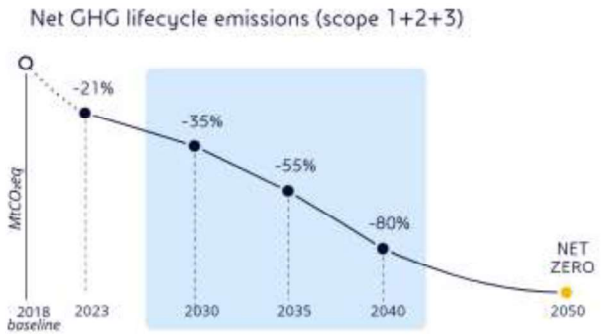
DIGITAL CENTER OF EXCELLENCE

eni

Innovating with AI at scale: from complex R&D challenges to widespread generative AI applications

13/02/2025

Digital for R&D: Motivation & Context



- We have embarked on an **industrial transformation** involving all business lines to decarbonize the entire company. To this end, we invest in researching, developing, and implementing **transition technologies**.
- According to the **technological neutrality principle**, there is no single solution to achieve the energy transition, we need a **technological mix** that can be adapted to different applications and needs. This is why we are developing a wide range of technologies that **support** the **decarbonisation** of each sector of the economy and our daily lives.

Eni applications in R&D to achieve Net Zero Emission

Energy from renewables
Electric and thermal energy

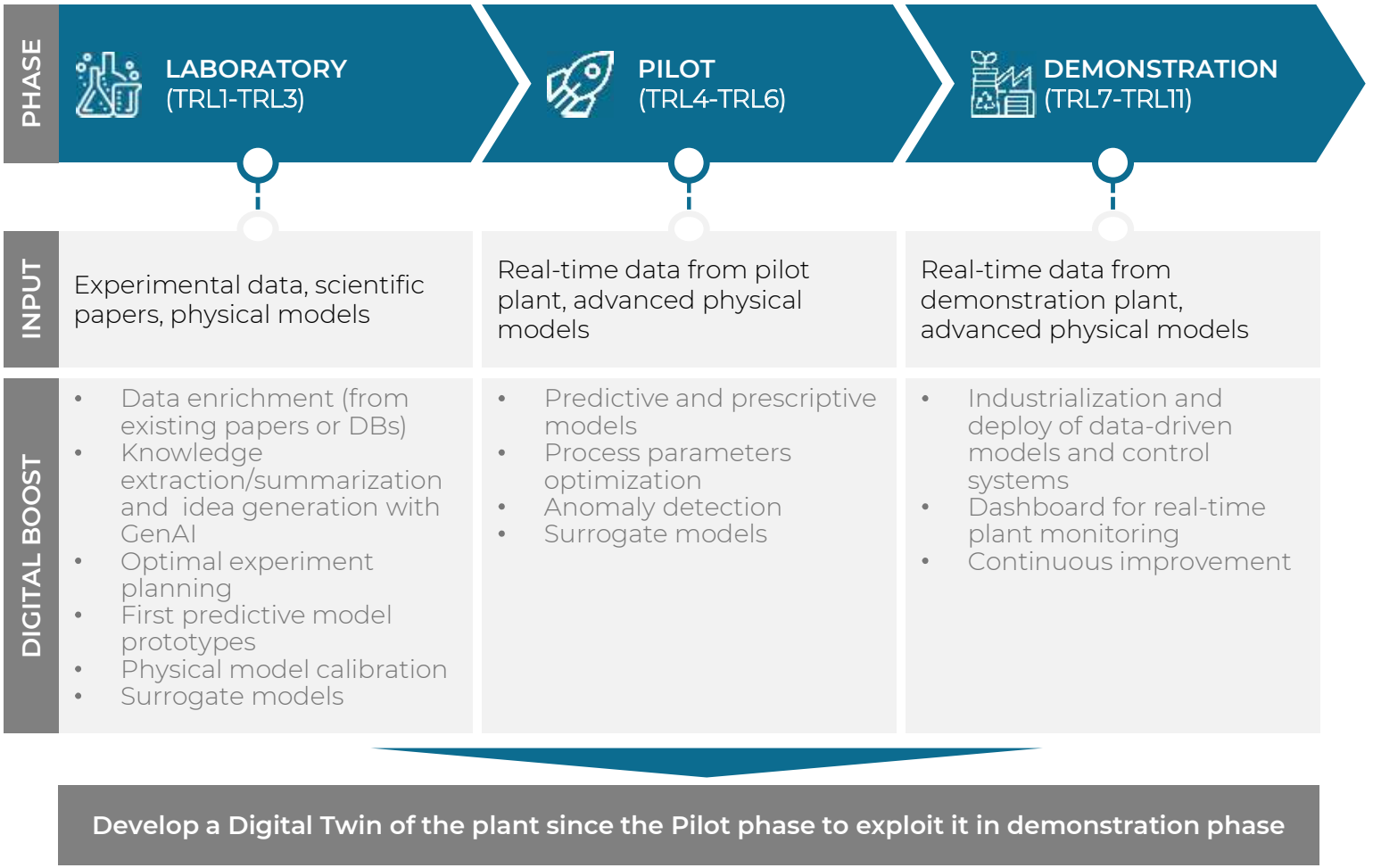
Fusion
The electricity and thermal energy of tomorrow

Circular Economy
Biofuels, sustainable chemistry and critical materials

CCUS
Decarbonization of processes

Environment
Ecosystem restoration

Artificial Intelligence for R&D



Use Case: Biomethane

Objectives

- **Define a framework for the yield % estimation** in the process of anaerobic digestion of single feedstock and feedstocks mix
- **Optimize the experiment number** to model the anaerobic digestion process for primary and secondary product
- **Prescribe** the optimal set of new experimental points to maximize the predictive capability of yield the model and increase process information

Challenges

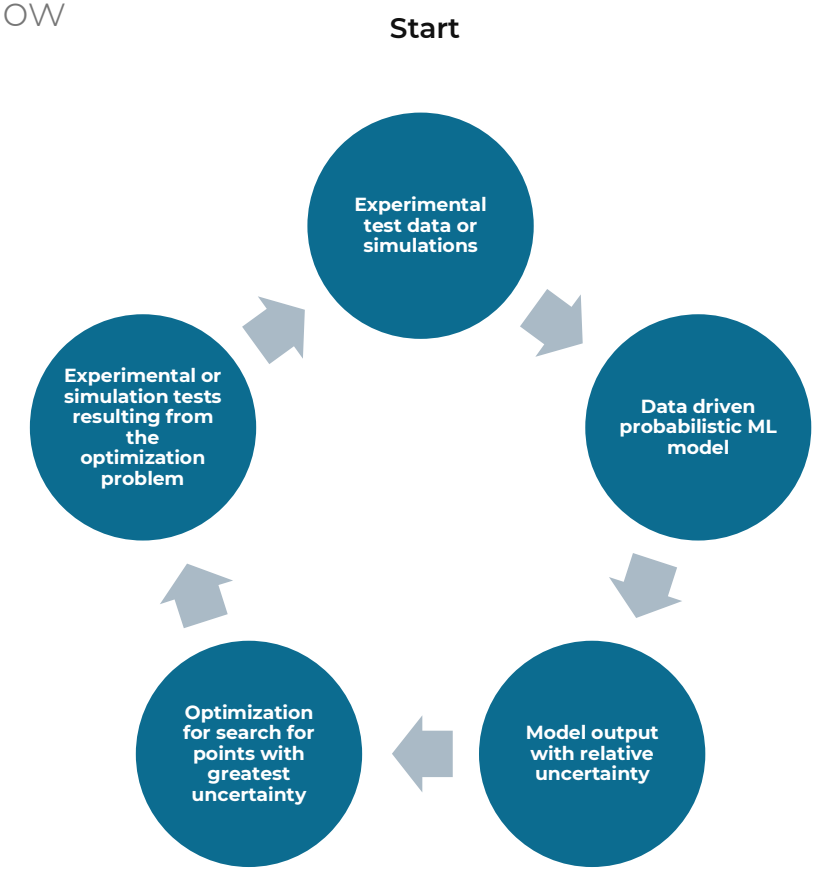
- **Small dataset** available due to the lack of a consistent feedstock stream at the plants
- **Months** are required to obtain a **complete dataset** on a single feedstock

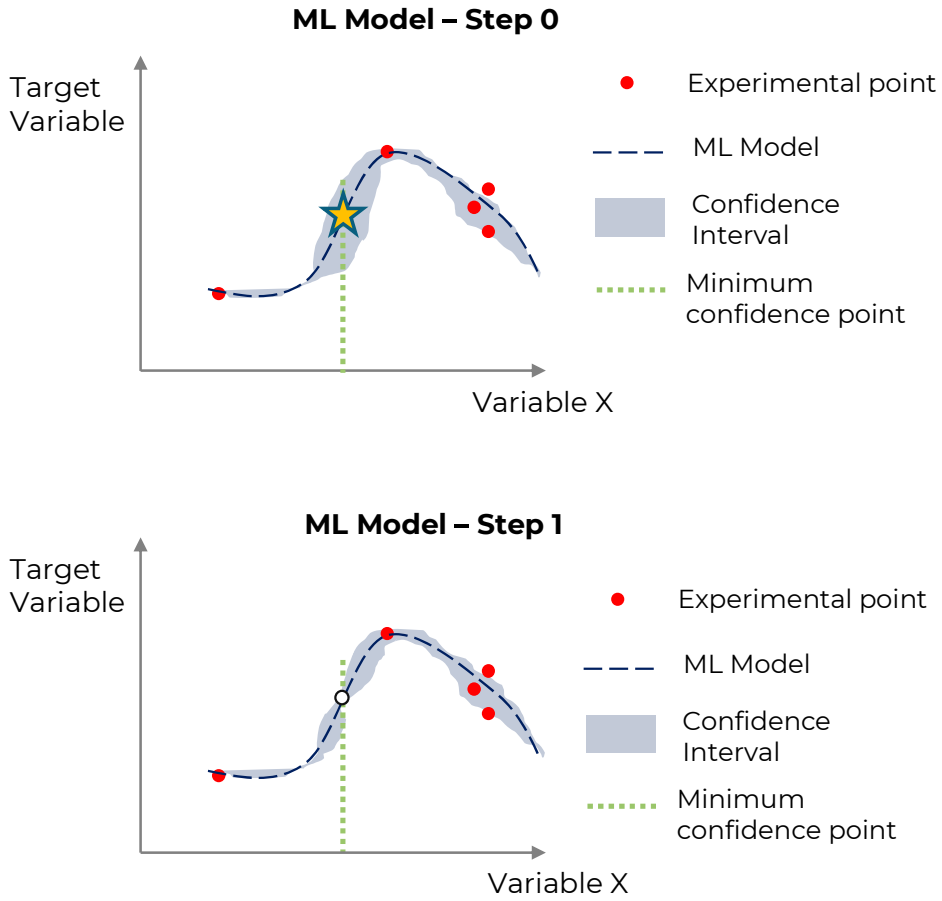
The project fits into the optimization of the development and production of biogas used as green fuel

Biomethane production primarily occurs through the anaerobic digestion (AD) process, a biological process that takes place in the absence of oxygen. In this process, organic materials such as agricultural waste, sewage sludge, food scraps, and other biomass are broken down by anaerobic microorganisms. The main products of anaerobic digestion are: Biogas and digestate, a solid residue that can be used as fertilizer.

Optimal Experimental Design

Workflow





Project Phases

1 Simulator Development

$$\frac{\partial \rho}{\partial t} + \nabla \cdot (\rho \mathbf{u}) = 0$$

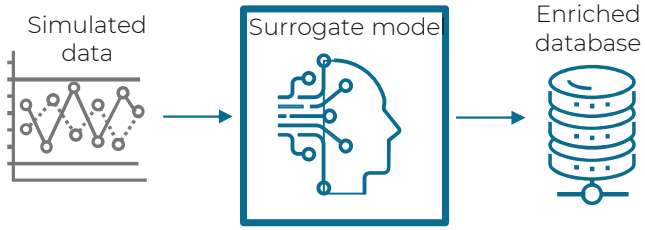
$$\frac{\partial (\rho \mathbf{u})}{\partial t} + \mathbf{u} \cdot \nabla (\rho \mathbf{u}) = \nabla \cdot \sigma + \rho \mathbf{f}$$

$$\frac{\partial E_t}{\partial t} + \nabla \cdot (E_t \mathbf{u}) = \nabla \cdot \sigma \mathbf{u} - \nabla \cdot \mathbf{q}$$

→ Solver

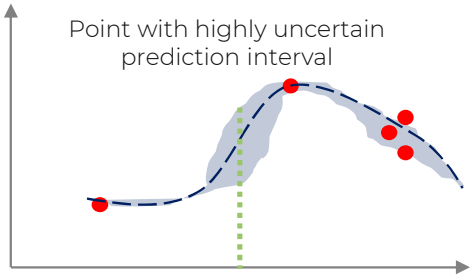
- Extensive literature review to find a **first principles model** that reproduces the anaerobic digestion process
- The **Anaerobic Digestion Model (ADM) 1** based simulator has been validated using experimental data
- The capability of correctly predicting the **feedstock yield** using known examples has been assessed

2 Surrogate Model



- Development of a **surrogate-based ML model** capable of reproducing the **ADM1** predictions **Biochemical Methane Potential** (**BMP**) using the feedstock properties as input and process conditions
- Using a proxy model allow to reproduce the local solution of the numerical method in **less time** and using **less computational resources**
- The **proxy model** is then used to enrich the available dataset

3 Design of Experiment



- Investigating points **where the uncertainty is higher** can have the highest impact on the information gain
- **OED** associates input variables and process properties to the output with its relative uncertainty of prediction
- On suitable domain points the **full simulator** or **experimental sessions** will be used to explore the output

Results
The tool have suggested experimental tests which all achieved the required performance and validated by domain experts

AI for accelerating carbon capture technologies

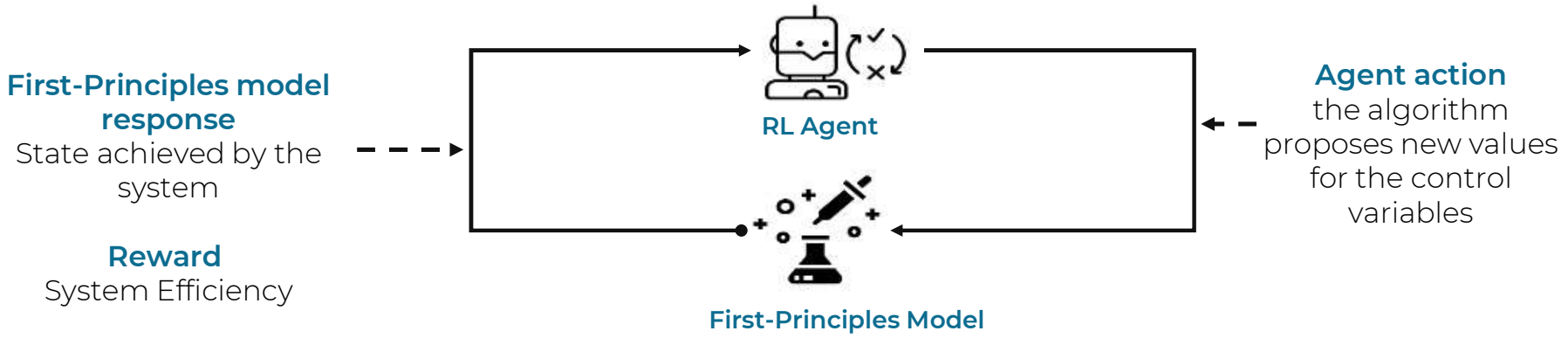
Objective

Support research and development in **designing, validating and industrializing a new technology for CO2 capture** through developing **artificial intelligence tools**

	Objective	Input	Developed solution
FIRST-PRINCIPLES MODELING	Provide a **mathematical description** of the system behavior for a better understanding of the system and simulate scenarios of interest	• Experimental data • Data of literature • Subject Matter Experts knowledge	• **First-Principles model** based on differential equations that allows simulating the trajectory of an experiment • Meta-heuristic optimization algorithms (**differential evolution**) to calibrate physical model parameters
OPTIMIZATION AND CONTROL	**Prescribing** the **optimal set–points** for the experimental setup in order to performance in **real-time**	• Simulation from the calibrated first-principles model	• **Reinforcement learning** model to prescribe the **best set points** for the experimental setup to optimize system performance in real-time using **simulations** from the first-principles model
PREDICTIVE MODELING	Providing real-time and automated **assessment** and **prediction** of quantities of interest	• Experimental data • Calibrated first-principles model	• Machine learning (deep **neural networks**) model to predict quantity of interest to be monitored

Reinforcement Learning for optimal system control

- **Modeling approach**: the system is represented by the **first-principles model**. The agent interacts instant by instant with the first-principles model by proposing new values of the variables to be optimized (actions) and causing the model to evolve (new state) and return a new value of **system efficiency*** (reward).



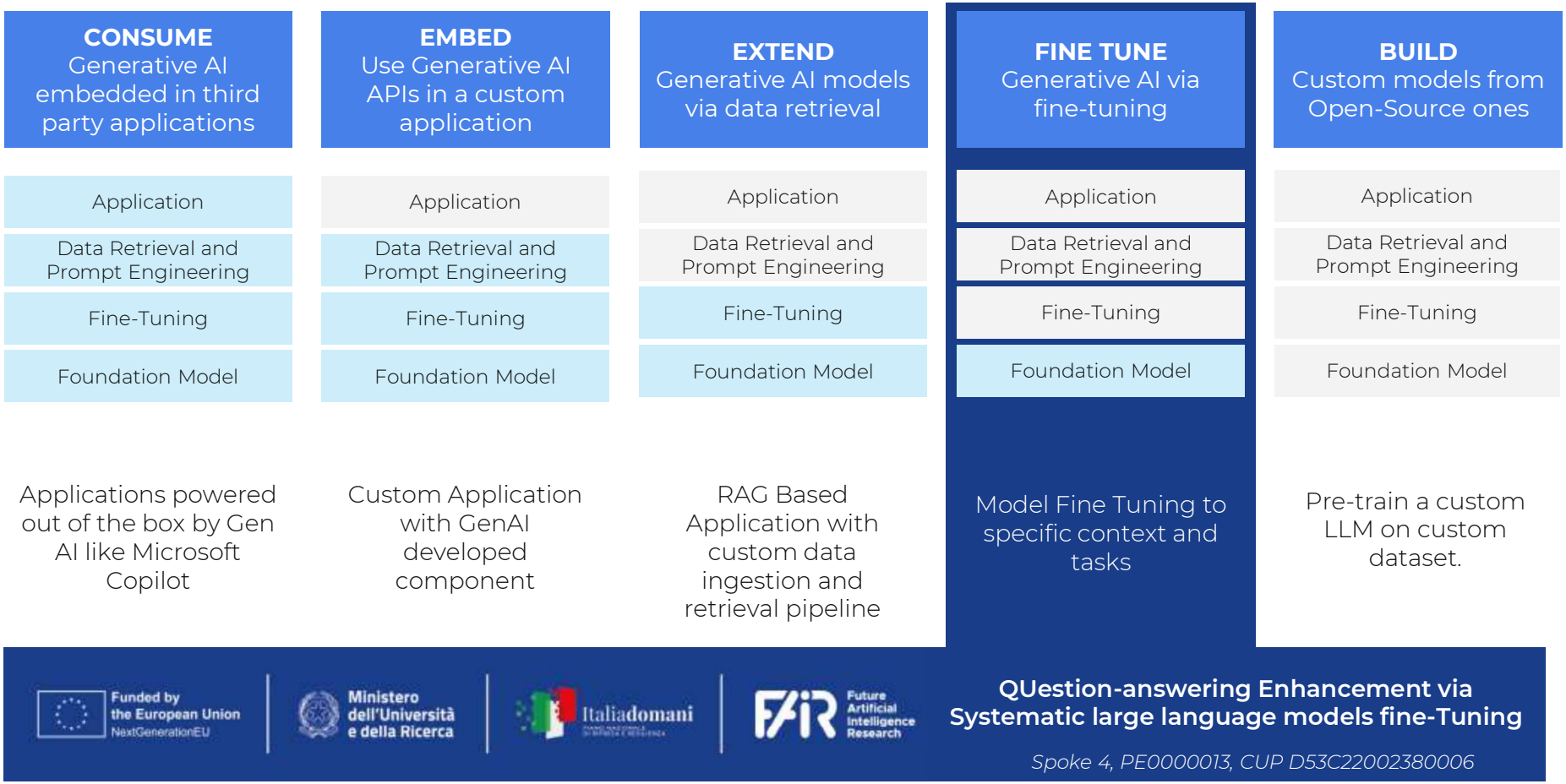
- **RL Algorithm:** Deep Deterministic Policy Gradient (DDPG)

Results
System performance obtained with RL is **doubled** with respect to the not optimized setting

*metric related to system performance while taking into account energy consumption (higher values are better)

Generative AI Deployment Approaches

Using GenAI as an example, Gartner sees five approaches emerging for deploying AI:



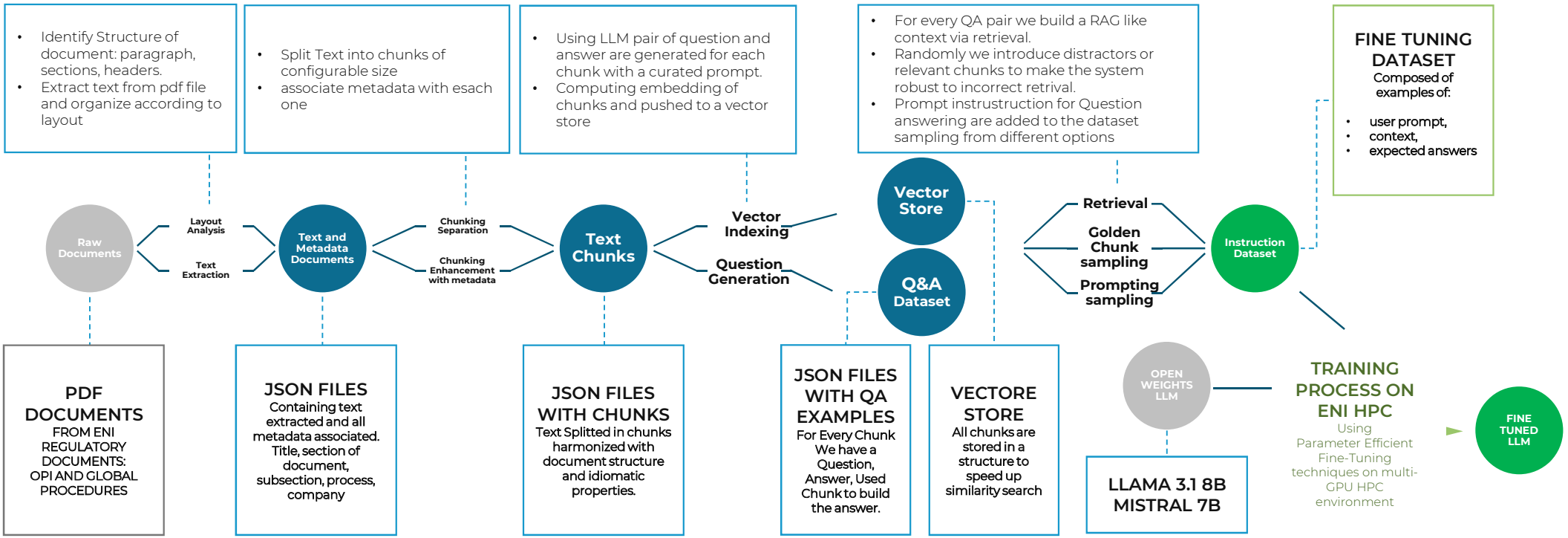
Funded by the European Union NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
FAIR Future Artificial Intelligence Research
QUestion-answering Enhancement via Systematic large language models fine-Tuning
Spoke 4, PE0000013, CUP D53C22002380006

Source https://www.gartner.com/en/information-technology/topics/ai-readiness

PROVIDER-MANAGED SELF-MANAGED

Open Source LLM Fine Tuning

For Q&A Task on a corpus of documents



Funded by the European Union NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
FAIR Future Artificial Intelligence Research

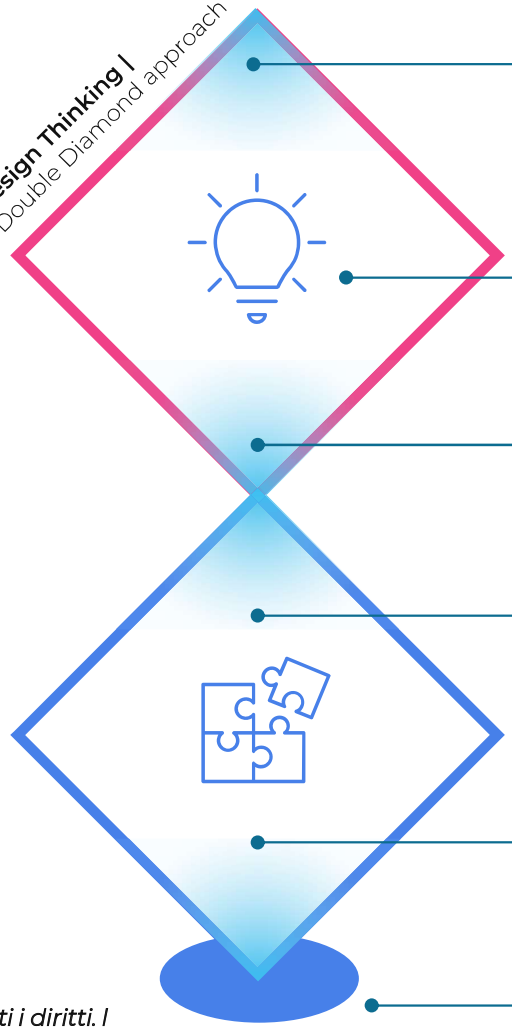
In contrast to pre-training, where you train the LLM using vast amounts of **unstructured textual data** via selfsupervised learning, **fine-tuning** is a supervised learning process where you use a data set of labeled examples to update the weights of the LLM.

Ideation & Prioritization: from Awareness to Use Cases

USE CASE **GENERATED** THROUGH DESIGN THINKING **WORKSHOPS**...

...INCLUDING **SPONTANEOUS USE CASE** FROM BUSINESSES OR FROM OTHER ACTIVITIES

Design Thinking | Double Diamond approach



AI & GEN AI AWARENESS

Experts explain **what AI & Gen AI are**, how they works and limits/opportunities in order to **give the basis to the working group to be able to ideate**.

IDEATE

Collaborative sessions in which to **co-design possible use-cases** based on specific topic for each business.

SELECT

Selection of ideas to be deepened in the next phase based on a first preliminary evaluation on business value and complexity.

RATIONALIZE

Ideas are explored in depth to understand **how they works, if they can be clustered together, the databases and the AI capabilities** of the to-be solution.

EVALUATE

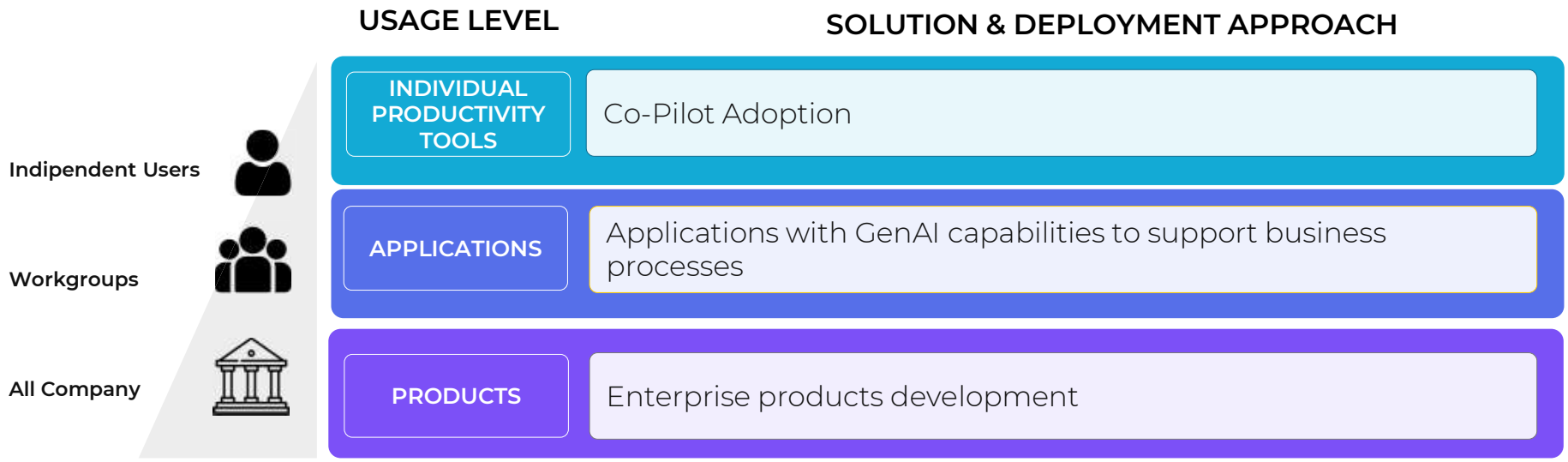
The use cases are then evaluated in more detail to understand the **next steps and, if necessary, the development of prototypes**.

DEVELOP PRIORITIZED USE CASES

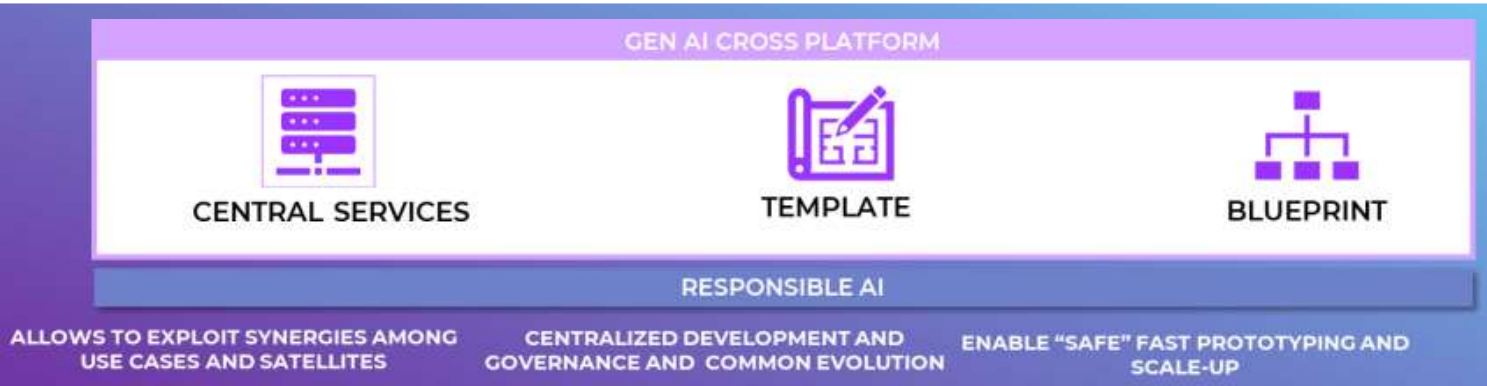
with Agile Methodology

Use Case Development

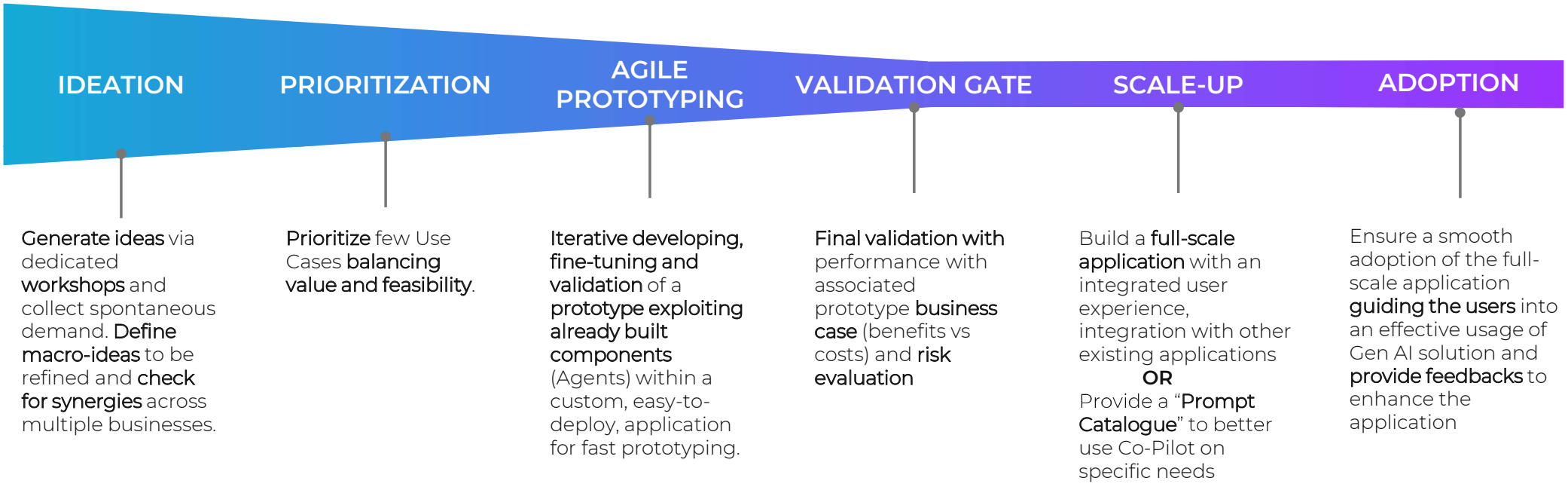
Leveraging synergies and building governance of Gen AI Applications



FOUNDATIONS



Our Approach to Generative AI



DEPLOYMENT APPROACH

CONSUME, EMBED, EXTEND
Enable quick development and validation of the use case

BUILD
Enable better performance

Eni Knowledge Hub

Improve the **search experience** of **certified documents** by **asking questions** to the **system** and **generating answers** using **Generative AI models**.

Chat interface
Ask question to the assistant within company chat application

Quick Information Access
Immediate and precise answer within the chat box

Certified and authored sources
Explicit reference to source documents with link to original source

USERS

INTERFACES WITH KNOWLEDGE HUB VIA MS TEAMS OR WITH WIDGET AVAILABLE FOR PRE-EXISTENT ENI WEB APPLICATIONS

AI

AI MODELS AND SERVICES ARE PROVIDED WITH SAFETY AND AUDIT CONTROL BY ENI GEN AI PLATFORM

KNOWLEDGE

DOCUMENTS ARE PROCESSED AND INDEXED WHTIN KH KNOWLEDGE BASE

SYSTEMS

INTEGRATION WITH KEY SYSTEM ENSURING DOCUMENTS ARE KEPT UP TO DATE

Artificial Threat Intelligence

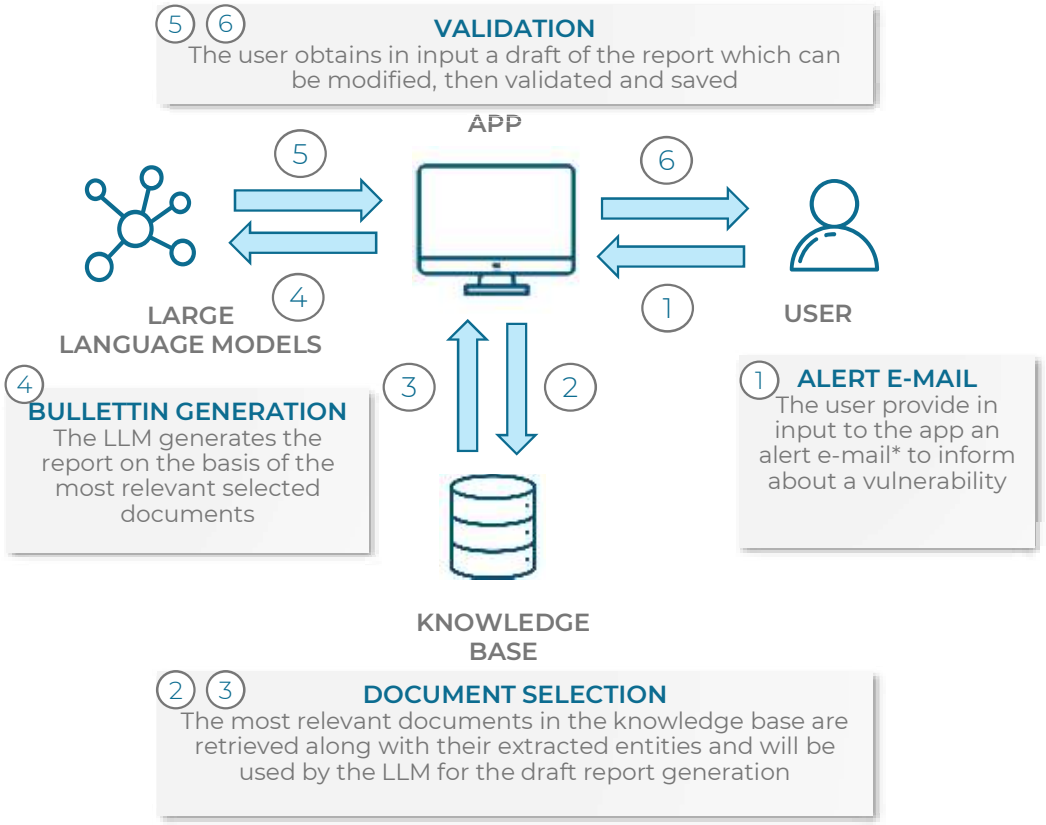
AI powered drafting of intelligence report of vulnerability readiness

SCOPE

To swiftly mitigate new **cyber threats**, a large volume of information, including impacted technologies, used techniques or tools, and at-risk areas, must be processed. This information comes from various sources, often in different formats. Analysts then compile this data into a concise **report** that outlines the threat and suggested actions.

REQUIREMENTS

Develop an intelligent tool to speed up cyber risk identification and analysis by monitoring threat information. This tool will **automatically create** a concise **report** that contextualizes the risk for Eni and its affiliates, enabling faster and even predictive mitigation planning.



GENERATED OUTPUT

Summary

Il seguente documento rappresenta una sintesi in merito alla vulnerabilità CVE-2024-21410 avente score CVSS pari a 9.8 che ha coinvolto il prodotto Microsoft Exchange Server.

Analysis

La vulnerabilità indicata nell'input è la CVE-2024-21410, che affligge il prodotto Microsoft Exchange Server. Si tratta di una vulnerabilità di tipo Elevation of Privilege, che consente a un attore malintenzionato di ottenere le credenziali NTLM di un utente e di impersonarlo su un server Exchange vulnerabile. La vulnerabilità è stata sfruttata attivamente in rete da diversi Threat Actor. Per mitigare possibili tentativi di sfruttamento, si consiglia di verificare la presenza delle configurazioni vulnerabili e di provvedere all'aggiornamento dei prodotti software esposti, in particolare per le versioni Microsoft Exchange Server 2016 Cumulative Update 23, Microsoft Exchange Server 2019 Cumulative Update 13 e Microsoft Exchange Server 2019 Cumulative Update 14. Maggiori dettagli e misure di mitigazione sono disponibili sul Portale pubblico del CSIRT Italia e sui riferimenti forniti.

Mitigation Details

Per mitigare i potenziali tentativi di sfruttamento della vulnerabilità CVE-2024-21410 in Microsoft Exchange Server, si consiglia di adottare le seguenti misure:

1. Verificare la presenza delle configurazioni vulnerabili e assicurarsi di utilizzare una versione del prodotto non soggetta alla vulnerabilità. In particolare, verificare se si sta utilizzando una delle seguenti versioni:
   - Microsoft Exchange Server 2016 Cumulative Update 23
   - Microsoft Exchange Server 2019 Cumulative Update 13 (dalla versione 15.02.0 fino a 15.2.1544.004 esclusa)
   - Microsoft Exchange Server 2019 Cumulative Update 14 (dalla versione 15.02.0 fino a 15.2.1544.004 esclusa)
2. Applicare gli aggiornamenti software disponibili forniti da Microsoft per correggere la vulnerabilità. Maggiori dettagli e le relative misure di mitigazione possono essere trovati sul Portale pubblico di CSIRT Italia.
3. Seguire le indicazioni fornite da Microsoft per le mitigazioni e i possibili workaround specifici per la vulnerabilità CVE-2024-21410. Ulteriori dettagli possono essere trovati nei seguenti riferimenti:
   - Microsoft Security Response Center - CVE-2024-21410