D2.1: ECOSYSTEM DEFINITION AND REQUIREMENTS

ANNEX 2: INITIAL PLATFORM DESIGN

This annex presents the COP-PILOT architecture across its vertical layers, maps it to key technical work packages WP3 and WP4, and outlines the general platform requirements.

D2.1: Ecosystem definition and requirements

Work package	WP Number 2
Task	Task Number T2.1, T2.2, T2.3
Due date	14/05/2026
Submission date	12/05/2026
Deliverable lead	RedZinc
Version	1.1
Authors	NETCOMPANY-INTRASOFT SA (INTRA) NOVA TELECOMMUNICATIONS & MEDIA SINGLE MEMBER SA (NOVA) ORGANISMOS TILEPIKOINONION TIS ELLADOS OTE AE (OTE) TATA COMMUNICATIONS (UK) LTD (TATA) GIOUMPITEK MELETI SCHEDIASMOS YLOPOIISI KAI POLISI ERGON PLIROFORIKIS ETAIREIA PERIORISMENIS EFTHYNIS (UBI) ONE SOURCE CONSULTORIA INFORMATICA LDA (ONE) SUITE5 DATA INTELLIGENCE SOLUTIONS LIMITED (SUITE5) AGENTSCAPE AG (AGE) AXON LOGIC IDIOTIKI KEFALAIOUXIKI ETAIREIA (AXON) KONNEKT ABLE TECHNOLOGIES LIMITED (KON) INCITES CONSULTING SA (INC) ARTHUR'S LEGAL BV (ARTHUR) EREVNITIKO PANEPISTIMIAKO INSTITOUTO SYSTIMATON EPIKOINONION KAI YPOLOGISTON (ICCS) UNIVERSITY OF BRADFORD (UBRAD) INSTITUTO PEDRO NUNES ASSOCIACAO PARA A INOVACAO E DESENVOLVIMENTO EM CIENCIA E TECNOLOGIA (IPN) FIWARE FOUNDATION EV (FIWARE) DIGITAL FOR PLANET-D4P (D4P) LULEA UNIVERSITY OF TECHNOLOGY (LTU) RISE RESEARCH INSTITUTES OF SWEDEN AB (RISE) HOSCH FÖRDERTECHNIK RECKLINGHAUSEN GmbH (HOSCH) THINGWAVE AB (TAB) PREDGE AB (PAB) ROCKSIGMA (ROC) LTU BUSINESS AB (LTUB) UNIVERSITAT POLITECNICA DE VALENCIA (UPV) FUNDACION DE LA COMUNIDAD VALENCIANA PARA LA INVESTIGACION, PROMOCION Y ESTUDIOS COMERCIALES DE VALENCIAPORT (VPF) TELEFONICA INNOVACION DIGITAL SL (TID) NESPRA (NES) 5G COMMUNICATIONS FOR FUTURE INDUSTRY VERTICALS SL (FIVE) FUNDACION DE LA COMUNITAT VALENCIANA PARA LA PROMOCION ESTRATEGICA EL DESARROLLO Y LA INNOVACION URBANA (VCH) AYUNTAMIENTO DE ALMUSSAFES (ALM) PANEPISTIMIO PATRON (UoP) AGRICULTURAL UNIVERSITY OF ATHENS (AUA) UNIVERSITA DI ROMA "TOR VERGATA" (TOR) DIMOSIA EPICHEIRISI ILEKTRISMOU ANONYMI ETAIREIA (DEI) MPARMPA STATHIS ANONYMI VIOMICHANIKIKAI EMPORIKI ETAIRIA

	(BAR) BIOGAS PREVEZA ONE PC (BPO) AGRICULTURAL APPLICATIONS IKE (AGA) P-NET NEW GENERATION EMERGING NETWORKS & VERTICALS PRIVATE COMPANY (PNET) ILINK NEES TEXNOLOGIES OE (ILINK) ENAKRONIK- KATANEMIMENES LYSEIS TECHNITIS EFFYIAS P.C. (ENIC) REDZINC SERVICES Ltd (RZ) J.I.G. INTERNET CONSULTING SL (JIG) TERRAVIEW GMBH (TER)
Reviewers	NETCOMPANY-INTRASOFT SA (INTRA) GIOUMPITEK MELETI SCHEDIASMOS YLOPOIISI KAI POLISI ERGON PLIROFORIKIS ETAIREIA PERIORISMENIS EFTHYNIS (UBI) NOVA TELECOMMUNICATIONS & MEDIA SINGLE MEMBER SA (NOVA) ORGANISMOS TILEPIKOINONION TIS ELLADOS OTE AE (OTE)
Abstract	The COP-PILOT platform is an open collaborative system for managing services across IoT, edge and core computing environments. COP-PILOT is built to enable secure and intelligent operations that connect diverse sectors. This document brings together an ecosystem of technical blueprints and services models across 5 main domains to support the development of these infrastructures. With a focus on seamless cross domain integration, it lays the foundation for private edge deployments and digital ecosystems across Europe. This deliverable sets the direction for building a platform that drives smarter, more secure, and collaborative digital transformations across multiple industries.
Keywords	IoT Interoperability. Edge Computing. 5G Connectivity, System Intelligence, Automation, Private Edge Systems, Large Scale. Mining, Ports and Logistics, Energy, Agriculture, Viticulture,

Document Revision History

Version	Date	Description of change	List of contributors(s)
V0.1a	3.7.2025	Table of Contents	Donal Morris, RedZinc
V0.1b	4.7.2025	Table of Contents PMT Review	PMT
V0.1c	10.7.2025	Table of Contents WP2 Review	WP2
V0.2	24.9.2025	Working Draft	WP2
V0.3	15.10.2025	Working Draft	WP2
V0.4	15.10.2025	Working Draft	WP2
V0.5	20.10.2025	Working Draft	WP2
V0.6	15.10.2025	Working Draft	WP2
V0.7	24.10.2025	Review Document	WP2
V0.8	25.10.2025	Quality Control Document	WP2
V0.9	25.10.2025	Quality Control Document	RedZinc Team
V1.0	31.10.2025	Final Version for Submission	RedZinc Team NetCompany
V1.0	22.1.2025	Final Version for Submission with info graphics	RedZinc Team NetCompany
V1.0	12.05.2026	Sections made into a separate annexes	RedZinc Team NetCompany

Grant Agreement No: 101189819 | **Topic:** HORIZON-CL4-2024-DATA-01-03
Call: HORIZON-CL4-2024-DATA-01 | **Type of action:** HORIZON-IA

DISCLAIMER

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Co-funded by the European Union (COP-PILOT, 101189819). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

COPYRIGHT NOTICE

Project Co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page)	X
SEN	Sensitive, limited under the conditions of the Grant Agreement	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* R: Document, report (excluding the periodic and final reports)

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

DATA: Data sets, microdata, etc.

DMP: Data management plan

ETHICS: Deliverables related to ethics issues.

SECURITY: Deliverables related to security issues

OTHER: Software, technical diagram, algorithms, models, etc.

INITIAL PLATFORM DESIGN

This chapter outlines the initial version of the COP-PILOT architecture - split across several vertical layers – as described in Section 1.1. Section 1.2 maps this initial version of the architecture with key technical work packages (i.e., WP3 and WP4) and tasks, while a list of general platform requirements is provided in Section 1.3.

DETAILED ARCHITECTURE DESCRIPTION

Figure 2.1 introduces the initial version of the COP-PILOT architecture. This figure takes the simplified version of the architecture introduced in Figure 2.2 of the main D2.1 document to the next level, introducing additional details in every layer of the architecture as described in the rest of this section.

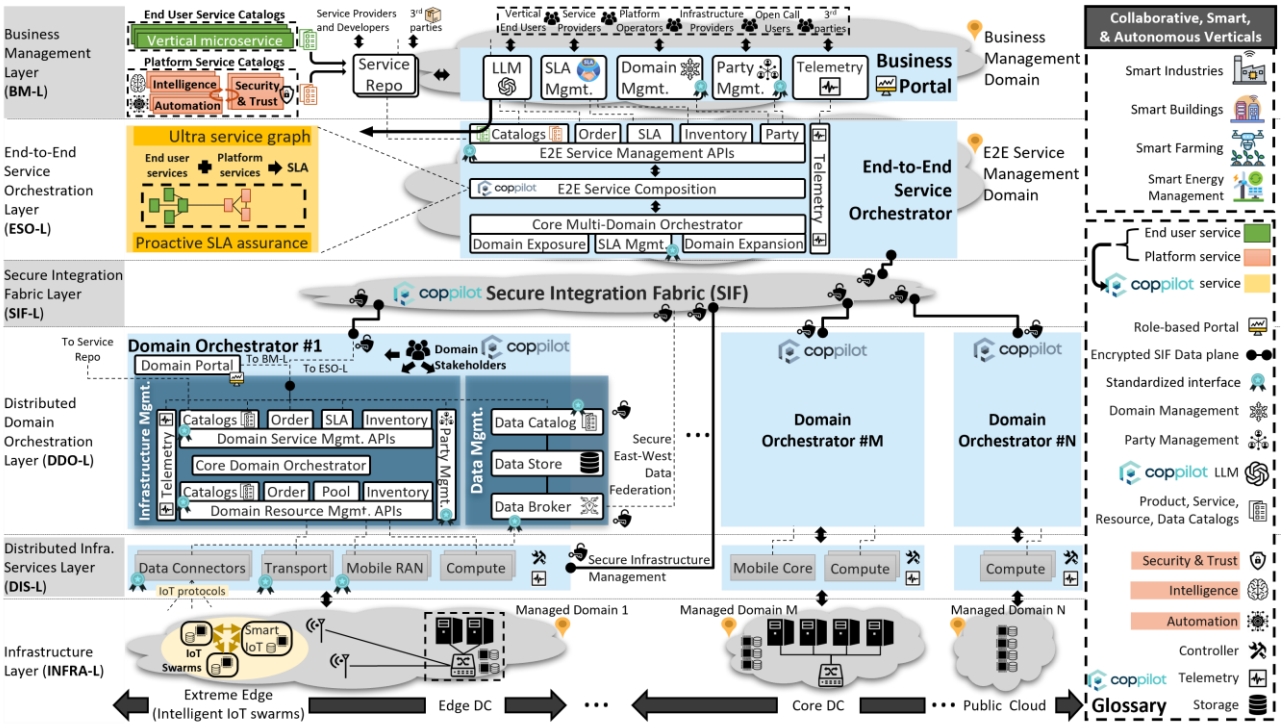

Figure 2.1: Initial COP-PILOT architecture.

Infrastructure Layer (INFRA-L)

Today's infrastructures exhibit a great amount of heterogeneity due to the rapid expansion of the network towards the end users, where user equipment (UE) is surrounded by a plethora of individual or collaborative processing-capable IoT devices, programmable network elements, commodity off-the-shelf (CotS), and specialized edge devices. This largely heterogeneous device manifests itself across multiple domains of different scales ranging from extreme edge domains of intelligent IoT swarms to private edge domains, core network domains and datacenters, as well as hyperscaler-level public cloud domains as shown at the bottom part in Figure 2.1. This is the physical or "Infrastructure layer" – also abbreviated as INFRA-L - on top of which the COP-PILOT architecture must develop and provide solutions.

COP-PILOT Distributed Infrastructure Services Layer (DIS-L)

The distributed infrastructure landscape outlined in INFRA-L creates the need for developing industrial-grade infrastructure services which directly interact with the underlying hardware through a multitude of protocols, while providing unified northbound management knobs for taming the southbound complexity. The global IT community has been striving for decades to build open-source platforms that undertake this challenging role of dealing with so much hardware heterogeneity, producing outstanding projects that provide industrial-grade solutions for compute, network, and data management. The technologies around these services will be studied and analyzed in the context of WP3, however, from an architectural perspective, COP-PILOT looks at these services as a distinct layer atop INFRA-L, titled “Distributed Infrastructure Layer” and abbreviated as DIS-L (see Figure 2.1). This layer is highly distributed, as does the underlying INFRA-L, while the owners of the infrastructure may mix and match legacy vs. advanced and open vs. proprietary technologies of their choice to manage the underlying infrastructure. Nevertheless, COP-PILOT shall provide a solid overlay platform for dealing with the plethora of northbound interfaces of the DIS-L, as explained next.

COP-PILOT Distributed Domain Orchestration Layer (DDO-L)

To facilitate business within every large or small administrative domain, while ensuring maximum security and independence, COP-PILOT fosters a low-tier orchestration layer for managing every single resource and service within a domain. Because the COP-PILOT ecosystem comprises on multiple domains, this layer is also distributed (like INFRA-L and DIS-L), titled “Distributed Domain Orchestration Layer” and abbreviated as DDO-L (see Figure 2.1). The role of this layer is to interact with the northbound APIs for the underlying infrastructure services and expose the resources that these services manage as-a-service. To do so, the industry has been attempting to standardize resource and service orchestration for decades, designing and evolving APIs for (i) describing a resource and/or service using resource/service specifications, (ii) classifying resource and/or service specifications across relevant categories, and (iii) organizing these categories in resource and/or service catalogues, effectively creating the notion of a resource/service marketplace. Additional APIs are also designed for ordering resources and services from the marketplace, towards a specific infrastructure and managing the instantiated resources/services (the so-called resource/service inventory) once being successfully provisioned as a result of an order. COP-PILOT leverages these well-structured standardization efforts to introduce a Domain Orchestration (DO) platform that implements all these APIs for ultimately offering compute and network resource-as-a-service. Alongside resources and services, the COP-PILOT Domain Orchestration platform offers APIs for encoding the role of domain stakeholders (either individuals or organizations) as parties in the domain ecosystem, while also capturing the state of the domain’s resources via compute and network telemetry. The COP-PILOT Domain Orchestration platform is visualized in Figure 2.1 as a core part of the DDO-L.

Modern infrastructures pose extra requirements for managing data in tandem with compute and network resources and services, especially since the emergence of Internet of Things (IoT). For this reason, COP-PILOT caters for a dedicated Data Management platform withing DDO-L (aside to the DO) for serving the complementary purpose of offering Data-as-a-Service. This platform interacts with Data Connectors from the underlying DIS-L, brings their data in, and provides essential services, such as (i) data manipulation and/or pre-processing, (ii) data persistence, (iii) east-west data sharing, and (iv) data cataloguing/exposure towards overlay service as shown in Figure 2.1. The COP-PILOT Data Management platform is also abbreviated as “Data Mgmt.” or DM.

A Domain Portal service complements the DO and DM platforms visualizing their key domain-level operations, thus introducing business management within every COP-PILOT domain. More detailed analysis of the business layer follows later in this section.

Note that the DDO-L is designed to be modular. This means that for domains that require only a DO (due to absence of data) or only a DM (due to absence of compute and network resources), the architecture allows us to deploy only the necessary part of the Domain Orchestration stack, thus cover only the true needs of every domain.

COP-PILOT Secure Integration Fabric Layer (SIF-L)

COP-PILOT is a highly distributed system that spans across multiple self-managed domains across Europe; as such, most of the COP-PILOT components, mainly from the DDO-L (domain services, resources, and data) towards the INFRA-L (i.e., hardware), may be deployed within private infrastructures, the owners of which may wish not to expose publicly. To integrate these components with the rest of the system and allow collaborative cross-domain service deployments, there is an imminent requirement to provide secure connectivity fabric among COP-PILOT components. Doing so via a classical VPN is cumbersome as a huge administrative effort is required per IT department to issue VPN accounts, credentials, and configuration files for several external parties, not to mention that this needs to happen across tens of different IT departments by the partners who provide infrastructure and/or services. COP-PILOT revisits the way private networking should be done nowadays by leveraging recent advancements in secure software-defined overlay networking, effectively offering programmable VPN-as-a-Service. This service resides in COP-PILOT's Secure Integration Fabric Layer, also abbreviated as SIF-L, as shown in Figure 2.1.

Using SIF, COP-PILOT sets up a root-of-trust domain where the SIF control plane will be publicly exposed as a cloud-managed service to the entire ecosystem. COP-PILOT parties who wish to enter the COP-PILOT ecosystem will exploit the COP-PILOT portal (provided by the BM-L in Section 0) to register to the platform, authenticate using state-of-the-art OAUTH2 mechanisms, and use the portal's dedicated domain expansion view to register a new domain under the COP-PILOT realm through an authentication token, and consequently declare domain resources and services that the domain owner wishes to expose through the integration fabric. This information will flow from the COP-PILOT portal to the secure integration fabric backend, triggering the creation of dynamic policies that will associate the domain's resources and services with certain parties and party services who are eligible to consume these endpoints. Both the SIF control and data planes are encrypted; thus, no unprotected packet traverses the public internet, creating a secure programmable overlay network dedicated to the COP-PILOT platform. This is aligned with the "Integration Fabric" component of the ETSI ZSM architecture and goes one step further by adding key security and trust features.

COP-PILOT End-to-End Service Orchestration Layer (ESO-L)

Modern services may span across multiple domains of different scales ranging from extreme edge to edge and core domains, thus falling outside of a DO's scope. For this reason, COP-PILOT introduces a high-tier orchestration platform titled "End-to-End Service Orchestrator" (ESO) to manage services across multiple geo-distributed COP-PILOT domains in an end-to-end manner (see the top part in Figure 2.1). The COP-PILOT ESO consumes the standardized service and resource management interfaces exposed by each COP-PILOT DO instance to acquire the state of each domain by means of available/consumed compute and network resource services. At the northbound, the ESO exposes similar standardized TMF APIs to (i) design and onboard multi-domain end user services on a desired catalog, (ii) order a multi-domain service or service bundle (composite service chain) with certain SLA requirements, and (iii) monitor a multi-domain service instance's runtime through a service inventory API and a service telemetry engine. When such an end-to-end service is ordered, the ESO breaks this service down to one or more service order requests (towards one or more DO instances), thus partitioning the service graphs across domains. Each DO instance manages its own partition of the end-to-end service, while ESO ensures secure connectivity between service components either within a domain or across domains. Dynamic service runtime updates are

supported by the COP-PILOT ESO, either through update operations on the service order and inventory APIs or via a policy API which allows us to construct custom rules and apply them in various checkpoints of a service's lifecycle. Finally, the ESO possesses APIs to manage the COP-PILOT SIF in a dynamic way. These APIs allow to (i) attach/detach new SIF instances under the ESO, thus expand the COP-PILOT platform network accordingly, (ii) manage the identities (i.e., stakeholders) within every SIF instance, and (iii) create/delete encrypted tunnels on-the-fly. This allows the ESO to drive the expansion of the platform towards new private domains and automate the process of deploying new COP-PILOT DO instances in these domains, hence transforming new domains to orchestrated platform environments in a glimpse of time.

COP-PILOT Business Management Layer (BM-L)

Today's service and network management platforms not only require powerful abstractions and APIs for managing heterogeneous resources and services, but also means to render these capabilities friendly to the overlay ecosystem of users. These users may range from platform administrators with domain-level expertise on orchestration to end users with zero understanding on how the platform works. Due to this heterogeneity of users and their backgrounds, a business layer atop COP-PILOT's domain-level (DO-L) and end-to-end service management (ESO-L) layers is introduced to complement the rest of the system with high-level tools that render important platform operations simple and intuitive. This layer is titled Business Management Layer – also abbreviated as BM-L – as shown in Figure 2.1. The core of the BM-L is Portal that resides both on top of the COP-PILOT DO and the ESO. At the level of the DO, the portal facilitates domain-level operations that need to be taken by e.g., the domain administrator/owner, domain service providers, and domain infrastructure owners. Such operations could be resource and service management (i.e., ordering, lifecycle management, and termination) within a domain, management of parties within a domain, management of domain-level SLAs, and domain-level visibility tools (i.e., resource and service telemetry). At the level of the ESO, the same set of operations are required for end-to-end services, but also additional views that (i) provide the state of the entire platform, visualizing the hierarchy of orchestrators (ESO and multiple DO instances) across domains and the underlying resources/services in each domain and (ii) allow the platform administrator to easily expand the platform to new domains, embracing more infrastructure owners under the COP-PILOT realm. Finally, the advent of Large Language Models (LLMs) inspired COP-PILOT to leverage the power of AI for the benefit of the COP-PILOT users, offering both a domain-level and end-to-end LLM agent on the COP-PILOT portal. The COP-PILOT LLM facilitates the interaction of end users with the platform by means of (i) guiding the user to the right service catalogs and service categories and (ii) ordering composite service with certain SLA requirements on behalf of the user.

MAPPING OF THE INITIAL COP-PILOT ARCHITECTURE WITH TECHNICAL WORK PACKAGES AND TASKS

To break down the responsibilities for realizing the COP-PILOT architecture, a mapping of this architecture with key technical work packages (i.e., WP3 and WP4) and tasks is necessary. This mapping is visualized in Figure 2.2, which is an annotated version of Figure 2.1.

In short, WP3 is responsible for the core COP-PILOT platform (BM-L, ESO-L, DDO-L, SIF-L highlighted in purple color), while WP4 offers the ecosystem around the platform by means of (i) the underlying infrastructure (i.e., INFRA-L highlighted in green color at the bottom part in Figure 2.2) and infrastructure services (i.e., DIS-L highlighted in gray color in in Figure 2.2) to be managed by the platform and (ii) the overlay vertical sector services, either stemming from the COP-PILOT Clusters or external (e.g., Open Calls or third-parties) to be managed by the platform (see green-highlighted top part in Figure 2.2).

Co-funded by the European Union

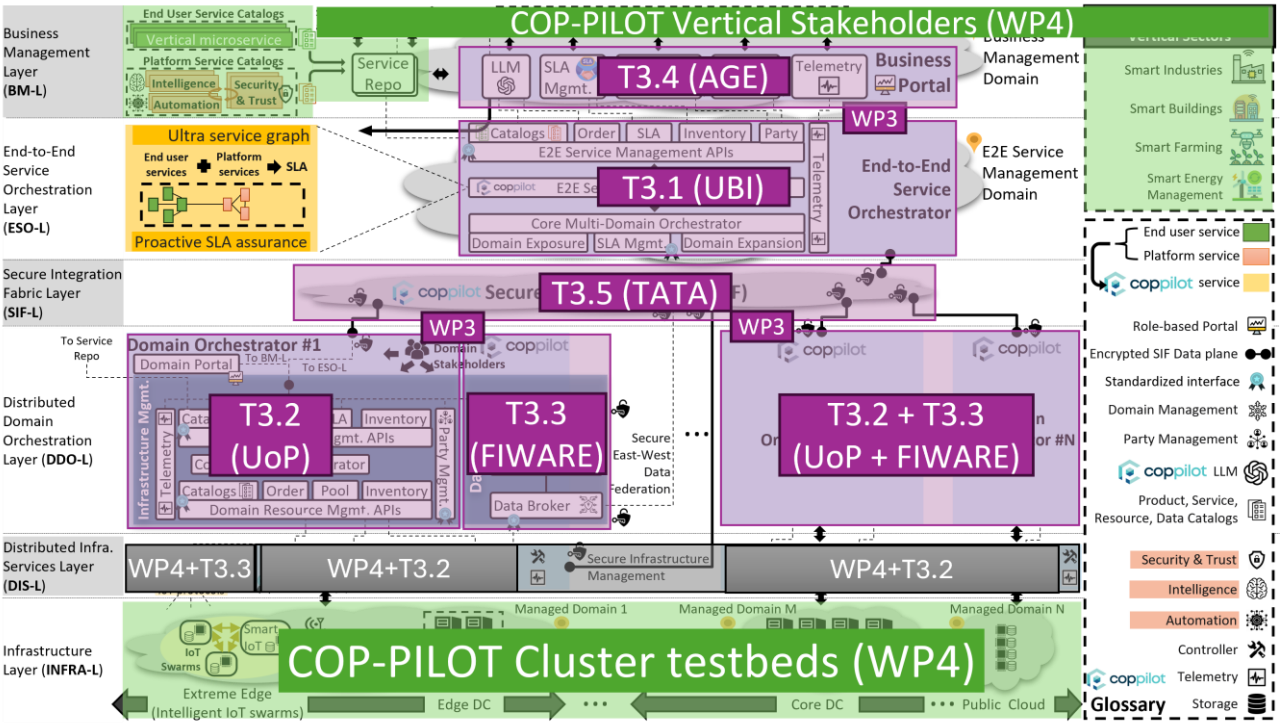

Figure 2.2: Initial COP-PILOT architecture mapped to technical WPs.

Regarding the COP-PILOT platform core, WP3 contributes to the COP-PILOT architecture as follows:

Task 3.1 is responsible for the COP-PILOT ESO-L, offering the end-to-end service orchestrator along with all its capabilities and APIs. This task ensures proper interfacing of the ESO with the DO (T3.2) and SIF (T3.5) platform components for managing the entire COP-PILOT platform and its expansion to new domains.

Task 3.2 undertakes the resource and service management part of the COP-PILOT DDO-L, offering the domain-level orchestrator (i.e., the DO) and the integration of the DO with the underlying compute and network infrastructure services that reside in the DIS-L. This task ensures proper interfacing of edge-to-core compute resources, 5G, and transport network resources with the platform and exposure of these resources as-a-Service towards the ESO.

Task 3.3 undertakes the data management part of the COP-PILOT DDO-L, offering the Data Management platform (i.e., the DM) and the integration of the DM with the underlying Data Connector infrastructure services that reside in the DIS-L. This task ensures proper interfacing of all data spaces (e.g., sensors, legacy data sources) with the platform and exposure of Data catalogs and services towards the COP-PILOT applications.

Task 3.4 undertakes the development of the COP-PILOT portal, both atop the ESO and DO. Important portal views that pertain to this task are (i) resource catalogs/ordering/inventory management, (ii) resource catalogs/ordering/inventory management, (iii) SLA management, (iv) Platform visualization and domain expansion, and (v) LLM assistants to facilitate service ordering. This task ensures integration with both the ESO and DO APIs.

Task 3.5 is responsible for the entire COP-PILOT SIF-L, effectively developing the core part of the SIF and a highly distributed set of SIF clients across all COP-PILOT clusters and Open Call activities to create a secure ecosystem for collaborating COP-PILOT domains and services that belong to multiple stakeholders.

Regarding the surroundings of the COP-PILOT platform, WP4 contributes as follows:

Task 4.1 is responsible for ensuring the integration of the COP-PILOT architecture with the infrastructure (INFRA-L) and infrastructure services (DIS-L) that correspond to the COP-PILOT clusters.

Task 4.3 is responsible for ensuring the integration of the COP-PILOT use case applications with the COP-PILOT platform via the NBIs offers by the ESO, DO, and DM components as well as the business management portal (BMP).

Task 4.4 is responsible for ensuring the integration of the COP-PILOT architecture with the infrastructure (INFRA-L) and infrastructure services (DIS-L) that correspond to the COP-PILOT Open Call projects.

GENERAL PLATFORM REQUIREMENTS

The objective of this section is to provide COP-PILOT's general platform requirements. These requirements are listed in Figure 2.1.

Table 2.1: Functional generic platform requirements.

Requirement ID	Requirement Analysis
FNR.GP.01	Description: The COP-PILOT platform **MUST** provide open, standardized APIs to ensure interoperability.

	Affected Components: ALL
	Contributing Partners: All platform component providers
	Comment: Ensure that the platform uses well-accepted (by the industry) APIs to facilitate integration and interoperability across different components and domains.
FNR.GP.02	Description: The COP-PILOT platform **MUST** ensure orchestration of services and resources across multiple - potentially heterogeneous - administrative domains
	Affected Components: ESO, DO, SIF
	Contributing Partners: UBI, UOP, ONE, TATA
	Comment: Ensures that the platform can manage services of different vertical sectors, across multiple domains, and different types of infrastructures.
FNR.GP.03	Description: The COP-PILOT platform **MUST** provide APIs to interconnect services across private domains in a secure and trusted manner.
	Affected Components: SIF
	Contributing Partners: TATA
	Comment: Ensures that the platform has secure mechanisms for connecting private components, services, and/or domains in a programmatic manner (i.e., no need for offline VPN tunnelling)
FNR.GP.04	Description: The COP-PILOT platform **MUST** enable secure expansion to new (private or public) domains with minimal human intervention.
	Affected Components: BP, ESO, DO, Data Mgmt.
	Contributing Partners: AGE, UBI, ONE, UOP, FIWARE, LTU
	Comment: Ensures that the platform possesses east-west APIs that allow the orchestration and data management components to expand to new (private or public) domains and resources in a highly automated manner.
FNR.GP.05	Description: The COP-PILOT platform **MUST** provide standardized APIs for SLA management.
	Affected Components: BP, ESO, DO, Data Mgmt.
	Contributing Partners: ONE, AGE, UBI, UOP
	Comment: Ensures that SLAs will be defined and managed in a way relevant for real systems.
FNR.GP.06	Description: The COP-PILOT platform **MUST** integrate with existing, popular infrastructure controllers for resource management.
	Affected Components: DO, Data Mgmt.
	Contributing Partners: UOP, FIWARE, LTU

	Comment: Ensures that the platform can work with existing infrastructure controllers (compute, network, data) to manage resources efficiently.
FNR.GP.07	Description: The COP-PILOT platform **MUST** support federated and secure data management across the continuum.
	Affected Components: Data Mgmt., SIF
	Contributing Partners: FIWARE, LTU, TATA
	Comment: Ensures that the platform can manage data across the IoT-edge-core continuum in a secure manner.
FNR.GP.08	Description: The COP-PILOT platform **MUST** expose Northbound APIs to external stakeholders or overlay systems
	Affected Components: ESO, DO, Data Mgmt.
	Contributing Partners: UBI, UoP, ONE, FIWARE, LTU
	Comment: Ensures interoperability with other platforms, such
FNR.GP.09	Description: The COP-PILOT platform **MUST** visualize key NBIs to every type of stakeholder through a modern Portal
	Affected Components: BP
	Contributing Partners: AGE and rest of T3.4 partners
	Comment: -
FNR.GP.10	Description: The COP-PILOT platform **MUST** be able to facilitate critical operations, such as secure domain registration, secure domain onboarding, service design, service onboarding, service ordering, service real-time management, SLA definition, SLA assurance, data cataloguing, data exposure via the Portal
	Affected Components: BP
	Contributing Partners: AGE and rest of T3.4 partners
	Comment: -
FNR.GP.11	Description: The COP-PILOT platform **MUST** be easily extensible with new NBIs to support future evolution of existing standardized APIs or the introduction of new ones.
	Affected Components: BP, ESO, DO, Data Mgmt., SIF
	Contributing Partners: BP, ESO, DO, Data Mgmt., SIF
	Comment: Ensures viability of the platform is beyond COP-PILOT.