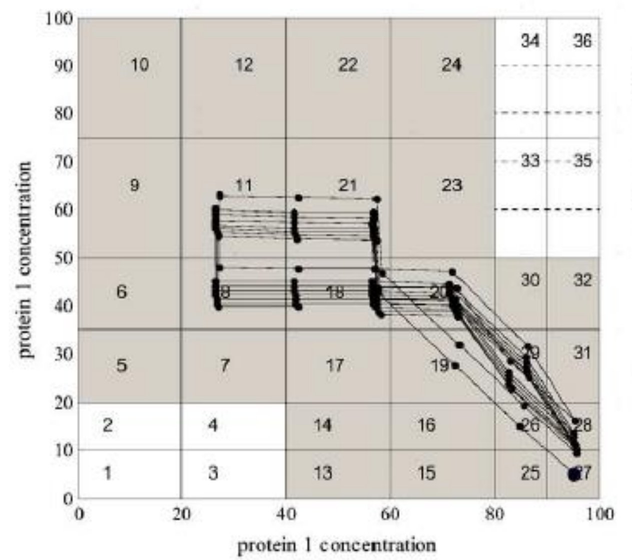
Specifications: Regular languages

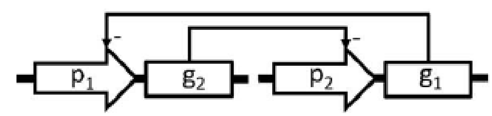
Example #4: Systems Biology (synthetic gene network*)

<u>Specification:</u> Enforce low concentration of protein 1 and high concentration of protein 2 while avoiding intermediate concentrations of both proteins

How to formalize this specification as a regular language?

Same approach as in Example #2





* Taken from :


IEEE TRANSACTIONS ON AUTOMATIC CONTROL, VOL. 57, NO. 6, JUNE 2012 1491

Temporal Logic Control of Discrete-Time Piecewise Affine Systems

Boyan Yordanov, *Member, IEEE*, Jana Tůmová, Ivana Černá, Jiří Barnat, and Calin Belta, *Senior Member, IEEE*

Control Problem Formulation

Given

- the network of control systems P_i
- a regular language specification L_Q
- a desired accuracy $\theta > 0$
- a sampling time $\tau > 0$

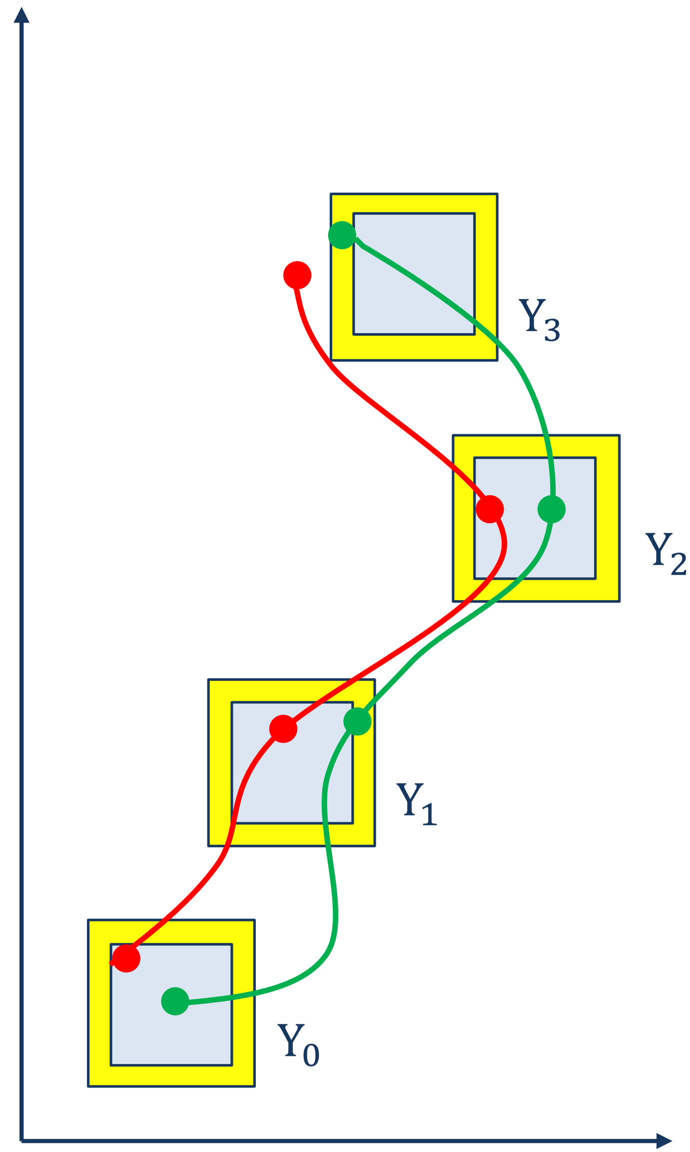
Find

- a set of initial states $X_0 \subseteq \mathbb{R}^n$
- a collection of decentralized controllers C_i

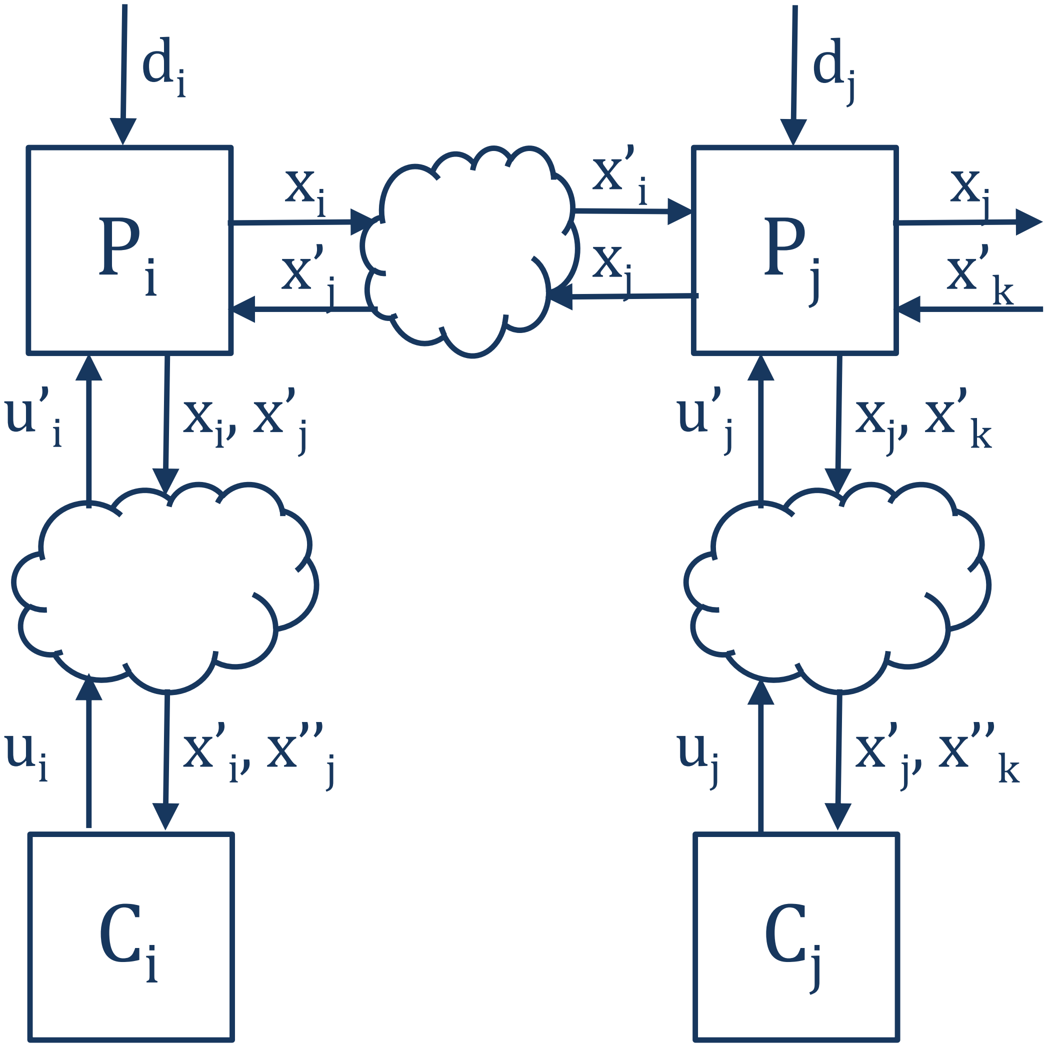
such that the controlled network, denoted P^C, satisfies the specification L_Q up to the accuracy θ, i.e.

for any trajectory $x(.)$ of P^C with $x(0) \in X_0$, there exists a word $q_0 q_1 \ldots q_{s_f}$ of the specification L_Q such that

$$| x(s\tau) - q_s | \leq \theta, \text{ for all } s \in [0; s_f]$$



The approach we take …



… a complementary approach :

- Single plants with no disturbances and delays
- Control design with logic specifications
- Efficient algorithms for control design
- Single plants with disturbances
- Single plants with delays
- Single, possibly unstable, plants
- Single plant, controller and communication infrastructure
- Decentralized control of networks of control systems with logic specifications

Schedule of the course

day	morning/ afternoon	lecture	title	who	duration (min)
1	m	1	Introduction	Di Benedetto	45
		2a	Review on internal and external stability notions for nonlinear systems	Pepe	45
			Break		
		2b	Review on internal and external stability notions for nonlinear systems	Pepe	45
		3	Metric transition systems	Di Benedetto	45
			lunch		
	a	4	Regular languages	Pola	90
			Break		
		5	Relations among metric transition systems	Di Benedetto	90
2	m	6	Symbolic models for stable nonlinear systems	Pola	90
			Break		
		7	Control design and efficient algorithms	Borri	90
			lunch		
	a	8	Symbolic models and control for nonlinear systems with disturbances and applications	Borri	60
		9a	Nonlinear time-delay systems: basic theory and stability	Pepe	30
			Break		
		9b	Nonlinear time-delay systems: basic theory and stability	Pepe	90
3	m	10	Symbolic models for time-delay systems	Pola	30
		11	Symbolic models for possibly unstable nonlinear systems	Pola	30
		12	Symbolic models and control for networked nonlinear systems	Borri	30
			Break		
		13	Decentralized control of networks of nonlinear systems	Pola	30
		14	Tools	Borri	30
		15	Conclusions	Pola	30

Keys:	background	basic	advanced