analysys mason

PERSPECTIVE

ASSURING 5G AND CLOUD EDGE APPLICATIONS

Michelle Lam and Justin van der Lande

NOVEMBER 2021

analysysmason.com

Contents

Analysys Mason Limited
North West Wing, Bush House
Aldwych
London WC2B 4PJ
UK
Tel: +44 (0)20 7395 9000

london@analysysmason.com

www.analysysmason.com

Registered in England and Wales No. 5177472

1 Executive summary

Next-generation 5G networks will have a huge impact on the telecoms industry because they provide communications service providers (CSPs) with new opportunities for digital transformation. 5G connectivity promises to support diverse industry use cases that have varying demands, such as service dynamicity, quality of service and latency requirements. In addition, enterprises across different industry verticals will demand specific service-level agreements (SLAs) based on differentiated services. These demands will introduce significant network and operational complexity, and present new challenges for CSPs to guarantee high-quality network performance.

The launch of 5G is a revolutionary point for CSPs to migrate from legacy networks to a disaggregated, virtualised, cloud-native infrastructure to support the delivery of new digital services. CSPs are deploying a service-based architecture for 5G networks that is enabled by network function virtualisation (NFV), software-defined networking (SDN), edge clouds and network slicing technologies. The delivery of 5G services using edge clouds will bring high-performance computing closer to the point of service in order to support low-latency and IoT applications for enterprise and consumer use cases.

To ensure high quality of service (QoS), CSPs must achieve real-time, end-to-end visibility across multiple network domains (core, transport, RAN) and across different cloud infrastructure (public, private, edge). As virtualised network functions (VNFs) are being migrated to public clouds, CSPs that rely on network and monitoring systems alone will lose insights into customer data and face challenges in identifying faults in application service performance.

Active assurance plays a key role in enabling end-to-end monitoring of application performance throughout the service network lifecycle. Always-on active testing solutions involve synthetically injecting test traffic into the network and use virtualised or containerised test agents, which allow CSPs to validate SLAs before and after service activation to guarantee a superior quality of service.

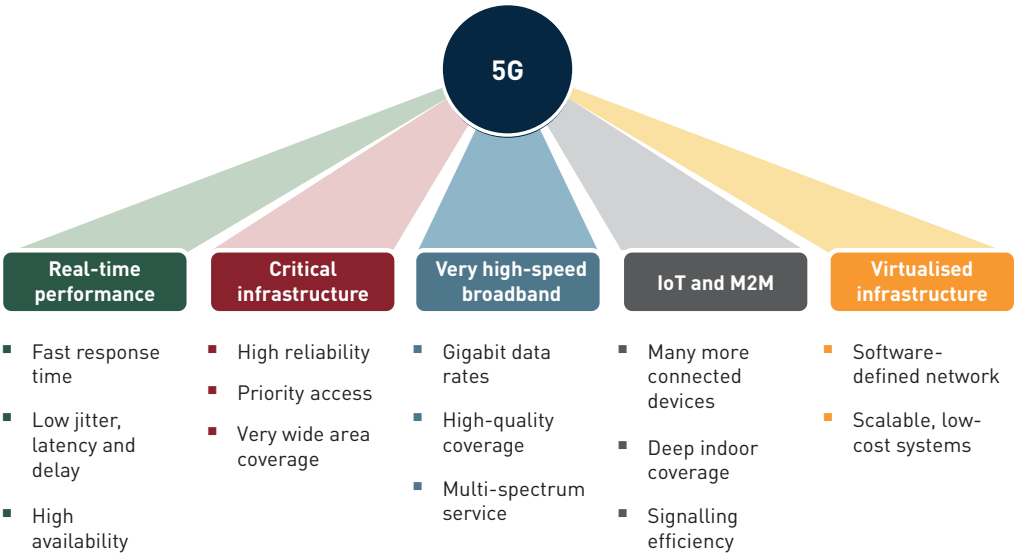
CSPs that deploy network automation with active assurance stand to benefit from real-time visibility of performance, automated testing and validation of VNFs in the edge cloud environments, and immediate identification and resolution of network issues before customer experience is affected.

Automated active assurance for 5G networks is vital for CSPs to enable closed-loop automation of key service assurance solutions, therefore maximising operational efficiency and agility in the provision and management of network services.

2 CSPs are looking to 5G as a network platform to enable network functions and support enterprise applications

The proliferation of new 5G use cases such as IoT, AR/VR and connected vehicles is driving enterprise and consumer demands for faster connectivity, greater bandwidth and ultra-low latency to support application connectivity requirements. The enhanced network capabilities that 5G delivers (see Figure 1) have created new opportunities for CSPs to provide edge cloud-enabled 5G networks that can be defined by service requirements and user experience, and to generate new revenue from enterprise and consumer services.

FIGURE 1: 5G KEY CHARACTERISTICS [SOURCE: ANALYSYS MASON, 2020–25]



2.1 5G will be a key enabler of digital transformation and new services

One of the main 5G strategies that CSPs are exploring is to deploy 5G as a network platform for providing a diverse range of services to industry verticals such as finance, manufacturing, healthcare and entertainment. As a result, operators and systems integrators are increasing their collaboration to develop new cloud networking and edge computing solutions to support the connectivity requirements of new 5G use cases.

The use cases for 5G multi-access edge computing (MEC) can be divided into internal and external use cases.

- **Internal use cases** consist of virtualising and distributing 5G core network functions to the edge for agile capacity planning, efficient capital allocation and dynamic memory/CPU utilisation during peak hours. MEC will also help CSPs in their O-RAN deployments by providing a cloud-native, multi-vendor platform to increase the flexibility and agility of network operations.
- **External use cases** provide low-latency connectivity and edge cloud capabilities such as storage and compute functions for consumer and enterprise applications that need them.

5G will support diverse consumer and enterprise use cases

Telecoms standards bodies have been working together on a list of 5G use cases that will support the digital transformation of consumer and enterprise services (see Figure 2).

These use cases can be classified into three generic categories:

- enhanced mobile broadband (eMBB)
- massive machine-type communications (mMTC)
- ultra-reliable and low-latency communications (URLLC).

"We are seeing quick wins with enterprise clients implementing a combination of private 5G and cloud computing to deliver industry-based use cases. These companies demand good network and service performance."

A senior manager at a Tier-1 operator in Western Europe

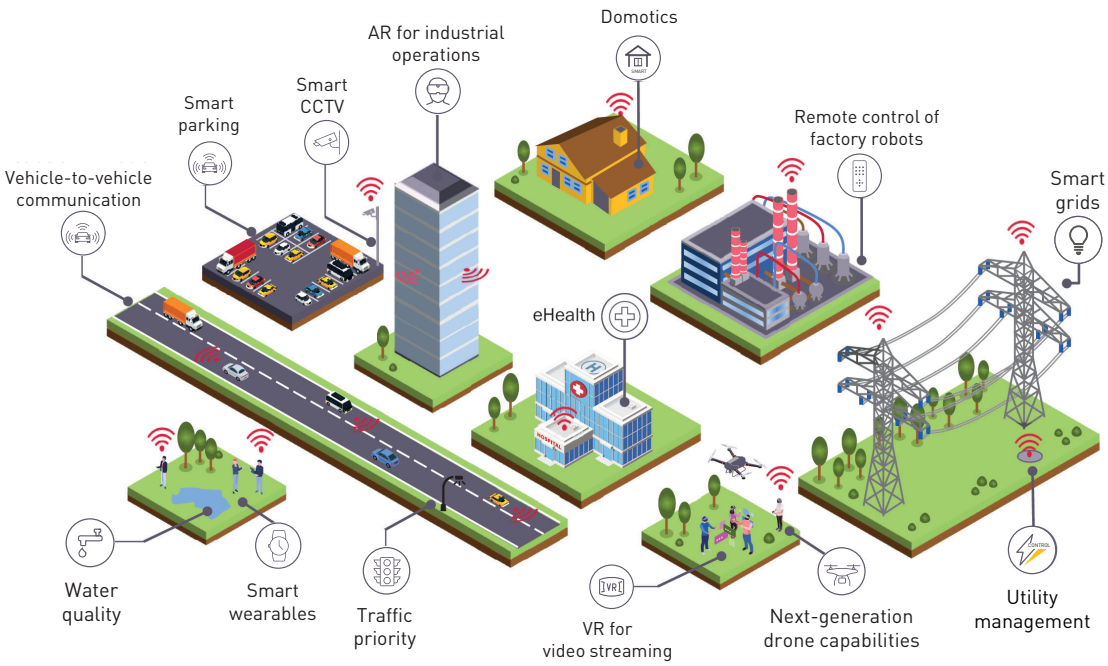
5G telco cloud

The deployment of a virtualised and cloud-native architecture has become a strategic focus for CSPs to achieve efficient, scalable and interoperable networks. CSPs have begun developing NFV, SDN and cloud-native computing solutions to rearchitect their core, transport and edge networks and improve operational efficiency. Cloud-native architecture is a requirement not only for 5G networks but also for deploying applications on top of those networks. Containerised infrastructure and NFV/SDN tools will enable CSPs to maximise their compute, storage and network resources as well as host virtualised network services on the cloud as microservice applications. These cloud-native applications will unlock the benefits of improved management, and orchestration and automation of networks, thus allowing CSPs to develop flexible operating models and deliver new digital services for enterprise and consumer applications, with enhanced QoS and quality of experience (QoE).

Edge clouds

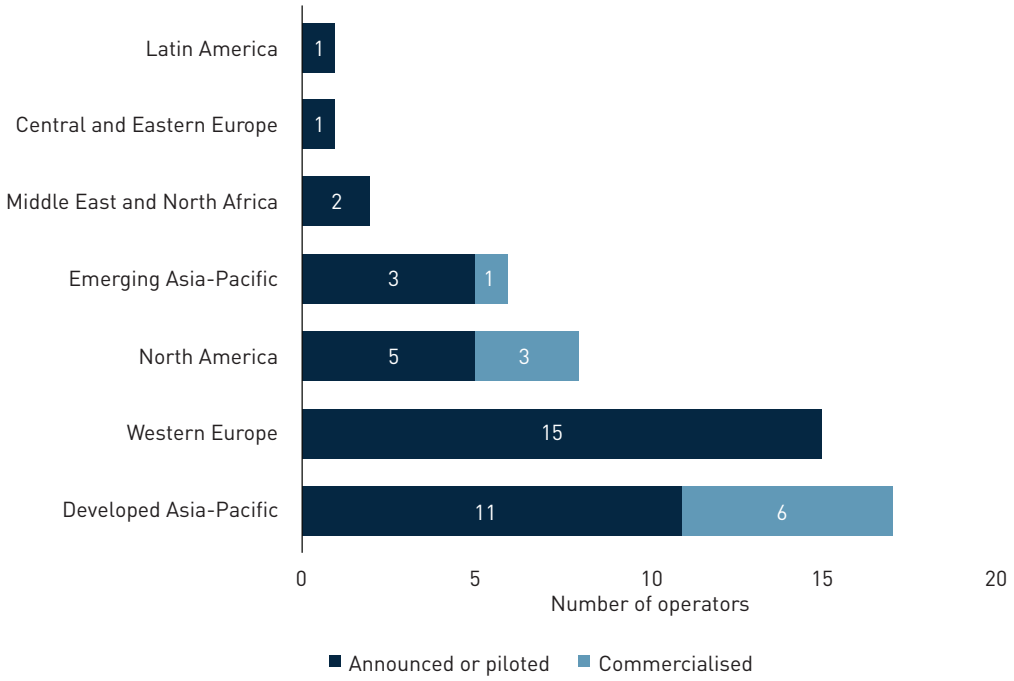
Edge clouds involve distributing cloud-enabled applications at the edge of networks to achieve ultra-low round-trip latencies of approximately 10ms as opposed to centralised cloud data centres which give latencies as high as 100ms. As edge computing brings data processing capabilities closer to end users, near real-time analytics can be performed to monitor latency-sensitive applications and ensure improved

FIGURE 2: OVERVIEW OF EMERGING 5G-ENABLED SERVICES [SOURCE: ANALYSYS MASON, 2021]



speeds and performance. Storing and processing data in multiple, highly distributed edge clouds also enables CSPs to scale their operations with more flexibility and lower transmission costs. CSPs worldwide are deploying edge clouds to support URLLC use cases in various industry verticals for enterprise and consumer applications such as IoT, video optimisation, warehouse robotics and autonomous vehicles (see Figure 3).

FIGURE 3: PUBLIC ANNOUNCEMENTS OF EDGE CLOUD OFFERS, BY TYPE AND REGION, WORLDWIDE, 1Q 2021 [SOURCE: ANALYSYS MASON, 2021]



2.2 Cloud delivery models

CSPs are exploring various cloud deployment strategies to reduce network infrastructure costs and introduce new revenue streams by launching a variety of enterprise services as part of their 5G roll-out plans. Three key edge cloud deployment strategies have been trialled worldwide as part of operators' digital transformations which include partnering with vendors to build their own private edge clouds, connecting to hyperscale public edge infrastructure with 5G and deploying hyperscale edge cloud platforms in a private cloud environment.

Cloud computing and network virtualisation company VMware unveiled its Telco Cloud Platform in 2020 to enable CSPs to streamline network operations and deliver 5G applications using their own private edge cloud. Similarly, Linux Foundation Edge established the EdgeX Foundry project to provide an open-source, vendor-neutral, interoperable framework for IoT edge computing that simplifies the process to design, develop and deploy solutions across industrial, enterprise and consumer applications.

CSPs worldwide have been partnering with hyperscalers such as AWS, Google and Microsoft to launch edge cloud offerings. In May 2021, Telefónica and Microsoft signed an agreement to jointly develop a private 5G network for Industry 4.0 solutions using the Azure Private Edge Zone. This collaboration will enable industrial clients to deploy 5G connectivity on premises over a secure network and boost the efficiency and performance of business operations. Swisscom is taking a similar approach by deploying its cloud-native core network on a hybrid cloud platform using its own private cloud infrastructure and AWS Outpost to bring AWS infrastructure, services, APIs and tools to virtually any on-premises facility.

CSPs could also tap into public cloud servers to deliver edge applications. For example, KDDI, SK Telecom, Telefónica and Verizon are deploying AWS Wavelength at the edge of their 5G networks to enable enterprises and developers to build and deploy ultra-low latency applications and deliver services closer to mobile devices and end users.

FIGURE 4: PARTNERSHIPS BETWEEN OPERATORS AND CLOUD PROVIDERS [SOURCE: ANALYSYS MASON, 2021]

Cloud vendor	Services	Key CSP partnerships
AWS	AWS Local Zones, AWS Wavelength, AWS Outpost	Dish, KDDI, Swisscom, SK Telecom, Verizon, Vodafone
Dell	Dell EMC Network Virtualization, Dell EMC PowerEdge, OneBox MEC	AT&T, DISH, Orange, SK Telecom, Vodafone
Google	Google Cloud Platform	AT&T, Bell Canada, BT Group, NTT Communications, Telecom Italia, Telefónica, Vodafone, Windtre
IBM	IBM Cloud Pak for Automation, IBM Cloud Satellite, IBM Edge Application Manager, IBM Telco Network Cloud Manager	AT&T, Bouygues Telecom, Telecom Egypt, Telefónica, Verizon
Microsoft	Azure Edge Zones, Azure Private Edge Zone	AT&T, Etisalat, Proximus, Rogers, SK Telecom, Telefónica, Telstra, Vodafone
VMware	Telco Cloud Platform	Deutsche Telekom, KDDI, Millicom Tigo, NTT Docomo, Orange, Rogers, Sky, Swisscom, T-Mobile, Telefónica

3 New-generation assurance solutions can address 5G and telecoms cloud complexity

The launch of 5G services will introduce new challenges in guaranteeing the quality of network performance as dynamic, cloud-native networks must host a diverse range of industry-specific use cases. These services will be distributed across multiple edge locations in the network, making the telco platform more complex to operate and assure.

3.1 Dynamic infrastructure and services

Dynamicity of networks and services is a key feature of virtualised and cloud-native networks. As CSPs roll out 5G wireless networks in multi-cloud platforms, end-to-end network slicing solutions are being implemented to deliver network as a service (NaaS) and create new revenue opportunities. These network slicing solutions leverage NFV and SDN to enable multiplexing of virtualized networks on a single, shared physical network, where each portion is dedicated to a specific customer service.

CSPs that are deploying virtualized network services should consider NFV-compliant, virtualized active testing solutions that feature run-time control and automation as part of the orchestration process. These orchestrated active test solutions deliver critical on-demand testing options to support the dynamic implementation of network functions and network slicing.

"As we are moving to cloud native, we are developing tracing capabilities into the platform layer. Now, we have two different environments in the network: traditional NFV and containerized functions that are running on the webscaler platform."

A director of network planning from a Tier-1 operator in North America

3.2 Distributed network functions and applications

A prominent use case for 5G is providing high-speed wireless connectivity to radio access networks (RAN). As NFV is increasing as part of telco digital transformation journeys, CSPs are looking to develop virtual radio access networks (vRAN) to monetise 5G investment. The migration of workloads to the cloud and the desire for architectural flexibility, vendor diversity and innovation has led to CSPs adopting open radio access network (Open RAN) initiatives to break away from monolithic architecture and vendor lock-in and deploy disaggregated, open-interface, multi-vendor, multi-domain RAN infrastructure.

"We had SLAs specific to level 1, 2 and 3 based on uptime and downtime. However, for Open RAN, the types of profiles and the level of involvement for each SLA needs to be changed. Specifically, we need to find a way to apply all the cloud-native continuous integration/continuous delivery (CI/CD) principles to facilitate component creation and use the old cloud-native monitoring stack to monitor some of the layers of Open RAN deployment."

A senior manager from a Tier-1 operator in Western Europe

This necessitates the deployment of real-time network traffic monitoring and active test systems to monitor network performance and guarantee service quality across different network domains. Next-generation assurance tools such as containerized active probes, OpenTracing and network telemetry can provide real-time user data in containerized 5G environments to help CSPs to gain an end-to-end view of the network and develop efficient solutions to monitor and troubleshoot their networks. CSPs must insist on an open solution that supports open APIs for easy integration with adjunct and third-party applications when choosing an active test solution.

3.3 Diverse, industry-specific use cases

5G edge clouds can provide high-speed, low-latency connectivity to support a wide variety of use cases in different industry verticals. Each use case has a distinct

set of network resources and topology with specified SLAs to meet the needs of individual applications.

Active assurance enables testing for 5G deployment configurations and slices before the network is live, and continuously monitors these configurations and slices to guarantee performance expectations. This provides CSPs greater flexibility and agility in delivering specialised services with diversified requirements across different network domains. Automated active testing options use containerised test agents to assure control plane/user plane separation (CUPS) technology enabling the control and user planes to be scaled independently of each other and allowing CSPs to host the user plane in edge clouds. This approach provides data centre and backhaul cost savings and supports new low-latency use cases.

4 Active assurance can play a pivotal role in assuring telco cloud and edge-based 5G services

The acceleration of 5G roll-out is a driver for CSPs to adopt an open and disaggregated network architecture based on cloud-native principles to scale their operations and support new protocols and services. The disaggregation of networking software from white box hardware will enable flexible 5G network deployments that are built on open interfaces to allow multi-vendor control over the management systems through open APIs.

As CSPs are disaggregating 5G edge networks and distributing new services across multiple edge locations, this increases the complexity of the network architecture and creates more challenges in guaranteeing network performance and isolating network issues.

4.1 Comparison of passive and active assurance methods

CSPs use two well-accepted service assurance methods to monitor the performance of their networks (see Figure 5).

FIGURE 5: COMPARISON OF THE BENEFITS OF PASSIVE AND ACTIVE ASSURANCE [SOURCE: ANALYSYS MASON, 2021]

Passive assurance	Active assurance
Collects live network data at specific points in the network.	Actively injects synthetic traffic to test and measure network performance.
Requires network traffic data to be available and requires comparison with historical data to be effective.	Network turn-up tests can be performed before live traffic data is available. Active tests are 'always on', proactively identifying and isolating faults.
Provides detailed network performance metrics such as signalling protocols, application usage or high-bandwidth consumers.	Emulates end users and provides real-time QoE metrics such as latency, jitter and packet loss on a per-service basis.
Probe data correlation is easily affected by network topology change, making it difficult to manage passive probing in dynamic SDN networks.	Automatically mimics the service as the network changes to optimise itself, without interrupting KPI generation.
Passive probes must be engineered into the network at key points to monitor traffic flow and do not affect the services.	Does not need to be engineered into the network as active probes are implemented as part of the service traffic.

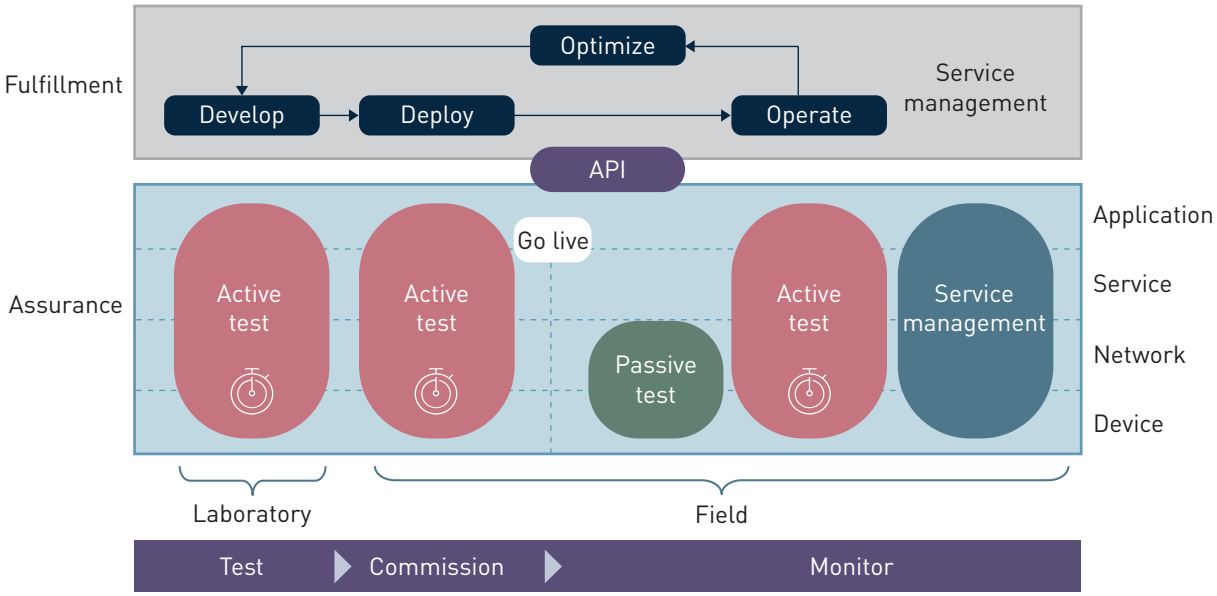
In **passive assurance**, physical probes are installed at key points in the network (for example, along the delivery chain, server sites, core/access networks, user's terminal) to capture, collect and analyse live traffic flowing through that point in the network. In turn, they generate KPIs on QoS-related network-level parameters such as latency, packet loss, jitter and throughput, and can detect faults in the network and trigger alarms.

On the other hand, **active assurance** involves generating small amounts of synthetic test traffic on the live network with the capability of emulating network functions and usage patterns using virtual test agents. The network service is observed and measured in response to the test traffic, and tests can be performed either one-way or round-trip, allowing CSPs to obtain an end-to-end view of the network. Since the test traffic is synthesised to mimic the service network,

active assurance provides real-time visibility into the service-level performance, making it the primary method for policing SLAs. This makes active assurance particularly well suited to testing and validating services that are delivered at the edge.

Active and passive assurance methods should be used concurrently to gain high-quality network performance and service quality insights. Active assurance is important for generating predictive data that can be used to monitor the service network and identify potential problems, validating VNFs and SLAs before service activation and maintaining real-time, end-to-end visibility of the network. Meanwhile, passive monitoring uses real performance data, which is crucial for understanding more detailed network data such as used bandwidth, application usage and signalling performance for deep troubleshooting and root-cause analysis (see Figure 6).

FIGURE 6: ACTIVE ASSURANCE LIFECYCLE [SOURCE: ANALYSYS MASON, 2021]



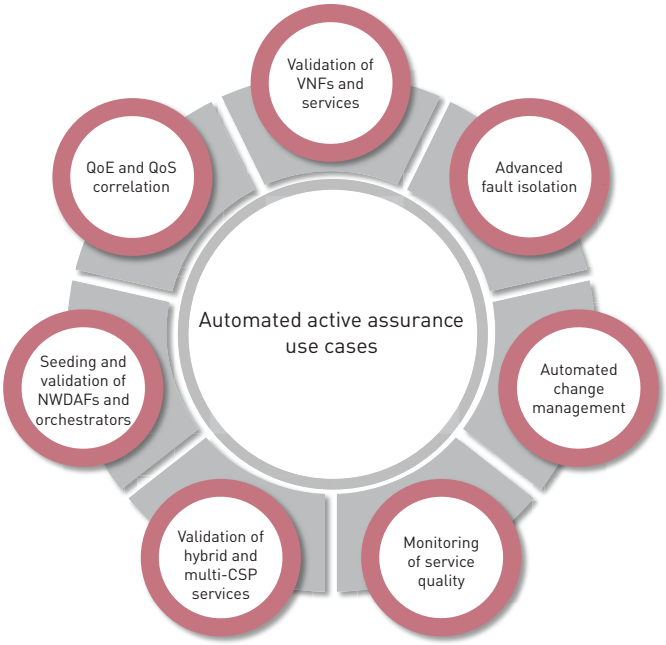
4.2 Automated active assurance use cases

CSPs are heavily investing in network automation to reduce operational costs and improve service agility in virtual and cloud-native networks. Automated active testing presents an early opportunity for CSPs to automate a plethora of service assurance processes, and provides end-to-end, real-time network performance and service quality insights that can be used for a variety of use cases such as:

- validation and certification of VNFs and services as they are instantiated and activated.
- seeding and validation of NWDAF predictions and network orchestration actions.
- validation of hybrid services that span across physical and virtual networks, or across multiple CSP network clouds.
- proactive monitoring of the quality of mobile, backhaul, voice and data services.
- advanced fault isolation and automated root-cause analysis to prevent network performance degradations.
- external and internal visibility to provide correlation between user perceived experience (QoE) and network-delivered performance (QoS).

CSPs should embrace automated active testing based on virtual and containerised agents, which enables assurance automation and provides insights to drive network and service automation.

FIGURE 7: AUTOMATED ACTIVE TESTING USE CASES THAT ENABLE NETWORK AUTOMATION [SOURCE: ANALYSYS MASON, 2021]



4.3 The value proposition for active assurance methods for edge cloud computing

5G standalone core will enable high levels of service modularity to support rapid provisioning of new, cloud-native network functions and services. Different network domains have different requirements and use different methods to generate and orchestrate network slices, and each domain requires an assurance approach that is specific to its needs. These network slices span across the access, transport and core networks, as well as edge and public clouds, therefore increasing the complexity of assuring end-to-end network quality.

A strong network and service assurance solution will benefit CSPs by enabling them to deliver superior performance and experience to their customers and differentiate themselves from market competition. CSPs are seeking to deploy service assurance platforms across the laboratory testing stage and the live network stages, which include deploying, managing and optimising the network. The platforms must also seamlessly integrate with the provisioning and orchestration systems that are responsible for automatically instantiating and activating network resources and services on demand. It is crucial for CSPs to efficiently manage new service delivery models and conduct testing for the different layers within the service framework to achieve faster identification and resolution of network anomalies before the service is affected.

Active assurance provides a new paradigm of network service assurance that leverages a CI/CD pipeline model to achieve faster time-to-market for the delivery of 5G edge cloud services. CSPs are using CI/CD pipelines to configure network operations into smaller, verifiable units in a DevOps environment and apply small incremental changes to network functions without the risk of affecting the entire network. By combining active testing methods with CI/CD processes, CSPs can simplify their network processes, rapidly introduce new network functions, and continuously validate virtual or physical network functions across different service requirements. This is essential for monitoring network slice KPIs and delivering contracted SLAs of the slices in a dynamically changing edge cloud environment.

Dynamic lifecycle management will be required for functions such as instantiation, configuration and test

script provisioning for the active test endpoints deployed in operational networks. To enable this, CSPs should demand test controller software along with the active test agents. The controller should also interface with NFV orchestrators to enable the automation of test and validation use cases as part of resource and service activation. CSPs must also insist on an open solution that supports open APIs for easy integration with adjunct and third-party applications when choosing an active test solution.

Furthermore, artificial intelligence/machine learning (AI/ML) capabilities can be embedded in automated active test solutions in order to spot trends and anomalies, and to predict the most-likely network and service issues based on the test data generated. CSPs should also combine their fulfillment and assurance solutions in an orchestrated closed loop for maximised benefits.

"At some point, we will evolve in the journey from resource orchestration to lifecycle management or individual level functions to service orchestration, and assurance has to be a part of that service. You also select the levels of assurance that are applicable for that particular service and gather the kind of characteristics of the level of assurance you want to perform."

A director of network planning from a Tier-1 operator in North America

5 Recommendations for CSPs

Automated active testing bolsters CSPs' overall network automation initiatives and supports a variety of use cases to achieve operations and service agility in NFV/SDN architectures for cloud-native 5G edge networks. To enable this, CSPs should make automated active testing a key part of their network automation strategies. Analysys Mason recommends that CSPs should:

- identify specific 5G edge use cases and develop automated active testing solutions to support a wide range of internal and external use cases.
- combine passive and active assurance to continuously monitor network performance by complementing the management plane data with data plane measurements based on synthetic traffic.
- incorporate AI/ML techniques into active assurance solutions to provide predictive assurance and automated root-cause analysis using real-time network and service topology, and network-slice topology.
- choose an active assurance solution that conforms to the principles of cloud-native design and open APIs, so they can be seamlessly integrated into their preferred network automation platforms.

6 Spirent's 5G assurance solution

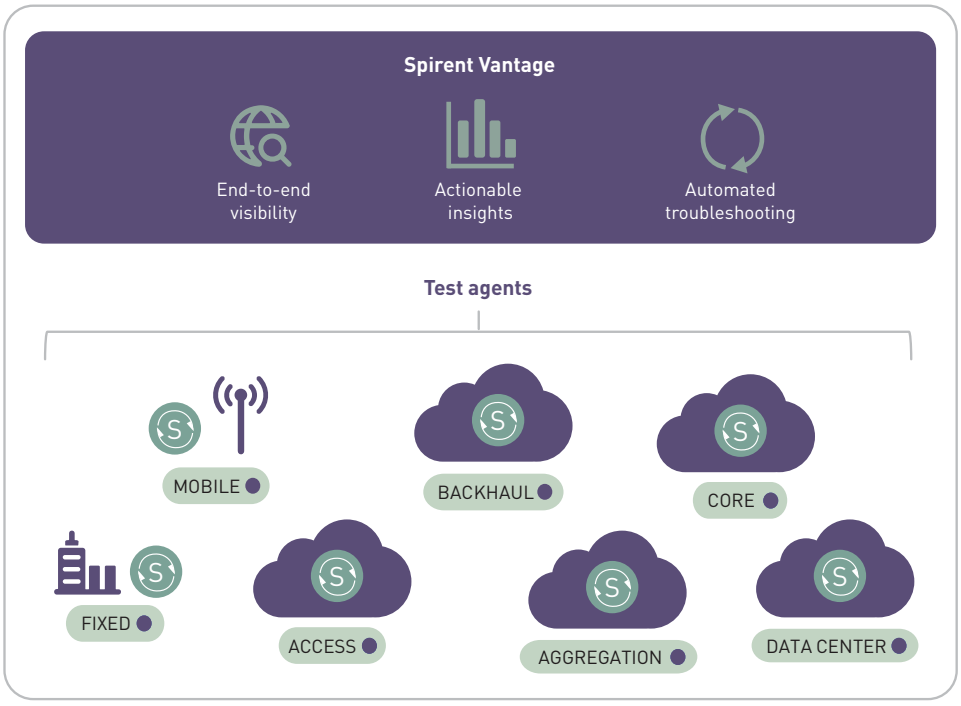
The Spirent Vantage 5G assurance solution enables operators to optimize performance with automated, end-to-end network, service, and experience assurance. With its network-aware mobility service assurance, operations teams get an at-a-glance visualization of where issues are happening before users are affected. Once identified, automated workflows guide users through intuitive and machine-learning-based data visualizations to isolate the causal domain and prescribe root-cause analysis (RCA) for remediation.

Vantage was built on Spirent's industry-leading assurance technology and is a next-generation service assurance solution that puts performance management into the hands of any operations team. Its features and capabilities include the following.

- **Easy to deploy and scale for testing on day one**. Consistent deployment paradigm for cloud-native agents supporting private, public, and hybrid cloud with pre-built test suites that are ready 'out-of-the-box' for on-demand and continuous testing.
- **Network-aware service assurance with expansive coverage**. Understand service performance in the context of the underlying network via test agents that are deployable in virtualized mobile core networks and over-the-air (OTA) RAN supporting 5G SA, 5G NSA, and 4G.
- **Layered visibility that can drill down to root-cause analysis (RCA)**. Provides custom visibility filters with overlays such as technology, region/market, or interfaces with intuitive and automated workflows that guide users from problem identification to RCA in three easy steps.

Spirent Vantage helps to protect subscriber experiences, avoid SLA violations, and deliver CSPs' 5G services.

FIGURE 8: SPIRENT VANTAGE 5G ASSURANCE SOLUTION [SOURCE: SPIRENT, 2022]



7 About the authors

Michelle Lam (Research Analyst) is a member of the Applications practice within the Telecoms Software and Networks research team in London. She holds a BSc in physics and an MSc in quantum technologies from University College London (UCL), where she was an academic representative to the Students' Union and assisted with research at the UCL Centre for Blockchain Technologies. She has also worked as a data analyst in machine learning and experimental physics, and has undertaken quantum computing research at the London Centre for Nanotechnology.

Justin van der Lande (Research Director) leads the Applications practice, which is part of Analysys Mason's Telecoms Software and Networks research stream. He specialises in business intelligence and analytics tools, which are used in all telecoms business processes and systems. In addition, Justin provides technical expertise for Analysys Mason in consultancy and bespoke large-scale custom research projects. He has more than 20 years' experience in the communications industry in software development, marketing and research. He has held senior positions at NCR/AT&T, Micromuse (IBM), Granite Systems (Telcordia) and at the TM Forum. Justin holds a BSc in Management Science and Computer Studies from the University of Wales.


5G
5G
5G
5G
5G

Stay connected

You can stay connected by following Analysys Mason via Twitter, LinkedIn and YouTube.


linkedin.com/company/analysys-mason


@AnalysysMason


youtube.com/AnalysysMason


analysysmason.podbean.com