# ETSI GR NFV-REL 010 V3.1.1 (2019-06)

GROUP REPORT

## Network Functions Virtualisation (NFV) Release 3; Reliability; Report on NFV Resiliency for the Support of Network Slicing



***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-REL010

Keywords
network, NFV, resiliency, slicing

***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



***Important notice***

The present document can be downloaded from:
http://www.etsi.org/standards-search

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 at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

# Contents

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables 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.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those 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.

# Introduction

The present document studies diverse NFV resiliency facets for supporting network slicing. Following a reminder of the way slicing can be conducted with respect to the NFV framework, several aspects of slicing oriented NFV design are described, including the design of network services for network slices with availability targets. In support of network slicing, the following network service operations are discussed:

- scaling, i.e. the dynamic provisioning or deprovisioning of resources granted to VNFs;
- migration, i.e. the move of virtualised resources from one set of physical resources to another;
- restoration following failures if resources are available;
- resource reallocation, i.e. restoration if the desired resources are insufficient.

Modification of VNF software and NFVI resource software and their impact on network slice resiliency are examined. Recommendations regarding the support of network slicing are finally provided covering:

1) design time;
2) run time;
3) VNF and /NFVI software modification.

It is noteworthy that NFV-MANO resiliency is considered in ETSI GR NFV-REL 007 [i.11], i.e. it is not discussed in the present document.

# 1 Scope

The present document reports on the guiding principles of NFV resiliency assurance for the support of network slicing based on an NFV infrastructure. In order to achieve this objective, it covers all resiliency related operational facets supporting network slicing. This includes design, scaling, migration, software modification, resource reallocation in time of scarcity, and restoration following a failure (including failure containment). The present document finally provides recommendations for building NFV based dependable network slicing.

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

[i.1] Recommendation ITU-R M.2083-0 (2015): "IMT Vision - Framework and overall objectives of the future development of IMT for 2020 and beyond".

[i.2] ETSI TS 128 530 (V15.0.0) (2018): "5G; Management and orchestration; Concepts, use cases and requirements (3GPP TS 28.530 version 15.0.0 Release 15)".

[i.3] ETSI GR NFV-EVE 012: "Network Functions Virtualisation (NFV) Release 3; Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework".

[i.4] 3GPP TR 28.801 (V15.1.0) (2018): "Study on management and orchestration of network slicing for next generation network (Release 15)".

[i.5] ETSI TS 123 501 (V15.5.0) (2019): "5G; System architecture for the 5G system (3GPP TS 23.501 version 15.5.0 Release 15)".

[i.6] 3GPP TS 22.261 (V15.2.0) (2017): "Service requirements for next generation new services and markets".

[i.7] ETSI GS NFV-REL 001: "Network Functions Virtualisation (NFV); Resiliency Requirements".

[i.8] ETSI GS NFV-REL 003: "Network Functions Virtualisation (NFV); Reliability; Report on Models and Features for End-to-End Reliability".

[i.9] Network Functions Virtualisation (NFV) - Network Operator Perspectives on NFV priorities for 5G, February 21st, 2017.

NOTE: Available at http://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf.

[i.10] ETSI GS NFV-REL 006: "Network Functions Virtualisation (NFV) Release 3; Reliability; Maintaining Service Availability and Continuity Upon Software Modification".

[i.11] ETSI GR NFV-REL 007: "Network Functions Virtualisation (NFV); Reliability; Report on the resilience of NFV-MANO critical capabilities".

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

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in ETSI GS NFV 003 [i.12] and the following apply:

**dedicated network service:** nested network service which is only part of a single composite network service

**N+M:** Pool of N+M active resources allowing the failure of M (typically $M \leq N$) resources without impacting the availability of the service capacity of N resources

**shared network service:** nested network service which is shared by two (or more) composite network services

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.12] and the following apply:



| | |
|---|---|
| (R)AN | (Radio) Access Network |
| 3GPP | 3rd Generation Partnership Project |
| 5G | 5th Generation |
| AF | Application Function |
| AMF | Access and Mobility Management Function |
| AN | Access Network |
| API | Application Programming Interface |
| AUSF | Authentication Server Function |
| CN | Core Network |
| CS | Communication Service |
| CSMF | Communication Service Management Function |
| DC | Data Center |
| DN | Data Network |
| eMBB | enhanced Mobile Broadband |
| IMT | International Mobile Telecommunications |
| IoT | Internet of Things |
| ITU-R | International Telcommunication Union - Radiocommunication Sector |
| MIMO | Multiple Inputs, Multiple Outputs |
| mMTC | massive Machine Type Communications |
| NOMA | Non Orthogonal Multiple Access |
| NSMF | Network Slice Management Function |
| NSS | Network Slice Subnet |
| NSSF | Network Slice Selection Function |
| NSSMF | Network Slice Subnet Management Function |
| OSS | Operations Support System |
| PCF | Policy Control Function |
| RM | Redundancy Model |
| SDN | Software Defined Networking |
| SMF | Session Management Function |
| UDM | Unified Data Management |
| UE | User Equipment |
| UPF | User Plane Function |
| uRLLC | ultra Reliable and Low Latency Communications |

# 4 NFV for supporting network slicing

## 4.1 Network slicing for providing diverse SLA

Although network slicing is not a new feature in the context of 5G systems, its applicability comes to fruition in the context of the new capabilities enabled by 5G. The 5G technologies can be viewed as disruptive technologies allowing to go beyond mass market mobile communications which can/will unify extremely diverse applications and use cases within a single framework. As an enabler for all types of usage in a digital society, e.g. energy, health, media and entertainment, factories of the future, automotive, these technologies do not focus exclusively on bandwidth increase, as the previous mobile generations. Instead they are being developed and offered as a universal technology: 5G is presented as a polymorphous approach capable of handling, from its conception, a variety of needs.

IMT 2020, defined by ITU-R, has listed some usage scenarios covering these needs [i.1]:

- enhanced Mobile Broadband (eMBB), i.e. improved performance and increased user experience, both outdoor (wide area coverage) and indoor (hotspot) - both scenarios have different requirements, i.e. seamless coverage and medium to high mobility for the former, high traffic capacity and high user data rate for the latter;
- ultra Reliable and Low Latency Communications (uRLLC), i.e. stringent requirements for capabilities such as throughput, latency, reliability and availability - the scenarios include critical needs for wireless control of industrial manufacturing or production processes, remote medical surgery, distribution automation in a smart grid, transportation safety, etc.;
- massive Machine Type Communications (mMTC), i.e. low volume of data not sensitive to latency transmitted by a very large number of connected devices - this scenario tackles the exponential increase of low cost and long battery life objects for IoT.



To address such diverse market segments, the multiservice 5G network will leverage new technologies at the air interface, e.g. MIMO (Multiple Inputs, Multiple Outputs), NOMA (Non Orthogonal Multiple Access), and new networking architectures relying on recent paradigms such as NFV (Network Functions Virtualisation) and SDN (Software Defined Networking). An expectation for the 5G system is to be able to provide optimized support for a variety of different services with diverse reliability and availability requirements, different traffic loads, and different end user communities through the use of network slicing. Network slicing uses virtualisation rather than provisioning dedicated physical networks for each type of usage, e.g. current Long Range network for IoT.

Indeed, the technical requirements for the wide variety of usage scenarios targeted cannot be met simultaneously. Instead usage classes are defined, each of which is being fulfilled by a network slice. Based on a common physical infrastructure providing virtualised resources, all slices may comprise one or more subnet slices that cover various components of the end-to-end network, such as the Access Network (AN) part and the Core Network (CN) part, and are optimized to fulfill the requirements of the network functions needed to support those use cases.

The current 3GPP vision [i.2] relates each *Communication Service (CS)*, e.g. usage scenario, to a particular *network slice* spanning over both the access network and the core network (Figure 4.1). Each slice is made of *network slice subnets* composed of network functions (not shown in the figure) which in the present document are assumed to share the same infrastructure.

The illustrative figure shows three communication services ($CS_1$, $CS_2$, $CS_3$) designed to use three network slices. Each of these network slices is composed of dedicated network slice subnets, and/or shared network slice subnets. For instance, network slice 1 is formed by one dedicated core network slice subnet ($NSS\_CN_1$) and one dedicated access network slice subnet ($NSS\_AN_1$). In contrast, network slice 3 is formed by two dedicated network slice subnets ($NSS\_CN_3$, $NSS\_AN_3$) and one network slice subnet shared with network slice 2 ($NSS\_AN_2$).

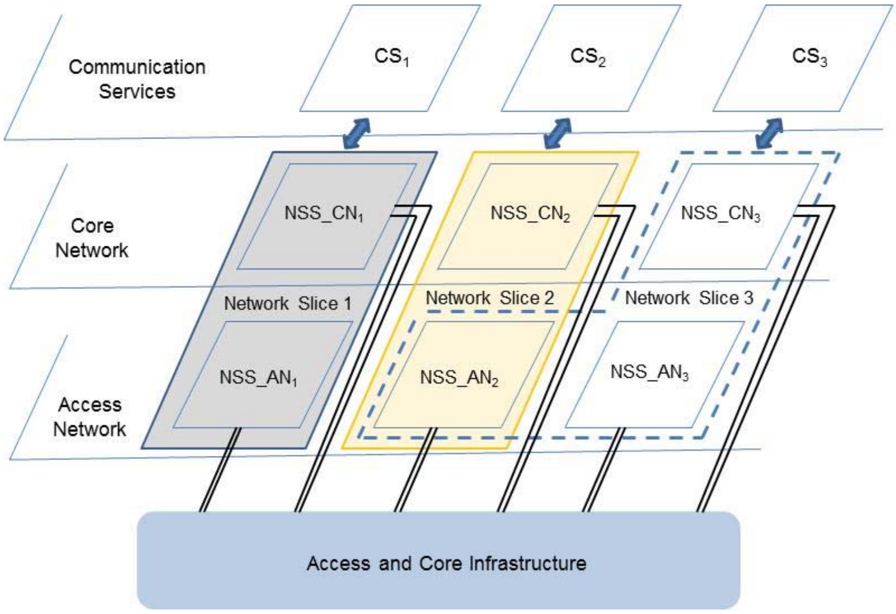


**Figure 4.1: Customized slices for communication services**

## 4.2 Mapping of NFV and network slicing concepts

Network slices and network slice subnets contain 3GPP network functions. If any of these functions is virtualised, the NFV approach can be utilized. For such cases, the 3GPP slicing concepts were mapped to the NFV concepts in ETSI GR NFV-EVE 012 [i.3]. A network slice or a network slice subnet can contain other network slice subnets, and their resources view can be realized via the network service concept in NFV, which also supports a nested network service hierarchy. Figure 4.2 (extracted from [i.3]) shows the proposed touchpoints between network slices and network services. This representation shows the relation between network slices, or network slice subnets, and the network services from a resource-centric standpoint.



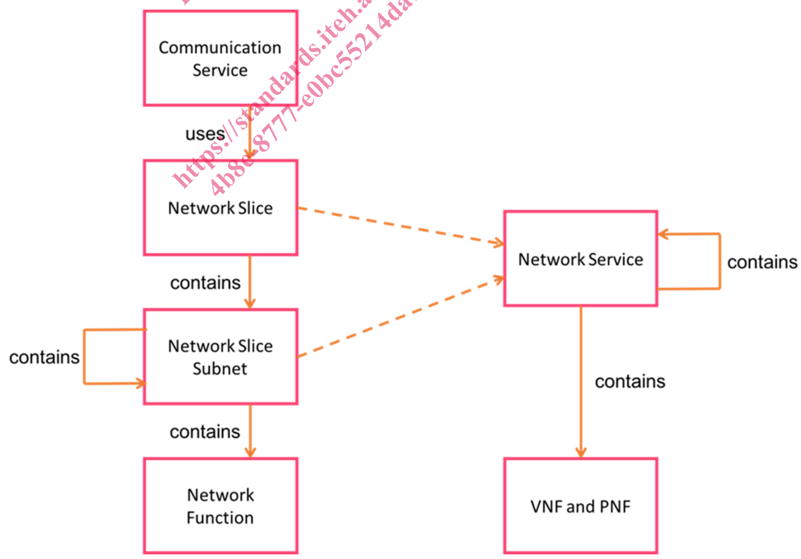


**Figure 4.2: Network slicing and its counterpart in NFV [i.3]**

Although 3GPP SA5 currently favours, in the context of network slicing, a service-based approach to the management of 3GPP 5G Core systems ETSI TS 128 530 [i.2], i.e. dealing with REST API services instead of management functional blocks, their previous report 3GPP TR 28.801 [i.4] has defined three management functions:

- Communication Service Management Function (CSMF) used to translate the communication service requirements to network slice requirements;

- Network Slice Management Function (NSMF) managing/orchestrating network slices, and deriving network slice subnet requirements from the network slices requirements;
- Network Slice Subnet Management Function (NSSMF) managing/orchestrating network slice subnets.

These management functions can interact with the NFV architecture as shown in Figure 4.3 via the Os-Ma-Nfvo interface.

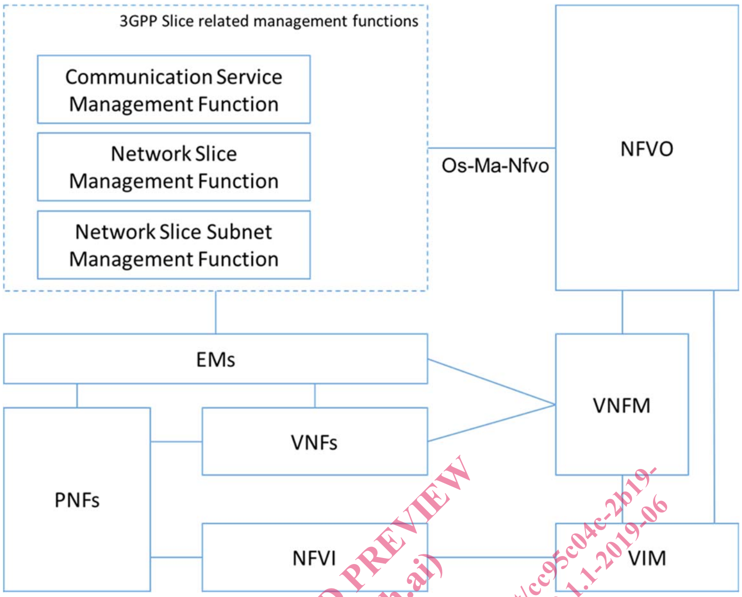


**Figure 4.3: Network slice management in an NFV framework [i.3]**



## 4.3 Network services and 3GPP network functions

As shown in Figure 4.2, 3GPP network functions are the constituents of network slices or network slice subnets. These network slices or network slice subnets can in turn be mapped to network services from a resource management viewpoint. These network services can be made of VNF(s) and can contain PNF(s), together with the Virtual Links between them, or can be made of *nested* network service(s) in addition to the VNF(s)/PNF(s) and the Virtual Links for the connectivity between them.

The 3GPP reference architecture for a 5G core system consists of different 3GPP network functions interacting with each other through various reference points $N_i$ [i.5]:

- Application Function (AF);
- Access and Mobility Management Function (AMF);
- Authentication Server Function (AUSF);
- Network Slice Selection Function (NSSF);
- Policy Control Function (PCF);
- Session Management Function (SMF);
- Unified Data Management (UDM);
- User Plane Function (UPF);
- etc.

As an example, Figure 4.4 shows the non-roaming 5G system architecture using the reference point representation.

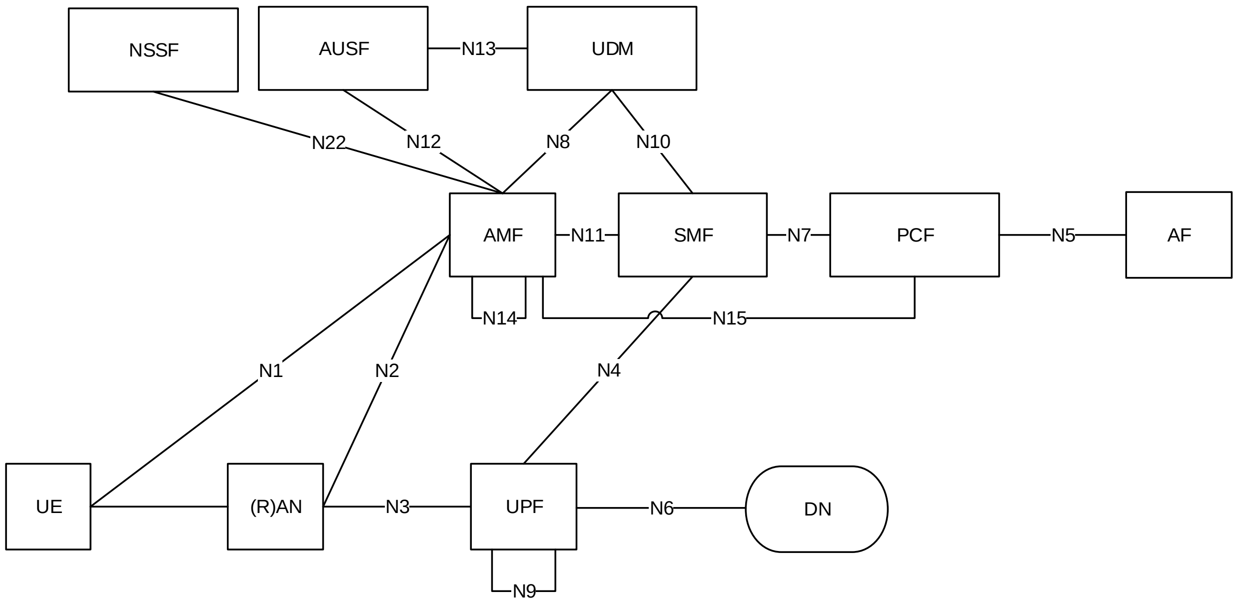


**Figure 4.4: (Non-roaming) 5G system architecture [i.5]**



A 5G system can be exposed and managed by using different network slice (or slice subnet) instances, for which the resources can be managed via NFV network service instances (see clause 4.2). While many models can be used to support the deployment of 3GPP network functions that are part of a network slice or a network slice subnet, two of the more complex deployment cases are selected below for analysis from a resiliency perspective:

- a 3GPP network function deployed as a network service instance, which is shared by different slice (slice subnet) instances. As the NFV-MANO is not aware of how the consumer (e.g. NSMF, NSSMF, OSS) is using the NS instances, then NFV-MANO does not know if a NS instance is shared or not between either network slice instances nor by different tenants;
- a 3GPP network function deployed as a network service instance dedicated to a given slice (subnet) instance.

It is noteworthy that a group of 3GPP network functions may be deployed as one VNF. In this case, the VNF resiliency and availability aspects apply, so it not further analysed in the present document.

The choice between these options is outside of the scope of NFV. NFV-MANO is not aware of the network slice instances, of network slice subnet instances, nor of the 3GPP network function instances that may be using a network service as part of their deployment. However, the information on whether a network service is shared or not has an impact on how NFV-MANO handles resiliency for the network service (e.g. see clause 6.1.1).

Figure 4.5 shows the example of a composite network service 1 (corresponding to a network slice or network slice subnet) instance with its dedicated network service $NS_1$ instance and sharing the network service $NS_3$ instance with a network service 2 (corresponding to another network slice or network slice subnet) instance. The latter also includes a dedicated network service $NS_2$ instance.

It is noteworthy to mention that the concept of shared network service instance is only visible to NFV-MANO in a nesting configuration. The analysis of the reliability and resiliency aspects in this study focuses then on the scenarios where nested NS instances are shared between composite NSs.

The NFV-MANO is only aware of the network service instances and their constituents, i.e. $NS_1$, $NS_2$ and $NS_3$, i.e. it is not aware of the network slices (or network slice subnets) using these resources.

NOTE: A top-level composite NS instance can also be shared by multiple network slices (or network slice subnets). However, this is not visible to NFV-MANO.