Doctoral Seminar in Information Systems

Intelligent Organisational Ecosystems

A Research Agenda for Trustworthy Digital Transformation

Henrique S. Mamede
INESC TEC & Universidade Aberta
Portugal
henrique.s.mamede@inesctec.pt

University of Saint-Joseph
Macau

April 2026

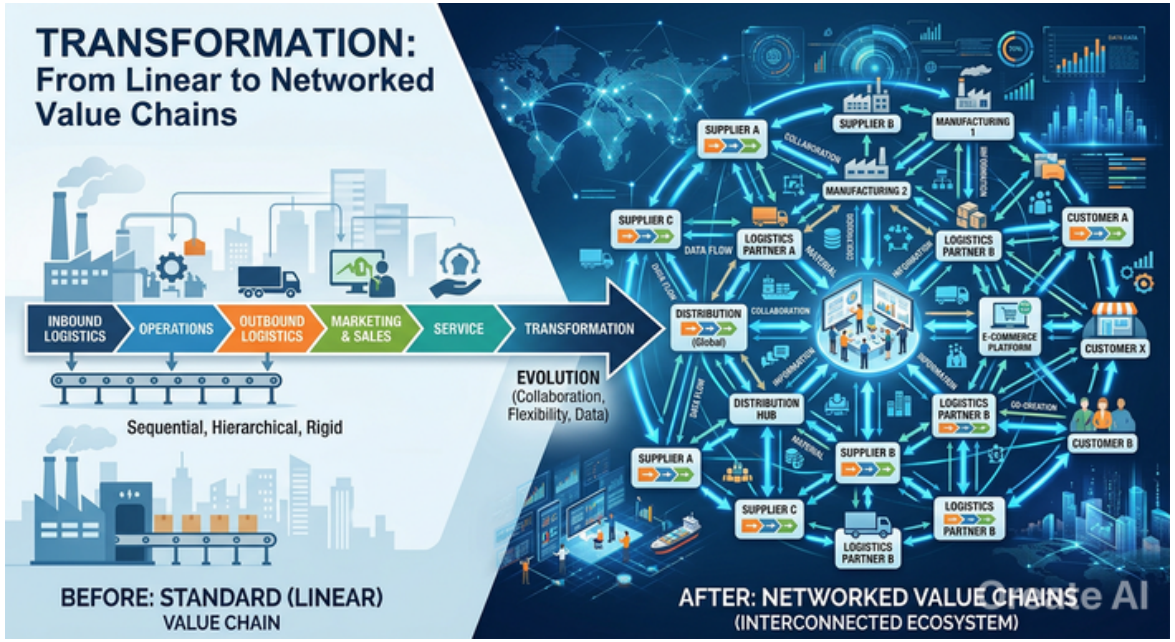
Henrique S. Mamede

- Associate Professor with Habilitation at Universidade Aberta (Portuguese Open University), in the Dep. Of Sciences and Technology
- Senior Researcher at INESC TEC - Institute for Systems and Computer Engineering, Technology and Science
- 30 years of experience in real-world organizations, with companies of all sizes (from SME's to large multinational companies), with Management Board roles

- More than 130 scientific publications in journals and conferences
- Supervised 12 PhD students and 68 master students

Motivation and problem setting

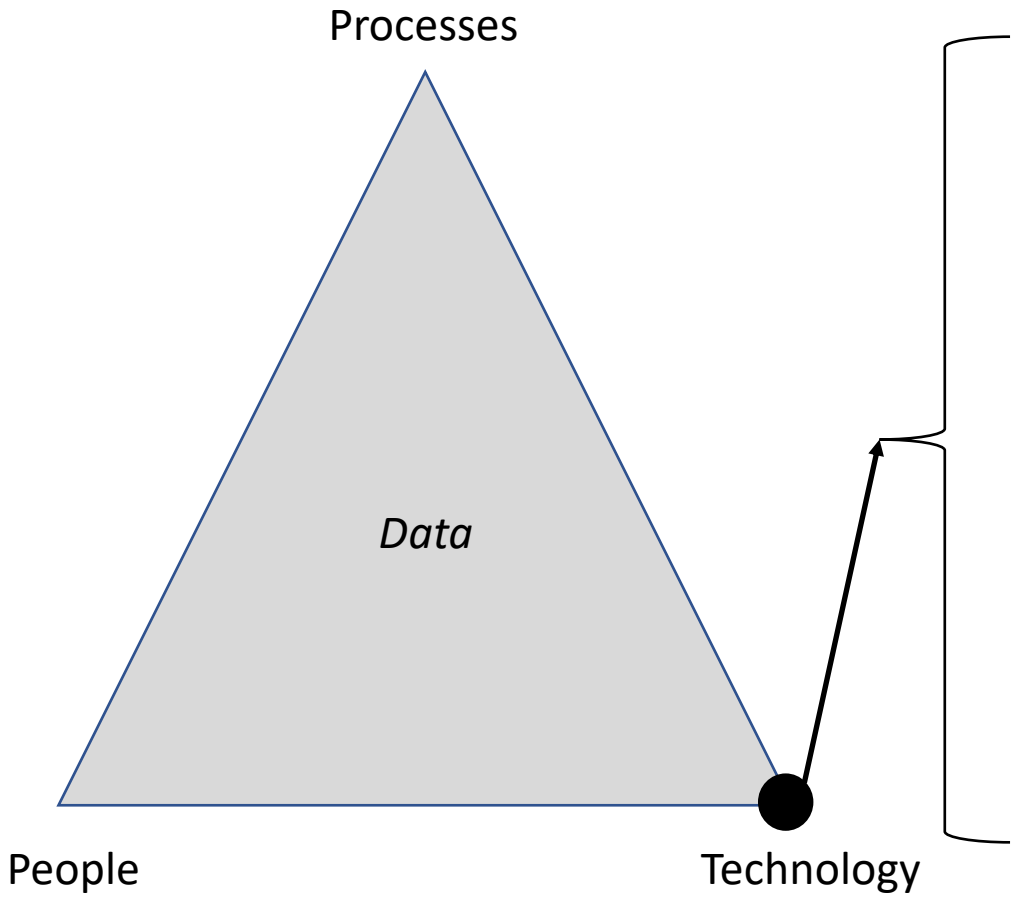
- The next cycle of digital transformation is shaped by AI, automation, interoperable data and cybersecurity.
- Organisations can no longer manage these domains separately.
- Fragmented transformation creates inefficiency, opacity and vulnerability.
- The relevant unit of analysis is the intelligent organisational ecosystem.

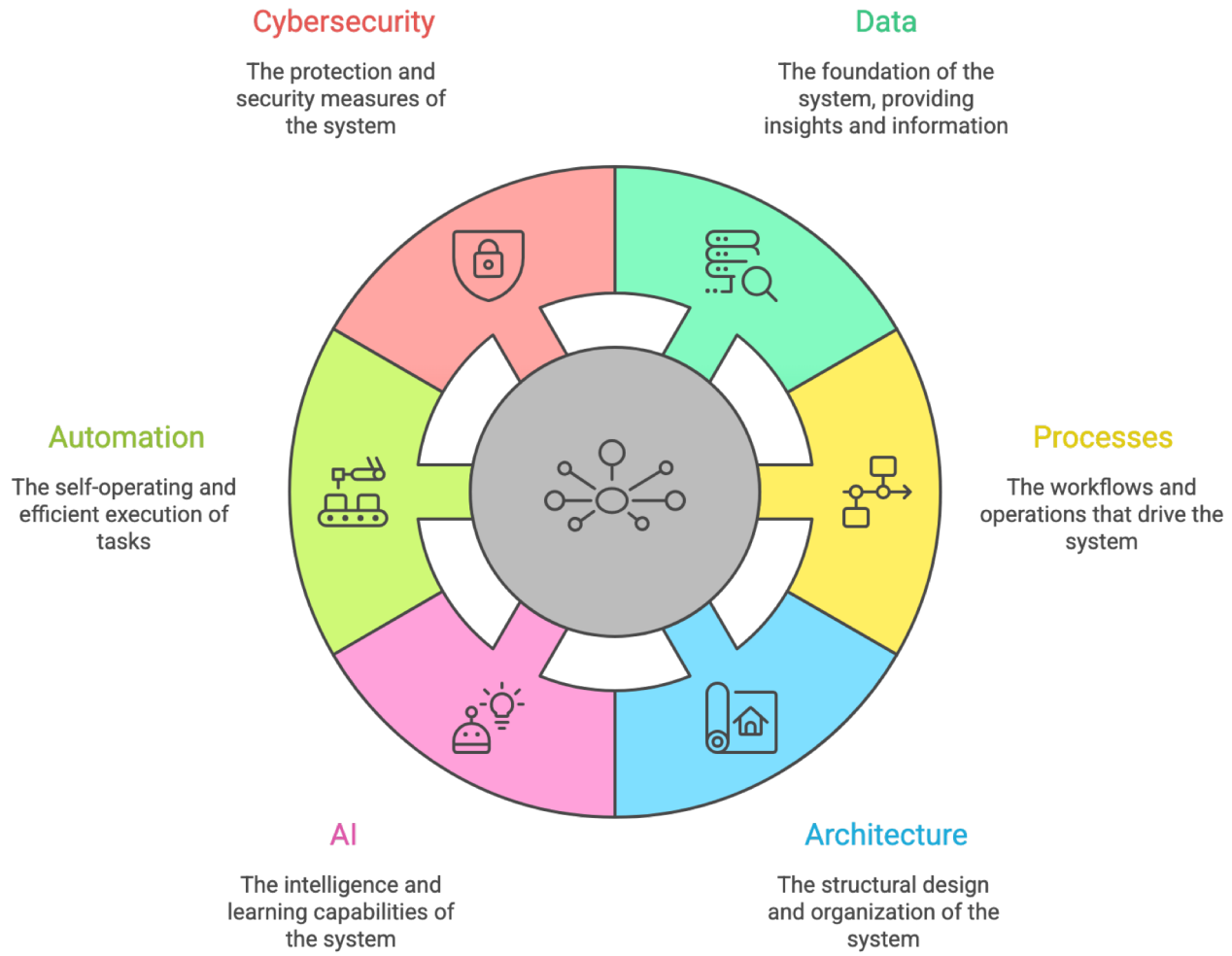


Conceptual positioning

- An intelligent organisational ecosystem is a socio-technical system.
- It integrates data, processes, enterprise architecture, AI, automation and cybersecurity.
- It coordinates human and artificial agents through governance and interoperability.
- Its purpose is to support decision-making, value creation, adaptability and resilience.

“Complex network of complexities”





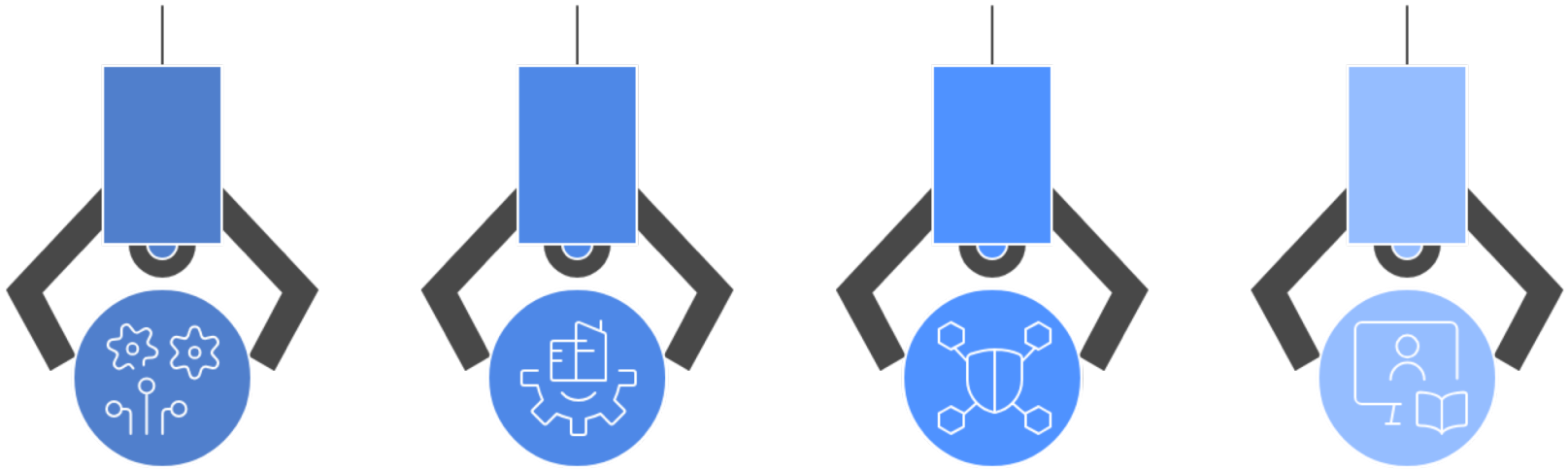
Research question and central hypothesis

- **Research question**
  - How can we model, design and validate intelligent, secure and data-driven organisational ecosystems?

- **Central hypothesis**
  - Organisations that integrate these dimensions as one coherent system achieve greater resilience, trustworthiness and long-term competitiveness.

Scientific agenda at a glance

Research Axes



Ecosystem Modelling

Conceptual and architectural modelling of intelligent ecosystems.

Enterprise Architectures

Intelligent automation and adaptive enterprise architectures.

Cybersecurity Property

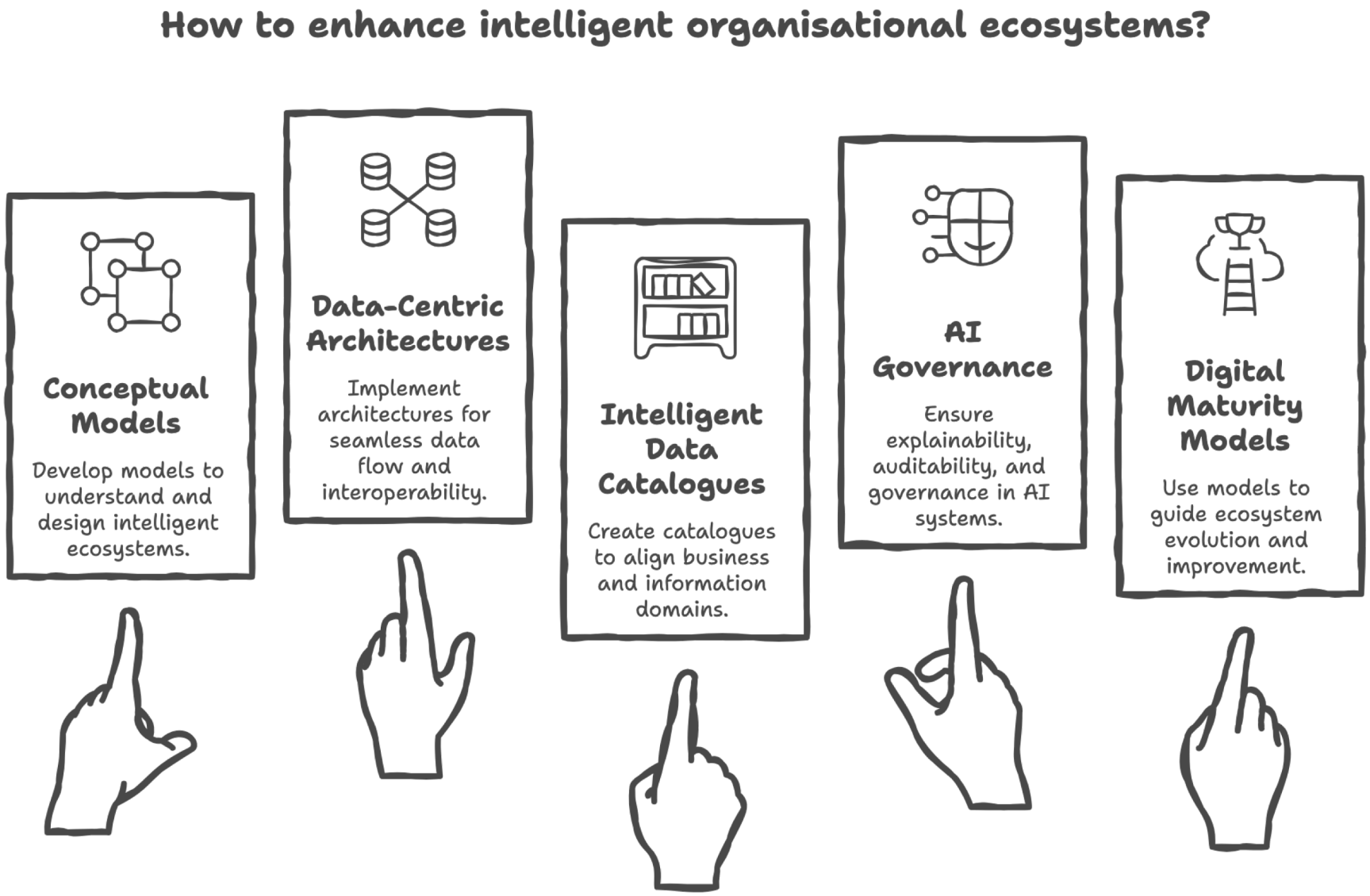
Cybersecurity as a systemic organisational property.

Digital Transformation

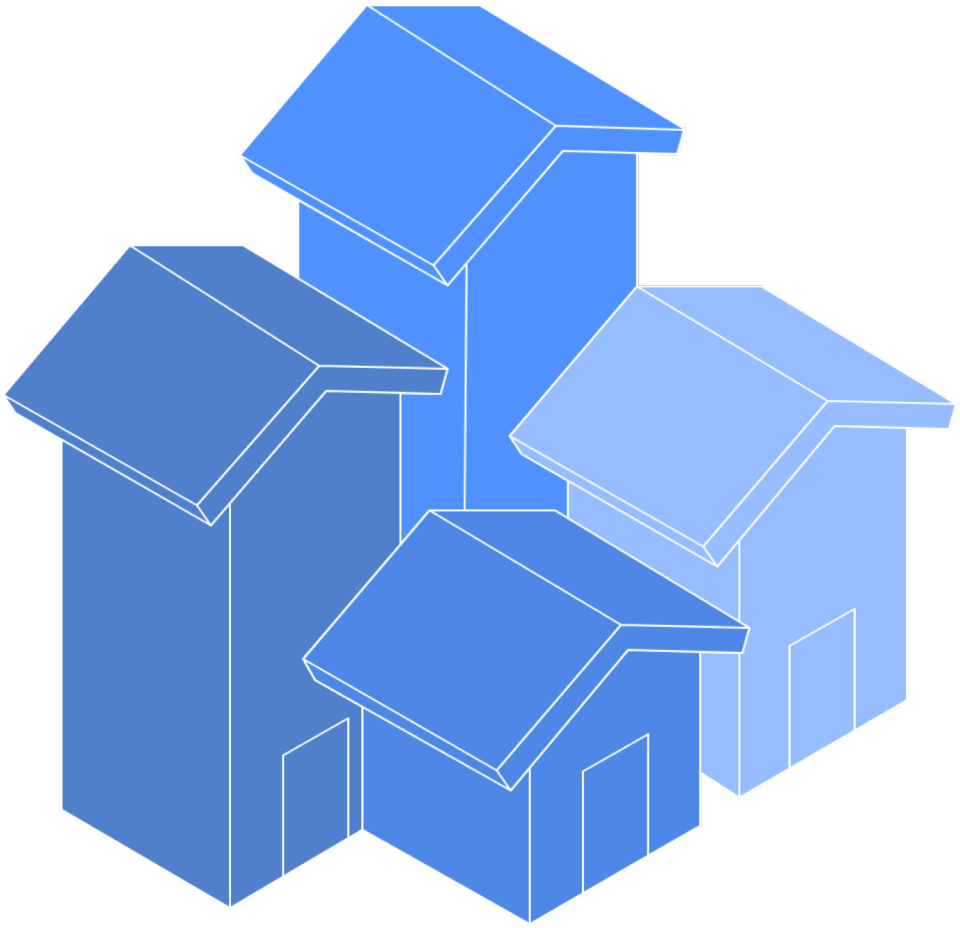
Digital transformation, human capabilities and advanced training.

Shared objective: reusable artefacts, frameworks and evaluation instruments

Axis 1 — Conceptual and architectural modelling



Axis 2 — Intelligent automation and adaptive architecture



1

Integration

Integration of BPM, process mining, RPA, LLMs and enterprise architecture.

2

Automation decisions

Methods to decide what to automate, how to automate, and with what expected value.

3

Adaptive architectures

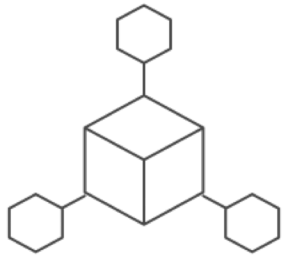
Adaptive architectures informed by real execution data.

4

Organisational redesign

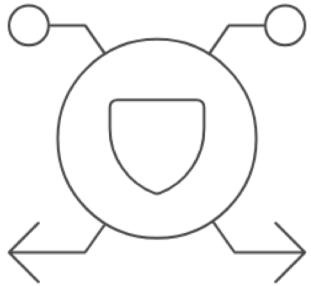
Automation as organisational redesign, not only operational efficiency.

Axis 3 — Cybersecurity as a systemic property



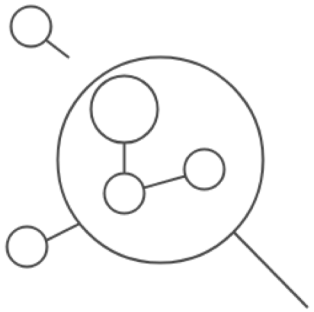
Structural Property

Cybersecurity is a fundamental part of the ecosystem's structure.



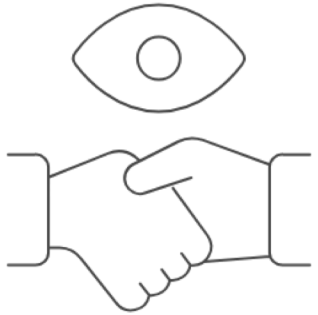
Security by Design

Security is integrated into all aspects of the digital environment.



Risk Focus

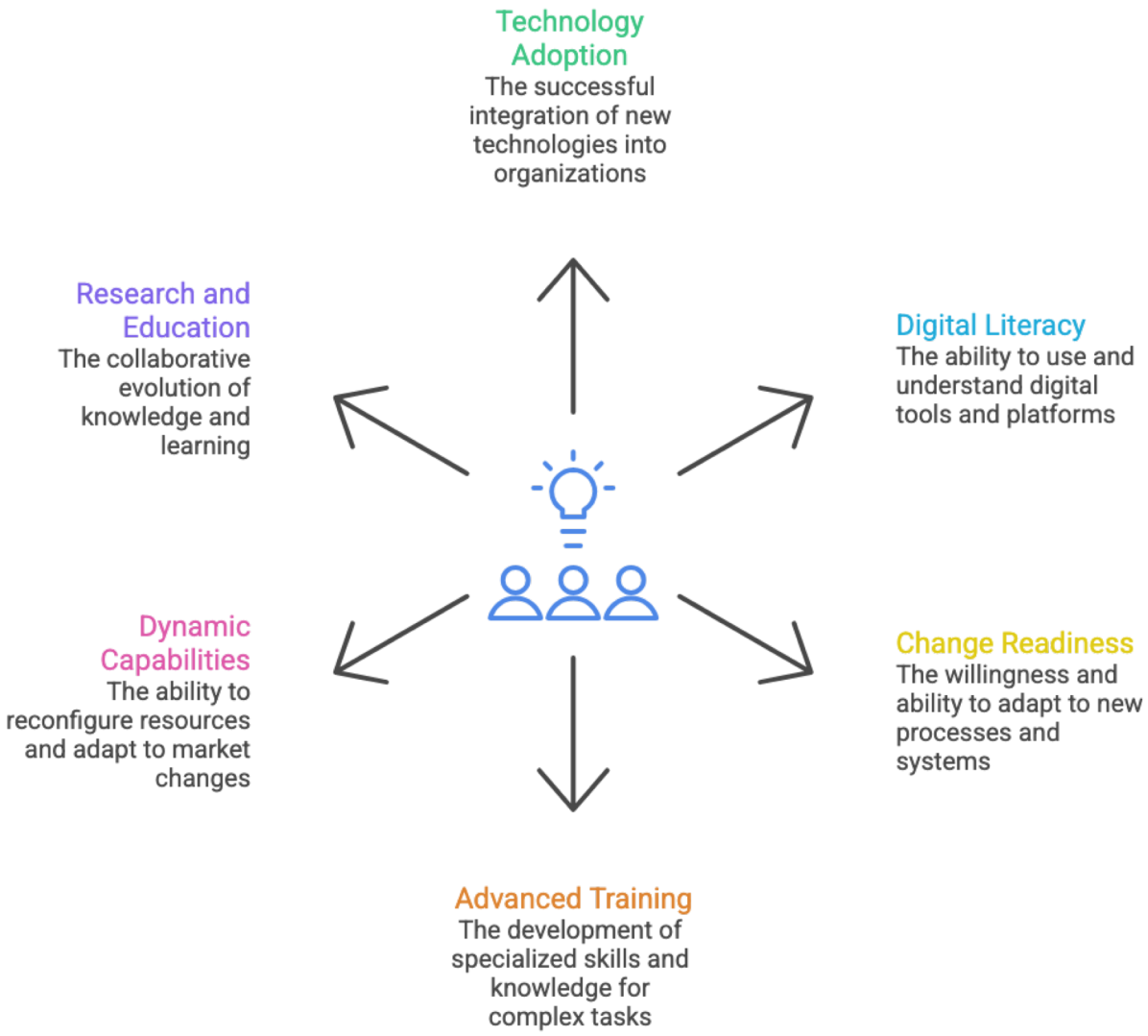
Emphasis is placed on predicting risks and ensuring continuity.



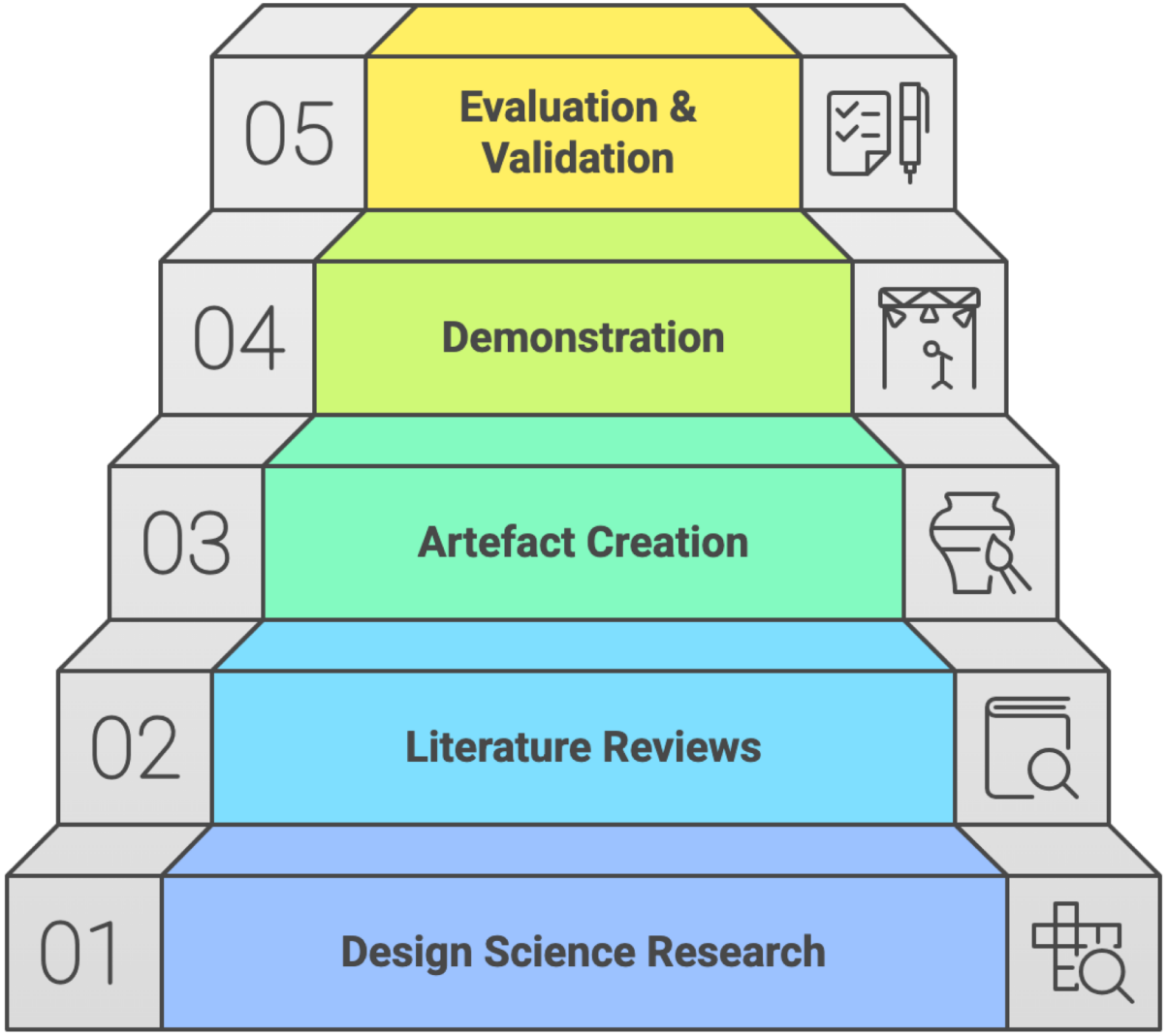
Trustworthy Infrastructure

Digital infrastructures are built on trust for successful transformation.

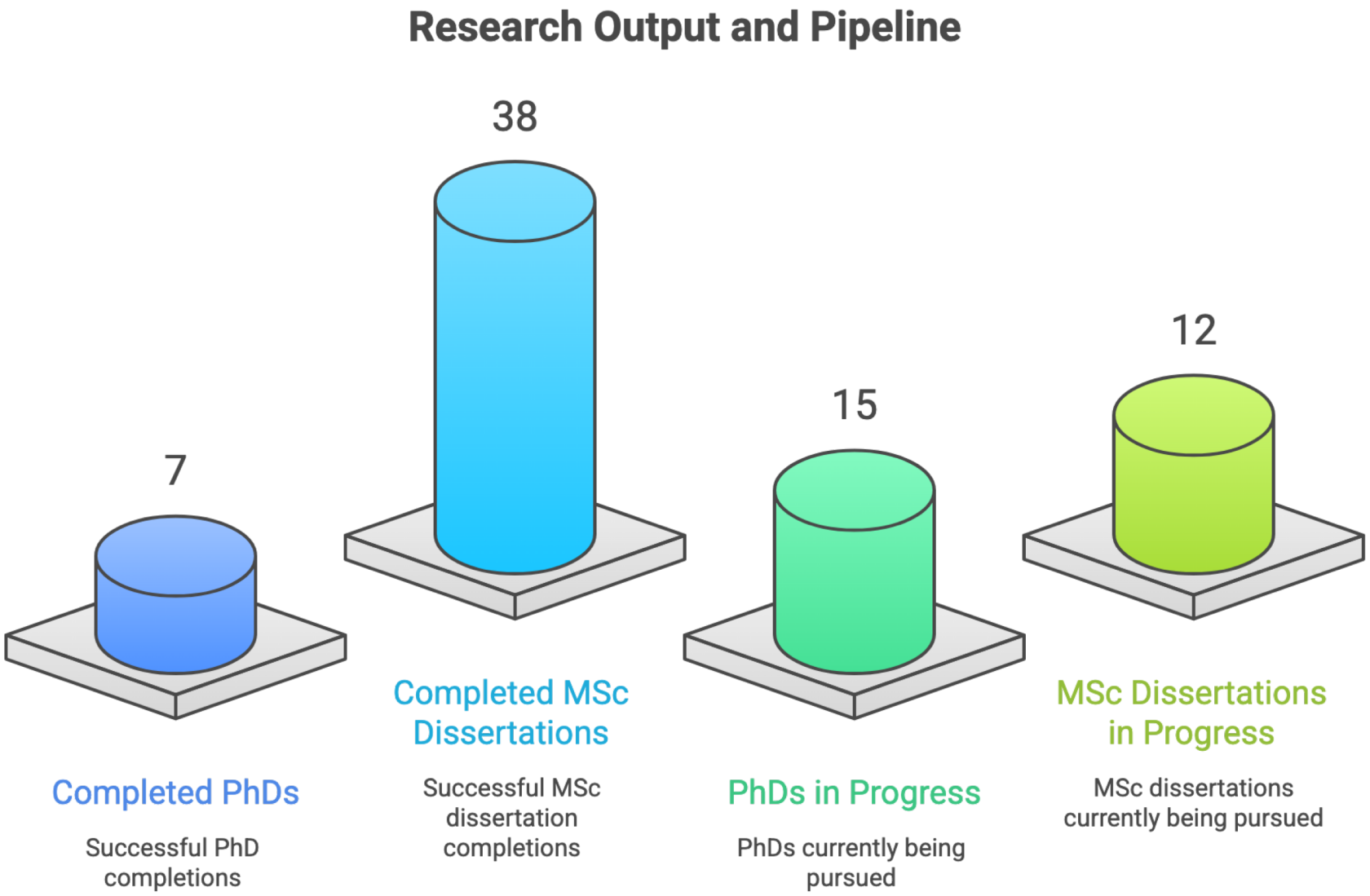
Axis 4 — Human capabilities and advanced training



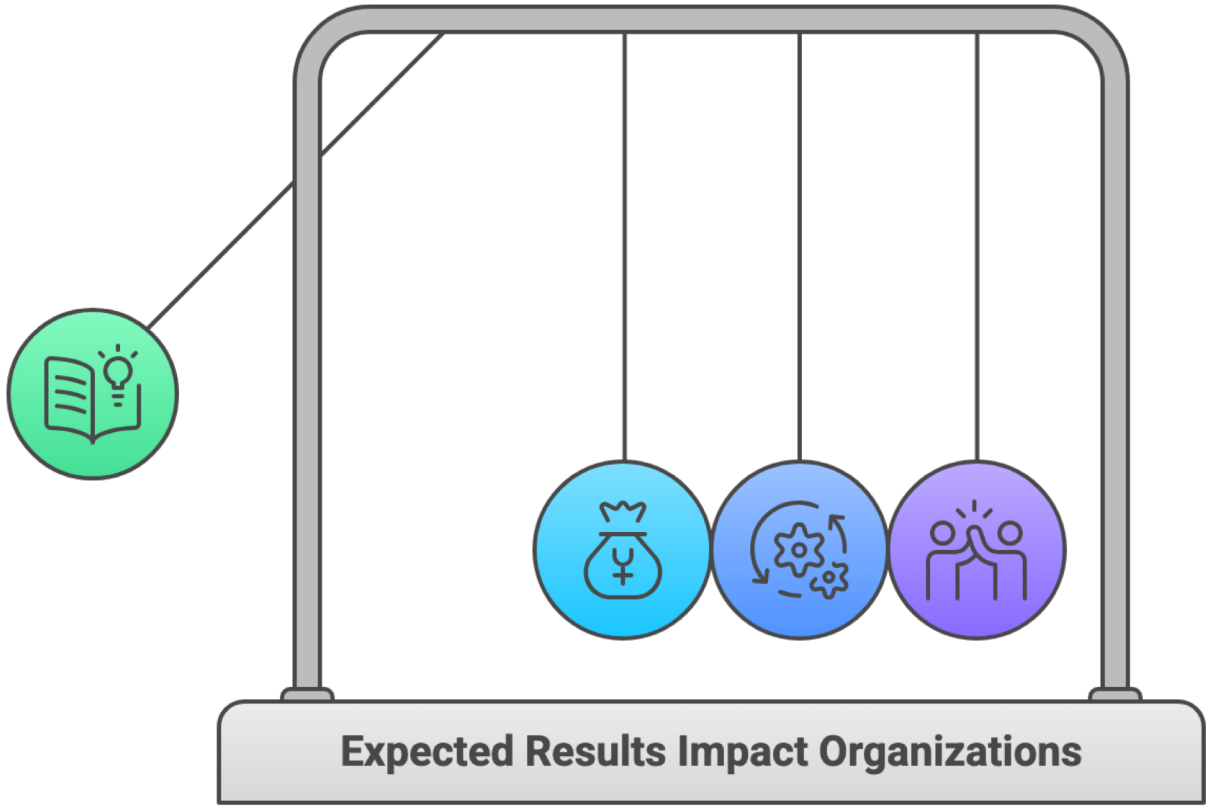
Methodological approach



Feasibility and scientific leadership



Expected results and impact (2026–2030)



High-Quality Publications

Disseminating research findings

Competitive Funding

Securing financial resources

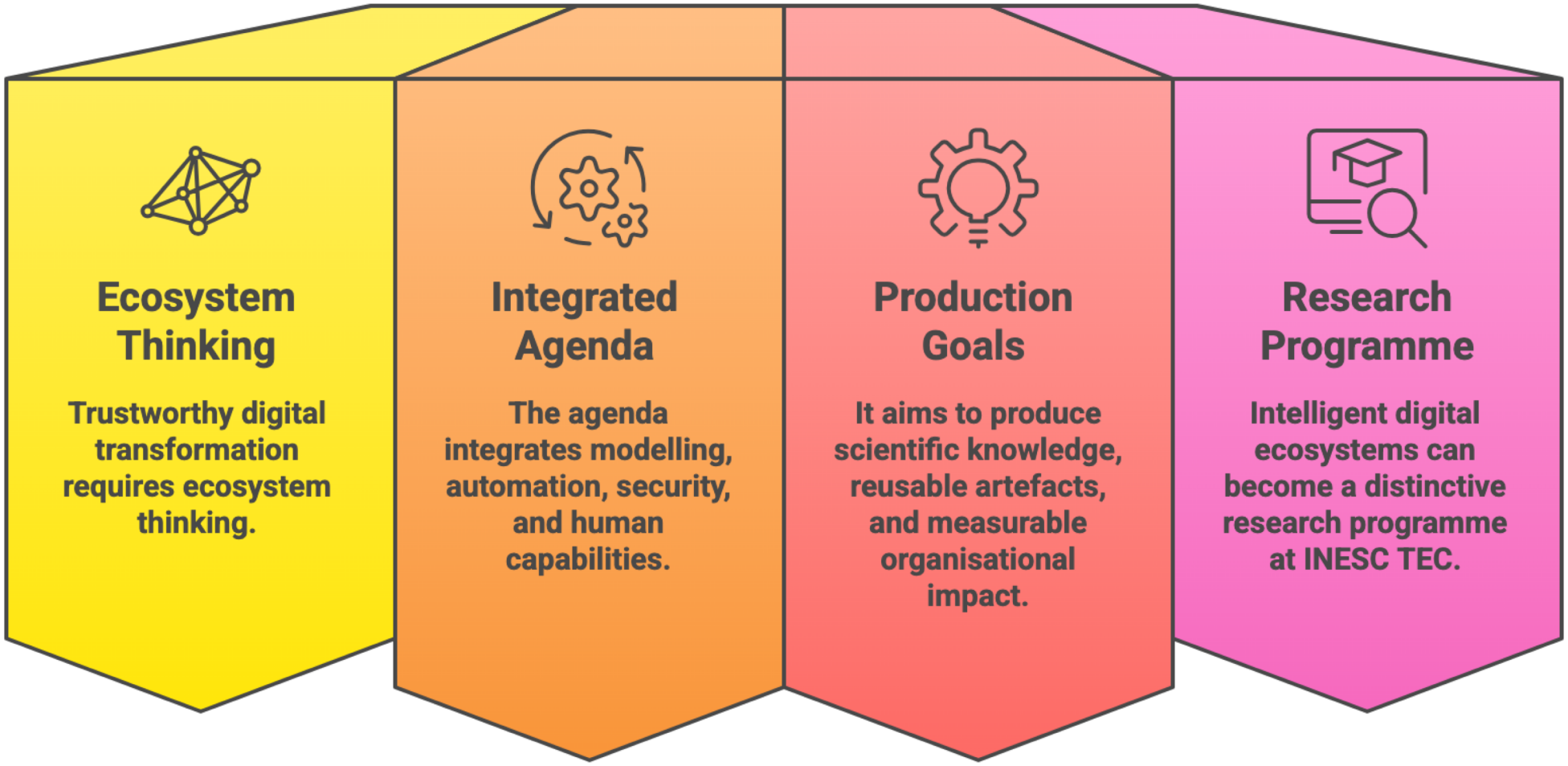
Reusable Artefacts

Creating valuable intellectual property

Organizational Impact

Transforming public and private sectors

Final message



Thank you for your time!

Henrique S. Mamede

henrique.s.mamede@inesctec.pt