1.0 Overall Principle for High Availability in NFV

The ultimate goal for the High Availability schema is to provide high availability to the upper layer services.

High availability is provided by the following steps once a failure happens:

Step 1: failover of services once failure happens and service is out of work

Step 2: Recovery of failed parts in each layer.

1.1 Framework for High Availability in NFV

Framework for Carrier Grade High availability:

A layered approach to availability is required for the following reasons:

- fault isolation
- fault tolerance
- fault recovery

Among the OPNFV projects the OPNFV-HA project's focus is on requirements related to service high availability. This is complemented by other projects such as the OPNFV - Doctor project, whose focus is reporting and management of faults along with maintenance, the OPNFV-Escalator project that considers the upgrade of the NFVI and VIM, or the OPNFV-Multisite that adds geographical redundancy to the picture.

A layered approach allows the definition of failure domains (e.g., the networking hardware, the distributed storage system, etc.). If possible, a fault shall be handled at the layer (failure domain) where it occurs. If a failure cannot be handled at its corresponding layer, the next higher layer needs to be able to handle it. In no case, shall a failure cause cascading failures at other layers.

The layers are:

Service	End customer visible service
Application	VNF's, VNFC's
NFVI/VIM	Infrastructure, VIM, VNFM, VM
Hardware	Servers, COTS platforms

The following document describes the various layers and how they need to address high availability.

1.2 Definitons

Reference from the ETSI NFV doc.

Availability: Availability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided.

Accessibility: It is the ability of a service to access (physical) resources necessary to provide that service. If the target service satisfies the minimum level of accessibility, it is possible to provide this service to end users.

Admission control: It is the administrative decision (e.g. by operator's policy) to actually provide a service. In order to provide a more stable and reliable service, admission control may require better performance and/or additional resources than the minimum requirement. Failure: deviation of the delivered service from fulfilling the system function.

Fault: adjudged or hypothesized cause of an error

Service availability: service availability of <Service X> is the long-term average of the ratio of aggregate time between interruptions to scheduled service time of <ServiceX> (expressed as a percentage) on a user-to-user basis. The time between interruptions is categorized as Available (Up time) using the availability criteria as defined by the parameter thresholds that are relevant for <Service X>.

Accoring to the ETSI GS NFV-REL 001 V1.1.1 (2015-01) document service availability in the context of NFV is defined as End-to-End Service availability

Service Availability refers to the End-to-End Service Availability which includes all the elements in the end-to-end service (VNFs and infrastructure components) with the exception of the customer terminal. This is a customer facing (end user) availability definition and it is the result of accessibility and #admission control (see their respective definitions above).

Service Availability=total service available time/

(total service available time + total restoration time)

Service continuity: Continuous delivery of service in conformance with service's functional and behavioural specification and SLA requirements, both in the control and data planes, for any initiated transaction or session until its full completion even in the events of intervening exceptions or anomalies, whether scheduled or unscheduled, malicious, intentional or unintentional.

The relevant parts in NFV-REL: The basic property of service continuity is that the same service is provided during VNF scaling in/out operations, or when the VNF offering that service needs to be relocated to another site due to an anomaly event (e.g. CPU overload, hardware failure or security threat).

Service failover: when the instance providing a service/VNF becomes unavailable due to fault or failure, another instance will (automatically) take over the service, and this whole process is transparent to the user. It is possible that an entire VNF instance becomes unavailble while providing its service.

Service failover time: Service failover is when the instance providing a service becomes unavailable due to a fault or a failure and another healthy instance takes over in providing the service. In the HA context this should be an automatic action and this whole process should be transparent to the user. It is possible that an entire VNF instance becomes unavailble while providing its service.

Failure detection: If a failure is detected, the failure must be identified to the component responsible for correction.

Failure detection time: Failure detection time is the time interval from the moment the failure occurs till it is reported as a detected failure.

Alarm: Alarms are notifications (not queried) that are activated in response to an event, a set of conditions, or the state of an inventory object. They also require attention from an entity external to the reporting entity (if not then the entity should cope with it and not raise the alarm).

Alarm threshold condition detection: Alarm threshold condition is detected by the component responsible for it. The component periodically evaluates the condition associated with the alarm and if the threshold is reached, it generates an alarm on the approprite channel, which in turn delivers it to the entity(ies) responsible, such as the VIM.

Alarm threshold detection time: the threshold time interval between the metrics exceeding the threshold and the alarm been detected.

Service recovery: The restoration of the service state after the instance of a service/VNF is unavailable due to fault or failure or manual interuption.

Service recovery time: Service recovery time is the time interval from the occurrence of an abnormal event (e.g. failure, manual interruption of service, etc.) until recovery of the service.

SAL: Service Availability Level

1.3 Overall requirements

Service availability shall be considered with respect to the delivery of end to end services.

- There should be no single point of failure in the NFV framework

- All resiliency mechanisms shall be designed for a multi-vendor environment, where for example the NFVI, NFV-MANO, and VNFs may be supplied by different vendors.
- Resiliency related information shall always be explicitly specified and communicated using the reference interfaces (including policies/templates) of the NFV framework.

1.4 Time requirements

The time requirements below are examples in order to break out of the failure detection times considering the service recovery times presented as examples for the different service availability levels in the ETSI GS NFV-REL 001 V1.1.1 (2015-01) document.

The table below maps failure modes to example failure detection times.

Failure Mode	Time
Failure detection of HW	<1s
Failure detection of virtual resource	<1s
Alarm threshold detection	<1min
Failure detection over of SAL 1	<1s
Recovery of SAL 1	5-6s
Failure detectionover of SAL 2	<5s
Recovery of SAL 2	10-15s
Failure detectionover of SAL 3	<10s
Recovery of SAL 3	20-25s