H2020 5GASP Project

Grant No. 101016448

D4.4 Principles and Recommendations for Network Application development in Automotive and PPDR verticals

Abstract

The aim of this task in this project is to formulate the experiences, principles, recommendations, good practices and lessons learned that could help SMEs to develop their own Network Applications focusing on the different and specific requirements that each vertical has by applying the aspects of the methodology proposed in T4.1. This effort will facilitate both the future Network Applications development in general, but also will contain experiences and specific guidelines and optimizations for Automotive and PPDR verticals. For example, how to tackle with the special requisites of vertical specific physical assets, such as OBUs, PPDR UE, and how to deliver well-tested, interoperable, with low Service Creation time, ready-to-be-used Network Applications. All valuable information will be included in the D4.4. The resulting guidelines will assist SMEs to smoothly adapt their Network Applications to the platform. Using the guidelines, SMEs will be able to save time and effort and expedite the time to market of their Network Application.

This deliverable will contain all the details about the development phases in the process of creating the proposed Network Applications in the task **T4.2, T4.3,** and also the principles and recommendations formulated in **T4.4**, specifically related to the Automotive and PPRD verticals.

Document properties

Document number	1
Document title	D4.4 **Principles and Recommendations for Network Application development in Automotive and PPDR verticals**
Document responsible	Eli Shapira
Document editor	
Editorial team	
Target dissemination level	Public
Status of the document	reviewed version
Version	1.0

Document history

Revision	Date	Issued by	Description
0.1	21/08/2023	DriveU	Initial draft
0.2	25/09/2023	DriveU	Final draft
0.3	10/10/2023	EANTC	Review
0.4	11/10/2023	Neobility	Review
0.5	14/10/2023	OdinS	Review
1.0	16/11/2023	OdinS	Final version

List of Authors

Company	Name	Contribution
DriveU	Eli Shapira	Table of Contents, editor Network Application experience
ITAv	Diogo Gomes Rafael Direito	IT Aveiro Facility Testbed owners experience
UNIVBRIS	Adrian-Cristian Nicolaescu Juan Parra Ullauri Xenofon Vasilakos	Testbed owners experience Network Application experience
UoP	Kostis Trantzas Christos Tranoris Ioannis Chatzis	Patras Facility Testbed owners experience Network Application experience
Neobility	Andrei Radulescu	Network Application experience
OdinS	Ana Hermosilla Jorge Gallego-Madrid	Murcia Facility Testbed owners experience Network Application experience
Lambda	Leonidas Lymberopoulos	Network Application experience

Disclaimer

This document has been produced in the context of the 5GASP Project. The research leading to these results has received funding from the European Community's H2020 Programme under grant agreement number 101016448.

Contents

Contents

ABSTRACT **2**
DOCUMENT PROPERTIES **3**
DOCUMENT HISTORY **3**
LIST OF AUTHORS **3**
DISCLAIMER **4**
CONTENTS **5**
LIST OF FIGURES **6**
LIST OF ACRONYMS **7**
DEFINITIONS **10**
1. INTRODUCTION **11**
EXECUTIVE SUMMARY 11
OBJECTIVES OF THIS DOCUMENT 11
DOCUMENT STRUCTURE 11
2. OVERVIEW **13**
SUMMARY FOR NETWORK APPLICATION DEVELOPERS 13
Design *14*
Development *14*
Testing *14*
Validation *14*
5G FOR AUTOMOTIVE 15
Automotive-vertical Use Case (AUTO-V): Vehicle Routing Optimizer in a Virtual OBU with inter-domain migration support and testing of privacy of involved streaming data *15*
5G FOR PPDR (PUBLIC PROTECTION AND DISASTER RELIEF) 17
PPDR-vertical Use Case (PPDR-V): 5G Network Resilience and Privacy in the International Public Safety Operations *17*
Cross-vertical Use Case (CROSS-V): Autonomous Vehicle Teleoperations / Remote Driving Use Case *20*
3. 5GASP TESTBEDS EVOLUTION TO SATISFY VERTICAL REQUIREMENTS **22**
AUTOMOTIVE 22
PPDR 23
TESTBEDS FEATURES AND CAPABILITIES TO SUPPORT VERTICAL-SPECIFIC NETWORK APPLICATIONS 24
IT Aveiro Facility *24*
University of Patras Facility *27*
Murcia facility *29*
Internet Institute facility *29*
Bucharest Facility *31*
4. 5GASP NETWORK APPLICATIONS DEPLOYMENT EXPERIENCE **35**
NETWORK APPLICATION ADAPTATION FOR TESTBED REQUIREMENTS 35
Integration with Testbed Process Description *36*
Testing the Network Application *38*
RECEIVING RESULTS AND CERTIFICATION 39
5. CASE STUDIES **43**
CASE STUDY 1 43
CASE STUDY 2: 44

Cases studies summary 45
6. SUMMARY 46
Key Takeaways: 46
Importance of Guidelines: 46
Recommendations for SMEs: 46
BIBLIOGRAPHY 47

List of Figures

Figure 1 Verticals description 13
Figure 2 Methodology for Network Application Developers 14
Figure 3 Automotive use case – Initial setup 15
Figure 4 Automotive use case – OBU connects to the network 16
Figure 5 Automotive use case - Vehicle changes cell 16
Figure 6 Automotive use case – New vOBU assigned 17
Figure 7 PPDR-vertical use case – normal operation 18
Figure 8 PPDR-vertical use case – disaster operation 19
Figure 9 PPDR-vertical use case – improving network operation 19
Figure 10 PPDR-vertical use case – cross-border operation 20
Figure 11 Cross vertical use case 20
Figure 12 NPCF Policy Authorization API 23
Figure 13 ITAV Industry-grade 5G Locations 25
Figure 14 5Gainer distributed 5G network 26
Figure 15 ITAV Industry-grade Available 5G Core Functions 26
Figure 16 5G Transport Network SDN Switch 27
Figure 17 University of Patras facility 27
Figure 18 Patras5G quadruped robot 28
Figure 19 OBUs in the vehicle in Murcia facility 29
Figure 20 ININ's 5G mobile system running in IOPS mode 30
Figure 21 ORO's facility architecture 32
Figure 22 Bristol testbed locations 32
Figure 23 Real trace map 33
Figure 24 Real-world results 33
Figure 25 Certification process workflow 40

List of Acronyms

5GASP	5G Application & Services experimentation and certification Platform
AMF	Access and Mobility Management Function
AI	Artificial Intelligence
API	Application Programming Interface
ARFCN	Absolute Radio-Frequency Channel Number
AWS	Amazon Web Services
BBU	Base-band Unit
BW	Bandwidth
CI/CD	Continuous Integration and Continuous Deployment
C-ITS-S	Cooperative Intelligent Transport Systems Station
CN	Core Network
CNF	Cloud-native Network Function
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
C-V2X	Cellular Vehicle to Everything
D2D	Device-to-Device
DevOps	Development and Operations
DL	Download
DNS	Domain Name Service
DQT	Data Quality Testing
DRT	Demand Responsive Transport
DSP	Digital Services Provider
EMHO	Efficient MEC Handover
eNB	Evolved NodeB (=LTE/4G Base Station)
FTP	File Transfer Protocol
gNB	gNodeB (= 5G Base Station)
GPS	Global Positioning System
GST	Generic Network Slice Template
GTP	General Tunneling Protocol
HDD	Hard Disk Drive
HW	Hardware
HTTP(S)	HyperText Transfer Protocol (Secure)
ICMP	Internet Control Message Protocol
IOPS	Isolated Operations for Public Security
IoT	Internet of Things
IPv6	Internet Protocol version 6
ITS	Intelligent Transport Systems
ITS-S	Intelligent Transport Systems Station
JSON	JavaScript Object Notation
K8s	Kubernetes
KNF	Kubernetes Native Function
KPI	Key Performance Indicator
MANO	MANagement and Orchestration

MC	Mission-Critical
MCC	Mobile Country Code
MEC	Multi-access Edge Computing
MNC	Mobile Network Code
MNO	Mobile network operator
OBU	On-Board Unit
OSM	Open-Source MANO
nApp	Network Application
NEST	Network Slice Type
NFV	Network Function Virtualization
NFVI	Network Functions Virtualization Infrastructure
NFVO	NFV Orchestrator
NS	Network Services
NSA	Non-Standalone
NSD	Network Service Descriptor
NSP	Network Service Provider
NR	New Radio
OBU	On-Board Unit
OSM	Open-source MANO
PII	Personal Identifiable Information
PLMN	Public Land Mobile Network
PLR	Packet Loss Ratio
PNFD	Physical Network Function Descriptor
PoC	Proof of Concept
PoP	Point of Presence
PPDR	Public Protection and Disaster Relief
R2C	Roadside-to-Cloud
RAM	Random Access Memory
RAN	Radio Access Network
RAT	Radio Access Technology
REST	REpresentational State Transfer
R-ITS-S	Road-side Intelligent Transport System Station
RO	Resource Orchestrator
RQT	Radio Quality Testing
RSU	Road-Side Unit
RT	Real-Time
RTSP	Real-Time Streaming Protocol
SA	Standalone
SDR	Software Defined Radio
SNMP	Simple Network Management Protocol
SMEs	Small and Medium-sized Enterprises
SDN	Software Defined Network
UE	User Equipment
UL	Upload
URL	Uniform Resource Locator
V&V	Validation and Verification

V2C/C2V	Vehicle-to-Cloud / Cloud-to-Vehicle
V2X	Vehicle-to-everything
V-ITS-S	Vehicle Intelligent Transport Systems Station
VIM	Virtual Infrastructure Management
VM	Virtual Machine
VNF	Virtual Network Function
VNFD	Virtual Network Function Descriptor
vOBU	Virtual On-Board Unit
vRSU	Virtual Road-Side Unit
WP	Work Package

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

Executive summary

The document synthesizes a wealth of experiences, principles, and good practices, particularly focusing on the Automotive and PPDR verticals. Moreover, it lays special emphasis on the methodology proposed in Task T4.1 as a foundational framework for navigating the unique challenges these verticals present.

What sets this document apart are its guidelines, which are not just theoretical constructs. They are the culmination of hands-on experiences and lessons learned from the field. These guidelines are designed to simplify the development process, ensuring the creation of well-tested, interoperable Network Applications. For SMEs, this streamlines the adaptation process to various platforms, thus saving both time and effort.

The document also underscores the importance of understanding vertical-specific requirements, especially those concerning the Automotive and PPDR sectors. It provides actionable recommendations for dealing with special requisites like vertical-specific physical assets. By closely adhering to these guidelines and recommendations, SMEs position themselves favorably to expedite the time-to-market of their Network Applications, gaining a significant competitive edge.

In conclusion, the D4.4 document is an invaluable resource for SMEs. Its practical guidelines and actionable recommendations offer a clear pathway to rapid market entry and sustainable growth in the field of Network Applications development.

Objectives of this document

- To provide a comprehensive overview of experiences and principles that can guide SMEs in Network Applications development.
- To offer actionable recommendations and good practices for effective Network Applications creation and deployment.
- To outline the specific requirements and challenges faced by different verticals, with a focus on the Automotive and PPDR sectors.
- To discuss methods and optimizations that can accelerate the time-to-market of Network Applications.
- To present a methodology that integrates these aspects, aiding SMEs in adapting their Network Applications to various platforms.

Document structure

The H2020 5GASP Project's D4.4 Principles and Recommendations for Network Application development in Automotive and PPDR verticals is structured as follows:

1. Document properties: This section includes the document number, title, responsible person, editor, target dissemination level, status of the document, and document history.

2. Overview: This section provides an overview of the document's purpose, which is to offer actionable recommendations and good practices for effective Network Applications creation and deployment. It also outlines the specific requirements and challenges faced by different verticals, with a focus on the Automotive and PPDR sectors. Additionally, this section discusses methods and optimizations that can accelerate the time-to-market of Network Applications and presents a methodology that integrates these aspects, aiding SMEs in adapting their Network Applications to various platforms.
3. Development Phases: This section contains all the details about the development phases in the process of creating the proposed Network Applications in the task T4.2, T4.3, and also the principles and recommendations formulated in T4.4, specifically related to the Automotive and PPDR verticals.
4. Guidelines and Optimizations: This section provides valuable information and specific guidelines and optimizations for Automotive and PPDR verticals. It includes how to tackle with the special requisites of vertical-specific physical assets, such as OBUs, PPDR UE, and how to deliver well-tested, interoperable, with low Service Creation time, ready-to-be-used Network Applications.
5. Use Cases: This section identifies Automotive and PPDR verticals as those of most relevance to showcase the innovation with a set of use cases resulting from different Network Applications orchestrations. It targets 3 use-cases: Automotive, PPDR, and a Cross Vertical.
6. Conclusion: This section summarizes the key takeaways from the document and emphasizes the importance of the guidelines and recommendations provided for SMEs looking to develop Network Applications in the Automotive and PPDR verticals.

2. Overview

In order to provide opportunities for SMEs and developers to experiment their applications in the context of specific vertical use cases we have identified Automotive and PPDR vertical as those of most relevance to showcase our innovation with a set of use cases resulting from different Network Applications orchestrations. We will target 3 use-cases: Automotive, PPDR and a Cross Vertical.

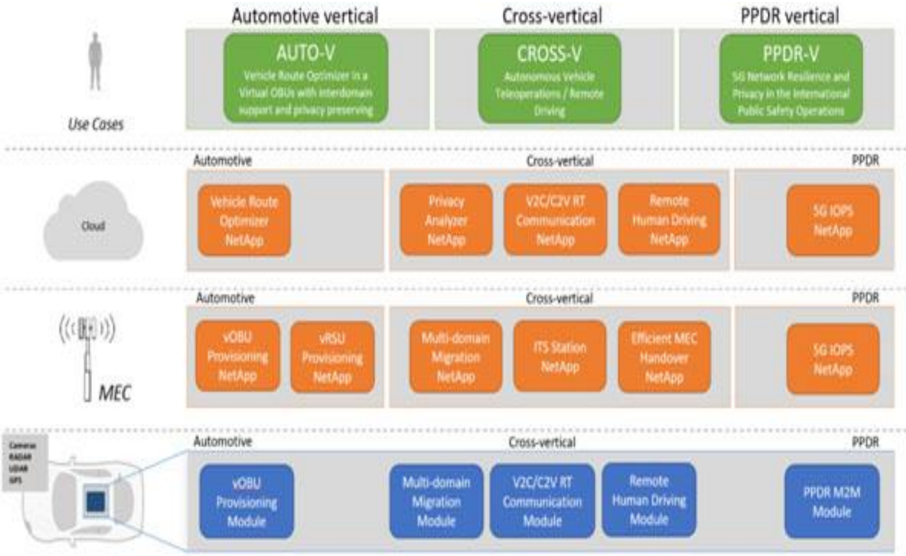

Figure 1 Verticals description

To integrate existing applications in the 5G ecosystem, the 5GASP project defined a Network Application design and development methodology [1]. By following these steps, the developers and experimenters can easily adapt their services to interact with the 5G system and to be validated and certified in the 5GASP framework. This methodology is the result of the work among developers, experimenters, testbed owners, customers and verticals to define an easy way of entering the 5G Network Applications world with little previous knowledge. The 5GASP methodology is composed of four main phases: design, development, testing, and validation.

Summary for Network Application Developers

1. Design: analysis of the Network Application and definition of the main descriptors.
2. Development: materialize the previous design considerations and develop the main descriptors, the result is a Network Application ready to be on-boarded to the 5GASP portal.
3. Testing: evaluate different dimensions of the network application, such as 5G readiness, security, performance, availability, etc.
4. Validation: validate the results of the testing phase to determine whether it satisfies the specified requirements and can be certified.

Figure 2 Methodology for Network Application Developers

Design

Several 5G-specific considerations have to be addressed by the Network Application developers to adapt their existing services to the 5G ecosystem. The first step is to define the main components of the Network Application and their interconnections. With this, the developers will be able to clearly define the list of VNFs or CNFs needed. Then they have to come up with the 5G network requirements the application will demand, so it can be properly hosted in the 5G testbeds. Finally, the developers have to define the suite of tests that will validate the functioning and performance of the Network Application so it can be certified to operate in 5G networks.

Development

When the design is finalized, the development of the different descriptors that compose the Network Application can be performed. In first place, the VNFDs/NSDs or the Helm Charts have to be developed, then the GST/NEST that represents the required network slice, and then the test suite that will assess the Network Application once deployed. At this point, it will be ready to be on-boarded.

Testing

Once deployed, the 5GASP framework will automatically execute the suite of tests defined by the developer or experimenter that will stress the Network Application and will evaluate its performance, functioning, security and 5G readiness, among other things.

Validation

The results of the tests will be evaluated and compared with the requirements demanded by the Network Application owner. If the results are not good enough, extensive and detailed feedback will be provided to the developer. If the Network Application passes the whole test suite, it will be certified by the 5GASP platform.

5G for Automotive

Automotive-vertical Use Case (AUTO-V): Vehicle Routing Optimizer in a Virtual OBU with inter-domain migration support and testing of privacy of involved streaming data

As part of the automotive use case, OdinS proposes an orchestration between Virtual On-Board Units Provisioning and Multi-domain Migration Network Applications in order to provide a service of vOBUs that can travel close to the corresponding vehicle switching between different virtualization and network domains seamlessly. Maintaining the transference of data between the vehicle and the cloud applications transparently with no operation disruptions or degradations in the service.

An example of the operation of these two Network Applications is detailed in the following.

- Initial setup:
    - The application is running in the first domain and ready to operate.
    - No OBUs are connected, so the vOBUs are available to be assigned.

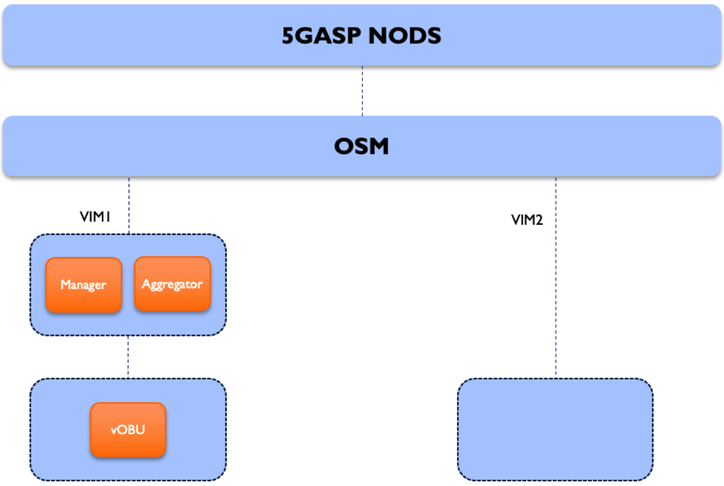

Figure 3 Automotive use case – Initial setup

- Vehicle OBU connects to the network:
    - A new vehicle appears in the scenario and the OBU requests a new vOBU.
    - A new vOBU is assigned to the physical OBU in the first domain.

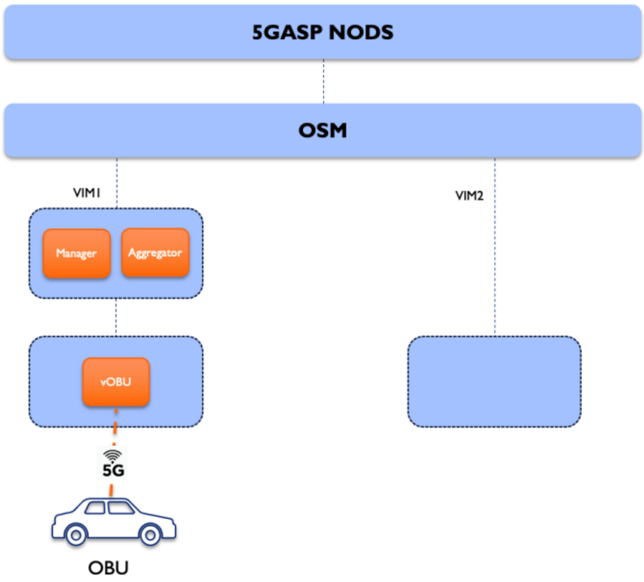

Figure 4 Automotive use case – OBU connects to the network

- Vehicle changes from one cell to another:
    - The vehicle moves form the cell currently serving in the first domain, to another cell in the second domain.
    - This change is detected through the monitorization of the real 5G data.
    - The migration process starts.

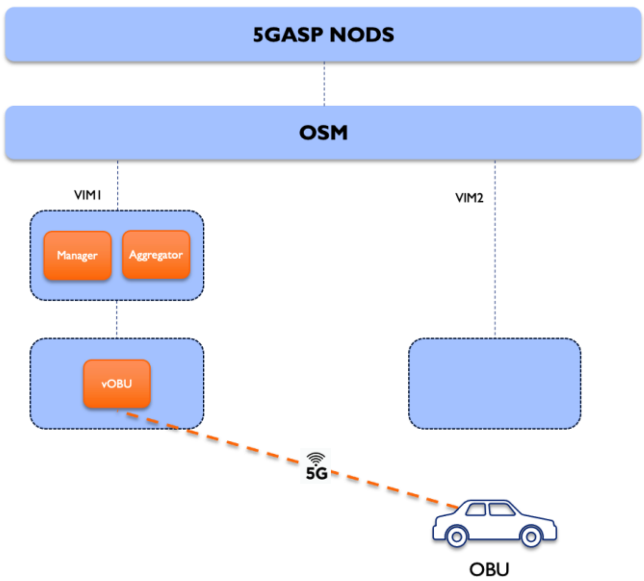

Figure 5 Automotive use case - Vehicle changes cell

- New vOBU is assigned:
    - A new vOBU is instantiated in the second domain and starts serving the physical OBU. The transition is performed seamlessly.

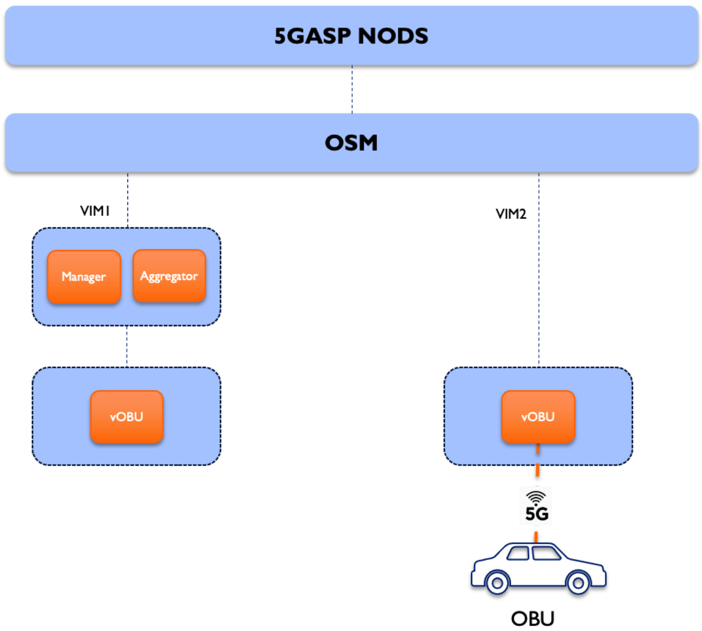

Figure 6 Automotive use case – New vOBU assigned

5G for PPDR (Public Protection and Disaster Relief)

PPDR-vertical Use Case (PPDR-V): 5G Network Resilience and Privacy in the International Public Safety Operations

Natural and man-made disasters such as large forest fires, flooding, earthquakes and terrorist attacks presents ongoing threats to the EU citizens and can lead to large numbers of casualties and significant damage to public infrastructures in the affected areas. The scale of some of the recent EU disaster events calls for cross-border and international cooperation where different first responder teams (firefighters, medical rescue and security services) from different EU countries need to communicate in a reliable and efficient way and exchange mission-critical related data.

ININ's 5G Isolated Operation for Public Safety (5G IOPS) and UoP's FIDEGAD are 5GASP Network Applications that are targeting resilience aspects of the future 5G enabled PPDR communications systems and showcasing cross-testbed and cross-border capabilities of the 5GASP platform that can be used to deploy and operate the components during the course of the international public safety interventions.

As part of the PPDR use case, ININ is showcasing automated deployment of portable PPDR communications incorporating 5G network and cloud-native capabilities that are deployed and operated as interconnected container-based VNFs in integrated 5GASP environment provided by Ljubljana facility, exploring cross-border capabilities of the 5GASP platform and high availability features of the developed 5G IOPS Network Application for the case of PPDR disaster situations. In this environment, UoP's FIDEGAD Network application will be used as an example of 3PTY PPDR application used on an international first responder mission where emergency teams are using video streaming and image recognition services provided by FIDEGAD to automatically detect the fire sources from the videos captured by drones.

Example of such scenario is described with the following steps:

- Normal operation (initial state, no disaster is taking place):
  - Public node domain hosting a telco-provided 5G Core Network and primary FIDEGAD server responsible to receive video streams from FIDEGAD client and provide image recognition services;
  - IOPS node domain represents a gNB node with IOPS capabilities, currently connected to the public node 5G Core Network function;
  - Secondary FIDEGAD server acting as a redundant component in case the public node domain is not reachable.

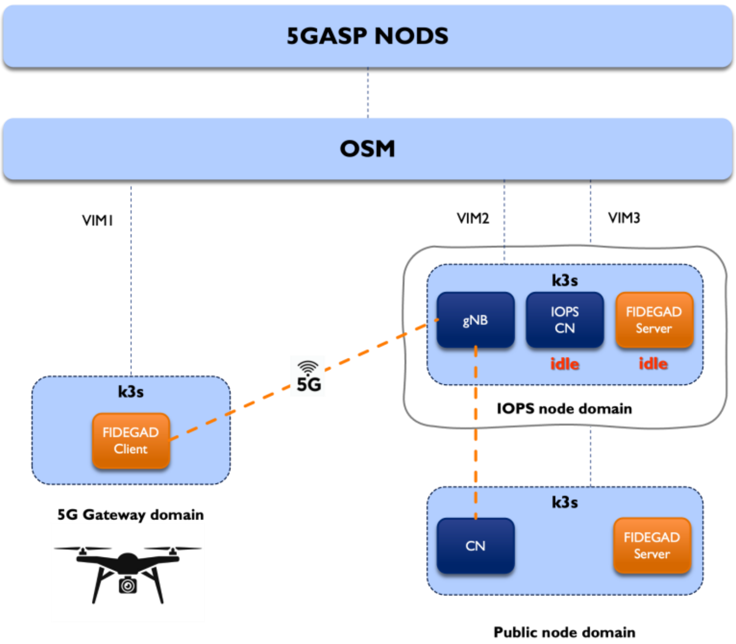

Figure 7 PPDR-vertical use case – normal operation

- Disaster operation (public node domain services are not available):
  - Network connectivity with the public 5G Core is lost;
  - IOPS node is reconfigured to use the local IOPS 5G Core, 5G connectivity is restored and FIDEGAD client switches stream to secondary FIDEGAD server serving as a backup and deployed on the IOPS node.

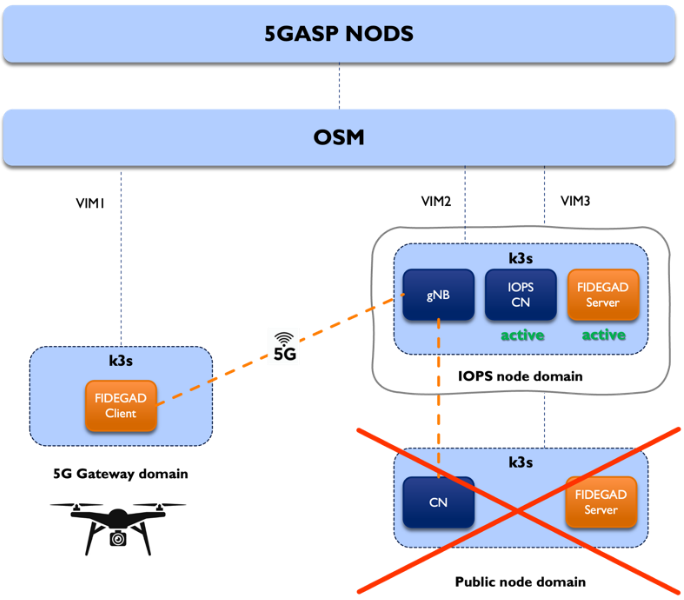

Figure 8 PPDR-vertical use case – disaster operation

- Network slice change operation:
    - 5G network served from the IOPS node is becoming saturated;
    - Mission-critical operation application (i.e., FIDEGAD Network Application) requests priority to improve network conditions by changing the 5G network slice and capabilities with the use of NPCF-like API function implemented on the IOPS node.

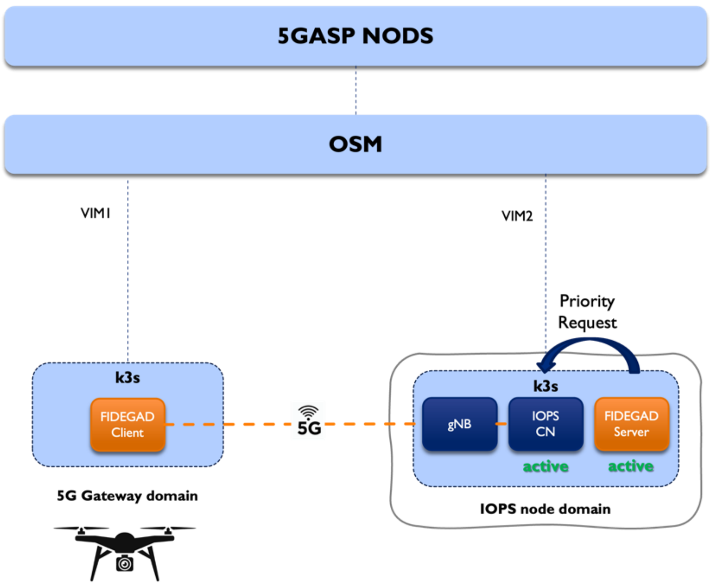

Figure 9 PPDR-vertical use case – improving network operation

- Cross-border operation:
    - FIDEGAD Network Application (i.e. image recognition service) deployed on the IOPS node is exhausting the infrastructure resources needed to operate other mission-critical services;

- Agreement between involved partners/countries is allowing to move resources-intensive applications to other partner/country;
- FIDEGAD server is deployed in a partner infrastructure and undeployed from the IOPS node, FIDEGAD client is re-orchestrated to use the newly deployed FIDEGAD server.

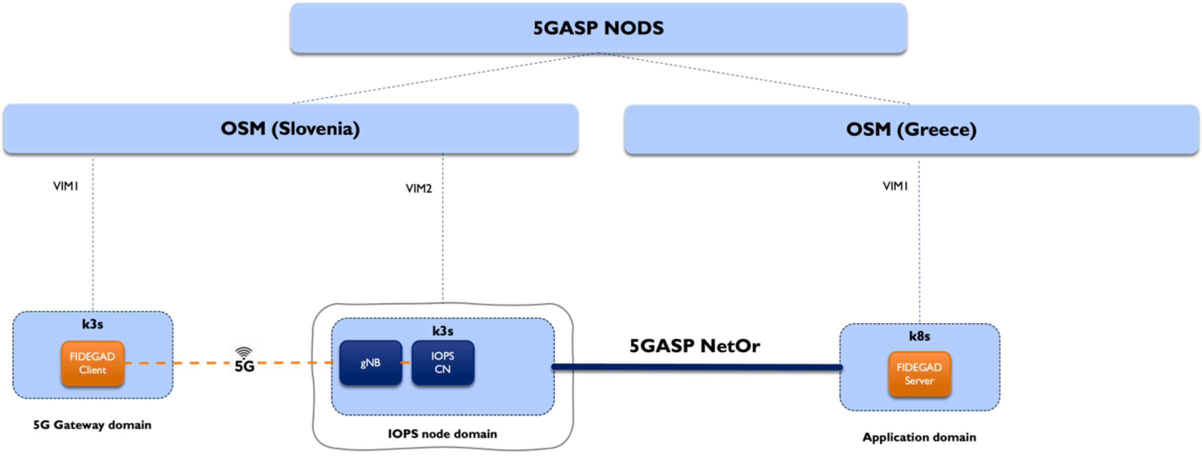

Figure 10 PPDR-vertical use case – cross-border operation

Cross-vertical Use Case (CROSS-V): Autonomous Vehicle Teleoperations / Remote Driving Use Case

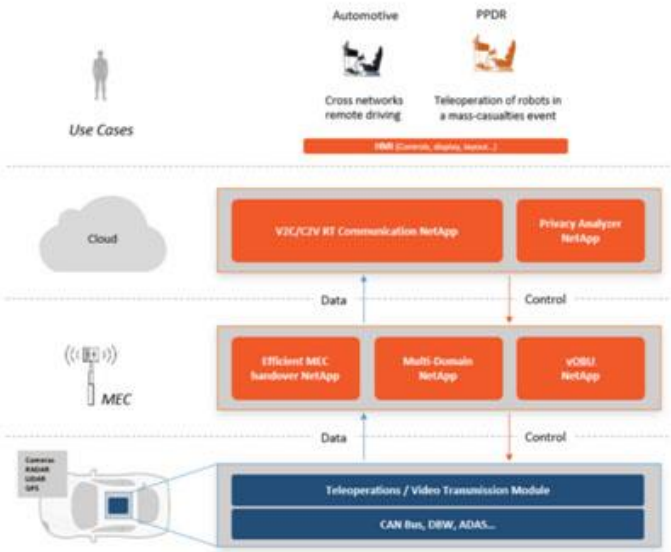

Figure 11 Cross vertical use case

There is an industry consensus today that autonomous vehicles will need help in making decisions, especially in unusual, dangerous situations that can happen on the road and may require violating the traffic laws (e.g., crossing double yellow lines). For these cases, the industry has started to adopt teleoperation/remote driving solutions that enable a remote human operator to monitor and take control over the car if needed. In addition, some countries have issued regulations that mandate the ability of systems that enable a remote human to take control over the vehicle if needed. The teleoperation use case enables a remote operator to take full/partial control over an autonomous vehicle in unusual/dangerous situations that can happen on the road. Ensuring safe teleoperation and human remote assistance entails reliable and secured transmission of high-quality real-time video with minimum latency. The use case will use various Network Applications provided by different 5GASP SME partners.

To test and validate the above discussed use cases, 5GASP offered a novel integrated development and operations (DevOps) environment, catering for both VM-based and Container-based Network Applications. Moreover, 5GASP will provide a service-based environment for validation, verification and certification of Network Applications, so that 5G operators are aware of their behavior before deploying them on their production networks. To achieve all the above, 5GASP introduces novel procedures and a novel fully automated tool chain that caters for the production of any Network Application with very little or without any human interaction through OSS automation tools.

These novelties shall be demonstrated on top of well-known and mature 5G facilities, 5G services and 5G/NFV experimentation tools to overall offer a DevOps-like and open platform for deploying, validating, verifying and certifying Network Applications; subsequently use-cases that are consisted from selected interworking Network Applications in order to faces the challenges posed from use cases that are emerging with an unprecedented rate in the 5G world.

3. 5GASP testbeds evolution to satisfy vertical requirements

5GASP infrastructure counts with six different locations distributed across Europe in Aveiro (Portugal), Murcia (Spain), Patras (Greece), Bristol (UK), Bucharest (Romania) and Ljubljana (Slovenia). The characteristics and configurations of each one of the testbeds have already been described in past documents, such as D2.1 [2] and others.

Although the testbeds already offered capabilities to enable the operation of Automotive and PPDR use cases, during the development of the project certain needs from the network applications were identified that the testbeds needed to address. In this way, during the last two years, the testbed owners were in continuous communication with the network application developers to satisfy special requirements that would improve the performance of the services or enable new functionalities.

In this way, in the context of WP4, a collection of hardware requirements demanded by the network applications was conducted and detailed in D4.3 [3]. As a result, the consortium obtained a clear view of the necessities of each one of the network applications participating and the restrictions that the testbeds had to accommodate them in the different verticals.

In the following, we present a summary of how the testbeds have evolved during the development of the project to address the vertical-specific needs of the network applications.

Automotive

The Automotive vertical poses a significant challenge due to its nature, as these use cases typically require mobility scenarios that can be complex to prepare, execute and schedule. Besides, it demands the usage of specific equipment to be on-boarded on the vehicles and to provide connectivity in moving environments. The 5GASP testbeds have worked together to improve their Automotive capabilities and offer a better service to these network applications, being Aveiro and Murcia testbeds the ones that hosted the automotive use cases in the different demos showcased during the project, showing this work.

One of the main needs demanded by the applications was the availability of 5G UEs prepared to be on-boarded in vehicles and with extra connectivity to vehicular-specific networks. In this way, the testbeds acquired versatile On-Board Units (OBUs) with 5G modems and space to connect 802.11p/ITS-G5 modems. With these, the 5GASP experimentation sites gained much more flexible hardware units to support the deployment of 5G Automotive services. Besides, 5G/802.11p/ITS-G5 USB modems were also acquired to provide connectivity to existing hardware with no vehicular-specific connectivity.

Regarding the 5G connectivity in the testbeds, the configuration of the 5G networks was also tuned to better support the mobility use-cases present in the Automotive vertical. For example, the 5G radio parameters were adjusted to improve the coverage of the 5G network and enable longer trips with the vehicles to permit extensive testing. Besides, the handover configurations have also been adjusted to improve the behavior of the changes between cells, avoiding long disconnection times and reducing the connectivity degradation in handover areas. With this, it was possible to effectively demonstrate the functioning of network applications dependent of the 5G handover such as the Multi-domain migration network application, whose operation was showcased in Murcia’s testbed.

Another improvement was the inclusion of computing and networking resources near the base stations (gNBs) in order to provide offloading and fast processing capabilities to mobile applications in which the latency or the processing time is critical. For example, by providing GPU resources in the MEC to enable video processing in real time.

Finally, although not directly related to the 5G connectivity, the availability of vehicles to make experiments in the different testbeds have been improved and they are available to be scheduled during certain periods of time.

PPDR

5GASP testbed ecosystem provides some advanced PPDR features to be tested with the network applications:

- Dynamic slice change
- Isolated operation

Dynamic slice change capability provides the option to network application to request the 5G slice to be changed by providing the NPCF Policy Authorization API endpoint. Some mandatory request parameters include:

- afAppId – Application Function Identifier
- dnn – Data Network Name
- SUPI – Subscription Permanent Identifier
- sliceInfo – requested SST/SD

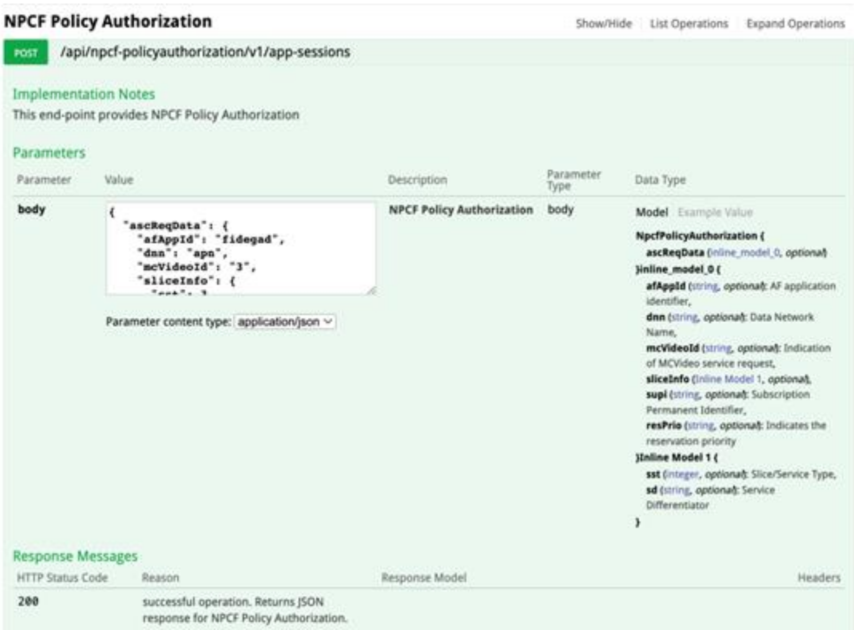

Figure 12 NPCF Policy Authorization API

Example of a such slice change operation is presented with the following steps:

- UE (identified by SUPI) is connected to the 5G network with the assigned slice (SST/SD 1/0)
- Request is triggered from the network application when the UE needs a different slice capability
- Request includes mandatory parameters (i.e., SUPI and SST/SD 3/10)
- The UE receives de-register request with the flag signaling it has to reconnect immediately,
- The 5G system is reconfigured to assign a different slice to specified SUPI
- The UE is reconnected and assigned the changed slice (SST/SD 3/10)

Another possibility is to simulate a disaster scenario in terms of PPDR vertical where the isolated operation takes place. This capability can be automated and allows the network applications to operate and test the switchover between public and local-only services, operation under isolated operation mode (i.e., only local services are available) and the network restoration. Example of such simulation is presented before in section 5G for PPDR (Public Protection and Disaster Relief).

Testbeds features and capabilities to support vertical-specific network applications

IT Aveiro Facility

The Aveiro Site embodies a comprehensive platform that leverages a set of capabilities and characteristics that transcend the mere aggregation of equipment. This overarching infrastructure offers a rich composition of solutions, encompassing those tailored for research purposes and those meeting industry standards, creating a real-world setting to develop and test new 5G and future technologies. It brings together academics, operators, vendors, and different industries to speed up the progress of mobile communications and innovative business models.

Notably, the infrastructure remains inclusive to all researchers and innovators, whether from academic or industrial backgrounds, to nurture innovation within the realm of 5G technologies and their practical application. To make this possible, it is connected to GEANT 66 and can set up secure connections using OpenVPN and Secure Shell Protocol (SSH) tunnels when needed.

The research infrastructure is equipped with substantial computational resources, including over 500 physical CPU cores, seven terabytes (TB) of RAM, and 350 TB of storage space. It also features a network infrastructure comprising four Gigabit switches and five 10-Gigabit switches. This platform runs the OpenStack Cloud Platform (Queens release) on bare metal. Regarding networking capabilities, the platform has a high-performance communication infrastructure designed to facilitate advanced integration and experimentation endeavours. It encompasses high-speed fiber optic links, equipped with OpenFlow-enabled switching capabilities (currently with HPE, Aruba, and Pica8 switches). Additionally, it offers conventional Internet Protocol (IP) and Multiprotocol Label Switching (MPLS) connectivity to external networks and the broader Internet through Cisco 3xxx routers. These resources are hosted in a controlled environment datacenter at the IT Aveiro premises, supporting the research activities of over 60 researchers and serving as the technological backbone for crucial initiatives, such as open source evolved Node B (eNB). Furthermore, there is an outdoor test system called the Advanced Mobile Wireless Network playground (AMazING). It stands out for its enhanced controllability and the ability to replicate tests, even for mobility scenarios. AMazING consists of a wireless testbed with 24 stationary nodes on the rooftop of IT-Aveiro, and it includes a high-speed mobile node capable of exceeding 30 kilometers per hour, allowing for highly reproducible mobile experiments.

The industry-grade infrastructure comprises both in-door and out-door radio cells, being further augmented by a 5G Standalone Architecture (SA) Core, enriched with Multi-Access Edge Computing (MEC) capabilities. More precisely, the 5G environment is powered by Huawei containing (BBU 5900 + AAU 5649) and indoor (BBU 5900 + RHUB 5963 + pRRU 5961) radio cells. This infrastructure is geographically distributed in four different sites, on 3 locations as depicted in Figure 13:

- two on - campus indoor deployments;
- one off - campus outdoor deployment;
- one off - campus indoor, edge - based deployment.

Figure 13 ITAV Industry-grade 5G Locations

Figure 14 depicts the overall architectural framework, illustrating the various hardware components and their intricate interconnections. On the left-hand side, we observe the four distinct site locations. Those locations equipped with multiple antennas are configured to establish automatic neighboring relationships, facilitating seamless handovers for uninterrupted connectivity. The network's core is depicted on the right-hand side of the figure, alongside the networking that provides vital communication support for the Network Function Virtualization Infrastructure (NFVI), where the 5G functions are instantiated. Noteworthy is the monitoring of NFVI, a task facilitated through the eSight platform, along with the Mobile Automation Engine (MAE) solution. It is important to emphasize that the MAE assumes a pivotal role in orchestrating and managing the life cycle of network resources, ensuring their efficient operation and optimization.

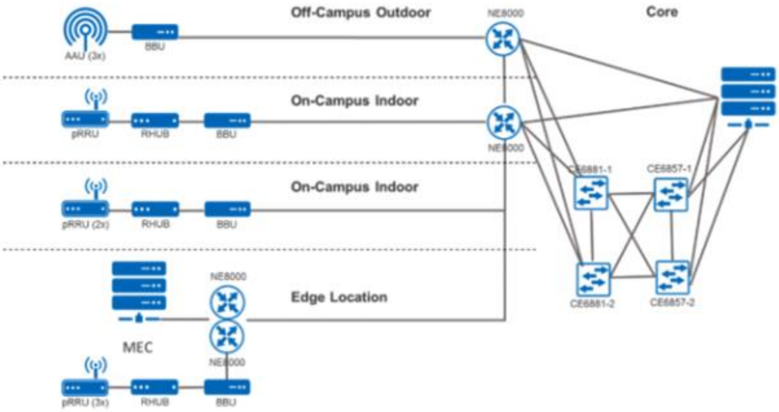

Figure 14 5Gainer distributed 5G network

In terms of its functional capabilities, the 5G core infrastructure offers a comprehensive suite of essential functions. These include the Access and Mobility Management Function (AMF), Session Management Function (SMF), Authentication Server Function (AUSF), User Plane Function (UPF), Network Slicing Selection Function (NSSF), Network Repository Function (NRF), and Unified Data Manager (UDM), all thoughtfully illustrated in Figure A. This deployment is enriched with the instantiation of the UPF at the edge site, optimizing data processing and routing. Finally, user devices are also available: (i) 10 x Huawei Customer - Premises Equipment (CPE) Pro 2 (H122 - 373) and (ii) 5 x Huawei P40 Pro.

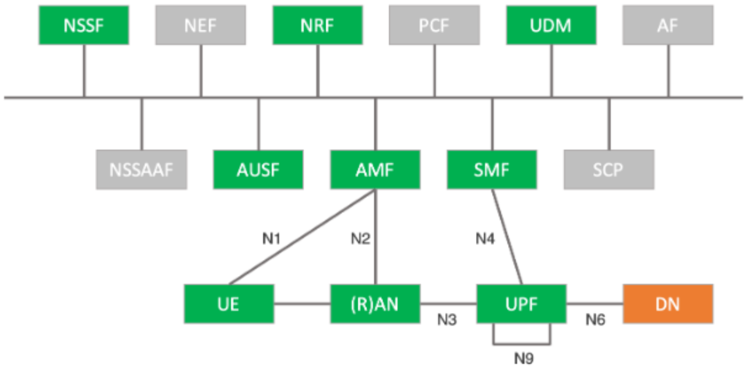

Figure 15 ITAV Industry-grade Available 5G Core Functions

ITAv's facilities also offers a platform for monitoring the 5G Network. To make this possible, we rely on an SDN Switch, which provides a mechanism for collecting metrics from the 5G Transport Network. Figure 16 depicts the complete architecture for collecting the 5G metrics.

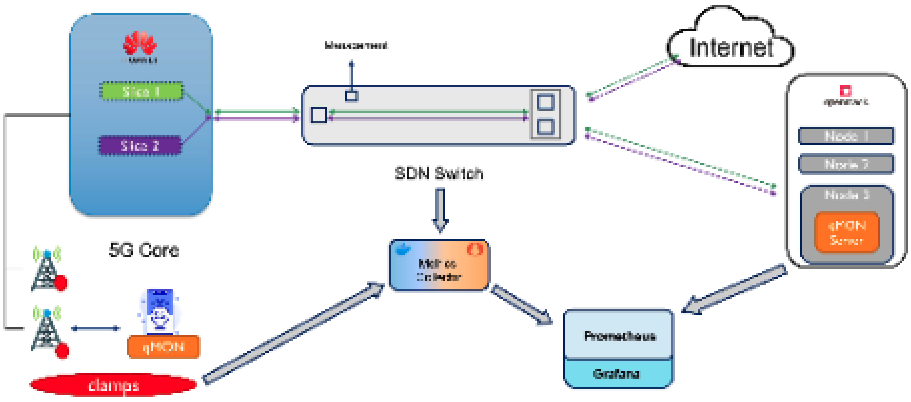

Figure 16 5G Transport Network SDN Switch

University of Patras Facility

The University of Patras facility, namely Patras5G, is a 5G/6G infrastructure 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.

Furthermore, the Patras5G testbed boasts a mmWave backhaul that connects the 5G Core with various locations (red dots in Figure 17) across the city of Patras, where 5G RAN points of presence (yellow dots in Figure 17) have been deployed, hosting vertical experiments over the course of several EU projects. Additionally, some of these locations offer broadband services through Fixed Wireless Access.

An extensive description of Patras5G testbed can be found in terms of architecture D2.3 [4] and D3.2 [5].

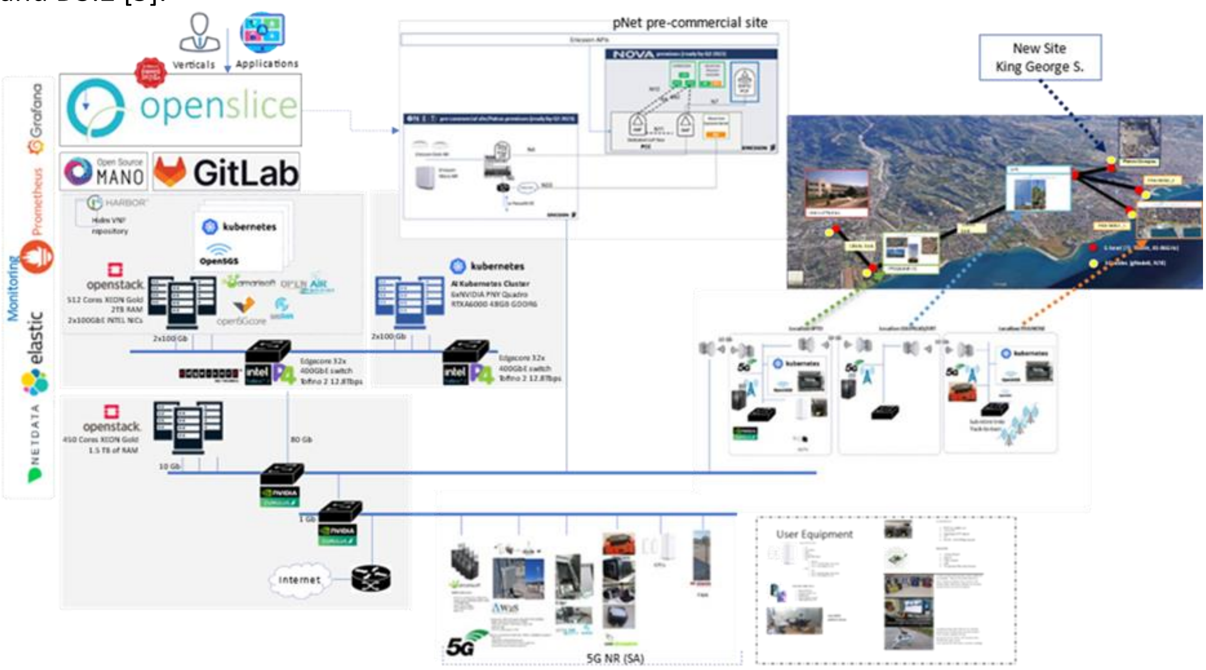

Figure 17 University of Patras facility

Following the general topological description of the previous section, in terms of verticals' requirements fulfillment, especially in PPDR, the Patras5G testbed also 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. The initial technical testbed description in terms of resource specifications can be found in D2.1, thus omitted. However, the addition of the aforementioned resources provides a breeding ground for verticals that may require intense computational processing as per definition, such as PPDR.

Patras5G, being an open infrastructure, yet operating as private, 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. Furthermore, MEC orchestration and mobility management features are also 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. All the aforementioned services are offered to users and verticals through the open-source Operations Support System (OSS) Openslice (http://openslice.io).

Apart from the testbed's offered UEs, described in previous documents, Patras5G offers a quadruped robot for experimentation, as seen in Figure 18. Specifically, it can carry anything out of 5G models or UE (mobile phones/CPEs) to various difficulty-accessible and rugged terrains. PPDR use cases can leverage its current abilities to provide remote system monitoring, video-stream from the provided cameras and teleoperation.

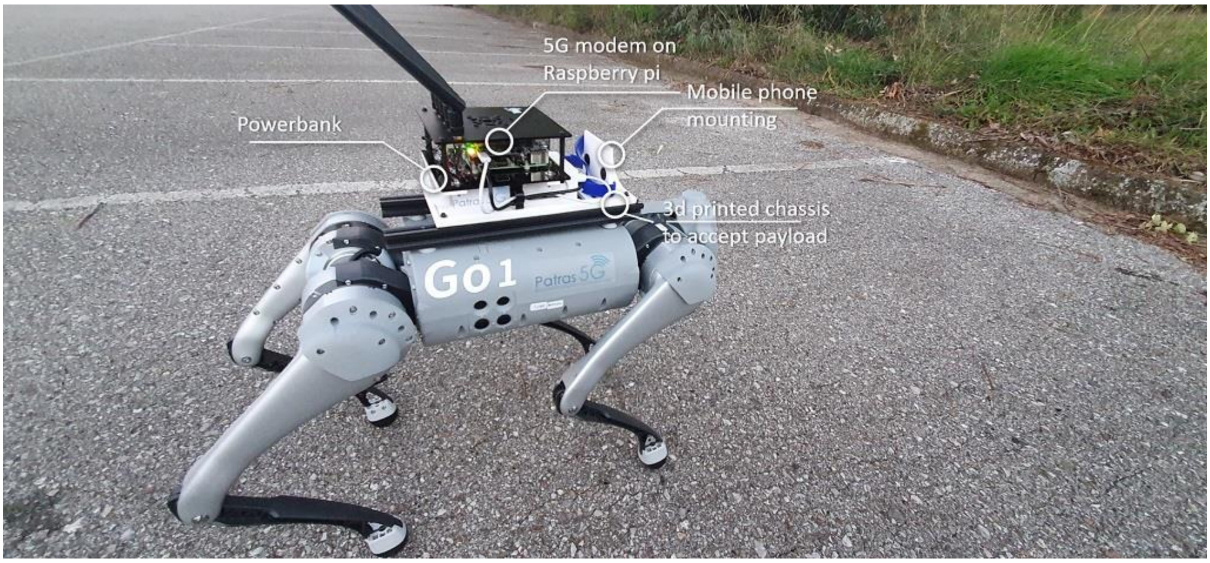

Figure 18 Patras5G quadruped robot

Murcia facility

Gaia 5G is a laboratory for experimentation located in the Computer Science Faculty in the University of Murcia, with research purposes 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. In the context of the 5GASP project, the testbed focused on hosting the automotive vertical, as it has been used to accommodate vehicular use cases. To enable this, several On-Board Units (OBUs) were prepared with connectivity to both the 5G network and the vehicular one (see Figure 19). The OBUs were also capable of providing connectivity to other devices acting as a CPE. Besides, software was also developed to control the 5G modems and obtain better control of the OBU behavior. Finally, the 5G infrastructure was configured to optimize the use of vehicular applications in the testbed. To do so, radio parameters were finely tuned to improve the performance of inter-cell handovers and video transmission. Although not directly related to the communication infrastructure of the GAIA-5G testbed, multiple vehicles were available to mount the OBUs on and drive them around the campus. More details of the testbed can be found in D2.3 [4].

Figure 19 OBUs in the vehicle in Murcia facility

Internet Institute facility

The Internet Institute (ININ) facility provides a fully orchestrated 5G SA private mobile network with VNF container-based deployment model using Kubernetes infrastructure and in-house prepared Helm charts. 5G mobile network can be deployed using Helm directly, using OSM or using 5GASP deployment platform. Additionally, certain 5G mobile network configuration parameters can be easily changed after the deployment by using day-2 configuration principle supported by the OSM. In terms of deploying network applications, the facility supports VNF/VM deployment on OpenStack and CNF/container-based deployments on Kubernetes.

Since the testbed is mainly oriented towards PPDR vertical it also provides some distinctive features such as:

- NPCF-like API enabling other applications to trigger the slice change request and thus dynamically change the 5G network performance needed in certain PPDR scenarios
- Isolated operations (IOPS) capability allowing other network applications to verify their operation in normal and disaster scenarios (i.e., only local services are available)
- 5G gateway capable of running Kubernetes cluster exposed to the OSM and provides the ability to orchestrate network applications also on the UE

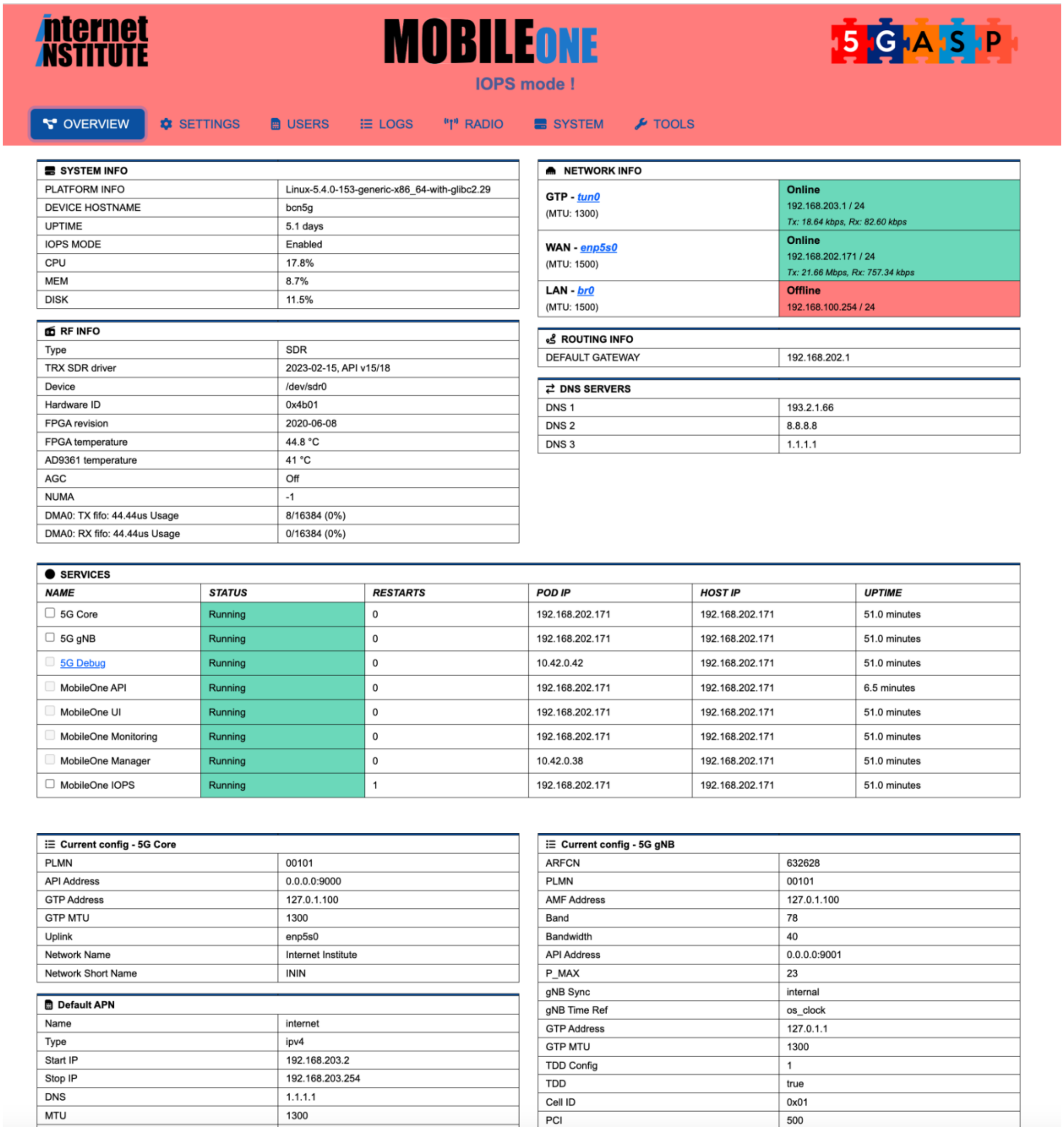

Figure 20 ININ's 5G mobile system running in IOPS mode

Furthermore, the testbed provides excellent end-to-end 5G network performance and service monitoring using qMON monitoring tool developed by ININ. The monitoring is comprised of the agents running on 5G UEs (i.e., ININ's 5G gateway, Samsung S23 smart phone running qMON agant as an application) and backend services deployed in the 5G core domain and also on other network segments if needed. Alongside 5G network performance and service monitoring the infrastructure/cloud monitoring is realized using Prometheus/node-exporter and aggregated into the 5GASP's central monitoring portal.

More detailed architecture and functional description of the testbed can be found in D2.3 [4] and D3.2 [5].

Bucharest Facility

ORO's Testbed is a multi-site testbed covering series of technologies (5G SA RAN & Core, Network Transport, Virtualization and Automation), capable to provide at its EDGE platform microservices deployments supported by K8s and orchestration tools already deployed in the testbed. The two sites are interconnected through high-broadband links (100Gbps) with capabilities to prioritize different traffic services flow (QoS assurance).

The multi-site testbed is composed by the fully EDGE-RAN-Core and transport network hardware and software tools that can provide E2E cloud-native services deployment and instantiation within the computing clusters between the 2 physical located sites, as each of the sites are equipped with edge computing and virtualization technologies related to micro-services instantiation.

The testbed has developed and E2E monitoring framework that collect in real-time network metrics and KPIs (CPU, Load, RAM, Disk Usage, Power Consumption) and based on which advanced analytics can be performed, to offer the "actual" site resources status, available capacity and optimized resources for different micro-services instantiation.

The testbed is capable to provide multi-slices implementations, with QoS/QoE guarantee in the concurrent services implementation, as eMBB (1500Mbps DL/200MBps UL) or URLLC (E2E one-way delay <2.5 ms), based in 3GPP NSSAI parameters. Another advanced key component of the testbed is the Next-Generation SDN Data Centre, integrated IPFABRIC concept, open to be orchestrated, dynamic configuration and zero touch management within the E2E network slice and automated service deployment.

ORO's testbed has hosted NEO's Network Application, thus enhanced the capabilities of having Android-based Smart-devices associated through the RAN. Furthermore, ORO's testbed is hosting a third-party Network Application, developed and onboarded through the Orange Fab program. This Network Application offers MEC-based processing of video streams from various cameras, and requires eMMB capabilities, MEC capabilities with CP-GPU and NPU support and secure transport capabilities.

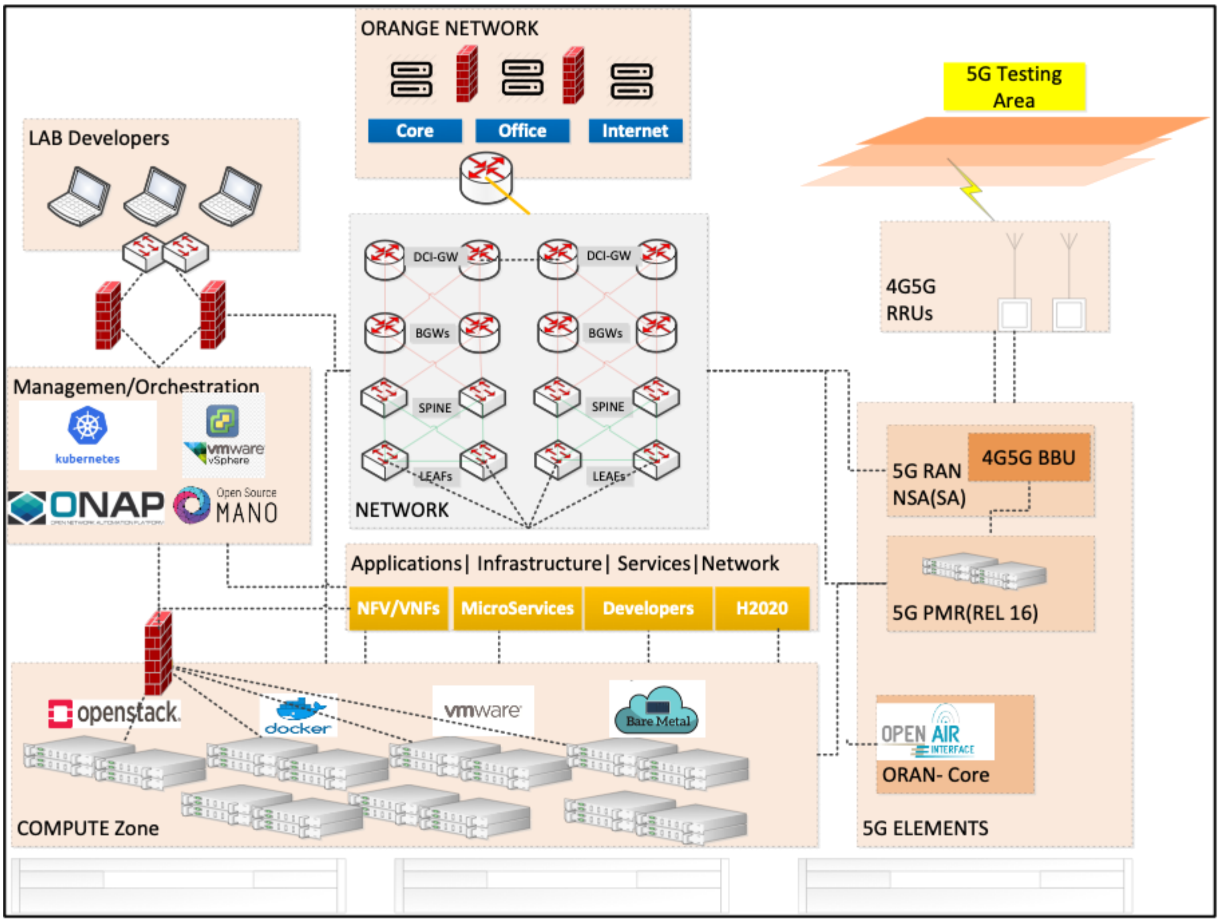

Figure 21 ORO's facility architecture

Bristol Facility

UNIVBRIS has three main Edge sites, of which two have 5G Cells. The river-side, M-Shed, has two cells and We The Courious (WTC) has another. They are shown in the below map image, and were previously used in mobility-based experiments. They could be used and/or support vehicular mobility, as well.

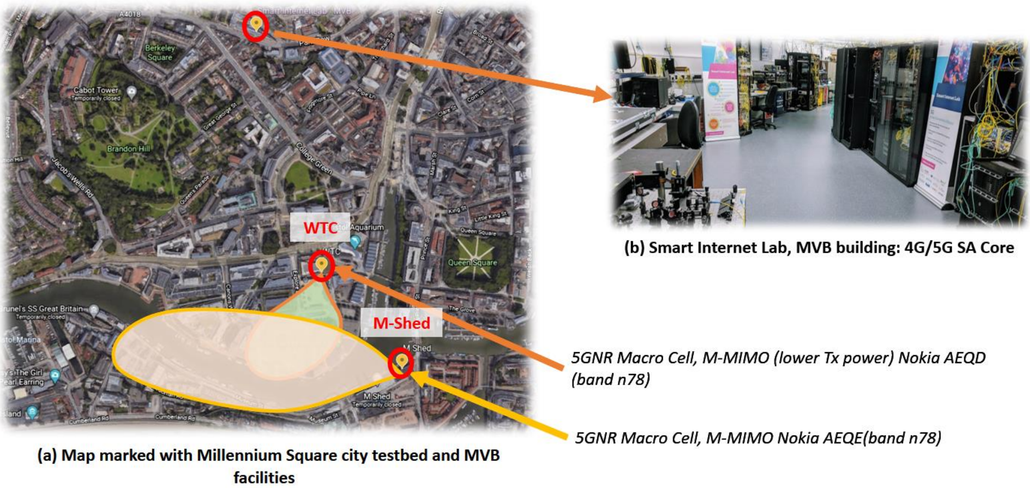

Figure 22 Bristol testbed locations

The following images are part of how the testbed is demonstrated to have supported user mobility, through our Network Application.

The following is the real trace map (there were simulated traces, as well):

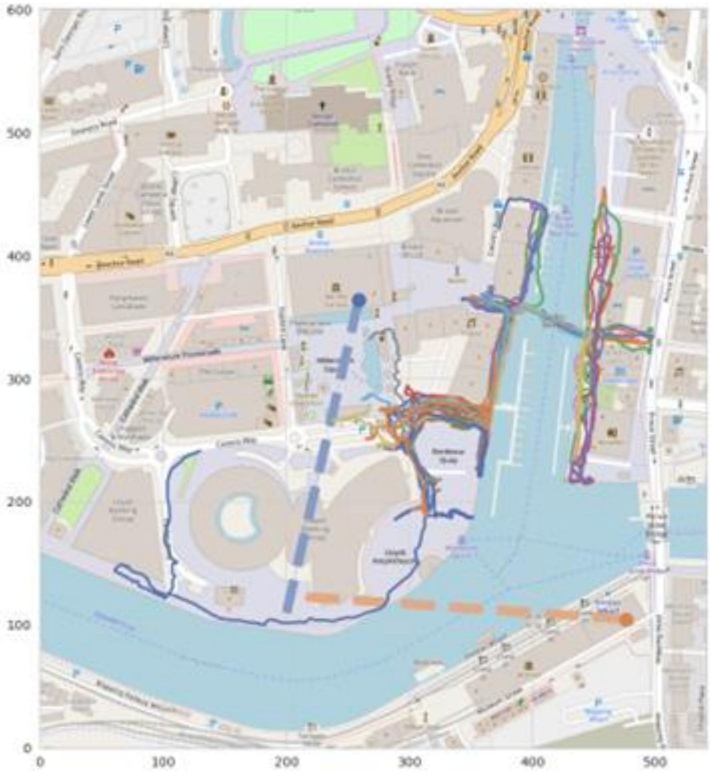

Figure 23 Real trace map

The real-world results of our nApp's application can be seen in the following snippets:

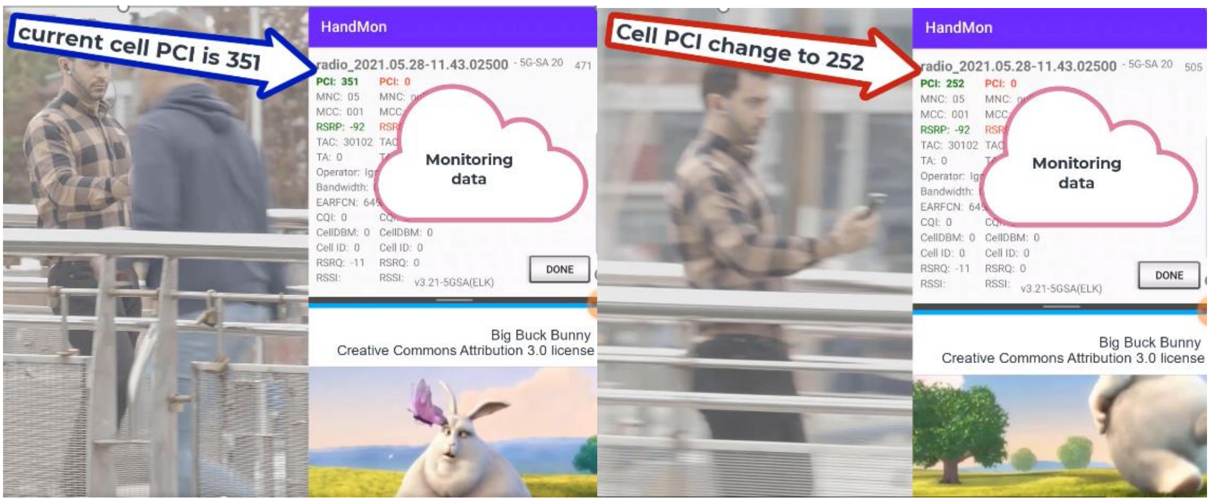

Figure 24 Real-world results

Since the demo has been run, there were other changes made to the testbed, that have improved its ability to support mobility. Some of these changes were as follows:

- Overhaul of the virtualisation solution deployed within the cloud infrastructure, referred to as Cloud+ in our network. This has enabled us with upgraded computational capability CPU+GPU (cloud and edge); gNB software upgrades for indoor and outdoor cells, currently we have Accelleran, Parallel Wireless and Nokia RAN solutions in our testbed; Indoor 5G cells deployment with handover; 5G Core monitoring capability; All of which contributed to the overall improvement in mobility support.

- Implemented a Kubernetes cluster, for CNF support, and adapted the Network Application accordingly, to make both the deployment (testbed network and servers) and development (Network Application repositories and CI/CD process) environments more dynamic and adaptable.

4. 5GASP Network Applications Deployment Experience

A Network Application is designed to provide specific functionalities and services in the context of a particular vertical, such as the automotive or PPDR verticals. The Network Applications developed in the H2020 5GASP Project are intended to leverage the capabilities of 5G networks to provide innovative and efficient solutions for the challenges faced by these verticals.

Network Application Adaptation for Testbed Requirements

Network Application adaptation for testbed requirements is the process of modifying a network application to make it compatible with the specific requirements of a testbed environment. This may involve making changes to the network application's code, configuration, or deployment.

There are some factors to consider when adapting a Network Application for a testbed environment, i.e., being compatible with the network, security, and performance requirements of the testbed environments. To do so, the Network Application owner should:

- **Identify the network connectivity requirements of the network application.** This includes identifying the protocols that the network application uses, the ports that it needs to be open, and the IP addresses that it needs to be able to communicate with.
- **Identify the security requirements of the network application.** This includes identifying the data that the network application needs to protect and the threats that it needs to protect against.
- **Identify the performance requirements of the network application.** This includes identifying the amount of CPU, memory, and storage that the network application needs to perform well.
- **Compare the requirements of the network application to the capabilities of the testbed environment.** Identify any areas where the two are not compatible.
- **Develop a plan to adapt the network application to the testbed environment.** This may involve making changes to the network application's code, configuration, or deployment.

Experiences from the 5GASP Community

Concerning this, the experiences from the 5GASP community were:

- One user reported that they had to modify the network configuration of their network application to make it compatible with the network connectivity in the 5GASP testbed.

- Another user reported that they had to add additional security features to their network application to make it compatible with the security policies of the 5GASP testbed.

- A third user reported that they had to scale down their network application to make it perform well on the computing resources available in the 5GASP testbed.

- Another user deployed their Network Applications using a cloud-native approach in a testbed via the Network Operator Deployment Service, requiring specific resources such as container images, CNF descriptors, and Helm charts.

- Another user reported that the CNF-based Network Application's configuration had to be slightly modified. Specifically, two issues had to be solved with the testbed owner when onboarding the Network Application, i.e., its containers and dependencies defined in 'Charts.yaml'. The first issue was that the namespace had to be agreed between the developer and the testbed owner. It can now be said that it could be a common practice that the Kubernetes namespace is the name of the Network Application, which can be the naming defined in the Helm chart that it is uploaded on the 5GASP Harbor repo. The second issue was the security permissions when creating Persistence Volumes. We can derive that a good solution is to specify in the Helm chart (or sub-chart) that the container runs as user 'root' and the 'fsGroup' is set to 0 in the 'podSecurityContext' section of the Helm chart.

Integration with Testbed Process Description

The process of integrating a network application with a testbed typically involves the following steps:

1. **Configure the network application for the testbed environment.** This may involve updating the network application's configuration to reflect the testbed's network connectivity, security policies, and computing resources.
2. **Test the network application.** This may involve running a variety of tests to verify that the network application is working properly in the testbed environment. Thanks to the 5GASP framework, the developer will have feedback from the tests execution and results.
3. **Fix any problems that are found during testing.** This may involve making changes to the network application's code, configuration, or deployment.
4. **Repeat steps 2 and 3 until the network application is working properly in the testbed environment.**

Best Practices by Stage

Thanks to the feedback that has been received from the developers and users of the 5GASP platform, we have gathered some suggestions of best practices for each stage of the integration with testbed process:

Configure the network application for the testbed environment:

- Update the network application's configuration to reflect the testbed's specific configuration or hardware. The specific network details will be configured by the 5GASP framework in the onboarding process.
- Document the Network Application's configuration so that you can easily understand and troubleshoot any problems that may arise.

Test the network application:

- Develop a test plan that covers all of the functionality, performance, security and 5G connectivity and readiness of the network application.
- Onboard the network application to the 5GASP platform so it can be deployed, tested and validated.
- Document the test results so that you can easily identify and troubleshoot any problems that are found.

Fix any problems that are found during testing:

- Diagnose the cause of each problem.
- Make the necessary changes to the network application's code, configuration, or deployment to fix the problem.

Expected Results

The expected result of the integration with testbed process is a network application that is working properly in the testbed environment. This means that the network application should be able to:

- Start and run successfully.
- Communicate with other devices on the testbed network.
- Implement the required security features.
- Perform well under expected load conditions.

Once the network application is working properly in the testbed environment, 5GASP can provide a certification, which is later explained.

What to Do and Not to Do

Here are some things to do and not to do when integrating a network application with a testbed:

Do:

- Plan carefully and document each step of the process.
- Make sure that the testbed environment has the required network connectivity, security policies, and computing resources.
- Test the network application thoroughly in the testbed environment before deploying it to a production environment.

Don't:

- Make changes to the network application without documenting the changes.
- Deploy the network application to a production environment without testing it thoroughly in the testbed environment.

By following the best practices and avoiding the common pitfalls, you can increase your chances of successfully integrating a network application.

Testing the Network Application

To test a network application, you can follow these steps:

1. **Identify the test cases.** What functionality do you need to test? What are the different scenarios that you need to cover?
2. **Develop a test plan.** This should include the steps that you will take to execute each test case and the expected results.
3. **Implement the test plan.** Develop the necessary tests and analyze if the existing tests in the 5GASP repository suit any of your needs.
4. **Onboard the network application and wait for the test results.** The network application will be deployed and tested, generating an output with the test results.
5. **Analyze the results.** Compare the actual results to the expected results. If there are any discrepancies, investigate the cause and make the necessary changes.
6. **Repeat steps 3, 4 and 5 until all of the test cases have been successfully executed.**

Here are some specific examples of test cases that you may want to consider for testing a network application:

- **Start and run the network application.**
- **Communicate with other devices on the network.**
- **Implement the required security features.**
- **Perform well under expected load conditions.**
- **Test all of the different features and functionality of the network application.**
- **Validate the connection with the 5G network.**
- **Validate the registration in the 5G network.**

Here are some additional tips gathered from network applications developers and experimenters for testing network applications:

- **Use a variety of test cases.** This will help you to identify any problems that may occur under different conditions.
- **Use appropriate tools and techniques.** This will help you to efficiently and effectively test the network application.
- **Document your test results.** This will help you to track your progress and identify any trends.

Receiving Results and Certification

Once the testing of the network application is complete, the applicant will receive the test results from the testbed. The test results will include a detailed report on how the network application performed during testing, as well as any issues that were found.

If the network application passed all of the tests, the applicant will receive a certificate from the 5GASP certification authority. The certificate will indicate that the network application has been certified by 5GASP and meets all of the requirements for 5G Network Applications.

If the network application did not pass all of the tests, the applicant will need to make the necessary changes to the network application and retest it. Once the network application has passed all of the tests, the applicant will receive a certificate from the 5GASP certification authority.

- **Applicant** (Equipment Manufacturer providing a Network Application supporting the 5GASP requirements):
    - Select an authorized Testbed which meets the Applicant's needs and schedule a certification testing slot
    - Complete Network Application certification application and submit all required supporting documentation
    - Submit required materials to the Testbed for certification testing
    - Coordinate with Testbed on monitoring/supporting the certification test execution
    - Coordinate with Testbed on investigation/debugging of Network Application test issues as required

- **Authorized Testbeds** (Independent Testbed which has 5GASP approval to provide test reports for Network Application certification):
    - Respond promptly to testing inquiries from Applicants
    - Coordinate with Applicant to schedule timely testing window
    - Coordinate with Applicant to complete all pre-testing logistics
    - Execute formal certification testing
    - Review testing results for test environment integrity and accuracy
    - Escalate abnormal test findings to 5GASP certification authority for disposition

- Facilitate investigation/debugging of product test issues with Applicant as requested
- Communicate completed test results to the 5GASP certification repository

- **5GASP Certification Authority** (Logo owner and Program Administration):
    - Review/approve product certification application and supporting documentation
    - Collaborate with Testbeds on investigation/disposition of abnormal test findings
    - Review testing results for product compliance
    - Arbitrate any escalated issues from Testbed and Applicant
    - Issue certificate and associated logo
    - Maintain certified product listing

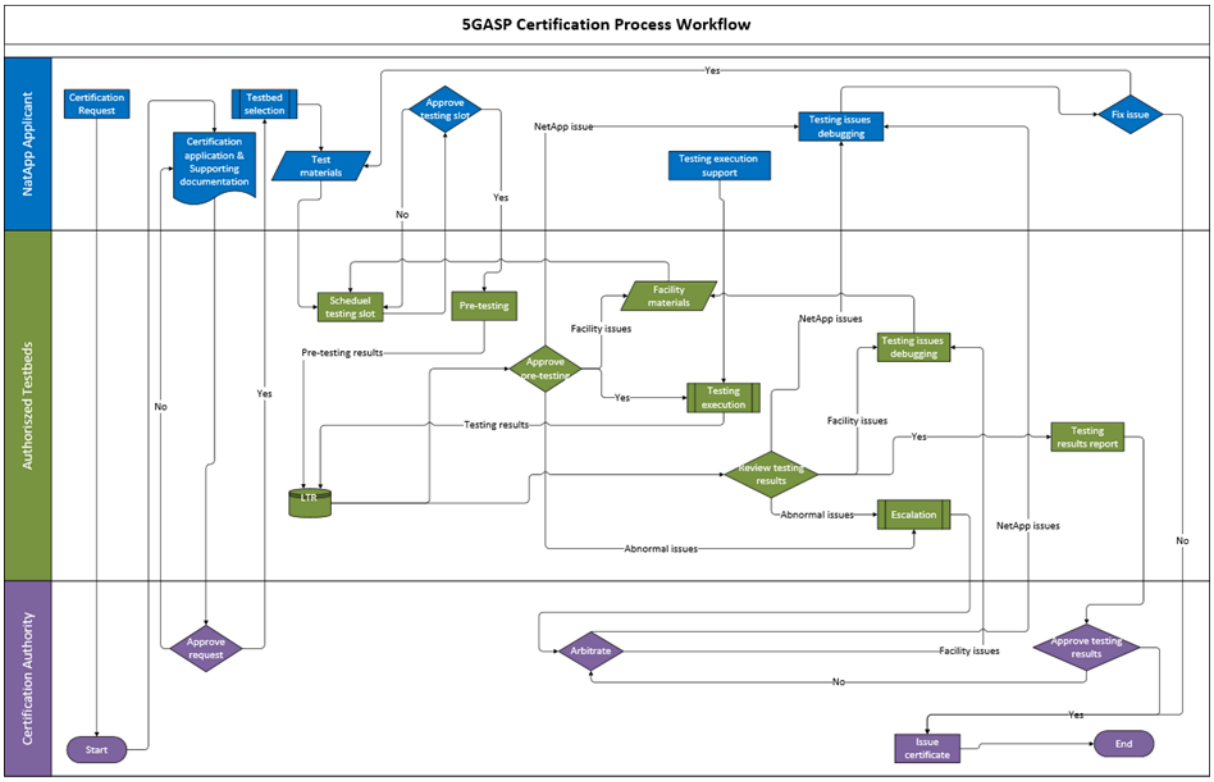

Figure 25 Certification process workflow

Upon availability of Network Application for the Testbed, testing shall be scheduled and conducted by the Testbed in an automated fashion.

In general, the Network Application certification is a procedure performed by a third party, independent of the manufacturer (seller) and consumer of software products, to confirm the compliance of a certain program or software package with the established requirements. The third party should be a Testbed that has been authorized (accredited) for the purpose of 5GASP certification testing. During the accreditation, the Testbed's technical capabilities to conduct certification testing are assessed, and the Testbed's qualification to verify results and discriminate pass/fail criteria are reviewed. Each Testbed needs to agree with 5GASP regarding administrative and legal aspects of certification testing. This is typically done by entering into a Testbed agreement contract. There are six accredited Testbeds in 5GASP, which are named after the city of the facility – Aveiro, Murcia, Bristol, Ljubljana, Patras, and Bucharest.

Certification testing is considered organized into “test runs”, in which a unique combination of hardware and software undergoes the entire applicable test suite. Test runs are carried out automated and supervised by a Testbed personnel. Applicants may monitor certification testing but may not physically interact with the Network Application throughout the duration of a test run. Upon successful completion of all applicable testing, the Testbed shall submit test results for the final test run of the Network Application to 5GASP Certification Authority for final review.

Different grades of certification are created, starting with a minimum scope of test cases and/or a minimum set of KPI requirements for an initial step. Subsequently, the scope could be expanded and/or sets of KPIs could be strengthened. Different levels of certification (bronze / silver / gold) are created with different sets of criteria. The requirements of the certification levels are as follows:

- Bronze – all initial criteria
- Silver – all initial criteria and a minimum of 50 percent of available expanded criteria points
- Gold – all initial criteria and a minimum of 80 percent of available expanded criteria points

No certification would be issued by 5GASP Certification Authority if the initial criteria is not fully met. In this case, the Network Application Applicant could ask for a re-certification with a new software version. The certificate will mirror only the tested parameters in a transparent manner.

In the re-certification process, some workflows could be skipped (e.g., Certification Request), some documents could be only updated (e.g., Supporting documentation and Test materials), and the Testbed could be re-used. The re-certification process could also be used when a Network Application Applicant wants to get a higher level of certification (e.g., bronze was initially issued and later, silver or gold level is the goal for a new software version).

Here are some tips for receiving results and certification:

- **Review the test results carefully.** This will help you to understand how the network application performed during testing and identify any areas where improvement is needed.
- **Communicate with the testbed.** If you have any questions about the test results, do not hesitate to contact the testbed.
- **Make the necessary changes to the network application.** If the network application did not pass all of the tests, make the necessary changes to the network application and retest it.
- **Submit the network application for certification.** Once the network application has passed all of the tests, submit it to the 5GASP certification authority for certification.

By following these tips, you can increase your chances of successfully receiving results and certification for your network application.

Here are some additional tips:

- **Be prepared for the possibility of failure.** Even if you have carefully tested your network application, there is always a chance that it may not pass all of the tests. Be prepared to make the necessary changes to your network application and retest it if necessary.
- **Be patient.** The certification process can take some time, so be patient and persistent.
- **Celebrate your success!** Once your network application has been certified, take some time to celebrate your success. You have achieved a significant milestone.

5. Case studies

Case Study 1

A User's Experience in 5GASP Testbed Integration

One user developed an Efficient MEC (Multi-Access Edge Computing) Handover Network Application designed to improve performance in MEC environments using Machine Learning. The application utilizes radio monitoring data to predict User Equipment transitions within a specified time frame. It was packaged using a cloud-native approach and deployed at a testbed using a Network Operator Deployment Service.

Challenges:

- Application-related challenges include the development of a Machine Learning pipeline involving data collection, preprocessing, model selection, and training.

- Kernel-related challenges involve the selection of an appropriate kernel for the operating system, affecting portability and networking between containers, pods, and services.

- Testbed-related challenges include the need for the testbed to support Kubernetes and overlay virtual networks, as well as challenges in migrating from VMs to containers.

- Tests-related challenges involve the need for functionality and performance tests that must be evaluated both locally and, in a CI/CD pipeline.

- Deployment-related challenges include hosting the docker image in a private repository and defining secrets for authentication.

Best Practices:

- Development is more efficient using a cloud-native approach compared to a Virtual Network Function (VNF) approach.

- Engage with community documentation and tutorials to avoid common pitfalls.

- Utilize tools like Postman and local instances of robot frameworks for test validation before production deployment.

Common Issues:

- Connection issues and improperly defined secrets can lead to deployment failures.

- Lack of certain security measures and outdated CI/CD configurations can halt the integration process.

Solutions:

- Check community documentation and engage with the community for troubleshooting and best practices.

Case study 2:

Transition Network Application from a monolithic, infrastructure-dependent solution to a more flexible and interoperable one.

The first version relied on an SDN controller, but it now uses the 5G NEF component, making it more adaptable to different testbeds. The application also includes a complete test suite for performance and operation validation.

Challenges:

- The main challenge was designing descriptors that could be used across various networks, especially given that IP addresses might be randomly assigned.

- Adapting the application logic to use the NEF component instead of the SDN controller.

Best Practices:

- Design the application for dynamic deployment and make it agnostic to specific testbeds.

- Develop a comprehensive test suite to quickly validate the application's operation and performance.

Common Mistakes:

- Developing the application as if it were a regular application, without considering the peculiarities of NFV and dynamic deployment.

Advice for Test Development:

- Identify what needs to be tested and how to test it, then follow community guides to implement the test logic.

Issues and Solutions:

- A common issue is having dependencies on static IPs. This can be resolved by designing the application to handle randomly assigned IPs.

- Community portals and testbed owner advice were invaluable during both development and deployment. Issues faced during the testing phases were resolved by following existing guides.

Cases studies summary

Case Study	Challenges	Best Practices	Common Issues/Mistakes	Solutions/Advice
A User's Experience in 5GASP Testbed Integration	- Application and Kernel-related challenges - Testbed and Tests-related challenges - Deployment-related challenges	- Use cloud-native approach - Engage with community documentation - Utilize tools like Postman	- Connection issues - Lack of certain security measures	- Check community documentation - Engage with the community
Transition Network Application	- Designing descriptors for various networks - Adapting application logic	- Design for dynamic deployment - Develop a comprehensive test suite	- Developing as a regular application	- Design to handle randomly assigned IPs - Follow existing guides and community advice

6. Summary

Key Takeaways:

The document serves as a comprehensive guide for SMEs aiming to develop Network Applications, particularly in the Automotive and PPDR verticals. It synthesizes valuable experiences, principles, and good practices into actionable guidelines. The methodology proposed in Task T4.1 is highlighted as a foundational framework for addressing the unique requirements that each vertical presents.

Importance of Guidelines:

The guidelines in this document are not just theoretical; they are born from hands-on experiences and lessons learned in the field. They are designed to streamline the development process, ensuring well-tested, interoperable Network Applications with low service creation time. For SMEs, this means a smoother adaptation process to the platform, thereby saving both time and effort.

Recommendations for SMEs:

The document stresses the importance of understanding vertical-specific requirements, such as those for Automotive and PPDR. Recommendations are given for dealing with special requisites like vertical-specific physical assets. By adhering to these guidelines and recommendations, SMEs are better positioned to expedite the time-to-market of their Network Applications, a critical factor for competitive advantage.

Bibliography

[1] 5GASP, "D4.2 Final Methodology for Designing and Developing NetApps," 5GASP, 2023.

[2] 5GASP, "D2.1 The 5GASP reference architecture," 2021.

[3] 5GASP, "D4.3 Initial Design of NetApps in the Automotive and PPDR Verticals," 5GASP, 2023.

[4] 5GASP, "D2.3: The 5GASP Revised Reference Architecture and Community Components," 5GASP, 2023.

[5] 5GASP, "D3.2 5GASP experimentation services, middleware and multi-domain facilities continuous integration, 2nd release," 5GASP, 2022.

[6] 5GASP, "D4.1 Initial Methodology for Designing and Developing NetApps," 2021.

[7] 5GASP, "D5.3 Final test specification on test-plan creation and testing methodologies," 2022.

[8] 5GASP, "D3.1 5GASP experimentation services, middleware and multi-domain facilities continuous integration," 2021.

[9] 5GASP, "D5.2 Integration guide and API reference manual," 2022.