

# **Work Plan Resume – Rafael Silva**

**Title:** Human-centric Agent-based Adaptive Intelligent Communities

## **Abstract:**

The proposed research aims to conceive, develop, implement, and validate a novel and adaptive intelligent solution for intelligent facilities, designed to model, mediate, and respond to human preferences and contextual dynamics in real time. The proposed solution will use agents to resolve conflicts between users, manage and operate the system within defined permission boundaries. The system will integrate graph neural networks and large/small language models to model the user preferences, and to provide autonomous, personalized and context-aware control. This research also envisions agents that can identify users' latent needs to autonomously discover and deploy additional services. This will enable a more accurate digital representation of the user, interactions that will adapt to each given user, and enable communication and resource sharing between intelligent buildings.

**Keywords:** Intelligent Buildings, User Preference Elicitation, Context Awareness, Digital Twin, Edge Computing

## **United Nations Sustainable Development Goals:**

Objective 9: Industry, innovation and infrastructure

Objective 11: Sustainable Cities and Communities

## **Intelligent Specialisation Areas:**

Digital Transition

## **State of the art:**

The field of artificial intelligence is rapidly transforming various sectors, and its application in intelligent buildings presents a significant opportunity to enhance human-centric adaptation [1], [2]. The core challenge is to create systems that are adaptive to human needs, interactive in a natural way, and ensuring privacy and responsiveness [3].

In user modeling, general solutions focus more on behavioral modeling, using approaches such as deterministic, stochastic, or agent-based [4]. However, for preference modeling, more traditional solutions rely on rule-based methods [5] that while providing many advantages such as explainability, do not capture nuanced variations in human preferences or handle the complexity in multi-occupant scenarios [6]. The emergence of graph-based representations [7], [8], [9], particularly knowledge graphs has provided a more robust method for modeling the

connections between, users, devices, spaces, and context, when compared with machine learning solutions which typically capture behavioral patterns from sensor data [10].

From an architectural standpoint, the dominant paradigm has been centralized, cloud-based systems [11]. While powerful, this approach introduces problems in latency, reliability, privacy, and security [12], [13]. In response, a shift towards distributed and edge computing has gained momentum [14], [15], [16], aiming to process data closer to its source and, also, agent systems have been explored for decentralized control [17], [18].

Interaction between human and buildings has evolved from simple dashboards to voice-activated commands. While an improvement, these forms of interaction often lack context-awareness, and are largely transactional and reactive [19]. The integration of large language models (LLM) [20], [21], [22] and small language models (SLM) [23], [24] present an opportunity to create fluid interaction and, also, enable proactive assistance. The primary gap is to integrate these language models with real-time and structured system context so they can leverage proactive preference elicitation, personalized system behavior, and handle conflict mediation [25], [26].

In conclusion, while the literature presents advances in user preference modeling, distributed systems, and language models, there is a gap in research that combines these concepts into a unified framework. The work will evolve from model proposed by the candidate in [27], [28]. This project directly addresses this multi-faceted gap, aiming to deliver a holistic solution that is more adaptive, interactive, and resilient than the current state of the art.

## **Objectives:**

The primary objective of this research project is to conceive, develop, implement, test, and validate a novel distributed and adaptive intelligence framework for intelligent buildings, capable of modeling, mediating, and responding to human preferences and contextual dynamics in real time.

To achieve this goal, a set of intermediary objectives are established:

1. Continuous monitoring and update of the state of the art (RQ0-4).
2. Conceive and develop a graph-based user-modelling (RQ1).
3. Conceive and develop a multi-agent architecture, based on LLM/SLM mechanisms, for user interaction and latent needs discovery (RQ2).
4. Develop an agentic control framework that enables agents to autonomously manage the system (RQ3).

5. Define and implement a comprehensive security and privacy-preserving architecture (RQ4).
6. Integrate, test and validate the complete models using realistic scenarios and real pilots (RQ1-4).

Throughout the development of the PhD, efforts to disseminate the discoveries and achievements will be made to advance more in state of the art in this scientific field.

### **Detailed description:**

#### **Research Questions:**

Main research question: RQ0 – How can agents effectively manage an intelligent community?

RQ1. How can intelligent buildings dynamically model and adapt to the user's individual and group preferences using graph-based heterogeneous representations?

RQ2. In what ways can LLMs and SLMs be employed, not only to infer user intent and contextual relevance, but also to interact with occupants through dialog for clarification, negotiation, and preference definition?

RQ3. How can an agent identify a user's latent needs and autonomously discover, negotiate for, and deploy and use containerized services to address them?

RQ4. What mechanisms are required to enable peer-to-peer sharing of resources, such as computational availability and sensor data, between the autonomous agents of different users while preserving privacy and individual control?

#### **Work Packages:**

##### **WP 1: Literature Review**

WP1 focuses on conducting a systematic and continuous review of the state of the art, especially regarding intelligent buildings, user modelling targeting the preferences with context awareness using Graph Neural Networks (GNNs), LLMs and SLMs regarding Model Context Protocol (MCP) and user interaction. These concepts will be reviewed with a particular focus on edge devices or low powered devices. Additionally, this work package will identify the key challenges and gaps on the current literature.

#### Tasks:

- T1.1 – Define search strings, inclusion/exclusion criteria
- T1.2 – Execute systematic literature review

Outcomes:

- State of the art review;
- Systematic literature report, considering (PRISMA);

## **WP 2: System Design and Requirements Specification**

WP2 regards the conception and design of the overall system, defining how each component will interact and communicate with each other. The technical aspect of the requirements, use cases, functional specifications, and performance indicators of the project will be defined here. The objective is to design a scalable distributed architecture that can handle real-time interactions and personalization, using microservice oriented principles.

Tasks:

- T2.1 – Define the functional and non-functional requirements
- T2.2 – Describe the use cases
- T2.3 – Identify KPIs and Metrics
- T2.4 – Design the system architecture
- T2.5 - Define the framework's data management plan

Outcomes:

- Requirements specification document
- Data Management document
- System Architecture Design

## **WP 3: Distributed Digital Twin Infrastructure**

WP3 is dedicated to building the core technical infrastructure, including the development of the simulated building environment, and the creation of the agent communication structure and data protocols. Additionally, it focuses on establishing the inter-agent communication protocol, which will support both direct agent-to-agent and remote connectivity, enabling peer-to-peer resource sharing.

- T3.1 – Create a data ingestion pipeline, using Kafka
- T3.2 – Implement Inter-agent Communication
- T3.3 – Build the digital twin environment
- T3.4 – Build an initial basic frontend prototype
- T3.5 – Develop tools to allow the LLM operation

Outcomes:

- Data Ingestion Pipeline
- Digital Twin Software Prototype

- Real-Time dashboard

#### **WP 4: User Preference and Context Modeling**

WP4 focuses on creating a dynamic model of users and their environments. Using heterogeneous graphs to understand and predict their needs and using dialogue to gather information. The heterogeneity will allow the model to capture the different relations between the different entities, such as users, preferences and context. The objective is to accurately model often unstated human preferences from indirect and potentially noisy sensor data and to infer latent needs rather than simply reacting to explicit commands. One of the key enablers is the robust modeling of context, given that it has a significant role in the definition of the latent preference.

Task:

- T4.1 – Design the heterogeneous graph schema
- T4.2 – Define the model's training methodology, including metrics
- T4.3 – Conceive the algorithm for conflict identification
- T4.4 – Implement the training loop, evaluation scripts and conflict identification model
- T4.5 – Develop the LLM/SML interaction model

Outcomes:

- GNN preference model
- User interaction component using LLMs and SMLs

#### **WP 5: Human-centric Agent-based Adaptive Intelligent Communities Framework**

This WP focuses on the agent's ability to manage the system and act autonomously. This includes making decisions, negotiating between users, sharing resources with other agents, and dynamically deploying new services as needed. The agent will also interact proactively with the user when taking decisions above its autonomy.

Task:

- T5.1 - Create the JSON schema for the MCP that will be used to prime the LLMs
- T5.2 – Develop the agent's decision logic, considering the constraints of Bounded Autonomy
- T5.3 – Develop the service discovery and management mechanism
- T5.4 – Implement peer-to-peer resource sharing
- T5.5 – Implement the agent's core control and interaction with the user

Outcomes:

- Agent Control Software
- Dynamic Service Provisioning Framework

#### **WP6: Test and Validation using realistic scenarios and real pilots**

WP6 ensures the individual components from the previous WPs work together seamlessly, as a single system. Then the proposed solution is tested to prove that the system meets the goals defined in WP2. The use cases will be executed and analyzed to perform iterative refinement of the models and agents.

Task:

- T5.1 – Create the deployment configuration for the entire application stack
- T5.2 – Define the initial state for each use case
- T5.3 – Develop and validate the measurement procedures for the KPIs and metrics
- T5.4 – Implement the integration configurations and automated deployment scripts
- T5.5 – Execute the experimental scenarios within the Digital Twin
- T5.6 - Analyze and evaluate the experiments in the realistic environment

Outcomes:

- Integrated System Prototype
- Demonstration of each use case
- Evaluation Report

#### **WP 7: Dissemination and Communication**

WP7 regards the dissemination and communication of the research activities and results. The goal is to publish a minimum of 10 open-access scientific papers, where at least 4 will be in SCIE-indexed journals and the rest in international conferences. These numbers are considering the historic number of publications of the applicant. In order to ensure broader dissemination of the results and contribute to open science, the datasets, models, and software developed during the PhD. This research could also contribute to R&D projects running in GECAD/ISEP, namely Sa4CPS (ITEA: 22007, Compete2030: FEDER-00368800 – 12737), EnergyP2P (Compete2030: FEDER-00960500–14646), and AdOff (Compete2030:FEDER-01236200  
ITEA: 23048).

- T7.1 - Document with the dissemination plan
- T7.2 - Annual and final reports for FCT
- T7.3 - Final Technical Report and Publications

## Milestones:

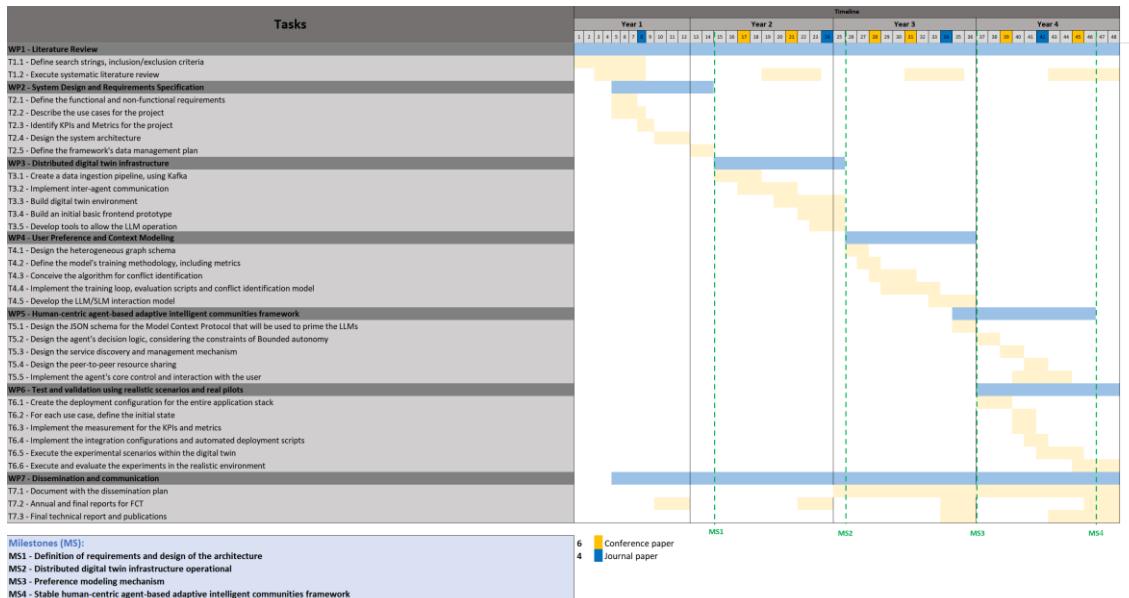
MS1- Definition of requirements and design of the architecture

MS2- Distributed Digital Twin infrastructure operational

MS3 – Preference modeling mechanism

MS4 – Stable Human-centric Agent-based Adaptive Intelligent Communities Framework

## Timeline:



## Bibliographic References:

- [1] Y. Wang and Y. Lu, “Interaction, Process, Infrastructure: A Unified Architecture for Human-Agent Collaboration,” Jun. 2025, Accessed: Aug. 01, 2025. [Online]. Available: <https://arxiv.org/abs/2506.11718v1>
- [2] A. Al Safadi *et al.*, “Self-learning Buildings: integrating Artificial Intelligence to create a building that can adapt to future challenges,” *IOP Conf Ser Earth Environ Sci*, vol. 1019, no. 1, p. 012047, Apr. 2022, doi: 10.1088/1755-1315/1019/1/012047.
- [3] H. Bier, A. Hidding, S. Khademi, C. van Engelenbrug, H. Alavi, and S. Zhong, “Advancing Applications for Artificial-Intelligence-Supported Ambient Control in the Built Environment,” *Technology|Architecture + Design*, vol. 8, no. 1, pp. 155–164, 2024, doi: 10.1080/24751448.2024.2322927.
- [4] F. Mofidi and H. Akbari, “Intelligent buildings: An overview,” *Energy Build*, vol. 223, p. 110192, Sep. 2020, doi: 10.1016/J.ENBUILD.2020.110192.

- [5] E. Purificato, L. Boratto, and E. W. De Luca, “User Modeling and User Profiling: A Comprehensive Survey,” Feb. 2024, Accessed: Aug. 01, 2025. [Online]. Available: <https://arxiv.org/abs/2402.09660v2>
- [6] J. Kim, S. Schiavon, and G. Brager, “Personal comfort models – A new paradigm in thermal comfort for occupant-centric environmental control,” *Build Environ.*, vol. 132, pp. 114–124, Mar. 2018, doi: 10.1016/J.BUILDENV.2018.01.023.
- [7] Z. Guo and H. Wang, “A Deep Graph Neural Network-Based Mechanism for Social Recommendations,” *IEEE Trans Industr Inform.*, vol. 17, no. 4, pp. 2776–2783, Apr. 2021, doi: 10.1109/TII.2020.2986316.
- [8] C. Zhang, D. Song, C. Huang, A. Swami, and N. V. Chawla, “Heterogeneous graph neural network,” *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 793–803, Jul. 2019, doi: 10.1145/3292500.3330961.
- [9] X. Li, L. Sun, M. Ling, and Y. Peng, “A survey of graph neural network based recommendation in social networks,” *Neurocomputing*, vol. 549, p. 126441, Sep. 2023, doi: 10.1016/J.NEUCOM.2023.126441.
- [10] N. Vaska, K. Leahy, and V. Helus, “Context-Dependent Anomaly Detection with Knowledge Graph Embedding Models,” *IEEE International Conference on Automation Science and Engineering*, vol. 2022-August, pp. 2020–2027, Mar. 2022, doi: 10.1109/CASE49997.2022.9926631.
- [11] Z. Chang, S. Liu, X. Xiong, Z. Cai, and G. Tu, “A Survey of Recent Advances in Edge-Computing-Powered Artificial Intelligence of Things,” *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13849–13875, Sep. 2021, doi: 10.1109/JIOT.2021.3088875.
- [12] A. R. Khouas, M. R. Bouadjenek, H. Hacid, and S. Aryal, “Training Machine Learning models at the Edge: A Survey,” Mar. 2024, Accessed: Aug. 01, 2025. [Online]. Available: <https://arxiv.org/abs/2403.02619v3>
- [13] M. G. Sarwar Murshed, C. Murphy, D. Hou, N. Khan, G. Ananthanarayanan, and F. Hussain, “Machine Learning at the Network Edge: A Survey,” *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, Oct. 2021, doi: 10.1145/3469029.
- [14] X. Jin *et al.*, “Edge Security: Challenges and Issues,” Jun. 2022, Accessed: Aug. 01, 2025. [Online]. Available: <https://arxiv.org/abs/2206.07164v1>
- [15] D. V. Talati and D. V. Talati, “Decentralized AI: The role of edge intelligence in next-gen computing,” *International Journal of Science and Research Archive*, vol. 2, no. 1, pp. 216–232, Jun. 2021, doi: 10.30574/IJSRA.2021.2.1.0050.

- [16] D. Xu *et al.*, “Edge Intelligence: Architectures, Challenges, and Applications,” Mar. 2020, Accessed: Aug. 01, 2025. [Online]. Available: <https://arxiv.org/abs/2003.12172v2>
- [17] S. Tuli *et al.*, “AI augmented Edge and Fog computing: Trends and challenges,” *Journal of Network and Computer Applications*, vol. 216, p. 103648, Jul. 2023, doi: 10.1016/J.JNCA.2023.103648.
- [18] P. Grzesik and D. Mrozek, “Combining Machine Learning and Edge Computing: Opportunities, Challenges, Platforms, Frameworks, and Use Cases,” *Electronics 2024, Vol. 13, Page 640*, vol. 13, no. 3, p. 640, Feb. 2024, doi: 10.3390/ELECTRONICS13030640.
- [19] A. Fuad and M. Al-Yahya, “Recent Developments in Arabic Conversational AI: A Literature Review,” *IEEE Access*, vol. 10, pp. 23842–23859, 2022, doi: 10.1109/ACCESS.2022.3155521.
- [20] S. M. Wasti, K. Q. Pu, and A. Neshati, “Large Language User Interfaces: Voice Interactive User Interfaces powered by LLMs,” *Lecture Notes in Networks and Systems*, vol. 1065 LNNS, pp. 639–655, Feb. 2024, doi: 10.1007/978-3-031-66329-1\_41.
- [21] T. N. Nguyen, K. Jamale, and C. Gonzalez, “Predicting and Understanding Human Action Decisions: Insights from Large Language Models and Cognitive Instance-Based Learning,” Jul. 2024, Accessed: Aug. 01, 2025. [Online]. Available: <https://arxiv.org/abs/2407.09281v2>
- [22] J. Chen *et al.*, “When Large Language Models Meet Personalization: Perspectives of Challenges and Opportunities,” *World Wide Web*, vol. 27, no. 4, Jul. 2023, doi: 10.1007/s11280-024-01276-1.
- [23] L. C. Magister, J. Mallinson, J. Adamek, E. Malmi, and A. Severyn, “Teaching Small Language Models to Reason,” *Proceedings of the Annual Meeting of the Association for Computational Linguistics*, vol. 2, pp. 1773–1781, Dec. 2022, doi: 10.18653/v1/2023.acl-short.151.
- [24] P. Zhang, G. Zeng, T. Wang, and W. Lu, “TinyLlama: An Open-Source Small Language Model,” Jan. 2024, Accessed: Aug. 01, 2025. [Online]. Available: <https://arxiv.org/abs/2401.02385v2>
- [25] M. Marge *et al.*, “Spoken language interaction with robots: Recommendations for future research,” *Comput Speech Lang*, vol. 71, p. 101255, Jan. 2022, doi: 10.1016/J.CSL.2021.101255.
- [26] K. Fujita, · Kazuki Takashima, Y. Itoh, and · Yoshifumi Kitamura, “Human-Workspace Interaction: prior research efforts and future challenges for

supporting knowledge workers," *Quality and User Experience* 2023 8:1, vol. 8, no. 1, pp. 1–19, Aug. 2023, doi: 10.1007/S41233-023-00060-9.

- [27] R. Silva, L. Gomes, and Z. Vale, "Caravels: A Decentralized Container-Based Infrastructure for Sustainable Human-Centric Intelligent Energy Communities," *Lecture Notes in Networks and Systems*, vol. 888 LNNS, pp. 241–250, 2024, doi: 10.1007/978-3-031-75013-7\_23.
- [28] R. Silva, R. Costa, L. Gomes, and Z. Vale, "CARAVELS: A Case Study Using Peer-to-Peer Transaction, Voluntary Demand Response, and Energy Storage Optimization," *International Conference on the European Energy Market, EEM*, 2025, doi: 10.1109/EEM64765.2025.11050157.

### **Ethical Issues:**

For this PhD project, ethical question number 4, "Protection of personal data," is a central and critical concern that will be managed proactively through a "privacy by design" approach. Several areas of the project are particularly sensitive, namely: the modeling of user preferences and context which inherently involves personal data (WP4); the use of pre-trained LLMs which may have been trained on private data (WP4, WP5); and the potential use of real-world data to validate the digital twin (WP3).

To mitigate these concerns, the following measures will be strictly enforced. The primary development and testing of the framework will be conducted using synthetic data generated within the Digital Twin, minimizing the need for real user data. In any instance where real data is required for validation in later stages (T6.6), it will only be collected after obtaining explicit and informed consent, and all data will be immediately anonymized or pseudonymized using established techniques. Regarding the selection of pre-trained AI models, it will be ensured that only models with transparent data policies and a clear history of GDPR-compliant training are utilized. Furthermore, all data presented during the dissemination phase, whether in publications or presentations, will be aggregated and fully anonymized to prevent the exposure of any private or sensitive information related to individuals, datasets, or the internal operations of the GECAD institution. These protocols will be formally documented in the Data Management Plan to be developed in WP2.