Assuring 5G: operators should take a four-pronged approach to automated assurance

February 2018

Anil Rao

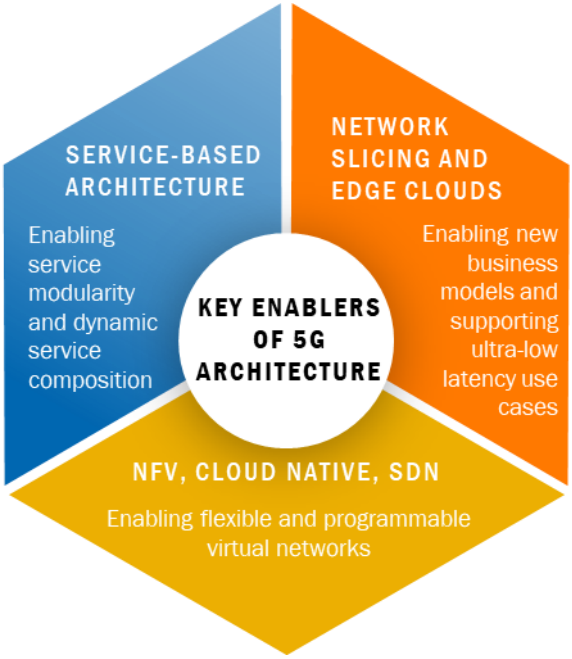
5G promises to support diverse industry use cases with varying demands such as service dynamicity, quality of service and latency requirements, which cannot be achieved using traditional physical networks and rigid network architecture. The industry has coalesced around service-based architecture (SBA) for 5G, which will be enabled by network functions virtualisation (NFV), cloud-native computing (CNC) and software-defined networking (SDN). 5G networks will also incorporate edge clouds and network slicing technology; edge clouds will bring high-performance computing closer to the point of service use to support low-latency and Internet of Things (IoT) use cases, while network slicing will offer quality of service (QoS) and service-level agreements (SLAs) based differentiated services to enterprises Together, these technology innovations enable communications service providers (CSPs) to transform their network into a digital infrastructure platform for agile service innovation, both for CSPs and third parties.

On the flipside, these innovations and the diverse service demands introduce significant network and operational complexity. CSPs must implement high levels of network automation to tackle this 5G complexity and keep operational costs in check. An assurance-led network automation approach can help CSPs to operationalise 5G at scale.

5G networks will require high levels of network automation to tackle the network and operational complexity

The introduction of the SBA, NFV, CNC and SDN-based networks for 5G, and further supported by edge clouds and network slicing will make 5G networks significantly more complex than those of previous generations. The radically different, dynamic and complex architectural approaches that underpin 5G will require high levels of network automation to achieve the intended scale and impact of 5G.

Figure 1: The key architectural enablers for 5G



Service-based architecture (SBA) brings IT concepts to 5G networks

SBA bolsters the 5G network to use open APIs for dynamic interlinking of network functions to create service chains, which enables rapid service innovation and cuts the service creation timescale to minutes. Furthermore, the SBA allows the network capabilities of the 5G core to be exposed to third parties, transforming CSPs into innovation enablers and supporting new business models (for example, B2B2C). A Tier 1 European CSP shared its approach for new 5G-enabled services.

> ***We plan to explore a small number of 5G services under a B2C model, offered directly to the end customer. The majority of 5G services will be launched by third parties leveraging our platform under a B2B2C model.***
>
> ***- Tier 1 CSP in Europe***

Edge clouds and network slicing will bolster critical 5G use cases

5G-enabled services leveraging mMTC and URLLC capabilities cannot be delivered through the traditional networking approach. These services will require new technologies: multi-access edge computing (MEC) to bring computing resources closer to the edge; and network slicing to offer a guaranteed quality of service (QoS) and differentiated service-level agreements (SLAs) for different industries, users or services.

Together with the SBA, edge clouds and network slicing allow CSPs to use the 5G network as a highly automated cloud platform to deliver mission-critical use cases with differentiated QoS. It will bolster CSPs' ability to deliver service innovation rapidly and will enable external innovation through the B2B2C business model.

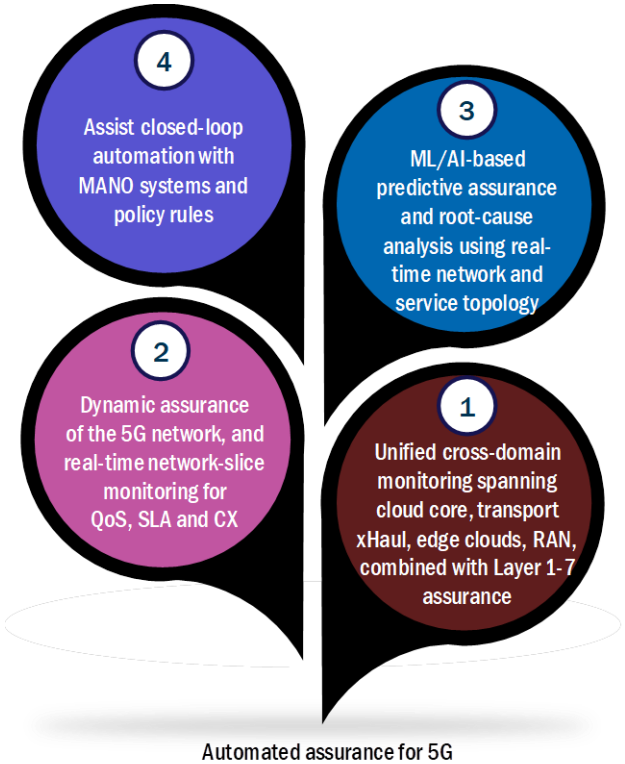
NFV, CNC and SDN are pivotal to realise the vision of 5G

NFV and CNC are the fundamental building blocks for a flexible, dynamic, programmable and highly automated cloud-native network, replacing the traditional physical networks with pre-defined interfaces. NFV will allow CSPs to achieve higher network efficiency through optimum resource utilisation, while CNC technologies such as containers and microservices prepare the network to be deployed in the cloud. SDN enables centralised traffic management capabilities to optimise service delivery, reduce network costs and improve the customer experience. With these capabilities, CSPs will be able to create and modify network resources to reflect the changing service requirements on-demand.

A four-pronged automated assurance approach will bolster CSPs' ability to automate 5G networks

Service assurance systems will play a pivotal role in enabling network automation. For decades, assurance systems were mainly deployed for network validation, and fault and performance issue reportage, leaving the expensive and often manual task of performing root-cause analysis and issue resolution to engineers in the network and operations departments. In its new incarnation for 5G, assurance systems will take on the role of the operational 'nervous system' responsible for driving the network automation and lifecycle management of the 5G services. We recommend that CSPs take a four-pronged approach to automated assurance for 5G (see Figure 2).

Figure 2: Key pillars of automated assurance for 5G



1. **Unified cross-domain assurance including application performance monitoring.** The current approach to service assurance is based on siloed systems and processes with rigid software architecture and custom integrations across functions, which cause poor automation and rely on manual, repetitive and error-prone processes. CSPs must accept the idea of end-to-end cross-domain assurance for 5G that

spans all aspects of the network, from the cloud core to the customer, including the backhaul, edge clouds, front haul and 5G New Radio. Furthermore, the solution must also incorporate Layer 1–7 monitoring including the application layer, which is going to be essential to guarantee the service performance for enterprises. CSPs may consider a unified monitoring solution based on a combination of active and passive probes, in software, virtual and cloud-native formats to achieve maximum coverage and impact.

2. **Dynamic monitoring of the 5G network and network slices to guarantee QoS, SLAs and customer experience.** Assurance in static networks tends be an afterthought, often considered only at the last stage in the investment cycle before handover to operations. This approach is not fit for purpose for the 5G era where the VNFs (or cloud-native NF) and service instances can be created and altered on-demand including dynamic traffic-flow changes based on SDN policies. Assurance systems must adapt and, if required, scale in line with the changing network, to monitor the portable VNFs and the modified service chains. For instance, it is likely that the user plane VNFs will move to the edge cloud to support an URLLC use case – in this case, an assurance end-point, such as virtual probe, must be instantiated if it does not already exist and situated in the service chain along with the VNF in the edge cloud to capture the associated network performance data.

3. **Machine-learning (ML) and artificial intelligence (AI)-based predictive assurance and root-cause analysis.** CSPs must bolster the end-to-end monitoring and dynamic assurance capabilities with machine learning and artificial intelligence capabilities. The ability to allow software programs and algorithms to learn insights and relationships by applying ML techniques means analytics can be applied to human-intensive operational use cases such as complex root-cause analysis routines. A key prerequisite for performing highly accurate ML-based root-cause analysis and predictive assurance, is that the ML algorithms must have an accurate view of the network and service topology, and fully correlated network slice topology. For instance, large enterprises are concerned about using NFV-based services because the portable nature of network functions would make it difficult to guarantee quality of service. To address such concerns, CSPs must use a one true source of real-time topology that provides the basis for root-cause analysis and associated assurance processes.

4. **Assurance-assisted closed-loop automation with MANO.** The focus of the traditional assurance approach has been largely unidirectional – that is, process the network events and present the fault and performance data for visualisation via dashboards and reports. Following this processing, operations personnel would analyse the outputs and manually execute a workflow of steps to identify the root causes of the performance and service degradation, and manually carry out the actions to rectify the network issues through configuration changes. Closed-loop automation seamlessly integrates the two sets of processes by triggering policy-driven network changes through the MANO systems such as NFV orchestration, SDN control and multi-domain WAN configuration.