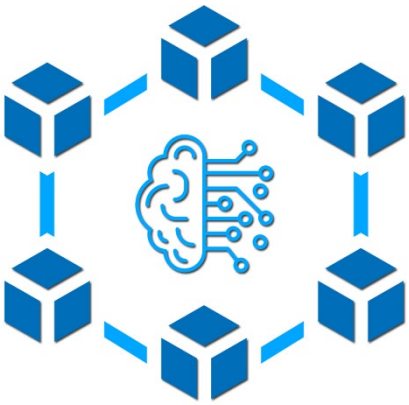

NANCY

An Artificial Intelligent Aided Unified Network for Secure Beyond 5G Long Term Evolution [GA: 101096456]

Deliverable 6.1

B-RAN and 5G End-to-end Facilities Setup

Programme: HORIZON-JU-SNS-2022-STREAM-A-01-06

Start Date: 01 January 2023

Duration: 36 Months

Co-funded by the European Union

6GSNS

NANCY project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101096456.

Document Control Page

Deliverable Name	B-RAN and 5G End-to-end Facilities Setup
Deliverable Number	D6.1
Work Package	WP6 NANCY System Integration, Validation & Demonstration
Associated Task	Task 6.1 Integration plan and facilities
Dissemination Level	Public
Due Date	31 August 2024
Completion Date	28 August 2024
Submission Date	31 August 2024
Deliverable Lead Partner	UBITECH
Deliverable Author(s)	Georgios P. Katsikas (UBITECH), Dimitris Manolopoulos (UBITECH), Dimitris Klonidis (UBITECH), Antonella Clavenna (ITL), Marco Beccari (ITL), Abir Yasser Barakat (TEI), Giancarlo Sacco (TEI), Giuseppe Celozzi (TEI), Marco Tambasco (TEI), Antonio Skarmeta (UMU), Ramon Sanchez Iborra (UMU), Jorge Sasiain (EHU), Eduardo Jacob (EHU), Panos Matzakos (INTRA), Mauro Marinoni (SSS), Daniel Casini (SSS), Alessandro Biondi (SSS), Dimitrios Pliatsios (UOWM), Athanasios Liatifis (UOWM), Panagiotis Sarigiannidis (UOWM), Thomas Lagkas (UOWM), Sotirios Tegos (UOWM), Konstantinos Kyranou (SID), Charalampos Eleftheriadis (SID), Christina Lessi (OTE), Maria Belesioti (OTE), Jean-Paul Truong (TDIS)
Version	1.0

Document History

Version	Date	Change History	Author(s)	Organisation
0.1	17 May 2024	Initial version	Georgios P. Katsikas, Dimitris Manolopoulos	UBITECH
0.2	10 July 2024	Section 2	Georgios P. Katsikas, Dimitris Manolopoulos	UBITECH
0.3	12 July 2024	Final ToC and clear assignment of partners to sections	Georgios P. Katsikas, Dimitris Manolopoulos	UBITECH
0.3	23 July 2024	Contribution to sections 3.3.1 and 5.2.2	Antonella Clavenna	ITL
0.4	26 July 2024	First round of contributions to Section 2, 3, 4, and 5	Abir Yasser Barakat,, Giancarlo Sacco, Giuseppe Celozzi, Marco Tambasco / Antonio Skarmeta, Ramon Sanchez Iborra / Jorge Sasiain, Eduardo Jacob / Panos Matzakos / Mauro Marinoni, Daniel Casini, Alessandro Biondi	TEI/ UMU/ EHU/ INTRA/ SSS
0.5	26 July 2024	Contribution to sections 3.2.1 and 5.2.1	Dimitrios Pliatsios, Athanasios Liatifis,	UOWM/ SID

			Panagiotis Sarigiannidis, Thomas Lagkas, Sotirios Tegos / Konstantinos Kyranou, Charalampos Eleftheriadis	
0.6	30 July 2024	Contribution to sections 3.2.2 and 5.2.1	Christina Lessi, Maria Belesioti	OTE
0.7	01 August 2024	Remaining missing information provided	Antonella Clavenna, Marco Beccari	ITL
0.8	09 August 2024	Final editing before internal review	Georgios P. Katsikas	UBITECH
0.9	20 August 2024	Review comments	Jean-Paul Truong/ Daniel Casini	TDIS/ SSS
1.0	29 August 2024	Quality Revisions	Anna Triantafyllou, Dimitrios Pliatsios	UOWM

Internal Review History

Name	Organisation	Date
Jean-Paul Truong	TDIS	20 August 2024
Daniel Casini	SSS	20 August 2024

Quality Manager Revision

Name	Organisation	Date
Anna Triantafyllou, Dimitrios Pliatsios	UOWM	29 August 2024

Table of Contents

Table of Contents 4
List of Figures 6
List of Tables 7
List of Acronyms 9
Executive Summary 10
1. Introduction 11
1.1. Purpose of the Document 11
1.2. Relation to other Tasks and Deliverables 12
1.3. Structure of the Deliverable 12
2. Deployment of the NANCY Reference Architecture 13
2.1. Functional and Deployment View of the NANCY Architecture 13
2.1.1. NANCY Infrastructure Layer 14
2.1.2. NANCY Controllers' Layer 14
2.1.3. NANCY Orchestration Layer 15
2.1.4. NANCY Business Layer 16
3. NANCY Testbeds 18
3.1. Terminology 18
3.2. Greek Testbeds 18
3.2.1. Greek In-lab Testbed 18
3.2.2. Greek Demonstrator Testbed 20
3.3. Italian Testbeds 23
3.3.1. Italian In-lab Testbed 23
3.3.2. Italian Demonstrator Testbed 24
3.4. Spanish Testbeds 26
3.4.1. Spanish Demonstrator Testbed 26
3.4.2. Spanish Demonstrator Extension 28
4. Integration 32
4.1. Terminology and Definitions 32
4.2. NANCY Platform Interfaces 32
4.2.1. NANCY Interfaces' Description 33
5. NANCY Platform Instantiation atop the NANCY Testbeds 36
5.1. Central NANCY Platform 36
5.2. Distributed NANCY Components 36
5.2.1. Greek Testbed Software Components 36

5.2.2. Italian Testbed Software Components 39
5.2.3. Spanish Testbed Software Components 42
5.3. NANCY CI/CD Platform 45
5.3.1. CI/CD hosting environment and Services 45
5.3.2. Continuous Integration 46
5.3.3. Continuous Delivery 47
6. Conclusion 48
6.1. Key Achievements 48
6.2. Future Directions 48
6.3. Final Remarks 48
Bibliography 49

List of Figures

Figure 1-1: Visualization of relationships among T6.1 and other key NANCY tasks and deliverables. . 12
Figure 2-1: Functional and deployment view of the NANCY architecture. 13
Figure 3-1: Overview of the Greek in-lab testbed. 19
Figure 3-2: Overview of the Greek demonstrator testbed. 21
Figure 3-3: Overview of the Italian in-lab testbed. 23
Figure 3-4: Overview of the Italian demonstrator testbed. 25
Figure 3-5: Overview of the Spanish demonstrator testbed (EHU premises). 27
Figure 3-6: Overview of the Spanish demonstrator extension (UMU premises). 29
Figure 4-1: Functional and deployment view of the NANCY architecture (Figure 2-1) annotated with interface IDs. 32
Figure 5-1: Reference CI pipeline. 47
Figure 5-2: Reference CD pipeline with Service Orchestration. 47

List of Tables

Table 3-1: Greek in-lab testbed - UE and IoT device components. 19
Table 3-2: Greek in-lab testbed - RAN hardware components. 19
Table 3-3: Greek in-lab testbed – Commodity or specialized servers. 20
Table 3-4: Greek demonstrator testbed - UE and IoT device components 21
Table 3-5: Greek demonstrator testbed - RAN hardware components. 22
Table 3-6: Greek demonstrator testbed - (Programmable) networking hardware components. 22
Table 3-7: Greek demonstrator testbed – Commodity or specialized servers. 22
Table 3-8: Italian in-lab testbed - UE and IoT device components. 23
Table 3-9: Italian in-lab testbed - RAN hardware components. 24
Table 3-10: Italian in-lab testbed – Commodity or specialized servers. 24
Table 3-11: Italian demonstrator testbed - UE and IoT device components. 25
Table 3-12: Italian demonstrator testbed - RAN hardware components. 25
Table 3-13: Italian demonstrator testbed - networking hardware components. 26
Table 3-14: Italian demonstrator testbed – Commodity or specialized servers. 26
Table 3-15: Spanish demonstrator testbed - UE and IoT device components. 27
Table 3-16: Spanish demonstrator testbed - RAN hardware components. 27
Table 3-17: Spanish demonstrator testbed – Commodity or specialized servers 28
Table 3-18: Spanish demonstrator extension testbed - UE and IoT device components. 29
Table 3-19: Spanish demonstrator extension testbed - (IoT) gateway components. 30
Table 3-20: Spanish demonstrator extension testbed - RAN hardware components. 30
Table 3-21: Spanish demonstrator extension testbed - (Programmable) networking hardware components 30
Table 3-22: Spanish demonstrator extension testbed – Commodity or specialized servers. 30
Table 4-1: NANCY interfaces and the related NANCY architecture components. 33
Table 5-1: List of components deployed on the NANCY Central domain. 36
Table 5-2: List of orchestration components supported by the Greek In-lab testbed. 36
Table 5-3: List of controllers supported by the Greek In-lab testbed. 37
Table 5-4: List of telemetry services supported by the Greek In-lab testbed. 37
Table 5-5: List of NANCY services provided by the In-lab Greek Testbed. 37
Table 5-6: List of orchestration components supported by the Greek Demonstrator testbed. 37
Table 5-7: List of controllers supported by the Greek Demonstrator testbed. 38
Table 5-8: List of telemetry services supported by the Greek Demonstrator testbed. 38
Table 5-9: List of NANCY services provided by the Greek Demonstrator testbed. 38
Table 5-10: List of controllers supported by the Italian In-lab testbed 39
Table 5-11: List of telemetry services supported by the Italian In-lab testbed. 39
Table 5-12: List of NANCY services provided by the Italian In-lab testbed. 40
Table 5-13: List of controllers supported by the Italian Demonstrator testbed. 41
Table 5-14: List of telemetry services supported by the Italian Demonstrator testbed. 41
Table 5-15: List of NANCY services provided by the Italian Demonstrator testbed. 41
Table 5-16: List of orchestration components supported by the Spanish Demonstrator testbed. 42
Table 5-17: List of controllers supported by the Spanish Demonstrator testbed. 42
Table 5-18: List of telemetry services supported by the Spanish Demonstrator testbed. 42
Table 5-19: List of NANCY services provided by the Spanish Demonstrator testbed. 43
Table 5-20: List of orchestration components supported by the Spanish Demonstrator extension testbed. 43
Table 5-21: List of controllers supported by the Spanish Demonstrator extension testbed. 43

Table 5-22: List of telemetry services supported by the Spanish Demonstrator extension testbed.... 44
Table 5-23: List of NANCY services provided by the Spanish Demonstrator extension testbed. 44

List of Acronyms

Acronym	Explanation
5G	Fifth Generation
5GC	5G Core
AI	Artificial Intelligence
BC	Blockchain
BSS	Business Support System
CD	Continuous Delivery
CI	Continuous Integration
COTS	Commercial Off-The-Shelf
eNB	4G eNodeB
gNB	5G gNodeB
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure-as-a-Service
IoT	Internet of Things
Near-RT RIC	Near-Real-Time RAN Intelligent Controller
NFVO	Network Functions Virtualization Orchestrator
NI	NANCY Interface
NIS	NANCY Interface Set
Non-RT RIC	Non-Real-Time RAN Intelligent Controller
NSA	Non-Standalone
OBU	On-Board Unit
OCI	Open Container Initiative
O-CU	O-RAN Central Unit
O-CU-CP	O-RAN Central Unit Control Plane
O-CU-UP	O-RAN Central Unit User Plane
O-DU	O-RAN Distributed Unit
O-RAN	Open Radio Access Network
O-RU	O-RAN Radio Unit
OSS	Operations Support System
PaaS	Platform-as-a-Service
RAN	Radio Access Network
rApp	O-RAN Non-RT RIC Application
RIC	RAN Intelligent Controller
RO	Resource Orchestrator
RRH	Remote Radio Head
SA	Standalone
SDN	Software-Defined Networking
SMO	Service Management and Orchestration
SO	Service Orchestrator
SSH	Secure Shell
TN	Transport Network
UE	User Equipment
xApp	O-RAN Near-RT RIC eXtended Application

Executive Summary

This document, D6.1 “B-RAN and 5G End-to-end Facilities Setup", is part of the NANCY project, which focuses on establishing a comprehensive infrastructure for Beyond 5G networks. It details the setup and integration of NANCY's Reference Architecture and its deployment across various testbeds in Greece, Italy, and Spain.

Objectives

The main goals of this deliverable are to:

1. Outline the deployment view of the NANCY architecture.
2. Annotate the architecture with the interfaces among all components and the testbeds.
3. Identify the tasks and work packages responsible for each component and interface.
4. Assign blocks and interfaces to partners to streamline the integration effort.
5. Provide a detailed deployment plan for the NANCY platform across the three main testbeds.

NANCY Reference Architecture

The NANCY Reference Architecture is divided into four layers:

1. **Infrastructure Layer**: Provides the foundational hardware and software environment.
2. **Controllers’ Layer**: Manages the various network functions and services.
3. **Orchestration Layer**: Coordinates the deployment and management of network services.
4. **Business Layer**: Facilitates business logic and service delivery.

Testbeds

Three testbeds are described for the deployment and validation of the NANCY platform:

1. **Greek Testbeds**:
    - In-lab Testbed
    - Demonstrator Testbed (OTE)
2. **Italian Testbeds**:
    - In-lab Testbed
    - Demonstrator Testbed
3. **Spanish Testbeds**:
    - Demonstrator Testbed
    - Demonstrator Extension

Each testbed is equipped with specific software and hardware components necessary for the NANCY platform's operation.

Integration and Deployment

The document outlines how NANCY components will be integrated, focusing on secure communications, continuous integration (CI), and continuous delivery (CD). Key elements include:

- **Security**: HTTPS, VPNs, firewall protection, and SSH key-based authentication.
- **CI/CD**: Automated testing and deployment pipelines to ensure stability and readiness for deployment.

This early version of the NANCY integrated system aims to provide a clear vision and establish a foundation for subsequent updates and refinements in future deliverables.

1. Introduction

1.1. Purpose of the Document

The objective of this document is to describe the B-RAN and 5G end-to-end facilities of NANCY to establish a solid infrastructure plane for the NANCY platform. This work is mainly done in Section 3. However, WP6 is also in charge of defining how the NANCY platform components will be integrated among each other as well as how the NANCY platform as-a-whole will integrate with the three (3) NANCY testbeds to enable the validation activities of the various use cases. This effort is mainly planned for M25 and beyond in the context of D6.2 "NANCY Integrated System – Initial Version". However, WP6 believes that it is crucial to conduct this work earlier than M25, to obtain a clear view on the required efforts towards setting up the NANCY testbeds and the NANCY platform on top of these testbeds.

This document also establishes an early – yet complete - version of the integrated NANCY system to appear in D6.2 "NANCY Integrated System – Initial Version" in M25. Specifically, Section 2 introduces the deployment view of the NANCY architecture as this was introduced in D3.1 "NANCY Architecture Design", Section 4 annotates this architecture with interfaces among all components and the testbeds, while Section 5 outlines how NANCY envisions to deploy the platform as-a-whole atop the three testbeds.

This is clearly effort for an early version of D6.2 "NANCY Integrated System – Initial Version", which is presented in D6.1 "B-RAN and 5G End-to-end Facilities Setup". For this reason, the effort that the NANCY consortium will put into D6.2 "NANCY Integrated System – Initial Version" will be incremental to the material presented in this deliverable.

In summary, D6.1 "B-RAN and 5G End-to-end Facilities Setup" puts an effort to:

- Devise a clear deployment view of the NANCY architecture, as this was presented in D3.1 "NANCY Architecture Design".
- Annotate this deployment view with interface names among all the blocks.
- Identify the Work Packages (WPs) and Tasks responsible for each block and interface.
- Assign blocks and interfaces to partners to clarify how the integration effort will be distributed across the important actors of the platform.
- Provide a project-wide deployment plan of the NANCY platform across the three NANCY testbeds.

1.2. Relation to other Tasks and Deliverables

Figure 1-1 visualizes the relationships among T6.1 and this deliverable (D6.1) with important NANCY tasks and deliverables in WP2, WP3, and WP6.

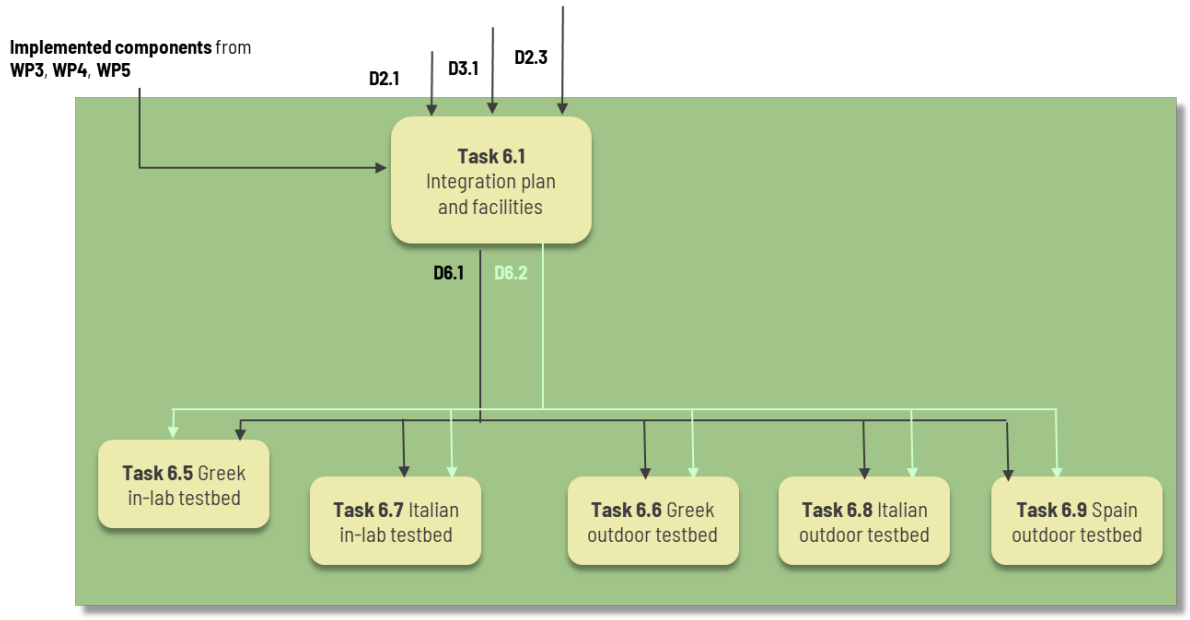

Figure 1-1: Visualization of relationships among T6.1 and other key NANCY tasks and deliverables.

1.3. Structure of the Deliverable

This document is organised into sections that address different aspects of the project. Here, a brief overview of these sections is presented:

- **Section 2 – Deployment of the NANCY Reference Architecture** defines a deployment view of the NANCY architecture as this was initially defined in D3.1 “NANCY Architecture Design”.
- **Section 3 – NANCY Testbeds** describes the three NANCY testbeds to identify crucial details that will guide the integration.
- **Section 4 – Integration** introduces details about the integration of the various logical components of the NANCY architecture. This section lays the ground for an early integration before D6.2 “NANCY Integrated System – Initial Version”.
- **Section 5 - NANCY Platform Instantiation atop the NANCY Testbeds** introduces how the entire platform will be deployed across the three testbeds.
- **Section 6 – Conclusion** concludes this document.

2. Deployment of the NANCY Reference Architecture

This section defines the functional and *deployment view* of the NANCY architecture as this was initially defined in D3.1 "NANCY Architecture Design", aiming at facilitating the integration by using this deployment view as the de-facto NANCY platform figure throughput the rest of the project. A joint work between WP3 and WP6 is also done to map the deployment view presented in this deliverable with:

- the abstract figure of the NANCY architecture in D3.1 "NANCY Architecture Design"
- the WPs and tasks in charge of designing and implementing the NANCY architecture components, and
- the partners behind each component.

The objective of this section is to deliver a system with clear components (i.e., blocks) and links among these components (i.e., interfaces), so that Section 4 will introduce the details of these interfaces, atop the NANCY testbeds described in Section 3.

2.1. Functional and Deployment View of the NANCY Architecture

Figure 2-1 visualizes the functional and deployment view of the NANCY architecture. This figure provides both a horizontal split of the system across domains (from user equipment at the left-hand side to a core domain at the right-hand side) as well as a vertical split across layers (from the infrastructure layer at the bottom to the business layer at the top). These domains and layers are explained in the rest of this section.

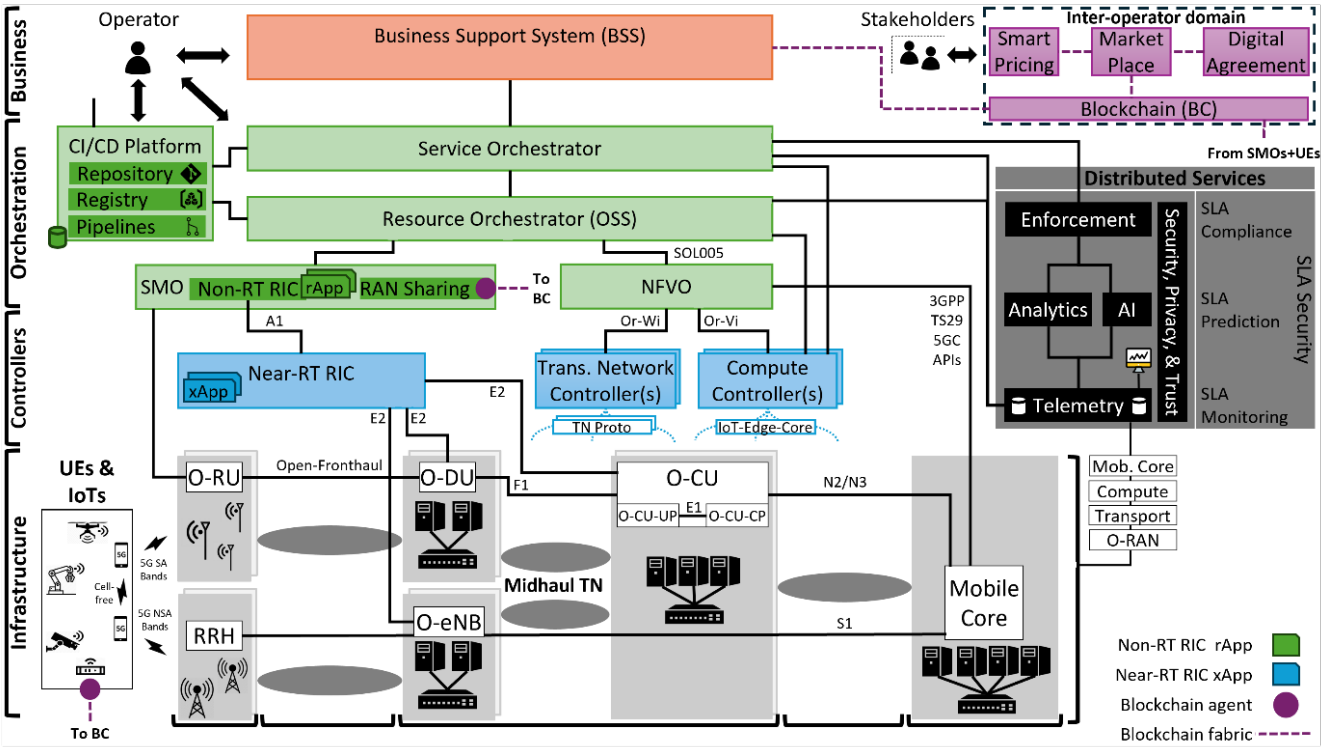

Figure 2-1: Functional and deployment view of the NANCY architecture.

2.1.1. NANCY Infrastructure Layer

NANCY infrastructures comprise geo-distributed and heterogeneous physical appliances that span across multiple interconnected domains as shown in Figure 2-1. We call this infrastructure NANCY's "Infrastructure layer". This layer is split across radio, transport, and core domains introduced next.

NANCY Radio Access Network (RAN): On the left-hand side in Figure 2-1, end user equipment (UE) and Internet of Things (IoT) devices require connectivity to modern services, by means of (i) 5G and beyond connectivity using 5G Standalone (SA) bands, (ii) legacy 4G/4G+ connectivity using 5G Non-Standalone (NSA), or (iii) cell-free connectivity (i.e., using a neighbouring 5G UE as a relay to access 5G resources). NANCY facilitates all these different connectivity schemes via an O-RAN-based RAN that accommodates both 5G SA and NSA connections as shown in Figure 2-1. 5G SA is covered through the synergy among O-RAN Radio Units (O-RUs), Distributed Units (O-DUs), and Central Units (O-CUs), while 5G NSA is covered through legacy O-eNB or legacy gNB (i.e., a gNB that does not implement the O-RAN functional split) deployment connected to Remote Radio Heads (RRHs).

The NANCY RAN spans across the "Access", "Fronthaul Transport Network (TN)", "Edge", and "Midhaul TN" domains shown in Figure 2-1. This is because, according to the O-RAN specifications [3], a fronthaul TN connects the many O-RUs with the corresponding O-DUs, while a midhaul TN provides connectivity among O-DUs and O-CUs. Both O-DUs and O-CUs are typically deployed at the edge.

NANCY Core Domain: To provide end-to-end 5G connectivity, a "Backhaul TN" is responsible for bridging various RANs with the Mobile Core, which typically sits in a "Core Domain" as shown in Figure 2-1. The Mobile Core uses different 3GPP interfaces to associate with either O-RAN-based cells or legacy gNBs/eNBs as shown in Figure 2-1.

NANCY Telemetry Infrastructure Services: To acquire a precise view of the underlying domains, NANCY employs a set of telemetry services for O-RAN, TN, Mobile Core, and Compute domains as shown on the right-hand side in Figure 2-1. Each domain is responsible for its own devices and resources, yet all this telemetry shall be accessible to overlay services that wish to exploit this information for managing services for different NANCY stakeholders.

2.1.2. NANCY Controllers' Layer

Atop the distributed NANCY Infrastructure layer, a set of infrastructure controllers – highlighted in blue colour – manage the underlying resources in every horizontal domain. We classify these controllers in three (3) categories as follows:

(O-)RAN Controller (s): One or more Near Real-Time RAN Intelligent Controllers (Near-RT RIC) for O-RAN domains that manage O-RUs, O-DUs, and O-CUs as virtualized network functions (NFs) using the standardized O-RAN interfaces (e.g., E2, F1, etc.) depicted in Figure 2-1. These controllers also support the management of legacy eNBs and gNBs in case these are available in parts of the NANCY testbeds.

Transport Network Controller(s): One or more TN controllers for managing connectivity services in the fronthaul, midhaul, and backhaul transport network domains. This is done using either legacy or Software-Defined TN protocols.

Compute Controller(s): One or more compute infrastructure controllers for managing either physical or virtual compute resources across the cloud continuum and over the NANCY testbeds. Depending on the type of computing resource (e.g., a physical server, a virtual machine), clusters of nodes can be created either in the form of Infrastructure-as-a-Service (IaaS) using e.g., OpenStack [4] or Platform-as-a-Service (PaaS) using e.g., Kubernetes [5].

NANCY leverages existing state-of-the-art controllers to manage infrastructure resources, focusing mostly on the correct integration of these controllers with the rest of the NANCY platform, mainly towards the orchestration layer that is described next.

2.1.3. NANCY Orchestration Layer

Atop the NANCY Controllers layer, spread across the various NANCY testbeds, a set of orchestration components – highlighted in green colour – provide (i) end-to-end service and resource management within an operator's realm and (ii) continuous integration and delivery of the operator's own or customer services. Figure 2-1 depicts how NANCY envisions a synergy among five (5) orchestration entities within the NANCY "Orchestration" layer. We briefly highlight the role of each entity next.

Service Management and Orchestration (SMO) is a key entity for NANCY as it provides end-to-end management knobs within O-RAN-based or legacy 5G RAN domains. Among other functionalities, this platform provisions a Non-Real-Time RIC which coordinates with the Near-RT RIC in the controllers' layer to manage O-RAN network functions (e.g., O-DUs, O-CUs) for smart radio resource management, power control, etc. NANCY promotes an extended SMO with secure RAN-sharing capabilities through a novel blockchain-based interface towards the inter-operator domain.

Network Functions Virtualization Orchestrator (NFVO) is a crucial platform for managing the rest of the network functions in the transport and core networks. Standardized solutions (e.g., ETSI OSM [6]) are leveraged by NANCY to manage the ensemble of 5G Core Network functions within a cloud-native environment with full control and programmability of the mobile core elements, while the NFVO can also manage connectivity services between the 5GC and the various radio segments.

Resource Orchestrator (RO) stands as the manager of an operator's resources in an end-to-end fashion across radio, transport, and core domains as per 3GPP [7]. Such a system is typically titled Operations Support System (OSS) in the telco terminology. The role of an OSS is to establish bindings with every part of the infrastructure through integration with the SMO, NFVO, and various controllers (e.g., compute) and expose an operator's resources as a service. This functionality is important as it hides the resources behind service APIs, thus forcing overlay systems (e.g., a service orchestrator) to have direct access to critical resource blocks. In other words, an OSS is responsible for establishing end-to-end slices (i.e., a radio slice connected with a transport network slice, which is in turn connected with a core network slice and a compute slice for an application), while offering these slices through APIs.

Service Orchestrator (SO) is the overarching entity in the NANCY Orchestration layer. The SO consumes resource-as-a-service APIs from the RO to provide end-to-end slices to the operator's customers while undertaking the provisioning and runtime management of these services atop the allocated slices. This is done through standardized APIs to allow an operator to store new services in the SO's catalogs, order these services for provisioning atop a certain infrastructure, activate/de-activate these services on demand, and use lifecycle management knobs to control the real-time behaviour of these services, allowing the operator to scale them in/out, migrate to different domains, etc.

Continuous Integration (CI)/Continuous Delivery (CD) is essential in modern times as an operator wishes to roll-out new features of platform and customer services in an automated fashion and with ultimate control on matters, such as real-time service upgrade, rollback recovery, etc. NANCY promotes a tight integration between the CI/CD platform and the NANCY service and resource orchestrators as the latter need to use software registries to pull service images before their provisioning and runtime management begins. For this reason, NANCY establishes an automated CD pipeline that is spawned within the CI/CD platform, upon every stable release of a NANCY service; this

pipeline triggers the SO's NBI to order this service for deployment on a designated testbed, ensuring that the service is deployed, all of its components are in "running" state, and integration tests are spawned to test the runtime behaviour of the service.

2.1.4. NANCY Business Layer

Network operators employ components in the NANCY "Business" layer to manage products and their billing within their internal realm, but also integrate with other operators to exchange products, services, and resources through a secure inter-operator domain as shown in Figure 2-1.

Intra-Operator Business Components

Business Support System (BSS) stands at the top part in Figure 2-1– highlighted in orange colour. This component oversees the services residing in the SO's catalogs and associates these services with products offered through the operator's "local" marketplace. To do so, the BSS introduces product catalogs, where each product is mapped to one or more services from the SO's catalog. Customers access this catalog to order products, which results in (i) a corresponding (set of) service order(s) from the BSS to the SO and (ii) a billing process that begins to charge the customer according to a charging policy agreed between the operator and the customer. Once an ordered product results in a provisioned service instance, a product inventory summarizes runtime information about the services associated with the product and the runtime view of the product's billing balance.

Inter-Operator Business Components

NANCY advocates the use of an inter-operator domain – highlighted in purple colour at the top right part in Figure 2-1 – as a common environment where multiple operators can share their products through a common marketplace, while a secure infrastructure is there to ensure that digital agreements are signed by the right parties when inter-operator orders are issued by customers of this "federated" market place.

Blockchain is a key component of the secure inter-operability among multiple operators. The blockchain fosters trust among partners by serving as a reliable and transparent ledger, ensuring data integrity and authenticity. A decentralized database provides a single source of truth, thereby enhancing the security and reliability of transactions between parties.

NEC blockchain is built on the Hyperledger Fabric project [22], an open-source, enterprise-grade framework for developing flexible, permissioned distributed ledger applications.

Marketplace is a Blockchain-based component which gathers all the information about the operators and their available services. It includes all the required details for feeding the Smart Pricing module to decide the most suitable price of the most suitable available service (and operator) as well as the Digital agreement creator to generate smart contracts for relevant parties (operators, consumers). The Marketplace includes all the historical updates of the operators and their services' features and prices, as well as signed agreements. As the marketplace interacts with external non-blockchain-based components, oracles and Blockchain events are considered for this communication. Additionally, a Blockchain monitor listening to the marketplace events is included to enhance the usability of the component.

Digital Agreement is an out-of-the-box solution for creating and deploying Smart Contracts among NANCY stakeholders. DAC receives inputs from the Marketplace concerning e.g., providerId, consumerId, service, price, conditions, etc. and creates ad-hoc containers that produce smart contracts for relevant parties based on the provided input. The latter containers include also other useful

information, such as a unique identification number (generated by the DAC), that works as a kind of hash of the smart contract.

Smart Pricing: When a user goes beyond the coverage area of their original MNO, other MNOs operating in that area compete to provide their most competitive prices to serve the user. The Smart Pricing module conducts an auction among the various MNOs depending on their pricing offers. Participation in this auction is limited to MNOs who fulfil the user's SLA. The Smart Pricing Module utilizes reverse auction theory, which is implemented with reinforcement learning. The Smart Pricing module receives a list of MNOs that satisfy the user's SLA, which is provided by blockchain oracles. Additionally, it receives the bidding prices published by each MNO in the Marketplace module. The Smart Pricing Module will function as a smart contract on the Blockchain, producing the MNO that wins and the winning bid as its output.

3. NANCY Testbeds

To define a successful integration strategy, it is important to acquire a clear view of the available facilities and capabilities of the underlying infrastructure. To this end, this section introduces the three NANCY testbeds, spread across three sites in south Europe. Section 3.2 introduces the Greek NANCY testbed (Task 6.5 and Task 6.6), Section 3.3 describes the Italian NANCY testbed (Task 6.7 and Task 6.8), while Section 3.4 introduces the Spanish NANCY testbed (Task 6.9).

3.1. Terminology

This section introduces key terms for the description and classification of the NANCY testbed facilities.

In-lab Testbed: Refers to indoor testbed facilities. NANCY offers three such testbeds:

1. **Testbed 1:** the Greek in-lab testbed provided by UoWM;
2. **Testbed 2:** the Italian in-lab testbed provided by ITL; and
3. **Testbed 3:** the Italian Massive IoT demonstrator testbed provided by TEI.

Demonstrator (Outdoor) Testbed: Refers to outdoor testbed facilities. NANCY offers three such testbeds:

1. **Testbed 4:** the Greek demonstrator testbed provided by OTE;
2. **Testbed 5:** the Spanish demonstrator testbed provided by EHU; and
3. **Testbed 6:** the Spanish demonstrator extension testbed provided by UMU.

3.2. Greek Testbeds

This section introduces the two Greek testbeds provided by UoWM (Greek in-lab testbed in Section 3.2.1) and OTE (Greek demonstrator testbed in Section 3.2.2).

3.2.1. Greek In-lab Testbed

Figure 3.1 depicts the hardware layout of the Greek In-lab testbed located at the UoWM premises in northern Greece. The rest of this section lists all hardware components present in this testbed. This laboratory deployment showcases a low TRL coverage expansion scenario consisting of two operators, namely the main operator and the micro-operator that deploy and manage a public and a private 5G standalone (SA) network, respectively. Two USRP B210 devices are managed by the srsRAN and configured to serve as gNBs, while the Open5GS software is used to provide core network functionalities. Moreover, the micro-operator is connected to the public 5G network using a Quectel 5G module which is mounted on a USB adaptor. In the micro-operator's private network, a Xiaomi smartphone and a ZTE 5G router are connected to the gNB. Finally, the ZTE 5G router acts as a traffic emulator by connecting various devices through WiFi or Ethernet.

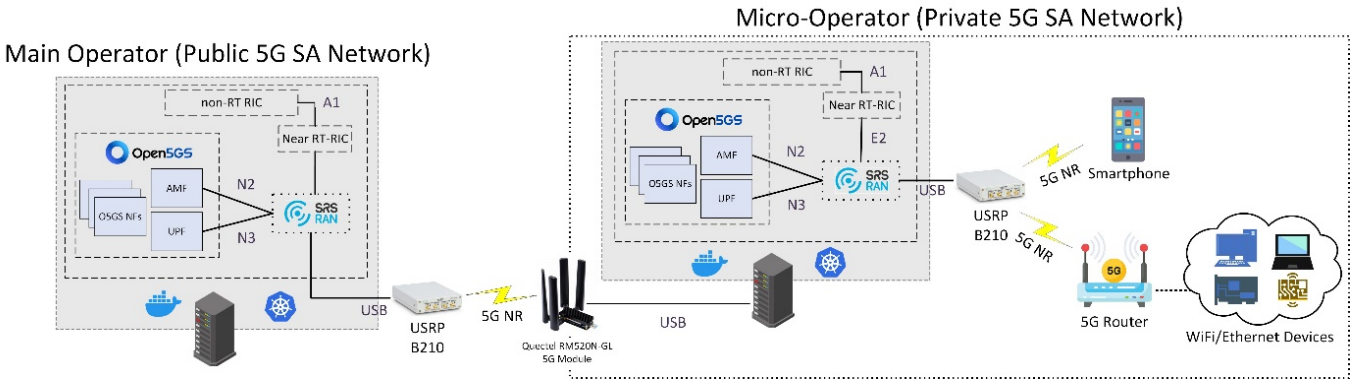

Figure 3-1: Overview of the Greek in-lab testbed.

Hardware Components

UE and IoT Hardware

Table 3-1 lists the UE and IoT components of the Greek in-lab testbed.

Table 3-1: Greek in-lab testbed - UE and IoT device components.

Device		(Radio) Network Interface		Connects with	Provided by
Vendor	Model	Type	Access Technology		
Xiaomi	11 Lite 5G NE	5G UE	5G NR SA	gNB (Micro operator)	UOWM
Quectel	RM520N-GL mounted in a USB adapter kit	5G UE	5G NR SA	gNB (Main operator)	UOWM
ZTE	MC888 Pro 5G Router	5G CPE	5G NR SA, Wifi, Ethernet	gNB (Main operator)	UOWM

(IoT) Gateway Hardware

No (IoT) gateway components are provided by the Greek in-lab testbed.

RAN Hardware

Table 3-2 lists the 5G RAN components of the Greek in-lab testbed.

Table 3-2: Greek in-lab testbed - RAN hardware components.

RAN Component					East Interface		West Interface		Provided by
Type	Vendor /Model	Model	OS/Distri-bution	CPU Vendor	Type	Connects with	Type	Connects with	
5G RU	Ettus Research	USRP B210	Ubuntu	Spartan 6 XC6SLX150 FPGA	5G NR	UEs	USB	gNB (srsRAN)	UOWM
5G RU	Ettus Research	USRP B210	Ubuntu	Spartan 6 XC6SLX150 FPGA	5G NR	UEs	USB	gNB (srsRAN)	UOWM

Networking Hardware

No other networking hardware components are provided by the Greek in-lab testbed.

Commodity or Specialized Servers

Table 3-3 lists the commodity or specialized processors (physical or virtual) provided by the Greek in-lab testbed.

Table 3-3: Greek in-lab testbed – Commodity or specialized servers.

Device			Processing Capacity					Provided by
Vendor	Model	OS/ Distribution	CPU vendor/model	# of CPUs	DRAM (GB)	Storage (TB)	# of NIC ports	
Dell	Precision 5530	Ubuntu 22.04	Intel i7 8850H	12	16	0.5	1 (through USB Type-C)	UOWM
Asus	Vivobook PRO 16X	Ubuntu 22.04	Intel i7 12700H	20	32	1	1 (through USB Type-C)	UOWM

Software Components

Section 5.2.1 discusses what additional software is provided by the Greek in-lab testbed in support of the above hardware components and how this software is deployed and connected with the rest of the NANCY platform.

3.2.2. Greek Demonstrator Testbed

Figure 3-2 depicts the hardware layout of the Greek demonstrator testbed located at the OTE premises in central Greece. The rest of this section lists all hardware components present in this testbed.

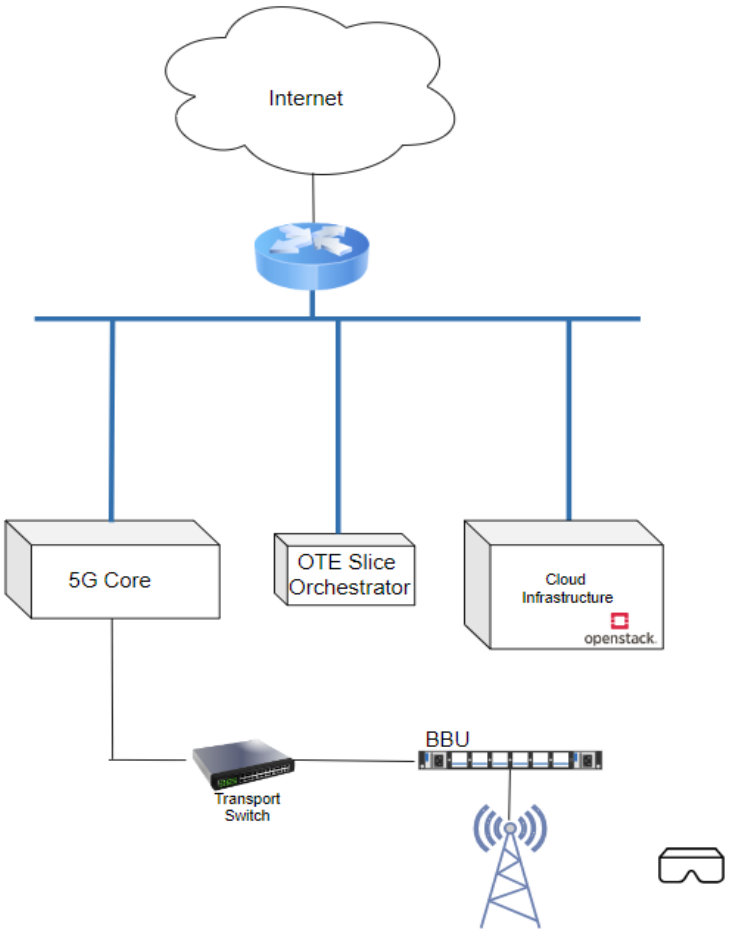

Figure 3-2: Overview of the Greek demonstrator testbed.

Hardware Components

UE and IoT Hardware

Table 3-4 lists the UE and IoT components of the Greek demonstrator testbed.

Table 3-4: Greek demonstrator testbed - UE and IoT device components.

Device		(Radio) Network Interface		Connects with	Provided by
Vendor	Model	Type	Access Technology		
Samsung	S24	5G UE	5G NR	5G gNB	OTE
Meta Quest	Oculus 2 (meta quest)	Wireless	Ultra-Wideband	5G CPE	OTE
TELTONIKA	rutx50	5G UE (CPE)	5G NR	5G gNB	OTE

(IoT) Gateway Hardware

No (IoT) gateway components are provided by the Greek demonstrator testbed.

RAN Hardware

Table 3-5 lists the 5G RAN components of the Greek demonstrator testbed. The radio unit that is installed supports both LTE and NR TDD with four duplex TX/RX branches supporting up to 4x5 W output power, while the baseband unit (BBU) includes 15 CPRI/9 eCPRI, LTE+NR with up to 12 CCs LTE and 12 CCs NR in dual mixed mode.

Table 3-5: Greek demonstrator testbed - RAN hardware components.

RAN Component					East Interface		West Interface		Provided by
Type	Vendor /Model	Model	OS/Distri-bution	CPU Vendor	Type	Connects with	Type	Connects with	
Radio Unit	Ericsson	ERS4408	-	-	5G NR	UE, IoT devices	Ethernet	Baseband Unit	OTE
Radio Unit	Ericsson	Dot	-		5G NR	UE, IoT devices	Ethernet	Baseband Unit	OTE
Baseband Unit	Ericsson	6630	-	-	Ethernet	Radio Unit	Optical fibre	5GC	OTE

Networking Hardware

Table 3-6 lists the networking hardware components of the Greek demonstrator testbed. Note that some entries may refer to programmable networking hardware (e.g., based on P4, OpenFlow, etc.), while others may refer to legacy networking hardware.

Table 3-6: Greek demonstrator testbed - (Programmable) networking hardware components.

Device					Capacity	Provided by
Vendor	Model	OS/Distribution	Mgmt. Protocol	# of Ports		
CISCO	WS-C4500X-32	N/A	SNMP	16	N/A	OTE
DELL	N4032F	N/A	SNMP	16	N/A	OTE

Commodity or Specialized Servers

Table 3-7 lists the physical servers that are provided by the Greek demonstrator testbed. More specifically, 4 HPE servers will be available.

Table 3-7: Greek demonstrator testbed – Commodity or specialized servers.

Device			Processing Capacity					Provided by
Vendor	Model	OS/ Distribution	CPU vendor/model	# of CPUs	DRAM (GB)	Storage (TB)	# of NIC ports	
HPE	ProLiant DL360 Gen9 Server	Ubuntu	E5-2650	32	128	2.4	4	OTE

Software Components

Section 5.2.1 discusses what additional software is provided by the Greek demonstrator testbed in support of the above hardware components and how this software is deployed and connected with the rest of the NANCY platform.

3.3. Italian Testbeds

This section introduces the two Italian testbeds, one provided by ITL (Italian in-lab testbed in Section 3.3.1) and the other provided by TEI (Italian Massive IoT demonstrator testbed in Section 3.3.2).

3.3.1. Italian In-lab Testbed

Figure 3-3 depicts the high-level hardware set-up of the Italian In-lab testbed located at ITL's headquarters in Milan, Italy. It provides a MEC-assisted 5G network scenario with a video streaming application for generating traffic. The rest of this section lists all hardware components present in this testbed.

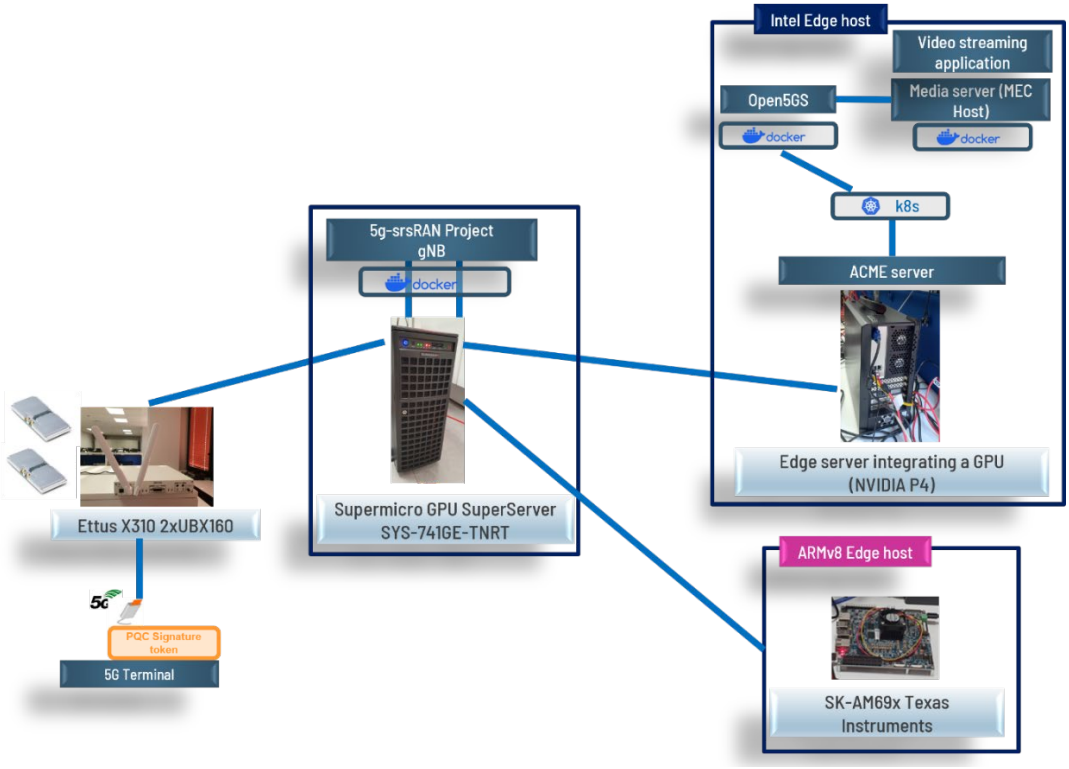

Figure 3-3: Overview of the Italian in-lab testbed.

Hardware Components

This section lists the hardware components of the Italian In-lab testbed. For detailed characteristics of each device, please refer to the description present in Deliverable D6.4 "In-lab testbeds definition", section 3.2 and corresponding appendices.

UE and IoT Hardware

Table 3-8 lists the UE and IoT components of the Greek demonstrator testbed.

Table 3-8: Italian in-lab testbed - UE and IoT device components.

Device		(Radio) Network Interface		Connects with	Provided by
Vendor	Model	Type	Access Technology		
Google	Pixel7 Android 5G	5G UE	5G NR	Ettus RU	ITL
Motorola	Moto G100	5G UE	5G NR	Ettus RU	ITL

(IoT) Gateway Hardware

No (IoT) gateway components are present in the Italian in-lab testbed.

RAN Hardware

Table 3-9 lists the 5G RAN components of the Italian in-lab testbed.

Table 3-9: Italian in-lab testbed - RAN hardware components.

RAN Component					East Interface		West Interface		Provided by
Type	Vendor /Model	Model	OS/Distri-bution	CPU Vendor	Type	Connects with	Type	Connects with	
5G RU	Ettus	X310 2xUBX160 board	-	-	5G NR	UEs	Ethernet	5G srsRAN	ITL

Networking Hardware

No other networking hardware components are present in the Italian in-lab testbed.

Commodity or Specialized Servers

Table 3-10 lists the commodity or specialized processors (physical or virtual) provided by the Italian in-lab testbed. The first device is used as an edge box for offloading, while the other two devices host the software-based part of the 5G gNB and the 5GC + end-user applications.

Table 3-10: Italian in-lab testbed – Commodity or specialized servers.

Device			Processing Capacity					Provided by
Vendor	Model	OS/ Distribution	CPU vendor/model	# of CPUs	DRAM (GB)	Storage (TB)	# of NIC ports	
Texas Instrument	SK-AM69	Linux Ubuntu	ARMv8	8 Cortex A72	32	0.032 (32GB)	1	VOS
Supermicro	GPU SuperServer SYS-741GE-TNRT + 2 GPU NVIDIA A40	Linux Ubuntu	Intel(R) Xeon(R) Silver 4410T @ 2.70GHz	40	128GBytes	4TBytes	4x 1GbE	ITL
Intel	ACME intel server	Linux Centos7	Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz	40	128GBytes	2TBytes	2x1GbytesBytes + 1x10GbytesBytes	ITL

Software Components

Section 5.2.2 discusses what additional software is provided by the Italian in-lab testbed in support of the above hardware components and how this software is deployed and connected with the rest of the NANCY platform.

3.3.2. Italian Demonstrator Testbed

Figure 3-4 depicts the high-level hardware set-up of the Italian Massive IoT demonstrator testbed located at Ericsson's facilities in Genoa (Italy). It provides a commercial grade 5G testbed to test

Massive IoT scenario deployed at the edge of the network with new Post Quantum Cryptography algorithms for secure traffic delivery. The rest of this section lists all hardware components present in this testbed.

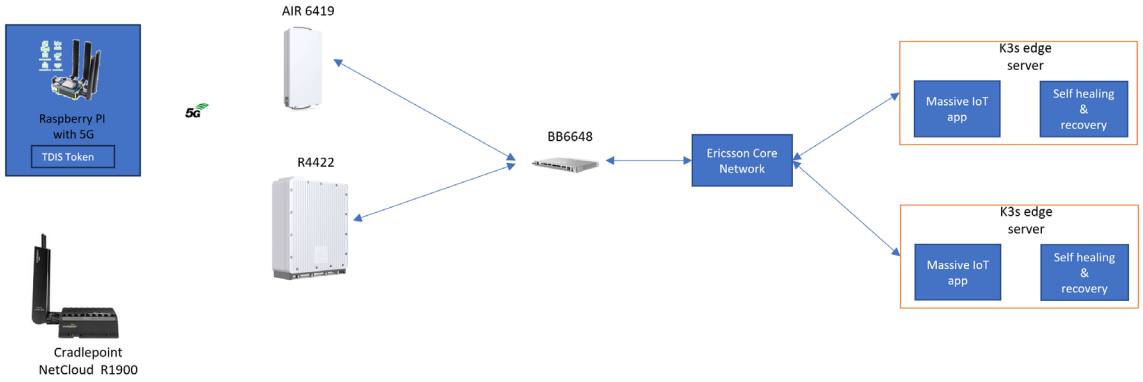

Figure 3-4: Overview of the Italian demonstrator testbed.

Hardware Components

UE and IoT Hardware

Table 3-11 lists the UE and IoT components of the Italian demonstrator testbed.

Table 3-11: Italian demonstrator testbed - UE and IoT device components.

Device		(Radio) Network Interface		Connects with	Provided by
Vendor	Model	Type	Access Technology		
-	Raspberry Pi 4 with 5G hat	Wireless	5G NR	5G gNB	TEI

(IoT) Gateway Hardware

No (IoT) gateway components are provided by the Italian demonstrator testbed.

RAN Hardware

The Ericsson mobile Network used for the tests will evolve along the project: it allows to collect results, during the application integration facilitating the comparison of the performances in the architectures. Table 3-12 lists the commercial grade 5G RAN components of the Italian Massive IoT demonstrator testbed. These components are currently considered for the setup but may change.

Table 3-12: Italian demonstrator testbed - RAN hardware components.

RAN Component					East Interface		West Interface		Provided by
Type	Vendor /Model	Model	OS/Distri-bution	CPU Vendor	Type	Connects with	Type	Connects with	
5G gNB	Ericsson	BB6648	-	-	5G NR	UE, IoTdevices	CPRI and eCPRI	5GC	TEI
5G gNB	Ericsson	R4422	-	-	5G NR	UE, IoT devices	Cpri_8	gNB	TEI
5G gNB	Ericsson	AIR6419	-	-	5G NR	UE, IoT devices	25G eCPRI	gNB	TEI

5G CPE	Cradlepoint	Netcloud R1900	-	-	WiFi, Ethernet	Non-5G UE/IoT devices	5G NR	gNB	TEI

Networking Hardware

Table 3-13 lists the networking hardware components of the Italian demonstrator testbed.

Table 3-13: Italian demonstrator testbed - networking hardware components.

Device					Capacity	Provided by
Vendor	Model	OS/Distribution	Mgmt. Protocol	# of Ports		
Ericsson	R6675	-	SNMP	28	-	TEI

Commodity or Specialized Servers

Table 3-14 lists the commodity processors (physical or virtual) provided by the Italian demonstrator testbed.

Table 3-14: Italian demonstrator testbed – Commodity or specialized servers.

Device			Processing Capacity					Provided by
Vendor	Model	OS/ Distribution	CPU vendor/model	# of CPUs	DRAM (GB)	Storage (TB)	# of NIC ports	
HP	HP 290 G4 Microtower PC	Windows 10 PRO	Intel(R) Core (TM) i7-10700 CPU	64	16	0.464	2	TEI
Dell	R640	Linux	Intel Xeon Scalable Processor	24	256	6,4	5	TEI

Software Components

Section 5.2.2 discusses what additional software is provided by the Italian demonstrator testbed in support of the above hardware components and how this software is deployed and connected with the rest of the NANCY platform.

3.4. Spanish Testbeds

This section introduces the Spanish demonstrator provided by EHU (main Spanish demonstrator in Section 3.4.1) and an extension to this testbed provided by UMU (Spanish demonstrator extension in Section 3.4.2).

3.4.1. Spanish Demonstrator Testbed

Figure 3-5 depicts the hardware layout of the Spanish demonstrator testbed located at the EHU premises in Spain. The rest of this section lists all hardware components present in this testbed.

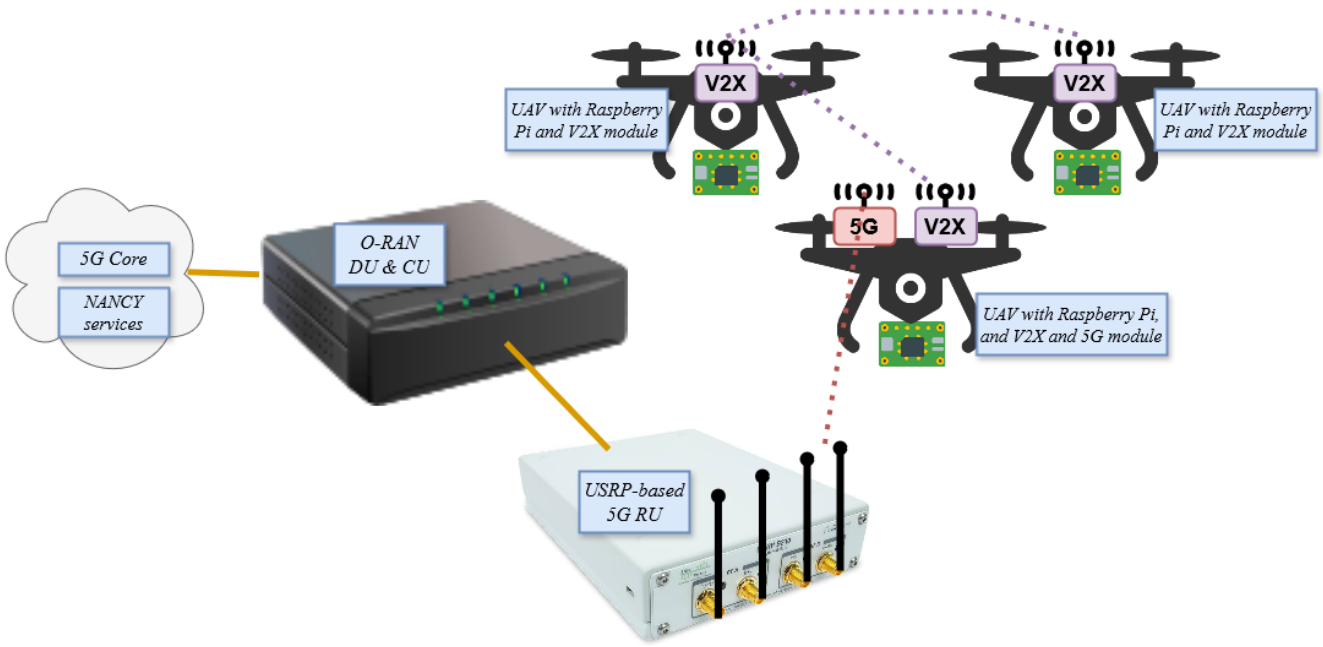

Figure 3-5: Overview of the Spanish demonstrator testbed (EHU premises).

Hardware Components

UE and IoT Hardware

Table 3-15 lists the UE and IoT components of the Spanish demonstrator testbed.

Table 3-15: Spanish demonstrator testbed - UE and IoT device components.

Device		(Radio) Network Interface		Connects with	Provided by
Vendor	Model	Type	Access Technology		
-	UAV node (x3)	Wireless	V2X and 5G NR	UAV network and 5G gNB	EHU
Unex	SOM-352UC (x3)	Wireless	V2X	UAV network	EHU
Quectel	RM520N-GL (x1)	Wireless	5G NR	5G network	EHU
-	Raspberry Pi 4 (x3)	Wireless	V2X and 5G NR	UAV network and 5G gNB	EHU

(IoT) Gateway Hardware

No (IoT) gateway components are used in the Spanish demonstrator testbed.

RAN Hardware

Table 3-16 lists the 5G RAN components of the Spanish demonstrator testbed.

Table 3-16: Spanish demonstrator testbed - RAN hardware components.

RAN Component					East Interface		West Interface		Provided by
Type	Vendor /Model	Model	OS/Distri-bution	CPU Vendor	Type	Connects with	Type	Connects with	
5G gNB	Amarisoft	Classic box	Fedora	x86/x64	5G NR	UE, IoT devices	Ethernet	5GC	EHU

USRP	Ettus	B210	-	-	5G NR	UE, IoT devices	Ethernet	O-RAN and 5GC	EHU

Networking Hardware

No networking hardware components are used in the Spanish demonstrator testbed.

Commodity or Specialized Servers

Table 3-17 lists the commodity or specialized processors (physical or virtual) provided by the Spanish demonstrator testbed.

Table 3-17: Spanish demonstrator testbed – Commodity or specialized servers.

Device			Processing Capacity					Provided by
Vendor	Model	OS/ Distribution	CPU vendor/model	# of CPUs	DRAM (GB)	Storage (TB)	# of NIC ports	
Supermicro	SYS-E200-8D	Ubuntu	Intel(R) Xeon(R) CPU D-1528 @ 1.90GHz	6	64	0.5	4	EHU

Software Components

Section 5.2.3 discusses what additional software is provided by the Spanish demonstrator testbed in support of the above hardware components and how this software is deployed and connected with the rest of the NANCY platform.

3.4.2. Spanish Demonstrator Extension

Figure 3-6 depicts the hardware layout of the Spanish demonstrator extension located at the UMU premises in Spain. The rest of this section lists all hardware components present in this testbed.

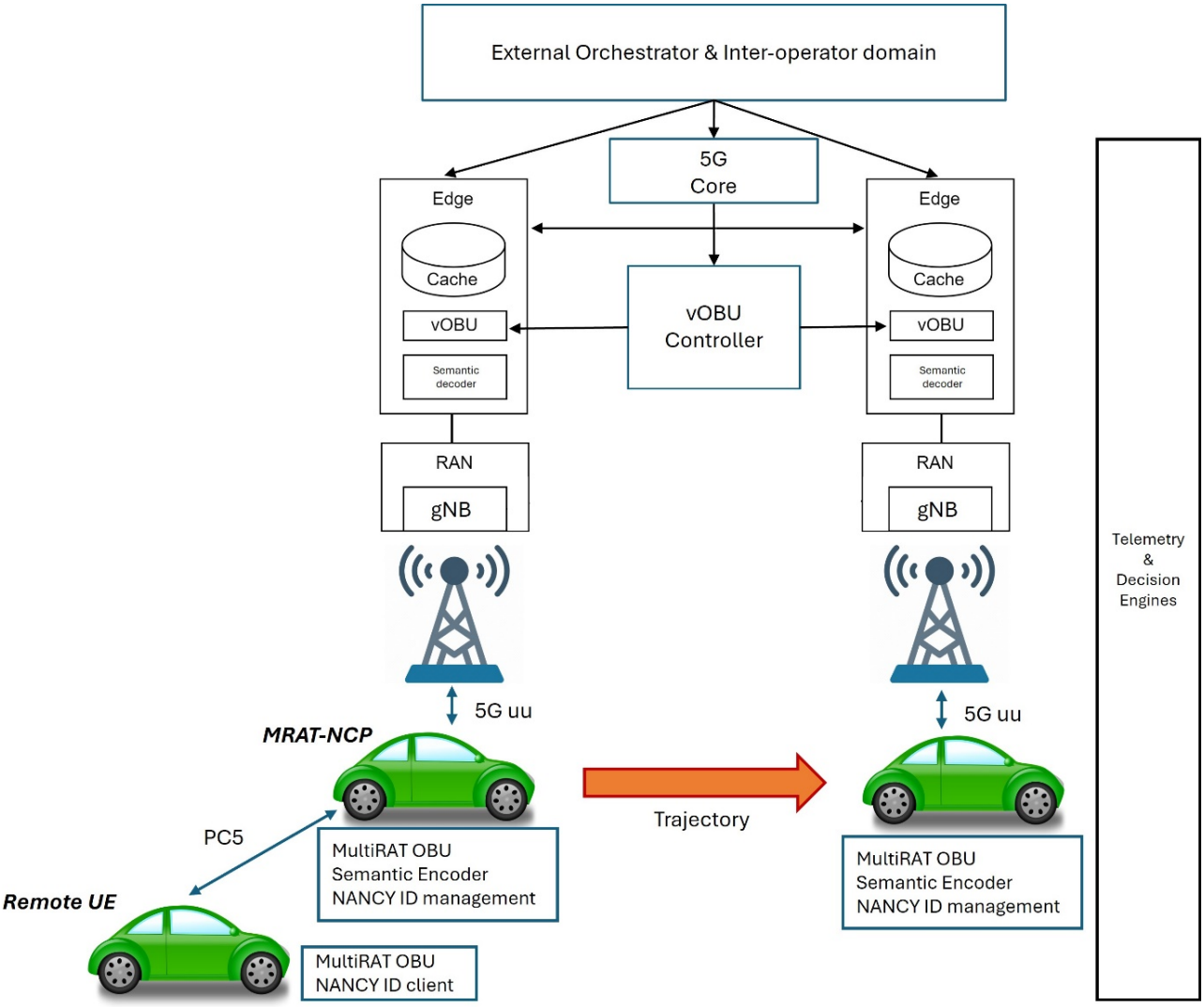

Figure 3-6: Overview of the Spanish demonstrator extension (UMU premises).

Hardware Components

UE and IoT Hardware

Table 3-18 lists the UE and IoT components of the Spanish demonstrator extension testbed.

Table 3-18: Spanish demonstrator extension testbed - UE and IoT device components.

Device		(Radio) Network Interface		Connects with	Provided by
Vendor	Model	Type	Access Technology		
Quectel	RM520N-GL (x1)	Wireless	5G NR	5G network	UMU
Cohda	OBU mk6	Wireless	V2X/PC5	5G network	UMU
Fibocom	160M	Wireless	5G NR	5G network	UMU

(IoT) Gateway Hardware

Table 3-19 lists the (IoT) gateway components of the Spanish demonstrator extension testbed.

Table 3-19: Spanish demonstrator extension testbed - (IoT) gateway components.

Device		(Radio) Network Interface		(Backbone) Network Interface		Provided by
Vendor	Model	Type	Access Technology	Type	Access Technology	
Raspberry	V5	USB Modem	5G NR	Wired	Ethernet	UMU
Lattepanda	3	USB Modem	5G NR	Wired	Ethernet	UMU

RAN Hardware

Table 3-20 lists the 5G RAN components of the Spanish demonstrator extension.

Table 3-20: Spanish demonstrator extension testbed - RAN hardware components.

RAN Component					East Interface		West Interface		Provided by
Type	Vendor /Model	Model	OS/Dis tri-bution	CPU Vendor	Type	Connects with	Type	Connects with	
5G gNB	Amarisoft	Classic box	Fedora	x86/x64	5G NR	UE, IoT devices	Ethernet /Optical Fiber	5GC	UMU
5G gNB	AW2S	Blackhawk	Fedora	X86/x64	5G NR	UEs	Ethernet /Optical Fiber	5GC	UMU

Networking Hardware

Table 3-21 lists the networking hardware components of the Spanish demonstrator extension testbed. Note that some entries may refer to programmable networking hardware (e.g., based on P4, OpenFlow, etc.), while others may refer to legacy networking hardware.

Table 3-21: Spanish demonstrator extension testbed - (Programmable) networking hardware components.

Device					Capacity	Provided by
Vendor	Model	OS/Distribution	Mgmt. Protocol	# of Ports		
Edgecore	AS7326-56x	SONIC, ONIE	SDN	48	TOR switch supporting 10/25 GbE to servers with 40/100 GbE uplinks	UMU

Commodity or Specialized Servers

Table 3-22 lists the commodity or specialized processors (physical or virtual) provided by the Spanish demonstrator extension testbed.

Table 3-22: Spanish demonstrator extension testbed – Commodity or specialized servers.

Device			Processing Capacity					Provided by
Vendor	Model	OS/ Distribution	CPU vendor/model	# of CPUs	DRAM (GB)	Storage (TB)	# of NIC ports	
Lenovo	SR650V2	Debian	AMD EPYC 7302P	16	64	0.256	4	UMU

Software Components

Section 5.2.3 discusses what additional software is provided by the Spanish demonstrator extension in support of the above hardware components and how this software is deployed and connected with the rest of the NANCY platform.

4. Integration

4.1. Terminology and Definitions

This section introduces key terms of the integration process, before delving into technical details.

NANCY Interface (NI): An API exposed by a logical component of the NANCY architecture for addressing a specific functionality.

NANCY Interface Set (NIS): A set of APIs exposed by a logical component of the NANCY architecture, each offering a different data model for addressing the same purpose. As an example, a Monitoring platform component may provide a set of APIs for exposing monitoring metrics from different domains, such as (i) an API for O-RAN telemetry, (ii) an API for transport network telemetry, (iii) an API for compute telemetry, and (iv) an API for mobile core network telemetry. In other words, a NIS is a "family" of similar interfaces, grouped together.

4.2. NANCY Platform Interfaces

Figure 4-1 is an annotated version of Figure 2-1, showing all the interfaces among the NANCY platform components. The role of this section is to identify the objective of each interface, which logical architecture components make use of each interface, as well as who are the NANCY consortium partners behind the implementation of these interface functions.

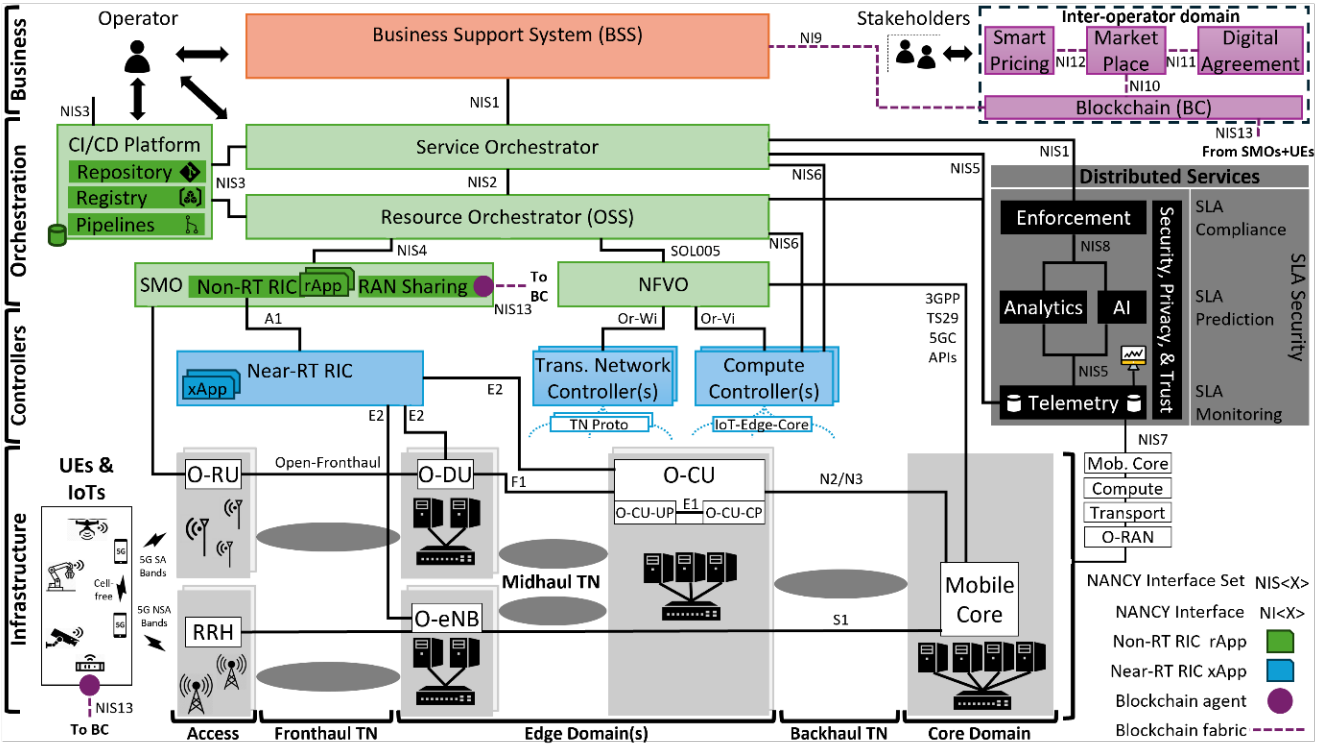

Figure 4-1: Functional and deployment view of the NANCY architecture (Figure 2-1) annotated with interface IDs.

Table 4-1 lists the NANCY interfaces and NANCY interface sets visualized in Figure 4-1. In column 1, each interface is associated with a unique identifier. NANCY interfaces begin with *NI* followed by an increasing number, while NANCY interface sets begin with *NIS* followed by an increasing number. Column 2 states the high-level objective of each NI and/or NIS, while Column 3 relates the interface

with one or more logical components of the NANCY architecture as shown in Figure 4-1. Finally, Column 4 states the partners responsible for the implementation of these components and interfaces.

Table 4-1: NANCY interfaces and the related NANCY architecture components.

Interface ID	Interface Objective	Related Logical Architecture Component(s)	Responsible Partners
NIS1	End user Service Exposure set of APIs	Service Orchestrator (NBI)	UBI, I2CAT
NIS2	Resource Service Exposure set of APIs	Resource Orchestrator (NBI)	UBI, I2CAT
NIS3	Service Repository and Registry set of APIs	CI/CD Platform, Service/Resource Orchestrator	INTRA, UBI/ I2CAT
NIS4	O-RAN Orchestration set of APIs	SMO NBI	Testbed owners (T6.5, T6.6, T6.8, T6.9)
NIS5	Service and Resource Telemetry Exposure set of APIs	Telemetry Infrastructure Service (NBI)	Testbed owners (T6.5, T6.6, T6.8, T6.9)
NIS6	Compute slice management set of APIs	Compute Controller(s) (NBI)	Testbed owners (T6.5, T6.6, T6.7, T6.8, T6.9)
NIS7	Telemetry collection set of APIs from various domains, including (O-)RAN, Transport Network, Compute, and Mob. Core	Telemetry, Infrastructure (Testbeds)	Testbed owners (T6.5, T6.6, T6.7, T6.8, T6.9) and T2.3 partners
NIS8	(Smart) events/outputs exposure set of APIs (AI and/or Analytics services)	AI/Analytics, Enforcement	Partners in T2.3-T2.4, T3.2-T3.4, T4.4, T5.4-T5.5
NI9	Secure Product Exposure API	Blockchain, BSS	NEC, TEC
NI10	Smart Contract deployed on the blockchain	Marketplace, Blockchain	TEC, NEC
NI11	Blockchain oracle – server API	Marketplace, Digital Agreement	TEC, DRAXIS
NI12	Blockchain oracle – server API	Marketplace, Smart Pricing	TEC, 8BELLS
NIS13	Secure (gRPC) interface between blockchain and wallet owners (e.g., UEs, IoTs, etc.)	Blockchain, user's wallet (can involve PQC)	NEC, TDIS, WP6 partners

4.2.1. NANCY Interfaces' Description

This section briefly introduces the interfaces listed in Table 4-1, providing links to open, standardized APIs behind these interfaces. We explain each interface in turn below.

NIS1 (UBI, I2CAT): A set of APIs for the exposure and management of end-user services towards the operator of a NANCY domain or the underlying BSS of the operator for associating domain services with products and their billing information. This set of interfaces will be materialized through the combination of the following interfaces:

- TMF 633 Service Catalog Management API [8]
- TMF 641 Service Ordering Management API [9]

- TMF 638 Service Inventory Management API [10]
- ETSI NFV SOL005 API [18][19][20]

NIS2 (UBI, I2CAT): A set of APIs for the exposure and management of (i) resource services and (ii) resources from the RO towards the SO. This set of interfaces will be materialized through the combination of the following interfaces:

- TMF 633 Service Catalog Management API [8]
- TMF 641 Service Ordering Management API [9]
- TMF 638 Service Inventory Management API [10]
- TMF 634 Resource Catalog Management API [15]
- TMF 652 Resource Ordering Management API [16]
- TMF 639 Resource Inventory Management API [17]
- ETSI NFV SOL005 API [18][19][20]

NIS3 (INTRA): A set of APIs for accessing public or private software repositories and registries where NANCY end-user and/or platform services are stored. Popular interfaces are behind this API set, as follows:

- Git interface using Hypertext Transfer Protocol (HTTP), HTTP Secure (HTTPS), Secure Shell (SSH), or Git protocols
- Registry interface using HTTPS or Open Container Initiative (OCI) [21] protocols.

NIS4 (OTE, UoWM, EHU/UMU): A set of APIs for the orchestration of O-RAN-based domains over the SMO's NBI. This API set is consumed by the Resource Orchestrator for managing O-RAN domains in tandem with other neighbouring domains, such as backhaul TN, compute, etc.

NIS5 (OTE, UoWM, ERI, EHU/UMU): A set of APIs for the exposure of service and resource-level telemetry. These APIs are consumed by (i) the NANCY orchestration platform for obtaining visibility on the underlying system's conditions as well as (ii) distributed NANCY services that use AI/Analytics or deterministic algorithms to make smart inference upon infrastructure data.

NIS6 (OTE, UoWM, ERI, EHU/UMU): A set of APIs for the management of compute slices atop physical and/or virtual cloud resources. This API set includes the following interfaces:

- OpenStack NOVA API for managing VMs
- Kubernetes server API for managing containers in Kubernetes clusters.

NIS7 (OTE, UoWM, ERI, EHU/UMU): A set of APIs for telemetry collection across various domains, including (O-)RAN, Transport Network, Compute, and Mobile Core.

NIS8 (T2.3, T2.4, T3.2, T3.3, T4.4, T5.4, T5.5): A set of APIs for the exposure of (smart) events or outputs stemming from AI/Analytics services.

NI9 (NEC, TEC): An API for securely exposing the product management APIs of an operator's BSS towards the inter-operator marketplace, through a blockchain. The APIs are gRPC calls exposed by the wallet.

NI10 (TEC, NEC): Smart contract deployed on the blockchain, based on the open-source project of the Linux Foundation, Hyperledger Fabric [22].

NI11 (TEC, DRAXIS): The digital agreement creator exposes its own REST API that will be consumed by the Oracle DAC used from the marketplace.

NI12 (TEC, 8BELLS): The smart pricing exposes its own REST API that will be consumed by the Oracle SP used from the marketplace.

NIS13 (NEC, TDIS, WP6 partners): Several gRPC interfaces allowing the owner of a wallet to communicate with the blockchain and generating PQC signature (if the user is allowed).

5. NANCY Platform Instantiation atop the NANCY Testbeds

This section outlines how NANCY envisions deploying the platform as a whole atop the 3 testbeds across south Europe (i.e., Greece, Italy, and Spain). To sketch such a deployment model, it is essential to consider what part of the NANCY platform will be centralized (see Section 5.1) and how the rest of the components will be distributed across the testbeds (see Section 5.2). Finally, Section 5.3 introduces how the NANCY CI/CD platform (T6.1 and T6.2) will assist the deployment and integration activities.

5.1. Central NANCY Platform

Table 5-1 summarizes the NANCY platform components that will be deployed on NANCY's central management domain. The table also shows the layer of the architecture where these components belong to, whether they appear within a single operator's realm or in the inter-operator domain, while also highlighting the actual deployment location of the component as well as the responsible partners.

Table 5-1: List of components deployed on the NANCY Central domain.

Component Name	Belongs to	Deployment Location	Responsible Partners
Blockchain	Inter-operator domain – Business Layer	NEC blockchain testbed	NEC
Marketplace	Inter-operator domain – Business Layer	NEC blockchain testbed	TEC
Digital Agreement	Inter-operator domain – Business Layer	NEC blockchain testbed	DRAXIS
BSS	Intra-operator domain – Business Layer	INTRA Cloud	TEC
Service Orchestrator	Intra-operator domain – Orchestration Layer	INTRA Cloud	UBI, I2CAT
Resource Orchestrator	Intra-operator domain – Orchestration Layer	INTRA Cloud	UBI. I2CAT

5.2. Distributed NANCY Components

5.2.1. Greek Testbed Software Components

Greek In-lab Testbed (UoWM)

Orchestration Services

Table 5-2 lists the orchestration components supported by the Greek In-lab testbed.

Table 5-2: List of orchestration components supported by the Greek In-lab testbed.

Orchestrator Name	Devices/Services under control	Supported Interface(s)	Responsible Partners
O-RAN Software Community non-RT RIC	Near-RT RIC	A1	UOWM

Controller Services

Table 5-3 lists the controllers supported by the Greek In-lab testbed.

Table 5-3: List of controllers supported by the Greek In-lab testbed.

Controller Name	Devices/Services under control	Supported Interface(s)	Responsible Partners
Kubernetes Compute Controller	Asus Vivobook Pro 16X and Dell Precision 5530 servers	NIS6 using the Kubernetes API server	UOWM, UBITECH
FlexRIC near-RT RIC	srsRAN	E2	UOWM
O-RAN Software Community near-RT RIC	srsRAN	E2	UOWM
srsRAN	Ettus Research USRP devices (B210)	Open Fronthaul, F1, E1, E2	UOWM

Telemetry Services

Table 5-4 lists the telemetry services supported by the Greek In-lab testbed.

Table 5-4: List of telemetry services supported by the Greek In-lab testbed.

Telemetry Service Name	Target Infrastructure	Telemetry Software Used	Supported Interface(s)	Responsible Partners
SDN CNI Telemetry	Compute cluster	Kube-prometheus [23]	NIS7 – SDN CNI metrics	UOWM

Use Case Services

Table 5-5 lists the NANCY services that will be used in the context of the Greek In-lab testbed facilities.

Table 5-5: List of NANCY services provided by the In-lab Greek Testbed.

Service Name	Objective and UC applicability	Supported Interface(s)	Responsible Partners
Multimedia Video Service	Video streaming over different operators' paths	N/A (Application Layer Service)	UOWM
Anomaly Detection	Detect network traffic anomalies	N2, NIS7, NIS5	UOWM, MINDS
XAI	Explain AI decision associated with the detection of AI network anomalies	NIS5	UOWM, MINDS

Greek Demonstrator Testbed (OTE)

Orchestration Services

The testbed supports an in-house orchestration component, the OTE Slice Orchestrator, which is a component responsible for the slicing. It provides a slice selection mechanism, allowing the use of a specific slice from a list of pre-defined slices. Table 5-6 lists the orchestration components supported by the Greek Demonstrator testbed.

Table 5-6: List of orchestration components supported by the Greek Demonstrator testbed.

Orchestrator Name	Devices under control	Supported Interface(s)	Responsible Partners
OTE Slice Orchestrator	Request to 5GC for specific slices	N/A	OTE

Controller Services

Table 5-7 lists the controllers supported by the Greek Demonstrator testbed.

Table 5-7: List of controllers supported by the Greek Demonstrator testbed.

Controller Name	Devices under control	Supported Interface(s)	Responsible Partners
Kubernetes Compute Controller	Physical COTS servers and/or VMs	NIS6 interface using the Kubernetes API server	UBI
OpenStack Compute Controller	Physical COTS servers and/or VMs	NIS6 interface using the OpenStack API	UBI

Telemetry Services

Table 5-8 lists the telemetry services supported by the Greek Demonstrator testbed.

Table 5-8: List of telemetry services supported by the Greek Demonstrator testbed.

Telemetry Service Name	Target Infrastructure	Telemetry Software Used	Supported Interface(s)	Responsible Partners
Compute Telemetry service	Compute clusters	Prometheus	NIS7 for gathering compute telemetry NIS5 for exposing compute telemetry	OTE
5G Telemetry service	5GC NFs and 5G gNBs	Prometheus	NIS7 for gathering 5G telemetry NIS5 for exposing 5G telemetry	OTE

Use Case Services

Table 5-9 lists the NANCY services that will be used in the context of the Greek Demonstrator testbed facilities.

Table 5-9: List of NANCY services provided by the Greek Demonstrator testbed.

Service Name	Objective and UC applicability	Supported Interface(s)	Responsible Partners
BC Adaptor	Allows non-5G UEs to interact with the blockchain.	NIS14	NEC
Offloading service	Implements the end-to-end workflow to manage a task offloading request and its lifecycle	NIS1, NIS2, NIS5, NIS6, NIS7	UBI, OTE
AR/VR service	Data collection and processing	NIS1, NIS3	UBI
Migration Service	Migrates VNFs from one node to another	NI18, NIS3	UBI, OTE

5.2.2. Italian Testbed Software Components

Italian In-Lab Testbed (ITL, TDIS, VOS, CRAT, SSS)

Orchestration Services

The "Italian in-lab testbed" scope focus on "RAN + edge" network segment; its aim is to test and demonstrate/validate single technology or functionality of NANCY. No orchestration components are supported by the testbed.

Controller Services

Table 5-10 lists the controllers supported by the Italian In-lab testbed. The controllers, internal to the testbed, are present only if and in case they are required for a specific set-up, based on the corresponding requirements.

Table 5-10: List of controllers supported by the Italian In-lab testbed.

Controller Name	Devices under control	Supported Interface(s)	Responsible Partners
Kubernetes Compute Controller	Physical COTS servers and/or VMs	NIS6 using the Kubernetes API server	ITL
OpenStack Compute Controller	Physical COTS servers and/or VMs	NIS6 using the OpenStack NOVA API	ITL

Telemetry Services

Table 5-11 lists the telemetry services supported by the Italian In-lab testbed. There are no telemetry services; relevant metrics are collected directly using the available Linux commands. No interface is supported.

Table 5-11: List of telemetry services supported by the Italian In-lab testbed.

Telemetry Service Name	Target Infrastructure	Telemetry Software Used	Supported Interface(s)	Responsible Partners
Compute Telemetry service	Compute clusters	Prometheus	NIS7 for gathering compute telemetry NIS5 for exposing compute telemetry	ITL

Use Case Services (ITL, TDIS, VOS, CRAT, SSS)

Table 5-12 lists the NANCY services that will be used in the Italian In-lab testbed facilities.

Table 5-12: List of NANCY services provided by the Italian In-lab testbed.

Service Name	Objective and UC applicability	Supported Interface(s)	Responsible Partners
Italtel VTU (video streaming and transcoding) application	To generate video streaming traffic to support the UCs of the Italian inlab testbed. It can convert audio and video streams from one format to another changing resolution, bitrate, and video parameters.	N/A	ITL
SCHED_DEADLINE	SCHED_DEADLINE scheduling policy to perform temporal isolation of Linux processes (OS kernel component)	N/A	SSS
Anomaly Detection of Software Workloads	Detect anomalies in the execution of software workloads by monitoring execution times and excessive memory traffic by exploiting the PAPI library and the ARM Performance Monitor Units hardware feature.	N/A	SSS
VOSySmonitor	ARMv8 monitor layer used to instantiate isolated, bare-metal, compartment for the edge, where VNFs/services are deployed and run	Only an internal interface is supported to interact with vManager	VOS
vManager	Management application (daemon) that interfaces with VOSySmonitor. This is needed as VOSySmonitor executes as a firmware in the highest privileged mode available and its interface with all the external components is very limited and requires ad-hoc support. In this context, vManager acts as a bridge.	In addition to the interface towards VOSySmonitor, vManager supports the libvirt protocol/interface	VOS
Anomaly Detection in the Edge	A Machine Learning procedure running in a docker container to identify anomalies and faults in the video streaming traffic from the Edge Server to the users	N/A	CRAT
PQC Signature Middleware	Software Library running under Linux published to upper layer applications to access to PQC Signature smartcard token	PQC Signature APIs	TDIS

Italian Demonstrator Testbed (TEI)

Orchestration Services

The "Italian Massive IoT Demonstrator testbed" focus is on the RAN, core and edge segments of the network. This testbed is designed with the primary objective of testing, demonstrating, and validating an IoT scenario considering self-healing and self-recovery components of NANCY. The testbed does not support any in-house orchestration components, but rather uses the central NANCY orchestration components.

Controller Services

Table 5-13 lists the controllers supported by the Italian Demonstrator testbed.

Table 5-13: List of controllers supported by the Italian Demonstrator testbed.

Controller Name	Devices under control	Supported Interface(s)	Responsible Partners
Kubernetes Compute Controller	Physical COTS servers and/or VMs	NIS6 using the Kubernetes API server	TEI

Telemetry Services

Table 5-14 lists the telemetry services supported by the Italian Demonstrator testbed.

Table 5-14: List of telemetry services supported by the Italian Demonstrator testbed.

Telemetry Service Name	Target Infrastructure	Telemetry Software Used	Supported Interface(s)	Responsible Partners
Compute Telemetry service	Compute clusters	Prometheus	NIS7 for gathering compute telemetry NIS5 for exposing compute telemetry	TEI

Use Case Services

Table 5-15 lists the NANCY services that will be used in the context of Massive IoT Italian Demonstrator testbed facilities.

Table 5-15: List of NANCY services provided by the Italian Demonstrator testbed.

Service Name	Objective and UC applicability	Supported Interface(s)	Responsible Partners
Massive IoT app	The objective is the demonstration of a massive machine-type communication (MTC) scenario.	N/A (Application Layer Service)	TEI
Self-healing and recovery	Distributed Self-healing and recovery algorithms for IoT applications integrated in the edge servers	N/A	CRAT

5.2.3. Spanish Testbed Software Components

Spanish Demonstrator Testbed (EHU)

Orchestration Services

Table 5-16 lists the orchestration components supported by the Spanish Demonstrator testbed.

Table 5-16: List of orchestration components supported by the Spanish Demonstrator testbed.

Orchestrator Name	Devices under control	Supported Interface(s)	Responsible Partners
SMO	O-RAN, Near-RT RIC	A1, NIS14	i2CAT

Controller Services

Table 5-17 lists the controllers supported by the Spanish Demonstrator testbed.

Table 5-17: List of controllers supported by the Spanish Demonstrator testbed.

Controller Name	Devices under control	Supported Interface(s)	Responsible Partners
Kubernetes Compute Controller	Physical COTS servers and/or VMs	NIS6 interface using the Kubernetes API server	EHU
OpenStack Compute Controller	Physical COTS servers and/or VMs	NIS6 interface using the OpenStack NOVA API	EHU
Near-RT RIC	Ettus B210 O-RAN RU, Physical COTS servers and/or VMs where O-DUs and O-CUs are deployed	A1 O-RAN interface and a custom interface towards the 5G gNB controller in Table 5-21	EHU

Telemetry Services

Table 5-18 lists the telemetry services supported by the Spanish Demonstrator testbed.

Table 5-18: List of telemetry services supported by the Spanish Demonstrator testbed.

Telemetry Service Name	Target Infrastructure	Telemetry Software Used	Supported Interface(s)	Responsible Partners
Compute Telemetry service	Compute clusters	Prometheus	NIS7 for gathering compute telemetry NIS5 for exposing compute telemetry	EHU

Use Case Services

Table 5-19 lists the NANCY services that will be used in the context of the Spanish Demonstrator testbed facilities.

Table 5-19: List of NANCY services provided by the Spanish Demonstrator testbed.

Service Name	Objective and UC applicability	Supported Interface(s)	Responsible Partners
V2X communication service	Provides the functionality to construct and transmit video frames across the V2X network and to the 5G network, forwarding it through multiple UAV hops when necessary.	-	EHU
Video preprocessing functions	Applies preprocessing to the video collected and streamed by the UAVs. Provided as VNFs that can leverage NANCY offloading mechanisms.	NIS6, NIS7	EHU
Wallet	Allows the UAV with the 5G module to interact with the blockchain. Installed in the Raspberry Pi installed in the UAV.	NIS14	NEC
BC Adaptor	Allows other UAVs that are not 5G UEs to interact with the blockchain. Installed in the Raspberry Pi installed in the UAV.	NIS14	NEC

Spanish Demonstrator Extension (UMU)

Orchestration Services

Table 5-20 lists the orchestration components supported by the Spanish Demonstrator extension testbed.

Table 5-20: List of orchestration components supported by the Spanish Demonstrator extension testbed.

Orchestrator Name	Devices under control	Supported Interface(s)	Responsible Partners
NFVO	Kubernetes Compute Controller	Or-Vi	UMU

Controller Services

Table 5-21 lists the controllers supported by the Spanish Demonstrator extension testbed.

Table 5-21: List of controllers supported by the Spanish Demonstrator extension testbed.

Controller Name	Devices under control	Supported Interface(s)	Responsible Partners
Kubernetes Compute Controller	Physical COTS servers and/or VMs	NIS6 interface using the Kubernetes API server	UMU
5G gNB Controller	gNBs	E2	UMU

Telemetry Services

Table 5-22 lists the telemetry services supported by the Spanish Demonstrator extension testbed.

Table 5-22: List of telemetry services supported by the Spanish Demonstrator extension testbed.

Telemetry Service Name	Target Infrastructure	Telemetry Software Used	Supported Interface(s)	Responsible Partners
Compute Telemetry service	Compute clusters	Prometheus	NIS7 for gathering compute telemetry NIS5 for exposing compute telemetry	UMU
5G Telemetry service	5GC NFs,5G gNBs and UEs	Prometheus, Proprietary software	NIS7 for gathering 5G telemetry NIS5 for exposing 5G telemetry	UMU

Use Case Services

Table 5-23 lists the NANCY services that will be used in the context of the Spanish Demonstrator extension facilities.

Table 5-23: List of NANCY services provided by the Spanish Demonstrator extension testbed.

Service Name	Objective and UC applicability	Supported Interface(s)	Responsible Partners
Cell-free access service	Provides the functionality to enable cell-free access by means of coverage extension through the PC5 link and 5G backhaul selection	NIS14, PC5-interface	UMU
Offloading service	Implements the end-to-end workflow to manage a task offloading request and its lifecycle	NIS1, NIS2, NIS5, SOL005, NIS6, NIS7	UMU
NANCY ID service	Implements the NANCY ID management methodology, which enables accessing the NANCY service by using a unique user NANCY ID.	NIS14	UMU
Migration Service	Migrates VNFs from one node to another	Or-Vi NIS3	UMU
Location Engine	Predicts the position of UE	NIS7, NIS5	IJS
Throughput estimation	Predicts UL/DL throughput	NIS7, NIS5	CERTH
Semantic Communications	Implements and shows the preprocessing of the videos transmitted by a vehicle	N/A	INNO
OBU Manager	Manages physical and virtual OBUs	E2, NIS3	UMU

5.3. NANCY CI/CD Platform

The NANCY platform leverages a wide range of open-source DevOps tools chosen for the purposes of building, testing, and deploying its various software components. Brief descriptions of the tools, as well as their cloud-based hosting environment are provided in section 5.3.1. These tools interoperate through a powerful Continuous Integration/Continuous Delivery (CI/CD) system. This system not only unifies the different software modules of NANCY but also sets up the necessary environments for both development/testing and release activities. To this end, a clear separation of the development and production (NANCY testbed/demonstrator) environments and the associated automation workflows has been made and is presented in Sections 5.3.2 and 5.3.3 through some reference automation workflows.

Detailed descriptions of the CI/CD system and its services, their configurations to meet the requirements of NANCY, as well as the associated CI/CD training materials provided to NANCY software component providers will be provided in D6.2: "NANCY Integrated System – Initial Version".

5.3.1. CI/CD hosting environment and Services

Hetzner cloud hosting infrastructure [24]: The software components implementing the CI/CD services, part of the central NANCY platform (Section 5.1), as well as the development/staging instances of other containerized NANCY components, are hosted under Hetzner cloud Linux Virtual Machines (VMs). Hetzner Cloud provides its servers in data centers located in Germany. It offers a range of useful features such as pay-as-you-go services, the capability to take VM snapshots, perform regular backups, and maintain strict data protection protocols.

NANCY GitHub organization Version Control System (VCS): GitHub has been selected as the version control system for the NANCY software, utilizing its powerful web-based platform to enable software development and version management through Git. It supports sophisticated access control mechanisms, enabling NANCY administrators to control who has viewing and/or editing permissions for a project, ensuring that sensitive parts of the software are accessible exclusively to authorized members. The NANCY private GitHub organization can be accessed at [32].

Jenkins CI server [25]: Jenkins has been selected as the Continuous Integration (CI) server within the CI/CD system for the NANCY platform. The Jenkins server for NANCY is deployed on a virtual machine supplied by Hetzner Cloud as a Docker container and can be accessed at [33]. The Jenkins service is responsible for configuring and automatically managing the CI workflows described in Section 5.3.2. Similarly to the NANCY GitHub organization, role-based access control (RBAC) has been put in place in the NANCY Jenkins server through the creation of dedicated workspaces attributed to different NANCY component providers.

Harbor private container registry [26]: Harbor has been selected as a powerful open-source registry managing container images and helm charts for NANCY. It integrates features such as RBAC, vulnerability scanning, and image signing and verification. The private NANCY Harbor registry can be found at [34].

Kubernetes [27] management and development cluster: Kubernetes is an open-source, cloud-native platform designed for automating the deployment, scaling, and operation of containerized applications. In the context of NANCY, the central Kubernetes cluster is used to host the development/testing and staging environments for NANCY containerized components, as well as the Service and Resource Orchestrators blocks of the central NANCY platform (Sections 5.1 and 2.1.3) that

will be controlling the deployments towards the demonstrator-specific Kubernetes clusters (Section 5.3.3).

Slack communication service [28]: Slack is the cloud-based communication platform that has been selected to be used for NANCY developers' exchanges. It can also be connected to the CI server (Jenkins) to get notifications from the execution of the different CI/CD pipelines (e.g., success, failure).

Security features of integration environment: A collection of security features has been incorporated into the CI/CD framework to protect the CI/CD infrastructure and services, as well as the NANCY artifacts:

- *Encryption & Secure communication over HTTPS:* Access to the CI/CD services (CI server, private container registry) is secured with Hypertext Transfer Protocol Secure (HTTPS) to protect user connections to the deployed applications. Similarly, access to deployed NANCY components in the central Kubernetes cluster is also secured over HTTPS. In this context, Let's Encrypt CA [29] has been used for the issuance of X.509 certificates offering TLS encryption.
- *User authentication and Role-based Access Control for the CI/CD services:* As described above, NANCY VCS, CI server and Private Registry are secured using user authentication and RBAC.
- *NANCY VPN:* An OpenVPN server has been set up to allow NANCY partners to access the deployed services and applications hosted on the Hetzner public cloud using the PFSense software firewall [30]. With the use of the OpenVPN server, registered external partners have the option to connect to reach these services via a private and encrypted VPN tunnel. Moreover, it is foreseen that the NANCY VPN will be used for the interconnection of the CI/CD environment with the NANCY testbeds/demonstrators.
- *Firewall protection:* A set of external firewalls have been configured within the Hetzner Cloud environment and deployed in front of the NANCY VMs infrastructure. In this context, access is restricted to authorized external IPs/subnets and ports exclusively, and is facilitated through the NANCY VPN, while permitting internal server communication among the NANCY servers.
- *SSH key-based authentication to the infrastructure:* For admin access to NANCY VM infrastructure, SSH key-based authentication is used exclusively, as a more secure means of authentication than password authentication.

5.3.2. Continuous Integration

Continuous Integration (CI) requires developers to regularly integrate their code changes into a shared repository. Each code submission is automatically tested, which helps in the early identification of errors during development. Automated builds and tests - such as unit, functional, integration and user acceptance (UA) tests - validate each integration to ensure the application remains stable as new changes are incorporated into the main branch. This process includes packaging software components into Docker container images, pushing them in a container image registry, and deploying them as containerized applications in a dedicated testing environment, which is set up under the central (management) NANCY Kubernetes cluster (Figure 5-1). The core objective of CI is to speed up the release cycle by detecting and fixing bugs early, thereby streamlining the development workflow and reducing the need for extensive rework. This enables teams to focus more on development and integration tasks.

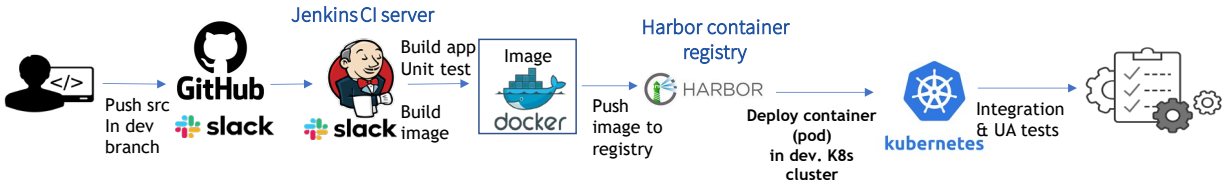

Figure 5-1: Reference CI pipeline.

5.3.3. Continuous Delivery

Continuous Delivery (CD) acts as the next phase following Continuous Integration in the software release pipeline. This stage prepares the software artifact for distribution to the end-users (NANCY testbeds/demonstrators execution environments). It is essential to keep this phase in a 'green' state, signifying that the artifact is always ready for deployment. Continuous Delivery mitigates the risks associated with software and feature releases by ensuring that every code change is released ready, after all testing verification has been performed in the CI phase. This strategy allows for smaller, more frequent updates to be delivered to the users.

In the context of NANCY, the core element of Continuous Delivery is the Service Orchestrator which, in association with the Resource Orchestrator, takes care of deploying service orders to the Kubernetes cluster related to a target NANCY demonstrator/testbed (Figure 5-2). To perform this action, the SO's NBI retrieves the deployment blueprint files describing the service orders from a corresponding NANCY GitHub repository and the deployment artifacts (container images, Kubernetes helm charts [31]) from NANCY's Harbor private registry. For deployments across the different demonstrator setups, appropriate VPN configurations will be put in place to connect the central Kubernetes management clusters with the demonstrator-specific deployment clusters.

Figure 5-2: Reference CD pipeline with Service Orchestration.

6. Conclusion

D6.1 “B-RAN and 5G End-to-end Facilities Setup “represents a significant milestone in the deployment and integration of the NANCY platform, laying a solid foundation for the Beyond 5G networks. This document has meticulously detailed the deployment view of the NANCY Reference Architecture and its integration across several testbeds in Greece, Italy, and Spain. By providing comprehensive guidelines and a structured deployment plan, this deliverable ensures a coherent and coordinated approach to setting up the NANCY platform.

6.1. Key Achievements

1. **Functional and Deployment View**: A clear and detailed functional & deployment view of the NANCY architecture has been established. This view includes all the necessary components and their interfaces, ensuring that each element's role and connectivity within the platform are well-defined.
2. **Testbed Preparation**: The document has thoroughly described the three main testbeds, specifying the software and hardware components required for the NANCY platform's operation. These testbeds will serve as the primary environments for validating the NANCY platform.
3. **Preliminary Integration**: A comprehensive preliminary integration process has been outlined, focusing on secure communications, CI/CD processes, and the detailed steps required to achieve seamless integration of the platform components.
4. **Component Assignment**: Responsibilities for each component and interface have been clearly assigned to specific partners. This allocation is essential for managing the integration effort efficiently and ensuring accountability throughout the deployment process.

6.2. Future Directions

This deliverable serves as the initial version of the integrated NANCY system. It sets the stage for further refinements and elaborations that will be documented in future deliverables, particularly D6.2. The next steps involve:

- **Validation Activities**: Detailed validation activities for various use cases will commence, primarily in M25 and beyond, as part of D6.2. These activities will ensure that the NANCY platform meets its intended objectives and operates effectively in real-world scenarios.
- **Continuous Improvement**: The deployment and integration processes outlined in this document will be continuously reviewed and improved based on feedback and results from the initial implementation phases.
- **Stakeholder Collaboration**: Ongoing collaboration among all project partners will be crucial for addressing any challenges and ensuring that the deployment and integration processes are executed smoothly.

6.3. Final Remarks

The work presented in this document is a testament to the collaborative efforts and technical expertise of the NANCY project team. By establishing a clear deployment and integration plan, this document paves the way for the successful implementation of the NANCY platform. As the project progresses, the foundations laid here will enable the team to achieve its ambitious goals and contribute significantly to the advancement of Beyond 5G networks.

Bibliography

[1] O-RAN Alliance, “O-RAN specifications”. [Online]. Available: https://www.o-ran.org/specifications

[2] OpenInfra Foundation, “OpenStack”. [Online]. Available: https://www.openstack.org/

[3] Cloud Native Computing Foundation, “Kubernetes: Production-Grade Container Orchestration”. [Online]. Available: https://kubernetes.io/

[4] ETSI, ”Open-Source MANO (OSM)”. [Online]. Available: https://osm.etsi.org/

[5] “3GPP – The Mobile Broadband Standard”. [Online]. Available: https://www.3gpp.org/.

[6] TMForum, “TMF633 Service Catalog Management API v4.0.0”, 2021. [Online]. Available: https://www.tmforum.org/resources/standard/tmf633-service-catalog-api-user-guide-v4-0-0/

[7] TMForum, “TMF641 Service Ordering Management API v4.1.1”, 2021. [Online]. Available: https://www.tmforum.org/resources/specifications/tmf641-service-ordering-management-api-user-guide-v4-1-1/

[8] TMForum, “TMF638 Service Inventory Management API v4.0.1”, 2020. [Online]. Available: https://www.tmforum.org/resources/specification/tmf638-service-inventory-api-user-guide-v4-0-0/

[9] TMForum, "TMF657 Service Quality Management API v4.0.1," 2020. [Online]. Available: https://www.tmforum.org/resources/specification/tmf657-service-quality-management-api-user-guide-v4-0/

[10] TMForum, "TMF623 SLA Management API v1.0.1," 2015. [Online]. Available: https://www.tmforum.org/resources/interface/tmf623-sla-management-api-rest-specification-r14-5-0/

[11] TMForum, “TMF632 Party Management API v5.0.0”, 2023. [Online]. Available: https://www.tmforum.org/resources/specifications/tmf632-party-management-api-rest-specification-v5-0-0/

[12] TMForum, “TMF669 Party Role Management API v5.0.0”, 2023. [Online]. Available: https://www.tmforum.org/resources/specifications/tmf669-party-role-management-api-user-guide-v5-0-0/

[13] TMForum, “TMF634 Resource Catalog Management API v4.1.0”, 2021. [Online]. Available: https://www.tmforum.org/resources/specification/tmf634-resource-catalog-management-api-user-guide-v4-1-0/

[14] TMForum, “TMF652 Resource Ordering Management API v4.0.0”, 2020. [Online]. Available: https://www.tmforum.org/resources/specification/tmf652-resource-order-management-api-user-guide-v4-0-0/

[15] TMForum, “TMF639 Resource Inventory Management API v4.0.0”, 2020, Available: https://www.tmforum.org/resources/specification/tmf639-resource-inventory-api-user-guide-v4-0/

[16] ETSI, “Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; RESTful protocols specification for the Os-Ma-nfvo Reference Point”, 2021. [Online]. Available:

https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/005/03.05.01_60/gs_nfv-sol005v030501p.pdf

[17] Open-Source MANO, «OSM SOL005 Interface», 2022. [Online]. Available: https://osm.etsi.org/gitweb/?p=osm/SOL005.git

[18] ETSI OSM NB API featuring ETSI NFV SOL005. [Online]. Available: https://forge.etsi.org/swagger/ui/?url=https%3A%2F%2Fosm.etsi.org%2Fgitweb%2F%3Fp%3Dosm%2FSOL005.git%3Ba%3Dblob_plain%3Bf%3Dosm-openapi.yaml%3Bhb%3DHEAD

[19] Linux Foundation, "Open Container Initiative". [Online]. Available: https://opencontainers.org/

[20] Hyperledger Foundation Projects, "Hyperledger Fabric". [Online]. Available: https://www.hyperledger.org/projects/fabric

[21] kube-prometheus GitHub repository. [Online]. Available: https://github.com/prometheus-operator/kube-prometheus

[22] "Hetzner Cloud". [Online].Available: https://www.hetzner.com/cloud/

[23] "Jenkins CI". [Online]. Available: https://www.jenkins.io/

[24] "Harbor Container Registry". [Online]. Available: https://goharbor.io/

[25] "Kubernetes". [Online]. Available: https://kubernetes.io/

[26] "Slack Communication Platform". [Online]. Available: https://slack.com/

[27] "Letsencrypt CA". [Online]. Available: https://letsencrypt.org/

[28] "pfSense Software Firewall". [Online]. Available: https://www.pfsense.org/

[29] "Kubernetes Helm Package Manager". [Online]. Available: https://helm.sh/

[30] "NANCY Private GitHub Organization" [Online]. Available: https://github.com/NANCY-PROJECT

[31] "NANCY Jenkins Server". [Online]. Available: https://jenkins.nancy.rid-intrasoft.eu/

[32] "Private NANCY Harbor Registry". [Online]. Available: https://harbor.nancy.rid-intrasoft.eu/