UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

itee PhD information technology electrical engineering

DIETI UNINA

Giorgio Farina

Methods and Tools for Test Automation and Failure Prevention in Mixed Criticality Systems

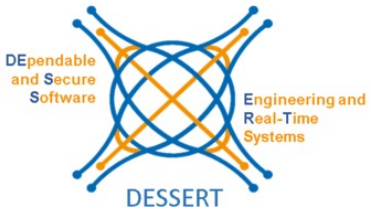
Tutor: Marcello Cinque

Cycle: XXXVII Year:2022/2023

itee PhD information technology electrical engineering

My background

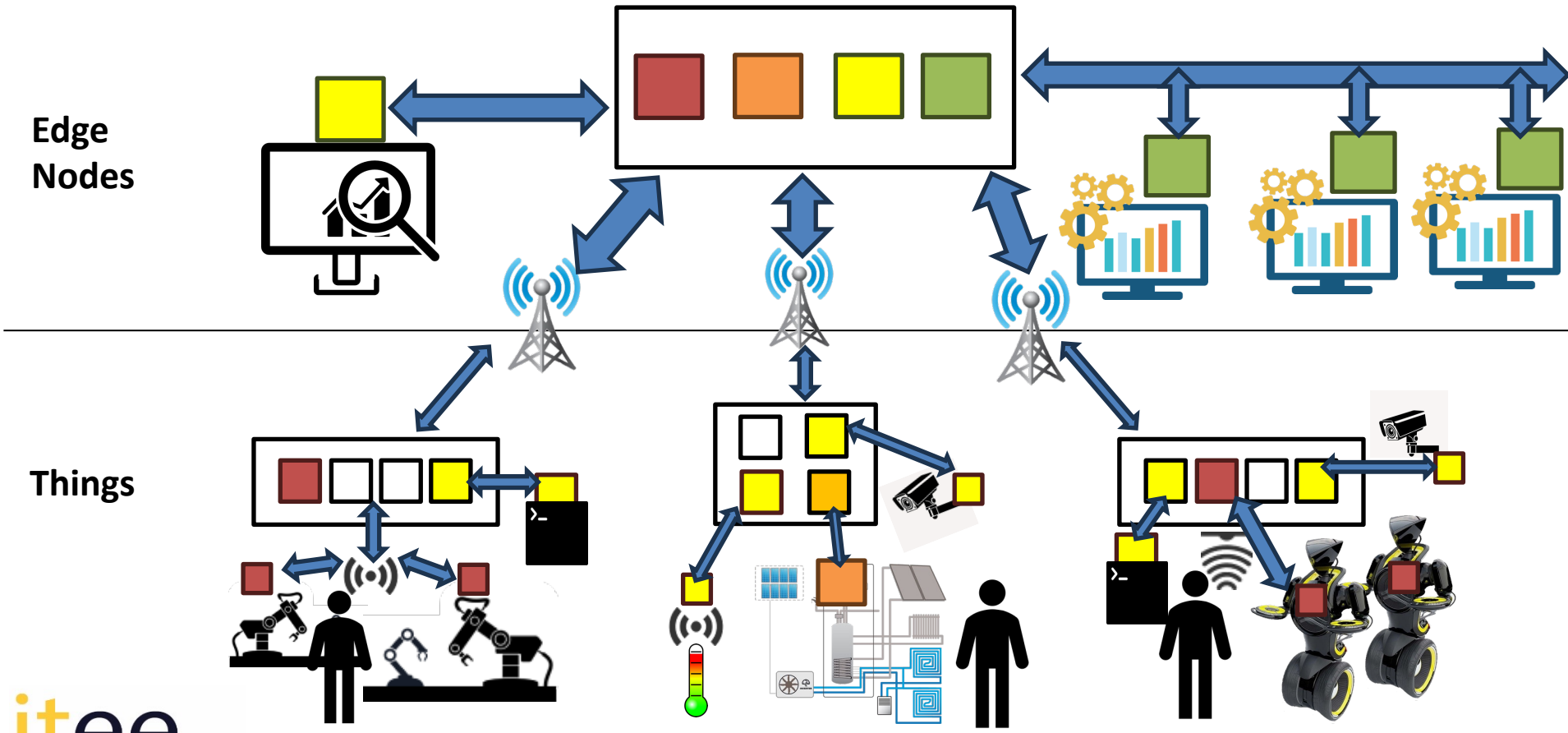
- MSc degree in Computer Engineering (October 2021)
- Research group: DESSERT
- PhD start date: 01/11/2021
- Scholarship type: CINI



Research field of interest

Criticality is the mapping of the failure of a component (either software or hardware) with the impact on the whole system and environment safety

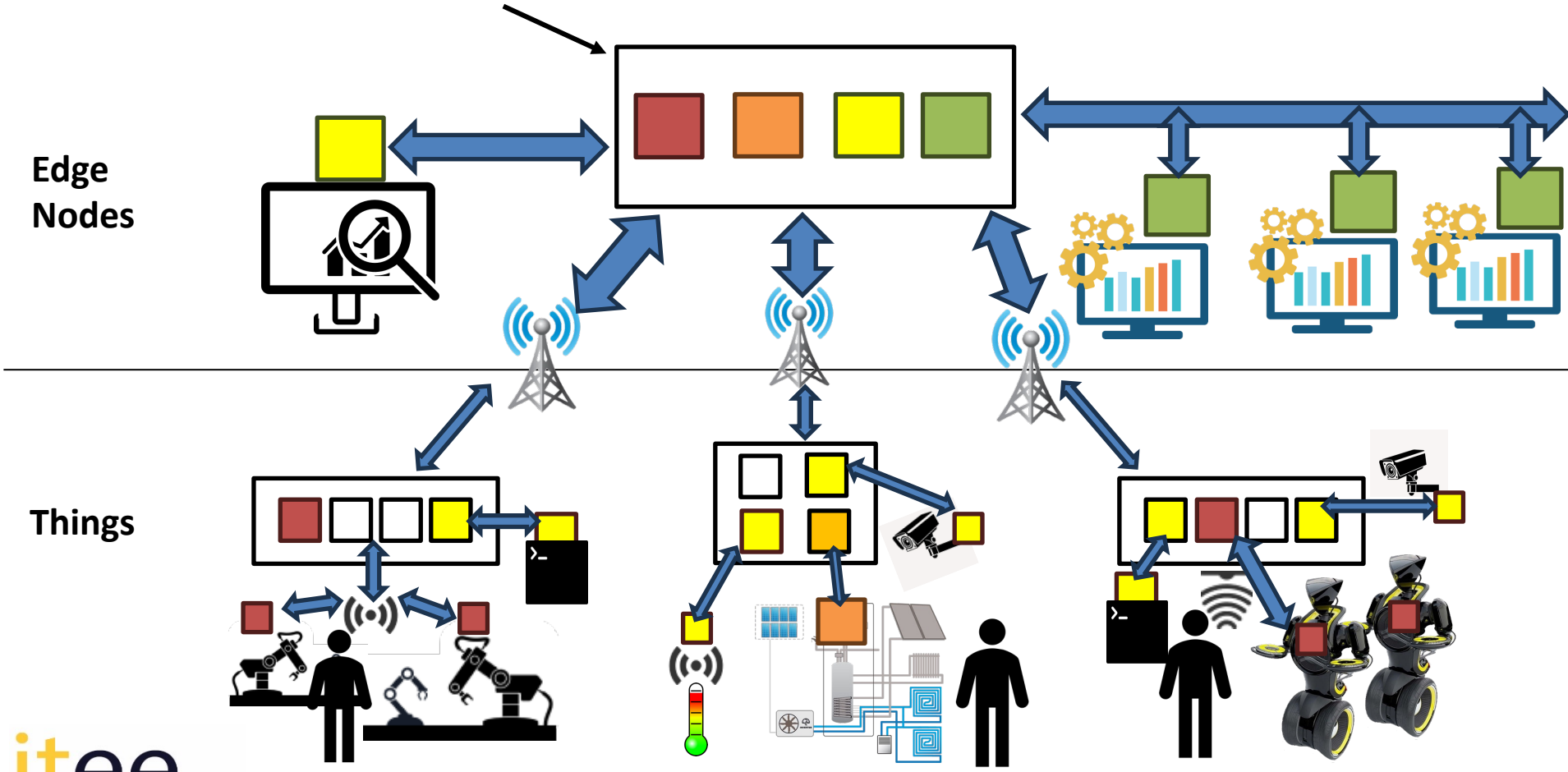
High-criticality, …, Low-criticality



Research field of interest

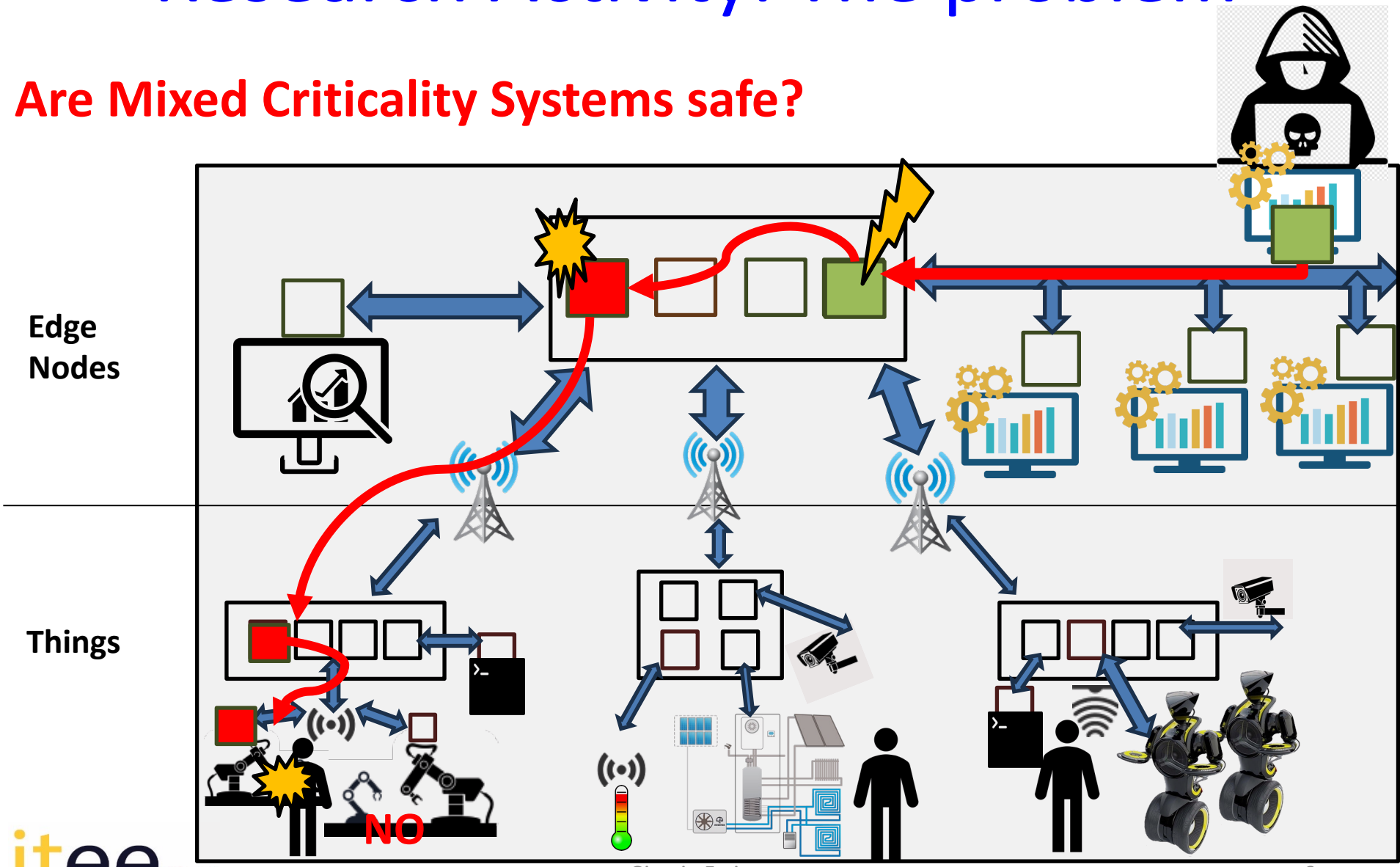
Mixed Criticality Systems:

- consolidate multiple applications into the same system, possibly with different criticality levels
- to reduce design and production costs of the systems



Research Activity: The problem

Are Mixed Criticality Systems safe?



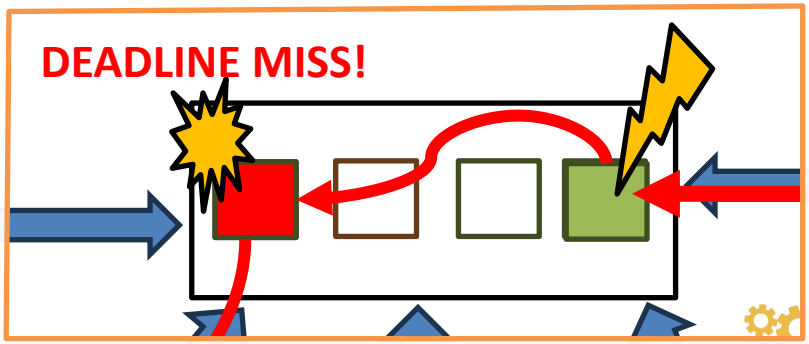
Research Activity: Overview

Are Mixed Criticality Systems safe?

Edge Nodes

Things

- **Problem**



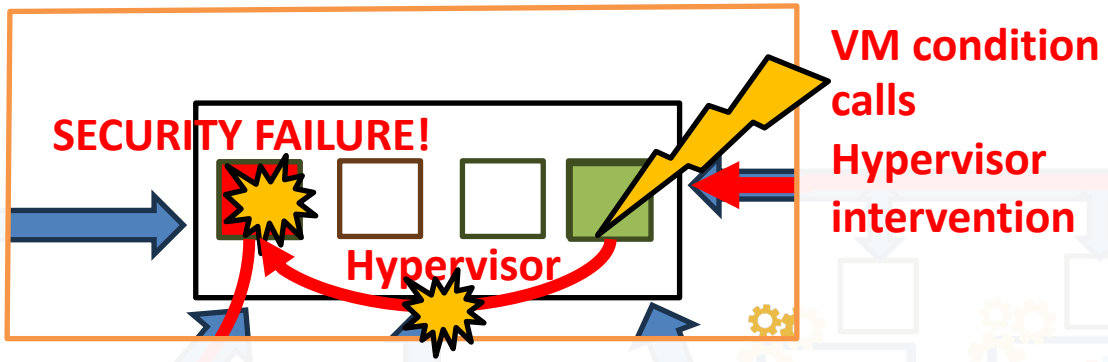
- **Solution** [P1]
  - We provide a **dection/regulation approach to mitigate the interference**
  - We provide a workload for exclusive archs, i.e., **LLC exclusive bomb**
  - We prove that the **queue occupancy** is a good observable indicator of the memory access interference
- **Methodology**
  - Detect the error state to prevent failures, i..e, deadline miss
  - Mitigate the error state

Research Activity: Overview

Are Mixed Criticality Systems safe?

Edge Nodes

- **Problem**



  - **Hypervisor intervention** involves a change in a **most privileged mode** ***-> hypervisor security can jeopardize the isolation of the hosted virtual machines***
  - **Testing hypervisor intervention is not a negligible task due to the difficulty of building valid test-cases**

Things

- **Solution** [P2]
  - We propose IRIS, a **record and replay** framework to **automate the test-case generation** to test hypervisor intervention.
- **Methodology**
  - «Record and replay» to move across hypervisor states
  - «Record and replay» to have valid test cases to mutate

Research Activity: Objectives

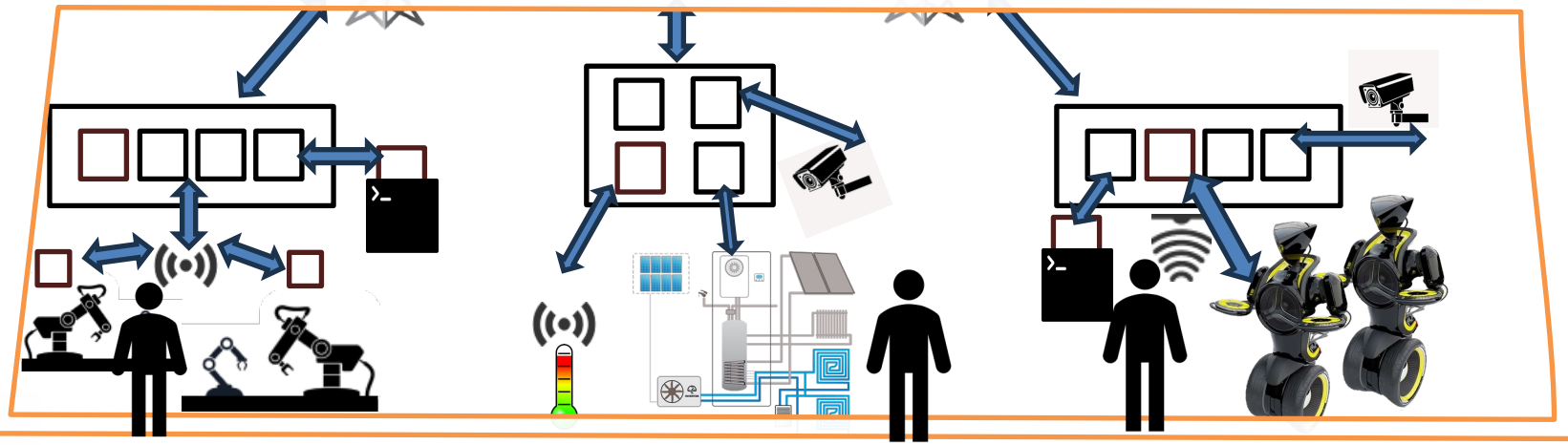
Are Mixed Criticality Systems safe?

Edge Nodes

- In the last year, my focus **moves to the security and safety of the things**, i.e., IoT devices
- Due to the **connected nature of IoT devices**, a vulnerability in any of the applications can spread on the interacting devices

1) How do we detect such a spread as close to the start as possible?
2) How do we mitigate the failures to avoid escalation, i.e., new spread?

Things



Summary of study activities

- **Ad hoc PhD courses / schools**
  - IoT Data Analysis
  - Verification and Validation of Automated Systems' Safety and Security
- **Conferences / events attended**
  - The 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN

Products

[P1]	*"Enabling memory access isolation in real-time cloud systems using Intel's detection/regulation capabilities",* ***G. Farina**, G. Gala, M. Cinque, G. Fohler* ***Journal of Systems Architecture**, JSA, published, 2023, indexed by Scopus*
[P2]	*"IRIS: a Record and Replay Framework to Enable Hardware-assisted Virtualization Fuzzing",* *C. Cesarano, M. Cinque, D. Cotroneo, L. De Simone**, G. Farina**,* *The 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, **DSN**, published, 2023, indexed by Scopus*
[P3]	*"Partitioned Containers: Towards Safe Clouds for Industrial Applications",* *M. Barletta, M. Cinque, L. De Simone, R. Della Corte, **G. Farina**, D. Ottaviano,* *The 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume, **DSN-S,** 2023, indexed by Scopus*