Probe systems will continue to play an important assurance role in the 5G era

October 2023

Dennisa Nichiforov

Assurance plays a critical role in the 5G context

The primary purpose of 'real' 5G (as opposed to 5G technology that has been bolted onto a 4G core) is to serve the needs of multiple industry verticals. Unlike previous generations of technology, 5G empowers communications service providers (CSPs) to perform a range of new operations, including dynamically setting quality of service (QoS) capabilities for different applications and efficiently optimising specialised network configurations and optimal network resources. CSPs can also use 5G's increased data exposure and analytics capabilities to gain valuable insights into network performance and customer behaviour. This data-driven approach can inform service development and optimisation.

To monetise the opportunities afforded by 5G, CSPs must ensure that their QoS requirements are achievable and sustainable. CSPs are no longer focused purely on how the network is functioning. Instead, CSPs are increasingly aiming to improve service quality and the end-to-end customer experience.

The new services enabled by 5G and their associated service level agreements (SLAs) will pose a challenge for current assurance systems, which currently focus on network performance rather than services. However, assurance capabilities in the 5G era will need to evolve to enable an end-to-end view of the network and the services running on top of it. As a result, probing will continue to play a critical role within the multitude of assurance processes.

Probe systems will play a more-important role in the 5G era

Probe systems perform many important roles as part of the assurance process, particularly in terms of their ability to provide an 'independent' view of the network and the services that run on top of the networks. Probe systems can also generate distinct datasets from traffic analysis to enable CSPs to perform detailed troubleshooting. For example, CSPs can use probes to analyse and troubleshoot traffic at different levels: per network element, per service, per customer or at session level. Network engineers use this information to understand how traffic flows through the network and to identify where degradations occur and where to troubleshoot. Put simply, probes watch all the traffic that flows through the network and then correlate the data into subscriber sessions to understand the overall service performance and to enable end-to-end network troubleshooting.

Probe systems have undergone a complex transformation

The complexity of 5G standalone (SA) has altered the traditional probes market. Alternative monitoring methods have been developed to meet the needs of 5G SA, but probes remain at the core of service assurance because of their ability to provide actionable insights and to independently assess network quality.

Probe systems have been transformed in the following ways.

- Probes are becoming software-based rather than hardware-based in line with the softwarisation of networks. This transition to software-based probe systems means that probes can now be deployed where needed and at virtually any time when a new issue arises. They can also be redeployed based on the needs of customers and the service life cycle, which simplifies the management of the probe process.
- Containerised probes support the deployment of containerised assurance solutions, which are controlled by Kubernetes.
- Active testing/probing is moving onto live networks where it can validate specific network or service elements or generate predictive data that can be used to monitor the network or service and identify problems to enhance predictive analysis.

Analysys Mason has reviewed its definition of probes

In line with the above developments, we have updated our definition of probe systems and renamed the probe systems sub-segment within our Automated Assurance taxonomy. These changes align with our research and help to provide a clearer understanding of the remit of this sub-segment, and also reflect the changes that have been taking place over the past few years.

Figure 1: Updates to the definition of the probe systems sub-segment in the automated assurance taxonomy

Old definition	New definition
Probe systems are a combination of hardware and software. Hardware devices are put into the network to either passively monitor signalling and data sessions, or to remotely test specific types of technology.	**Data acquisition, validation and analysis systems (DAVA)** Data acquisition systems provide sensor data through dedicated network appliances or network hosted software applications that independently gather performance data about the network or the services running over them. Sensor devices or applications are deployed in a network to either passively monitor signalling and data sessions or to actively validate specific network or service elements. Passive monitoring is achieved by deploying sensors at key points in the network to acquire and analyse live traffic flowing through that point in the network, generating KPIs on QoS-related network-level parameters (latency, packet loss, jitter and throughput) and can detect faults and trigger alarms. Active monitoring involves injecting small amounts of synthetic test traffic with the capability of emulating network functions and usage patterns. This process generates predictive data that can be used to monitor the service network and identify potential problems validating virtual network functions (VNFs) and SLAs before service activation and maintaining real-time, end-to-end visibility of the network.