NFV substantially changes how communication networks are designed, built, and managed. NFV pulls the functions necessary to run networks off proprietary hardware and places them on open-architecture-based servers and switches. This can significantly lower network operating costs, speed the introduction of new services, and introduce new business models for customers and virtual network operator (VNO) partners.

However, introducing NFV can be challenging:

- NFV represents a merging of telecom and IT; operations departments will require expertise and tools covering telecom functions, IT infrastructure, and their interrelationships.
- NFV, more than any previous new network technology, is experiencing a significant fragmentation of standards and software sources making up any given solution; this will lead to more inter-operability issues and a lack of clear ownership for solutions.
- Enabling the network to automatically decide on and execute real-time re-configuration changes that may negatively affect customer experience; it will take time and trial-and-error for network planning and operations departments to fully trust self-configuring networks.

The Need for Assurance in Virtualized Networks

To be successful, NFV networks will require more monitoring and troubleshooting insight than today’s non-virtualized physical networks. These needs factor in the following:

- Virtualized network elements (NEs) still deliver the same functions as physical NEs and therefore need the same assurance insight as their physical equivalents.
- VNF involves a virtualized IT infrastructure and a complex management infrastructure, both of which are potential sources of issues and will require monitoring and troubleshooting.

Enabling NFV to deliver maximum value will require the biggest change to associated assurance solutions in the last 20 years.
Enabling automatic NFV self-configuration decisions will require a real-time feed of telecom and IT infrastructure performance metrics/analytics.

The network flexibility enabled by NFV will introduce new services and business models that will require assurance insight.

Delivering the above could be a major problem for service providers looking to introduce virtualized networks. Traditional assurance solutions deployed in today’s networks cannot adapt to virtual environments because of the architectural limitations of hardware-based probes, slow response times, and closed architectures. The xSIGHT CEA portfolio introduces a new generation of assurance architecture. Its methodologies are purpose-built to address the requirements of hybrid physical and virtual networks.

Simple NFV Operator Evolution Model

A simple NFV operator evolution model has three stages:

- No virtualized functions
- Virtualized functions but with only manual orchestration
- Virtualized functions with real-time automated (self-configuring) orchestration

![Figure 1. Requirements to support VNF self-configuration](image)

The full benefits of virtualization will only be realized when NFV reaches the third stage. To deliver an effective, self-configuring NFV network, however, is not easy and involves the following two tasks:

- Enabling a policy control function to make re-configuration decisions that are good for business; for example, that either improve customer QoE and/or reduce operating costs
- The orchestrator, along with other NFV management infrastructure, implementing the network re-configuration decisions that the policy control function has determined

Figure 1 shows a simple outline of the closed loop monitoring required to support the policy control function in making real-time re-configuration decisions. An assurance solution must monitor the performance of the virtualized network functions and the underlying IT infrastructure. This solution must collect appropriate performance and financial metrics and forward these onto the policy control function where appropriate analytics will be used to make good network reconfiguration decisions. The orchestrator and other NFV management infrastructure will then implement the network configuration changes. The performance monitoring solution must also at this point be reconfigured to match the latest changes in the network and the monitoring closed loop process begins again.

Assurance Solution Requirements to Support Virtualization

In an NFV environment, both network functions and network interfaces between functions (which assurance tools need to access) are virtualized. To operate in an NFV environment, assurance tools must also become virtualized, or at least those parts of the assurance tools that interface to the network.

![Figure 2. Virtual NE functions and xSIGHT agents](image)

As mentioned previously, the assurance of virtualized network elements involves more than just performance monitoring and troubleshooting of the telecom functionality. The performance of the underlying IT infrastructure also affects the desired telecom functionality and must be included in the monitoring and troubleshooting coverage.

The xSIGHT CEA portfolio includes a family of data access agents able to operate in virtual environments to collect performance metrics by analyzing live traffic at virtual network interfaces (see Figure 2 for a typical configuration). It also includes agents that collect metrics on the performance of the virtual IT infrastructure. Thus, xSIGHT covers all performance aspects of the VNF environment. And, it supports the assurance of physical and hybrid (physical plus virtualized) networks, providing end-to-end visibility across the two domains.

Viavi Solutions innovated an NFV maturity model for network elements that has been adopted by TM Forum’s zero-touch orchestration, operation, and management (ZOOM) program.
Assurance Solution Requirements to Support Network Self-Configuration

Implementing NFV self-configuration consists of two tasks:

- The policy control function making the reconfiguration decision
- The orchestrator and other management infrastructure executing the reconfiguration

For the first task, an assurance solution will be critical in supplying appropriate performance data/analytics (relating to both the telecom functions and IT infrastructure) to the policy control function. This must be done in real time to ensure optimal policy control based on the current state—enabling network reconfiguration decisions that are good business decisions.

When the network reconfigures, the assurance solution must also self-configure in real-time to match it. This ensures that there is no gap in network monitoring and troubleshooting. To self-configure, the assurance solution must interface with the NFV orchestrator to receive information on how the network has reconfigured.

With both tasks, the assurance solution has effectively become part of the operational equipment chain, especially in the first case where the assurance solution is supplying intelligence that will be critical to ensuring the successful operation of the NFV network.

Figure 3 displays how the xSIGHT CEA solution integrates with NFV management infrastructure to support NFV self-configuring networks, highlighting the two linkages where information is exchanged. xSIGHT CEA architecture fully meets the requirements of supporting an NFV self-configuring network:

- Easy integration with NFV management infrastructure — xSIGHT has a fully open architecture and supports common API standards; when supplying intelligence to an NFV policy control function, xSIGHT can be configured to only deliver the required information, in the required format, at the required time
- Ability to respond in real time — xSIGHT architecture is memory-based, so the solution responds very quickly to both configuration changes and to the delivery of metrics/analytics; this ensures no downtime in monitoring and troubleshooting

xSIGHT CEA traffic analysis agents are proven in operator NFV field trials to access network traffic (and collect performance metrics) on virtual network interfaces

For NFV to deliver maximum value, associated assurance solutions must become self-configurable and integrated with operational equipment
Focus of NFV Industry Forums and Vendor Ecosystems

Having defined an NFV reference architecture, leading virtualization industry forums are now focusing on practical implementation aspects. Three areas of focus are:

- Evolution models for NFV
- The impact on associated network management tools/processes
- Interoperability across NFV solution components

Viavi actively participates in these efforts. Significant contributions include:

- The creation of a network equipment NFV maturity model that has been generally adopted within the TM Forum ZOOM program
- Definition and execution of the TM Forum NFV Catalyst project *Maximizing Profitability with NFV*, this demonstrates the performance data and analytics required to make good-for-business (NFV-enabled) network reconfiguration decisions (see Figure 4)
- Efforts addressing interoperability issues within vendor ecosystems including Intel Network Builders, VMware Alliance, and Alcatel-Lucent’s Cloudband

Why xSIGHT is the Preferred Choice for NFV Assurance

NFV networks will be widely introduced over the next few years. This will not happen, however, without the availability of new assurance tools appropriately equipped to support self-configuring, virtualized (and hybrid) environments. The xSIGHT CEA solution is such a tool and includes:

- Platform and data access agents able to operate on virtual machines
- Data access agents able to collect telecom and IT infrastructure metrics
- Real-time responses to required configuration changes and delivery of analytics
- Easy integration with NFV management infrastructure to exchange information

Supplementing this functionality with the virtualization expertise of the Viavi professional staff makes xSIGHT the preferred NFV assurance tool for many leading operators.