ETSI GR NFV-EVE 023 V6.1.1 (2025-09)

GROUP REPORT

Network Functions Virtualisation (NFV) Release 6; Evolution and Ecosystem; Report on new infrastructure resources for NFV

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGR/NFV-EVE023

Keywords

cloud, management, NFV, NFVI

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

Trademarks

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document investigates the aspects about enabling in the NFV framework new dimensions to extend and evolve the NFVI in terms of source, location, and mobility, resources distribution and resources heterogeneity, including but not limited to the study of use cases on:

- new locations for infrastructure resources (e.g. data centres for non-terrestrial networks);
- new types of infrastructure resources (e.g. SmartNICs, Reconfigurable Intelligent Surfaces); and
- new sources of infrastructure resources (e.g. public Cloud providers).

The present document also analyses key issues related to respective use cases and documents potential solutions, and where applicable, it also provides recommendations for enhancements to the NFV architectural framework and its functionality aiming to provide further support to address the inclusion of new NFV infrastructure resources.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] ETSI GS NFV 006: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Architectural Framework Specification".

[i.3] ETSI TS 123 501 (V18.9.0): "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 18.9.0 Release 18)".

[i.4] 3GPP TR 38.811: "Study on New Radio (NR) to support non-terrestrial networks (Release 15)".

[i.5] ETSI GR RIS 001: "Reconfigurable Intelligent Surfaces (RIS); Use Cases, Deployment Scenarios and Requirements".

[i.6] ETSI GR RIS 002: "Reconfigurable Intelligent Surfaces (RIS); Technological challenges, architecture and impact on standardization".

[i.7] ETSI GS NFV-IFA 001: "Network Functions Virtualisation (NFV); Acceleration Technologies; Report on Acceleration Technologies & Use Cases".

[i.8] ETSI SR 003 391: "Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing.

[i.9] ETSI GS NFV-IFA 032: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Interface and Information Model Specification for Multi-Site Connectivity Services".

[i.10] ETSI GS NFV-IFA 036: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Requirements for service interfaces and object model for container cluster management and orchestration specification".

[i.11] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[i.12] ETSI GS NFV-IFA 053: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Requirements and interface specification for Physical Infrastructure Management".

[i.13] ETSI GS NFV-IFA 030: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Multiple Administrative Domain Aspect Interfaces Specification".

[i.14] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

[i.15] ETSI GS NFV-SOL 011: "Network Functions Virtualisation (NFV) Release 4; Protocols and Data Models; RESTful protocols specification for the Or-Or Reference Point".

[i.16] ETSI GR NFV-IFA 035: "Network Functions Virtualisation (NFV) Release 5; Architectural Framework; Report on network connectivity integration and operationalization for NFV".

[i.17] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; VNF Descriptor and Packaging Specification".

[i.18] ETSI GR NFV-EVE 025: "Network Functions Virtualisation (NFV); Release 6; Evolution and Ecosystem; Report on Serverless and other application virtualization forms in NFV".

[i.19] ETSI GS NFV-IFA 049: "Network Functions Virtualisation (NFV); Release 5; Architectural Framework; VNF generic OAM functions and other PaaS Services specification".

[i.20] G. Karabulut Kurt et al.: "A Vision and Framework for the High Altitude Platform Station (HAPS) Networks of the Future," in IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 729-779, Secondquarter 2021, doi: 10.1109/COMST.2021.

[i.21] ETSI GS NFV-IFA 045: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Faults and alarms modelling specification".

[i.22] ETSI GS NFV-IFA 008: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[i.23] ETSI GS NFV-IFA 047: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Management data analytics Service Interface and Information Model Specification".

[i.24] ETSI GR NFV-IFA 041: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Report on enabling autonomous management in NFV-MANO".

[i.25] ETSI GS NFV-IFA 027: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Performance Measurements Specification".

[i.26] ETSI GR NFV-IFA 046: "Network Functions Virtualisation (NFV) Release 5; Architectural Framework; Report on NFV support for virtualisation of RAN".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR NFV 003 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR NFV 003 [i.1] and the following apply:

AI	Artificial Intelligence
ASIC	Application Specific Integrated Circuit
BS	Base Station
DC	Data Centre
DL	Deep Learning
DPDK	Data Plane Development Kit
DPU	Data Processing Unit
EPD	Extensible Para-virtualised Device
FPGA	Field Programmable Gate Array
FRU	Field Replaceable Unit
GEO	Geosynchronous Earth Orbit
GPU	Graphics Processing Unit
HAPS	High-Altitude Platform Station
ICT	Information and Communications Technology
LEO	Low Earth Orbit
LIS	Large Intelligent Surface
MEO	Medium Earth Orbit
ML	Machine Learning
NPU	Neural Processing Unit
NTN	Non-Terrestrial Network
OBU	On-Board Unit
RDMA	Remote Direct Memory Access
RIS	Reconfigurable Intelligent Surface
RSU	Roadside Unit
SoC	System-on-a-Chip
TPU	Tensor Processing Unit
TRM	Time-varying Resource Management
UAV	Unmanned Aerial Vehicle
UPF	User Plane Function
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VCC	Vehicular Cloud Computing

4 Introduction and overview

4.1 Introduction to NFVI

The NFV Infrastructure (NFVI) comprises the infrastructure used for NFV deployments. As defined in ETSI GR NFV 003 [i.1], the NFVI comprises the totality of all hardware and software components that build up the environment in which VNFs are deployed.

The types of resources comprising the NFVI are compute, storage and network. The NFVI hardware resources can be Field Replaceable Units (FRUs) or non-FRUs, still distinguishable as COTS components, and are referred as NFVI components. When these are virtualised, they are offered as virtual compute, virtual storage and virtual network resources, as described in clause 5.3.4.4 of ETSI GS NFV 006 [i.2]. The management of the virtualised resources is provided by the VIM.

NFVI also provides the resources, when necessary, to support CIS clusters. CIS is a service providing runtime environment for one or more container virtualisation technologies. The management of the CIS is responsibility of the CISM, and the management of CIS cluster is the responsibility of the CCM. A CIS cluster contains CISM instances and CIS instances.

Finally, the NFVI is regarded to be distributed, with infrastructure spanning one or multiple locations. These are referred as NFVI-PoPs or also simply sites. The network resources providing connectivity between the sites is also regarded to be part of the NFVI. The network connecting different NFVI-PoPs is referred to as transport network or WAN. WAN connectivity is managed by means of Multi-Site Connectivity Services (MSCS), which are managed by the WIM.

The following characteristics can be identified regarding the NFVI:

- it is made up of different components, leading to resource heterogeneity; and
- it can comprise resources distributed and placed at different locations.

These characteristics serve as the dimensions for further analysis when evaluating new NFVIs.

4.2 New NFVI dimensions

4.2.1 Resources heterogeneity

As introduced in clause 4.1, the NFVI is comprised of different types of resources and components. On a general basis, the resources are categorized as compute, storage and network. Acceleration resources in NFV are hardware or software components that provide a number of acceleration capabilities of a compute node.

However, as the telecom network services evolve to support new use cases, so do the underlying technologies and infrastructure components. Therefore, new kinds of resources warrant further investigation as potential key components for building future NFVI.

Examples of new types of components are high-performing compute and network resources, such as Smart-NICs, and new forms of programmable physical resources, such as Reconfigurable Intelligent Surfaces (RIS). Clause 4.3 further develops about new types of components or resources.

4.2.2 Locations, provision and distribution of resources

As introduced in clause 4.1, the NFVI is distributed, comprising resources, potentially, at different locations. Locations of NFVI presence are referred as NFVI-PoP or simply site.

In terms of locality, numerous use cases on enabling connectivity at far and remote locations are becoming prominent in various organizations' work. For instance, use cases related to Non-Terrestrial Networks (NTNs) which utilize High-Altitude Platform Stations (HAPSs), Unmanned Aerial Vehicles (UAVs), or satellites are becoming more prominent.

Another evolutionary aspect to be considered regarding resource provisioning and distribution is leveraging infrastructure provided by public Cloud providers. Such infrastructure is used for the deployment of telecom networks, and therefore, it is of vital importance to investigate its relationship with the already defined NFVI constructs.

4.2.3 Resources mobility

Another aspect of resource' location, provisioning and distribution, which is specially related to new infrastructure types like HAPS is mobility. In this respect, examples like HAPS, UAV, and satellites introduce a new dimension of "mobility", whereby resources can move among different locations, and their presence and availability can be sporadic, e.g. only available during certain periods of time.

4.3 New kinds of infrastructure resources

4.3.1 Data Processing Unit (DPU)

With the rapid development of Information and Communications Technology (ICT), infrastructure resource requirements for computing and network performance are exponentially increasing. Currently, massive data flows in Data Centre (DC) have driven the port rate per hardware to rapidly evolve from 10 Gbit/s level to 100 Gbit/s level, or even higher. Several solutions are used to improve the network I/O data processing performance and efficiency, such as Data Plane Development Kit (DPDK). However, it has not changed the traditional CPU serial computing model which makes it difficult to achieve computational efficiency given the network's high data forwarding capabilities. The growth rate of network bandwidth is far higher than the growth rate of CPU computing power which leads to increasing excessive CPU resources occupied by network data processing.

In this context, Data Processing Unit (DPU) was developed to relieve the main CPU of complex networking responsibilities and to solve the corresponding network I/O performance bottlenecks. A DPU is a programmable processor that integrates general-purpose ARM/x86 CPU with network interface hardware (which could be Application Specific Integrated Circuit (ASIC), Field Programmable Gate Array (FPGA), etc.).

DPU can be understood as a new type of processor used for offloading and accelerating network, storage, and security tasks from the CPU compared to CPU and GPU. DPUs as new kind of infrastructure resources can be managed by the NFV MANO, bringing additional challenges and opportunities for NFV. For example, the coordination of Remote Direct Memory Access (RDMA) and DPU, together with related issues like the object information model to be used and the support for multi-tenancy can be analysed to make full use of this new infrastructure resource in NFV.

4.3.2 Satellite

With the advances in aerospace technology and the decrease in satellite launch costs, satellite communication networks, especially the low-orbit satellite communication systems, satellites are now effectively complementing terrestrial mobile cellular networks.

As shown in table 4.3.2-1, satellites in different kind of orbit can perform different functions in communication.

Compared with terrestrial mobile communication network, satellite communication network has the advantages that it provides wide coverage for sparsely populated area, is not restricted by radio base station terrain occlusion, and has stronger survivability in the event of natural disasters. However, satellite communication systems face challenges brought by communication link characteristics such as long transmission distances between satellites and ground as well as the fast movement of low-orbit satellites with reference to the ground.

Table 4.3.2-1: Satellites for communications overview

	Low Earth Orbit (LEO)	Medium Earth Orbit (MEO)	Geosynchronous Earth Orbit (GEO)
Functions	• High-speed broadband • Internet access • Telemetry • Remote sensing • Intl Space Stations	• Navigation and positioning • High-throughput satellites • Fixed/Mobile communications	• Navigation and positioning • Meteorology • Radio and Television • Low-speed communications
Distance	300 - 2 000 km	2 000 ~ 35 785 km	357 855 km
Latency	4 ms at 600 km	66 ms at 10 000 km	240 ms

According to ETSI TS 123 501 [i.3], for some 5G deployments, some network functions (such as User Plane Function (UPF)) can be deployed on satellites. Satellite, as a new kind of network infrastructure for hosting these network functions, leads to specific characteristics such as infrastructure mobility and distribution to be analysed in the present document.

4.3.3 AI processors

AI processors are integrated circuits specifically designed for executing Artificial Intelligence (AI) computational tasks. These AI processors are used to enhance the efficiency of Machine Learning (ML) and Deep Learning (DL) models, particularly when dealing with large volumes of data in parallel and complex neural networks. AI models like deep learning are compute-intensive, and using general purpose CPUs for this kind of processing is inefficient. AI processors can perform, among other functions, thousands of multiplications and additions in a mathematical process called matrix multiplication. For processing those computations at scale, AI processors are designed with specific architecture and large number of cores.

There are various types of AI computing processors emerging in recent years, including but not limited to:

- Graphics Processing Unit (GPU): Chips initially designed for graphics rendering, which have been widely adopted for AI computing due to their parallel processing capabilities.

- Tensor Processing Unit (TPU): Custom-designed Application-Specific Integrated Circuit (ASIC) developed specifically for accelerating Machine Learning (ML) workloads.

- Neural Processing Unit (NPU): Processors specifically designed to accelerate machine learning algorithms, especially mimicking the structure and function of the human brain's neural networks in these chips' architecture.

AI is going to expand the boundary of telecom network services, which underscores the importance of various AI processors as new kinds of NFVI resources to be used in the telco Cloud. The introduction and type choice of AI processors is expected to be based on the types of the tasks, performance requirements, and energy efficiency considerations, etc.

4.3.4 High-Altitude Platform Stations

High-Altitude Platform Stations (HAPSs) are quasi-stationary nodes of the aerial network that operate at an altitude of around 20 km with a coverage of a radius 50 - 100 km [i.4].

HAPS systems are now widely regarded as a viable enabling technology for future wireless communication networks. This is due to the evolution of communication technologies and the progress in solar panels technology, combined with the economic viability of the HAPS system, enabled by the emergence of cost-effective technologies and materials.

In areas with low user density, where no coverage is available due to lack of network infrastructure (e.g. rural areas, ships, desert, offshore platforms), HAPS systems can be an alternative to the terrestrial systems, helping thus in providing broadband access and contributing to disaster relief. Regarding communication services in heavily concentrated urban areas, HAPS systems can help coping with the ever-increasing demand that exceeds terrestrial networks capacity. As HAPS nodes are quasi-stationary, have a large footprint, and feature greater computational capacity, they can achieve better network coverage than the small Base Station (BS) deployments in dense areas**.** However, HAPS system is no substitute for macro-BS, this latter is a key component in terrestrial wireless access architecture. Rather, HAPS system can play a complementary role to support the terrestrial communication: a terrestrial network, for instance, can satisfy moderate user demand, whereas unexpected or rapidly increasing user demand might be handled by a HAPS system.

Compared to satellite, launching and maintaining HAPS nodes involves lower costs, and can directly provide end users with wireless services thanks to their low-latency characteristics. In addition, HAPS nodes are rapidly deployable and can be relocated as required, making them ideal for temporary events or emergency situations.

A variety of applications can be envisioned for HAPS systems, for instance, the rolling-out of airborne mini-data centres within HAPS nodes, which can be an enabler to extend the operator's infrastructure with additional computing and storage resources. Another application could be supporting LEO satellite transfers to ensure seamless connectivity. Yet HAPS systems pose several significant challenges. Unlike satellites, HAPS nodes are limited by their altitude and can only provide coverage to relatively small areas. They are also dependant on weather conditions, which can hamper their proper functioning. Moreover, HAPS nodes' limited power source might make them unsuitable for handling the deployment of applications/workloads with high peak power consumption or extended periods of time.

HAPS systems consist of two parts [i.20]:

- The non-terrestrial segment (or the HAPS node) encompasses the onboard systems, which include:

  i) the flight control component in charge of mobility management. It also manages the interface between the platform and the ground control station (handling tasks such as tracking and command signals, health reports of the platform, etc.);

  ii) the energy management component that handles the energy generation, storage, and consumption of the energy by other components;

  iii) the communications payload component responsible of the communications between the HAPS and other entities (e.g. gateways).

- The terrestrial segment of the HAPS system consists of two components:

  i) the control station, which manages the communication between HAPS and different types of users. It coordinates the communication links and manages the resources among multiple HAPS nodes and other TNs/NTNs. Additionally, it handles take-off and landing processes and controls remotely the position of the HAPS;

  ii) communications gateway which connects the HAPS to the core network through wired backhaul. HAPS communication with the terrestrial users can occur directly or the data can be relayed through the communication gateway.

4.3.5 Vehicular Infrastructure

With the rapid increase in the number of vehicles connected to the Internet and to one another, vehicular networks are becoming a key enabler of ubiquitous communication in new-generation networks. Designed to share information quickly and efficiently between the vehicles and the underlying infrastructure, these networks feature a wide range of applications and use cases. The vehicles that form these networks are equipped with an On-Board Unit (OBU) transmitting data to other vehicles (Vehicle-to-Vehicle (V2V) communication) as well as to a remote-control centre (Vehicle-to-Infrastructure (V2I) communication) via various infrastructures such as BSs or Roadside Units (RSUs).

Initially, when the vehicular networks were first adopted, their use was limited to accessing Internet resources, either to download content or to store it in the Cloud. However, uploading content or searching and retrieving it, to and from the Internet-Cloud is time-consuming and costly in terms of resource usage. Furthermore, it is possible that adjacent vehicles tend to search for content that is similar/related in terms of the following aspects:

i) the specific region at which they are situated (e.g. information about nearby accidents);

ii) the temporal aspect (e.g. information on roadwork in progress over a period of time); and

iii) content that was produced by neighbouring vehicles.

Taking all these elements into account and harnessing onboard computing and storage capabilities of the vehicles, resulted in the emergence of Vehicular Cloud Computing (VCC) concept, whereby vehicles together constitute a Cloud within which content is generated, stored, and consumed.

VCC now offers a cost-effective alternative to conventional Cloud computing and gives rise to new uses, beyond improving road safety, optimising traffic flow or providing navigation guidance. An example of how VCCs can be used is the transfer of compute-intensive tasks to vehicles to help accelerate time-sensitive applications, rather than transferring these tasks to data centres, which can lead to an increase in latency. Another use case can be offering a storage service by storing distributed data in available vehicles. Other uses could be the provisioning network connectivity during peak hours or at major events, in stadiums or in rural areas where connectivity is always a concern.

Overall, it can be concluded that vehicles are now designed and manufactured in a way that these become also platforms of compute, storage and network resources on their own, making them a complementary source of infrastructure.

4.3.6 Reconfigurable Intelligent Surfaces

In wireless communications, the propagation environment has, until recently, been considered an unmanaged resource associated with stochastic and unpredictable interactions between the emitted radio waves and the surrounding environment, which adversely affect the quality of the signal received by mobile users.

Towards 6G, new wireless technologies have emerged offering a solution to overcome this issue. It is worth highlighting the emergence of Reconfigurable Intelligent Surfaces (RISs), which can be used to control the propagation of wireless waves in different dimensions like time, space frequency and phase. RIS technologies can be found under the terms smart mirrors, Spatial Modulators, and Large Intelligent Surfaces (LISs). In the present document RIS is used to represent all different variations/technologies.

An RIS is a tile manufactured using metamaterials with real-time adjustable electromagnetic properties, enabling the manipulation of the impinging radio waves by performing specific actions, such as, repolarization, absorption, steering, etc. In 6G, RISs are the main building blocks of the recently proposed programmable wireless environments, which aim to offer a complete protocol stack, specifying the system's physical, network, control and application layers, and detailing ways in which RISs can be integrated into legacy network infrastructure using the SDN paradigm.

RISs and their integration into the existing network infrastructure can address to some extent the stochastics of the environment. Furthermore, RISs as a new type of mobile network resource can be even abstracted and virtualised to enable their representation as a Cloud resource and enable the deployment of customised E2E services. However, integration of RISs to existing infrastructures imposes new challenges, mainly in terms of management. For example, in a cloudified NFV-MANO based environment it is not yet clear how RISs can be seamlessly managed together with already available communication resources, and the overall relationship of RISs with NFVI needs to be assessed.

An ISG covering RIS investigates relevant use cases, deployment scenarios, requirements, and key technological challenge [i.5]. It also documents reference E2E network architecture featuring RIS elements and outlines practices/guidelines for RIS-based deployment [i.6].

4.3.7 Smart-NICs

Cloud data centres are increasingly constrained by the sheer number of running applications, a number that is growing with the transition to technologies such as data-parallel distributed applications. As a result, data centres are struggling to meet stringent throughput and latency requirements. To match line rates as network bandwidth increases, Cloud service providers have sought uncompromising alternatives to overcome this issue, one of which is adding Network Interface Cards (NICs) with acceleration or packet processing capabilities to the servers. Operations like pre-filtering all packets in the NICs offer a practical approach to offload CPUs' cores; delegation of network tasks to the NICs, alleviates the CPUs of managing some network-related workload and releasing a substantial part of server's CPUs' resources.

An NIC is a hardware device with the main function to deliver I/O (physical or logical) to/from the CPU [i.7]. It can include hardware acceleration engines for encryption, encapsulation, forwarding, and switching, while such functions are hardcoded in NICs. Hence, NICs in principle, serve the functionality of interfacing the CPU and the network and perform specific predefined functions. Additional functions cannot be added due to NICs' lack of flexibility and programmability.

Smart-NICs combine regular NICs capabilities with a compute layer. In addition to the functionalities provided by regular NICs, Smart-NICs feature the ability to accelerate storage and security functions, while they can also support virtualisation, load balancing, and routing optimization.

Depending on the Smart-NICs type a variety of applications with new requirements can be supported. Smart-NICs can be build using different processing units. FPGA-based smart-NICs can achieve good performance due to parallel processing of data flows, and although it is difficult to integrate new functions in them, they still offer flexibility for hardware developers. ASIC-based Smart-NICs on the other hand achieve higher performance and are easily programmable, however, they sacrifice the flexibility given by their FPGA counterparts. Finally, SoC-based Smart-NICs offer easy programmability with the highest flexibility but they are considered less efficient.

Despite all their advantages, Smart-NICs also have drawbacks such as high energy consumption, although, this can be compensated by the higher energy efficiency in realizing the network I/O compared to other solutions.

When it comes to considering Smart-NICs in an NFV environment, in terms of Cloud management several challenges arise regarding integration of Smart-NICs with other Cloud infrastructure resources, additional considerations to be made related to abstraction and virtualisation of their acceleration capabilities to enable the delivery of end-to-end services that leverage the capabilities offered by Smart-NICs.

4.3.8 Hybrid Cloud

In principle, network operators set up and maintain their own private Clouds, giving them complete control and customization across their network infrastructure virtualisation and cloudification. As traffic demands increase and more Cloud resources are needed to deploy telecom networks, private Cloud solutions are no longer sufficient to cope with this ever-increasing demand. Network operators have therefore started adopting a hybrid Cloud approach by combining public Cloud with private Clouds.

If properly executed, hybrid Cloud strategies can yield significant benefits. With the public Cloud being an option under the hybrid approach, availability of storage and computing power is made easier. A network operator, as a Cloud service customer can choose to deploy less demanding and less critical or time-sensitive applications on the public Cloud while reserving their own private Cloud for security-sensitive and resource-intensive network applications.

The move to a hybrid Cloud solution can have an impact on the way VNFs are designed, built, deployed, and operated within such a heterogeneous ecosystem. Furthermore, the orchestration of this environment comes with its own challenges; public Cloud service providers have their own dedicated set of monitoring tools lacking a global view of the system, leading the customers to use disparate tools to monitor the deployment of their applications and assess their performance in end-to-end fashion. Particularly, deploying VNFs using public Cloud infrastructure confronts network operators with critical interoperability issues, given that they are expected to deploy and manage VNFs over different infrastructures and to be able to exchange VNFs data between different parts of the Cloud, as described in ETSI SR 003 391 [i.8].

This could imply additional challenges when it comes to integrating the NFV-MANO with the public Cloud management systems to ensure the monitoring of VNFs deployed therein. Moreover, it is essential for operators as Cloud service customers to gain an understanding of the failure patterns of the Cloud service providers as well as their impact on the applications.

5 Use cases

5.1 Overview

Expanding and evolving the NFVI by investigating new possibilities in resource distribution, heterogeneity, and location leads to various use cases relevant to the scope of the present document on the new infrastructure for NFV. The following clauses document use cases related to hybrid Cloud supporting NFVI deployments, new types of NFVI resources, and location and mobility of the infrastructure.

5.2 Use cases about new sources of infrastructure

5.2.1 Use case #1: Network service deployment across hybrid Cloud

5.2.1.1 Introduction

This use case showcases a scenario in which the goal is to deploy an NS across several NFVI-PoPs located in a private Cloud and a public Cloud respectively. The private Cloud is managed by the operator via NFV-MANO, and the public Cloud can be provided by one or more Cloud service providers. They are all distributed across different regions and can be interconnected via a WAN. The NFV-MANO provides the overall orchestration of network services within multi-source environment.

The following assumptions are considered in the present use case:

- for the resource fulfilment, resources from Cloud service providers are available for the deployment of the NSs. The operator has been provided access to the Cloud service provider's Cloud to secure the necessary resources to meet the end-user request;
- use of the Cloud service provider's resources can be determined either due to certain deployment requirements, resource requirements, or present capacity of the private Cloud resources managed by the network operators.

5.2.1.2 Actors and roles

Table 5.2.1.2-1 describes the use case actors and roles.

Table 5.2.1.2-1: Use case #1 actors and roles

#	Actor and role	Description
1	Operator	A human being or an organization seeking to deliver network services to end-users.
2	OSS/BSS	The entity that receives the Operator's request for the initiation or termination of a VNF/NS.
3	NFV-MANO system	The management and orchestration entity in charge of VNFs/NSs lifecycle management and OAM support and resource orchestration.
4	Public Cloud Management system	The entity from the Cloud service provider which is responsible for managing the public Cloud.

5.2.1.3 Trigger

Table 5.2.1.3-1 describes the use case trigger.

Table 5.2.1.3-1: Use case #1 trigger

Trigger	Description
1	The use case is triggered when an Operator requests to instantiate an NS across the hybrid Cloud.

5.2.1.4 Pre-conditions

Table 5.2.1.4-1 describes the use case pre-conditions.

Table 5.2.1.4-1: Use case #1 pre-conditions

#	Pre-condition	Description
1	The NFV-MANO system is operational.	
2	Public cloud resources are ready and can be used by the NFVI.	
3	The NFV-MANO can interact with the management system of the public Cloud provider	

5.2.1.5 Post-conditions

Table 5.2.1.5-1 describes the use case post-conditions.

Table 5.2.1.5-1: Use case #1 post-conditions

#	Post-condition	Description
1	The NS is instantiated successfully using resources across the hybrid Cloud and it is ready for subsequent lifecycle management by the NFV-MANO system.	

5.2.1.6 Flow description

Table 5.2.1.6-1 describes the use case flow.

Table 5.2.1.6-1: Use case #1 flow description

#	Actor/Role	Action/Description
Begins when	Operator -> OSS/BSS	The Operator request, via the OSS/BSS to deploy an NS across the hybrid Cloud.
1	OSS/BSS -> NFV-MANO system	The OSS/BSS requests the deployment of the NS. The request can include specific requirements regarding location of different constituents of the NS, including the case of locations fulfilled by resources provided by the public Cloud.
2	NFV-MANO system	The NFV-MANO system analyses the NS instantiation request and deems that the NS can be deployed across NFVI-PoPs from both, private Cloud and public Cloud. The NFV-MANO system determines the resource capacity needed at each NFVI-PoPs from private Cloud and public Cloud.
3	NFV-MANO system	Decides of the optimal placement of the NS and its constituents at the NFVI-PoPs.
4	NFV-MANO	The NFV-MANO requests the allocation of resources from the private Cloud needed for the NS to be instantiated.
5	NFV-MANO <-> Public Cloud Management system	The NFV-MANO requests to the Public Cloud Management system the allocation of resources from the public Cloud needed for the NS to be instantiated.
6	NFV-MANO	Proceeds with the instantiation of the NS through the deployment of its constituent VNFs.
Ends when	NFV-MANO system -> OSS/BSS	Notifies that the NS has been instantiated successfully across hybrid Cloud.

5.2.2 Use case #2: Building/Setting up the NFVI of the hybrid Cloud

5.2.2.1 Introduction

This use case showcases a scenario where an operator deems that the private Cloud can no longer cope with the load of VNFs and NSs that need to be deployed and decides to scale out its private Cloud resources by expanding it using resources from the public Cloud offered by a Cloud service provider.

5.2.2.2 Actors and roles

Table 5.2.2.2-1 describes the use case actors and roles.

Table 5.2.2.2-1: Use case #2 actors and roles

#	Actor and role	Description
1	Operator	A human being or an organization seeking to deliver network services to end-users.
2	OSS/BSS	The entity that receives the Operator's request for the initiation or termination of a VNF/NS.
3	NFV-MANO	The management and orchestration entity in charge of VNFs/NSs lifecycle management and OAM support and resource orchestration.
4	Public Cloud Management system	The entity from the Cloud service provider which is responsible for managing the public Cloud.

5.2.2.3 Trigger

Table 5.2.2.3-1 describes the use case trigger.

Table 5.2.2.3-1: Use case #2 trigger

Trigger	Description
1	The use case is triggered when an Operator decides to scale out their NFVI by expanding their available resources at their private Cloud by reserving additional infrastructure resources from a public Cloud.

5.2.2.4 Pre-conditions

Table 5.2.2.4-1 describes the use case pre-conditions.

Table 5.2.2.4-1: Use case #2 pre-conditions

#	Pre-condition	Description
1	Connectivity between Operator's private Cloud and the public Cloud of the Cloud service provider is feasible.	The Operator knows that connectivity is feasible, even if not yet established.
2	NFV-MANO can interact with the public Cloud service provider's management system.	N/A.

5.2.2.5 Post-conditions

Table 5.2.2.5-1 describes the use case post-conditions.

Table 5.2.2.5-1: Use case #2 post-conditions

#	Post-condition	Description
1	Operator's NFVI is successfully scaled out across private and public Cloud.	Additional steps would be needed to setup the new private/public Cloud NFVI-PoPs with the proper management systems to integrate/interwork with the Operator's NFV-MANO.

5.2.2.6 Flow description

Table 5.2.2.6-1 describes the use case flow.

Table 5.2.2.6-1: Use case #2 flow description

#	Actor/Role	Action/Description
Begins when	Operator -> OSS/BSS	The Operator requests, via the OSS/BSS to scale out the NFVI with resources also from public Cloud.
1	OSS/BSS -> Public Cloud Management System	To provision the necessary resources at the public Cloud side, the OSS/BSS provides the necessary information in terms of resource requirements and capacity to the Public Cloud Management system.
2	Public Cloud Management system	Proceeds to the allocation of the necessary resources at the public Cloud.
3	Public Cloud Management System -> OSS/BSS	The Public Cloud Management system notifies the OSS/BSS that the necessary resources from the public Cloud are ready to be used.
4	OSS/BSS -> NFV-MANO	The OSS/BSS informs the NFV-MANO that new NFVI-PoPs are ready to use based on the resources available at the private and the public Clouds.
Ends when	NFV-MANO	NFV-MANO starts interacting with the management system of the public Cloud provider and can use the resources provided by the public Cloud provider.

5.3 Use cases about new types of infrastructure resources

5.3.1 Use case #3: Allocating acceleration resources to VNFs

5.3.1.1 Introduction

Use cases about the use of acceleration resources and mechanisms in NFV environment are described in ETSI GS NFV-IFA 001 [i.7]. The intent of the present use case is to introduce new hardware accelerators such as DPUs, smart-NICs, AI processors, etc., to deliver acceleration capabilities to VNFs in VM-based but also container-based deployment environments.

The use case assumes that the NFV-MANO is aware of the acceleration resources, capabilities, and capacity in the NFVI and can manage the allocation of the acceleration resources to the VNF instances. As analysed in ETSI GR NFV-IFA 046 [i.31] the NFV-MANO framework up to Release 5 is not able to manage acceleration resources for container-based deployments since the Extensible Para-virtualised Device (EPD) model is tailored to VM-based and hypervisor-based solutions.

5.3.1.2 Actors and roles

Table 5.3.1.2-1 describes the use case actors and roles.

Table 5.3.1.2-1: Use case #3 actors and roles

#	Actor and role	Description
1	NFV-MANO system	The management and orchestration entity in charge of VNFs/NSs lifecycle management and OAM support and resource orchestration.
2	NFVI	The compendium of physical and virtualised resources, including software elements of the infrastructure. The NFVI provides the required acceleration resources for the deployment and operation of VNF instances.
3	OSS/BSS	The entity that receives the Operator's request for the initiation of a VNF instance which requires acceleration support.

5.3.1.3 Trigger

Table 5.3.1.3-1 describes the use case trigger.

Table 5.3.1.3-1: Use case #3 trigger

Trigger	Description
1	The use case is triggered when a VNF requires acceleration resources to be used.

5.3.1.4 Pre-conditions

Table 5.3.1.4-1 describes the use case pre-conditions.

Table 5.3.1.4-1: Use case #3 pre-conditions

#	Pre-condition	Description
1	The NFV-MANO system is operational.	
2	The VNF package is already onboarded.	The VNFD describes the requirements of acceleration capabilities.
3	The acceleration resources are available in the NFVI.	

5.3.1.5 Post-conditions

Table 5.3.1.5-1 describes the use case post-conditions.

Table 5.3.1.5-1: Use case #3 post-conditions

#	Post-condition	Description
1	The necessary acceleration resources are successfully allocated to the VNF instance.	

5.3.1.6 Flow description

Table 5.3.1.6-1 describes the use case flow.

Table 5.3.1.6-1: Use case #3 flow description

#	Actor/Role	Action/Description
1	OSS/BSS-> NFV-MANO	The OSS triggers the instantiation of a VNF which requires acceleration support.
2	NFV-MANO system	The NFV-MANO assesses the acceleration capability requirements for the VNF (e.g. by processing the VNFD) and the available acceleration resources. This includes the selection of the appropriate resource zones and/or CIS clusters providing such acceleration resources.
3	NFV-MANO system<-> NFVI	The NFV-MANO performs the allocation of the appropriate NFVI resources, including the proper acceleration resources, needed for the VNF to be instantiated. See note.
4	NFV-MANO system	The NFV-MANO proceeds with the instantiation of the VNF, including the acceleration resources to the VNF instance.
NOTE: The NFV-MANO interacts with the appropriate management entity if needed for the configuration of the acceleration resources.		

5.3.2 Use case #4: Creating bare-metal server pool with DPUs

5.3.2.1 Introduction

The purpose of this use case is to create a pool of bare-metal servers consisting of DPUs and install requisite software components to these bare-metal servers, needed for provisioning virtual networking and acceleration resources offered by the DPUs.

5.3.2.2 Actors and roles

Table 5.3.2.2-1 describes the use case actors and roles.

Table 5.3.2.2-1: Creating bare-metal server pool with DPUs actors and roles

#	Actor and role	Description
1	Consumer	The entity which consumes the bare-metal server pools provided by the PIM.
2	PIM	The entity responsible for managing physical resources in the NFVI.
3	NFVI	The compendium of physical and virtualised resources, including software elements of the infrastructure.

5.3.2.3 Trigger

Table 5.3.2.3-1 describes the use case trigger.

Table 5.3.2.3-1: Creating bare-metal server pool with DPUs trigger

Trigger	Description
1	The Consumer requests the PIM to create a bare-metal server pool with DPUs in the NFVI.

5.3.2.4 Pre-conditions

Table 5.3.2.4-1 describes the use case pre-conditions.

Table 5.3.2.4-1: Creating bare-metal server pool with DPUs pre-conditions

#	Pre-condition	Description
1	The PIM is operational.	
2	The NFVI is operational.	

5.3.2.5 Post-conditions

Table 5.3.2.5-1 describes the use case post-conditions.

Table 5.3.2.5-1: Creating bare-metal server pool with DPUs post-conditions

#	Post-condition	Description
1	A bare-metal server pool with DPUs is created successfully in the NFVI.	

5.3.2.6 Flow description

Table 5.3.2.6-1 describes the use case flow.

Table 5.3.2.6-1: Creating bare-metal server pool with DPUs flow description

#	Actor/Role	Action/Description
Begins when	Consumer -> PIM	The consumer requests the PIM to create a bare-metal server pool, in which the constituent bare-metal server instances with DPUs are to be created.
1	PIM<-> NFVI	The PIM creates the bare-metal server pool with DPUs managed object. The PIM also creates each respective bare-metal server instance in the pool, having both DPUs and CPUs according to the resource requirements of the bare-metal server pool.
2	PIM	The PIM powers on each respective bare-metal server instance in the pool and checks physical server status including the DPU components (e.g. DPU OS) to be available. The PIM installs requisite software components to these bare-metal servers, needed for provisioning virtual networking and acceleration resources offered by the DPUs.
Ends when	PIM -> Consumer	The PIM responds to the Consumer with the successful indication of creating bare-metal server pool.

5.3.3 Use case #5: Create CIS cluster on bare-metal server pool with DPUs

5.3.3.1 Introduction

The present use case proposes a process on creating a CIS cluster on a bare-metal server pool with DPUs in the NFVI. The prerequisite of this use case is that the bare-metal server pool with DPUs has been successfully created and the requisite software components (e.g. the vSwitch, iSCSI-Initiator, and OpenStack® Neutron and Cinder agents) have been successfully installed in the DPUs.

NOTE: The OpenStack® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. ETSI is not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

5.3.3.2 Actors and roles

Table 5.3.3.2-1 describes the use case actors and roles.

Table 5.3.3.2-1: Create CIS cluster on bare-metal server pool with DPUs actors and roles

#	Actor and role	Description
1	Consumer	The entity which consumes the CIS cluster created on the bare-metal server pool with DPUs.
2	CCM	The entity responsible for the lifecycle and OAM management of the CIS cluster.
3	VIM	The entity responsible for managing virtualised resources in the NFVI.
4	PIM	The entity responsible for managing physical resources in the NFVI.
5	NFVI	The compendium of physical and virtualised resources, including software elements of the infrastructure.

5.3.3.3 Trigger

Table 5.3.3.3-1 describes the use case trigger.

Table 5.3.3.3-1: Create CIS cluster on bare-metal server pool with DPUs trigger

Trigger	Description
1	The Consumer requests CCM to create a CIS cluster on a bare-metal server pool with the DPUs in the NFVI.

5.3.3.4 Pre-conditions

Table 5.3.3.4-1 describes the use case pre-conditions.

Table 5.3.3.4-1: Create CIS cluster on bare-metal server pool with DPUs pre-conditions

#	Pre-condition	Description
1	CCM is operational.	
2	VIM is operational.	
3	PIM is operational.	
4	NFVI is operational.	The bare-metal server pool with the DPUs is created and the requisite software components are installed in the DPU.

5.3.3.5 Post-conditions

Table 5.3.3.5-1 describes the use case post-conditions.

Table 5.3.3.5-1: Create CIS cluster on bare-metal server pool with DPUs post-conditions

#	Post-condition	Description
1	A CIS cluster is created successfully on a bare-metal server pool with the DPUs in NFVI.	

5.3.3.6 Flow description

Table 5.3.3.6-1 describes the use case flow.

Table 5.3.3.6-1: Create CIS cluster on bare-metal server pool with DPUs flow description

#	Actor/Role	Action/Description
Begins when	Consumer -> CCM	The Consumer requests CCM to create a CIS cluster on a bare-metal server pool with DPUs.
1	CCM -> VIM/PIM	The CCM requests VIM/PIM to assign a set of available bare-metal servers from the server pool to the CIS cluster to be created.
2	VIM/PIM <-> NFVI	The VIM/PIM installs operating system on the bare-metal servers if needed and creates virtualised network and storage resources in the DPUs of the bare-metal servers.
3	VIM/PIM -> CCM	The VIM/PIM responds to CCM that the bare-metal servers are successfully assigned to the CIS cluster to be created.

#	Actor/Role	Action/Description
4	CCM	The CCM installs the CIS cluster software to the bare-metal servers and make them available as CIS cluster nodes.
Ends when	CCM -> Consumer	The CCM responds to the Consumer with the successful indication of creating the CIS cluster on the target bare-metal server pool with DPUs (as requested in the "begins when").

5.3.4 Use case #6: Offloading components to DPUs of a bare-metal server pool

5.3.4.1 Introduction

The present use case proposes a process of offloading components to DPUs of a bare-metal server pool in the NFVI. Components contain requisite software to the bare-metal servers needed for provisioning virtual networking and storage resources offered by the DPU, e.g. vSwitch, iSCSI-Initiator, OpenStack® Neutron and Cinder agents.

5.3.4.2 Actors and roles

Table 5.3.4.2-1 describes the use case actors and roles.

Table 5.3.4.2-1: Offloading components to DPUs of a bare-metal server pool actors and roles

#	Actor and role	Description
1	Consumer	The entity which consumes the bare-metal server pools provided by the PIM.
2	VIM	The entity responsible for managing virtualised resources in the NFVI.

5.3.4.3 Trigger

Table 5.3.4.3-1 describes the use case trigger.

Table 5.3.4.3-1: Offloading components to DPUs of a bare-metal server pool trigger

Trigger	Description
1	The Consumer requests the VIM to install components to DPUs of a bare-metal server pool.

5.3.4.4 Pre-conditions

Table 5.3.4.4-1 describes the use case pre-conditions.

Table 5.3.4.4-1: Offloading components to DPUs of a bare-metal server pool trigger pre-conditions

#	Pre-condition	Description
1	The VIM is operational.	
2	The bare-metal server pool with the DPUs has been created, and each respective bare-metal server in the pool are powered on and with normal status.	

5.3.4.5 Post-conditions

Table 5.3.4.5-1 describes the use case post-conditions.

Table 5.3.4.5-1: Offloading components to DPUs of a bare-metal server pool trigger post-conditions

#	Post-condition	Description
1	The components have been installed (offloaded) to DPUs of the bare-metal server pool.	

5.3.4.6 Flow description

Table 5.3.4.6-1 describes the use case flow.

Table 5.3.4.6-1: Offloading components to DPUs of a bare-metal server pool trigger flow description

#	Actor/Role	Action/Description
Begins when	Consumer -> VIM	The consumer requests the VIM to install components to DPUs of a bare-metal server pool.
1	VIM	The VIM installs necessary components to DPUs of the bare-metal server pool and makes the installed components available.
Ends when	VIM -> Consumer	The VIM responds to the Consumer with the successful indication of installing (offloading) components to DPUs of a bare-metal server pool.

5.3.5 Use case #7: Instantiating container-based VNFs on a bare-metal CIS cluster with DPUs

5.3.5.1 Introduction

The present use case proposes a process on instantiating container-based VNFs on a bare-metal CIS cluster. The bare-metal CIS cluster is created by using bare-metal server instances from a bare-metal server pool with DPUs.

5.3.5.2 Actors and roles

Table 5.3.5.2-1 describes the use case actors and roles.

Table 5.3.5.2-1: Instantiating container-based VNFs on a bare-metal CIS cluster with DPUs actors and roles

#	Actor and role	Description
1	NFVO	The entity which initiates the instantiation process of container-based VNFs.
2	VNFM	The entity which performs the instantiation process of container-based VNFs.
3	CISM	The entity which performs the instantiation process of containerized workloads (VNFs/VNFCs) based on an MCIOP.

5.3.5.3 Trigger

Table 5.3.5.3-1 describes the use case trigger.

Table 5.3.5.3-1: Instantiating container-based VNFs on a bare-metal CIS cluster with DPUs trigger

Trigger	Description
1	The NFVO requests the VNFM to instantiate container-based VNFs. The NFVO triggers the instantiation of a container-based VNFs, upon request from OSS-BSS.

5.3.5.4 Pre-conditions

Table 5.3.5.4-1 describes the use case pre-conditions.

Table 5.3.5.4-1: Instantiating container-based VNFs on a bare-metal CIS cluster with DPUs pre-conditions

#	Pre-condition	Description
1	The bare-metal CIS cluster on top of a bare-metal server pool with DPUs has been created and is operational.	
2	The NFVO, VNFM, CISM and CIS are operational.	
3	Storage and networking resource requirements related to bare-metal server nodes to accommodate the VNF are specified in the VNFD as well as in declarative descriptors of the VNF's constituent MCIOs belonging to an MCIOP.	

5.3.5.5 Post-conditions

Table 5.3.5.5-1 describes the use case post-conditions.

Table 5.3.5.5-1: Instantiating container-based VNFs on a bare-metal CIS cluster with DPUs post-conditions

#	Post-condition	Description
1	Container-based VNFs are instantiated, by using the bare-metal server resources in the bare-metal CIS cluster with DPUs.	

5.3.5.6 Flow description

Table 5.3.5.6-1 describes the use case flow.

Table 5.3.5.6-1: Instantiating container-based VNFs on a bare-metal CIS cluster with DPUs flow description

#	Actor/Role	Action/Description
Begins when	NFVO -> VNFM	The NFVO requests the VNFM to instantiate container-based VNFs.
1	VNFM -> CISM	The VNFM requests the CISM to instantiate container-based VNFs and their constituent VNFCs based on an MCIOP referenced in the VNFD. The CIS components instantiate and schedule MCIOs that use the DPU resources in the CIS cluster nodes of the bare-metal CIS cluster.
2	CISM -> VNFM	The CISM responds to the VNFM with a successful indication of instantiating container-based VNFs/VNFCs based on an MCIOP.
Ends when	VNFM -> NFVO	The VNFM responds to the NFVO with a successful indication of instantiating container-based VNFs.

5.3.6 Use case #8: Reconfigurable intelligent surfaces as a network resource

5.3.6.1 Introduction

As part of the propagation wireless environment, RISs can perform various operations on the impinging wireless signal/ wavefronts (e.g. polarization, beam steering, refraction, etc.). As a result of these operations, coverage and network efficiency can be improved and the signal received by mobile users can be enhanced.

This use case introduces the onboarding of an RIS as a new type of physical network resources. RISs can be understood as an additional type of NFVI resource which can be used to extend the RAN segment one hop closer to the end user.

5.3.6.2 Actors and roles

Table 5.3.6.2-1 describes the use case actors and roles.

Table 5.3.6.2-1: Use case #8 actors and roles

#	Actor and role	Description
1	NFVO	The NFV-MANO component in charge of resource orchestration.
2	PIM	The entity responsible for physical resources management.
3	OSS/BSS	The entity adding the new RIS resource information in NFV-MANO.

5.3.6.3 Trigger

Table 5.3.6.3-1 describes the use case trigger.

Table 5.3.6.3-1: Use case #8 trigger

Trigger	Description
1	The use case is triggered when the OSS/BSS calls the PIM inventory management service to add a new RIS resource.

5.3.6.4 Pre-conditions

Table 5.3.6.4-1 describes the use case pre-conditions.

Table 5.3.6.4-1: Use case #8 pre-conditions

#	Pre-condition	Description
1	The PIM inventory can manage information related to RIS.	
2	The RIS has been installed and is connected to the NFVI.	

5.3.6.5 Post-conditions

Table 5.3.6.5-1 describes the use case post-conditions.

Table 5.3.6.5-1: Use case #8 post-conditions

#	Post-condition	Description
1	A new RIS resource has been successfully added in the inventory of the physical resources managed by PIM.	

5.3.6.6 Flow description

Table 5.3.6.6-1 describes the use case flow.

Table 5.3.6.6-1: Use case #8 flow description

#	Actor/Role	Action/Description
1	OSS/BSS ->PIM	OSS/BSS calls the PIM Physical resource inventory management service interface to add a new RIS resource.
2	PIM	PIM updates the physical resource inventory with the new RIS resource.
3	PIM -> NFV-MANO, OSS/BSS	PIM informs NFV-MANO and OSS/BSS about the inventory update.

5.3.7 Use case #9: RIS as a PNF

5.3.7.1 Introduction

The previous use case describes the onboarding of an RIS as new network resource that extends the RAN part. This use case investigates the scenario where an RIS is considered a PNF rather than a new resource type. This means an RIS PNF can be connected to other VNFs (i.e. VNFs supporting RAN related functionalities) as part of an integrated NS.

5.3.7.2 Actors and roles

Table 5.3.7.2-1 describes the use case actors and roles.

Table 5.3.7.2-1: Use case #9 actors and roles

#	Actor and role	Description
1	NFV-MANO system	The management and orchestration entity in charge of VNFs/NSs lifecycle management and OAM support and resource orchestration.
2	OSS/BSS	The entity providing the description of a NS and requesting the instantiation of NS including new PNFs of type RIS.

5.3.7.3 Trigger

Table 5.3.7.3-1 describes the use case trigger.

Table 5.3.7.3-1: Use case #9 trigger

Trigger	Description
1	The use case is triggered when the OSS/BSS request to instantiate an NS that include an RIS-PNF.

5.3.7.4 Pre-conditions

Table 5.3.7.4-1 describes the use case pre-conditions.

Table 5.3.7.4-1: Use case #9 pre-conditions

#	Pre-condition	Description
1	The RIS PNF is available in the NFVI.	
2	The NSD and the PNFD specifying the characteristics of the connection points exposed RIS PNF are onboarded.	

5.3.7.5 Post-conditions

Table 5.3.7.5-1 describes the use case post-conditions.

Table 5.3.7.5-1: Use case #9 post-conditions

#	Post-condition	Description
1	An NS comprising an RIS as a PNF is successfully instantiated.	

5.3.7.6 Flow description

Table 5.3.7.6-1 describes the use case flow.

Table 5.3.7.6-1: Use case #9 flow description

#	Actor/Role	Action/Description
1	OSS/BSS -> NFV-MANO system	The OSS/BSS requests the NFVO to instantiate an NS that makes use of an RIS as a PNF.
2	NFVO	The NFVO verifies (if not already done previously when onboarding the NSD) that all descriptors referenced in the selected NS deployment flavour, or a respective overriding descriptor indicated in the operation, are on-boarded.
3	NFV-MANO system -> NFVI	The NFVO assesses the request of the OSS/BSS and requests from the NFVI the availability of the RIS PNF and the necessary resources to deploy the rest of the VNFs comprising the NS.
4	NFV-MANO system	The NFV-MANO proceeds with the instantiation of the NS, including connecting the RIS with other VNFs or other PNFs according to the information provided by the NSD. All VLs, VNF FGs and PNF Connection Points (CPs) are created and configured.
5	NFV-MANO system -> OSS/BSS	NFV-MANO notifies OSS/BSS about the successful instantiation of the NS.

5.4 Use cases about location and mobility of infrastructure

5.4.1 Use case #10: Network service deployment across vehicular infrastructure

5.4.1.1 Introduction

This use case is about deploying NSs across a vehicular infrastructure. The use case assumes that the NFV-MANO has full knowledge of the location, the availability of resources in each vehicle, as well as the time interval during which the resources are expected to be around (due to vehicles' mobility). The NFV-MANO then selects the VNFs placement based on this information.

5.4.1.2 Actors and roles

Table 5.4.1.2-1 describes the use case actors and roles.

Table 5.4.1.2-1: Use case #10 actors and roles

#	Actor and role	Description
1	Operator	A human being or an organization seeking to deliver NSs to end-users.
2	OSS/BSS	The entity that receives the Operator's request for the initiation or termination of a VNF/NS.
3	NFV-MANO system	The management and orchestration entity in charge of VNFs/NSs lifecycle management and OAM support and resource orchestration.
4	NFVI	Includes the physical and the virtualised resources. The NFVI provides the required resources for the deployment and operation of NS/VNF instances. The NFVI also includes compute, network and storage resources available at the vehicles.

5.4.1.3 Trigger

Table 5.4.1.3-1 describes the use case trigger.

Table 5.4.1.3-1: Use case #10 trigger

Trigger	Description
1	The use case is triggered when an Operator requests to instantiate an NS with constituent VNFs deployed in vehicles.

5.4.1.4 Pre-conditions

Table 5.4.1.4-1 describes the use case pre-conditions.

Table 5.4.1.4-1: Use case #10 pre-conditions

#	Pre-condition	Description
1	The NFV-MANO system is operational.	
2	The NFV-MANO system is aware of the availability of infrastructure resources provided by the vehicles.	This information includes location and time.

5.4.1.5 Post-conditions

Table 5.4.1.5-1 describes the use case post-conditions.

Table 5.4.1.5-1: Use case #10 post-conditions

#	Post-condition	Description
1	The NS is successfully instantiated across both the Cloud infrastructure and the vehicular network, and it is ready for subsequent lifecycle management by the NFV-MANO system.	

5.4.1.6 Flow description

Table 5.4.1.6-1 describes the use case flow.

Table 5.4.1.6-1: Use case #10 flow description

#	Actor/Role	Action/Description
1	Operator -> OSS/BSS	The Operator requests, via the OSS/BSS, to deploy the NS.
2	OSS/BSS -> NFV-MANO system	The OSS/BSS instructs the NFV-MANO to deploy the NS.
3	NFV-MANO system	The NFVO receives the NS instantiation request. Based on its knowledge of resources availability in terms of time and location, the NFVO decides on the optimal placement of the NS's VNFs within both the Cloud and the vehicular network.
4	NFV-MANO system	The NFV-MANO performs the allocation of NFVI resources needed for the NS to be instantiated.
5	NFV-MANO system -> OSS/BSS	NFV-MANO notifies the OSS/BSS that the NS has been instantiated successfully.

5.4.2 Use case #11: Network service scaling using infrastructure on HAPS

5.4.2.1 Introduction

This use case covers the scenario of scaling out an NS by deploying more instances of VNFs in a HAPS node. This can occur when some VNFs require additional computational capacity due to a sudden increase in the workload (e.g. large and temporary events, flash crowds, etc.) and there are no available ground-based Cloud resources.

The use case assumes that the NFV-MANO has knowledge of the resources available at the HAPS node, its location, and the time interval during which the node is available near the targeted area. The NFV-MANO provides the necessary NS orchestration for the VNFs deployed in the ground-based Cloud and those deployed in the HAPS node.

5.4.2.2 Actors and roles

Table 5.4.2.2-1 describes the use case actors and roles.

Table 5.4.2.2-1: Use case #11 actors and roles

#	Actor and role	Description
1	NFV-MANO system	The management and orchestration entity in charge of VNFs/NSs lifecycle management and OAM support and resource orchestration.
2	NFVI	Includes the physical and the virtualised resources. The NFVI provides the required resources for the deployment and operation of NS/VNF instances. In this context, the NFVI comprises ground-based Cloud as well as HAPS Cloud infrastructure.

5.4.2.3 Trigger

Table 5.4.2.3-1 describes the use case trigger.

Table 5.4.2.3-1: Use case #11 trigger

Trigger	Description
1	The use case is triggered when there is a need to scale an NS using HAPS resources due to a sudden or planned increase in workload.

5.4.2.4 Pre-conditions

Table 5.4.2.4-1 describes the use case pre-conditions.

Table 5.4.2.4-1: Use case #11 pre-conditions

#	Pre-condition	Description
1	The NFV-MANO system is operational.	
2	The NFV-MANO is aware of the availability of the infrastructure resources supplied by the HAPS.	This information includes location and time.
3	HAPS NFVI-PoP has connectivity to the NFV-MANO system and other ground-based NFVI-PoPs.	

5.4.2.5 Post-conditions

Table 5.4.2.5-1 describes the use case post-conditions.

Table 5.4.2.5-1: Use case #11 post-conditions

#	Post-condition	Description
1	The additional VNF(s) are successfully instantiated in the HAPS node, and ready for subsequent lifecycle management by the NFV-MANO.	

5.4.2.6 Flow description

Table 5.4.2.6-1 describes the use case flow.

Table 5.4.2.6-1: Use case #11 flow description

#	Actor/Role	Action/Description
1	NFV-MANO system	The NFV-MANO receives a request to scale out the NS or NS scale decision is made based on the information provided in the NSD (auto-scaling).
2	NFV-MANO system	The NFV-MANO allocates the needed resources in the NFVI to instantiate the VNFs instances on the HAPS NFVI-PoP.
3	NFV-MANO system	The NFV-MANO system instantiates the new VNF instances in the HAPS node.

6 Key issue analysis

6.1 Introduction

From the use cases documented in clause 5, the following key issues are identified. Additional key issues are expected to be documented in future versions of the present document.

6.2 Key issues on resources heterogeneity

6.2.1 RIS related key issues

Key issue #1.1: Integration of RISs as new NFVI resources and NFV-MANO management

The use case in clause 5.3.6 describes the onboarding of RISs as new physical network resources. RISs can be considered as an additional type of NFVI resources which can be used to extend the RAN. Similarly to the case of network devices (e.g. routers), RISs are typically controlled by an entity that can resemble an SDN controller in how it manages network devices.

Some management and control aspects to consider related to these new resource types are the following:

- Which data is relevant to the management aspects (LCM, FM, PM, etc.) of RISs resources and how this data can be collected and communicated to an NFV-MANO entity (e.g. PIM)?
- Based on which information the NFV-MANO entity (e.g. PIM) can perform the allocation of RISs resources and how this allocation is performed?
- How can the NFV-MANO monitor RISs, for example, regarding energy consumption metrics?

Key issue #1.2: RISs as new NFVI resources managed by an external entity

In contrast to the other physical network resources (e.g. routers, switches, CPU resources, acceleration resources, etc.), RISs are likely to be owned by an external service provider (e.g. a building owner). Thus, the operator's NFV-MANO system might need to interact with the RIS management and control system of the external RIS provider to manage and control these resources.

The following questions are therefore being raised:

- Integrating RIS technology into the NFVI means that there is a need to define the interface through which the NFV-MANO can manage these resources. Which NFV-MANO entity (e.g. PIM) and over which interface it will communicate with the RIS management and control system?
- Since RISs are likely to be infrastructure that is provided by a third-party, what is the demarcation point regarding the management performed of the NFV-MANO system and that of the RISs management and control entity?

6.2.2 Acceleration resources related key issues

Key issue #2.1: Energy consumption management

As stated in clause 4.3.7, smart-NICs have a major drawback which is their high energy consumption:

- For both virtualised and containerized environments how can the NFV-MANO monitor the energy consumption of the acceleration hardware (i.e. with which entity it needs to interact)?
- For both virtualised and containerized environments which performance metrics can be associated to energy efficiency with regard to the use of hardware acceleration resources?
- For VNFs/VNFCs using acceleration resources, which performance metrics can be associated to energy efficiency with regard to the use of hardware acceleration resources?

6.3 Key issues on location, provision and distribution of resources

6.3.1 Hybrid Cloud related key issues

Key issue #3.1: Defining the management scopes of the NFV-MANO and the Cloud service provider

When considering hybrid Cloud deployments, the management aspects of VNFs and NSs through the NFV-MANO system need to consider how to interact with the Cloud service provider's management system whenever VNFs or certain NS constituents are deployed on a public Cloud (see use case #1).

This key issue aims at investigating aspects related to service management scope when considering hybrid Cloud infrastructures by asking some related questions:

- To manage VNFs and NSs deployed using public Cloud resources, what are the boundaries of responsibility regarding functionalities provided by the NFV-MANO and functionalities supported by the management system of the public Cloud provider? For example, what are the potential splits of functionality and scope between the two management domains (e.g. NS-level by operator, VNF and resource-level by Public Cloud provider) for all management aspects (LCM, performance, fault, etc.)?

  How the operator decides common management principles for both private and public Clouds depending on the Cloud computing model (e.g. IaaS, PaaS, FaaS, etc.)?

Key issue #3.2: Interactions and modelling between NFV-MANO and public Cloud management system

In order to manage VNFs or NSs deployed in the public Cloud, the NFV-MANO system of the operator might need to interact with public Cloud management system. This might involve setting up dedicated interfaces and using specific APIs. It may also suggest that there are changes to be made at the descriptors level. Following are some questions related to these issues:

- What standardized or other de-facto interfaces can be used for the interaction between the NFV-MANO and the management systems of the public Cloud provider?
- Which Cloud provider agnostic templates/descriptors can be used to facilitate interactions related for example to resource management?

Key issue #3.3: VNF placement

In hybrid Cloud deployments, the network operator's NFV-MANO system may need to learn the available deployment locations at the public Cloud side. Based on this information, as well as resource requirements and affinity/anti-affinity rules, the NFV-MANO system selects the preferred placement of VNFs/NS to be deployed at the public Cloud NFVI-PoPs. This key issue rises the following questions to understand the process of VNFs/NSs placement in hybrid Cloud:

- How can the public Cloud management system communicate to the NFV-MANO system information about the available deployment locations? And what is the granularity of the location information?

Key issue #3.4: Connection between the operator's private Cloud NFVI-PoPs and infrastructure provided by the Cloud provider

Use case #2 in clause 5.2.2 describes how an operator can expand its NVFI resources by making use of public Cloud resources. Related questions about connectivity aspects between public and private Clouds are the following:

- Considering WIM operations according to ETSI GS NFV-IFA 032 [i.9] for the inter NFVI-PoP connectivity which network management systems can be used to establish connectivity between different hybrid Cloud-based NFVI-PoPs and/or other infrastructure?

6.4 Key issues on resources mobility

6.4.1 HAPS related key issues

Key issue #4.1: Generic issues related to HAPS operations

Use case #11 illustrates the scaling out of an NS by resorting to HAPS node. Unlike the deployment/scaling out of VNFs/NSs by means of ground-based Cloud infrastructure, the use of HAPS infrastructure for such rollouts - in specific situations – carries certain limitations and/or requires further setups.

This key issue identifies the potential limitations that might impact the NSs/VNFs deployments and operations. Questions raised in the context of this key issue include, but are not exhaustive, the following:

- How can the NFV-MANO become aware of the energy efficiency capabilities as well as energy consumption of HAPS nodes?
- In such resource-constrained environment, what are the virtualisation technologies that can be considered to deploy VNFs in HAPS?
- How can the NFV-MANO manage remote HAPS nodes to efficiently handle the scarcity of computing and storage resources?
- How can the infrastructure provided by HAPS be available and "stable" from the perspective of NFV-MANO, despite their energy lifespan limitations?

Key issue #4.2: Handling failures and performance monitoring

As discussed in clause 4.3.4 of the present document, HAPS nodes can be subject to weather conditions susceptible to introduce delay and leading to increase in the latency impacting for example time-sensitive VNFs. Furthermore, inter-HAPS communication might also be affected.

Failures due to power shortage or server crashes on the HAPS nodes or a malfunction in one of a VNF deployed on a HAPS node, can affect NSs deployed across both ground-based Cloud and HAPS nodes.

This key issue is about performance issues like latency related issues and failure management of the HAPS node. Related questions to this key issue are (the list is not exhaustive):

- How is the FM and PM data collected within HAPS system and how it is communicated to the NFV-MANO?
- How the NFV-MANO manages failures by leveraging such information?
- What is the process by which the NFV-MANO performs failovers considering the location and the availability limitations of HAPS?
- Which HAPS metrics can be monitored by NFV-MANO?

Key issue #4.3: HAPS mobility and joint management of HAPS system and ground-based Cloud

This key issue concerns HAPS mobility aspect and its impact on ensuring uninterrupted availability of services provided by VNF/NS instances deployed across ground and HAPS Cloud domains. Questions associated with this key issue include, but are not limited to, the following:

- How the NFV-MANO can be made aware of the trajectory, location, the time intervals during which a HAPS node will be available to supply target area with connectivity, as well as computing, storage, and network capabilities that it will deliver?
- Can the NFV-MANO anticipate mobility and latency issues and decide VNF placement proactively?
- How the NFV-MANO reacts when time-sensitive VNFs are impacted by latency due to HAPS mobility?
- How to enable the NFV-MANO to operate a joint/federated ground-based Cloud and HAPS resource management?

Key issue #4.4: Management of signalling between HAPS and ground-infrastructure

Data exchange between HAPS and terrestrial infrastructure (e.g. ground-based Cloud, BS, vehicular network, end-users, etc.) can induce signalling overhead that may have an impact on the entire NS performance . This key issue discusses the communication between the ground infrastructure and the HAPS nodes. Questions that could possibly rise in this context include the following (the list is not exhaustive):

- How to minimize the signalling overhead when it comes to the VNF management signalling protocols?

6.4.2 Vehicular infrastructure related key issues

Key issue #5.1: Limitations of vehicular infrastructure

As shown in use case #10 clause 5.4.1, VNFs and NSs can be deployed across both the Cloud and the vehicular infrastructure, expanding the connectivity coverage, and thus, allowing the delivery of services to remote areas or the performance of time-sensitive computational tasks at the end-user's proximity. This coverage expansion brings certain challenges which need to be addressed. Questions that can be associated with this key issue include the following:

- The on-boarded hardware in the vehicular nodes tends to be of a relatively small size, implying that processing and storage capabilities are limited. Therefore, virtualisation technologies that would be considered in such a context need to take into consideration resource limitations.

Key issue #5.2: Connectivity establishment

The possibility of deploying some VNFs of a NS in the Cloud and others in vehicular nodes means that multiple endpoints of infrastructure need to be connected. Furthermore, the NFVI-PoPs within the vehicular network need to support network connectivity for the NFV-MANO operations. Establishing the connectivity requires considering the types of information exchanged within NFV-MANO, between NFV-MANO and VNFs deployed in the vehicles and between VNFs deployed in vehicles themselves. Hence, related questions to this key issue are:

- How the NFV-MANO components can be connected to VNFs deployed on the vehicular nodes for management purposes? How the VNFs in different vehicular nodes are connected to each other? And what are the appropriate access technologies to use?
- How to address the volatility issue of communication paths between nodes from the NFV framework perspective?

Key issue #5.3: Orchestration and management of VNFs/NSs considering mobility and availability of vehicular infrastructure

Vehicular nodes are moving and to deploy and monitor VNFs/NSs, the NFV-MANO needs to access information about the vehicles' mobility pattern, their locations, time intervals in which each node is present in a certain area, as well as the storage and computational capabilities of each node. This key issue involves the mobility aspects of vehicular nodes and how it affects the NFV-MANO decisions for determining the placement of the VNFs/NSs and their monitoring.

Location information can be also used to facilitate decision making for placement, routing, and jointly managing the Cloud and the vehicular network. Questions associated with this key issue include, but are not limited to, the following:

- How the NFV-MANO can collect data, and which data is necessary, e.g. about vehicular nodes mobility, location, the time intervals during which a vehicular node will be available to offer storage and/or computational resources?
- Vehicles are present in a certain point for a relatively short period of time, making the topology of the vehicular infrastructure changing constantly and, in some cases, in an unpredictable manner. Considering this, are there any specific considerations that NFV-MANO and the network operator should consider for the kinds of workloads that can be placed on vehicular infrastructure?
- How to enable the NFV-MANO to jointly manage the Cloud and the vehicular infrastructure resources, and their performance and faults monitoring?

Key issue #5.4 Structure of vehicular infrastructure

In order to expose the resources made available by the vehicular nodes to the NFV-MANO, the vehicular infrastructure needs to be modelled, e.g. in the form of NFVI nodes, considering vehicular nodes as an NFVI-PoPs, or the whole vehicular infrastructure as an NFVI-PoP, etc. This raises the following questions:

- How the vehicular infrastructure can be modelled and exposed to NFV-MANO for orchestration and management purposes?

Key issue #5.5 Security and privacy aspects

One of the main challenges for vehicular infrastructure is that the infrastructure provided is under control by various actors, not just the network operator. This situation imposes specific security and privacy challenges. Hence it is important to examine its impact on the deployment of VNFs/NSs in the vehicular nodes from a security and privacy perspective:

- Deploying VNFs and NSs in vehicular nodes means that the NFV-MANO need to be made aware of new types of security threats.

- How can the NFV-MANO supervise the security status of the deployed VNFs/NSs?

- Can the existing NFV-MANO certificate management framework be applied for the case of vehicular networks?

- Do vehicular network security threats have an impact on how VNFs are deployed (e.g. type of virtualisation technologies or any other additional considerations)?

- What are the privacy aspects to be considered and addressed for consuming infrastructure that is provided by a third-party?

7 Framework and potential solutions

7.1 Introduction

Clause 7 documents potential solutions addressing the key issues discussed in clause 6 of the present document. Each solution is organised as follows:

- introduction describing the background and the conceptual information underlying the solution;

- description of the solution;

- reference to the key issues tackled by the solution; and

- identification of the gaps in the ETSI NFV architectural framework and/or referenced ETSI NFV specifications, if applicable.

Table 7.1-1 includes a list of the solutions devised and the key issues they cover.

Table 7.1-1: Summary of solutions and related key issues

Solution	Title	Related key issues
Solution #1	Management scopes and interactions between the NFV-MANO and the public Cloud in case of infrastructure provisioning	#3.1: Defining the management scopes of the NFV-MANO and the Cloud service provider #3.2: Interactions and modelling between NFV-MANO and public Cloud management system
Solution #2	Management scopes and interactions between the NFV-MANO and public Cloud in case of infrastructure provisioning and VNFs management.	#3.1: Defining the management scopes of the NFV-MANO and the Cloud service provider #3.2: Interactions and modelling between NFV-MANO and public Cloud management system
Solution #3	Management scopes and interactions between the NFV-MANO and public Cloud in case of infrastructure provisioning and VNFs and NSs management	#3.1: Defining the management scopes of the NFV-MANO and the Cloud service provider #3.2: Interactions and modelling between NFV-MANO and public Cloud management system
Solution #4	Multi-site connectivity service between private Cloud sites and public Cloud sites provided by WIM	#3.4: Connection between the operator's private Cloud NFVI-PoPs and infrastructure provided by the Cloud provider
Solution #5	VNF placement in the public Cloud	#3.3: VNF placement
Solution #6	VNF placement in the public Cloud with prior knowledge of available locations	#3.3: VNF placement
Solution #7	NFV-MANO aware of HAPS mobility, power consumption, and hardware resources	#4.1: Potential limitations of HAPS system #4.3: HAPS mobility and joint management of HAPS system and ground-based Cloud
Solution #8	Mapping VNFs' requirements to HAPS availability	#4.1: Potential limitations of HAPS system #4.3: HAPS mobility and joint management of HAPS system and ground-based Cloud
Solution #9	Suitable virtualisation technologies for resource- and power-constrained environment such as HAPS	#4.1: Potential limitations of HAPS system
Solution #10	LCM and OAM operations related to VNFs deployed over NFVI provided by HAPS	#4.2: Handling failures and performance monitoring
Solution #11	Predicting and handling failures of VNFs and NSs deployed on infrastructure provided by HAPS	#4.2: Handling failures and performance monitoring

7.2 Potential solutions

7.2.1 Solutions related to hybrid Cloud resource provisioning and management

7.2.1.1 Introduction

As stated in key issues #3.1, #3.2, and use cases #1 and #2, a network operator might need to deploy VNFs and NSs across the hybrid Cloud. The demarcation of the management areas of the NFV-MANO and the public Cloud service provider, as well as the interaction between these two systems, are aspects to be considered to ensure the proper operability of the network.

Depending on the VNFs specific characteristics (e.g. monolithic/microservices architecture, stateful/stateless, short-lived/persistent VNFs, etc.) and requirements (e.g. latency, computing resources, privacy and security, etc.) the network operator can decide to either deploy VNFs on their private Cloud or at the public Cloud. In the latter scenario, three cases are possible, and they are devised as follows:

- Case #1: the network operator leverages the public Cloud to provision infrastructure resources. The management of the deployed VNFs/NSs is done by the network operator using NFV-MANO.
- Case #2: the network operator leverages the public Cloud to provision infrastructure resources. The management of the VNFs is made using tools offered by the public Cloud provider. NS are managed by the network operator.

- Case #3: the network operator outsources the provisioning of the infrastructure resources, the management of VNFs as well as the management of NSs deployed in the public Cloud to the Cloud service provider. The operator is responsible for OSS related operations.

7.2.1.2 Solution #1: Management scopes and interactions between the NFV-MANO and public Cloud management system in case of infrastructure provisioning

7.2.1.2.1 Solution description

The present solution investigates the above-mentioned case #1, to define the boundary between the NFV-MANO and the Cloud service provider in terms of management and their interactions.

In this case, network operators access the Cloud infrastructure resources (i.e. compute, storage, network, VMs) exposed by the public Cloud service provider, to deploy their VNFs and NSs. The management of the latter is handled by the operator using NFV-MANO. The operator can opt for this approach in the cases, for instance, where:

- the VNFs to be deployed at the public Cloud side are computationally intensive and expect to leverage pools of acceleration resources provided by the Cloud;
- the functions load varies drastically (unpredictable scaling needs).

IaaS and CaaS can be the appropriate Cloud computing models in this context. Under the IaaS model, the operator has more configurability, since it provides freedom of resources selection and on-demand access to these resources which enables the operator to scale up/down according to the NFs needs. CaaS can also be adopted in the case of deploying containerized NFs. In this case the deployment environment is managed and maintained by the public Cloud service provider.

In case of IaaS computing model, VNFM can be deployed on the public Cloud for LCM and FCAPS of VNFs, but still under management control by the network operator. As for the PIM and VIM functionalities, they are handled by the public Cloud service provider who takes care of managing the infrastructure and the virtual resources. The CISM and CCM can be deployed on the public Cloud in case if containerized workloads are envisaged, but still under management control by the network operator.

In case of CaaS computing model, VNFM can be deployed on the public Cloud for LCM and FCAPS of VNFs, but still under management control by the network operator. The PIM, CCM and VIM functionalities are handled by the public Cloud service provider who takes care of managing the container cluster infrastructure (and the virtual resources if needed). The CISM functionalities are provided by the Cloud service provider. Furthermore, CCM can be provided by the public Cloud to manage the CIS clusters deployed therein, to interact with the NFVO (see note), or to configure additional CIS cluster capabilities [i.10] (if not provided by the Cloud service provider).

NOTE: In both cases the network operator manages the NSs LCM through NFVO, deployed across private and public Clouds. The NFVO has a global view of the hybrid Cloud.

Interactions of the NFV-MANO managed entities by the network operator with the Cloud service provider system(s) can be identified in case existing specifications like for example ETSI GS NFV-IFA 005 [i.11] for the management of virtualised resources, ETSI GS NFV-IFA 053 [i.12] for the management of physical resources, ETSI GS NFV-IFA 036 [i.10] for the management of CIS clusters, are also supported by the public Cloud provider.

7.2.1.2.2 Key issues addressed

The present solution addresses the following key issues described in clause 6:

- Key issue #3.1;
- Key issue #3.2.

7.2.1.2.3 Gap analysis

No gaps are identified.

7.2.1.3 Solution #2: Management scopes and interactions between the NFV-MANO and public Cloud management system in case of infrastructure provisioning and NFs management

7.2.1.3.1 Solution description

The present solution investigates case #2 introduced in clause 7.2.1.1, where the public Cloud service provider provides the infrastructure resources to the network operator but also provides the tools for managing specific types of VNFs to be deployed on these resources. As in solution #1, the demarcation between the NFV-MANO and the Cloud service provider's system in terms of management, their interactions, are established and proposals for the suitable Cloud computing models are provided.

In the case #2, the Cloud service provider is in charge of supplying the infrastructure resources and manage the deployed set of specific types of VNFs also. This can be suitable for the network operator in the case, for instance, of short-lived VNFs. The network operator is driven more about network service delivery agility and provisioning, rather than NFs provisioning.

For example, Cloud computing models such as PaaS and FaaS are related to such types of deployments. FaaS is more intended for short-lived, stateless VNFs, with no particular scalability pattern. More detailed study about FaaS can be found in ETSI GR NFV-EVE 025 [i.18]. Telco PaaS comprises a collection of Cloud services associated with computing, networking, and storage management. These services are designed to decouple the Telco Cloud infrastructure from the processes of application development and operation, specifically pertaining to VNFs within the Telco Cloud domain. PaaS can support operations for VNFs with perpetual computational resources needs, predictable scaling requirement, prompt processing of the incoming requests (i.e. with no start-up delay), and stateful VNFs. An example of PaaS used by public Cloud providers is Openshift Container Platform®, which relies on a Kubernetes® environment to support the LCM of container-based applications and their dependencies on various computing platforms. Table 7.2.1.3.1-1 shows, in both cases, the components that are managed by the Cloud provider, and those managed by the network operator.

NOTE 1: Openshift® is a trademark of is a trademark of Red Hat®, Inc., registered in the United States and other countries. Kubernetes® is a registered trademark of the Linux Foundation® in the United States and other counties. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of the products named.

Table 7.2.1.3.1-1: Management scopes of the Cloud service provider and network operator while mapping to NFV-MANO scopes according to the chosen Cloud computing model

Cloud computing model	Management scope of the Cloud provider	Management scope of the network operator	NFV-MANO entities to deploy at the public Cloud side
PaaS	Network, storage, compute, virtualisation, OS, containers management, runtime,	VNFs, data.	VNFM, PIM, VIM, CISM, and CCM related functionalities are provided by the Cloud service provider who takes care of managing the infrastructure, the virtual resources, and the LCM/OAM of the deployed VNFs. See notes 1 and 2.
FaaS	Network, storage, compute, virtualisation, OS, containers management, runtime, NFs (scalability, OAM, etc.)	VNFs (providing the code of the functions and the triggering events to instantiate them), data.	
NOTE 1: In both cases the network operator manages the NSs deployed across private and public Clouds. NFVO can have a global view of the hybrid Cloud. NOTE 2: In case of PaaS computing model, the PaaS Service Manager (PSM) and the PaaS Service Repository (PSR) functionalities can be provided by the Cloud service provider management system or by the NFV-MANO system of the network operator.			

Interactions of the NFV-MANO managed entities by the network operator with the Cloud service provider system(s) can be identified. NFV-MANO process can be exploited in case existing specifications like for example ETSI GS NFV-IFA 005 [i.11] for the management of virtualised resources, ETSI GS NFV-IFA 053 [i.12] for the management of physical resources, and ETSI GS NFV-IFA 036 [i.10] for the management of CIS clusters, are also supported by the public Cloud service provider management system:

- In the case of FaaS, the network operator can communicate via the NFVO to the Cloud service provider VNFs management the events triggering the instantiation of VNFs when implemented in a FaaS form.
- Between the network operator's NFVO and the PaaS service management functions of the Cloud service provider: if the PaaS services are offered by the public Cloud provider, the interface between the NFVO and the PSM-related functionality provided by the public Cloud can be used by the NFV-MANO to request the association with one or more PaaS service instances provided by the public Cloud.
- Between the network operators PaaS Service Management functions (PSM and PSR) and the public Cloud virtualised resource management:
    - If the PaaS services are provided by the network operator as VNFs, then the PSM can interact with the public Cloud provider management system to support the VNFs LCM.
    - The PSM can also interact with the cloud provider entity providing CISM related functionality to deploy, terminate or scale a PaaS service if the latter consists of MCCO(s).

NOTE 2: The public Cloud provider can still use the interfaces specified in ETSI GS NFV-IFA 049 [i.19] for PaaS service management.

7.2.1.3.2 Key issues addressed

The present solution addresses the following key issues described in clause 6:

- Key issue #3.1;
- Key issue #3.2.

7.2.1.3.3 Gap analysis

The referenced ETSI NFV specifications in the present solution do not specify:

Gap #2.1: The support of FaaS related management capabilities and related modelling.

Gap #2.2: The usage of the interface between NFVO and PSM to request the association with PaaS services offered by a 3rd party.

7.2.1.4 Solution #3: Management scopes and interactions between the NFV-MANO and public Cloud management system in case of infrastructure provisioning and VNFs and NSs management

7.2.1.4.1 Solution description

In the case #3, the network operator provision resources from the public Cloud service provider, the latter is also in charge of the management of VNFs and NSs deployed on its infrastructure. In this case, to manage VNFs, the reference points and the interfaces referred to in solutions #1 and #2 can be used by the Cloud service provider according to the Cloud computing model chosen by the network operator.

In the case that the network operator delegates the management of the NS instances to the Cloud service provider, the OSS/BSS of the network operator can interact with an entity providing NFVO-like functionality supported by the Cloud service provider by leveraging the NS LCM and other management functionalities services and corresponding interfaces specified in the ETSI GS NFV-IFA 013 [i.14].

The public Cloud can also host nested NS instances that are part of composite NS instances spanning the hybrid Cloud. To exchange information related to NSs such as LCM, OAM, usage notification of NSs, etc., the network operator needs to interact with the public Cloud service provider management system.

ETSI GS NFV-IFA 030 [i.13] specifies functional requirements, interfaces and operations to support the provision of NSs across multiple administrative domains. These latter can be used in the case of hybrid Cloud, in fact, the NFVO-like functionality provided by the public Cloud service provider can be considered as the NFVO-N (according to ETSI GS NFV-IFA 030 [i.13] terminology) managing the NS instances which are part of composite NS instances managed by the network operator's NFVO, which can be considered in this case as the NFVO-C that manages the composite NSs.

Figure 7.2.1.4.1-1 shows a composite NS instance deployed across the operator's private Cloud and the public Cloud managed by the NFVO-C with a nested NS deployed in the public Cloud and under the management of NFVO-N. The Or-Or reference point provided in NFV-MANO architecture [i.15] can be used to provide the interoperability needed to run the composite NSs across the hybrid Cloud.

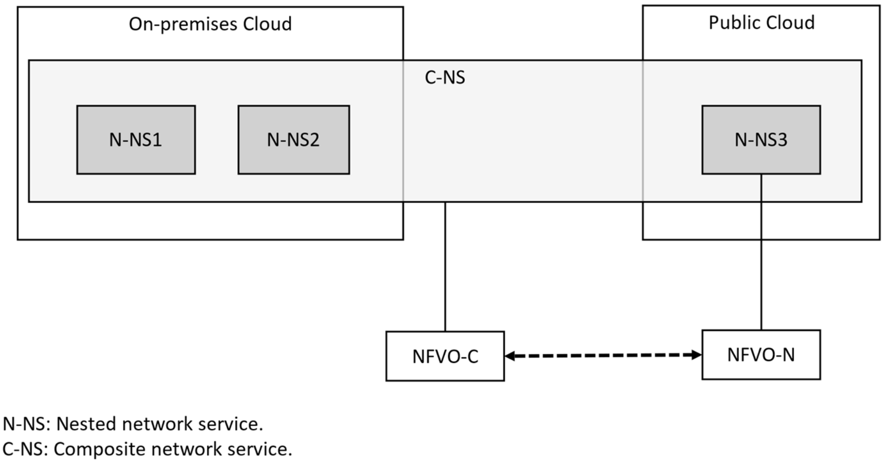

On-premises Cloud
Public Cloud
C-NS
N-NS1
N-NS2
N-NS3
NFVO-C
NFVO-N
N-NS: Nested network service.
C-NS: Composite network service.

Figure 7.2.1.4.1-1: Interaction between the NFVO-like functionality of the public Cloud (NFVO-N) and the NFV-MANO NFVO (NFVO-C)

7.2.1.4.2 Key issues addressed

The present solution addresses the following key issues described in clause 6:

- Key issue #3.1;
- Key issue #3.2.

7.2.1.4.3 Gap analysis

No gaps are identified.

7.2.2 Solutions related to connectivity for hybrid Cloud deployments

7.2.2.1 Introduction

Key issue #3.4 deals with the connectivity between private Cloud NFVI-PoP(s) and public Cloud NFVI-PoP(s) in case of hybrid Cloud deployments. VNFs deployed across multiple NFVI-PoPs of hybrid Cloud might require network connectivity via WAN to form a network service spanning across multiple sites. The following clauses provide solutions related to multi-site connectivity for hybrid Cloud deployments.

7.2.2.2 Solution #4: Multi-site connectivity service between private Cloud sites and public Cloud sites provided by WIM

7.2.2.2.1 Solution description

The present solution leverages the Multi-Site Connectivity Service (MSCS) managed by the WIM in the NFV-MANO framework to establish connectivity between VNFs deployed across private Cloud sites and public Cloud sites. The MSCS and set of interfaces and information elements that WIM exposes for MSCS management are specified in ETSI GS NFV-IFA 032 [i.9].

Figure 7.2.2.2-1-1 illustrates the logical view of a simple hybrid Cloud deployment where two network functions (VNF A and VNF B), that compose a network service, are deployed across NFVI-PoPs belonging to private Cloud and public Clouds. The NS virtual link between the two VNFs extends across the WAN that connects the two NFVI-PoPs. Detailed relationship between such a multi-site NS and multi-site connectivity framework is described in ETSI GS NFV-IFA 032 [i.9].

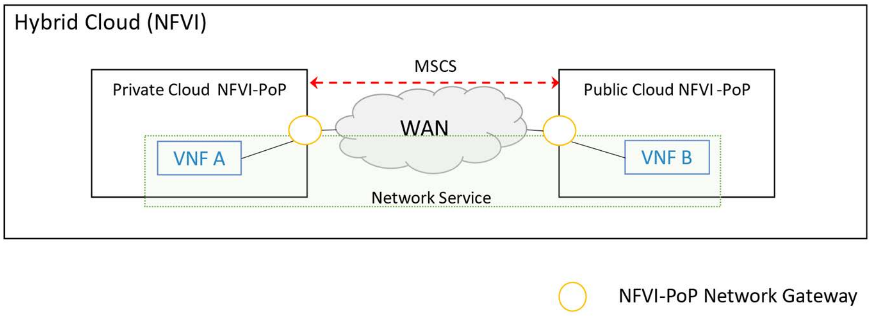


Figure 7.2.2.2.1-1: Multi-site connectivity service between private Cloud sites and public Cloud sites

The MSCS management interface produced by the WIM, specified in ETSI GS NFV-IFA 032 [i.9], enables creation of MSCS between multiple NFVI-PoPs. In addition to MSCS, the WIM manages another object related to multi-site connectivity, Multi-site Network Connection (MSNC). MSNCs represent connectivity service endpoints establishing connectivity and enabling the data forwarding between different NFVI-PoPs. For the hybrid Cloud setup illustrated in figure 7.2.2.2.1-1, the MSCS endpoints (i.e. MSNCs) are associated to ports/interfaces on the corresponding NFVI-PoP network gateways of private Cloud and public Cloud NFVI-PoPs. These MSNCs can be established via diverse network protocols (e.g. VPLS, EVPN, MPLS, MP-BGP) and at different network layers, i.e. layer 2 or layer 3.

The inter-site connectivity in hybrid Cloud deployments, i.e. between private Cloud and public Cloud sites, can be realized by L2 or L3 Virtual Private Network (VPN) technologies. Detailed analysis of L2 and L3 VPN technologies and how the MSCS managed by the WIM can be used to realize and configure these VPN technologies is provided in ETSI GR NFV-IFA 035 [i.16].

NOTE: Connectivity of Public Cloud to other network operator assets that are not NFVI-PoPs are not investigated in the present document version.

7.2.2.2.2 Key issues addressed

The present solution addresses the following key issues described in clause 6:

- Key issue #3.4.

7.2.2.2.3 Gap analysis

Gap #4.1: In the case of hybrid Clouds, it is not specified which management entity is managing the gateway system and how the demarcation point is specified. It is also not clear under which management domain the WIM resides.

7.2.3 Solution related to VNF placement in the hybrid Cloud

7.2.3.1 Solution #5: VNF placement in the public Cloud

7.2.3.1.1 Introduction

Key issue #3.3 addresses VNF placement in the context of hybrid Cloud deployment. Requirements and constraints about VNFs' placement at the operator's private Cloud are discussed in the existing specifications (refer to ETSI GS NFV-IFA 011 [i.17]). However, with the hybrid Cloud and the integration of public Cloud infrastructure, the operator's NFV-MANO system needs to learn about the available deployment locations at the public Cloud in order to decide of the VNFs placement.

7.2.3.1.2 Solution description

As specified ETSI GS NFV-IFA 011 [i.17] the VNFD metadata contains description about constraints and requirements related to the placement of VMs/containers making the VNF/VNFC. For instance, the Vdu information element, which supports the description of the deployment and operational behaviour of VNFC presents attributes such as:

- mcioConstraintParams indicating the expected constraints to be assigned to MCIOs realizing the VDU, the constraints can be about location, affinity/anti-affinity rules, etc.

- requestedAdditionalCapabilities specifying requirements for additional capabilities such as acceleration related capabilities.

- extendedResourceRequest specifying the resources to be extended in order to accommodate properly the VNF.

The information contained in these attributes and in the VNFD metadata can be interpreted by the NFVO of the operator's NFV-MANO which can identify possible deployment locations in the public Cloud corresponding to the requirement expressed through the aggregated information. The public Cloud management system can advise the operator of the available location(s) that are suitable for the deployment of the VNF. The operators' NFV-MANO system can then confirm the location proposed by the public Cloud management system or choose among the proposed locations if several have been suggested.

Along with the metadata and the aforementioned attributes the operator might need to provide information about location (e.g. edge, central Cloud, etc.), specific geographical region, latency, energy consumption, etc., to refine the selection of appropriate location(s) by the public Cloud management system.

7.2.3.1.3 Key issues addressed

The present solution addresses the following key issues:

- Key issue #3.3.

7.2.3.1.4 Key issues addressed

The current ETSI NFV specifications do not specify:

Gap #5.1: The granularity of the location information for VNF deployment at the public Cloud side.

7.2.3.2 Solution #6: VNF placement in the public Cloud with prior knowledge of available locations

7.2.3.2.1 Introduction

Solution #5 addresses the VNF placement key issue by considering that the NFVO of the operator's NFV-MANO communicate to the public Cloud management system the requirement of the VNFs, the latter identifies possible deployment locations corresponding to these requirements and suggests them to the operator's NFV-MANO. The present solution assumes that the operator's NFVO has prior knowledge about available locations at the public Cloud side.

7.2.3.2.2 Solution description

The operator's NFV-MANO has already collected information about available locations from the public Cloud (e.g. geographical data, operational capacities, such as, processing capabilities, storage, network bandwidth, etc.). Using this information, the operator's NFV-MANO can then choose effectively the most suitable location(s) that accommodates the needs of each VNFs to be deployed.

Once the selection is made, the operator's NFV-MANO communicates this pre-selection to the management system of the public Cloud. The latter can assess the proposed selection and reserves the requested resources in the selected placement. Otherwise, the management system of the public Cloud notifies the operator's NFV-MANO that the proposed placement is not possible, for it to revise its selection.

The same information contained in the attributes (refer to ETSI GS NFV-IFA 011 [i.17]) mentioned in the previous solution and in the VNFDs can be used by the operator's NFVO to perform the placement selection.

7.2.3.2.3 Key issues addressed

The present solution addresses the following key issues:

- Key issue #3.3

7.2.3.2.4 Gap analysis

The current ETSI NFV specifications do not specify:

Gap #6.1: the interface and information elements exposed by the NFVO to communicate the selected placement and receiving notifications from the public Cloud management system.

7.2.4 Solution related to HAPS

7.2.4.1 Introduction

As outlined in clause 4.3.4, HAPS present a viable solution for numerous use cases. In use case #11, the process of scaling out an NS through HAPS infrastructure is described. To fully leverage HAPS, it is crucial to find a workaround for certain issues, including their constrained power supply, which limits their availability to a brief timeframe. As a result, a HAPS, which offers network coverage to a designated area, can be substituted by another HAPS that is not necessarily equipped with the same hardware resources. This ongoing cycle of substitution can challenge the NFV-MANO system in managing resources provided by HAPS as a "stable" resource and providing uninterrupted service to end users. This clause provides solutions to the aforementioned key issues.

7.2.4.2 Solution #7: NFV-MANO aware of HAPS mobility, power consumption, and hardware resources

7.2.4.2.1 Introduction

To manage NFVI resources hosted by HAPS, the NFV-MANO system needs to gather information about HAPS mobility and trajectory (as indicated in key issue #4.3), HAPS energy capabilities (refer to key issue #4.1), as well as the hardware resources they provide. The present solution focuses on enabling the NFV-MANO system to collect this information from the ground facilities that control HAPS.

7.2.4.2.2 Solution description

It is essential to collect data regarding HAPS mobility and trajectories as well as hardware resources available on-board of each HAPS and information about power storage. The collected information can be used later to plan VNFs/NSs migration when a HAPS is substituted by another to serve a particular area (as depicted in figure 7.2.4.2.2-1).

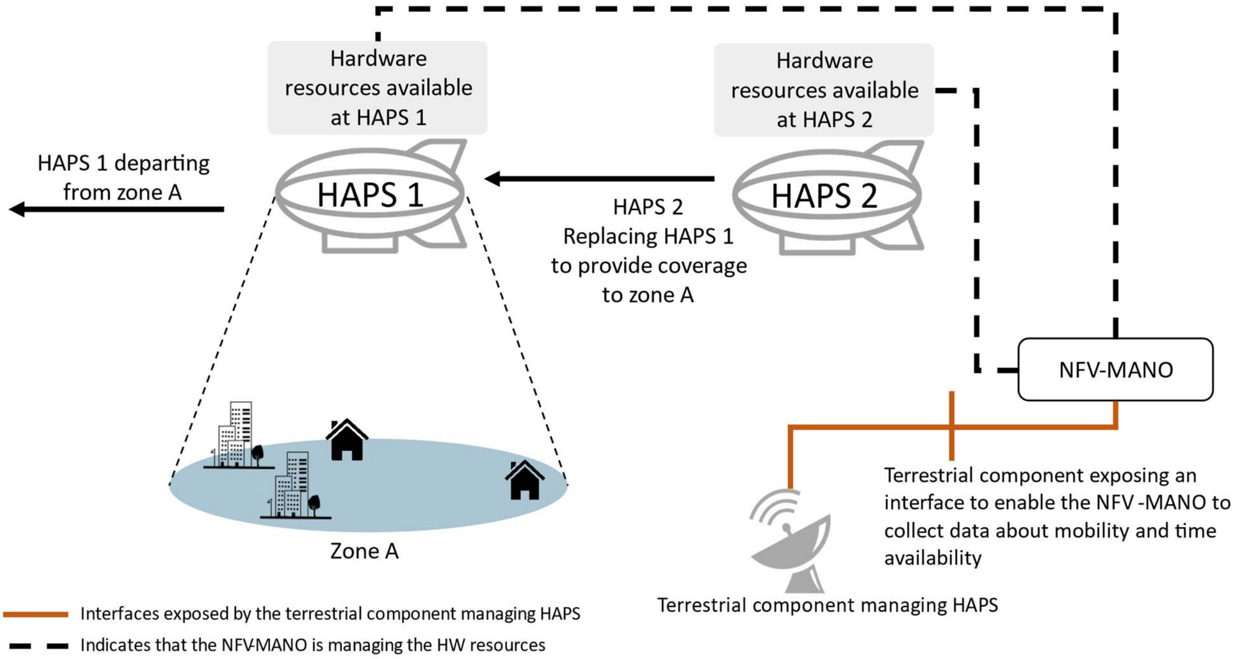

Hardware resources available at HAPS 1
Hardware resources available at HAPS 2
HAPS 1 departing from zone A
HAPS 1
HAPS 2
HAPS 2 Replacing HAPS 1 to provide coverage to zone A
NFV-MANO
Zone A
Terrestrial component exposing an interface to enable the NFV -MANO to collect data about mobility and time availability
Terrestrial component managing HAPS
Interfaces exposed by the terrestrial component managing HAPS
Indicates that the NFV-MANO is managing the HW resources

Figure 7.2.4.2.2-1: HAPS system architecture

HAPS systems consist of an airship and a terrestrial component. The airship features a platform that accommodates NFV infrastructure for the deployment VNFs/NSs. The terrestrial facilities include the control station which is linked to the airship (via a feeder link). The ground control station is managing the altitude and trajectory of the airship. The ground control station managing the HAPS can expose an interface to enable the NFV-MANO to collect data about mobility, time availability as well as hardware resources available at each HAPS.

More specifically, once it is decided that infrastructure resources provided by a HAPS will be managed by the NFVO of the NFV-MANO system, this latter can collect information about HAPS trajectory and power consumption to decide of the deployment (or otherwise the migration) timing of VNFs/NSs and to estimate the timeframe during which the HAPS will be managed by the NFV-MANO. The PIM, which performs inventory of physical resources, can start collecting information about the hardware resources provided by the HAPS and update its inventory (ETSI GS NFV-IFA 053 [i.12]).

7.2.4.2.3 Key issues addressed

The present solution addresses the following key issues described in clause 6:

- Key issue #4.1;
- Key issue #4.3.

7.2.4.2.4 Gap analysis

The referenced ETSI NFV specifications in the present solution do not specify:

Gap #7.1: To support communication between the NFV-MANO system and HAPS management systems like the terrestrial component managing HAPS mobility.

Gap #7.2: Information about mobility and time availability of the infrastructure resources provided by HAPS.

7.2.4.3 Solution #8: Mapping VNFs' requirements to HAPS availability

7.2.4.3.1 Introduction

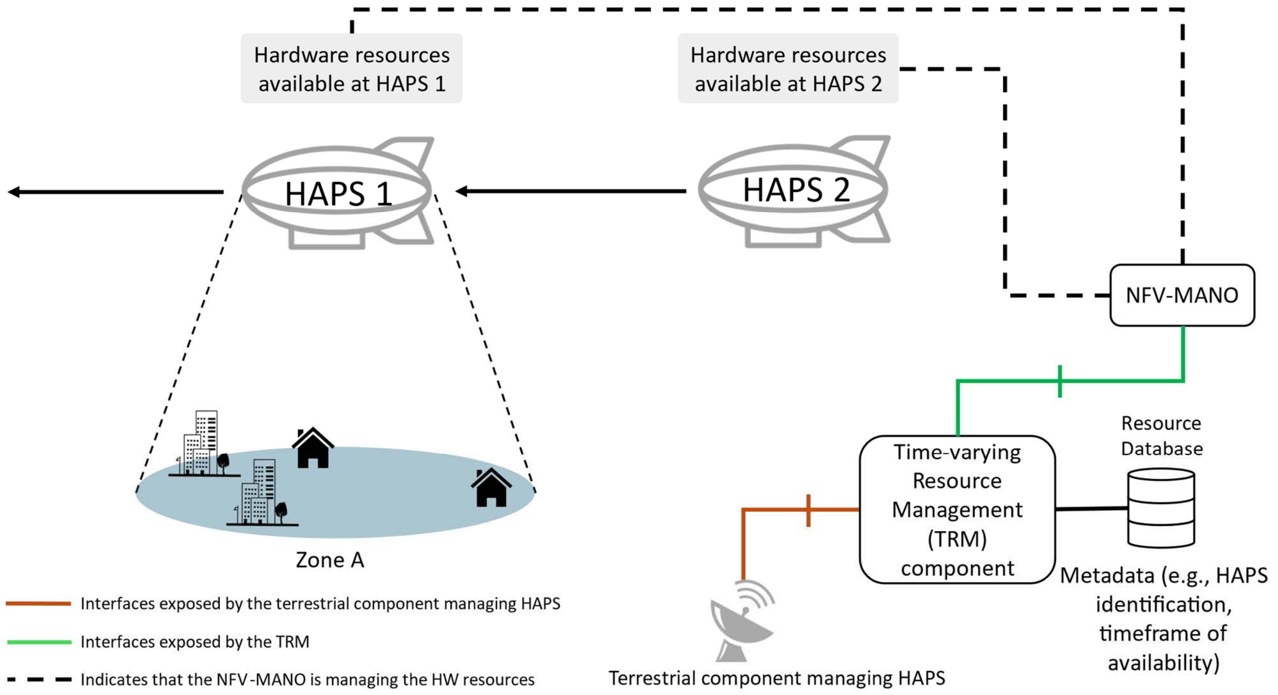
Solution #7 in clause 7.2.2.2 describes how the NFV-MANO can collect the necessary information about HAPS trajectory, availability timeframe, power consumption, and on-board hardware resources from the ground facilities controlling the HAPS. The present solution outlines how the NFV-MANO can delegate this task to a Time-varying Resource Management (TRM) component. Besides this task, the latter can perform a mapping between the requirements of the VNFs/NSs to the most suitable HAPS (or collection of HAPS) in terms of timeframe availability, geographical availability, and hardware resources provided on-board.

7.2.4.3.2 Solution description

The NFV-MANO managing the NFVI can indicate to the TRM the requirements of the VNFs/NSs to be deployed on the NFVI provided by HAPS. The requirements communicated by the NFV-MANO comprises:

- the location at which the VNFs/NSs need to be provided;
- the time period during which the VNFs/NSs need to be provided; and
- the hardware resources expected to enable the deployment of these VNFs/NSs.

The TRM (refer to figure 7.2.4.3.2-1) requests from the ground facilities managing the HAPS information about locations at which HAPS hardware resources are available (compute, storage, memory, network), as well as their capacity, the time periods at which the hardware resources are available at these locations, and the energy consumption information. The TRM can store this information in a resource database. The TRM can then match the aforementioned information with the requirements expressed by the NFV-MANO to determine which HAPS can be used to provide the VNFs/NSs at the specified locations and within the specified timeframes. It should be noted that to provide coverage at one location, the hardware resources available at one or more HAPS can be used.



Hardware resources available at HAPS 1
Hardware resources available at HAPS 2
HAPS 1
HAPS 2
NFV-MANO
Zone A
Resource Database
Time-varying Resource Management (TRM) component
Metadata (e.g., HAPS identification, timeframe of availability)
Terrestrial component managing HAPS
Interfaces exposed by the terrestrial component managing HAPS
Interfaces exposed by the TRM
Indicates that the NFV-MANO is managing the HW resources

Figure 7.2.4.3.2-1: The TRM component mapping between the VNFs/NSs requirements and the availability of the hardware resources provided by HAPS

The TRM can forward the information about the possible options of hardware resource availability to the NFV-MANO, which can then choose the most suitable option from the ones offered. Alternatively, the TRM can perform the selection itself. Once the selection of the HAPS (or multiple HAPS) has been made, the TRM transmits the necessary metadata about the selected HAPS to the NFV-MANO (e.g. HAPS identification), enabling it to request access granting from the ground facilities controlling the HAPS, in order to deploy the VNFs/NSs. An NFV-MANO entity like PIM can start collecting information about the hardware resources provided by the HAPS and update its inventory accordingly (ETSI GS NFV-IFA 053 [i.12]).

7.2.4.3.3 Key issues addressed

The present solution addresses the following key issues described in clause 6:

- Key issue #4.1;
- Key issue #4.3.

7.2.4.3.4 Gap analysis

The referenced ETSI NFV specifications in the present solution do not specify:

Gap #8.1: The interfaces and the information elements used for the exchanges between the NFV-MANO and the Time-varying Resource Management component.

7.2.4.4 Solution #9: Suitable virtualisation technologies for resource- and power-constrained environment such as HAPS

7.2.4.4.1 Introduction

Decreasing the power consumption related to VNFs operations can enable sustainable HAPS coverage for longer periods. Therefore, a comprehensive understanding of resource utilization associated with each virtualisation technology, can facilitate the virtualisation technology selection and identify trade-offs between resource consumption, and the VNFs requirements such as security, computational efficiency, and latency.

The present solution describes some key characteristics that can be used with regard to resource management and energy consumption for VMs, containers, Wasm, MicroVMs, eBPF, and unikernels. A detailed analysis is needed for the selection of the appropriate technology when considering HAPS infrastructures.

7.2.4.4.2 Solution description

Table 7.2.4.4.2-1 provides a brief overview of the key architectural design aspects of each virtualisation technology that could influence their resource consumption. More details can be found in ETSI GR NFV-EVE 025 [i.18].

Table 7.2.4.4.2-1: Aspects of virtualisation technologies impacting their resource consumption

Virtualisation technology	Resource consumption
VMs	• Each VM operates with a full OS, including its own kernel, drivers, and user-space applications. Consequently, the demand for CPU and memory resources is anticipated to be substantial. Also, as each VM maintain its own OS image, the disk space usage can be significant. Furthermore, the booting process of a full OS can take seconds to minutes increasing power consumption. • A single machine can host a limited number of VMs compared to other virtualisation technologies.
Containers	• Containers share the host OS kernel and run as isolated user-space processes. This design implies low consumption of memory and CPU resources. Additionally, the applications and their dependencies are encapsulated within lightweight container, leading to relatively minimal storage requirement. They also offer fast startup time. • Many containers can run on a single host.
Wasm	• Wasm modules are compiled into highly optimized bytecode therefore they are extremely lightweight. They also have low CPU and memory usage, as the runtime manages their access to these components. Additionally, Wasm modules are designed to be portable across different architectures, and they are executed with near-native performance.
MicroVMs	• MicroVMs characterized by a reduced set of device models and drivers which results in low resource consumption due to the elimination unnecessary OS components. However, they can have higher resource consumption than, for example containers, as microVMs still use a minimal OS. Additionally, MicroVMs has a fast boot time. • MicroVMs can achieve higher density on physical hosts. This consolidation means more workloads per server.
eBPF	• eBPF operates within the kernel, reducing the necessity for context switching between user and kernel space, potentially lowering CPU usage. • eBPF exhibits low resource consumption for observability and networking tasks.
Unikernels	• In unikernels, the application and the OS components are compiled into a single binary, eliminating user-space/kernel-space separation, thereby reducing syscall overhead and context switching which can consume more resources. • The absence of OS boot process enables unikernels to achieve fast boot times.

In principle VMs are not ideal for resource- and power-constrained environments, such as HAPS. In contrast, containerization can offer a moderate level of efficiency compared with the other virtualisation technologies, making it a viable option for deploying VNFs on infrastructure supplied by HAPS. MicroVMs facilitate running multiple instances of VNFs on a single host, which is suitable for resource-constrained environment like HAPS. Wasm is precompiled and hence the bytecode provided is optimized and consume low resources. eBPF can be used for high performance networking, system monitoring, security, and observability, thereby eliminating the need for extra resource consumption Finally, unikernels, offer an immediate startup time, making them useful for on-demand microservices while optimizing resource utilization which is needed in NFVI provided by HAPS.

NOTE: The preceding analysis is not exhaustive; consequently, the definitive selection of a virtualisation technology necessitates a multifaceted and detailed examination.

7.2.4.4.3 Key issues addressed

The present solution addresses the following key issues described in clause 6:

- Key issue #4.1.

7.2.4.4.4 Gap analysis

The referenced ETSI NFV specifications in the present solution do not specify:

Gap #9.1: The use of Wasm, MicroVMs, eBPFs and Unikernels is not currently supported by NFV-MANO. See ETSI GR NFV-EVE 025 [i.18] for ongoing activities.

7.2.4.5 Solution #10: the LCM and OAM operations related to VNFs deployed over NFVI provided by HAPS

7.2.4.5.1 Solution description

The focus of this solution is to describe how the LCM and OAM operations related to VNFs deployed on NFVI provided by HAPS can be performed:

- Uploading VNFs images and the specific artifacts for deployments.

The images of a VNF as well as all the artifacts (e.g. runtimes, plugins, etc.) needed for its deployment can be uploaded by the NFV-MANO system to the HAPS via the gateway which then send them to the HAPS using a communication link (also known as feeder link) as shown in figure 7.2.4.5.1-1.

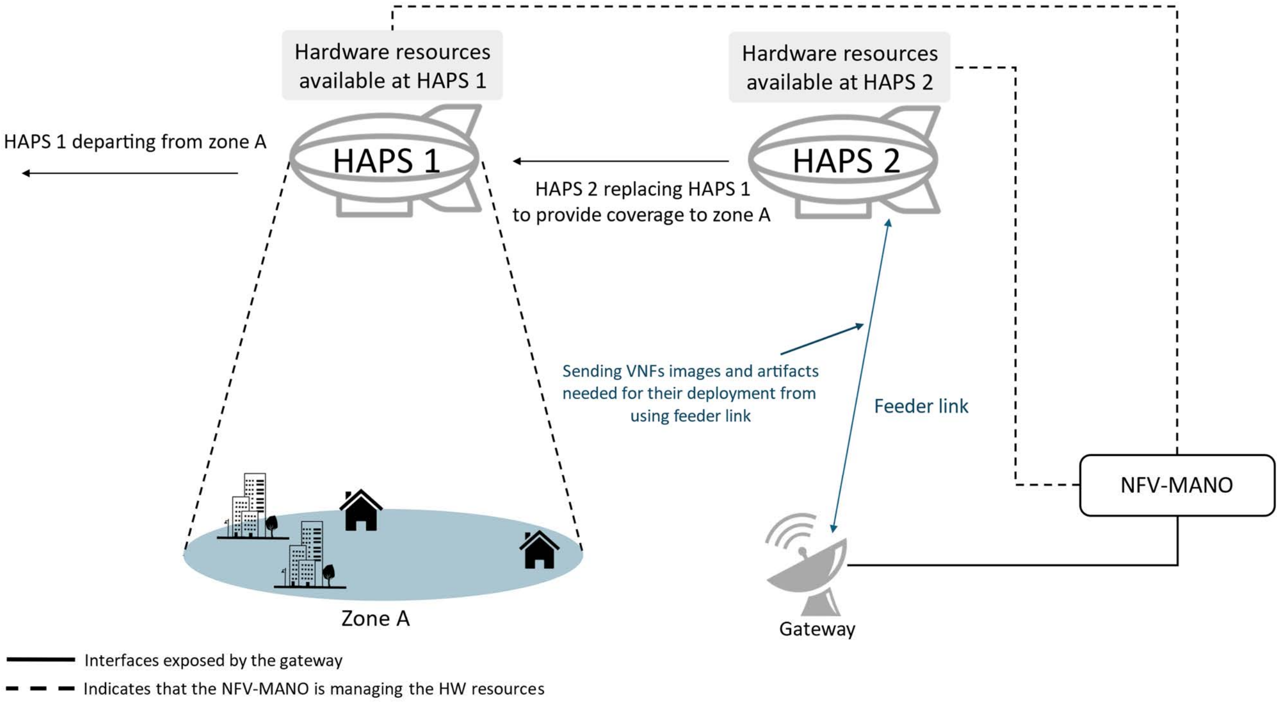

Hardware resources available at HAPS 1
Hardware resources available at HAPS 2
HAPS 1 departing from zone A
HAPS 1
HAPS 2
HAPS 2 replacing HAPS 1 to provide coverage to zone A
Sending VNFs images and artifacts needed for their deployment from using feeder link
Feeder link
NFV-MANO
Zone A
Gateway
Interfaces exposed by the gateway
Indicates that the NFV-MANO is managing the HW resources

Figure 7.2.4.5.1-1: Uploading VNFs images and the necessary artifacts for the deployment of VNFs to the HAPS

- LCM and OAM:

According to solution #7 and solution #8, the PIM can perform the inventory of physical resources provided by the HAPS (by communicating with the ground control station). When the NFV-MANO system receives a request from the OSS (or other consumers) to deploy an NS on the NFVI provided by the HAPS, NFVO together with VNFM perform the NS and VNF deployment. Resource orchestration is performed by NFVO. The feeder link can be used to forward signals related to the deployment operation. After the deployment, the feeder link can also be used for other LCM operations (e.g. terminating, healing, or scaling a VNF among others). Similarly, alarms and OAM related information can be forwarded using the same link, i.e. the NFV-MANO system sends/receives data packets related to LCM and OAM through the link with the gateway and the latter handles the packets transmission to/from HAPS.

7.2.4.5.2 Key issues addressed

The present solution addresses the following key issues described in clause 6:

- Key issue #4.2.

7.2.4.5.3 Gap analysis

Gap #10.1: The role of the HAPS gateway in connectivity establishment between NFV-MANO and HAPS introduces new design of NFVI-PoP network segment.

7.2.4.6 Solution #11: Predicting and handling failures of VNFs and NSs deployed on infrastructure provided by HAPS

7.2.4.6.1 Solution description

The present solution describes how the NFV-MANO system can perform failure predictions and failures root cause analysis for VNFs deployed over physical resources provided by HAPS. To do so the NFV-MANO system can continuously collect data about:

- **The virtualised resources:** ETSI GS NFV-IFA 045 [i.21] specifies a collection of alarms that pertain to virtualised resources, which signal, for instance, that potential service disruption can occur stemming from the hosting server's potential adverse impacts on the virtualised resources. More critical alarms can indicate for example that the virtualised resources cease to function entirely. Furthermore, the specification also details alarms related to CPU, memory, storage, and network, reflecting the degree of impact on the virtualised resources, etc. (refer to ETSI GS NFV-IFA 045 [i.21] clause 7.2). These alarms can be gathered by the NFV-MANO through the gateway when VNFs are deployed on resources supplied by HAPS.

- **The deployed VNF instances:** Clause 7.3 in ETSI GS NFV-IFA 045 [i.21] outlines a range of alarms associated with VNFs, VNFCs, VNFs' virtual links, and both internal and external CPs. For managed object, a distinct set of alarms is established to reflect the different severity levels. These alarms can be gathered by the NFV-MANO through the gateway when VNFs are deployed on resources supplied by HAPS. Additionally, the NFV-MANO system can collect information about the VNF indicators specified by the VNF provider in the VNFD (clause 7.1.11.2 of ETSI GS NFV-IFA 011 [i.17]). The VNF indicators are supplied by the VNF or the EM (refer to clause 6.3 of ETSI GS NFV-IFA 008 [i.22]), they provide some indication on the VNF behaviour.

- **Performance measurements:** Clause 7 of ETSI GS NFV-IFA 027 [i.25] specifies the performance measurements generated by the NFV-MANO that are related to the managed objects. The measurements include CPU, memory, and disk usage, incoming and outgoing packets, energy consumption of a virtualised resource, etc. It also specifies performance measurements to VNF instances and NS instances among others.

The collected data can be used by MDAF which can perform predictions using pre-trained AI/ML models. This process can assess in mitigating the impact of potential failures. MDAF can also perform analysis of the received alarms to identify the root cause of the issues. MDAF concepts are described in ETSI GR NFV-IFA 041 [i.24] and exposed interfaces are specified in ETSI GS NFV-IFA 047 [i.23].

7.2.4.6.2 Key issues addressed

The present solution addresses the following key issues described in clause 6:

- Key issue #4.2.

7.2.4.6.3 Gap analysis

The referenced ETSI NFV specifications in the present solution do not specify:

Gap #11.1: alarms related to new virtualisation technologies that are more likely to be used in the HAPS scenario (e.g. WASM, Unikernels).

Gap #11.7: alarms related to HAPS physical resources.

Gap #11.8: performance measurements related to HAPS operations.

7.3 Evaluation of solutions

7.3.1 Overview

The present clause provides an assessment of the solutions outlined in clause 7.2. If multiple solutions address the same key issue and serve as alternatives for its resolution, the evaluation will reflect this relationship. This solutions' analysis provides a foundation for developing recommendations and for conducting the normative work phase.

7.3.2 Evaluation of solutions for key issues about hybrid Cloud

Table 7.3.2-1 presents an evaluation of the pros and cons of the different solutions associated with hybrid Cloud key issues as introduced in clause 6.3.

Table 7.3.2-1: Pros/cons analysis of solutions for key issues related to hybrid Cloud

Solution	Pros	Cons
Solution #1 Management scopes and interactions between the NFV-MANO and the public Cloud management system for infrastructure provisioning	Existing NFV-MANO functional blocks and functions are leveraged for managing virtualised resources, VNFs, NSs and acquiring information about physical resources provided by the public Cloud. Standard interfaces and reference points are reused to interact with the resource management of the Cloud service provider.	Additional overhead is expected due to the NFV-MANO system interacting with the management system of the Cloud provider, the latter is already optimized to perform specific operations (e.g. Cluster management). The management capabilities for other application virtualisation technologies (e.g. microVMs, Wasm, etc.) as well as FaaS, need to be defined and modelled in a standardized way.
Solution #2 Management scopes and interactions between the NFV-MANO and public Cloud management system for infrastructure provisioning and NFs management.	Existing NFV-MANO functional blocks and functions are leveraged for managing virtualised resources and acquiring information about physical resources provided by the public Cloud.	The management capabilities of FaaS computing model need to be defined and modelled in a standardized way to avoid vendor lock-ins. Relying on PaaS service supplied by the Cloud service provider can lead to potential Cloud vendor lock-in issues. The operator lacks full control of the operations related to VNF LCM (they rely on the management system of the Cloud provider to perform troubleshooting in case of failures). It could be that it is not possible to use standardized FM/PM.
Solution #3 Management scopes and interactions between the NFV-MANO and public Cloud management system for infrastructure provisioning and NFs and NSs management	Existing NFV-MANO functional blocks and functions are leveraged for managing virtualised resources and acquiring information about physical resources provided by the public Cloud. Optimized procedures for resource management and VNF and NS LCM.	The operator lacks full control of the operations related to VNF and NS LCM (they rely on the management system of the Cloud provider to perform troubleshooting in case of failures). If NS LCM operations are not supported over a standardized interface, there is a potential vendor lock-in. It could be that it is not possible to use standardized FM/PM.

Solution	Pros	Cons
Solution #4 Multi-site connectivity service between private Cloud sites and public cloud sites provided by WIM	The WIM function is leveraged for managing the virtual links between private Cloud and public Cloud. Standard interfaces, reference points, and information elements exposed by the WIM are reused to manage connectivity with the public Cloud. Standard-defined transport network management for multi-site connectivity is compatible with various modes of operation and administration of NFVI-PoP network gateway (e.g. customer edge network device).	The management of connectivity of the public Cloud to the WAN network is using proprietary solutions and the concept of connection points needs to be mapped to the public Cloud provider constructs.
Solution #5 VNF placement at the public Cloud	Reuse of the metadata about constraints and requirements related to VNFs placement that are defined in the VNFD. Presents the operator with the possibility of choosing from the available locations suggested by the management system of the public Cloud.	There is a need to specify the granularity of the location information for the deployments at the public Cloud side, and how the public Cloud makes such information available to the operator.
Solution #6 VNF placement in the public Cloud with prior knowledge of available locations	Reuse of the metadata about constraints and requirements related to VNFs placement that are defined in the VNFD.	There is a need to specify the granularity of the location information for the deployment at the public Cloud side, and how the public Cloud makes such information available to the operator.

7.3.3 Evaluation of solutions for key issues about HAPS

Table 7.3.3-1 presents an evaluation of the pros and cons of the different solutions associated with HAPS key issues as introduced in clause 6.4.1.

Table 7.3.3-1: Pros/cons analysis of solutions for key issues related to hybrid Cloud

Solution	Pros	Cons
Solution #7 NFV-MANO aware of HAPS mobility, power consumption, and hardware resources	Enables the operator to obtain information about the availability of the infrastructure provided by HAPS (timeframe and location).	The connectivity and the interfaces between the NFV-MANO and the terrestrial component managing HAPS need to be defined and modelled. The information element about HAPS mobility, time availability, infrastructure resources provided by HAPS, etc. that are exchanged between the NFV-MANO and the terrestrial component managing HAPS need to be defined. No mapping between the requirements of the VNFs/NSs to the HAPS availability (e.g. placement of VNF/NS and use of HAPS resources can be sub-optimal, etc.).
Solution #8 Mapping VNFs requirements to HAPS availability	Enables the operator to obtain information about the availability of the infrastructure provided by HAPS (timeframe and location). Provides a mapping between the requirements of VNFs in terms of hardware resources needed and time interval of instances deployment, and the HAPS availability.	The connectivity and the interfaces between the NFV-MANO and the terrestrial component managing HAPS need to be defined and modelled. The information element about HAPS mobility, time availability, infrastructure resources provided by HAPS, etc. that are exchanged between the NFV-MANO and the terrestrial component managing HAPS need to be defined.
Solution #9 Suitable virtualisation technologies for resource- and power-constrained environment such as HAPS	Different options can be considered based on architectural design aspects of each virtualisation technology and the impact in resource and energy consumption.	The alarms and performance measurements related to new virtualisation technologies that are likely to be used in the HAPS need to be defined.
Solution #10 LCM and OAM operations related to VNFs deployed over NFVI provided by HAPS	Existing NFV-MANO functional blocks and functions are leveraged for virtualised resources, VNFs, NSs and acquiring information about physical resources provided by the HAPS.	The connectivity and the interfaces between the NFV-MANO and the terrestrial component managing HAPS need to be defined and modelled. The connectivity and the interfaces between the NFV-MANO and the gateway in charge of forwarding the LCM/OAM information via the feeder link need to be defined and modelled.
Solution #11 Predicting and handling failures of VNFs and NSs deployed on infrastructure provided by HAPS	Existing NFV-MANO alarms and performance measurements are reused. Existing NFV-MANO functional blocks and functions, such as MDAF, are reused.	N/A.

8 Recommendations

8.1 Overview

The recommendations are structured and elaborated as follows:

- aspects related to the architecture and framework (refer to clause 8.2);
- functional aspects (refer to clause 8.3); and

- interfaces and associated information/data model (refer to clause 8.4).

NOTE: The present document only includes solutions and recommendations related to hybrid Cloud and HAPS.

8.2 Recommendations related to the NFV architectural framework

The present clause documents recommendations intended to enhance the NFV architectural framework by identifying potential new functions or functional blocks, and interactions among these functional blocks and functions.

Tables 8.2-1 provides recommendations related to the NFV architectural framework.

Table 8.2-1: NFV architectural framework recommendations

Identifier	Recommendation description	Comments and/or traceability
haps.arch.001	It is recommended to specify a requirement for the NFV architectural framework consider interactions with external management systems for the purpose of resource and application management.	Refer to gap #10.1. This can be specified in a generic form (not specific to NTN), e.g. by modelling some form of "gateway to an external system".

8.3 Recommendations related to functional aspects

The present clause provides recommendations that focus on functional aspects of the functional blocks within the NFV architectural framework, identifying new or extended functionalities of the NFV architectural framework functional blocks and functions.

Tables 8.3-1 provides recommendations related to functional aspects.

Table 8.3-1: Functional aspects recommendations

Identifier	Recommendation description	Comments and/or traceability
haps.func.001	It is recommended to specify a requirement for an NFV-MANO management entity to support the collection of HAPS data related to availability of their infrastructure (including spatial and temporal availability) and map it to the requirements of the VNFs/NSs.	Refer to gap #8.1

8.4 Recommendations related to interfaces and information model

The present clause provides recommendations focusing on interfaces and associated information.

Tables 8.4-1 provides the recommendations related to interfaces and associated information for hybrid Cloud as well as HAPS.

Table 8.4-1: Recommendations related to interfaces and information model

Identifier	Recommendation description	Comments and/or traceability
hybridcloud.if.001	It is recommended to specify a requirement for the PaaS service management interface(s) produced by the NFV-MANO to support requesting PaaS services provided by the public Cloud.	Refer to gap #2.2
hybridcloud.if.002	It is recommended to specify a requirement to query information related to potential location for VNF deployments at the public Cloud and to specify the granularity of the location information.	Refer to gaps #5.1 and #6.1
hybridcloud.if.003	It is recommended to specify a requirement for the interface to receive notifications from the public Cloud management system about the available locations.	Refer to gap #6.1

Identifier	Recommendation description	Comments and/or traceability
haps.if.001	It is recommended to specify a requirement for the interface to enable the exchange of information between the NFV-MANO and the terrestrial component managing HAPS.	Refer to gaps #7.1 and #7.2
haps.if.002	It is recommended to specify a requirement for the NFV-MANO to support producing alarms related to new virtualisation technologies (see note).	Refer to gap #11.1
haps.if.003	It is recommended to specify a requirement for the NFV-MANO to specify generic alarms about physical resources.	Refer to gap #11.2
NOTE: The virtualisation technologies referred to in haps.if.002 are the ones introduced in ETSI GR NFV-EVE 025 [i.18].		

9 Conclusion

The present document investigates the NFVI evolution trends in respect to new locations, new types and new sources of NFV infrastructure resources. A couple of use cases and key issues associated to certain use cases are described and analysed in this regard. Potential solutions for addressing the identified key issues (mainly for hybrid Cloud and HAPS use cases in the present document) are proposed, and finally recommendations for potential enhancements to the NFV architectural framework are summarized. Future stage 2 specification work is expected to consider the recommendations and potential enhancements in the subsequent normative work phase.

Annex A: Change history

Date	Version	Information about changes
September 2023	0.0.1	Implementation of the skeleton contribution approved at EVE#260: - NFVEVE(23)000175r1: EVE023 Skeleton
September 2023	0.1.0	Implementation of contributions agreed at EVE#260: - NFVEVE(23)000176: EVE023 Clause 1 Adding scope - NFVEVE(23)000184r1: EVE023 Clause 4.x New kinds of infrastructure resources: DPU Rapporteur actions: - Clause 4.3.1: spelled out the ICT abbreviation. Since "T" is from technology, deleted the "technologies". - Clause 3.3: added abbreviations coming from contribution 184r1.
December 2023	0.2.0	Implementation of contributions approved at EVE#270: - NFVEVE(23)000243: FEAT36 EVE023 Clause 4.1 Adding NFVI introduction - NFVEVE(23)000244: FEAT36 EVE023 Clause 4.2 Adding dimensions for new NFVI - NFVEVE(23)000240: EVE023 clause 4.2.2 and 4.2.3 on resources including satellite - NFVEVE(23)000245r1: EVE023 clause 4.3.2 New kinds of infrastructure resources Satellite Rapporteur edits: - Added missing abbreviations of LEO, MEO and GEO. - Performed additional editorial changes in table 4.3.2-1.
March 2024	0.3.0	Implementation of approved contributions from EVE#271 until EVE#278. - NFVEVE(24)000006r1: FEAT36 EVE023 clause 4.3.x New kinds of infrastructure resources AI Chips - NFVEVE(24)000018r2: FEAT36 EVE023 Clause 4.3 Adding concept of HAPS - NFVEVE(24)000019: FEAT36 EVE023 Clause 4.3 Adding concept vehicular infrastructure - NFVEVE(24)000025r1: FEAT36 EVE023 Clause 4.3 Adding programmable meta-surfaces - NFVEVE(24)000026r1: FEAT36 EVE023 Clause 4.3 Adding Smart-NICs - NFVEVE(24)000033r1: FEAT36 EVE023 Clause 4.3 Adding hybrid Cloud Rapporteur edits: - Clause 3.3: added missing abbreviations based on the content of implemented contributions.
April 2024	0.4.0	Implementation of approved contribution from EVE#280/#281: - NFVEVE(24)000038r1: FEAT36 EVE023 Clause 5.1 Use case about hybrid Cloud - NFVEVE(24)000052r2: FEAT36 EVE023 Clause 5.1 Use cases about acceleration resources Additional rapporteur changes: - Table 5.3.1.6-1: corrected the step numbers, last one changed to #4. - Clause 5.3.1: change the use case number form #1 to #2, to avoid colliding use case number present in clause 5.2.1. - Clause 5.3: updated the title to follow format as clause 5.2, i.e. "use cases about XYZ". - Corrected several punctuation typos in table references.
May 2024	0.5.0	Implementation of approved contributions from EVE#283 and: - NFVEVE(24)000057r1: FEAT36 EVE023 Clause 5.1 Use cases about vehicular infrastructure - NFVEVE(24)000065: FEAT36 EVE023 Clause 5.2 Use case about building the NFVI of the hybrid Cloud - NFVEVE(24)000071r1: FEAT36 EVE023 Clause 5.4 Use case about HAPS Additional rapporteur changes: - corrected the numbering of several clauses when implementing 065. - changed the title of clause 5.4 to make it more generic and align to the NFVI dimensions (clause 4.2) terminology; proposed: "Use cases about location and mobility of infrastructure"

Date	Version	Information about changes
September 2024	0.6.0	Implementation of approved contributions from EVE#289 until EVE#298: - NFVEVE(24)289002r1_HAPS_related_key_issues - NFVEVE(24)000090r1 FEAT36 EVE023 Clause 5.x Use case about programmable meta-surfaces - NFVEVE(24)000122_FEAT36_EVE023_Clause_5_x_Use_case_about_RIS - NFVEVE(24)000096r1_FEAT36_EVE023_Clause_6_4_vehicular_infrastructure_key_issues - NFVEVE(24)000097_FEAT36_EVE023_Clause_6_3_Key_issues_related_to_hybrid_Cloud - NFVEVE(24)000101r1_FEAT36_EVE023_Clause_6_2_Key_issues_related_to_acceleration_ - NFVEVE(24)000121_FEAT36_EVE023_Clause_6_2_Key_issues_related_to_meta-surfaces Additional rapporteur changes: - Changed the numbering of the new reference. - Corrected numbering of use cases and tables numbering therein. - Removed template of use case. - Updated PMS to RIS according to Change #1 in contribution 121
November 2024	0.7.0	Implementation of approved contributions from EVE#299 until EVE#306: - NFVEVE(24)000138r2_FEAT36_EVE023_Clause_7_solution_1_hybrid_Cloud - NFVEVE(24)000141r1_FEAT36_EVE023_Clause_7_Solution_2_related_hybrid_Cloud - NFVEVE(24)000155r1_FEAT36_EVE023_Clause_7_Solution_3_related_hybrid_Cloud Additional rapporteur changes: - Changed the numbering of the new reference. - Corrected numbering of some added clauses and number of use case in clause 7.2.1.1. - Removed template of solution clause. - Made editorial changes to align references and to correct titles' font size.
February 2025	0.8.0	Implementation of approved contributions from EVE#307 until EVE#317 - NFVEVE(24)000190r1_EVE023_Clause_7_Solution_related_to_connectivity_for_hybrid_Cloud - NFVEVE(24)000206_FEAT36_EVE023_Clause_6_3_1_updating_KI_of_VNF_placement_in_hybrid_Cloud - NFVEVE(24)000207_FEAT36_EVE023_Clause_7_Solution_5_about_VNF_placement - NFVEVE(25)000014r1_FEAT36_EVE023_Clause_7_VNF_placement_prior_knowledge_about_locations - NFVEVE(25)000011_FEAT36_EVE023_updating_the_table_of_solutions - NFVEVE(25)000010r1_FEAT36_EVE023_Clause_7_3_2_Evaluation_of_solutions_related_to_hybrid_Cloud - NFVEVE(25)000002r1_FEAT36_EVE023_Solution_related_to_HAPS_mobility - Additional rapporteur changes: - Corrected numbering of some added clauses. - Removed some ENs that are not anymore needed. - Made editorial changes. - Corrected the title of clause 7.2.3

Date	Version	Information about changes
March 2025	0.9.0	Implementation of approved contributions from EVE#317 until EVE#320 - NFVEVE(25)000041r2_NFV_EVE023_5_x_Use_case_on_creating_CIS_cluster_on_bare-meta - NFVEVE(25)000036r2_FEAT36_EVE023_5_3_x_Use_case_on_offloading_Hypervisor_compon - NFVEVE(24)000208r6_FEAT36_EVE023_5_3_x_Use_case_on_creating_bare-metal_server_pool - NFVEVE(25)000044r2_FEAT36_EVE023_Mapping_VNFs__requirements_to_HAPS_availability - NFVEVE(25)000042r1_FEAT36_EVE023_Suitable_virtualisation_technologies_for_HAPS - NFVEVE(25)000006r2_FEAT36_EVE023_Clause_7_hybrid_Cloud_adding_interaction_with_PaaS - NFVEVE(25)000045r1_FEAT36_EVE023_Clause_7_HAPS_solutions_VNFs_LCM_and_OAM - NFVEVE(25)000046r1_FEAT36_EVE023_Clause_7_HAPS_solutions_prediction_and_handling_of_failures Additional rapporteur changes: - Changed the numbering of the new references - Fixed the numbering of the introduced clauses - Added abbreviation - Fixed style of tables - Fixed the numbering of the key issues - Fixed clause, figure, and solutions numbering in 7.2.2 - Added reference of IFA045 in Solution #11
May 2025	0.10.0	Implementation of approved contributions from EVE#320 until EVE#327 - NFVEVE(25)000066_FEAT36_EVE023_correcting_gaps_numbering - NFVEVE(25)000064r2_FEAT36_EVE023_5_3_x_Use_case_on_instantiating_container-base - NFVEVE(25)000052_FEAT36_EVE023_Clause_7_updating_table_of_solutions - NFVEVE(25)000053r1_FEAT36_EVE023_Clause_7_updating_evaluation_of_solutions - NFVEVE(25)000057r3_FEAT36_EVE023_recommendations_clause_8 Additional rapporteur changes: - Fixed the numbering of the use cases
July 2025	0.11.0	Implementation of approved contributions from EVE#330 until EVE#335: - NFVEVE(25)000083r1_FEAT36_EVE023_review_hybrid_Cloud_use_case_improvements - NFVEVE(25)000082_FEAT36_EVE023_review_clause_1-3_clean-up - NFVEVE(25)000110r1_FEAT36_EVE023_conclusions - NFVEVE(25)000106r5_EVE023_stable_draft_review_comments_for_ed611 Additional rapporteur changes: - Fixed typos - Fixed titles of solutions - Fixed numbering of use case tables - Deleted empty clauses - Removed all the editor's note
July 2025	0.12.0	Editorial updates in clause 8.4

History

V6.1.1	September 2025	Publication