UNIVERSITÀ di VERONA

Dipartimento di INFORMATICA

ESD Electronic Systems Design

Synthesis Verification Testing Power Communication

Methodologies for large-scale smart cyber-physical systems

Recent research of the Cyber-Physical Systems group of the University of Verona, department of Computer Science

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

Speaker: Nicola Bombieri

5th Italian Workshop on Embedded Systems, 2020, Catania

Outline

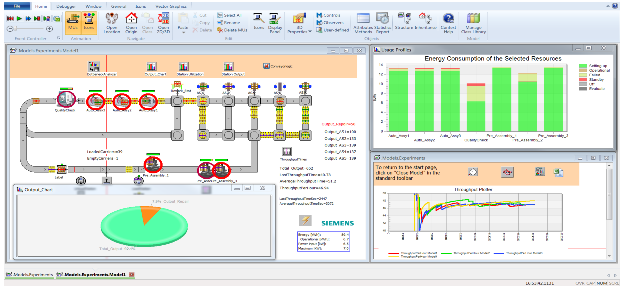
- Application context
- Design
  - Network synthesis
  - Embedded vision applications
- Modeling & Verification
  - Analysis of industrial plants
  - Joint system-network simulation
  - ROS-compliant containerized verification monitors
  - Catching sources of vulnerabilities
  - Automatic analog abstraction
  - Formal Methods for System Design
  - Run-time verification of parametric systems
- References

Outline

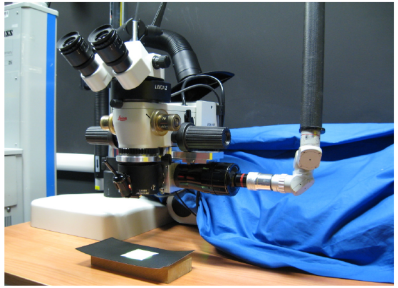
- **Application context**
- Design
  - Network synthesis
  - Embedded vision applications
- Modeling & Verification
  - Analysis of industrial plants
  - Joint system-network simulation
  - ROS-compliant containerized verification monitors
  - Catching sources of vulnerabilities
  - Automatic analog abstraction
  - Formal Methods for System Design
  - Run-time verification of parametric systems
- References

Large scale smart cyber-physical systems

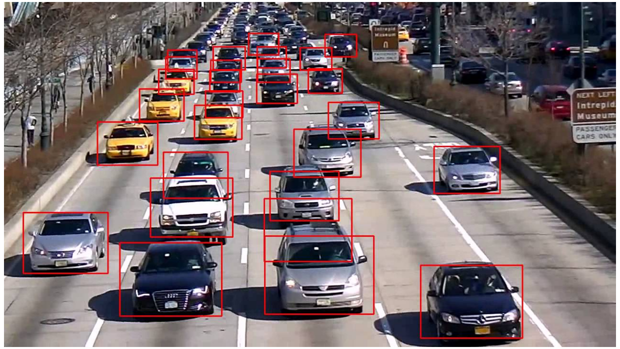
Industry 4.0



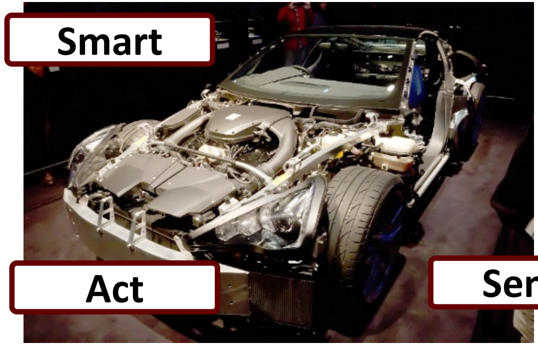
Robotic surgery



Embedded vision



Automotive



Smart

Act

Sense

Tight interaction between
- **processing,**
- **communication** and
- **sensing/actuation** devices

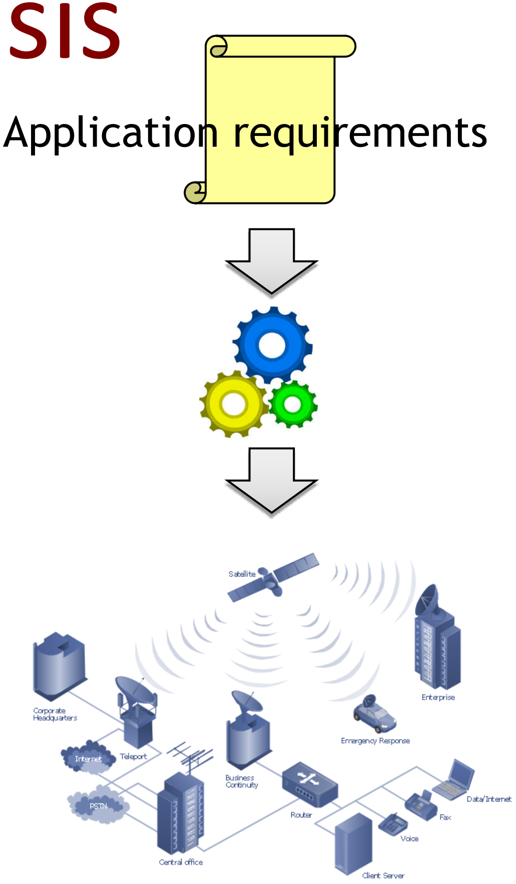
Outline

- Application context
- **Design**
  - Network synthesis
  - Embedded vision applications
- Modeling & Verification
  - Analysis of industrial plants
  - Joint system-network simulation
  - ROS-compliant containerized verification monitors
  - Catching sources of vulnerabilities
  - Automatic analog abstraction
  - Formal Methods for System Design
  - Run-time verification of parametric systems
- 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


Application requirements

Davide Quaglia
Enrico Fraccaroli

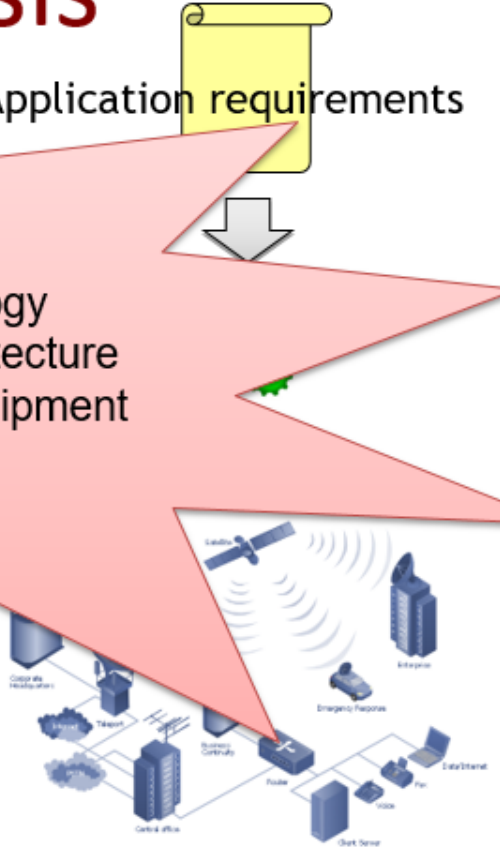
Network Synth sis

- Auto ethodology n the netw ct
  - Topolog
  -
  - Prot
- Opt respect to given bandwidth, del ust
- Needed to ad ess the ch ng size and heterogeneity of e's networks

Application to Industry 4.0

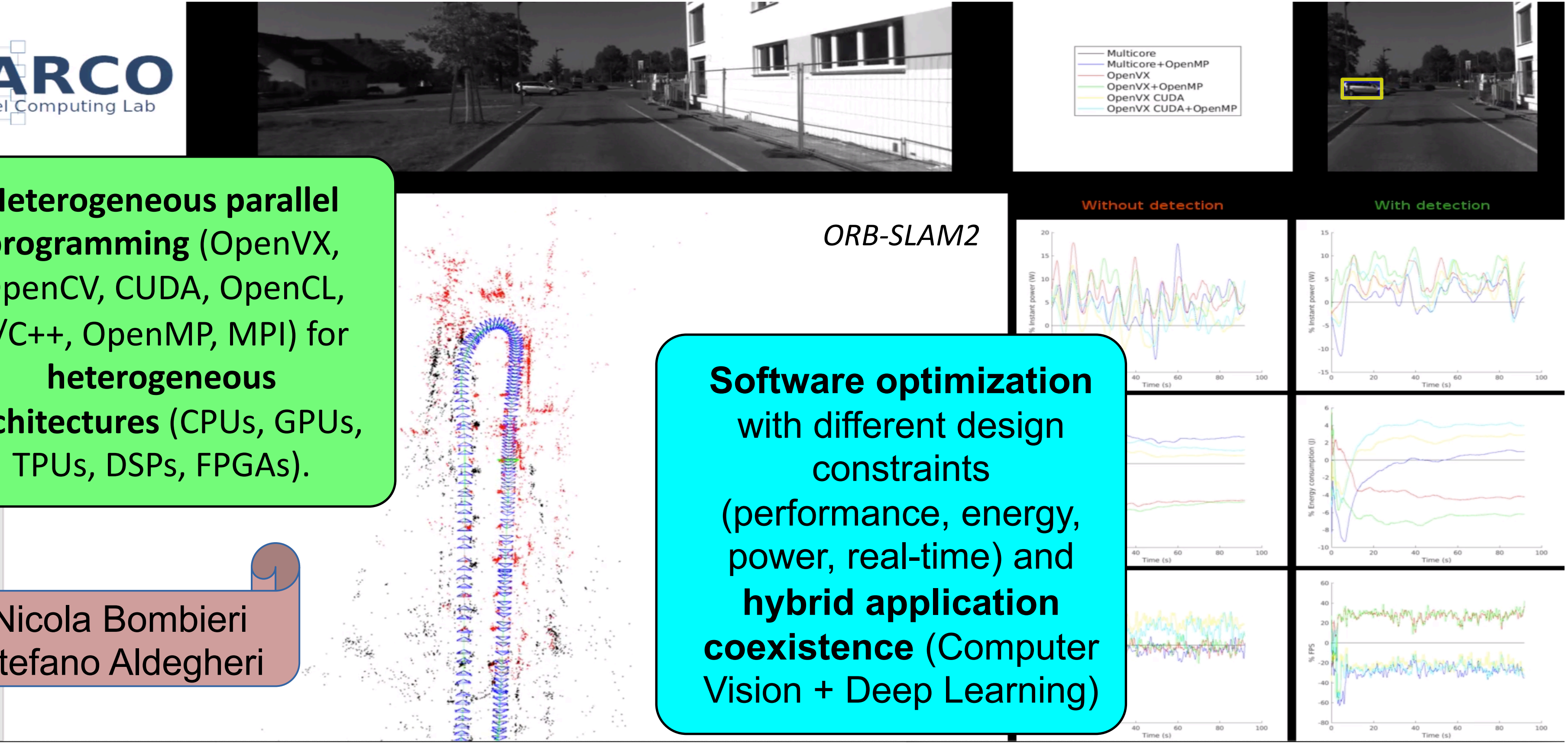
- Automatic design of the physical topology
- Automatic design of the OPC-UA architecture
- Automatic configuration of network equipment for cyber-security

Application requirements



Embedded vision applications

PARCO
Parallel Computing Lab



Heterogeneous parallel programming (OpenVX, OpenCV, CUDA, OpenCL, C/C++, OpenMP, MPI) for **heterogeneous architectures** (CPUs, GPUs, TPUs, DSPs, FPGAs).

Software optimization with different design constraints (performance, energy, power, real-time) and **hybrid application coexistence** (Computer Vision + Deep Learning)

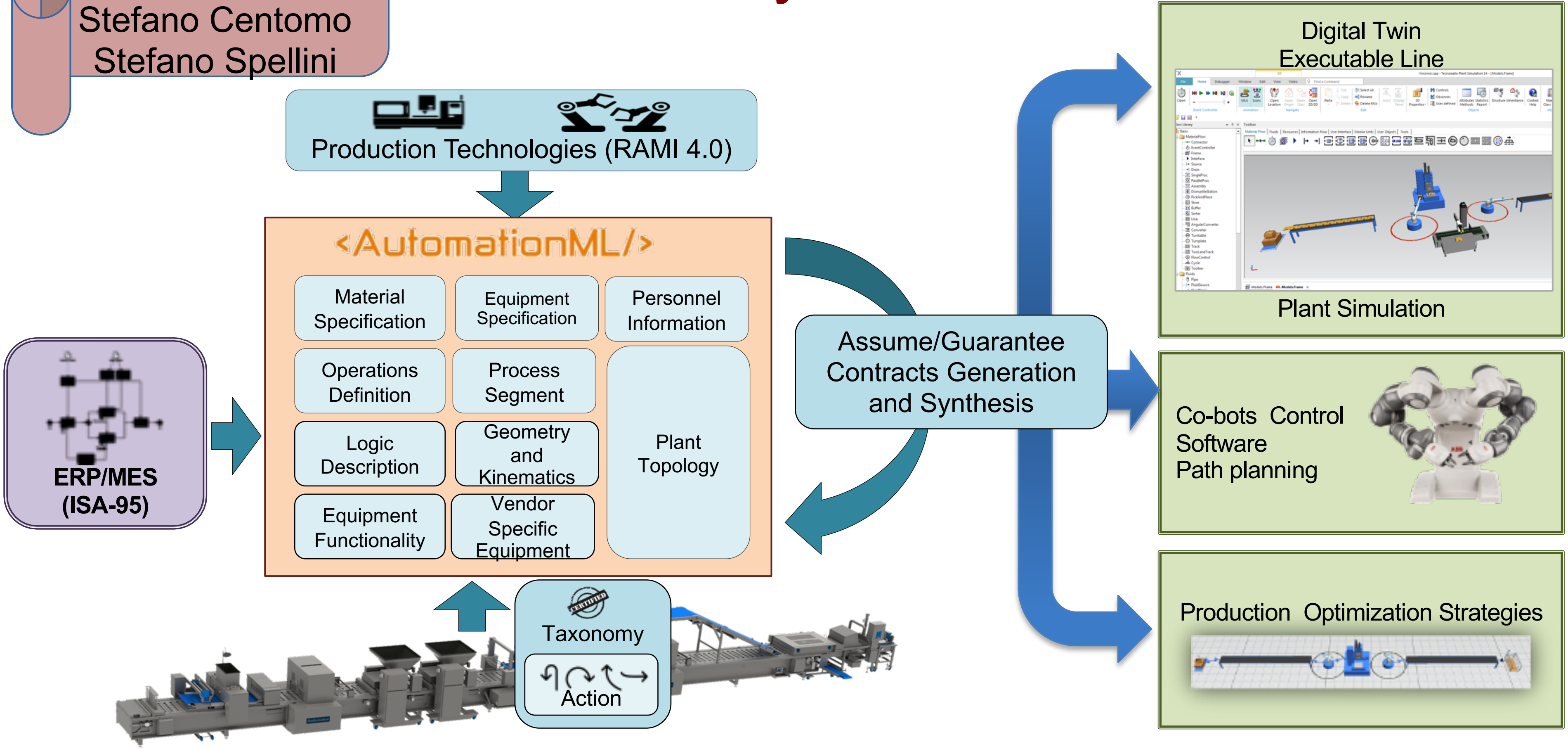
Nicola Bombieri
Stefano Aldegheri

Outline

- Application context
- Design
  - Network synthesis
  - Embedded vision applications
- **Modeling & Verification**
  - Analysis of industrial plants
  - Joint system-network simulation
  - ROS-compliant containerized verification monitors
  - Catching sources of vulnerabilities
  - Automatic analog abstraction
  - Formal Methods for System Design
  - Run-time verification of parametric systems
- References

Formal Analysis of Industrial Plants

Franco Fummi
Stefano Centomo
Stefano Spellini



Production Technologies (RAMI 4.0)

<AutomationML/>

- Material Specification
- Equipment Specification
- Personnel Information
- Operations Definition
- Process Segment
- Plant Topology
- Logic Description
- Geometry and Kinematics
- Equipment Functionality
- Vendor Specific Equipment

ERP/MES (ISA-95)

Taxonomy

Action

Assume/Guarantee Contracts Generation and Synthesis

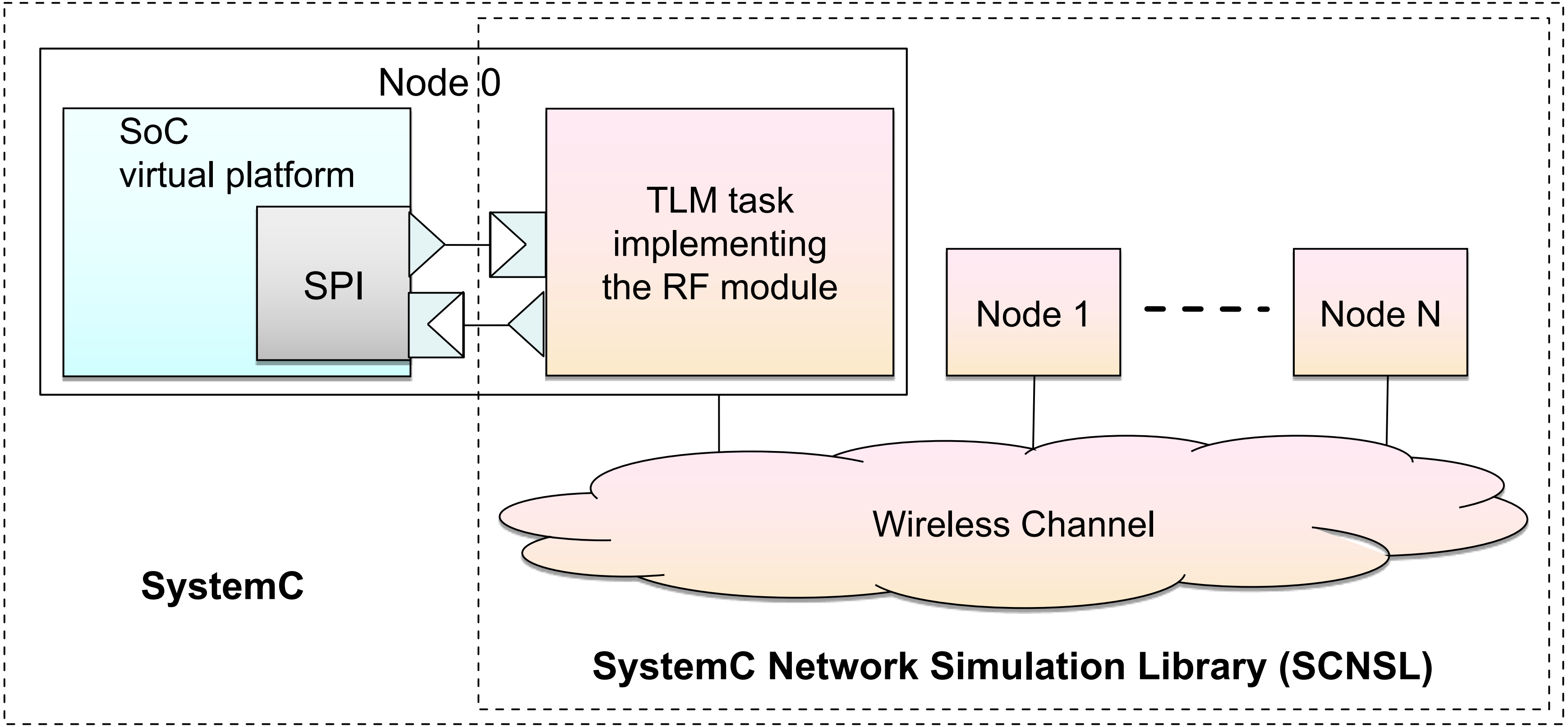
Digital Twin Executable Line

Plant Simulation

Co-bots Control Software
Path planning

Production Optimization Strategies

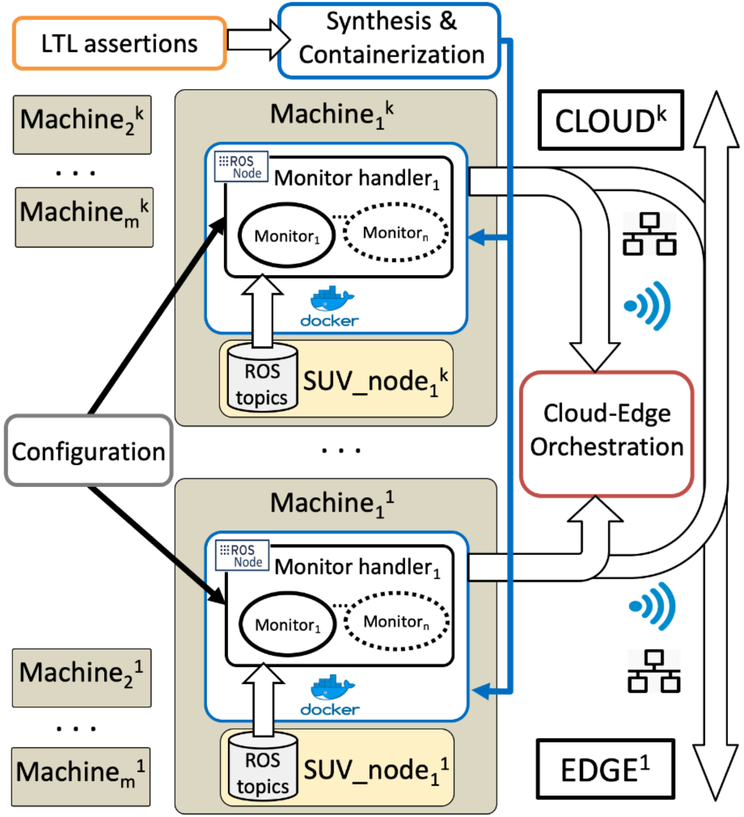
Joint System-Network Simulation



Graziano Pravadelli
Nicola Bombieri
Samuele Germiniani

ROS-compliant containerized verification monitors

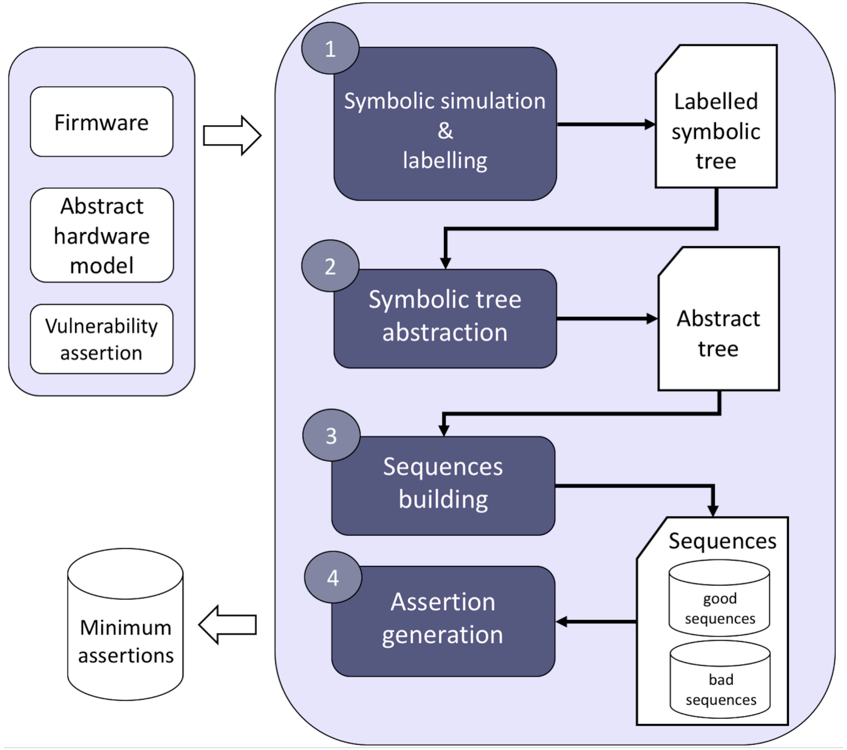
- Architecture and automatic flow to generate, orchestrate and deploy a ROS-compliant verification environment for robotic systems.
- Assertion-based verification through ROS-based monitors automatically synthesized from LTL assertions.
- Verification accuracy and real-time constraints addressed thorugh conteinerization across edge-server-cloud.



Graziano Pravadelli
Samuele Germiniani
Alessandro Danese

Catching sources of vulnerabilities

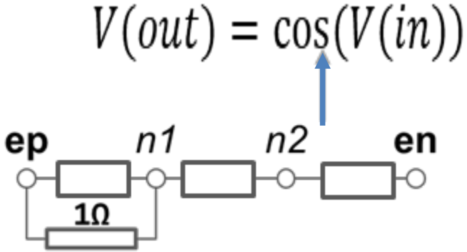
- Many tools for detecting vulnerabilities, but understanding the origin is more challenging
- Given an unwanted behavior, the proposed framework catches source of vulnerabilities
  - Through:
    - ✓ symbolic simulation and
    - ✓ sequence alignment
  - To generate:
    - ✓ assertions representing the minimum sequence of FW instructions that trigger the vulnerability



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



$$V(out) = \cos(V(in))$$

Methodology

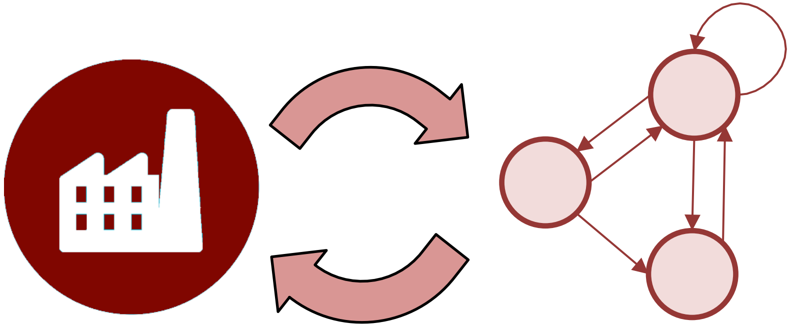
1. Parse circuit description
2. Apply Kirchhoff's laws
3. Reconstruct input-output relations of the model
4. Outlines the minimal set of equations for describing its behavior
5. Discretize and symbolicaly solves the minimal set of equations
6. Generate optimized C++ code

Tool: **HIFSuite**

Luca Geretti
Matteo Zavatteri
Davide Quaglia
Romeo Rizzi
Viktor Teren
Tiziano Villa

Formal Methods for System Design

with applications to Industry 4.0



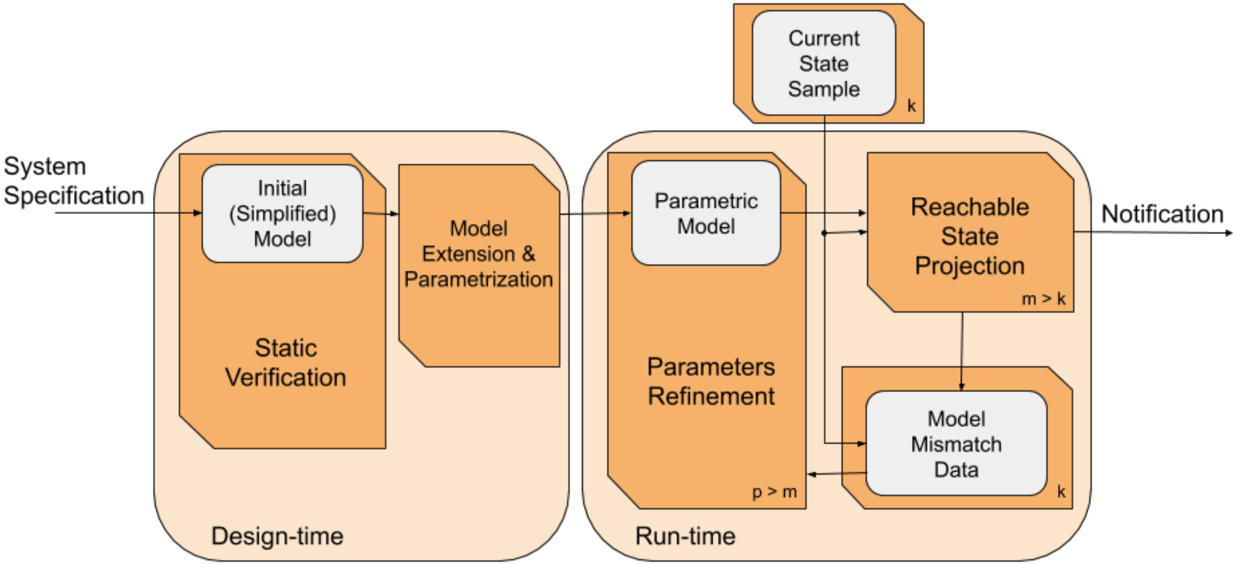
Activities:

- Application of formal methods to the industrial context and integration with edge/cloud techniques, with special reference to occupational safety
- Planning and scheduling under uncertainty: formal methods for temporal and resource controllability of industrial business processes
- Compositional and computational semantics for hybrid automata
- Characterization of quotient computation in discrete structures
- Decomposition of transition systems into Petri nets
- Logic synthesis

Luca Geretti
Tiziano Villa

Run-time Verification of Parametric Systems

- **Domain:** robotic and manufacturing systems
- **Problem**: identify potential unsafe behaviors of the real system during operation;
- **Approach**: from real states, evolve the model of the system in the future; periodically adapt the model to match the real states;
- **Methodology:** *parametric interval analysis* allows to model bounded uncertainties in the system;
- **Implementation**: in Ariadne with an additional ROS interface.



Outline

- Application context
- Design
  - Network synthesis
  - Embedded vision applications
- Modeling & Verification
  - Analysis of industrial plants
  - Joint system-network simulation
  - ROS-compliant containerized verification monitors
  - Catching sources of vulnerabilities
  - Automatic analog abstraction
  - Formal Methods for System Design
  - Run-time verification of parametric systems
- **References**

Recent 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, 2018
- S.Vinco, N.Bombieri, D.Pagliari, F.Fummi, E.Macii, M.Poncino, “A Cross-level Verification Methodology for Digital IPs Augmented with Embedded Timing Monitors”, ACM TODAES 2019
- M.Lora, S.Vinco, F.Fummi, “Translation, Abstraction and Integration for Effective Smart System Design”, IEEE TCOMP 2019
- S. Aldegheri, N. Bombieri, D. Bloisi, A. Farinelli “Data flow ORB-SLAM for real-time performance on embedded GPU boards”. In Proc. of IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). 2019
- E. Fraccaroli, F. Stefanni, R. Rizzi, D. Quaglia, F. Fummi, “Network Synthesis for Distributed Embedded Systems”, IEEE TCOMP, 2018
- A. Danese, V. Bertacco and G. Pravadelli, “Symbolic assertion mining for security validation”, DATE, 2018
- D. Bresolin, P. Collins, L. Geretti, R. Segala, T. Villa, S. Zivanovic, “A computable and compositional semantics for hybrid automata”, 23rd ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2020), Sydney (Australia) 21-24 April 2020, pp. 1-11
- A. Bernasconi, V. Ciriani, J. Cortadella, T. Villa, “Computing the Full Quotient in Bi-decomposition by Approximation”, Proceedings of DATE, Grenoble, France, March 2020, pp. 580-585
- I. Incer, L. Mangeruca, T. Villa, A. Sangiovanni-Vincentelli, “The Quotient in Preorder Theories”, GandALF 2020, 11th International Symposium on Games, Automata, Logics and Formal Verification, EPTCS 326, September 2020, September 2020, pp. 216-233
- M. Zavatteri, R. Rizzi, T. Villa, “Dynamic Controllability and (J,K)-Resiliency in Generalized Constraint Networks with Uncertainty”, 30th Int. Conference on Automated Planning and Scheduling (ICAPS 2020): 314-322(2020). AAAI Press

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