H2020 5GASP Project
Grant No. 101016448

D2.3 : The 5GASP Revised Reference Architecture and Community Components

Abstract

This deliverable is a revised version of D2.1 including new definitions and reflections to the 5GASP architecture from the project developments. This deliverable also provides final design and documentation of the community-facing materials to support interaction and experimentation with the 5GASP platform through the open repository.

Document properties

Document number	D2.3
Document title	5GASP reference certification pipeline
Document responsible	Miguel Ponce de Leon (VMware)
Document editor	Miguel Ponce de Leon (VMware); Vesselin Arnaudov (VMware) Sven van der Meer (VMware)
Editorial team	VMWare; ITAV; University of Bristol (UNIVBRIS)
Target dissemination level	PU
Status of the document	Final
Version	1.0

Document history

Revision	Date	Issued by	Description
0.1	2023-04-25	VMware	ToC
0.2	2023-07-07	UnivBris, ITAv, BLB, ININ, UoP, EANTC, VMware, DriveU, YoGoKo ORO, OdinS, Neobility, Lamda Networks	Updates to sub-sections
0.3	2023-07-14	VMware	Initial draft
0.4	2023-07-19	VMware, ORO, UnivBris, ITAv, ININ, UoP, OdinS.	Addressed review comments
1.0	2023-07-21	VMware	Final version for submission

Disclaimer

List of authors

Company	Name	Contribution
UnivBris	Adrian-Cristian Nicolaescu, Xenofon Vasilakos, Constantinos Vrontos	Contributed to Section 2.5.3 on other 5G Infrastructure Testbeds (UK), Section 3.2.3 Bristol Site, Sections 4.2 & 4.3 on User Community Portal and Developer Forum
ITAv	Rafael Direito, Eduardo Santos, Daniel Gomes, Diogo Gomes.	Contributed to Section 2.1 on Network Application E2E workflow, Section 3.1 5GASP NODS, Section 3.2.1 Aveiro Site, Section 3.2.7 Inter-site connectivity, Section 3.3 CI/CD Service, Section 4.4 Experimental API Service.
BLB	Yevgeniya Sulema	Contributed to Section 4.2 User community interaction portal
ININ	Luka Korsic Rudolf Susnik	Contributed to Section 2.4 on Network Application vertical specific requirements, and Section 3.2.4 Ljublijana Site
UoP	Kostis Trantzas, Christos Tranoris, Ioannis Chatzis	Contributed to Section 2.1 on Network Application E2E workflow, Section 2.2 Commonality in infrastructure architecture and capabilities, Section 2.3 External Interfaces, Section 3.1 5GASP NODS update, and Section 3.2.2 Patras Site
EANTC	Dirk Hetzer	Contributed to Section 2.5.3 on other 5G Infrastructure Testbeds (DE), and Section 4.1 5GASP Marketplace
VMware	Miguel Ponce de Leon, Vesselin Arnaudov, Sven van der Meer	As docucment editors contributed to the Abstract, Introduction, Objectives of the Document - Document Structure, Section 2.5 Commonality across related projects, Section 5 on Guidelines for Future Experimentation and the Conclusion.
DriveU.auto	Eli Shapira	Contributed to Section 2.4 on Network Application vertical specific requirements and document reviewer
YoGoKo	Thierry Ernst Yakub M. AbuAlhoul	Contributed to Section 2.4 on Network Application vertical specific requirements, Section 5 Guidelines for Future Experimentation and document reviewer
ORO	Elena-Madalina Oproiu, Ioan Constantin	Contributed to Section 2.2 “Commonality in infrastructure architecture and capabilities”, Section 3.2.6 Bucharest Site and document reviewers
OdinS	Ana Hermosilla, Jorge Gallego-Madrid	Contributed to Section 2.4 on Network Application vertical specific requirements, and Section 3.2.5 Murcia site
Neobility	Andrei Radulescu	Contributed to Section 2.4 on Network Application vertical specific requirements and Section 5 Guidelines for Future Experimentation.
Lamda Networks	Leonidas Lymberopoulos	Contributed to Section 2.4 on Network Application vertical specific requirements and Section 5 Guidelines for Future Experimentation.

Contents

List of Figures

List of Tables

Acronyms

3GPP	3rd Generation Partnership Project
5GASP-C	5GASP Certification
API	Application Programming Interface
CI/CD	Continues Integration Continuous Development
CRUD	Create, Read, Update and Delete
ETSI	European Telecommunications Standards Institute
KPI	Key Performance Indicator
LTR	Local Test Repository
NEST	Network Slice Template
NFV	Network Function Virtualization
NODS	Network Application Onboarding and Deployment Services
NS	Network Service
NSD	Network Service Descriptor
OSM	Open Source MANO
TRVD	Test Results Visualization Dashboard
VNF	Virtualized Network Function
YANG	Yet Another Next Generation

Definitions

This document contains specific terms to identify elements and functions that are considered to be mandatory, strongly recommended or optional. These terms have been adopted for use similar to that in IETF RFC2119 and have the following definitions:

- **MUST** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **MUST NOT** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- **SHOULD** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY** This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to inter-operate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to inter-operate with another implementation which does not include the option (except, of course, for the feature the option provides).

1 Introduction

1.1 Objectives of this document

The main objectives of this deliverable is to document a revised version of 5GASP D2.1 [1], which is including new definitions and reflections to the 5GASP architecture from the projects developments in to the creation of a common 5G Network Application platform.

This deliverable does not replace the precursor document, 5GASP D2.1 [1], but rather complements it with information that corresponds to the progress made in Tasks T2.1 and across the whole 5GASP work programme since the delivery of 5GASP D2.1 [1] in December 2021. However wherever specified, the contents in this document shall take precedence over those in D2.1 [1].

Therefore this document shall report on:

- A workflow process for the automated transformation of vertical applications to interoperable 5G/NFV artefacts.
- The definition of an architecture that supports the 5GASP open repository and knowledge base.
- The definition of components of the 5GASP infrastructure that show that the platform is open, interoperable, extensible and standard.
- The definition of the 5GASP experimentation infrastructure that supports i) standardized 5G/NFV interfaces, ii) multi-domain scenarios, iii) seamless integration of 5G/NFV technologies, iv) automated transformations of 5G/NFV models.

This deliverable also provides the final design and documentation of the community-facing materials to support interaction and experimentation with the 5GASP platform through the open repository.

There will be an update on the 5GASP certification process for Network Applications, with an aim that this report can be used by the Network Application developers as a supporting guide throughout the certification and deployment process.

Figure 1 High-level workflow of a Network Application through 5GASP-C program

1.2 Introduction to the 5GASP Network Application certification (5GASP-C)

The 5GASP Certification Process aims to provide a meaningful way and method to measure the ability of a 5G Network Application to perform with the expected quality and performance standards, inherent both from the application's scope and the target deployment environment.

On the process side, the certification testing is thoroughly defined in D6.2 [2], illustrating an End-to-End (E2E) workflow along with the employed stakeholders. On the business side, driven by the effort to investigate and incorporate certification aspects with significant technical scope and match market requirements, the project has relied on the definitions updated in Subsection 2.1 of 5GASP D5.4 [3] to steer the development of 5GASP's Certification Process.

From the list of 19 Network Applications certification definitions in 5GASP D5.4, it is clear that all Network Applications must address definitions 4 and 19 to obtain the 5GASP's certification.

Definition 4 states that any Network Application should follow the NFV model, which will be validated by statically analyzing the syntax, semantics, and references of the NSDs and VNFDs uploaded to the 5GASP framework. These aspects are validated during the onboarding of a Network Application to the 5GASP Network Application Onboarding and Deployment Service (NODS). If the Network Application does not comply with Definition 4, it will not be orchestrated in one of the 5GASP's testbeds.

Definition 19, states that a Network Application should follow relevant 3GPP security definitions and recommendations. All Network Applications must be compliant with this definition, proving they are secure and will not pose any risk to the operators that choose to on-board such Network Applications.

To certify a Network Application, 5GASP has created a vast collection of tests as recorded in D5.4. Given the different scopes of the certification definitions, 5GASP has opted to define a multi-dimensional certification process. Thus, several testing scopes were considered to address the different certification methodologies. Also, the existence of different testing scopes heavily influences 5GASP's certification process since each Network Application will be given a certification grade according to each testing scope.

Based on the previously presented certification definitions D5.4 covers the following testing scopes/axis: (i) 5G Readiness Testing, (ii) Security & Privacy Testing, (iii) Performance & Scalability Testing, and (iv) Availability & Continuity Testing. Given that all Network Applications must comply with definitions 4 and 19, when considering these testing scopes, we can affirm that all Network Applications must fulfil the 5G Readiness and the Security & Privacy testing scopes.

Once the Network Application end-to-end workflow, as described in Section 2.1, is followed then the mandatory definitions can be said to be are addressed, it is up to Network Application developers and experimenters to determine if their solutions are compliant with other definitions. These additional formulations are considered as certification expanded criteria and comprise a set of optional definitions that can be considered in the certification process and be later reflected in the 5GASP certification of the Network Application.

Therefore with a Network Application developer leveraging the 5GASP workflows, infrastructure, and community portal material they can attain 5GASP Network Application certification.

1.3 Document organisation

This document is organised into five different sections. Starting with an introduction, that focuses on providing an overview of the 5GASP Network Application certification process. Section 2 gives detail on the 5GASP workflow and the supporting infrastructure architecture, highlighting the commonality of capabilities achieved across 5GASP testbeds along with commonality across related external testing facilities.

Section 3 provides a summary of updates to internally hosted and externally facing components of the 5GASP platform. Section 4 provides an update on the community facing material of 5GASP for Network Application developers and finally in Section 5 some guidelines on future experimentation is provided.

2 5GASP Infrastructure Architecture (Update)

The main objective of 5GASP, i.e. to apprehend verticals' and experimenters' requirements along with the provision of seamless on-boarding, deployment, and testing processes through an interconnected reference ecosystem of experimental facilities, was captured and facilitated by the high-level system architecture as illustrated in Figure 2.

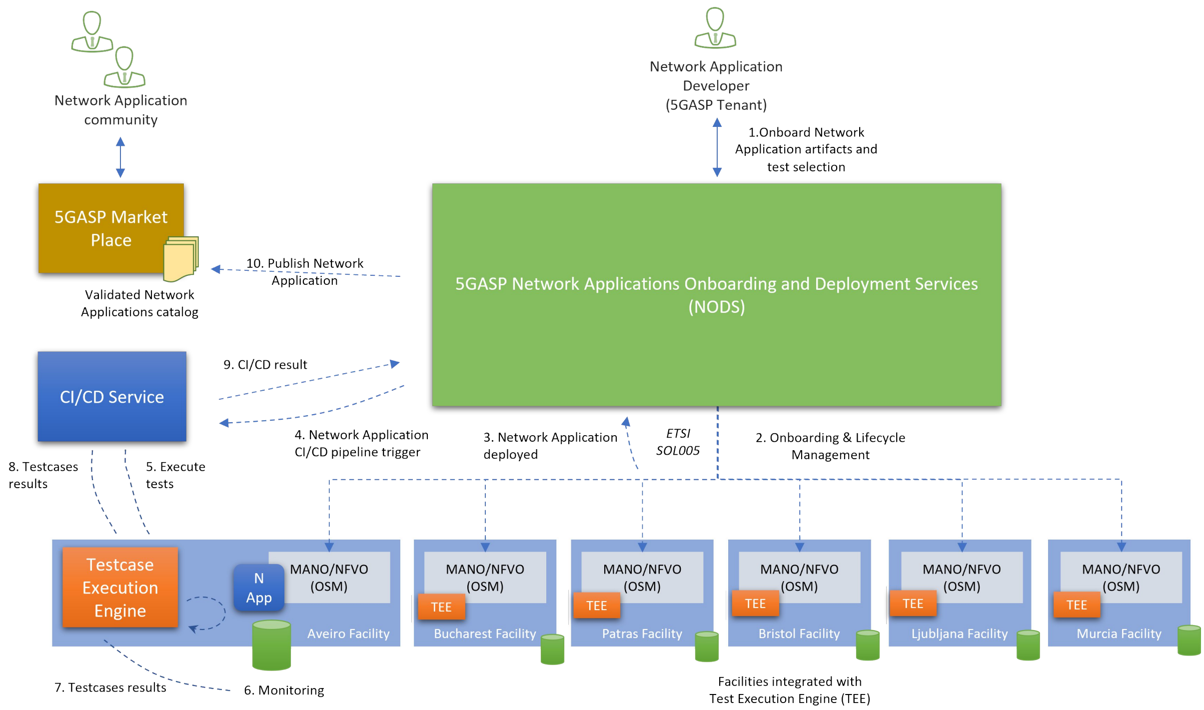

Figure 2 5GASP Architectural Workflow

Specifically, a single entry point to the 5GASP platform is provided in the form of a user-friendly portal solution that supports the uploading of Network Application's NFV artefacts, the onboarding of the latter to relevant experimental facilities, and the selection of predefined test suites or the design of custom ones to be executed against the onboarded Network Application (step 1). The entity that encapsulates the aforementioned management interface is referred to as 5GASP Network Applications Onboarding and Deployment Services (NODS). NODS, aside from an entry point to the 5GASP system, provides a Service Order Management (SOM) service and offers its own Service and Network Orchestrator that coordinates actions with the underlying facilities or other NFV/3GPP compliant systems. Following the capture of the Network Application's deployment order, NODS is charged with the fulfilment of the latter employing its internal services, and eventually with the supervision of its deployment over the multi-domain NFV fabric, comprising of the 5GASP facilities (step 2). Should this procedure be successfully conducted (step 3), NODS then triggers the testing pipeline, which is accountable for the Network Application's validation and certification processes. Accordingly, the flow is committed to the respective entity, namely the CI/CD Service (step 4). Eventually, after a successful CI/CD pipeline execution, the flow is reverted to NODS (steps 5-9), which i) grants access to the CI/CD results, along with the potentially applicable certification based on various criteria and rankings, and ii) in the case of a certification acquisition the Network Application is published in the 5GASP Market Place, therefore making it publicly available (step 10).

The above architecture, interactions, and workflows are meticulously described in previous deliverables, i.e. D2.1 [1], D3.1 [4], D3.2 [5], and are briefly presented in this abstract shape for the sake of the document's integrity. Throughout the project's lifetime, enhancements were made to the initial representation to fulfil the ever-changing requirements of the growing community, which are depicted in Figure 3. Particularly, these adaptations primarily affected the 5GASP facilities enriching them with extended monitoring capabilities to further complement the test process results but also offering extensive testing ability towards 5G awareness of the Network Applications under test. Following, the next section presents the aforementioned endeavours in detail.

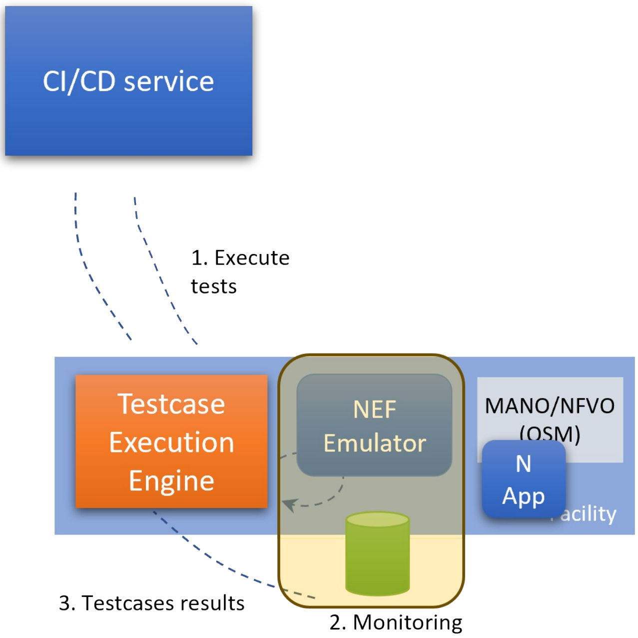

Figure 3 5GASP Facility enhancements

2.1 5GASP Network Application End-to-End Workflow

As illustrated in the introductory section 2, the overall 5GASP workflow cycle comprises of the Network Application onboarding, deployment, testing, and ultimately, its validation. This section aims to distinguish between these various phases and to provide a more profound insight through the respective workflows.

The 5GASP cycle begins with the Network Application onboarding, as seen in Figure 4. The Network Application Developer interacts with the 5GASP Network Application Onboarding and Deployment Services (NODS) and the respective 5GASP Facilities to onboard its Network Application within the 5GASP environment. The workflow begins with the developer selecting the appropriate hosting Network Slice and uploading the Virtual Network Function (VNF) packages to the 5GASP NODS, which subsequently onboard them into the 5GASP Facility.

Confirmation of successful VNF onboarding is received, and then the developer uploads the Network Service (NS) packages, which are also onboarded into the 5GASP Facility. Once the NS packages are successfully onboarded, the developer can either choose an existing Test Suite or create a new one by uploading testing artifacts to the 5GASP NODS. The chosen or newly created Test Suite is reviewed and confirmed by the developer, resulting in the creation of the "Triplet" comprising the Network Application, Network Slice, and Test Suite. Finally, the developer receives confirmation of the successful creation of the "Triplet", signifying that the Network Application is ready for deployment and testing within the 5GASP environment.

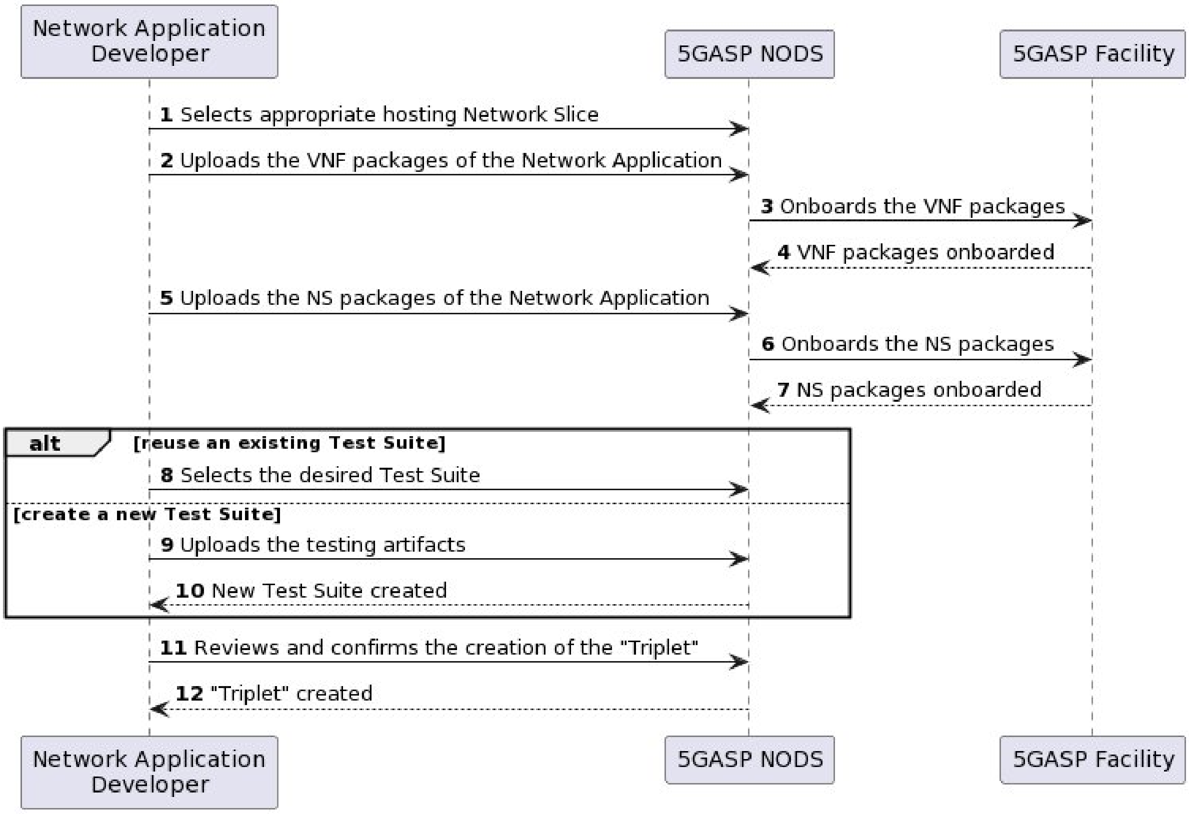

Figure 4 Network Application onboarding workflow

Hereafter, the lifecycle continues with the Network Application deployment and testing that eventually leads to its validation and publishing at the 5GASP Marketplace, as depicted in Figure 5. For this to happen, the Network Application Developer interacts with the 5GASP NODS, which respectively delegates the appropriate actions to the 5GASP Service Orchestrator, 5GASP Facility, CI/CD Manager, 5GASP Certification Entity, and 5GASP Marketplace to deploy and certify a Network Application within the 5GASP environment. The workflow proceeds as follows: The developer places an order for the desired "triplet" and receives an acknowledgement from the 5GASP NODS. The NODS forwards the acknowledged order to the Service Orchestrator, which then proceeds to instantiate the hosting Network Slice in the 5GASP Facility. Once the Slice is instantiated, the Orchestrator deploys the Network Application within the Slice. The Orchestrator notifies the NODS that the Slice and Network Application are ready for use. Then, the NODS triggers the test phase, involving the CI/CD Manager. Test results are sent back to the NODS, which grants access to the developer. Subsequently, the NODS initiates the certification process employing the 5GASP Certification

Entity. The Certification Entity requests the test results from the CI/CD Manager, and if the certification criteria are met, it instructs the 5GASP Marketplace to publish the certified Network Application. The Certification Entity then shares the certification results with the NODS, which therefore grants access to them for the developer.

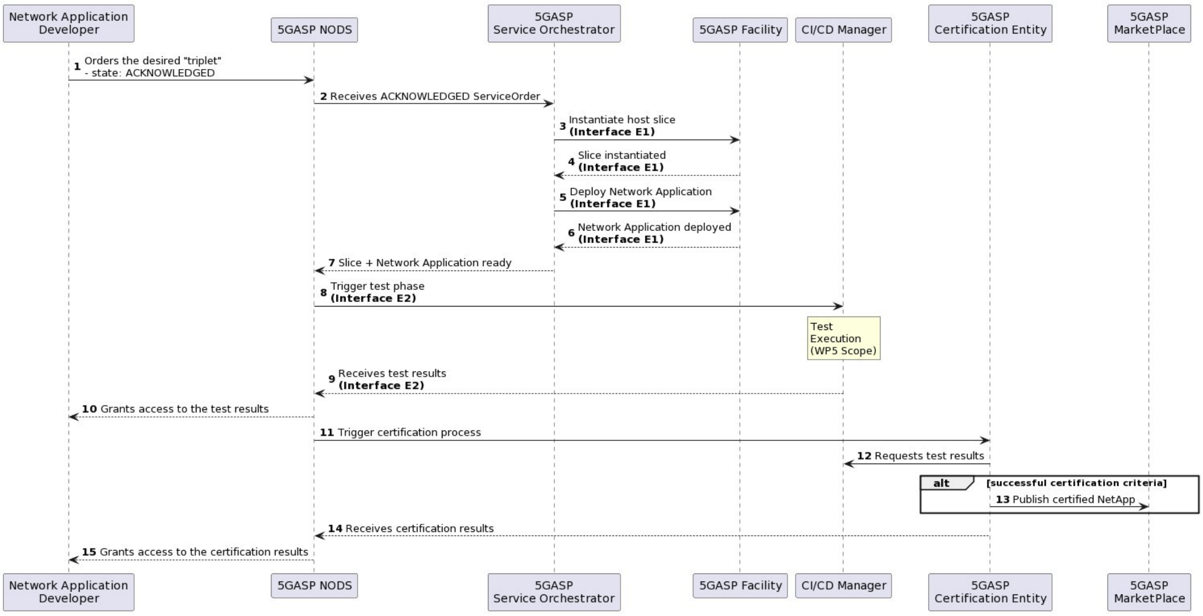

Figure 5 Network Application deployment, testing, and validation workflow

To conclude, the overall 5GASP cycle completes through the final step, i.e. the validation process. The validation process relies on the initially onboarded Testing Artefacts, such as the Testing Descriptor and the onboarded Tests, described in Section 4.4.2.

After the triggering of the CI/CD Manager by the NODS, the Manager will obtain the Testing Descriptor and use it to create a Testing Pipeline, which will then be shipped to the Testing Agents that live in the same testbed as the one where the Network Application was deployed. Such Testing Pipeline will be responsible for gathering both pre-defined and developer-defined tests, execute them, collect their outcomes and results, and return them to the CI/CD Manager. Regarding the tests, the pre-defined ones already exist in 5GASP's ecosystem and are made available to all Network Application developers, as they can be performed on any Network Application. These tests are stored in the testbeds' Local Testing Repositories, from where they are collected by the CI/CD Agents. Contrastingly, the developer-defined tests are specific to a Network Application and can be used to validate the intended behavior of the Application, and thus must be onboarded by the developers.

After the CI/CD Manager receives the test results, it will parse the result files, extracting meaningful information, and create a Test Report. This Report entails all tests that were performed on a Network Application, along with the test results and logs. Once created, the Report will be available through the Test Results Visualization Dashboard, from where the developers may gather it. Figure 6 presents the overall workflow of the validation process.

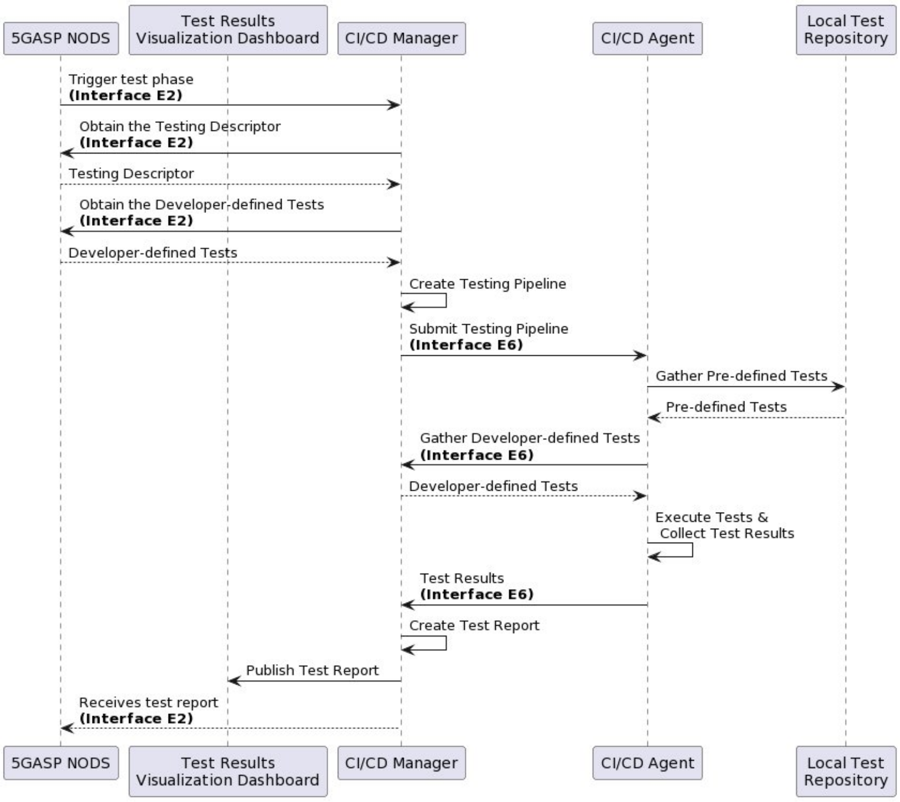

Figure 6 Network Application Validation Workflow

2.2 Commonality in 5GASP Infrastructure Architectures and Capabilities (Testbeds)

One of the key requirements within the scope of 5GASP project is to establish a common platform of a seamless unified infrastructure comprising of several testbeds. Though, to ensure the performance, availability, and reliability of the underlying resources, during the 5GASP experimentation cycle, a monitoring platform plays a crucial role. Again, leveraging the unified solution approach, the envisaged monitoring platform can provide valuable insights about the performance of the employed infrastructure, throughout the overall 5GASP lifecycle. Thus, enabling the developer to observe its application in the context of a live and ever-changing system.

To achieve this goal, we have proposed the adoption of the widely used Prometheus [6]/Grafana [7] stack as the common monitoring platform. Prometheus, being an open-source software that excels at collecting and storing time-series data that enables efficient querying and alerting of various metrics, was already employed within some 5GASP testbeds to gather metrics from various infrastructure nodes, so it was elected as the perfect candidate for data aggregation. Grafana, on the other hand, provides a powerful and user-friendly interface to create and expose interactive dashboards and visualizations based on the data collected by Prometheus. The seamless integration between the latter, along with the capability for each testbed to create its own dashboards to host its own heterogeneous data from various monitoring nodes under a common platform and the aptness of a widely spread data presentation stack, appointed Grafana as the elected visualization tool.

By utilizing the aforementioned Prometheus stack, we can establish a centralized monitoring solution that enables seamless integration with different components of the underlying

5GASP infrastructure towards a federated approach, as seen in Figure 7. This unified approach ensures consistent monitoring practices across the infrastructure, thereby facilitating effective troubleshooting and performance optimization of the Network Application undergoing the 5GASP CI/CD lifecycle.

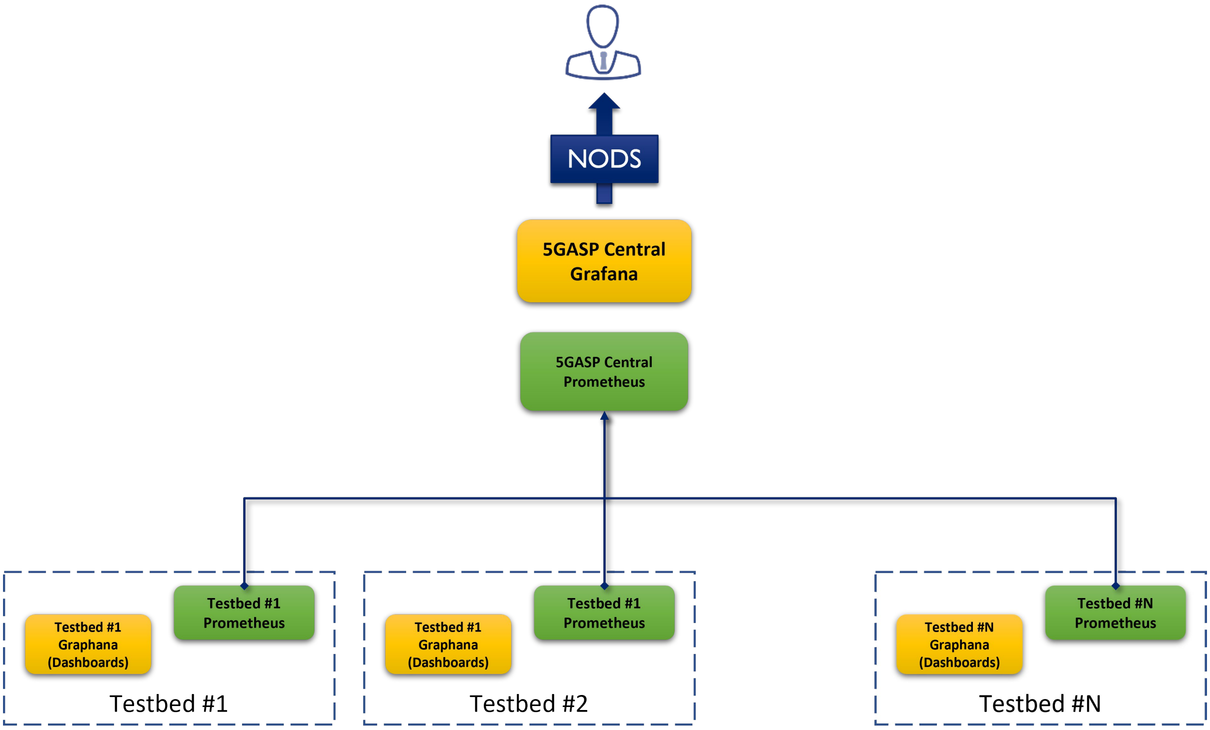

Figure 7 5GASP Federated Prometheus approach

Furthermore, the common monitoring platform will expose metrics through a unified portal, i.e. 5GASP Central Grafana, accessible to the respective stakeholders. This portal will serve as a central point for visualizing and analysing the collected metrics, enabling real-time monitoring throughout the experiment lifecycle. Through the common portal, the developer can gain insights into the behaviour and performance of the infrastructure, in relation with the Network Application functioning, thus enabling efficient resource utilization.

Throughout the overall research, it was made obvious that 5GASP would need to support programmable interaction towards a 5G System component of the underlying infrastructure, so as to support the 5G readiness tests of external Network Applications. Specifically, the Network Exposure Function (NEF) is a key component within the 5G System that facilitates the exposure of network services and functions to external entities, such as third-party applications and services. Given that the state-of-the-art implementations of 5G Cores hosted within the project do not provide a fully functioning NEF, and the ones that do foster extensive inconsistencies among their implementations, a standards-based, reprogrammable, and deterministic solution was found under the open-source project of NEF Emulator [8]. It was developed within the scope of another ICT-41 Project, i.e. EVOLVED-5G, and was further extended by 5GASP. The NEF Emulator offered the standardized 3GPP NEF APIs in a configurable emulated environment, where specific simulation configurations can be defined (e.g. number and type of UEs, the position of gNBs, etc), thus laying the required foundation for the respective Network Applications to be tested against the interaction with the emulated exposed NEF APIs.

2.3 5GASP External Interfaces & 5G Awareness

As part of the overall research on Network Applications, and to further enable 5G-awareness testing of the latter, 5GASP investigated the proposed ways of the industry in terms of interaction with the 5G System. To that matter, 3GPP [9] has identified two interfaces, as illustrated in Figure 8, namely the N33 and N5 interfaces. The provided figure illustrates the potential interaction of a 5G Media Streaming Application with the 5G System but can be expanded to any Network Application regardless of the vertical use case. Specifically, a Network Application may communicate with 5G Core functions via the Network Exposure Function (NEF) using N33 and the Policy Control Function (PCF) using N5, respectively.

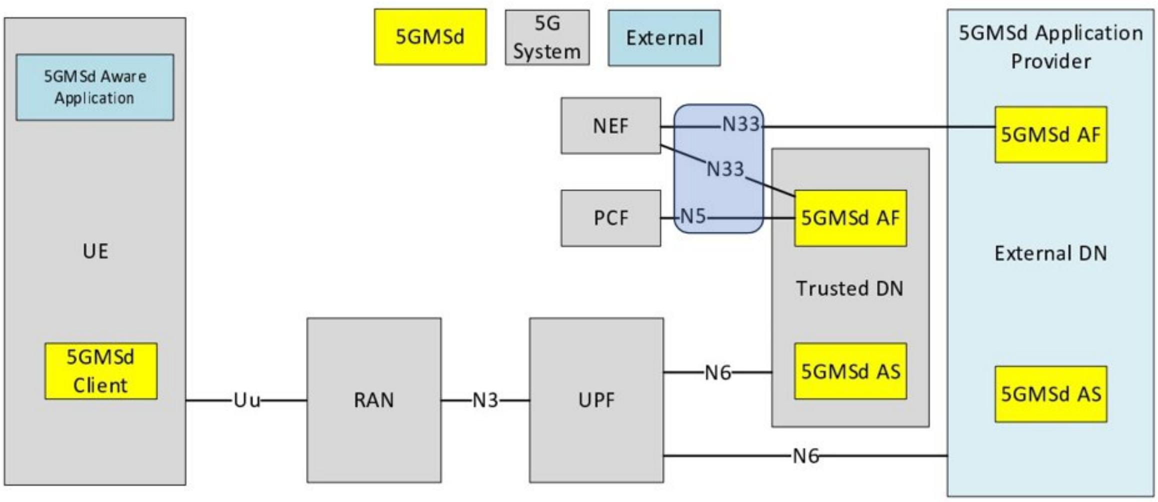

Figure 8 5G Downlink Media Streaming with 5G System [9]

To that extent, 3GPP envisions two discrete categories of Network Applications with distinct levels of access to the 5G System, i.e. the Trusted and the External. The former are considered as a structural part of the overall 5G System, as they are trusted by the Network Provided, thus able to interact directly with PCF to enforce policy changes to the overall System using N5. Whereas the latter can also communicate with the 5G System externally but acquire limited access to the system's resources with respect to policy enforcement. They are mainly focused on the system's events generation and capturing, e.g. UE mobility, QoS degradation, etc. Within the context of 5GASP, the Network Applications provided by the project's stakeholders are considered strictly external, as they should behave in an isolated manner in regard to the hosting 5G System, but they would simultaneously like to acquire 5G related events and metrics.

2.4 Conforming to 5GASP Network Application vertical-specific requirements

The development and further deployment of the eleven proposed Network Applications over the 5GASP platform led to the definition of some vertical-specific requirements in terms of hardware and functionality, which led into some changes to be applied into the architecture. Some of these needs identified in a joint work between the network application developers and the testbed owners were defined in D3.2 [5] as hardware requirements, as it is shown in Table 1. This table shows the requirements that the different network applications needed to operate translated in specific hardware necessities to be present in the testbeds to support the proper functioning of the network applications. As it can be seen, the testbed owners showed there how they can accommodate the different network applications and from that list, several collaborations followed to host specific network applications in certain testbeds with full-hardware support. The requirements marked with a (*) (ids = 9, 14, 15) became obsoleted since the submission of D3.2, as the Network Applications that requested them changed their design, thus those requirements are no longer required.

Id	**Requirement**	**Network Applications**	**ITAv (PT)**	**UoP (GR)**	**ORO (RO)**	**OdinS (SP)**	**ININ (SL)**	**UNIVBRIS(GB)**
1	UE with specs similar to Raspberry Pi4 - Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz - 1GB to 8GB LPDDR4-3200 SDRAM - 8GB storage - 5G Connectivity	All	Yes	No	Yes	Yes	Yes	No
1.a	Vehicular vertical specific - 802.11p/ITS-G5 or C-V2X connectivity - Geolocalization - C-ITS software stack	1,2,3,4	No	No	No	Yes	No	No
1.b	PPDR vertical specific - K8S installation - Camera module	11	Partial	Yes	No	Yes	Yes	Partial
1.c	PPDR vertical specific - GPU module	5,6	In Progress	No	No	No	No	Yes
1.d	Android smartphone with 5G connectivity	7,10	Yes	Yes	Yes	Yes	Yes	Yes

2	USB3 5G SA modems that can be connected to an UE if no built-in connectivity	All	Yes, 3. d	No	Yes	Yes	Yes. Industrial linux-based PC with integrated 5G SA capable modem using in-house developed M.2 board.	Yes. In-house built 5G CPE devices on Linux. Support for 5G SA, WiFi AP and 2xGbE.
3	802.11p/ITS-G5 modems that can be connected to an UE if no built-in connectivity	1,2,3,4	No	No	Yes	Yes	No	No
4	C-V2X modems that can be connected to an UE if no built-in connectivity	1,2,3,4	No	No	No	No	No	No
5	Vehicle available (usage slots scheduled with testbed owners) to deploy vehicular Network Applications under mobility conditions. It would host the physical OBU.	1,2,3,4	If needed	No	N/A	Yes	No	Shared with other groups. Possibly depending on car state and availability.
6	eNB with 4G/3G data support	2	No	Yes, 4G	Yes, 4G	Yes, 4G	Yes, 4G	Yes
7	UEs with 4G/3G data support	2	Yes	Yes	Yes	Yes, 4G	Yes	Yes
8	High number of instantiated containers	3	Under study	Yes	Yes	Under study	Under study	Yes
9	*Interaction with the SDN controller of the domains to be able to react to the domain changes. Although this is the initial approach that was considered when developing the initial PoC service, other options can be explored to do this, such as a dynamic allocation of a network slice. This is a WIP by OdinS, further details will be given. (*)*	*4*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*No/N/A*
10	MEC/Cloud with GPU resources available for containers or VNFs	5,6	Just RTX GPUs, but Jetsons may be acquired, if needed	No	Yes (4 x nVIDIA Tesla T4)	WIP: Integrating GPUs with VIMs	No	Yes
11	Radio monitoring data from the UE or the RAN available	7	No	Yes (data from RAN)	Yes	Yes	Yes	Not readily available. Need integration..

12	Radio access points with edge compute nodes 1:1	7	Under study	Under study	No	Under study	Yes	Yes
13	Modified RO's OSM10 to allow selecting flavors with extra specs	9	No, but we can try to implement it if needed	No	Yes	No	Yes	Yes
14	*Openstack flavor with extra specs (PCI PASSTHROUGH:ALIAS, HW:CPU_SOCKETS, HW:CPU_CORES, HW:CPU_THREADS) (*)*	*9*	*N/A*	*N/A*	*N/A*	*N/A*	*Yes*	*N/A*
15	*Openstack host with SDR card exposed to OSM (*)*	*9*	*N/A*	*N/A*	*N/A*	*N/A*	*Yes*	*N/A*
16	*Kubernetes host with SDR card exposed to OSM*	*9*	*No*	*No*	*N/A*	*No*	*Yes*	*N/A*
17	Wide area of coverage for vehicular scenario testing, not just indoor or near the gNB	10	Yes	No	Yes, NSA	No	No	More radios are required

Table 1: Mapping of hardware requirements, Network Applications and testbeds (from D3.2)

With regards to the specific needs requested from each one of the verticals, several enhancements have been done to accommodate certain requirements that characterise these verticals:

Automotive Network Applications:

- Tuned to improve the performance of 5G handovers in vehicular scenarios where the car is moving and switching among cells quickly.The vehicular network applications were adapted to retrieve specific vehicular metrics to be used by the network applications of the verticals.
- Network slices with guaranteed service were created and deployed so that the automotive applications with critical-mission needs could make use of them.
- The RAN configuration of the different gNBs was configured to optimize the connectivity with moving UEs.
- The 5G modems were tuned to increase their performance in scenarios with disconnections due to lack of coverage in shadowed areas.
  Equipment to assemble vehicles capable of hosting the automotive network applications was acquired and put into effect in mobility demonstrations.

PPDR Network Applications:

- The infrastructure was enhanced to allow using IOPS in both modes:
  - Normal operation (two physical nodes, one acting as IOPS gNB and other one providing a “public” core)
  - Disaster operation (one physical node acting as IOPS gNB and IOPS core)
- Automated scenarios based on ROBOT framework allowing switching between “Normal” operation and “Disaster” operation

- Two network slices are available:
    - SST 1, SD 0 (eMBB) – providing maximum available bandwidth to end-users (e.g. utilize this slice when using bandwidth intensive applications such as video in PPDR)
    - SST 3, SD 10 (mMTC) – limited bandwidth via CBR/GBR policies (utilize this slice for scenarios where applications transport minimum traffic, e.g. environmental sensing)

Cross-Vertical Network Applications:

- New interaction APIs were developed for NEF interaction, both on the emulator and the NApp;
- Further, some modifications were made in some Network Applications, i.e., EMHO (NApp 7), to make it container-deployable and thus take advantage of its benefits, as:
    - The NApp was "*dockerised*" and provided with all the source code data in-container, in order to account for privacy and security threats.
    - The service was containerised within a helm chart, and using the 5GASP harbor deployed in 5GASP to store the image.

Additionally, during the second year of the project it was detected a crucial need to support the operation of the 5GASP platform in the different verticals: a common monitoring platform. Aside from the extensive feedback provided by the 5GASP platform after the deployment, testing, evaluation and certification of the network applications, it is necessary to provide to the experimenters real-time monitoring of what is happening in the testbed where their application is being validated. In this way, the 5GASP consortium, specially the testbed owners, made the commitment to develop a common monitoring platform to give the developers and experimenters this additional information. Several common KPIs related to the different verticals were defined and in less than one year, the monitoring solution was deployed and started to supply this data. Its functioning and usefulness was showcased during the intermediate review of the project hosted in Murcia (Spain) in M30, by providing real-time monitoring of the vehicular and PPDR demos.

In this way, the infrastructure of the testbeds participating in the project has evolved significantly in the last months to accommodate the necessities required by the network applications and by the verticals. Further details of these upgrades are detailed in Section 3.2.

2.5 Commonality across related projects

In order to identify commonality across ICT-41 testbed architectures an extensive review of all architectures under the programme was undertaken, and collaborative meetings were hosted with technical leads of architecture work across ICT-41 projects was completed. The following sections highlight outcomes from this exercise.

2.5.1 Automotive Infrastructure Architectures

There are two distinctive projects in the ICT-41 programme that cover the automotive industry, VITAL-5G and 5G-IANA.

VITAL-5G [10] offers a set of tools and functionalities to facilitate the design, development, provisioning and experimental validation of network applications and end-to-end vertical services for the Transport & Logistics (T&L) sector. To this end VITAL-5G experimentation services have been made available not only for the partners of the VITAL-5G consortium, but also for 3rd parties, who aim to simplify and speed up the creation and delivery of new T&L services, promoting the exchange, re-usage, extension and composition of Network Applications distributed by different vendors and software providers.

Through the VITAL-5G deliverable D1.3 [11] a full description of the specification of the VITAL-5G system is given, along with updates on changes and new features introduced since the initial design was defined in D1.2 [12]. Importantly this VITAL-5G D1.3 integrates suggestions received from experimenters executing trials on the VITAL-5G system, as well as 3rd party partner feedback on using the platform to deploy and test their own network applications or to build new services re-using the Network Applications originally available in the VITAL-5G catalogue.

The structuring of the VITAL-5G system in a centralized and unified VITAL-5G platform (the red box) that operates over three testbeds in Athens, Antwerp and Galati (the three brownish boxes at the bottom of the picture), each of them integrating T&L facilities with 5G network infrastructures.

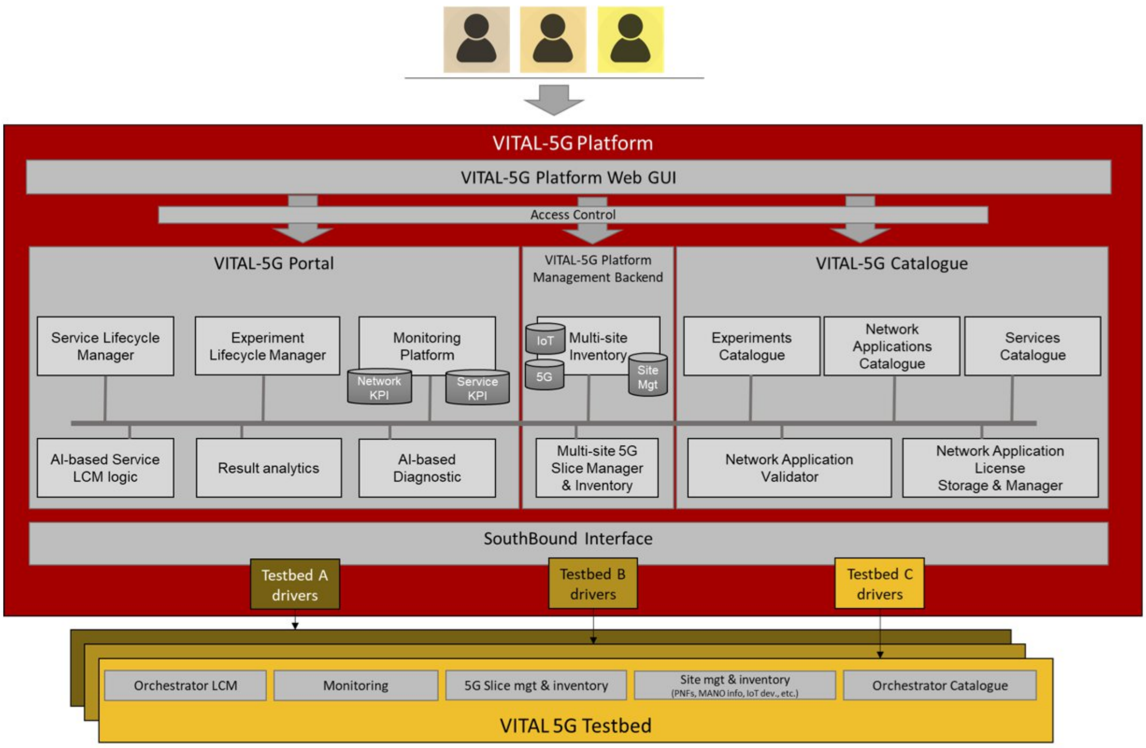

Figure 9 VITAL5G Functional Architecture

The VITAL-5G Platform is structured in two main components, i.e., the VITAL-5G Portal back end and the VITAL-5G Catalogue, each of them including a number of functional elements and supported by a set of management back end services.

The VITAL-5G platform functional elements provide interfaces to expose their functionalities, which can be consumed by all the other elements, and it follows a Service Based Architecture pattern. The VITAL-5G Catalogue and Portal back end north-bound interfaces (NBI) allow the VITAL-5G users to securely access the authorized VITAL-5G services in a programmable manner, mostly via REST APIs.

On top of the VITAL-5G Platform programmable interfaces, a centralized web-based GUI offers an additional graphical Portal with dedicated tools, designed to simplify a users' manual interaction with the VITAL-5G Platform, for both VITAL-5G Portal and Catalogue services.

On its south-bound interface (SBI), the VITAL-5G Platform interacts with the three VITAL-5G testbeds. In particular, this interface mediates the interaction with the following components of VITAL-5G testbeds:

- the management system of 5G networks (5G Slice management and inventory);
- the NFV MANO platforms for onboarding and provisioning/management of Network Applications and vertical services (Orchestrator catalogue and Orchestrator Lifecycle Manager – LCM);
- the monitoring platforms for collection, storage and exposure of metrics and KPIs related to 5G network, edge/cloud computing infrastructure and vertical applications or services (Monitoring).

The VITAL-5G Platform can also interact with additional management platforms and inventories to retrieve dynamically information about the hardware, IoT devices, physical functions, system settings, etc., configured in the testbed and its T&L facility.

The southbound interface of the VITAL-5G Platform is designed with a modular and plugin-based approach that deals with the diversity of capabilities and APIs related to the three testbeds while exposing a uniform layer towards the internal elements of the VITAL-5G Platform

Section 5.3.2 of VITAL-5G D1.3 [11] provides a listed table of the VITAL-5G Platform functional elements, describing their functionalities and identifying their NBI and/or SBI where relevant.

For the purpose of finding common ground between 5GASP – VITAL-5G, technical leads from both projects undertook an interactive session (May 2023) using this high-level view of the features supported by each component in the global architecture VITAL-5G as a way to place a foundation on the workflow and component commonality between both project architectures.

From this exercise a number of common components were identified, such as the Network Applications Catalogue, Experiment Catalogue and Network Application Validator from the VITAL-5G Catalogue which relate directly to the 5GASP Network App Onboarding and Deployment Services (NODS).

There was also one component, the Network Application License Storage & Manager (VITAL-5G) that was found to be a possible interesting addition to the 5GASP architecture. This component in VITAL-5G provides a storage for the licenses associated to the Network Application and assists with the on-boarding of license information to the VITAL-5G platform. Such a component in the 5GASP NODS would be a excellent addition.

5G-IANA [13] provides an open and flexible experimentation platform to third-parties developers that want to develop new 5G-based services devoted to the Automotive vertical industry. The project has developed an Automotive Open Experimentation Platform (AOEP) which is an easy-to-use experimentation environment that can facilitate the launch of new 5G services that actively address the configuration of the 5G network (e.g., network slicing, edge resources, etc.) with the objective to verify if the current 5G implementation can adequately satisfy the highly demanding performance requirements of the Automotive services.

Through the 5G-IANA deliverable D2.1 [14] a description of the two main layers of the AOEP architecture are presented, namely the Network Application Orchestration and Development (NOD) layer and the Slice Management and Resource Orchestration (SMRO) layer. The first layer offers the functionalities to design, model, and provision a Vertical Service/Network Application, while the Slice Management and Resource Orchestration layer is in charge of allocating and managing the 5G Network Slices and the compute resources of the 5G-IANA infrastructure. Other layers of the 5G-IANA AOEP are the Distributed Machine Learning (DML) Orchestration layer, which manages DML Vertical Services/Network Applications, the Monitoring and Analytics layer, and the Distributed Data Collection layer.

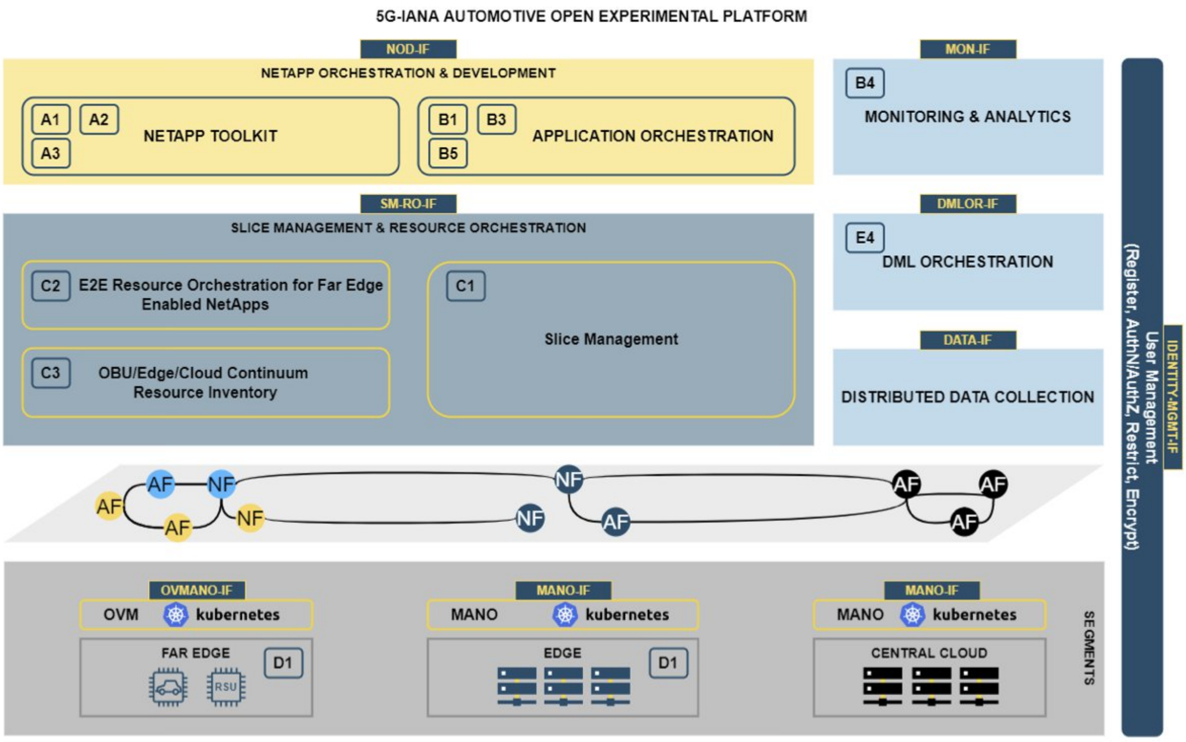

Figure 10 5G-IANA Architecture

The 5G-IANA AOEP integrates the ability to manage and orchestrate Services/Network Applications across an extended compute continuum and comprises of multiple interconnected and virtualized segments including centralized, edge and far-edge resources. In the latter case the integrated virtualized infrastructure segment includes resources constituted by Cooperative Intelligent Transport Systems (C-ITS) equipment, namely the On-Board Units (OBU) on the vehicles and by Road-Side Units (RSU).

Section 2.4 of 5G-IANA D2.1 [14] provides two listed tables (Table 1 and Table 2), wherein the main building blocks of the 5G-IANA functional components are described.

The 5G-IANA NOD layer, includes the NetworkApp Toolkit and the Application Orchestrator, these provide the functionalities related to modelling/design and provisioning/orchestration phases of the Vertical Service lifecycle.

The 5G-IANA Slice Management and Resource Orchestration layer provides the E2E Resource Orchestration for Far-edge Enabled Network Apps, the Far-edge/Edge/Cloud Continuum Resource Inventory and the Slice Management.

Again for the purpose of finding common ground between 5GASP – 5G-IANA, technical leads from both projects undertook an interactive online session (June 2023) using this high-level view of the features supported by each component in the global architecture of 5G-IANA as a way to explore component commonality between both project architectures.

From this exercise the component of most common ground was the NetworkApp Toolkit from the 5G-IANA NOD's layer which relates directly to the functionality of the 5GASP Network App Onboarding and Deployment Services (NODS). Sub-component elements of both architecture were extensively discussed and some revision to the 5GASP architecture has been considered.

The Network Slice Template Management component of the 5G-IANA SMRO layer was also identified as a common piece of functionality that could be considered as part of an upgrade to the OpenSlice functionality of 5GASP.

In fact from an overall perspective it has been found that the Network Application Validator component (VITAL-5G), the NetworkApp Toolkit (5G-IANA) and the NODS Validation Service (5GASP) are the best places to further collaboration between the 3 projects from an architecture/software component perspective as commonality in the network application packaging would help facilitate Network Application deployment across all 3 testbed of VITAL-5G, 5G-IANA and 5GASP.

Another area of commonality identified was the Monitoring Platform (VITAL-5G), Monitoring & Analytics (5G-IANA) and Federated Prometheus platform (5GASP) of all three projects. Given that traceability and logging, of each Network Application streams have to be captured by the execution environment, collated together with all other streams from the application, and routed to one or more final destinations for viewing and long-term archival and analysis. The collection of such monitoring data can be meaningful for Network Application developers to undertake some introspection on an application's behaviour over time and thus for profiling purposes. Having a common way of hosting monitoring and analytics data across all 3 projects would be significantly beneficial to Network Application developers.

2.5.2 PPDR Infrastructure Architectures

There is one distinctive project in the ICT-programme that covers the PPDR industry, 5G-EPICENTRE

5G-EPICENTRE [15] has built an open end-to-end experimentation 5G platform focusing on software solutions that serve the needs of PPDR. The project has lowered barriers to 5G adoption and market entry for European SMEs to conduct rigorous experimentation of their products and applications aimed at the public safety market, through the provision of an open, federated, end-to-end experimentation facility. 5G-EPICENTRE has:

- Federated multiple constituent 5G platforms into an advanced, user-friendly, zero-touch orchestration single point of control;
- Overseen these facilities' cloud-native transformation in support of transformational technologies in the realization of the 5G vision for PPDR agencies, such as e.g. multi-access edge compute (MEC);
- Demonstrated value of the 5G-EPICENTRE facilities to stakeholders, key/emerging players in the public safety market by helping to accelerate widespread adoption of low-entry 5G virtualized experimental environments and vertical-specific network functions configured specifically to service the needs of the modern first responder;

Through the 5G-EPICENTRE deliverable D1.4 [16] a description of the final list of technical requirements; component specifications; and overall platform architecture driving the design of the 5G-EPICENTRE integrated solution is presented. Given this 5G-EPICENTRE deliverable D1.4 [16] complements the original deliverable D1.3 [17], with a refinement of the 5G-EPICENTRE architectural model, it is interesting to note the top-down re-design of the 5G-EPICENTRE platform architecture, were both new and obsolete building blocks and functionalities are identified.

5G-EPICENTRE is a federation of four independent testbeds/facilities, each characterized by different 5G stand-alone implementation and technologies, yet all capable to support deployment of (containerized) network functions and applications, that are managed by a Kubernetes (K8s) cluster architecture. On top of this federation, a centralized experimentation platform enables access to each of the underlying testbeds' resources, either deploying the experimenter's K8s applications to any of the facilities independently, or across multiple Kubernetes clusters distributed across the facilities.

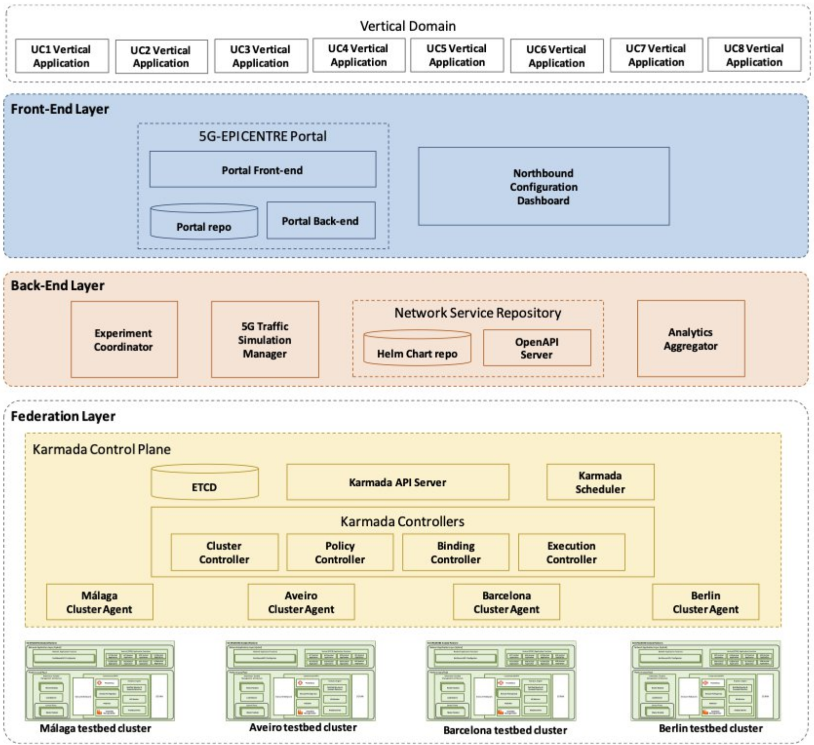

Figure 11 5G-EPICENTRE overall functional architecture component diagram

The final 5G-EPICENTRE platform architectural view is shown in Figure 11, and deeply explained in Section 3.4 of 5G-EPICENTRE deliverable D1.4 [16]. Clearly shown are 5G-EPICENTREs architectural layers of ‘Front-end layer’, ‘Back-end layer’, ‘Federation layer’. The three layers constitute the entities comprising the 5G-EPICENTE platform. The ‘Infrastructure layer’, is a sub-layer to the Federation layer, and it corresponds to the framework describing the augmentations necessary for each individual testbed in the federation, so as to support the 5G-EPICENTRE technical requirements.

For the purpose of finding common ground between 5GASP – 5G-EPICENTRE, technical leads from both projects undertook an interactive online session using this high-level view of the features supported by each component in the global architecture of 5G-EPICENTRE as a way to explore component commonality between both project architectures.

While there was significant overlap between the functionalities of the 5G-EPICENTRE Front-end layer and 5GASP NODS Web UI, the architectural component of most common ground was the Network Service Repository from the 5G-EPICENTRE Back-End layer which relates directly to the functionality of the 5GASP NODS Service Orchestrator. Specifically 5G-EPICENTRE utilizes a JFrog Artifactory [18] private Helm repository to store chart packages, providing methods for uploading, retrieving, updating and deleting chart packages. Whereas covering this same functionality 5GASP utilizes Habor [19] as the Helm repository and there is an ongoing discussion on how to expand Repository API endpoints exposed by 5G-EPICENTRE and 5GASP so as to further support the fully automated provisioning of Helm charts to Kubernetes clusters of the platforms involved.

2.5.3 Other 5G Infrastructure Testbeds

2.5.3.1 5G Berlin Association -- Innovation Cluster

The 5G network in Berlin refers to the fifth generation of mobile network technology that is deployed in the central part of Berlin, Germany. The 5G network is focused on open architectures (O-RAN) that offer significant improvements over previous generations, including faster speeds, lower latency, and increased capacity.

The deployment of the 5G network in Berlin involves collaborations between telecommunication companies, manufacturers, testing facilities, and government entities.

The 5G network in Berlin enables a wide range of applications and services that benefit both consumers and businesses. Some key functionalities include:

Enhanced Mobile Connectivity: Users can experience significantly faster download and upload speeds, seamless streaming of high-definition videos, and smoother browsing on their 5G-enabled mobile devices.

Internet of Things (IoT): 5G enables massive machine-type communications, allowing for a vast number of IoT devices to connect simultaneously. This functionality supports various smart applications, such as smart home automation, industrial automation, and smart city infrastructure.

Augmented and Virtual Reality: The low latency and high bandwidth of 5G make it ideal for augmented reality (AR) and virtual reality (VR) applications. Users can enjoy immersive experiences, whether it's in gaming, education, or virtual meetings.

Autonomous Vehicles: 5G enables reliable and low-latency communication between vehicles, infrastructure, and other road users. This functionality is crucial for the development and deployment of autonomous vehicles, improving safety and enabling advanced driver assistance systems (ADAS).

Remote Healthcare: With 5G, healthcare providers can offer remote consultations, remote surgeries, and real-time patient monitoring. The low latency and high bandwidth of 5G facilitate reliable and high-quality healthcare services even in remote areas.

It's important to note that the specific capabilities, partners, and functionality of the 5G network in Berlin may evolve over time as technology advances and new partnerships form.

5G Berlin Association is part of the 5G eco-system with many projects, like 5GASP and the lab facilities of Deutsche Telekom, Fraunhofer HHI, Fraunhofer Fokus, and EANTC.

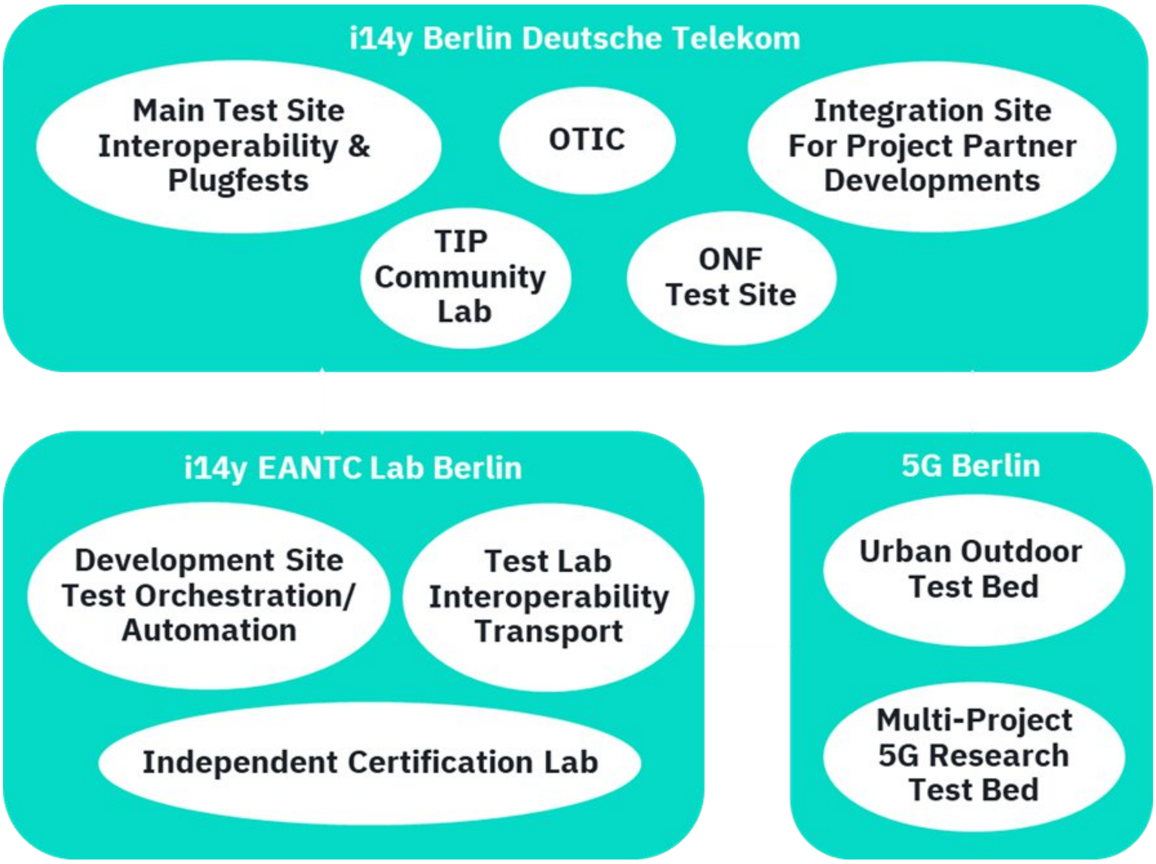

Figure 12 5G Berlin Association - Innovation Cluster

5G Berlin is a potential strong user for services from 5GASP certifications.

2.5.3.1.1 i14y Lab Berlin (EANTC / Deutsche Telekom)

The i14y Lab is the open lab for interoperability testing of disaggregated telco systems, such as Open RAN, led by Deutsche Telekom, operated by a consortium of strong partners with funding support from the German Ministry of Digital and Transport (BMDV).

We provide infrastructure for integration tests with the aim to certify market readiness and accelerate time to market for multi-vendor disaggregated telcommunications solutions. By creating and providing a vendor independent environment, we promote the development of an innovative, open, and interoperable telcommunications ecosystem.

i14y Lab brings the whole telcommunications industry together: Start-ups, vendors, system integrators and international operators. Here, all partners meet on equal footing – and jointly develop advanced test automation capabilities and integrations for future networks.

The i14y Lab will give companies of all sizes quick and easy access to permanent, standardized test setups based on a reference architecture agreed upon by the three major European operators - Deutsche Telekom, Telefónica and Vodafone, which are part of the i14y Lab consortium. Furthermore, O-RAN test specifications and relevant TIP test plans as well as TIP | MoU Group priority requirements will evolve with the needs of the reference architecture and allow for continuous testing.

All of them are free to use the lab's capacities as an environment to test, validate and integrate compliant hardware and software developed for a disaggregated and interoperable telcommunications ecosystem – compatible with the largest possible group of partners and supporters.

In this relation i14y lab is a ideal test environment for 5GASP certifications.

2.5.3.2 UNIVBRIS' 5GUK Testbed

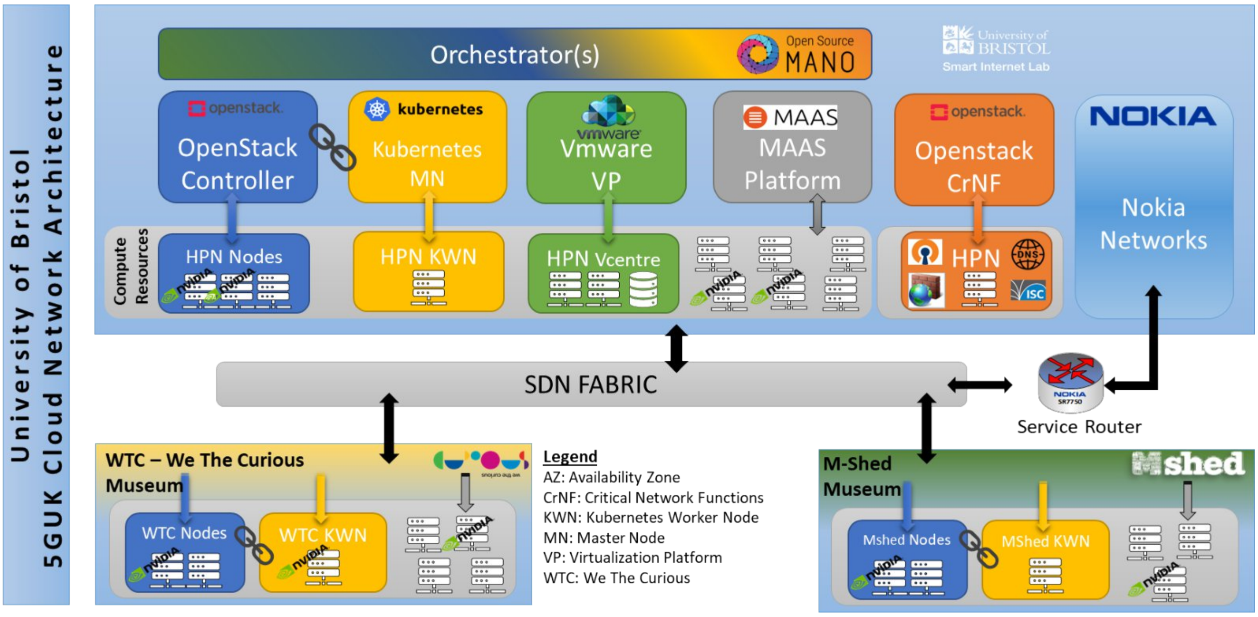

Figure 13 5GUK Network Architecture

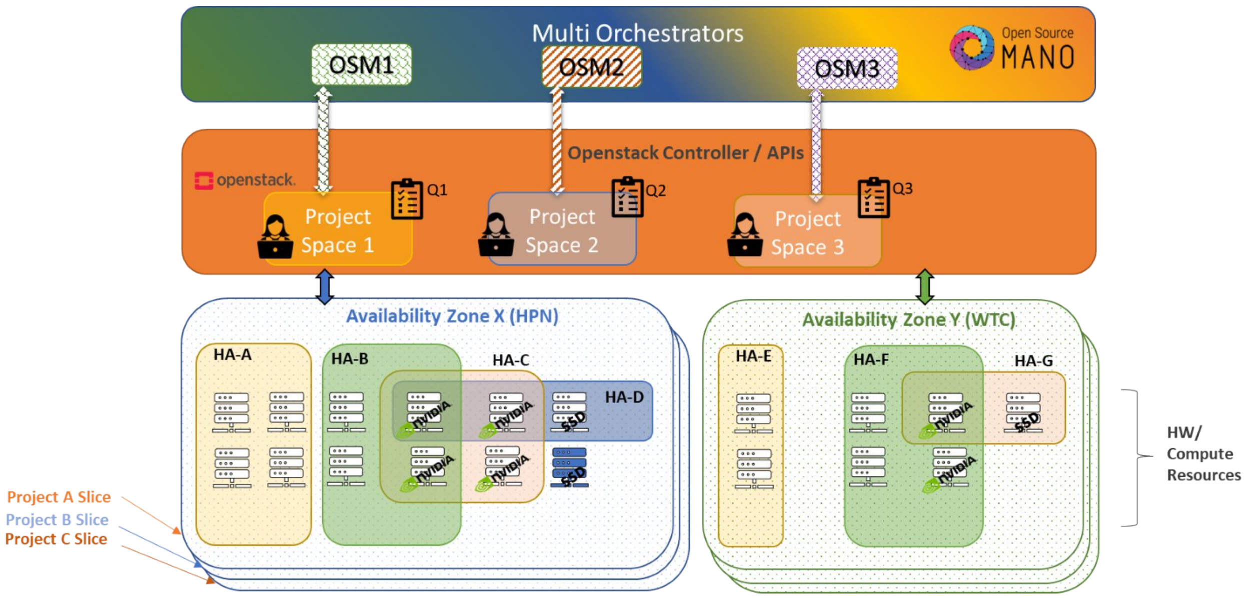

Figure 14 Per-project Slicing and Orchestration Processes in 5GUK Testbed

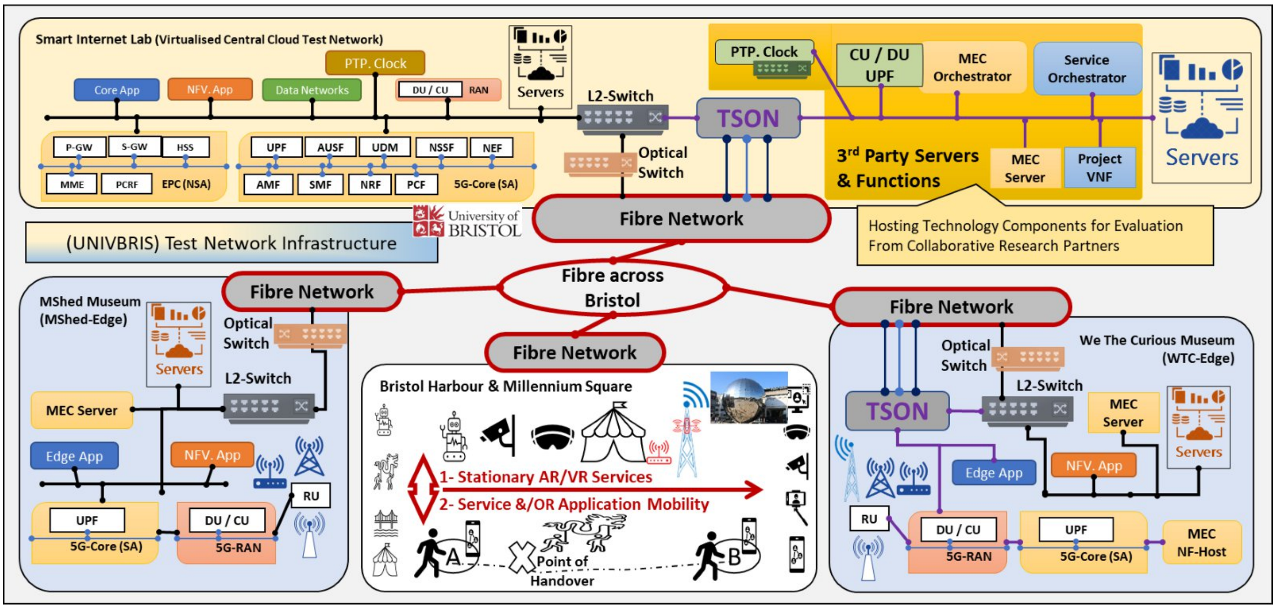

Figure 15 Physical Network Infrastructure of 5GUK Testbed

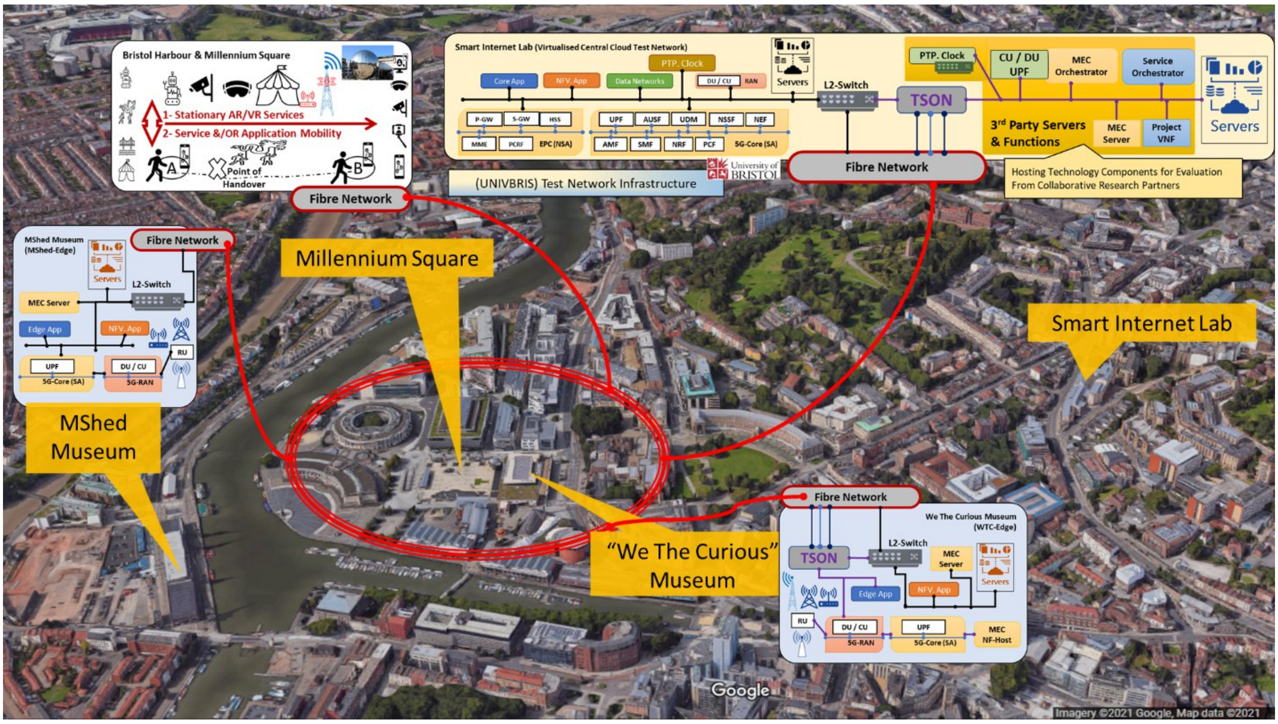

Figure 16 Geographical Placement and Connection Structures Associations for 5GUK Testbed

The general capabilities of the 5GUK Testbed are as follows. Hosting VNFs, CNFs and managing network slices for different projects, with Virtualization platform (Openstack/Kubernetes), covering:

- Compute Resources
    - CPU based servers
    - GPU enabled servers

- Network Resources
    - SDN enabled transport network
    - 5G Access technology
    - WIFI Access technology
- Storage Resources
    - Ceph/Cinder

The key features of the testbed are (mainly) based on open source solutions, like Openstack and Kubernetes, and include MaaS, scalability, customizability and multi tenancy.

The different edges of the testbed provide advantages like the space to demonstrate the 5G use-cases, interconnectivity through the fibre network between the buildings and towers of the edges, the network resources like racks & switches at the base of each tower and rooftops, with 5G NR (Nokia/Benetel) radios and the rest of the access technologies, like:

- WiFi 5 (Nokia/Ruckus)
- WiFi 6 (Ruckus)
- mm-Wave Mesh transport network

The currently implemented technologies are as follows:

- Virtualised infrastructure using private Cloud Network Technologies
- Orchestration of Networks and Services (OSM)
- Service Based Architecture using 5G Core Network (Attocore, Open5Gs)
- Intelligent Transport Network using SDN.
- Intelligent Access Network using Open RAN Architecture (Parallel Wireless, Benetel, Accelleran).
- MEC solution for Network Functions and Application Services
- Nomadic Node: 5G-in-a-box with MEC/cloud capabilities and multi-access technology support. A platform to provide Data from all layers for Machine Learning applications in creating Artificial Intelligent solutions.
- in-house developed CPEs used at a backhaul and/or access level.

3 5GASP Internal and external components (Update)

3.1 5GASP Network Application Onboarding and Deployment Service (NODS)

The 5GASP platform offers a single-entry point portal for its respective stakeholders to facilitate the seamless onboarding, design, and orchestration of both Network Applications and their corresponding test suites. This portal is part of 5GASP Network Application Onboarding and Deployment Services (NODS), which also incorporates the component to actuate the aforementioned actions, i.e. the Service Orchestrator. The implementation of NODS is based on the open-source project Openslice [20]. Openslice, and NODS consequently, employ a service-based architecture utilizing standards and practices from major Standard Development Organizations (SDOs), i.e. European Telecommunications Standards Institute (ETSI), 3rd Generation Partnership Project (3GPP), and TeleManagement Forum (TMF) to design and deliver Network Slices as Services (NSaaS) in an interoperable way. The detailed architecture of NODS can be found in D3.1 [4] and D3.2 [5], respectively. By the end of the project, the final architecture will be presented and commented on in D3.3.

In the context of 5GASP, the interaction with the NODS is achieved by the introduction of a unified standards-based model, seen as a “Triplet”. This specific model comprises the Network Application itself, the suitable accommodating Network Slice, and the respective test suite. Specifically, the above entities are modelled under the TMF633 Service Specification [21] and TMF653 Service Test Specification [22]. The provision of northbound standardized solutions allows for the overall process, i.e. onboarding, deployment, and validation, to be performed to any NFV/3GPP compliant 5G system and not solely on the 5GASP integrated facilities. Extensive details on the employed unified model can be found in D3.1, thus omitted in this document.

While the capabilities of the first two entities of the “Triplet”, i.e. the hosting Network Slice and the Network Application retained their properties and descriptions unaffected since the aforementioned documents, the testing-related entity has undergone specific changes to facilitate additional test procedures and extend the already existing ones by also integrating external, or "developer-defined tests". To that extent, the NODS enhanced its capabilities to accept third-party testing artefacts, apart from solely offering project-wide ones. Particularly, these changes affected both the capabilities of the portal to accommodate the uploading of external test artefacts in the appropriate format and simultaneously the entity responsible for describing the test execution workflow, i.e. the Testing Descriptor.

As previously mentioned, the Testing Descriptor is enclosed in the test suite artefacts onboarded to the NODS. It is a YAML file that lists not only the tests to be performed, but also their execution order. Furthermore, it can reference both pre-defined tests and developer-defined tests. More information on these tests is provided in Section 3.3 and a snippet of a Testing Descriptor is provided in Figure 26. Regarding the developer-defined tests, these are implemented through the Robot Framework [23] and must be packaged as a tar.gz file so they can be onboarded. More details on the Testing Descriptor and the supported Tests can be found in Section 4.4.2.

3.2 5GASP Facility Updates

3.2.1 Aveiro Site

Table 2 lists all the updates conducted in ITAv's facility.

Non-5G Infrastructure	• Upgrade of the Openstack Cluster used as VIM for the 5GASP Project (CPU, RAM, Disk, NICs); • Deployment of a new Proxmox Cluster to support the deployment of new 5GASP architectural components; • Deployment of Prometheus and Grafana, to provide Infrastructure/Network metrics; • Implementation of a more granular Firewall and VLANing of the different project-related networks.
5G Infrastructure	• Provisioning of an SDN Switch to control de 5G Transport Network and collect metrics on it (see Figure 17); • Development of a Slicing API to programmatically configure ITAv's Network Slices;
Testing and Certification Components	• Deployment of the Certification Entity; • Deployment of the NEF Emulator/Simulator to support 5G-readiness tests; • Several upgrades on the CI/CD Manager to cope with the certification workflows.
Inter-domain Scenario	• Deployment of a VPN Node in ITAv, to support inter-domain scenarios.

Table 2 ITAv - Facility Updates

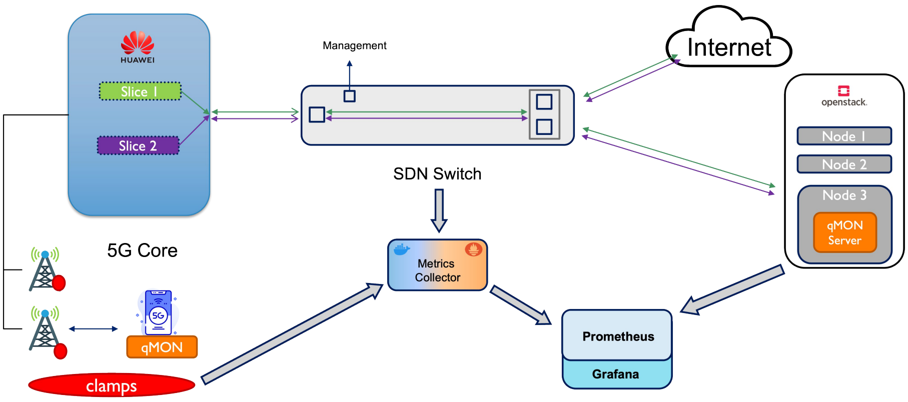

Figure 17 5G Transport Network SDN Switch

3.2.2 Patras Site

Patras5G is a 5G/6G infrastructure built over the course of several EU and operates as a "private" but open infrastructure and comprises both open-source and commercial components, with dedicated components and services that support large-scale experimentation for 5G and IoT applications. The Patras5G testbed supports containerized and virtualized deployments from 5G RAN to 5G Core, including 5G standalone (SA) setups.

It features an AI-dedicated Kubernetes cluster with NVIDIA GPUs, a 400Gbps programmable network based on P4 switches, and the necessary cloud and SDN fabric to host any service that needs to be tested and integrated with the testbed infrastructure. Open-source Operations Support System (OSS) Openslice (http://openslice.io/) enables access to users and applications.

Being an open infrastructure, yet operating as private, it is available for testing and experimentation activities, using licensed and unlicensed spectrum and privately owned SIM cards. It is fully 5G SA standard compliant (5G RAN and 5G Core Release 16) with the future 3GPP Releases upgrades in the process.

The Patras5G testbed boasts an mmWave backhaul that connects the 5G Core with various locations (red dots in the above figure) across the city of Patras, where 5G RAN points of presence (yellow dots in the above figure) have been deployed, hosting vertical experiments from EU projects. Additionally, some of these locations offer broadband services through Fixed Wireless Access. Various open-source or commercial 5G Cores are integrated with SDR platforms and UEs and g/eNB. MEC orchestration and mobility management features are supported for interactive mobile streaming edge services. Most of the installed components are offered as Open Source, but there are also dedicated components and services to support 5G and IoT scenarios.

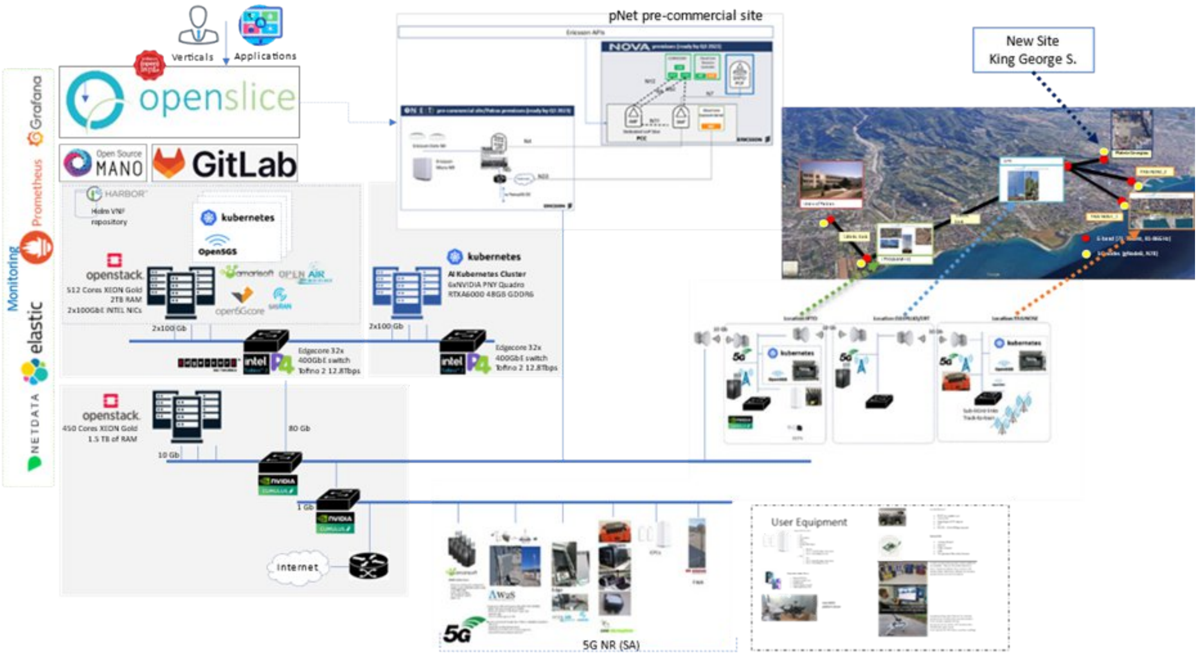

Figure 18 Patras5G Facility Infrastructure

All the above components offer monitoring probes which are aggregated through various instances of Prometheus into one central Prometheus node of the infrastructure. Particularly, to align with the 5GASP needs for the provision of monitoring data along with the experimentation results, metrics from the RAN and cloud-based infrastructure are being exposed along with the nominated metrics from the 5G Core itself. Consequently, the Patras infrastructure Prometheus is part of the 5GASP federation of Prometheus instances that fuel the respective 5GASP Grafana, which offer monitoring dashboards from the overall 5GASP infrastructure, i.e. the six underlying facilities, through the same portal.

To end up, Patras site also hosted an instance of the 5GASP branch of NEF emulator , to further support the 5G-awareness testing of the employed Network Applications. This enabled and supported a unified approach among the project's testbeds, so as to introduce the uniform way of 5G system interaction regardless of the topology of its deployment. Furthermore, the NEF Emulator database was populated with a set of the actual infrastructure, in regard to gNodeB placement and indicative UE routes with the Patras site. A worth mentioning feature that was also explored and supported is the simultaneous monitoring of NEF Emulator events, not only from the indicatory subscribed Network Application but also from the testbed itself so as to emulate the respective network restrictions to the data plane of the Network Application under test, through a designated network controller.

3.2.3 Bristol Site

Updates for the past 12 months:

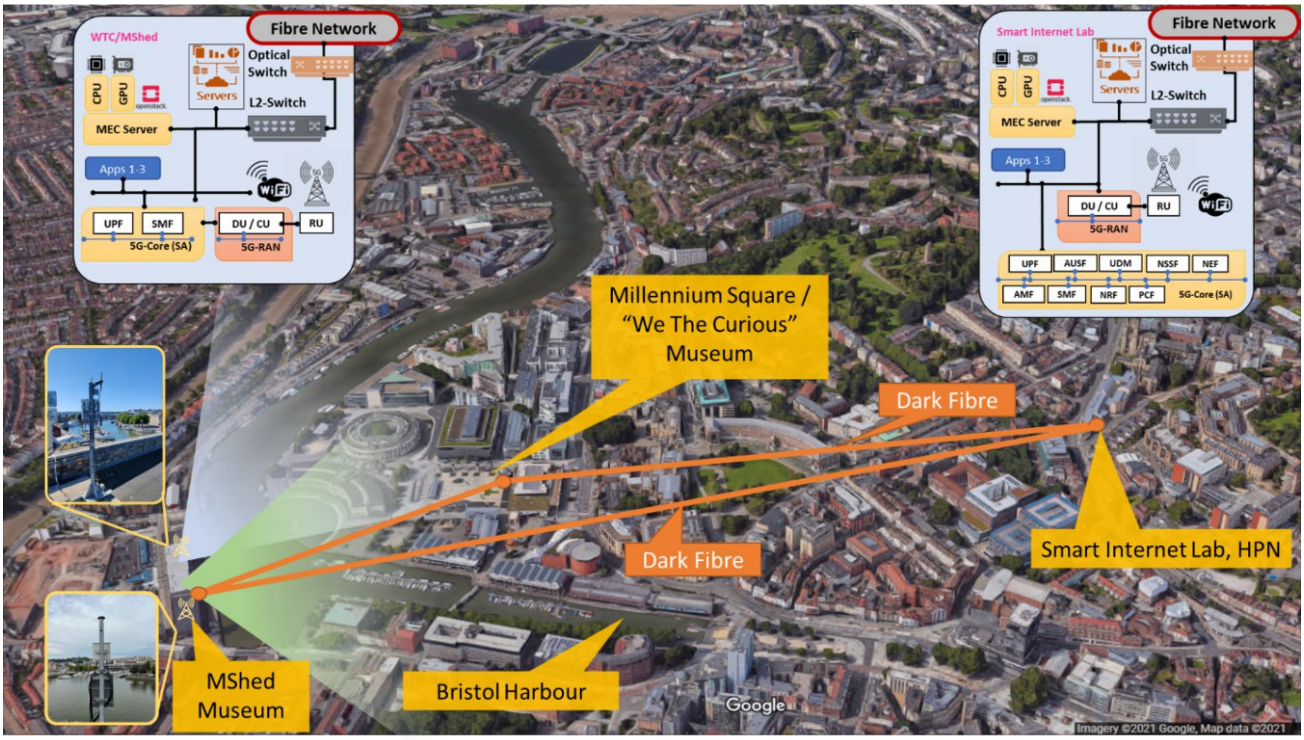

Figure 19 Geographical Placement and Connection Structures Associations for 5GUK Testbed

The main deltas from the last update are covered by the following bullet point

- WTC fire – On 12 May 2022, a fire burst on the roof of the "We the Curious" building (shown in the above figure), and as a result, the following measures were taken during the next few months:
  - WTC edge has now been returned to operational state, only as a MEC site.
  - WTC 5G RAN was moved to MShed where two 5G cells are now operating.
- The gNBs' software was upgraded, and, as a result, the improvements in the following metrics have been made:
  - Throughput performance
  - Xn handover now fully implemented.
  - All n78 5G NR were decomissioned, in order to commision the following:
  - 2 additional n77 5G micro cells at MShed (100MHz).
  - 2 additional n77 5G indoor pico cells at HPN (100MHz).
  - 1 additional n77 O-RAN micro cell (100MHz, currently installed in HPN lab).
- While previously, the 5G Core Monitoring was done via ElasticSearch and Kibana, we have now changed to an Open5GS integration with Prometheus and Grafana.
- For the monitoring of UE Devices, the following actions have been/need to be taken:
  - Android monitoring app developed
  - Integrated with ElasticSearch
  - Prometheus Integration – pending
- In order to also demonstrate secure and privacy-preserving interfacing capabilities with a 5G core, we have implemented a NEF Emulator (provided by 5G-Evolved1), which focuses on the standardisation of the exposure of network capabilities with a special focus on security and privacy, through the emulation of the API interfaces

between a 5G Core and the network applications. Further, for realistic interactions and environment emulation, a mobility and access network simulator, which we have modified with extra capabilities, is implemented alongside the emulator. The extra capabilities in the simulator are now also reflected in the APIs of the emulator, which have also been extended accordingly.

3.2.4 Ljubljana Site

The Public Protection and Disaster Relief facility for Outdoor and Indoor 5G Experiments (PPDR ONE) site is located at ININ's premises in Ljubljana, Slovenia. Besides widely used 4G/5G-NSA technologies, the facility offers a modern private 5G SA radio and mobile core system, cloud backend infrastructure using OpenStack and Kubernetes, with both of them supporting NFV-based orchestration using OSM.

Additionally, extensive monitoring capabilities are provided using qMON Monitoring Suite (i.e. qMON backend services and distributed monitoring agents) and MobileONE solution that provides 5G network slice capabilities.

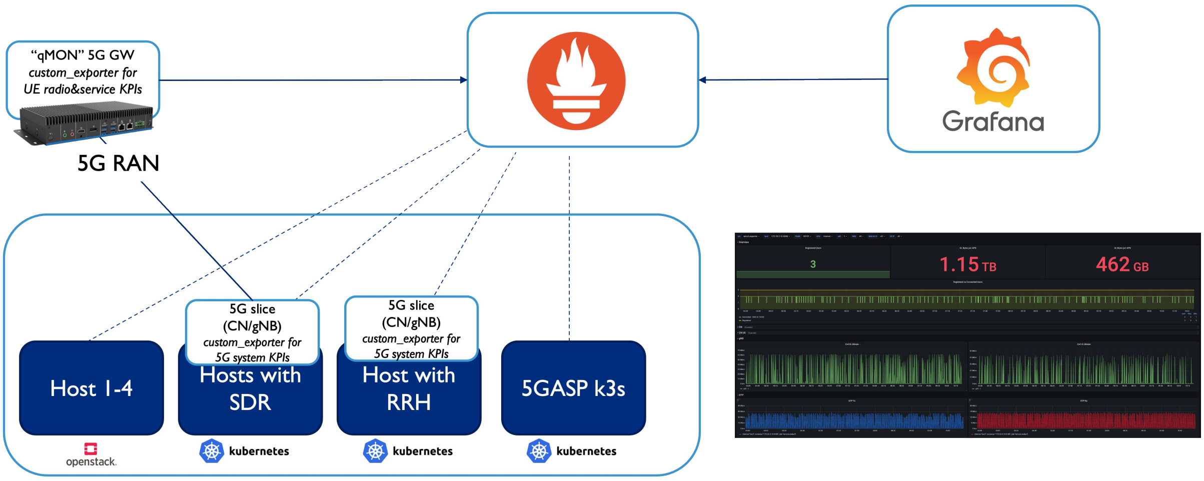

Figure 20 ININ's testbed infrastructure and monitoring architecture

Testbed updates were mainly related to monitoring of the cloud and 5G infrastructure, NFV/OSM orchestration, automation of IOPS operation and support for inter-testbed connectivity. More details are provided in the following sections:

- Monitoring:
  - Dedicated Prometheus and Grafana instances to provide extensive monitoring capabilities for:
    - Cloud-based infrastructure, e.g. physical nodes hosting OpenStack and Kubernetes;
    - 5G System monitoring that includes Core Network KPIs (e.g., number of connected/registered devices, NAS signalling, GTP bitrates), gNB KPIs (e.g., cell bitrates) and per UE KPIs (e.g., UE bitrates, UE retransmissions)

        - UE end-to-end monitoring using qMON Network Performance Tool including private 5G SA capable UE devices:
            - 5G Gateway with Sierra Wireless EM9191 modem,
            - Samsung S23 with Android 13.
        - Environmental sensing providing temperature, humidity and CO/CO2 readings.
    - All KPIs are also available in centralized 5GASP Prometheus/Grafana.

- 5G infrastructure:
    - Multiple upgrades to newer releases of commercial 5G software running on CN and gNB with in-house adaptations to provide fully orchestratable 5G system solution (i.e., MobileONE).
    - 5G Network Slice instantiation moved from VNF-based orchestration to cloud-native CNF-based orchestration based on Kubernetes/Helm-charts with extensive day-1 and day-2 configuration support.
    - Multiple IOPS-capable nodes:
        - 2x Indoor based on SDR cards,,
        - 1x Outdoor with RRH and external antennas
        - Each node can operate in multiple modes:
            - CN-only,
            - gNB-only,
            - CN+gNB (providing all-in-one private 5G solution),
            - CN+gNB w/ IOPS support.
    - Multiple 5G network slice support with the capability to assign and change specific slice on the UE via in-house developed API.
    - NEF emulator support.

- Testing:
    - Providing scripts to automate switching between IOPS modes based on ROBOT framework.

- Inter-domain support:
    - Orchestrated deployment of a VPN node providing mesh VPN for Network Applications requiring connectivity to other testbeds.

3.2.5 Murcia Site

Gaia-5G is a laboratory for experimentation located in the Computer Science Faculty in the University of Murcia. Its research purposes are focused on the area of 5G technologies with virtualization and backhaul infrastructure for the Wireless connectivity, including 5G, LoRaWAN and PC5/G5 self-managed infrastructure that allows experimentation in different fields.

The infrastructure of the testbed has evolved since the start of the project (see Figure 21). From the three original sites (two outdoor and one lab), two outdoor and two indoor new sites have been deployed in the campus network. Besides, PC5/G5 RSUs are being deployed and they are expected to be available in the coming months.

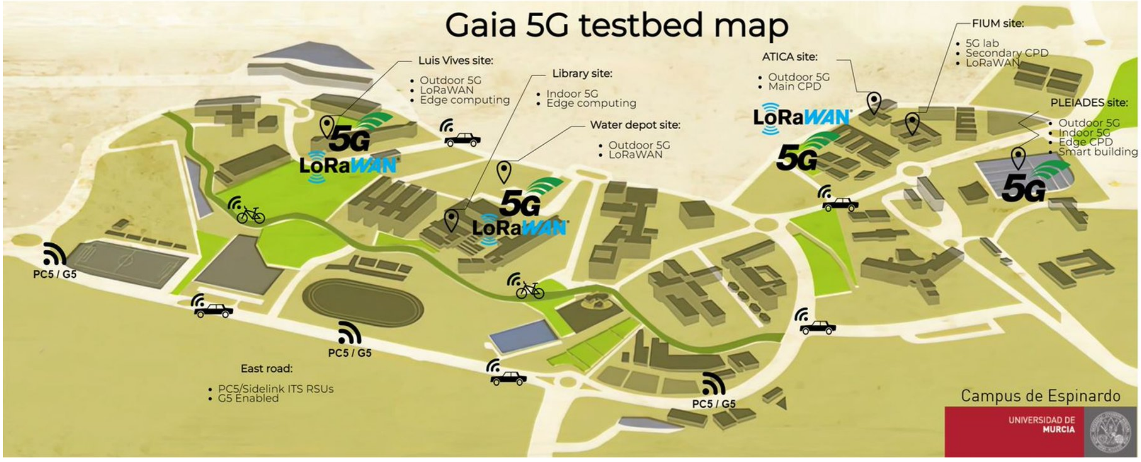

Figure 21 Gaia 5G testbed updated map

Regarding the 5G infrastructure, the software of the gNBs has been updated and the overall performance of the network has improved, obtaining better results in terms of latency and bandwidth. Besides, the radio parameters have been tuned to improve the coverage and to enhance the behaviour of the handovers among the different cells.

In the same line, an important work has been done with the 5G modems used to connect the UEs. Several On-Board Units (OBUs) were prepared during the last year to accommodate the vehicular use cases, and it was necessary to develop a software to control and monitor the used 5G modems.

To be completely aligned with the project, and also to improve the Gaia 5G management, a monitoring architecture was defined, implemented and deployed to obtain a full view of the network and provide observability. As it can be seen in Figure 22, the monitoring platform is based in several tools widely adopted by the community such as syslog-ng, collectd, ELK, netdata, Prometheus and Grafana. Furthermore, multiple developments have been done to integrate everything and provide monitoring in components with no prior monitoring capabilities, such as the 5G modems, the 5G RAN and the 5G core.

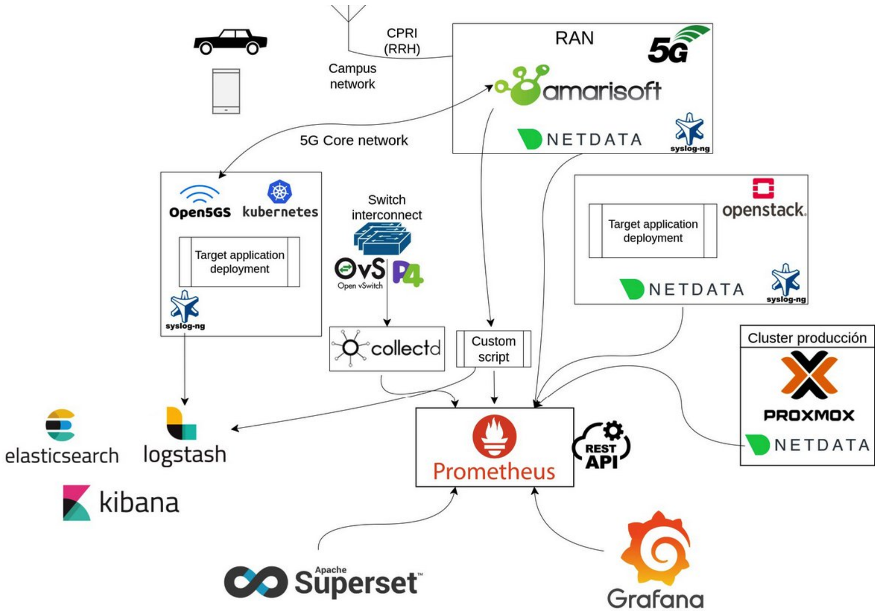

Figure 22 Gaia 5G monitoring architecture

Finally, to permit the design, development and experimentation of 5G network applications, an instance of the NEF Emulator has been deployed in the infrastructure. This is because it has been detected a lack of a real NEF implementation in both open source and commercial 5G solutions. By doing this, we enable the creation of 5G network applications that interact with the 5G network via the NEF interface because the developers can evaluate the operation interacting with the NEF emulator. This developed code and behaviours can be later migrated to a 5G network with a real NEF with no further effort.

3.2.6 Bucharest Site

ORO's 5G Testbed is architecturally composed of 5G Network Components that have evolved during the lifespan of 5GASP, currently offering an E2E 5G Infrastructure, compliant with the requirements of Network Applications and complex CI/CD frameworks. Hosted within Orange 5G Lab, a beyond-state-of-the-art experimentation and development facility, built and operated by Orange Romania and Universitatea POLITEHNICA of Bucharest, ORO's 5G Testbed has been updated in the previous 12 months according to the initial planning, set forward in D2.1 [1], and referenced here in Figure 23 - ORO Facility Planning (Reference to D2.1 - Page 92).

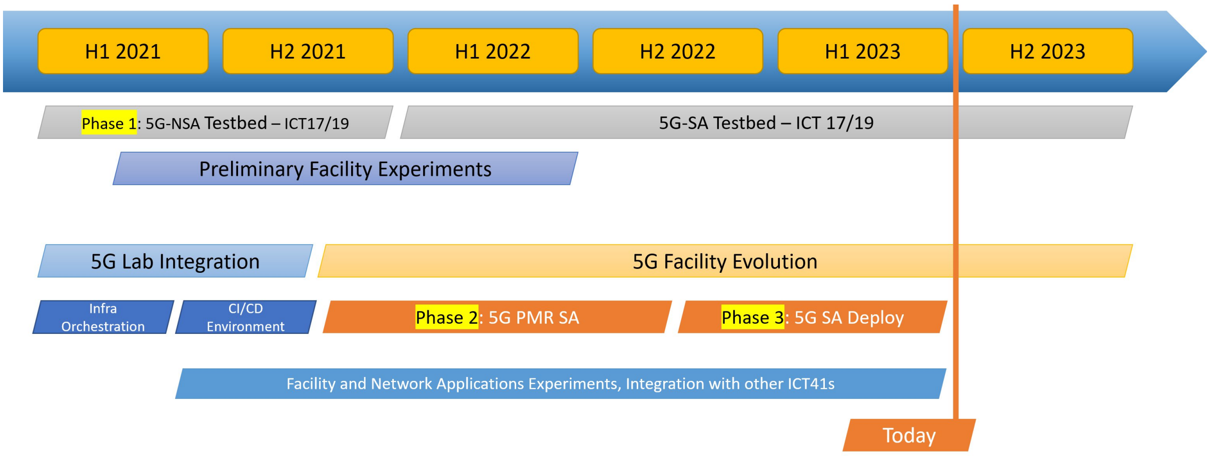

Figure 23 ORO Facility Planning

During the H2-2022 to H1 2023 period, updates to the 5G Test bed include the deployment of 5GSA experimentation environment, as per the Phase 3 planning of activities. This update consisted of the deployment of a 5GSBA-compliant infrastructure of virtualised and "bare-metal" COTS network components modularized services, to achieve flexible and adaptable, automatic and on-demand service creation, fast network slices deployment cycles, dynamic services launched in the facility. The facility also introduces virtualisation capabilities and the multi services slicing concepts with the ability of adapting to the services as network slices for each type of usage, as in this case eMBB and URLLC.

Several network slices have been implemented, following 5G SA Option 2 release capabilities, as per initial planning, to include:

- 5GSA RAN and Core, Option 2 (Commercial Grade)
- Orange Spectrum for testing (N78, B3, B7)
- Cloud-based Services Infrastructure for VNFs, CNFs and Bare-Metal Components
- Virtualised Infrastructure deployment including Iaas/CaaS Capabilities through OpenStack and K8s
- 5G UEs and CPEs capable of running NEO's Network Application's Front-end(s)
- IP-FABRIC network Architecture for Services Delivery, IP Transport and Network Orchestration
- NEF Emulator Available in the facility, to circumvent the lack of availability of Commercial-Grade and/or Open-Source NEF Deployments. This NEF Emulator Instance permits Network Applications Developers to interact with the 5G SBA in an DevOps-enabled paradigm and enables ORO to anticipate the transition to a Commercial-Grade NEF, upon the availability of the technology.
- A full-stack SBA Monitoring Platform, based on Prometheus and Grafana has been enabled in the 5G Test bed, alongside the existing, custom-build Click-based monitoring platform. This monitoring platform has been integrated in the Centralized Monitoring Solution, available across the 5GASP Test beds.

3.2.7 Inter-Site Connectivity

One of the 5GASP objectives is to provide a solution to instantiate an E2E Service across multiple domains without prior negotiations. Technically, this is possible by using an E2E Network Slice composed of NSs or Network Slices. In 5GASP, we connect the independent E2E Network Slice Subnets by creating and configuring a VPN tunnel between them, providing a secure channel where communication between domains can successfully occur. For this project and use cases, the technology that we rely upon to instantiate the proposed VPN tunnel is Wireguard. This simple and minimalist framework enables the swift instantiation and deployment of VPNs.

NetOr enables the orchestration of inter-domain services. This system provides the capabilities to offer connectivity between the NSs in the different domains. NetOr also handles inter-domain scenarios by coordinating the NFV Orchestrators (NFVOs) that reside in the various domains. As a result, our approach leads to a fully automated orchestration of a full-mesh VPN between all domains without prior negotiation.

The configuration of the VPN Tunnels aims to be automatic, resulting in a truly-zero touch approach. We can accomplish this by providing a central entity forwarding all required information. Thus, we employ a central entity offering Service Discovery (SD) mechanisms. More precisely, we use DNS-Based SD, a standardized approach by IETF. The domains' VPN Nodes store their public key and all necessary information in a DNS Server, present on NetOr. Consequently, the remaining VPN Nodes can access and retrieve this data for establishing the VPN Tunnels.

Upon a request to instantiate our solution, NetOr's Coordinator component creates a specific DNS zone for the Vertical service. Consequently, the Coordinator modifies the instantiation request to include parameters necessary for performing SD. One of the parameters is a unique cipher key that each VPN Node shall use to publish and share protected information. Such information comprises the VPN Nodes' public key, location, and other information about the networks that should be exposed through the VPN tunnels. Once this process is done, the Coordinator contacts the Domain Manager component to instantiate the NFV artefacts in each domain using the augmented instantiation request.

Once all VPN Nodes' VNFs are instantiated in all domains, the Wireguard configuration step can start. During this step, the VPN nodes, a private and a public key, are generated. Wireguard will use these to encrypt the network traffic that circulates through the VPN tunnels. At this point, the VPN Nodes are ready to share the necessary information for the VPN Tunnels establishment. Hence, these will publish in NetOr's DNS Server (I) their public key, (ii) their location, and (iii) additional information about the networks that should be accessible to the remaining nodes that belong in the Mesh VPN. To publish their information, the VPN Nodes must use the cipher key that NetOr injected priorly in the instantiation request. Besides this, all the information exchange complies with the IETF's RFC 6763 Standard [24].

After a VPN node has published its information in the DNS Server, it will continue to query this entity to look for other operational VPN nodes. Once a new node is discovered, the VPN tunnel establishment phase begins. The Wireguard's configuration file is updated to include the information gathered from the DNS Server, and a new VPN Tunnel is created. Figure 24 depicts the full-mesh VPN scenario that results from our approach.

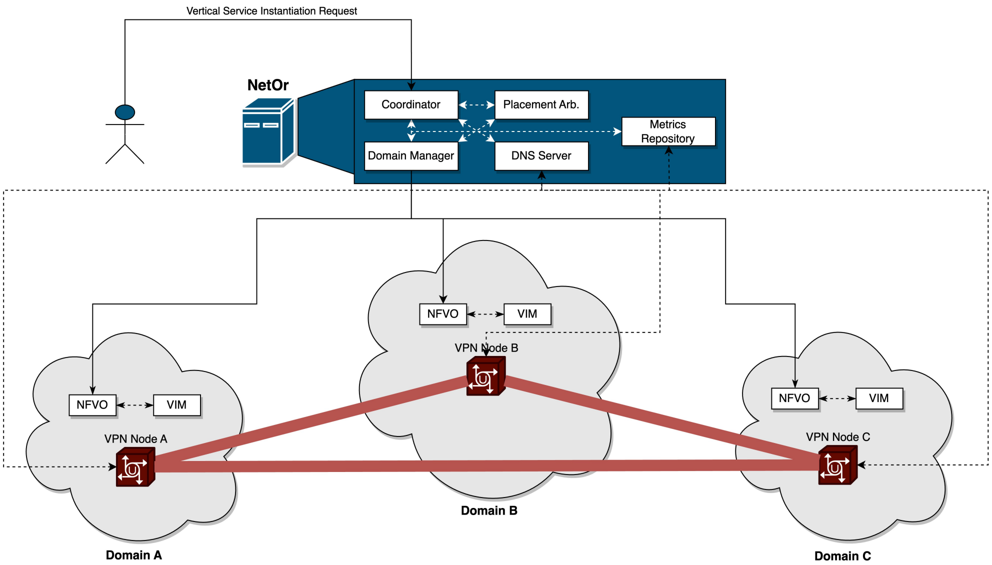

Figure 24 Architecture of the presented Full Mesh VPN Solution

3.3 5GASP CI/CD Service

5GASP's CI/CD Service allows for a thorough testing and validation of Network Applications. After the orchestration of a Network Application in a 5GASP testbed, the NODS will trigger a new validation process through the CI/CD Service. To do so, the NODS creates a TMF 653 Service Test payload with all the meaningful information required to validate a Network Application and sends it to the CI/CD Manager, which will then leverage the received payload to create a testing pipeline for the Network Application.

The created pipeline will then be forwarded to a CI/CD Agent that lives in the same testbed where the Network Application was deployed. The CI/CD Agent is the component that performs the tests on the Network Applications by leveraging (i) tests already onboarded in the 5GASP ecosystem, available in the testbed's Local Test Repository (LTR), and (ii) custom tests onboarded by the Network Application developers.

Figure 25 entails the high-level architecture of 5GASP's CI/CD Service, with its components highlighted in blue.

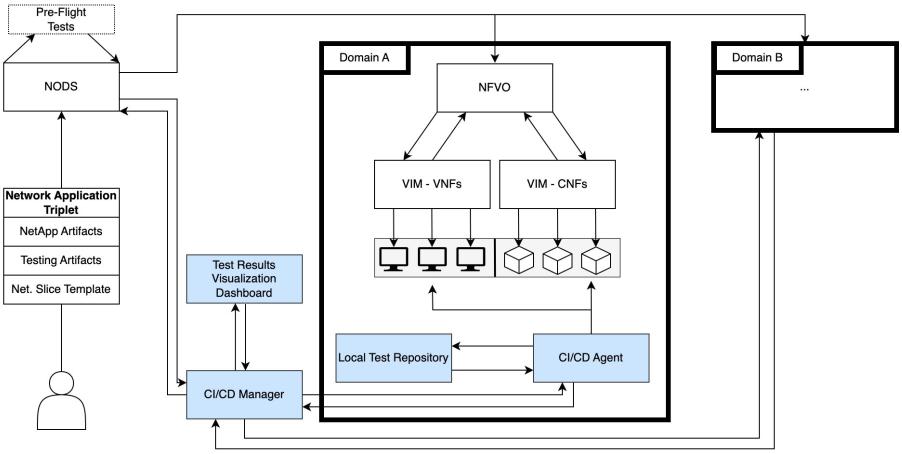

Figure 25 5GASP's CI/CD Service High Level Architecture

Having briefly introduced the purpose and the main components of 5GASP's CI/CD Service we now move on to a more detailed description of all the phases involved in the process of validating a Network Application.

Stage 1 – Testing Artifacts Onboarding: When a developer wishes to validate his/her Network Application in 5GASP's ecosystem, he/she must start by onboarding the Testing Artefacts to the NODS. These artefacts entail (i) a Testing Descriptor – a YAML file that will be relied upon to create a testing pipeline – and (ii) a collection of developer-defined tests – custom tests developed by the Network Application developers, which will be performed on the Network Application.

Figure 26 showcases a snippet of a Testing Descriptor.

```yaml
test_info:
  netapp_id: OdinS-NetApp
  network_service_id: vOBU
  testbed_id: testbed_itav
  description: Validation tests for OdinS NetApp - June 2023

test_phases:
  setup:
    deployments:
      ...

    testcases:
      #######################################################
      #                   Pre-Defined Test                  #
      #                     Open Ports                      #
      #######################################################

      - testcase_id: 1
        type: predefined
        scope: security
        name: open_ports
        description: Check if the Aggregator's open ports are the ones desired
        parameters:
          - key: host
            value: {{deployment_info|testing_migrate_nsd|vnf3|agg-vnf-eth0-ext|ip-address}}
          - key: expected_open_ports
            value: 22/tcp,9042/tcp,9160/tcp,8090/tcp

      #######################################################
      #                Developer-Defined Test               #
      #                  API Request Test                   #
      #######################################################
      - testcase_id: 2
        type: developer-defined
        scope: operational
        name: api_request_test
        description: Test if the Manager's API is ready
        parameters:
          - key: host
            value: {{deployment_info|testing_migrate_nsd|vnf1|mgmt-vnf-eth0-ext|ip-address}}
          - key: port
            value: 8070

      ...
```

Figure 26 Example Testing Descriptor

From Figure 26, we notice that the Testing Descriptor onboarded by the developers supports the execution of (i) pre-defined tests – already onboarded in the 5GASP ecosystem that may be used by all Network Applications, and (ii) pre-defined tests.

Furthermore, one may also notice the usage of 'template tags' in the Testing Descriptor. E.g.:*{{deployment_info|testing_migrate_nsd|vnf1|mgmt.-vnf-eth0-ext|ip-address}}*. This template tag will be rendered by the CI/CD Service to replace it with the 'IP address' of the interface with the id 'mgmt-vnf-eth0-ext' of the VNF with the id 'vnf1'. This VNF is enclosed in the Network Service with the id 'testing_migrate_nsd'.

Stage 2 – Network Application Orchestration: Even though this stage is not under the scope of the CI/CD Service, it is necessary as it is during this stage that the Network Application will be deployed in a Testbed

Stage 3 – CI/CD Service Triggering: After a successful deployment of a Network Application, the NODS will compose a TMF 653 Service Test payload with all the meaningful information required to validate a Network Application and send it to the CI/CD Manager. This payload comprises information on how the CI/CD Manager can obtain the Testing Artifacts onboarded by the developer to the NODS and information on the deployment of the Network Application (crucial to render the template tags), for instance.

Stage 4 – Testing Pipeline Creation and Triggering of the CI/CD Agents:After receiving the TMF 653 Service Test payload from NODS, the CI/CD Manager will create a Testing Pipeline configuration file. This configuration file will then be shipped to a CI/CD Agent that lives in the same testbed as the Network Application. The CI/CD Agent will then perform the Testing Pipeline to validate the Network Application.

Stage 5 – Tests Execution: During this stage, both pre-defined tests and developer-defined tests will be performed, and their outputs and results collected by the CI/CD Agent. The pre-defined tests are available in the testbed's LTR, while the developer-defined test can be obtained through the CI/CD Manager, who collected them from the NODS. When the tests execution phase finishes, the CI/CD Agent will send all the collected outputs and results to the CI/CD Manager.

Stage 6 – Test Results Publication: After receiving the testing results and outputs the CI/CD Manager will create a Test Report and make it available via the Test Results Visualization Dashboard (TRVD). Moreover, an URL to the TRVD will also be provided to the NODS, so that the developer may have access to the Test Report.

Regarding the tests execution, the CI/CD Service executes 4 different batches/scopes of tests (defined in D5.4 [3]).

The 5G Readiness tests mainly rely on the NEF Emulator previously introduced. To validate the interactions between the Network Application and the NEF Emulator a Reporting API was developed and attached to the NEF Emulator.

The NEF Emulator Reporting API serves to create and obtain a report regarding all the interactions between the Network Application and the NEF Emulator. The NEF Emulator is being relied upon to evaluate the Network Application's capability to interact with the NEF. Instead of the Network Application interacting with a real NEF, it interacts with a NEF Emulator that fully mimics the APIs offered by a real NEF. This way, through the NEF Emulator Reporting API we can collect a report on all these interactions and use it to validate the interaction of the Network Application with a NEF. In regard to the endpoints offered by this API, these are very simple and straightforward, as only 2 endpoints are offered: *POST /report/name=<report_name>* and *GET /report/name=<report_name>*. The first endpoint is used to create a new report while the second is used to obtain the report. The CI/CD Agent is responsible for invoking these endpoints and will also parse the final report in order to validate that the Network Application can correctly interact with the NEF.

4 Community-facing Components (Update)

4.1 5GASP Marketplace

Our vision for the 5GASP ecosystem is of an open market, where developers, verticals and network operators can meet and create added value. 5GASP has already developed a portal called the 5GASP Services Marketplace [25], where Network Applications developers have the opportunity to showcase their products along with certifications on the supported software platforms (interoperability) and functionality (as assessed by a 3rd party certification entity). This showcase portal is therefore more than a network application directory, it includes operational information provided by the 5GASP platform independently from application developers and network operators. Such information is collected automatically from a pool of testbeds that run tests defined by various entities such as developers of the Network Applications, Verticals surveying possible acquisitions/partnerships and Network Providers validating that they can support the network applications.

The 5GASP Services Marketplace aims to support business around network applications, network functions, and network services. It provides a public registry of SMEs and their reusable products. Any useful information and documentation for SMEs is available at this portal as well. The network applications community (https://community.5gasp.eu/) supports developers of network applications, network functions, and network services. It provides developers' forum, technical documentation, user guides, and other related information for developers, operators, and vertical industries.
The marketplace is organized in to 6 sections: Service, Resources, NFV, Testing, Products and Networking.
Each section guides potential partner through the 5GASP processes and helps to speed up test and development for network applications.

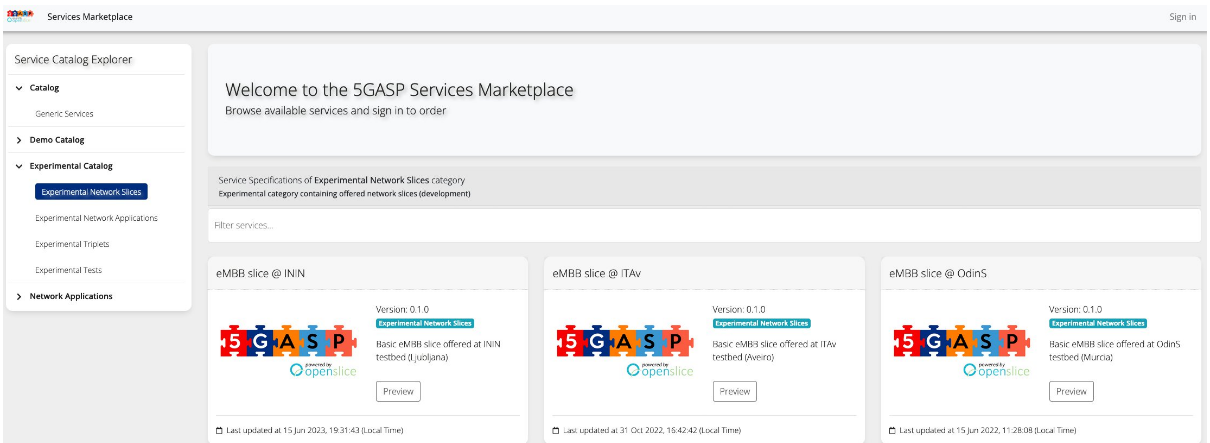

Figure 27 5GASP Services Marketplace

4.2 User community interaction portal

The Network Application Community portal [26] is a platform that supports the community of developers and users of the Network Applications developed within the 5GASP environment and the supporting implementation systems. The final portal version is deployed now and ready to use. The Network Application Community portal comprises technical documentation, user guides, videos and other related information to support all interested visitors. It also provides a discussions platform, through the developers' forum, where registered members can address questions and provide answers for 5GASP-related platforms and extra technical support.

4.2.1 Updated Requirements, Site Map and Contents

The deployed Network Application Community portal now provides a page for the "5G Network Application Lab", which comprises of the Network Application Lab concept, history and upcoming events. The site map has been updated to reflect the updated website, as shown in Figure 28.

In its final version, the main menu includes six items:

1. Network Application Community,
2. Wiki Space,
3. Developer Forum,
4. Public Repository,
5. Multimedia,
6. Register.

The section 'Network Application Community' now has a new page, named '5G Network Application Lab' (Figure 29). This page presents the generic information about the 5GASP Development Community, its members and engagement activities.

The section 'Wiki Space' has 7 sub-sections:

1. Knowledge Center
2. Tutorials
3. Certification Guidelines
4. Network Application Case Studies
5. Blog
6. 5GASP Documentation
7. FAQ

The Knowledge Center provides the essential information on the knowledge base (definitions, papers and 5GASP-specific terminology). The tutorials subsection comprises of tutorials supporting most of the mechanics surrounding the development surrounding the 5GASP architecture; specifically tutorials on the development and testing guidelines towards the onboarding and implementation of 5GASP-certified Network Applications. The Certification guidelines offer insightful information and guides on the certification process that the project implements for the certification of Network Applications. The Network Application case studies associated to different Network Applications are also comprised of the specific application use cases, within which they were developed and deployed. Through the Blog, the site users can get an insight on the newest achievements, work and information that the community members have studied, discussed and/or developed. Finally, the 5GASP Project documentation, and FAQs can provide most other information that a Community Portal general public user may be interested in and/or have questions about, regarding the community, the Network Applications, the testbeds or the project itself.

The 'Developer Forum' (Figure 29) hosts dynamic content within the portal domain. On this forum, the registered users can ask questions, provide answers and experts can provide answers and encourage discussions on 5GASP-relevant topics, like Network Application development issues, testbed and technology-implementation.

The page 'Public Repository of Experiments' presents the currently-implemented and exposed Network Applications. This page currently shows 11 Network Applications, that are in the process of being tested and certified, within the 5GASP infrastructure.

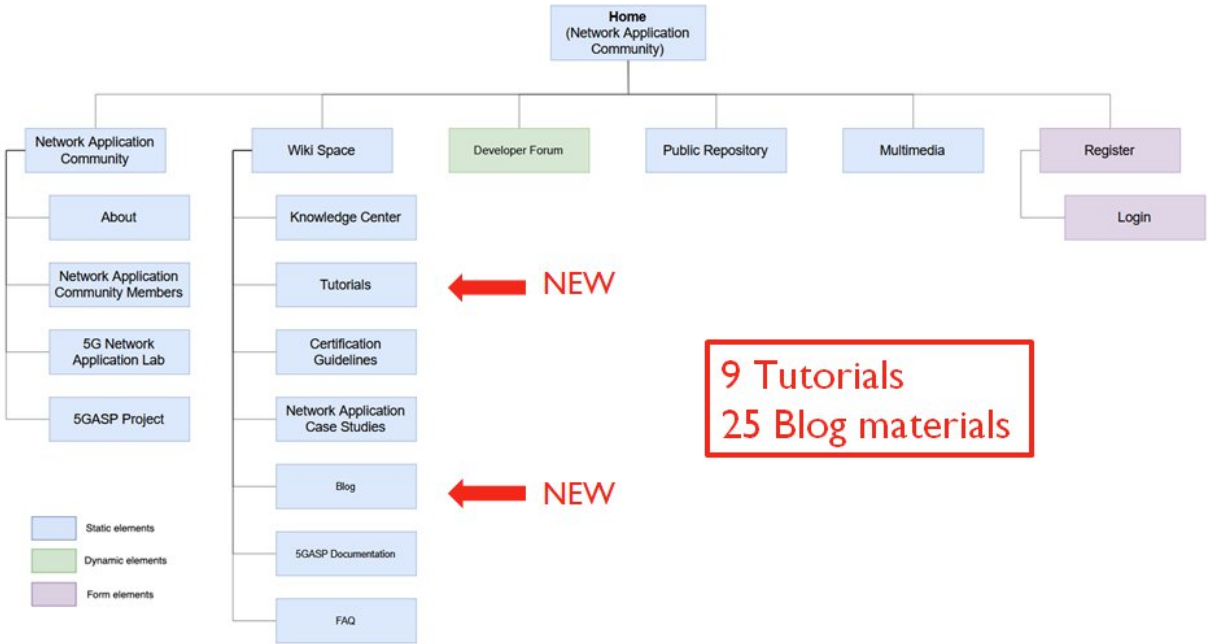

Figure 28 Updated site map for the Network Application Community portal.

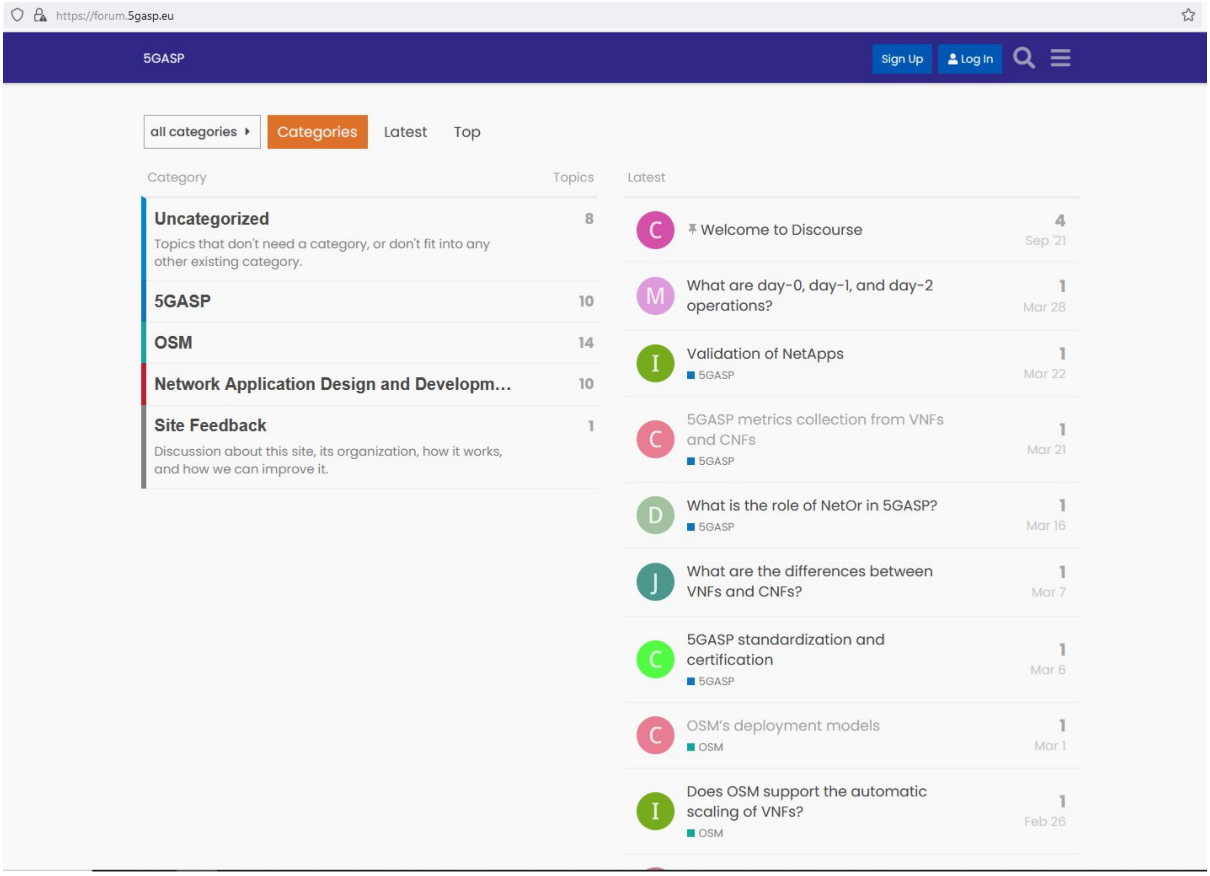

Figure 29 5GASP Developer Forum

The ‘Multimedia’ page currently provides video and photo materials, mostly in the form of video tutorials and lectures placed on the YouTube platform.

The ‘Registration’ page provides the site visitors with the opportunity to become Community members. When a new member organization is registered to the Community portal, a logo or representative photo of their choosing is added to the Network Application Community Members page (Figure 30).

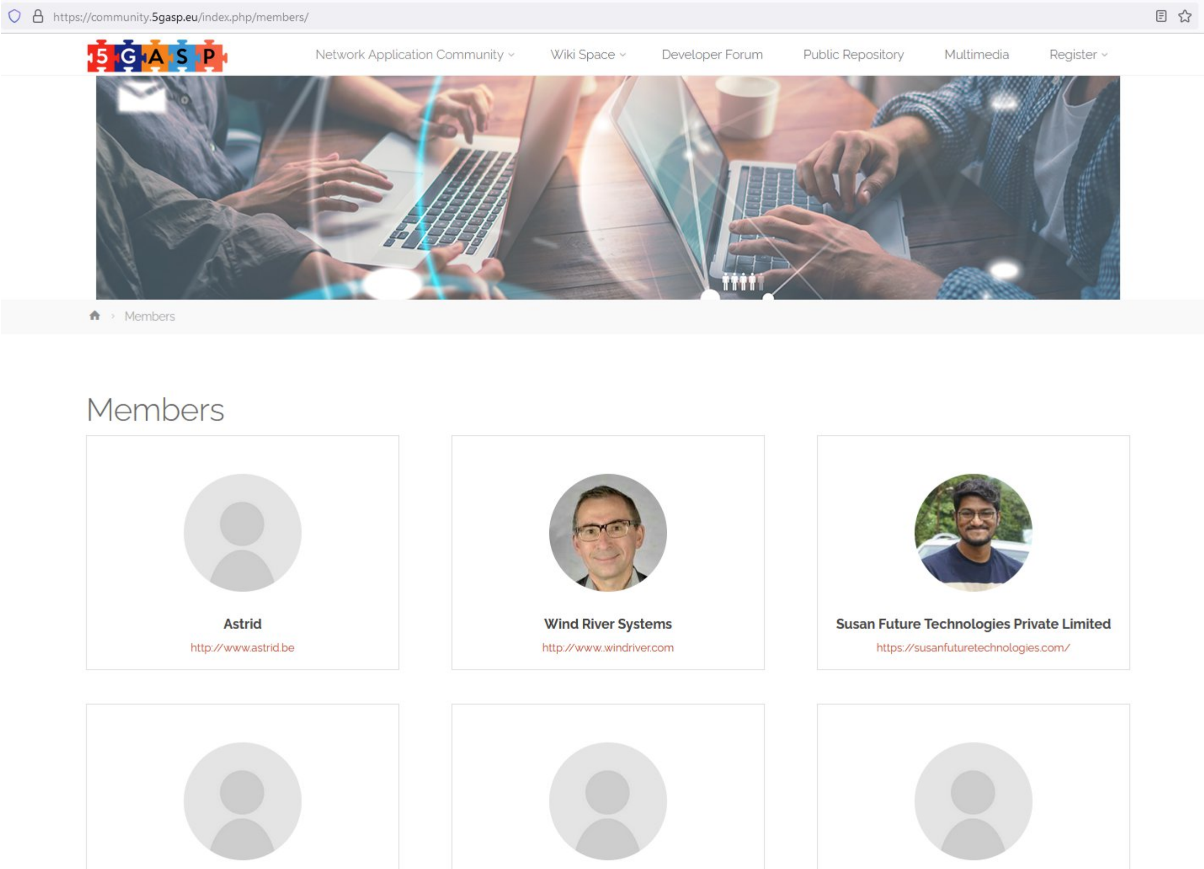

Figure 30 ‘Network Application Community Members’ page.

It is also important to note the re-integration and deployment of several pages essential for promotional activity and dissemination inside the Community Portal website:

- Events;
- News;
- Blog.

The main page of the portal also highlights the above-mentioned, by showcasing and categorising the latest posts appropriately (Figure 31), with the associated links attached.

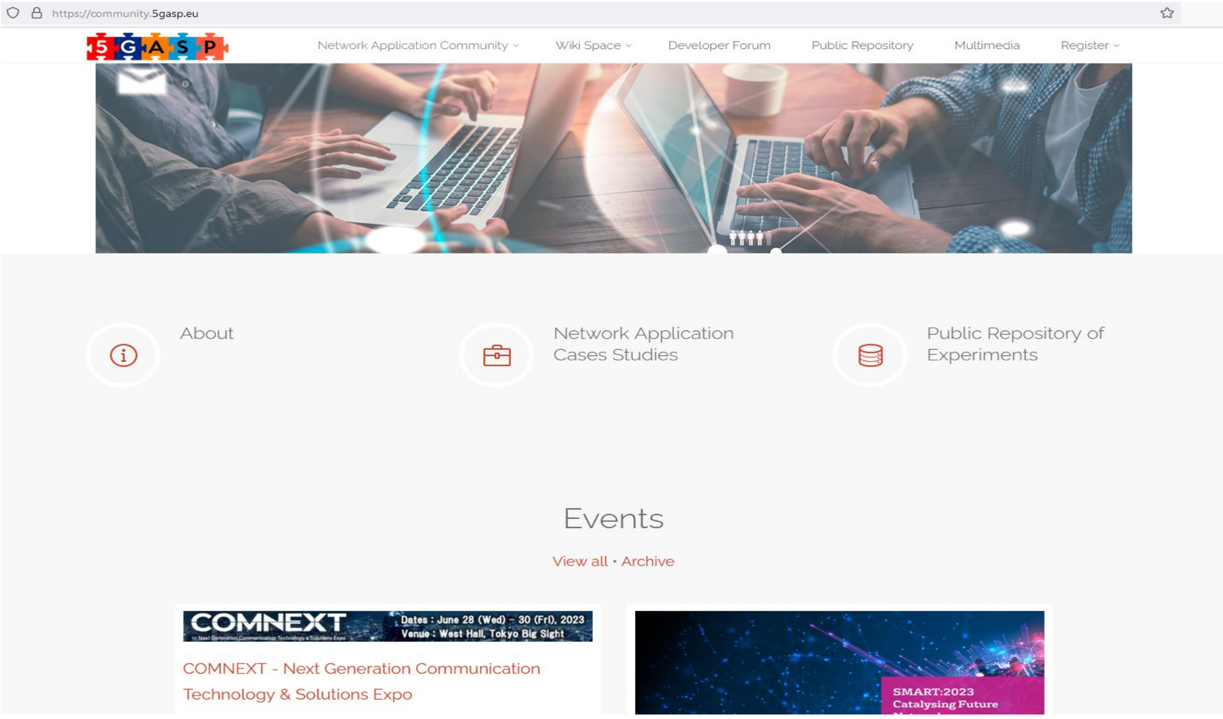

Figure 31 The main page of the Network Application Community portal

The developed final version satisfies all requirements of the Network Application Community development defined in our initial report D6.1 [27].

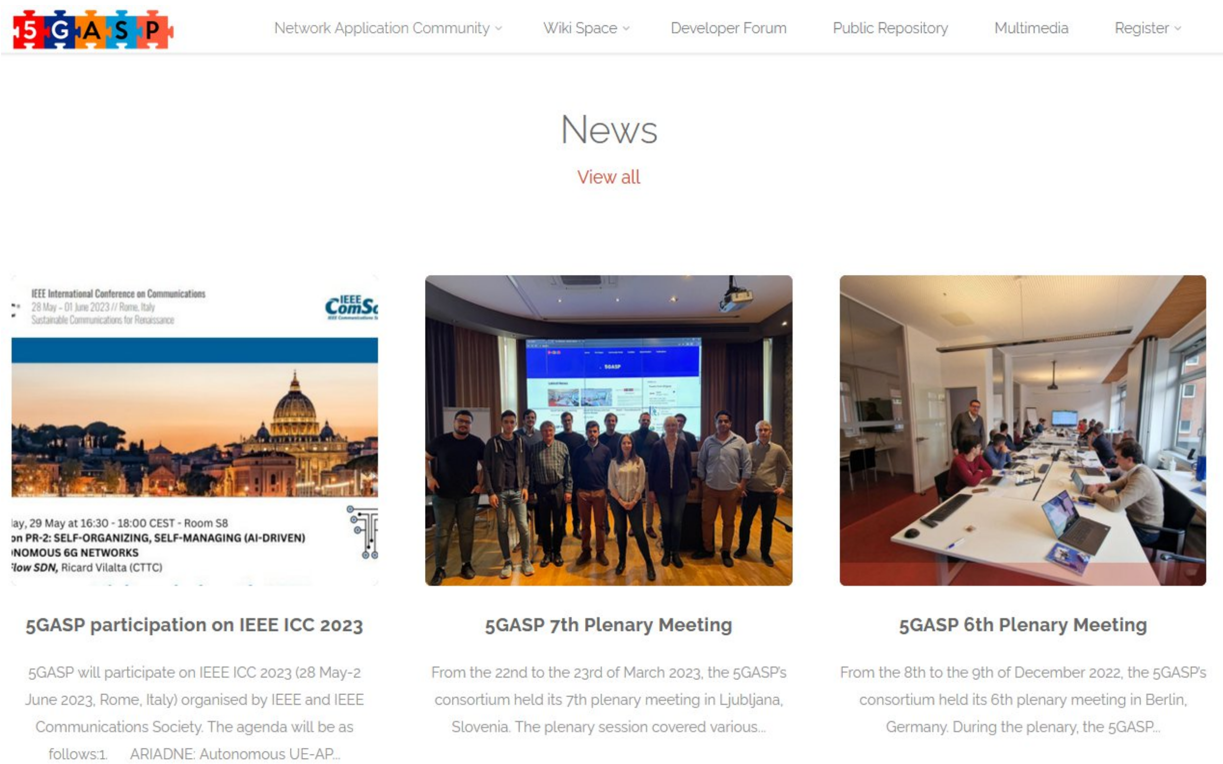

Figure 32 The Community Portal News

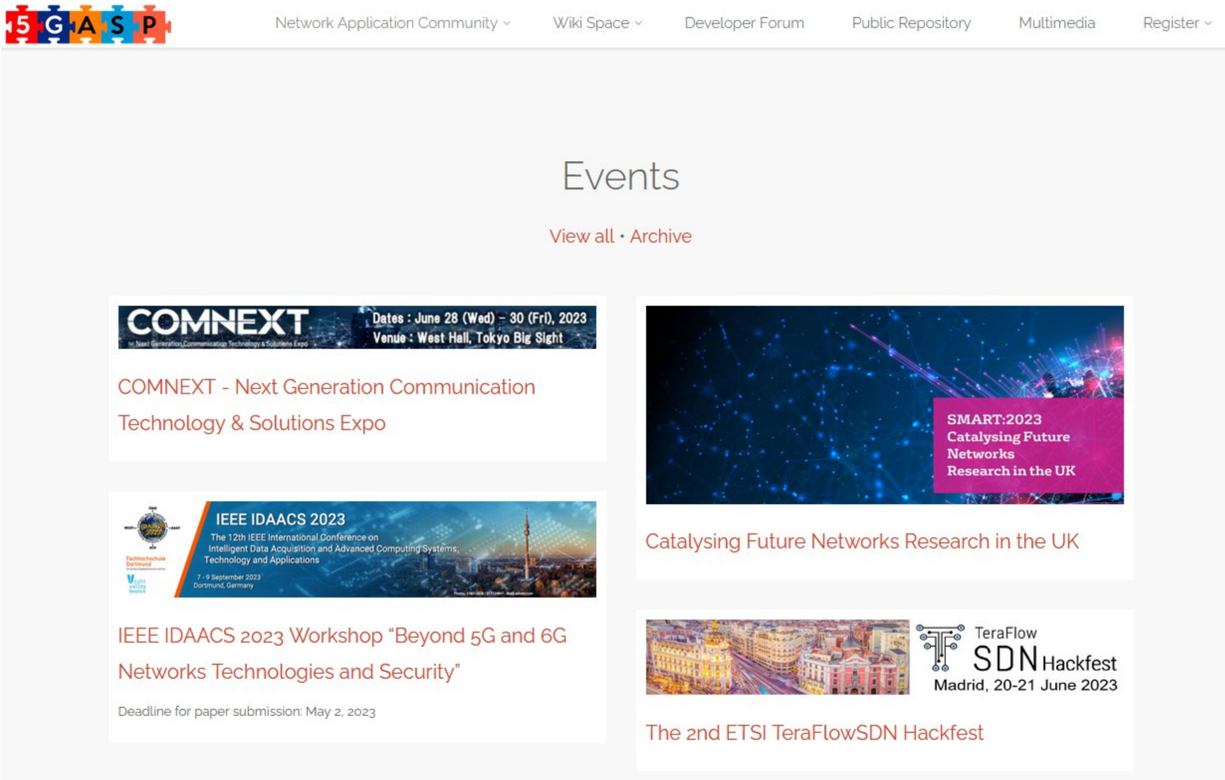

Figure 34 The Community Portal Events

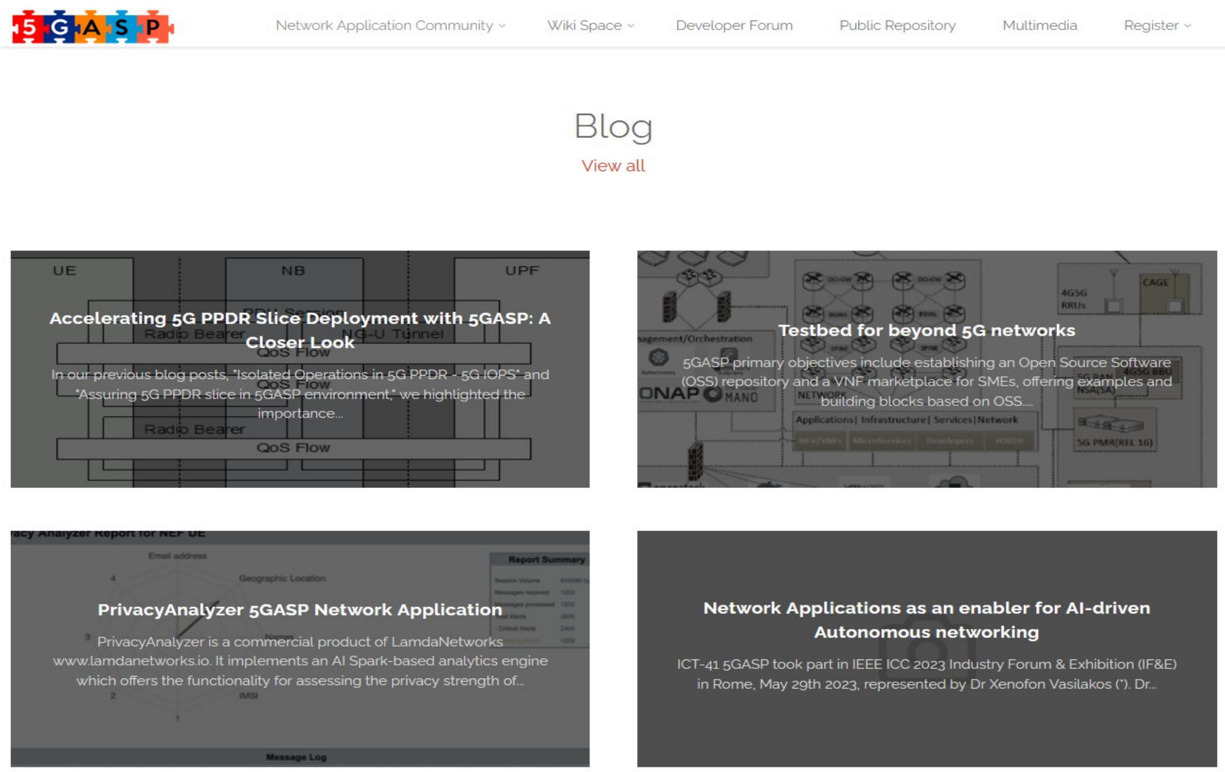

Figure 35 The Developer Forum Blog

4.3 Developer Forum

The developer forum was revised since the last update, and the delta is mainly covered in the above subsection. To start with, the supporting forum platform was changed. There is increased activity on the forum already, since the change and further dissemination, and the discussions around development and architecture have been started. As a result, further tutorials have been provided on the Community Portal(Figure 35).

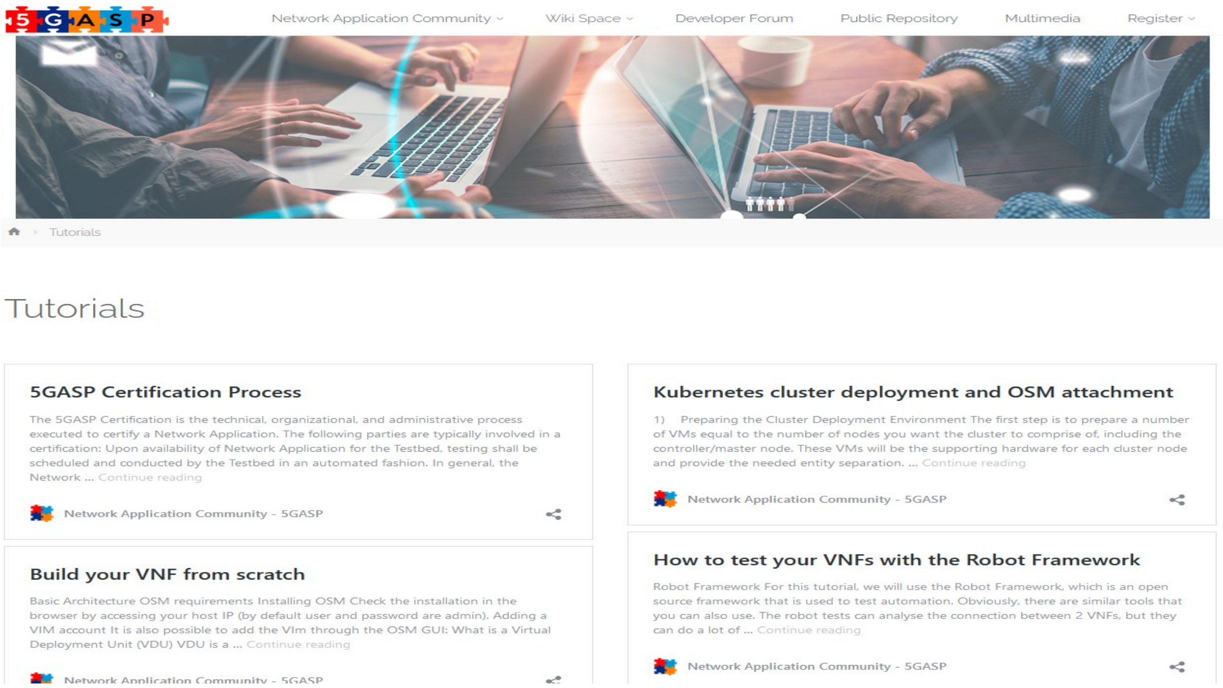

Figure 36 The Community Portal-based Tutorials

4.4 5GASP experimentation API services

This section provides an overview of all the APIs offered by 5GASP's Experimentation Services to the community.

4.4.1 CI/CD Service APIs

5GASP's CI/CD Service relies on a collection of APIs to (i) configure the testing and validation processes and (ii) to execute the tests offered by the 5GASP ecosystem.

Regarding the API for the testing/validation processes configuration, it is offered by the CI/CD Manager and can be used by (i) the CI/CD Service Admins, to perform create, read, update and delete (CRUD) operations on the CI/CD Agents, on the tests offered by the 5GASP ecosystem, etc, and (ii) by the NODS to trigger new validation processes and make available their results.

Figure 36 showcases the OpenAPI Specification of this API. Through this image, the reader may get acquainted with the operations supported through this API.

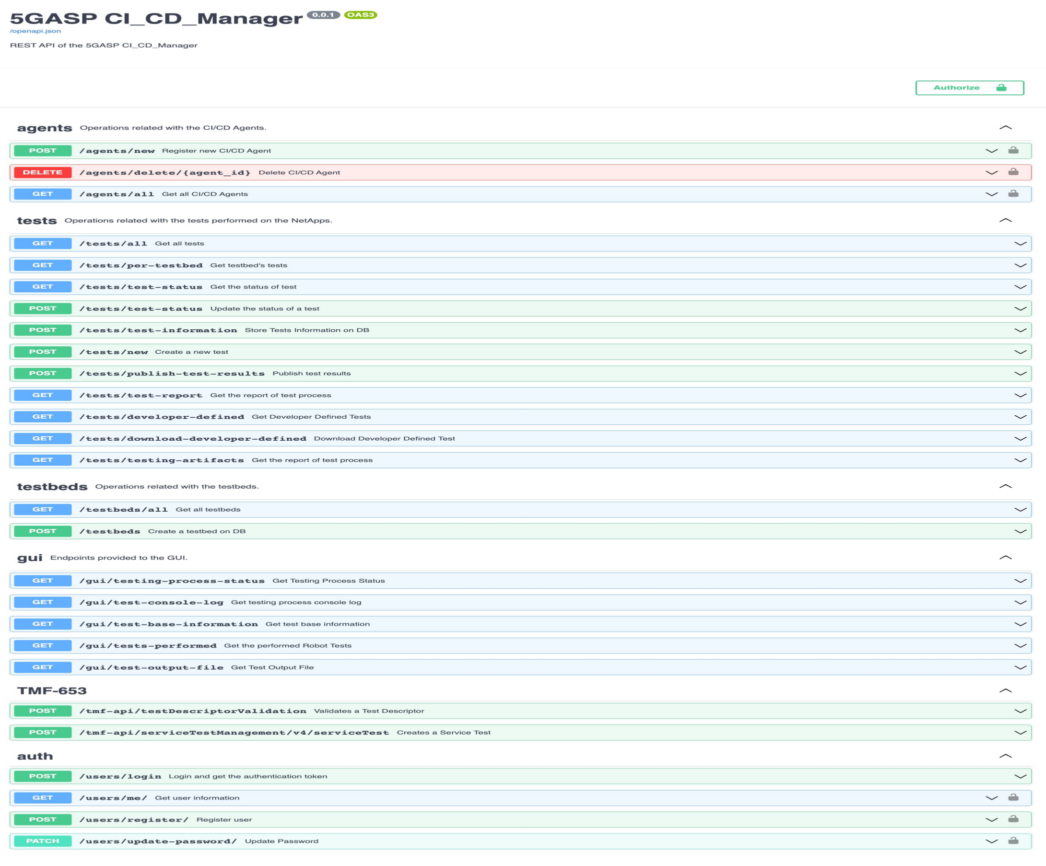

Figure 37 CI/CD Manager - OpenAPI Specification

Moving on to the APIs leveraged during the execution of the tests, 5GASP mainly relies on a Network Application-level API, which is used to trigger the execution of specific operations in the Network Application and thus allows for control of the tests execution flow.

Network Application-level API: This API must be implemented by the Network Application developers in order to support the triggering of specific operations in the Network Application. An example of this operations is the triggering of the interaction between the Network Application and the 5G System. When trying to validate this interaction, the CI/CD Service must be aware of when the interaction was started so it can monitor it and collect the logs of such integration, which will then be processed by the CI/CD Agents. Thus, we opted to define a Network Application-level API to trigger these interactions.

The CI/CD Agent is responsible for triggering the operations through this API and thus it is aware of when the interaction was started and can collect more meaningful logs. Even though the development of this API is delegated to the Network Application developers, the 5GASP Consortium provided a scaffold of it, to further support the developers in this effort. Figure 37 showcases the OpenAPI Specification of the developed scaffold API.

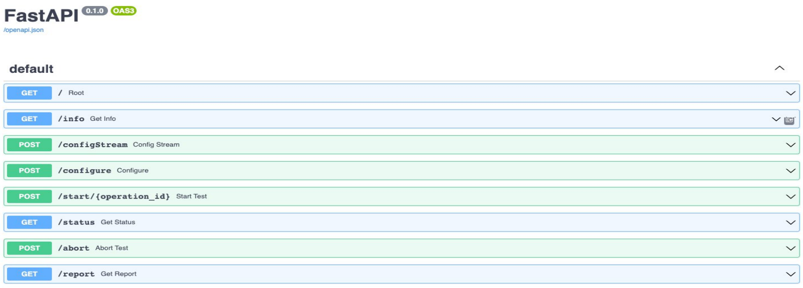

Figure 38 Network Application-level API - OpenAPI Specification (Scaffold)

The most crucial endpoints are the /configure and /start/{operation_id}ones. The /configure endpoint allows for the setting of specific information in the Network Application. For instance, the credentials needed for the Network Application to register itself with the 5G System.

On the other end, the /start/{operation_id} endpoint is used to trigger specific operations on the Network Application, for instance, to trigger the registering of the Network Application with the 5G System.

4.4.2 Test Descriptor Creation CLI

5GASP's CLI was developed to support the Network Application developers while developing the Testing Descriptors that shall steer the validation processes of their Network Applications. The CLI was specifically designed for the creation of Testing Descriptors for Virtualized Network Functions (VNFs) and in the future will be upgraded to support Containerized Network Functions (CNFs).

With its intuitive features and streamlined workflow, the 5GASP CLI empowers developers to accelerate the testing processes provided by 5GASP and deliver high-quality 5G applications. The CLI currently offers the following features:

List Testbeds: One of the features of the 5GASP CLI is its ability to effortlessly list available testbeds. By simply invoking a command, developers gain valuable insights into the various testbeds at their disposal, as well as the tests they make available. This feature facilitates informed decision-making when selecting the appropriate test environment, ensuring accurate and comprehensive testing scenarios for 5G applications.

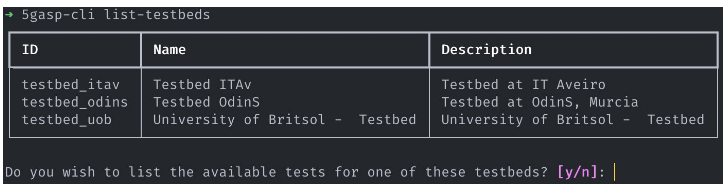

Figure 39 5GASP CLI - List Testbeds Command

List Available Tests: The 5GASP CLI provides a seamless method to list all the available tests in 5GASP ecosystem. Developers can easily explore a comprehensive catalogue of test cases, enabling them to align their testing strategies with specific requirements and industry standards. This feature fosters precision in testing, enhancing the overall quality of 5G applications.

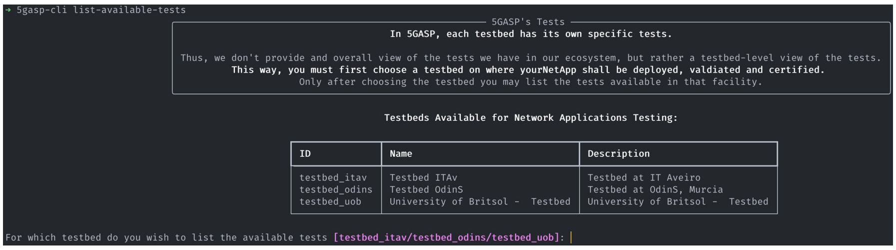

Figure 40 5GASP CLI - List Available Tests Command

Create a Testing Descriptor: The core functionality of the 5GASP CLI lies in its ability to create testing descriptors. With a straightforward command, developers can generate comprehensive and well-structured testing descriptors for their VNFs. This includes defining the desired test cases on a specific testbed, and any additional parameters necessary for testing Network Applications. The 5GASP CLI automates the process, saving developers valuable time and effort while ensuring consistency and accuracy in test descriptor creation.

The 5GASP CLI's intuitive features empower developers, SMEs, startups, and researchers to streamline the testing services provided by 5GASP and deliver robust and reliable 5G applications. By simplifying the creation of testing descriptors, providing visibility into available testbeds, and offering a comprehensive catalogue of test cases, the 5GASP CLI enhances productivity, accelerates development cycles, and contributes to the advancement of the 5G ecosystem.

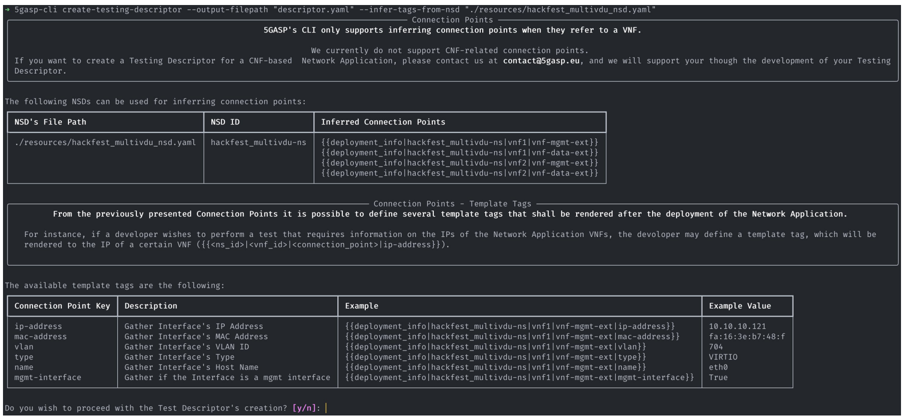

Figure 41 5GASP CLI - Create Testing Descriptor Command

5 Guidelines for Future Experimentations

This section covers off insights, lessons learned and recommendations as expressed and from the viewpoint of the Network Application developers using the 5GASP platform and getting certified through the 5GASP Certification Process.

5.1 Translation of Network Applications to suit 5GASP infrastructure

From the viewpoint of developers of the 5GASP consortium, it can be now said that the onboarding process through the 5GASP portal is a fairly user-friendly procedure. In terms of testing and certification, getting familiar with 5GASP's relevant procedures does require some time to read the relevant documentation and be acquainted with these procedures; however the learning curve is not steep and this is backed up by the support of the 5GASP testing and certification experts who have helped developers via replying to questions and organizing face-to-face video calls.

To develop a network application effectively, particularly for cooperative connectivity in the automotive vertical, the key is to document a high-level architecture for each application, and the developer-specific test cases. This documentation should encompass vertical design principles, all utilized standards, data flows, decision-making processes, and operational aspects. By creating documentation that is developer-friendly and promoting knowledge sharing, future developers can easily grasp the components, dependencies, and operational procedures of the system. This fosters potential collaboration, interoperability among similar network applications, and future enhancements.

In the case of a VNF Network Application Developer that has a commercial grade network application already, we had to take an approach to create a simplified "stripped" network application to be capable of working with the hardware available in 5GASP testbeds. The VNF also had to be adapted to consider certain network limitations of 5GASP Infrastructure. Effort was invested in this activity because we are new to 5G and had to adapt to the flexibility 5G introduced in terms of network, configuration and APIs. We did consider that this may not always be the case as developing application from scratch might be much easier to take in these considerations.

In the case of a CNF Network Application Developer 5GASP onboarding does not require any modifications to the codebase of the CNF application, or at least not much effort needed at the design time as the network application is Kubernetes based form scratch (already CNFised by design). Thus the main adaptation point was in regards to the 3GPP NEF NBI integration and API development for enabling direct communication by enhanced applications. For example as a CNF network application developer we had to move from a FlaskAPI framework to FastAPI, for the miniAPI adaptation, and to help support some security (SSL) requirements within the Kubernetes cluster environment of the 5GASP Platform.

A lesson learnt by the developers using container technology is that there are some cases (e.g. when persistent volumes are required by the network application) where the Helm chart of the developer might need a certain adaptation in order for all containers (along with their persistent volumes) to be successfully deployed on the relevant 5GASP testbed.

Certainly, there will always be cases where the developer might need to communicate with the testbed owners in order to solve such technical issues related to onboarding and to that end, the 5GASP consortium should be working on setting up a HelpDesk service that shall be mobilized to solve reported issues. Indeed, a HelpDesk service would significantly contribute to the project's mission to offer a user-friendly platform for Network Application developers.

Lesson Learned: The onboarding process through the 5GASP portal is a fairly user-friendly procedure, however time is needed to study and get familiar with 5GASP's relevant documentation and thus get acquainted with the 5GASP procedures.

Lesson Learned: Document a high-level architecture for each network application, and the developer-specific test cases. By creating documentation that is developer-friendly helps to promote knowledge sharing, between the hosting 5GASP testbed and network application developer, and once further shared on the community portal will help future developers to easily grasp the components, dependencies, and operational procedures of the 5GASP system.

5GASP Response: More detailed and specific technical lesson learned will be incorporated into the main content of the final deliverable for Work Package 4.

Lesson Learned: Creation of the testbed APIs for the standard general tests, this is a must to use as internal VNF tests would not be general enough and would not include a testbed interface, like the NEF.

Lesson Learned: How to design and develop robot network tests specific for our VNF application, basically the creation of the APIs according to the 5GASP defined standard.

Lesson Learned: How to update the network application, the descriptors and other required files for the next development cycle.

Lesson Learned: There are cases (e.g. when persistent volumes are required by the Network Application) where the Helm chart of the developer needs a certain adaptation in order for that container to be successfully deployed on the relevant 5GASP testbed.

5GASP Response: To this end, 5GASP is gathering the most frequent use cases demanding adaptation of the developer's Helm chart and are publishing them in our community portal in the form of FAQs.

Recommendation: A 5GASP Platform HelpDesk service to address cases where the developer might need to communicate with the testbed owners in order to solve technical issues related to onboarding.

5.2 Level of integration

As a Network Application developer the initial step we had to undertake was to adapt our application to suit the 5GASP platform and methodology was to transform our application towards the required NFV artefacts. In this context, VM-based applications are represented as VNFs, while cloud-native applications as CNFs, respectively. Optionally, in the case of a commercial Network Application, a centralized private image repository, i.e. 5GASP Harbor, is provided to facilitate the need for non-public access to the respective images. In terms of testing, we had to create the appropriate Test Descriptors referencing the desired tests to be executed.

Despite the extensive documentation provided, 5GASP also introduced the Test Descriptor creation CLI, which constructs the testing artefact from user-guided input, thus rendering the process even more accessible. Furthermore, along with the project-wide available tests made available through the 5GASP platform, it also facilitates the developer to onboard its own defined tests. In such a case, the latter are created through the Robot Framework, following the respective guidelines. Finally, to test and validate against the 5G awareness pipeline of 5GASP, the Network Application itself must incorporate the respective application logic, essentially consuming the 3GPP NEF NBI.

As a VNF Network Application developer in the PPDR space, our solution heavily depends on the underlying hardware since it uses real radio interface based on SDR (Software Defined Radio) or CPRI (Common Public Radio Interface) card connected to RRH (Remote Radio Head), so our initial deployment was realized via the VNF/VM principle. This was the “simplest” approach for us, since we are using commercial binaries, and all we had to do is pack everything that we typically do on a phyisical host into a VM. After that we were ready to deploy. But using that approach we were also limited regarding the dynamic configuration, upgrading meant building new VM images, we had to deal with various issues on the VM OS level, and maybe biggest disadvantage – the deployment time (cca 15 min).

During the project we decided to move to real cloud-native solution based on CNF/Kubernetes using Helm-chart. There were some initial issues that we had to solve since the commercial binaries were really not designed to be used in containers, so we invested a lot of time in this but in the end, we achieved completely configurable solution allowing us full day-1/day-2 config via OSM or even bypassing OSM and deploy natively on Kubernetes via Helm. The upgrades are now much easier since we just take the new binary and pack it in the container while not being so heavily dependent on the underlying OS. Finally, the deployment time now is about 3 min (without OSM is even closer to 2 min) for the whole 5G system – which we take as a great achievement.

As a CNF Network Application developer we wrote two tutorials “How to develop a Helm Chart” and "How to develop your CNF and orchestrate it through OSM". By reading the tutorials on the 5GASP Community Portal in specific order, you basically have all the steps as new developers to go from "zero to hero". In our case, before 5GASP, we were not using Helm charts and Kubernetes, we had containers just in Dockerfiles with everything running on managed AWS with ECS.

During 5GASP, we created helm charts for the first time, we worked with Kubernetes for the first time, it was not simple, this had a learning curve. Working with 5G NFV defined CNFs/NSDs also had a learning curve since we never heard of OSM. Working with OSM, we found the installation was difficult, and we had to come up to speed on writing and changing CNFs/NSDs, although this was a hassle since the documentation for OSM was not that friendly.

Using the NEF Emulator was a little simpler for us to understand, since we work with external APIs a lot in our company and it was not that hard to integrate and play with it. Making the application network aware was the last hassle since on AWS you usually do not prepare for network issues. They happen, but up to this point we never really dealt with them but now making our application network aware is something we actively back port into existing application work and consider as a must in new designs.

Lesson Learned: How to describe a Network Application using 5G NFV artefacts and getting clear that VMs = VNFs, Containers = CNFs and how and were the VNF and CNF are hosted and deployed on the 5GASP Platform. Adapting an application to the 5GASP platform can initially appear challenging due to the unfamiliarity with the NFV structure.

Lesson Learned: If privacy is needed for the network application container image, the Network Application Developer would need to onboard the respective images to the 5GASP Harbor repository.

Lesson Learned: Create developer-defined tests using the Robot Framework. This was the ability to create the appropriate Test Descriptors referencing the desired tests to be executing. This process is simplified by the Test Descriptor CLI, which constructs the Test Descriptor from user guided input.

Lesson Learned: How to onboard the newly created network application NFV artefacts to the 5GASP platform. This procedure was simplified by the introduction of an onboarding UI wizard, guiding the user through concise steps.

Lesson Learned: Make the move from VNF to CNF to be more flexible in terms of orchestration and configuration. Invest time and resources to develop Helm charts that will allow you to deploy in various ways, such as natively to Kubernetes/Helm or by using an orchestrator like OSM that uses Helm in the background too.

Lesson Learned: Kubernetes can be deployed over VM or physical infrastructure so using Helm you can basically deploy your Network Application everywhere. Also using Kubernetes/Helm enables many other options; one can be the integration of other Helm charts into your own Helm chart, e.g. include Prometheus/Grafana as an integral part of the Network Application and everything is deployed and managed via Helm.

Recommendation: Introduce code blocks to implement the 5G interaction logic (consume 3GPP NEF NBI)

6 Conclusions

The main goal of this document is to act as a revised version of 5GASP deliverable D2.1 [1], to essentially complement the D2.1 with information that corresponds to the progress made in Tasks T2.1 and across the whole 5GASP work programme since the delivery of 5GASP D2.1 [1] in December 2021.

To this end, D2.3 has four key topics to report on:

- A workflow process for the automated transformation of vertical applications to interoperable 5G/NFV artefacts;
- The definition of components of the 5GASP infrastructure that show that the platform is open, interoperable, extensible and standard;
- The definition of the 5GASP experimentation infrastructure that supports i) standardized 5G/NFV interfaces, ii) multi-domain scenarios, iii) seamless integration of 5G/NFV technologies and iv) automated transformations of 5G/NFV models;
- The definition of an architecture that supports the 5GASP open repository and knowledge base.

Updates to the 5GASP workflow process: Section 2.1 provided a full insight of the 5GASP workflow cycle, which comprises of the Network Application onboarding, deployment, testing, and validation. Section 2.1 provided a distinction between these various phases and provides deep insight through each respective workflow. This is complemented by the overview of the CI/CD Service in Section 3.3 and the CI/CD Services API and Test Description Creation CLI as presented in Section 4.4.

Updates to the definition of components of the 5GASP infrastructure: Section 2.2 and 2.3 provided an update on the commonality in 5GASP Infrastructure capabilities by presenting insight on the federated monitoring capability that was added to the 5GASP platform testbeds, along with how network applications may now communicate with 5G Core functions within 5GASP via the Network Exposure Function (NEF) using the 3GPP defined N33 interface for NEF. Section 2.4 gives an insight in to how the 5GASP infrastructure is conforming to network application vertical-specific requirements as originally stated in D2.1. Section 2.5 provides an overview of commonality identified across the ICT-41 programme and also some insights from the perspective of other commercially focused 5G labs.

Updates on the Internal and External Components of 5GASP: Section 3 is dedicated to providing updates on the 5GASP NODS, highlighting the single-entry point portal that facilitates the seamless onboarding, design, and orchestration of both network applications and their corresponding test suites. Section 3 also provides an update per 5GASP test site, which complements the presentations already reported from D2.1.

Updates to the 5GASP open repository and knowledge base: Section 4 provides an update on the 5GASP Marketplace, the 5GASP Community Portal, and the 5GASP Developer Forum, along with Section 5 which provides lessons learned and recommendations as expressed and from the viewpoint of the Network Application developers using the 5GASP platform.

Overall, this deliverable presented the current status of the 5GASP experimentation infrastructure, with a view on how it is designed to support the 5GASP Network Application Certification Process and highlighted how standardized 5G/NFV interfaces are used; how multi-domain scenarios are supported across testbeds; how there is seamless integration of 5G/NFV technologies that can be used by both VNF & CNF network application developers; and how automated transformations of 5G/NFV models is performed via the 5GASP End-to-End Workflow.

7 References

[1] 5GASP Deliverable D2.1 Architecture, Model Entities Specification and Design, December 2021, Available online: https://www.5gasp.eu/assets/documents/deliverables/D2.1%20Architecture,%20Model%20Entities%20Specification%20and%20Design.pdf

[2] 5GASP Deliverable D6.2 Interim progress report on NetApps Community & Certification process, December 2022, Available online: https://www.5gasp.eu/assets/documents/deliverables/D6.2.pdf

[3] 5GASP Deliverable D5.4 Initial Report for the Network Application certification testing, March 2023, Available online: https://www.5gasp.eu/assets/documents/deliverables/D5.4%20Initial%20Report%20for%20the%20Network%20Application%20certification%20testing.pdf

[4] 5GASP Deliverable D3.1. Available online: https://www.5gasp.eu/assets/documents/deliverables/D3.1%20Experimentation%20Services,%20Middleware%20and%20Multi-Domain%20Facilities%20Continuous%20Integration.pdf

[5] 5GASP Deliverable D3.2 5GASP experimentation services, middleware and multi-domain facilities continuous integration, 2nd release, June 2022, Available online: https://www.5gasp.eu/assets/documents/deliverables/D3.2%205GASP%20experimentation%20services,%20middleware%20and%20multi-domain%20facilities%20continuous%20integration.pdf

[6] Prometheus, https://prometheus.io/, online

[7] Grafana, https://grafana.com/, online

[8] NEF Emulator, https://github.com/EVOLVED-5G/NEF_emulator, online

[9] 3GPP, "TS 26.501, 5G Media Streaming (5GMS); General description and architecture, Release 17, v17.5.0", Mar. 2023

[10] VITAL-5G, https://www.vital5g.eu/, online

[11] VITAL-5G Deliverable D1.3, "VITAL-5G system specifications and architecture including experiment-based upgrades", February 2023.

[12] VITAL-5G Deliverable D1.2, "System Specifications and Architecture", December 2021.

[13] 5G-IANA, https://www.5g-iana.eu , online

[14] 5G-IANA Deliverable D2.1 Specification of the 5G-IANA architecture, May 2022

[15] 5G-EPICENTRE, https://www.5gepicentre.eu , online

[16] 5G-EPICENTRE Deliverable D1.4 Experimentation requirements and architecture specification final version, January 2023

[17] 5G-EPICENTRE Deliverable D1.3 Experimentation requirements and architecture preliminary version, June 2021

[18] JFrog Artifactory, https://jfrog.com/artifactory/ , online.

[19] Habor, https://goharbor.io/ , online.

[20] Openslice: An opensource OSS for Delivering Network Slice as a Service https://arxiv.org/abs/2102.03290, online

[21] TM Forum, "TMF633 – Service Catalog Management API REST Specification", 2021

[22] TM Forum, "TMF653 – Service Test Management API REST Specification", 2021

[23] Robot Framework - https://robotframework.org/ , online

[24] IETF RFC 6763, Cheshire, S. and Krochmal, M. (2013). DNS-Based Service Discovery

[25] 5GASP Services Marketplace, https://portal.5gasp.eu , online

[26] 5GASP Network Application Community portal, https://community.5gasp.eu , online

[27] 5GASP Deliverable D6.1 Initial report on building NetApps Community & defining a certification process, Available online: https://www.5gasp.eu/assets/documents/deliverables/D6.1%20Initial%20report%20on%20building%20NetApps.pdf

Appendix

Testbed facilities capabilities

Table 3. Testbed capabilities per facilities site.

	Aveiro	**Murcia**	**Bristol**	**Ljubljana**	**Patras**	**Bucharest**
Maximum number of Cores per VNF	4	8	6	8	8	8
Maximum RAM per VNF	4GB	16GB	10GB	16GB	16GB	16GB
Maximum Storage per VNF	50GB	30GB	30GB	40GB	40GB	40GB
Maximum number of VNF's	40 (Total)	40 (Total)	2 per network service	20 (Total)	80	40 (Total)
5G Release	Release 15 - SA	Release 16 - SA	Release 15	Release 15	Rel.15/Rel.16 5G NSA/SA	Release16
MANO Version	OSM Release 10	OSM Release 10	OSM Release 10	OSM Release 10	OSM Release 10	OSM Release 10
VIM	Openstack Wallaby	Openstack Rocky	Openstack Wallaby	OpenStack Wallaby	Openstack Rocky	
CIM	-	-	K8s 1.21	K8s 1.21	K8s 1.23	
Bandwidth available to reach testbed	Approx. 1Gbps Mbps (GEANT)	Approx. 1Gbps (GEANT)	Approx. 70 Mbps	100Mbps	Approx. 1Gbps Mbps (GEANT)	100Mbps (Internet)
Bandwidth available to UE	DL: 1.1Gbps UL: 160 Mbps	DL: ~600 Mbps UL: ~160 Mbps	DL: ~700 Mbps UL: 150 Mbps	1000Mbps/100Mbps	DL: ~720 Mbps UL: 120 Mbps	1000Mbps/150Mbps
Number of UE	5	1 Smartphone + 5 USB Modems + 64 Simbox vUEs	20	4	12	5
Number of CPE	10	5 custom	-	2	6	5
Support Automotive Vertical	YES	Yes	Provisionally (under cross-use case scenarios with PPDR)	Yes (No RSUs or V2X devices)	Yes (No RSUs or V2X devices)	Yes
Support PPDR Vertical	YES	Yes	YES	Yes	Yes	Yes

5GASP Certification process workflow

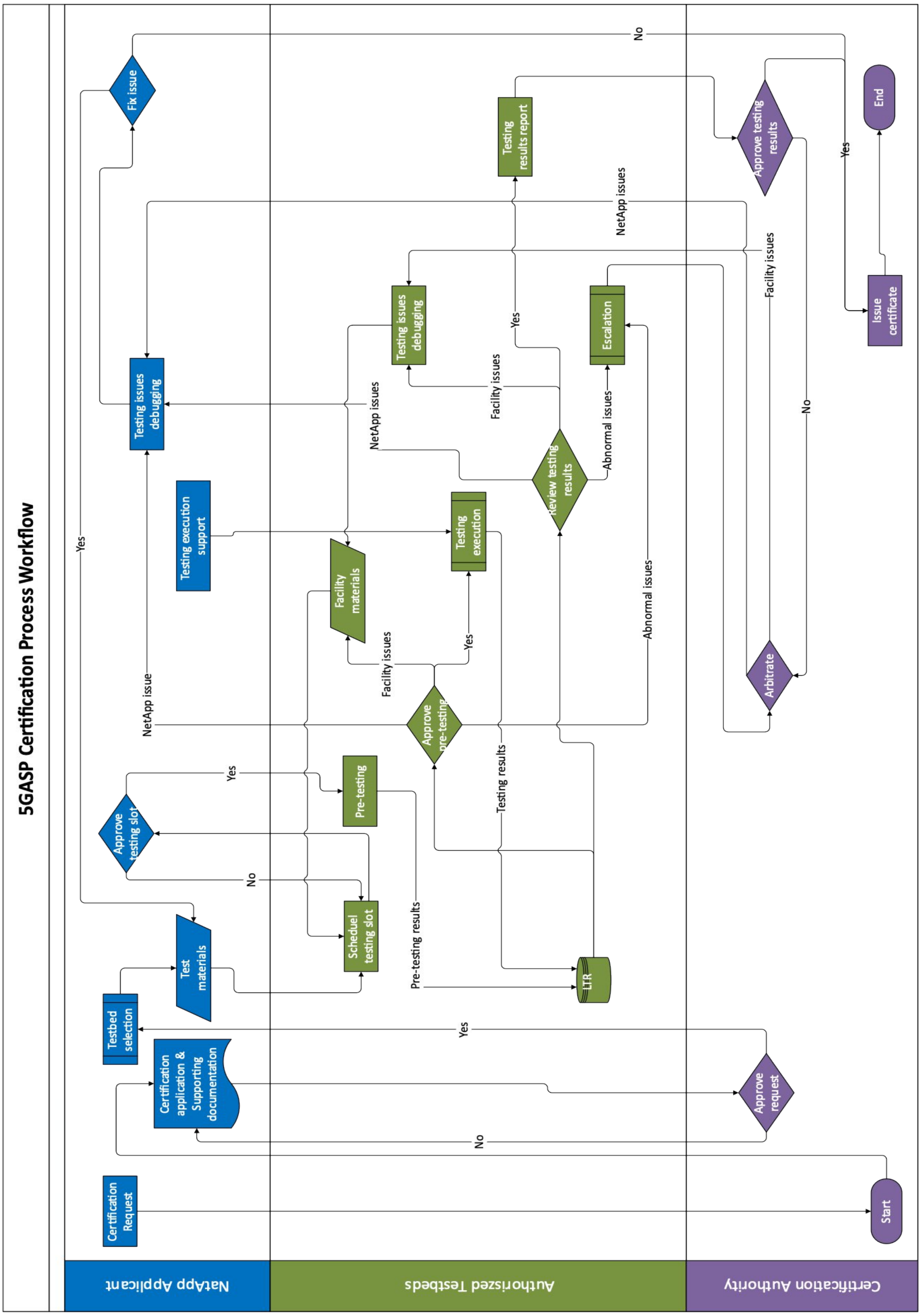

Figure 42. 5GASP Certification process workflow