ETSI GS NFV-EVE 007 V3.1.1 (2017-03)

Network Functions Virtualisation (NFV) Release 3;
NFV Evolution and Ecosystem;
Hardware Interoperability Requirements Specification

Disclaimer

Reference

DGS/NFV-EVE007

Keywords

interoperability, NFV, NFVI, requirements

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 develops a set of normative interoperability requirements for the Network Function Virtualisation (NFV) hardware ecosystem and telecommunications physical environment to support NFV deployment. It builds on the work originated in ETSI GS NFV 003 [i.3].

The present document focusses on the development of requirements to enable interoperability of equipment in the telecommunications environment to support NFV deployment. The following areas are examined:

- Operations
- Environmental
- Mechanical
- Cabling
- Maintenance.
- Security

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

[1] ETSI ES 205 200-2-1 (V1.2.1) (03-2014): "Access, Terminals, Transmission and Multiplexing (ATTM); Energy management; Global KPIs; Operational infrastructures; Part 2: Specific requirements; Sub-part 1: Data centres".

[2] IEC 60297-3-105:2008: "Mechanical structures for electronic equipment - Dimensions of mechanical structures of the 482,6 mm (19 in) series - Part 3-105: Dimensions and design aspects for 1U high chassis".

[3] ETSI ETS 300 119 (all parts): "Equipment Engineering (EE); European telecommunication standard for equipment practice".

[4] ETSI GS NFV 004 (V1.1.1) (10-2013): "Network Functions Virtualisation (NFV); Virtualisation Requirements".

[5] IEEE Std 1588™-2008: "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[6] IEEE Std 802.1AS™-2011: "Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks".

[7] NEBS™ GR-63: "NEBS™ Requirements: Physical Protection".

[8] ETSI GS NFV-SEC 009 (V1.1.1): "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[9] ETSI GS NFV-SEC 012 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[10] DMTF Specification DSP0266 V1.0.0 (2015): "Scalable Platform Management API Specification".

[11] DMTF Specification DSP8010 V1.0.0 (2015): "Scalable Platforms Management API Schema".

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 are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS NFV 001 (V1.1.1) (10-2013): "Network Functions Virtualisation (NFV); Use Cases".

[i.2] ETSI GS NFV 002 (V1.2.1) (12-2014): "Network Functions Virtualisation (NFV); Architectural Framework".

[i.3] ETSI GS NFV 003 (V1.2.1) (12-2014): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.5] ETSI GS NFV-EVE 003 (V1.1.1): "Network Functions Virtualisation (NFV); Ecosystem; Report on NFVI Node Physical Architecture Guidelines for Multi-Vendor Environment".

[i.6] ETSI EN 300 386: "Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements; Harmonised Standard covering the essential requirements of the Directive 2014/30/EU".

[i.7] IEC 60950-1: "Information technology requirement - Safety - Part 1: General requirements".

[i.8] ETSI EN 300 019-1-3: "Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-3: Classification of environmental conditions; Stationary use at weatherprotected locations".

[i.9] ASHRAE 3rd edition, 2012: "Thermal Guidelines for Data Processing Environment".

[i.10] ETSI GS NFV-REL 003 (V1.1.2) (07-2016): "Network Functions Virtualisation (NFV); Reliability; Report on Models and Features for End-to-End Reliability".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

delta: three phase power connection where phases are connected like a triangle

wye: three phase power connection where phases are connected like a star with all phases connected at a central "Neutral" point

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.3] and the following apply:

ASHRAE	American Society of Heating, Refrigerating, and Air-Conditioning Engineers
BBU	Battery Backup Unit
BMC	Basement Management Controller
CDC	Customer Data Centre
DC	Direct Current
FRU	Field Replaceable Unit
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HTTP	HyperText Transfer Protocol
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
JSON	JavaScript Object Notation
kW	kilo Watts
MANO	MANagement and Orchestration
MiFID	Markets in Financial Instruments Directive
NIC	Network Interface Controller
NID	Network Interface Device
NFV	Network Function Virtualisation
NFVI	Network Function Virtualisation Infrastructure
ODC	Operator Data Centre
OTT	Over The Top
PoP	Point of Presence
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
VNF	Virtual Network Function
VNFC	Virtual Network Function Component

4 NFV Hardware Ecosystem

4.1 Introduction

The present document develops a set of normative interoperability requirements for the NFV hardware ecosystem and telecommunications physical environment to support NFV deployment. The intent is to develop a reference that enables compatibility between hardware equipment provided by different hardware vendors and suppliers. The environment in which NFV hardware will be deployed is taken into consideration for developing this reference. Telecommunications Service Providers currently have the following hardware office environments:

- Central Office
- Access Node
- Transport Node
- Data Centre
- Hybrids (e.g. Central Office partitioned into or converted to a Data Centre)

It is expected that the bulk of the NFV environment will be deployed in Data Centres; this evolution supports the move towards a Cloud based environment. The focus of this document is primarily on Data Centre environments; however it also applies to the setup of an NFV Point of Presence (POP) in any of the above environments.

4.2 Data Centres

A Data Centre [1] is defined as follows:

"structure, or group of structures, dedicated to the centralized accommodation, interconnection and operation of information technology and network telecommunications equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control together with the necessary levels of resilience and security required to provide the desired service availability."

According to ETSI ES 205 200-2-1 [1], a data centre is divided into Operator Data Centre (ODC) and Customer Data Centre (CDC). An ODC is a facility embedded within the core network. The facility, therefore, is considered as a service provider's asset. A CDC is, on the other hand, a facility that is not directly connected to the core network. The facility is reachable with access networks. It is considered as a large branch office, a corporate headquarter, and a data centre operated by an Over-The-Top (OTT) provider. A Data Centre is also considered a place where Network Function Virtualisation Infrastructure (NFVI) nodes would be installed [i.1] and [i.2].

Figure 1 shows how a central office, Operator Data Centre, and Customer Data Centre are mapped onto the use case #2 [i.1].

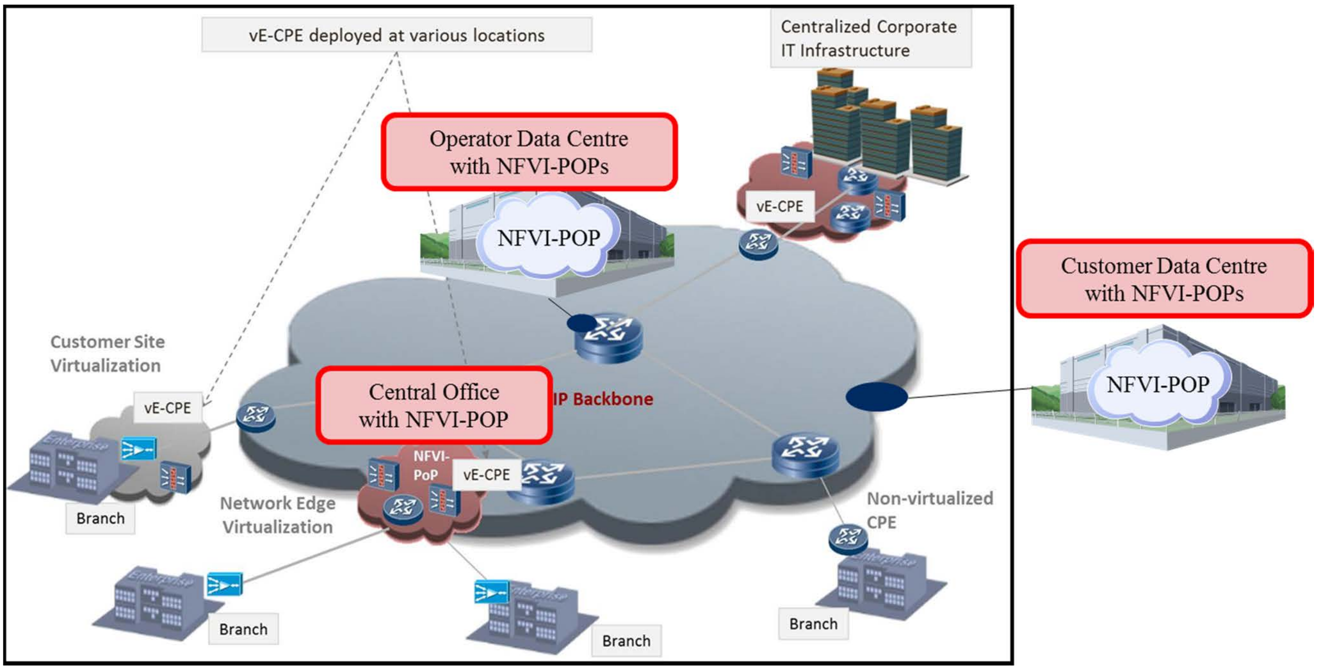

Figure 1: NFVI Node Profiles

4.3 Hardware Interoperability Environment

The main features for the NFV hardware ecosystem are depicted as follows.

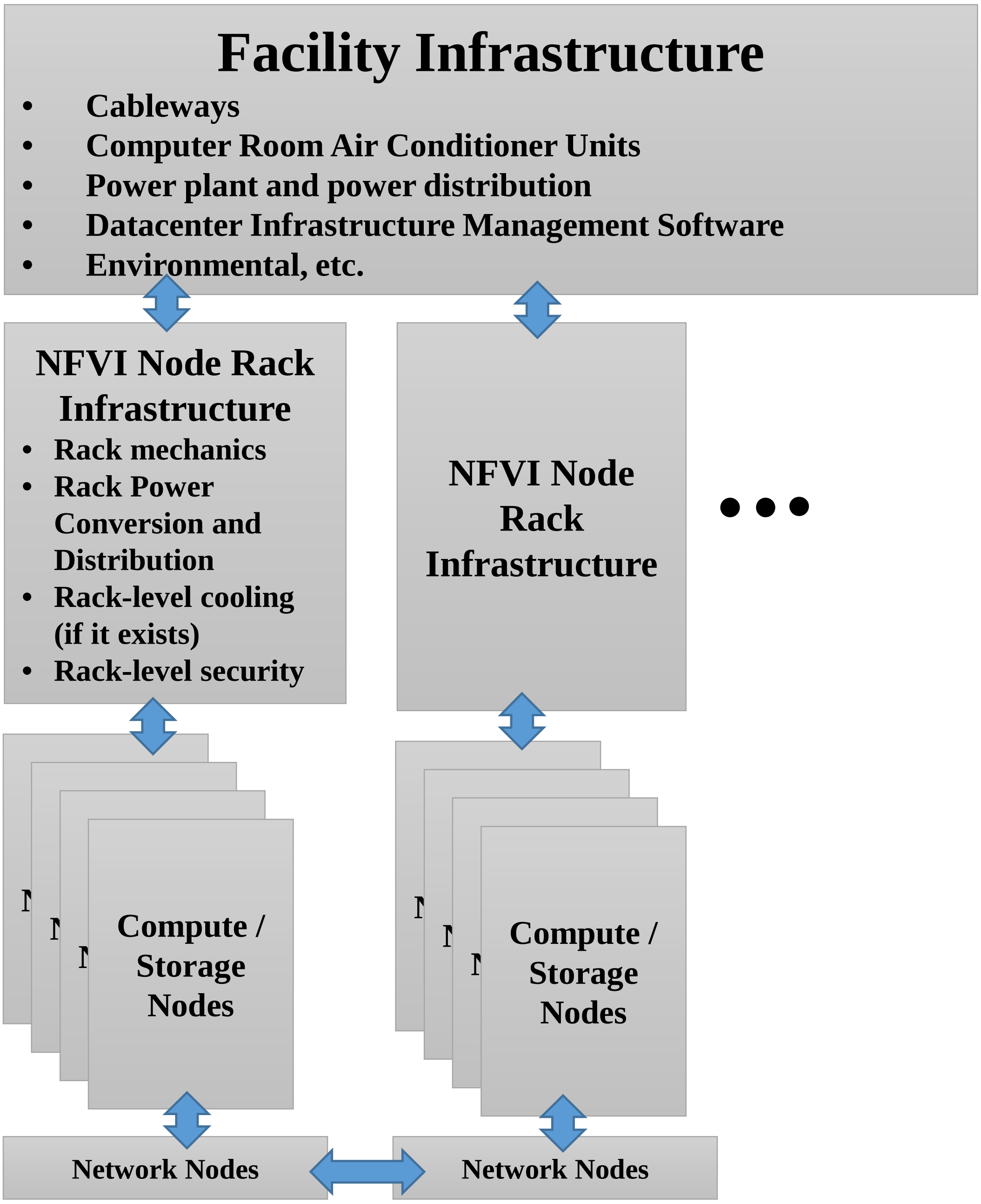

Figure 2: Facility Infrastructure Overview

The main components of this ecosystem view are described as follows:

- Facility Infrastructure - the infrastructure (hardware/software/environmental/mechanical provided by the POP site. All NFVI equipment within the POP is subject to interfacing within the constraints of the facility infrastructure. Some elements of the facility infrastructure may include cableways, computer room air conditioning units, power plant and power distribution, infrastructure management software and environmental conditions.

- NFVI Node Rack Infrastructure - the rack, and associated rack infrastructure that provides power, cooling, physical security and rack-level hardware management to the compute, storage and networking nodes. Typical elements for NFVI node rack infrastructure may include rack mechanics, power conversion and power distribution, cooling, and rack-level physical security measures (door locks, etc.). Multiple rack infrastructures may exist within the NVFI POP - one for each equipment rack deployed.

- Compute/Storage nodes - the NFV nodes that provide compute and storage functions to the NFVI. Multiple compute or storage nodes may exist per rack. It is assumed that these nodes draw power from the rack infrastructure and exist within the environmental and mechanical constraints of the rack infrastructure.

- Network Nodes - the NFV nodes that provide networking function to the NFVI. Multiple networking nodes may exist per rack. Like compute and storage nodes, these nodes also draw power and reside within the environmental and mechanical constraints imposed by the rack. In addition, these nodes provide network connectivity between network/compute/storage nodes both within and external to the rack.

The dashed line in figure 3 shows a proposed boundary for the scope of this document. The areas of interoperability that cross the boundary are considered for specification. Additionally, functions within the boundary may also need to be specified in order to provide interoperability. The four main areas of interoperability (numbered in figure 3) are:

1) Facility to Rack: This defines the interaction between the data centre facility and each individual NFVI rack. Expected components of this interface include: facility power feeds, facility climate, facility size and weight restrictions, radiated emissions and susceptibility, acoustics, physical security, and facility infrastructure management.

2) Rack to Compute/Storage Node: This defines the interaction between the compute and storage nodes with the rack infrastructure provided by the NFVI rack. Expected elements of this interface include: Rack power, rack-level forced air cooling (if it exists), mechanical dimensions for rack "slots" and weight per slot.

3) Compute/Storage Node to Network Node: this defines the communications path between the various nodes within the NFVI rack. Expected elements of this interface include physical layer protocol, bandwidth, connector, and cabling types.

4) Rack to Rack network: this defines the communication path between network nodes within one rack to network nodes within another rack within the NFVI POP. Expected elements of this interface will include physical layer protocol, bandwidth, connector, and cabling types.

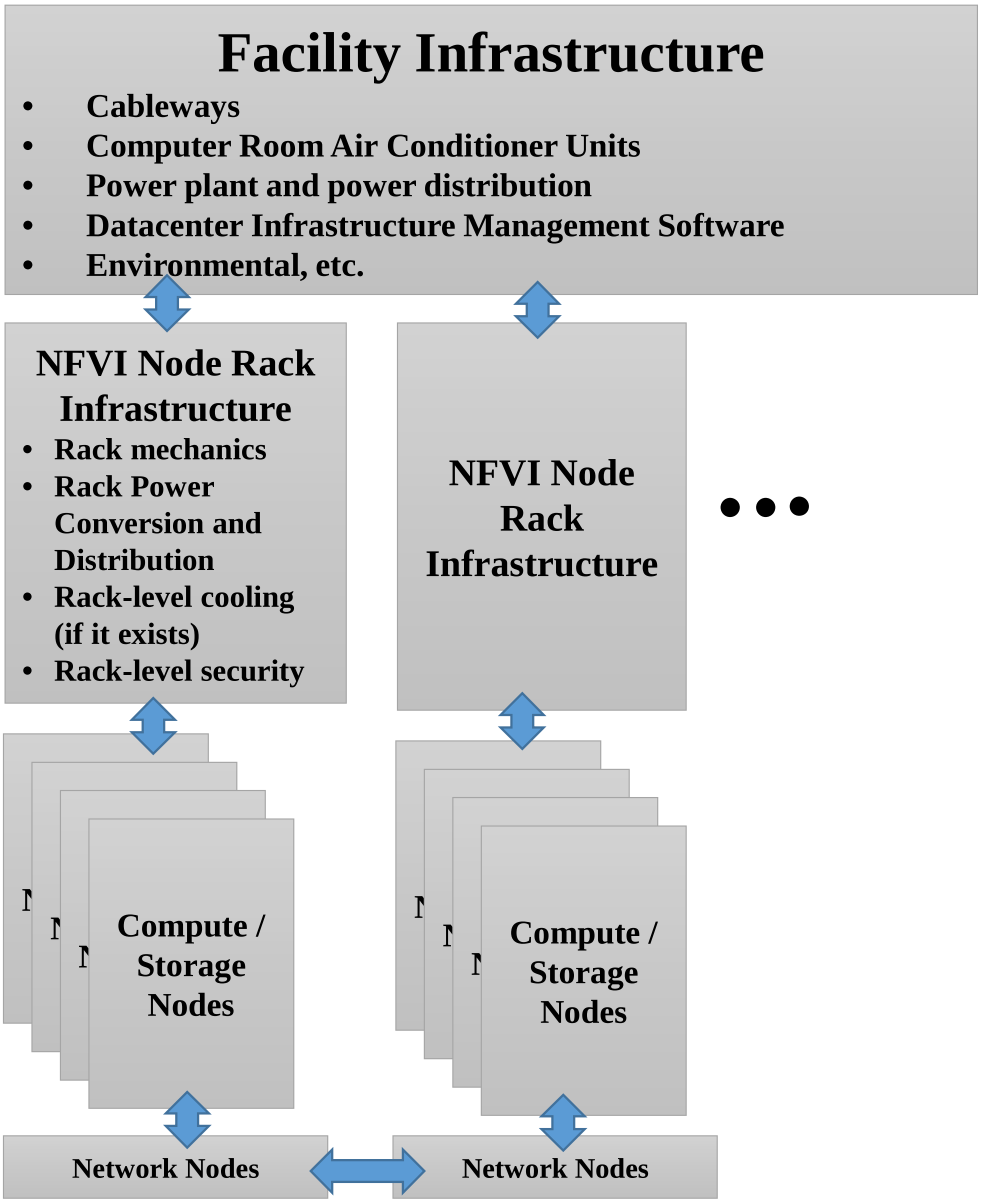

Figure 3: Scope of the present document

Based on the above discussion, the areas of interoperability for which requirements are developed are summarized in table 1. This table also lists applicable factors that need to be considered for the development of interoperability requirements.

Table 1: Areas of Interoperability and Applicable Factors

Areas of Interoperability	Applicable Factors
Racks/Frames	• Physical Dimensions • Deployment Considerations • Safety Considerations
Processors and Storage	
Power	• Distribution and Conversion • Subsystem Architectures • Local Energy Storage
Interconnections	• Compute and Infrastructure Domain Interconnections
Cooling	• General Cooling • Rack Level Cooling • Compute/Storage/Network Node Level Cooling
Hardware Platform Management	
Hardware Security Measures	
Radiated Emissions and Electromagnetic Compliance	
Climatic and Acoustic Considerations	
Timing and Synchronization	
Reliability	
Lawful Intercept	

5 Hardware Interoperability Requirements

5.1 Racks/Frames

5.1.1 Dimension Requirements

Racks/frames can be deployed at different sites (e.g. central office, data centre, etc.) and in different regions. The design of the racks/frames varies based on the adopted specifications. For easier interoperability with legacy equipment and reducing reconstruction needs for the deployment sites, the racks/frames used for NFVI Node deployment shall comply with the relevant regional and global standards.

Requirements:

REQ 5.1.1.1: The dimensions of racks/frames shall comply with one of the following NFVI Node profiles:

- Profile 1: IEC 60297 specifications [2]
- Profile 2: ETSI ETS 300 119 specifications [3]

NOTE 1: Profile 1 is recommended for deployment in legacy central office or data centre environment. Profile 2 is recommended for deployment in legacy access & transport scenarios.

NOTE 2: Dimension requirement samples of the referenced specifications are listed in table 2.

Table 2: Dimension requirement samples of the referenced specifications

Site Type	Height	Width	Depth	Ref standards
central office	2 200 mm	600 mm	800 mm	IEC 60297 [2]
data centre	2 000 mm	600 mm	1 200 mm	IEC 60297 [2]
access & transport nodes	2 200 mm	600 mm	300 mm or 600 mm	ETSI ETS 300 119 [3]

Note that today due to cabling, specifically for optical cables, there might be racks with more width advisable due to the number and radius of cables per rack. That depends a bit on the type NFV node.

5.1.2 Radiated emission requirements

Requirements:

REQ 5.1.2.1: The racks/frames shall comply with the regional radiated emissions specifications for the types of equipment hosted.

EXAMPLE: ETSI EN 300 386 [i.6] is an EMC requirement specification for racks/frames in Europe.

5.1.3 Deployment requirements

The racks/frames are used to host and facilitate the NFVI Node equipment, which can be categorized into compute, storage, network and gateway nodes, to support execution of VNFs.

Requirements:

REQ 5.1.3.1: The racks/frames shall support a variety of NFVI Node scales.

REQ 5.1.3.2: The racks/frames shall support a mapping of an arbitrary number of NFVI Nodes onto one or more physical racks of equipment (e.g. N:M mapping).

REQ 5.1.3.3: The racks/frames shall support geographical addressing in order to facilitate ease of maintenance and possible optimizations based on locality of compute/storage/networking resources.

5.1.4 Safety requirements

Requirements:

REQ 5.1.4.1: The racks/frames shall comply with regional safety requirements for the types of equipment hosted.

EXAMPLE: IEC 60950-1 [i.7] is an international safety specification defined by the International Electrotechnical Commission (IEC).

5.2 Processors and Storage

Processors and storage are essential components of NFVI nodes. They both play important roles in data processing and have a big influence on the performance of the NFVI node. To enjoy the benefits of the technology development, the NFVI nodes are expected to support latest processors and storage products for service expansion or upgrade.

The key criteria of processors are performance and power consumption. The performance of the processors is typically measured by core numbers, clock rate, and instructions per clock. And with some specific capabilities, the processors can further improve their performance. ETSI GS NFV-EVE 003 [i.5] has studied some of these processor capabilities and lists some recommendations. Besides performance, power consumption is also an essential criterion for processors. While the current Central Processing Units (CPUs) are capable of handling most of the work, under some cases, they are less power-efficient compared with the Graphic Processing Units (GPUs) or specific designed accelerators. It is expected that different forms of processors would be utilized for different types of services to improve power efficiency.

The key criteria of storage are performance (I/O throughput), capacity, and scalability. Performance and capacity are the key factors to be considered when building the storage system. Some capabilities can improve the performance of the storage system; for example, ETSI GS NFV-EVE 003 [i.5] has studied the advantages offered by registers, cache and memory. As the data rapidly grows, the storage system can be expanded. Storage systems can be scaled and/or maintained as appropriate.

5.3 Power

5.3.1 Introduction

This clause specifies requirements for the rack power architecture of the NFVI node. Two power architectures are specified. The first architecture consists of a rack-level power entry module which distributes facility power to each of the Compute/Storage/Network nodes within the NFVI equipment rack where individual power supplies convert the power to appropriate DC formats to be used by the equipment. This architecture is consistent with traditional telecommunications and enterprise Data Centre deployments. The second architecture incorporates a rack-level power shelf for the primary conversion stage. This architecture might provide some benefits in system cost due to resource pooling and represents an emerging architecture used by Hyperscale cloud providers [i.8]. These two architectures can be seen in figure 4.

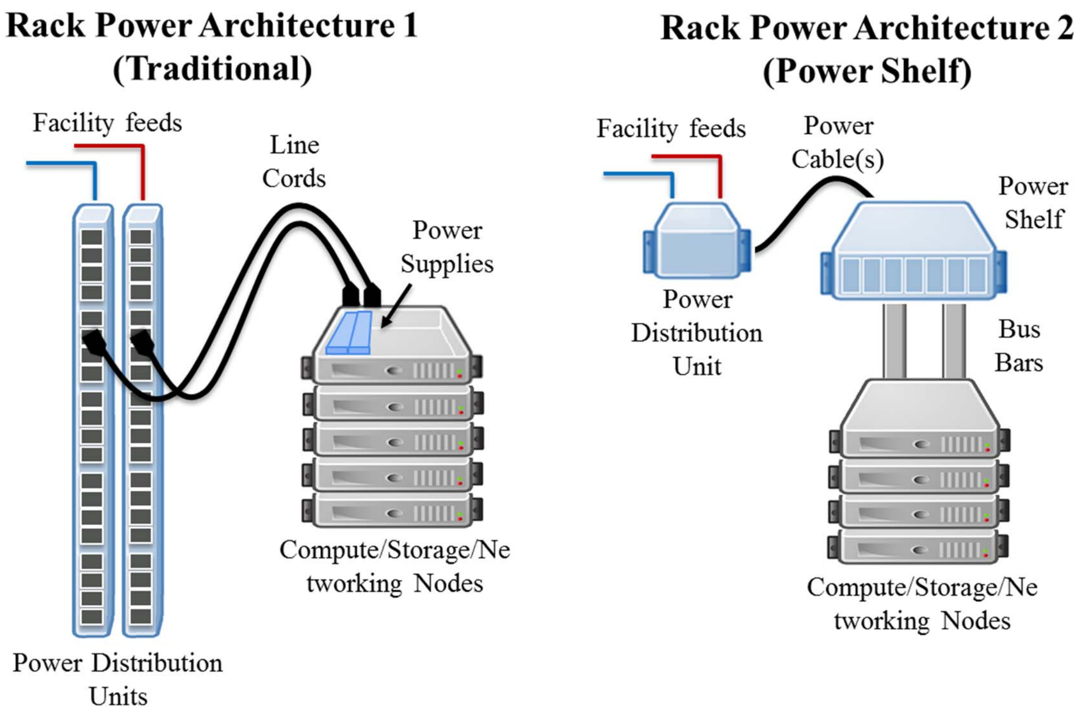

Figure 4: Two NFVI Node Rack-Level Power Architectures

5.3.2 General Power Requirements

5.3.2.1 Introduction

The requirements in this clause apply to all implementations of NFVI node rack power subsystems, regardless of the particular rack power architecture.

5.3.2.2 Safety

REQ 5.3.2.2.1: The rack power subsystem should meet all regional/national safety requirements for the region in which it is deployed.

5.3.2.3 Reliability

REQ 5.3.2.3.1: The rack power subsystem should be designed with no single points of failure in order to avoid possible loss of availability of the NFVI node function.

REQ 5.3.2.3.2: Power failures should not impact more than a single compute/storage/networking node within the NFVI rack.

REQ 5.3.2.3.3: The rack power subsystem should provide a means to report power system fault events to the hardware platform management entity and/or Data Centre infrastructure management software.

5.3.2.4 Total Power

REQ 5.3.2.4.1: The rack power subsystem should be able to support loads of 10 kW per full size rack.

NOTE: This is a minimum value based on typical rack deployments at the time of writing of the present document. Rack deployments capable of 40 kW or more are known to exist.

5.3.2.5 Energy Efficiency

REQ 5.3.2.5.1: The rack power subsystem should support a variety of energy efficiency levels in order to meet the particular deployment needs.

NOTE: Higher energy efficiency is preferred, however, the highest efficiency levels also might require more complex designs and specialized components. The economic benefits of a higher efficiency power subsystem needs to be evaluated within the context of NFV POP operational optimization. Having a variety of energy efficiency options at the rack-level will facilitate this optimization.

5.3.2.6 Facility Feeds

REQ 5.3.2.6.1: A configuration of the rack power subsystem shall support -48VDC input facility feeds in order to provide interoperability with existing central office infrastructures.

REQ 5.3.2.6.2: Configurations of the rack power subsystem should support the following three-phase formats.

Table 3

Connection	Voltage	Frequency
WYE	208	50 Hz to 60Hz
WYE	480	50 Hz to 60Hz
WYE	400	50 Hz to 60Hz
DELTA	208	50 Hz to 60Hz
DELTA	240	50 Hz to 60Hz
DELTA	230	50 Hz to 60Hz

REQ 5.3.2.6.3: Configurations for single phase facility feeds may be supported.

REQ 5.3.2.6.4: Configurations for high voltage DC facility feeds may be supported.

REQ 5.3.2.6.5: Configurations of the rack power subsystem shall support redundant input power feeds.

5.3.3 Requirements for Power Subsystem Architecture 1 (Traditional)

5.3.3.1 Power Distribution Unit Requirements

REQ 5.3.3.1.1: The power distribution unit shall accept power from one or more facility feeds.

REQ 5.3.3.1.2: The power distribution unit shall provide power from the facility feeds to the compute/storage/network nodes without regulation.

REQ 5.3.3.1.3: For three phase power inputs, the power distribution unit shall allow load balancing of power drawn from each phase of the input power.

NOTE: This can be facilitated by providing multiple output sockets distributed evenly among the phases.

REQ 5.3.3.1.4: To facilitate high-power racks, multiple power distribution units may be used.

REQ 5.3.3.1.5: Power distribution unit outputs should provide over-current protection by circuit breakers or similar method.

REQ 5.3.3.1.6 Power distribution units should be capable of measuring and remotely reporting the following operational parameters:

- Input Current
- Input Voltage
- Output Current (each output)
- Circuit Breaker Condition (tripped, not tripped)

REQ 5.3.3.1.7 Power distribution units should support generation of alarm events with programmable limits for each of the following conditions:

- Input Over Current
- Input Over/Under Voltage
- Output Over Current (each output)
- Circuit Breaker Trip

REQ 5.3.3.1.8: Power distribution units should allow individual outputs to be powered up/down under software control.

REQ 5.3.3.1.9: Power distribution units should support programmable power sequencing of the outputs / soft start to prevent large current spikes when rack power is applied.

REQ 5.3.3.1.10: The power distribution unit should be capable of providing the following information to the rack management or Data Centre infrastructure management software for asset tracking purposes:

- Manufacturer
- Model
- Serial Number

5.3.3.2 Compute/Storage/Network Node Power Supply Requirements

The function of the compute/storage/network node power supply is to convert power provided by the power distribution unit into a format that can be used by the node. The primary purpose of the power supply is to rectify and regulate the supplied power.

REQ 5.3.3.2.1: Compute/Storage/Network Nodes should accept one or more power supply units.

REQ 5.3.3.2.2: Compute/Storage/Network node power supply units should accept power from one and only one power distribution unit feed.

REQ 5.3.3.2.3: Power supply redundancy may be achieved by installing more than one power supply unit within a Compute/Storage/Network node.

REQ 5.3.3.2.4: Each power supply unit should be capable of measuring and remotely reporting the following operational parameters:

- Output Current for Each Output Voltage
- Output Voltage Value for Each Output Voltage

REQ 5.3.3.2.5: Each power supply unit should support generation of alarm events with programmable limits for each of the following conditions:

- Output Over Current for Each Output Voltage
- Output Over /Under Voltage for Each Output Voltage
- Output Loss of Regulation

REQ 5.3.3.2.6: Each power supply unit should be capable of providing the following information to the rack management or Data Centre infrastructure management software for asset tracking purposes:

- Manufacturer
- Model
- Serial Number
- Date of Manufacture

5.3.4 Requirements for Power Subsystem Architecture 2 (Rack Power Shelf)

5.3.4.1 Power Distribution Unit Requirements

REQ 5.3.4.1.1: The power distribution unit shall accept power from one or more facility feeds.

REQ 5.3.4.1.2: The power distribution unit shall provide power from the facility feeds to the rack-level power shelf/shelves without regulation.

REQ 5.3.4.1.3: Power distribution unit should be capable of measuring and remotely reporting the following operational parameters:

- Input Current
- Input Voltage
- Output Current (each output)

REQ 5.3.4.1.4: The power distribution unit should support generation of alarm events with programmable limits for each of the following conditions:

- Input Over Current
- Input Over/Under Voltage
- Output Over Current (each output)

REQ 5.3.3.1.5: The power distribution unit should be capable of providing the following information to the rack management or Data Centre infrastructure management software for asset tracking purposes:

5.3.4.2 Power Shelf Requirements

The function of the power shelf is to convert power provided by the power distribution unit into a format that can be used by the compute/storage/network nodes. The primary purpose of the power supply is to rectify and regulate the supplied power.

REQ 5.3.4.2.1: The power shelf shall accept one or more power supply units for both capacity and redundancy purposes.

REQ 5.3.4.2.2: Power shelf may accept power from more than one power distribution unit feed.

REQ 5.3.4.2.3: More than one power shelf may be installed in an NFVI rack for capacity or redundancy purposes.

REQ 5.3.4.2.4: Output power shall be delivered from the power shelf to compute/storage/network nodes via bus bar or bussed cables.

REQ 5.3.4.2.5: The power delivered from the power shelf shall be protected from over current by circuit breaker or other similar safety device.

REQ 5.3.4.2.6: The power shelf should be capable of measuring and remotely reporting the following operational parameters:

- Output Current for Each Output Voltage
- Output Voltage Value for Each Output Voltage
- Number of Power Supplies Installed in the Shelf
- Maximum Capacity of the Shelf Based on Installed Supplies

REQ 5.3.4.2.7: Each power supply unit should be capable of measuring and remotely reporting the following operational parameters:

- Output Current for Each Output Voltage
- Output Voltage Value for Each Output Voltage

REQ 5.3.4.2.8: The power shelf should support generation of alarm events with programmable limits for each of the following conditions:

- Output Over Current for Each Output Voltage
- Output Over/Under Voltage for Each Output Voltage
- Output Loss of Regulation

REQ 5.3.4.2.9: The power shelf should be capable of providing the following information to the rack management or Data Centre infrastructure management software for asset tracking purposes:

- Manufacturer
- Model
- Serial Number
- Date of Manufacture

REQ 5.3.4.2.10: The power supplies should be capable of providing the following information to the rack management or Data Centre infrastructure management software for asset tracking purposes:

- Manufacturer
- Model
- Serial Number
- Date of Manufacture

5.3.5 Local Energy Storage

Local energy storage is the practice of using batteries within the equipment rack in order to replace centralized UPS systems. To do so, a Battery Backup Unit (BBU) is placed either in the individual compute/storage/network nodes or within the rack power shelf. For some system deployments there could be economic, reliability, or safety advantages to local energy storage.

Localized energy storage within NFVI nodes is not required, however, if it is present, the requirements are as follows:

REQ 5.3.5.1: Localized energy storage should be capable of providing power from the time that facility power is lost and generator (or backup power) is stabilized.

NOTE: 15 to 90 seconds is a typical time for alternate power to stabilize.

REQ 5.3.5.2: In racks with power shelves, BBU units should be placed within the power shelf power supply unit bays.

REQ 5.3.5.3: In NFVI racks without power shelves, BBU units should be placed within one of the compute/storage/network node's power supply bays.

REQ 5.3.5.4: BBU mechanical form-factor should be identical to power supply units in order to facilitate interchangeability.

REQ 5.3.5.5: The BBU should be capable of measuring and remotely reporting the following operational parameters:

- Output Current
- Output Voltage
- Charge Level
- Total Capacity
- Battery Temperature

REQ 5.3.5.6: The BBU should support generation of alarm events with programmable limits for each of the following conditions:

- Output Over Current
- Battery Over Temperature

REQ 5.3.5.7: The BBU should be capable of providing the following information to the rack management or Data Centre infrastructure management software for asset tracking purposes:

- Manufacturer
- Model
- Serial Number
- Date of Manufacture
- Rated Capacity

5.4 Interconnections

5.4.1 Introduction

This clause deals with the methods by which elements of the NFV Node infrastructure are physically connected and linked together. It refers to physical configuration, capacity, modularity, scalability, racking, traffic engineering, cooling, etc. The key criteria are:

- Common interconnection methods (e.g. Ethernet) for all nodes;
- Capacity scalable to order of Terabits/s per rack unit;
- Modular capacity can grow as installation needs demand;
- Support high bandwidth and low latency switching to meet the resource pooling requirements;
- Support isolation of north-south data flow and east-west data flow;
- Support isolation of service data flow and management data flow;
- Cabling methods with cooling considerations.

5.4.2 Requirements for compute and infrastructure network domain

In the NFVI Node physical architecture, an infrastructure network domain includes all networking that interconnects compute/storage infrastructure, and a compute domain includes servers and storage.

Requirements:

REQ 5.4.2.1: NFVI network nodes shall incorporate one or more Ethernet network ports for interconnect with devices beyond the rack (northbound links).

REQ 5.4.2.2: NFVI network node northbound links should support a variety Ethernet physical interfaces through industry standard modules in order to facilitate specific installation needs.

REQ 5.4.2.3: NFVI network nodes may support northbound links of types other than Ethernet.

REQ 5.4.2.4: NFVI network nodes shall incorporate one or more Ethernet network ports for interconnect with devices within the same rack as the network node (east/west links).

REQ 5.4.2.5: NFVI network node east/west ports should support a variety of Ethernet physical interfaces through industry standard modules or connectors in order to facilitate specific installation needs.

REQ 5.4.2.6: NFVI network node east/west ports should exist for each additional compute/storage/network node within the rack.

REQ 5.4.2.7: NFVI network nodes may supply more than one east/west port for each additional compute/storage/network node within the rack.

REQ 5.4.2.8: NFVI network nodes may support east/west links of types other than Ethernet.

REQ 5.4.2.9: NFVI network nodes may allow northbound links to be used for east/west connections within the rack and vice versa in order to facilitate flexibility based on installation needs.

REQ 5.4.2.10: NFVI Compute/Storage nodes shall incorporate one or more Ethernet network ports for interconnect with the rack-level Network Nodes.

REQ 5.4.2.11: Compute/Storage node ports should support a variety Ethernet physical interfaces through industry standard modules or connectors in order to facilitate specific installation needs.

REQ 5.4.2.12: NFVI Compute/Storage nodes may support links of types other than Ethernet.

REQ 5.4.2.13: Compute domain nodes should be able to physically be interconnected with the same hops in order to keep predictable latency

REQ 5.4.2.14: Cabling methods for the interconnections shall not block airflow for cooling.

5.5 Cooling

5.5.1 Introduction

As NFVI hardware operates, it generates heat that shall be dissipated and removed. This clause details requirements for proper cooling of the equipment. The assumed environment for the equipment is an indoor facility with no, partial, or full temperature and humidity control typical of most central office and Data Centre spaces.

Other environments, while not precluded, might imply more stringent requirements than those found in this clause. These requirements are explicitly beyond the scope of the present document.

5.5.2 General Cooling Requirements

The following are general requirements for cooling of the NFVI hardware.

REQ 5.5.2.1: Forced air cooling is required. Other options may be supported.

REQ 5.5.2.2: The direction of airflow shall be from the front of the equipment (inlet) to the rear of the equipment (exhaust).

REQ 5.5.2.3: Air filters shall be present at the inlet side of the airflow path in order to protect the equipment from dust and particulates.

REQ 5.5.2.4: Air filters shall be field serviceable without the use of specialized tools.

REQ 5.5.2.5: Normal operating temperature range of the equipment shall be between 10 °C and 35 °C as measured at the inlet.

NOTE: This requirement was derived from ASHRAE Data Centre [i.9] and ETSI thermal requirements for Data Centre [i.8] with the upper limit being the more stringent of the ranges defined by the referenced specifications.

REQ 5.5.2.6: Blanking panels or air baffles shall be supported in order to reduce recirculation of airflow through the rack.

REQ 5.5.2.7: NFVI equipment should comply with acoustic limits found within NEBS™ GR-63 [7].

5.5.3 Rack Level Cooling

When present, rack cooling solutions are responsible for providing cooling to all components within the rack. Rack cooling solutions generally consist of multiple fans to move cool air into the rack and heated air out. The following requirements apply if rack-level cooling is used.

REQ 5.5.3.1: Rack level fans shall be field serviceable while the equipment is in operation.

REQ 5.5.3.2: Redundancy within the rack cooling system shall provide appropriate levels of cooling to all the rack equipment while the rack cooling system is serviced.

REQ 5.5.3.3 Redundancy within the rack cooling system shall provide appropriate levels of cooling to all the rack equipment in the event of any single fan failure within the rack cooling system.

REQ 5.5.3.4: Rack Fans shall either be guaranteed for a specified service life or shall be serviceable without the use of specialized tools.

REQ 5.5.3.5: Rack-level telemetry shall be available to detect latent fan fault conditions (e.g. fan speed) for each rack fan.

REQ 5.5.3.6: Rack level temperature sensors shall be present at the air inlet and exhaust locations.

REQ 5.5.3.7: Fan speed control shall support autonomous mode where speed is controlled locally within the rack.

5.5.4 Compute/Storage/Network Node-Level Cooling

When present, compute/storage/network node-level cooling solutions are responsible for providing airflow through the node. Requirements for this type of cooling are given below.

REQ 5.5.4.1: Fans may be field serviceable. Serviceability while the equipment is in operation is not required.

REQ 5.5.4.2: Telemetry shall be available to detect fan speed for each fan.

REQ 5.5.4.3: Compute/storage/network node-level temperature sensors shall be present at the air inlet and exhaust locations.

REQ 5.5.4.4: The compute/storage/network node shall monitor the temperatures of critical components.

REQ 5.5.4.5: The compute/storage/network node shall have the capability to autonomously take action to prevent damage if an over temperature condition is detected. This may include increasing fan speed, clock throttling, placing some components into low-power states.

REQ 5.5.4.6: Action that the compute/storage/network node takes when an over temperature condition is detected shall be software configurable, but with a pre-configured non-changeable default value/behaviour.

REQ 5.5.4.7: Fan speed control shall support autonomous mode where speed is controlled locally within compute/storage/network node.

5.6 Hardware Platform Management

5.6.1 Introduction

Hardware platform management is optimally accomplished by a mechanism that allows client or control applications to manage power, state, and inventory, as well as monitor, configure and update all the equipment and components in the racks/frames. The mechanism for manageability is typically a Baseboard Management Controller (BMC) or service processor located in each piece of equipment or as a device that manages multiple pieces of equipment. The BMC/service processor is an out-of-band resource. Out-of-band resource can be understood in the context of in-band resources. In-band resources host the operating system and out of band resources operate independently of the in-band resources. The out-of-band resource is operational on auxiliary power (e.g. receives power when the equipment is connected to a power source whether the equipment is turned on or not) and is accessible remotely via a network interface. Out-of-band resources may also provide a host interface for access by in-band entities.

Out-of-band resources support a secure and modern interface protocol that is applicable to compute, storage, and network hardware and, at minimum, covers traditional baseboard management domains including chassis and component Field Replaceable Unit (FRU) information, power and thermal representation and control.

Other management domains such as firmware update, BIOS, storage, network interface, etc. management, while not precluded, might imply more stringent requirements than those found in this clause. These requirements are explicitly beyond the scope of this document.

5.6.2 General Platform Management Requirements

The following are general requirements for management of the NFVI hardware.

REQ 5.6.2.1: Platform management shall be implemented in a BMC or Service processor. The BMC/service processor should be located in each separate equipment, but may separate and manage multiple compute/storage/network nodes.

REQ 5.6.2.2: The BMC/service processor shall be available, regardless of whether the equipment is turned on and be available when the equipment is connected to power source.

REQ 5.6.2.3: A modern, secure management interface protocol and network transport shall be required.

REQ 5.6.2.4: The platform management interface should be standards based, extensible to support new and vendor specific capabilities, and enable new capabilities to be added while remaining backwards compatible with earlier versions.

REQ 5.6.2.5: The BMC/service processor shall be accessible remotely via Ethernet network. The network interface should be configurable to service either a management or production network.

5.6.3 Interface Protocol Requirements

The following are requirements for the management interface of the NFVI hardware.

REQ 5.6.3.1: The management interface shall be structured as a REST Application Program Interface (API) service conformant with the Redfish REST API specification [10].

REQ 5.6.3.2: The protocol transport shall leverage internet protocol standards such as TCP/IP, HTTP and utilize SSL for in-flight encryption.

REQ 5.6.3.3: The protocol shall be RESTful using a JSON payload and be based on a published standardized Entity Data Model.

REQ 5.6.3.4: The interface shall include Open Data Protocol metadata conventions as specified by Redfish REST API specification [10].

5.6.4 Hardware Platform Representation Requirements

The following are requirements for representation of the NFVI hardware.

REQ 5.6.4.1: The hardware platform management service shall implement a service root, Chassis, Manager and other collections as required by Redfish REST API specification [10]. The hardware platform management service may implement Systems collections and other collections as appropriate for representing the equipment hardware capabilities.

REQ 5.6.4.2: Instrumentation representing and providing control of power domains within equipment shall be implemented using the Power entity schema defined in Redfish Schema [11].

REQ 5.6.4.3: Instrumentation representing and providing control of thermal/cooling domains within equipment shall be implemented using the Thermal entity schema defined in Redfish Schema [11].

5.6.5 Logging Representation Requirements

The following are requirements for representation of hardware platform logging the NFVI hardware.

REQ 5.6.5.1: Hardware platform event log information shall be represented in a consistent format. The format should be consistent with the Log Entry entity schema defined in the Redfish Schema [11].

REQ 5.6.5.2: Client application access to hardware platform log information shall be consistent with RESTful API operations aligned with Redfish API specification [10].

5.7 Hardware Security Measures

For hardware security measures several issues need to be taken into consideration. NFV hardware component support for sensitive security processes (e.g. Lawful Interception, Retained Data, and Critical National Infrastructure) have been described in ETSI GS NFV-SEC 009 [8]. Detailed requirements for the corresponding sensitive components are specified in ETSI GS NFV-SEC 012 [9] and should be implemented.

For the purpose of this document, it is important to consider a secure hardware anchor; several solutions exist and different approaches are described in ETSI GS NFV-SEC 009 [8]. The selected security measure will be a function of the security requirements; they depend on the deployment and security policies of the operators.

REQ 5.7.1: The hardware nodes shall support at least one hardware security element such as hardware-mediated execution enclave (clause 6.16 of ETSI GS NFV-SEC 009 [8]), Trusted Platform Module (TPM, clause 6.17 of ETSI GS NFV-SEC 009 [8]) or Hardware Security Modules (HSM, clause 6.20 of ETSI GS NFV-SEC 009 [8]).

5.8 Radiated Emissions and Electromagnetic Compliance

Correctly handling radiated emissions and electromagnetic compliance are important factors when deploying NFV nodes. Computing equipment generates radiated electromagnetic emissions that can come from a variety of sources including fans, power supplies, integrated circuits, and others. Without proper containment, it can impact other sensitive equipment and disrupt radio transmissions.

It is expected that NFV node equipment will be designed using industry best practices in order to avoid the generation of excessive radiated emissions. Likewise, it is expected that reasonable practices be employed to contain emissions generated by the equipment.

Most countries have regulations dictating the maximum amount of radiated emissions allowable from computing equipment. Compliance of NVF Node equipment deployed within a specific country is expected to meet the applicable regional standards for radiated emissions and electromagnetic compliance.

5.9 Climatic and Acoustic Considerations

Temperature and noise are the basic environmental factors that need consideration when building an NFVI-PoP.

The climatic issues include several aspects as follows:

- The NFVI nodes are expected to function well within a specified temperature range.
- The cooling system of the NFVI-PoP (includes the rack level and the NFVI node level) is expected to keep the NFVI nodes within the specific temperature range.
- Air flow management (such as separation of hot and cold airstreams) could be adopted to improve the cooling efficiency and ease the maintenance.

Within these factors, this document mainly focuses on the cooling requirements which are specified in clause 5.5.

The NFVI nodes produce noise as they operate; excessive noise could harm the health of the people in the environment or cause noise pollution. Most of the noise in the NFVI-PoP is caused by the cooling equipment, such as fans, air conditioners. The acoustic requirement of cooling equipment can be found in clause 5.5.2.

5.10 Timing and Synchronization Issues

5.10.1 Background

Some applications require high accuracy synchronization and/or time-stamping of events.

For example, the Markets in Financial Instruments Directive (MiFID), which is the EU legislation regulating firms providing services to clients linked to 'financial instruments', requires that as of some date to be determined in 2018, participants will timestamp every 'reportable event', in a financial transaction's lifecycle to millisecond accuracy and granularity. High frequency traders will record to an even more stringent 1 microsecond resolution with 100 microsecond accuracy.

Other industries, such as industrial automation, telecommunications and the power industry have even higher accuracy requirements. Some examples of these requirements are shown in table 4.

Table 4: Examples of Required Time Accuracy by Industry

Industry	Requirement	Accuracy Requirement
Telecommunications	Phase alignment between LTE Base Station Transmitters	±1,5 us
Power	Synchronization of generators	±1 us
Financial	MIFID - high frequency trading	±100 us

To achieve these levels of accuracy requires the distribution of time from some central reference source to individual nodes within the network. Technologies exist to do this, for example a Global Navigation Satellite System (GNSS) system such as Global Positioning System (GPS) may act as a central source of Universal Coordinated Time (UTC), which is then transferred over networks perhaps using IEEE 1588™ Precision Time Protocol (PTP) [5] to ensure that all the end nodes are properly synchronized. Typically, a PTP clock is physically realized within a Network Interface Card (NIC) or device (NID). This has the benefit of removing variability due to software operations.

Achieving the required levels of accuracy inside virtual machines and networks with current technology is extremely challenging - solutions will require both hardware and software technology. Instead the approach to date for NFV has focused on providing this capability in the hardware and then fetching results from the hardware for further processing within VNFs. This was proposed in ETSI GS NFV 004 [4] and this approach is continued within this document.

IEEE 1588™ [5] specifies a protocol and associated set of state machines for transferring time over a network. There are a number of configuration options and choices within the standard that determine exactly how it should operate. A specific set of configuration choices forms the definition of a profile.

The aim of a profile is to:

a) allow nodes to interoperate; and

b) provide the capability of achieving a known level of precision at the target nodes.

The required level of precision is defined by the application.

IEEE 802.1AS™ [6] is derived from IEEE 1588™ [5] and is described as a profile, although its underlying principle of operation is a little different. It is designed to achieve high levels of accuracy with relatively low grade and thus cheaper oscillators as might be found in off the shelf NICs. As such it may be more suitable for use within a typical NFV environment.

5.10.2 Requirements

REQ 5.10.2.1: Where accurate timing is required (e.g. timing as a service,) Network Providers shall install NICs that support time distribution using an appropriate technology such as PTP. The choice of the technology will be driven by the required level of accuracy.

NOTE 1: The exact hardware chosen will depend upon the application requirements - but all physical nodes within the time distribution network will have a capability sufficient to meet the overall accuracy requirements.

REQ 5.10.2.2: The hardware shall maintain a suitably accurate clock within the NIC for timestamping of external events and also to be read as a time source by VNFs, either directly or through a function abstracted in the hypervisor.

REQ 5.10.2.3: If PTP is used, then the NICs shall utilize technology based on IEEE 1588™ Precision Time Protocol (PTP) [5] or the derivative IEEE 802.1AS™ (gPTP) [6].

REQ 5.10.2.4: Events will be indicated by the arrival of particular network packets at the NIC or by some physical signal which triggers the recording of a timestamp associated with that event.

NOTE 2: Regardless of the events, the recorded timestamps can then be read and logged/analysed by the VNF in a non-timing critical manner.

5.11 Reliability Criteria

Service availability and reliability are key criteria of the telecommunication service. To optimize the user experience, it's expected that the service outage is in milliseconds and service recovery is automatically performed. These require the telecom system to achieve a high level of reliability; typically, a reliability of 99,999 % is expected in traditional telecommunications environments.

In the NFV environment, the expectation of high service availability and reliability is unchanged. However, unlike the traditional solely hardware composed system, software are introduced in the NFV environment. As a result, the service reliability is impacted by both the infrastructure (including the hardware and virtualisation layer) and the software which includes Virtual Network Functions (VNF) and/or Management and Orchestration (MANO). Also, the availability and reliability requirements may vary for different kinds of service.

ETSI GS NFV-REL 003 [i.10] has researched these impacts and modelled the end-to-end reliability in the NFV environment. Basically, the reliability of a VNF Component (VNFC) is the product of the reliability of the host server, the virtualisation layer and the software, and the final result is limited by the weakest one. If the VNFCs composing the service are deployed on different host servers, some techniques (e.g. N+M Active-Standby, N-way and N-way Active) can be applied to improve the service's reliability. However, the reliability of the network connections needs to be taken into consideration in this case.

In summary, hardware still plays an important role with regard to the NFV system's availability and reliability, but it's no longer the dominant element that influences the result. Nevertheless, server, switch or other hardware with poor reliability will limit the reliability of the whole system. So it's still preferable for the service providers to use reliable hardware. On the other hand, hardware with fast failure detection, isolation, and automatic fault recovery features can help ease the maintenance and reduce the recovery and remediation time, and thus improve the service availability.

Generally, in terms of hardware reliability, the key criteria are:

- The reliability of the key components of the infrastructure, including power supply, cooling, switching, and avoidance of single point of failure.
- Supporting fault management features, including failure detection, isolation, diagnosis, recovery, notification.
- Supporting hot-plug for vulnerable components, including hard drive and optical modules.

Annex A: Authors & Contributors

The following people have contributed to the present document:

Rapporteur:
Percy S. Tarapore, AT&T

Contributors:
Joe Barzycki, Dell Inc.

Markus Brunner, Swisscom SA

Hiroshi Dempo, NEC Corporation

Eric Percival, Calnex Solutions Ltd

Doug Sandy, Artesyn Embedded Computing Inc.

Yang Xu, Huawei Technologies Co. Ltd

History

Document history		
V3.1.1	March 2017	Publication