2017

# Next-Generation Assurance in NFV Networks

Huawei Technologies Co., Ltd.

## The advent of digital economy

In the advent of digital economy, Communications Service Providers (CSPs) are seeing their profits stagnate, while watching the over-the-top players erode their revenue. The changing trend of their users moving to alternative services was one of the reasons for their decision to start on the journey to digital transformation.

Service innovation and customer experience are the main drivers for their digital transformation, which requires a cultural and technological transformation. Network virtualization will play an important role in CSPs technology transformation.

The main benefits that network function virtualization (NFV) brings in are: reduced time to market, agility, innovation, open ecosystem to avoid vendor lock-in, and future CAPEX and OPEX reduction. On the other hand, operational transformation brings a lot of challenges that CSPs need to overcome too.

## The challenges

Currently, some of the CSP's top priorities are network's reliability and performance. Telecom networks must be always-on and guarantee always-on services, no matter what technology is used, because society, business and industries depend on reliable connections for both routine and critical communications.

Product or service development within the telecommunication industry has traditionally followed rigorous standards for stability, protocol adherence and quality, reflected by the use of the term carrier-grade to designate equipment demonstrating this reliability. Over decades, telecom service providers have engineered an extensive range of sophisticated features into their networks, to the point where they guarantee their high reliability.

Telecom service providers have built their networks, reputations and revenue streams on a foundation of carrier-grade reliability.

By decoupling software and hardware and introducing the virtualization layer, a multi-layer environment will be created and in most cases each layer could be delivered by different suppliers. This will bring a lot of new challenges to CSPs regarding assurance, such as:

- Lower reliability
- Security risks
- Interoperability issues
- Difficulties in fault demarcation
- Need for new skills and processes

Taking into consideration these big changes due to virtualization layer and the dynamic environment, there is a need for new generation service assurance solutions.

Suppliers will also play an important role in this transformation journey, since they can assist with their global experience, product competence, and expertise, providing new type of services and systems to support CSPs in each step.

## Requirements for NFV assurance

Practically, there are 3 key areas in achieving NFV-driven carrier-grade reliability: product, network deployment (design and integration) and network maintenance. For example, application should be deployed with resilience (i.e. N+M, 1+1), the Cloud OS should support VM migration, servers should have multiple NICs, storage with multiple controllers, and so on.  Network designers should consider VNF in Pool, distributed design, proper dimensioning, resource clustering, security and network resilience.

Even if a redundant network is deployed, failures can happen, thus network maintenance and assurance capabilities are very important to minimize service downtime. That's the area where this white paper focuses on.

A carrier-grade network guarantees a five-9s availability standard, allowing no more than 5.27 minutes of downtime per year per service. If there is just one failure in the system, the NOC (Network Operations Centre) should get notified and proceed with remediation in less than 5 minutes so that the five-9s target can still be met. That's not a new challenge, but the introduction of virtualization into the network adds complexity. Hence there is an overwhelming need to automate the entire process, including quick service recovery processes, and to rely heavily on resiliency to provide seamless transfer from the failing element to healthy elements.

In legacy networks, reliability, redundancy and recoverability were managed in a reactive manner focused on fault detection and troubleshooting.  Over the years, CSPs introduced more proactive tools, applying analysis of customer and network data to determine potential network performance issues, which enabled faster detection and resolution of faults, often before the customer became aware of them. The next stage in network management is automating the detection and correction of issues through the application of "smart" or artificial intelligence technologies. These solutions provide automated responses where the network components react to policy-based thresholds, enabling greater complexity in the network and decreased operations intervention.

NFV will accelerate the movement from monitoring to real-time intelligence and analytics that respond to preset policies to enact orchestrated alterations in the network. Zero-touch operations and automation is in an incubation phase and it may take years for CSPs to see it materialized, thus service assurance still requires significant manual intervention. Therefore, they will need to enhance the current re-active maintenance capabilities for fault management and then introduce gradually smart maintenance capabilities.

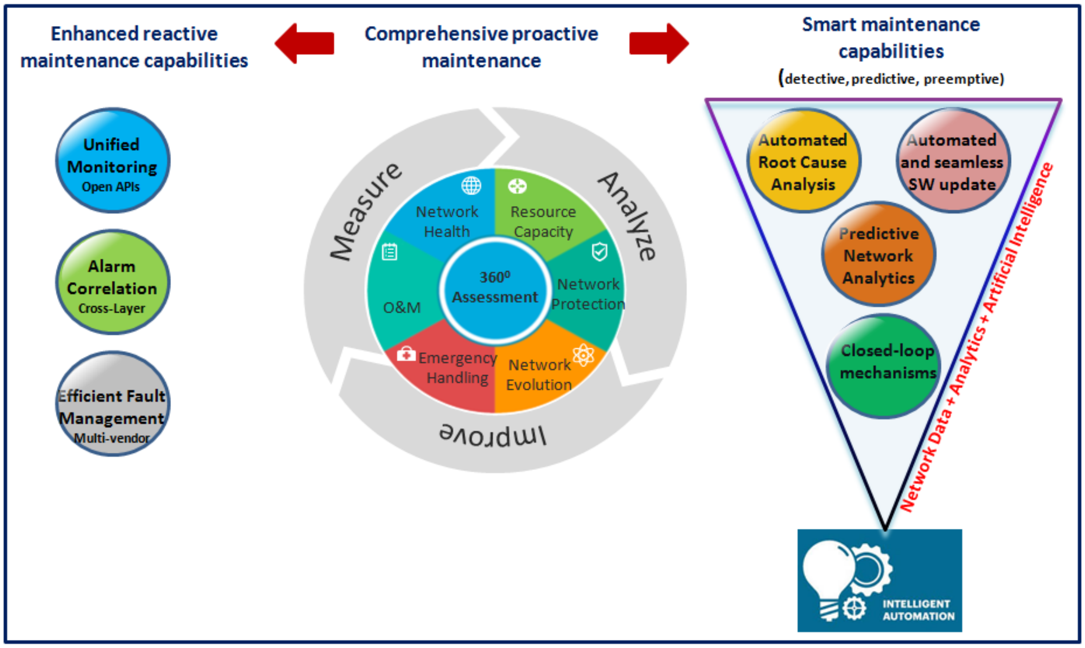

Enhanced reactive maintenance capabilities
Comprehensive proactive maintenance
Smart maintenance capabilities
(detective, predictive, preemptive)
Unified Monitoring
Open APIs
Alarm Correlation
Cross-Layer
Efficient Fault Management
Multi-vendor
Measure
Analyze
Improve
Network Health
Resource Capacity
Network Protection
Network Evolution
Emergency Handling
O&M
360⁰ Assessment
Automated Root Cause Analysis
Automated and seamless SW update
Predictive Network Analytics
Closed-loop mechanisms
Network Data + Analytics + Artificial Intelligence
INTELLIGENT AUTOMATION

Figure 1: Next generation NFV assurance capabilities

Considering the above challenges, some of the main requirements regarding NFV assurance and network maintenance are described below:

### 1. Unified monitoring

First of all, it’s important to avoid information silos and alarms, events and logs should be propagated to the upper layers, if possible, thus achieving unified alarm and log monitoring. It seems like a basic requirement, but real experience shows that it is a very complex task. Most of the existing issues are related to interoperability, mainly due to proprietary APIs. If there is no unified monitoring, network engineers will need to log into each node separately, collect information and then perform troubleshooting. Alarm and log collection in a single place will enhance and shorten the fault demarcation process.

Finally, network virtualization will not happen overnight, and CSPs will need also to manage hybrid network for several years. Unified monitoring should also consider alarm and log collection from physical network functions.

### 2. Alarm correlation

Once the important step of unified monitoring has been achieved, CSPs need to face another challenge. There are now too many alarms in one place and some of them appear multiple times. That complicates fault demarcation even more.

Smart filters or pre-defined rules are needed to correlate the alarms automatically and help network engineers to identify quickly the potential root cause. The list of the rules/policies can always be expanded based on experience and past incidents.

### 3. Automated root cause analysis

Alarm correlation needs someone to analyze the results manually and identify the root cause. The ideal scenario would be CSPs to have an automated process to output the root cause analysis. That output would come from a server that analyzes existing alarms and logs that have been collected, using a fault library as a reference. The fault library can be expanded with more cases in the future.

The automated process will reduce manual intervention and eventually the labor cost.

### 4. Closed-loop mechanisms

A network should be designed properly for its resilience to avoid single point of failure. Even if a redundant network is deployed, failures must inevitably happen, so, it is critical for the operations to follow a proactive, predictive and preemptive approach. Most fault conditions which are identified by network probes and management tools should be responded to by pre-programmed event responders (autonomics – big data analytics), to the extent possible. There is huge amount of data that CSPs need to digest and analyze in real time, which is not doable without analytics engine and policy rules. These elements are very important for the closed loop automation. The network should be able to recover automatically where possible (VM migration, reconstruction, scaling etc).

A robust network shouldn't be vulnerable to any kind of threats. For example, if an important service’s KPIs deteriorated the system should identify it immediately, isolate the faulty VM or VNF, and migrate traffic to the healthy components.

### 5. Fault Management capabilities in multi-vendor  environment

CSPs need to enhance their capabilities and processes to manage efficiently all elements in this multi-vendor ecosystem. Whenever there is an incident, CSPs need to be in a position to promptly answer the questions:

a. *Whose fault is? Who should I escalate the trouble ticket to?*
b. *Who should recover the service?*

In the past, application and equipment were provided by one supplier, thus any trouble ticket was sent to that one supplier. Now, there may be at least three or four different suppliers who provide the application, virtualization layer, servers, and storage. We also need to consider that each one of them may support different SLAs for service restoration and resolution. It’s a fact that multi-vendor management has been impacted in NFV and CSPs need to consider it thoroughly.

Service continuity remains the priority for the CSPs, thus in case of failures, their focus is mainly on application layer, but fault may lie on infrastructure and this could cause a trouble ticket ping-pong game. From one side new tools for fault demarcation could help, as described earlier, but multi- vendor management has its own challenges and CSPs could build a team of experts to handle these cases.

The ideal scenario would be the application supplier to offer “premium customer support services” by becoming the single point of contact for the CSPs, regardless where the fault is. In this role, the service provider would be responsible to perform the initial demarcation, coordinate with the infrastructure suppliers for service restoration and resolution, and govern trouble ticket management and reporting.

Support from other product suppliers will not be totally eliminated, but the SPoC role could make the fault management process more efficient and shorten the resolution time.

### 6. Predictive network analytics

As mentioned earlier the evolution from proactive to smart maintenance is underway and this requires near real-time network data, analytics and artificial intelligence. Predictive networks analytics can be used for different tasks, such as service assurance, capacity planning and efficient resource utilization. Some ways to use these systems are:

- to predict potential capacity bottlenecks
- to identify grey failures and security loopholes
- to manage physical and virtual resources efficiently

### 7. Automated and seamless software upgrade

Each supplier provides software packages with bug fixes and requires CSPs to load them into their network regularly. Suppliers may have different release dates and frequency. One of the CSP’s responsibilities is to synchronize and plan these activities.

In the past software upgrades were done by one supplier per node, but now CSPs need to consider the impact of a new software package on any layer, before it’s actually loaded in the live network. Thus, multi-vendor verification (vertical stack) is recommended in a CSP’s test bed, mirroring the real network solution. Alternatively, suppliers may provide their own NFV Lab accessed remotely (Lab as a Service).

The software upgrade process should ensure that it doesn’t cause service downtime and a quick rollback procedure should be in place. It also requires skills and processes more in line with IT’s agile DevOps methods than traditional network operations practices.

Some of the requirements regarding software upgrade are:

- Online software update capability
- Automated testing of the new software in order to detect issues quickly and before the end users
- Automated rollback option in case of failure
- Capabilities to migrate only small amount of traffic to the new instances until services are verified
- In case of VNF pool, isolate traffic towards the ready-to-be-upgraded VNF automatically

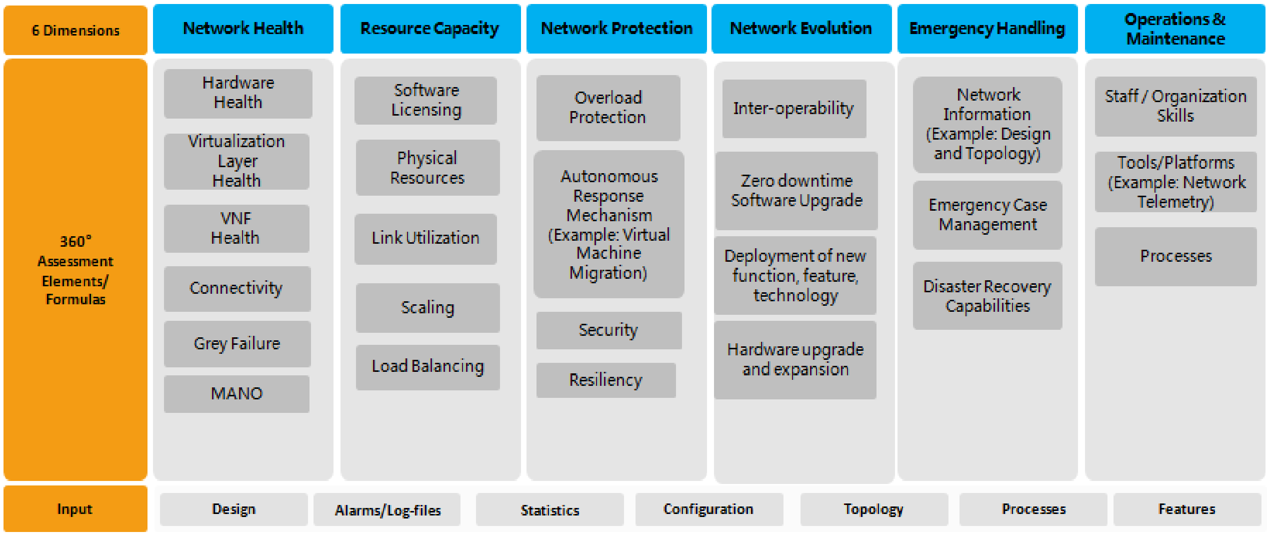
## 8. Proactive maintenance and continuous improvement

Once the virtualized appliances handle live traffic, a continuous improvement process should start. This requires CSPs to perform regular network health check in order to identify current issues, potential threats and other network weaknesses. Virtualization makes network's health assessment more challenging.

The traditional break-and-fix mode is not the right way to maintain the network. CSPs and suppliers usually are picking specific elements for monitoring, since there is not a standard way to monitor the network or a well-defined framework to describe what exactly needs to be checked or what the best practices are.

In a lot of cases, this is proven to be unstructured, inefficient, insecure, and could cause long time recovery and high risk. If CSPs don't look into these challenges they will risk customer churn, decrease market share and profit.

The first goal is to build a comprehensive assessment framework, which provides a 360° in depth view, covering different areas such as performance, security, network risks or even processes and capabilities.



| 6 Dimensions | Network Health | Resource Capacity | Network Protection | Network Evolution | Emergency Handling | Operations & Maintenance |
|---|---|---|---|---|---|---|
| 360° Assessment Elements/ Formulas | Hardware Health | Software Licensing | Overload Protection | Inter-operability | Network Information (Example: Design and Topology) | Staff / Organization Skills |
| | Virtualization Layer Health | Physical Resources | Autonomous Response Mechanism (Example: Virtual Machine Migration) | Zero downtime Software Upgrade | Emergency Case Management | Tools/Platforms (Example: Network Telemetry) |
| | VNF Health | Link Utilization | Security | Deployment of new function, feature, technology | Disaster Recovery Capabilities | Processes |
| | Connectivity | Scaling | Resiliency | Hardware upgrade and expansion | | |
| | Grey Failure | Load Balancing | | | | |
| | MANO | | | | | |

| Input | Design | Alarms/Log-files | Statistics | Configuration | Topology | Processes | Features |
|---|---|---|---|---|---|---|---|

Figure 2: Carrier Grade NFV Reliability Assessment Framework

Once the network is assessed, CSPs will be able to identify the key areas that need improvement, and apply the appropriate solutions to minimize risks and mitigate any future incidents. Some of the potential solutions could involve network optimization, troubleshooting, training, new processes, new features and tools, hardware or software license expansion and so on.

## Conclusion

Network reliability is very important for CSPS to maintain always-on services. NFV introduced new challenges into the networks and new capabilities are needed in NFV assurance and network maintenance.

Automation will play a key role in NFV assurance, but first CSPs and suppliers need to take some concrete steps towards this goal. Operational transformation is a journey and collaboration between them is essential.

Even though human intervention will still be needed, CSPs should focus on proactive maintenance to detect and predict network failures quickly and gradually introduce smart systems that use network data, analytics and artificial intelligence to automate network operations.