RESEARCH

analysys mason

WHITE PAPER

# Reimagining service assurance for NFV, SDN and 5G

Anil Rao

August 2018

analysysmason.com

RADCOM

# Contents



# List of figures

# 1. Executive summary

Network function virtualization (NFV) and software-defined networking (SDN) technologies introduce fundamental changes to the way telecommunications networks and services are built and managed. Based on the principles of cloud infrastructure, software control and automation, NFV and SDN are among the most important enablers for the transition of traditional communications service providers (CSPs) to digital service provider (DSPs). Along with a highly agile and flexible cloud network infrastructure, DSPs will be able to rapidly introduce innovative communication and digital services, achieve automated operations, offer superior real-time digital experiences, and generate new revenue streams through 5G and IoT services.

The network virtualization evolution is occurring over three overlapping phases introducing new assurance requirements that existing systems cannot fulfil. In the virtualization phase, physical network functions being ported to software and virtual form factors on commercial hardware require new monitoring and virtual passive probing capabilities; in the orchestration phase, the virtual functions are dynamically provisioned and strung together to create network services, which requires the assurance functions to be tightly integrated with orchestration systems to support closed-loop automation and adapt to the changing network configuration; and finally, in the cloud native phase the network functions are rearchitected as containerized applications running in a highly automated cloud environment, which requires granular and containerized assurance supporting the goal of achieving zero-touch networks and autonomous operations.

However, the journey to cloud native networks and autonomous operations is not going to happen overnight. The existing physical networks will coexist with the new NFV networks for the foreseeable future, creating a complex network environment and introducing a new dimension of assurance and operations complexity. New-age automated assurance systems must provide monitoring and operations automation capability for hybrid physical, virtual and cloud native networks and services. They must also support the new NFV/SDN-enabled 5G/IoT networks and associated use cases around ultra-low latency, edge clouds and network slicing.

CSPs and vendors must reimagine service assurance to support these business and technology imperatives. The new-age service assurance systems must demonstrate six key traits (see Figure 1.1), with the ability to exploit the inherent capabilities of cloud-based networking infrastructure and a roadmap to support autonomous operations.

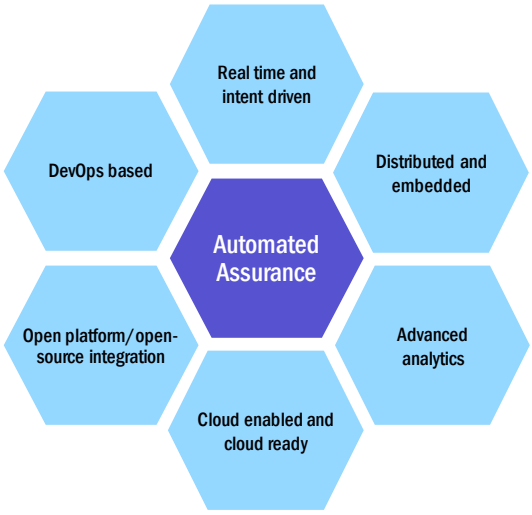



***Figure 1.1: The six key traits of new-age service assurance [Source: Analysys Mason, 2018]***

These new systems must also comply with the plethora of industry organizations and CSPs such as The Linux Foundation's Open Network Automation Platform (ONAP), ETSI's Open Source MANO (OSM), MEF Lifecycle Service Orchestration (LSO), AT&T Domain 2.0 and Network 3.0, Telefónica Unica, etc. New assurance systems must also be powered by a new-age network visibility platform that supports diverse form factors to support a hybrid network and enable the CSPs' virtualization evolution towards cloud-native network and operations environment.

# 2. Network virtualization is a key strategic initiative for many CSPs worldwide

## 2.1 NFV and SDN technologies are foundational for CSPs to become digital service providers

With increasing competition from alternative service providers, commoditization of communication services and a decline in revenue from traditional sources, many CSPs are embarking on a journey to become DSPs. As illustrated in Figure 2.1, the multi-faceted digital transformation includes:

- evolving the network and IT assets to a more software-driven, virtualized and cloud-based infrastructure, using NFV and SDN technologies
- exploring 5G and IoT to generate new revenue streams
- providing real-time digital experiences to delight customers
- employing automated operations approaches to achieve the highest efficiencies and employee productivity at a fraction of the cost.

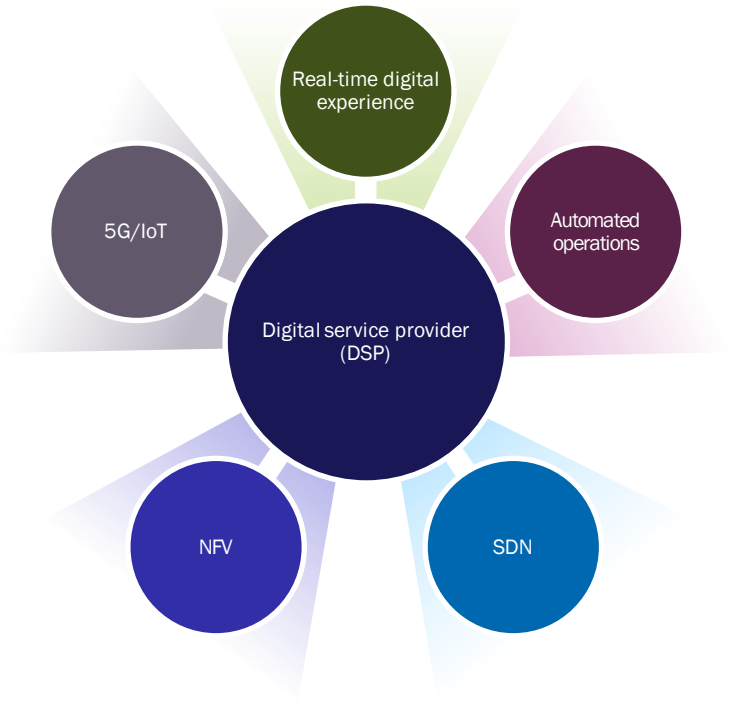



***Figure 2.1: The key attributes of a digital service provider [Source: Analysys Mason, 2018]***

NFV involves the migration of the networking infrastructure from proprietary hardware-based networks to a shared cloud-based resource layer running virtual network functions (VNFs); and SDN makes the networks programmable and controllable for dynamic traffic management and service optimization. At the heart of this transformation is the goal to achieve business and service agility by increasing the speed of service development and delivery, increase operational agility and flexibility through operations automation, and reduce the costs of delivering services.

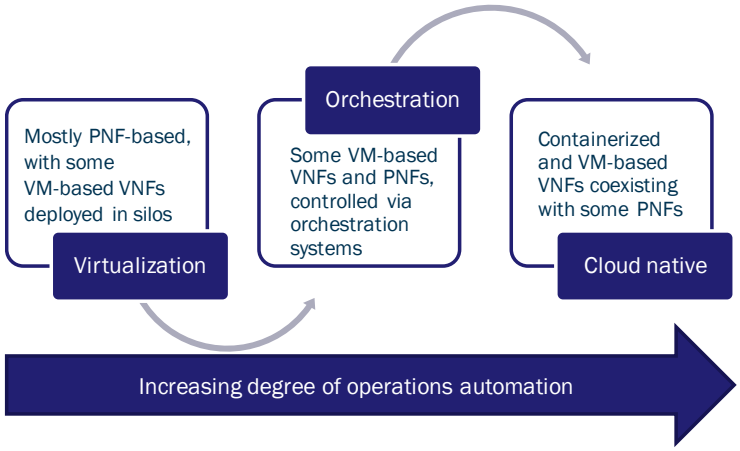
Ultimately, the objective is to better compete against the webscale alternative service providers such as Facebook, Amazon, Google and Netflix, and other digital economy competitors, to not only protect existing revenue streams, but also generate additional revenue by offering new digital services such as smart homes, autonomous cars and other industry-specific IoT services, augmented/virtual reality services and 5G services aimed at specific vertical sectors.

NFV is fundamentally based on cloud technologies that are key to service agility and personalization, and allows CSPs to create service instances that can be configured for the specific needs of an individual customer. CSPs can leverage the efficiency and flexibility of cloud-based resource utilization and SDN's centralized traffic management capabilities to optimize service delivery, reducing network costs while maintaining and improving customer experience. Together, NFV and SDN support the rapid and automated modification of services, in response to numerous scenarios, from fulfilling new customer requests to preserving service-level agreements (SLAs), from lowering delivery costs to the integration of new features.

## 2.2 NFV and SDN create new operational requirements

The network virtualization evolution is progressing over three overlapping phases, as illustrated in Figure 2.2.

***Figure 2.2: Different phases of network virtualization [Source: Analysys Mason, 2018]***




- **Virtualization**: in this phase, network functions will be migrated from the physical network functions (PNF) form executing in proprietary hardware environment to a piece of software running on commercial off-the-shelf hardware, and subsequently, deployed as a VNF in a virtual machine running on hypervisor-enabled hardware. While these steps provide some capex benefits because of a shared infrastructure environment running multiple VNFs, it does create some management challenges as CSPs need to manage and assure a hybrid physical and virtual network from an end-to-end perspective, in addition to assuring the NFV environment differently because of the inherently different nature of the virtual network.

- **Orchestration**: in this phase, multiple VNFs will execute in a shared execution environment under the control of a management and orchestration (MANO) stack. MANO automates the cloud management aspects of the VNF lifecycle, such as instantiation, placement, scale in/out, upgrades, migration, and self-healing. The MANO stack and SDN capabilities that manage data center/WAN connectivity between VNFs introduce new operational processes and automation. In this phase of deployment, the basic hypervisor and infrastructure manager layers are supplemented with additional MANO systems including the VNF manager (VNFM) and NFV orchestrator (NFVO) to automate the VNF lifecycle.

- **Cloud-native networks**: this is the end goal of the virtualization evolution, where cloud-native approaches will be the key to the CSPs' ability to transform into DSPs. In this phase, VNFs will be rearchitected as microservices-based cloud-native applications, executing in a secure, cloud and managed/orchestrated environment. Customer-facing services will be delivered across a largely virtualized network and connectivity will be completely automated using SDN. A cloud-native network and operating environment is expected to significantly reduce the economics of building and operating networks, increase the speed of service delivery, and generate revenue from new services.

## 2.3 Assurance solutions must cater for a complex hybrid network environment

Today, most of the CSPs are either in phase 1 or phase 2 of this evolution, with some advanced CSPs making the leap in deploying cloud-native VNFs in a limited capacity. However, all CSPs making the virtualization journey will have a mix of network environments consisting of physical, virtual and cloud-native VNFs supporting different services. For example, an operator may initially deploy some instances of virtual EPC (vEPC) to carry incremental VoLTE traffic (in addition to the already operational physical EPC carrying existing VoLTE traffic), with a view to eventually deploying cloud-native vEPC for VoLTE.

Such diverse network environments demand a multi-pronged assurance approach that caters for the physical networks, which still account for most of the network deployments and the fast emerging virtual and cloud native networks that are being rolled out (see Figure 2.3).

***Figure 2.3: Assurance considerations for the NFV journey [Source: Analysys Mason, 2018]***

| NFV/SDN phase | Assurance implications |
|---|---|
| Virtualization | In the early stages of the virtualization journey, from an assurance perspective, CSPs need to monitor the virtualization infrastructure and the new VNFs, and correlate the KPIs to obtain an end-to-end view of service performance. |
| Orchestration | In this phase of deployment, some of the assurance functions will become embedded in the various layers of the MANO stack, including the virtualization infrastructure manager (VIM), VNFM, and NFVO, to enable assurance-driven local closed-loop automations. The various layers of the MANO will integrate into an umbrella end-to-end hybrid assurance engine, which will provide a higher layer of 'intelligence' to drive automation based on higher order KPIs such as service quality, customer experience, cost metrics, etc. Advanced analytics paradigms, such as machine learning combined with policy rules, will power service assurance enabling rapid root-cause analysis, anomaly detection, and issue prediction. |
| Cloud native | In a cloud-native environment, assurance components will need to support an extremely high level of granular monitoring and automation, which will be achieved by the deployment of containerized monitoring functions that will coexist with the cloud-native network functions. Along with other operational components, cloud-native assurance will become an integral part of a digital network and operations platform. |

### 2.4 5G, enabled by NFV and SDN, presents a whole other dimension of complexity that must be addressed by assurance

5G use cases require ultra-low latency – for example, a response rate of less than 2ms for applications such as autonomous driving. The latency on an LTE network is 50ms, which is half that of a 3G network, and to achieve the required ultra-low latency, the gateways carrying the traffic must be moved closer to the network edge, and therefore, the core and radio elements must become more distributed than is required for LTE. This requirement for flexible architecture will be met with a plethora of technology enablers including multi-access edge computing (MEC) where networking resources must be placed closer to the point of consumption, and, enabled by NFV and SDN to support agile and distributed network topologies.

Network slicing is another area that is increasingly being associated with 5G, enabling CSPs to completely transform the economics of the connectivity business, but adding another dimension of network and service complexity. Network slicing provides an end-to-end virtual network with dedicated capacity and/or other service-specific characteristics. NFV will allow CSPs to optimize the network to address the individual needs of different services through the creation of multiple, separate virtual network slices, each providing differentiated latency, performance, reliability, availability, and other characteristics, tuned to the needs of each use case/service.

Assurance must therefore not only evolve to address the changing nature of the network infrastructure with NFV and SDN, but also the new imperatives around the ultra-low latency requirements of 5G, the emergence of edge clouds, and the new paradigm of network slicing.

## 3. Service assurance must be reimagined to support the CSP goals of NFV, SDN, and 5G

Legacy assurance solutions were designed to monitor physical networks and were not fit for purpose to support the operational requirements of NFV, SDN, 5G/IoT. New-age service assurance must be designed to exploit the inherent capabilities of cloud-based networking infrastructure and support high levels of operations automation with a roadmap to enable autonomous operations and zero-touch networks (see Figure 3.1).

## 3.1 New-age service assurance must demonstrate six key traits

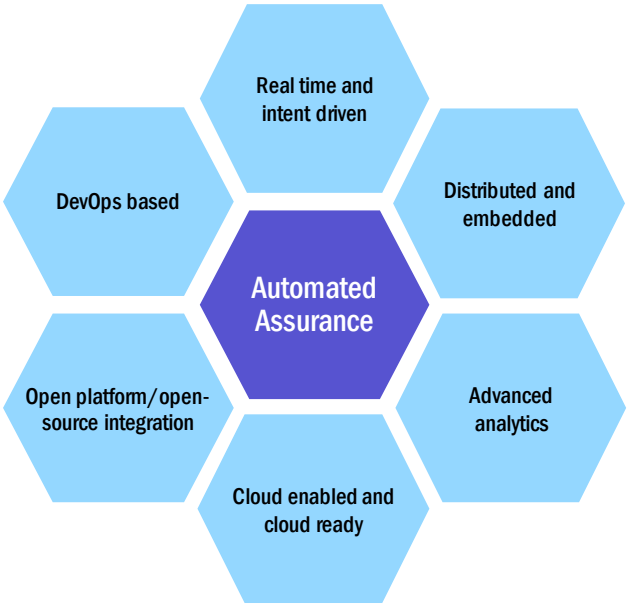



*Figure 3.1: The six key traits of new-age service assurance [Source: Analysys Mason, 2018]*

### Cloud enabled and cloud ready

Two aspects to the cloud must be considered for assurance:

- **Assurance must support a dynamically changing cloud-based virtual network**, i.e. it must be cloud ready because the VNFs can be created, moved, or terminated based on service demands. This means that the assurance functions must adapt to the network and service configurations as they change, so that they can provide accurate monitoring and root-cause analysis of issues and enable feedback loops for orchestration and automation.
- **Assurance components must themselves be cloud enabled**, i.e. virtualized and ultimately become cloud native to support a highly virtualized and cloud-native network. This is vital because of the primary reason that some of the assurance functions, such as the physical network probes, are incompatible with virtual networks, i.e. they cannot be used to monitor the inter-VM and inter-container traffic. This is discussed in further detail below.

### Advanced analytics

Advanced analytics capabilities, such as machine learning, will play a pivotal role in enabling CSPs to deliver proactive and predictive service assurance. Additionally, the insights generated from the analytics form the basis for automation. Machine learning augments the analytics models with learning abilities and provides the basic mechanisms for continuously enhancing the intelligence of the model, which can then be used for a wide range of use cases, such as predicting and preventing network performance and service quality issues before they occur.

With growing confidence in machine learning, AI-led models can be gradually introduced to work with automated workflows. With their self-learning and self-calibrating capabilities, they can constantly tune themselves to increase the accuracy of the root-cause analysis and actions, which can ultimately enable the goal of autonomous operations. Together, machine learning and AI provide the capabilities to spot trends and anomalies, predict the most likely network and service issues, and trigger policy-based pre-emptive actions to prevent service impact, and potentially churn.

### Distributed and embedded

The layered MANO stack for NFV/SDN management and control provides the all-important network abstraction but, on the other hand, adds operational complexity. Some of this complexity can be alleviated by empowering each of the management layers with control and monitoring functions such as service assurance.

In the context of achieving high levels of automation, the distributed assurance approach can provide dynamism and lower reaction times. This approach will also enable CSPs to approach operations from a service management perspective, i.e. focus on ensuring network and service availability by triggering localized closed-loop automation nearer to the source of the issue. Policy rules and network analytics will enable the local automation loops with precise trigger conditions at each management layer, and the umbrella assurance system will provide the intelligence to drive business level assurance based on KPIs such as service quality, SLA, financial metrics, and customer experience.

### Open platform and open-source integration

Traditional assurance systems were designed as proprietary full stack solutions with limited ability to integrate with adjacent systems. With the increasing focus on automation, especially around closed-loop automation where assurance systems and adjacent systems (e.g. MANO) will need to seamlessly communicate with each other to automatically execute the network configuration changes, assurance software must be designed with loosely coupled modules based on microservices and open APIs for easy integration.

Furthermore, a lot of the innovation in data analytics and messaging technologies, and many others, is coming out of the open-source ecosystem (e.g. Hadoop, Apache), with many companies specializing in and contributing to the community. Technologies such as the Apache Kafka messaging system are already being deployed across CSPs and will continue to be adopted in a wide range of IT and networking use cases.

### DevOps

There are two aspects of DevOps that CSPs must consider for assurance:

- **DevOps for automated assurance code delivery**: assurance systems must be designed to foster rapid innovation so new incremental features can be delivered in small chunks using processes such as continuous integration (CI) and continuous delivery (CD).
- **Network and service DevOps**: assurance must become an integral part of the network and service design process right from the start, rather than an afterthought. Assurance and automation routines must be embedded in VNF and service descriptions so that they can be executed when the trigger conditions are met.

### Real time, near real time and intent driven

Extreme automation of the assurance processes and closed-loop processes based on the service intent involving the MANO components in NFV/SDN enabled networks will rely on real-time network insights. There will be a broad spectrum of assurance use cases that will have different levels of time sensitiveness, i.e. some will be real time in nature (e.g. reconfiguring of a VNF to maintain service availability), and others maybe non-real time (e.g. identifying the root cause of a VNF fault).

## 3.2 Next-generation network visibility solutions will be pivotal to achieve the new assurance and operational goals

Network visibility solutions such as the network packet brokers and passive probes have long been used in physical networks to gather and analyze packet data. From an assurance perspective, such solutions have been used for a variety of use cases including network performance monitoring, quality-of-service monitoring, control plane signaling performance analysis, user plane data analysis for subscriber and application level visibility, etc. As networks move to software-based NFV and cloud-native formats, the associated network visibility solutions must also evolve to support these networks. Current physical packet brokers and probes are not suitable for monitoring network interfaces in NFV- and SDN-enabled virtual networks.

First, the new network visibility solutions must satisfy the primary requirement of being compatible with the NFV networks, i.e. provide visibility into the inter-VM traffic that does not traverse a physical connection across the data center or between data centers. Second, the visibility solutions must themselves be elastic and flexible, i.e. grow and shrink with the NFV network; this is vital because the traditional solutions for physical networks are overprovisioned for peak traffic, making them highly inefficient from the perspectives of resource and capex allocation (see Figure 3.2).

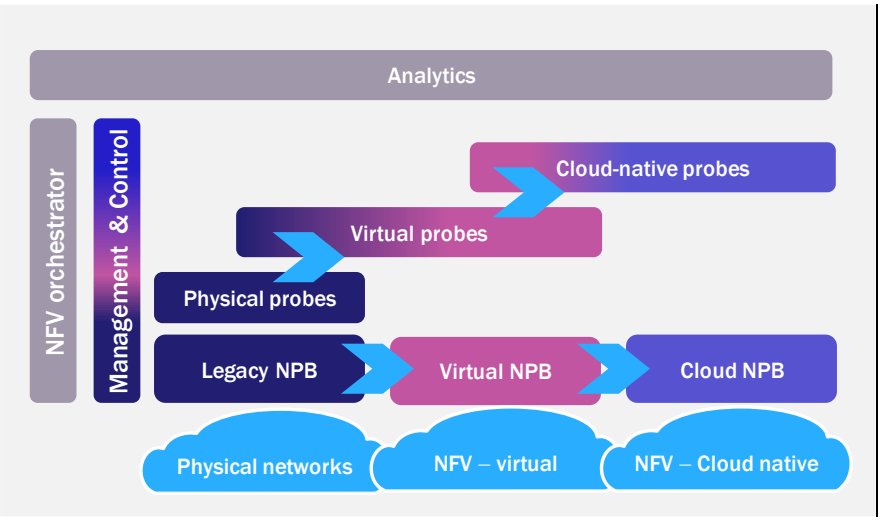



*Figure 3.2: Next-generation network visibility [Source: Analysys Mason, 2018]*

A virtualized network visibility solution supporting basic NFV networks and a microservices-based solution for cloud-native networks will be necessary to support the virtualization journey. CSPs embarking on this journey will face the prospect of operating a hybrid network environment with all three network formats in production – physical, virtual, and cloud native. Consequently, CSPs will need a full suite of network visibility solutions that must cater to all network types (refer to Figure 3.2). Additionally, the solution must provide three key capabilities:

- Provide management and control software to orchestrate the visibility infrastructure. This is required to fully exploit the elastic nature of next-generation visibility software.
- Integrate with the NFV orchestration system providing dynamic control and flexibility to choose the right form factor (e.g. large, mini, micro), instantiate, configure and scale the visibility infrastructure based on service and traffic conditions.
- Expose the network data northbound into big data and analytics platform to drive assurance automations and closed-loop automation.

## 3.3 Service assurance must address a plethora of industry, CSP, and vendor initiatives

The telecom industry is abuzz with many initiatives to address the challenge of operationalizing NFV and SDN (see Figure 3.3). Industry organizations such as the Linux Foundation and ETSI are proposing pseudo-standards-based operational and automation frameworks, and in some cases, even providing the base open-source components to accelerate the operationalization of virtual networks.

CSPs have employed open source, albeit in a limited scale, in their software development and operations environments for many years. However, the introduction of NFV and SDN is increasing the proliferation and influence of open source across the telecom infrastructure and operations value chain. For example:

- Openstack is considered by many CSPs as the de-facto standard for VIM.
- The Linux Foundation's Open Network Automation Platform (ONAP), a comprehensive network and operations automation framework based on open source, has been adopted by AT&T and Bell Canada, and many other CSPs such as Orange and Vodafone are participating in the initiative.
- Open Source MANO (OSM) is another example of an open-source initiative spearheaded by Telefónica under the ETSI banner.

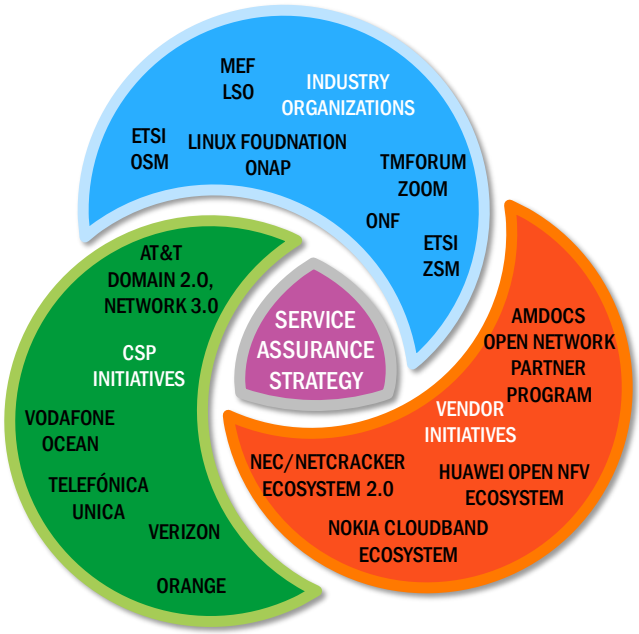



*Figure 3.3: Illustrative set of industry, CSP and vendor initiatives [Source: Analysys Mason, 2018]*

Complementing and supplementing these initiatives, industry organizations such as TM Forum and MEF are focusing on creating standards and specifications with initiatives such as Zoom and LSO respectively.

Large influential vendors such as Nokia, NEC/Netcracker, Ericsson, Huawei, and Amdocs, and many more, have created ecosystems with solution partners but based on their own flagship platforms. CSPs typically work with these vendors as prime systems integrators (SIs), giving them the primary responsibility of fulfilling an engagement, such as implementing a network domain and the associated operations.

Finally, many CSPs such as AT&T, Telefónica and Vodafone are executing their own multi-pronged transformation strategy to evolve into a DSP. A common theme among these initiatives is that CSPs want to define and build a digital network and operations platform (DNOP), a curated set of disaggregated software components from which a CSP's network, customer-facing services and operations will be composed. CSPs will

source DNOP services from different suppliers, including vendors and open-source communities, but will differentiate themselves by curating their own sets of DNOP services and extending and changing them over time to meet market needs.

Service assurance vendors must take into consideration these multiple developments while they chart a course for their company and product portfolios, and identify where they fit in this fast-evolving industry landscape.

# 4. Conclusion

Many CSPs worldwide are in the midst of an NFV/SDN-led virtualization evolution and transformation journey to become DSPs. Virtualized and cloud-native networks are going to enable CSPs to not only deliver traditional communications services at a fraction of the cost but also allow them to rapidly conceive and launch new digital services and deploy new revenue-generating 5G and IoT use cases. The journey to cloud-native networks is going to be gradual, starting with the virtualization phase followed by the orchestration phase, with each phase progressively introducing new network and operational complexity that CSPs must manage.

Reimagined service assurance will be necessary to achieve the CSPs' goals of NFV/SDN, autonomous operations, and the overall digital transformation. New-age service assurance must be distributed and powered by analytics. It must provide real-time insights and trigger closed-loop automation, must be cloud enabled and cloud ready, must be based on DevOps and easily integrate with open-source operational frameworks. Furthermore, it must support a complex hybrid network and services environment, and also offer a family of network visibility solutions to support the journey towards a cloud-native network and autonomous operations.

# About the author

**Anil Rao** (Principal Analyst) is the lead analyst for Analysys Mason's Automated Assurance and Service design and Orchestration research programs, covering a broad range of topics on the existing and new-age operational systems that will power telcos' digital transformation. His main areas of focus include: service creation, provisioning, and service operations in NFV/SDN-based networks, 5G, IoT, and edge clouds; the use of analytics, ML and AI to increase operations efficiency and agility; and the broader imperatives around operations automation and zero-touch networks. In addition to producing quantitative and qualitative research for both programs, Anil also works with clients on a range of consulting engagements such as strategy assessment and advisory, market sizing, competitive analysis and market positioning, and marketing support through thought-leadership collateral. Anil is also a frequent speaker and chair at industry events, and holds a BEng in Computer Science from the University of Mysore and an MBA from Lancaster University Management School, UK.

This white paper was commissioned by RADCOM. Analysys Mason does not endorse any of the vendor's products or services.

Published by Analysys Mason Limited • Bush House • North West Wing • Aldwych • London • WC2B 4PJ • UK
Tel: +44 (0)20 7395 9000 • Email: research@analysysmason.com • www.analysysmason.com/research

Registered in England No. 5177472

# Analysys Mason's consulting and research are uniquely positioned

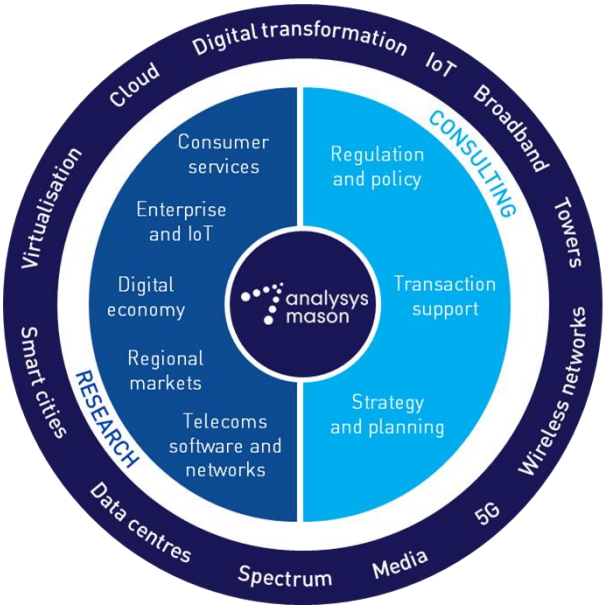
Analysys Mason is a trusted adviser on telecom, technology and media. We work with our clients, including communications service providers (CSPs), regulators and end users to:

- design winning strategies that deliver measurable results
- make informed decisions based on market intelligence and analytical rigor
- develop innovative propositions to gain competitive advantage.

We have around 220 staff in 14 offices and are respected worldwide for the exceptional quality of our work, as well as our independence and flexibility in responding to client needs. For over 30 years, we have been helping clients in more than 110 countries to maximize their opportunities.

## Consulting

- We deliver tangible benefits to clients across the telecom industry:
  - communications and digital service providers, vendors, financial and strategic investors, private equity and infrastructure funds, governments, regulators, broadcasters, and service and content providers.
- Our sector specialists understand the distinct local challenges facing clients, in addition to the wider effects of global forces.
- We are future-focused and help clients understand the challenges and opportunities that new technology brings.




## Research

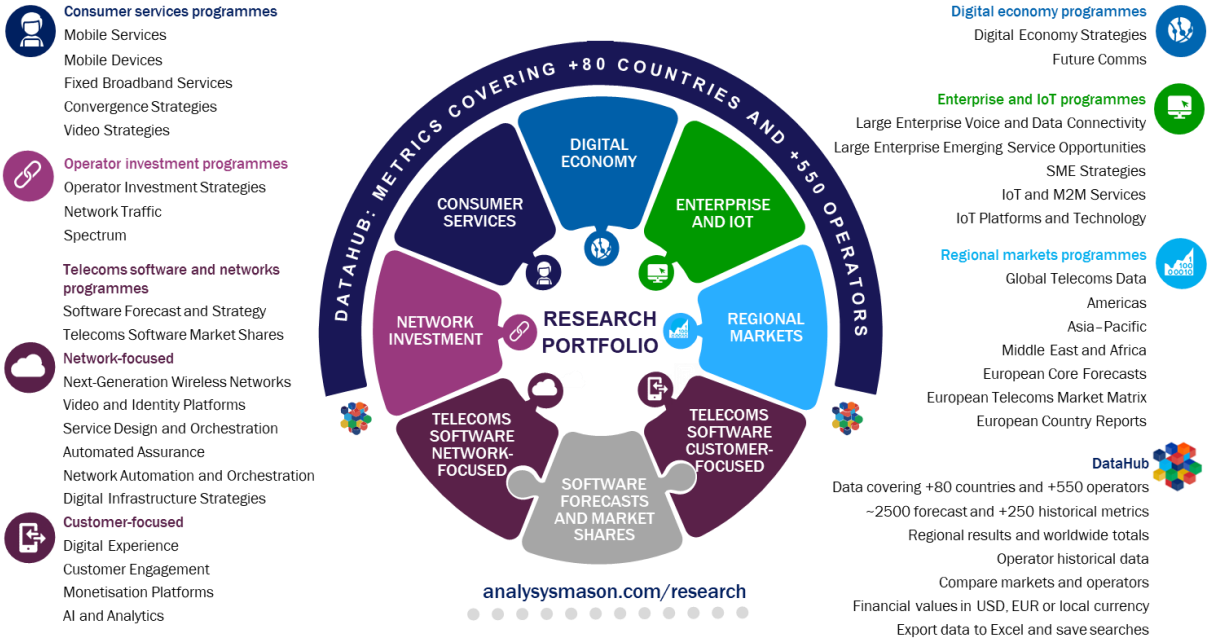
- Our dedicated team of analysts track and forecast the different services accessed by consumers and enterprises.
- We offer detailed insight into the software, infrastructure and technology delivering those services.
- Clients benefit from regular and timely intelligence, and direct access to analysts.

# Research from Analysys Mason

### We provide dedicated coverage of developments in the telecom, media and technology (TMT) sectors, through a range of research programs that focus on different services and regions of the world

The division consists of a specialized team of analysts, who provide dedicated coverage of TMT issues and trends. Our experts understand not only the complexities of the TMT sectors, but the unique challenges of companies, regulators and other stakeholders operating in such a dynamic industry.

Our subscription research programs cover the following key areas.




Each subscription program provides a combination of quantitative deliverables, including access to more than 3 million consumer and industry data points, as well as research articles and reports on emerging trends drawn from our library of research and consulting work.

### Our custom research service offers in-depth, tailored analysis that addresses specific issues to meet your exact requirements

Alongside our standardized suite of research programs, Analysys Mason's Custom Research team undertakes specialized, bespoke research projects for clients. The dedicated team offers tailored investigations and answers complex questions on markets, competitors and services with customized industry intelligence and insights.

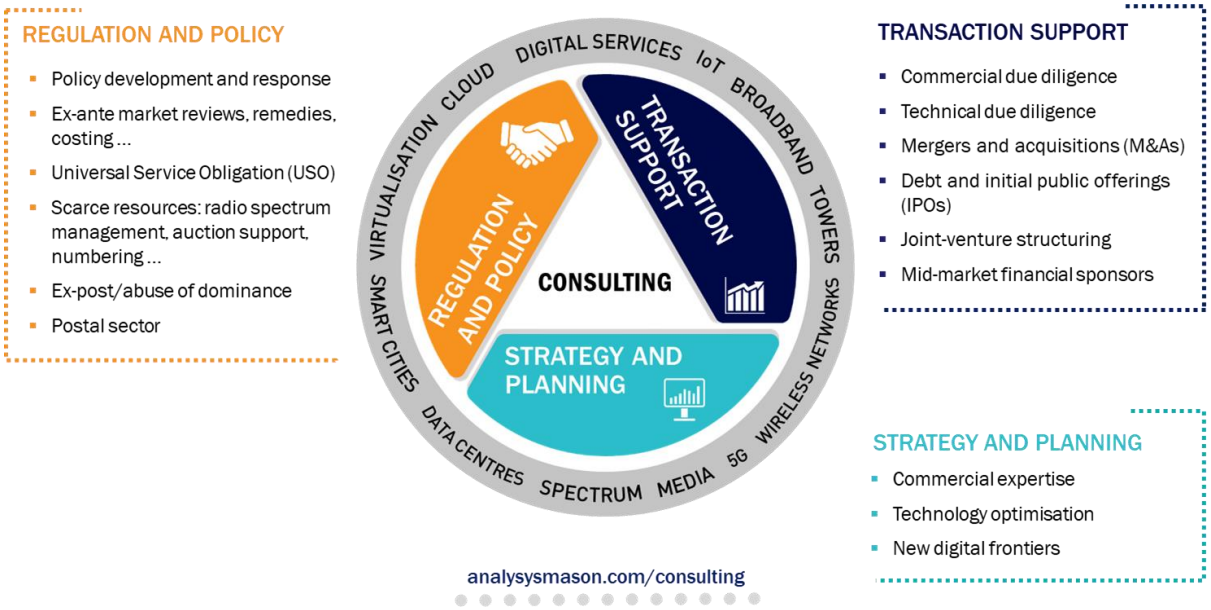
For more information about our research services, please visit www.analysysmason.com/research.

# Consulting from Analysys Mason

**For more than 30 years, our consultants have been bringing the benefits of applied intelligence to enable clients around the world to make the most of their opportunities**

Our clients in the telecom, media and technology (TMT) sectors operate in dynamic markets where change is constant. We help shape their understanding of the future so they can thrive in these demanding conditions. To do that, we have developed rigorous methodologies that deliver real results for clients around the world.

Our focus is exclusively on TMT. We advise clients on regulatory matters, help shape spectrum policy and develop spectrum strategy, support multi-billion dollar investments, advise on operational performance and develop new business strategies. Such projects result in a depth of knowledge and a range of expertise that sets us apart.




We look beyond the obvious to understand a situation from a client's perspective. Most importantly, we never forget that the point of consultancy is to provide appropriate and practical solutions. We help clients solve their most pressing problems, enabling them to go farther, faster and achieve their commercial objectives.

For more information about our consulting services, please visit www.analysysmason.com/consulting.