White paper

Assurance built for the 5G era: delivering high-quality services in the next generation

December 2020

William Nagy and Anil Rao

Contents

List of figures

1. Executive summary

Communications service providers (CSPs) are rolling out 5G networks that will enable a wide array of use cases and innovative new services, many of which will support enterprises' critical business functions and needs. CSPs must therefore ensure that the quality of their networks and the services provisioned over them remain high and that they meet increased expectations. Assurance tools for 5G networks and services must be purpose-built with new and diverse monitoring solutions that can gather data from a variety of sources. Tools such as containerised probes, OpenTracing and network telemetry can provide highly granular and real-time data in containerised 5G environments. These monitoring solutions must also collect service data, which can be correlated with network data to gain a holistic and end-to-end view of the network from the customer's perspective, thereby enabling efficient troubleshooting and advanced automation capabilities.

Assurance solutions for 5G networks and services will need to have embedded machine learning/artificial intelligence (ML/AI). ML/AI will be needed to analyse, in real time, the reams of data streaming in from the network and it must be embedded at every layer in the assurance stack. This will enable the algorithms to be much more targeted towards the specific application and provide more robust insights and predictions of service quality. It will also create efficiencies in data processing and adaptation compared to systems that use external ML/AI. A library of ML/AI models will be required by network and service monitoring solutions to support different scenarios and services. This means that network engineers can select the most appropriate model for a particular use case. These models must be modular to enable simple replacements and updates to model components as they gain experience.

Assurance for 5G must be cloud-native and cloud-agnostic in order to enable CI/CD pipelines, DevOps processes and microservices-based solution architecture. CSPs are demanding solutions that support these concepts because they provide the agility that is needed to adapt to changing business requirements and customer demands. Vendors and CSPs must work together to reap the benefits of these consistent, collaborative implementation methodologies. They are critical to rapidly introduce new features and functions to the network and they create a lightweight, easy-to-manage network that will enable CSPs to quickly adjust the assurance framework to fit the needs of a particular service.

2. Assurance for 5G must be purpose-built in order to guarantee business-critical enterprise services

2.1 Assuring 5G network and service performance will become even more important as enterprises increasingly rely on connectivity services to achieve business goals

5G networks will support a variety of new use cases such as uRLLC, mMTC, eMBB and network slicing. These use cases will enable CSPs to provide innovative, differentiated and specialised services to consumers and enterprises. Examples of such services include support for self-driving cars, drones, emergency response services, AR/VR and Industry 4.0 initiatives.

Many of these new services will be critical to enterprise business functions and any disruption to them, no matter how slight, may lead to business disruption and lost revenue. Enterprise customers will have high expectations for the quality and reliability of these services. CSPs' approach to assurance must therefore evolve to meet these expectations if they are to maintain their reputations and remain competitive in a market where these services are highly valued.

The key areas of investment for CSPs that are in the assurance market are outlined in Analysys Mason's Automated assurance: worldwide market shares 2019 and Automated assurance: worldwide forecast 2020–2025. The three that are the most pertinent to 5G services are the evolution to a cloud-native assurance platform, ML/AI-based assurance and the end-to-end assurance of performance and service quality. CSPs' frameworks must deliver on these key areas to assure the reliability and speed of business-critical services.

2.2 New monitoring and assurance capabilities must be purpose-built for 5G SA

5G standalone (SA) networks have a higher level of operational complexity than previous mobile network generations. The SA core will be based on cloud-native, containerised architecture and will be orchestrated by an abstraction layer such as Kubernetes. Cloud-native networks are much more complex than physical, and even VM-based, networks.

The network will be formed of a container orchestration layer, which will encapsulate the container network functions. The underlying network architecture can be altered on-demand to optimise and adapt to the needs of the services deployed on it. CSPs have also started the journey towards vRAN, which will create further complexities and potential points of failure in the network.

Consequently, CSPs' approach to assurance must change for 5G; they must adopt a service-quality-oriented approach so that enterprise customers can receive a consistently high reliability and superior service experience. To achieve this, CSPs must expand the scope of their assurance solutions to include the monitoring of service quality KPIs and should correlate these metrics with other contextual customer metrics such as location, device type and subscriber type. The data must be processed in real time to generate rapid service insights, which will not only enable CSPs to manage the network and services in real time, but will also feed into higher-level analytics.

Containerised probes will enable real-time subscriber analysis and in-depth troubleshooting for 5G

Appliance-based network probes are a traditional and well-used method of gathering network data. However, software-based, cloud-native probes will be required to monitor 5G networks. Containerised probes are much more scalable and flexible than their appliance-based and virtualised predecessors. They are able to follow applications through container instances and can be instantiated on-demand as new services are activated.

CSPs will need to consider the network performance from the customer's point of view in order to completely understand the customer experience. Implementing containerised probes in their assurance solutions will provide visibility into the 5G cloud-native networks. Combining the network layer visibility of the cloud-native network with the higher service quality KPIs provides a holistic view of the customer experience. It also enables CSPs to pinpoint issues that affect customers directly and efficiently troubleshoot them.

A range of data sources is required to monitor 5G networks and services

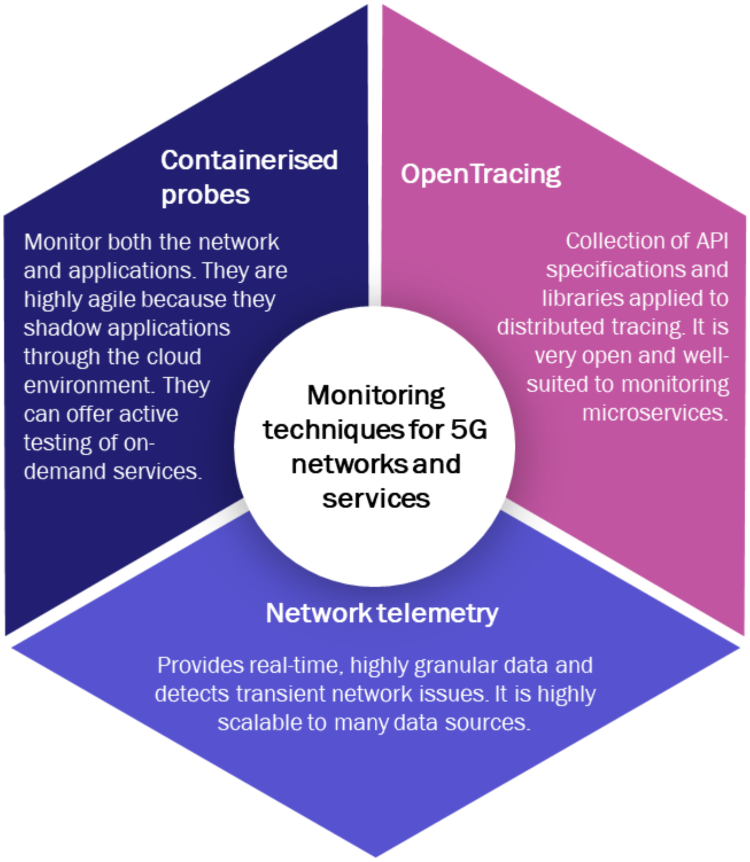
Network monitoring must evolve to use highly granular data if it is to support the agile nature of 5G cloud-native networks. A variety of data sources such as packets, events and event data records must be used to monitor the network and service status. Using a variety of data sources is critical to validate network events, service metrics and other customer data and to correlate these data to produce contextual insights. A combination of tools such as containerised probes, OpenTracing and network telemetry can be used to monitor and report these data in 5G containerised environments.

The industry is also moving towards the use of open and standards-based software architecture, such as OpenTracing and OpenCensus. The OpenTelemetry project has been formed from the merger of these two open-source projects. Industry adoption of these projects enables monitoring solutions to be highly standardised, open and interoperable, thereby creating a more simplified monitoring stack.

CSPs will develop new services on-demand and these services should be assured from the point of instantiation. This is key to assuring the customer experience from the very beginning. To achieve this, network monitoring solutions must be highly integrated with network and service orchestrators. The orchestrators need to interface with the monitoring solutions in order to synchronise the assurance solution with the service. CSPs can use tools such as containerised probes to address this use case because they are able to follow the network functions as they move within the 5G environment from the point of instantiation.

Data sources such as those depicted in Figure 2.1 will collectively generate reams of data to be ingested into data lakes for each network domain. These data lakes, together with the domain-level assurance modules that are unified by an end-to-end service assurance platform, will be critical to optimise operations in all levels of the network, as well as the services that run on top.

Figure 2.1: Monitoring techniques for containerised environments


Containerised probes
Monitor both the network and applications. They are highly agile because they shadow applications through the cloud environment. They can offer active testing of on-demand services.
OpenTracing
Collection of API specifications and libraries applied to distributed tracing. It is very open and well-suited to monitoring microservices.
Monitoring techniques for 5G networks and services
Network telemetry
Provides real-time, highly granular data and detects transient network issues. It is highly scalable to many data sources.

Source: Analysys Mason, 2020

3. Targeted, modular machine learning and artificial intelligence must be embedded into assurance solutions

ML/AI will be critical to achieve the operational scale and cost economics of managing 5G networks and services. These intelligent algorithms will be required to sift through the massive amount of service and network data that will be generated, make correlations between different data sources and detect faults and anomalies. This will not only enable real-time analysis, but it will free up network engineers to deal with more important and higher-level functions.

ML/AI will enable predictive operations by recognising the patterns that lead to degradations in service quality. Algorithms will make predictions potentially days in advance of any impact on customers; they will then be used to perform root-cause analysis and activate remediation routines to mitigate these impacts. This will be crucial for CSPs as they move to ensure that there is no lapse in business-critical service connectivity and that high service quality is maintained.

3.1 ML/AI must be embedded into assurance solutions in order to provide relevant insights and enable extreme automation

Assurance solutions must have built-in ML/AI in order for businesses to reap the full benefits. This is particularly important given the high expectations and complexities that will arise in the 5G era. Embedded ML/AI enables assurance solutions to use intelligence that is more targeted towards a specific application and functionality. For example, monitoring solutions must be able to identify both service issues and nascent trends and patterns that lead to drops in service quality. Embedded ML/AI also saves valuable computing resources compared to using an external intelligence system, thereby resulting in greater efficiency. Embedded systems can use data that has already been gathered by the monitoring solution, whereas an external ML/AI system would need to gather the data of its own accord.

ML/AI should be embedded hierarchically at every level of the assurance stack, from the data source management system to domain-level analytics and the higher-level end-to-end analytics layer. AI at every layer enables assurance to become more efficient. Each layer can take more-direct actions as dictated by more-specialised algorithms, instead of data having to be fed northbound and operational commands having to be sent back southbound. Domain-level assurance will allow the ML/AI-enabled analytics to be tailored to each individual domain and the domain orchestrator to take actions to maintain domain-level assurance KPIs.

Using ML/AI to automate analysis and remediation in the assurance domain is a key aspect of end-to-end network automation. Embedding ML/AI across all aspects of the assurance stack enables operational processes to be streamlined and intelligently automated at every point, without being bottlenecked by non-intelligent systems.

ML/AI must be modularised and implemented in online/offline scenarios and for specific use cases

ML/AI must be trained and used in both offline and online scenarios. In offline training, the reams of historical data collected in the data lakes is used to directly supervise and teach the algorithms to recognise faults, service quality degradations and the trends leading to them. The algorithms are then told directly which actions to take based on each event; these are configured as policy rules.

In the online mode, the trained ML/AI algorithms are applied to the real-time data to make predictions and produce recommendations. Engineers can evaluate the accuracy of the predictions, and can decide on the appropriate actions. However, once the engineers are confident with the predictions, they can then enable automatic decision making, with the only manual intervention being approving and denying automated decisions. This creates a feedback loop, which allows ML/AI to become more accurate over time.

A library of ML/AI models will be required by network and service monitoring solutions in order to support the range of different use cases and scenarios that services can be provisioned under. The selection of an appropriate model for each aspect of network monitoring is critical to success. The library should consist of preconfigured ML/AI models for generalised out-of-the-box use cases, as well as custom models that can be adapted by CSP software engineers to focus on specific or unique deployment scenarios. Models with specific domain expertise will reduce adaptation times and improve the quality of predictions and insights.

The models themselves must be modular in design, and specific model components and functionality must be separated into easily replaceable segments. Modularisation will make it easier to replace and update components because adaptations and improvements can be made as the model gains experience and increases its accuracy.

4. Vendors and CSPs must adopt DevOps and CI/CD processes to support an agile operating model

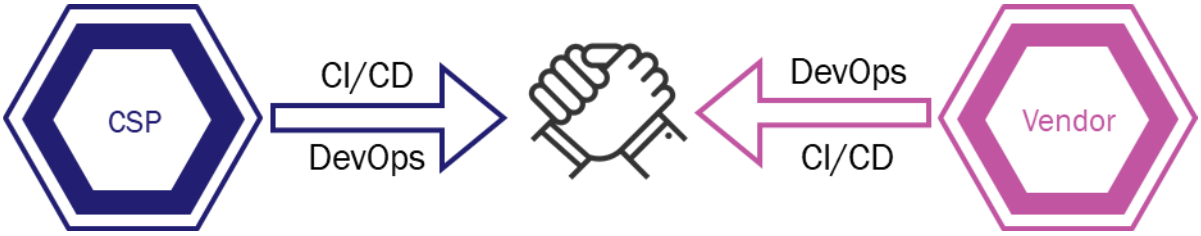
CSPs are increasingly demanding software solutions with DevOps, CI/CD pipelines and microservices-based architecture to give them the ability to rapidly introduce new features and functions. Such requirements are a major component of the digital transformation that they are undergoing to support 5G networks and services. They enable CSPs to adapt to changing business demands and objectives, as well as changing customer requirements. Network functions, such as the 5G cloud-native core functions, are expected to use these methods of development; it is therefore becoming essential for the supporting operational software (including assurance) to follow the same approach in order to keep pace with changes and adaptations in the network.

Cloud-native assurance solutions must support these agile pipelines and operations. In addition, they must become cloud-agnostic so that they are deployable in multi-cloud environments (be it public, private or hybrid cloud), with the ability to be orchestrated across the hybrid environment.

The industry is coalescing around using microservices to build solutions. Microservices are a step away from the monolithic, rigid software stacks that were traditional in telecoms software, and instead offer solution functionality as a lightweight, modular service. The microservice operating model enables CSPs to add and remove functionality as needed, and allows solutions to scale at a microservice level in containerised environments such as the 5G core.

DevOps delivery is another component that enables an agile, CI/CD operating model. It allows solutions to be tailored to specific implementations and use cases, and greatly reduces the time to deployment. DevOps methodologies can be implemented in a variety of ways depending on the CSP’s expertise and needs, but these rapid development and implementation models are most effective when both the vendor and the CSP are ready and engaged in the process. A collaborative effort between the vendor and the CSP will be the pinnacle of solution implementation (Figure 4.1). Co-development and synergised timelines for updates and adaptations will result in the most time- and cost-efficient solution implementations and will allow CSPs to keep pace with changing network function service demands and network requirements.

Figure 4.1: DevOps and CI/CD must be a collaborative process



Source: Analysys Mason, 2020

Rapid development and the ability to dynamically adapt assurance solutions is critical for on-demand 5G services. CSPs must be able to adapt and optimise the monitoring for all new services that are instantiated on the network. The adoption of cloud-native solutions, microservices, DevOps and CI/CD by vendors and CSPs will enable the rapid deployment of new, specially developed assurance solutions in a light, easy-to-manage framework.

5. Conclusion

Assurance for the 5G networks and services that CSPs will be operating must be purpose-built. This will require CSPs to use a variety of new, cloud-native monitoring techniques in order to gain an end-to-end view of the network and services. They must also employ use-case-specific ML/AI to generate accurate service quality predictions.

CSPs need to adopt monitoring tools such as OpenTracing, network telemetry and containerised probes to monitor the dynamic, containerised environments requiring assurance. They will provide highly granular data and can be instantiated along with services to provide monitoring from the outset. These tools will gather a wide range of data such as service metrics and data about network events, which can be correlated and combined with contextual customer data to create an end-to-end view of the service.

Vendors should embed ML/AI in their assurance solutions because these algorithms will play a central role in assuring critical services on 5G networks. ML/AI will sift through the masses of data to analyse and predict service quality degradations and perform automated remedial actions. ML/AI must be embedded in every layer of an assurance solution, and there should be a library of models that can be trained in offline scenarios and executed in online conditions. This will ensure that each ML/AI model is specialised and attuned to the use case in question.

Vendors and CSPs should use DevOps and CI/CD to deliver and develop assurance solutions. To do so, the solutions must be cloud-native and cloud-agnostic so that they can be rapidly provisioned over the CSP's preferred cloud environment. Microservices-based solution architecture will enable a lightweight and agile approach to building an assurance stack and, when combined with DevOps, will enable vendors and CSPs to rapidly on-board and tune solutions towards specific service needs.

.

6. About the authors

Anil Rao (Principal Analyst) is the lead analyst on network and service automation research that includes the *Network Automation and Orchestration*, *Automated Assurance* and *Service Design and Orchestration* research programmes, covering a broad range of topics on the existing and new-age operational systems that will power operators' digital transformations. 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. 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.

William Nagy (Analyst) is a member of the *Telecoms Software and Networks* research team in London, contributing to various research programmes with a focus on *Automated Assurance*, *Service Design and Orchestration* and *Forecast and Strategy*. He previously worked with the regional markets team. William holds a BSc in Physics from Queen Mary University of London.

This whitepaper 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 and Wales No. 5177472

Analysys Mason Limited maintains that all reasonable care and skill have been used in the compilation of this publication. However, Analysys Mason Limited shall not be under any liability for loss or damage (including consequential loss) whatsoever or howsoever arising as a result of the use of this publication by the customer, his servants, agents or any third party.