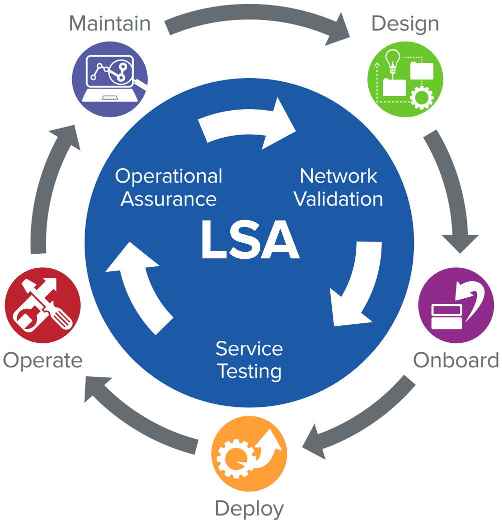
White Paper

# Transforming for NFV, 5G and IoT:

## The Need for Lifecycle Service Assurance

This whitepaper explores the key challenges of NFV, 5G and IoT transformations from the perspective of testing and assurance challenges and needs. To address these needs, Spirent is pioneering a new approach to testing and assurance called Lifecycle Service Assurance (LSA). The key principles which drive LSA are:

- Adoption of DevOps continuous testing across the service lifecycle
- Support for virtual, physical and hybrid networks
- Enhanced utilization of active testing
- Closed-loop automation driven by analytics and machine learning



*Lifecycle Service Assurance (LSA) automates and accelerates the service lifecycle.*

# Transforming for NFV, 5G and IoT:

## The Need for Lifecycle Service Assurance

We've seen our share of technology transformations at Spirent. We led the innovation of the first active assurance systems when Time-Division Multiplex (TDM) and Digital Subscriber Line (DSL) networks rolled out years ago. As TDM and DSL networks transformed to Ethernet, we reinvented our approach to active assurance and were first to market with 1G, 10G and 100G Ethernet assurance probes. When LTE and Wi-Fi rolled out, and later IoT, we pioneered the use of network emulation to validate mobile infrastructure and test services. More recently, as 5G lab testing kicked off, we delivered the world's first 5G Lab as a Service (LaaS) to bring unprecedented speed and efficiency to 5G network validation.

How does the transformation to network functions virtualization (NFV) compare to previous transformations? It's truly unprecedented! That's because adoption of NFV is more than just a technology transformation—it's a business transformation. Fortunately, it's not going to happen overnight. Our customers are indicating they'll apply virtualization to a targeted set of network functions over time, gradually phasing out physical infrastructure. That means networks will consist of a hybrid of physical and virtual infrastructure for many years.

NFV transformations are driven by a simple goal. Service providers with legacy fixed and mobile networks want to innovate faster and bring down costs dramatically so they can compete with cloud-based over-the-top (OTT) services. Achieving this goal will require streamlining and automation of the service lifecycle so it runs much faster with far fewer resources. Unfortunately, many providers have a highly-fragmented approach to testing and assurance consisting of multiple, unintegrated systems siloed by lifecycle stage, network domain, technology and data source. This siloed approach inhibits collaboration across development and operations teams and leads to manual, swivel-chair workflows. These legacy workflows have evolved over years and represent a critical obstacle to achieving the speed and efficiency goals of NFV.

To realize the promise of NFV and the technologies it enables, such as 5G and IoT, we need a new approach to testing and assurance that breaks down the silos of traditional approaches. Development and operations teams need a unified set of metrics, methodologies and systems that allows them to adopt streamlined DevOps continuous testing practices. Because of the gradual, targeted rollout of NFV, this unified testing approach must support physical, virtual, and hybrid networks. In addition, the approach must enable unprecedented automation to improve efficiency and to proactively address quality issues in highly dynamic NFV networks.

As deployments of NFV ramp up, Spirent is pioneering a new approach to testing and assurance called Lifecycle Service Assurance (LSA). LSA represents a set of best practices for unified testing and assurance across the service lifecycle including network validation, service testing, and operational assurance workflows. These best practices are based on Spirent's unique expertise with automated testing in lab and production environments and integration of proactive service quality assurance in physical, virtual, and hybrid networks.

## Key Challenges for Service Assurance

Historically, service assurance strategies have been developed and deployed months or even years after the initial service launch. That's driven an approach to designing service assurance systems which has focused on narrowly defined testing and monitoring needs, typically within discrete silos. These silos include:

- Lifecycle stage (network validation, service testing, operational assurance)
- Network domain and technology (fixed/mobile, business/consumer, 4G/5G/IoT)
- Network segment (access, backhaul/transport, core)
- Data source (active test vs. passive network and customer data)

As a result, service assurance practices have often relied on disparate systems and manual, swivel-chair practices. The following sections explore the challenges created by new technologies such as NFV, 5G, and IoT and the limitations of traditional manual and siloed service assurance with respect to addressing these challenges.

### NFV is in Its Infancy

It's early days for NFV, with most providers just taking the first steps in a complex, multi-year transformation. The industry is still learning about the complexities of using common infrastructure, the performance and quality this infrastructure can provide, and how it compares to traditional infrastructure. Couple this with implementing virtual network functions (VNFs) in dynamic environments and a myriad of new requirements for managing service quality, performance, and scaling emerge. While it is early days, one thing is very clear: The manual service assurance approaches currently employed by many service providers cannot identify and address quality, performance, and scaling issues fast enough to keep up with highly dynamic NFV environments.

### The Need to Support Hybrid Networks

Virtualization is an evolution that will take years—we're not going to wake up tomorrow in a completely virtualized environment. Service providers have invested significantly in physical infrastructure that has many years of useful life left. Also, certain high speed network functions such as 100 and 400Gbps provider edge switches may require specialized hardware for years. At the same time, we know that virtualization of certain functions such as customer premises equipment (vCPEs) and evolved packet core (vEPCs) has been embraced by providers. So we are going to be living in a world of hybrid networks for many years, where virtual and physical infrastructure coexist. Traditional service assurance needs to evolve to support both virtual and physical networks and enable seamless automation of assurance workflows across hybrid networks.

### Fragmented Initiatives and Lack of Service Assurance Focus

While there are multiple NFV standardization initiatives in progress, detailed definitions of the architecture and functions needed to enable practical implementations are just emerging. This has led to fragmentation, with major service providers taking the bull by the horns and defining their own extended architectures (e.g. AT&T, Verizon, and Vodafone). Furthermore, service assurance has not been well defined in the broader set of standards and detailed definitions to enable practical implementations have not yet emerged.

The evolution of service assurance will be fundamental to the successful realization of open network management platforms and their key objectives such as zero-touch automation, lifecycle management, and vendor-agnostic openness. Without a next generation of service assurance, designed with the openness and flexibility required by these frameworks, open source initiatives may fail to deliver on their real potential.

### The Growth of IoT and Evolution Towards 5G

There will be a continuous and growing demand on our networks as we move to an IoT world dominated by machine communications. Layered on top of NFV, IoT potentially creates a perfect storm for failures and service quality issues due to a unique combination of changing signaling and traffic patterns and increased technology complexity. Because certain types of IoT traffic are sporadic (e.g. remote alarm systems), passive approaches to assurance cannot validate the end-to-end availability of services. Adding 5G into the mix brings additional change and complexity. To assure quality and stability of future technologies such as IoT and 5G, service assurance will need to provide a unified approach across these technology and domain silos and rely on a mix of active and passive assurance approaches.

### The Need for Agility and Cost Reduction

NFV promises providers benefits such as rapid service innovation and significantly reduced Opex and Capex. Initial virtualization efforts, which essentially repackage existing network functions as virtual appliances, sometimes called NFV 1.0, have failed to deliver on this promise. As providers look to evolve from NFV 1.0 to 2.0, they must leverage orchestration, process automation, and new operational approaches such as DevOps to accelerate on-boarding of new services and reduce costs. A key element of DevOps is the concept of continuous, highly automated testing across the service lifecycle from development to operations. Unfortunately, most service providers with legacy fixed and mobile networks have a highly-fragmented, manual approach to testing and assurance which directly inhibits adoption of a DevOps continuous testing approach.

### The Need to Manage Quality

Quality is king. It's the only true differentiator in networks today and being reactive in approach is simply not an option. Modern service assurance needs to be proactive, predictive, and prescriptive. It needs to anticipate what network issues will impact service quality and identify resolutions that solve these problems. Traditional service assurance has relied on assurance systems that are siloed by data source. For example, active test assurance systems and passive network probe assurance systems typically exist as separate, non-integrated applications. In dynamic NFV networks where the network configuration is constantly changing, there is no time for a manual, swivel-chair approach to leveraging systems across data source silos. Furthermore, service assurance also needs to close the loop to ensure issues can be addressed as fast as the network is changing.

## Lifecycle Service Assurance

To address the challenges of NFV, hybrid networks, 5G, and IoT, service assurance must become an integral part of the service across its lifecycle, from initial design and development to operations. Furthermore, service assurance must break through legacy silos that have prevented adoption of DevOps continuous testing and closed-loop automation. To realize the full promise of NFV and the technologies it enables, Spirent has pioneered a new approach to assuring services called Lifecycle Service Assurance (LSA). Lifecycle Service Assurance unifies testing and assurance across the service lifecycle including network validation, service testing, and operational assurance workflows.

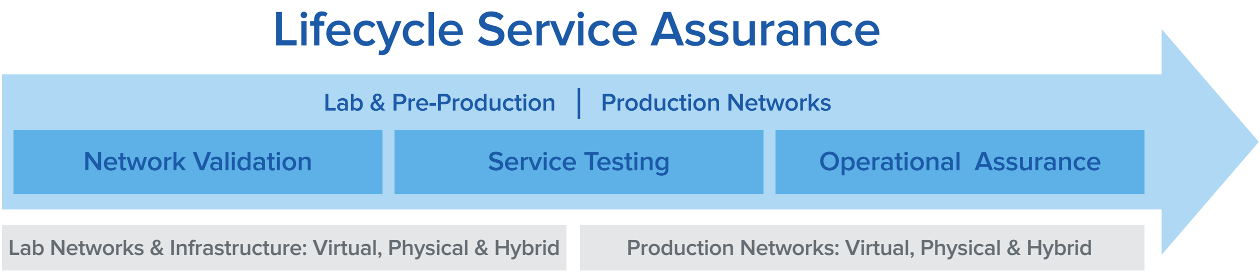

Lifecycle Service Assurance
Lab & Pre-Production
Production Networks
Network Validation
Service Testing
Operational Assurance
Lab Networks & Infrastructure: Virtual, Physical & Hybrid
Production Networks: Virtual, Physical & Hybrid

*Figure 1: Lifecycle Service Assurance unifies testing and assurance workflows to enable providers to rapidly on-board new services, reduce costs, and differentiate service quality.*

| | |
|---|---|
| **Network Validation** | Validation of virtual and physical network functions and infrastructure to establish benchmarks and assure the network will meet performance and capacity targets. Includes benchmarking and testing of VNFs, NFV infrastructure (NFVi) and physical network functions in lab-based development and pre-production environments. |
| **Service Testing** | Testing of services in virtual, physical, and hybrid networks to assure service quality targets will be met at launch, to verify newly activated services meet performance and quality targets, and to isolate the root causes of service issues detected by operational assurance applications. Includes testing of Quality of Experience (QoE) and underlying protocol stack performance in pre-production and production networks. |
| **Operational Assurance** | Continuous monitoring of network performance, service quality, and customer experience as defined by service level agreements. Data sources may include active test agents and probes as well as passive network and customer data from probes, agents, OSS, BSS, and network management data sources. |

*Table 1: Lifecycle Service Assurance workflows defined.*

LSA breaks down silos between development and operations teams by harmonizing test metrics and methodologies across network validation, service testing, and operation assurance workflows. That means the same approach used to benchmark and validate NFV infrastructure (NFVi) in the lab can be used to isolate issues and measure the health of cloud infrastructure as part of pre-launch service testing and operational assurance activities. Likewise, analytics developed and refined for operational assurance needs can be used to recreate issues and identify fixes or improvements to network functions in lab and pre-production environments.

LSA gives providers the ability to automate processes and implement DevOps practices in virtual, physical, or hybrid networks. LSA makes extensive use of active testing, which is poised to take on a new level of importance in virtual networks. However, LSA utilizes both active test and passive network and customer data so providers can leverage analytics and machine learning to 'close the loop' on assurance processes. The following sections explore key principles of LSA including support for DevOps,  hybrid networks, active testing, and analytics.

### DevOps Continuous Testing

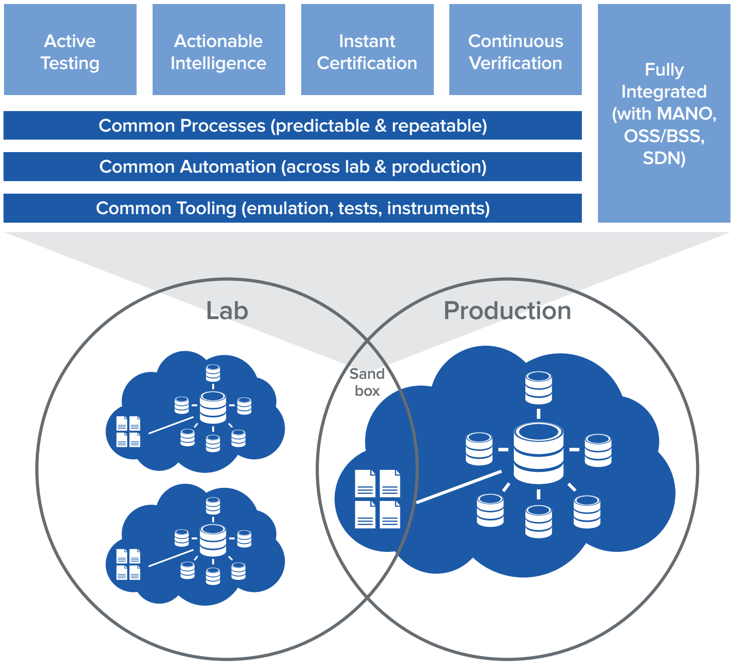

Active Testing
Actionable Intelligence
Instant Certification
Continuous Verification
Fully Integrated (with MANO, OSS/BSS, SDN)
Common Processes (predictable & repeatable)
Common Automation (across lab & production)
Common Tooling (emulation, tests, instruments)
Lab
Production
Sand box

*Figure 2: DevOps adoption requires consistent network implementations in lab and production environments and a coherent approach to testing processes, automation, and tooling.*

A core principle of Lifecycle Service Assurance is support for DevOps adoption, especially DevOps continuous testing. With NFV and SDN, labs and production networks are merging into a seamless environment, where the production network also serves as a sandbox for pre-production and development tests. This trend creates a perfect environment for adoption of DevOps practices. But to successfully exploit this opportunity, we need to break down traditional boundaries between development and operations which have led to disparate approaches. Lifecycle Service Assurance seeks to harmonize testing processes, tools, and automation techniques across development and operations teams, so they can adopt DevOps continuous testing and achieve benefits such as faster development cycles, automated testing, and improved efficiency.

## Support for Virtual, Physical & Hybrid Networks

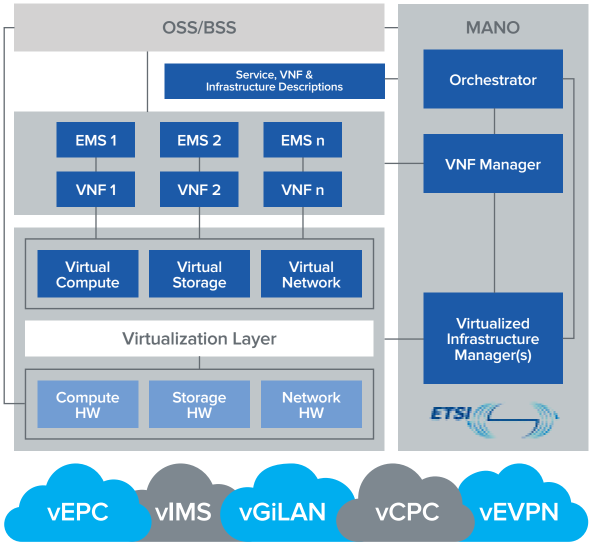


*Figure 3:*

*The goal of virtualization is a highly flexible and scalable network composed of software running on common infrastructure.*

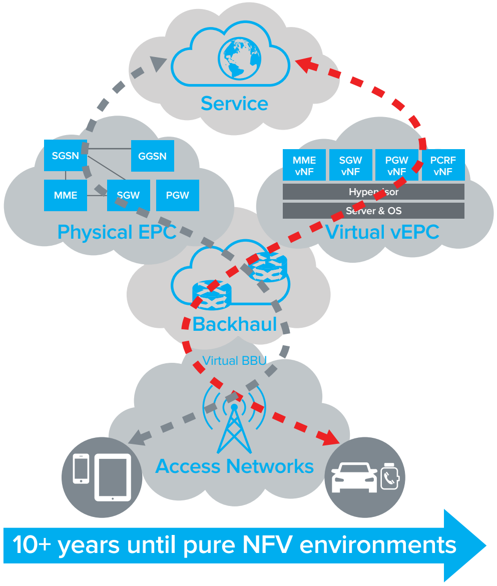


*Figure 4:*

*Providers will gradually virtualize networks resulting in hybrid networks which leverage virtualization for some services and network segments (such as vEPCs for IoT) but not others.*

The reality of hybrid networks is that the industry has an enormous sunk investment in physical infrastructure and, while virtualization has great promise, it is still in its infancy. We going to live for many years in a hybrid world as providers gradually implement virtualization for various applications or services. A good example is providers who are trialing or rolling out islands of virtualization, such as virtual EPCs or a virtual CPEs. We expect certain parts of the network, especially as we move to the RAN, not to be virtualized until we are well into 5G deployments and even beyond.

Lifecycle Service Assurance isn't just about adapting traditional service assurance to address this hybrid reality. We see LSA as a unifying element bridging the chasm between physical and virtual environments and enabling the success of providers as the evolve their hybrid networks. LSA enables success by bringing forward some of the benefits of virtual networks to hybrid networks. LSA helps providers adopt a nimbler, faster DevOps approach by integrating service assurance and network management functions in both physical and virtual networks. This allows seamless automation of network validation, service testing, and operation assurance workflows across hybrid networks, accelerating on-boarding and improving operational efficiency.

## Active Testing & Monitoring

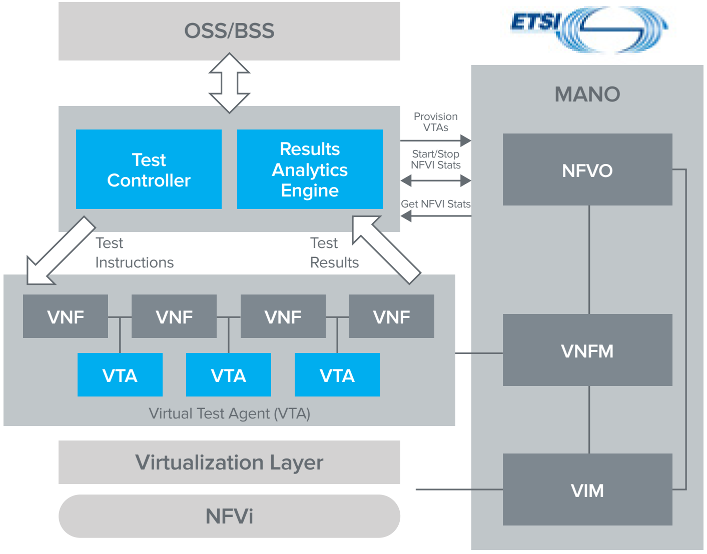


*Figure 5: ETSI NFV Active Monitoring Framework*

Lifecycle Service Assurance embraces and recognizes an enhanced importance for active testing and monitoring in virtual networks. Active testing and monitoring provides unique capabilities for assessing performance and quality at various times:

- Immediately after turn-up of a new network element or service (when passive traffic is limited or non-existent)
- During the operational phase when SLAs need to be monitored continuously, even when a specific application or service type isn't being used by actual customers
- When SLA violations occur and problems need to be segmented to a specific location, infrastructure element, network function, or protocol layer

The cost of performing active testing and monitoring in physical networks has historically relegated this approach to a limited set of applications such as Ethernet turn-up verification and SLA monitoring, and device-based (outside the network) QoE monitoring. With the introduction of virtual networks, active testing and monitoring no longer requires expensive physical probe hardware: instead, virtualized active test agents (VTAs) can now be deployed on-demand anywhere in the network, unleashing a powerful new capability for assuring networks.

Spirent is working with ETSI to define a common framework for implementing active testing and monitoring with NFV. It's a simple open architecture, which aligns not only with the standard NFV architecture, but can also integrate seamlessly into carrier-specific initiatives. The architecture consists of three key components as shown in Figure 5. Virtual test agents (VTAs) are essentially software test functions which can be dynamically spun up and down across the network to execute a relevant set of active test cases. For example, validating turn up of a new vEPC function, monitoring SLAs for end-to-end services or testing individual network segments to try to isolate a fault in the network.

The Test Controller and the Analytics Engine sit above the VTA at the heart of the framework. The Management and Network Orchestration (MANO) function instantiates the VTA based on provisioning information provided by the Test Controller and then leverages the Test Controller to completely automate the testing and monitoring process including starting and stopping tests. The Analytics Engine is essentially the brain, utilizing all available data sets (active, passive, VNF KPIs, and more) to provide actionable intelligence to allow MANO functions to drive decision-making.

The key features of the ETSI Active Monitoring framework include:

- Proactive approach using emulated traffic to verify performance and quality
- Highly automated, configurable, and repeatable
- Ideal for 24/7 continuous monitoring, enhanced troubleshooting, service turn-up, and verification

The framework complements passive monitoring, which is reactive and requires user traffic. Used together, active and passive monitoring approaches provide the best of both worlds including proactive and reactive capabilities.

## Analytics Driven Assurance

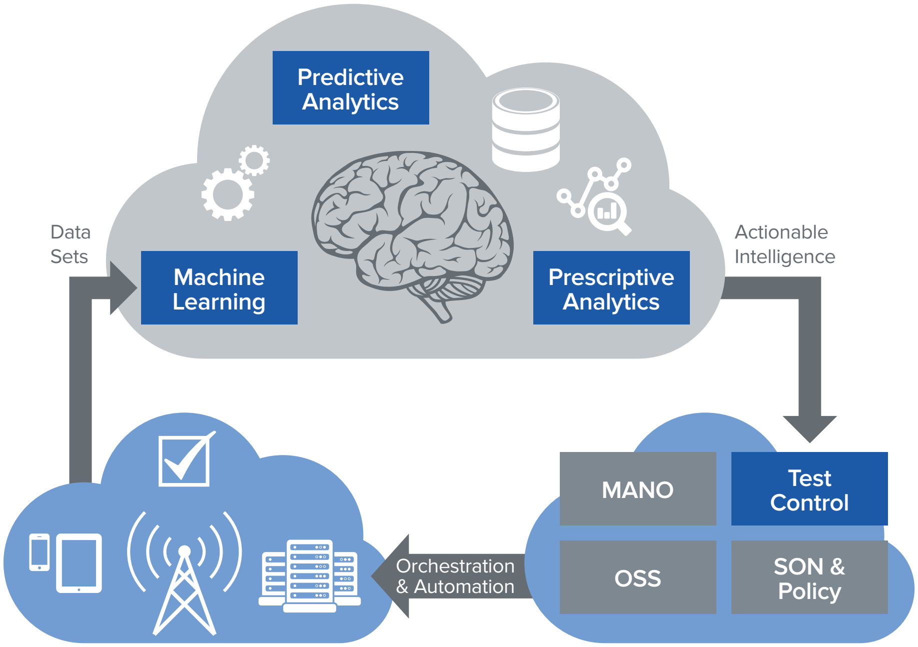


*Figure 6: Closed-loop, fully automated assurance leverages predictive and prescriptive analytics and machine learning.*

As described in the Active Testing and Monitoring section, the application of intelligence to automate processes is a core principle of LSA. Analytics that transform network test data into actionable insights are a key element of intelligence but the full realization of this principle includes the application of machine learning alongside both predictive and prescriptive analytics. The goal isn't just to predict issues before they manifest, but also to prescribe a potential resolution and, feeding and interworking with the relevant control and orchestration functions, to close the loop and resolve the issue.

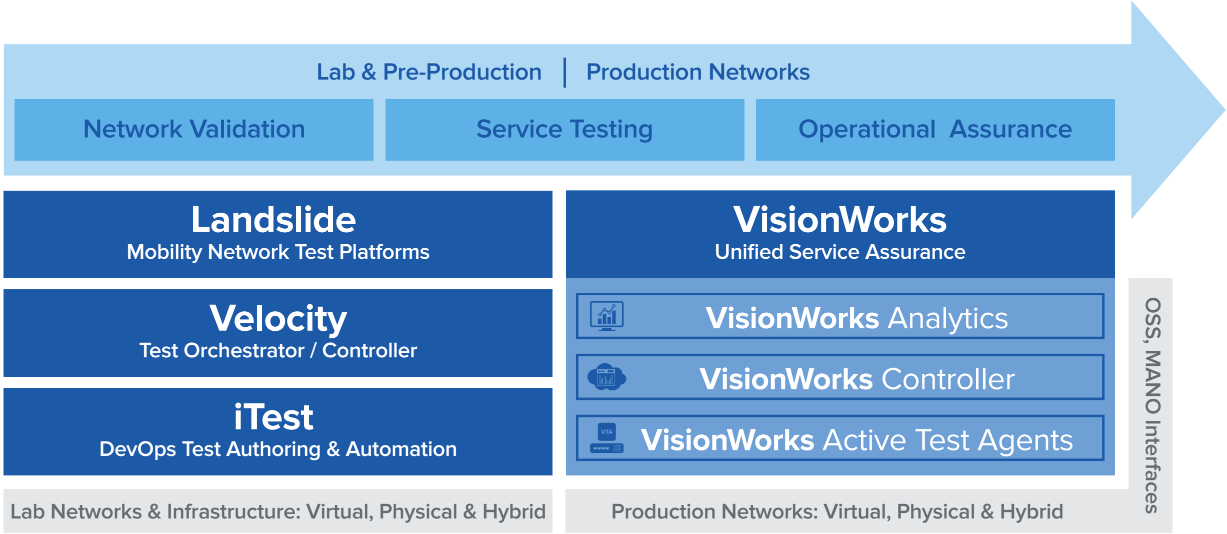
Key features and benefits of analytics in LSA include:

- Transforming network and test data into actionable insights
- Providing end-to-end quality and performance visibility
- Utilizing analytics to enable proactive assurance and orchestration
- Increasing responsiveness
- Enhancing operational agility
- Reducing Opex

## Spirent Lifecycle Service Assurance Solutions

As operators transform their networks for NFV, 5G, and IoT, service assurance must adapt to address a new generation of challenges. Legacy manual/siloed approaches won't work in the coming era: We need a new, highly automated approach to service assurance that supports the dynamic, distributed nature of these new technologies. Working together with leading service and network providers and open network management initiatives such as ETSI and ONAP, Spirent is pioneering a new approach to service assurance called Lifecycle Service Assurance (LSA). LSA unifies and automates testing and assurance across the service lifecycle, so service providers can rapidly launch new services, dramatically reduce operational costs, and differentiate on service quality.

Spirent's suite of Lifecycle Service Assurance solutions embody the principles detailed in this whitepaper, including support for open frameworks, DevOps continuous testing, hybrid physical/virtual networks, active testing, and analytics-driven automation. As shown in Figure 7, our LSA solutions suite addresses network validation, service testing, and operational assurance workflows across the service lifecycle. The suite consists of three products focused on lab and pre-production testing, Landslide, Velocity, and iTest, and one product focused on production network testing and assurance, VisionWorks.


Lab & Pre-Production
Production Networks
Network Validation
Service Testing
Operational Assurance
Landslide
Mobility Network Test Platforms
Velocity
Test Orchestrator / Controller
iTest
DevOps Test Authoring & Automation
VisionWorks
Unified Service Assurance
VisionWorks Analytics
VisionWorks Controller
VisionWorks Active Test Agents
OSS, MANO Interfaces
Lab Networks & Infrastructure: Virtual, Physical & Hybrid
Production Networks: Virtual, Physical & Hybrid

Landslide emulates a comprehensive range of mobile network functions, base stations and devices and then uses these emulated functions to test the performance and capacity of new or updated mobile core functions (both physical elements and virtual network functions). Velocity orchestrates lab infrastructure and lab test tools to fully automate lab testing. Velocity also provides a Lab as a Service (LaaS) portal, which allows test teams around the world to run automated tests using a shared set of lab infrastructure. iTest integrates seamlessly with Velocity to streamline test authoring and automation.

VisionWorks delivers unified service assurance for hybrid networks and for mobile, fixed, and transport services. VisionWorks automates service activation testing, monitors SLAs and enables rapid detection, isolation, and resolution of service issues across the end-to-end network. VisionWorks consists of a set of components with open interfaces: VisionWorks Analytics (formerly InTouch), VisionWorks Controller (formerly Lumos), and VisionWorks Active Test Agents (formerly Lumos VTA/Probe and Landslide Virtual).

To learn more about VisionWorks and Lifecycle Service Assurance solutions from Spirent, please visit: www.spirent.com/Solutions/Service-Assurance.

### About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

spirent™
Promise. Assured.

### Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

**www.spirent.com**

**Americas 1-800-SPIRENT**
+1-800-774-7368 | sales@spirent.com

**US Government & Defense**
info@spirentfederal.com | spirentfederal.com

**Europe and the Middle East**
+44 (0) 1293 767979 | emeainfo@spirent.com

**Asia and the Pacific**
+86-10-8518-2539 | salesasia@spirent.com

Rev B | 08/18