Welcome to the World of Standards

Source:
REL chairmen and rapporteurs
For: Discussion/Info.

Introduction to ETSI's NFV Reliability and Availability WG

May 11th, 2015

Overview

- **ETSI ISG NFV was established in February 2014**
  - Duration per ETSI policy: 2years
  - All reports are considered “informative”
  - Four WGs (INF, SWA, MANO, REL) and two EGs (SEC, PER)
  - ~15 work items
  - Very aggressive work plan: weekly calls; 4 plenaries per year
  - Terminology and technology alignment across the industry
- **ETSI ISG NFV phase 2**
  - Successor with objective to develop “normative” documents
  - Duration again 2 years

Welcome to the World of Standards

ETSI World Class Standards

NFV REL PHASE1

RELA Scope

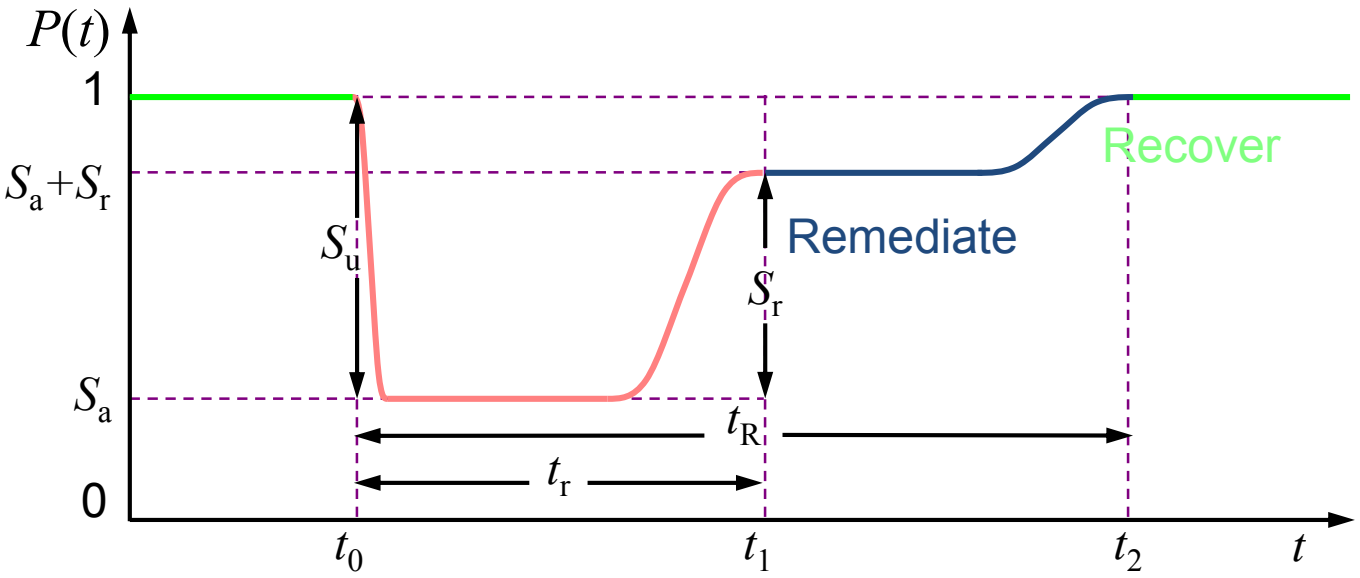
- **Use case analysis** for reliability and availability in a virtualized network environment
- Analysis of **service availability levels**
- Identification of **requirements for maintaining network resiliency and service availability,** the focus being additional requirements introduced by virtualization. The mechanisms to be considered include the following:
  - Network function migration within and across system boundaries
  - Failure detection and reporting at the various layers
  - Failure prediction, prevention, and remediation
  - Solving network availability issues caused by overload/call blocking conditions
- **Engineering and deployment guidelines** for maintaining network resiliency and ensuring service availability

RELA principles - examples

- **Prerequisites**
  - Failures of any NFV M&O component should be isolated within this component and should not impact any operational VNF.
  - The VIM shall not have knowledge of the VNF internals (including related resiliency or scalability mechanisms).
- **Trade-offs**
  - Optimize the placement of VNFs in a configuration that balances the number of components involved (minimize detection and remediation time) and independence of resources (to avoid simultaneous failure).
- **Resiliency Enablers**
  - The ability to obtain additional resources rapidly increases the resiliency of VNFs.
- **Resilient System Behaviour**
  - The automatic scale up/out is not sufficient to prevent VNF overload situations.

Fault Management

- **Detection** of adverse service conditions and service failures
- **Remediation** that the service delivered is on an acceptable level
- **Recovery** that the service operates normally (what it was designed for) again



Failure prevention

- **Containment of Failures at Each Level**
  - Prevent failure propagation
  - Notification of affected entities
- **Failure Prediction**
  - Initiation of preventive measure to minimize impact
- **Overload/call blocking prevention**
  - Scale-out capability of NFVI helps mitigating some types of overload situations but not for all
- **Prevention of Single Point of Failure**

Detection and Remediation

- **Hardware Failure Detection and Notification**
  - Local repair
  - Information sent to NFVO or VNF
- **Cross-Layer Monitoring**
  - Independent (from hostOS) or cooperative (from within VNF(C))
- **Fault Correlation**
  - Local correlation of information with a central top-level correlator
- **VNF health checking**
  - Heartbeat
  - Watchdog: physical vs. virtual
- **Failure Detection and Remediation**

Deployment Guidelines

- Network Function Virtualization Management and Orchestration
- Virtualised Network Function
- Network Function Virtualization Infrastructure
- High Availability of Management and Orchestration
- End-to-end Service Availability

Extensive Fault-Challenge Catalogue

- **Identification of fault and challenges**
  - Categories based on NIST cloud charateristics plus
    - **virtualization**
    - physical infrstructure
    - organizational

ID	Name	Description	Link to	Aspect	Mapping to NFV Framework
VN-F3	Failure and challenge detection mechanisms not in place	Mechanisms to detect challenges to or failures of VIM or NFVI components are not in place.	VN-Ch4, VN-Ch8, VN-Ch9, VN-Ch11, VN-Ch12	C-I-A	NFVI (Virtualisation Layer, Computing, Storage, Network)/VIM

ID	Name	Description	Link to	Aspect	Mapping to NFV Framework
VN-Ch4	Side-channel attack	Cross virtual machine side-channel attack leading to information leakage	VN-F2, VN-F3	C	Vn-Nf
VN-Ch8	Virtual resource intrusion	An attacker breaks into the resources of other tenants	VN-F3, VN-F5	C-I	Vn-Nf

Welcome to the World of Standards

ETSI World Class Standards

NFV REL PHASE2

ETSI NFV REL phase2 Scope

- Specifications in areas of reliability and availability in the practical context of an operational virtual environment.
- Investigating enhancements in the context of a NFV environment to ensure reliable and highly available NFV-based network services.
- Analysing reliability and availability techniques in a NFV environment.
- Responding to requests on analysing reliability and availability for current or new features to be supported in the context of the NFV.
- Provide guidance on mechanisms for validation, assurance and SLAs.
- Providing guidance on interworking with PNFs in the area of reliability, availability and assurance.
- Driving the necessary contributions and/or change requests in other ISG documents and working drafts in order to reflect specific aspects on reliability, availability and assurance.

Work item overview

REL002: Scalable Architecture for Reliability Management

- Stable draft during NFV#10 (mid May)

REL003: E2E reliability models

- Stable draft during NFV#10 (mid May)

REL004: Active monitoring & failure detection

- Stable draft during NFV#10 (mid May)

Scalable Architectures for Reliability Management

- **Goal – Develop an Informative Technical Report that:**
  - Examines Cloud/Data Center Techniques for Reliability Management for delivery of High Availability
  - Develops Scalable Methods for Managing Network Reliability in NFV Environment
- **Scope:**
  - Describe various types of conditions where Scalable Methods apply:
    - Resource failures
    - Bursty Traffic Conditions
  - Describe scale-out techniques for instantiating new VNFs for such conditions
  - Provide corroborating lab results

Scalable Architectures for Reliability Management

- **Challenges for Maintaining State:**
  - Scaling new VNFs require that the state of existing traffic flows be captured.
  - Scaling new VNFs also require load balancing for efficiency while maintaining state.
- **Categories of State:**
  - Control State (e.g., Data Structures that store forwarding entries or access control lists)
  - Per-flow State (e.g., counters tracking number of bytes/packets for any given flow)
  - Aggregate State (e.g., counters tracking number of connections, rate limiters)

Scalable Architectures for Reliability Management

- **Migration Avoidance Technique**
  - Applies to conditions where Dynamic Scaling of New VNFs needed to meet greater traffic load demand
  - General Architecture:
    - Multiple S/W switches controlled by a H/W switch
    - External Controller manages process
  - Process:
    - Controller determines if VNF A on S/W switch S1 is overloaded
    - Controller instantiates new VNF A' on S/W switch S2
    - Existing flows continue through existing VNF A
    - New flows split between existing VNF A and new VNF A' per load balancing rules
    - As existing flows die out, new flows get split in efficient manner between the two VNFs
  - Advantage: Minimizes need to migrate state between VNFs A & A'

Scalable Architectures for Reliability Management

- **Lightweight Rollback Recovery:**
  - Applies when existing VNFs are lost due to any type of failure
  - Architecture Overview:
    - Master & Backup VNFs
    - Failure Detector & Virtualization Layer
  - Three Options
- **Option 1 - Checkpointing Method:**
  - Periodic snapshots taken of VNF state by Virtualization Layer
  - Restores Last Available State onto Backup VNF when Master VNF fails
  - Pro: Easy to Implement
  - Con: Backup may be “old” – existing flows may not be recovered correctly

Scalable Architectures for Reliability Management

- **Lightweight Rollback Recovery Option Two – Checkpointing with Buffering:**
  - Packets held in buffer until a Checkpointing Snapshot is completed.
  - Pro: Failed VNF always gets correct state
  - Con: Delay introduced into system as Packets are held in buffer
- **Option Three – Checkpointing with Replay:**
  - Periodic snapshots taken of VNF state by Virtualization Layer
  - In addition, Master creates logs of events
  - Backup VNF loads last available state AND “REPLAYS” (re-processes) packets based on logs created AFTER last backup.
  - Pro: Correct State with Low Latency
  - Con: May not be an option on legacy VNFs

Scalable Architectures for Reliability Management

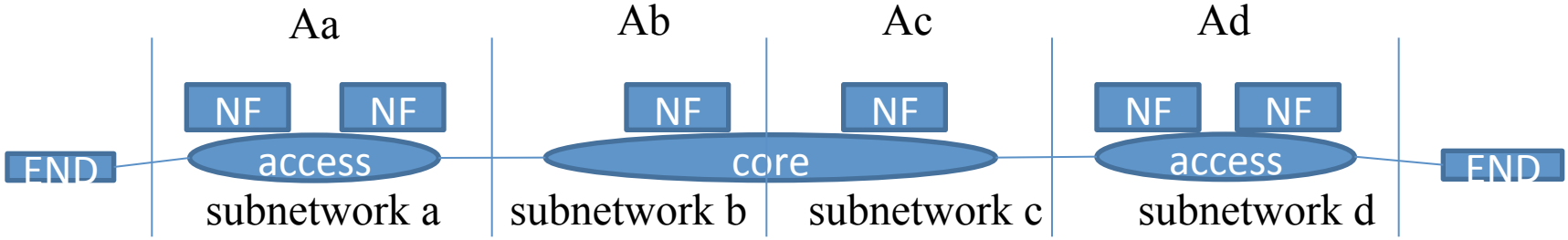
- **Status of Current Draft:**
  - Techniques for Scalable Reliability Management under Final Stages of Discussion
  - Section on Lab Results to be Provided
  - Two Additional Issues for Discussion:
    - Develop understanding of Impacts on Network & Element Availability based on such Techniques
    - Develop Guidance for NFV Components that may be involved in administering such techniques (e.g., Controllers)
  - Target for Completion: July 2015

Models and Features for E2E Reliability

- **Objective and Scope**
  - Study and develop reliability estimation model for NFV environment
  - Aspects to be considered are as follows:
    - Software reliability
    - Protection schemes and involvement of NFV-MANO (including fault management, failure detection, etc)
    - Dynamic aspects of operation: impact of load, life-cycle operations, such as software upgrade, scaling etc.
  - Recommendations or guidelines will be provided to realize services of different resiliency levels.

Models and Features for E2E Reliability

- **Process**
  - When we partition an end-to-end network into several sub-networks, the end-to-end availability/reliability is represented using the availability/reliability of the sub-networks. For example, if we divide an end-to-end network into a series of subnetworks connected in line as shown below, the end-to-end availability will be the product of the availability of the subnetworks.
  - When a subnetwork is virtualized, its availability/reliability should be the same as that of the replaced traditional subnetwork in order to keep the same level of end-to-end availability.
  - In this work item, we focus on the reliability and availability of the virtualized subnetwork, study and develop reliability estimation model for NFV environment as a basis for estimating E2E reliability.



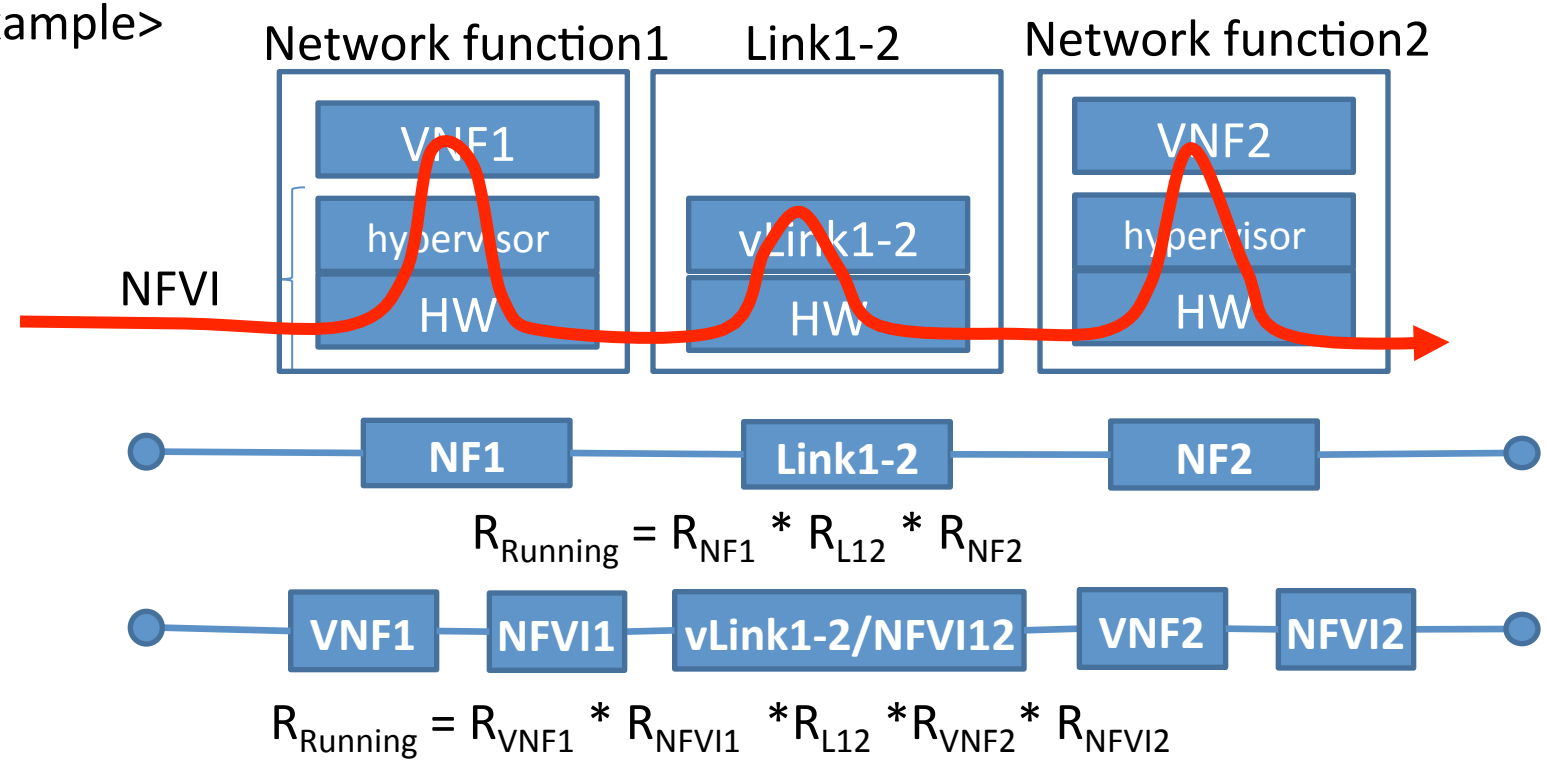
Atotal = Aa * Ab * Ac * Ad

Ax : availability of network x.

Models and Features for E2E Reliability

- **Process**
  - Break up NFV environment and study their relationship for the normal operation and each phase of lifecycle management, such as software upgrade, scaling and so on.

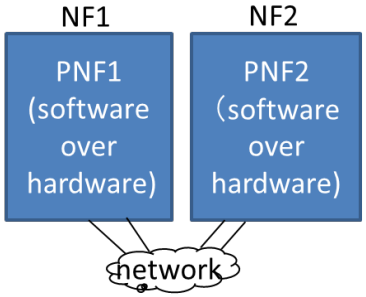
<Example>



Models and Features for E2E Reliability

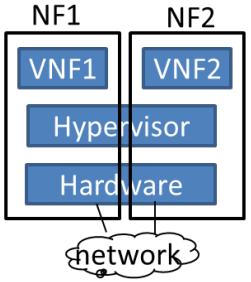
- **Process**
  - Several protection schemes are studied as well.
  - On estimating the reliability or availability in NFV environment, what we have to think about is the use of COTS hardware and the relationship among NFV components.

The reliability of NF1 and that of NF2 are independent.



An example of traditional network functions' deployment

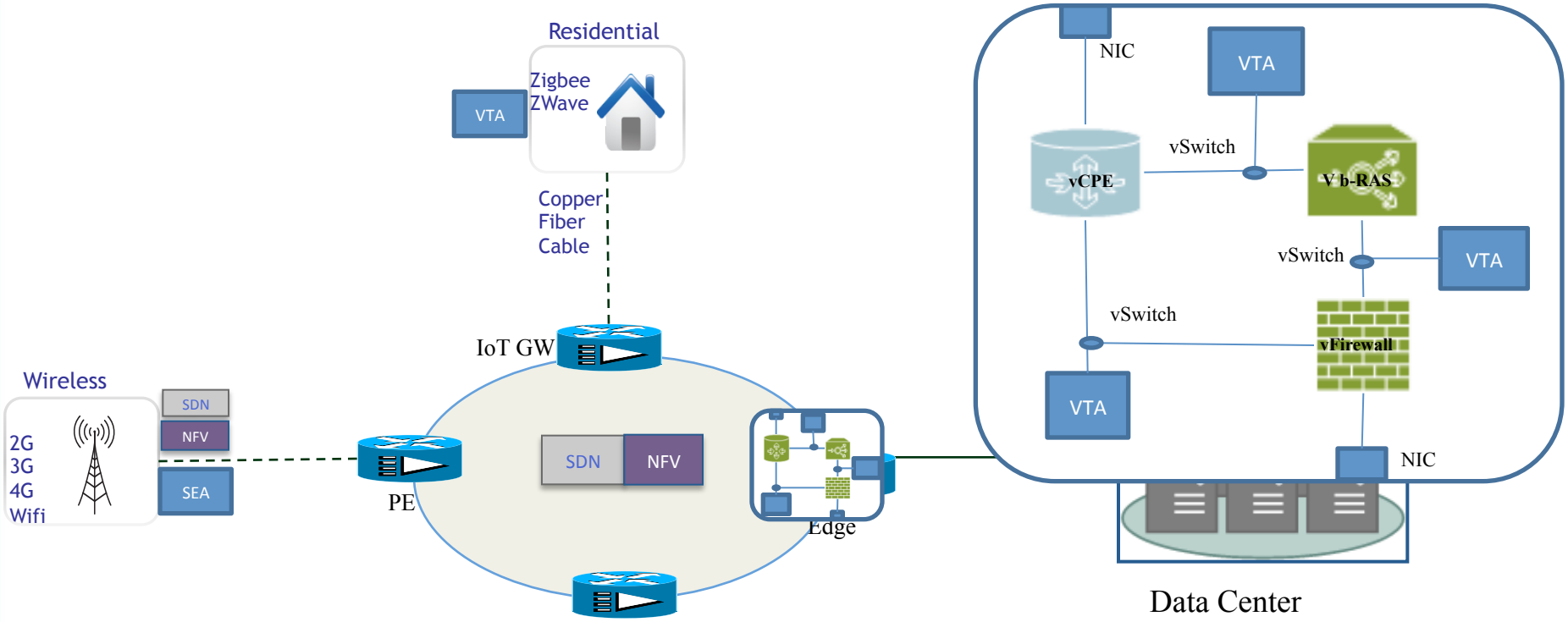
The reliability of NF1 and that of NF2 are not independent.



An example of virtualised network functions' deployment

  - Software upgrade requirements will also be provided.

E2E Active Test Measurement



- Service Activation
- SLA Validation
- E2E QoE measurement
- Capacity Planning
- Fault Diagnosis

How NFV Impacts Active Testing For Live Networks?

- Multiple VNFs on the same physical server
- VNFs may be re-provisioned or moved to different servers as a result of failures or auto-scaling
- Service chains may be ever changing, depending on load conditions

- Active monitoring probes must not degrade the performance of other VNFs in NFV environment
- Probes must move automatically to keep up with the VNFs and services they are monitoring
- Active Monitoring probes must be virtual

Active Monitoring Components

VTA

Virtual Test Agent

- L2-L7 Traffic Generation
- Small footprint
- Fault detection
- Portability within NFV environment

Test Controller

- Controls & tracks test execution
- Tracks resources for test agents
- Interfaces to NFV/ IoT SP back end

Test Results Analytics Module

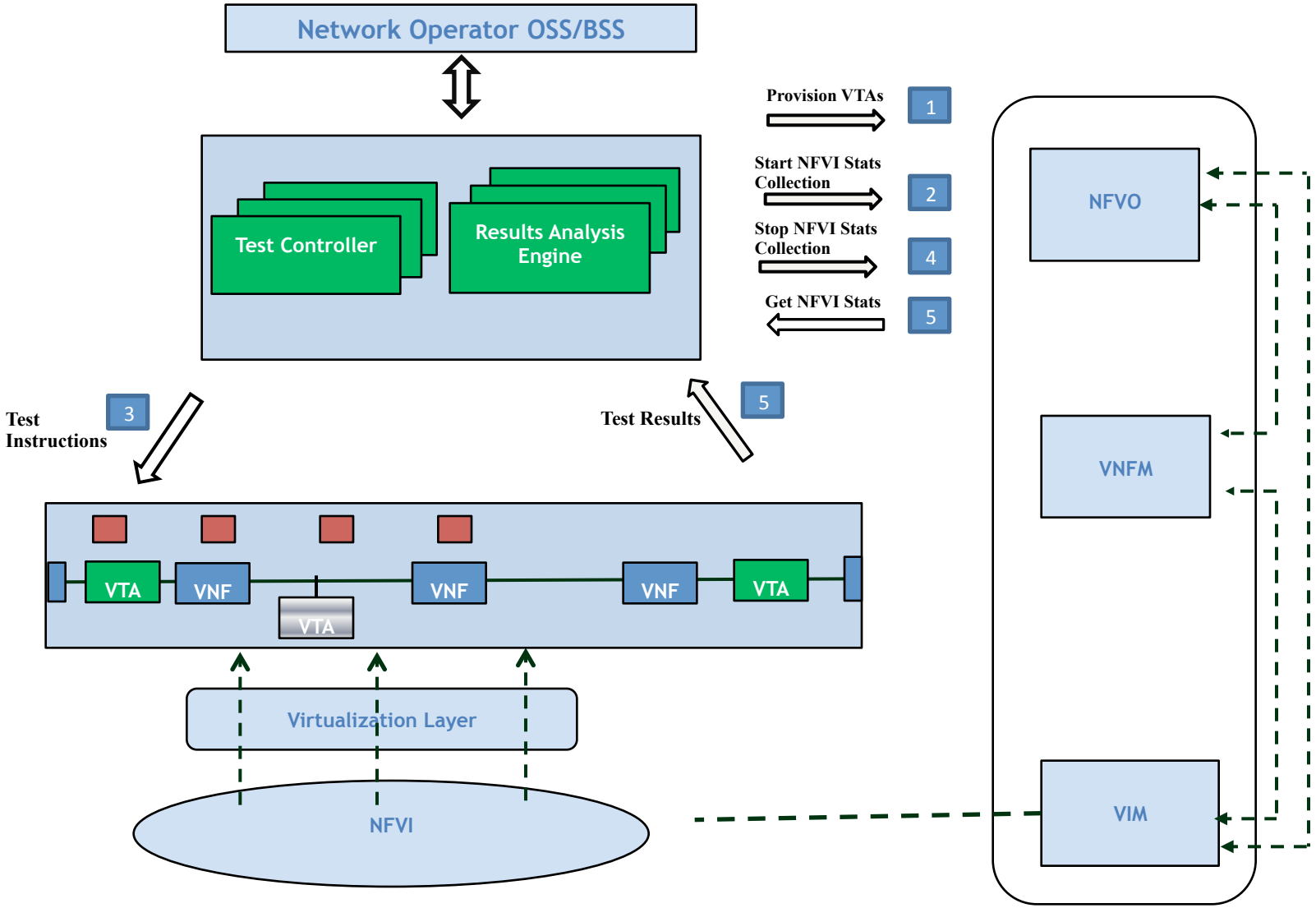
- Interfaces with VTA, VIM & NFVI to obtain stats
- Provides results & insights to test controller

Business impact of Active Monitoring Test Solution for NFV

Reduced OPEX

- Optimize the number of required active test agents
- Extreme automation of live testing framework
- Improved result analysis and analytics

NFV Active Monitoring Architecture



Schedule and upcoming events

- **NFV#10 in Sanya, CN**
  - May 18th – 22nd
- **NFV#11 in San Jose, US**
  - July 27th – 31st
- **REL is not planning physical interim meetings**
  - Weekly GTM from 4:00 to 6:00pm CEST
- **Publication of documents planned for autumn 2015**

Participation only for ETSI NFV members

Welcome to the World of Standards

ETSI World Class Standards

QUESTIONS?