White Paper

Overcoming the Service Assurance Challenge of a Hybrid NFV Environment

Prepared by

James Crawshaw
Senior Analyst, Heavy Reading
www.heavyreading.com

on behalf of

TEOCO

www.teoco.com

October 2016

Introduction

So far, service assurance has had a somewhat low profile in the industry discussions surrounding network functions virtualization (NFV). However, as operators gain more experience with live NFV deployments, service assurance will likely become a more critical component of hybrid and virtualized networks.

On the one hand, the dynamic configuration changes inherent in NFV could lead to unexpected impacts on network and service performance. At the same time, separating physical elements from their software-defined functions, and then recombining software and hardware in different permutations and multiple layers, introduces greater complexity that will make service assurance functions, such as root cause analysis, a greater challenge.

In its SDN-NFV reference architecture document, Verizon notes that traditional service assurance mechanisms, which largely comprise a combination of network management system (NMS), element management system (EMS) and logging functions, are poorly defined and inconsistently implemented.

Today's service assurance solutions are generally statically-defined, point solutions, often isolated from provisioning systems. Such solutions are ill equipped to cope with the dynamic nature of virtualization. This calls for a rethink of service assurance to take advantage of new data analytics techniques and enable true real time management of the network.

While the end-to-end orchestration capability of NFV systems handles configuration and provisioning, an adjunct but tightly-integrated service assurance solution is needed to provide the other key telecommunications management network tasks: fault and performance management.

Automated service assurance will become a key enabler of the agile, low-touch, end-to-end service orchestration solution to which service providers are striving in their NFV implementations. To "close the loop," the service assurance system must collect and analyze the relevant data, pinpoint the problem and then recommend remedial actions.

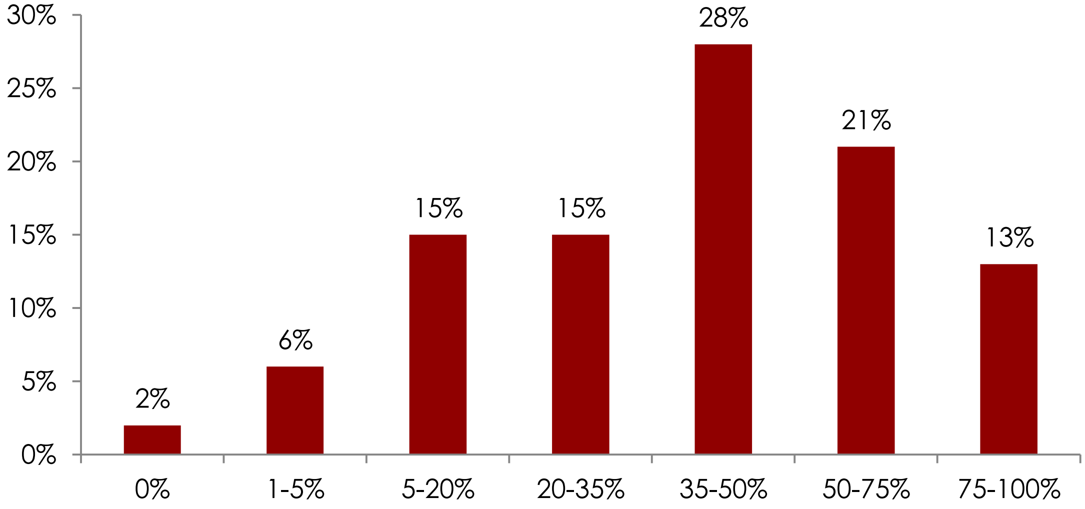
With sophisticated algorithms, operators can also take advantage of predictive analytics applied to network and service performance. By combining closed-loop automation with predictive analytics, service providers can increase their operational agility and improve quality of service (QoS), while also keeping operating expenses under control.

Hybrid NFV Requires an End-to-End SA Solution

Hybrid physical and virtualized networks will persist for many years and some core infrastructure may never be successfully migrated to software running on commodity hardware. Management and orchestration (MANO) will have its own closed-loop capabilities, but in hybrid networks the NFV MANO is not planned, and will not be able, to support end-to-end network and service monitoring.

AT&T, one of the most ardent proponents of NFV, in its ECOMP Architecture White Paper set the ambitious goal of virtualizing 75 percent of its target network uploads by 2020. However, AT&T hasn't specified what proportion of its total network footprint these "target network uploads" comprise. **Figure 1**, which is based on Heavy Reading's 2015 NFV Strategies Survey, suggests that only a third of operators expect to have more than half of network traffic running on NFV by 2020.

Figure 1: What Percentage of Your Company's Total Network Traffic Will Run on Virtualized Network Functions by 2020?



Source: Heavy Reading

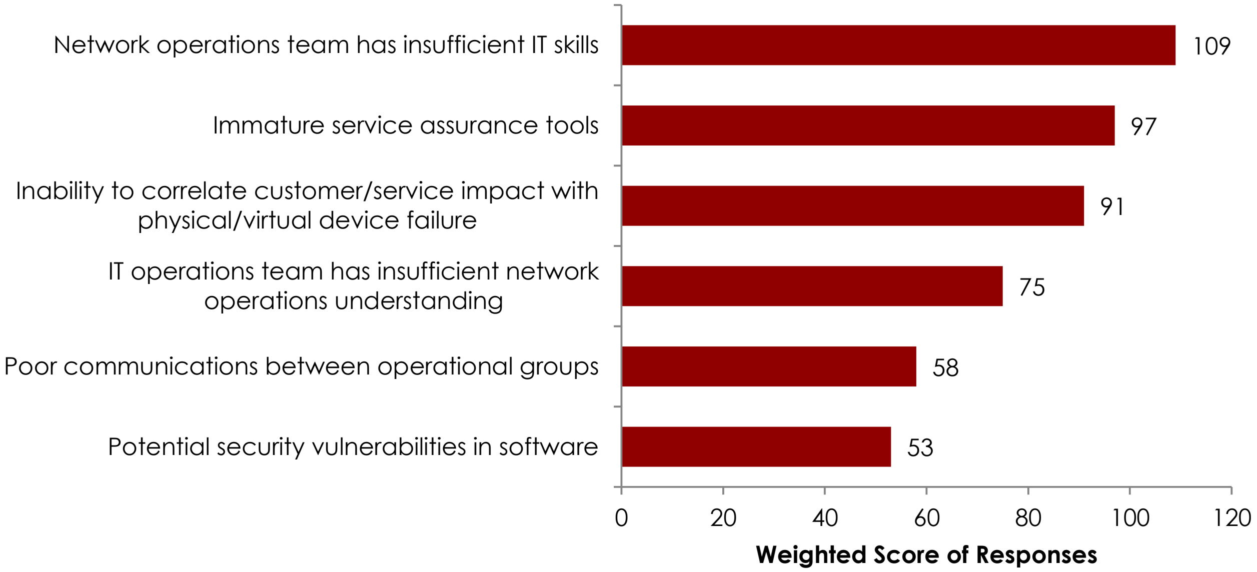
So for the near future, services will be fulfilled by a mix of physical and virtual network elements. Consequently, the service assurance system must have a unified view of network topology, both physical and virtual, across different domains (e.g., fixed and mobile), myriad technologies and multiple network equipment vendors.

Frequent configuration changes of the NFV environment mean that periodical, nightly updates to the operations support system (OSS) of network resources are inadequate. The service assurance solution for NFV must operate in near real time. Static, non-real-time, legacy service assurance solutions cannot support dynamic, NFV-enabled networks.

Many networks today have different systems for service and resource management. Moreover, operators typically have separate OSS for different services (e.g., fixed broadband, mobile) as the costs of integration have outweighed the expected benefits of systems consolidation. For hybrid NFV, however, a unified, holistic, end-to-end view of services is needed.

Figure 2, drawn from Heavy Reading's 2015 MANO and OSS Survey, shows that service assurance tools are a top concern among operators regarding the implementation of NFV alongside staff skills and difficulties in correlating service impact with network device failures.

Figure 2: What Are Your Company's Top Three Operational Concerns Regarding NFV?



Source: Heavy Reading

A New Approach to SA for a Hybrid NFV World

While different operators and different vendors clearly have their own views on how to design the ideal service assurance solution for hybrid NFV networks, there is some consensus on the key pillars: greater automation, enhanced analytics and better integration with other management systems.

Automation

Given the dynamic nature of NFV-based networks, operators are looking to enable greater automation in their management. In the "holy grail" of closed-loop automation, the service assurance system not only collects and analyzes data, but also pinpoints the network and service issues and then makes recommendations. These recommendations are passed on, either to the NFV orchestrator or, for the legacy/ physical side of the network, to the service fulfillment systems. Closed-loop automation thereby reduces the mean time to repair for the network.

Such closed-loop, or automated, resolution can use performance measurement data, fault data and even customer experience measurements to identify problems before they have a significant impact on the service level. These problems can then be fixed by issuing requests to the MANO or a traditional EMS, with a minimum of human intervention. This automation should enable the network to be "self-healing" in the short term, but also ensure a more highly optimized network over the long term.

A key requirement for such self-healing properties is that the service assurance systems are kept up to date on the state of the network in near real time. This represents a significant increase in the amount of data the service assurance system has to store and analyze.

Analytics

The dynamic nature of an NFV network means that hand-written rules for establishing root cause analysis (RCA) will not suffice. Instead, algorithms or even artificial intelligence and machine learning must be used to parse a greater data set.

Combining service and resource management into one unified system can enable operators to correlate across data sets and aid RCA. By identifying and fixing problems at the lowest possible level in the network architecture, operators can save themselves both time and money while reducing mean time to repair (MTTR) and decreasing network downtime.

As well as enhancing the operator's ability to discover the cause of network problems, analytics can predict where the network might malfunction next, based on an analysis of historical data and associated faults. This will enable operators to take preemptive actions to prevent interruption of service, much like the preventative maintenance of jet engines or elevators.

Analytics data should encompass both bottom-up and top-down inputs. Bottom-up inputs include fault management data (e.g., infrastructure events, logs) and performance management data (active and passive monitoring). Top-down inputs include application and service level information (including customer-reported issues, data from probes, usage information, such as xDRs, etc.) to determine service health.

Integration

In implementing NFV, service providers must avoid the trap of considering it as a separate silo to their existing network. Their service assurance solution should be cross-domain, encompassing both NFV and physical networks. In physical networks, service assurance should provide a common view across multiple services, such as voice and data. It should even span the network and IT assets of the operator providing monitoring capabilities and cross-layer correlation. Within the NFV environment, as well as collecting traditional data (such as throughput, drop rates and errors), CPU utilization of the underlying computing and switching hardware should be monitored. The MANO will be a key data source for service assurance, as well as its virtualized infrastructure manager (VIM) and VNF manager subcomponents.

Within the OSS stack, service assurance should, of course, be integrated with the policy management systems that define the service-level agreements (SLAs) that the service assurance system is required to meet. Additionally, service assurance should be more closely integrated with service fulfillment in order to enable operators to rapidly provision and assure services. The concept of orchestrated assurance was developed by ETSI in its NFV PoC #39, which describes virtual service assurance management as "an E2E service assurance fabric that spans NFVI-PoPs and WAN underlay." This approach aims to bridge the gap between service fulfillment and assurance that typically exists in legacy OSS today.

Another aspect of integration that operators must consider is greater integration and cooperation between their network operating center and engineering teams. With NFV, the lines between these two departments start to blur as, for example, the concept of self-healing means that problems are fixed within the operations environment without the need for engineering to intervene. The service assurance system should serve both teams within an operator and through the use of common tools and dashboards facilitate inter-departmental collaboration.

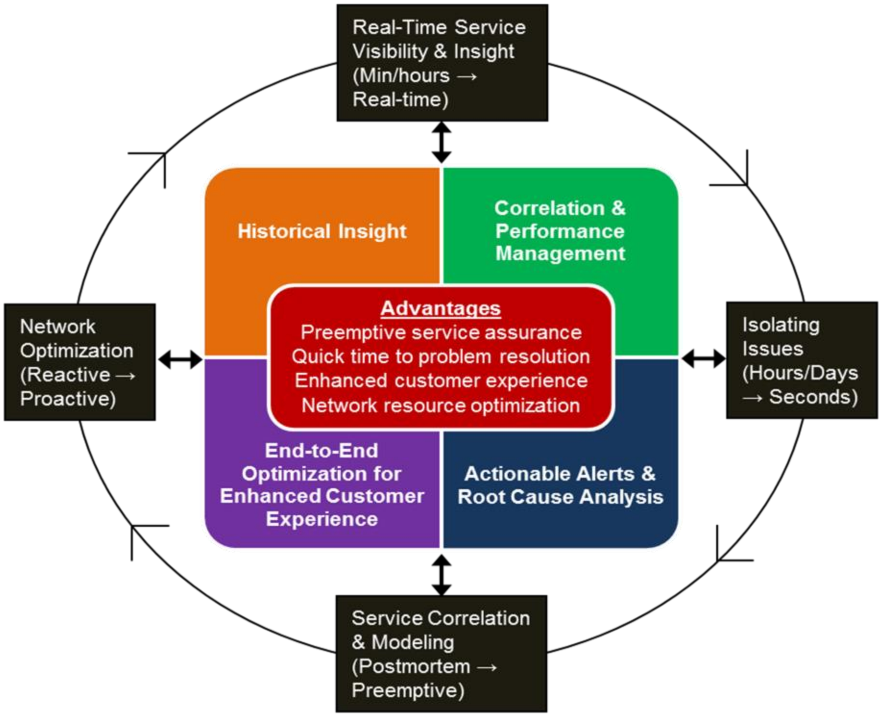
Key to enabling better integration of service assurance solutions are the application programming interfaces (APIs) and common information models that allow multiple vendors' systems to coexist on one network. Traditional service assurance solutions were typically designed as closed systems that required proprietary integration with other OSS and network systems. This imposed a large cost burden for operators. Under NFV, the proposition changes such that standards bodies and consortia are defining APIs to which solution vendors must conform. At the service assurance level, these APIs could be for alarm management or processor performance data. Service assurance systems should support open APIs to enable a microservices-based architecture.

Closely aligned with the API concept is the notion of a common information model for network infrastructure and services. It is unlikely that the global telecom industry will finally agree on a single data model. Instead, we expect that several different data models will emerge from standards bodies and that middleware tools will enable them to be mapped together. Examples of such data models include TM Forum's Open Digital Ecosystem data model, the IETF's YANG and OASIS' TOSCA.

Service Assurance for Hybrid NFV

As **Figure 3** shows, a service assurance solution for a hybrid NFV environment uses a large data set (including historical and near real-time data) to perform correlation analysis and RCA, and make recommendations to preempt a network problem or rapidly resolve a problem that has manifested itself.

Figure 3: Service Assurance Solution for Hybrid NFV Environment


Real-Time Service Visibility & Insight (Min/hours → Real-time)
Historical Insight
Correlation & Performance Management
Advantages
Preemptive service assurance
Quick time to problem resolution
Enhanced customer experience
Network resource optimization
Network Optimization (Reactive → Proactive)
Isolating Issues (Hours/Days → Seconds)
End-to-End Optimization for Enhanced Customer Experience
Actionable Alerts & Root Cause Analysis
Service Correlation & Modeling (Postmortem → Preemptive)

Source: Heavy Reading

By combining closed-loop automation with predictive analytics, service providers can increase their operational agility and improve QoS, while also keeping operating expenses under control.

Business Benefits of Hybrid-NFV-Ready SA

A service assurance solution that meets the criteria outlined above should enable operators to rapidly identify problems and keep up with the constantly changing state of a virtualized network. By enabling closed-loop resolution, operators should be able to reduce the time to resolve network errors. Increased automation should additionally allow for a reduction in the operating costs of the network.

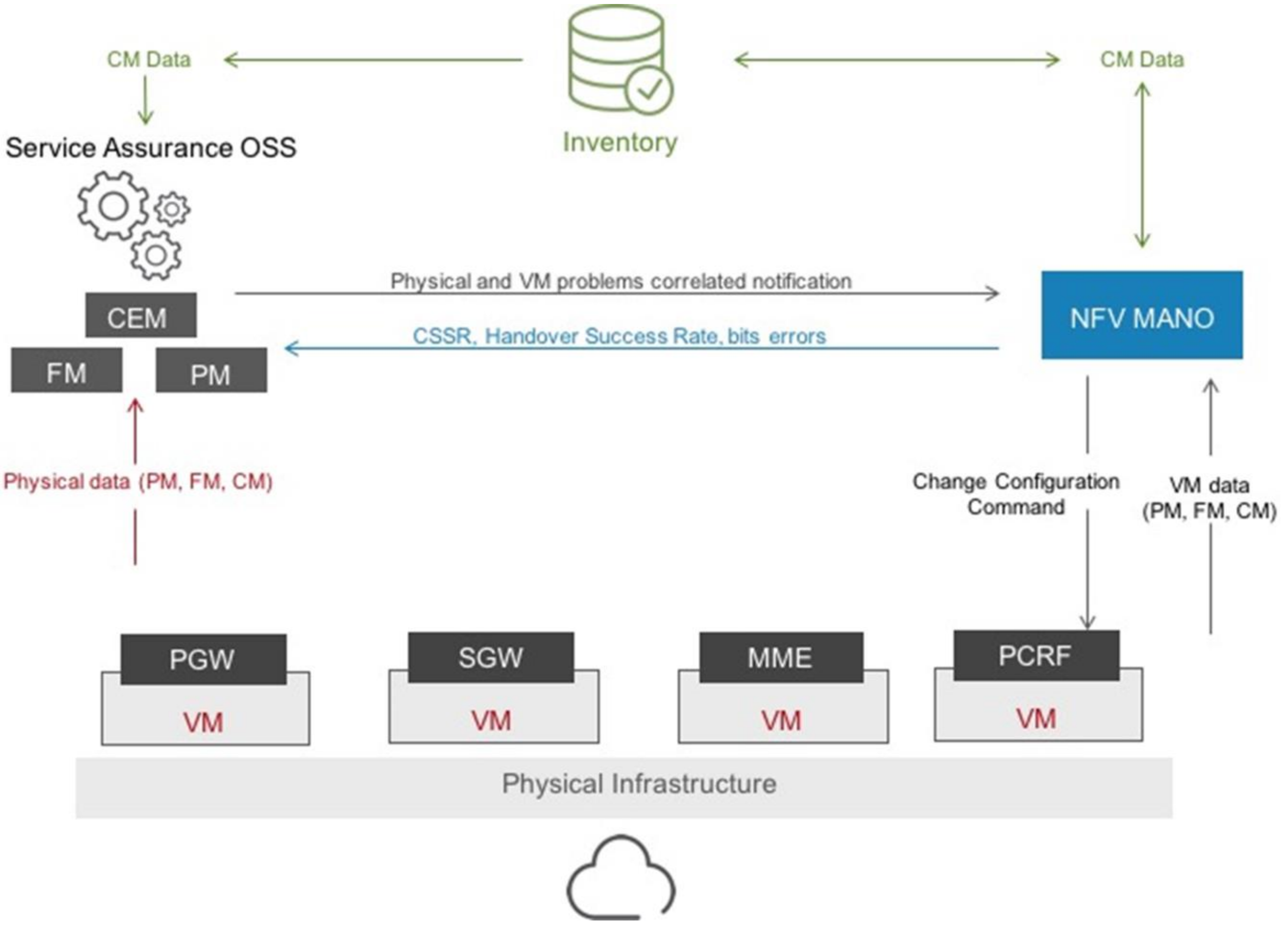
The most important benefit is improved QoS and customer satisfaction. At the end of the day, service assurance comes down to one thing: Is the customer getting the quality of experience (QoE) they deserve, regardless of whether this is delivered with virtualized or physical infrastructure? If the answer is yes, then the operator stands a better chance of winning and retaining the new customers it hopes to win with hybrid-NFV-based services.

Highly-automated service assurance is key to enabling operators' on-demand, self-service offerings. Service assurance closely connected with service fulfillment enables telcos to provision and assure services in minutes, not hours or days. This is key as our operator surveys increasingly show that service agility and flexibility – or more simply, time to market – is the main business driver for NFV in the first place.

Practical Use Case Example of Hybrid NFV SA

Figure 4 shows a closed-loop, service-assurance-led automation in a hybrid network, based on a TM Forum NFV Catalyst program. In this "real life" scenario, one of the physical servers that support the virtual infrastructure is malfunctioning.

Figure 4: Healing a Physical Server Malfunction


CM Data
Inventory
CM Data
Service Assurance OSS
Physical and VM problems correlated notification
CSSR, Handover Success Rate, bits errors
NFV MANO
CEM
FM
PM
Physical data (PM, FM, CM)
Change Configuration Command
VM data (PM, FM, CM)
PGW
VM
SGW
VM
MME
VM
PCRF
VM
Physical Infrastructure

Source: TEOCO

The VIM within the MANO is aware that a problem exists, but is unable to pinpoint the specific hardware to blame as the virtualization layer makes it both hardware agnostic and hardware ignorant. However, the physical servers are monitored by an existing service assurance system, along with other network infrastructure.

By correlating performance data collected from the MANO together with data collected directly from the underlying physical server, the service assurance system is able to get an end-to-end view of the problem to pinpoint the problem and instruct the MANO how to remediate it.

Below we outline each of the steps in the process:

1. Key performance indicators (KPIs) on the virtualized Mobility Management Entity (vMME) show decreased call setup success rate (CSSR) and decreased handover success percentage. At the same time the dropped call rate increases.

2. The calculated IP throughput error rate on the virtualized Serving Gateway (vSGW) starts to increase.

3. The service assurance systems uses trending thresholds on the data from the two steps above to conclude there are problems in the vSGW and vMME.

4. Service assurance detects a sudden voltage drop in a physical server.

5. Service assurance uses its configuration model to correlate the physical server to the vSGW and vMME.

6. Service assurance sends a message to the MANO about a problem on a specific physical server.

7. MANO changes virtual machine (VM) configuration, so the relevant VM functions are moved to a different physical server.

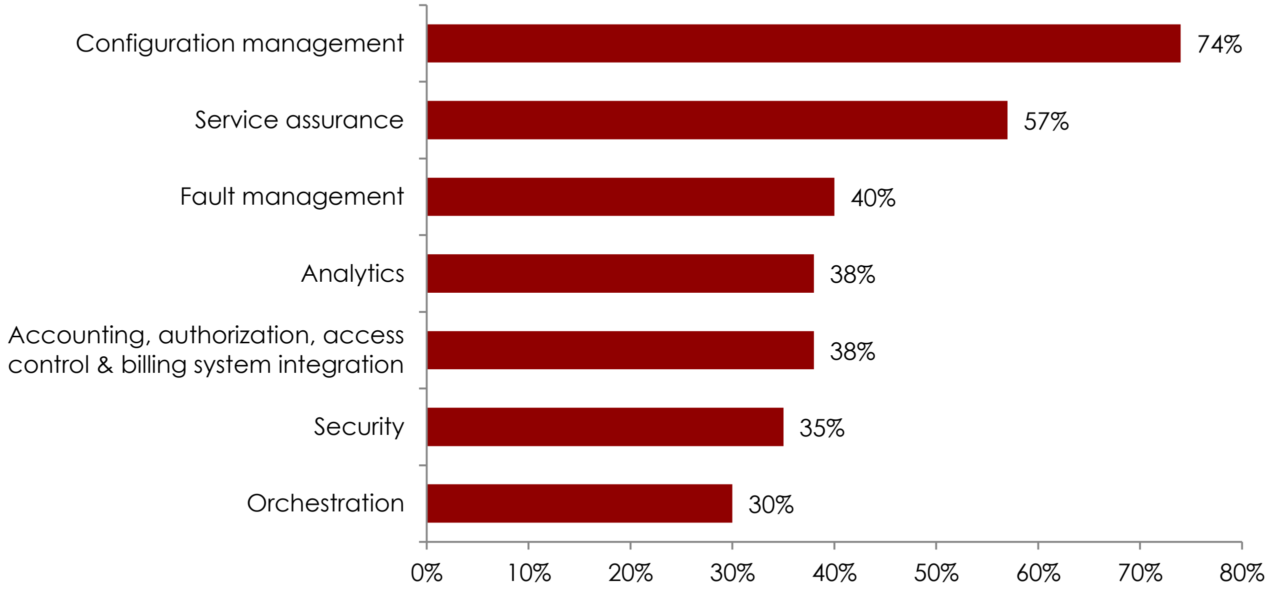
8. Service assurance creates an automatic Trouble Ticket for a technician to fix the physical server.

The example above demonstrates closed-loop healing in a hybrid network running on both physical and virtualized infrastructures. Closing the loop is an ongoing process that requires closely tracking and monitoring critical data to ensure optimal service performance.

Conclusion

Service providers have traditionally invested in service assurance as an afterthought. Investment in order management, service fulfillment and billing have typically take priority as these elements are critical to provision and bill for their services. Investment in service assurance typically came much later when QoE became a problem. However, as **Figure 5** shows, service providers are taking a different approach in their NFV deployments and recognize the importance of service assurance.

Figure 5: Network Management Functions That Should Be Included Prior to Deployment of SDN/NFV



Source: Heavy Reading

In an NFV world, service assurance is taking greater priority as operators realize its importance in delivering QoE in hybrid networks. Traditional service assurance is often based on data collection and analytical processes that are slow and error-prone. Clearly, these are not adequate for the near real-time, high-scale world of NFV. Service assurance is a key enabler of the end-to-end service orchestration solution to which service providers are striving in their NFV implementations.

Automation and agility are the cornerstones of NFV and software-defined networking (SDN). Service assurance and analytics plays a key role in supporting these initiatives by providing proactive and predictive intelligence upon which to act. To provide an end-to-end service assurance of a hybrid network, the solution must correlate across legacy network information (alarms, traps, etc.), NFV data (via the MANO or directly from VIMs) and SDN controller data.

Operators that reengineer their service assurance systems for a hybrid NFV world should be able to meet the high service quality demands their customers exact while keeping network operating costs under control. Simultaneous instantiation and assurance of virtual network functions is an imperative for delivering reliable services on demand – the key to the new revenue potential from NFV-based services.