SAPIENZA
UNIVERSITÀ DI ROMA

Model Checking Lab

Toni Mancini, Annalisa Massini, Federico Mari,
Igor Melatti, Ivano Salvo, **Enrico Tronci**

Computer Science Department
Sapienza University of Rome, Italy

http://mclab.di.uniroma1.it

Sapienza University of Rome

- Founded in **1303**
- The **largest** university in Europe
  - **115K** students
  - **7K** foreign students
  - **1K** incoming Erasmus students / year
- Steadily within **top 3%** world universities
  [Shangai Ranking]
- **250** Bachelor & Master Programmes
- **11** Faculties
- **63** Departments

Computer Science Dept. @ Sapienza

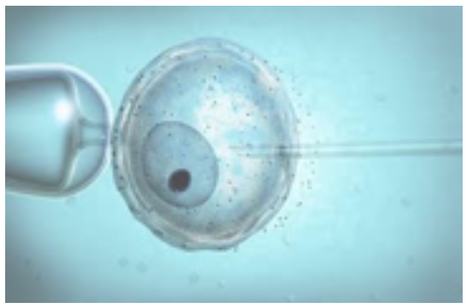
- **45** Faculty Members
- **23** Post-Doc Researchers
- **20** PhD Students

- Internationally active in most of the major CS **research areas**:

- ✦ Algorithms & Data Structures
- ✦ **Artificial Intelligence**
- ✦ Combinatorics
- ✦ Computational Complexity
- ✦ **Computer Architectures**
- ✦ Computer Networks
- ✦ Computer Security
- ✦ **Database Systems**
- ✦ Web Information Retrieval
- ✦ **Formal Methods**
- ✦ Human-Computer Interaction
- ✦ Computer Graphics
- ✦ Information Theory
- ✦ **Software Engineering**

Model Checking Lab @ Sapienza

- Research group within the Computer Science Department
- **6** faculty members, **1** post-docs, **3** PhD students,
  1 research fellow, **10** graduate students
- **Research focus**: design and development of software tools for **model-based** verification, validation and synthesis of **mission-** and **safety-critical embedded control systems**:
  - aerospace
  - critical infrastructures
  - transportation
  - medicine
  - smart grids



MClab

Model-Based System Verification @ MCLab

Disturbance Model (formal model of operational scenarios)

SyLVer

System Level Formal Verifier

https://bitbucket.org/mclab/sylver-simulink-driver

LOAD - RUN - FREE -STORE

Optimised Simulation Campaign

Simulator Driver

Parallel (cluster)

Optimised Simulation Campaign

Simulator Driver

Simulation Based Verification

Simulator

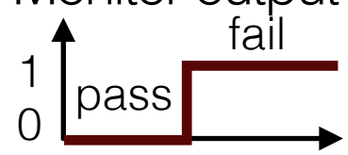
CPS Model + Monitor

Simulator

CPS Model + Monitor

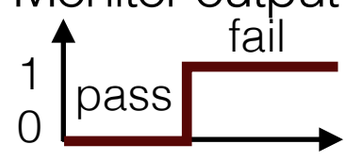
Omission Probability

Monitor output



Omission Probability

Monitor output



Model-Based Control SW Synthesis @ MCLab

Desired Controllable Region

Goal Region

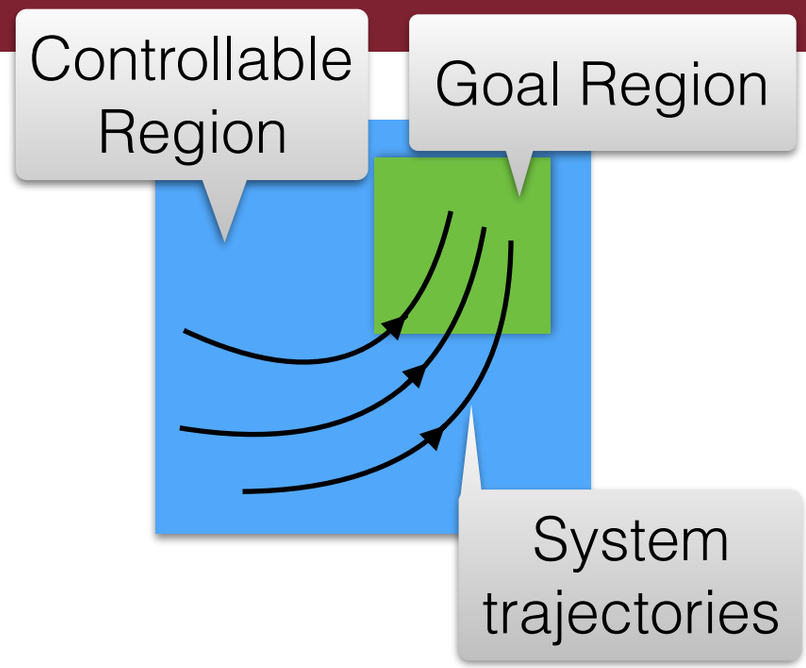
AD/DA n. of bits

Plant Model

QKS

Quantized Controller Software Generator

https://bitbucket.org/mclab/qks

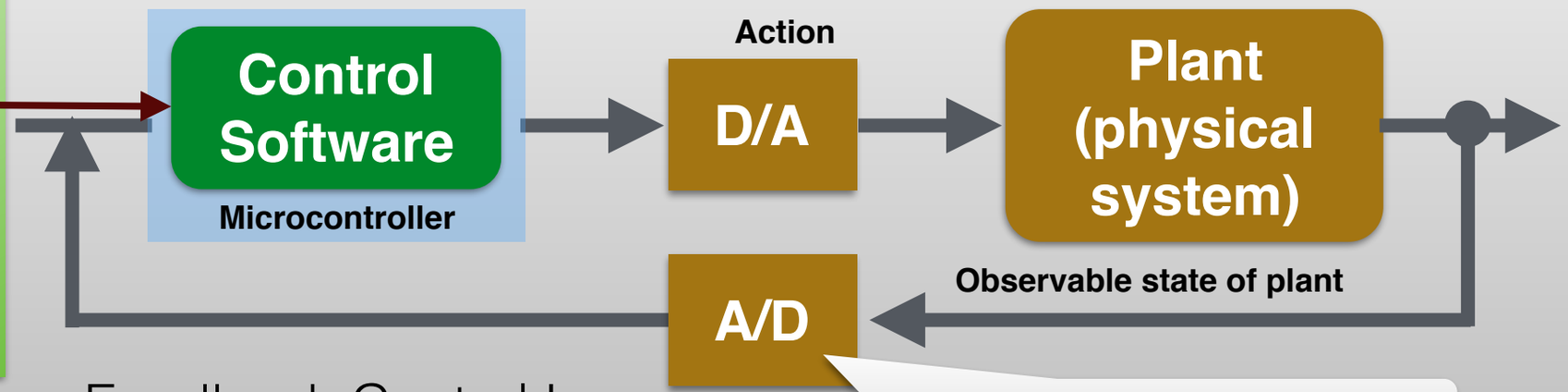


NoSol

Unknown

SOL

Control Software
Actual Controllable Region
Robustness by Construction
Guaranteed WCET



Feedback Control Loop

MCLab in Aerospace

EC FP7 Ulisse (4.8 M€)
Verification & Validation of mission planning and on-board procedures

ESA ITI Verifying Satellite Operational Procedures (150 k€)
Verification & Validation of ground segment satellite operational procedures

ESA ITT System & Software Functional Requirements Technique (200 k€)
Verification & Validation of system level design for satellite and avionics vehicles

MCLab in Transportation

MIUR Tramp, Setram, Interception (3.5 M€)
Optimal management of intermodal transportation of dangerous goods, guaranteeing security standards

Safety verification of communication protocols and control policies for the control center

FILAS Sintesi (100 k€)
Sense and response system for critical resource management

MCLab in Critical Infrastructures

SAPP, IRRIIS, Safeguard, SafeTunnel, Icaro (10 M€)
Design and safety verification of control and communication systems for critical infrastructures

LOG.IN

ENEA

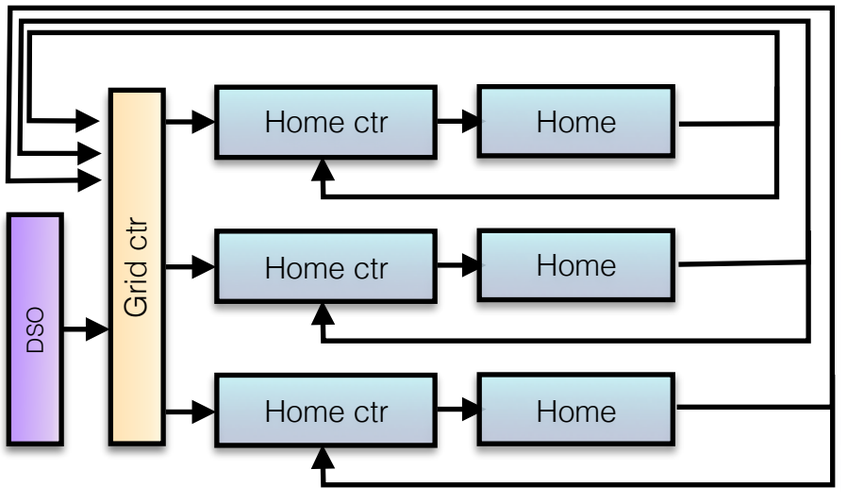
MCLab in Smart Grids

EC FP7 SmartHG (3.5 M€)
Energy Demand Aware Open Services for Smart Grid Intelligent Automation

Coordinator: MCLab

Design and formal verification of hierarchical control policies for the Smart Grid

SmartHG benefits: optimisation of grid management, minimisation of energy cost and CO2 emissions

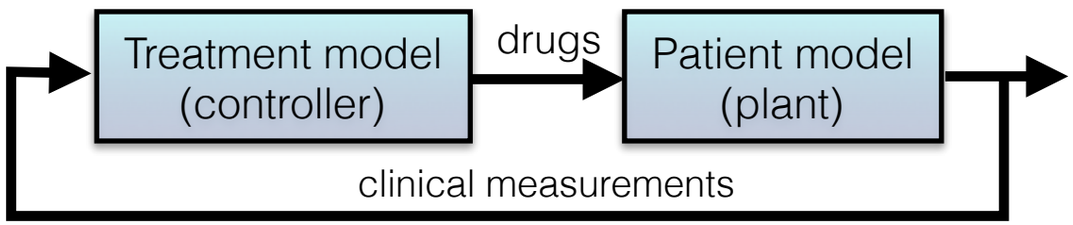


MCLab in Medicine

EC FP7 Paeon (2.5 M€)
Model Driven Computation of Treatments for Infertility Related Endocrinological Diseases

Coordinator: MCLab

SAPIENZA
UNIVERSITÀ DI ROMA



Modelling of human physiology (virtual physiological human)

Model based automatic verification and synthesis of personalised clinical treatments

UniversitätsSpital Zürich

HOCHSCHULE LUZERN

Hannover Medical School

Contacts

Toni Mancini, Annalisa Massini, Federico Mari,
Igor Melatti, Ivano Salvo, **Enrico Tronci**

Computer Science Department
Sapienza University of Rome
Via Salaria 113
00198 Rome, Italy

tronci@di.uniroma1.it
http://mclab.di.uniroma1.it