ETSI GR NFV-REL 012 V1.1.1 (2021-11)

Network Functions Virtualisation (NFV); Reliability; Report on availability and reliability under failure and overload conditions in NFV-MANO

Disclaimer

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

Reference
DGR/NFV-REL012

Keywords
availability, MANO, NFV, robustness

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

This study assumes a fault management model as defined by 3GPP TS 32.111-1 [i.3], which in turn is based on Recommendation ITU-T X.733 [i.4].

This is done in consistency with ETSI GS NFV-IFA 031 [i.6].

Modal verbs terminology

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

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

1 Scope

The present document reports on impacts of NFV-MANO failures and overload conditions, including human errors, on the availability and reliability of NFV-MANO. A set of use cases will be described and analysed which include interactions between NFV-MANO functional entities under such conditions and other functional blocks (VNF, EM, OSS, ...). Also situations are analysed, where availability is achieved by a system of collaborating NFV-MANO functional entities possibly provided by different vendors. As a result, recommendations for the requirements of an available and reliable NFV-MANO system will be derived.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

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

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

[i.3] 3GPP TS 32.111-1 (V16.0.0): "Telecommunication management; Fault Management; Part 1: 3G fault management requirements".

[i.4] Recommendation ITU-T X.733: "Systems Management: Alarm reporting function".

[i.5] ETSI GR NFV-REL 011: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Report on NFV-MANO Software Modification".

[i.6] ETSI GS NFV-IFA 031 (V3.4.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Requirements and interfaces specification for management of NFV-MANO".

[i.7] ETSI GS NFV-IFA 008 (V3.4.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[i.8] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

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] and the following apply:

alarm: information about a specific condition requiring attention

NOTE: An alarm does or does not represent an error.

alarm notification: message used to report an alarm

error: discrepancy between a computed, observed, or measured value or condition and a true, specified, or theoretically correct value or condition

NOTE 1: Error is a consequence of a fault.

NOTE 2: See ETSI GS NFV-REL 001 [i.2].

failure: deviation of the service from fulfilling its functionality

NOTE: See ETSI GS NFV-REL 001 [i.2].

fault: adjudged or hypothesized cause of an error

NOTE: See ETSI GS NFV-REL 001 [i.2].

3.2 Symbols

Void.

3.3 Abbreviations

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

DDoS	Distributed Denial of Service
FE	Functional Entity
RU	Resource Unit
RUI	Resource Unit Instance
SU	Service User

4 Architectural overview

4.1 NFV-MANO architectural considerations

The internal architecture of an NFV-MANO functional entity is not visible to the external world and it can follow different architectural paradigms.

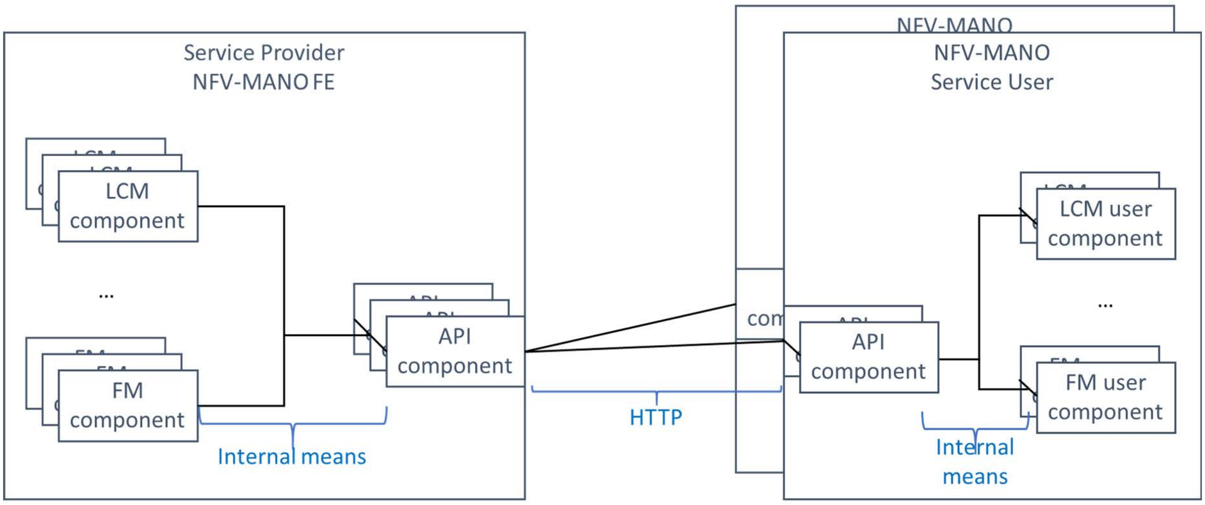

Figure 4.1-1: Example of the internal architecture of an NFV-MANO functional entity and the users of its services

One of the popular paradigms is the microservice based architecture according to which an NFV-MANO functional entity could be built as a set of different microservices. For example, an NFV-MANO functional entity can include a microservice implementing the Life Cycle Management (LCM) operations, another for Fault Management (FM) and yet another handling the HTTP API communication needs of the microservices as shown in figure 4.1-1. These different microservices are supported by different sets of components of the NFV-MANO functional entity to provide the NFV-MANO services in accordance with the ETSI GS NFV-IFA 031 [i.6]. An example of the Service Provider (SP) NFV-MANO functional entity could be a VNFM.

The same architectural considerations apply to the users of the NFV-MANO services provided by the NFV-MANO functional entity. Examples of the NFV-MANO Service User (SU) could be a VNF or the NFVO.

NOTE: The SP NFV-MANO functional entity is not aware of the internal structure of the NFV-MANO SU and vice versa. These details are shown and discussed for the purpose of the use case analysis.

When it comes to the reliability of the communication between these two categories of entities, i.e. the SP NFV-MANO functional entity and the NFV-MANO SU, two kinds of communication segments need to be considered. On the one hand, between the entities on the external portion of the communication path, HTTP is used as the communication protocol as defined in the ETSI NFV-SOL specifications. On the other hand, the means of internal communication - among the components of each of the entities - is left to the implementer (e.g. vendor) of each of these entities.

In addition, in the ETSI NFV specifications, two communication patterns are considered. The two-way communication pattern is implemented through the exchange of a request followed by a response. While in the one-way communication pattern (also referred as fire-and-forget), a message is sent without the need for follow-up.

This means that, in case of two-way communication, for example, when an LCM user component of the SU sends a request to an LCM component of the SP, the request passes through the SU-internal, the external and again on the SP-internal portions of the communication path between these components. The same applies in reverse order to the response. If the communication fails on any portion of this communication path, it can be detected by the SU LCM user component as it would not receive the response sent by the SP; and therefore, it can take actions as needed or sees appropriate.

In case of one-way communication, the sender, for example, an FM component of the SP, does not expect any response to the notification it sends. Nevertheless, the delivery of this notification to all intended receivers, i.e. FM user components of the SUs, is important to ensure that they can take any necessary actions. However, the sender of such communication - the FM component of the SP - has no way to detect if the notification was not delivered. Therefore, it is typically expected that the underlying communication mechanism guarantees the delivery to the receiving end(s) - FM user components of the SUs.

To this end, the HTTP protocol mandated for the external portion of the communication path does not cover the internal portions of the path, hence it cannot detect any loss occurring on the internal portions of the communication path.

With respect to the HTTP portion of the communication path itself, according to IETF RFC 7230 [i.8]:

"HTTP does not define specific error handling mechanisms except when they have a direct impact on security, since different applications of the protocol require different error handling strategies."

Also, HTTP allows for the chaining of connections through intermediaries, in which case the end-to-end delivery through this chain cannot always be guaranteed without appropriate error handling mechanism.

In clauses 5.2.3 and 5.2.4, different message loss scenarios and their mitigation are investigated through different use cases.

4.2 NFV-MANO functional entity redundancy

The internal architecture of an NFV-MANO functional entity is exposed only to the extent of enabling a network operator to manage the redundancy of the deployment of the NFV-MANO functional entity. For this purpose, the ETSI GR NFV-REL 011 [i.5] report has proposed a refinement to the concepts defined in the ETSI GS NFV-IFA 031 [i.6] specification. Accordingly, an NFV-MANO functional entity consists of one or more NFV-MANO functional entity Redundancy Unit(s)(RU). Each RU can be deployed redundantly according to a redundancy model. This redundancy model is one of the vendor defined redundancy models. An NFV-MANO functional entity redundancy unit might be further decomposed into NFV-MANO functional entity components. However, these NFV-MANO functional entity components are generally hidden from the network operator. If desired and available, the network operator can choose a redundancy model that deploys multiple RU instances.

To clarify these concepts that are essential for the understanding of use cases described in clause 5.2.2, figure 4.2-1 provides an example of the internal architecture of a deployed NFV-MANO functional entity.

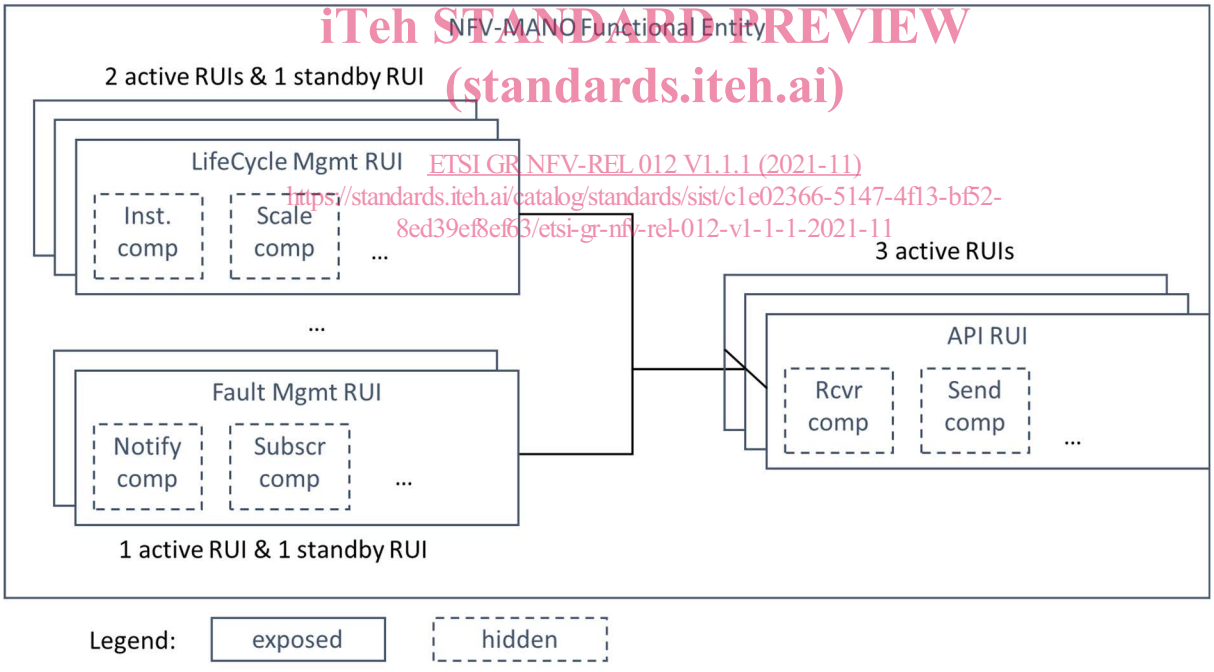

Figure 4.2-1: Example of the internal architecture of an NFV-MANO functional entity

The NFV-MANO functional entity in this example has three NFV-MANO functional entity redundancy units:

- The LifeCycle Mgmt redundancy unit (LifeCycle Mgmt RU) is deployed with two active and a standby Redundancy Unit Instances (RUIs). This is a selectable redundancy model for this redundancy unit specified by the vendor. The redundancy unit is further decomposed into components for handling the instantiation (Inst. comp), the scaling (Scale comp) and other services the LifeCycle Mgmt redundancy unit provides, which are not exposed. The components of the active and standby instances of the redundancy unit collaborate with each other to provide these services seamlessly in case of failures of components or an entire redundancy unit instance.

- The Fault Mgmt redundancy unit (Fault Mgmt RU) is deployed with one active and one standby instances. Again, this is one of the selectable redundancy models for this redundancy unit and accordingly the active and standby instances collaborate with each other. In the example, this redundancy unit consists of at least two components not visible for the network operator: one for handling the subscriptions (Subscr comp) and another for generating the notifications (Notify comp).

- The API Redundancy Unit (API RU) is deployed with three active instances. The redundancy unit is composed of the sender (Send comp) and the receiver (Rcvr comp) components. These RU instances do not collaborate with each other, meaning that if one of them fails the other RU instances will not have any information about the messages sent and received by the failed RU instance. But they will handle any new incoming and outgoing messages. The service thus remains available, but its continuity might not be guaranteed.

An NFV-MANO functional entity might include an internal availability management, which is capable of deploying the appropriate number of redundancy unit instances according to the redundancy model selected for instantiation. It would also monitor these instances and perform healing actions as they might become necessary. Note, however, that the internal availability management cannot detect and heal failures impacting the entire NFV-MANO functional entity. This requires an external manager.

It is also possible that there is no internal availability management, but, due to their need for collaboration, for example, the redundancy units or their components can detect that their instances have been deployed redundantly by an external manager. In this case, the redundancy units are able to report if there is any problem with their redundant peer. But since the life cycle of the redundancy unit instances is managed externally, the task of healing a failed redundancy unit instance also remains with this external manager. In addition, the external manager would need to monitor the health of the NFV-MANO functional entity redundancy unit instances if they cannot report each other's failure - for example because they are deployed all active without any need for collaboration other than sharing the load. Such external monitoring and management are also necessary to detect and heal a failure impacting the entire NFV-MANO functional entity.

Finally, it is possible that an entire NFV-MANO functional entity is deployed redundantly. In this case, the NFV-MANO functional entity instances are not aware of each other by default and the external manager should not only manage the life cycle of the NFV-MANO functional entity instances, but also facilitate their collaboration. This collaboration might be very limited and typically would be implemented by external means, e.g. via external database/file.

To achieve higher reliability and availability, the options above can be combined. That is, the internal and external availability/life cycle managers can be used in combination with each other, each responsible for a particular scope of management. For example, the internal availability manager would handle the internal failures of components and redundancy units of the NFV-MANO functional entity. While the external life cycle manager monitors the NFV-MANO functional entity as a whole and performs healing actions at the NFV-MANO functional entity level.

For certain NFV-MANO functional entities, geo-redundant deployment might be necessary. This could be achieved either by redundant deployment of the entire NFV-MANO functional entity or its redundancy units. The main difference is that when the NFV-MANO functional entity redundancy unit(s) is/are deployed redundantly, they still act together as a single NFV-MANO functional entity instance, as they all represent the same identity. When the entire NFV-MANO functional entity is deployed redundantly, each instance will have its own identity and the collaboration of these different instances does not go beyond any applicable interface specifications (e.g. Or-Or).

5 Use cases

5.1 Introduction

Clause 5 describes use cases for NFV-MANO failure and overload conditions. Two functions are introduced for the purpose to describe the use cases, the Alarm-Aggregator and the MANO-Monitor functions. The task of the Alarm-Aggregator function is to maintain an aggregated list of alarm conditions that exist in the NFV system, while the MANO-Monitor function is responsible to take actions towards resolving the root cause of an alarm.

The use cases do not make any assumption what entity or entities can play such roles. The roles could be fulfilled by an administrator or OSS, or they could be new functionalities offered by NFV-MANO.

5.2 NFV-MANO failures

5.2.1 NFV-MANO failure detection and reporting

5.2.1.1 Handling of an alarm reported by an NFV-MANO functional entity

5.2.1.1.1 Introduction and goal

An NFV-MANO functional entity may detect an internal error that prevents it from providing a service as specified. If this error cannot be recovered internally, it is a failure. This failure situation should be reported to other interested parties by sending an alarm notification. The NFV-MANO functional entity will track the state of this alarm by adding it to its own active alarm list.

When receiving an alarm notification, the Alarm-Aggregator will inform the registered entities to enable them to take precautions to mitigate the impact of the failure of the faulty NFV-MANO functional entity.

The MANO-Monitor will acknowledge the alarm notification and take over the responsibility to resolve the root cause of the alarm. The MANO-Monitor will maintain a list of active alarms that it has acknowledged. After resolving the root cause, the normal operation resumes.

NOTE: It cannot always be assumed, that an NFV-MANO functional entity is able to detect, that it cannot provide service as specified and report this. The NFV-MANO functional entity may not even be operational anymore. The use case of the detection ofa potential failure by an external entity is described in clause 5.2.1.2.

5.2.1.1.2 Actors and roles

Table 5.2.1.1.2-1 describes the use case actors and roles.

Table 5.2.1.1.2-1: Handling of an alarm reported by an NFV-MANO functional entity actors and roles

#	Role	Description
1	Faulty NFV-MANO functional entity	The entity that detects a failure on itself.
2	Registered entity	Entity that has registered with the Alarm-Aggregator to be informed in case of an alarm.
3	MANO-Monitor	Entity responsible to resolve the root cause of the alarm.
4	Alarm-Aggregator	Entity responsible for maintaining an aggregated list of alarm conditions in the NFV system. For this purpose, it has registered with the NFV-MANO functional entities to receive alarm notifications. The Alarm-Aggregator will forward notifications to registered entities.

5.2.1.1.3 Pre-conditions

Table 5.2.1.1.3-1 describes the use case pre-conditions.

Table 5.2.1.1.3-1: Handling of an alarm reported by an NFV-MANO functional entity pre-conditions

#	Pre-condition	Additional description
1	All NFV-MANO functional entities, the Alarm-Aggregator and the MANO-Monitor are running correctly	This includes the NFV-MANO functional entity that will become faulty.
2	The Alarm-Aggregator has registered with all the NFV-MANO functional entities to receive alarm notifications	
3	The MANO-Monitor has registered with the Alarm-Aggregator to receive alarm notifications	
4	All NFV-MANO functional entities have registered with the Alarm-Aggregator to be informed about alarms they are interested in	

5.2.1.1.4 Post-conditions

Table 5.2.1.1.4-1 describes the use case post-conditions.

Table 5.2.1.1.4-1: Handling of an alarm reported by an NFV-MANO functional entity post-conditions

#	Post-condition	Additional description
1	All NFV-MANO functional entities, the Alarm-Aggregator and the MANO-Monitor are running correctly	This includes the NFV-MANO functional entity that was faulty.

5.2.1.1.5 Flow description

Table 5.2.1.1.5-1 describes the use case flow.

Table 5.2.1.1.5-1: Handling of an alarm reported by an NFV-MANO functional entity flow description

#	Actor/Role	Action/Description
Begins when	Faulty NFV-MANO functional entity	The faulty NFV-MANO functional entity detects an internal error. This error prevents it from providing a service as specified, thus it is a failure. It cannot recover from this failure on its own. It creates an entry in its active alarm list.
Step 1	Faulty NFV-MANO functional entity -> Alarm-Aggregator	The faulty NFV-MANO functional entity sends an alarm notification to the Alarm-Aggregator.
Step 2	Alarm-Aggregator -> Registered entities	The Alarm-Aggregator creates an entry in its global list of active alarms and sends the alarm notification to the registered entities. This includes the MANO-Monitor.
Step 3	MANO-Monitor-> Faulty NFV-MANO functional entity	The MANO-Monitor acknowledges to the faulty NFV-MANO functional entity that it has received the alarm notification and the responsibility to recover from the failure is taken over. The faulty NFV-MANO functional entity can stop trying to recover from the failure locally and it does not need to send subsequent alarm notifications for the same failure if the state of the alarm is the same.
Step 4	Faulty NFV-MANO functional entity -> Alarm-Aggregator	The faulty NFV-MANO functional entity sends an updated alarm notification with ackState set to true to the Alarm-Aggregator.
Step 5	Alarm-Aggregator -> Registered entities	The Alarm-Aggregator updates its global list of active alarms and forwards the alarm notification to the registered entities. This includes the MANO-Monitor.
Step 6	MANO-Monitor	The MANO-Monitor takes the necessary actions to recover from the failure. This may include the involvement of other NFV-MANO functional entities, non NFV-MANO functional entities, or an administrator.
Step 7	MANO-Monitor-> Faulty NFV-MANO functional entity	The MANO-Monitor detects/is informed that the root cause of the failure of the faulty NFV-MANO functional entity was probably removed. It informs the faulty NFV-MANO functional entity about the potential removal of the root cause (see note 1).
Step 8	Faulty NFV-MANO functional entity -> MANO-Monitor	The faulty NFV-MANO functional entity confirms the message about the potential removal of the root cause.
Step 9	Faulty NFV-MANO functional entity -> Alarm-Aggregator	The faulty NFV-MANO functional entity checks that the root cause of the failure was removed. It sends an alarm cleared notification to the Alarm-Aggregator and marks the corresponding entry in its active alarm list accordingly (see note 2).
Ends when	Alarm-Aggregator -> Registered entities	The Alarm-Aggregator sends the alarm cleared notification to the registered entities. This includes the MANO-Monitor. It sets the state of corresponding entry in its global list of active alarms to cleared.
NOTE 1: The information may be transmitted by proposing a change of the perceived severity to cleared, similar to the EscalatePerSevRequest operation available in ETSI GS NFV-IFA 008 [i.7]. NOTE 2: If there is still a failure condition, an updated alarm notification is sent to the Alarm-Aggregator and the flow continues in Step 2.		

5.2.1.2 Detection of a failure of another NFV-MANO functional entity

5.2.1.2.1 Introduction and goal

An NFV-MANO functional entity can detect that another NFV-MANO functional entity might be in a failure situation if, for example, it receives from the other NFV-MANO functional entity an unexpected message.

5.2.1.2.2 Actors and roles

Table 5.2.1.2.2-1 describes the use case actors and roles.

Table 5.2.1.2.2-1: Detection of a failure of another NFV-MANO functional entity actors and roles

#	Role	Description
1	Faulty NFV-MANO functional entity	Entity not providing a service as specified.
2	Failure detecting NFV-MANO functional entity	Entity that detects that another NFV-MANO functional entity does not provide a service as expected.
3	Registered entity	Entity that has registered with the Alarm-Aggregator to be informed in case of an alarm.
4	MANO-Monitor	Entity responsible to resolve the root cause of alarms.
5	Alarm-Aggregator	Entity responsible for maintaining an aggregated list of alarm conditions in the NFV system. For this purpose, it has registered with the NFV-MANO functional entities to receive alarm notifications. The Alarm-Aggregator will forward notifications to registered entities.

5.2.1.2.3 Pre-conditions

Table 5.2.1.2.3-1 describes the use case pre-conditions.

Table 5.2.1.2.3-1: Detection of a failure of another NFV-MANO functional entity pre-conditions

#	Pre-condition	Additional description
1	All NFV-MANO functional entities, the Alarm-Aggregator and the MANO-Monitor are running correctly	This includes the NFV-MANO functional entity that will detect the failure.
2	The Alarm-Aggregator has registered with all the NFV-MANO functional entities to receive alarm notifications	
3	The MANO-Monitor has registered with the Alarm-Aggregator to receive alarm notifications	
4	All NFV-MANO functional entities have registered with the Alarm-Aggregator to be informed about alarms they are interested in	

5.2.1.2.4 Post-conditions

Table 5.2.1.2.4-1 describes the use case post-conditions.

Table 5.2.1.2.4-1: Detection of a failure of another NFV-MANO functional entity post-conditions

#	Post-condition	Additional description
1	All NFV-MANO functional entities, the Alarm-Aggregator and the MANO-Monitor are running correctly	This includes the NFV-MANO functional entity that was faulty.

5.2.1.2.5 Flow description

Table 5.2.1.2.5-1 describes the use case flow.

Table 5.2.1.2.5-1: Detection of a failure of another NFV-MANO functional entity flow description

#	Actor/Role	Action/Description
Begins when	Faulty NFV-MANO functional entity -> Failure detecting NFV-MANO functional entity	The failure detecting NFV-MANO functional entity receives a message from an NFV-MANO functional entity which it was not expecting.
Step 1	Failure detecting NFV-MANO functional entity -> Alarm-Aggregator	By receiving an unexpected message, the failure detecting NFV-MANO functional entity assumes that the sender NFV-MANO functional entity is faulty. Therefore, it raises an alarm and creates an entry in its active alarm list and sends an alarm notification to the Alarm-Aggregator.
Step 2	Alarm-Aggregator -> Registered entities	The Alarm-Aggregator creates an entry in its global list of active alarms and forwards the alarm notification to the registered entities. This includes the MANO-Monitor. It can also include the faulty NFV-MANO functional entity.
Step 3	MANO-Monitor-> Failure detecting NFV-MANO functional entity	The MANO-Monitor acknowledges that it has received the alarm notification from the failure detecting NFV-MANO functional entity about the faulty NFV-MANO functional entity. The failure detecting NFV-MANO functional entity does not need to send subsequent alarm notifications for the same failure other than updates, including clearing it when the failure is not present anymore.
Step 4	Registered entities	The registered entities take notice of the alarm notification. If possible and beneficial, the registered entities take precautions to mitigate the impact of the failure of the faulty NFV-MANO functional entity.
Step 5	Failure detecting NFV-MANO functional entity -> Alarm-Aggregator	The failure detecting NFV-MANO functional entity sends an updated alarm notification with ackState set to true to the Alarm-Aggregator.
Step 6	Alarm-Aggregator -> Registered entities	The Alarm-Aggregator updates the entry in the global list of active alarms and forwards the alarm notification to all registered entities. This includes the MANO-Monitor.
Step 7	MANO-Monitor	The MANO-Monitor takes the necessary actions to recover from the failure. This can include the involvement of other NFV-MANO functional entities, including the faulty NFV-MANO functional entity and/or the failure detecting NFV-MANO functional entity, non NFV-MANO functional entities or an administrator.
Step 8	MANO-Monitor -> Failure detecting NFV-MANO functional entity	The MANO-Monitor detects/is informed that the root cause of the failure of the faulty NFV-MANO functional entity was successfully removed. Accordingly, it proposes to the failure detecting NFV-MANO functional entity to clear the alarm.
Step 9	Failure detecting NFV-MANO functional entity -> MANO-Monitor	The failure detecting NFV-MANO functional entity confirms the reception of the clearing proposal.
Step 10	Failure detecting NFV-MANO functional entity	The failure detecting NFV-MANO functional detects that the problem is solved (see note).
Step 11	Failure detecting NFV-MANO functional entity -> Alarm-Aggregator	The failure detecting NFV-MANO functional removes the alarm from its active alarm list and sends the alarm clearing notification to the Alarm-Aggregator.
Ends when	Alarm-Aggregator -> Registered entities	The Alarm-Aggregator sends the alarm clearing notification to all registered entities. This includes the MANO-Monitor and could include the faulty NFV-MANO functional entity. The Alarm-Aggregator removes the entry from the global list of active alarms.
NOTE: If the failure condition persists, the flow continues at Step 1 with sending an updated alarm notification to the Alarm-Aggregator.		