ETSI GS NFV-REL 003 V1.1.2 (2016-07)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a551566e-9ec8-4006-90eb-50c6b40458aa/etsi-gs-nfv-rel-003-v1.1.2-2016-07

Network Functions Virtualisation (NFV); Reliability; Report on Models and Features for End-to-End Reliability

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
RGS/NFV-REL003ed112

Keywords
availability, NFV, reliability, resiliency

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a5a1566e-eec8-4006-98eb-50e0b40458aa/etsi-gs-nfv-rel-003-v1.1.2-2016-07

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a5515566e-0ec8-4007-900b-50c6b404582a/etsi-gs-nfv-rel-003-v1.1.2-2016-07

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a551560c-0ec8-4006-90eb-50c6b0458aa/etsi-gs-nfv-rel-003-v1.1.2-2016-07

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a8515660-9ec8-4006-90eb-50c6b40458aa/etsi-gs-nfv-rel-003-v1.1.2-2016-07

1 Scope

The present document describes the models and methods for end-to-end reliability in NFV environments and software upgrade from a resilience perspective. The scope of the present document covers the following items:

- Study reliability estimation models for NFV including modelling architecture.
- Study NFV reliability and availability methods.
- Develop reliability estimation models for these methods, including dynamic operational aspects such as impact of load and life-cycle operations.
- Study reliability issues during NFV software upgrade and develop upgrade mechanisms for improving resilience.
- Develop guidelines to realise the differentiation of resiliency for different services.

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.

The following referenced documents are necessary for the application of the present document.

Not applicable.

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 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[i.2] ETSI GS NFV-REL 001: "Network Functions Virtualisation (NFV); Resiliency Requirements".

[i.3] http://www.crn.com/slide-shows/cloud/240165024/the-10-biggest-cloud-outages-of-2013.htm.

[i.4] http://www.crn.com/slide-shows/cloud/300075204/the-10-biggest-cloud-outages-of-2014.htm.

[i.5] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.6] ETSI GS NFV-SWA 001: "Network Functions Virtualisation (NFV); Virtual Network Functions Architecture".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a5515666-5f68-4006-90eb-5bc6b4049aaa/etsi-gs-nfv-rel-003-v1.1.2-2016-07

[i.7] SA Forum SAI-AIS-AMF-B.04.01: "Service Availability Forum Application Interface Specification".

[i.8] ETSI GS NFV-REL 002: "Network Functions Virtualisation (NFV); Reliability; Report on Scalable Architectures for Reliability Management".

[i.9] ETSI GS NFV-REL 004: "Network Functions Virtualisation (NFV); Assurance; Report on Active Monitoring and Failure Detection".

[i.10] ETSI GS NFV-INF 010: "Network Functions Virtualisation (NFV); Service Quality Metrics".

[i.11] ETSI GS NFV-INF 001: "Network Functions Virtualisation (NFV); Infrastructure Overview".

[i.12] IEEE 802.1ax™: "IEEE standard for local and metropolitan area networks -- Link aggregation".

[i.13] IEEE 802.1aq™: "Shortest Path Bridging".

[i.14] ETSI GS NFV-REL 005: Network Functions Virtualisation (NFV); Assurance; Quality Accountability Framework.

[i.15] QuestForum: "TL 9000 Measurements Handbook", release 5.0, July 2012.

NOTE: Available at http://www.tl9000.org/handbooks/measurements_handbook.html.

[i.16] QuEST Forum: "Quality Measurement of Automated Lifecycle Management Actions," 1.0, August 18th, 2015.

NOTE: Available at http://www.tl9000.org/resources/documents/QuEST_Forum_ALMA_Quality_Measurement_150819.pdf.

[i.17] B. Baudry and M. Monperrus: "The multiple facets of software diversity: recent developments in year 2000 and beyond", 2014. <hal-01067782>.

[i.18] L.H. Crow: "Reliability analysis for complex repairable systems", in "Reliability and biometry - statistical analysis of lifelength" (F. Prochan and R.J. Serfling, Eds.), SIAM Philadelphia, 1974, pp. 379-410.

[i.19] Y. Deswarte, K. Kanoun and J.-C. Laprie: "Diversity against accidental and deliberate faults", Conf. on Computer Security, Dependability, and Assurance: From Needs to Solutions, Washington, DC, USA, July 1998.

[i.20] J.T. Duane: "Learning curve approach to reliability monitoring", IEEE™ Transactions on Aerospace, AS-2, 2, 1964, pp. 563-566.

[i.21] A.L. Goel and K. Okumoto: "Time dependent error detection rate model for software reliability and other performance measures", IEEE™ Transactions on Reliability, R-28, 1, 1979, pp. 206-211.

[i.22] Z. Jelinski Z. and P.B. Moranda: "Statistical computer performance evaluation", in "Software reliability research" (W. Freiberger, Ed.), Academic Press, 1972, pp. 465-497.

[i.23] J.E. Just and M. Cornwell: "Review and analysis of synthetic diversity for breaking monocultures", ACM Workshop on Rapid Malcode, New York, NY, USA, 2004, pp. 23-32.

[i.24] J.C. Knight: "Diversity", Lecture Notes in Computer Science 6875, 2011.

[i.25] P. Larsen, A. Homescu, S. Brunthaler and M. Franz: "Sok: automated software diversity", IEEE™ Symposium on Security and Privacy, San Jose, CA, USA, May 2014, pp. 276-291.

[i.26] B. Littlewood, P. Popov and L. Strigini: "Modeling software design diversity: a review", ACM Computing Surveys (CSUR), 33(2), 2001, pp. 177-208.

[i.27] P.B. Moranda: "Event altered rate models for general reliability analysis", IEEE™ Transactions on Reliability, R-28, 5, 1979, pp. 376-381.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:

[i.28] J.D. Musa and K. Okumoto: "A logarithmic Poisson execution time model for software reliability measurement", 7th Int. Conf. on Software Engineering, Orlando, FL, USA, March 1984, pp. 230-238.

[i.29] I. Schaefer et al.: "Software diversity: state of the art and perspectives", International Journal on Software Tools for Technology Transfer, 14, 2012, pp. 477-495.

[i.30] S. Yamada, M. Ohba and S. Osaki: "S-shaped reliability growth modelling for software error detection", IEEE Transactions on Reliability, R-35, 5, 1983, pp. 475-478.

[i.31] ETSI GS NFV-INF 003: "Network Functions Virtualisation (NFV); Infrastructure; Compute Domain".

[i.32] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for main concepts in NFV".

[i.33] IEEE Reliability Society: "Recommended Practice on Software Reliability", IEEE™ Std 1633, 2008.

[i.34] NFV PoC#35 final report.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS NFV 003 [i.32], ETSI GS NFV-REL 001 [i.2] and the following apply:

fault detection: process of identifying an undesirable condition (fault or symptom) that may lead to the loss of service from the system or device

fault diagnosis: high confidence level determination of the required repair actions for the components that are suspected to be faulty

NOTE: Diagnosis actions are generally taken while the component being diagnosed is out of service.

fault isolation: isolation of the failed component(s) from the system

NOTE: The objectives of fault isolation include avoidance of fault propagation to the redundant components and/or simultaneous un-intended activation of active and backup components in the context of active-standby redundancy configurations (i.e. "split-brain" avoidance).

fault localization: determining the component that led to the service failure and its location

fault management notification: notification about an event pertaining to fault management

EXAMPLE: Fault management notifications include notifications of fault detection events, entity availability state changes, and fault management phase related state progression events.

fault recovery: full restoration of the original intended system configuration, including the redundancy configuration

NOTE: For components with protected state, this phase includes bringing the new protecting unit online and transferring the protected state from the active unit to the new unit.

fault remediation: restoration of the service availability and/or continuity after occurrence of a fault

fault repair: removal of the failed unit from the system configuration and its replacement with an operational unit

NOTE: For the hardware units that pass the full diagnosis, it may be determined that the probable cause was a transient fault, and the units may be placed back into the operational unit pool without physical repair.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a551566e-2ec8-4006-90eb-50c6140458aa/etsi-gs-nfv-rel-003-v1.1.2-2016-07

state protection: protection of the service availability and/or service continuity relevant portions of system or subsystem state against faults and failures

NOTE: State protection involves replicating the protected state to a redundant resource.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	Third Generation Partnership Project
AIS	Application Interface Specification
API	Application Programming Interface
ATCA	Advanced TCA (Telecom Computing Architecture)
BER	Bit Error Rates
CoS	Class of Service
COTS	Commercial Off-The-Shelf
CP	Connection Point
CPU	Central Processing Unit
DARPA	Defence Advanced Research Projects Agency
DNS	Domain Name Service
E2E	End-to-End
ECMP	Equal-Cost Multi-Path
EM	Element Manager
EMS	Element Management System
ETBF	Exponential Times Between Failures
GTP	GPRS Tunnelling Protocol
HPP	Homogenous Poisson Process
IMS	IP Multimedia Subsystem
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LB	Load Balancer
LCM	Life Cycle Management
LOC	Lines of Code
MAN	Metropolitan Area Network
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
MTBF	Mean Time Between Failure
MTD	Moving Target Defense
MTTF	Mean time To Failure
MTTR	Mean Time To Repair
NF	Network Function
NFP	Network Forwarding Path
NFVI	Network Functions Virtualisation Infrastructure
NFV-MANO	Network Functions Virtualisation Management and Orchestration
NFVO	Network Functions Virtualisation Orchestrator
NHPP	Non-Homogenous Poisson Processes
NIC	Network Interface Card
NOP	No Operation
NS	Network Service
NSD	Network Service Descriptor
OS	Operation System
OSNR	Optical Signal to Noise Ratio
OSPF	Open Shortest Path First
OSS	Operations Support System
PCI	Peripheral Component Interconnect
PDP	Packet Data Protocol
PNF	Physical Network Function
PNFD	Physical Network Function Descriptor
QoS	Quality of Service
RPO	Recovery Point Objective

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a551566e-beca-4006-90eb-50c6b40458aa/etsi-gs-nfv-rel-003-v1.1.2-2016-07

RTO	Recovery Time Objective
SA	Service Availability
SAL	Service Availability Level
SDN	Software Defined Networking
SFF	Service Function Forwarding
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SO	Service Outage
SQL	Structured Query Language
SR-IOV	Single Root I/O Virtualisation
TCP	Transmission Control Protocol
TMR	Triple Modular Redundancy
ToR	Top of Rack
VDU	Virtualisation Deployment Unit
VIM	Virtualised Infrastructure Manager
VL	Virtual Link
VLAN	Virtual Local Area Network
VLD	Virtual Link Descriptor
VM	Virtual Machine
VNF	Virtualised Network Function
VNFC	Virtualised Network Function Component
VNFCI	VNFC Instance
VNFD	Virtualised Network Function Descriptor
VNFFG	VNF Forwarding Graph
VNFFGD	VNF Forwarding Graph Descriptor
VNFI	VNF Instance
VNFM	VNF Manager
VXLAN	Virtual eXtensible Local Area Network
WAN	Wide Area Network

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a551566e-9e8f-4006-9eb-50c6b40458aa/etsi-gs-nfv-rel-003-v1.1.2-2016-07

4 Overview

4.1 End-to-End network service chain

In most cases, an End-to-End (E2E) network service (e.g. mobile voice/data, Internet access, virtual private network) can be described by one (several) NF Forwarding Graph(s) linking end points through interconnected Network Functions (NFs). The network service behaviour is a combination of the behaviour of its constituent functional blocks, which can include individual NFs and virtual links. Therefore, the reliability and availability of a network service have to be estimated based on the reliability and availability of these constituent functional blocks.

These network functions can be implemented in a single operator network or interwork between different operator networks ETSI GS NFV 002 [i.1], by partitioning the E2E network service into multiple service chains, e.g. service chains for access network and core network. Each service chain can be regarded as a chain of NFs. Each network service has E2E characteristics referring to an explicitly demarked service chain that includes multiple network functions. A service chain may have the ingress demarcation to some peripheral elements, like the customer-facing edge of a network service, e.g. a session border controller protecting a voice-over LTE IMS core, and the other demarcation of this service chain might be the border gateway with another service provider for a voice call between service providers. Thus, the chain of this network service includes:

1) Both ingress and egress perimeter elements.

2) All PNFs and VNFs in the service delivery path between the two perimeter elements.

3) All networking and interworking equipment and facilities between the two perimeter elements.

4) Supporting infrastructure (e.g. data centres) and inputs (e.g. electric power, operator policies, etc.).

An E2E service, where both "ends" are customers, comprises several E2E service delivery chains, which are mutually connected in parallel or in series, to construct a network service graph.

4.2 Reliability model of an end-to-end service

Reliability and availability of E2E services are among the subjects that operators take into consideration when deploying service, which need network functions and links for connecting these functions. Though the quality metrics, such as key performance indicators (KPIs) for reliability, availability and others (see Annex B) are monitored after deployment, traditionally, network operators estimate the reliability and availability of E2E services by evaluating those of each "demarcated service chain" described in clause 4.1, and by calculating them according to the connected patterns of the chains.

This concept is applicable for networks in the virtualised environment as well as in the traditional physical environment. The availability of the end-to-end network service composed of several service chains can be estimated as a function of the availability of each service chain and the topological connection pattern of the chains.

An example of this concept is shown in Figure 1. The availability of an end-to-end service is calculated as the product of the availabilities of the demarcated service chains comprising the E2E network.

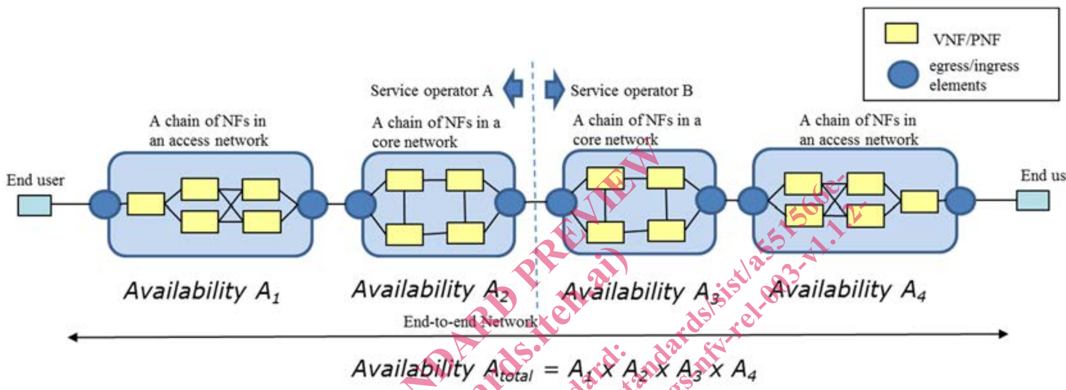

Figure 1: E2E availability of a network service composed of four demarcated service chains connected in series provided by two service operators

iTeh STANDARD PREVIEW (standards.iteh.ai)

Thus, the first part of this study focuses on the area where network functions are virtualised, and analyses the models and features to maximize the reliability of the E2E service chains.

Though there are multiple methods to treat the availability of an E2E service, such as the ones shown in Annex C and ETSI GS NFV-REL 005 [i.14], the present document describes the modelling of an "E2E service" in an NFV environment for estimating its reliability and availability and the features to ensure the targeted objectives during operation.

In an NFV environment, VNFs and virtual links are placed over an NFV Infrastructure, which is composed of a virtualisation layer and hardware resources in physical locations. The present document investigates the relationship among these elements and NFV-MANO functions, taking the following functions into consideration in order to estimate the reliability and availability of a virtualised service chain: lifecycle operations, fault management cycle, and mechanisms to implement them which affect reliability and service downtime.

4.3 Structure of the present document

Reliability estimation techniques and software reliability models are presented in clause 5, and reliability/availability methods are further developed in clause 6 for use in an NFV environment. Following that, reliability estimation models are developed in two sample use cases based on these methods in clause 7. Software upgrade in an NFV environment is also described as one of the methods to increase availability and reliability in clause 8. Since the NFV framework is such that the service availability and reliability do not need to be "built to the peak" for all service flows, Service Level Agreements (SLAs) can be defined and applied according to given resiliency classes. Clause 9 presents a method for deploying service resilience requirements and principles for managing service availability and reliability differentiation of service flows.

5 Generic reliability and availability modelling and estimation

5.1 Introduction

This clause provides generic concepts on reliability and availability modelling and estimation. It starts with an example of estimation using the reliability block diagram technique. Software reliability modelling and estimation are then presented to show how to evaluate the reliability of software.

5.2 Reliability models and estimations

5.2.1 Basic equations

The reliability and availability of a complex system such as an NFV deployment can be modelled by breaking it down into its constituent components, of which the reliability and availability are known. For repairable components, this can be expressed using cycles of uninterrupted working intervals (uptime), followed by a repair period after a failure has occurred (downtime). The average length of the first interval is usually called the *Mean Time Between Failures* (MTBF), while the average length of the second is the *Mean Time To Repair* (MTTR, see clause 6.1 for a discussion of MTTR in NFV environments). Thus, the *availability* A of a component is:

$$A = \frac{\text{Uptime}}{\text{Uptime}+\text{Downtime}} = \frac{\text{MTBF}}{\text{MTBF}+\text{MTTR}}. \quad (5.1)$$

On the other hand, the *reliability* of a component is the probability that this component has not failed after a time period t, and is thus a function R(t) of t. It is typically modelled using the exponential distribution, using the failure rate $\lambda = \frac{1}{MTBF}$ as the parameter:

$$R(t) = e^{-t\lambda} = e^{\frac{-t}{MTBF}} \quad (5.2)$$

The probability that a component has failed at least once within the same time period t is thus:

$$F(t) = 1 - R(t) = 1 - e^{\frac{-t}{MTBF}} \quad (5.3)$$

and is called *unreliability*.

Even if availability and reliability may appear to be interchangeable, they do have different meanings. From (5.1) and (5.2) it is clear that availability takes into account and is influenced by both MTBF and MTTR, whereas the reliability is only based on MTBF. As a result, two systems with the same MTBF can have quite different availabilities, while they have the same reliability (assuming that the exponential distribution is chosen for both in the reliability model).

To illustrate this difference, one can imagine a component that has a short MTBF, e.g. 10 hours, which means that R(t) is becoming low already for small values of t: R(20h) = 0,1353, i.e. the probability for the system to have run without failure for 20 hours is 13,53 %.

However, if this component has an even shorter MTTR (e.g. because it is using redundancy or it is simply re-instantiated quickly in case of failure), then the availability of the component would still be quite high, because it is available during a high share of the overall time. For an MTTR = 1 min, the availability would still be 99,83 %, although the reliability would continue being low because the component fails with a high probability after a short time.

A definition of what constitutes a failure in the context of NFV is also necessary. In extreme cases with very short service repair times, e.g. due to very fast failover in redundant configurations, the service might only be slightly degraded for a short time or even be seen as uninterrupted by external clients, particularly in scenarios with stateless VNFs. Thus, while individual components might fail, due to the composition of these components, e.g. in the form of resilience patterns, the composite might not experience a failure event. The basic effect of component composition on the reliability model is discussed in the following.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a55150c6-9ec8-4006-90eb-50c6b4e158aa/etsi-gs-nfv-rel-003-v1.1.2-2016-07

5.2.2 Modelling of composed systems

A service deployed in an NFV context can generally be assumed to be composed of a number of VNFs, which in turn may be composed of VNFCs. In order to be able to estimate and manage the reliability and availability of the composite system, these characteristics need to be derived from the individual parts it comprises. Two abstract patterns exist for this derivation, which will be shortly introduced in the following.

When combining components, two basic dependencies are possible, parallel and serial. A serial dependency of two subcomponents (Figure 2) means in the general sense that both need to function in order for the composite to function, i.e. both need to be available at the same time. As an example, SC1 could be the virtual infrastructure while SC2 the VNF running on top of it. Both need to work at the same time in order for the system to be available.

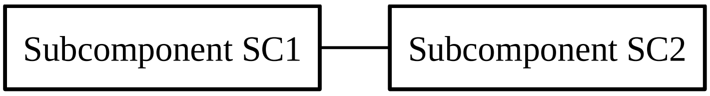

Figure 2: Serial composition of components

Therefore, for such a serial dependency, the availability of the composite C of two (independent) subcomponents SC1 and SC2 is:

$$\mathrm{A_C} = \mathrm{A_{SC1}} \times \mathrm{A_{SC2}} \tag{5.4}$$

Regarding the reliability, the composite system does not fail during time period t only if all of its subcomponents do not fail during this period. Thus,

$$\mathrm{R_C(t)} = \mathrm{R_{SC1}(t)} \times \mathrm{R_{SC2}(t)} \tag{5.5}$$

In contrast, a parallel dependency of two independent subcomponents models the situations where either of the two can be used (Figure 3). This abstract model assumes that the two subcomponents are fully redundant, i.e. that the service offered by the composite can be provided by SC1 or SC2 without any difference in service quality (in particular, it is assumed that there is no service interruption due to failover). The Active-Active resilience patterns described in the present document are typical examples for the instantiation of this abstract model, as long as the failure of one subcomponent does not imply overloading the remaining one or loss of information.

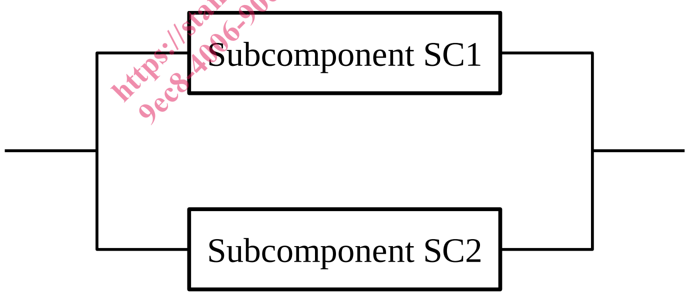

Figure 3: Parallel composition of components

Under these assumptions, the availability of such a composite parallel system C is the probability that at least one of the subcomponents is available:

$$\mathrm{A_C} = 1 - ((1 - \mathrm{A_{SC1}}) \times (1 - \mathrm{A_{SC2}})) \tag{5.6}$$

With respect to the reliability, C is considered to fail during a time period t if both SC1 and SC2 fail during t:

$$F_C(t) = F_{SC1}(t) \times F_{SC2}(t),$$

or, in the general case with N redundant subcomponents,

$$F_C(t) = \prod_{i=1}^{N} F_{SCi}(t).$$

iTeh STANDARD PREVIEW (standards.iteh.ai)