UNIVERSITÀ di VERONA

Dipartimento di INFORMATICA

ESD Electronic Systems Design

Methodologies for large-scale smart cyber-physical systems

Nicola Bombieri, Franco Fummi, Luca Geretti,
Graziano Pravadelli, Davide Quaglia, Tiziano Villa

Speaker: Gabriele Miorandi

3rd Italian Workshop on Embedded Systems, Sept. 13-14, 2018, Siena

Outline

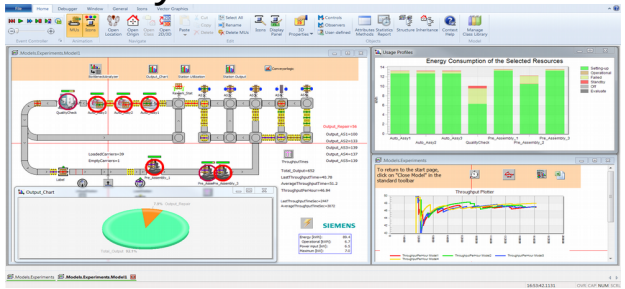
- Application context
- Approach
- Design
  - Network synthesis
  - Embedded vision applications
- Modeling & Verification
  - Simulation
  - Formal verification
  - Functional Safety evaluation
  - Detection of firmware vulnerabilities
- References

Outline

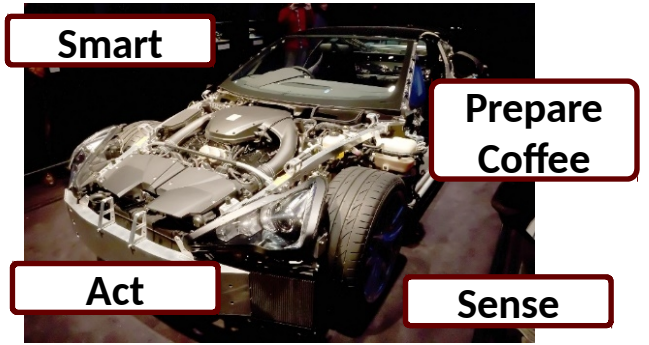
- **Application context**
- Approach
- Design
  - Network synthesis
  - Embedded vision applications
- Modeling & Verification
  - Simulation
  - Formal verification
  - Functional Safety evaluation
  - Detection of firmware vulnerabilities
- References

Large scale smart cyber-physical systems

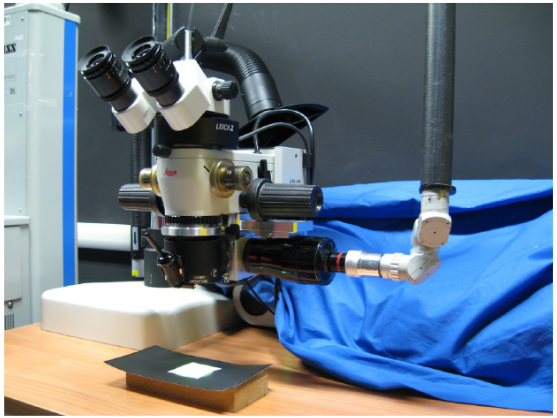
Industry 4.0



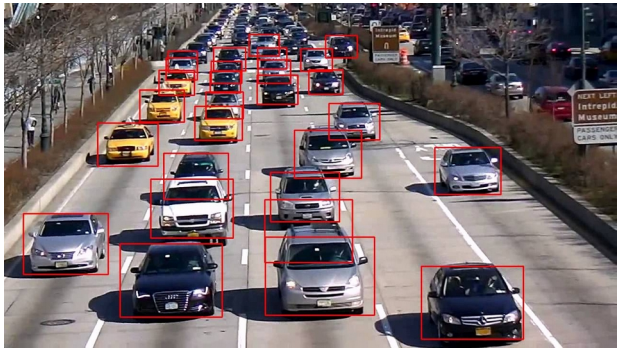
Automotive



Robotic surgery

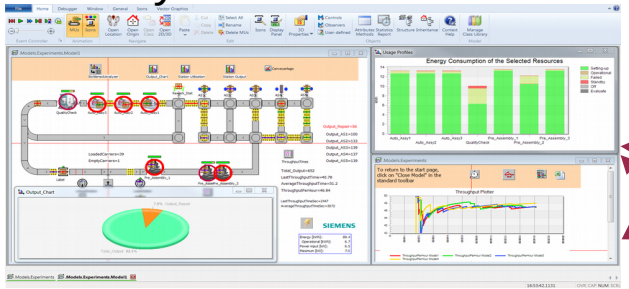


Embedded vision

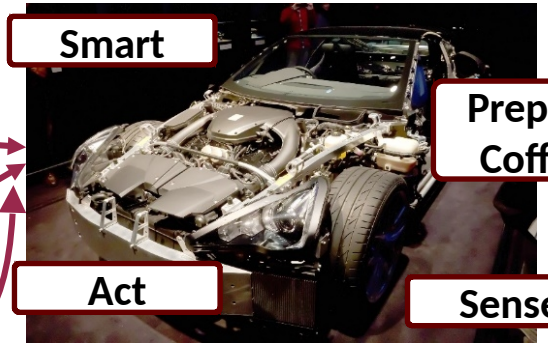


Large scale smart cyber-physical systems

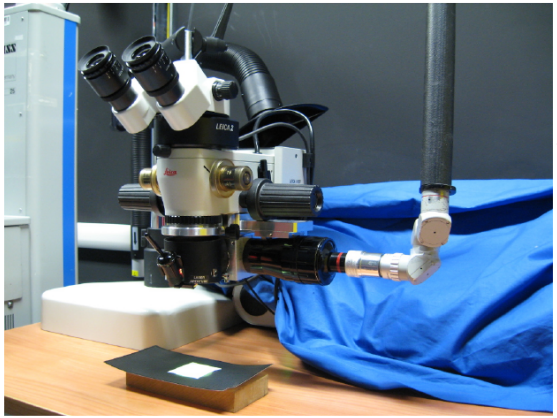
Industry 4.0



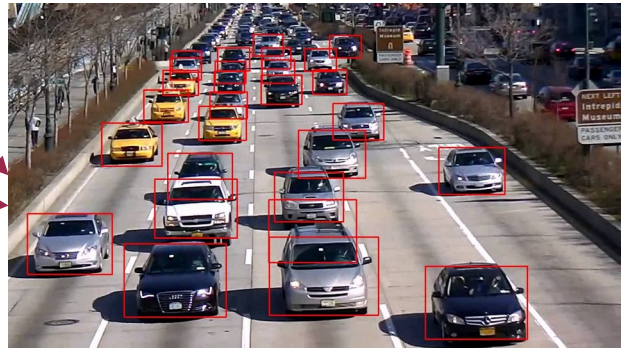
Automotive



Robotic surgery



Embedded vision



Outline

- Application context
- **Approach**
- Design
  - Network synthesis
  - Embedded vision applications
- Modeling & Verification
  - Simulation
  - Formal verification
  - Functional Safety evaluation
  - Detection of firmware vulnerabilities
- References

Holistic approach

- Analog and digital **harware** components
  - Register transfer level (RTL) vs. Transaction Level (TL)
  - Structural vs. behavioral
  - Linear vs. non-linear
- Embedded and HW-dependent **software** (firmware)
  - Tight connection with HW
  - Reactive to stimula from HW and from the environment
- Physical **environment**
- **Network**
  - Internet, ZigBee, CAN, Time-sensitive networks, …

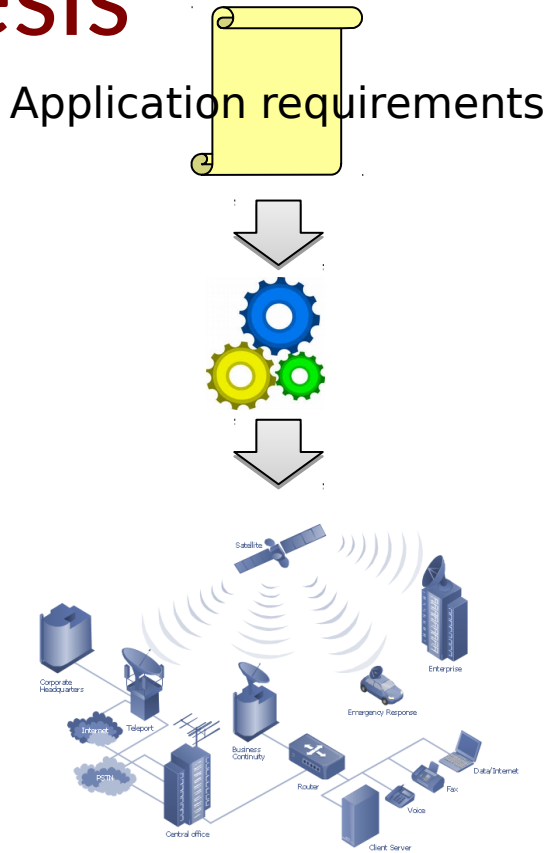
Outline

- Application context
- Approach
- **Design**
  - Network synthesis
  - Embedded vision applications
- Modeling & Verification
  - Simulation
  - Formal verification
  - Functional Safety evaluation
  - Detection of firmware vulnerabilities
- References

Davide Quaglia
Enrico Fraccaroli

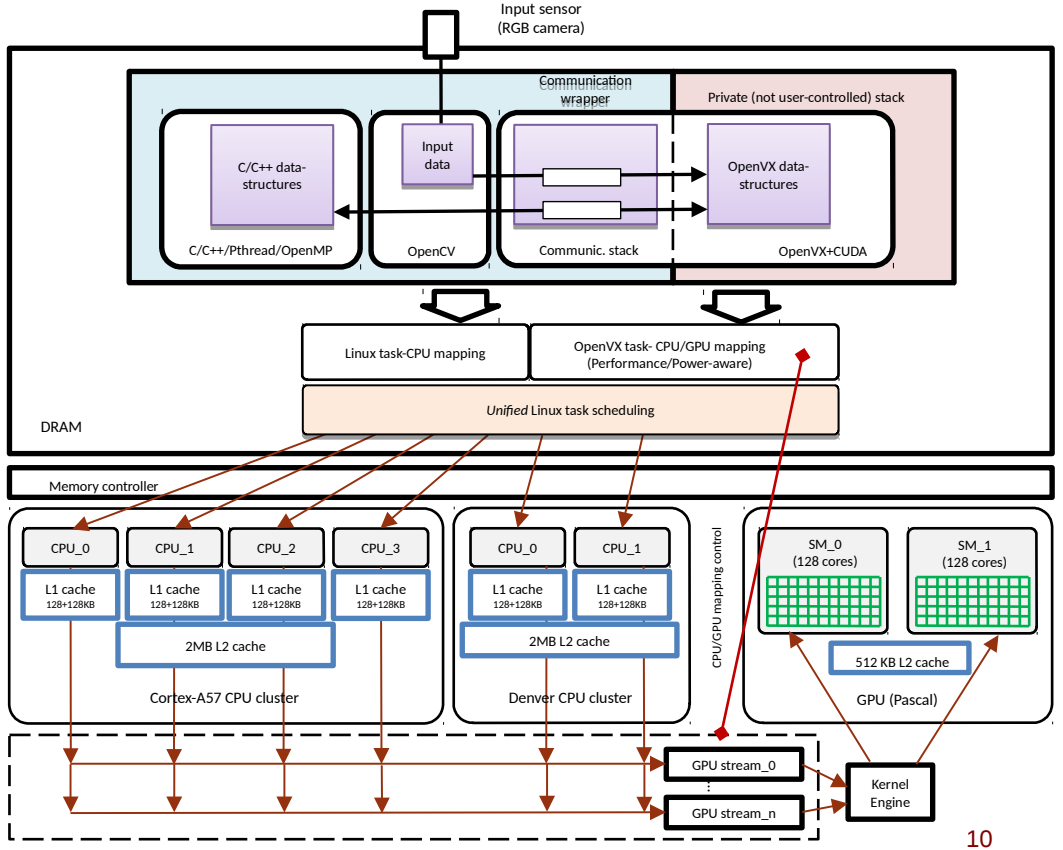
Network Synthesis

- Automatic methodology to design the network infrastructure
  - Topology
  - Nodes (number, type)
  - Channel types
  - Protocols
- Optimal allocation of resources with respect to given metrics (e.g., cost, bandwidth, delay, robustness)
- Needed to address the challenging size and heterogeneity of future's networks



Embedded vision applications

- Software optimization by considering different design constraints!
  - Performance
  - Energy & Power
- Efficiently use system resources (CPUs, GPUs, DSPs, FPGAs, etc.) to improve energy efficiency!



Nicola Bombieri
Stefano Aldegheri

Outline

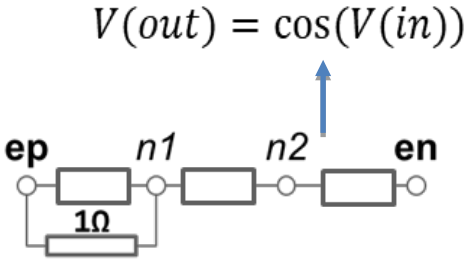
- Application context
- Approach
- Design
  - Network synthesis
  - Embedded vision applications
- **Modeling & Verification**
  - Simulation
  - Formal verification
  - Functional Safety evaluation
  - Detection of firmware vulnerabilities
- References

Franco Fummi
Enrico Fraccaroli

Automatic Analog Abstraction

Transform an analog design from **circuit level** to **functional level** and **move complexity** from **simulation** to **generation-time**

- *Functional* : **Mathematical** signal-flow description
- *Circuit* : Connection of **circuit** components



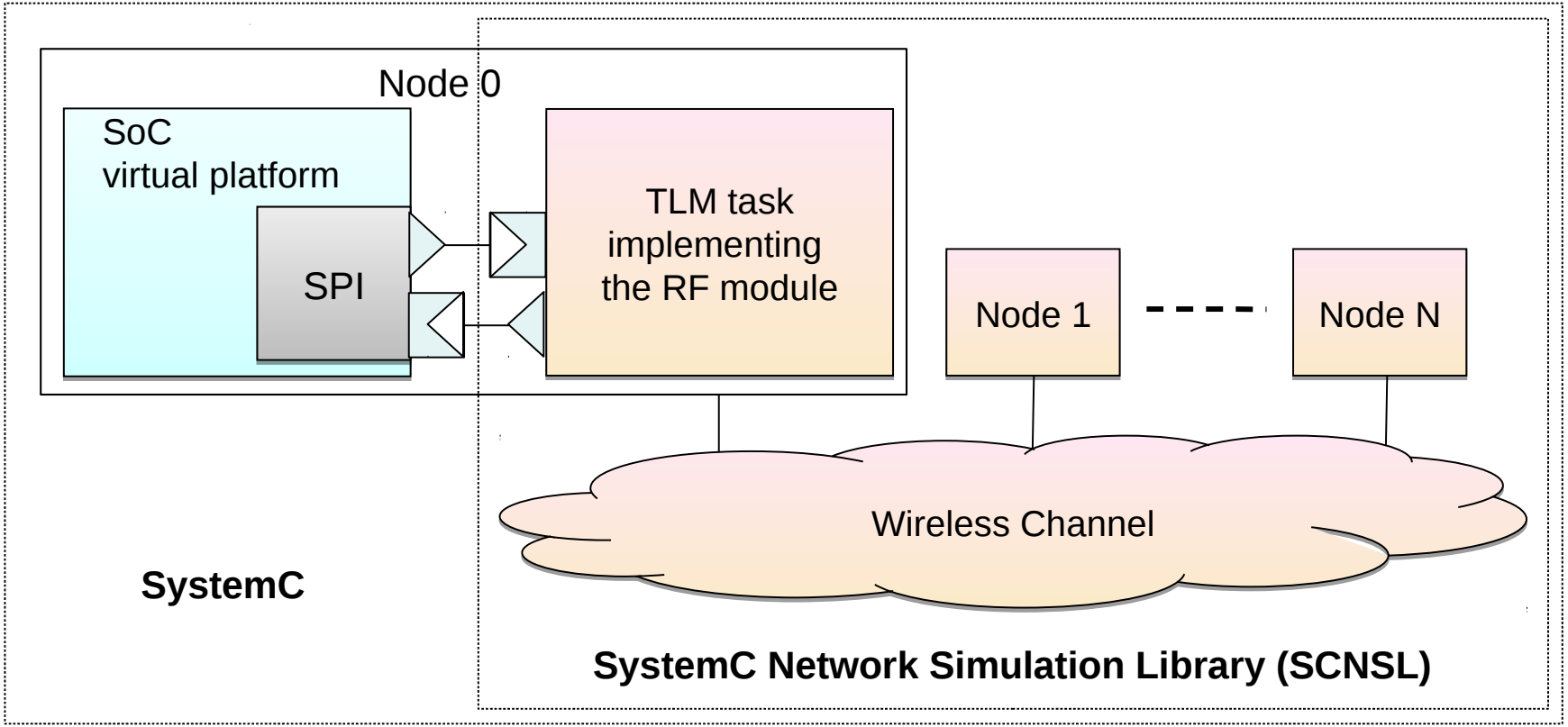
Methodology

1. Parse circuit description
2. Apply Kirchhoff's laws
3. Reconstruct input-output relations of the model
4. Outlines the minimal set of equations for describing its behavior
5. Discretize and symbolicaly solves the minimal set of equations
6. Generate optimized C++ code

Tool:
HIFSuite

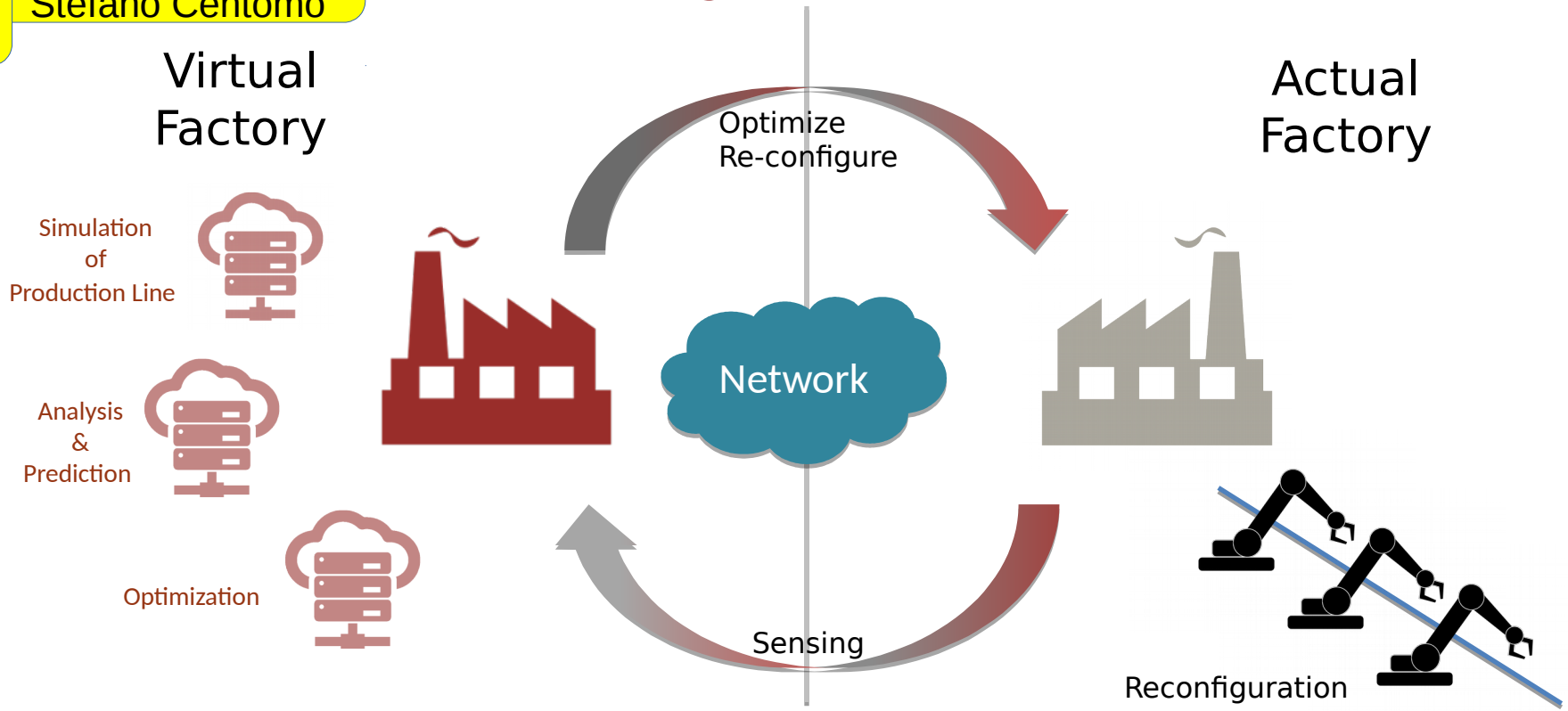
Davide Quaglia

Joint System-Network Simulation



Franco Fummi
Stefano Centomo

Digital Twin



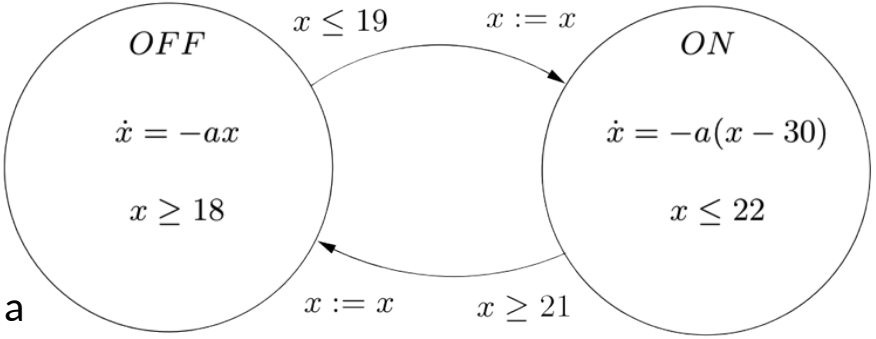
A simulation model of the plant is maintained during the life time of the actual plant

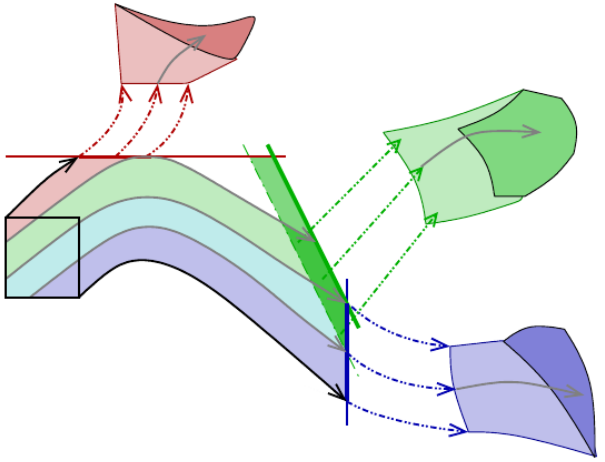
- It is refined by using data sensed from the actual plant
- It is used to test optimizations and re-configurations of the actual plant

Tiziano Villa
Luca Geretti

Formal Verification

- **Hybrid automata**: formal approach to mix continuous and discrete behaviors
  - Finite state machines enriched with continuous dynamics for each state
- **Reachable set**: the set of states reached after a (possibly infinite) evolution time
  - From the reachable set we can extract properties of the system under analysis
- **Ariadne**: tool for formal verification based on hybrid automata and reachability analysis
  - Jointly developed by UNIVR and the University of Maastricht
  - Written as a C++ library, released as an open source distribution: http://www.ariadne-cps.org

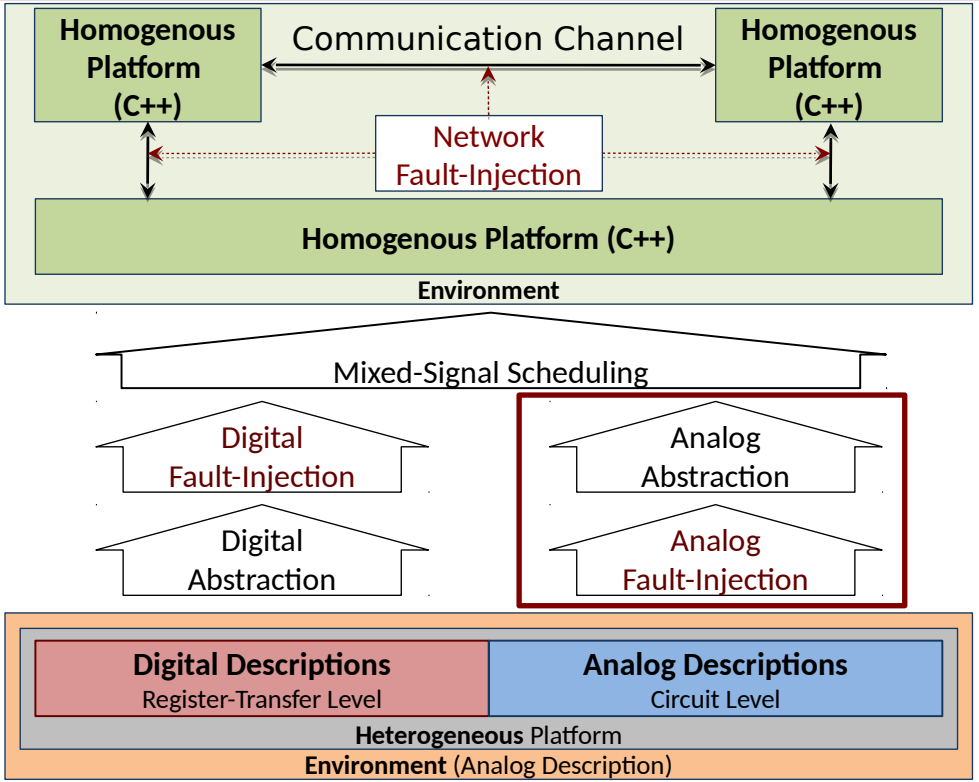




Franco Fummi
Enrico Fraccaroli

Functional Safety Evaluation

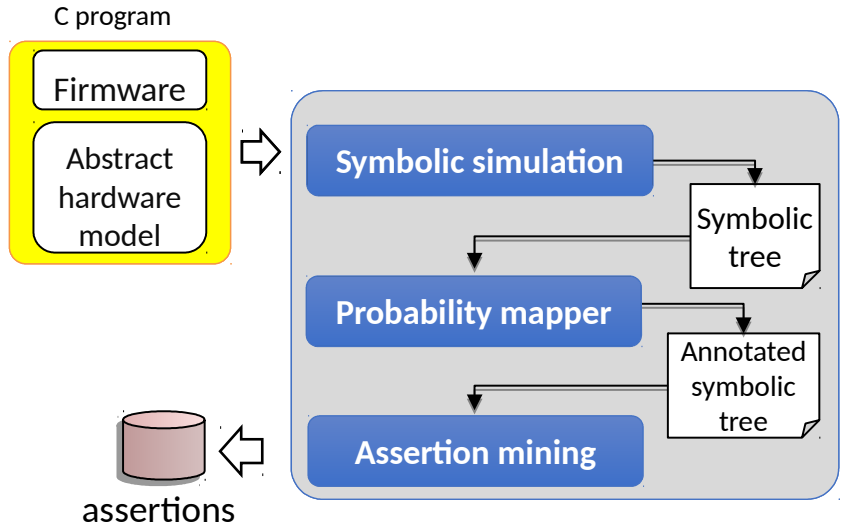
Development of a **functional safety** methodology for **Cyber-Physical System**



Tool:
HIFSuite

Detection of firmware vulnerabilities

- A hardware/software component affected by bugs is an excellent back door for attackers
- Bugs always hide in places we have not looked in (verified)
  - Those places must be difficult to exercise
  - They can only be reached through complex/rare execution paths
- The proposed approach mines **rare execution paths** in three sequential steps:



Graziano Pravadelli
Alessandro Danese

Outline

- Application context
- Approach
- Design
  - Network synthesis
  - Embedded vision applications
- Modeling & Verification
  - Simulation
  - Formal verification
  - Functional Safety evaluation
  - Detection of firmware vulnerabilities
- **References**

Some last year's references

- M. Lora, S. Vinco, E. Fraccaroli, D. Quaglia, and F. Fummi, "Analog Models Manipulation for Effective Integration in Smart System Virtual Platforms", IEEE TCAD, 2017
- E. Fraccaroli, F. Stefanni, F. Fummi, and M. Zwolinski. "Fault Analysis in Analog Circuits through Language Manipulation and Abstraction", FDL, 2017
- E. Fraccaroli, F. Stefanni, R. Rizzi, D. Quaglia, F. Fummi, "Network Synthesis for Distributed Embedded Systems", IEEE TCOMP, 2018
- A. Geraldes, L. Geretti, R. Muradore, P. Fiorini, L.S. Mattos, T. Villa, "Verification of medical CPS: a laser incision case study", ACM TCPS, Vol. 2, N. 4, July 2018
- A. Danese, V. Bertacco and G. Pravadelli, "Symbolic assertion mining for security validation", DATE, 2018

1st PhD School on Emerging Technologies for Design and Engineering of Electronics Systems

- Verona, October 5-7 2018, Department of Computer Science
- The school will be co-located with the 26th IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC 2018), to be held in Verona, 8-10 October 2018
- Lectures:
  1. Machine learning techniques for resilient system design (Mehdi B. Tahoori, Karlsruhe Institute of Technology, Germany)
  2. Secure processor architectures (Todd Austin, University of Michigan, USA)
  3. Memristive devices for computing: circuits, architectures and applications (Said Hamdioui, Delft University of Technology, Netherlands)
  4. Advances in wearable sensors and interfaces: Cyber-physical systems for bio-signals real-time processing and actuators control (Daniela De Venuto, Politecnico di Bari, Italy)
  5. Test & reliability challenges in the internet of things (Yervant Zorian, Synopsys Fellow & Chief Architect)

Register at scheme.di.univr.it

Thank you!

For questions and further details:
name.surname@univr.it