ETSI GS NFV-IFA 045 V4.5.1 (2023-10)

Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Faults and alarms modelling specification

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
DGS/NFV-IFA045

Keywords
FM, information model, management, NFV

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

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 specifies alarms associated to the objects that are managed by NFV-MANO, and whose information can be exposed over the interfaces of the NFV-MANO architectural framework. Specifically, the present document specifies alarms associated to virtualised resources, containerized workloads/managed container infrastructure objects, VNF instances, NS instances, Multi-Site Connectivity Service (MSCS), and CIS clusters.

The present document also provides a set of use cases illustrating the types of faults that can occur in NFV deployments, the correlation of fault information for the generation of alarms, and the use of the information contained in the alarms in fault management processes.

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 https://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.

[1] Recommendation ITU-T X.733: "Information technology - Open Systems Interconnection - Systems Management: Alarm reporting function".

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 GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] Recommendation ITU-T M.3400 (02-2000): "Telecommunications management network: TMN management functions".

[i.3] ETSI GS NFV-REL 001: "Network Functions Virtualisation (NFV); Resiliency Requirements".

[i.4] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[i.5] ETSI GS NFV-IFA 006: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification".

[i.6] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[i.7] ETSI GS NFV-IFA 008: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[i.8] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

[i.9] ETSI GS NFV-IFA 030: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Multiple Administrative Domain Aspect Interfaces Specification".

[i.10] ETSI GS NFV-IFA 032: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Interface and Information Model Specification for Multi-Site Connectivity Services".

[i.11] ETSI GS NFV-EVE 007: "Network Functions Virtualisation (NFV) Release 3; NFV Evolution and Ecosystem; Hardware Interoperability Requirements Specification".

[i.12] ETSI GS NFV-IFA 040 (V4.4.1): "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Requirements for service interfaces and object model for OS container management and orchestration specification".

[i.13] ETSI GS NFV-IFA 036: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Requirements for service interfaces and object model for container cluster management and orchestration specification".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

3.2 Symbols

Void.

3.3 Abbreviations

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

ECC	Error Correction Code
MSCS	Multi-Site Connectivity Service
PCI	Peripheral Component Interconnect
PCIE	PCI Express
RAID	Redundant Array of Independent Disks
SCSI	Small Computer System Interface
SMART	Self-Monitoring Analysis and Reporting Technology
TMN	Telecommunications Management Network

4 Overview

4.1 Introduction

Fault management is one of the five functional areas of the Telecommunications Management Network (TMN) model. Recommendation ITU-T M.3400 [i.2] defines fault management as the set of functions which enables the detection, isolation and correction of abnormal operation of the telecommunication network and its environments.

As summarized by ETSI GS NFV-REL 001 [i.3], fault management systems comprise two main aspects:

a) managing alarms and their propagation through the system, and

b) mitigating the impact of an occurring failure.

Thus, one key functionality related to fault management is alarm management. Alarm surveillance refers to the capabilities to monitor faults on systems. In NFV, different types of resources or elements (logical, virtual, physical) are considered, so monitoring objectives go beyond physical network elements, as typically performed in legacy telecommunications networks.

When a fault occurs, an indication can be raised in the form of an alarm. As defined in ETSI GR NFV 003 [i.1], an alarm is the information about a specific condition requiring attention, with the additional clarification that an alarm does, but not always, represent an error.

NOTE: As defined in ETSI GR NFV 003 [i.1], the terms "failure", "fault", "error" and "alarm" have different meanings.

For interoperability purposes, the information that an alarm contains is typically specified and it contains data related to what objects are affected by the fault, the severity of the fault, when the fault event has been observed, the type of event, etc. The specification of alarms is contained in so called "information elements" in the stage 2 level specifications (see related references in clause 4.2) or "data types" in the stage 3 level specifications of ETSI NFV. However, a subset of the attributes of the Alarm information element are either unspecified in terms of their content type, or when a content type is specified, possible values are not defined. Some of the affected attributes (see the list below) are of key importance for establishing correlation and relationship between alarms raised by different systems, possibly supplied by different providers, including:

- "faultType": provides additional information related to the type of fault;
- "probableCause": provides information about the probable cause of the fault; and
- "faultDetails": provides additional information about the fault.

In addition, a specified relationship between "severity", "faultType" and the corresponding resource or managed object types is necessary to enable consumers (network operators or other management systems) interpret the faults and perform root cause analysis in an interoperable multi-vendor environment.

The present document defines the alarms (see clause 6), associating the content for the listed attributes to the various NFV-MANO managed objects (see clause 5), with the purpose to specify the missing content of Alarms described above, which is referred in clause 4.2 as the "part of the content of the alarm".

4.2 Relationship with other ETSI NFV deliverables

The present document relates to other ETSI NFV deliverables as follows:

- ETSI GS NFV-IFA 005 [i.4]: specifies the Or-Vi reference point requirements and interfaces including the Virtualised Resource Fault Management interface, which includes the operations for subscribing to, and raising alarm notifications related to virtualised resources. Clause 8.6.4 of ETSI GS NFV-IFA 005 [i.4] specifies the Alarm information element for virtualised resources. The present document specifies part of the content of the alarms (i.e. valid values for certain attributes) related to the faults associated to virtualised resources.
- ETSI GS NFV-IFA 006 [i.5]: idem as ETSI GS NFV-IFA 005 [i.4] but concerning to the Vi-Vnfm reference point.
- ETSI GS NFV-IFA 007 [i.6]: specifies the Or-Vnfm reference point requirements and interfaces including the VNF Fault Management interface, which includes the operations for subscribing to, and raising alarm notifications related to VNF instances. Clause 8.8.4 of ETSI GS NFV-IFA 007 [i.6] specifies the Alarm information element for VNF instances. The present document specifies part of the content of the alarm related to the faults associated to VNF instances.
- ETSI GS NFV-IFA 008 [i.7]: idem as ETSI GS NFV-IFA 007 [i.6] but concerning to the Ve-Vnfm reference point.

- ETSI GS NFV-IFA 013 [i.8]: specifies the Os-Ma-nfvo reference point requirements and interfaces including the NS Fault Management interface, which includes the operations for subscribing to, and raising alarm notifications related to NS instances. Clause 8.5.4 of ETSI GS NFV-IFA 013 [i.8] specifies the Alarm information element for NS instances. The present document specifies part of the content of the alarm related to the faults associated to NS instances.

- ETSI GS NFV-IFA 030 [i.9]: idem as ETSI GS NFV-IFA 013 [i.8] but concerning to the Or-Or reference point.

- ETSI GS NFV-IFA 032 [i.10]: specifies the interface requirements and interfaces for the management of multi-site connectivity services including the Fault Management interface, which includes the operations for subscribing to, and raising alarm notifications related to MSCS instances. Clause 8.4.2 of ETSI GS NFV-IFA 032 [i.10] specifies the Alarm information element for MSCS instances. The present document specifies part of the content of the alarm related to the faults associated to MSCS instances.

- ETSI GS NFV-IFA 040 [i.12]: specifies the service interface requirements and object model for the management of containerized workloads and OS container-related resources. See note. The present document specifies part of the content of the alarm related to the faults associated to containerized workloads.

- ETSI GS NFV-IFA 036 [i.13]: specifies the service interface requirements and object model for the management of CIS clusters, which includes the requirements for operations to subscribe to, and raise alarm notifications related to CIS clusters. The present document specifies part of the content of the alarm related to the faults associated to CIS clusters.

NOTE: The referenced version of the ETSI GS NFV-IFA 040 [i.12] does not specify requirements for fault management related service interfaces.

5 Fault monitored object types

5.1 Introduction

Clause 5 identifies and specifies the object types that can be monitored from a fault management perspective by the NFV-MANO. Alarms are associated to the specified fault monitored object types.

As specified in the ETSI NFV specification referenced in clause 4.2, the Alarm information element contains the attribute "managedObjectId", which identifies the managed object associated to the Alarm. For each of the fault monitored object types, the corresponding managed object instance identifiers are identified with a reference to the respective referenced ETSI NFV specification in which such a managed object is specified.

5.2 Object type definitions

5.2.1 Virtual compute

The fault monitored object type "VirtualCompute" is used to collect and report alarms for one or more instances of virtualised compute resource, i.e. a Virtual Machine (VM).

The "managedObjectId", when used in an Alarm, corresponds to "computeId" (see clause 8.4.3.2.2 of ETSI GS NFV-IFA 006 [i.5] or clause 8.4.3.2.2 of ETSI GS NFV-IFA 005 [i.4]) of the monitored virtualised compute resource.

5.2.2 Virtual CPU

The fault monitored object type "VirtualCpu" is used to collect and report alarms for one or more instances of virtual CPU which are part of a virtual compute resource.

The report of alarm information of virtual CPU is provided via an Alarm associated to the contained object type "VirtualCompute" defined in clause 5.2.1.

5.2.3 Virtual memory

The fault monitored object type "VirtualMemory" is used to collect and report alarms for one or more instances of virtual memory which are part of a virtual compute resource.

The report of alarm information of virtual memory is provided via an Alarm associated to the contained object type "VirtualCompute" defined in clause 5.2.1.

5.2.4 Virtual storage

The fault monitored object type "VirtualStorage" is used to collect and report alarms for one or more instances of virtualised storage resource.

The "managedObjectId", when used in an Alarm, corresponds to "storageId" (see clause 8.4.7.2.2 of ETSI GS NFV-IFA 006 [i.5] or clause 8.4.7.2.2 of ETSI GS NFV-IFA 005 [i.4]) of the monitored virtualised storage resource.

5.2.5 Virtual NIC

The fault monitored object type "VirtualNetworkInterface" is used to collect and report alarms for one or more instances of virtualised network interface resource.

The "managedObjectId", when used in an Alarm, corresponds to "resourceId" (see clause 8.4.3.6.2 of ETSI GS NFV-IFA 006 [i.5] or clause 8.4.3.6.2 of ETSI GS NFV-IFA 005 [i.4]) of the monitored virtualised network interface resource.

5.2.6 Virtual network

The fault monitored object type "VirtualNetwork" is used to collect and report alarms for one or more instances of virtualised network resource.

The "managedObjectId", when used in an Alarm, corresponds to "networkResourceId" (see clause 8.4.5.2.2 of ETSI GS NFV-IFA 006 [i.5] or clause 8.4.5.2.2 of ETSI GS NFV-IFA 005 [i.4]) of the monitored virtualised network resource.

5.2.7 VNF

The fault monitored object type "Vnf" is used to collect and report alarms for one or more instances of a VNF.

The "managedObjectId", when used in an Alarm, corresponds to "vnfInstanceId" (see clause 9.4.2.2 of ETSI GS NFV-IFA 008 [i.7] or clause 8.5.2.2 of ETSI GS NFV-IFA 007 [i.6]) of the monitored VNF instance.

5.2.8 VNF component

The fault monitored object type "Vnfc" is used to collect and report alarms for one or more instances of a VNFC.

The report of alarm information of VNFC is provided via an Alarm associated to the contained object type "Vnf" defined in clause 5.2.7. The identifier of the VNFC, when used in an Alarm, corresponds to "vnfcInstanceId" (see clause 9.4.13.2 of ETSI GS NFV-IFA 008 [i.7] or clause 8.5.4.2 of ETSI GS NFV-IFA 007 [i.6]) of the monitored VNFC instance.

5.2.9 VNF virtual link

The fault monitored object type "VnfVirtualLink" is used to collect and report alarms for one or more instances of an internal VL in a VNF.

The report of alarm information of VNF virtual link is provided via an Alarm associated to the contained object type "Vnf" defined in clause 5.2.7. The identifier of the internal VL, when used in an Alarm, corresponds to "virtualLinkInstanceId" (see clause 9.4.5.2 of ETSI GS NFV-IFA 008 [i.7] or clause 8.5.5.2 of ETSI GS NFV-IFA 007 [i.6]) of the monitored internal VL instance of a VNF.

5.2.10 VNF internal CP

The fault monitored object type "VnfIntCp" is used to collect and report alarms for one or more instances of VNF internal CP.

The report of alarm information of VNF internal CP is provided via an Alarm associated to the contained object type "Vnf" defined in clause 5.2.7. The identifier of the VNF internal CP, when used in an Alarm, corresponds to "cpInstanceId" (see clause 9.4.15.2 of ETSI GS NFV-IFA 008 [i.7] or clause 8.5.14.2 of ETSI GS NFV-IFA 007 [i.6]) of the monitored VNF internal CP instance.

5.2.11 VNF external CP

The fault monitored object type "VnfExtCp" is used to collect and report alarms for one or more instances of VNF external CP.

The report of alarm information of VNF external CP is provided via an Alarm associated to the contained object type "Vnf" defined in clause 5.2.7. The identifier of the VNF external CP, when used in an Alarm, corresponds to "cpInstanceId" (see clause 9.8.2.2 of ETSI GS NFV-IFA 008 [i.7] or clause 8.5.12.2 of ETSI GS NFV-IFA 007 [i.6]) of the monitored VNF external CP instance.

5.2.12 NS

The fault monitored object type "Ns" is used to collect and report alarms for one or more instances of a NS.

The "managedObjectId", when used in an Alarm, corresponds to "nsInstanceId" (see clause 8.3.3.2.2 of ETSI GS NFV-IFA 013 [i.8]) of the monitored NS instance.

5.2.13 NS virtual link

The fault monitored object type "NsVirtualLink" is used to collect and report alarms for one or more instances of an NS virtual link.

The report of alarm information of NS virtual link is provided via an Alarm associated to the contained object type "Ns" defined in clause 5.2.12. The identifier of the NS virtual link, when used in an Alarm, corresponds to "nsVirtualLinkInstanceId" (see clause 8.3.3.10.2 of ETSI GS NFV-IFA 013 [i.8]) of the monitored NS virtual link instance.

5.2.14 NS service access point

The fault monitored object type "Sap" is used to collect and report alarms for one or more SAP instances of an NS instance.

The report of alarm information of NS SAP is provided via an Alarm associated to the contained object type "Ns" defined in clause 5.2.12. The identifier of the NS SAP, when used in an Alarm, corresponds to "sapInstanceId" (see clause 8.3.3.12.2 of ETSI GS NFV-IFA 013 [i.8]) of the monitored SAP instance.

5.2.15 MSCS

The fault monitored object type "Mscs" is used to collect and report alarms for one or more instances of an MSCS.

The "managedObjectId", when used in an Alarm, corresponds to "mscsId" (see clause 8.2.2.5.2 of ETSI GS NFV-IFA 032 [i.10]) of the monitored MSCS.

5.2.16 MSNC

The fault monitored object type "Msnc" is used to collect and report alarms for one or more instances of an MSCN.

The report of alarm information of MSNC is provided via an Alarm associated to the contained object type "Mscs" defined in clause 5.2.15. The identifier of the MSNC, when used in an Alarm, corresponds to "msncId" (see clause 8.2.2.6.2 of ETSI GS NFV-IFA 032 [i.10]) of the monitored MSNC.

5.2.17 CIS cluster

The fault monitored object type "CisCluster" is used to collect and report alarms for one or more instances of a CIS cluster.

The "managedObjectId", when used in an Alarm, corresponds to "cisClusterId" (see clause 4.2.4 of ETSI GS NFV-IFA 036 [i.13]) of the monitored CIS cluster.

5.2.18 CIS cluster node

The fault monitored object type "CisClusterNode" is used to collect and report alarms for one or more instances of a CIS cluster node, which can be a CIS instance, a CISM instance, or both.

The report of alarm information of CIS cluster node is provided via an Alarm associated to the contained object type "CisCluster" defined in clause 5.2.17. The identifier of the CIS cluster node, when used in an Alarm, corresponds to "cisClusterNodeId" (see clause 4.2.4 of ETSI GS NFV-IFA 036 [i.13]) of the monitored CIS cluster node.

5.2.19 CIS cluster storage

The fault monitored object type "CisClusterStorage" is used to collect and report alarms for one or more instances of a CIS cluster storage resource.

The report of alarm information of CIS cluster storage resource is provided via an Alarm associated to the contained object type "CisCluster" defined in clause 5.2.17. The identifier of the CIS cluster storage resource, when used in an Alarm, corresponds to "cisClusterStorageId" (see clause 4.2.4 of ETSI GS NFV-IFA 036 [i.13]) of the monitored CIS cluster storage resource.

5.2.20 CIS cluster network

The fault monitored object type "CisClusterNetwork" is used to collect and report alarms for one or more instances of a CIS cluster nodes network resource.

The report of alarm information of CIS cluster nodes network resource is provided via an Alarm associated to the contained object type "CisCluster" defined in clause 5.2.17. The identifier of the CIS cluster nodes network resource, when used in an Alarm, corresponds to "cisClusterNetworkId" (see clause 4.2.4 of ETSI GS NFV-IFA 036 [i.13]) of the monitored CIS cluster nodes network resource.

5.2.21 MCCO

The fault monitored object type "Mcco" is used to collect and report alarms for one or more instances of an MCCO applied to the CIS cluster.

The report of alarm information of an MCCO is provided via an Alarm associated to the contained object type "CisCluster" defined in clause 5.2.17. The identifier of the MCCO, when used in an Alarm, corresponds to "mccoId" (see clause 4.2.4 of ETSI GS NFV-IFA 036 [i.13]) of the monitored MCCO.

5.2.22 CISI

The fault monitored object type "Cisi" is used to collect and report alarms for one or more instances of a CIS.

The "managedObjectId", when used in an Alarm, corresponds to "cisiId" (see clause 4.2.4 of ETSI GS NFV-IFA 036 [i.13]) of the monitored CIS instance.

5.2.23 MCIO-C

The fault monitored object type "Mcio-c" is used to collect and report alarms for one or more instances of a compute MCIO.

The "managedObjectId", when used in an Alarm, corresponds to "ID of Compute MCIO" mapped to the resource handle's "resourceId" (see clause 8.5.7 of ETSI GS NFV-IFA 007 [i.6] or clause 9.4.7 of ETSI GS NFV-IFA 008 [i.7]) of the monitored compute MCIO.

6 Alarm definition template

The present clause introduces the template used to specify the additional alarm information. A description is provided about the meaning of the different fields in the template.

a) Alarm Definition Identifier

This field contains the unique identification of the alarm definition and corresponds to the value of the FaultType of the alarm information element. The identification shall be unique among defined Alarms and be defined as a string.

b) Description

This field contains the description of the alarm.

c) Managed Object Type

This field contains the definition of the applicable managed object associated to the alarm. See clause 5 for the managed object types specified in the present document.

d) Event Type

This field contains the event type of alarm. The event type shall take one of the following values:

COMMUNICATIONS_ALARM: an alarm of this type is associated with the procedure and/or process required for conveying information from one point to another (as defined by Recommendation ITU-T X.733 [1]).

PROCESSING_ERROR_ALARM: an alarm of this type is associated with a software or processing fault (as defined by Recommendation ITU-T X.733 [1]).

ENVIRONMENTAL_ALARM: an alarm of this type is associated with a condition related to an enclosure in which the equipment resides (as defined by Recommendation ITU-T X.733 [1]).

QOS_ALARM: an alarm of this type is associated with degradation in the quality of service (as defined by Recommendation ITU-T X.733 [1]).

EQUIPMENT_ALARM: an alarm of this type is associated with an equipment fault (as defined by Recommendation ITU-T X.733 [1]). Equipment can be either logical devices that are realized via some form of virtualisation or physical devices.

e) Perceived Severity

This field contains information about the perceived severities that is applicable to the alarm. The values of the perceived severity shall be selected from the following list:

CRITICAL: it indicates that a service affecting condition has occurred and an immediate correction action is required (as defined by Recommendation ITU-T X.733 [1]).

MAJOR: it indicates that a service affecting condition has developed and an urgent correction action is required (as defined by Recommendation ITU-T X.733 [1]).

MINOR: it indicates the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious fault (as defined by Recommendation ITU-T X.733 [1]).

WARNING: it indicates the detection of a potential or impeding service affecting fault, before any significant effects have been felt. Action should be taken to further diagnose (if necessary) and correct the problem in order to prevent it from becoming a more serious service affecting fault (as defined by Recommendation ITU-T X.733 [1]).

INDETERMINATE: it indicates that the severity level cannot be determined (as defined by Recommendation ITU-T X.733 [1]).

NOTE 1: The referenced ETSI NFV specifications that specify NFV-MANO interfaces include "CLEARED" as one of the enumeration values for "Perceived Severity". However, this value indicates the clearing of one or more previously reported alarms, and therefore it is a value that indicates the status of an Alarm and it is not used as a value in the Alarm definition.

f) Probable Cause

This field contains a description of the probable causes of the alarm. If there is any probable cause details that can be defined, this shall be defined as a string.

g) Fault Details

This field contains the additional details about the fault associated to the alarm. It can provide information about the form of creation of the alarm (direct or indirect, see note 2). If there are any fault details that can be defined, this shall be defined as one or more elements in an array of strings.

NOTE 2: In direct mode, the NFV-MANO functional blocks generate an alarm based on metrics, faults, etc. information received from monitored objects directly. In indirect mode, the NFV-MANO functional blocks generate an alarm based on metrics, faults, etc. information generated by itself and/or alarms received from other functional blocks.

7 Alarm definitions

7.1 Introduction

Clause 7 specifies alarms associated to their NFV-MANO managed objects. The specification of the Alarms adheres to the following structure:

- Specification of common definitions applicable to one or more specified Alarms. This includes the definition of which probable causes of Alarms can be mapped to event types and be associated to respective managed object types.
- Specification of Alarms following the template defined in clause 6.

The present document specifies Alarms generated by:

- VIM (see clause 7.2);
- VNFM (see clause 7.3);
- NFVO (see clause 7.4);
- WIM (see clause 7.5);
- CCM (see clause 7.6); and
- CISM (see clause 7.7).

7.2 Alarms produced by VIM

7.2.1 Common definitions

7.2.1.1 Probable causes and fault details

Table 7.2.1.1-1 specifies probable causes and fault details that can be associated to alarms produced by VIM applicable to the relevant managed object types.

NOTE: Entries in table 7.2.1.1-1 are ordered alphabetically per "probable cause".

Table 7.2.1.1-1: Probable causes on alarms produced by VIM

Probable cause	Description	Event type	Managed object types
BIT_ERROR	Event related to single/multiple bit errors of the resource associated to the managed object.	PROCESSING_ERROR_ALARM	VirtualMemory VirtualStorage
CERTIFICATE_EXPIRATION	Event related to expiration of certificate(s) for the managed object.	PROCESSING_ERROR_ALARM	VirtualCompute VirtualStorage
CONFIGURATION	Event related to configuration or state change of the managed object.	PROCESSING_ERROR_ALARM	VirtualCpu VirtualMemory VirtualStorage VirtualNetwork VirtualNetworkInterface
CPU_BUS	Event related to CPU's buses.	EQUIPMENT_ALARM	VirtualCpu
CPU_DOWN	CPU is down/not available.	EQUIPMENT_ALARM	VirtualCpu
CPU_PROTOCOL	CPU protocol related event, e.g. initialization procedure, state transitions, etc.	PROCESSING_ERROR_ALARM	VirtualCpu
CPU_THROTTLING	CPU throttling related event or state change.	EQUIPMENT_ALARM	VirtualCpu
ECC	Event related to changes in states or rates concerning Error Correction Code (ECC) of memory or storage resources.	PROCESSING_ERROR_ALARM	VirtualMemory VirtualStorage
HOST_OS_ERROR	Event related to a processing failure in the host OS.	PROCESSING_ERROR_ALARM	VirtualCompute
MEMORY_STATE	Event related to change of state on the memory.	PROCESSING_ERROR_ALARM	VirtualMemory
NETWORK_CONNECTVITY_SIGNAL	Event related to loss or changes in the connectivity signal provided/supported by the network resource.	COMMUNICATIONS_ALARM	VirtualNetwork
NETWORK_CPU_OVERLOAD	Event related to overload in the CPU/compute subsystems of the network resource.	PROCESSING_ERROR_ALARM	VirtualNetwork
NETWORK_MEMORY_OVERLOAD	Event related to overload in the memory subsystems of the network resource.	PROCESSING_ERROR_ALARM	VirtualNetwork
NETWORK_OVERLOAD	Event related to overload network input/output on the network resource.	QOS_ALARM	VirtualNetwork
NETWORK_PACKET_LOSS	Event related to packet loss experienced on the network resource.	COMMUNICATIONS_ALARM	VirtualNetwork VirtualNetworkInterface
NETWORK_QOS	Event related to degradation of QoS levels of the network resource, such as jitter and delay degradation.	QOS_ALARM	VirtualNetwork
NFVI_COMPONENT_MAINTENANCE	Event related to maintenance of an NFVI component.	EQUIPMENT_ALARM	VirtualCompute
NFVI_COMPONENT_POWER_OUTAGE	Event related to power outage of an NFVI component.	EQUIPMENT_ALARM	VirtualCompute
NIC_CABLE	Event related to cabling/connection of the network interface.	EQUIPMENT_ALARM	VirtualNetworkInterface
NIC_LINK_DOWN	Event related to a network interface link being down.	COMMUNICATIONS_ALARM	VirtualNetworkInterface
NIC_LINK_TUNING	Event related to network interface link tuning.	COMMUNICATIONS_ALARM	VirtualNetworkInterface
NIC_PCI_ERROR	Event related to a component of a Peripheral Component Interconnect (PCI) device.	EQUIPMENT_ALARM	VirtualNetworkInterface
NIC_PCI_PARITY_ERROR	Event related to PCI parity errors.	PROCESSING_ERROR_ALARM	VirtualNetworkInterface
NIC_PCIE_ERROR	Event related to a component of a PCI Express (PCIE) device.	EQUIPMENT_ALARM	VirtualNetworkInterface

Probable cause	Description	Event type	Managed object types
NODE_DOWN	Event related to the compute server (machine) hosting the associated managed object is down/not available.	EQUIPMENT_ALARM	VirtualCompute
REDUNDANCY	Event related to the redundancy configuration of the managed object.	EQUIPMENT_ALARM	VirtualMemory VirtualStorage
SENSOR	Event related to the state of the sensor associated to the managed object.	EQUIPMENT_ALARM	VirtualCpu VirtualStorage
STORAGE_BLOCK_ERROR	Event related to bad blocks on the storage drive.	PROCESSING_ERROR_ALARM	VirtualStorage
STORAGE_CACHE	Event related to the storage cache.	EQUIPMENT_ALARM	VirtualStorage
STORAGE_CAPACITY	Event related to the storage disk capacity such as shortage.	QOS_ALARM	VirtualStorage
STORAGE_CHECK	Event related to consistency checks on a storage drive.	PROCESSING_ERROR_ALARM	VirtualStorage
STORAGE_COMMUNICATION	Event related to the communication to/from the storage.	EQUIPMENT_ALARM	VirtualStorage
STORAGE_CONTROLLER	Event related to the controller of the storage.	EQUIPMENT_ALARM	VirtualStorage
STORAGE_DEFRAGMENTATION	Event related to the defragmentation of the storage.	PROCESSING_ERROR_ALARM	VirtualStorage
STORAGE_DOWN	Storage is down/not available.	PROCESSING_ERROR_ALARM	VirtualStorage
STORAGE_DRIVE_ARRAY	Event related to storage's drive array.	EQUIPMENT_ALARM	VirtualStorage
STORAGE_ENCLOSURE	Event related to the storage's enclosure.	ENVIRONMENTAL_ALARM	VirtualStorage
STORAGE_FAILURE_PREDICTION	Event related to a predictive failure confirmed on a storage drive	PROCESSING_ERROR_ALARM	VirtualStorage
STORAGE_MEMORY	Event related memory resources of the storage drive.	PROCESSING_ERROR_ALARM	VirtualStorage
STORAGE_PHYSICAL_DISK_DEGRADED	Event related to the performance of the physical disk.	QOS_ALARM	VirtualStorage
STORAGE_PHYSICAL_DISK_STATE	A physical disk state has changed.	PROCESSING_ERROR_ALARM	VirtualStorage
STORAGE_POWER	Event related to power supply and/or power status of the storage.	PROCESSING_ERROR_ALARM	VirtualStorage
STORAGE_REBUILD	Event related to the rebuild process of the storage drive.	PROCESSING_ERROR_ALARM	VirtualStorage
STORAGE_SCSI	Event related to the Small Computer System Interface (SCSI) of the storage drive.	EQUIPMENT_ALARM	VirtualStorage
STORAGE_SMART	Event related to the Self-Monitoring Analysis and Reporting Technology (SMART) feature of the storage drive.	EQUIPMENT_ALARM	VirtualStorage
STORAGE_VIRTUAL_DISK_DEGRADED	Event related to the performance of the virtual disk.	QOS_ALARM	VirtualStorage
STORAGE_VIRTUAL_DISK_STATE	A virtual disk state has changed.	PROCESSING_ERROR_ALARM	VirtualStorage
SYSTEM_LICENSE_EXPIRATION	Event related to expiration of a license applicable to the managed object.	PROCESSING_ERROR_ALARM	VirtualCompute
TEMPERATURE	Event related to the temperature on the managed object.	ENVIRONMENTAL_ALARM	VirtualCpu VirtualMemory VirtualStorage VirtualNetwork VirtualNetworkInterface
VERSION_ERROR	Event related to version mismatches or incompatibilities, e.g. incompatibility between firmware and the resource on which is applied, wrong driver version.	PROCESSING_ERROR_ALARM	VirtualCpu VirtualStorage

7.2.2 COMPUTE_WARNING

a) **Alarm definition identifier:** COMPUTE_WARNING.

b) **Description:** The compute server (machine) hosting the virtualised compute resource has potential impeding service impacts, but the virtualised compute resource is still operational.

c) **Managed object type:** VirtualCompute.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system).

7.2.3 COMPUTE_MINOR

a) **Alarm definition identifier:** COMPUTE_MINOR.

b) **Description:** The compute server (machine) hosting the virtualised compute resource has non-service affecting fault conditions.

c) **Managed object type:** VirtualCompute.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system).

7.2.4 COMPUTE_MAJOR

a) **Alarm definition identifier:** COMPUTE_MAJOR.

b) **Description:** The compute server (machine) hosting the virtualised compute resource has service affecting conditions, but the virtualised compute resource is still operational.

c) **Managed object type:** VirtualCompute.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system).

7.2.5 COMPUTE_CRITICAL

a) **Alarm definition identifier:** COMPUTE_CRITICAL.

b) **Description:** The compute server (machine) hosting the virtualised compute resource has service affecting conditions and the virtualised compute resource is not fully operational.

c) **Managed object type:** VirtualCompute.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system).

7.2.6 CPU_WARNING

a) **Alarm definition identifier:** CPU_WARNING.

b) **Description:** One or multiple CPUs supporting the virtual CPU used by the virtualised compute resource have potential impeding service impacts, but the CPU is still operational.

c) **Managed object type:** VirtualCpu.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "cpuId=$cpuId", wherein "$cpuId" indicates the CPU id associated to the issue.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the CPU is enclosed.

7.2.7 CPU_MINOR

a) **Alarm definition identifier:** CPU_MINOR.

b) **Description:** One or multiple CPUs supporting the virtual CPU used by the virtualised compute resource have non-service affecting fault conditions.

c) **Managed object type:** VirtualCpu.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type:

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "cpuId=$cpuId", wherein "$cpuId" indicates the CPU id associated to the issue.

- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the CPU is enclosed.

7.2.8 CPU_MAJOR

a) **Alarm definition identifier:** CPU_MAJOR.

b) **Description:** One or multiple CPUs supporting the virtual CPU used by the virtualised compute resource have service affecting conditions, but the CPU is still operational.

c) **Managed object type:** VirtualCpu.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "cpuId=$cpuId", wherein "$cpuId" indicates the CPU id associated to the issue.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the CPU is enclosed.

7.2.9 CPU_CRITICAL

a) **Alarm definition identifier:** CPU_CRITICAL.

b) **Description:** One or multiple CPUs supporting the virtual CPU used by the virtualised compute resource have service affecting conditions and the CPU is not fully operational.

c) **Managed object type:** VirtualCpu.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "cpuId=$cpuId", wherein "$cpuId" indicates the CPU id associated to the issue.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the CPU is enclosed.

7.2.10 MEMORY_WARNING

a) **Alarm definition identifier:** MEMORY_WARNING.

b) **Description:** One or multiple memory modules supporting the virtual memory used by the virtualised compute resource have potential impeding service impacts, but the memory resource is still operational.

c) **Managed object type:** VirtualMemory.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "raid", indicating the redundancy issues are related to Redundant Array of Independent Disks (RAID).
- "mirrored", indicating redundancy issues are related to mirrored memory.
- "spare", indicating redundancy issues are related to spare memory.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the memory is enclosed.

7.2.11 MEMORY_MINOR

a) **Alarm definition identifier:** MEMORY_MINOR.

b) **Description:** One or multiple memory modules supporting the virtual memory used by the virtualised compute resource have non-service affecting fault conditions.

c) **Managed object type:** VirtualMemory.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "raid", indicating the redundancy issues are related to RAID.
- "mirrored", indicating redundancy issues are related to mirrored memory.
- "spare", indicating redundancy issues are related to spare memory.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the memory is enclosed.

7.2.12 MEMORY_MAJOR

a) **Alarm definition identifier:** MEMORY_MAJOR.

b) **Description:** One or multiple memory modules supporting the virtual memory used by the virtualised compute resource have service affecting conditions, but the memory resource is still operational.

c) **Managed object type:** VirtualMemory.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "raid", indicating the redundancy issues are related to RAID.
- "mirrored", indicating redundancy issues are related to mirrored memory.

- "spare", indicating redundancy issues are related to spare memory.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the memory is enclosed.

7.2.13 MEMORY_CRITICAL

a) **Alarm definition identifier:** MEMORY_CRITICAL.

b) **Description:** One or multiple memory modules supporting the virtual memory used by the virtualised compute resource have service affecting conditions and the memory is not fully operational.

c) **Managed object type:** VirtualMemory.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "raid", indicating the redundancy issues are related to RAID.
- "mirrored", indicating redundancy issues are related to mirrored memory.
- "spare", indicating redundancy issues are related to spare memory.
- "memoryBank=$memId", wherein "$memId" indicates the memory bank id associated to the issue.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the memory is enclosed.

7.2.14 STORAGE_WARNING

a) **Alarm definition identifier:** STORAGE_WARNING.

b) **Description:** One or multiple drives supporting the virtual storage have potential impeding service impacts, but the storage resource is still operational.

c) **Managed object type:** VirtualStorage.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "driveId=$driveId", wherein "$driveId" indicates the drive id associated to the issue.
- "redundancy=$redundancyInfo", wherein "$redundancyInfo" provides information about the current redundancy state of the storage.
- "endpoint=$endpointId", wherein "$endpointId" indicates the identifier of the endpoint/port of the storage for connectivity associated to the issue.
- "availableCapacity=$availableCapacity", wherein "$availableCapacity" indicates the available capacity of the storage associated to the issue.

- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer or storage system) where the storage drive is enclosed.

7.2.15 STORAGE_MINOR

a) **Alarm definition identifier:** STORAGE_MINOR.

b) **Description:** One or multiple drives supporting the virtual storage have non-service affecting fault conditions.

c) **Managed object type:** VirtualStorage.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "driveId=$driveId", wherein "$driveId" indicates the drive id associated to the issue.
- "redundancy=$redundancyInfo", wherein "$redundancyInfo" provides information about the current redundancy state of the storage.
- "endpoint=$endpointId", wherein "$endpointId" indicates the identifier of the endpoint/port of the storage for connectivity associated to the issue.
- "availableCapacity=$availableCapacity", wherein "$availableCapacity" indicates the available capacity of the storage associated to the issue.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer or storage system) where the storage drive is enclosed.

7.2.16 STORAGE_MAJOR

a) **Alarm definition identifier:** STORAGE_MAJOR.

b) **Description:** One or multiple drives supporting the virtual storage have service affecting conditions, but the storage resource is still operational.

c) **Managed object type:** VirtualStorage.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "driveId=$driveId", wherein "$driveId" indicates the drive id associated to the issue.
- "redundancy=$redundancyInfo", wherein "$redundancyInfo" provides information about the current redundancy state of the storage.
- "endpoint=$endpointId", wherein "$endpointId" indicates the identifier of the endpoint/port of the storage for connectivity associated to the issue.
- "availableCapacity=$availableCapacity", wherein "$availableCapacity" indicates the available capacity of the storage associated to the issue.

- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer or storage system) where the storage drive is enclosed.

7.2.17 STORAGE_CRITICAL

a) **Alarm definition identifier:** STORAGE_CRITICAL.

b) **Description:** One or multiple drives supporting the virtual storage have service affecting conditions and the storage is not fully operational.

c) **Managed object type:** VirtualStorage.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "driveId=$driveId", wherein "$driveId" indicates the drive id associated to the issue.
- "redundancy=$redundancyInfo", wherein "$redundancyInfo" provides information about the current redundancy state of the storage.
- "endpoint=$endpointId", wherein "$endpointId" indicates the identifier of the endpoint/port of the storage for connectivity associated to the issue.
- "availableCapacity=$availableCapacity", wherein "$availableCapacity" indicates the available capacity of the storage associated to the issue.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer or storage system) where the storage drive is enclosed.

7.2.18 NIC_WARNING

a) **Alarm definition identifier:** NIC_WARNING.

b) **Description:** One or multiple network interface cards supporting the virtual network interface have potential impeding service impacts, but the network interface resource is still operational.

c) **Managed object type:** VirtualNetworkInterface.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "address=$busId:$deviceId.$functionId", wherein "$busId" indicates the bus id, "$deviceId" is the device id and "$functionId" is the function id, respectively, of the PCI device associated to the event.
- "slot=$slotId", wherein the "$slotId" is the slot number of the device associated to the event.
- "ipAddress=$ipAddress", wherein "$ipAddress" is the IP address of the virtual network interface.
- "macAddress=$macAddress", wherein "$macAddress" is the MAC address of the virtual network interface.

- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the network device is enclosed.

7.2.19 NIC_MINOR

a) **Alarm definition identifier:** NIC_MINOR.

b) **Description:** One or multiple network interface cards supporting the virtual network interface have non-service affecting fault conditions.

c) **Managed object type:** VirtualNetworkInterface.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "address=$busId:$deviceId.$functionId", wherein "$busId" indicates the bus id, "$deviceId" is the device id and "$functionId" is the function id, respectively, of the PCI device associated to the event.
- "slot=$slotId", wherein the "$slotId" is the slot number of the device associated to the event.
- "ipAddress=$ipAddress", wherein "$ipAddress" is the IP address of the virtual network interface.
- "macAddress=$macAddress", wherein "$macAddress" is the MAC address of the virtual network interface.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the network device is enclosed.

7.2.20 NIC_MAJOR

a) **Alarm definition identifier:** NIC_MAJOR.

b) **Description:** One or multiple network interface cards supporting the virtual network interface have service affecting conditions, but the network interface resource is still operational.

c) **Managed object type:** VirtualNetworkInterface.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "address=$busId:$deviceId.$functionId", wherein "$busId" indicates the bus id, "$deviceId" is the device id and "$functionId" is the function id, respectively, of the PCI device associated to the event.
- "slot=$slotId", wherein the "$slotId" is the slot number of the device associated to the event.
- "ipAddress=$ipAddress", wherein "$ipAddress" is the IP address of the virtual network interface.
- "macAddress=$macAddress", wherein "$macAddress" is the MAC address of the virtual network interface.

- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the network device is enclosed.

7.2.21 NIC_CRITICAL

a) **Alarm definition identifier:** NIC_CRITICAL.

b) **Description:** One or multiple network interface cards supporting the virtual network interface have service affecting conditions and the network interface is not fully operational.

c) **Managed object type:** VirtualNetworkInterface.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "address=$busId:$deviceId.$functionId", wherein "$busId" indicates the bus id, "$deviceId" is the device id and "$functionId" is the function id, respectively, of the PCI device associated to the event.
- "slot=$slotId", wherein the "$slotId" is the slot number of the device associated to the event.
- "ipAddress=$ipAddress", wherein "$ipAddress" is the IP address of the virtual network interface.
- "macAddress=$macAddress", wherein "$macAddress" is the MAC address of the virtual network interface.
- "hostId=$hostId", wherein "$hostId" indicates the identifier of the host (computer system) where the network device is enclosed.

7.2.22 NETWORK_WARNING

a) **Alarm definition identifier:** NETWORK_WARNING.

b) **Description:** One or multiple networks supporting the virtual network have potential impeding service impacts, but the network resource is still operational.

c) **Managed object type:** VirtualNetwork.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "device=$deviceId", wherein "$deviceId" indicates the affected network resource device id.
- "port=$portId", wherein the "$portId" is the interface port identifier of the affected network resource devices.
- "link=$linkId", wherein the "$linkId" is the link identifier on the affected network resource.

7.2.23 NETWORK _MINOR

a) **Alarm definition identifier:** NETWORK _MINOR.

b) **Description:** One or multiple networks supporting the virtual network have non-service affecting fault conditions.

c) **Managed object type:** VirtualNetwork.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "device=$deviceId", wherein "$deviceId" indicates the affected network resource device id.
- "port=$portId", wherein the "$portId" is the interface port identifier of the affected network resource devices.
- "link=$linkId", wherein the "$linkId" is the link identifier on the affected network resource.

7.2.24 NETWORK _MAJOR

a) **Alarm definition identifier:** NETWORK _MAJOR.

b) **Description:** One or multiple networks supporting the virtual network have service affecting conditions, but the network resource is still operational.

c) **Managed object type:** VirtualNetwork.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "device=$deviceId", wherein "$deviceId" indicates the affected network resource device id.
- "port=$portId", wherein the "$portId" is the interface port identifier of the affected network resource devices.
- "link=$linkId", wherein the "$linkId" is the link identifier on the affected network resource.

7.2.25 NETWORK _CRITICAL

a) **Alarm definition identifier:** NETWORK _CRITICAL.

b) **Description:** One or multiple networks supporting the virtual network have service affecting conditions and the network resource is not fully operational.

c) **Managed object type:** VirtualNetwork.

d) **Event type:** The event type associated to the probable cause as specified in table 7.2.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.2.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "device=$deviceId", wherein "$deviceId" indicates the affected network resource device id.
- "port=$portId", wherein the "$portId" is the interface port identifier of the affected network resource devices.
- "link=$linkId", wherein the "$linkId" is the link identifier on the affected network resource.

7.3 Alarms produced by VNFM

7.3.1 Common definitions

7.3.1.1 Probable causes and fault details

Table 7.3.1.1-1 specifies probable causes and fault details that can be associated to alarms produced by VNFM applicable to the relevant managed object types.

NOTE: Entries in table 7.3.1.1-1 are ordered alphabetically per "probable cause".

Table 7.3.1.1-1: Probable causes on alarms produced by VNFM

Probable cause	Description	Event type	Managed object types
CERTIFICATE_EXPIRATION	Event related to expiration of certificate(s) for the managed object.	PROCESSING_ERROR_ALARM	Vnf, Vnfc See note 1
CPU_BUS	Event related to buses of a CPU resource associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1
CPU_CONFIGURATION	Configuration related event or state change on a CPU resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
CPU_DOWN	CPU resource associated to the managed object is down/not available.	EQUIPMENT_ALARM	Vnfc See note 1
CPU_PROTOCOL	Event related to CPU protocol, e.g. initialization procedure, state transitions, etc., on a CPU resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
CPU_TEMPERATURE	Event related to the temperature on a CPU resource associated to the managed object.	ENVIRONMENTAL_ALARM	Vnfc See note 1
CPU_THROTTLING	Throttling related event or state change on a CPU resource associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1
HOST_OS_ERROR	Event related to a processing failure in the host OS supporting the applicable managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
MCIO-C_STATE	Event related to error states on the set of OS containers realizing an MCIO-C associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc
MEMORY_BIT_ERROR	Event related to single/multiple bit errors of the memory resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
MEMORY_CONFIGURATION	Event related to configuration of the memory resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
MEMORY_ECC	Event related to changes in states or rates concerning Error Correction Code (ECC) of the memory resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
MEMORY_REDUNDANCY	Event related to redundancy configuration of the memory resource associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1
MEMORY_STATE	Event related to change of state on the memory resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
MEMORY_TEMPERATURE	Event related to the temperature of memory resource associated to the managed object.	ENVIRONMENTAL_ALARM	Vnfc See note 1
NETWORK_CONFIGURATION	Event related to configuration issues with a network resource associated to the managed object.	PROCESSING_ERROR_ALARM	VnfVirtualLink
NETWORK_CONNECTVITY_SIGNAL	Event related to loss or changes in the connectivity signal provided/supported by a network resource associated to the managed object.	COMMUNICATIONS_ALARM	VnfVirtualLink
NETWORK_CPU_OVERLOAD	Event related to overload in the CPU/compute subsystems of a network resource associated to the managed object.	PROCESSING_ERROR_ALARM	VnfVirtualLink

Probable cause	Description	Event type	Managed object types
NETWORK_MEMORY_OVERLOAD	Event related to overload in the memory subsystems of a network resource associated to the managed object.	PROCESSING_ERROR_ALARM	VnfVirtualLink
NETWORK_OVERLOAD	Event related to overload network input/output on a network resource associated to the managed object.	QOS_ALARM	VnfVirtualLink
NETWORK_PACKET_LOSS	Event related to packet loss experienced on a network resource associated to the managed object.	COMMUNICATIONS_ALARM	VnfVirtualLink
NETWORK_QOS	Event related to degradation of QoS levels of a network resource associated to the managed object, such as jitter and delay degradation.	QOS_ALARM	VnfVirtualLink
NFVI_COMPONENT_MAINTENANCE	Event related to maintenance of an NFVI component associated to the managed object.	EQUIPMENT_ALARM	Vnfc VnfVirtualLink See note 1
NIC_CABLE	Event related to cabling/connection of the network interface associated to the managed object.	EQUIPMENT_ALARM	VnfIntCp, VnfExtCp
NIC_CONFIGURATION	Event related to a configuration of the network interface associated to the managed object.	PROCESSING_ERROR_ALARM	VnfIntCp, VnfExtCp
NIC_LINK_DOWN	Event related to a link down on the network interface associated to the managed object.	COMMUNICATIONS_ALARM	VnfIntCp, VnfExtCp
NIC_LINK_TUNING	Event related to link tuning of the network interface associated to the managed object.	COMMUNICATIONS_ALARM	VnfIntCp, VnfExtCp
NIC_PCI_ERROR	Event related to a component of a Peripheral Component Interconnect (PCI) device of the network interface associated to the managed object.	EQUIPMENT_ALARM	VnfIntCp, VnfExtCp
NIC_PCI_PARITY_ERROR	Event related to PCI parity errors of the network interface associated to the managed object.	PROCESSING_ERROR_ALARM	VnfIntCp, VnfExtCp
NIC_PCIE_ERROR	Event related to a component of a PCI Express (PCIE) device of the network interface associated to the managed object.	EQUIPMENT_ALARM	VnfIntCp, VnfExtCp
NONRESOURCE_COMMUNICATIONS_ERROR	Event related to communication errors not related to underlying resources associated to the managed object.	COMMUNICATIONS_ALARM	Vnf, Vnfc, VnfVirtualLink, VnfIntCp, VnfExtCp See note 1
NONRESOURCE_PROCESSING_ERROR	Event related to processing errors not related to underlying resources associated to the managed object.	PROCESSING_ERROR_ALARM	Vnf, Vnfc, VnfVirtualLink, VnfIntCp, VnfExtCp See note 1
NONRESOURCE_QOS_ERROR	Event related to quality of service errors not related to underlying resources associated to the managed object.	QOS_ALARM	Vnf, Vnfc, VnfVirtualLink, VnfIntCp, VnfExtCp See note 1
PROCESSOR_SENSOR	Sensor related event or state change on a processor resource associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1

Probable cause	Description	Event type	Managed object types
STORAGE_BIT_ERROR	Event related to single/multiple bit errors on the storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_BLOCK_ERROR	Event related to bad blocks on the storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_CACHE	Event related to the cache of the storage resource associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1
STORAGE_CAPACITY	Event related to capacity (such as shortage) of the storage resource associated to the managed object.	QOS_ALARM	Vnfc See note 1
STORAGE_CHECK	Event related to consistency checks on a storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_COMMUNICATION	Event related to the communication to/from the storage resource associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1
STORAGE_CONFIGURATION	Event related to the configuration of the storage associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_CONTROLLER	Event related to the controller of the storage resource associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1
STORAGE_DOWN	Storage resource associated to the managed object is down/not available.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_DRIVE_ARRAY	Event related to storage's drive array associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1
STORAGE_ECC	Event related to changes in states or rates concerning Error Correction Code (ECC) of the storage or memory resources associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_ENCLOSURE	Event related to the enclosure of the storage resource associated to the managed object.	ENVIRONMENTAL_ALARM	Vnfc See note 1
STORAGE_FAILURE_PREDICTION	Event related to a predictive failure confirmed on a storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_MEMORY	Event related memory resources of the storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_PHYSICAL_DISK_DEGRADED	Event related to the performance on a physical disk resource associated to the managed object.	QOS_ALARM	Vnfc See note 1
STORAGE_PHYSICAL_DISK_STATE	The state has changed on a physical disk resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_POWER	Event related to power supply and/or power status of the storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_REBUILD	Event related to the rebuild process of the storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
STORAGE_REDUNDANCY	Event related to redundancy configuration of the storage resource associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1
STORAGE_SCSI	Event related to the Small Computer System Interface (SCSI) of the storage resource associated to the managed object type.	EQUIPMENT_ALARM	Vnfc See note 1

Probable cause	Description	Event type	Managed object types
STORAGE_SENSOR	Event or state change related to sensor of the storage resource associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1
STORAGE_SMART	Event related to the Self-Monitoring Analysis and Reporting Technology (SMART) feature of the storage resource associated to the managed object.	EQUIPMENT_ALARM	Vnfc See note 1
STORAGE_TEMPERATURE	Event related to the temperature of the storage resource associated to the managed object.	ENVIRONMENTAL_ALARM	Vnfc See note 1
STORAGE_VIRTUAL_DISK_DEGRADED	Event related to the performance on a virtual disk resource associated to the managed object.	QOS_ALARM	Vnfc See note 1
STORAGE_VIRTUAL_DISK_STATE	The state has changed on a virtual disk resource associated to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
SYSTEM_LICENSE_EXPIRATION	Event related to expiration of a license applicable to the managed object.	PROCESSING_ERROR_ALARM	Vnfc See note 1
NOTE 1: The probable cause for VNFC is applicable to both virtual compute based VNFC and containerized VNFC. See note 2. NOTE 2: The present document version does not specify the path (i.e. from which NFV-MANO functional block or function) and alarm/event correlation point by which the VNFM can learn about the events or alarms to associate the indicated probable cause to a containerized VNFC.			

7.3.2 VNF_WARNING

a) **Alarm definition identifier:** VNF_WARNING.

b) **Description:** One or multiple of the underlying resources of the VNF instance have potential impeding service impacts, but the VNF instance is still operational.

c) **Managed object type:** Vnf.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.3.3 VNF_MINOR

a) **Alarm definition identifier:** VNF_MINOR.

b) **Description:** One or multiple of the underlying resources of the VNF instance are experimenting non-service affecting fault conditions and the VNF instance has non-service affecting fault conditions.

c) **Managed object type:** Vnf.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.3.4 VNF_MAJOR

a) **Alarm definition identifier:** VNF_MAJOR.

b) **Description:** One or multiple of the underlying resources of the VNF instance have service affecting conditions, but the VNF instance is still operational.

c) **Managed object type:** Vnf.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.3.5 VNF_CRITICAL

a) **Alarm definition identifier:** VNF_CRITICAL.

b) **Description:** One or multiple of the underlying resources of the VNF instance has service affecting conditions and the VNF instance is not fully operational.

c) **Managed object type:** Vnf.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.3.6 VNFC_WARNING

a) **Alarm definition identifier:** VNFC_WARNING.

b) **Description:** One or multiple of the underlying resources of the VNFC instance have potential impeding service impacts, but the VNFC instance is still operational.

c) **Managed object type:** Vnfc.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNFC instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.3.7 VNFC_MINOR

a) **Alarm definition identifier:** VNFC_MINOR.

b) **Description:** One or multiple of the underlying resources of the VNFC instance are experimenting non-service affecting fault conditions and the VNFC instance has non-service affecting fault conditions.

c) **Managed object type:** Vnfc.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNFC instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.3.8 VNFC_MAJOR

a) **Alarm definition identifier:** VNFC_MAJOR.

b) **Description:** One or multiple of the underlying resources of the VNFC instance have service affecting conditions, but the VNFC instance is still operational.

c) **Managed object type:** Vnfc.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNFC instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.3.9 VNFC_CRITICAL

a) **Alarm definition identifier:** VNFC_CRITICAL.

b) **Description:** One or multiple of the underlying resources of the VNFC instance have service affecting conditions and the VNFC instance is not fully operational.

c) **Managed object type:** Vnfc.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNFC instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.3.10 VNFVIRTUALLINK_WARNING

a) **Alarm definition identifier:** VNFVIRTUALLINK_WARNING.

b) **Description:** One or multiple of the underlying resources of the VNF virtual link have potential impeding service impacts, but the VNF virtual link is still operational.

c) **Managed object type:** VnfVirtualLink.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF virtual link instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.11 VNFVIRTUALLINK_MINOR

a) **Alarm definition identifier:** VNFVIRTUALLINK_MINOR.

b) **Description:** One or multiple of the underlying resources of the VNF virtual link are experimenting non-service affecting fault conditions and the VNF virtual link has non-service affecting fault conditions.

c) **Managed object type:** VnfVirtualLink.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF virtual link instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.12 VNFVIRTUALLINK_MAJOR

a) **Alarm definition identifier:** VNFVIRTUALLINK_MAJOR.

b) **Description:** One or multiple of the underlying resources of the VNF virtual link have service affecting conditions, but the VNF virtual link is still operational.

c) **Managed object type:** VnfVirtualLink.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF virtual link instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.13 VNFVIRTUALLINK_CRITICAL

a) **Alarm definition identifier:** VNFVIRTUALLINK_CRITICAL.

b) **Description:** One or multiple of the underlying resources of the VNF virtual link have service affecting conditions and the VNF virtual link is not fully operational.

c) **Managed object type:** VnfVirtualLink.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF virtual link instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.14 VNFINTCP_WARNING

a) **Alarm definition identifier:** VNFINTCP_WARNING.

b) **Description:** One or multiple of the underlying resources of the VNF internal CP have potential impeding service impacts, but the VNF internal CP is still operational.

c) **Managed object type:** VnfIntCp.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF internal CP instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.15 VNFINTCP_MINOR

a) **Alarm definition identifier:** VNFINTCP_MINOR.

b) **Description:** One or multiple of the underlying resources of the VNF internal CP are experimenting non-service affecting fault conditions and the VNF internal CP has non-service affecting fault conditions.

c) **Managed object type:** VnfIntCp.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF internal CPinstance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.16 VNFINTCP_MAJOR

a) **Alarm definition identifier:** VNFINTCP_MAJOR.

b) **Description:** One or multiple of the underlying resources of the VNF internal CP have service affecting conditions, but the VNF internal CP is still operational.

c) **Managed object type:** VnfIntCp.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF internal CPinstance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.17 VNFINTCP_CRITICAL

a) **Alarm definition identifier:** VNFINTCP_CRITICAL.

b) **Description:** One or multiple of the underlying resources of the VNF internal CP have service affecting conditions and the VNF internal CP is not fully operational.

c) **Managed object type:** VnfIntCp.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF internal CPinstance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.18 VNFEXTCP_WARNING

a) **Alarm definition identifier:** VNFEXTCP_WARNING.

b) **Description:** One or multiple of the underlying resources of the VNF external CP have potential impeding service impacts, but the VNF external CP is still operational.

c) **Managed object type:** VnfExtCp.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF external CP instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.19 VNFEXTCP_MINOR

a) **Alarm definition identifier:** VNFEXTCP_MINOR.

b) **Description:** One or multiple of the underlying resources of the VNF external CPs are experimenting non-service affecting fault conditions and the VNF external CP has non-service affecting fault conditions.

c) **Managed object type:** VnfExtCp.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF external CP instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.20 VNFEXTCP_MAJOR

a) **Alarm definition identifier:** VNFEXTCP_MAJOR.

b) **Description:** One or multiple of the underlying resources of the VNF external CP have service affecting conditions, but the VNF external CP is still operational.

c) **Managed object type:** VnfExtCp.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF external CP instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.3.21 VNFEXTCP_CRITICAL

a) **Alarm definition identifier:** VNFEXTCP_CRITICAL.

b) **Description:** One or multiple of the underlying resources of the VNF external CP have service affecting conditions and the VNF external CP is not fully operational.

c) **Managed object type:** VnfExtCp.

d) **Event type:** The event type associated to the probable cause as specified in table 7.3.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.3.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the VNF external CP instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.4 Alarms produced by NFVO

7.4.1 Common definitions

7.4.1.1 Probable causes and fault details

Table 7.4.1.1-1 specifies probable causes and fault details that can be associated to alarms produced by NFVO applicable to the relevant managed object types.

NOTE: Entries in table 7.4.1.1-1 are ordered alphabetically per "probable cause".

Table 7.4.1.1-1: Probable causes on alarms produced by NFVO

Probable cause	Description	Event type	Managed object types
NETWORK_CONFIGURATION	Event related to configuration issues with the network resource associated to the managed object type.	PROCESSING_ERROR_ALARM	NsVirtualLink
NETWORK_CONNECTVITY_SIGNAL	Event related to loss or changes in the connectivity signal provided/supported by the network resource associated to the managed object type.	COMMUNICATIONS_ALARM	NsVirtualLink
NETWORK_CPU_OVERLOAD	Event related to overload in the CPU/compute subsystems of the network resource associated to the managed object type.	PROCESSING_ERROR_ALARM	NsVirtualLink
NETWORK_MEMORY_OVERLOAD	Event related to overload in the memory subsystems of the network resource associated to the managed object type.	PROCESSING_ERROR_ALARM	NsVirtualLink
NETWORK_OVERLOAD	Event related to overload network input/output on the network resource associated to the managed object type.	QOS_ALARM	NsVirtualLink
NETWORK_PACKET_LOSS	Event related to packet loss experienced on the network resource associated to the managed object type.	COMMUNICATIONS_ALARM	NsVirtualLink
NETWORK_QOS	Event related to degradation of QoS levels of the network resource associated to the managed object type, such as jitter and delay degradation.	QOS_ALARM	NsVirtualLink
NONRESOURCE_COMMUNICATIONS_ERROR	Event related to communication errors not related to underlying resources associated to the managed object.	COMMUNICATIONS_ALARM	Ns, NsVirtualLink, Sap

Probable cause	Description	Event type	Managed object types
NONRESOURCE_PROCESSING_ERROR	Event related to processing errors not related to underlying resources associated to the managed object.	PROCESSING_ERROR_ALARM	Ns, NsVirtualLink, Sap
NONRESOURCE_QOS_ERROR	Event related to quality of service errors not related to underlying resources associated to the managed object.	QOS_ALARM	Ns, NsVirtualLink, Sap
PNF_EXT_CP	Event related to network interface resources for external connectivity of a PNF instance associated to the managed object.	COMMUNICATIONS_ALARM PROCESSING_ERROR_ALARM EQUIPMENT_ALARM See note	Ns, Sap
VNF_EXT_CP	Event related to network interface resources for external connectivity of a VNF instance associated to the managed object.	COMMUNICATIONS_ALARM PROCESSING_ERROR_ALARM EQUIPMENT_ALARM See note	Ns, Sap
VNF_INT_CP	Event related to network interface resources for internal connectivity of a VNF instance associated to the managed object.	COMMUNICATIONS_ALARM PROCESSING_ERROR_ALARM EQUIPMENT_ALARM See note	Ns
VNF_VL	Event related to network resources of a VNF instance associated to the managed object.	COMMUNICATIONS_ALARM QOS_ALARM PROCESSING_ERROR_ALARM See note	Ns
VNF_VNFC_COMPUTE	Event related to compute resources of a VNF instance associated to the managed object.	PROCESSING_ERROR_ALARM EQUIPMENT_ALARM ENVIRONMENTAL_ALARM See note	Ns
VNF_VNFC_MEMORY	Event related to memory resources of a VNF instance associated to the managed object.	PROCESSING_ERROR_ALARM EQUIPMENT_ALARM ENVIRONMENTAL_ALARM See note	Ns
VNF_VNFC_STORAGE	Event related to storage resources of a VNF instance associated to the managed object.	PROCESSING_ERROR_ALARM EQUIPMENT_ALARM QOS_ALARM ENVIRONMENTAL_ALARM See note	Ns
NOTE: If more than one event type is mapped to the probable cause and the alarm is generated based on some underlying alarm received by the NFVO, the value of the event type shall be the same as the one from the underlying alarm. If the alarm cannot be correlated to another underlying alarm, the NFVO should set the value to EQUIPMENT_ALARM by default.			

7.4.2 NS_WARNING

a) **Alarm definition identifier:** NS_WARNING.

b) **Description:** One or multiple of the underlying resources and/or constituents of the NS instance have potential impeding service impacts, but NS instance is still operational.

c) **Managed object type:** Ns.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "constituentId=$constituentId", wherein "$constituentId" indicates the instance id of the NS constituent (VNF, PNF) associated to the issue.

7.4.3 NS_MINOR

a) **Alarm definition identifier:** NS_MINOR.

b) **Description:** One or multiple of the underlying resources and/or constituents of the NS instance are experimenting non-service affecting fault conditions and the NS instance has non-service affecting fault conditions.

c) **Managed object type:** Ns.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "constituentId=$constituentId", wherein "$constituentId" indicates the instance id of the NS constituent (VNF, PNF) associated to the issue.

7.4.4 NS_MAJOR

a) **Alarm definition identifier:** NS_MAJOR.

b) **Description:** One or multiple of the underlying resources and/or constituents of the NS instance have service affecting conditions, but the NS instance is still operational.

c) **Managed object type:** Ns.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "constituentId=$constituentId", wherein "$constituentId" indicates the instance id of the NS constituent (VNF, PNF) associated to the issue.

7.4.5 NS_CRITICAL

a) **Alarm definition identifier:** NS_CRITICAL.

b) **Description:** One or multiple of the underlying resources and/or constituents of the NS instance have service affecting conditions and the NS instance is not fully operational.

c) **Managed object type:** Ns.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "constituentId=$constituentId", wherein "$constituentId" indicates the instance id of the NS constituent (VNF, PNF) associated to the issue.

7.4.6 NSVIRTUALLINK_WARNING

a) **Alarm definition identifier:** NSVIRTUALLINK_WARNING.

b) **Description:** One or multiple of the underlying resources of the NS virtual link have potential impeding service impacts, but NS virtual link resource is still operational.

c) **Managed object type:** NsVirtualLink.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the NS virtual link instance id associated to the issue.

- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.4.7 NSVIRTUALLINK_MINOR

a) **Alarm definition identifier:** NSVIRTUALLINK_MINOR.

b) **Description:** One or multiple of the underlying resources of the NS virtual link are experimenting non-service affecting fault conditions and the NS virtual link has non-service affecting fault conditions.

c) **Managed object type:** NsVirtualLink.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the NS virtual link instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.4.8 NSVIRTUALLINK_MAJOR

a) **Alarm definition identifier:** NSVIRTUALLINK_MAJOR.

b) **Description:** One or multiple of the underlying resources of the NS virtual link have service affecting conditions, but the NS virtual link is still operational.

c) **Managed object type:** NsVirtualLink.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the NS virtual link instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.4.9 NSVIRTUALLINK_CRITICAL

a) **Alarm definition identifier:** NSVIRTUALLINK_CRITICAL.

b) **Description:** One or multiple of the underlying resources of the NS virtual link have service affecting conditions and the NS virtual link is not fully operational.

c) **Managed object type:** NsVirtualLink.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the NS virtual link instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network resource associated to the issue.

7.4.10 SAP_WARNING

a) **Alarm definition identifier:** SAP_WARNING.

b) **Description:** One or multiple of the underlying resources of the NS service access point have potential impeding service impacts, but the NS service access point is still operational.

c) **Managed object type:** Sap.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the SAP instance id associated to the issue.
- "constituentId=$constituentId", wherein "$constituentId" indicates the instance id of the NS constituent (VNF, PNF) associated to the issue.

7.4.11 SAP_MINOR

a) **Alarm definition identifier:** SAP_MINOR.

b) **Description:** One or multiple of the underlying resources of the NS service access point have non-service affecting fault conditions and the NS service access point has non-service affecting fault conditions.

c) **Managed object type:** Sap.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the SAP instance id associated to the issue.
- "constituentId=$constituentId", wherein "$constituentId" indicates the instance id of the NS constituent (VNF, PNF) associated to the issue.

7.4.12 SAP_MAJOR

a) **Alarm definition identifier:** SAP_MAJOR.

b) **Description:** One or multiple of the underlying resources of the NS service access point have service affecting conditions, but the NS service access point is still operational.

c) **Managed object type:** Sap.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the SAP instance id associated to the issue.
- "constituentId=$constituentId", wherein "$constituentId" indicates the instance id of the NS constituent (VNF, PNF) associated to the issue.

7.4.13 SAP_CRITICAL

a) **Alarm definition identifier:** SAP_CRITICAL.

b) **Description:** One or multiple of the underlying resources of the NS service access point have service affecting conditions and the NS service access point is not fully operational.

c) **Managed object type:** Sap.

d) **Event type:** The event type associated to the probable cause as specified in table 7.4.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.4.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following:

- "instanceId=$instanceId", wherein "$instanceId" indicates the SAP instance id associated to the issue.
- "constituentId=$constituentId", wherein "$constituentId" indicates the instance id of the NS constituent (VNF, PNF) associated to the issue.

7.5 Alarms produced by WIM

7.5.1 Common definitions

7.5.1.1 Probable causes and fault details

Table 7.5.1.1-1 specifies probable causes and fault details that can be associated to alarms produced by WIM applicable to the relevant managed object types.

NOTE: Entries in table 7.5.1.1-1 are ordered alphabetically per "probable cause".

Table 7.5.1.1-1: Probable causes on alarms produced by WIM

Probable cause	Description	Event type	Managed object types
ADAPTER_ERROR	See note. Associated to network edge points (ports/interfaces) of a network node.	EQUIPMENT_ALARM	Msnc
APPLICATION_SUBSYSTEM_FAILURE	See note. Associated to network nodes.	PROCESSING_ERROR_ALARM	Mscs, Msnc
BANDWIDTH_REDUCED	See note.	QOS_ALARM	Mscs, Msnc
CALL_ESTABLISHMENT_ERROR	See note.	COMMUNICATIONS_ALARM	Mscs, Msnc
COMMUNICATIONS_PROTOCOL_ERROR	See note.	COMMUNICATIONS_ALARM	Mscs, Msnc
COMMUNICATIONS_SUBSYSTEM_FAILURE	See note.	COMMUNICATIONS_ALARM	Mscs, Msnc
CONFIGURATION_ERROR	See note.	PROCESSING_ERROR_ALARM	Mscs, Msnc
CONGESTION	See note.	QOS_ALARM	Mscs, Msnc
CORRUPT_DATA	See note.	PROCESSING_ERROR_ALARM	Mscs, Msnc
CPU_CYCLES_LIMIT_EXCEEDED	See note. Associated to network nodes.	PROCESSING_ERROR_ALARM	Msnc
DEGRADED_SIGNAL	See note. Associated to network links.	COMMUNICATIONS_ALARM	Msnc
EQUIPMENT_MALFUNCTION	See note. Associated to network nodes.	EQUIPMENT_ALARM	Msnc
FILE_ERROR	See note. Associated to network nodes.	PROCESSING_ERROR_ALARM	Mscs, Msnc
FRAMING_ERROR	See note.	COMMUNICATIONS_ALARM	Msnc
INPUT_DEVICE_ERROR	See note. Associated to network edge points (ports/interfaces) of a network node.	EQUIPMENT_ALARM	Msnc
IO_DEVICE_ERROR	See note.	EQUIPMENT_ALARM	Msnc
LOCAL_NODE_TRANSMISSION_ERROR	See note.	COMMUNICATIONS_ALARM	Msnc
LOSS_OF_FRAME	See note.	COMMUNICATIONS_ALARM	Msnc
LOSS_OF_SIGNAL	See note. Associated to network edge points (ports/interfaces) of a network node and network links.	COMMUNICATIONS_ALARM	Msnc
MULTIPLEXER_PROBLEM	See note. Associated to network links.	EQUIPMENT_ALARM	Msnc
OUT_OF_MEMORY	See note. Associated to network nodes.	PROCESSING_ERROR_ALARM	Msnc
OUTPUT_DEVICE_ERROR	See note. Associated to network edge points (ports/interfaces) of a network node.	EQUIPMENT_ALARM	Msnc
PERFORMANCE_DEGRADED	See note.	QOS_ALARM	Mscs, Msnc
POWER_PROBLEM	See note. Associated to network nodes.	EQUIPMENT_ALARM	Msnc
PROCESSOR_PROBLEM	See note. Associated to network nodes.	EQUIPMENT_ALARM	Msnc
QUEUE_SIZE_EXCEEDED	See note. Associated to network nodes.	QOS_ALARM	Msnc
RECEIVE_FAILURE	See note. Associated to network edge points (ports/interfaces) of a network node, network nodes and links.	EQUIPMENT_ALARM	Msnc
RECEIVER_FAILURE	See note. Associated to network nodes.	EQUIPMENT_ALARM	Msnc
REMOTE_NODE_TRANSMISSION_ERROR	See note. Associated to network links.	COMMUNICATIONS_ALARM	Msnc
RESOURCE_NEARING_CAPACITY	See note. Associated to network nodes.	QOS_ALARM	Msnc
RETRANSMISSION_RATE_EXCESSIVE	See note.	QOS_ALARM	Mscs, Msnc
SOFTWARE_ERROR	See note. Associated to network nodes.	PROCESSING_ERROR_ALARM	Msnc
SOFTWARE_PROGRAM_ABNORMALLY_TERMINATED	See note. Associated to network nodes.	PROCESSING_ERROR_ALARM	Msnc
SOFTWARE_PROGRAM_ERROR	See note. Associated to network nodes.	PROCESSING_ERROR_ALARM	Msnc

Probable cause	Description	Event type	Managed object types
STORAGE_CAPACITY_PROBLEM	See note. Associated to network nodes.	PROCESSING_ERROR_ALARM	Msnc
TIMING_PROBLEM	See note. Associated to network nodes.	EQUIPMENT_ALARM	Msnc
TRANSMIT_FAILURE	See note. Associated to network edge points (ports/interfaces) of a network node, network nodes and network links.	EQUIPMENT_ALARM	Msnc
TRANSMITTER_FAILURE	See note. Associated to network nodes.	EQUIPMENT_ALARM	Msnc
UNDERLYING_RESOURCE_UNAVAILABLE	See note. Associated to network nodes.	PROCESSING_ERROR_ALARM	Msnc
VERSION_MISMATCH	See note.	PROCESSING_ERROR_ALARM	Mscs, Msnc
NOTE: As defined in clause 8.1.2.1 of Recommendation ITU-T X.733 [1].			

7.5.2 MSCS_WARNING

a) **Alarm definition identifier:** MSCS_WARNING.

b) **Description:** One or multiple of the underlying resources of the MSCS have potential impeding service impacts, but the MSCS is still operational.

c) **Managed object type:** Mscs.

d) **Event type:** The event type associated to the probable cause as specified in table 7.5.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.5.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network node, network edge point or network link.

7.5.3 MSCS_MINOR

a) **Alarm definition identifier:** MSCS_MINOR.

b) **Description:** One or multiple of the underlying resources of the MSCS are experimenting non-service affecting fault conditions and the MSCS has non-service affecting fault conditions.

c) **Managed object type:** Mscs.

d) **Event type:** The event type associated to the probable cause as specified in table 7.5.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.5.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network node, network edge point or network link.

7.5.4 MSCS_MAJOR

a) **Alarm definition identifier:** MSCS_MAJOR.

b) **Description:** One or multiple of the underlying resources of the MSCS have service affecting conditions, but the MSCS is still operational.

c) **Managed object type:** Mscs.

d) **Event type:** The event type associated to the probable cause as specified in table 7.5.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.5.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network node, network edge point or network link.

7.5.5 MSCS_CRITICAL

a) **Alarm definition identifier:** MSCS_CRITICAL.

b) **Description:** One or multiple of the underlying resources of the MSCS has service affecting conditions and the MSCS is not fully operational.

c) **Managed object type:** Mscs.

d) **Event type:** The event type associated to the probable cause as specified in table 7.5.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.5.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network node, network edge point or network link.

7.5.6 MSNC_WARNING

a) **Alarm definition identifier:** MSNC_WARNING.

b) **Description:** One or multiple of the underlying resources of the MSNC have potential impeding service impacts, but the MSNC is still operational.

c) **Managed object type:** Msnc.

d) **Event type:** The event type associated to the probable cause as specified in table 7.5.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.5.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the identifier of the MSNC associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network node, network edge point or network link.

7.5.7 MSNC_MINOR

a) **Alarm definition identifier:** MSNC_MINOR.

b) **Description:** One or multiple of the underlying resources of the MSNC are experimenting non-service affecting fault conditions and the MSNC has non-service affecting fault conditions.

c) **Managed object type:** Msnc.

d) **Event type:** The event type associated to the probable cause as specified in table 7.5.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.5.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the identifier of the MSNC associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network node, network edge point or network link.

7.5.8 MSNC_MAJOR

a) **Alarm definition identifier:** MSNC_MAJOR.

b) **Description:** One or multiple of the underlying resources of the MSNC have service affecting conditions, but the MSNC is still operational.

c) **Managed object type:** Msnc.

d) **Event type:** The event type associated to the probable cause as specified in table 7.5.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.5.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the identifier of the MSNC associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network node, network edge point or network link.

7.5.9 MSNC_CRITICAL

a) **Alarm definition identifier:** MSNC_CRITICAL.

b) **Description:** One or multiple of the underlying resources of the MSNC have service affecting conditions and the MSNC is not fully operational.

c) **Managed object type:** Msnc.

d) **Event type:** The event type associated to the probable cause as specified in table 7.5.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.5.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the identifier of the MSNC associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying network node, network edge point or network link.

7.6 Alarms produced by CCM

7.6.1 Common definitions

7.6.1.1 Probable causes and fault details

Table 7.6.1.1-1 specifies probable causes and fault details that can be associated to alarms produced by CCM applicable to the relevant managed object types.

NOTE: Entries in table 7.6.1.1-1 are ordered alphabetically per "probable cause".

Table 7.6.1.1-1: Probable causes on alarms produced by CCM

Probable cause	Description	Event type	Managed object types
CERTIFICATE_EXPIRATION	Event related to expiration of certificate(s) for the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage
CIS_CLUSTER_COMMUNICATION	Event related to the communication within the CIS cluster between CIS cluster nodes (e.g. between CISM and CIS instances).	COMMUNICATIONS_ALARM	CisCluster
CPU_BUS	Event related to buses of a CPU resource associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode See note 1
CPU_CONFIGURATION	Configuration related event or state change on a CPU resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
CPU_DOWN	CPU resource associated to the managed object is down/not available.	EQUIPMENT_ALARM	CisClusterNode See note 1
CPU_PROTOCOL	Event related to CPU protocol, e.g. initialization procedure, state transitions, etc., on a CPU resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
CPU_TEMPERATURE	Event related to the temperature on a CPU resource associated to the managed object.	ENVIRONMENTAL_ALARM	CisClusterNode See note 1
CPU_THROTTLING	Throttling related event or state change on a CPU resource associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode See note 1
HOST_OS_ERROR	Event related to processing failure in the host OS of the CIS cluster node.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
MCCO_CONFIGURATION	Event related to a configuration of the MCCO instance applied on the CIS cluster.	PROCESSING_ERROR_ALARM	Mcco
MCCO_CONTROLLER	Event related to malfunctioning of the controller part of an MCCO instance applied on the CIS cluster.	PROCESSING_ERROR_ALARM	Mcco
MCCO_RESOURCE	Event related to the resources realizing the MCCO instance.	EQUIPMENT_ALARM	Mcco
MEMORY_BIT_ERROR	Event related to single/multiple bit errors of the memory resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
MEMORY_CONFIGURATION	Event related to configuration of the memory resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
MEMORY_ECC	Event related to changes in states or rates concerning Error Correction Code (ECC) of the memory resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
MEMORY_REDUNDANCY	Event related to redundancy configuration of the memory resource associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode See note 1
MEMORY_STATE	Event related to change of state on the memory resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
MEMORY_TEMPERATURE	Event related to the temperature of memory resource associated to the managed object.	ENVIRONMENTAL_ALARM	CisClusterNode See note 1
NETWORK_CONFIGURATION	Event related to configuration issues with a network resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNetwork

Probable cause	Description	Event type	Managed object types
NETWORK_CONNECTVITY_SIGNAL	Event related to loss or changes in the connectivity signal provided/supported by a network resource associated to the managed object.	COMMUNICATIONS_ALARM	CisClusterNetwork
NETWORK_CPU_OVERLOAD	Event related to overload in the CPU/compute subsystems of a network resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNetwork
NETWORK_MEMORY_OVERLOAD	Event related to overload in the memory subsystems of a network resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNetwork
NETWORK_OVERLOAD	Event related to overload network input/output on a network resource associated to the managed object.	QOS_ALARM	CisClusterNetwork
NETWORK_PACKET_LOSS	Event related to packet loss experienced on a network resource associated to the managed object.	COMMUNICATIONS_ALARM	CisClusterNetwork
NETWORK_QOS	Event related to degradation of QoS levels of a network resource associated to the managed object, such as jitter and delay degradation.	QOS_ALARM	CisClusterNetwork
NFVI_COMPONENT_MAINTENANCE	Event related to maintenance of an NFVI component associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode
NFVI_COMPONENT_POWER_OUTAGE	Event related to power outage of an NFVI component.	EQUIPMENT_ALARM	CisClusterNode
NIC_CABLE	Event related to cabling/connection of the network interface associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode See note 1
NIC_CONFIGURATION	Event related to a configuration of the network interface associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
NIC_DOWN	Event related to the NIC associated to the managed object is down/not available.	EQUIPMENT_ALARM	CisClusterNode See note 1
NIC_LINK_DOWN	Event related to a link down on the network interface associated to the managed object.	COMMUNICATIONS_ALARM	CisClusterNode See note 1
NIC_LINK_TUNING	Event related to link tuning of the network interface associated to the managed object.	COMMUNICATIONS_ALARM	CisClusterNode See note 1
NIC_PCI_ERROR	Event related to a component of a Peripheral Component Interconnect (PCI) device of the network interface associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode See note 1
NIC_PCI_PARITY_ERROR	Event related to PCI parity errors of the network interface associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
NIC_PCIE_ERROR	Event related to a component of a PCI Express (PCIE) device of the network interface associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode See note 1
NIC_RECEIVE_FAILURE	Event related to errors in the reception of packet/frames by the network interface associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode See note 1
NIC_TRANSMIT_FAILURE	Event related to errors in the transmission of packet/frames by the network interface associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode See note 1

Probable cause	Description	Event type	Managed object types
NODE_DOWN	Event related to the virtual compute or bare-metal machine associated to the managed object is down/not available.	EQUIPMENT_ALARM	CisClusterNode See note 1
PROCESSOR_SENSOR	Sensor related event or state change on a processor resource associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode See note 1
STORAGE_BIT_ERROR	Event related to single/multiple bit errors on the storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_BLOCK_ERROR	Event related to bad blocks on the storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_CACHE	Event related to the cache of the storage resource associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_CAPACITY	Event related to capacity (such as shortage) of the storage resource associated to the managed object.	QOS_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_CHECK	Event related to consistency checks on a storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_COMMUNICATION	Event related to the communication to/from the storage resource associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_CONFIGURATION	Event related to the configuration of the storage associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_CONTROLLER	Event related to the controller of the storage resource associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_DOWN	Storage resource associated to the managed object is down/not available.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_DRIVE_ARRAY	Event related to storage's drive array associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_ECC	Event related to changes in states or rates concerning Error Correction Code (ECC) of the storage or memory resources associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_ENCLOSURE	Event related to the enclosure of the storage resource associated to the managed object.	ENVIRONMENTAL_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_FAILURE_PREDICTION	Event related to a predictive failure confirmed on a storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2

Probable cause	Description	Event type	Managed object types
STORAGE_MEMORY	Event related memory resources of the storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_PHYSICAL_DISK_DEGRADED	Event related to the performance on a physical disk resource associated to the managed object.	QOS_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_PHYSICAL_DISK_STATE	The state has changed on a physical disk resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_POWER	Event related to power supply and/or power status of the storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_REBUILD	Event related to the rebuild process of the storage resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_REDUNDANCY	Event related to redundancy configuration of the storage resource associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_SCSI	Event related to the Small Computer System Interface (SCSI) of the storage resource associated to the managed object type.	EQUIPMENT_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_SENSOR	Event or state change related to sensor of the storage resource associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_SMART	Event related to the Self-Monitoring Analysis and Reporting Technology (SMART) feature of the storage resource associated to the managed object.	EQUIPMENT_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_TEMPERATURE	Event related to the temperature of the storage resource associated to the managed object.	ENVIRONMENTAL_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_VIRTUAL_DISK_DEGRADED	Event related to the performance on a virtual disk resource associated to the managed object.	QOS_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
STORAGE_VIRTUAL_DISK_STATE	The state has changed on a virtual disk resource associated to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode CisClusterStorage See notes 1 and 2
SW_CISI_NODE	Event related to malfunctioning of the software supporting and (partially) realizing the CIS instance.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
SW_CISM_API	Event related to malfunctioning of API related components of the software supporting and (partially) realizing the CISM instance.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1
SW_CISM_DB	Event related to malfunctioning of database components of the software supporting and (partially) realizing the CISM instance.	PROCESSING_ERROR_ALARM	CisClusterNode See note 1

Probable cause	Description	Event type	Managed object types
SYSTEM_LICENSE_EXPIRATION	Event related to expiration of a license applicable to the managed object.	PROCESSING_ERROR_ALARM	CisClusterNode
NOTE 1: The probable cause for CisClusterNode is applicable to both virtual compute and bare-metal CIS cluster node. NOTE 2: If an alarm is raised associated to a CisClusterNode, the failure relates to the storage resources "local" to the node, and not as exposed via CisClusterStorage managed object.			

7.6.2 CISCLUSTER_WARNING

a) **Alarm definition identifier:** CISCLUSTER_WARNING.

b) **Description:** One or multiple of the underlying resources of the CIS cluster have potential impeding service impacts, but the CIS cluster is still operational.

c) **Managed object type:** CisCluster.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.6.3 CISCLUSTER_MINOR

a) **Alarm definition identifier:** CISCLUSTER_MINOR.

b) **Description:** One or multiple of the underlying resources of the CIS cluster are experimenting non-service affecting fault conditions and the CIS cluster has non-service affecting fault conditions.

c) **Managed object type:** CisCluster.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.6.4 CISCLUSTER_MAJOR

a) **Alarm definition identifier:** CISCLUSTER_MAJOR.

b) **Description:** One or multiple of the underlying resources of the CIS cluster have service affecting conditions, but the CIS cluster is still operational.

c) **Managed object type:** CisCluster.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.6.5 CISCLUSTER_CRITICAL

a) **Alarm definition identifier:** CISCLUSTER_CRITICAL.

b) **Description:** One or multiple of the underlying resources of the CIS cluster has service affecting conditions and the CIS cluster is not fully operational.

c) **Managed object type:** CisCluster.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.6.6 CISCLUSTERNODE_WARNING

a) **Alarm definition identifier:** CISCLUSTERNODE_WARNING.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster node have potential impeding service impacts, but the CIS cluster node is still operational.

c) **Managed object type:** CisClusterNode.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster node instance id associated to the issue.

- "cisiId=$cisiId", wherein "$cisiId" indicates the CIS instance identifier, in case the CIS cluster node is a CIS instance.
- "cismId=$cismId", wherein "$cismId" indicates the CISM instance identifier, in case the CIS cluster node is a CISM instance.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.7 CISCLUSTERNODE_MINOR

a) **Alarm definition identifier:** CISCLUSTERNODE_MINOR.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster node are experimenting non-service affecting fault conditions and the CIS cluster node has non-service affecting fault conditions.

c) **Managed object type:** CisClusterNode.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster node instance id associated to the issue.
- "cisiId=$cisiId", wherein "$cisiId" indicates the CIS instance identifier, in case the CIS cluster node is a CIS instance.
- "cismId=$cismId", wherein "$cismId" indicates the CISM instance identifier, in case the CIS cluster node is a CISM instance.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.8 CISCLUSTERNODE_MAJOR

a) **Alarm definition identifier:** CISCLUSTERNODE_MAJOR.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster node have service affecting conditions, but the CIS cluster node is still operational.

c) **Managed object type:** CisClusterNode.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster node instance id associated to the issue.
- "cisiId=$cisiId", wherein "$cisiId" indicates the CIS instance identifier, in case the CIS cluster node is a CIS instance.

- "cismId=$cismId", wherein "$cismId" indicates the CISM instance identifier, in case the CIS cluster node is a CISM instance.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.9 CISCLUSTERNODE_CRITICAL

a) **Alarm definition identifier:** CISCLUSTERNODE_CRITICAL.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster node has service affecting conditions and the CIS cluster node is not fully operational.

c) **Managed object type:** CisClusterNode.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster node instance id associated to the issue.
- "cisiId=$cisiId", wherein "$cisiId" indicates the CIS instance identifier, in case the CIS cluster node is a CIS instance.
- "cismId=$cismId", wherein "$cismId" indicates the CISM instance identifier, in case the CIS cluster node is a CISM instance.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.10 CISCLUSTERSTORAGE_WARNING

a) **Alarm definition identifier:** CISCLUSTERSTORAGE_WARNING.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster storage resource have potential impeding service impacts, but the CIS cluster storage resource is still operational.

c) **Managed object type:** CisClusterStorage.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster storage resource instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.11 CISCLUSTERSTORAGE_MINOR

a) **Alarm definition identifier:** CISCLUSTERSTORAGE_MINOR.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster storage resource are experimenting non-service affecting fault conditions and the CIS cluster storage resource has non-service affecting fault conditions.

c) **Managed object type:** CisClusterStorage.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster storage resource instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.12 CISCLUSTERSTORAGE_MAJOR

a) **Alarm definition identifier:** CISCLUSTERSTORAGE_MAJOR.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster storage resource have service affecting conditions, but the CIS cluster storage resource is still operational.

c) **Managed object type:** CisClusterStorage.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster storage resource instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.13 CISCLUSTERSTORAGE_CRITICAL

a) **Alarm definition identifier:** CISCLUSTERSTORAGE_CRITICAL.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster storage resource has service affecting conditions and the CIS cluster storage resource is not fully operational.

c) **Managed object type:** CisClusterStorage.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster storage resource instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.14 CISCLUSTERNETWORK_WARNING

a) **Alarm definition identifier:** CISCLUSTERNETWORK_WARNING.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster network resource have potential impeding service impacts, but the CIS cluster network resource is still operational.

c) **Managed object type:** CisClusterNetwork.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster network resource instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.15 CISCLUSTERNETWORK_MINOR

a) **Alarm definition identifier:** CISCLUSTERNETWORK_MINOR.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster network resource are experimenting non-service affecting fault conditions and the CIS cluster network resource has non-service affecting fault conditions.

c) **Managed object type:** CisClusterNetwork.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster network resource instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.16 CISCLUSTERNETWORK_MAJOR

a) **Alarm definition identifier:** CISCLUSTERNETWORK_MAJOR.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster network resource have service affecting conditions, but the CIS cluster network resource is still operational.

c) **Managed object type:** CisClusterNetwork.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster network resource instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.17 CISCLUSTERNETWORK_CRITICAL

a) **Alarm definition identifier:** CISCLUSTERNETWORK_CRITICAL.

b) **Description:** One or multiple of the underlying resources or software of the CIS cluster network resource has service affecting conditions and the CIS cluster network resource is not fully operational.

c) **Managed object type:** CisClusterNetwork.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the CIS cluster network resource instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.18 MCCO_WARNING

a) **Alarm definition identifier:** MCCO_WARNING.

b) **Description:** One or multiple of the underlying resources or software of the MCCO instance have potential impeding service impacts, but the MCCO instance is still operational.

c) **Managed object type:** Mcco.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the MCCO instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.19 MCCO_MINOR

a) **Alarm definition identifier:** MCCO_MINOR.

b) **Description:** One or multiple of the underlying resources or software of the MCCO instance are experimenting non-service affecting fault conditions and the MCCO instance has non-service affecting fault conditions.

c) **Managed object type:** Mcco.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the MCCO instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.20 MCCO_MAJOR

a) **Alarm definition identifier:** MCCO_MAJOR.

b) **Description:** One or multiple of the underlying resources or software of the MCCO instance have service affecting conditions, but the MCCO instance is still operational.

c) **Managed object type:** Mcco.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the MCCO instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.6.21 MCCO_CRITICAL

a) **Alarm definition identifier:** MCCO_CRITICAL.

b) **Description:** One or multiple of the underlying resources or software of the MCCO instance has service affecting conditions and the MCCO instance is not fully operational.

c) **Managed object type:** Mcco.

d) **Event type:** The event type associated to the probable cause as specified in table 7.6.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.6.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "instanceId=$instanceId", wherein "$instanceId" indicates the MCCO instance id associated to the issue.
- "resourceId=$resourceId", wherein "$resourceId" indicates the identifier of the underlying compute, storage and/or network resource associated to the issue.

7.7 Alarms produced by CISM

7.7.1 Common definitions

7.7.1.1 Probable causes and fault details

Table 7.7.1.1-1 specifies probable causes and fault details that can be associated to alarms produced by CISM applicable to the relevant managed object types.

NOTE: Entries in table 7.7.1.1-1 are ordered alphabetically per "probable cause".

Table 7.7.1.1-1: Probable causes on alarms produced by CISM

Probable cause	Description	Event type	Managed object types
CISI_SCHEDULER	Event related to issues with the workload scheduler of the CIS instance.	PROCESSING_ERROR_ALARM	Cisi
MCIO-C_STATE	Event related to error states on the set of OS containers realizing an MCIO-C.	PROCESSING_ERROR_ALARM	Mcio-c
SW_CISI_CPU	Event related to CPU utilization issues corresponding to the software realizing the CIS instance.	PROCESSING_ERROR_ALARM	Cisi
SW_CISI_DISK	Event related to disk space issues corresponding to the software realizing the CIS instance.	PROCESSING_ERROR_ALARM	Cisi
SW_CISI_MEM	Event related to memory utilization issues corresponding to the software realizing the CIS instance.	PROCESSING_ERROR_ALARM	Cisi
SW_CISI_SERVICE	Event related to errors establishing connectivity and/or service to the CIS instance.	PROCESSING_ERROR_ALARM	Cisi

7.7.2 CISI_WARNING

a) **Alarm definition identifier:** CISI_WARNING.

b) **Description:** One or multiple of the underlying resources or software components of the CISI have potential impeding service impacts, but the CISI is still operational.

c) **Managed object type:** Cisi.

d) **Event type:** The event type associated to the probable cause as specified in table 7.7.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.7.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.7.3 CISI_MINOR

a) **Alarm definition identifier:** CISI_MINOR.

b) **Description:** One or multiple of the underlying resources or software components of the CISI are experimenting non-service affecting fault conditions and the CISI has non-service affecting fault conditions.

c) **Managed object type:** Cisi.

d) **Event type:** The event type associated to the probable cause as specified in table 7.7.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.7.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.7.4 CISI_MAJOR

a) **Alarm definition identifier:** CISI_MAJOR.

b) **Description:** One or multiple of the underlying resources or software components of the CISI have service affecting conditions, but the CISI is still operational.

c) **Managed object type:** Cisi.

d) **Event type:** The event type associated to the probable cause as specified in table 7.7.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.7.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.7.5 CISI_CRITICAL

a) **Alarm definition identifier:** CISI_CRITICAL.

b) **Description:** One or multiple of the underlying resources or software components of the CISI has service affecting conditions and the CISI is not fully operational.

c) **Managed object type:** Cisi.

d) **Event type:** The event type associated to the probable cause as specified in table 7.7.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.7.1.1-1 for the applicable managed object type.

g) **Fault details:** None defined.

7.7.6 MCIOC_WARNING

a) **Alarm definition identifier:** MCIOC_WARNING.

b) **Description:** One or multiple of the underlying resources or components of the compute MCIO have potential impeding service impacts, but the MCIO-C is still operational.

c) **Managed object type:** Mcio-c.

d) **Event type:** The event type associated to the probable cause as specified in table 7.7.1.1-1.

e) **Perceived severity:** WARNING.

f) **Probable cause:** One of the probable causes specified in table 7.7.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "mcio_state=$mcio_state", wherein "$mcio_state" indicates the specific state of the MCIO-C.

7.7.7 MCIOC_MINOR

a) **Alarm definition identifier:** MCIOC_MINOR.

b) **Description:** One or multiple of the underlying resources or components of the compute MCIO are experimenting non-service affecting fault conditions and the MCIO has non-service affecting fault conditions.

c) **Managed object type:** Mcio-c.

d) **Event type:** The event type associated to the probable cause as specified in table 7.7.1.1-1.

e) **Perceived severity:** MINOR.

f) **Probable cause:** One of the probable causes specified in table 7.7.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "mcio_state=$mcio_state", wherein "$mcio_state" indicates the specific state of the MCIO-C.

7.7.8 MCIOC_MAJOR

a) **Alarm definition identifier:** MCIOC_MAJOR.

b) **Description:** One or multiple of the underlying resources or components of the compute MCIO have service affecting conditions, but the MCIO is still operational.

c) **Managed object type:** Mcio-c.

d) **Event type:** The event type associated to the probable cause as specified in table 7.7.1.1-1.

e) **Perceived severity:** MAJOR.

f) **Probable cause:** One of the probable causes specified in table 7.7.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "mcio_state=$mcio_state", wherein "$mcio_state" indicates the specific state of the MCIO-C.

7.7.9 MCIOC_CRITICAL

a) **Alarm definition identifier:** MCIOC_CRITICAL.

b) **Description:** One or multiple of the underlying resources or components of the compute MCIO has service affecting conditions and the MCIO is not fully operational.

c) **Managed object type:** Mcio-c.

d) **Event type:** The event type associated to the probable cause as specified in table 7.7.1.1-1.

e) **Perceived severity:** CRITICAL.

f) **Probable cause:** One of the probable causes specified in table 7.7.1.1-1 for the applicable managed object type.

g) **Fault details:** Depending on the value of the probable cause, zero, one or multiple occurrences of the following strings:

- "mcio_state=$mcio_state", wherein "$mcio_state" indicates the specific state of the MCIO-C.

Annex A (informative): Use cases

A.1 Use cases about FM alarms

A.1.1 Overview

Clause A.1 documents use cases guiding the identification of the scope and potential types of alarms to be considered in NFV-MANO. The use cases also identify the association of alarms to specific NFV-MANO managed objects.

A.1.2 Use cases about FM alarms associated to virtualised resources and containerized workloads

A.1.2.1 Monitoring of NFVI resources faults and generation of alarms

NFVI-nodes are the physical devices deployed and managed as a single entity, which provide the NFVI functions to support the execution environment for VNFs, as defined in ETSI GR NFV 003 [i.1]. In addition, the NFVI-nodes are interconnected to other various facility infrastructure elements such as cooling systems, power plants and distribution, cables, racks, etc. Clause 4 of ETSI GS NFV-EVE 007 [i.11] describes the various types of hardware elements conforming the NFVI and the infrastructure facilities. Figure A.1.2.1-1 illustrates a high-level diagram of the NFVI and its composition.

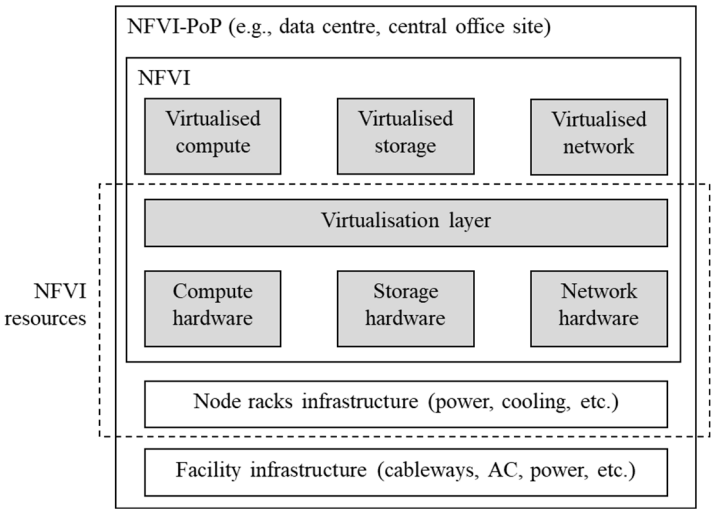

Figure A.1.2.1-1: NFVI and high-level composition

Figure A.1.2.1-1 also illustrates the scope of "NFVI resources" considered in the present use case, which include virtualisation layer, compute/storage/network hardware and node racks infrastructure which support the enclosure, power, cooling of the installed hardware in the NFVI-PoP.

VNF instances are conformed of VNFC instances and internal VLs that are deployed using compute, storage and network virtualised resources. The virtualised resources are in turn allocated within the NFVI and make use of underlying hardware and software infrastructure. Due to this dependency on the underlying NFVI resources, faults occurring in the NFVI, and its composed resources can impact the behaviour and service fulfilment of the virtualised resources and containerized workloads towards the VNF normal operation.

Network operators and equipment suppliers are thus interested in monitoring faults of NFVI resources, so that faults that can impact the virtualised resources and containerized workloads allocated to the VNF and NS are identified, and corresponding alarms raised. This enables operators or management systems acting upon such alarms and performing actions to resolve the faults or minimize their impacts.

Considering the above, faults can be associated to various types of NFVI resources:

- CPU: for instance, machine check exceptions, bus parity errors, configuration errors in processing units, etc.
- Memory: for instance, read/write errors in memory modules, spare redundancy loss, etc.
- Disk and drives: examples include read/write errors of storage devices, loss of sync, loss of redundancy, disk cache subsystems, faults in logical and physical storage drives, array controllers, and faults on sub-systems related to power as batteries, backup power, etc.
- NIC: examples include faults on network interface or adapter cards, such as loss of connectivity, redundancy, PCI system and parity errors, etc.
- Power: faults and exceptions related to power supply systems and their redundancy, disconnection from power supply systems, errors in the power supply sensors, and power-related faults on equipment such as compute servers, etc.
- Fan: examples include changes in the states of the tolerant fans, their redundancy, removal or issues in their enclosure, revolution per minute changes under/above certain thresholds, etc.
- Temperature: examples include the changes of temperature of certain systems, e.g. servers, to levels outside normal operating range, faults in the temperature sensors, etc.
- Software: examples include software subsystems such as the operating system on a host, the hypervisor software, etc.
- Other or miscellaneous: for instances faults related to the lack of connectivity of management systems towards the NFVI resources, such as host servers.

Furthermore, depending on the conditions and impact of the fault on the NFVI resource, different severity levels can be applied. Taking disk (storage) type resources for instance, on the one hand, a degradation of the physical or virtual disk could be raised as a warning, with the assumption that such degradation does not impact read/write operations of applications making use of such disk. On the other hand, a virtual disk bad block error, which can impact read/write operations of an application, could be raised as a critical failure.

Since the number of resource types in the NFVI and the number of faults applicable to each of them can be great, it is expected that fault and alarm modelling enables the network operator and equipment suppliers to categorize relevant faults into standard fault types. The standard fault types can then be correlated to specific faults to be raised associated to virtualised resources. Figure A.1.2.1-2 illustrates an example of the consolidation of raw faults on NFVI resources to a set of "L" standard fault types.

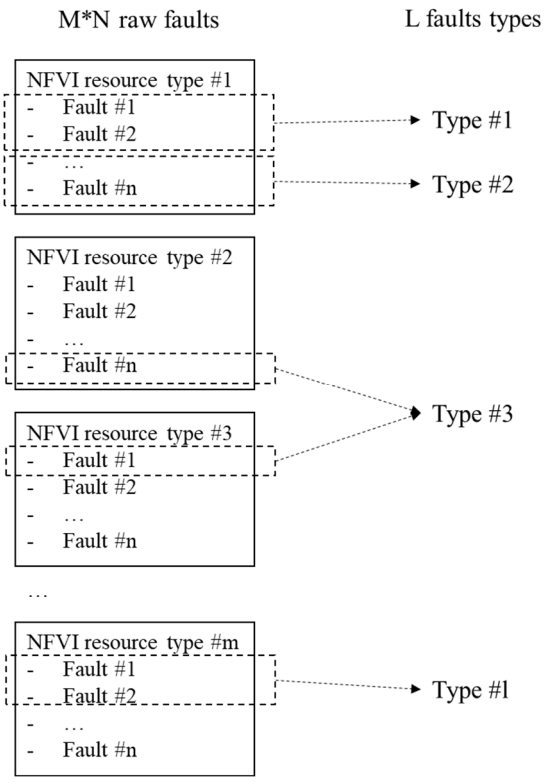

Figure A.1.2.1-2: Faults consolidation

It is assumed in the figure that "M*N" is greater than "L". The fault consolidation process can be based on (not an exhaustive list):

- Dimension #A: a set of faults on different NFVI resource types have similar severity impact on same types of virtualised resources. For instance, a fault on CPU and a fault on memory have critical severity level and deliver a similar impact on virtualised resources.
- Dimension #B: a set of faults associated to same NFVI resource type impact a specific subsystem of the virtualised resources. For instance, two or more faults of a server/host in the NFVI are related to CPU which particularly affect the virtual CPU subsystem of the virtualised compute resource.
- Dimension #C: a set of faults associated to different NFVI resource types impact a specific subsystem of the virtualised resources. For instance, a temperature related fault on CPU and a fault related to the fan cooling the server can be regarded to introduce a performance degradation to the virtual CPU subsystem of the virtualised compute resource.
- A combination of dimensions, e.g. combining aspects of dimension #A and dimension #C.

A.1.2.2 Monitoring of virtualised resources of VM-based VNFC/VNF and generation of alarms

As described in clause A.1.2.1, VNF instances are conformed of VNFC instances and internal VLs that are deployed using compute, storage and network virtualised resources. NS instances constituents such as NS VL are also deployed using network virtualised resources.

The types of virtualised resources are defined ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5]. In the referred specifications, three main types of consumable virtualised resources are defined as well as relevant attributes that model subsystems of them. Table A.1.2.2-1 provides a summary of the different types of virtualised resources derived from the modelling in the referenced specifications.

Table A.1.2.2-1: Virtualised resource types and subsystems

Virtualised resource	Subsystems	Additional comments (if any)
Virtual compute	Virtual memory	
	Virtual CPU	
	Acceleration	
	Virtual network interface	
	Virtual disk	
Virtual storage	n/a	Virtual storage can be of different types: volume, object, or block.
Virtual network	Network subnet	
	Virtual network port	Virtual ports can be sub-ports or trunk ports, in case of trunking.
	Routing resource	Logical network resource that provides routing capabilities between different virtualised network resources.

Network operators and VNF providers are interested in monitoring faults associated to the virtualised resources and corresponding alarms be raised by the VIM, so that faults that can impact the VNF are identified. This enables network operators and the VNFM to act upon such alarms and perform actions to resolve the faults or minimize their impact on the VNF's normal operation.

For this purpose, as specified in ETSI GS NFV-IFA 005 [i.4] and ETSI GS NFV-IFA 006 [i.5], the Virtualised Resource Fault Management interface enables the VIM providing alarms result from the faults related to the virtualised resources visible to the consumer functional block, the NFVO and VNFM, respectively.

NOTE: The referred Virtualised Resource Fault Management interface also describes that faults related to other managed objects other than virtualised resources, such as resource reservations, can also be exposed through the interface. However, these are not considered in the present use case, as not being specifically associated to virtualised resources used by a VNF.

As introduced in clause A.1.2.1, the number of faults in the NFVI that can impact virtualised resources is great. Exposing this level of fault details to the consumers of the virtualised resources management (VNFM and NFVO) is not feasible, also because the consumer is not aware of the full details of how the NFVI is designed and deployed. In this scenario, the process of faults consolidation introduced in clause A.1.2.1 becomes relevant.

A.1.2.3 Monitoring of containerized workloads of container-based VNFC/VNF and generation of alarms

The containerized workloads and types of MCIO that can be used for deploying container-based VNF are defined in ETSI GS NFV-IFA 040 [i.12]. Regarding the compute MCIO, being a concrete form of it the "group of one or more OS containers" (e.g. a Pod in the case of Kubernetes®), the flow of monitoring and generation of alarms can follow the following schema, as depicted in figure A.1.2.3-1.

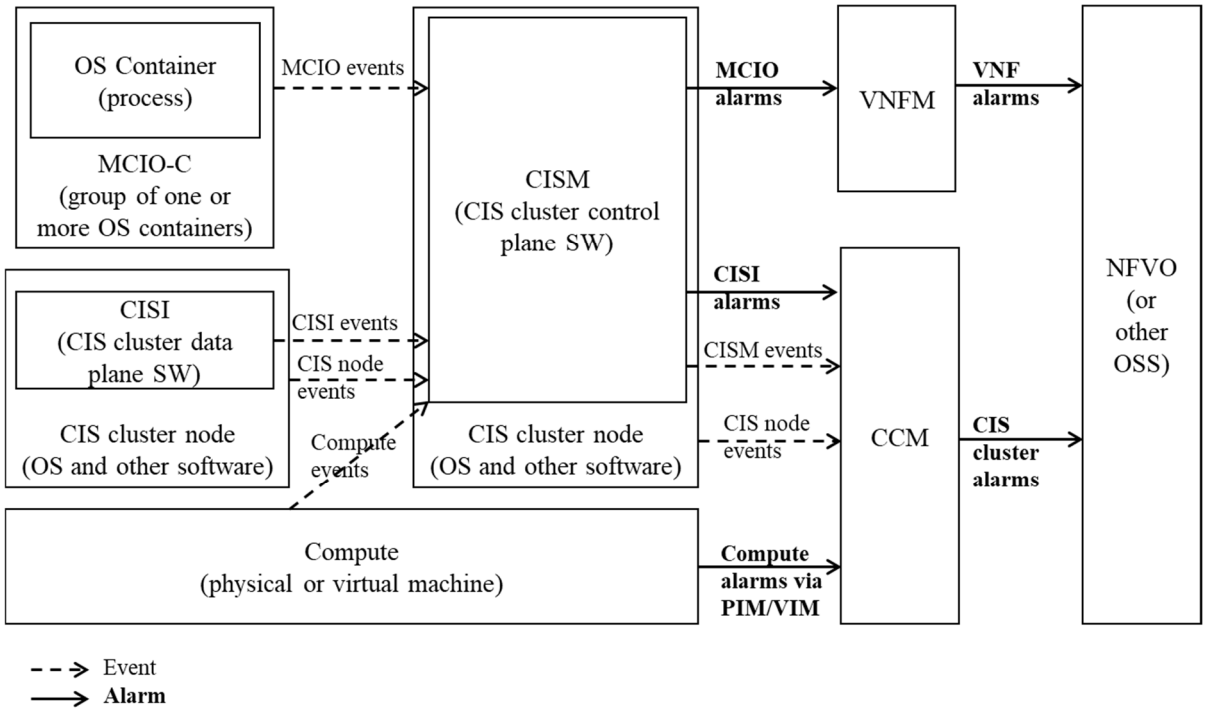

Figure A.1.2.3-1: Flow of monitoring and generation of alarms concerning container-based VNFC/VNF

NOTE 1: MCCO, CIS cluster storage and network are not depicted in figure A.1.2.3-1 to simplify the illustration.

Figure A.1.2.3-1 represents three main aspects concerning the monitoring of containerized workloads of container-based VNFC/VNF and the generation of relevant alarms:

- Alarms concerning CIS cluster, on which the containerized workloads are deployed.
- Alarms concerning the containerized workloads.
- Alarms concerning VNF/VNFC.

The alarms concerning the CIS cluster are produced by the CCM. These alarms can be created based on events monitored from the CIS cluster nodes, the CISM, as well as based on defined alarms related to CIS instances and physical and virtual compute resources provided by infrastructure managers such as the VIM.

NOTE 2: Specification of physical infrastructure management (PIM) cannot be referenced in the present document version, and it is only shown in the figure for illustrative purposes to cover the case of bare-metal CIS clusters.

CISM produces alarms concerning the CIS instances, as managed objects. To generate such alarms, the CISM monitors events related to CIS instances, based on the events monitored from the CIS cluster data plane software, events from the CIS cluster node through the OS and other software conforming the CIS cluster node, and events about the compute resources (physical or virtual). For the different layers of events monitoring, CISM can leverage specialized software that is either part of or complementary to the CIS cluster control plane software building the CISM.

Regarding the alarms associated to containerized workloads, the CISM produces specified alarms associated to compute MCIOs. The CISM builds such alarms by correlating various sources, such as MCIO events, CIS instance events, CIS node events and compute events.

Finally, in the case of a container-based VNF, the VNFM is able to generate VNF alarms based on the collection of MCIO alarms concerning the containerized workloads.

NOTE 3: The present document version does not specify the path (i.e. from which NFV-MANO functional block or function) and alarm/event correlation point by which the VNFM can learn about the events or alarms to associate compute, storage and network resource related probable causes to a containerized VNFC. Possible options to be considered include (not an exhaustive list): CISM to perform the correlation against MCIO alarms, or the VNFM to perform the correlation of MCIO alarms from the CISM with CIS cluster related alarms or events.

A.1.2.4 Use case about packet loss alarm

Packet loss alarm is a typical type of alarm. For example, the VIM receives several performance metrics from NFVI (e.g. depending on the type of vNIC, this can be associated to a virtual function in a physical NIC) to calculate the packet loss rate of a vNIC and then compares it with the pre-defined threshold. If the threshold is crossed, the VIM generates a vNIC packet loss alarm.

The perceived severity of this alarm could be determined depending on the threshold. For instance, if the value is less than 10 %, the perceived severity is major; if the value is greater than 10 %, the perceived severity is critical. Moreover, there are several types of probable causes of this alarm. See note 1.

A) Probable causes specific to software:

   1) overload of network I/O;

   2) insufficient CPU resource for forwarding; and

   3) suboptimal network configuration.

B) Probable causes specific to hardware:

   1) malfunctioning physical network interface card.

NOTE 1: The probable causes listed above are informative and not exhaustive.

By including the information described above into the alarm information element of an alarm, the NFV-MANO functional blocks could solve them (e.g. by policies) or report this alarm to OSS/BSS for resolutions. To assist NFV-MANO and OSS/BSS to solve this alarm, the information related to probable causes could also be included. See note 2.

i) Additional information for probable causes specific to software:

   1) information related to the number of packets of network input and output could be included to determine the pressure of network I/O;

   2) information related to the number of the CPUs used and the corresponding names, usage rates could be included to determine the CPU resource sufficiency; and

   3) information related to the configuration data (e.g. the name and type of the vNIC, the corresponding IP address and MAC address, etc.) could be included to determine the correctness of the configuration.

ii) Additional information for probable causes specific to hardware:

   1) information related to physical resources (e.g. the host ID, the host name, etc.) could be included to assist the OSS/BSS to locate the corresponding physical hardware.

NOTE 2: The information listed above is informative and not exhaustive.

A.1.2.5 Use case about storage service alarm

Unavailable storage service alarm is a common alarm type regarding various storage-related faults such as storage equipment fault, capacity shortage and data inaccessibility. For example, the VIM receives the usage of the storage resource and determines if it crosses a predefined fault threshold which can impact the availability of the storage service. If the predefined fault threshold is crossed, the VIM generates a capacity shortage alarm. Another example is about VIM not being able to access to data stored in the storage resource. In this situation, the VIM generates a storage communication or storage down related alarm.

NOTE 1: A predefined fault threshold is configured/set by means other than "PM thresholds", typically at the assembly or deployment time of the resource. PM thresholds are managed and events notified via the PM-related interfaces, while predefined fault threshold related alarms are issued via the FM-related interfaces.

Unavailable storage service alarms can apply to different types of storage resources, such as networked external storage, software-defined storage or local storage to a compute node in the NFVI.

The perceived severity of this kind of alarms could be determined for instance, based on the threshold and the type of data that cannot be accessed. For example, if the unavailable data is for a service, the perceived severity can be determined to be critical; if the unavailable data is for the NFV-MANO system (such as in databases of use by an NFV-MANO functional entity) and the system can run without impact, the perceived severity could be minor. Moreover, there are several types of probable causes of this alarm. See note 2.

A) Probable causes:

1) unbalanced data distribution due to security requirements;

2) insufficient storage capacity;

3) too many malfunctioning storage instances (at the same time) impacting storage redundancy;

4) equipment power-off;

5) abnormal network connectivity among different storage resources/equipment instances. See note 3;

6) physical equipment issue (e.g. drive malfunction, excessive temperature);

7) storage defragmentation;

8) logical volume destruction; and

9) storage software license issue.

NOTE 2: The probable causes listed above are informative and not meant to be exhaustive.

NOTE 3: There could be additional probable causes regarding to abnormal links, e.g. insufficient link capacity, insufficient CPU capacity for usage.

By including the information described above into the alarm information element of an alarm, the NFV-MANO functional blocks could solve them (e.g. by policies) or further report this alarm to OSS/BSS that the network operator or other systems can take resolution actions. To assist NFV-MANO and OSS/BSS to solve this alarm, the information related to probable causes could also be included. See note 4.

i) Additional information for probable causes that can help determine the root causes of the alarm might include:

1) information related to the security requirements could be included to determine that existing number of storage instances is not sufficient;

2) information related to the used storage capacity and the remaining capacity could be included to determine the storage resource shortage;

3) information related to storage instances, (e.g. the NFVI-PoP name, the instance name and ID, etc.) could be included to locate the corresponding physical equipment; and

4) information related to the network links connecting the different storage instances and the type of the anomaly (e.g. packet loss, delay).

NOTE 4: The information listed above is informative and not meant to be exhaustive.

A.1.2.6 Use case about network link anomaly alarm

Alarms related to network link anomalies can be categorized, among others, as equipment alarms such as when the issue concerns to the cabling. Based on their severity, the link anomalies could include issues related to link breaks and link performance degradation.

The link break related alarms can be caused by hardware equipment or the physical links used to connect different equipment. The hardware equipment includes the equipment virtualised as network devices (e.g. switches, routers, ports, etc.) and the equipment (e.g. compute hardware, storage hardware, etc.) connected by network devices.

The link performance degradation related alarms include the alarms caused by high packet loss, delay, jitter, etc. Compared with link break related alarms, these alarms might have lower severities.

Since links have the responsibility to connect different equipment which run network services, alarms related to link anomaly can have relationships with other types of alarms (e.g. alarms related to equipment offline, service unavailability, etc.) and can cause several other alarms being generated at the same time.

The perceived severity of these alarms could be determined based on the caused service impacts. For example, for the alarms of link break, the services have a higher possibility to become unavailable. Therefore, the perceived severity could be critical. For the alarms of sub-health, the services have lower possibility to become unavailable but could be degraded. Therefore, the perceived severity could be major.

A) Probable causes specific to link break:

   1) removal or damage of network links; and

   2) malfunctioning of equipment (e.g. ports, optical interface modules, physical NICs, etc.).

B) Additional information for probable causes specific to link break:

   1) information related to the identifiers of links;

   2) information related to the identifiers of the equipment and the corresponding ports;

   3) information related to the identifiers of racks enclosing affected equipment; and

   4) information related to the types of alarms could be generated correspondingly (e.g. service offline related alarms, service unavailability related alarms). See note 1.

NOTE 1: There is a possibility that one type of alarms has correlation with another type of alarms. The correlation could be used for the NFV-MANO or the OSS/BSS to compress the number of the alarms and/or find the "root alarm" easily.

i) Probable causes specific to link performance degradation:

   1) overload of network I/O; and

   2) poor links's signal connection.

ii) Additional information for probable causes specific to link performance degradation:

   1) information related to the identifiers of links;

   2) information related to the identifiers of the equipment and the corresponding ports;

   3) information related to the identifiers of racks enclosing the affected equipment;

   4) information related to the details of the degradation (e.g. the specific values of jitter and delay); and

   5) information related to the types of alarms could be generated correspondingly (e.g. packet loss related alarms).

NOTE 2: The probable causes listed above are informative and not meant to be exhaustive.

NOTE 3: The additional information listed above is informative and not meant to be exhaustive.

A.1.3 Use cases about FM alarms associated to VNF

VNF instances are composed of VNFCs, internal VL and internal and external CPs. Each one of these are in turn fulfilled by various virtualised resources:

- VNFC instances typically comprise virtualised compute and storage resources, which in turn leverage physical compute and storage resources of the NFVI.

- Internal VL are realized by virtualised network resources, which in turn leverage network resources of the NFVI.
- Internal and external CP of a VNF instance are realized, in the general case, by virtual network interface cards, which are in turn supported by corresponding network interface cards on the compute resources.

The VNFM monitors the alarms received from the VIM about virtualised resources used by the VNF instance. As the VNFM is responsible for the lifecycle management of the VNF and its resources fulfilment and assurance, it can map the alarms on the virtualised resources to the corresponding VNF related managed object types.

NOTE: Currently, the ETSI GS NFV-IFA 040 [i.12], which specifies the service interfaces produced by the CISM for the management of containerized workloads, does not specify interfaces for fault management. Hence, the above statement references only to the VIM.

Figure A.1.3-1 illustrates the concept of mapping virtualised resources alarms and associated probable causes to alarms associated to VNF.

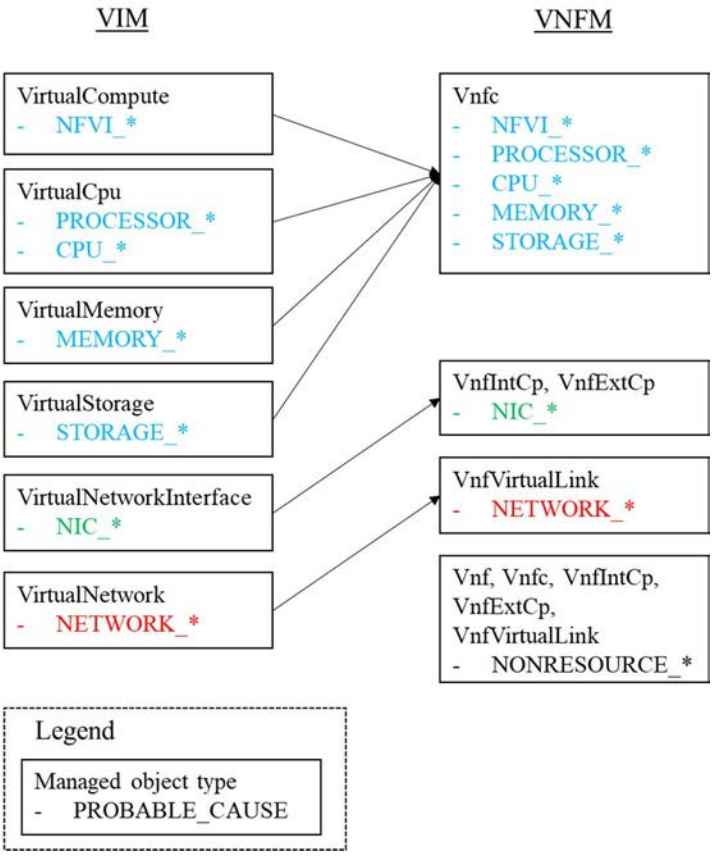

Figure A.1.3-1: Mapping of alarms, managed object types and probable causes between virtualised resources and VNF

As illustrated in the example in figure A.1.3-1:

- VNFM produces alarms on the following managed object types: VNF, VNFC, VNF internal CP, VNF external CP, VNF internal VL.
- VIM produces alarms on the following managed object types: virtual compute, virtual CPU, virtual memory, virtual storage, virtual network interface and virtual network.
- The managed object types between VIM and VNFM are mapped/related by the corresponding arrows, e.g. virtual CPU and virtual memory are part of resources realizing a VNFC.
- The probable causes with the same colour between the VIM and VNFM generated alarms are the same, i.e. the probable cause of a fault on a managed object type on the virtualised resource domain is reused as probable cause on the managed object type on the VNF domain.

- VNFM can also generate alarms with new probable causes which are not related to virtualised resources, which are indicated in the figure A.1.3-1 with the probable cause "NONRESOURCE_*".

A.1.4 Use cases about FM alarms associated to NS

NS instances are composed of VNF and PNF instances are NF constituents and NS virtual links. An NS can also contain other NS as nested constituents. NS virtual link are realized by virtualised network resources.

The NFVO monitors the alarms received from the VIM about virtualised resources and VNFM about VNF instances. As the NFVO is responsible for the lifecycle management of the NS and its resources fulfilment and assurance, it can map the alarms on the virtualised resources and VNF to the corresponding NS related managed object types.

NOTE: Currently, the ETSI GS NFV-IFA 040 [i.12], which specifies the service interfaces produced by the CISM for the management of containerized workloads, does not specify interfaces for fault management. Hence, the above statement references only to the VIM.

Figure A.1.4-1 illustrates the concept of mapping virtualised resources, VNF alarms and associated probable causes to alarms associated to NS.

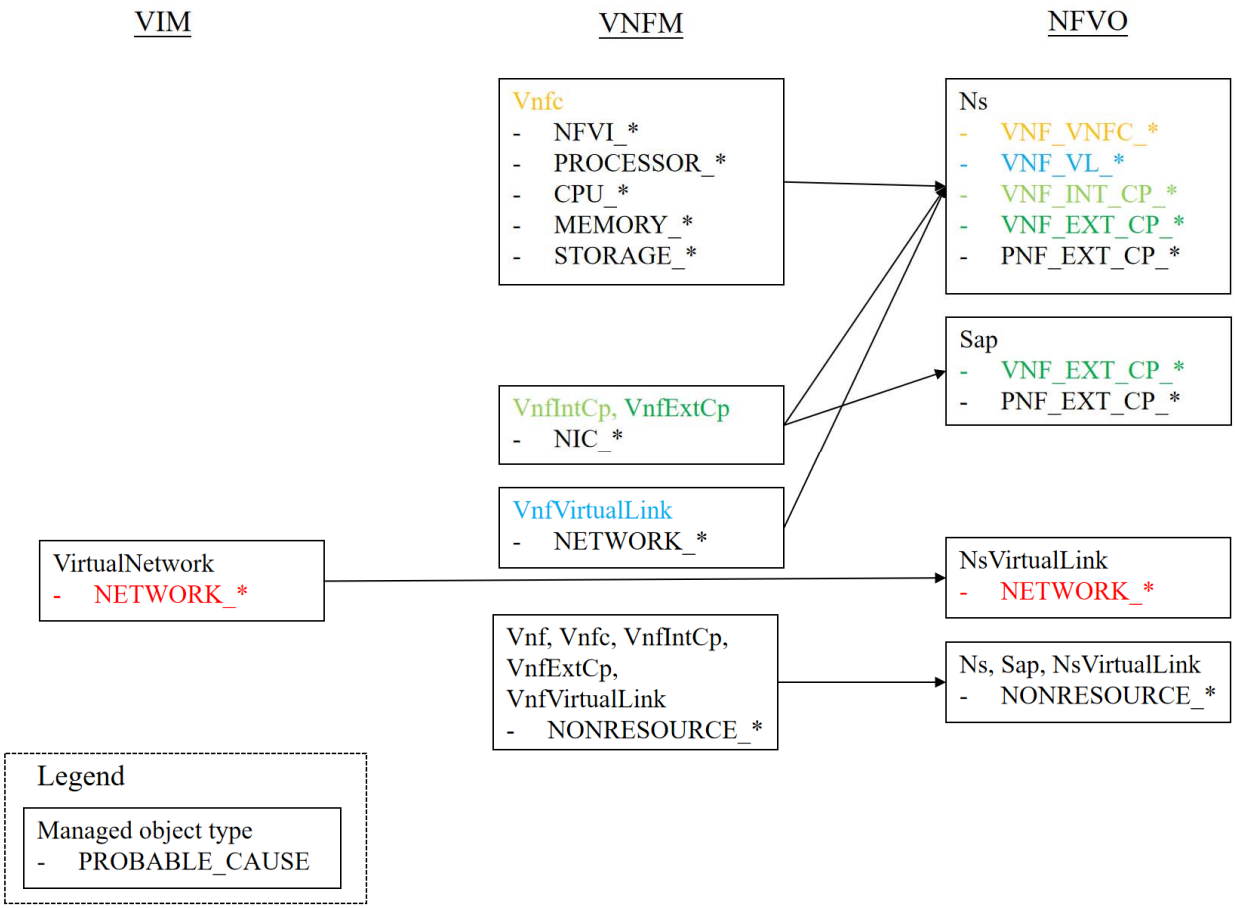

Figure A.1.4-1: Mapping of alarms, managed object types and probable causes between virtualised resources, VNF and NS

As illustrated in the example in figure A.1.4-1:

- NFVO produces alarms on the following managed object types: NS, SAP and NS VL.
- VNFM produces alarms on the following managed object types: VNF, VNFC, VNF internal CP, VNF external CP and VNF internal VL.
- VIM produces alarms on the following managed object types: virtual network.

- The managed object types between a) VIM and NFVO and b) VNFM and NFVO are mapped/related by the corresponding arrows, e.g. virtual networks are part of resources realizing an NS VL, and VNFC, VNF internal VL are part of VNF instances that as constituents of the NS.
- The probable causes for alarms on object types managed by the NFVO are related to the managed object types by the VNFM using same colour, i.e. the probable cause of fault on a managed object type on the NS domain is mapped to the managed object type on the VNF domain.
- NFVO can also generate alarms with new probable causes which are not related to virtualised resources used to build the NS parts and/or constituents, which are indicated in the figure A.1.4-1 with the probable cause "NONRESOURCE_*".

A.2 Use cases about use of Alarms information

A.2.1 Overview

Clause A.2 documents potential use cases related to how information contained in alarms can be used by NFV-MANO or the network operator, for instance, to enable root cause analysis, handling more automation, etc. Therefore, the use cases can be used to determine relevant information that the alarms are expected to contain.

A.2.2 Use case about procedure of using alarm information produced by the VIM with policies

This clause describes the informative generic procedure of how the VIM can collect and produce alarm information and how NFV-MANO can process these new alarms accordingly. The present procedure is generic and informative. The design of alarm modelling could reference the procedure.

1) The VIM monitors and collects different types of alarm information of virtualised resources.

2) The VIM processes the alarm information collected (e.g. alarm generation, alarm compression) to generate a standardized alarm associated to virtualised resources. See note 1.

3) The VIM matches the alarm generated with the policies predefined in the VIM to evaluate if the alarm triggers the policies or not. If a policy is triggered, conditions in the policy are evaluated. If the conditions are evaluated to be true, the actions defined by the policy are executed. Then, if the alarm is cleared, an alarm cleared notification is sent to the NFVO which can forward it to the OSS/BSS, as well as the VIM can send to the VNFM (if also subscribed to receive notifications), and the procedure ends. If the alarm is not cleared or no policy is executed, step 4 is executed.

4) The VIM sends an alarm notification with the standardized alarm to the NFVO and to the VNFM (if also subscribed to receive notifications) through the Virtualised Resource Fault Management Interface on the Or-Vi reference point and Vi-Vnfm reference point, respectively.

5.1) Based on the alarm information received, the NFVO forwards the alarm to the OSS/BSS transparently and step 8 is executed.

5.2) Based on the alarm information received from the VIM, alarm information received from the VNFM (if any) and the NFVO itself (if any), the NFVO processes the alarm information to generate a standardized alarm associated to NS(s) and step 6 is executed. See note 2.

6) The NFVO matches the alarm generated with the policies predefined in the NFVO to evaluate if the alarm triggers the policies or not. If a policy is triggered, conditions in the policy are evaluated. If the conditions are evaluated to be true, the actions defined by the policy are executed. Then, if the alarm is cleared, an alarm cleared notification is sent to the OSS/BSS and the procedure ends. If the alarm is not cleared or no policy is triggered, step 7 is executed.

7) The NFVO sends an alarm notification with the standardized alarm to the OSS/BSS through the NS Fault Management interface on the Os-Ma-nfvo reference point.

8) The OSS/BSS analyses the alarm information received to determine the solution.

9) The OSS/BSS can send an operation request (e.g. NS heal operation request) to the NFVO to heal the NFV-MANO managed objects.

10) The NFVO executes the operations requested and/or sends operation request(s) to the VNFM and/or the VIM respectively.

NOTE 1: The standardized alarm is expected to include attributes defined in clause 8.6 of ETSI GS NFV-IFA 005 [i.4] and reference the information given in clauses 6 and 7 of the present document.

NOTE 2: The standardized alarm is expected to include attributes defined in clause 8.5 of ETSI GS NFV-IFA 013 [i.8] and reference the information given in clauses 6 and 7 of the present document.

A.2.3 Use case about procedure of using alarm information produced by the VNFM with policies

This clause describes the informative generic procedure of how the VNFM can collect and produce alarm information and how NFV-MANO can process these new alarms accordingly. The present procedure is generic and informative. The design of alarm modelling could reference the procedure.

1) The VNFM monitors and collects different types of indicators information of VNFs and the alarm information received from the VIM. See note 3.

2) The VNFM processes the alarm and indicators information collected (e.g. alarm generation, alarm compression) to generate a standardized alarm associated to VNF(s). See note 1.

3) The VNFM matches the alarm generated with the policies predefined in the VNFM to evaluate if the alarm triggers the policies or not. If a policy is triggered, conditions in the policy are evaluated. If the conditions are evaluated to be true, the actions defined by the policy are executed. Then, if the alarm is cleared, an alarm cleared notification is sent to the NFVO which can forward it to the OSS/BSS, as well the VNFM can send it to the EM (if also subscribed to receive notifications) and the procedure ends. If the alarm is not cleared or no policy is executed, step 4 is executed.

4) The VNFM sends an alarm notification with the standardized alarm to the NFVO and to the EM (if also subscribed to receive notifications) through the VNF Fault Management Interface on the Or-Vnfm reference point and Ve-Vnfm-em reference point, respectively.

5.1) Based on the alarm information received, the NFVO forwards the alarm to the OSS/BSS transparently and step 8 is executed.

5.2) Based on the alarm information received from the VNFM, alarm information received from the VIM (if any) and the NFVO itself (if any), the NFVO processes the alarm information to generate a standardized alarm associated to NS(s) and step 6 is executed. See note 2.

6) The NFVO matches the alarm generated with the policies predefined in the NFVO to evaluate if the alarm triggers the policies or not. If a policy is triggered, conditions in the policy are evaluated. If the conditions are evaluated to be true, the actions defined by the policy are executed. Then, if the alarm is cleared, an alarm cleared notification is sent to the OSS/BSS and the procedure ends. If the alarm is not cleared or no policy is triggered, step 7 is executed.

7) The NFVO sends an alarm notification with the standardized alarm to the OSS/BSS through the NS Fault Management interface on the Os-Ma-nfvo reference point.

8) The OSS/BSS analyses the alarm information received to determine the solution.

9) The OSS/BSS can send an operation request (e.g. NS heal operation request) to the NFVO to heal the NFV-MANO managed objects.

10) The NFVO executes the operations requested and/or sends operation request(s) to the VNFM and/or the VIM respectively.

NOTE 1: The standardized alarm is expected to include attributes defined in clause 8.8 of ETSI GS NFV-IFA 007 [i.6] and reference the information given in clause 6 and 7 of the present document.

NOTE 2: The standardized alarm is expected to include attributes defined in clause 8.5 of ETSI GS NFV-IFA 013 [i.8] and reference the information given in clauses 6 and 7 of the present document.

NOTE 3: Semantics of "VNF indicators" is not specified in ETSI GS NFV-IFA 008 [i.7]. But it is assumed these can be used in case some indicators defined by the VNF provider are able to be processed by the VNFM either via LCM scripts or policies in the VNFD, and correlate them with alarms information received by the VNFM from the VIM. The correlation mechanism of VNF indicators with alarms is out of the scope of the present document.

A.2.4 Use case about procedure of using alarm information produced by the NFVO with policies

This clause describes the informative generic procedure of how the NFVO can collect and produce alarm information and how NFV-MANO can process these new alarms accordingly. The present procedure is generic and informative. The design of alarm modelling could reference the procedure.

1) The NFVO monitors and collects different types of alarm information of NSs and the alarm information received from the VNFM and the VIM.

2) The NFVO processes the alarm information collected (e.g. alarm generation, alarm compression) to generate a standardized alarm associated to NS(s). See note.

3) The NFVO matches the alarm generated with the policies predefined in the NFVO to evaluate if the alarm triggers the policies or not. If a policy is triggered, conditions in the policy are evaluated. If the conditions are evaluated to be true, the actions defined by the policy are executed. Then, if the alarm is cleared, an alarm cleared notification is sent to the OSS/BSS and the procedure ends. If the alarm is not cleared or no policy is executed, step 4 is executed.

4) The NFVO sends an alarm notification with the standardized alarm to the OSS/BSS through the NS Fault Management interface on the Os-Ma-nfvo reference point.

5) The OSS/BSS analyses the alarm information received to determine the solution.

6) The OSS/BSS can send an operation request (e.g. NS heal operation request) to the NFVO to heal the NFV-MANO managed objects.

7) The NFVO executes the operations requested and/or sends operation request(s) to the VNFM and/or the VIM respectively.

NOTE: The standardized alarm is expected to include attributes defined in clause 8.5 of ETSI GS NFV-IFA 013 [i.8] and reference the information given in clauses 6 and 7 of the present document.

Annex B (informative): Change history

Date	Version	Information about changes
September 2021	0.0.1	Implementations of approved skeleton: NFVIFA(21)000810 approved in IFA#255
November 2021	0.0.2	Implementations of approved contributions approved in IFA#260: NFVIFA(21)000914 NFVIFA(21)000915
December 2021	0.0.3	Implementations of approved contributions approved in IFA#265: NFVIFA(21)0001043r1 NFVIFA(21)0001044r1 NFVIFA(21)0001045r1
January 2022	0.0.4	Implementations of approved contributions approved in IFA#267: NFVIFA(21)0001067r2 NFVIFA(21)0001068r2
March 2022	0.0.5	Implementations of approved contributions approved in IFA#275: NFVIFA(22)000045r1 NFVIFA(22)000151
May 2023	0.1.0	Implementations of approved contributions approved until IFA#333: NFVIFA(23)000152 NFVIFA(22)000911 NFVIFA(23)000140r1 NFVIFA(23)000271 NFVIFA(22)000912r2 NFVIFA(22)000913r1 NFVIFA(22)000914 NFVIFA(22)000915 NFVIFA(22)000916r1 NFVIFA(22)000917 NFVIFA(23)000141r1 NFVIFA(23)000144 NFVIFA(23)000145 NFVIFA(23)000146 NFVIFA(23)000147r1 NFVIFA(23)000148r1 NFVIFA(23)000143 NFVIFA(23)000149 NFVIFA(23)000150r1 NFVIFA(23)000151 NFVIFA(23)000272 NFVIFA(23)000273 NFVIFA(23)000274 NFVIFA(23)000318r2
June 2023	0.2.0	Implementations of approved contributions approved until IFA#337: NFVIFA(23)000463 NFVIFA(23)000399 NFVIFA(23)000443r1 NFVIFA(23)000398r1 NFVIFA(23)000391 NFVIFA(23)000444 NFVIFA(23)000445 NFVIFA(23)000413r1 NFVIFA(23)000392r2 NFVIFA(23)000393r1 NFVIFA(23)000394r2 NFVIFA(23)000395r1 NFVIFA(23)000396r1 NFVIFA(23)000397r1 NFVIFA(23)000446 NFVIFA(23)000447 NFVIFA(23)000448 NFVIFA(23)000400r1 NFVIFA(23)000415 NFVIFA(23)000416 NFVIFA(23)000417

Date	Version	Information about changes
		NFVIFA(23)000401
August 2023	0.3.0	NFVIFA(23)000578 NFVIFA(23)000584 NFVIFA(23)000580 NFVIFA(23)000581r1 NFVIFA(23)000579 NFVIFA(23)000572r1 NFVIFA(23)000582 NFVIFA(23)000583 NFVIFA(23)000598

History

Document history		
V4.5.1	October 2023	Publication