Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Future Artificial Intelligence Research

Spoke 3: Resilient AI

Sergio Di Martino

Roma, 20 Ottobre 2023

Future Artificial Intelligence Research

Spoke 3: Partners

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

Consiglio Nazionale delle Ricerche

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA

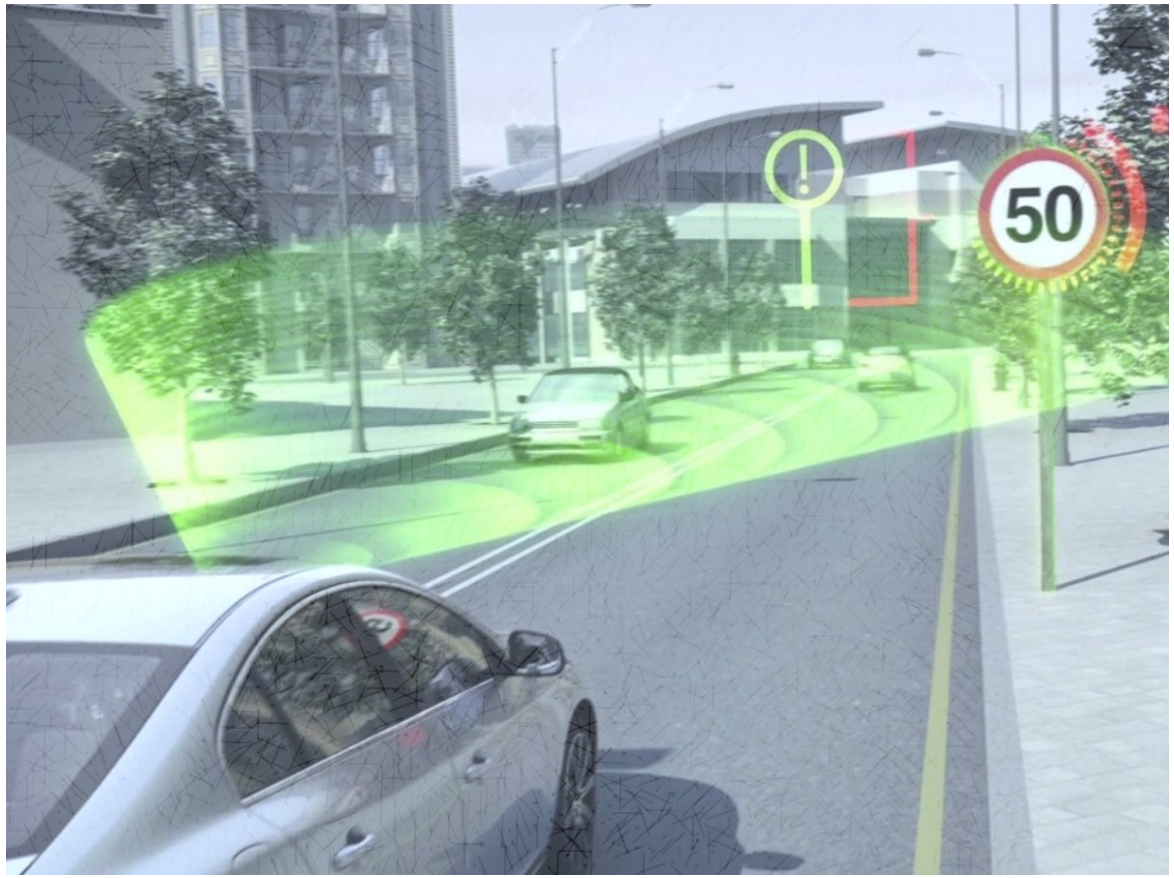
Critical mass

36 Professors/Senior Researchers

16 young Researchers

Resilient AI

- AI-based systems are becoming integrated into daily operational environments.

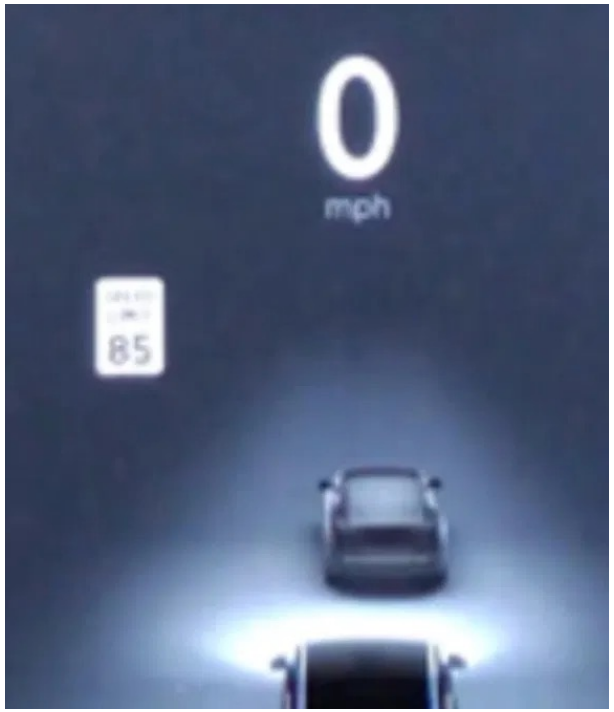


Resilient AI

- AI-based systems are expected to operate in daily, challenging environments, on **real-world data**;

Resilient AI

- AI-based systems are expected to operate even in **adversarial environments**;



Spoke 3: Resilient AI

- The Spoke 3 is addressing the study of AI foundational methodologies aimed at **processing data in-the-wild**, making the **performance of AI resilient and robust in challenging contexts**, based on real-world data.

Scientific Goals

Improve the state of the art in:

1. AI techniques with **incomplete or not adequately representative data**;
2. **Algorithms** that are both **resilient and robust**, also w.r.t. **possible external attacks** (incl. training with "malicious" data);
3. Design, **verification & validation**, and operation of AI algorithms, when they have to work in-the-wild;
4. **Ethical and legal issues** with real-world data.

Q1: AI techniques with incomplete or not adequately representative data

- Data imputation techniques based on generative models able to produce new data
- Missing modality imputation for Multimodal datasets
- Label imputation approaches for data annotations of large datasets
- Multi-task learning with unbalanced data or missing/ noisy labels

Q2: Resilient Algorithms, also to external attacks

- Adversarially resilient machine/federated learning (i.e., able to keep working correctly, despite in degraded conditions)
- Data inspection techniques for preventing violation of confidentiality in ML processes
- Strategic logics for unforeseen events
- Best-effort strategies to face unexpected or overwhelming disturbances

Q3: Design, verification & validation, and operation of AI algorithms

- Automated support for the development of ML pipelines
- Automated Verification of ML-intensive systems (with Automotive applications)
- Explainable and interpretable Human-Centered Intelligent Systems

Q4: Ethical and legal issues

- Determining the Regulatory System
- Picture of the European Independent Authorities and the future one
- AI for compliance with ethical and legal norms

(Q1) Incomplete Data

- WP 3.1 Creation and annotation of massive datasets
- WP 3.3 Resilient multi-task learning on the edge from incomplete and/or noisy data

(Q2) Resilient Algorithms

- WP 3.2 Resilient AI in adversarial environments
- WP 3.4 Enhanced Resilient AI through data pre-processing and HCI techniques
- WP 3.7 Resilient Strategic Reasoning in AI
- WP 3.5 Resilient multimodal systems

(Q3) Design, V&V, Operation of AI systems

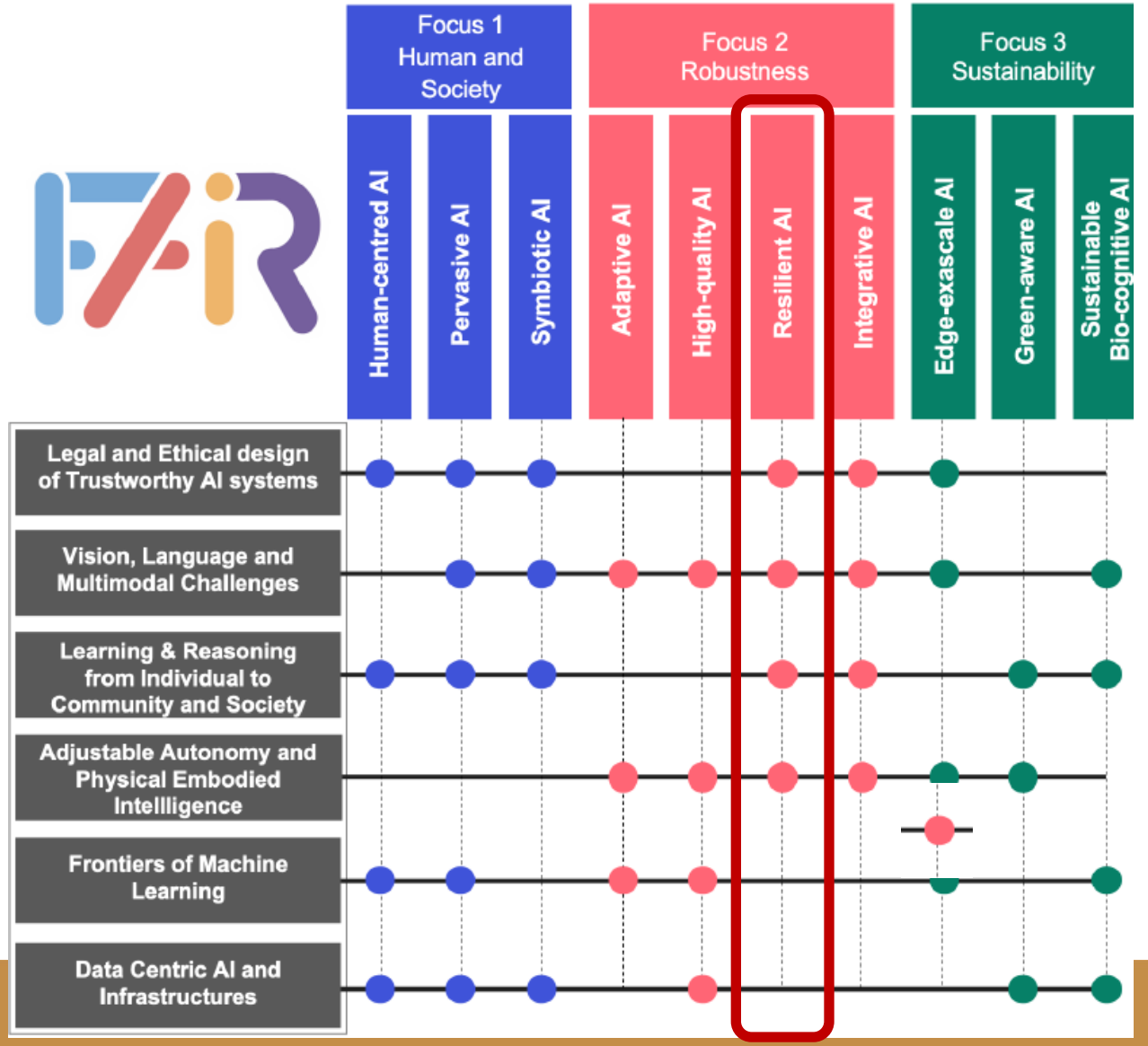
- WP 3.6 Automated Support for Resilient, Dependable, and Interpretable AI

(Q4) Ethical and Legal Issues

- WP 3.8 Ethical, Legal and Societal issues in resilient AI systems

- WP 3.9 Experiment case studies/pilots in challenging domains for Resilient AI

Integrative AI and Transversal Projects



FAIR – Spoke 3 – Resilient AI

- Riferimenti:
  - Sergio Di Martino (sergio.dimartino@unina.it)
  - Massimo Esposito (massimo.esposito@icar.cnr.it)