UNIVERSITÀ POLITECNICA DELLE MARCHE

Model-based design for increasing safety and security of autonomous systems

Supervisor: Prof. Alessandro Freddi

Department of Information Engineering
https://www.dii.univpm.it

UNIVERSITÀ POLITECNICA DELLE MARCHE

Supervisor: Prof. Alessandro Freddi

Supervisor short description

Prof. Alessandro Freddi, PhD, MS

Associate Professor in Systems and Control Engineering, DII, UNIVPM, **Assistant Head of Laboratory of Artificially Intelligent Robotics (LAIR)**, a laboratory based in the Faculty of Engineering, Università Politecnica delle Marche, Ancona.

More than 120 peer-reviewed research papers, with about 1,500 citations received https://orcid.org/0000-0002-9880-0238 (Publication List, H-index = 22 according to Google Scholar; H-index = 19 according to Scopus). More than 15 years of experience in fault diagnosis, fault-tolerant control, unmanned vehicles and assistive robotics.

Advisor / Co-Advisor of more than 10 PostDocs / PhD students in the field of automation and robotics.
Thesis Supervisor / Co-Supervisor of more than 50 students, mainly in the Degree and Master Degree Courses in Computer and Automation Engineering.
Currently working in a research group which includes 5 PostDocs and 4 PhD students, as well as 2 Researchers and 2 Professors.

- European projects participated by the LAIR group:
  - 2024: EMOTIVE - Empowering Mobility with affective cOmputing, brain-computer inTerface, Internet of Things, and Vital signs monitoring for Smart WhEelchairs, Pharaon Second Open Call winner, H2020
  - 2022-2025: DANTE EDIH - Digital Solutions for a Healthy, Active and Smart Life European Digital Innovation Hub
  - 2013-2016: AdriHealthMob - Adriatic Model of Sustainable Mobility in the Health and Care Sector, IPA Adriatic Cross-Border Cooperation Programme
  - 2011-2012: JADE - Joining Innovative Approaches for the Development of transnational integration and knowledge clusters of policies related to independent living Elderly, FP7

- National projects participated by the LAIR group:
  - 2022-2025: VITALITY - Ecosistema di Innovazione, Digitalizzazione e Sostenibilità per l'Economia Diffusa nell'Italia Centrale, PNRR – Ecosistema dell'Innovazione.
  - 2022-2024: INTELLIGENCE 5.0 - dai sistemi cyber fisici per la creazione di macchine utensili self aware ad innovativi modelli di servizi industriali evoluti", MiSE - settore applicativo "Fabbrica intelligente"
  - 2021-2023: ChAALenge, Progetto Nazionale - MiSE

UNIVERSITÀ POLITECNICA DELLE MARCHE

Supervisor: Prof. Alessandro Freddi

Research Group Description

Laboratory of Artificially Intelligent Robotics

https://dii.univpm.it/en-gb/lair_en/

STAFF: The group is currently formed by **one full Professor, two associate Professors, one visiting Associate Professor, one Researcher, four post-doc Researchers, four PhD students.**

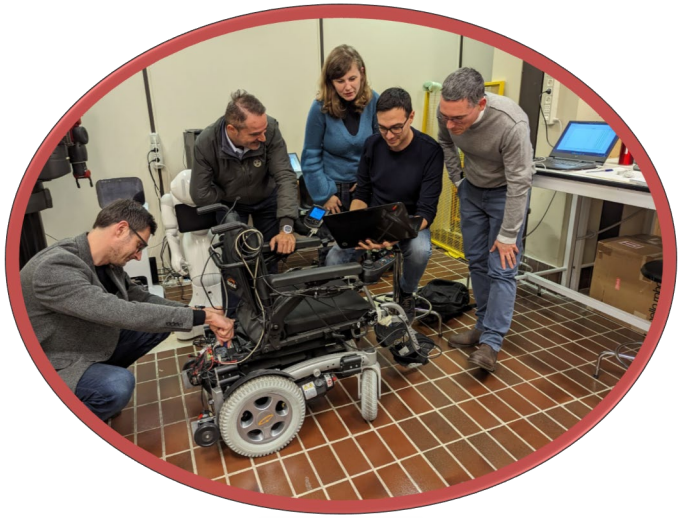
RESEARCH ACTIVITY

The Laboratory of Artificially Intelligent Robotics (LAIR) has a solid background in systems, control and automation engineering, and works mainly in these three fields:

1) model-based fault diagnosis and (fault-tolerant) control, with application to autonomous systems;

2) data-driven fault diagnosis and prognosis, with application to motors and industrial systems;

3) human-robot interaction, with main applications to service and assistive robotics.



LAIR
LABORATORY OF ARTIFICIALLY INTELLIGENT ROBOTICS

EQUIPMENT

3x DJI Drones, 1x Softbank Robotics Pepper Robot, 1x ReThink Robotics Baxter Robot, 2x OhmniLabs Robots, 2x Temi Robots, 1x Hello Robot Stretch, 2x Brain Computer Interface devices, 1x Sunrise Smart Wheelchair, 2x Haptic devices, several sensors and microcontroller kits for automation.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Dean: Prof. Franco Chiaraluce

Department description

https://dii.univpm.it/en-gb/home/

The **Department of Information Engineering** (**DII**) was established in 2011 following the merge of the previous DIBET (Department of Biomedical, Electronics and Telecommunication engineering) and DIIGA (Department of Computer, Management and Automation engineering).

The Department is a self-managing organizational branch of the university dedicated to scientific research and teaching, and contributes to the so called Third Mission of the Higher Education Institution through the dissemination of scientific research findings amongst the community.

Its main aims are to plan, organize and regularly assess the quality of the research activities carried out in the scientific sectors and disciplines under its jurisdiction; to plan, organize and manage bachelor and master courses in Information Engineering and, last but not least, to provide cultural and educational activities and contribute to training and guidance issues according to the students' needs.

AT A GLANCE

DII  2024

250+ Publications

> 4 M€ Research income

71 Research staff

112 PhD, Post-doc, Research fellows

BACHELOR DEGREES:
Biomedical Engineering, Electronic Engineering and Digital Technologies, Computer and Automation Engineering, Information Engineering for Videogame and Virtual Reality.
MASTER DEGREES:
Biomedical Engineering (in English), Electronic Engineering, Computer and Automation Engineering.
BACHELOR DEGREE WITH PROFESSIONAL ORIENTATION:
Industrial and Information Systems.

DII coordinates the PhD in Information Engineering, organized in two curricula:
- Biomedical, Electronics, Telecommunication Engineering and Nanotechnologies (IBETN)
- Computer, Management and Automation Engineering (IIGA)

Research laboratories **32**

11 Scientific Areas:
IINF-01/A, IINF-02/A, IINF-03/A, IINF-04/A, IINF-05/A, IBIO-01/A, IMIS-01/B, IIET-01/A, IEGE-01/A, MATH-06/A, ECON-04/A

UNIVERSITÀ POLITECNICA DELLE MARCHE

Supervisor: Prof. Alessandro Freddi

Project Idea: Model-based design for increasing safety and security of autonomous system

Background: Autonomous systems represent a subset of Cyber-physical systems (CPS) which possess the capability to make decisions and operate independently. These systems offer remarkable functionalities; however, they are also vulnerable to threats such as malicious cyberattacks, which negatively impact both security (as in the protection of the digital domain) and safety (as in the protection of the physical domain). CPS security is typically managed using cybersecurity (Information Technology - IT) and network security solutions. While integrating traditional IT security measures, such as encryption, remains essential, this approach alone is insufficient. A fundamental property that makes CPS unique compared to generic IT systems is that the physical evolution of a system's state must comply with immutable laws of nature. For this reason, research on CPS security now lies at the intersection of control systems and cybersecurity.

What we OFFER:

- expertise in the domain of model-based algorithms for systems' safety
- expertise in data-driven workflows for diagnosis and prognosis of autonomous systems
- benchmarks and testbeds to deploy and test new ideas

Multi-disciplinary approach

We SEARCH candidates with (one or more):

- knowledge in Networked Control Systems
- experience in ROS and robotic networks
- strong background in model-based design for dynamical systems

Project OBJECTIVES:

- Analysis of common attack types and their potential consequences
- Attack detection methods
- Secure estimation
- Secure control

Project OUTCOMES:

- Increased safety of CPS
- Increased security of CPS
- Application to Industrial plants
- Application to Autonomous Vehicles